Recommendations

- Huawei Talent Online Website
  - https://e.huawei.com/en/talent/#/
- Huawei e-Learning
  - https://e.huawei.com/en/talent/#/search?productTags=&productName=&navType=learningNavKey
- Huawei Certification
  - https://e.huawei.com/en/talent/#/cert?navType=authNavKey
- Find Training
  - https://e.huawei.com/en/talent/#/halp/home?navType=halp

Copyright © Huawei Technologies Co., Ltd. 2021.

Huawei Certification

HCIA-Datacom



Huawei Technologies Co.,Ltd.

Copyright © Huawei Technologies Co., Ltd. 2021. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

 and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Certification

HCIA-Datacom

V1.0

Preface

Introduction

This document is a training material for HCIA-Datacom certification. It is intended for personnel who want to become datacom engineers and those who want to obtain the HCIA-Datacom certification.

Content

This document consists of eleven modules, covering basic datacom knowledge, including routing, switching, and network services.

Module 1 Introduce basic concepts of data communication, network reference model, and Huawei VRP basics.

Module 2 Introduce IP routing basics, including IP network address planning, static route and OSPF.

Module 3 Introduce the working process and principles of switches, and describe the STP/RSTP in detail.

Module 4 Introduce network security and network access basics, including ACL, AAA and NAT.

Module 5 Introduce TFTP, FTP, DHCP and HTTP.

Module 6 Introduce basic concepts of WLAN, the common networking mode, and basic WLAN configuration.

Module 7 Introduce WAN technology basics and working principles of PPP.

Module 8 Introduce basic concepts of the NMS and O&M, including SNMP and SDN-based NMS and O&M.

Module 9 Introduce IPv6 basics.

Module 10 Introduce Huawei SDN and NFV solutions, network programming and automation.

Module 11 Introduce campus network architecture and construction practice.

Contents

Data Communication Network Basis 1

Network Reference Model 32

Huawei VRP 76

Network Layer Protocols and IP Addressing 123

IP Routing Basics 167

OSPF Basics 219

Ethernet Switching Basics 268

VLAN Principles and Configuration 311

STP Principles and Configuration 361

Inter-VLAN Communication 422

Eth-Trunk iStack and CSS 451

ACL Principles and Configuration 499

AAA Principles and Configuration 530

Network Address Translation 552

Network Services and Applications 584

WLAN Overview 634

WAN Technologies 717

Network Management and OM 773

IPv6 Basics 811

Introduction to SDN and NFV 852

Network Programmability and Automation 904

Typical Campus Network Architectures and Practices 938



Data Communication Network Basis

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- Communication has always been with us ever since the origin of human society. Communication has been playing an increasingly important role especially since human society entered the information era in the 1970s or 1980s.
- The communication mentioned in this course refers to the communication implemented through a data communication network. This course describes the concepts related to communication and a data communication network, information transfer process, network devices and their functions, network types, and typical networking. In addition, this course briefly introduces the concepts related to network engineering and network engineers.

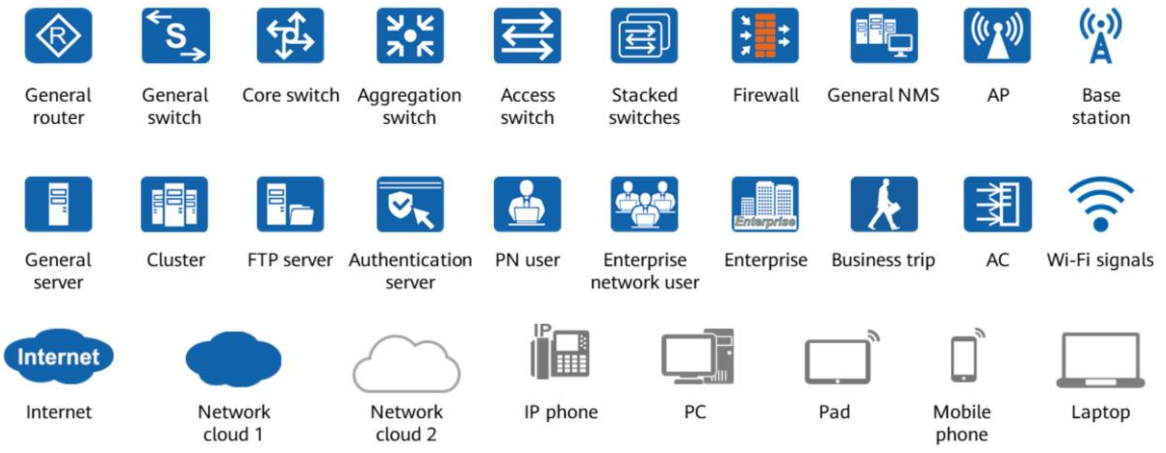
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand the concepts related to communication and a data communication network.
  - Be able to describe the information transfer process.
  - Differentiate network devices of different types and understand their basic functions.
  - Understand different network types and topology types.
  - Understand the concepts related to network engineering and network engineers.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Huawei Device Icons



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Contents

1. **Communication and Networks**
2. Network Types and Topology Types
3. Network Engineering and Network Engineers

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Concept of Network Communication

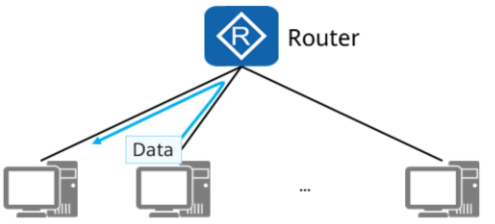
- Communication refers to the information transfer and exchange between people, between people and things, and between things through a certain medium and behavior.
- Network communication refers to communication between terminal devices through a computer network.
- Examples of network communication:



A. Files are transferred between two computers (terminals) through a network cable.



C. A computer (terminal) downloads files through the Internet.



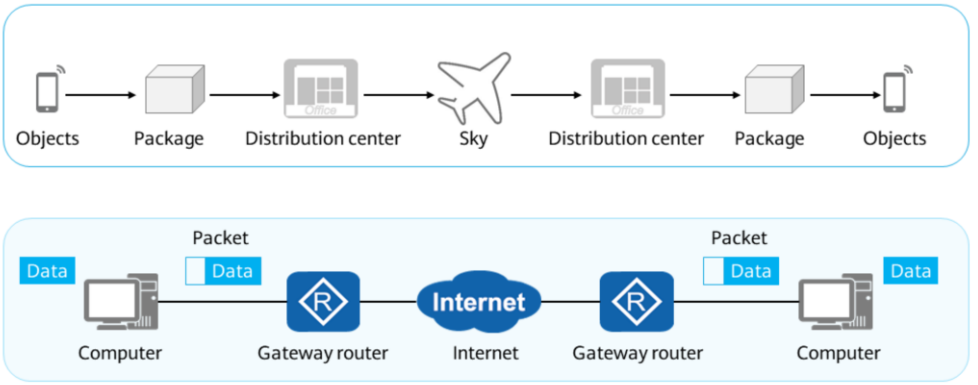
B. Files are transferred among multiple computers (terminals) through a router.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Examples of network communication:
  - A. Two computers connected with a network cable form the simplest network.
  - B. A small network consists of a router (or switch) and multiple computers. In such a network, files can be freely transferred between every two computers through the router or switch.
  - C. To download a file from a website, a computer must first access the Internet.
- The Internet is the largest computer network in the world. Its predecessor, Advanced Research Projects Agency Network (ARPAnet), was born in 1969. The wide popularization and application of the Internet is one of the landmarks of the information age.

Information Transfer Process

- Virtual information transfer is similar to real object transfer.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Comparison between express delivery (object transfer) and network communication:
- Objects to be delivered by express delivery:
  - The application generates the information (or data) to be delivered.
- The objects are packaged and attached with a delivery form containing the name and address of the consignee.
  - The application packs the data into the original "data payload", and adds the "header" and "tail" to form a packet. The important information in the packet is the address information of the receiver, that is, the "destination address".
  - The process of adding some new information segments to an information unit to form a new information unit is called encapsulation.
- The package is sent to the distribution center, where packages are sorted based on the destination addresses and the packages destined for the same city are placed on the same plane.
  - The packet reaches the gateway through the network cable. After receiving the packet, the gateway decapsulates the packet, reads the destination address, and then re-encapsulates the packet. Then, the gateway sends the packet to a router based on the destination address. After being transmitted through the gateway and router, the packet leaves the local network and enters the Internet for transmission.
  - The network cable functions similarly as the highway. The network cable is the medium for information transfer.

- Upon arrival at the destination airport, packages are taken out for sorting, and those destined for the same district are sent to the same distribution center.
    - After the packet reaches the local network where the destination address resides through the Internet, the gateway or router of the local network decapsulates and encapsulates the packet, and then sends the packet to the next router according to the destination address. Finally, the packet reaches the gateway of the network where the destination computer resides.
- The distribution center sorts the packages based on the destination addresses. Couriers deliver packages to recipients. Each recipient unpacks the package and accepts the package after confirming that the objects are intact, indicating that the whole delivery process is complete.
    - After the packet reaches the gateway of the network where the destination computer resides, the packet is decapsulated and encapsulated, and then sent to the corresponding computer according to the destination address. After receiving the packet, the computer verifies the packet. If the packet passes the verification, the computer accepts the packet and sends the data payload to the corresponding application for processing, indicating that the network communication process ends.

Common Terms

Term	Description
Data payload	Information conveyed
Packet	Data unit switched and transmitted on the network
Header	Information segment added before the data payload
Tail	Information segment added after the data payload
Encapsulation	Process of adding a header and a tail to a data payload to form a new packet
Decapsulation	Process of removing the header and tail from a packet to obtain the data payload
Gateway	Network device that provides functions such as protocol conversion, route selection, and data exchange
Router	Network device that selects a forwarding path for packets
Terminal device	End device of a data communication system, used as a sender or receiver of data

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Data payload: It can be considered as the information to be transmitted. However, in a hierarchical communication process, the data unit (packet) transmitted from the upper layer to the lower layer can be called the data payload of the lower layer.
- Packet: a data unit that is exchanged and transmitted on a network. It is in the format of header+data payload+tail. During transmission, the format and content of packets may change.
- Header: The information segment added before the data payload during packet assembly to facilitate information transmission is called the packet header.
- Tail: The information segment added after the payload to facilitate information transmission is called the tail of a packet. Note that many packets do not have tails.
- Encapsulation: A technology used by layered protocols. When the lower-layer protocol receives a message from the upper-layer protocol, the message is added to the data part of the lower-layer frame.
- Decapsulation: It is the reverse process of encapsulation. That is, the header and tail of a packet are removed to obtain the data payload.
- Gateway: A gateway is a network device that provides functions such as protocol conversion, route selection, and data exchange when networks using different architectures or protocols communicate with each other. A gateway is a term that is named based on its deployment location and functionality, rather than a specific device type.
- Router: a network device that selects a transmission path for a packet.
- Terminal device: It is the end device of the data communication system. As the data sender or receiver, the terminal device provides the necessary functions required by the user access protocol operations. The terminal device may be a computer, server, VoIP, or mobile phone.

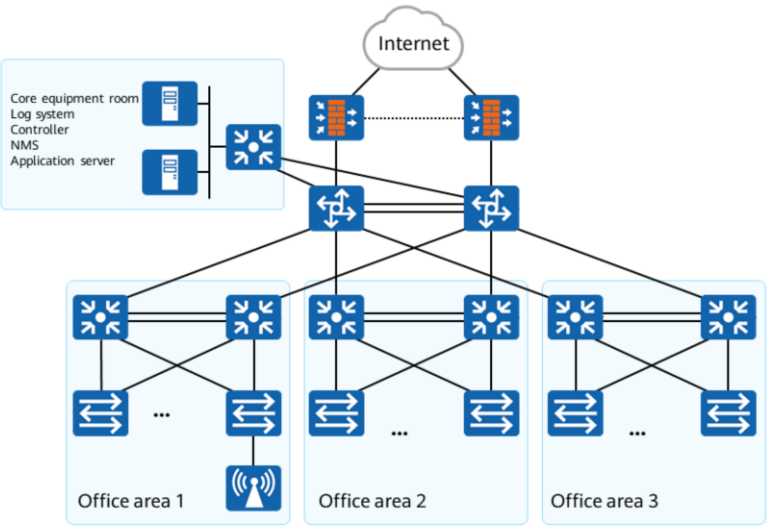
Concept of the Data Communication Network

- Data communication network:

  Communication network that consists of routers, switches, firewalls, access controllers (ACs), access points (APs), PCs, network printers, and servers

- Function:

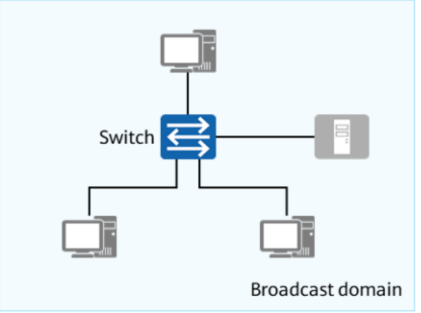
  To implement data communication



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Switches

- Switch: a device closest to end users, used to access the network and switch data frames
  - Network access of terminals (such as PCs and servers)
  - Layer 2 switching

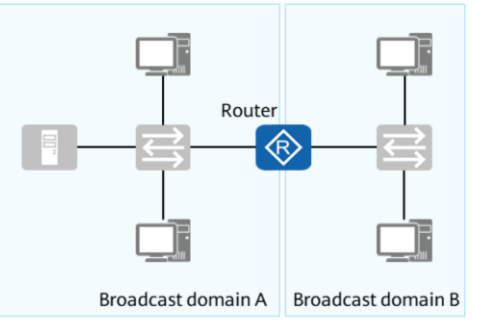


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Switches:
  - On a campus network, a switch is the device closest to end users and is used to connect terminals to the campus network. Switches at the access layer are usually Layer 2 switches and are also called Ethernet switches. Layer 2 refers to the data link layer of the TCP/IP reference model.
  - The Ethernet switch can implement the following functions: data frame switching, access of end user devices, basic access security functions, and Layer 2 link redundancy.
  - Broadcast domain: A set of nodes that can receive broadcast packets from a node.

Routers

- Router: a network-layer device that forwards data packets on the Internet. Based on the destination address in a received packet, a router selects a path to send the packet to the next router or destination. The last router on the path is responsible for sending the packet to the destination host.
  - Implementing communication between networks of the same type or different types
  - Isolating broadcast domains
  - Maintaining the routing table and running routing protocols
  - Selecting routes and forwarding IP packets
  - Implementing WAN access and network address translation
  - Connecting Layer 2 networks established through switches

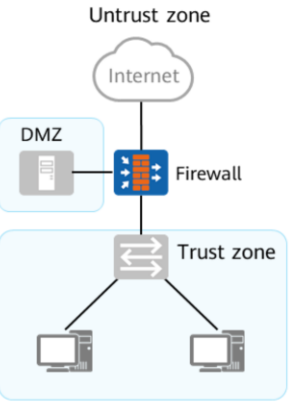


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Routers:
  - Routers work at the network layer of the TCP/IP reference model.
  - Routers can implement the following functions: routing table and routing information maintenance, route discovery and path selection, data forwarding, broadcast domain isolation, WAN access, network address translation, and specific security functions.

Firewalls

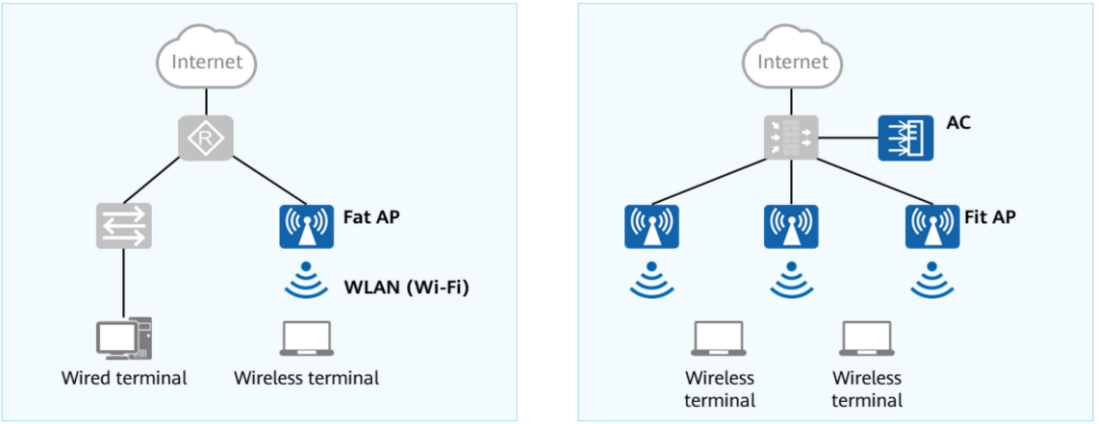
- Firewall: a network security device used to ensure secure communication between two networks. It monitors, restricts, and modifies data flows passing through it to shield information, structure, and running status of internal networks from the public network.
  - Isolating networks of different security levels
  - Implementing access control (using security policies) between networks of different security levels
  - Implementing user identity authentication
  - Implementing remote access
  - Supporting data encryption and VPN services
  - Implementing network address translation
  - Implementing other security functions



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Firewall:
  - It is located between two networks with different trust levels (for example, between an intranet and the Internet). It controls the communication between the two networks and forcibly implements unified security policies to prevent unauthorized access to important information resources.

Wireless devices



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

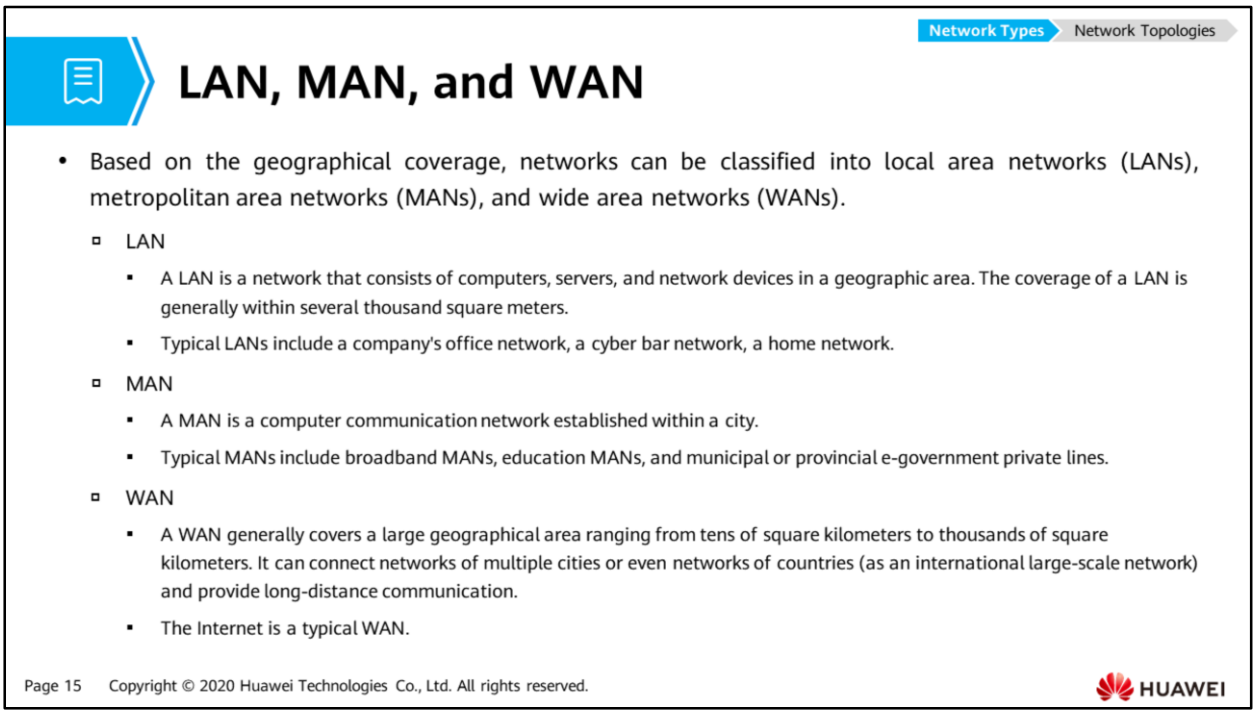
- In a broad sense, WLAN is a network that uses radio waves, laser, and infrared signals to replace some or all transmission media in a wired LAN. Common Wi-Fi is a WLAN technology based on the IEEE 802.11 family of standards.
- On a WLAN, common devices include fat APs, fit APs, and ACs.
  - AP:
    - Generally, it supports the fat AP, fit AP, and cloud-based management modes. You can flexibly switch between these modes based on network planning requirements.
    - Fat AP: It is applicable to homes. It works independently and needs to be configured separately. It has simple functions and low costs.
    - Fit AP: It applies to medium- and large-sized enterprises. It needs to work with the AC and is managed and configured by the AC.
    - Cloud-based management: It applies to small- and medium-sized enterprises. It needs to work with the cloud-based management platform for unified management and configuration. It provides various functions and supports plug-and-play.
  - AC:
    - It is generally deployed at the aggregation layer of the entire network to provide high-speed, secure, and reliable WLAN services.
    - The AC provides wireless data control services featuring large capacity, high performance, high reliability, easy installation, and easy maintenance. It features flexible networking and energy saving.

Contents

1. Communication and Networks
2. **Network Types and Topology Types**
3. Network Engineering and Network Engineers

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

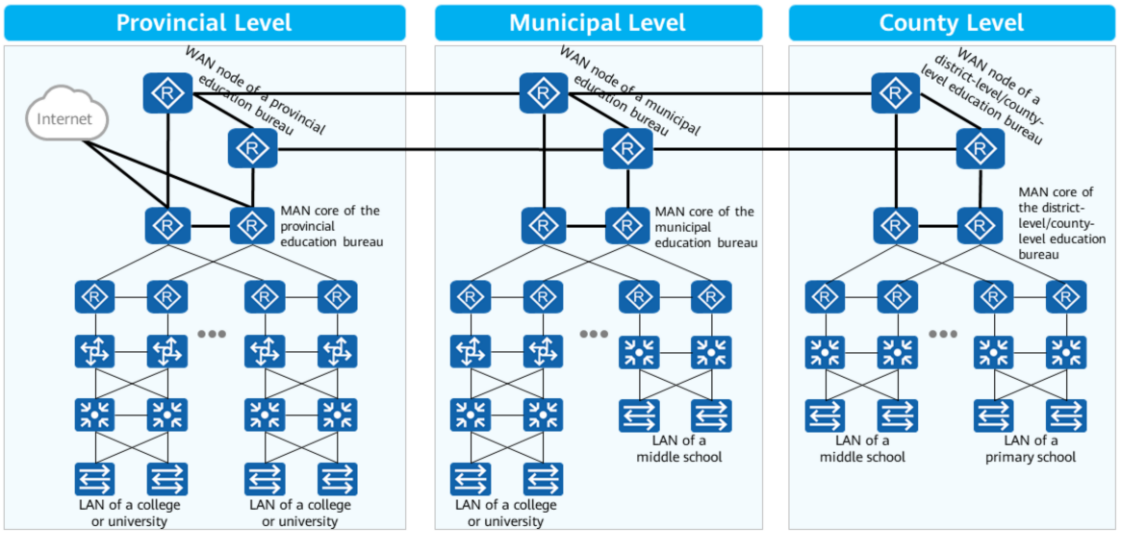
HUAWEI



- Based on the geographical coverage, networks can be classified into LANs, WANs, and MANs.
- LAN:
  - Basic characteristics:
    - An LAN generally covers an area of a few square kilometers.
    - The main function is to connect several terminals that are close to each other (within a family, within one or more buildings, within a campus, for example).
  - Technologies used: Ethernet and Wi-Fi.
- MAN:
  - Basic characteristics:
    - A MAN is a large-sized LAN, which requires high costs but can provide a higher transmission rate. It improves the transmission media in LANs and expands the access scope of LANs (able to cover a university campus or city).
    - The main function is to connect hosts, databases, and LANs at different locations in the same city.
    - The functions of a MAN are similar to those of a WAN except for implementation modes and performance.
  - Technologies used: such as Ethernet (10 Gbit/s or 100 Gbit/s) and WiMAX.

- WAN:
  - Basic characteristics:
    - A WAN generally covers an area of several kilometers or larger (thousands of kilometers for example).
    - It is mainly used to connect several LANs or MANs that are far from each other (for example, across cities or countries).
    - Telecom operators' communication lines are used.
  - Technologies used: HDLC and PPP.

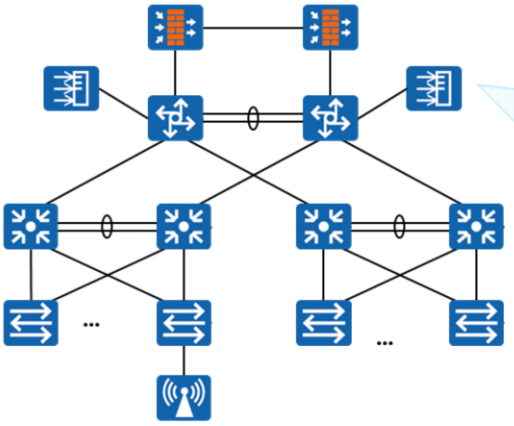
LAN, MAN, and WAN in the Education Industry



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Network Topologies

- A network topology is a structured layout presented using transmission media (such as twisted pairs and optical fibers) to interconnect various devices (such as computer terminals, routers, and switches).



The network topology is used to describe the physical or logical structure of a network in the network engineering field, and is a very important network concept.

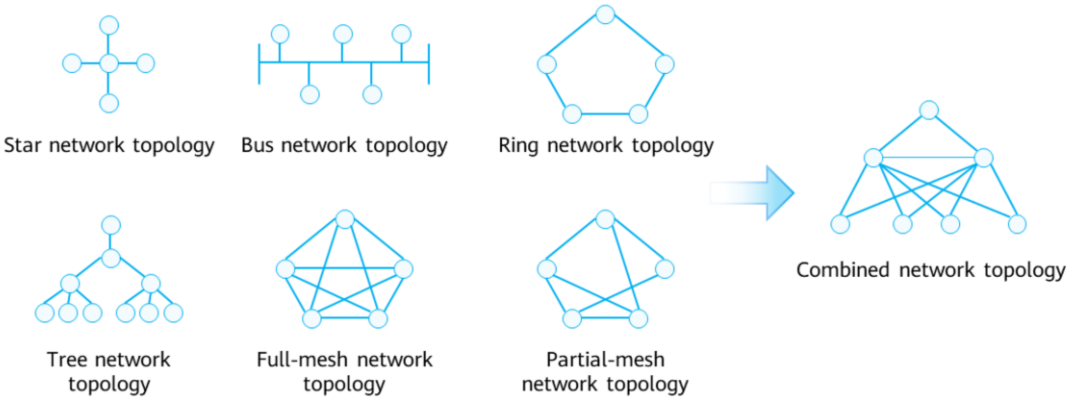
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Network topology drawing:
  - It is very important to master professional network topology drawing skills, which requires a lot of practice.
  - Visio and Power Point are two common tools for drawing network topologies.

Network Topology Types

- Network topologies are classified into star, bus, ring, tree, full-mesh, and partial-mesh network topologies.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Star network topology:
  - All nodes are connected through a central node.
  - Advantages: New nodes can be easily added to the network. Communication data must be forwarded by the central node, which facilitates network monitoring.
  - Disadvantages: Faults on the central node affect the communication of the entire network.
- Bus network topology:
  - All nodes are connected through a bus (coaxial cable for example).
  - Advantages: The installation is simple and cable resources are saved. Generally, the failure of a node does not affect the communication of the entire network.
  - Disadvantages: A bus fault affects the communication of the entire network. The information sent by a node can be received by all other nodes, resulting in low security.
- Ring network topology:
  - All nodes are connected to form a closed ring.
  - Advantages: Cables resources are saved.
  - Disadvantages: It is difficult to add new nodes. The original ring must be interrupted before new nodes are inserted to form a new ring.

- Tree network topology:
  - The tree structure is actually a hierarchical star structure.
  - Advantages: Multiple star networks can be quickly combined, which facilitates network expansion.
  - Disadvantages: A fault on a node at a higher layer is more severe.
- Full-mesh network topology:
  - All nodes are interconnected through cables.
  - Advantages: It has high reliability and high communication efficiency.
  - Disadvantages: Each node requires a large number of physical ports and interconnection cables. As a result, the cost is high, and it is difficult to expand.
- Partial-mesh network topology:
  - Only key nodes are interconnected.
  - Advantages: The cost of a partial-mesh network is lower than that of a full-mesh network.
  - Disadvantages: The reliability of a partial-mesh network is lower than that of a full-mesh network.
- In actual networking, multiple types of topologies may be combined based on the cost, communication efficiency, and reliability requirements.

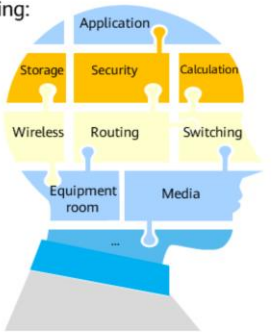
Contents

1. Communication and Networks
2. Network Types and Topology Types
3. **Network Engineering and Network Engineers**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Network Engineering

- Network engineering
  - Network engineering refers to planning and designing feasible solutions based on network application requirements and computer network system standards, specifications, and technologies under the guidance of information system engineering methods and complete organizations, as well as integrating computer network hardware devices, software, and technologies to form a cost-effective network system that meets user requirements.
- Technical modules covered by network engineering:



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Network engineering covers a series of activities around the network, including network planning, design, implementation, commissioning, and troubleshooting.
- The knowledge field of network engineering design is very wide, in which routing and switching are the basis of the computer network.

Network Engineer

- Network engineer
  - Network engineers are technology professionals who master professional network technologies, have professional skills, professionalism, and project implementation experience in the network engineering field, and are able to fully communicate with customers or other project stakeholders onsite. In addition, they can develop implementation solutions and project plans (recognized by project stakeholders) based on customer requirements and environment factors, fully mobilize resources of all parties to ensure timely and high-quality project implementation, and provide training for stakeholders and deliver engineering documents after the project is implemented.
- Comprehensive capability models for network engineers:



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Network Engineers' Technology Development Path



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Huawei Certification Injects Vitality into Talent Development for Enterprises

Certification exam

- Cultivate experts who understand both business and technologies.
- Cultivate platform construction and service application experts based on HUAWEI CLOUD.
- Focuses on ICT infrastructure and cultivates architecture talent in all ICT fields.

Providing talent with career development paths

- Meets enterprise talent's career evolution from an engineer to a senior engineer, and then to an expert.
- Provides a hierarchical certification system that provides customized talent growth paths in accordance with job-based capability requirements and supports in-depth professional development, integration, and expansion, reducing the talent cultivation cost for enterprises.

Facilitating enterprise innovation and transformation

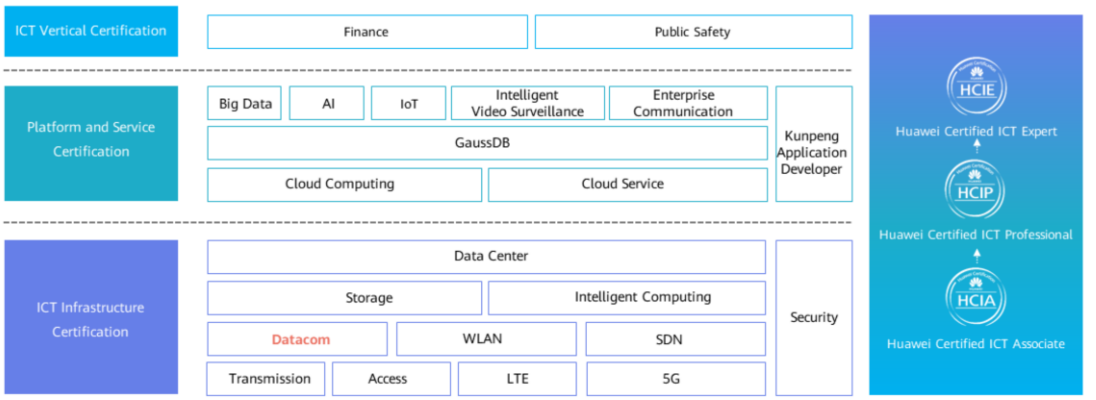
- Provides authoritative certification for ICT talent. The ICT talent with authoritative certification helps ensure project delivery quality and improve customer satisfaction.
- Enhances the overall performance and productivity of enterprises.
- Accelerates business innovation and transformation, and improve the overall operational efficiency.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Huawei Certification Portfolio

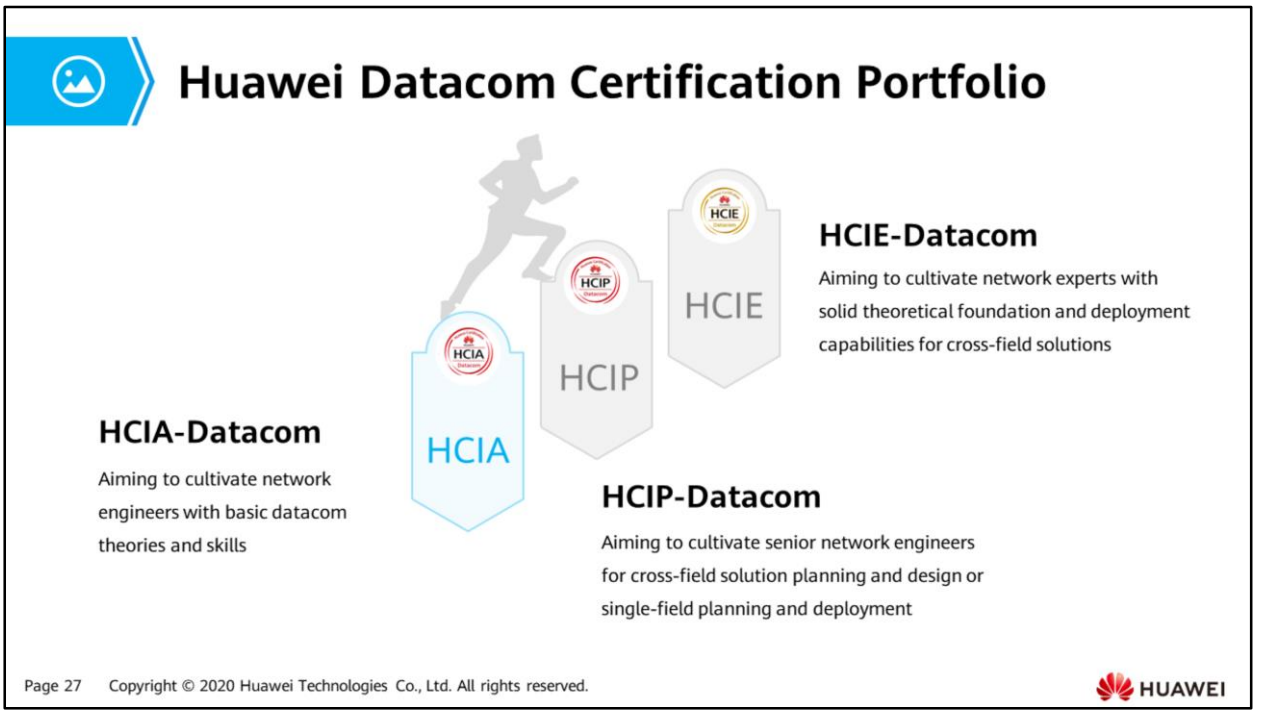
- Huawei certification covers all ICT fields and is committed to providing a leading talent cultivation architecture and certification standards, cultivating ICT professionals in the digital era, and building a healthy ICT talent ecosystem.

Huawei Certification



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Huawei talent ecosystem website: https://e.huawei.com/en/talent/#/home



- HCIA-Datacom: one course (exam)
  - Basic concepts of data communication, basis of routing and switching, security, WLAN, SDN and NFV, basis of programming automation, and network deployment cases
- HCIP-Datacom: one mandatory course (exam) and six optional sub-certification courses (exams)
  - Mandatory course (exam):
    - HCIP-Datacom-Core Technology
  - Optional courses (exams):
    - HCIP-Datacom-Advanced Routing & Switching Technology
    - HCIP-Datacom-Campus Network Planning and Deployment
    - HCIP-Datacom-Enterprise Network Solution Design
    - HCIP-Datacom-WAN Planning and Deployment
    - HCIP-Datacom-SD-WAN Planning and Deployment
    - HCIP-Datacom-Network Automation Developer
- HCIE-Datacom: one course (exam), integrating two modules
  - Classic network:
    - Classic datacom technology theory based on command lines
    - Classic datacom technology deployment based on command lines
  - Huawei SDN solution:
    - Enterprise SDN solution technology theory
    - Enterprise SDN solution planning and deployment

Quiz

1. (Single) Which of the following type of network topology has the highest reliability? ( )

   A. Star network topology

   B. Ring network topology

   C. Full-mesh network topology

   D. Tree network topology

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. C

Summary

- This section describes the concepts of network communication and data communication network. The basic function of a data communication network is to implement network communication.
- This section also introduces various network devices, the differences between LAN, MAN and WAN, and various network topologies. In actual networking, multiple topologies are combined according to the requirements of multiple parties.
- This section also describes network engineering and network engineers and introduces Huawei datacom certification system.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Network Reference Model

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- In the digital era, various information is presented as data in our life. What is data? How is data transmitted?
- In this course, we will use the network reference model to understand the "life" of data.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand the data definition and transmission process.
  - Understand the concepts and advantages of the network reference model.
  - Understand common standard protocols.
  - Understand the data encapsulation and decapsulation processes.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

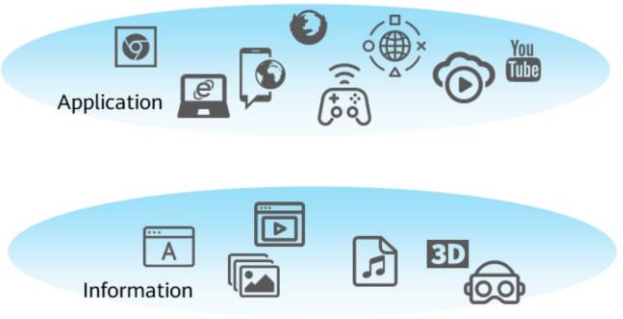
Contents

1. **Applications and Data**
2. Network Reference Model and Standard Protocols
3. Data Communication Process

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Origin of the Story - Applications

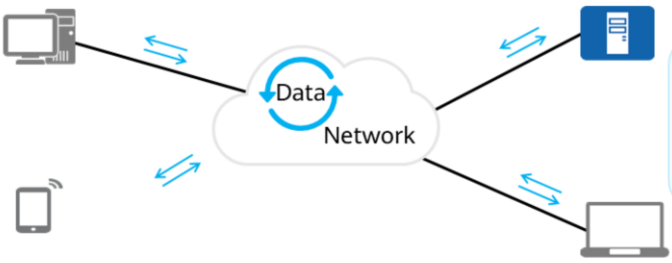
- Applications are used to meet various requirements of people, such as web page access, online gaming, and online video playback.
- Information is generated along with applications. Texts, pictures, and videos are all information presentation modes.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Application Implementation - Data

- Data generation
  - In the computer field, data is the carrier of all kinds of information.
- Data transmission
  - Data generated by most applications needs to be transmitted between devices.



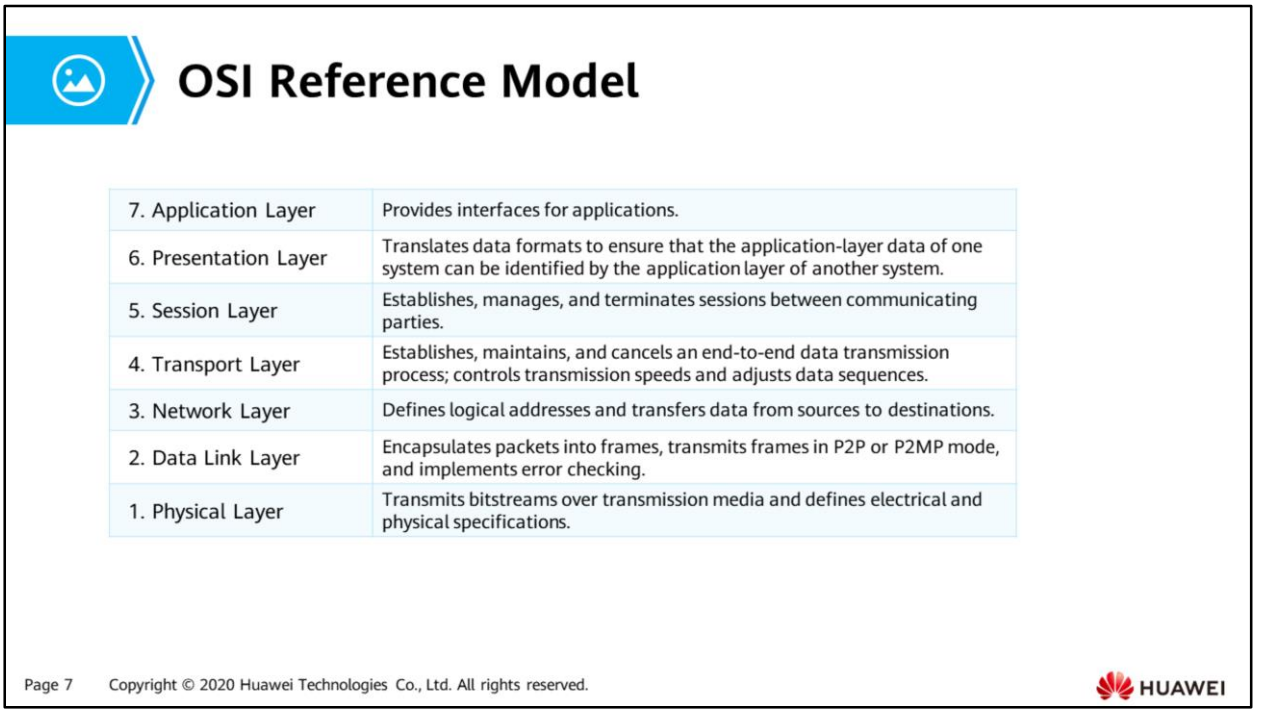
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A computer can identify only digital data consisting of 0s and 1s. It is incapable of reading other types of information, so the information needs to be translated into data by certain rules.
- However, people do not have the capability of reading electronic data. Therefore, data needs to be converted into information that can be understood by people.
- A network engineer needs to pay more attention to the end-to-end data transmission process.

Contents

1. Applications and Data
2. **Network Reference Model and Standard Protocols**
3. Data Communication Process

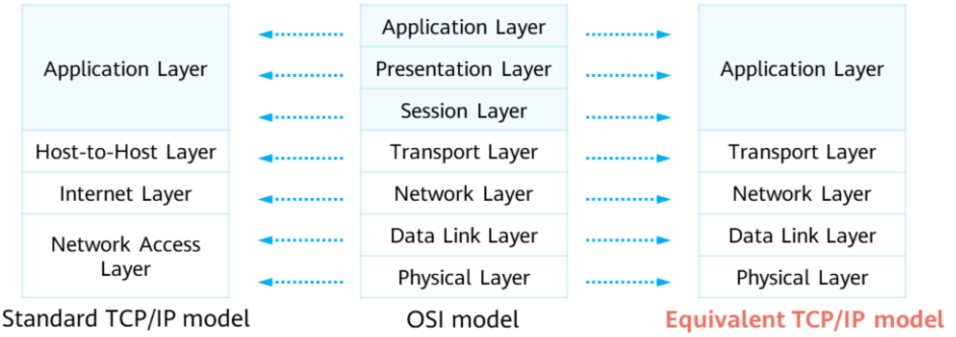
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The Open Systems Interconnection Model (OSI) was included in the ISO 7489 standard and released in 1984. ISO stands for International Organization for Standardization.
- The OSI reference model is also called the seven-layer model. The seven layers from bottom to top are as follows:
  - Physical layer: transmits bit flows between devices and defines physical specifications such as electrical levels, speeds, and cable pins.
  - Data link layer: encapsulates bits into octets and octets into frames, uses MAC addresses to access media, and implements error checking.
  - Network layer: defines logical addresses for routers to determine paths and transmits data from source networks to destination networks.
  - Transport layer: implements connection-oriented and non-connection-oriented data transmission, as well as error checking before retransmission.
  - Session layer: establishes, manages, and terminates sessions between entities at the presentation layer. Communication at this layer is implemented through service requests and responses transmitted between applications on different devices.
  - Presentation layer: provides data encoding and conversion so that data sent by the application layer of one system can be identified by the application layer of another system.
  - Application layer: provides network services for applications and the OSI layer closest to end users.

TCP/IP Reference Model

- The OSI protocol stack is complex, and the TCP and IP protocols are widely used in the industry. Therefore, the TCP/IP reference model becomes the mainstream reference model of the Internet.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The TCP/IP model is similar to the OSI model in structure and adopts a hierarchical architecture. Adjacent TCP/IP layers are closely related.
- The standard TCP/IP model combines the data link layer and physical layer in the OSI model into the network access layer. This division mode is contrary to the actual protocol formulation. Therefore, the equivalent TCP/IP model that integrates the TCP/IP standard model and the OSI model is proposed. Contents in the following slides are based on the equivalent TCP/IP model.

Common TCP/IP Protocols

- The TCP/IP protocol stack defines a series of standard protocols.

<table>
<tr><td rowspan="2">Application Layer</td><td>Telnet</td><td>FTP</td><td>TFTP</td><td>SNMP</td></tr>
<tr><td>HTTP</td><td>SMTP</td><td>DNS</td><td>DHCP</td></tr>
<tr><td>Transport Layer</td><td colspan="2">TCP</td><td colspan="2">UDP</td></tr>
<tr><td rowspan="2">Network Layer</td><td colspan="2">ICMP</td><td colspan="2">IGMP</td></tr>
<tr><td colspan="4">IP</td></tr>
<tr><td rowspan="2">Data Link Layer</td><td colspan="4">PPPoE</td></tr>
<tr><td colspan="2">Ethernet</td><td colspan="2">PPP</td></tr>
<tr><td>Physical Layer</td><td colspan="4">...</td></tr>
</table>

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

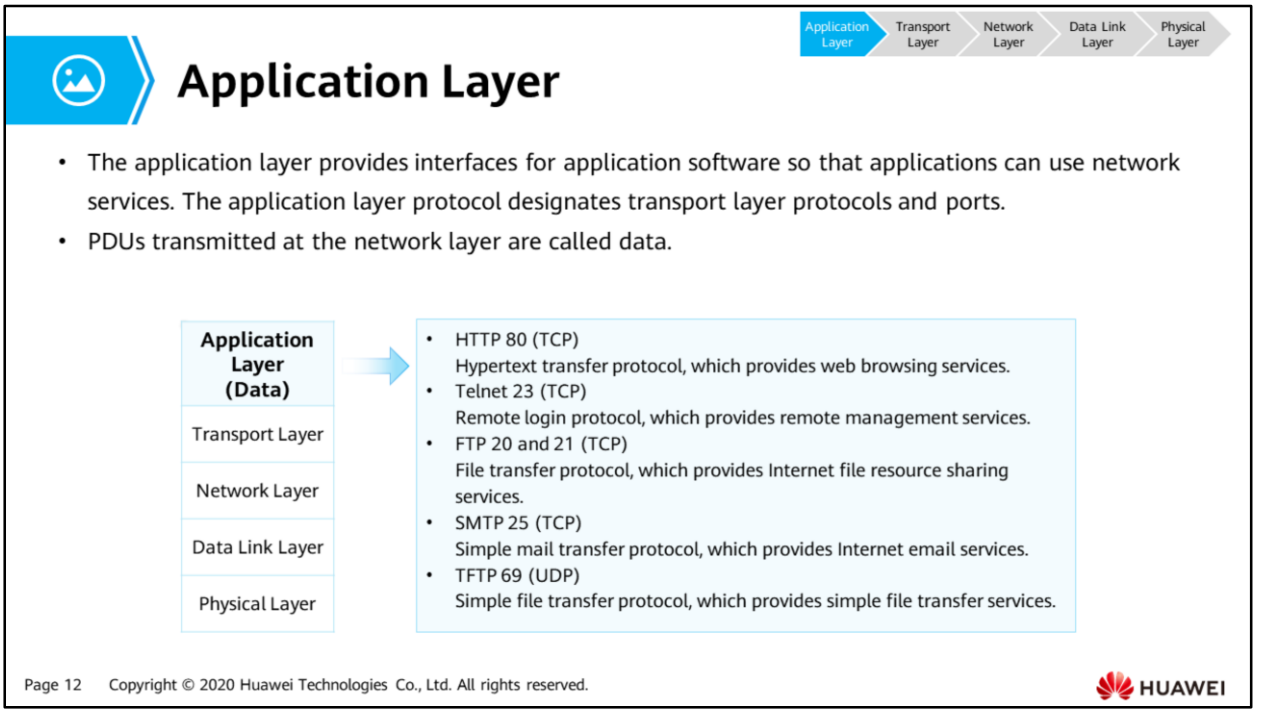
- Application Layer
  - Hypertext Transfer Protocol (HTTP): is used to access various pages on web servers.
  - File Transfer Protocol (FTP): provides a method for transferring files. It allows data to be transferred from one host to another.
  - Domain name service (DNS): translates from host domain names to IP addresses.
- Transport layer
  - Transmission Control Protocol (TCP): provides reliable connection-oriented communication services for applications. Currently, TCP is used by many popular applications.
  - User Datagram Protocol (UDP): provides connectionless communication and does not guarantee the reliability of packet transmission. The reliability can be ensured by the application layer.
- Network layer
  - Internet Protocol (IP): encapsulates transport-layer data into data packets and forwards packets from source sites to destination sites. IP provides a connectionless and unreliable service.
  - Internet Group Management Protocol (IGMP): manages multicast group memberships. Specifically, IGMP sets up and maintains memberships between IP hosts and their directly connected multicast routers.
  - Internet Control Message Protocol (ICMP): sends control messages based on the IP protocol and provides information about various problems that may exist in the communication environment. Such information helps administrators diagnose problems and take proper measures to resolve the problems.

- Data link layer
    - Point-to-Point Protocol (PPP): is a data link layer protocol that works in point-to-point mode. PPP is mainly used on wide area networks (WANs).
    - Ethernet: is a multi-access and broadcast protocol at the data link layer, which is the most widely used local area network (LAN) technology.
    - Point-to-Point Protocol over Ethernet (PPPoE): connects multiple hosts on a network to a remote access concentrator through a simple bridge device (access device). Common applications include home broadband dialup access.

Common Protocol Standardization Organizations

- Internet Engineering Task Force (IETF)
  - IETF is a voluntary organization responsible for developing and promoting Internet protocols (especially protocols that constitute the TCP/IP protocol suite), and releasing new or replacing old protocol standards through RFCs.
- Institute of Electrical and Electronics Engineers (IEEE)
  - IEEE has formulated about 30% of standards in the electronics, electrical, and computer science fields worldwide. Those standards include well-known IEEE802.3 (Ethernet) and IEEE802.11 (Wi-Fi).
- International Organization for Standardization (ISO)
  - ISO is an international organization that plays an important role in the formulation of computer network standards, such as the OSI model defined in ISO/IEC 7498-1.

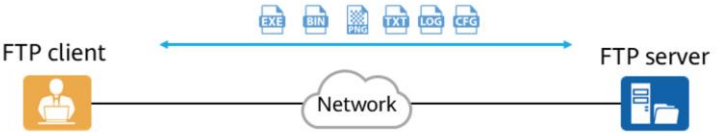
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The TCP/IP suite enables data to be transmitted over a network. The layers use packet data units (PDUs) to exchange data, implementing communication between network devices.
- PDUs transmitted at different layers contain different information. Therefore, PDUs have different names at different layers.

Common Application Layer Protocols - FTP

- The File Transfer Protocol (FTP) transfers files from one host to another to implement file download and upload. This protocol adopts the client/server (C/S) structure.



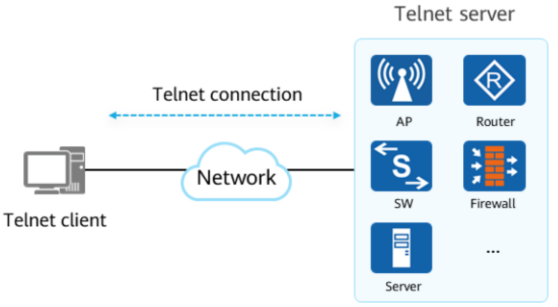
FTP client: provides commands for local users to operate files on a remote server. A user can install an FTP client program on a PC and set up a connection with an FTP server to operate files on the server.

FTP server: a device that runs the FTP service. It provides the access and operation functions for remote clients, allowing users to access the FTP server through the FTP client program and access files on the server.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Common Application Layer Protocols - Telnet

- Telnet is a standard protocol that provides remote login services on a network. It provides users with the ability to operate remote devices through local PCs.

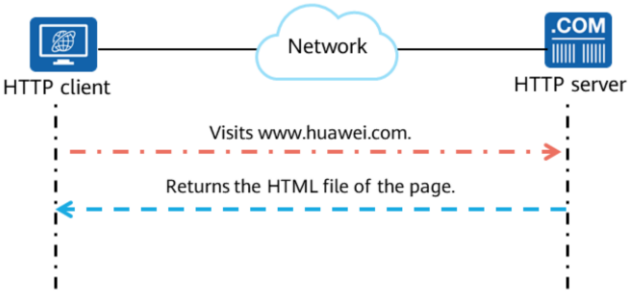


A user connects to a Telnet server through the Telnet client program. The commands entered on the Telnet client are executed on the server, as if the commands were entered on the console of the server.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Common Application Layer Protocols - HTTP

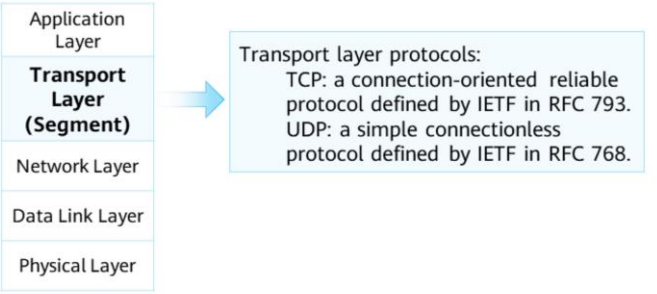
- Hypertext Transfer Protocol (HTTP): is one of the most widely used network protocols on the Internet. HTTP was originally designed to provide a method for publishing and receiving HTML pages.



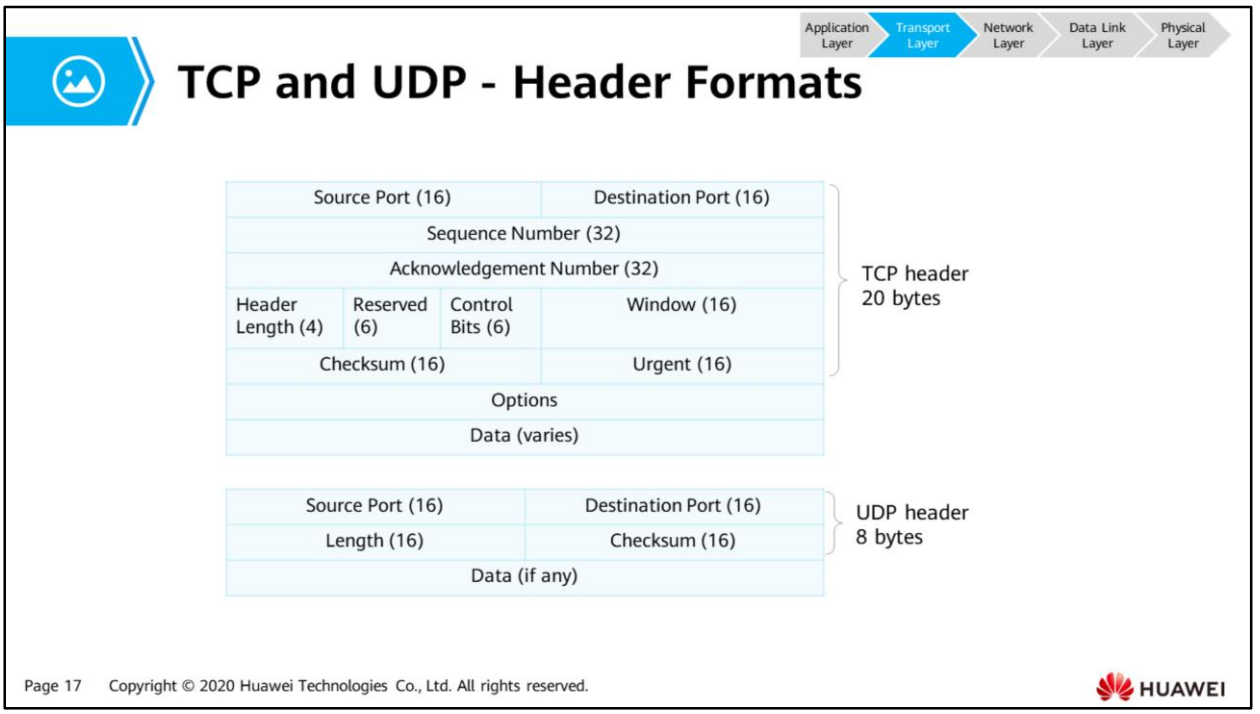
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Transport Layer

- A transport layer protocol receives data from an application layer protocol, encapsulates the data with the corresponding transport layer protocol header, and helps establish an end-to-end (port-to-port) connection.
- PDUs transmitted at the transport layer are called segments.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

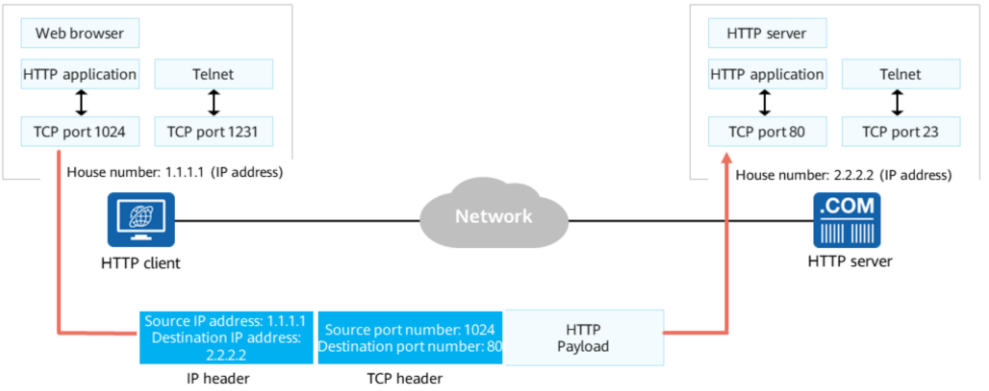


- TCP header:
  - Source Port: identifies the application that sends the segment. This field is 16 bits long.
  - Destination Port: identifies the application that receives the segment. This field is 16 bits long.
  - Sequence Number: Every byte of data sent over a TCP connection has a sequence number. The value of the Sequence Number field equals the sequence number of the first byte in a sent segment. This field is 32 bits long.
  - Acknowledgment Number: indicates the sequence number of the next segment's first byte that the receiver is expecting to receive. The value of this field is 1 plus the sequence number of the last byte in the previous segment that is successfully received. This field is valid only when the ACK flag is set. This field is 32 bits long.
  - Header Length: indicates the length of the TCP header. The unit is 32 bits (4 bytes). If there is no option content, the value of this field is 5, indicating that the header contains 20 bytes.
  - Reserved: This field is reserved and must be set to 0. This field is 6 bits long.
  - Control Bits: control bits, includes FIN, ACK, and SYN flags, indicating TCP data segments in different states.
  - Window: used for TCP flow control. The value is the maximum number of bytes that are allowed by the receiver. The maximum window size is 65535 bytes. This field is 16 bits long.
  - Checksum: a mandatory field. It is calculated and stored by the sender and verified by the receiver. During checksum computation, the TCP header and TCP data are included, and a 12-byte pseudo header is added before the TCP segment. This field is 16 bits long.

    - Urgent: indicates the urgent pointer. The urgent pointer is valid only when the URG flag is set. The Urgent field indicates that the sender transmits data in emergency mode. The urgent pointer indicates the number of urgent data bytes in a segment (urgent data is placed at the beginning of the segment). This field is 16 bits long.
    - Options: This field is optional. This field is 0 to 40 bytes long.

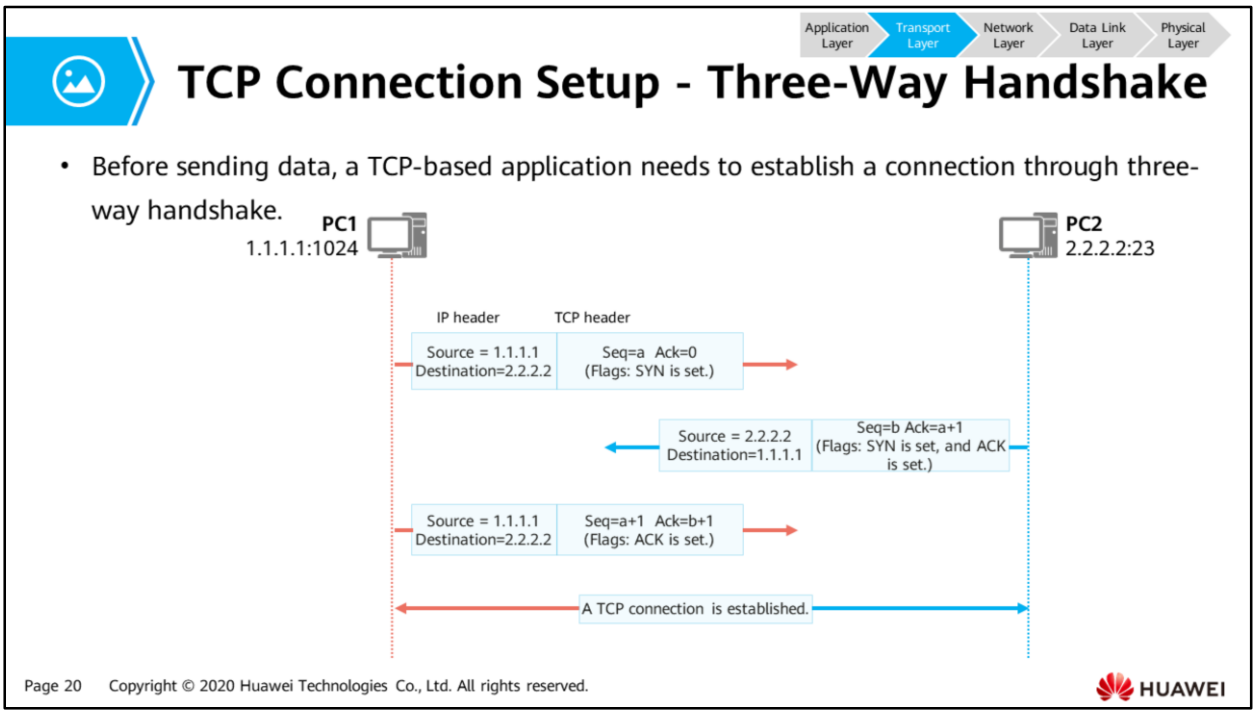
- UDP header:
    - Source Port: identifies the application that sends the segment. This field is 16 bits long.
    - Destination Port: identifies the application that receives the segment. This field is 16 bits long.
    - Length: specifies the total length of the UDP header and data. The possible minimum length is 8 bytes because the UDP header already occupies 8 bytes. Due to the existence of this field, the total length of a UDP segment does not exceed 65535 bytes (including an 8-byte header and 65527-byte data).
    - Checksum: checksum of the UDP header and UDP data. This field is 16 bits long.

TCP and UDP - Port Numbers

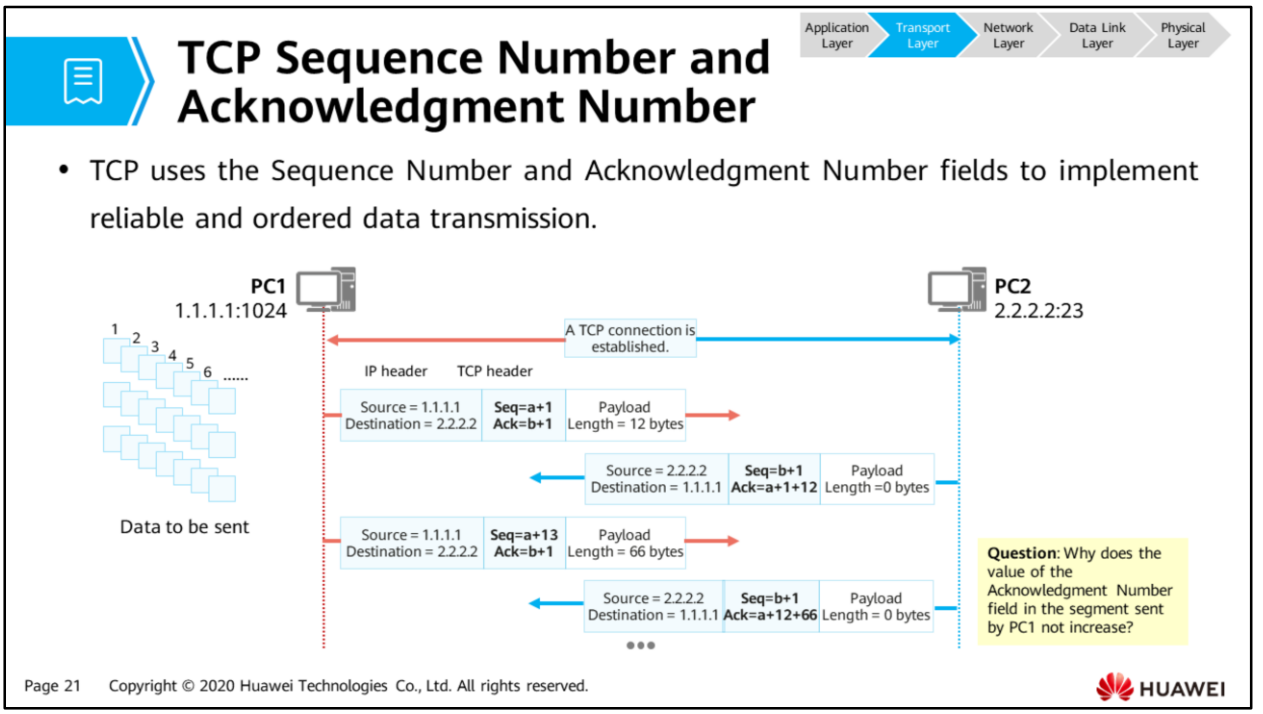


- Generally, the source port used by a client is randomly allocated, and the destination port is specified by the application of a server.
- The system generally selects a source port number that is greater than 1023 and is not being used.
- The destination port number is the listening port of the application (service) enabled on the server. For example, the default port number for HTTP is 80.

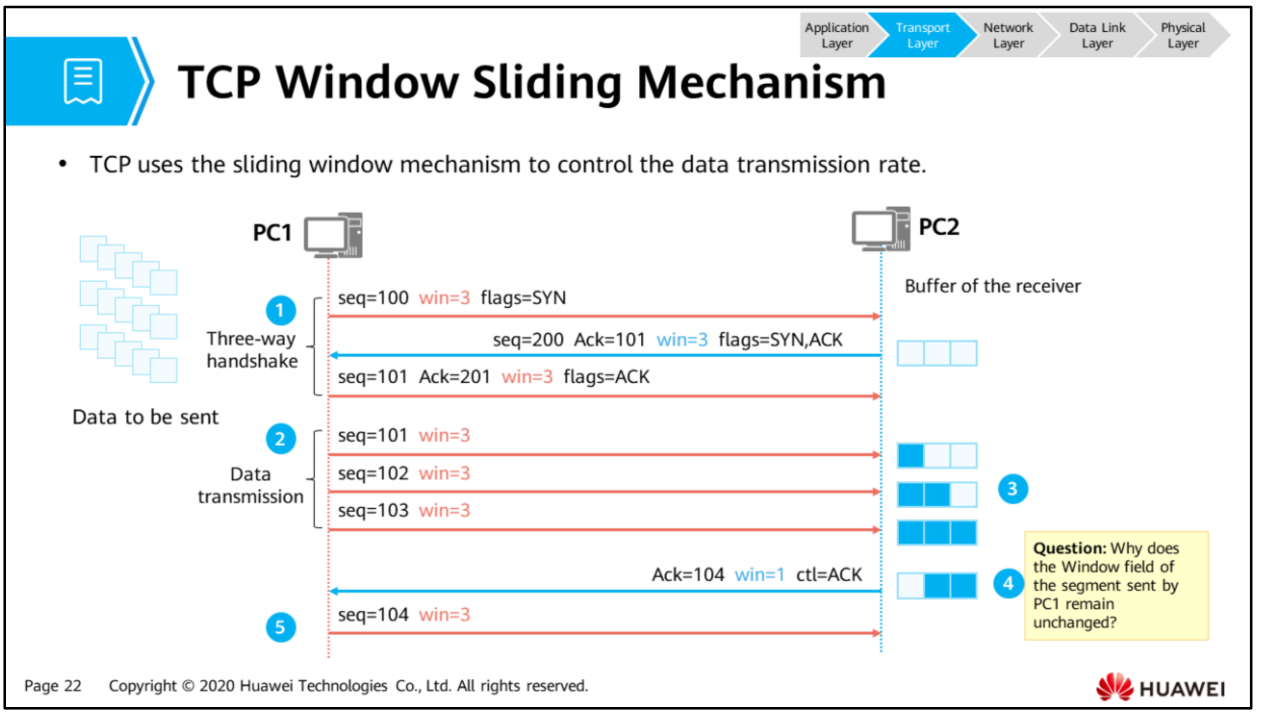
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



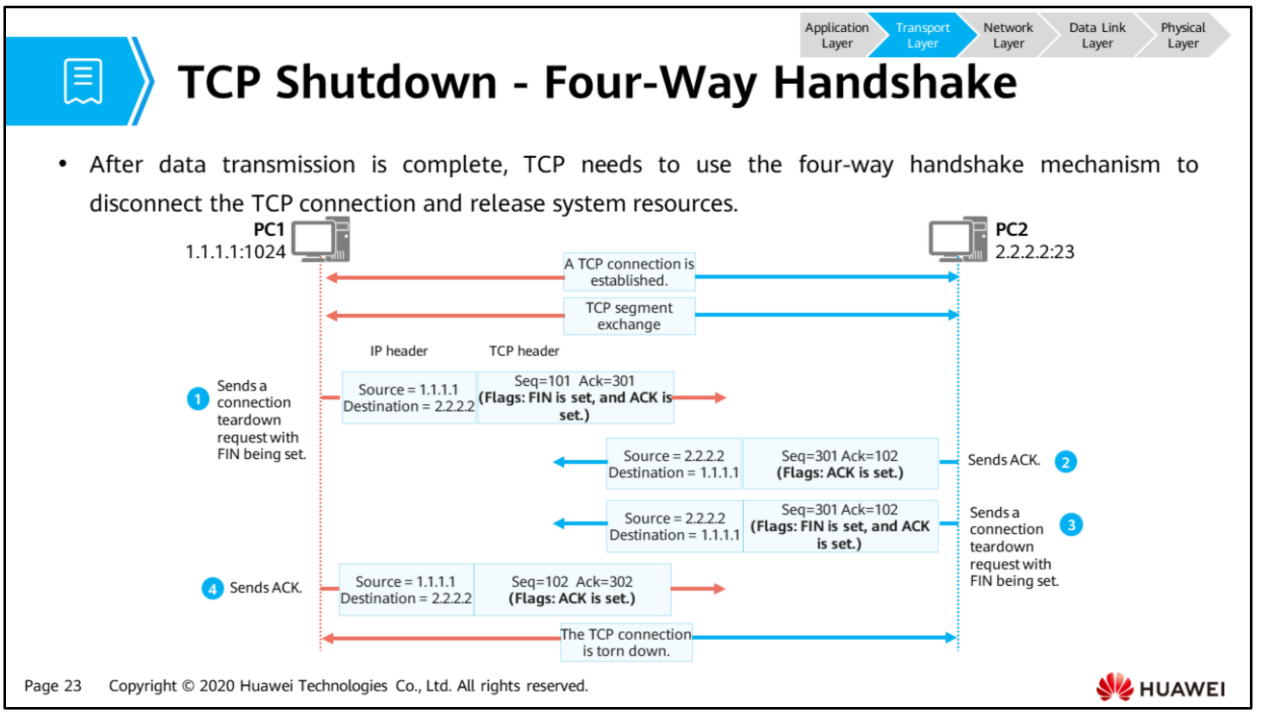
- The TCP connection setup process is as follows:
  - The TCP connection initiator (PC1 in the figure) sends the first TCP segment with SYN being set. The initial sequence number a is a randomly generated number. The acknowledgment number is 0 because no segment has ever been received from PC2.
  - After receiving a valid TCP segment with the SYN flag being set, the receiver (PC2) replies with a TCP segment with SYN and ACK being set. The initial sequence number b is a randomly generated number. Because the segment is a response one to PC1, the acknowledgment number is a+1.
  - After receiving the TCP segment in which SYN and ACK are set, PC1 replies with a segment in which ACK is set, the sequence number is a+1, and the acknowledgment number is b+1. After PC2 receives the segment, a TCP connection is established.



- Assume that PC1 needs to send segments of data to PC2. The transmission process is as follows:
    1. PC1 numbers each byte to be sent by TCP. Assume that the number of the first byte is a+1. Then, the number of the second byte is a+2, the number of the third byte is a+3, and so on.
    2. PC1 uses the number of the first byte of each segment of data as the sequence number and sends out the TCP segment.
    3. After receiving the TCP segment from PC1, PC2 needs to acknowledge the segment and request the next segment of data. How is the next segment of data determined? Sequence number (a+1) + Payload length = Sequence number of the first byte of the next segment (a+1+12)
    4. After receiving the TCP segment sent by PC2, PC1 finds that the acknowledgment number is a+1+12, indicating that the segments from a+1 to a+12 have been received and the sequence number of the upcoming segment to be sent should be a+1+12.
- To improve the sending efficiency, multiple segments of data can be sent at a time by the sender and then acknowledged at a time by the receiver.



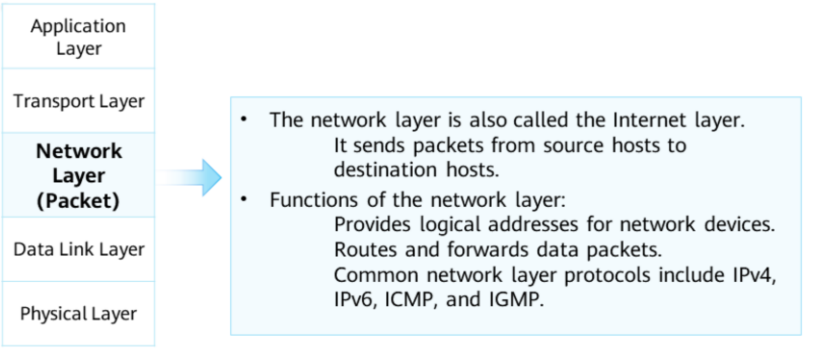
1. During the TCP three-way handshake, both ends notify each other of the maximum number of bytes (buffer size) that can be received by the local end through the Window field.
2. After the TCP connection is set up, the sender sends data of the specified number of bytes based on the window size declared by the receiver.
3. After receiving the data, the receiver stores the data in the buffer and waits for the upper-layer application to obtain the buffered data. After the data is obtained by the upper-layer application, the corresponding buffer space is released.
4. The receiver notifies the current acceptable data size (window) according to its buffer size.
5. The sender sends a certain amount of data based on the current window size of the receiver.



- TCP supports data transmission in full-duplex mode, which means that data can be transmitted in both directions at the same time. Before data is transmitted, TCP sets up a connection in both directions through three-way handshake. Therefore, after data transmission is complete, the connection must be closed in both directions. This is shown in the figure.
    1. PC1 sends a TCP segment with FIN being set. The segment does not carry data.
    2. After receiving the TCP segment from PC1, PC2 replies with a TCP segment with ACK being set.
    3. PC2 checks whether data needs to be sent. If so, PC2 sends the data, and then a TCP segment with FIN being set to close the connection. Otherwise, PC2 directly sends a TCP segment with FIN being set.
    4. After receiving the TCP segment with FIN being set, PC1 replies with an ACK segment. The TCP connection is then torn down in both directions.

Network Layer

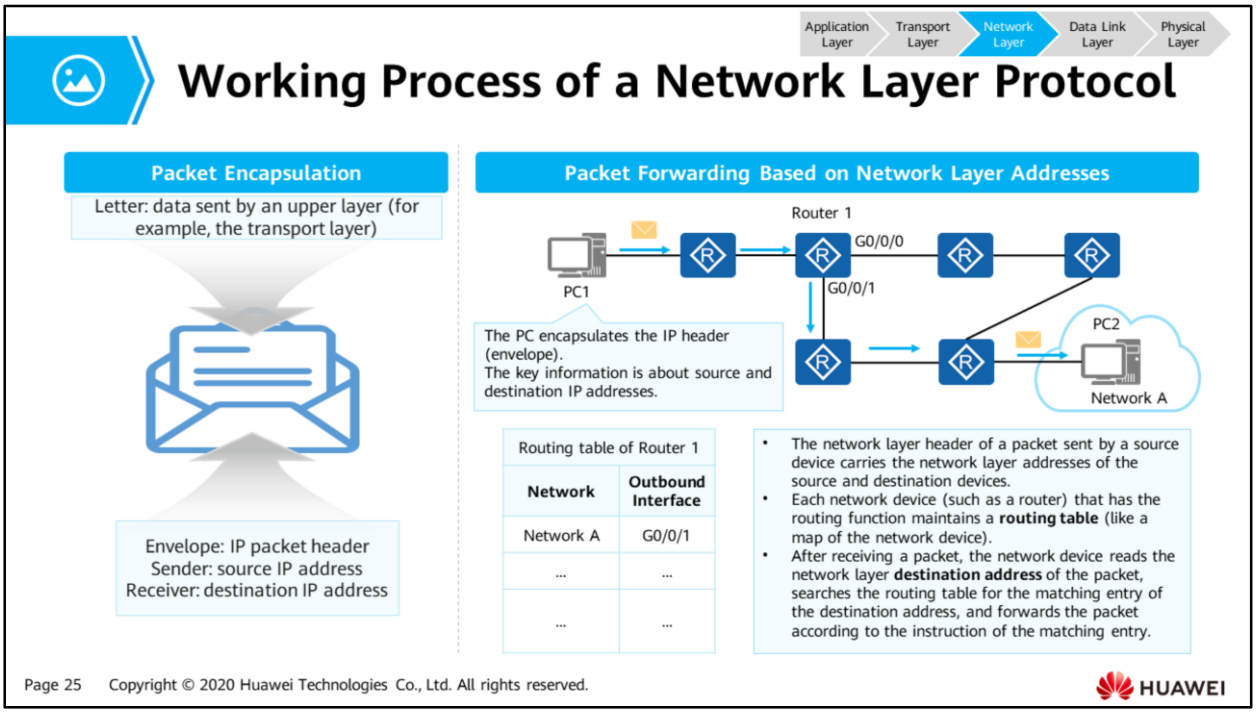
- The transport layer is responsible for establishing connections between processes on hosts, and the network layer is responsible for transmitting data from one host to another.
- PDUs transmitted at the network layer are called packets.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

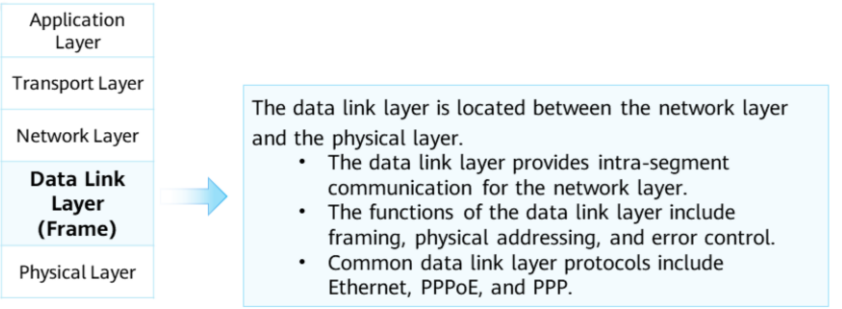
- Internet Protocol Version 4 (IPv4) is the most widely used network layer protocol.



- When IP is used as the network layer protocol, both communication parties are assigned a unique IP address to identify themselves. An IP address can be written as a 32-bit binary integer. To facilitate reading and analysis, an IP address is usually represented in dot-decimal notation, consisting of four decimal numbers, each ranging from 0 to 255, separated by dots, such as, 192.168.1.1.
- Encapsulation and forwarding of IP data packets:
  - When receiving data from an upper layer (such as the transport layer), the network layer encapsulates an IP packet header and adds the source and destination IP addresses to the header.
  - Each intermediate network device (such as a router) maintains a routing table that guides IP packet forwarding like a map. After receiving a packet, the intermediate network device reads the destination address of the packet, searches the local routing table for a matching entry, and forwards the IP packet according to the instruction of the matching entry.
  - When the IP packet reaches the destination host, the destination host determines whether to accept the packet based on the destination IP address and then processes the packet accordingly.
- When the IP protocol is running, routing protocols such as OSPF, IS-IS, and BGP are required to help routers build routing tables, and ICMP is required to help control networks and diagnose network status.

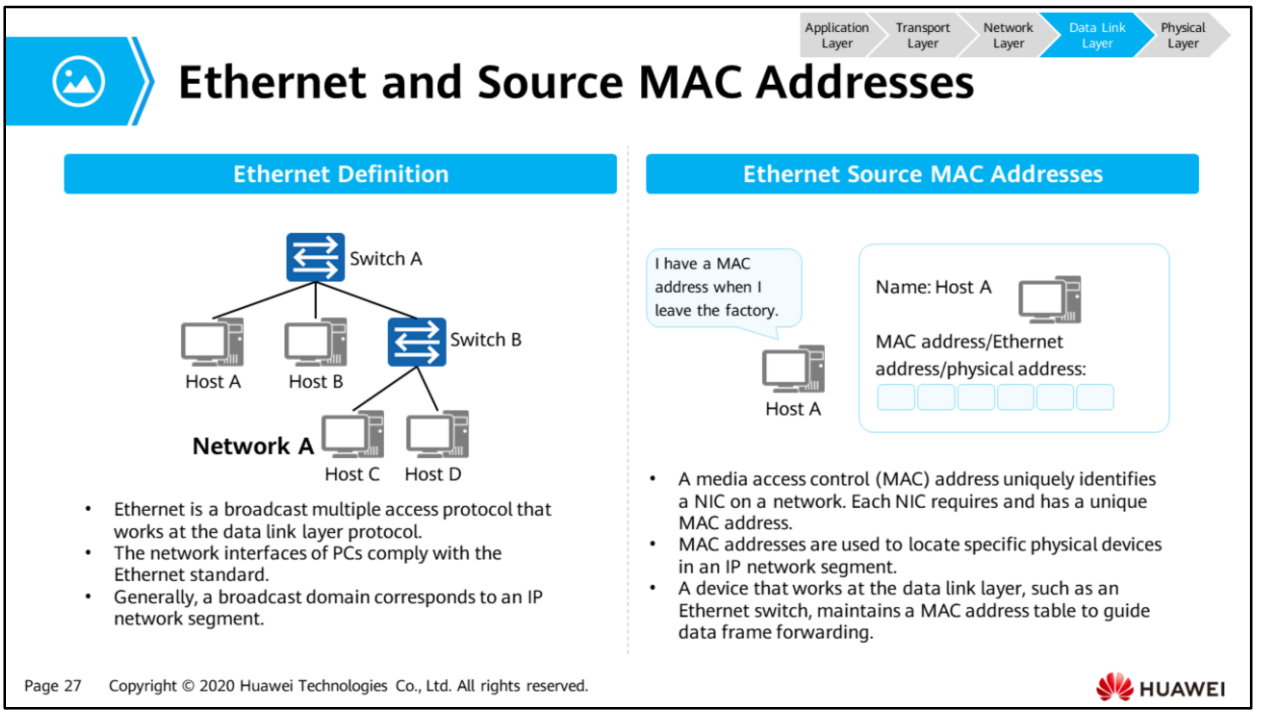
Data Link Layer

- The data link layer is located between the network layer and the physical layer and provides services for protocols such as IP and IPv6 at the network layer. PDUs transmitted at the data link layer are called frames.
- Ethernet is the most common data link layer protocol.

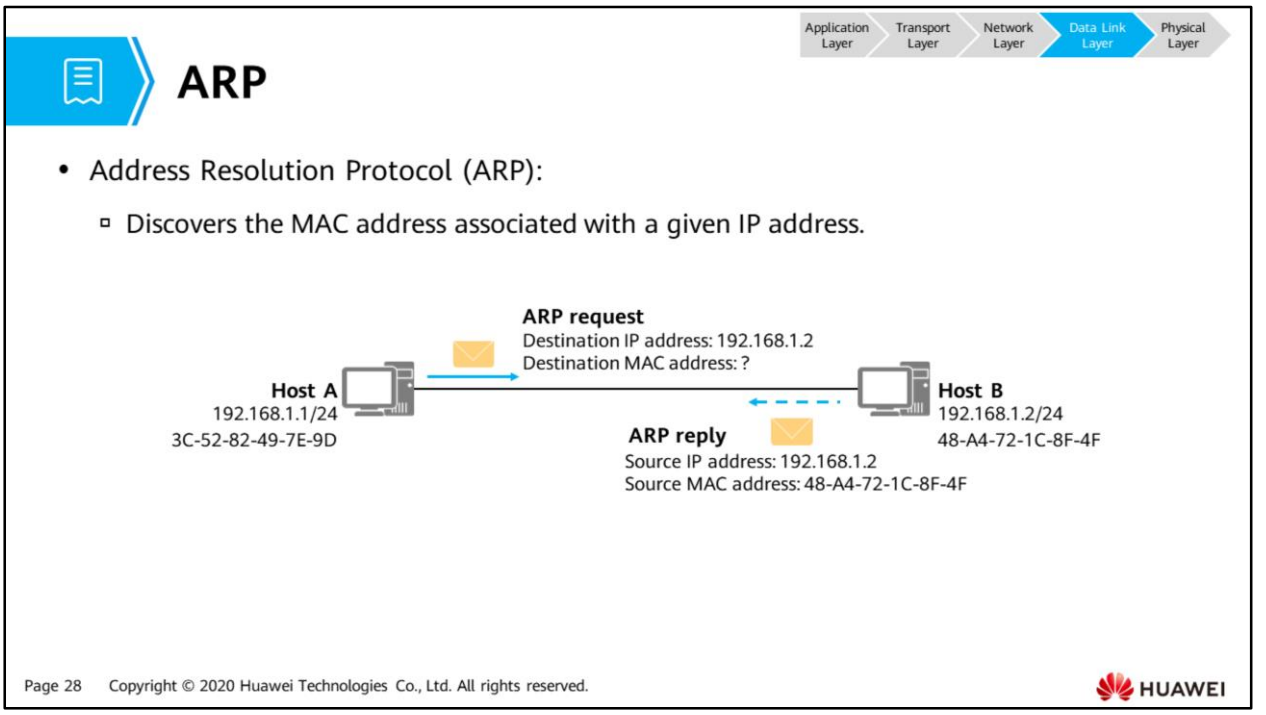


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

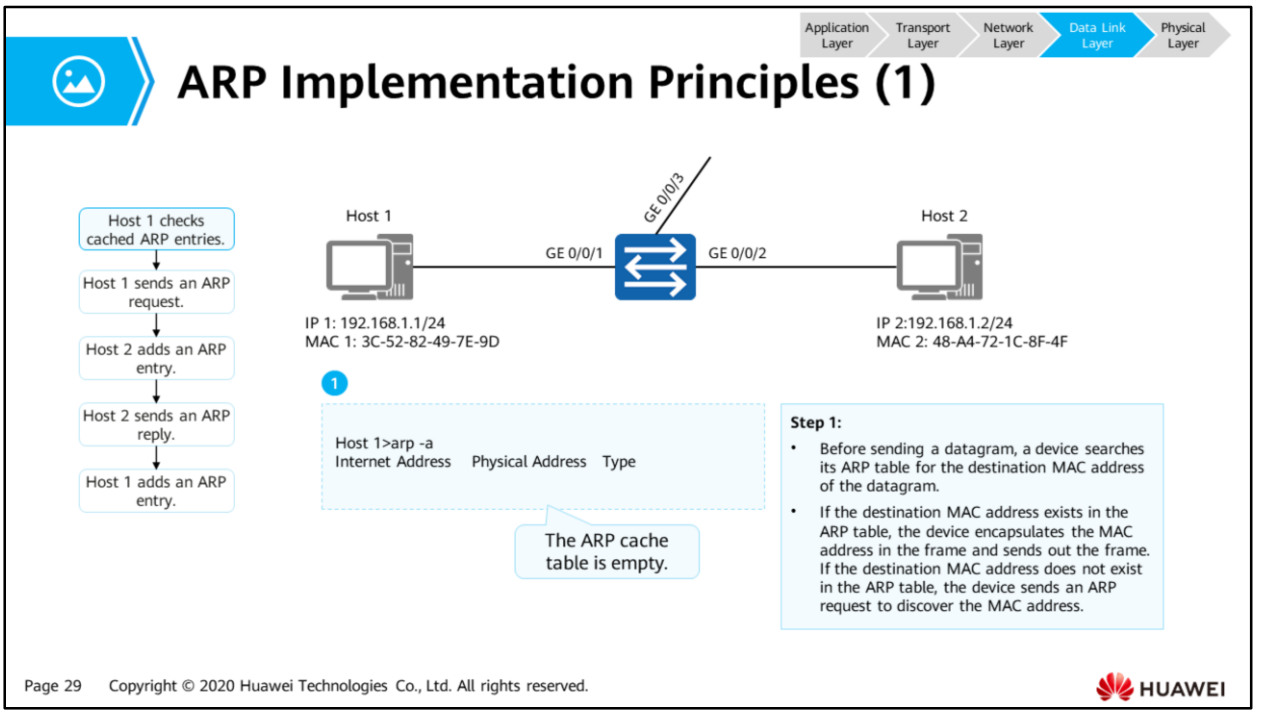
HUAWEI



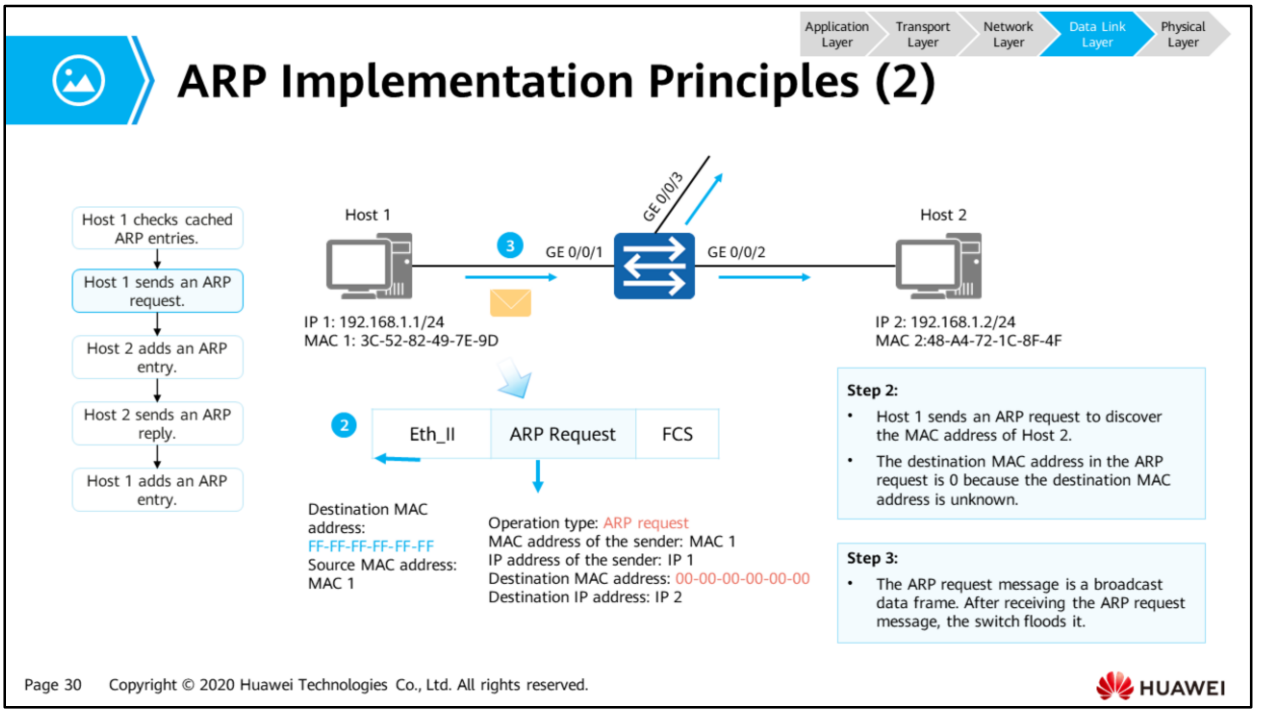
- A MAC address is recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator. Example: 48-A4-72-1C-8F-4F



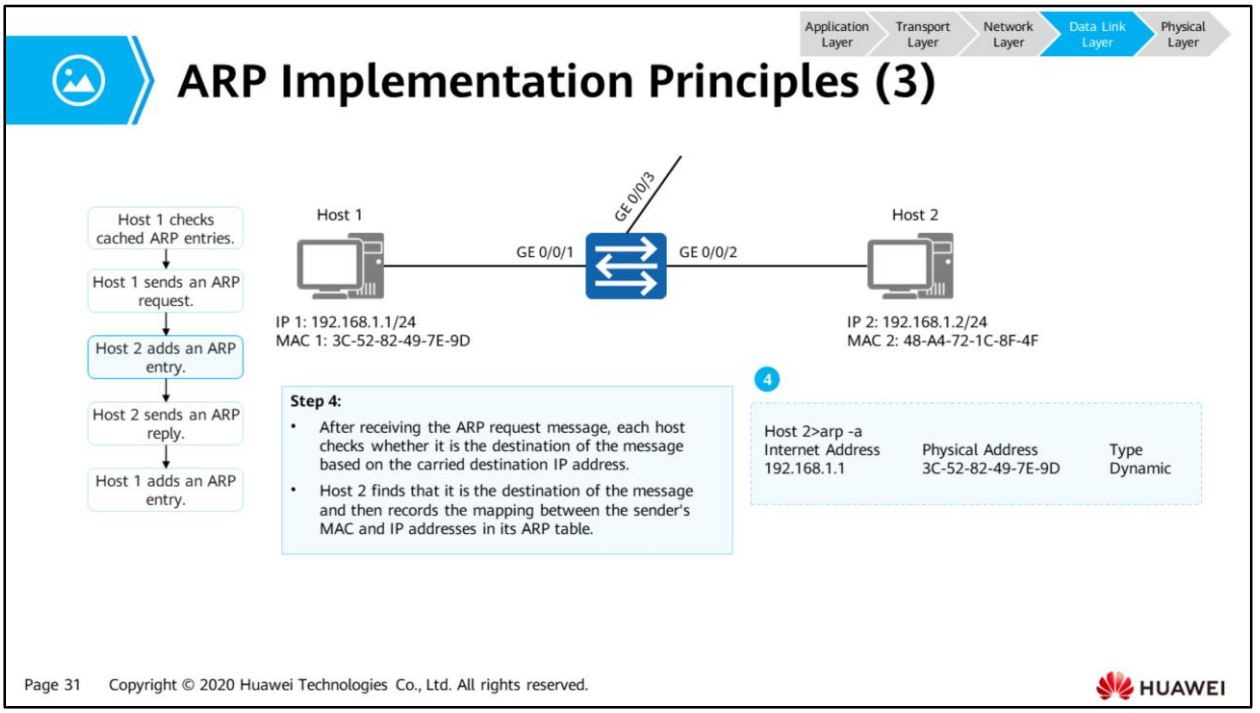
- The Address Resolution Protocol (ARP) is a TCP/IP protocol that discovers the data link layer address associated with a given IP address.
- ARP is an indispensable protocol in IPv4. It provides the following functions:
  - Discovers the MAC address associated with a given IP address.
  - Maintains and caches the mapping between IP addresses and MAC addresses through ARP entries.
  - Detects duplicate IP addresses on a network segment.



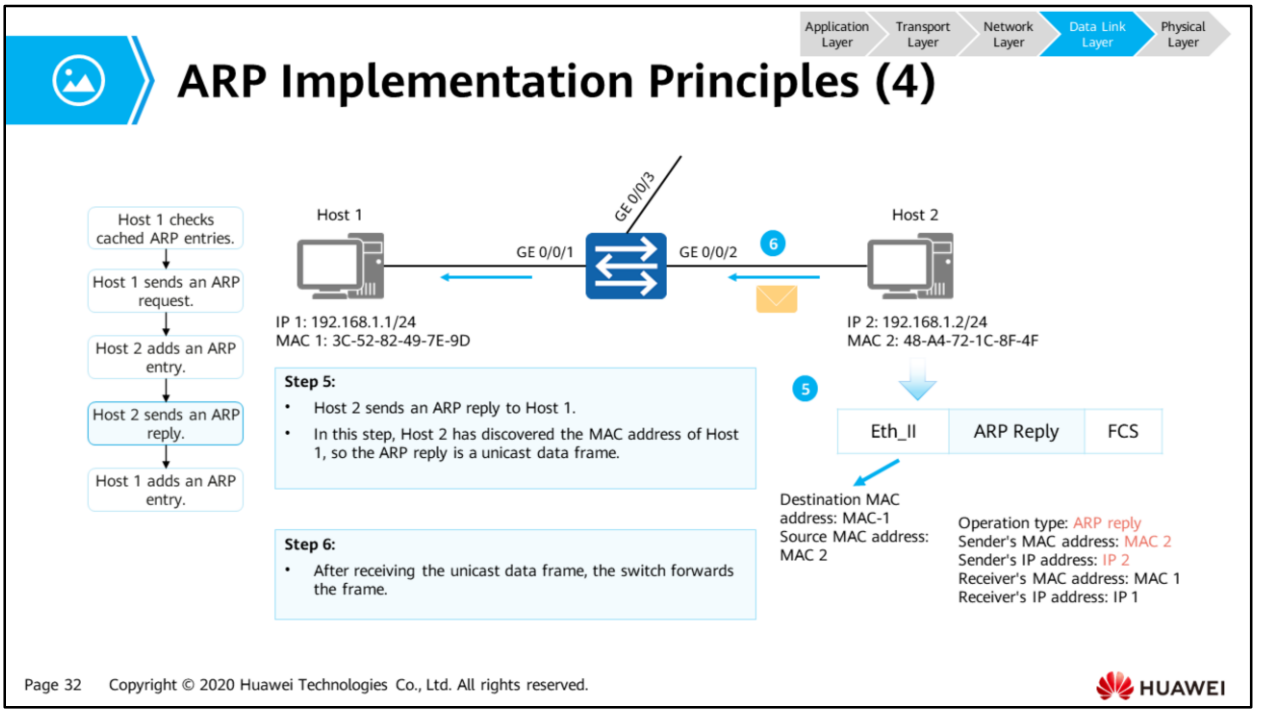
- Generally, a network device has an ARP cache. The ARP cache stores the mapping between IP addresses and MAC addresses.
- Before sending a datagram, a device searches its ARP table. If a matching ARP entry is found, the device encapsulates the corresponding MAC address in the frame and sends out the frame. If a matching ARP entry is not found, the device sends an ARP request to discover the MAC address.
- The learned mapping between the IP address and MAC address is stored in the ARP table for a period. Within the validity period (180s by default), the device can directly search this table for the destination MAC address for data encapsulation, without performing ARP-based query. After the validity period expires, the ARP entry is automatically deleted.
- If the destination device is located on another network, the source device searches the ARP table for the gateway MAC address of the destination address and sends the datagram to the gateway. Then, the gateway forwards the datagram to the destination device.



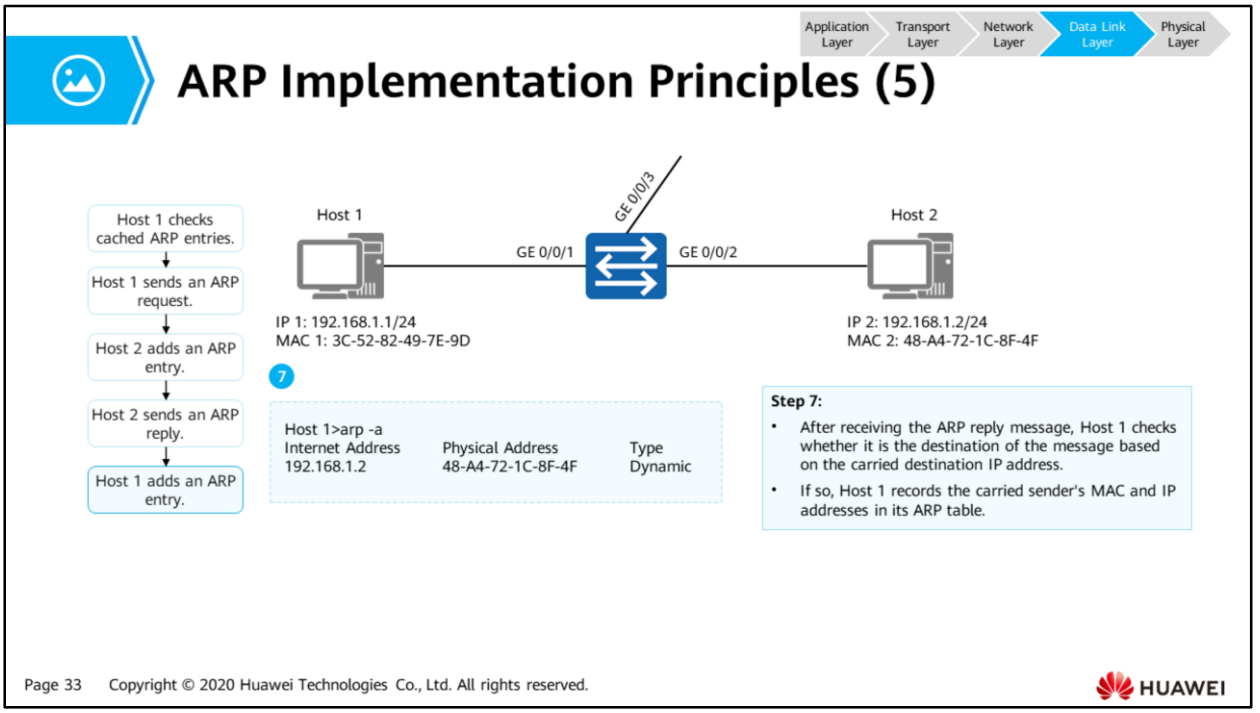
- In this example, the ARP table of Host 1 does not contain the MAC address of Host 2. Therefore, Host 1 sends an ARP request message to discover the destination MAC address.
- The ARP request message is encapsulated in an Ethernet frame. The source MAC address in the frame header is the MAC address of Host 1 at the transmit end. Because Host 1 does not know the MAC address of Host 2, the destination MAC address is the broadcast address FF-FF-FF-FF-FF-FF.
- The ARP request message contains the source MAC address, source IP address, destination MAC address, and destination IP address. The destination MAC address is all 0s. The ARP request message is broadcast to all hosts on the network, including gateways.



- After receiving the ARP request message, each host checks whether it is the destination of the message based on the carried destination IP address. If not, the host does not respond to the ARP request message. If so, the host adds the sender's MAC and IP addresses carried in the ARP request message to the ARP table, and then replies with an ARP reply message.



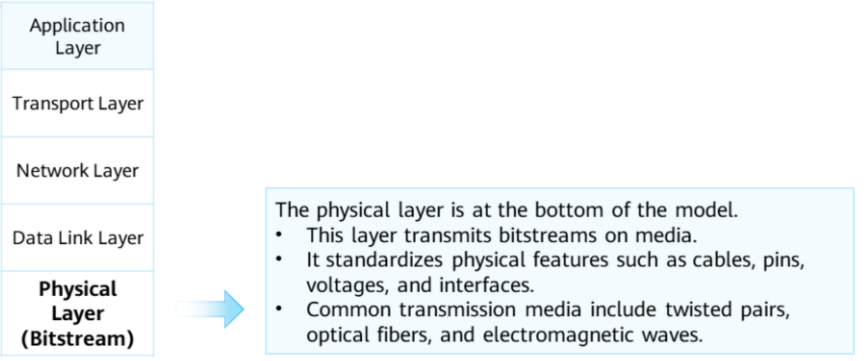
- Host 2 sends an ARP reply message to Host 1.
- In the ARP reply message, the sender's IP address is the IP address of Host 2 and the receiver's IP address is the IP address of Host 1. The receiver's MAC address is the MAC address of Host 1 and the sender's MAC address is the MAC address of Host 2. The operation type is set to reply.
- ARP reply messages are transmitted in unicast mode.



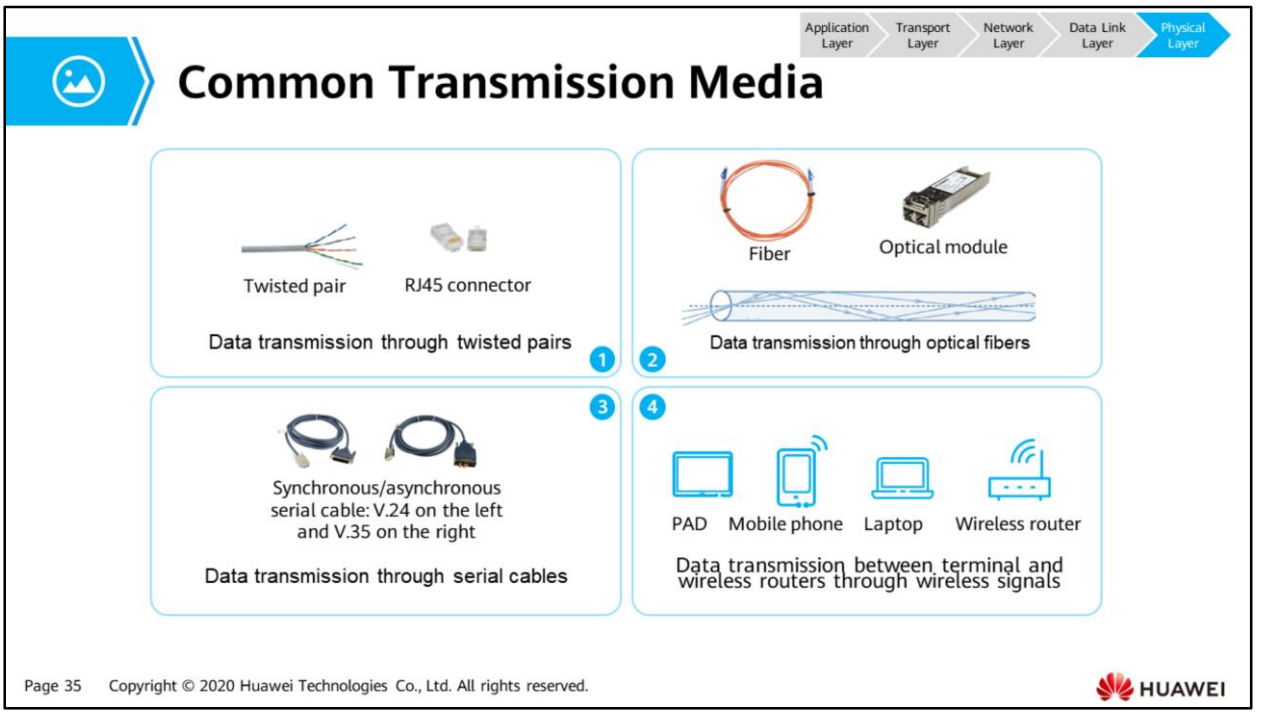
- After receiving the ARP reply message, Host 1 checks whether it is the destination of the message based on the carried destination IP address. If so, Host 1 records the carried sender's MAC and IP addresses in its ARP table.

Physical Layer

- After data arrives at the physical layer, the physical layer converts a digital signal into an optical signal, an electrical signal, or an electromagnetic wave signal based on the physical media.
- PDUs transmitted at the physical layer are called bitstreams.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

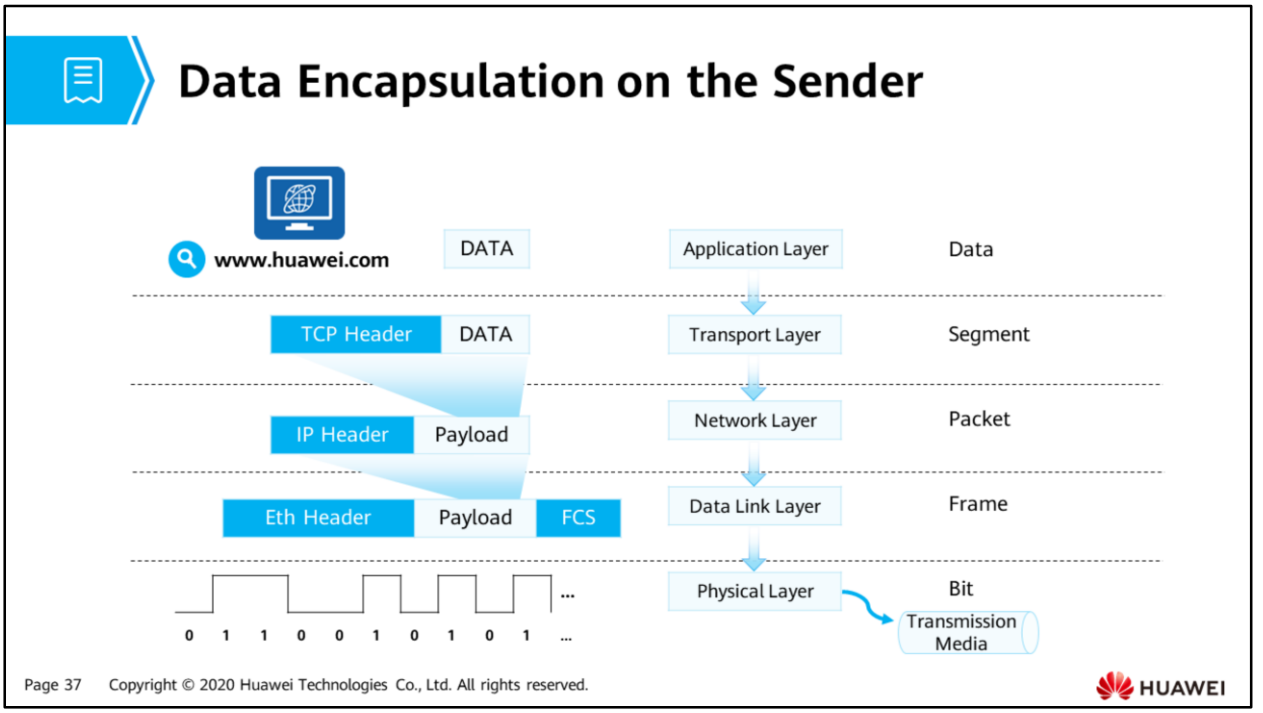


- Twisted pairs: most common transmission media used on Ethernet networks. Twisted pairs can be classified into the following types based on their anti-electromagnetic interference capabilities:
  - STP: shielded twisted pairs
  - UTP: unshielded twisted pairs
- Optical fiber transmission can be classified into the following types based on functional components:
  - Fibers: optical transmission media, which are glass fibers, used to restrict optical transmission channels.
  - Optical modules: convert electrical signals into optical signals to generate optical signals.
- Serial cables are widely used on wide area networks (WANs). The types of interfaces connected to serial cables vary according to WAN line types. The interfaces include synchronous/synchronous serial interfaces, ATM interfaces, POS interfaces, and CE1/PRI interfaces.
- Wireless signals may be transmitted by using electromagnetic waves. For example, a wireless router modulates data and sends the data by using electromagnetic waves, and a wireless network interface card of a mobile terminal demodulates the electromagnetic waves to obtain data. Data transmission from the wireless router to the mobile terminal is then complete.

Contents

1. Applications and Data
2. Network Reference Model and Standard Protocols
3. **Data Communication Process**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

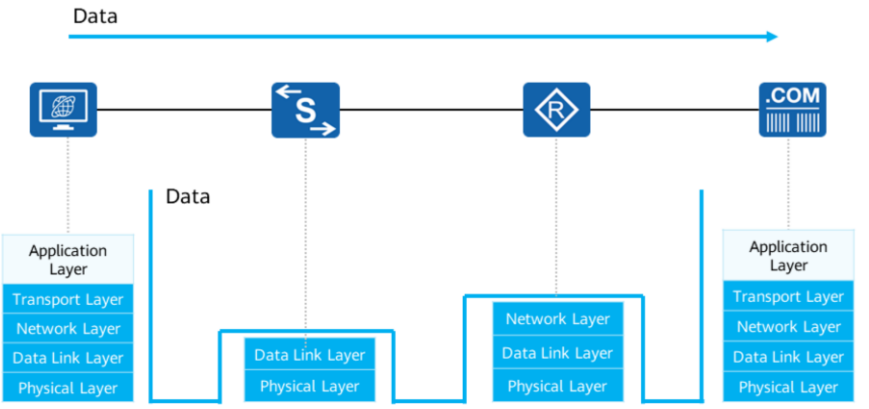


- Assume that you are using a web browser to access Huawei's official website. After you enter the website address and press Enter, the following events occur on your computer:
    1. The browser (application program) invokes HTTP (application layer protocol) to encapsulate the application layer data. (The DATA in the figure should also include the HTTP header, which is not shown here.)
    2. HTTP uses TCP to ensure reliable data transmission and transmits encapsulated data to the TCP module.
    3. The TCP module adds the corresponding TCP header information (such as the source and destination port numbers) to the data transmitted from the application layer. At the transport layer, the PDU is called a segment.
    4. On an IPv4 network, the TCP module sends the encapsulated segment to the IPv4 module at the network layer. (On an IPv6 network, the segment is sent to the IPv6 module for processing.)
    5. After receiving the segment from the TCP module, the IPv4 module encapsulates the IPv4 header. At this layer, the PDU is called a packet.

- Ethernet is used as the data link layer protocol. Therefore, after the IPv4 module completes encapsulation, it sends the packet to the Ethernet module (such as the Ethernet NIC) at the data link layer for processing.
- After receiving the packet from the IPv4 module, the Ethernet module adds the corresponding Ethernet header and FCS frame trailer to the packet. At this layer, the PDU is called a frame.
- After the Ethernet module completes encapsulation, it sends the data to the physical layer.
- Based on the physical media, the physical layer converts digital signals into electrical signals, optical signals, or electromagnetic (wireless) signals.
- The converted signals start to be transmitted on the network.

Data Transmission on the Intermediate Network

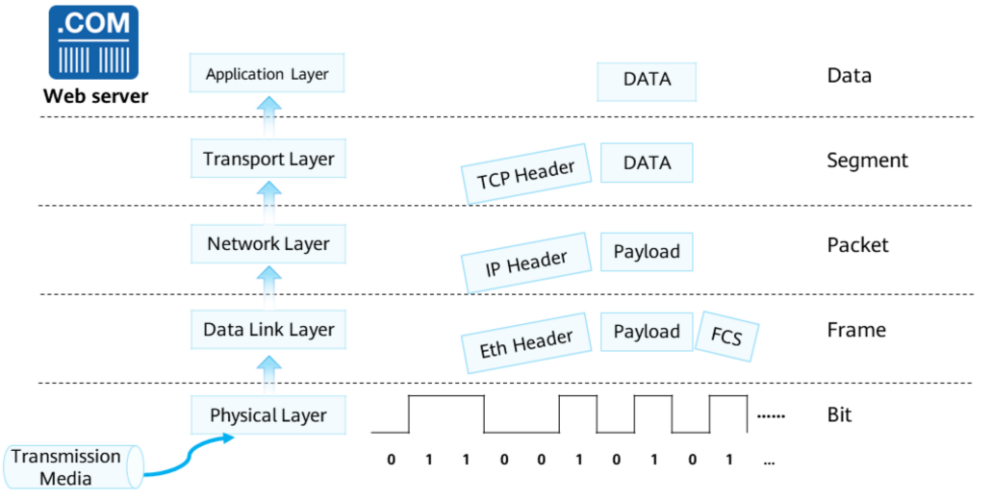
- Encapsulated data is transmitted on the network.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In most cases:
  - A Layer 2 device (such as an Ethernet switch) only decapsulates the Layer 2 header of the data and performs the corresponding switching operation according to the information in the Layer 2 header.
  - A Layer 3 device (such as a router) decapsulates the Layer 3 header and performs routing operations based on the Layer 3 header information.
  - Note: The details and principles of switching and routing will be described in subsequent courses.

Data Decapsulation on the Receiver



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- After being transmitted over the intermediate network, the data finally reaches the destination server. Based on the information in different protocol headers, the data is decapsulated layer by layer, processed, transmitted, and finally sent to the application on the web server for processing.

Summary

- Both the OSI reference model and the TCP/IP reference model adopt the layered design concept.
  - Clear division of functions and boundaries between layers facilitates the development, design, and troubleshooting of each component.
  - The functions of each layer can be defined to impel industry standardization.
  - Interfaces can be provided to enable communication between hardware and software on various networks, improving compatibility.
- Data generation and transmission require collaboration between modules. Meanwhile, each module must fulfill its own responsibilities.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Quiz

1. What are the benefits of the layered model?
2. What are the common protocols at the application layer, transport layer, network layer, and data link layer?

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. Answer:
   - Clear division of functions and boundaries between layers facilitates the development, design, and troubleshooting of each component.
   - The functions of each layer can be defined to impel industry standardization.
   - Interfaces can be provided to enable communication between hardware and software on various networks, improving compatibility.
2. Answer:
   - Application layer: HTTP, FTP, Telnet, and so on
   - Transport layer: UDP and TCP
   - Network layer: IP, ICMP, and so on
   - Data link layer: Ethernet, PPP, PPPoE, and so on


Thank You
www.huawei.com



Huawei VRP Basics

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- The Versatile Routing Platform (VRP) is a universal operating system (OS) platform for Huawei datacom products. It is based on IP and adopts a component-based architecture. It provides rich features and functions, including application-based tailorable and extensible functions, greatly improving the running efficiency of the devices that use this OS. To efficiently manage such devices, you must be familiar with VRP and VRP-based configuration.
- This course describes the basic concepts, common commands, and command line interface (CLI) of VRP.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand VRP basics.
  - Learn how to use CLI.
  - Master basic CLI commands.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

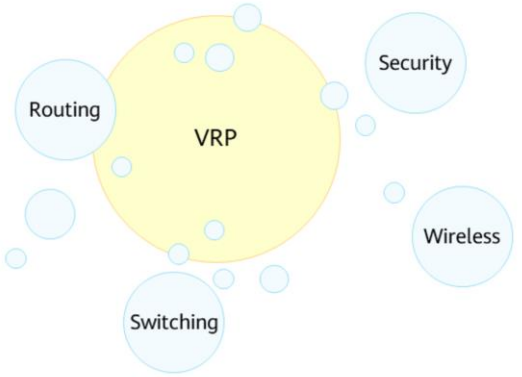
Contents

1. **VRP Overview**
2. Command Line Basics

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

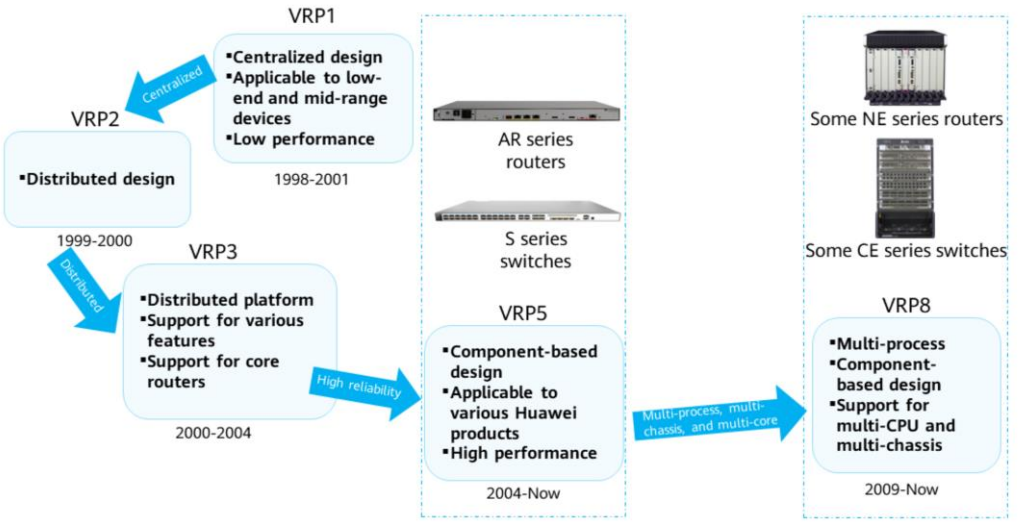
What Is VRP?



- VRP is a universal OS platform for Huawei datacom products. It serves as the software core engine of Huawei's full series of routers from low-end to core ones, Ethernet switches, service gateways, and so on.
- VRP provides the following functions:
  - Provides a unified user interface and a unified management interface.
  - Implements the functions of the control plane and defines the interface specifications of the forwarding plane.
  - Implements communication between the device forwarding plane and VRP control plane.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

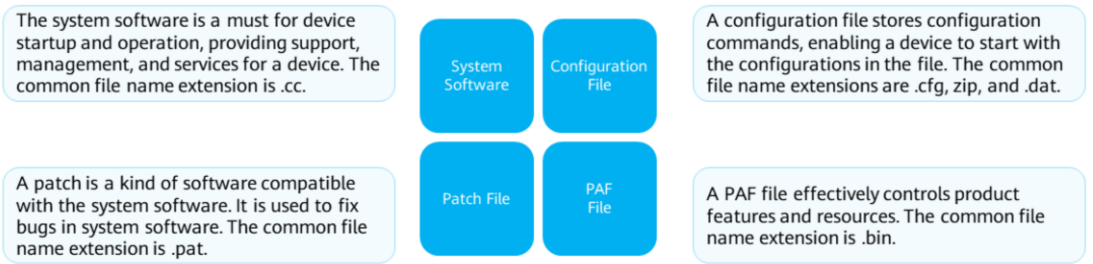
Development of the VRP



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

File System

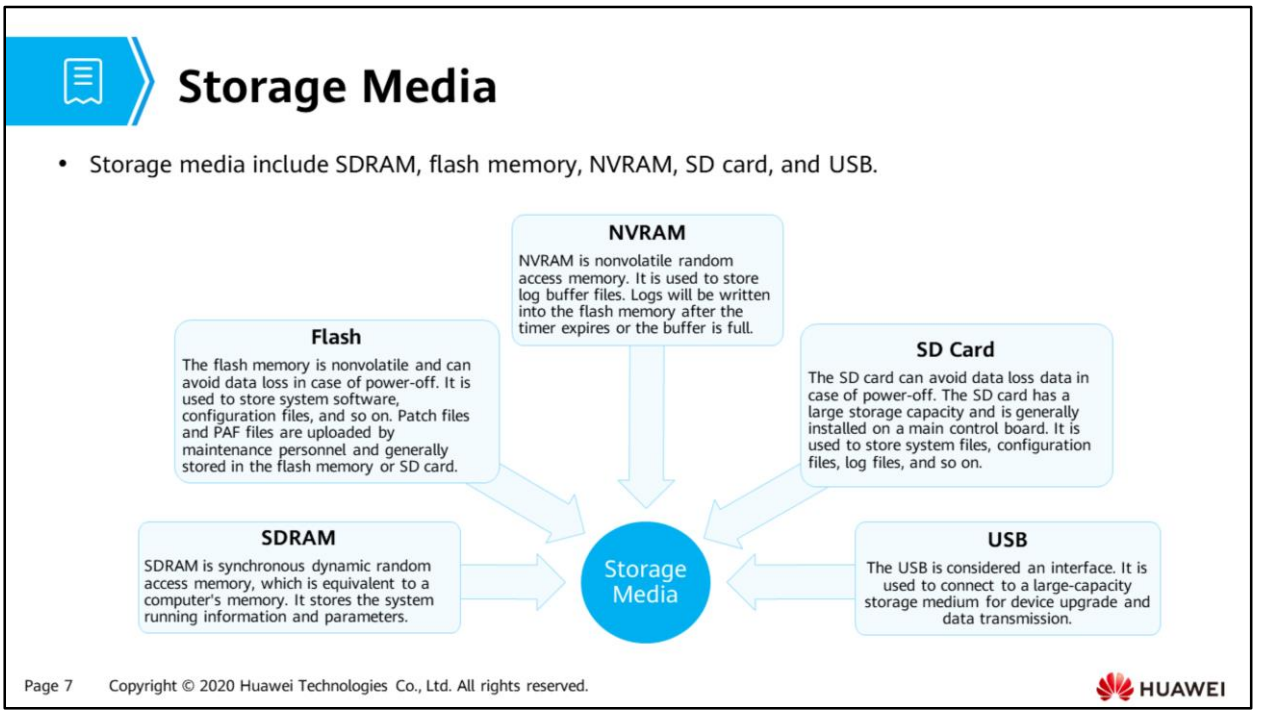
- The file system manages files and directories in storage media, allowing users to view, create, rename, and delete directories and copy, move, rename, and delete files.
- Mastering the basic operations of the file system is crucial for network engineers to efficiently manage the configuration files and VRP system files of devices.



Common File Types

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A configuration file is a collection of command lines. Current configurations are stored in a configuration file so that the configurations are still effective after the device restarts. Users can view configurations in the configuration file and upload the configuration file to other devices to implement batch configuration.
- A patch is a kind of software compatible with the system software. It is used to fix bugs in system software. Patches can also fix system defects and optimize some functions to meet service requirements.
- To manage files on a device, log in to the device through either of the following modes:
  - Local login through the console port or Telnet
  - Remote login through FTP, TFTP, or SFTP



- Storage media include SDRAM, flash memory, NVRAM, SD card, and USB.
  - SDRAM stores the system running information and parameters. It is equivalent to a computer's memory.
  - NVRAM is nonvolatile. Writing logs to the flash memory consumes CPU resources and is time-consuming. Therefore, the buffer mechanism is used. Specifically, logs are first saved to the buffer after being generated, and then written to the flash memory after the timer expires or the buffer is full.
  - The flash memory and SD card are nonvolatile. Configuration files and system files are stored in the flash memory or SD card. For details, see the product documentation.
  - SD cards are external memory media used for memory expansion. The USB is considered an interface. It is used to connect to a large-capacity storage medium for device upgrade and data transmission.
  - Patch and PAF files are uploaded by maintenance personnel and can be stored in a specified directory.

Device Initialization Process

- After a device is powered on, it runs the BootROM software to initialize the hardware and display hardware parameters. Then, it runs the system software and reads the configuration file from the default storage path to perform initialization.

```
BIOS Creation Date : Jan  5 2013, 18:00:24
DDR DRAM init : OK
Start Memory Test ? ('t' or 'T' is test):skip
Copying Data : Done
Uncompressing : Done
......
Press Ctrl+B to break auto startup ... 1
Now boot from flash:/AR2220E-V200R007C00SPC600.cc,
......
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Boot Read-Only Memory (BootROM) is a set of programs added to the ROM chip of a device. BootROM stores the device's most important input and output programs, system settings, startup self-check program, and system automatic startup program.
- The startup interface provides the information about the running program of the system, the running VRP version, and the loading path.

Device Management

- There are two commonly used device management modes: CLI and web system.
- To use a device management mode, you must first log in to a device through a login mode supported by this device management mode.

Web System	CLI
• The web system provides a graphical user interface (GUI) for easy device management and maintenance. This method, however, can be used to manage and maintain only some, not all, device functions. • The web system supports the HTTP and HTTPS login modes.	• The CLI requires users to use commands provided by a device to manage and maintain the device. This mode implements refined device management but requires users to be familiar with the commands. • The CLI supports the console port, Telnet, and SSH login modes.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

VRP User Interfaces

- When a user logs in to a device through a CLI-supported mode, the system allocates a user interface to manage and monitor the current session between the user terminal and device.
- Such a user interface can be a console user interface or virtual type terminal (VTY) user interface.

Console User Interface

- A console user interface is used to manage and monitor users who log in to a device through the console port.
- The serial port of a user terminal can be directly connected to the console port of a device for local access.

VTY User Interface

- The VTY user interface is used to manage and monitor users who log in to a device by means of VTY.
- After a Telnet or STelnet connection is established between a user terminal and a device, a VTY channel is established to implement remote access to the device.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

VRP User Levels

- VRP provides basic permission control functions. It defines the levels of commands that each level of users can execute to restrict the operations of users at different levels.

User Level	Command Level	Name	Available Command
0	0	Visit level	Network diagnosis commands (such as **ping** and **tracert**), commands for accessing external devices from the local device (such as Telnet client commands), and some display commands
1	0 and 1	Monitoring level	System maintenance commands, including display commands
2	0, 1, and 2	Configuration level	Service configuration commands, including routing commands and IP configuration commands, to directly provide users with network services
3-15	0, 1, 2, and 3	Management level	Commands for controlling basic system operations and providing support for services, including the file system, FTP, TFTP download, user management, and command level commands, as well as debugging commands for fault diagnosis

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- To limit users' access permissions to a device, the device manages users by level and establishes a mapping between user levels and command levels. After a user logs in to a device, the user can use only commands of the corresponding levels or lower. By default, the user command level ranges from 0 to 3, and the user level ranges from 0 to 15. The mapping between user levels and command levels is shown in the table.

Login to the Web System

Take the web system for a Huawei AR router as an example. Start a browser on a PC, enter **https://192.168.1.1** in the address bar, and press **Enter**. Then, the web system login page is displayed.





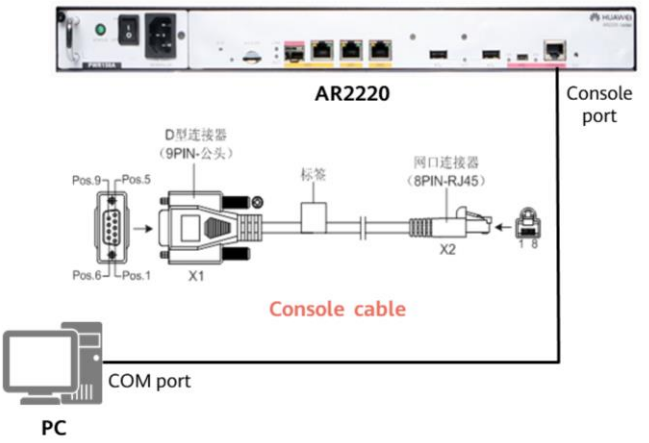
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Note: The login page, mode, and IP address may vary according to devices. For details, see the product documentation.

CLI - Local Login (1)

You can log in to a device in local or remote mode. Local login mode:

- Use this mode when you need to configure a device that is powered on for the first time. You can use the console port of the device for a local login.
- The console port is a serial port provided by the main control board of a device.
- To implement the login, directly connect your terminal's serial port to the device's console port, and use PuTTY to log in to the device. You can then configure the device after the login succeeds.



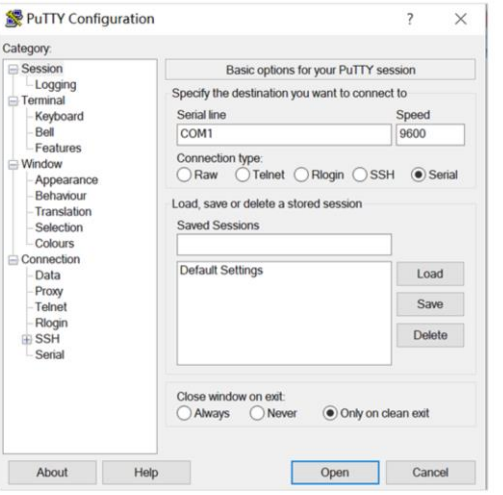
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Use a console cable to connect the console port of a device with the COM port of a computer. You can then use PuTTY on the computer to log in to the device and perform local commissioning and maintenance. A console port is an RJ45 port that complies with the RS232 serial port standard. At present, the COM ports provided by most desktop computers can be connected to console ports. In most cases, a laptop does not provide a COM port. Therefore, a USB-to-RS232 conversion port is required if you use a laptop.
- The console port login function is enabled by default and does not need to be pre-configured.

CLI - Local Login (2)

PuTTY is a connection software for login through Telnet, SSH, serial interfaces, and so on.

In local login, the terminal is connected to the console port of the Huawei device through a serial port. Therefore, set **Connection type** to **Serial**. Set **Serial line** based on the actually used port on the terminal. Set **Speed** to **9600**.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Many terminal simulators can initiate console connections. PuTTY is one of the options for connecting to VRP. If PuTTY is used for access to VRP, you must set port parameters. The figure in the slide shows examples of port parameter settings. If the parameter values were ever changed, you need to restore the default values.
- After the settings are complete, click Open. The connection with VRP is then set up.

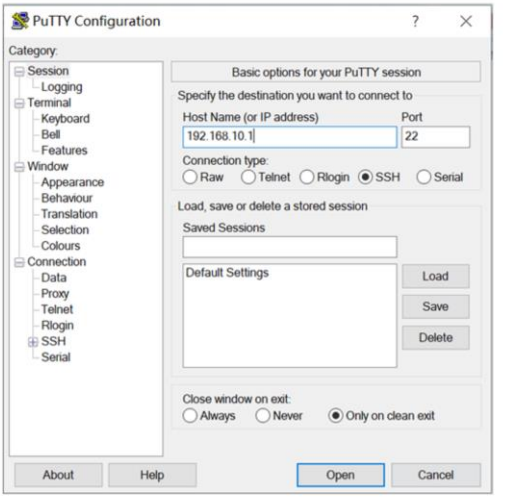
CLI - Remote Login

Remote login means that you log in to a device that can function as a remote login server, allowing you to centrally manage and maintain network devices. Remote login methods include Telnet and SSH.

- If you use the SSH login mode, set **Connection type** to **SSH**, enter the IP address of the remote login server, and use the default port number 22.
- If you use the Telnet login mode, set **Connection type** to **Telnet**, enter the IP address of the remote login server, and use the default port number 23.



192.168.10.1



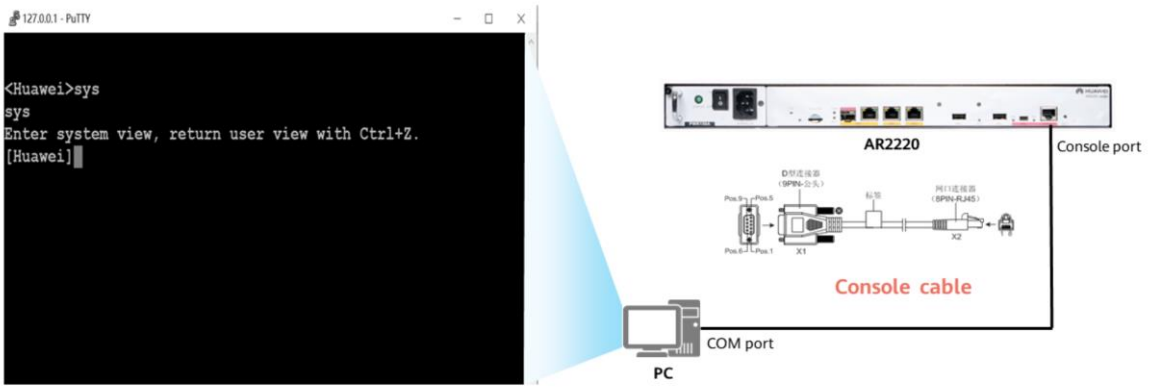
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- By default, the SSH login function is disabled on a device. You need to log in to the device through the console port and configure mandatory parameters for SSH login before using the SSH login function.

CLI

- After a login succeeds, the command line interface (CLI) is displayed.
- The CLI is a common tool for engineers to interact with network devices.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The CLI is an interface through which users can interact with a device. When the command prompt is displayed after a user logs in to a device, it means that the user has entered the CLI successfully.

Contents

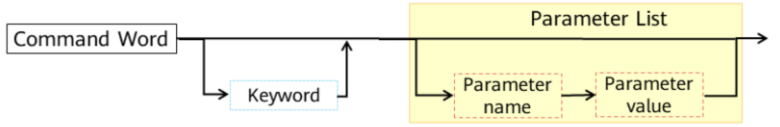
1. VRP Basics
2. **Command Line Basics**
   - **Command Line Overview**
   - Basic Configuration Commands
   - Case Analysis

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Basic Command Structure

- CLI commands follow a unified structure. After a command is entered on the CLI, the CLI parses the command and executes it to implement the function of the command, such as query, configuration, or management.



- **Command word**: specifies the operation to be executed in a command, such as display (device status query) or reboot (device restart).
- **Keyword**: a special character string that is used to further restrict a command. It is an extension of a command and can also be used to express the command composition logic.
- **Parameter list**: is composed of parameter names and values to further restrict the command function. It can contain one or more pairs of parameter names and values.

Example 1:
display ip interface GE0/0/0: displays interface information.
Command word: display
Keyword: ip
Parameter name: interface
Parameter value: GE0/0/0

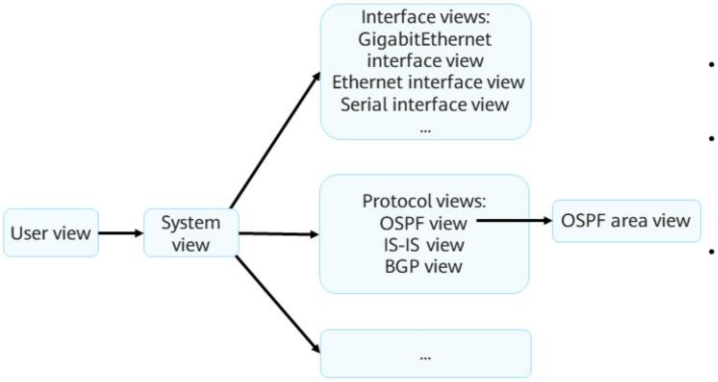
Example 2:
reboot: restarts a device.
Command word: reboot
Each operation command must start with a command word, and the command word is selected from the standard command word list.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Each command must contain a maximum of one command word and can contain multiple keywords and parameters. A parameter must be composed of a parameter name and a parameter value.
- The command word, keywords, parameter names, and parameter values in a command are separated by spaces.

Command Views (1)

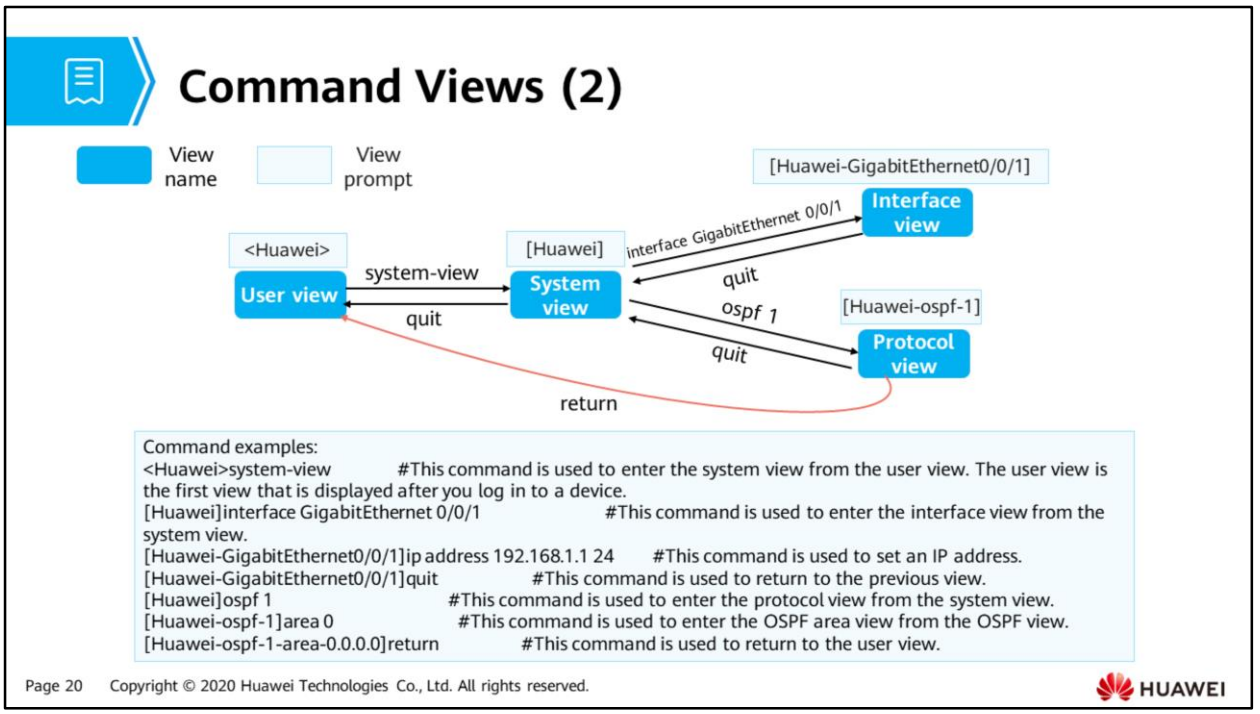
- A device provides various configuration and query commands. To facilitate the use of these commands, VRP registers the commands in different views according to their functions.



- User view: In this view, you can check the running status and statistics of a device.
- System view: In this view, you can set system parameters and enter the configuration views of other commands.
- Other views: In other views, such as the interface view and protocol view, you can set interface parameters and protocol parameters.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The user view is the first view displayed after you log in to a device. Only query and tool commands are provided in the user view.
- In the user view, only the system view can be accessed. Global configuration commands are provided in the system view. If the system has a lower-level configuration view, the command for entering the lower-level configuration view is provided in the system view.



- After you log in to the system, the user view is displayed first. This view provides only display commands and tool commands, such as **ping** and **telnet**. It does not provide any configuration commands.
- You can run the **system-view** command in the user view to enter the system view. The system view provides some simple global configuration commands.
- In a complex configuration scenario, for example, multiple parameters need to be configured for an Ethernet interface, you can run the **interface GigabitEthernet** *X* command (*X* indicates the number of the interface) to enter the GE interface view. Configurations performed in this view take effect only on the specified GE interface.

Editing a Command (1)

- The CLI of a device provides basic command editing functions. Common editing functions are as follows:

1. Command editing through function keys

- Backspace: deletes the character before the cursor and moves the cursor to the left. When the cursor reaches the beginning of the command, an alarm is generated.
- Left cursor key ← or **Ctrl+B**: moves the cursor one character to the left. When the cursor reaches the beginning of the command, an alarm is generated.
- Right cursor key → or **Ctrl+F**: moves the cursor one character to the right. When the cursor reaches the end of the command, an alarm is generated.

2. Incomplete keyword input

- A device allows the input of incomplete keywords. Specifically, if an entered character string can match a unique keyword, you do not need to enter the remaining characters of the keyword.

```
<Huawei>d cu
<Huawei>di cu
<Huawei>dis cu
<Huawei>d c
        ^
Error:Ambiguous command found at '^' position.
<Huawei>dis c
           ^
Error:Ambiguous command found at '^' position.
```

For example, the **display current-configuration** command is identified when you enter **d cu**, **di cu**, or **dis cu**. However, the command cannot be identified if you enter **d c** or **dis c** because the character string **d c** or **dis c** matches more than one command.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Note: "keyword" mentioned in this section means any character string except a parameter value string in a command. The meaning is different from that of "keyword" in the command format.

Editing a Command (2)

3. Command editing through the Tab key

- If an entered character string matches a unique keyword, the system automatically supplements the keyword after you press **Tab**. If the keyword is complete, it remains unchanged even if you press **Tab** repeatedly.

```
[Huawei] info-                  #Press Tab.
[Huawei] info-center
```

- If an entered character string matches more than one keyword, you can press **Tab** repeatedly. The system will then circularly display the keywords beginning with the entered character string to help you find the desired keyword.

```
[Huawei] info-center log        #Press Tab.
[Huawei] info-center logbuffer  #Press Tab repeatedly to circularly display all matched keywords.
[Huawei] info-center logfile
[Huawei] info-center loghost
```

- If an entered character string cannot identify any keyword, the entered string remains unchanged after you press **Tab**.

```
[Huawei] info-center loglog     #Enter an incorrect keyword and press Tab.
[Huawei] info-center loglog
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Using Command Line Online Help

- You can use command line online help to obtain real-time help without memorizing a large number of complex commands.
- The online help can be classified into full help and partial help. To obtain the online help, enter a question mark (?) when using a command.

Full Help

- To obtain full help, press **?** after a view displayed. The system will then display all commands in the view and their descriptions.

```
<Huawei> ?
User view commands:
  arp-ping      ARP-ping
  autosave      <Group> autosave command group
  backup        Backup  information
  cd            Change current directory
  clear         Clear
  clock         Specify the system clock
...
```

Partial Help

- To obtain partial help, press **?** after you enter the start character or character string of a command. The system will then display all the commands that start with this character or character string.

```
<Huawei> d?
  debugging  <Group> debugging command group
  delete     Delete a file
  dialer     Dialer
  dir        List files on a filesystem
  display    Display information
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- The command help information displayed in this slide is for reference only, which varies according to devices.

Interpreting Command Line Error Messages

- If a command passes the syntax check, the system executes it. Otherwise, the system reports an error message.

```
[Huawei] sysname
         ^
Error:Incomplete command found at '^' position.        #A supplement needs to be made at the position pointed by the arrow.

[Huawei] router if 1.1.1.1
                ^
Error: Unrecognized command found at '^' position.      #An identification failure occurs at the position pointed by the arrow. Check whether the command is correct.

[Huawei] a
         ^
Error: Ambiguous command found at '^' position.    #More than one command matches the keyword at the position pointed by the arrow. In this example, it indicates that there are multiple keywords starting with a.

[Huawei-GigabitEthernet0/0/0]ospf cost 800000          #The parameter value at the position pointed by the arrow is invalid.
                             ^
Error: Wrong parameter found at '^' position.
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Using Undo Command Lines

- If a command begins with the keyword **undo**, it is an undo command. An undo command is generally used to restore a default configuration, disable a function, or delete a configuration. For example:
  - Run an undo command to restore a default configuration.

```
<Huawei> system-view
[Huawei] sysname Server
[Server] undo sysname
[Huawei]
```

  - Run an undo command disable a function.

```
<Huawei> system-view
[Huawei] ftp server enable
[Huawei] undo ftp server
```

  - Run an undo command to delete a configuration.

```
[Huawei]interface g0/0/1
[Huawei-GigabitEthernet0/0/1]ip address 192.168.1.1 24
[Huawei-GigabitEthernet0/0/1]undo ip address
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Using Command Line Shortcut Keys

- A device provides command shortcut keys to speed up and simplify command input.
- Command shortcut keys are classified into user-defined shortcut keys and system shortcut keys.

User-defined Shortcut Keys

- There are four user-defined shortcut keys: **Ctrl+G**, **Ctrl+L**, **Ctrl+O**, and **Ctrl+U**.
- You can associate a user-defined shortcut key with any command. After you press a shortcut key, the system will automatically run the command associated with the shortcut key.

```
<Huawei> system-view
[Huawei] hotkey ctrl_l "display tcp status"
```

System Shortcut Keys

- **CTRL_A**: moves the cursor to the beginning of the current line.
- **CTRL_B**: moves the cursor one character to the left.
- **CTRL_C**: stops the running of the current command.
- **CTRL_E**: moves the cursor to the end of the current line.
- **CTRL_X**: deletes all characters on the left of the cursor.
- **CTRL_Y**: deletes the character at the cursor and all characters on the right of the cursor.
- **CTRL_Z**: returns to the user view.
- **CTRL+]**: terminates the current connection or switches to another connection.

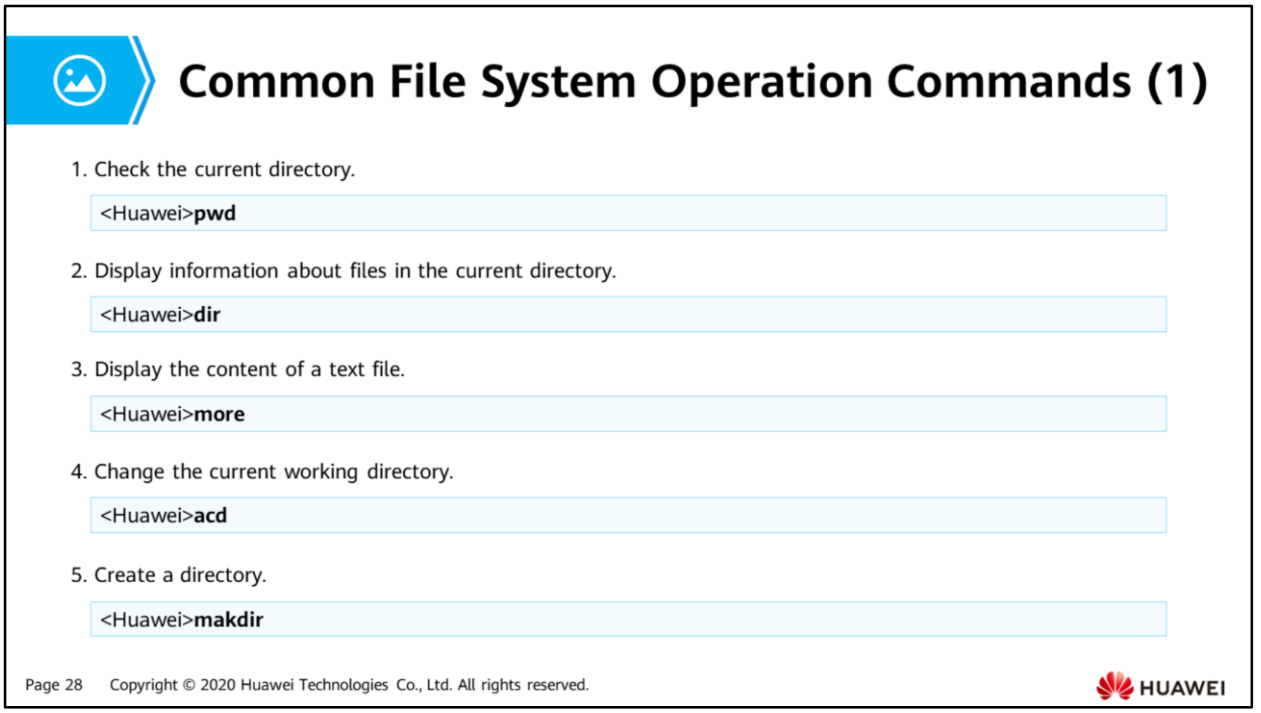
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

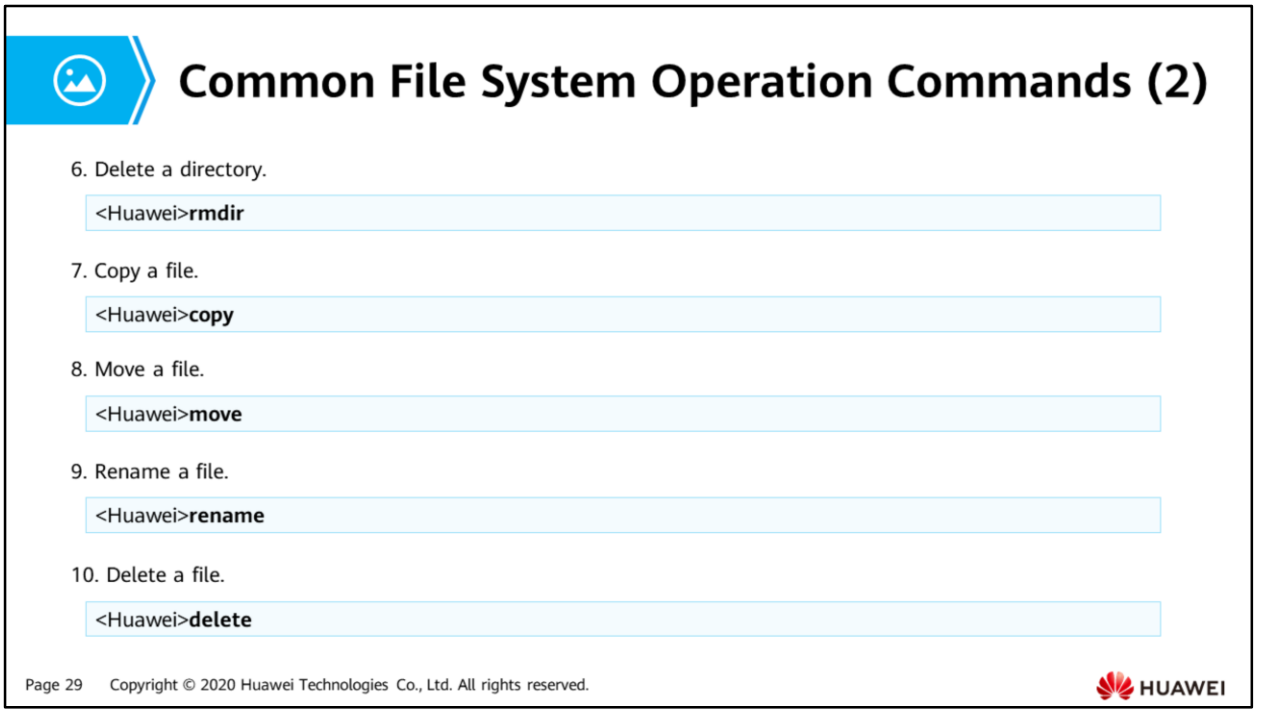
1. VRP Basics
2. **Command Line Basics**
   - Command Views and Use of Command Views
   - **Basic Configuration Commands**
   - Case Analysis

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

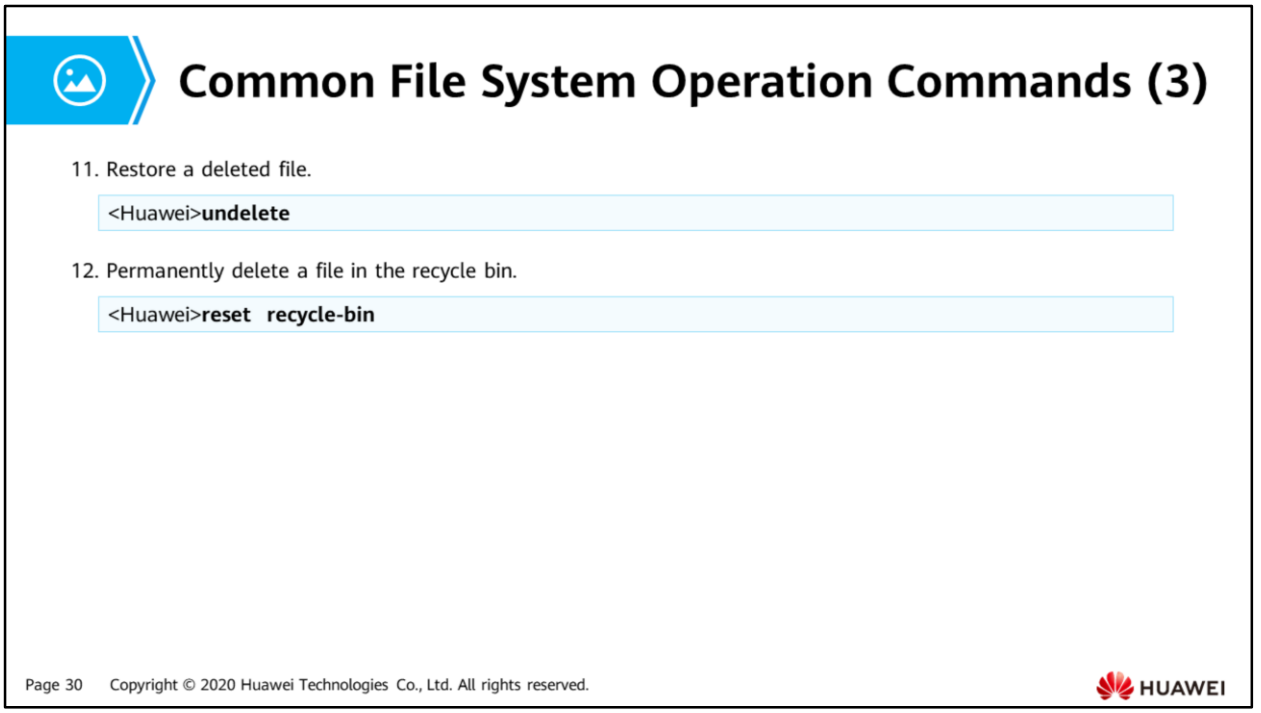
HUAWEI



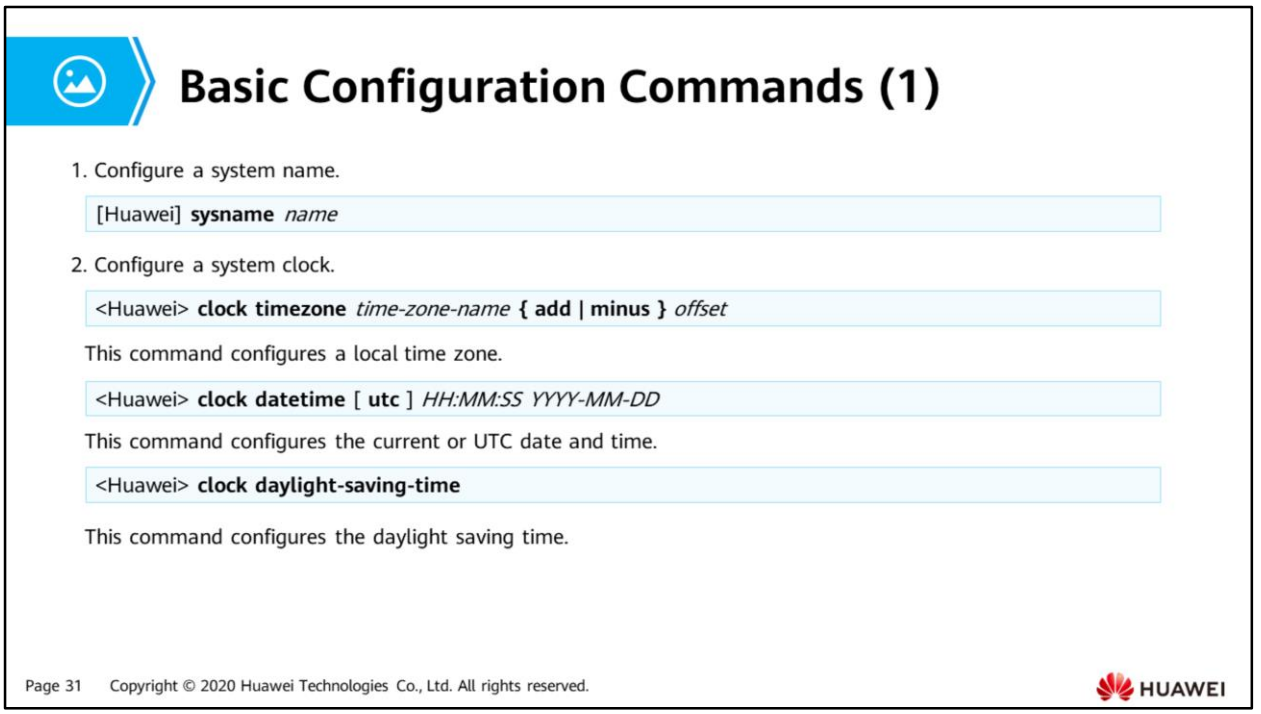
- VRP uses the file system to manages files and directories on a device. To manage files and directories, you often need to run basic commands to query file or directory information. Such commonly used basic commands include **pwd**, **dir [/all]** [*filename* | *directory*], and **more** [**/binary**] *filename* [*offset*] [**all**].
  - The **pwd** command displays the current working directory.
  - The **dir [/all]** [*filename* | *directory*] command displays information about files in the current directory.
  - The **more [/binary]** *filename* [*offset*] **[all]** command displays the content of a text file.
  - In this example, the **dir** command is run in the user view to display information about files in the flash memory.
- Common commands for operating directories include **cd** *directory*, **mkdir** *directory*, and **rmdir** *directory*.
  - The **cd** *directory* command changes the current working directory.
  - The **mkdir** *directory* command creates a directory. A directory name can contain 1 to 64 characters.



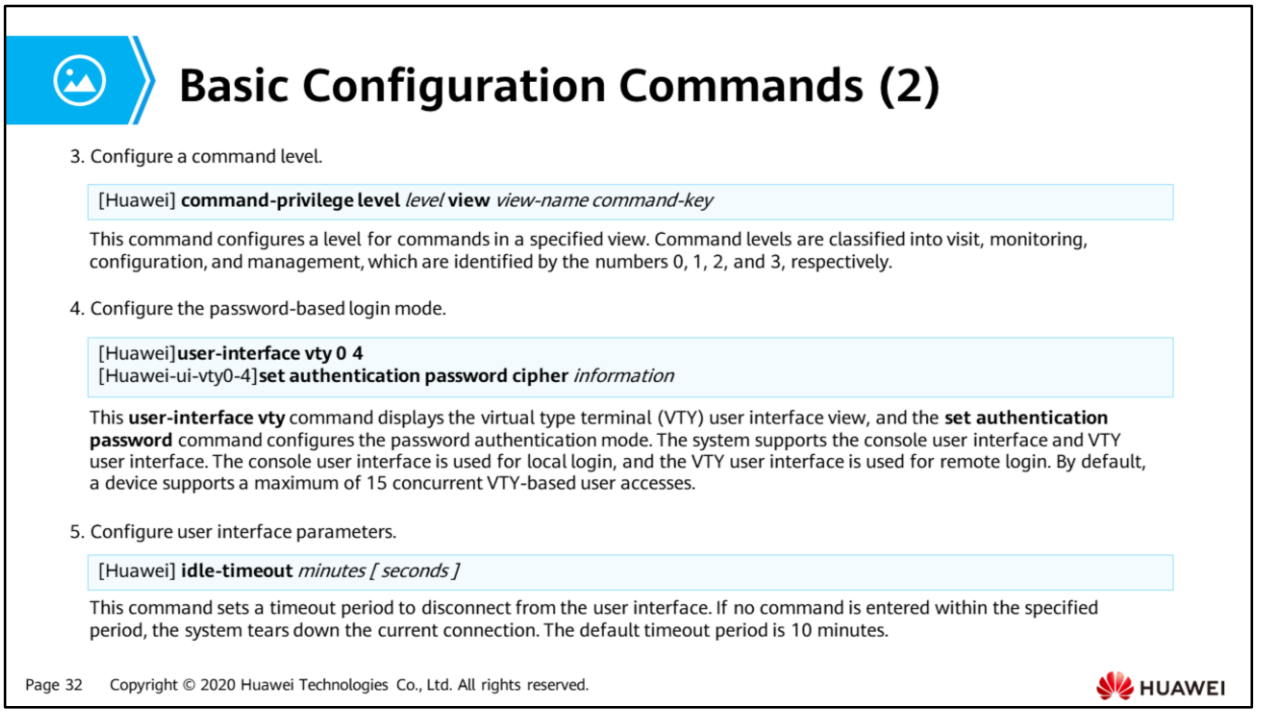
- The **rmdir** *directory* command deletes a directory from the file system. A directory to be deleted must be empty; otherwise, it cannot be deleted using this command.
- The **copy** *source-filename destination-filename* command copies a file. If the target file already exists, the system displays a message indicating that the target file will be replaced. The target file name cannot be the same as the system startup file name. Otherwise, the system displays an error message.
- The **move** *source-filename destination-filename* command moves a file to another directory. The **move** command can be used to move files only within the same storage medium.
- The **rename** *old-name new-name* command renames a directory or file.
- The **delete [/unreserved] [/force]** { *filename* | *devicename* } command deletes a file. If the *unreserved* parameter is not specified, the deleted file is moved to the recycle bin. A file in the recycle bin can be restored using the **undelete** command. However, if the **/unreserved** parameter is specified, the file is permanently deleted and cannot be restored any more. If the **/force** parameter is not specified in the **delete** command, the system displays a message asking you whether to delete the file. However, if the **/force** parameter is specified, the system does not display the message. *filename* specifies the name of the file to be deleted, and *devicename* specifies the name of the storage medium.



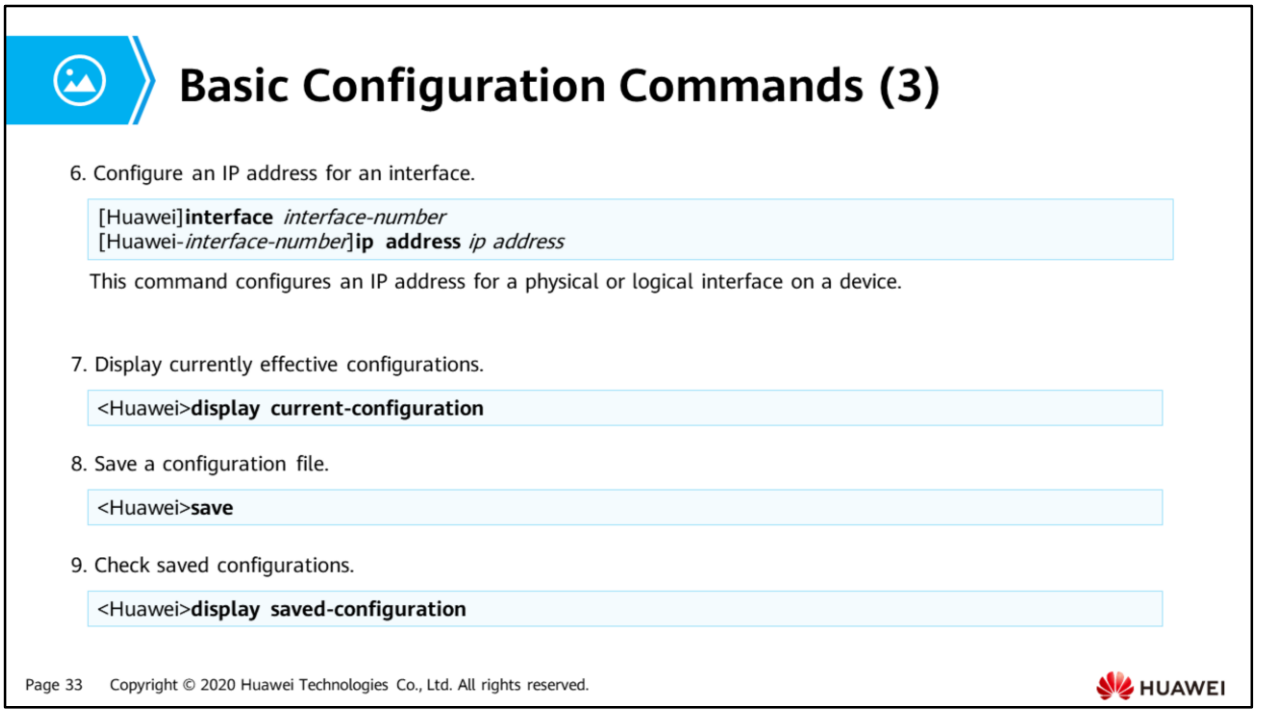
- The **reset recycle-bin** [*filename* | *devicename*] command permanently deletes all or a specified file in the recycle bin. *filename* specifies the name of the file to be permanently deleted, and *devicename* specifies the name of the storage medium.



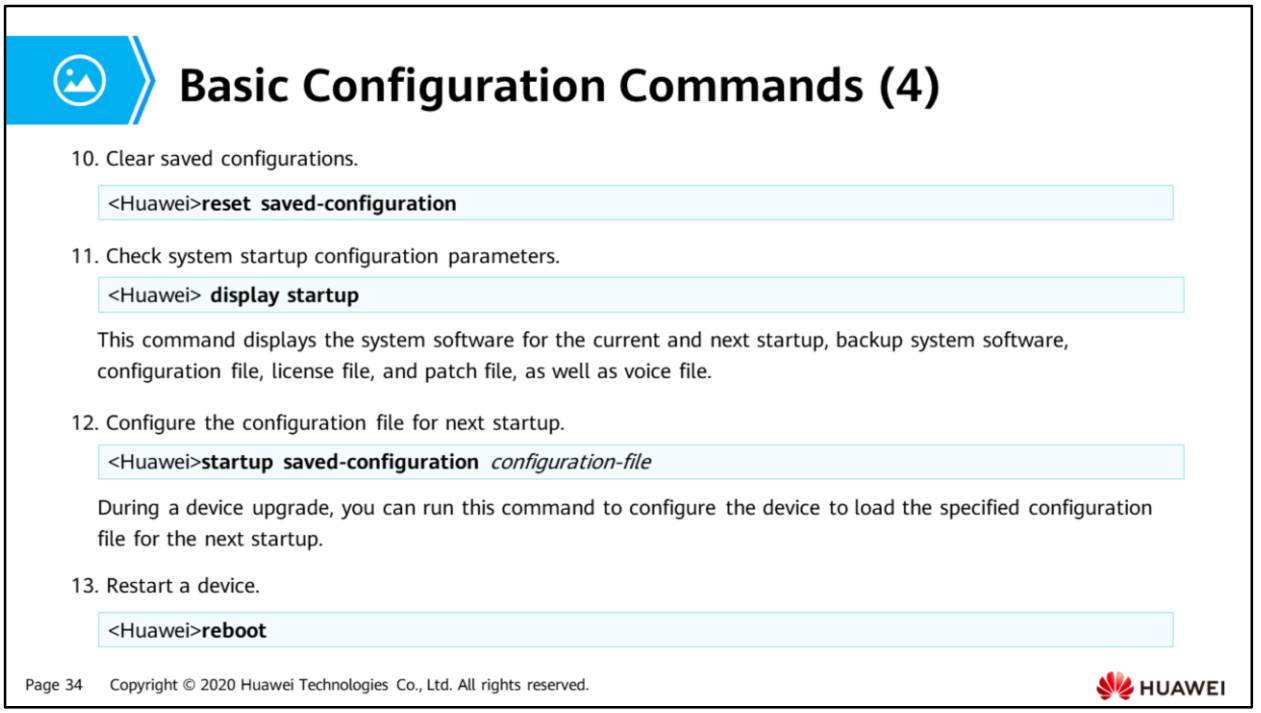
- Generally, more than one device is deployed on a network, and the administrator needs to manage all devices in a unified manner. The first task of device commissioning is to set a system name. A system name uniquely identifies a device. The default system name of an AR series router is Huawei, and that of an S series switch is HUAWEI. A system name takes effect immediately after being set.
- To ensure successful coordination with other devices, you need to correctly set the system clock. System clock = Coordinated Universal Time (UTC) ± Time difference between the UTC and the time of the local time zone. Generally, a device has default UTC and time difference settings.
    - You can run the **clock datetime** command to set the system clock of the device. The date and time format is HH:MM:SS YYYY-MM-DD. If this command is run, the UTC is the system time minus the time difference.
    - You can also change the UTC and the system time zone to change the system clock.
        - The **clock datetime utc** *HH:MM:SS YYYY-MM-DD* changes the UTC.
        - The **clock timezone** *time-zone-name* { **add** | **minus** } *offset* command configures the local time zone. The UTC is the local time plus or minus the offset.
    - If a region adopts the daylight saving time, the system time is adjusted according to the user setting at the moment when the daylight saving time starts. VRP supports the daylight saving time function.



- Each type of user interface has a corresponding user interface view. A user interface view is a command line view provided by the system for you to configure and manage all physical and logical interfaces working in asynchronous interaction mode, implementing unified management of different user interfaces. Before accessing a device, you need to set user interface parameters. The system supports console and VTY user interfaces. The console port is a serial port provided by the main control board of a device. A VTY is a virtual line port. A VTY connection is set up after a Telnet or SSH connection is established between a user terminal and a device, allowing the user to access the device in VTY mode. Generally, a maximum of 15 users can log in to a device through VTY at the same time. You can run the **user-interface maximum-vty** *number* command to set the maximum number of users that can concurrently access a device in VTY mode. If the maximum number of login users is set to 0, no user can log in to the device through Telnet or SSH. The **display user-interface** command displays information about a user interface.
- The maximum number of VTY interfaces may vary according to the device type and used VRP version.



- To run the IP service on an interface, you must configure an IP address for the interface. Generally, an interface requires only one IP address. For the same interface, a newly configured primary IP address replaces the original primary IP address.
- You can run the **ip address** { *mask* | *mask-length* } command to configure an IP address for an interface. In this command, *mask* indicates a 32-bit subnet mask, for example, 255.255.255.0; *mask-length* indicates a mask length, for example, 24. Specify either of them when configuring an IP address.
- A loopback interface is a logical interface that can be used to simulate a network or an IP host. The loopback interface is stable and reliable, and can also be used as the management interface if multiple protocols are deployed.
- When configuring an IP address for a physical interface, check the physical status of the interface. By default, interfaces are up on Huawei routers and switches. If an interface is manually disabled, run the **undo shutdown** command to enable the interface after configuring an IP address for it.



- The **reset saved-configuration** command deletes the configurations saved in a configuration file or the configuration file. After this command is run, if you do not run the **startup saved-configuration** command to specify the configuration file for the next startup or the **save** command to save current configurations, the device uses the default parameter settings during system initialization when it restarts.
- The **display startup** command displays the system software for the current and next startup, backup system software, configuration file, license file, and patch file, as well as voice file.
- The **startup saved-configuration** *configuration-file* command configures the configuration file for the next startup. The *configuration-file* parameter specifies the name of the configuration file for the next startup.
- The **reboot** command restarts a device. Before the device reboots, you are prompted to save configurations.

Contents

1. VRP Basics
2. **Command Line Basics**
   - Command Views and Use of Command Views
   - Basic Configuration Commands
   - **Case Analysis**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case 1: File Query Commands and Directory Operations

Requirement description:

- Check information about files and directories in the current directory of a router named RTA.
- Create a directory named **test**, and then delete the directory.



RTA

```
<Huawei>pwd
flash:
<Huawei>dir
Directory of flash:/
  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  drw-      -          Dec 27 2019  02:54:09  dhcp
    1  -rw-      121,802    May 26 2014 09:20:58  portalpage.zip
    2  -rw-      2,263      Dec 27 2019  02:53:59  statemach.efs
    3  -rw-      828,482    May 26 2014 09:20:58  sslvpn.zip

1,090,732 KB total (784,464 KB free)
<Huawei>mkdir test
<Huawei>dir
Directory of flash:/
  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  drw-      -          Dec 27 2019 02:54:39   test
    1  drw-      -          Dec 27 2019 02:54:09   dhcp
    2  -rw-      121,802    May 26 2014 09:20:58   portalpage.zip
    3  -rw-      2,263      Dec 27 2019 02:53:59   statemach.efs
    4  -rw-      828,482    May 26 2014 09:20:58   sslvpn.zip

1,090,732 KB total (784,460 KB free)
<Huawei>rmdir test
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case 2: File Operations (1)

Requirement description:

- Rename the **huawei.txt** file **save.zip**.
- Make a copy for the **save.zip** file and name the copy **file.txt**.
- Move the **file.txt** file to the **dhcp** directory.
- Delete the **file.txt** file.
- Restore the deleted file **file.txt**.



RTA

```
<Huawei>rename huawei.txt save.zip
<Huawei>dir
Directory of flash:/
Idx  Attr     Size(Byte)     Date        Time(LMT)    FileName
  0  drw-              -    Mar 04 2020 04:39:52    dhcp
  1  -rw-        121,802    May 26 2014 09:20:58    portalpage.zip
  2  -rw-        828,482    Mar 04 2020 04:51:45    save.zip
  3  -rw-          2,263    Mar 04 2020 04:39:45    statemach.efs
  4  -rw-        828,482    May 26 2014 09:20:58    sslvpn.zip

1,090,732 KB total (784,464 KB free)
<Huawei>copy save.zip file.txt
<Huawei>dir
Directory of flash:/
Idx  Attr     Size(Byte)     Date        Time(LMT)    FileName
  0  drw-              -    Mar 04 2020 04:39:52    dhcp
  1  -rw-        121,802    May 26 2014 09:20:58    portalpage.zip
  2  -rw-        828,482    Mar 04 2020 04:51:45    save.zip
  3  -rw-          2,263    Mar 04 2020 04:39:45    statemach.efs
  4  -rw-        828,482    May 26 2014 09:20:58    sslvpn.zip
  5  -rw-        828,482    Mar 04 2020 04:56:05    file.txt

1,090,732 KB total (784,340 KB free)
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case 2: File Operations (2)

Requirement description:

- Rename the **huawei.txt** file **save.zip**.
- Copy the **save.zip** file to the **file.txt** file.
- Move the **file.txt** file to the **dhcp** directory.
- Delete the **file.txt** file.
- Restore the deleted file **file.txt**.



RTA

```
<Huawei>move file.txt flash:/dhcp/
<Huawei>cd dhcp
<Huawei>dir
Directory of flash:/dhcp/
  Idx  Attr     Size(Byte)  Date        Time(LMT)    FileName
    0  -rw-           98    Dec 27 2019 02:54:09     dhcp-duid.txt
    1  -rw-      121,802    Dec 27 2019 03:13:50     file.txt

1,090,732 KB total (784,344 KB free)
<Huawei>delete file.txt
<Huawei>dir
Directory of flash:/dhcp/
  Idx  Attr     Size(Byte)  Date        Time(LMT)    FileName
    0  -rw-           98    Dec 27 2019 02:54:09     dhcp-duid.txt

1,090,732 KB total (784,340 KB free)
<Huawei>undelete file.txt
<Huawei>dir
Directory of flash:/dhcp/
  Idx  Attr     Size(Byte)  Date        Time(LMT)    FileName
    0  -rw-           98    Dec 27 2019 02:54:09     dhcp-duid.txt
    1  -rw-      121,802    Dec 27 2019 03:13:50     file.txt
1,090,732 KB total (784,340 KB free)
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case 3: VRP Basic Configuration Commands

- As shown in the figure, an engineer needs to configure a router. The requirements are as follows:
  - Connect the router and PC. Assign the IP addresses shown in the figure to the router and PC.
  - Allow other employees of the company to use the password **huawei123** to remotely log in to the router through the PC. Allow them to view configurations but disable them from modifying configurations.
  - Save current configurations and name the configuration file **huawei.zip**. Configure this file as the configuration file for the next startup.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Procedure (1)



Configure an interface IP address.

```
<Huawei>system-view
[Huawei]sysname AR1
[AR1]interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1]ip address 192.168.1.1 24
[AR1-GigabitEthernet0/0/1]quit
```

Configuring a user level and a user authentication mode.

```
[AR1]user-interface vty 0 4
[Huawei-ui-vty0-4]authentication-mode password
Please configure the login password (maximum length
16):huawei123
[AR1-ui-vty0-4]user privilege level 1
[AR1-ui-vty0-4]quit
```

The password configuration command may vary according to devices. For details, see the product documentation.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- For some devices, after the **authentication-mode password** command is entered, the password setting page will be displayed automatically. You can then enter the password at the page that is displayed. For some devices, you need to run the **set authentication-mode password** *password* command to set a password.

Configuration Procedure (2)



Specify the configuration file for next startup.

```
<HUAWEI>save huawei.zip
 Are you sure to save the configuration to huawei.zip? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<HUAWEI>startup saved-configuration huawei.zip
```

By default, configurations are saved in the **vrpcfg.cfg** file. You can also create a file for saving the configurations. VRPv5 and VRPv8 have the same command that is used to specify the configuration file for the next startup, but different directories for saving the file.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- To save configurations, run the **save** command. By default, configurations are saved in the **vrpcfg.cfg** file. You can also create a file for saving the configurations. In VRPv5, the configuration file is stored in the flash**:** directory by default.

Checking Configurations

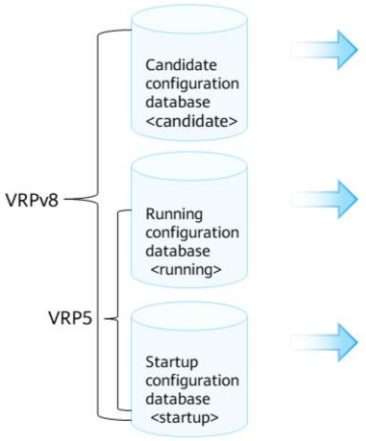



```
<AR1>display startup
MainBoard:
  Startup system software:                        null
  Next startup system software:                   null
  Backup system software for next startup:        null
  Startup saved-configuration  file:              flash:/vrpcfg.zip
  Next startup saved-configuration  file:         flash:/huawei.zip
  Startup license file:                           null
  Next startup license file:                      null
  Startup patch package:                          null
  Next startup patch package:                     null
  Startup voice-files:                            null
  Next startup voice-files:                       null
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- The **display startup** command displays the system software for the current and next startup, backup system software, configuration file, license file, and patch file, as well as voice file.
  - **Startup system software** indicates the VRP file used for the current startup.
  - **Next startup system software** indicates the VRP file to be used for the next startup.
  - **Startup saved-configuration file** indicates the configuration file used for the current system startup.
  - **Next startup saved-configuration file** indicates the configuration file to be used for the next startup.
  - When a device starts, it loads the configuration file from the storage medium and initializes the configuration file. If no configuration file exists in the storage medium, the device uses the default parameter settings for initialization.
- The **startup saved-configuration** [*configuration-file*] command sets the configuration file for the next startup, where the *configuration-file* parameter specifies the name of the configuration file.

More Information



<Huawei>display configuration candidate
This command displays the commands that have been configured but not committed.

If a series of configurations are completed but not committed, the command configurations are stored in the candidate configuration database.

<Huawei>display current-configuration
This command displays the effective parameter settings.

After configuration commands are committed, they are saved in the running configuration database.

<Huawei>display startup
The command displays the names of the system software, configuration files, PAF files, and patch files used for the current startup and to be used for the next startup.

After configurations are saved, the command configurations are stored in the startup configuration database.

VRPv5 has the running and startup configuration databases but does not have the candidate configuration database. Therefore, a command configuration takes effect immediately after the command is executed, without being committed. However, in VRPv8, the configuration command takes effect only after the command committed.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Quiz

1. What is the VRP version currently used by Huawei datacom devices?
2. What is the maximum number of users that are allowed to log in to a Huawei device through the console port concurrently?
3. How do I specify the configuration file for next startup if a device has multiple configuration files?

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. Currently, most Huawei datacom products use VRPv5, and a few products such as NE series routers use VRPv8.
2. A Huawei device allows only one user to log in through the console interface at a time. Therefore, the console user ID is fixed at 0.
3. To specify a configuration file for next startup, run the **startup saved-configuration** [*configuration-file*] command. The value of *configuration-file* should contain both the file name and extension.

Summary

- VRP is a Huawei proprietary network OS that can run on various hardware platforms. VRP has unified network, user, and management interfaces. To efficiently manage Huawei devices, you need to be familiar with VRP commands and configurations.
- You also need to understand some common commands and shortcut keys and learn how to use them.
- After learning this course, you need to know basic VRP concepts, functions of common commands, and CLI.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Network Layer Protocols and IP Addressing

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- Internet Protocol Version 4 (IPv4) is the core protocol suite in the TCP/IP protocol suite. It works at the network layer in the TCP/IP protocol stack and this layer corresponds to the network layer in the Open System Interconnection Reference Model (OSI RM).
- The network layer provides connectionless data transmission services. A network does not need to establish a connection before sending data packets. Each IP data packet is sent separately.
- This presentation describes the basic concepts of IPv4 addresses, subnetting, network IP address planning, and basic IP address configuration.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able:
  - Describe main protocols at the network layer.
  - Describe the concepts and classification of IPv4 addresses and special IPv4 addresses.
  - Calculate IP networks and subnets.
  - Use the IP network address planning method.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. **Network Layer Protocols**
2. Introduction to IPv4 Addresses
3. Subnetting
4. ICMP
5. IPv4 Address Configuration and Basic Application

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Network Layer Protocols

- The network layer is often called the IP layer. Network layer protocols include Internet Control Message Protocol (ICMP) and Internet Packet Exchange (IPX), in addition to IP.



Equivalent TCP/IP model

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Internet Protocol

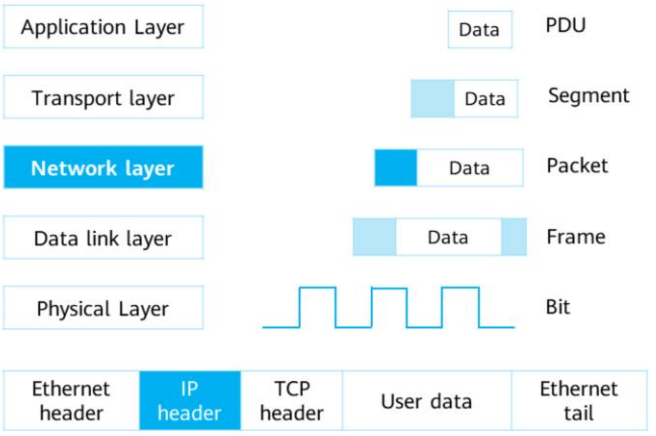
- IP is short for the Internet Protocol. IP is the name of a protocol file with small content. It defines and describes the format of IP packets.
- The frequently mentioned IP refers to any content related directly or indirectly to the Internet Protocol, instead of the Internet Protocol itself.

Function	Version
• Provides logical addresses for devices at the network layer. • Is responsible for addressing and forwarding data packets.	• IP Version 4 (IPv4) • IP Version 6 (IPv6)

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- IP has two versions: IPv4 and IPv6. IPv4 packets prevail on the Internet, and the Internet is undergoing the transition to IPv6. Unless otherwise specified, IP addresses mentioned in this presentation refer to IPv4 addresses.
    - IPv4 is the core protocol in the TCP/IP protocol suite. It works at the network layer in the TCP/IP protocol stack and this layer corresponds to the network layer in the Open System Interconnection Reference Model (OSI RM).
    - IPv6, also called IP Next Generation (IPng), is the second-generation standard protocol of network layer protocols. Designed by the Internet Engineering Task Force (IETF), IPv6 is an upgraded version of IPv4.

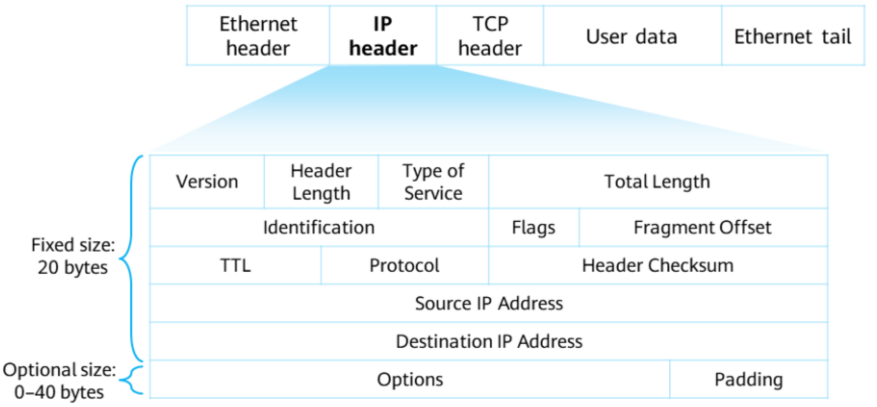
Data Encapsulation



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Application data can be transmitted to the destination end over the network only after being processed at each layer of the TCP/IP protocol suite. Each layer uses protocol data units (PDUs) to exchange information with another layer. PDUs at different layers contain different information. Therefore, PDUs at each layer have a particular name.
  - For example, after a TCP header is added to the upper-layer data in a PDU at the transport layer, the PDU is called a segment. The data segment is transmitted to the network layer. After an IP header is added to the PDU at the network layer, the PDU is called a packet. The data packet is transmitted to the data link layer. After the data link layer header and tailer are encapsulated into the PDU, the PDU becomes a frame. Ultimately, the frame is converted into bits and transmitted through network media.
  - The process in which data is delivered following the protocol suite from top to bottom and is added with headers and tails is called encapsulation.
- This presentation describes how to encapsulate data at the network layer. If data is encapsulated with IP, the packets are called IP packets.

IPv4 Packet Format



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The IP packet header contains the following information:
  - Version: 4 bits long. Value 4 indicates IPv4. Value 6 indicates IPv6.
  - Header Length: 4 bits long, indicating the size of a header. If the Option field is not carried, the length is 20 bytes. The maximum length is 60 bytes.
  - Type of Service: 8 bits long, indicating a service type. This field takes effect only when the QoS differentiated service (DiffServ) is required.
  - Total Length: 16 bits long. It indicates the total length of an IP data packet.
  - Identification: 16 bits long. This field is used for fragment reassembly.
  - Flags: 3 bits long.
  - Fragment Offset: 12 bits long. This field is used for fragment reassembly.
  - Time to Live: 8 bits long.

- Protocol: 8 bits long. It indicates a next-layer protocol. This field identifies the protocol used by the data carried in the data packet so that the IP layer of the destination host sends the data to the process mapped to the Protocol field.
  - Common values are as follows:
    - 1: ICMP, Internet Control Message Protocol
    - 2: IGMP, Internet Group Management Protocol
    - 6: TCP, Transmission Control Protocol
    - 17: UDP, User Datagram Protocol
- Header Checksum: 16 bits long.
- Source IP Address: 32 bits long. It indicates a source IP address.
- Destination IP Address: 32 bits long. It indicates a destination IP address.
- Options: a variable field.
- Padding: padded with all 0s.

Data Packet Fragmentation

- The process of dividing a packet into multiple fragments is called fragmentation.
- The sizes of IP packets forwarded on a network may be different. If the size of an IP packet exceeds the maximum size supported by a data link, the packet needs to be divided into several smaller fragments before being transmitted on the link.

Version	Header Length	Type of Service	Total Length
Identification		Flags	Fragment Offset
TTL	Protocol	Header Checksum	
Source IP Address			
Destination IP Address			
Options			Padding



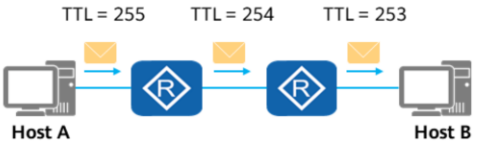
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Identification: 16 bits long. This field carries a value assigned by a sender host and is used for fragment reassembly.
- Flags: 3 bits long.
  - Reserved Fragment: 0 (reserved).
  - Don't Fragment: Value 1 indicates that fragmentation is not allowed, and value 0 indicates that fragmentation is allowed.
  - More Fragment: Value 1 indicates that there are more segments following the segment, and value 0 indicates that the segment is the last data segment.
- Fragment Offset: 12 bits long. This field is used for fragment reassembly. This field indicates the relative position of a fragment in an original packet that is fragmented. This field is used together with the More Fragment bit to help the receiver assemble the fragments.

Time to Live

- The TTL field specifies the number of routers that a packet can pass through.
- Once a packet passes through a router, the TTL is reduced by 1. If the TTL value is reduced to 0, a data packet is discarded.

Version	Header Length	Type of Service	Total Length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header Checksum	
Source IP Address				
Destination IP Address				
Options				Padding



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Time to Live: 8 bits long. It specifies the maximum number of routers that a packet can pass through on a network.
  - When packets are forwarded between network segments, loops may occur if routes are not properly planned on network devices. As a result, packets are infinitely looped on the network and cannot reach the destination. If a loop occurs, all packets destined for this destination are forwarded cyclically. As the number of such packets increases, network congestion occurs.
  - To prevent network congestion induced by loops, a TTL field is added to the IP packet header. The TTL value decreases by 1 each time a packet passes through a Layer 3 device. The initial TTL value is set on the source device. After the TTL value of a packet decreases to 0, the packet is discarded. In addition, the device that discards the packet sends an ICMP error message to the source based on the source IP address in the packet header. (Note: A network device can be disabled from sending ICMP error messages to the source ends.)

Protocol

- The Protocol field in the IP packet header identifies a protocol that will continue to process the packet.
- This field identifies the protocol used by the data carried in the data packet so that the IP layer of the destination host sends the data to the process mapped to the Protocol field.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- After receiving and processing the packet at the network layer, the destination end needs to determine which protocol is used to further process the packet. The Protocol field in the IP packet header identifies the number of a protocol that will continue to process the packet.
- The field may identify a network layer protocol (for example, ICMP of value 0x01) or an upper-layer protocol (for example, Transmission Control Protocol [TCP] of value 0x06 or the User Datagram Protocol [UDP] of value 0x11).

Contents

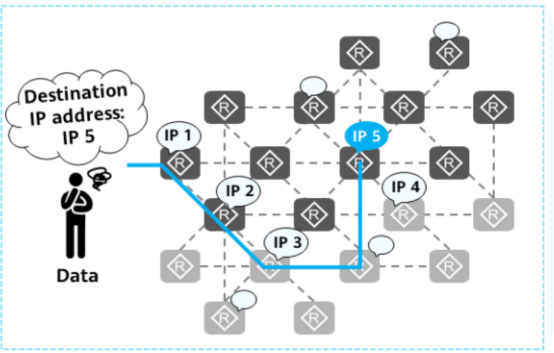
1. Network Layer Protocols
2. **Introduction to IPv4 Addresses**
3. Subnetting
4. ICMP
5. IPv4 Address Configuration and Basic Application

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

What Is an IP Address?

- An IP address identifies a node (or an interface on a network device) on a network.
- IP addresses are used to forward IP packets on the network.



IP Address

An IP address identifies a node on a network and is used to find the destination for data.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- On an IP network, if a user wants to connect a computer to the Internet, the user needs to apply for an IP address for the computer. An IP address identifies a node on a network and is used to find the destination for data. We use IP addresses to implement global network communication.
- An IP address is an attribute of a network device interface, not an attribute of the network device itself. To assign an IP address to a device is to assign an IP address to an interface on the device. If a device has multiple interfaces, each interface needs at least one IP address.

- Note: The interface that needs to use an IP address is usually the interface of a router or computer.

IP address Notation

- An IPv4 address is 32 bits long.
- It is in dotted decimal notation.

Dotted decimal notation

Decimal	192.	168.	10.	1	4 bytes
Binary	11000000	10101000	00001010	00000001	32 bits

Conversion between decimal and binary systems

Power	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
	128	64	32	16	8	4	2	1
Bit	1	1	0	0	0	0	0	0

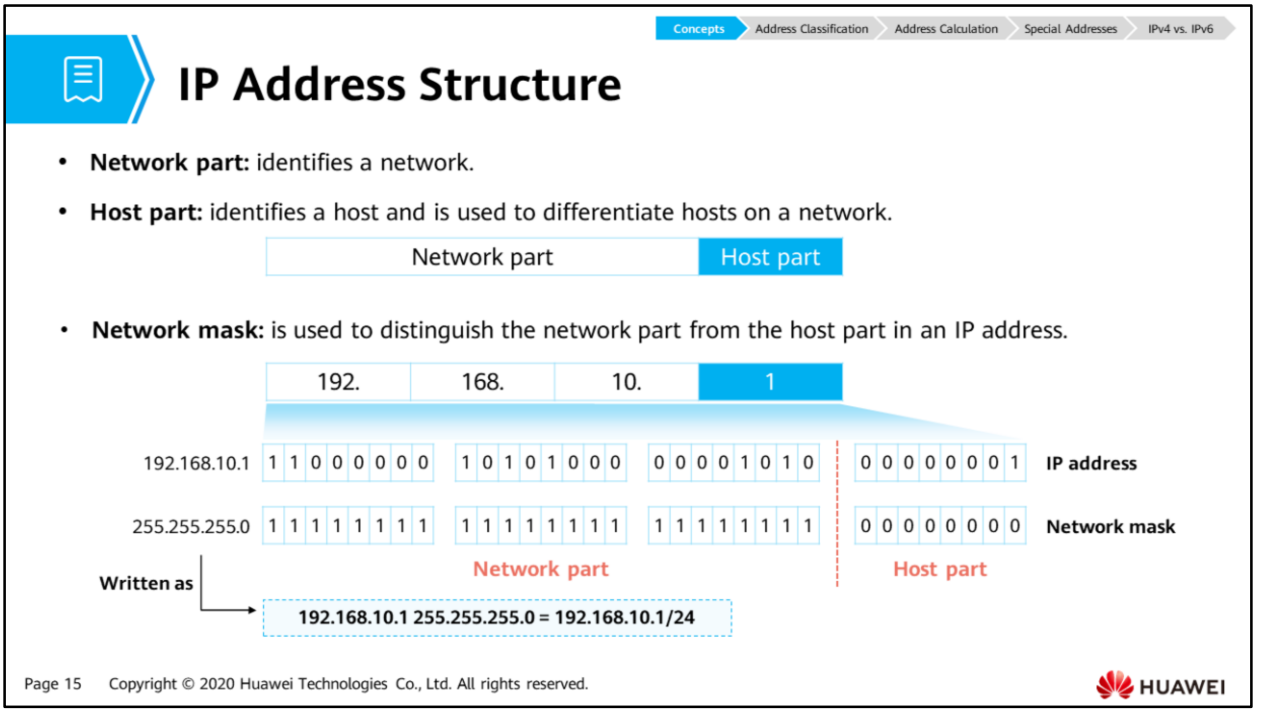
= 128 + 64 = 192

- IPv4 address range is 0.0.0.0–255.255.255.255.

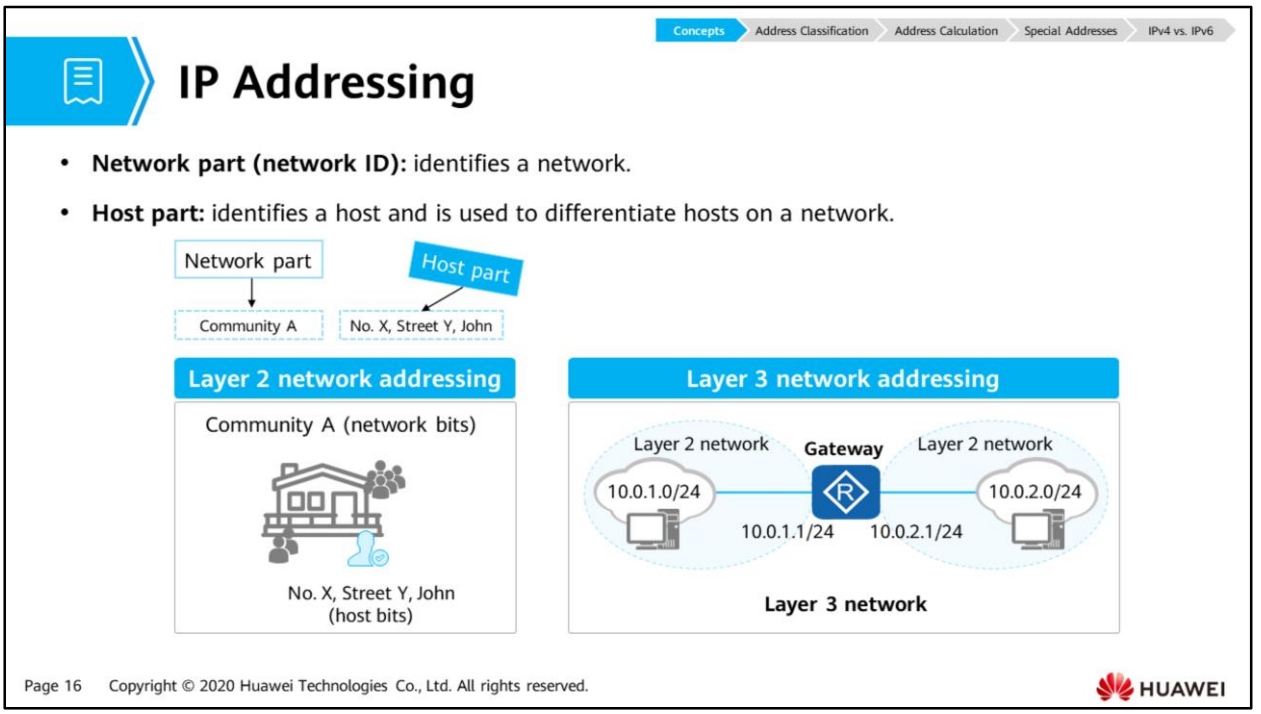
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

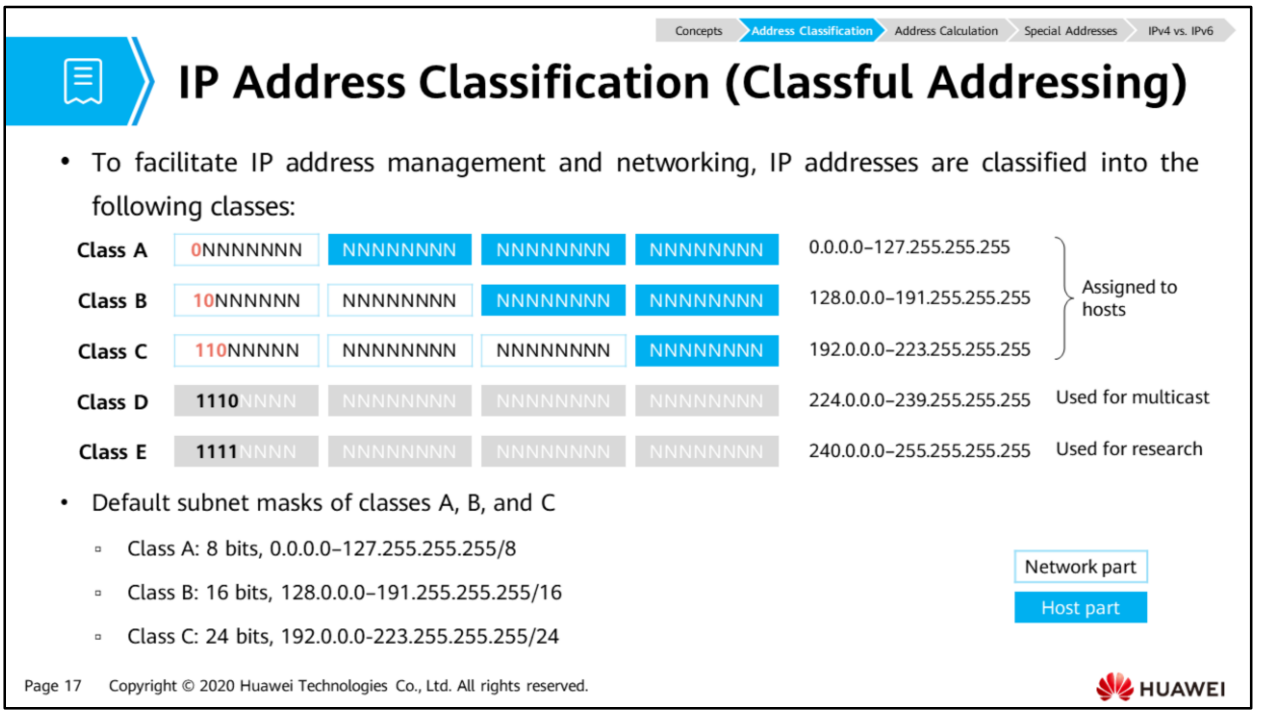
- IP address notation
  - An IP address is 32 bits long and consists of 4 bytes. It is in dotted decimal notation, which is convenient for reading and writing.
- Dotted decimal notation
  - The IP address format helps us better use and configure a network. However, a communication device uses the binary mode to operate an IP address. Therefore, it is necessary to be familiar with the decimal and binary conversion.
- IPv4 address range
  - 00000000.00000000.00000000.00000000–11111111.11111111.11111111.11111111, that is, 0.0.0.0–255.255.255.255



- An IPv4 address is divided into two parts:
  - **Network part** (network ID): identifies a network.
    - IP addresses do not show any geographical information. The network ID represents the network to which a host belongs.
    - Network devices with the same network ID are located on the same network, regardless of their physical locations.
  - **Host part:** identifies a host and is used to differentiate hosts on a network.
- A network mask is also called a subnet mask:
  - A network mask is 32 bits long, which is also represented in dotted decimal notation, like bits in an IP address.
  - The network mask is not an IP address. The network mask consists of consecutive 1s followed by consecutive 0s in binary notation.
  - Generally, the number of 1s indicates the length of a network mask. For example, the length of mask 0.0.0.0 is 0, and the length of mask 252.0.0.0 is 6.
  - The network mask is generally used together with the IP address. Bits of 1 correspond to network bits in the IP address. Bits of 0 corresponds to host bits in the IP address. In other words, in an IP address, the number of 1s in a network mask is the number of bits of the network ID, and the number of 0s is the number of bits in the host ID.

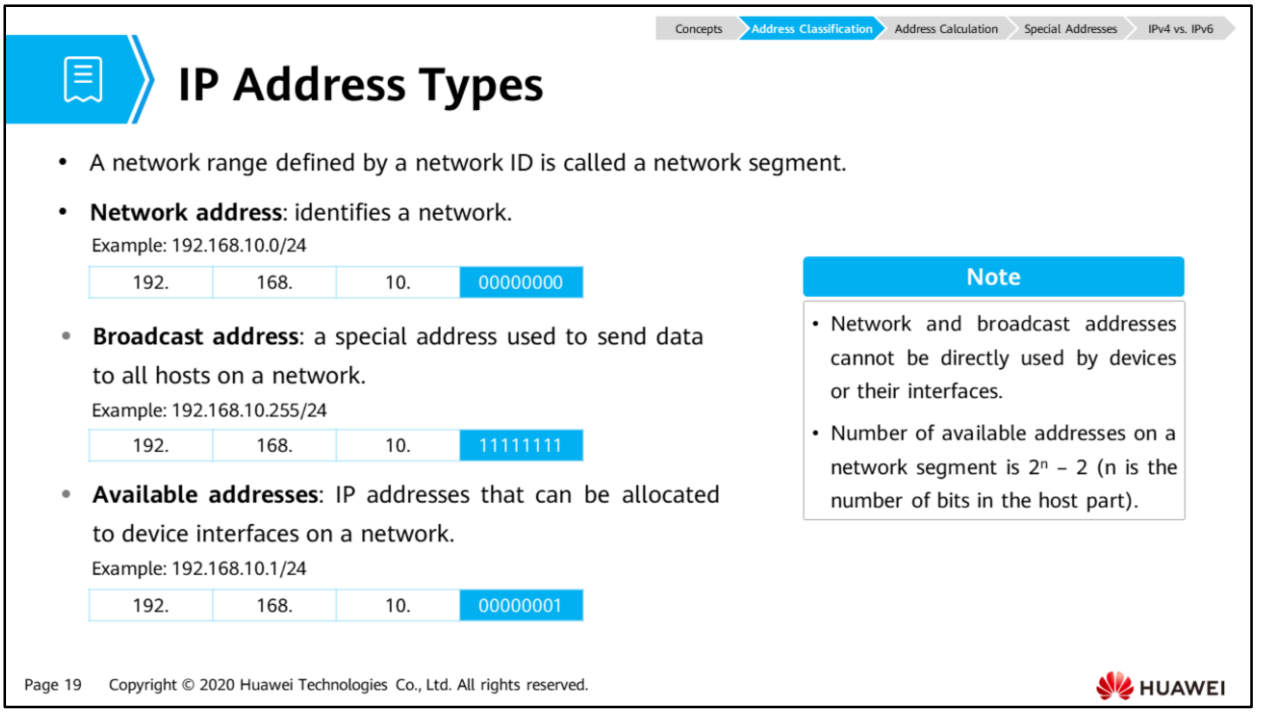


- A network ID indicates the network where a host is located, which is similar to the function of "Community A in district B of City X in province Y."
- A host ID identifies a specific host interface within a network segment defined by the network ID. The function of host ID is like a host location "No. A Street B".
- Network addressing:
  - Layer 2 network addressing: A host interface can be found based on an IP address.
  - Layer 3 network addressing: A gateway is used to forward data packets between network segments.
- Gateway:
  - During packet forwarding, a device determines a forwarding path and an interface connected to a destination network segment. If the destination host and source host are on different network segments, packets are forwarded to the gateway and then the gateway forwards the packets to the destination network segment.
  - A gateway receives and processes packets sent by hosts on a local network segment and forwards the packets to the destination network segment. To implement this function, the gateway must know the route of the destination network segment. The IP address of the interface on the gateway connected to the local network segment is the gateway address of the network segment.



- To facilitate IP address management and networking, IP addresses are classified into the following classes:
  - The easiest way to determine the class of an IP address is to check the most significant bits in a network ID. Classes A, B, C, D, and E are identified by binary digits 0, 10, 110, 1110, and 1111, respectively.
  - Class A, B, and C addresses are unicast IP addresses (except some special addresses). Only these addresses can be assigned to host interfaces.
  - Class D addresses are multicast IP addresses.
  - Class E addresses are used for special experiment purposes.
  - This presentation only focuses on class A, B, and C addresses.
- Comparison of class A, B, and C addresses:
  - A network using class A addresses is called a class A network. A network using class B addresses is called a class B network. A network that uses class C addresses is called a class C network.
  - The network ID of a class A network is 8 bits, indicating that the number of network IDs is small and a large number of host interfaces are supported. The leftmost bit is fixed at 0, and the address space is 0.0.0.0–127.255.255.255.
  - The network ID of class B network is 16 bits, which is between class A and class C networks. The leftmost two bits are fixed at 10, and the address space is 128.0.0.0–191.255.255.255.
  - The network ID of a class C network is 24 bits, indicating that a large number of network IDs are supported, and the number of host interfaces is small. The leftmost three bits are fixed at 110, and the address space is 192.0.0.0–223.255.255.255.

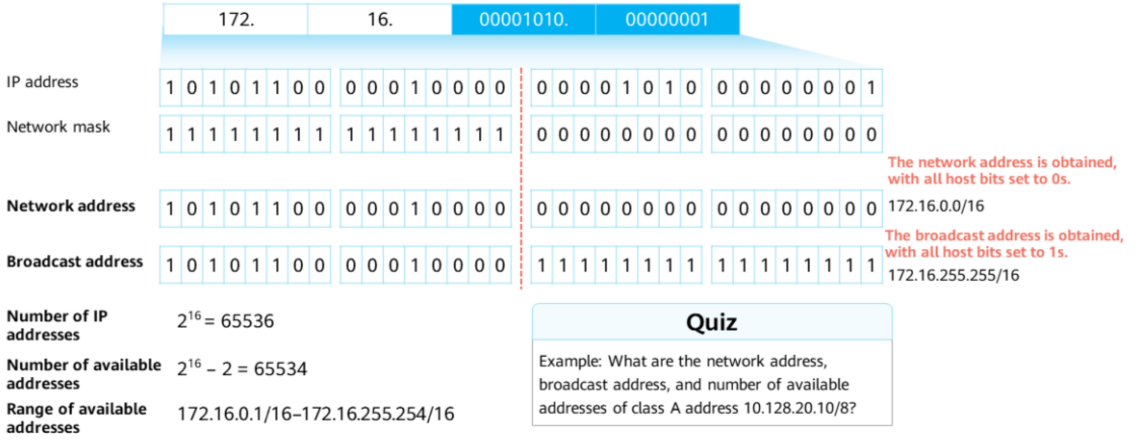
- Note:
  - A host refers to a router or a computer. In addition, the IP address of an interface on a host is called a host IP address.
  - Multicast address: is used to implement one-to-multiple message transmission.



- Network address
  - The network ID is X, and each bit in the host ID is 0.
  - It cannot be assigned to a host interface.
- Broadcast address
  - The network ID is X, and each bit in the host ID is 1.
  - It cannot be assigned to a host interface.
- Available address
  - It is also called a host address. It can be assigned to a host interface.
- The number of available IP addresses on a network segment is calculated using the following method:
  - Given that the host part of a network segment is n bits, the number of IP addresses is 2^n, and the number of available IP addresses is $2^n - 2$ (one network address and one broadcast address).

IP Address Calculation

- Example: What are the network address, broadcast address, and number of available addresses of class B address 172.16.10.1/16?



Number of IP addresses: $2^{16} = 65536$

Number of available addresses: $2^{16} - 2 = 65534$

Range of available addresses: 172.16.0.1/16–172.16.255.254/16

Quiz

Example: What are the network address, broadcast address, and number of available addresses of class A address 10.128.20.10/8?

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

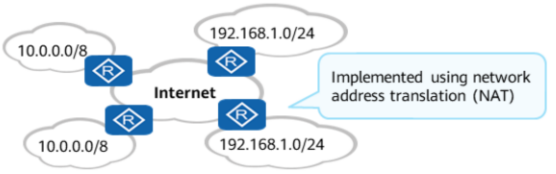
HUAWEI

- Network address: After the host part of this address is set to all 0s, the obtained result is the network address of the network segment where the IP address is located.
- Broadcast address: After the host part of this address is set to all 1s, the obtained result is the broadcast address used on the network where the IP address is located.
- Number of IP addresses: 2^n, where n indicates the number of host bits.
- Number of available IP addresses: $2^n - 2$, where n indicates the number of host bits.

- Answers to the quiz:
  - Network address: 10.0.0.0/8
  - Broadcast address: 10.255.255.255
  - Number of addresses: 2^{24}
  - Number of available addresses: $2^{24} - 2$
  - Range of available addresses: 10.0.0.1/8–10.255.255.254/8

Private IP Addresses

- **Public IP address:** An IP address is assigned by the Internet Assigned Numbers Authority (IANA), and this address allocation mode ensures that each IP address is unique on the Internet. Such an IP address is a public IP address.
- **Private IP address:** In practice, some networks do not need to connect to the Internet. For example, on a network of a lab in a college, IP addresses of devices need to avoid conflicting with each other only within the same network. In the IP address space, some IP addresses of class A, B, and C addresses are reserved for the preceding situations. These IP addresses are called private IP addresses.
  - Class A: 10.0.0.0–10.255.255.255
  - Class B: 172.16.0.0–172.31.255.255
  - Class C: 192.168.0.0–192.168.255.255

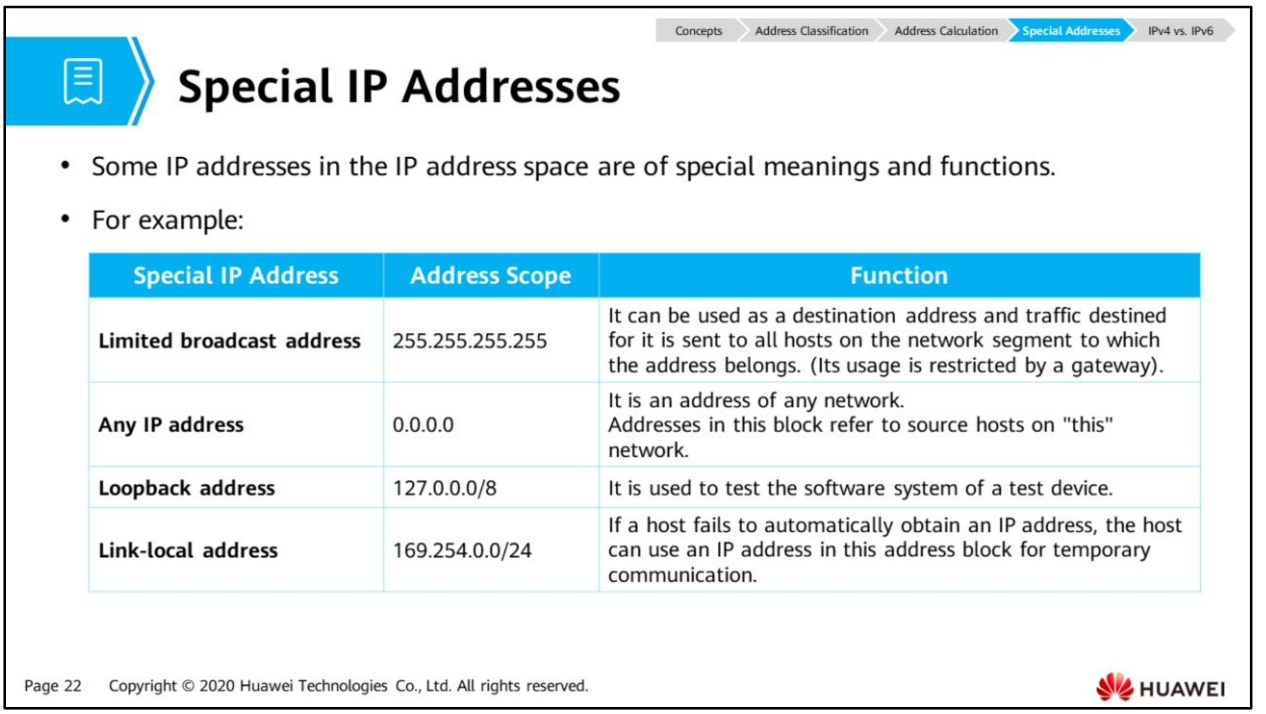


Connecting a private network to the Internet

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Private IP addresses are used to relieve the problem of IP address shortage. Private addresses are used on internal networks and hosts, and cannot be used on the public network.
  - Public IP address: A network device connected to the Internet must have a public IP address allocated by the IANA.
  - Private IP address: The use of a private IP address allows a network to be expanded more freely, because a same private IP address can be repeatedly used on different private networks.
- Connecting a private network to the Internet: A private network is not allowed to connect to the Internet because it uses a private IP address. Driven by requirements, many private networks also need to connect to the Internet to implement communication between private networks and the Internet, and between private networks through the Internet. The interconnection between the private network and Internet must be implemented using the NAT technology.

- Note: Network Address Translation (NAT) is used to translate addresses between private and public IP address realms.



- 255.255.255.255
  - This address is called a limited broadcast address and can be used as the destination IP address of an IP packet.
  - After receiving an IP packet whose destination IP address is a limited broadcast address, the router stops forwarding the IP packet.
- 0.0.0.0
  - If this address is used as a network address, it means the network address of any network. If this address is used as the IP address of a host interface, it is the IP address of a source host interface on "this" network.
  - For example, if a host interface does not obtain its IP address during startup, the host interface can send a DHCP Request message with the destination IP address set to a limited broadcast address and the source IP address set to 0.0.0.0 to the network. The DHCP server is expected to allocate an available IP address to the host interface after receiving the DHCP Request message.
- 127.0.0.0/8
  - This address is called a Loopback address and can be used as the destination IP address of an IP packet. It is used to test the software system of a test device.
  - The IP packets that are generated by a device and whose destination IP address is set to a Loopback address cannot leave the device itself.
- 169.254.0.0/16
  - If a network device is configured to automatically obtain an IP address but no DHCP server is available on the network, the device uses an IP address in the 169.254.0.0/16 network segment for temporary communication.
- Note: The Dynamic Host Configuration Protocol (DHCP) is used to dynamically allocate network configuration parameters, such as IP addresses.

IPv4 vs. IPv6

- IPv4 addresses managed by the IANA were exhausted in 2011. As the last public IPv4 address was allocated and more and more users and devices access the public network, IPv4 addresses were exhausted. This is the biggest driving force for IPv6 to replace IPv4.

IPv4	IPv6

• Address length: 32 bits
• Address types: unicast address, broadcast address, and multicast address
• Characteristics:
  ▫ IPv4 address depletion
  ▫ Inappropriate packet header design
  ▫ ARP dependency-induced flooding
  ▫ ...
	• Address length: 128 bits
	• Address types: unicast address, multicast address, and anycast address
	• Characteristics:
	  ▫ Unlimited number of addresses
	  ▫ Simplified packet header
	  ▫ Automatic IPv6 address allocation
	  ▫ ...

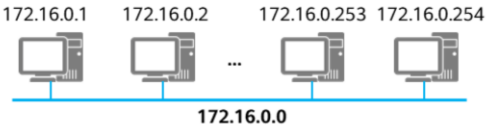
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. Network Layer Protocols
2. Introduction to IPv4 Addresses
3. **Subnetting**
4. ICMP
5. IPv4 Address Configuration and Basic Application

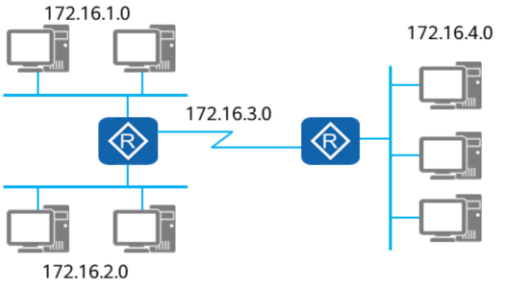
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Why Subnetting?



2^{16} = 65536 IP addresses

- A class B address is used for a broadcast domain, wasting addresses.
- The broadcast domain is too large. Once broadcast occurs, an internal network is overloaded.



- A network number is divided into multiple subnets, and each subnet is allocated to a separate broadcast domain.
- In this way, the broadcast domain is smaller, and the network planning is more reasonable.
- IP addresses are properly used.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Classful addressing is too rigid and the granularity of address division is too large. As a result, a large number of host IDs cannot be fully used, wasting IP addresses.
- Therefore, subnetting can be used to reduce address waste through the variable length subnet mask (VLSM) technology. A large classful network is divided into several small subnets, which makes the use of IP addresses more scientific.

Subnetting - Analyzing the Original Network Segment

- Example: 192.168.10.0/24

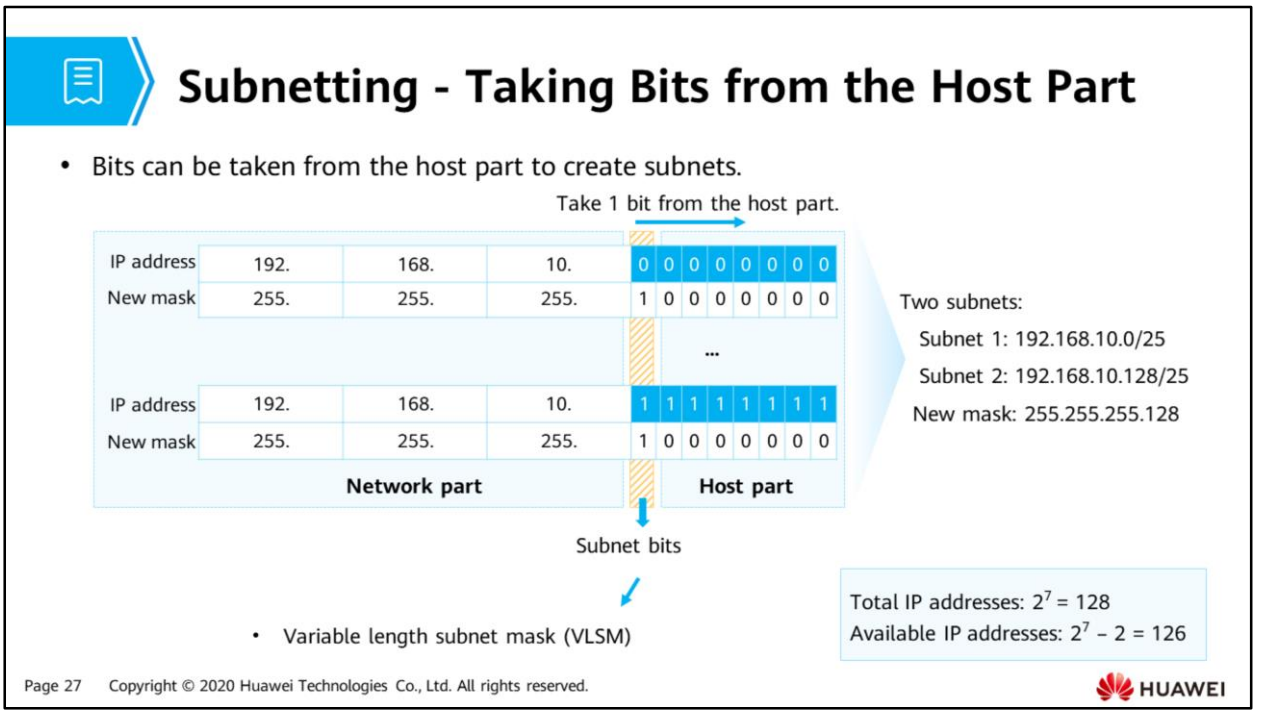
192.168.10.1										
IP address	192.	168.	10.	0	0	0	0	0	0	0	1
Default subnet mask	255.	255.	255.	0	0	0	0	0	0	0	0
...										
192.168.10.255										
IP address	192.	168.	10.	1	1	1	1	1	1	1	1
Default subnet mask	255.	255.	255.	0	0	0	0	0	0	0	0
	Network part			Host part						

One class C network:
192.168.10.0/24
Default subnet mask:
255.255.255.0

Network address: 192.168.10.0/24
Broadcast address: 192.168.10.255
Total IP addresses: $2^8 = 256$
Available IP addresses: $2^8 - 2 = 254$

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

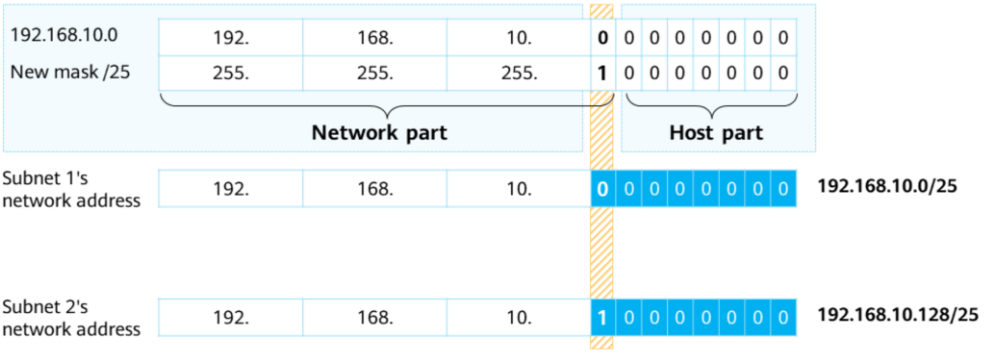
- Assume that a class C network segment is 192.168.10.0. By default, the network mask is 24 bits, including 24 network bits and 8 host bits.
- As calculated, there are 256 IP addresses on the network.



- Now, for the original 24-bit network part, a host bit is taken to increase the network part to 25 bits. The host part is reduced to 7 bits. The taken 1 bit is a subnet bit. In this case, the network mask becomes 25 bits, that is, 255.255.255.128, or /25.
- Subnet bit: The value can be 0 or 1. Two new subnets are obtained.
- As calculated, there are 128 IP addresses on the network.

Subnetting - Calculating the Subnet Network Address

- The network address is obtained, with all host bits set to 0s.

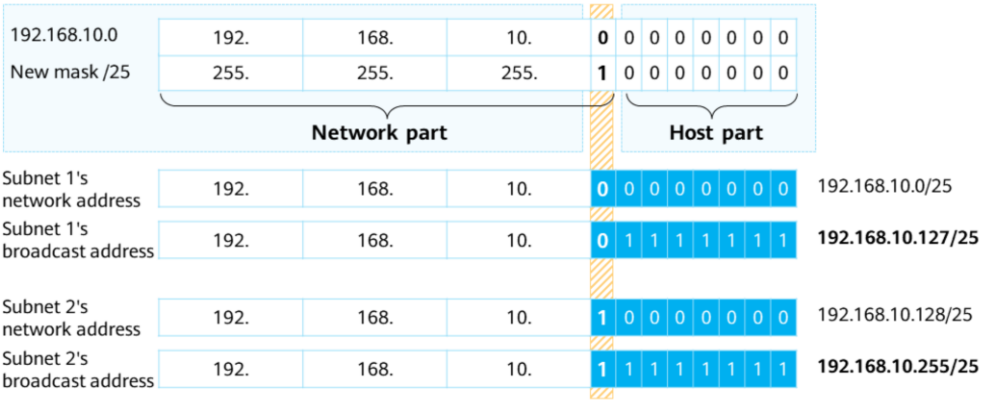


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Calculate a network address, with all host bits set to 0s.
  - If the subnet bit is 0, the network address is 192.168.10.0/25.
  - If the subnet bit is 1, the network address is 192.168.10.128/25.

Subnetting - Calculating the Subnet Broadcast Address

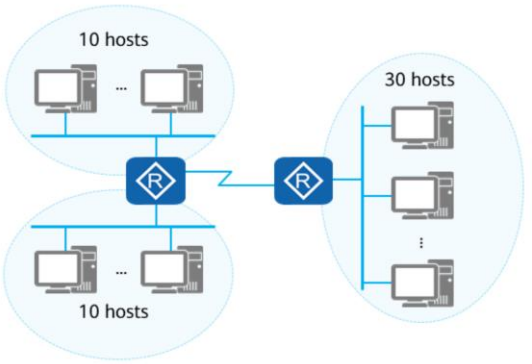
- The broadcast address is obtained, with all host bits set to 1s.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Calculate a broadcast address, with all host bits set to 1s.
  - If the subnet bit is 0, the network address is 192.168.10.127/25.
  - If the subnet bit is 1, the network address is 192.168.10.255/25.

Practice: Computing Subnets (1)



- **Question:** An existing class C network segment is 192.168.1.0/24. Use the VLSM to allocate IP addresses to three subnets.

- **Answer:** (Use a network with 10 hosts as an example.)

  Step 1: Calculate the number of host bits to be taken.

  $2^n - 2 \geq 10$

  $n \geq 4$, host bits

  Step 2: Take bits from the host part.

Take 4 bits from the host part.

IP address	192.	168.	1.	**0**	**0**	**0**	**0**	0	0	0	0
Subnet mask	255.	255.	255.	1	1	1	1	0	0	0	0

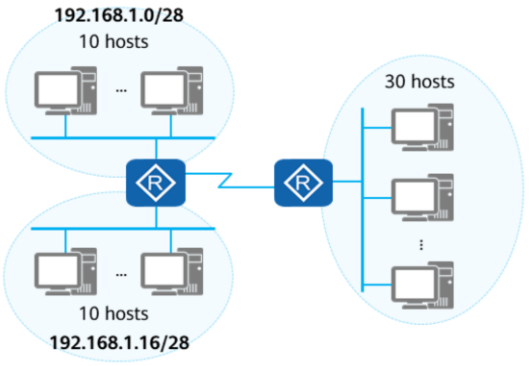
Subnet bits

Number of subnets: $2^4 = 16$ subnets

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In actual network planning, the subnet with more hosts is planned first.

Practice: Computing Subnets (2)



- **Question:** An existing class C network segment is 192.168.1.0/24. Use the VLSM to allocate IP addresses to three subnets.
- **Answer:** (Use a network with 10 hosts as an example.)

Step 3: Calculate subnet network addresses.

IP address	192.	168.	1.	**0**	**0**	**0**	**0**	0	0	0	0
New mask	255.	255.	255.	1	1	1	1	0	0	0	0
											Network address
Subnet 1	192.	168.	1.	0	0	0	0	0	0	0	192.168.1.0/28
Subnet 2	192	168.	1.	0	0	0	1	0	0	0	192.168.1.16/28
Subnet 3	192.	168.	1.	0	0	1	0	0	0	0	192.168.1.32/28
⋮											
Subnet 16	192.	168.	1.	1	1	1	1	0	0	0	192.168.1.240/28

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Subnet network addresses are:
  - 192.168.1.0/28
  - 192.168.1.16/28
  - 192.168.1.32/28
  - 192.168.1.48/28
  - 192.168.1.64/28
  - 192.168.1.80/28
  - 192.168.1.96/28
  - 192.168.1.112/28
  - 192.168.1.128/28
  - 192.168.1.144/28
  - 192.168.1.160/28
  - 192.168.1.176/28
  - 192.168.1.192/28
  - 192.168.1.208/28
  - 192.168.1.224/28
  - 192.168.1.240/28

Contents

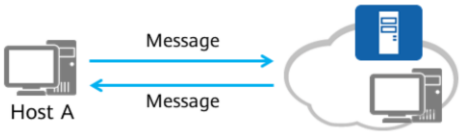
1. Network Layer Protocols
2. Introduction to IPv4 Addresses
3. Subnetting
4. **ICMP**
5. IPv4 Address Configuration and Basic Application

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

ICMP

- The Internet Control Message Protocol (ICMP) is an auxiliary protocol of the IP protocol.
- ICMP is used to transmit error and control information between network devices. It plays an important role in collecting network information, diagnosing and rectifying network faults.



Ethernet header	IP header	ICMP message	Ethernet tail

Type	Code	Checksum
ICMP message content		

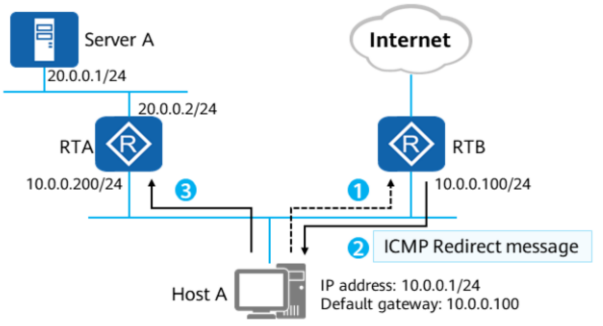
Type	Code	Description
0	0	Echo Reply
3	0	Network Unreachable
3	1	Host Unreachable
3	2	Protocol Unreachable
3	3	Port Unreachable
5	0	Redirect
8	0	Echo Request

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- To improve the efficiency of IP data packet forwarding and success rate of packet exchanges, ICMP is used at the network layer. ICMP allows hosts and devices to report errors during packet transmission.
- ICMP message:
  - ICMP messages are encapsulated in IP packets. Value 1 in the Protocol field of the IP packet header indicates ICMP.
  - Explanation of fields:
    - The format of an ICMP message depends on the Type and Code fields. The Type field indicates a message type, and the Code field contains a parameter mapped to the message type.
    - The Checksum field is used to check whether a message is complete.
    - A message contains a 32-bit variable field. This field is not used and is usually set to 0.
      - In an ICMP Redirect message, this field indicates the IP address of a gateway. A host redirects packets to the specified gateway that is assigned this IP address.
      - In an Echo Request message, this field contains an identifier and a sequence number. The source associates the received Echo Reply message with the Echo Request message sent by the local end based on the identifiers and sequence numbers carried in the messages. Especially, when the source sends multiple Echo Request messages to the destination, each Echo Reply message must carry the same identifier and sequence number as those carried in the Echo Request message.

ICMP Redirection

- ICMP Redirect messages are a type of ICMP control message. When a router detects that a host uses a non-optimal route in a specific scenario, the router sends an ICMP Redirect message to the host, requesting the host to change the route.

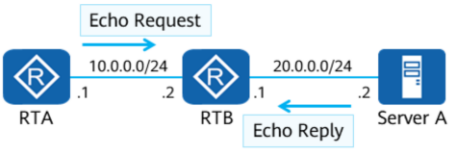


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- ICMP redirection process:
  1. Host A wants to send packets to server A. Host A sends packets to the default gateway address that is assigned to the gateway RTB.
  2. After receiving the packet, RTB checks packet information and finds that the packet should be forwarded to RTA. RTA is the other gateway on the same network segment as the source host. This forwarding path through RTA is better than that through RTB. Therefore, RTB sends an ICMP Redirect message to the host, instructing the host to send the packet to RTA.
  3. After receiving the ICMP Redirect message, the host sends a packet to RTA. Then RTA forwards the packet to server A.

ICMP Error Detection

- ICMP Echo messages are used to check network connectivity between the source and destination and provide other information, such as the round-trip time.



Function: Ping

Ping is a command used on network devices, Windows OS, Unix OS, and Linux OS. Ping is a small and useful application based on the ICMP protocol.

A ping tests the reachability of a destination node.

```
[RTA]ping 20.0.0.2
  PING 20.0.0.2: 56  data bytes, press CTRL_C to break
    Reply from 20.0.0.2: bytes=56 Sequence=1 ttl=254 time=70 ms
    Reply from 20.0.0.2: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 20.0.0.2: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 20.0.0.2: bytes=56 Sequence=4 ttl=254 time=40 ms
    Reply from 20.0.0.2: bytes=56 Sequence=5 ttl=254 time=30 ms

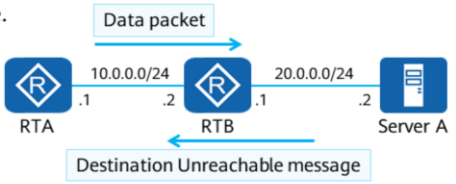
  --- 20.0.0.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/40/70 ms
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A typical ICMP application is ping. Ping is a common tool used to check network connectivity and collect other related information. Different parameters can be specified in a ping command, such as the size of ICMP messages, number of ICMP messages sent at a time, and the timeout period for waiting for a reply. Devices construct ICMP messages based on the parameters and perform ping tests.

ICMP Error Report

- ICMP defines various error messages for diagnosing network connectivity problems. The source can determine the cause for a data transmission failure based on the received error messages. For example, after a network device receives a packet, it cannot access the network where the destination device resides, the network device automatically sends an ICMP Destination Unreachable message to the source.




```
[RTA]tracert 20.0.0.2

traceroute to  20.0.0.2(20.0.0.2), max hops: 30 ,packet length: 40,press CTRL_C
to break

1 10.0.0.2          80 ms    10 ms    10 ms

2 20.0.0.2          30 ms    30 ms    20 ms
```

Function: Tracert

Tracert checks the reachability of each hop on a forwarding path based on the TTL value carried in the packet header.

Tracert is an effective method to detect packet loss and delay on a network and helps administrators discover routing loops on the network.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- ICMP defines various error messages for diagnosing network connectivity problems. The source can determine the cause for a data transmission failure based on the received error messages.
  - If a loop occurs on the network, packets are looped on the network, and the TTL times out, the network device sends a TTL timeout message to the sender device.
  - If the destination is unreachable, the intermediate network device sends an ICMP Destination Unreachable message to the sender device. There are a variety of cases for unreachable destination. If the network device cannot find the destination network, the network device sends an ICMP Destination Network Unreachable message. If the network device cannot find the destination host on the destination network, the network device sends an ICMP Destination Host Unreachable message.
- Tracert is a typical ICMP application. Tracert checks the reachability of each hop on a forwarding path based on the TTL value carried in the packet header. In a tracert test for a path to a specific destination address, the source first sets the TTL value in a packet to 1 before sending the packet. After the packet reaches the first node, the TTL times out. Therefore, the first node sends an ICMP TTL Timeout message carrying a timestamp to the source. Then, the source sets the TTL value in a packet to 2 before sending the packet. After the packet reaches the second node, the TTL times out. The second node also returns an ICMP TTL Timeout message. The process repeats until the packet reaches the destination. In this way, the source end can trace each node through which the packet passes based on the information in the returned packet, and calculate the round-trip time based on timestamps.

Contents

1. Network Layer Protocols
2. Introduction to IPv4 Addresses
3. Subnetting
4. ICMP
5. **IPv4 Address Configuration and Basic Application**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Basic IP Address Configuration Commands

1. Enter the interface view.

   [Huawei] **interface** *interface-type interface-number*

   You can run this command to enter the view of a specified interface and configure attributes for the interface.
   - *interface-type interface-number*: specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character.

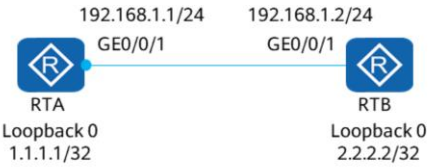
2. Configure an IP address for the interface.

   [Huawei-GigabitEthernet0/0/1] **ip address** *ip-address* { *mask* | *mask-length* }

   You can run this command in the interface view to assign an IP address to the interface on the network devices to implement network interconnection.
   - *ip-address*: specifies the IP address of an interface. The value is in dotted decimal notation.
   - *mask*: specifies a subnet mask. The value is in dotted decimal notation.
   - *mask-length*: specifies a mask length. The value is an integer ranging from 0 to 32.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case: Configuring an IP address for an Interface



On the preceding network where the two routers are interconnected, configure IP addresses for the interconnected physical interfaces and logical IP addresses.

Configure an IP address for a physical interface.

```
[RTA] interface gigabitethernet 0/0/1
[RTA-GigabitEthernet0/0/1] ip address 192.168.1.1 255.255.255.0
                Or,
[RTA-GigabitEthernet0/0/1] ip address 192.168.1.1 24
```

Configure an IP address for a logical interface.

```
[RTA] interface LoopBack 0
[RTA-LoopBack0] ip address 1.1.1.1 255.255.255.255
                Or,
[RTA-LoopBack0] ip address 1.1.1.1 32
```

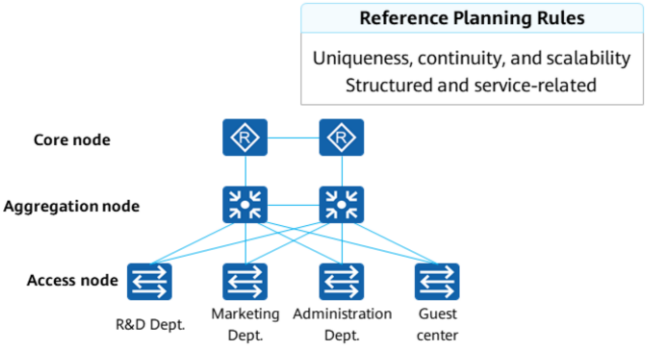
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Physical interface: is an existing port on a network device. A physical interface can be a service interface transmitting services or a management interface managing the device. For example, a GE service interface and an MEth management interface are physical interfaces.
- Logical interface: is a physically nonexistent interface that can be created using configuration and need to transmit services. For example, a VLANIF interface and Loopback interfaces are logical interfaces.
    - Loopback interface: is always in the up state.
        - Once a Loopback interface is created, its physical status and data link protocol status always stay up, regardless of whether an IP address is configured for the Loopback interface.
        - The IP address of a Loopback interface can be advertised immediately after being configured. A Loopback interface can be assigned an IP address with a 32-bit mask, which reduces address consumption.
        - No data link layer protocols can be encapsulated on a Loopback interface. No negotiation at the data link layer is performed for the Loopback interface. Therefore, the data link protocol status of the Loopback interface is always up.
        - The local device directly discards a packet whose destination address is not the local IP address but the outbound interface is the local Loopback interface.

Network IP Address Planning

- IP address planning must be considered together with the network structure, routing protocols, traffic planning, and service rules. In addition, IP address planning should be corresponding to the network hierarchy and performed in a top-bottom way.
- In conclusion, IP address planning objectives are to achieve easy management, easy scalability, and high utilization.
- **IP Address Planning Example**

Background	Address Type	Address Scope
Example: A company is assigned 192.168.0.0/16 as a network segment address.	Network segment of the R&D department	192.168.1.0/24
	Network segment of the marketing department	192.168.2.0/24
	Network segment of the administrative department	192.168.3.0/24
	Network segment of the guest center	192.168.4.0/24
	Others	...



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Planning rules:
  - Uniqueness: Each host on an IP network must have a unique IP address.
  - Continuity: Contiguous addresses can be summarized easily in the hierarchical networking. Route summarization reduces the size of the routing table and speeds up route calculation and route convergence.
  - Scalability: Addresses need to be properly reserved at each layer, ensuring the contiguous address space for route summarization when the network is expanded. Re-planning of addresses and routes induced by network expansion is therefore prevented.
  - Combination of topology and services: Address planning is combined with the network topology and network transport service to facilitate route planning and quality of service (QoS) deployment. Appropriate IP address planning helps you easily determine the positions of devices and types of services once you read the IP addresses.

Quiz

1. (Multiple) Which class does 201.222.5.64 belong? ( )
   A. Class A
   B. Class B
   C. Class C
   D. Class D
2. (Multiple) A company is assigned a class C network segment 192.168.20.0/24. One of its departments has 40 hosts. Which of the following subnets can be allocated? ( )
   A. 192.168.20.64/26
   B. 192.168.20.64/27
   C. 192.168.20.128/26
   D. 192.168.20.190/26

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. C
2. AC

Summary

- To connect a PC to the Internet, apply an IP address from the Internet Service Provider (ISP).
- This presentation provides an overview of the IP protocol and describes concepts related to IPv4 addresses and subnetting.
- This presentation also describes the planning and basic configuration of IP addresses.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



IP Routing Basics

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- There are typically multiple IP subnets on a typical data communication network. Layer 3 devices are required to exchange data between these IP subnets. These devices have the routing capability and can forward data across subnets.
- Routing is the basic element of data communication networks. It is the process of selecting paths on a network along which packets are sent from a source to a destination.
- This course introduces the basic concepts of routing.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand the basic principles of routers.
  - Know how routers select optimal routes.
  - Understand the contents of routing tables.
  - Master advanced routing features.

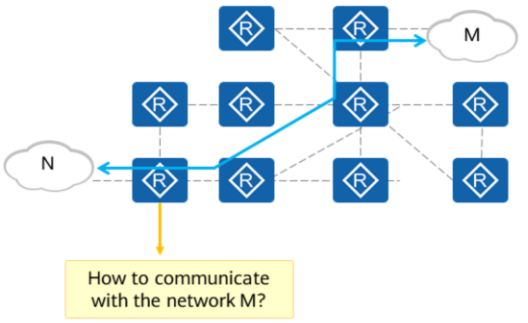
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. **Overview of IP Routing**
   - **Basic Concepts of Routing**
   - Generation of Routing Entries
   - Optimal Route Selection
   - Route-based Forwarding
2. Static Routing
3. Dynamic Routing
4. Advanced Routing Features

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Background: Inter-Subnet Communication



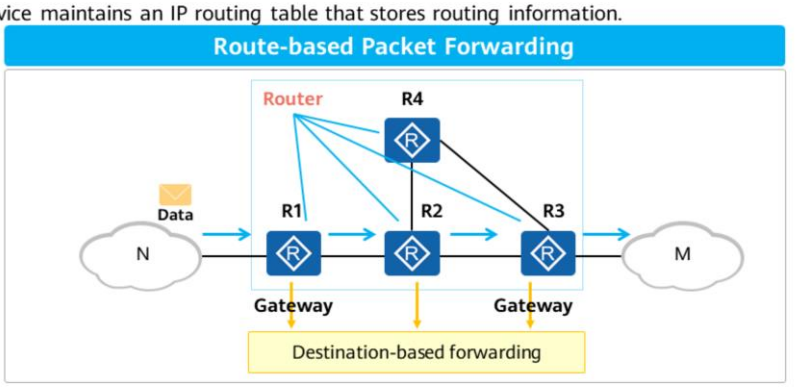
- An IP address uniquely identifies a node on a network. Each IP address belongs to a unique subnet, and each subnet may belong to a different area of the network.
- To implement IP addressing, subnets in different areas need to communicate with each other.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A unique network node can be found based on a specific IP address. Each IP address belongs to a unique subnet. These subnets may be distributed around the world and constitute a global network.
- To implement communication between different subnets, network devices need to forward IP packets from different subnets to their destination IP subnets.

Routes

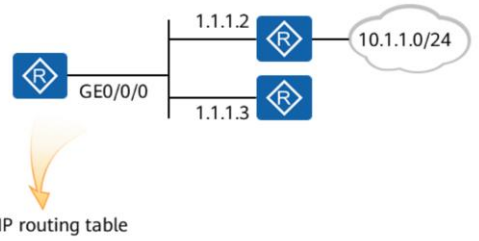
- Routes are the path information used to guide packet forwarding.
- A routing device is a network device that forwards packets to a destination subnet based on routes. The most common routing device is a router.
- A routing device maintains an IP routing table that stores routing information.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- A gateway and an intermediate node (a router) select a proper path according to the destination address of a received IP packet, and forward the packet to the next router. The last-hop router on the path performs Layer 2 addressing and forwards the packet to the destination host. This process is called route-based forwarding.
- The intermediate node selects the best path from its IP routing table to forward packets.
- A routing entry contains a specific outbound interface and next hop, which are used to forward IP packets to the corresponding next-hop device.

Routing Information



IP routing table

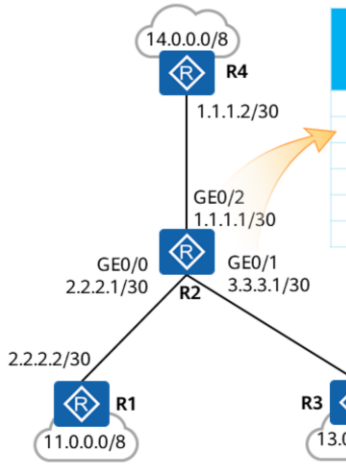
Destination/Mask	Outbound Interface	Next Hop
10.1.1.0/24	GE0/0/0	1.1.1.2

- A route contains the following information:
  - Destination: identifies a destination subnet.
  - Mask: identifies a subnet together with a destination IP address.
  - Outbound interface: indicates the interface through which a data packet is sent out of the local router.
  - Next hop: indicates the next-hop address used by the router to forward the data packet to the destination subnet.
- The information identifies the destination subnet and specifies the path for forwarding data packets.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Based on the information contained in a route, a router can forward IP packets to the destination along the required path.
- The destination address and mask identify the destination address of an IP packet. After an IP packet matches a specific route, the router determines the forwarding path according to the outbound interface and next hop of the route.
- The next-hop device for forwarding the IP packet cannot be determined based only on the outbound interface. Therefore, the next-hop device address must be specified.

IP Routing Table



Destination/Mask	Next Hop	Outbound Interface
11.0.0.0/8	2.2.2.2	GE0/0
13.0.0.0/8	3.3.3.2	GE0/1
14.0.0.0/8	1.1.1.2	GE0/2
...		
1.1.1.0/30	1.1.1.1	GE0/2
1.1.1.1/32	127.0.0.1	GE0/2

- Routers discover routes using multiple methods.
- A router selects the optimal route and installs it in its IP routing table.
- The router forwards IP packets based on routes in the IP routing table.
- Routers manage path information by managing their IP routing tables.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A router forwards packets based on its IP routing table.
- An IP routing table contains many routing entries.
- An IP routing table contains only optimal routes but not all routes.
- A router manages routing information by managing the routing entries in its IP routing table.

Contents

1. **Overview of IP Routing**
   - Basic Concepts of Routing
   - **Generation of Routing Entries**
   - Optimal Route Selection
   - Route-based Forwarding
2. Static Routing
3. Dynamic Routing
4. Advanced Routing Features

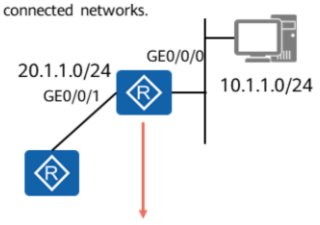
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

How to Obtain Routing Information

- A router forwards packets based on its IP routing table. To implement route-based packet forwarding, the router needs to obtain routes. The following describes the common methods of obtaining routes.

Direct Routes

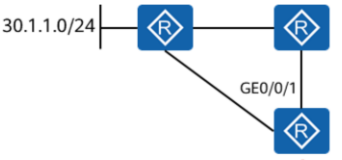
- Direct routes are automatically generated by devices and point to local directly connected networks.



Protocol	Destination/Mask	Outbound Interface
Direct	10.1.1.0/24	GE0/0/0
Direct	20.1.1.0/24	GE0/0/1

Static Routes

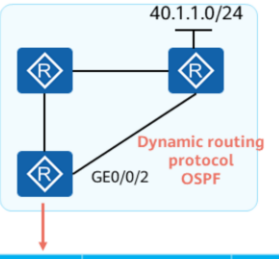
- Static routes are manually configured by network administrators.



Protocol	Destination/Mask	Outbound Interface
Static	30.1.1.0/24	GE0/0/1

Dynamic Routes

- Dynamic routes are learned by dynamic routing protocols running on routers.



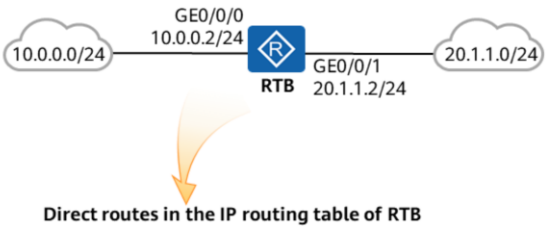
Protocol	Destination/Mask	Outbound Interface
OSPF	40.1.1.0/24	GE0/0/2

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Direct routes are the routes destined for the subnets to which directly connected interfaces belong. They are automatically generated by devices.
- Static routes are manually configured by network administrators.
- Dynamic routes are learned by dynamic routing protocols, such as OSPF, IS-IS, and BGP.

Direct Routes (1)

Direct Routes



Direct routes in the IP routing table of RTB

Destination/ Mask	Protocol	Next Hop	Outbound Interface
10.0.0.0/24	Direct	10.0.0.2	GE0/0/0
20.1.1.0/24	Direct	20.1.1.2	GE0/0/1

- A direct route is automatically generated by a device and points to a local directly-connected network.
- When a router is the last hop router, IP packets to be forwarded will match a direct route and the router will directly forward the IP packet to the destination host.
- When a direct route is used for packet forwarding, the destination IP address of a packet to be forwarded and the IP address of the router's outbound interface are in the same subnet.

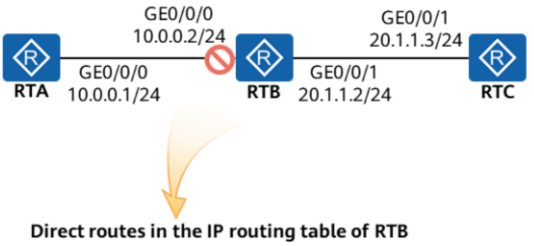
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- When a packet matches a direct route, a router checks its ARP entries and forwards the packet to the destination address based on the ARP entry for this destination address. In this case, the router is the last hop router.
- The next-hop address of a direct route is not an interface address of another device. The destination subnet of the direct route is the subnet to which the local outbound interface belongs. The local outbound interface is the last hop interface and does not need to forward the packet to any other next hop. Therefore, the next-hop address of a direct route in the IP routing table is the address of the local outbound interface.
- When a router forwards packets using a direct route, it does not deliver packets to the next hop. Instead, the router checks its ARP entries and forwards packets to the destination IP address based on the required ARP entry.

Direct Routes (2)

Direct routes



Direct routes in the IP routing table of RTB

Destination/Mask	Protocol	Next Hop	Outbound Interface
20.1.1.0/24	Direct	20.1.1.2	G0/0/1

- When GE0/0/0 goes down, the direct route for this interface is not installed in the IP routing table.

- Not all the direct routes generated for interfaces are installed in the IP routing table. Only the direct routes of which the physical status and protocol status of interfaces are up are installed in the IP routing table.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. **Overview of IP Routing**
   - Basic Concepts of Routing
   - Generation of Routing Entries
   - **Optimal Route Selection**
   - Route-based Forwarding
2. Static Routing
3. Dynamic Routing
4. Advanced Routing Features

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Examining the IP Routing Table

```
<Quidway> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Static  60   0           D   0.0.0.0         NULL0
        2.2.2.2/32  Static  60   0           D   100.0.0.2       Vlanif100
      100.0.0.0/24  Direct  0    0           D   100.0.0.1       Vlanif100
      100.0.0.1/32  Direct  0    0           D   127.0.0.1       Vlanif100
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Destination/Mask

Protocol

Route preference

Cost (Metric)

Flag

Next-hop address

Outbound interface

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Fields in the IP Routing Table

- Destination/Mask: indicates the destination network address and mask of a specific route. The subnet address of a destination host or router is obtained through the AND operation on the destination address and mask. For example, if the destination address is 1.1.1.1 and the mask is 255.255.255.0, the IP address of the subnet to which the host or router belongs is 1.1.1.0.
- Proto (Protocol): indicates the protocol type of the route, that is, the protocol through which a router learns the route.
- Pre (Preference): indicates the routing protocol preference of the route. There may be multiple routes to the same destination, which have different next hops and outbound interfaces. These routes may be discovered by different routing protocols or be manually configured. A router selects the route with the highest preference (with the lowest preference value) as the optimal route.
- Cost: indicates the cost of the route. When multiple routes to the same destination have the same preference, the route with the lowest cost is selected as the optimal route.
- NextHop: indicates the local router's next-hop address of the route to the destination network. This field specifies the next-hop device to which packets are forwarded.
- Interface: indicates the outbound interface of the route. This field specifies the local interface through which the local router forwards packets.

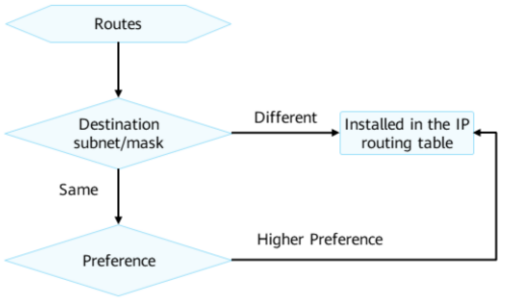
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- The Preference field is used to compare routes from different routing protocols, while the Cost field is used to compare routes from the same routing protocol. In the industry, the cost is also known as the metric.

Route Preference - Basic Concepts

Comparing Route Preferences

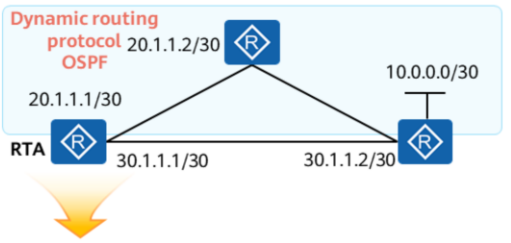


- When a router obtains routes to the same destination subnet from different routing protocols (these routes have the same destination network address and mask), the router compares the preferences of these routes and prefers the route with the lowest preference value.
- A lower preference value indicates a higher preference.
- The route with the highest preference is installed in the IP routing table.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Route Preference - Comparison Process

Comparing Route Preferences



IP routing table of RTA

Destination/Mask	Protocol	Preference	Next Hop
10.0.0.0/30	Static	**60**	30.1.1.2
10.0.0.0/30	OSPF	**10**	20.1.1.2

Installed in the IP routing table

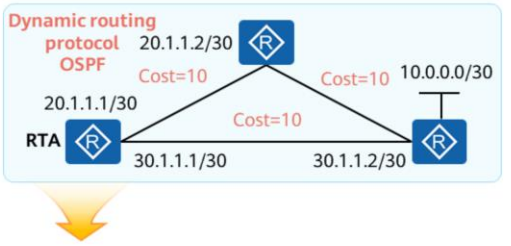
- RTA discovers two routes to 10.0.0.0/30, one is an OSPF route and the other a static route. In this case, RTA compares the preferences of the two routes and selects the route with the lowest preference value.
- Each routing protocol has a unique preference.
- OSPF has a higher preference. Therefore, the OSPF route is installed in the IP routing table.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- RTA learns two routes to the same destination, one is a static route and the other an OSPF route. It then compares the preferences of the two routes, and prefers the OSPF route because this route has a higher preference. RTA installs the OSPF route in the IP routing table.

Metric - Comparison Process

Metric comparison



IP routing table of RTA

Destination/Mask	Protocol	Cost	Next Hop
10.0.0.0/30	OSPF	**20**	20.1.1.2
10.0.0.0/30	OSPF	**10**	30.1.1.2

Installed in the IP routing table

- RTA learns two routes with the same destination address (10.0.0.0/30) and preference through OSPF. In this case, RTA needs to compare the metrics of the two routes.
- The two routes have different metrics. The OSPF route with the next hop being 30.1.1.2 has a lower metric (with the cost 10), so it is installed in the IP routing table.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Route Preference - Common Default Values

- The following table lists the default preference values of common route types:

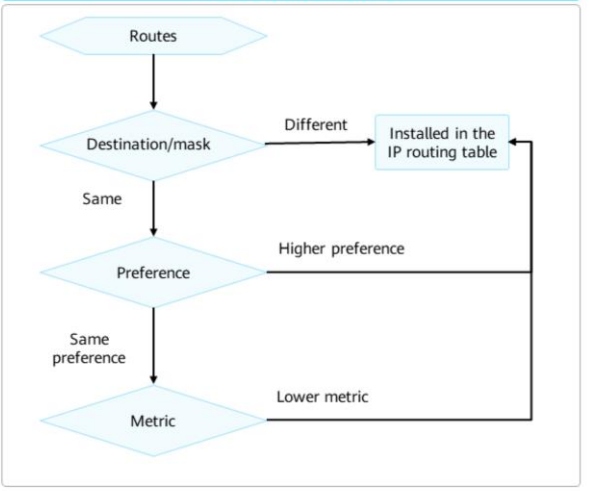
Protocol	Route Type	Default Preference
Direct	Direct route	0
Static	Static route	60
Dynamic routing protocol	OSPF internal route	10
	OSPF external route	150

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The table lists the preferences of some common routing protocols. Actually, there are multiple types of dynamic routes. We will learn these routes in subsequent courses.

Metric - Basic Concepts

Comparing Metrics



- When a router discovers multiple routes to the same destination network through the same routing protocol, the router selects the optimal route based on the metrics of these routes if these routes have the same preference.
- The metric of a route indicates the cost of reaching the destination address of the route.
- Common metrics include the hop count, bandwidth, delay, cost, load, and reliability.
- The route with the lowest metric is installed in the IP routing table.
- The metric is also known as the cost.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

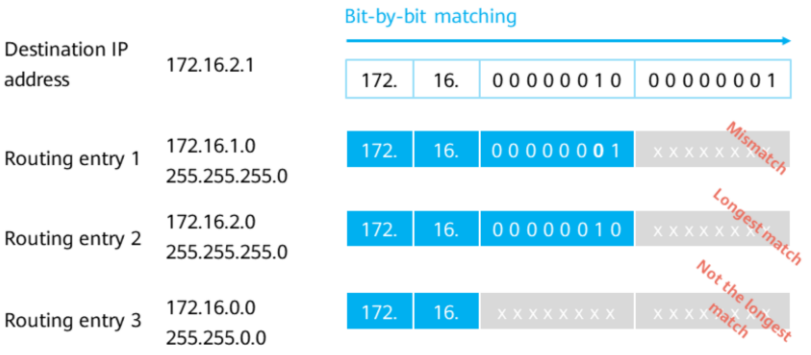
Contents

1. **Overview of IP Routing**
   - Basic Concepts of Routing
   - Generation of Routing Entries
   - Optimal Route Selection
   - **Route-based Forwarding**
2. Static Routing
3. Dynamic Routing
4. Advanced Routing Features

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Longest Matching

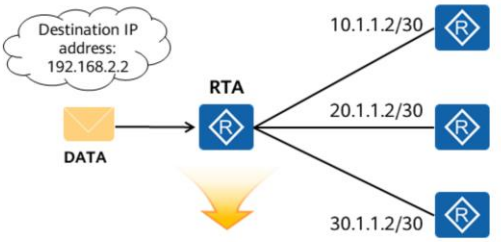
- When a router receives an IP packet, it compares the destination IP address of the packet with all routing entries in the local routing table bit by bit until the longest matching entry is found. This is the longest matching mechanism.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Example of Longest Matching (1)

Example of Longest Matching



IP routing table of RTA

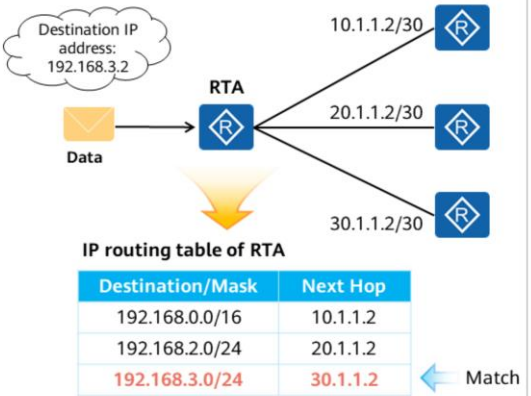
Destination/Mask	Next Hop	
192.168.0.0/16	10.1.1.2	
192.168.2.0/24	20.1.1.2	Match
192.168.3.0/24	30.1.1.2	

- There are two routes to 192.168.2.2 in the IP routing table of RTA, one has the 16-bit mask and the other has the 24-bit mask. According to the longest matching rule, the route with the 24-bit mask is preferred to guide the forwarding of packets destined for 192.168.2.2.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example of Longest Matching (2)

Example of Longest Matching

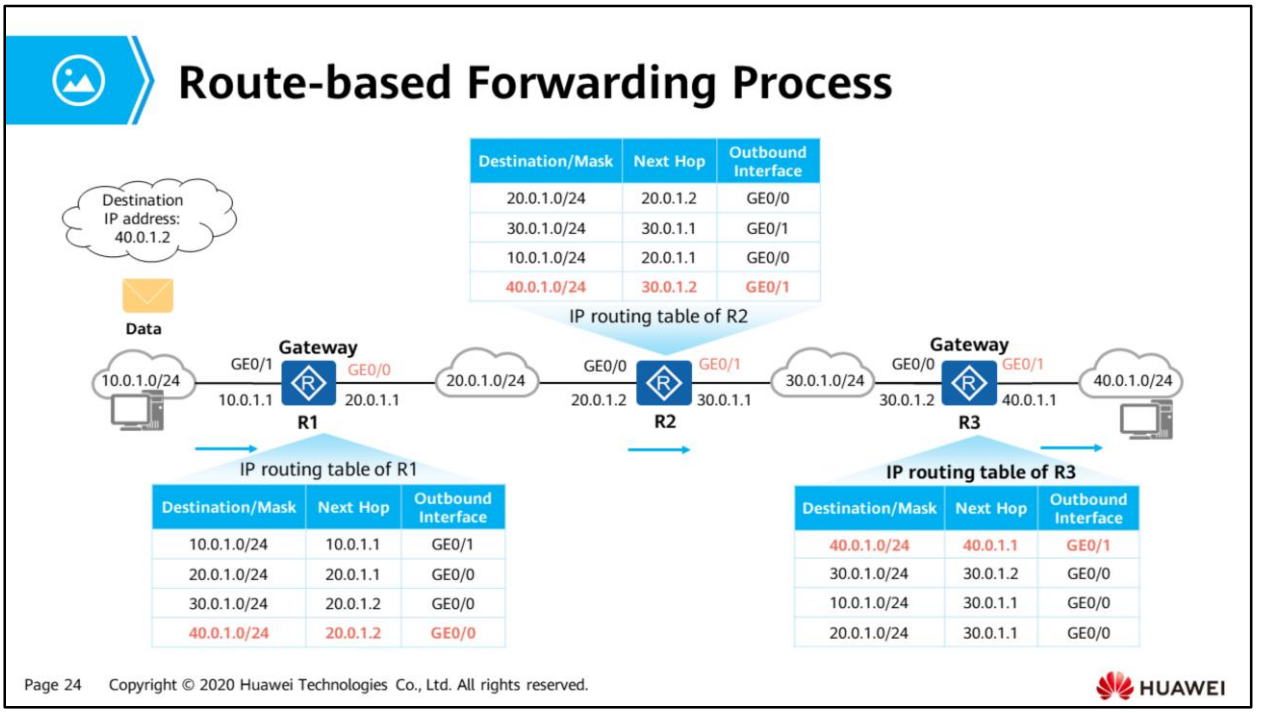


IP routing table of RTA

Destination/Mask	Next Hop	
192.168.0.0/16	10.1.1.2	
192.168.2.0/24	20.1.1.2	
192.168.3.0/24	30.1.1.2	Match

- According to the longest matching rule, only the route to 192.168.3.0/24 in the IP routing table matches the destination IP address 192.168.3.2. Therefore, this route is used to forward packets destined for 192.168.3.2.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The IP packets from 10.0.1.0/24 need to reach 40.0.1.0/24. After receiving these packets, the gateway R1 searches its IP routing table for the next hop and outbound interface and forwards the packets to R2. After the packets reach R2, R2 forwards the packets to R3 by searching its IP routing table. Upon receipt of the packets, R3 searches its IP routing table, finding that the destination IP address of the packets belongs to the subnet where a local interface resides. Therefore, R3 directly forwards the packets to the destination subnet 40.0.1.0/24.

Summary of the IP Routing Table

- When a router obtains routes to the same destination subnet with the same mask from different routing protocols, the router prefers the route with the lowest preference value of these routing protocols. If these routes are learned from the same routing protocol, the router prefers the route with the lowest cost. In summary, only the optimal route is installed in the IP routing table.
- When a router receives a packet, it searches its IP routing table for the outbound interface and next hop based on the destination IP address of the packet. If it finds a matching routing entry, it forwards the packet according to the outbound interface and next hop specified by this entry. Otherwise, it discards the packet.
- Packets are forwarded hop by hop. Therefore, all the routers along the path from the source to the destination must have routes destined for the destination. Otherwise, packet loss occurs.
- Data communication is bidirectional. Therefore, both forward and backward routes must be available.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



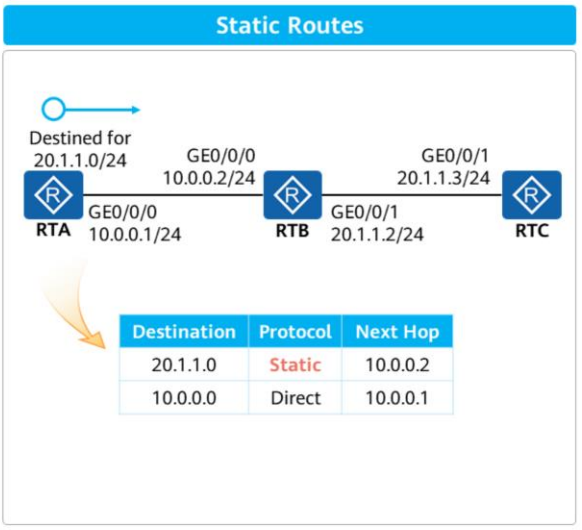
Contents

1. Overview of IP Routing
2. **Static Routing**
3. Dynamic Routing
4. Advanced Routing Features

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Application Scenarios of Static Routes



- Static routes are manually configured by network administrators, have low system requirements, and apply to simple, stable, and small networks.
- The disadvantage of static routes is that they cannot automatically adapt to network topology changes and so require manual intervention.
- RTA needs to forward the packets with the destination address 20.1.1.0/24. However, the IP routing table of RTA has only one direct route, which does not match 20.1.1.0/24. In this case, a static route needs to be manually configured so that the packets sent from RTA to 20.1.1.0/24 can be forwarded to the next hop 10.0.0.2.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Static Route Configuration

- Specify a next-hop IP address for a static route.

  [Huawei] **ip route-static** *ip-address* { *mask* | *mask-length* } *nexthop-address*

- Specify an outbound interface for a static route.

  [Huawei] ***ip route-static ip-address { mask | mask-length } interface-type interface-number***

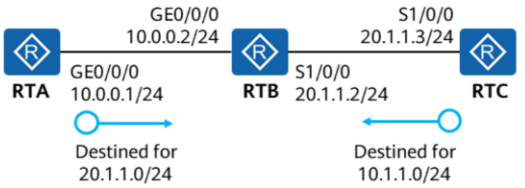
- Specify both the outbound interface and next hop for a static route.

  [Huawei] **ip route-static** *ip-address { mask | mask-length } interface-type interface-number [nexthop-address]*

  When creating a static route, you can specify both the outbound interface and next hop. Alternatively, you can specify either the outbound interface or next hop, depending on the interface type:
  For a point-to-point interface (such as a serial interface), you must specify the outbound interface.
  For a broadcast interface (for example, an Ethernet interface) or a virtual template (VT) interface, you must specify the next hop.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Example



- Configure static routes on RTA and RTC for communication between 10.0.0.0/24 and 20.1.1.0/24.
- Packets are forwarded hop by hop. Therefore, all the routers along the path from the source to the destination must have routes destined for the destination.
- Data communication is bidirectional. Therefore, both forward and backward routes must be available.

Configure RTA.

```
[RTA] ip route-static 20.1.1.0 255.255.255.0 10.0.0.2
```

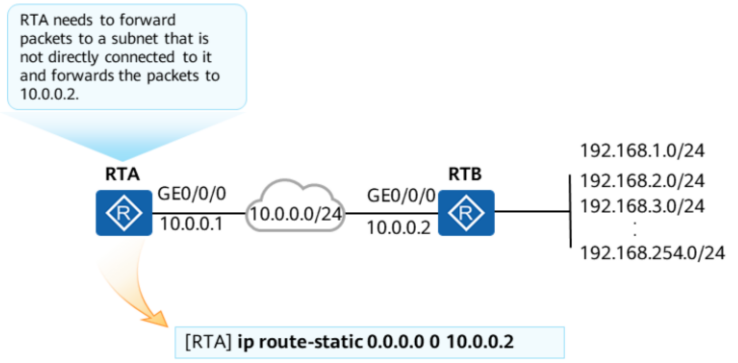
Configure RTC.

```
[RTC] ip route-static 10.0.0.0 255.255.255.0 S1/0/0
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Default Routes

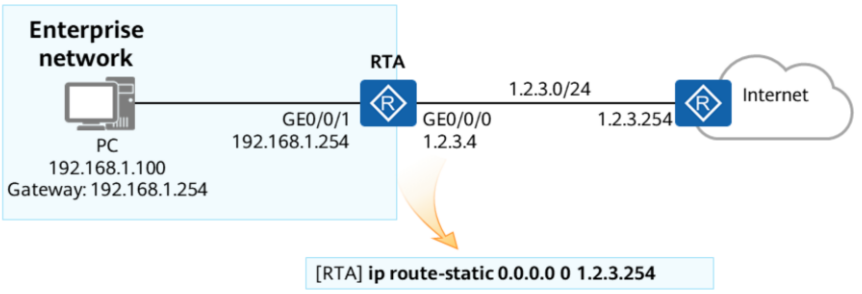
- Default routes are used only when packets to be forwarded do not match any routing entry in an IP routing table.
- In an IP routing table, a default route is the route to network 0.0.0.0 (with the mask 0.0.0.0), namely, 0.0.0.0/0.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Application Scenarios of Default Routes

- Default routes are typically used at the egress of an enterprise network. For example, you can configure a default route on an egress device to enable the device to forward IP packets destined for any address on the Internet.

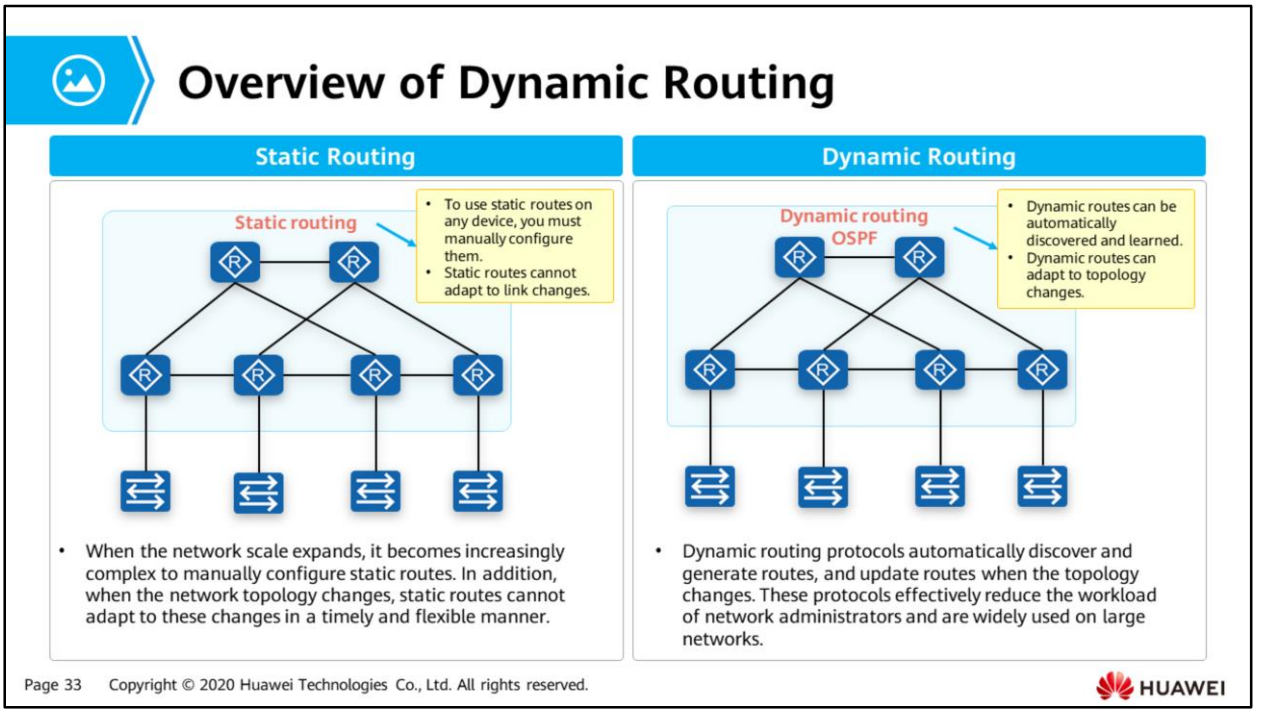


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

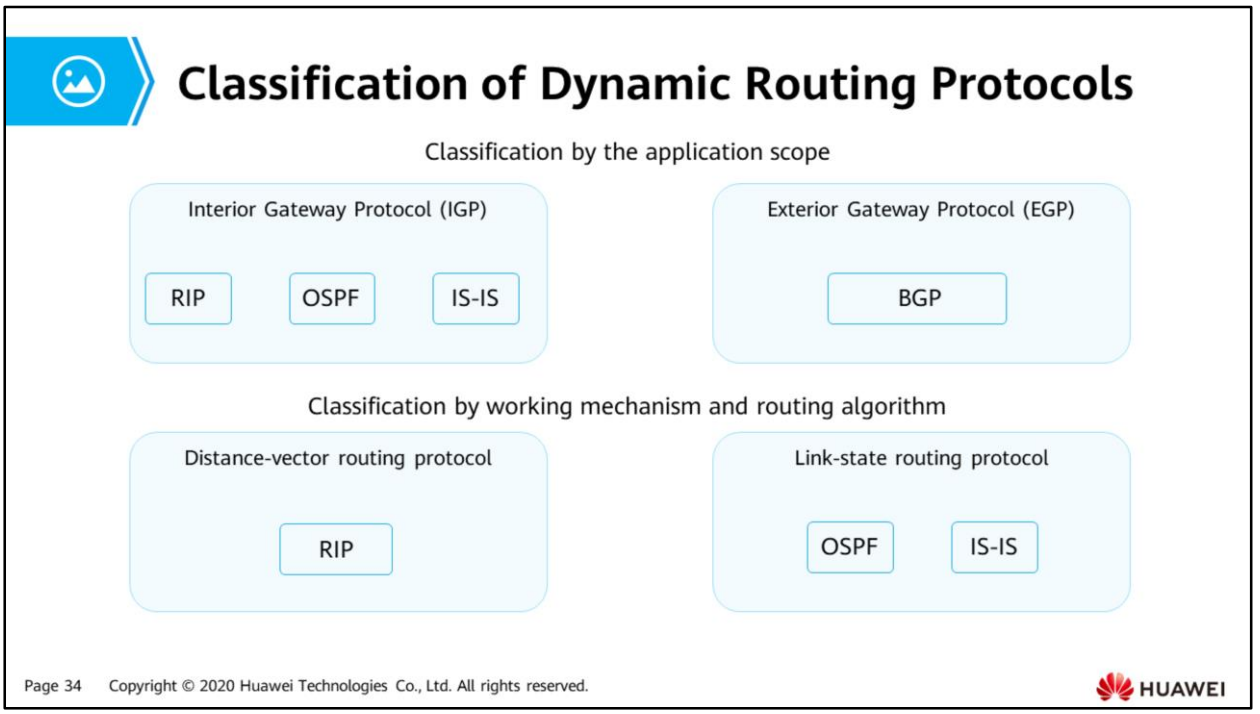
Contents

1. Overview of IP Routing
2. Static Routing
3. **Dynamic Routing**
4. Advanced Routing Features

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The disadvantage of static routes is that they cannot automatically adapt to network topology changes and so require manual intervention.
- Dynamic routing protocols provide different routing algorithms to adapt to network topology changes. Therefore, they are applicable to networks on which many Layer 3 devices are deployed.



- Dynamic routing protocols are classified into two types based on the routing algorithm:
  - Distance-vector routing protocol
    - RIP
  - Link-state routing protocol
    - OSPF
    - IS-IS
  - BGP uses a path vector algorithm, which is modified based on the distance-vector algorithm. Therefore, BGP is also called a path-vector routing protocol in some scenarios.
- Dynamic routing protocols are classified into the following types by their application scope:
  - IGPs run within an autonomous system (AS), including RIP, OSPF, and IS-IS.
  - EGP runs between different ASs, among which BGP is the most frequently used.



Contents

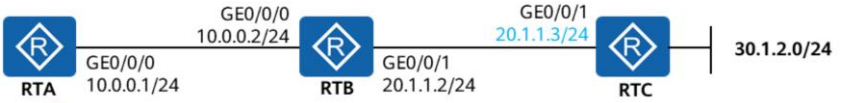
1. Overview of IP Routing
2. Static Routing
3. Dynamic Routing
4. **Advanced Routing Features**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Route Recursion (1)

- Route recursion is a recursive search process of the IP routing table where the next-hop IP address is wanted to route packets towards its destination but when found it is not part of any directly connected network.



[RTA] **ip route-static 30.1.2.0 24 20.1.1.3**

The next hop of the route to 30.1.2.0/24 is 20.1.1.3, which is not on a directly connected network of RTA. If the IP routing table does not have a route to 20.1.1.3, this static route does not take effect and cannot be installed in the IP routing table.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Route Recursion (2)



[RTA] **ip route-static 30.1.2.0 24 20.1.1.3**

Recursion

[RTA] **ip route-static 20.1.1.0 24 10.0.0.2**

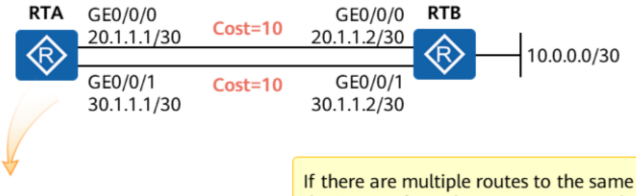
Destination/ Mask	Next Hop	Outbound Interface
30.1.2.0/24	20.1.1.3	GE0/0/0
20.1.1.0/24	10.0.0.2	GE0/0/0

Configure a route to 20.1.1.3, with the next hop pointing to 10.0.0.2 on the directly connected network. In this way, RTA can recurse the route with the destination 30.1.2.0/24 to the route with the destination 10.0.0.2.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Equal-Cost Route

- When there are equal-cost routes in the IP routing table, a router forwards IP packets to be sent to the destination subnet through all valid outbound interfaces and next hops in the equal-cost routes, achieving load balancing.



RTA's IP routing table

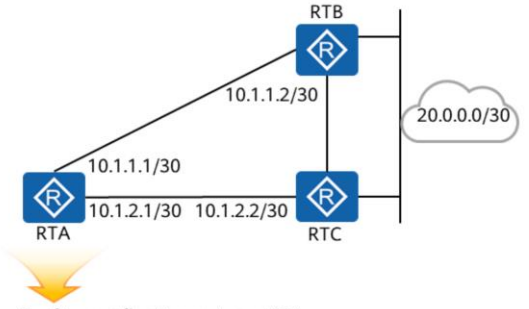
Destination/Mask	Next Hop
10.0.0.0/30	20.1.1.2
	30.1.1.2

If there are multiple routes to the same destination from the same source, with the same cost, but pointing to different next hops, the routes are installed in the IP routing table as equal-cost routes. Traffic to be sent to the destination will be distributed to these equal-cost routes.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Floating Route - Basic Concepts

Floating Route

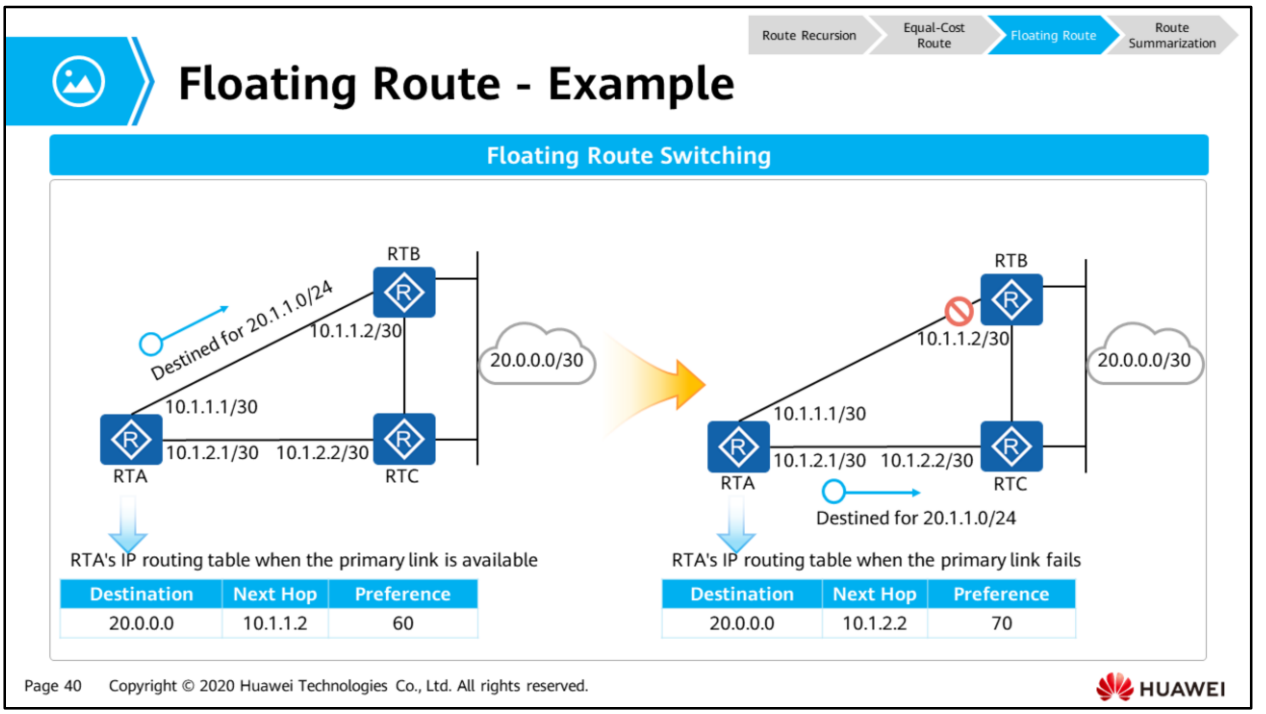


Configure a floating route on RTA.

```
[RTA] ip route-static 20.0.0.0 30 10.1.1.2
[RTA] ip route-static 20.0.0.0 30 10.1.2.2 preference 70
```

- Different preferences can be manually configured for static routes. Therefore, you can configure two static routes with the same destination address/mask but different preferences and next hops to implement backup of forwarding paths.
- A backup route is known as a floating route, which is used only when the primary route is unavailable. That is, a floating route is installed in the IP routing table only when the next hop of the primary route is unreachable.

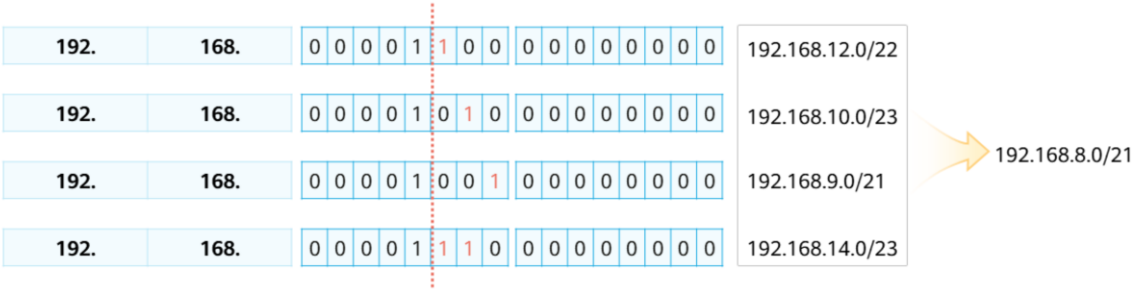
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI



- When the link between RTA and RTB is normal, the two routes to 20.0.0.0/30 are both valid. In this case, RTA compares the preferences of the two routes, which are 60 and 70 respectively. Therefore, the route with the preference value 60 is installed in the IP routing table, and RTA forwards traffic to the next hop 10.1.1.2.
- If the link between RTA and RTB is faulty, the next hop 10.1.1.2 is unreachable, which causes the corresponding route invalid. In this case, the backup route to 20.0.0.0/30 is installed in the IP routing table. RTA forwards traffic destined for 20.0.0.1 to the next hop 10.1.2.2.

CIDR

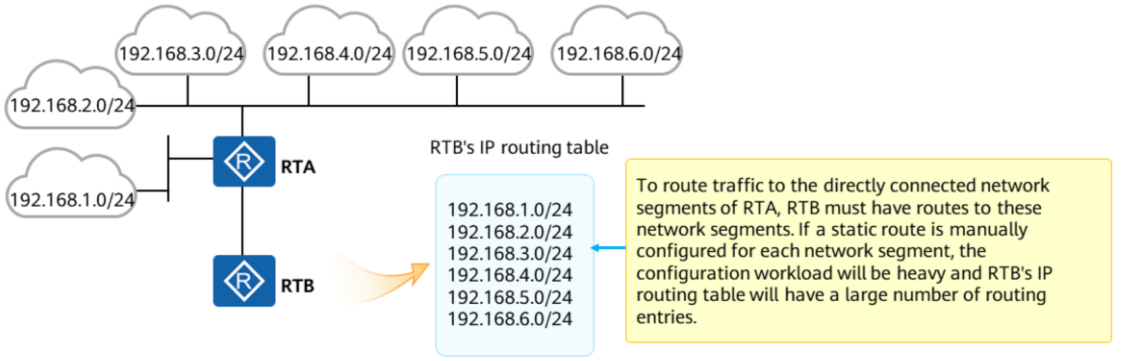
- Classless Inter-Domain Routing (CIDR) uses IP addresses and masks to identify networks and subnets. CIDR replaces the previous addressing architecture of classful network design (such as classes A, B, and C addresses).
- CIDR is based on variable length subnet mask (VLSM). CIDR uses prefixes of any lengths to divide the address space with continuous IP addresses. Multiple address segments with continuous prefixes can be summarized into a network, effectively reducing the number of routing entries.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Background of Route Summarization

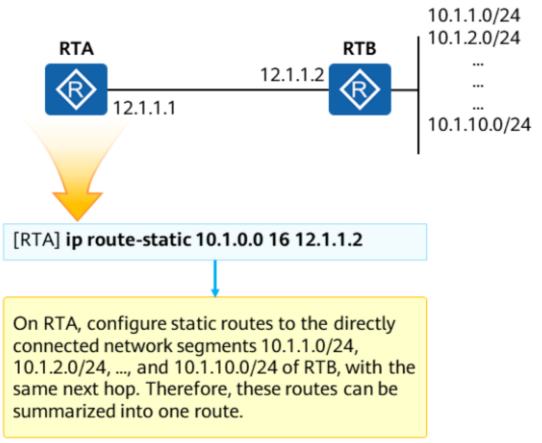
- Subnet division and VLSM resolve the problem of address space waste, but also bring a new challenge: increasing routing entries in the IP routing table.
- Route summarization can minimize routing entries.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- On a large-scale network, routers or other routing-capable devices need to maintain a large number of routing entries, which will consume a large amount of device resources. In addition, the IP routing table size is increasing, resulting in a low efficiency of routing entry lookup. Therefore, we need to minimize the size of IP routing tables on routers while ensuring IP reachability between the routers and different network segments. If a network has scientific IP addressing and proper planning, we can achieve this goal by using different methods. A common and effective method is route summarization, which is also known as route aggregation.

Overview of Route Summarization



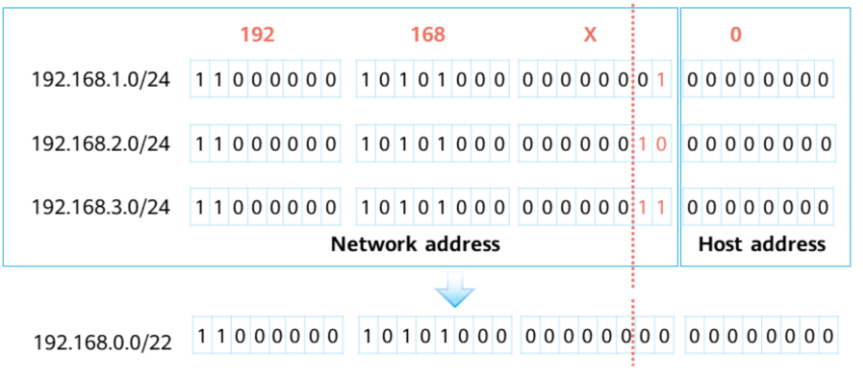
- Route summarization is an approach of summarizing routes with the same prefix into one summary route to minimize the IP routing table size and improve device resource usage.
- Route summarization uses CIDR to summarize network segments with the same prefix into a single one.
- The routes before being summarized are known as specific routes, and the routes created after summarization are known as summarized routes or summary routes.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- To enable RTA to reach remote network segments, we need to configure a specific route to each network segment. In this example, the routes to 10.1.1.0/24, 10.1.2.0/24, and 10.1.3.0/24 have the same next hop, that is, 12.1.1.2. Therefore, we can summarize these routes into a single one.
- This effectively reduces the size of RTA's IP routing table.

Summarization and Calculation

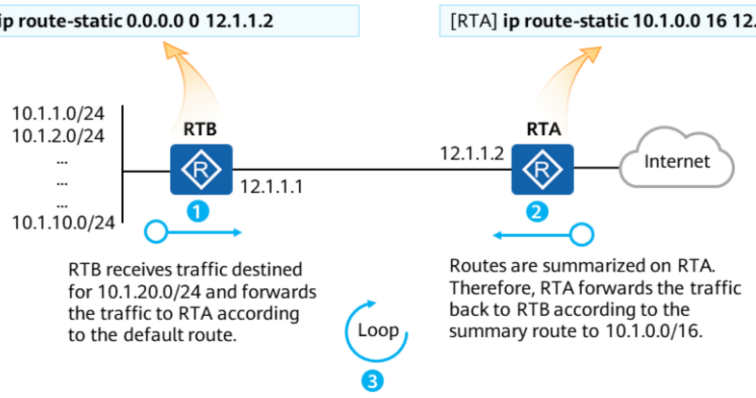


- To summarize routes to multiple continuous network segments into one summary route that just includes these network segments, ensure that the mask length of the summary route is as long as possible.
- The key to achieve this is to convert the destination addresses of specific routes into binary numbers and then find out the identical bits in these binary numbers.

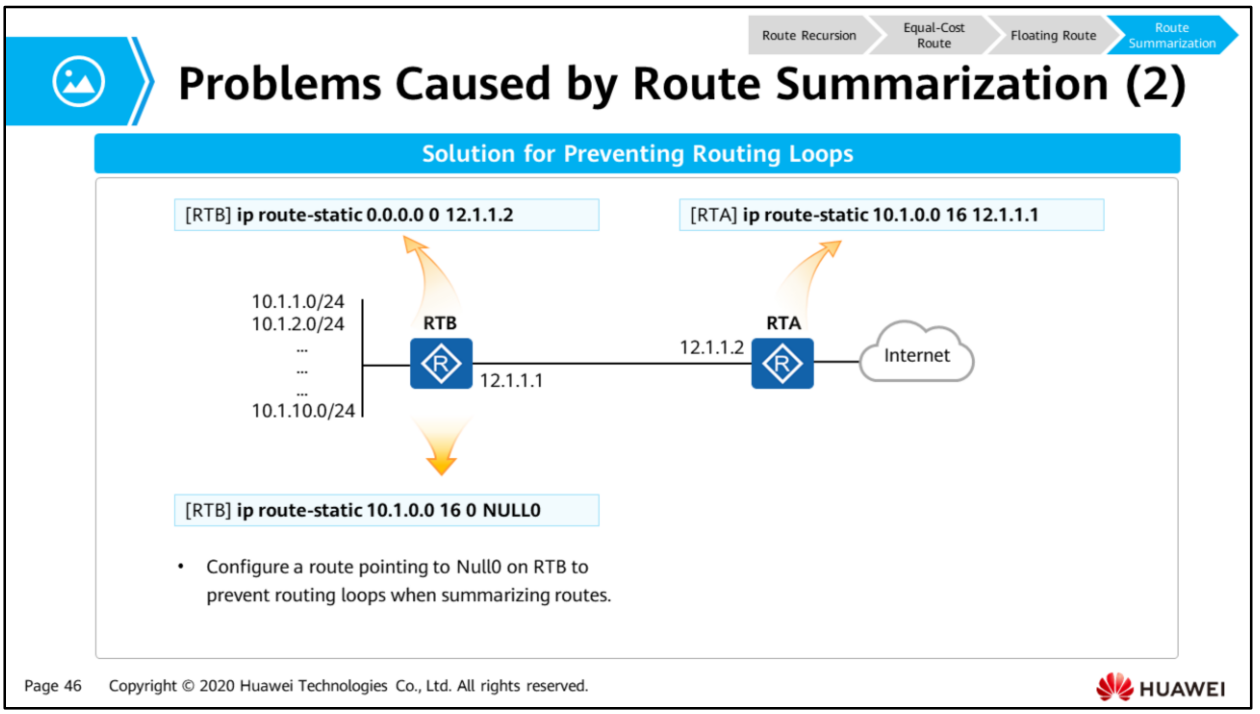
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Problems Caused by Route Summarization (1)

Routing Loop

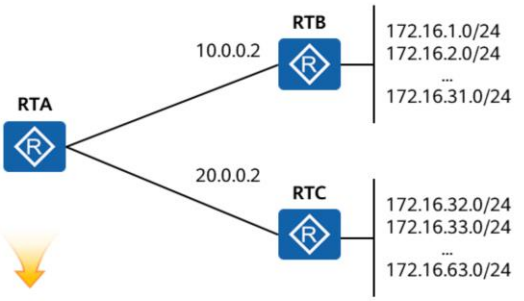


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- In most cases, both static and dynamic routes need to be associated with an outbound interface. This interface is the egress through which the device is connected to a destination network. The outbound interface in a route can be a physical interface such as a 100M or GE interface, or a logical interface such as a VLANIF or tunnel interface. There is a special interface, that is, Null interface. It has only one interface number, that is, 0. Null0 is a logical interface and is always up. When Null0 is used as the outbound interface in a route, data packets matching this route are discarded, like being dumped into a black-hole. Therefore, such a route is called a black-hole route.

Accurate Route Summarization (1)



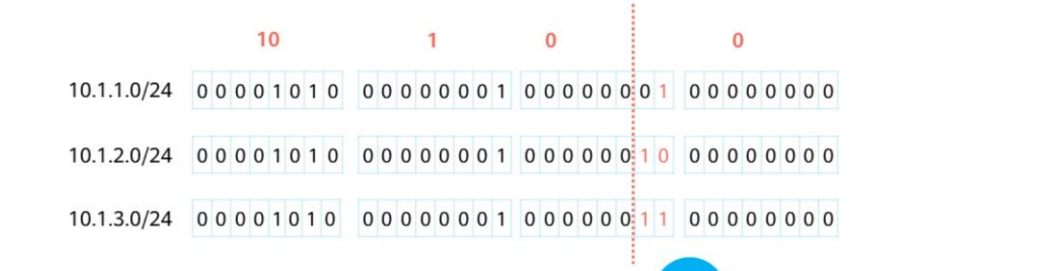
[RTA] **ip route-static 172.16.0 16 10.0.0.2**

- To simplify the configuration, an administrator may configure a static summary route on RTA to allow RTA to reach network segments 172.16.1.0/24 to 172.16.31.0/24 of RTB. However, this summary route also includes the network segments of RTC. As a result, RTA forwards the traffic destined for network segments of RTC to RTB, causing data packet loss. This problem is caused by inaccurate route summarization. To resolve this problem, the summary route must be as accurate as possible; that is, it just covers all specific routes that are to be summarized, with no extra route included.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Accurate Route Summarization (2)




```
ip route-static 10.1.1.0 24 12.1.1.2
ip route-static 10.1.2.0 24 12.1.1.2
ip route-static 10.1.3.0 24 12.1.1.2
```

/22

```
ip route-static 10.1.1.0 22 12.1.1.2
```

Accurately calculate the summarized network address and mask to ensure accurate route summarization.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Quiz

1. How does a router select the optimal route?
2. How do I configure a floating route?
3. What is the summary route for routes to 10.1.1.0/24, 10.1.3.0/24, and 10.1.9.0/24?

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. The router first compares preferences of routes. The route with the lowest preference value is selected as the optimal route. If the routes have the same preferences, the router compares their metrics. If the routes have the same metric, they are installed in the IP routing table as equal-cost routes.
2. To configure a floating route, configure a static route with the same destination network segment and mask as the primary route but a different next hop and a larger preference value.
3. The summary route is 10.1.0.0/20.

Summary

- This section presents the basic concepts of routes, how routes instruct routers to forward IP packets, common route attributes, and default routes (special static routes).
- In addition, this section describes advanced routing features including route recursion, floating routes, and equal-cost routes, which are widely used on live networks.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



OSPF Basics

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- Static routes are manually configured. If a network topology changes, static routes have to be manually adjusted, which restricts the large-scale application of static routes on the live network.
- Dynamic routing protocols are widely used on live networks because of their high flexibility, high reliability, and easy scalability. The Open Shortest Path First (OSPF) protocol is a widely used dynamic routing protocol.
- This course describes basic concepts, working mechanism, and basic configurations of OSPF.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Describe the advantages and classification of dynamic routing protocols.
  - Describe basic OSPF concepts and usage scenarios.
  - Describe the working mechanism of OSPF.
  - Implement basic OSPF configurations.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

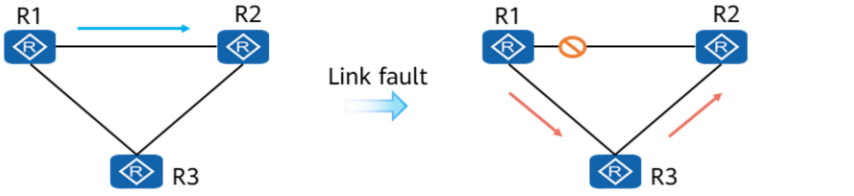
Contents

1. **OSPF Overview**
2. OSPF Working Mechanism
3. Typical OSPF Configuration

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Why Are Dynamic Routing Protocol Used?

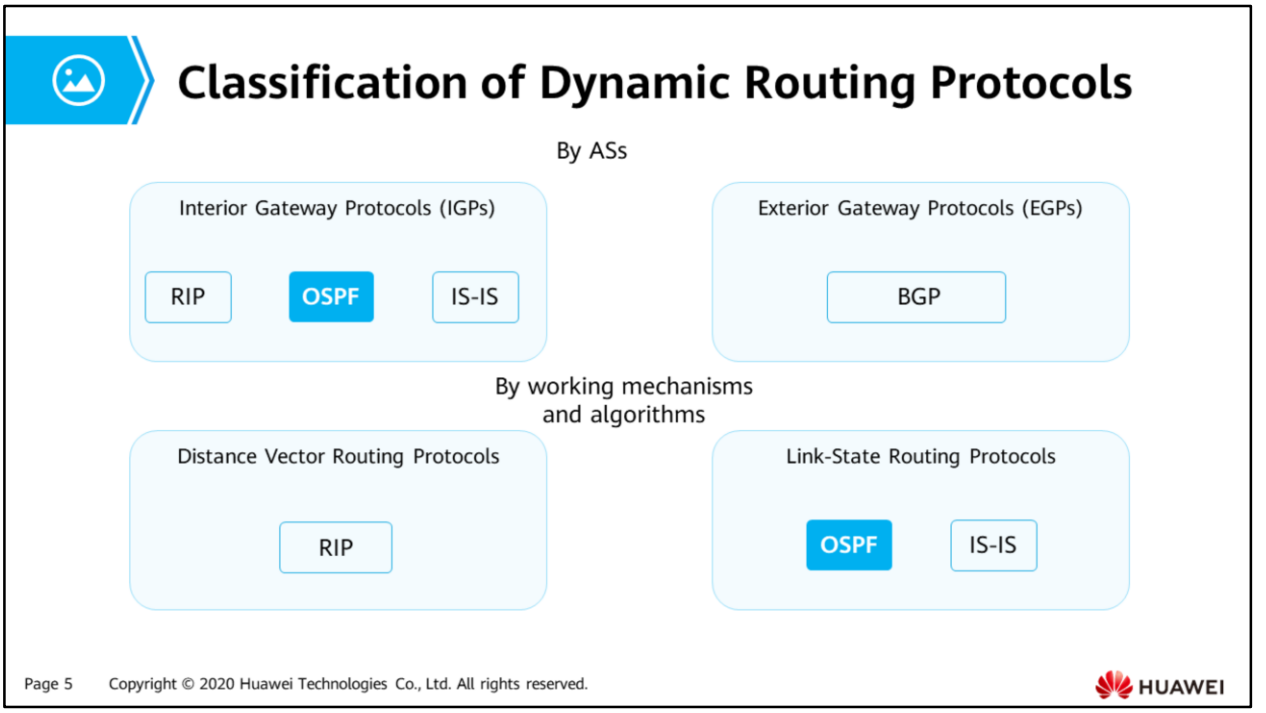
- Static routes are manually configured and maintained, and the command lines are simple and clear. They apply to small-scale or stable networks. Static routes have the following disadvantages:
  - Unable to adapt to large-scale networks: As the number of devices increases, the configuration workload increases sharply.
  - Unable to dynamically respond to network changes: If the network topology changes, the network cannot automatically converge, and static routes must be manually modified.



R1-to-R2 static route

Manually configured static route R1-R3-R2

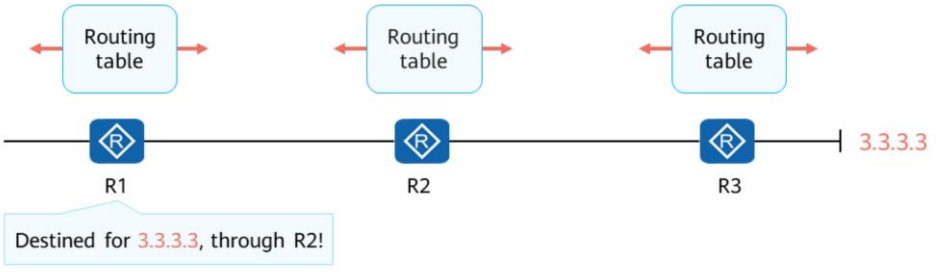
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- BGP uses the path-vector algorithm, which is a modified version of the distance-vector algorithm.

Distance-Vector Routing Protocol

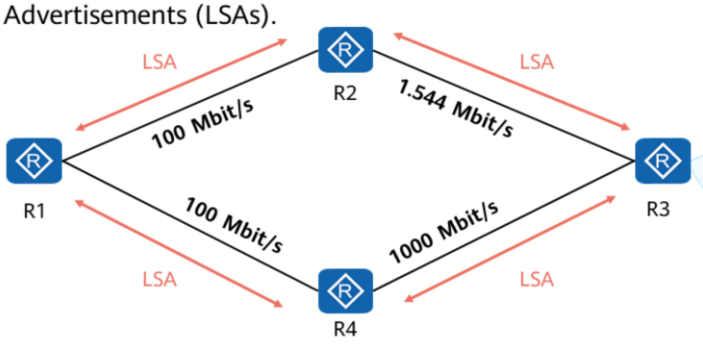
- A router running a distance-vector routing protocol periodically floods routes. Through route exchange, each router learns routes from neighboring routers and installs the routes into its routing table.
- Each router on a network is clear only about where the destination is and how far the destination is, but unclear about the whole network topology. This is the essence of the distance-vector algorithm.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Link-State Routing Protocol - LSA Flooding

- Different from a distance-vector routing protocol, a link-state routing protocol advertises link status information rather than routes in the routing table. Routers that run a link-state routing protocol establish a neighbor relationship and then exchange Link State Advertisements (LSAs).



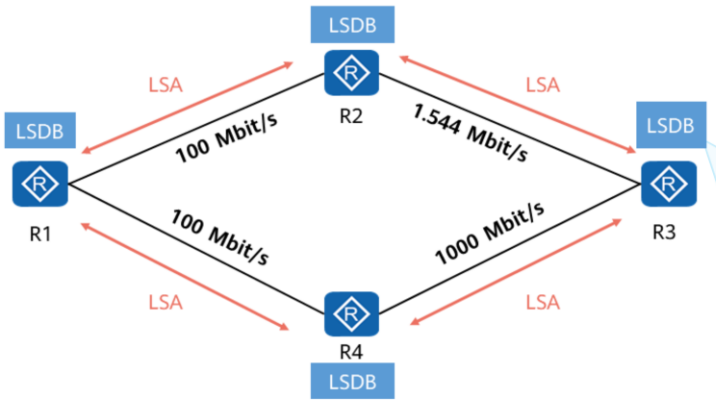
- LSAs, instead of routes, are advertised.
- An LSA describes a router interface's status information, such as the cost of the interface and a connected interface name.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Each router generates an LSA that describes status information about its directly connected interface. The LSA contains the interface cost and the relationship between the router and its neighboring routers.

Link-State Routing Protocol - LSDB Creation

- Each router generates LSAs and adds the received LSAs to its own link state database (LSDB). Routers learn the whole network topology through the LSDB.

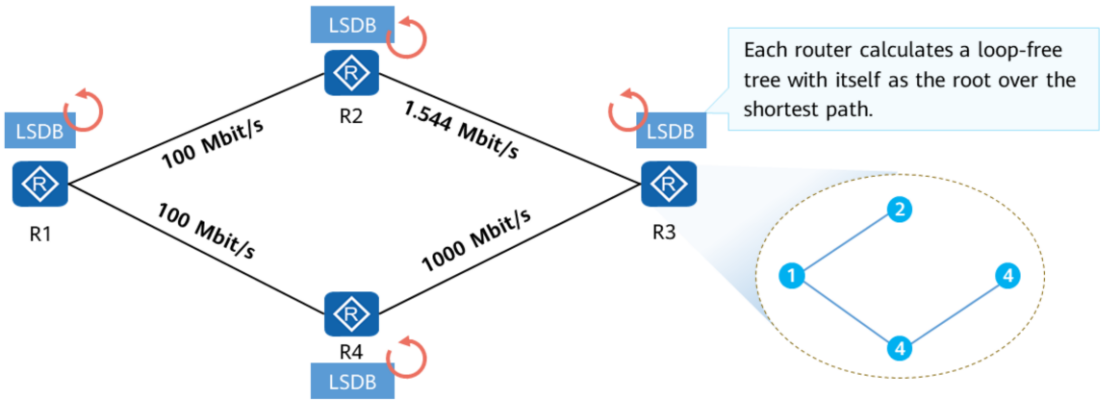


- The router stores LSAs in the LSDB.
- The LSDB contains the description of all router interfaces on the network.
- The LSDB contains the description of the entire network topology.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Link-State Routing Protocol - SPF Calculation

- Each router uses the Shortest Path First (SPF) algorithm and LSDB information to calculate routes. Each router calculates a loop-free tree with itself as the root and the shortest path. With this tree, a router determines the optimal path to each corner of a network.

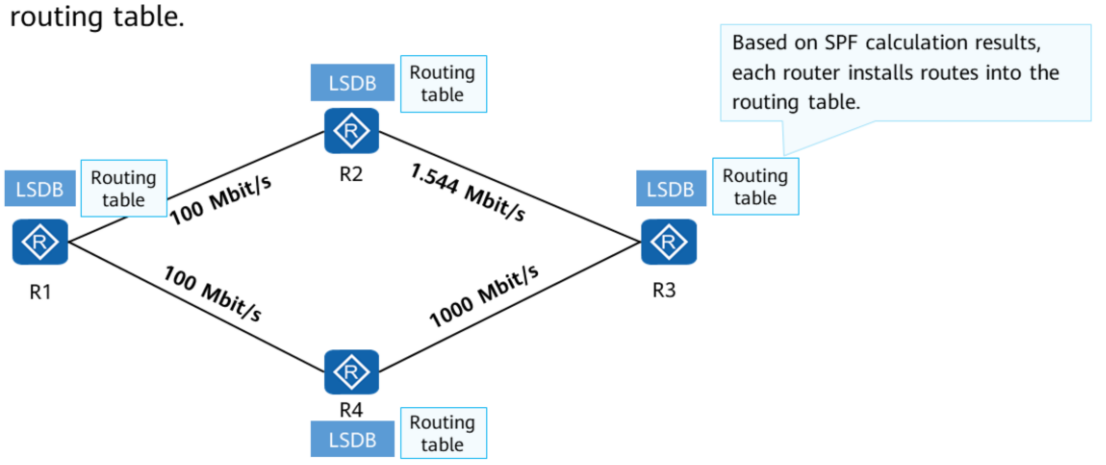


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

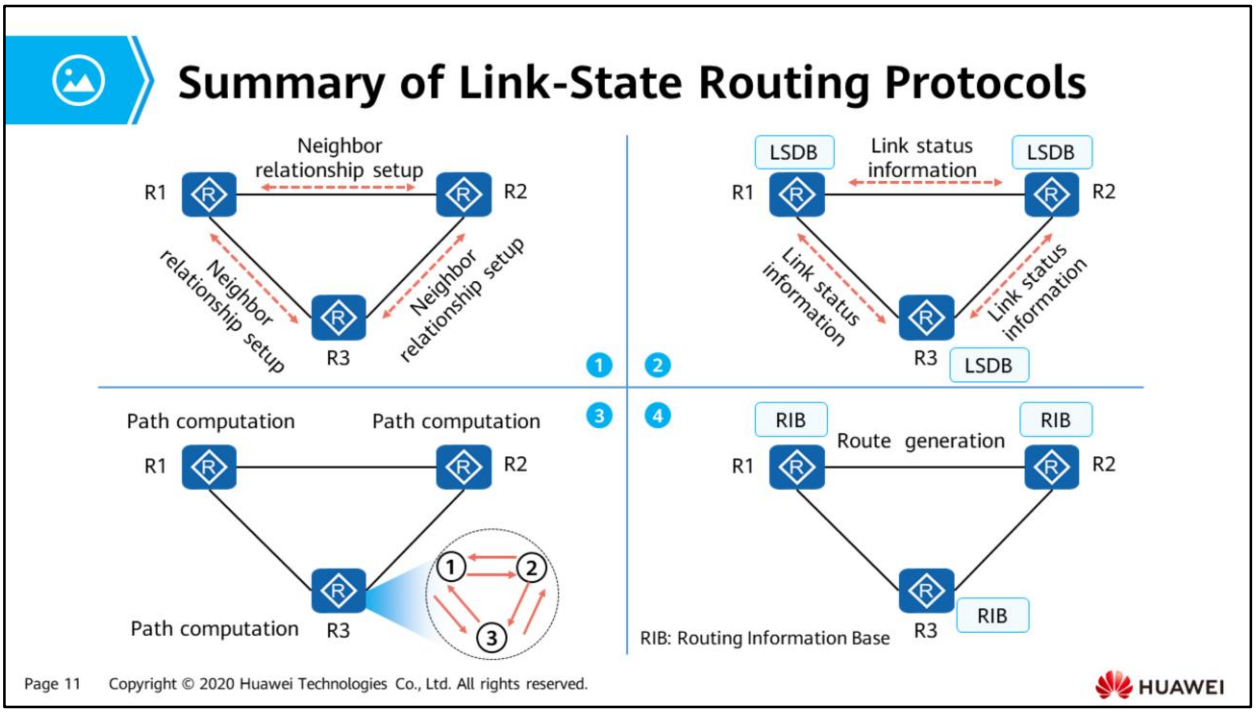
- SPF is a core algorithm of OSPF and used to select preferred routes on a complex network.

Link-State Routing Protocol - Routing Table Generation

- Ultimately, the router installs routes for the calculated preferred paths into its routing table.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



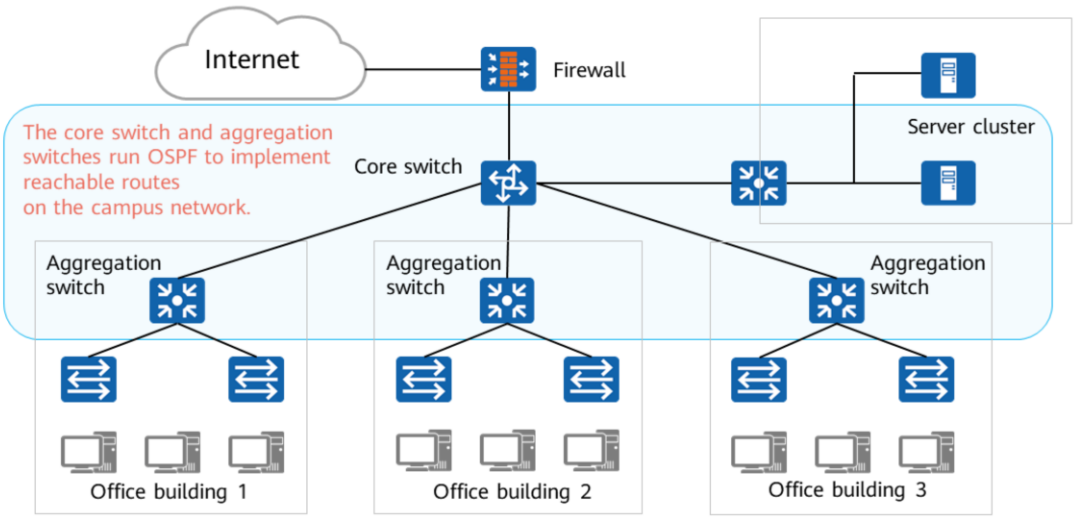
- The implementation of a link-state routing protocol is as follows:
  - Step 1: Establishes a neighbor relationship between neighboring routers.
  - Step 2: Exchanges link status information and synchronizes LSDB information between neighbors.
  - Step 3: Calculates an optimal path.
  - Step 4: Generates route entries based on the shortest path tree and loads the routing entries to the routing table.

Introduction to OSPF

- OSPF is a typical link-state routing protocol and one of the widely used IGPs in the industry.
- OSPFv2, as defined in RFC 2328, is designed for IPv4. OSPFv3, as defined in RFC 2740, is designed for IPv6. Unless otherwise specified, OSPF in this presentation refers to OSPFv2.
- OSPF routers exchange link status information, but not routes. Link status information is key information for OSPF to perform topology and route calculation.
- An OSPF router collects link status information on a network and stores the information in the LSDB. Routers are aware of the intra-area network topology and be able to calculate loop-free paths.
- Each OSPF router uses the SPF algorithm to calculate the shortest path to a specific destination. Routers generate routes based on these paths and install the routes to the routing table.
- OSPF supports the variable length subnet mask (VLSM) mechanism and manual route summarization.
- The multi-area design enables OSPF to support a larger network.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

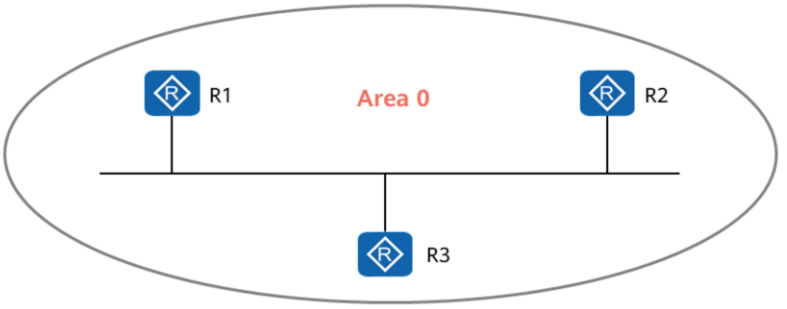
OSPF Application on a Campus Network



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic OSPF Concepts: Area

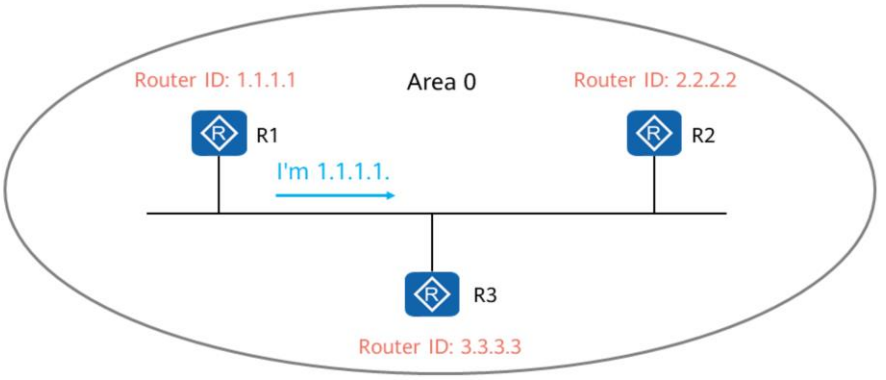
- The OSPF area keyword identifies an OSPF area.
- The area is considered as a logical group, and each group is identified by an area ID.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic OSPF Concepts: Router ID

- A router ID uniquely identifies a router in an OSPF area.
- The router ID can be manually specified or automatically assigned by the system.



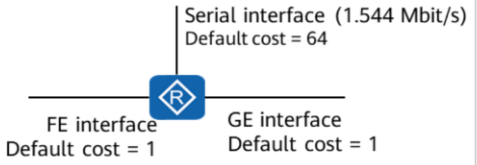
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In actual projects, OSPF router IDs are manually set for devices. Ensure that the router IDs of any two devices in an OSPF area are different. Generally, the router ID is set the same as the IP address of an interface (usually a Loopback interface) on the device.

Basic OSPF Concepts: Cost Value

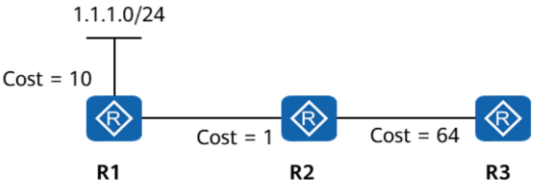
- OSPF uses costs as route metric values. Each OSPF-enabled interface maintains a cost value. Default cost value = $\frac{\text{100 Mbit/s}}{\text{Interface bandwidth}}$, where, 100 Mbit/s is the default reference value specified by OSPF and is configurable.
- Generally, the cost of an OSPF route is the sum of costs of all inbound interfaces along a path from the destination network segment to the local router.

Cost Value of an OSPF Interface



- Each OSPF interface has a specific cost because of the particular bandwidth value.

Accumulated Costs on an OSPF Path



- In the routing table of R3, the cost of the OSPF route to 1.1.1.0/24 is 75 (10 + 1 + 64).

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

OSPF Packet Types

- There are five types of OSPF protocol packets and implement different functions in interaction between OSPF routers.

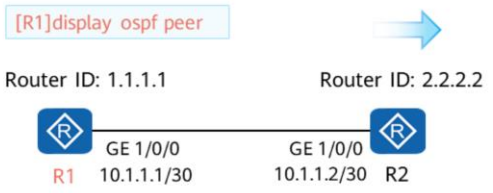
Packet Name	Function
Hello	Is periodically sent to discover and maintain OSPF neighbor relationships.
Database Description	Describes the summary of the local LSDB, which is used to synchronize the LSDBs of two devices.
Link State Request	Requests a needed LSA from a neighbor. LSRs are sent only after DD packets have been successfully exchanged.
Link State Update	Is sent to advertise a requested LSA to a neighbor.
Link State ACK	Is used to acknowledge the receipt of an LSA.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Neighbor Table | LSDB Table | OSPF Routing table

Three Types of OSPF Entries - Entries in the Neighbor Table

- OSPF provides entries in three important tables: OSPF neighbor table, LSDB table, and OSPF routing table. For the OSPF neighbor table, you need to know:
  - Before OSPF transmits link status information, OSPF neighbor relationships must be established.
  - OSPF neighbor relationships are established by exchanging Hello packets.
  - The OSPF neighbor table describes the status of the neighbor relationship between OSPF routers. You can run the **display ospf peer** command to view status information.




```
<R1> display ospf peer
    OSPF Process 1 with Router ID 1.1.1.1
                Neighbors
Area 0.0.0.0 interface 10.1.1.1 (GigabitEthernet1/0/0)'s neighbors
Router ID:  2.2.2.2    Address:  10.1.1.2    GR State: Normal
    State: Full  Mode:Nbr is  Master  Priority: 1
    DR:  10.1.1.1  BDR: 10.1.1.2   MTU: 0
    Dead timer due in 35  sec
    Retrans timer interval: 5
    Neighbor is up for 00:00:05
    Authentication Sequence: [ 0 ]
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

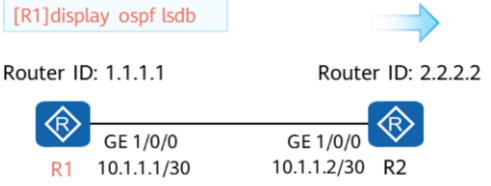
- The OSPF neighbor table contains much key information, such as router IDs and interface addresses of neighboring devices. For more details, see "OSPF Working Mechanism".

Neighbor Table | LSDB Table | OSPF Routing Table

Three Types OSPF Entries - Entries in the LSDB Table

- For the OSPF LSDB table, you need to know:
  - An LSDB stores LSAs generated by a router itself and received from neighbors. In this example, the LSDB of R1 contains three LSAs.
  - The **Type** field indicates an LSA type, and the **AdvRouter** field indicates the router that sends the LSA.
  - Run the **display ospf lsdb** command to query the LSDB.

[R1]display ospf lsdb



<R1> display ospf lsdb

OSPF Process 1 with Router ID 1.1.1.1

Link State Database

Router ID: 0.0.0.0

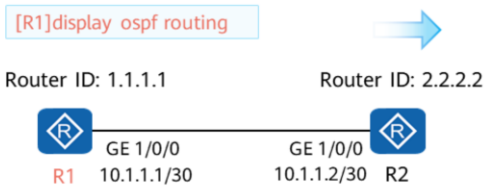
Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
Router	2.2.2.2	2.2.2.2	98	36	8000000B	1
Router	1.1.1.1	1.1.1.1	92	36	80000005	1
Network	10.1.1.2	2.2.2.2	98	32	80000004	0

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- For more information about LSAs, see information provided in HCIP-Datacom courses.

Three Types of OSPF Entries - Entries in the OSPF Routing Table

- For the OSPF routing table, you need to know:
  - The OSPF routing table and the router routing table are different. In this example, the OSPF routing table contains three routes.
  - An OSPF routing table contains information, such as the destination IP address, cost, and next-hop IP address, which guides packet forwarding.
  - Run the **display ospf routing** command to query the OSPF routing table.




```
<R1> display ospf routing
OSPF Process 1 with Router ID 1.1.1.1
Routing tables
Routing for Network
Destination        Cost  Type      NextHop         AdvRouter       Area
1.1.1.1/32         0     stub      1.1.1.1         1.1.1.1         0.0.0.0
10.1.1.0/20        1     Transit   10.1.1.1        1.1.1.1         0.0.0.0
2.2.2.2/32         1     stub      10.1.1.2        2.2.2.2         0.0.0.0

Total Nets: 3
Intra Area: 3  Inter Area: 0  ASE: 0  NSSA: 0
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- For more information about the OSPF routing table, see information provided in HCIP-Datacom courses.

Contents

1. OSPF Overview
2. **OSPF Working Mechanism**
3. Typical OSPF Configuration

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

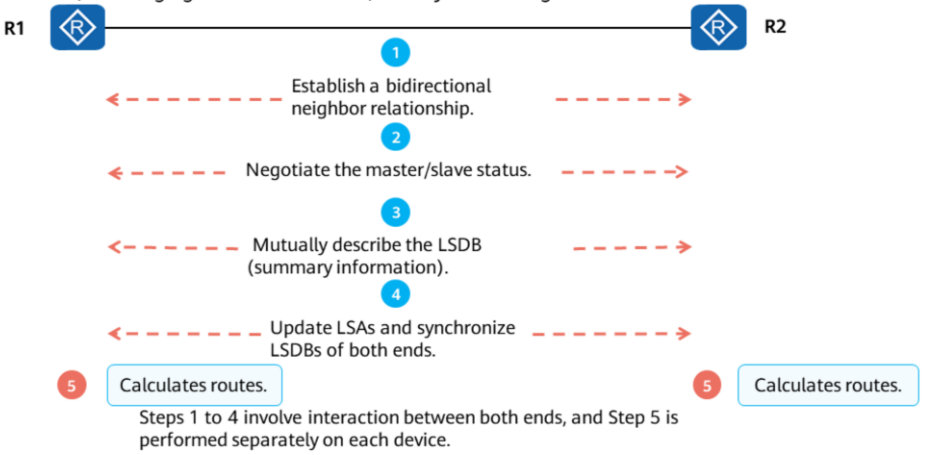
Relationships Between OSPF Routers

- There are two important concepts about the relationship between OSPF routers: neighbor relationship and adjacency.
- On a simple network, two routers are directly connected. OSPF is enabled on interconnected interfaces. The routers start to send and listen to Hello packets. After the two routers discover each other through Hello packets, they establish a neighbor relationship.
- The establishment of a neighbor relationship is just the beginning. A series of packets, such as DD, LSR, LSU, and LSAck packets, will be exchanged later. When LSDB synchronization between two routers is complete and the two routers start to calculate routes independently, the two routers establish an adjacency.

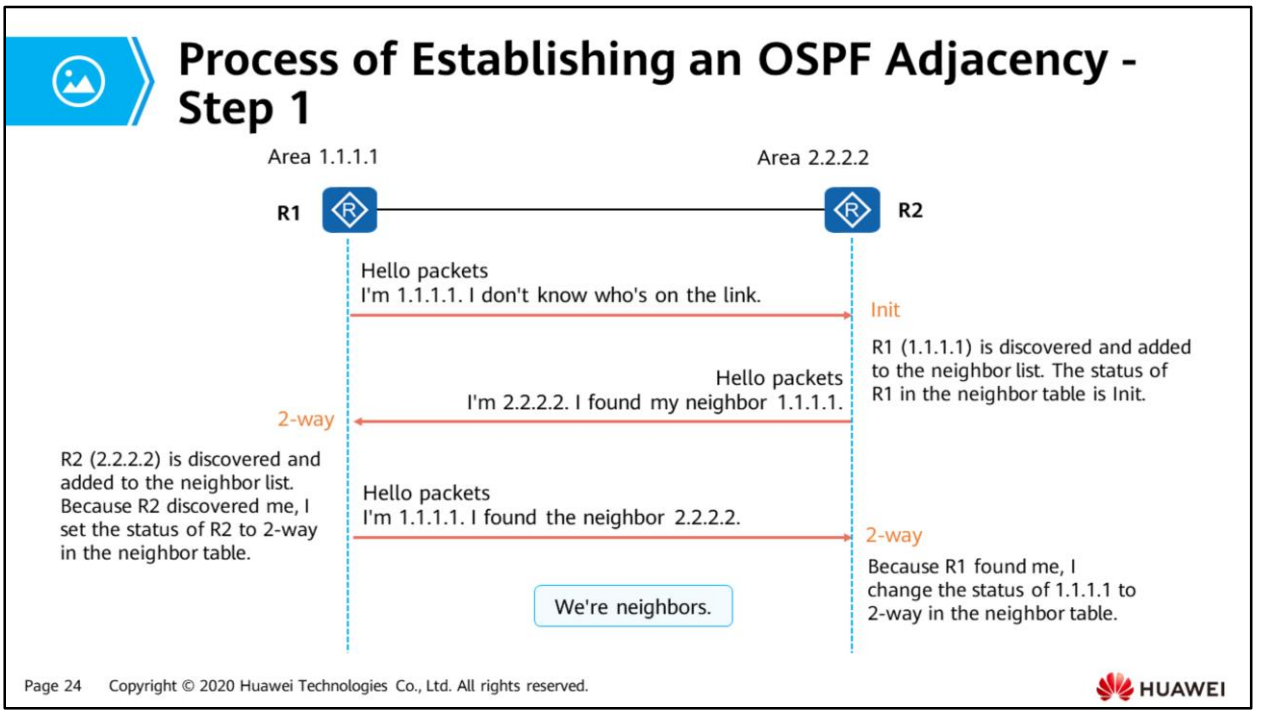
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Process of Establishing an OSPF Adjacency Relationship

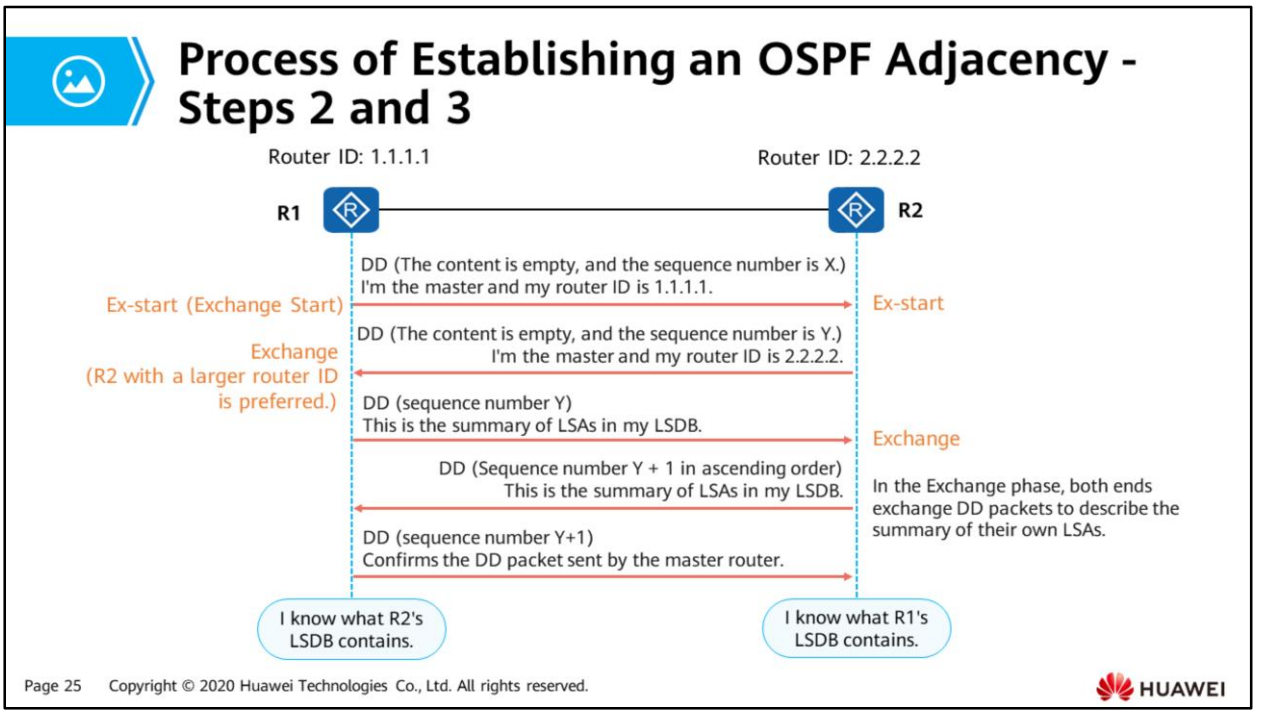
- OSPF adjacency relationship establishment involves four steps: establishing a neighbor relationship, negotiating the master/slave status, exchanging LSDB information, and synchronizing LSDBs.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

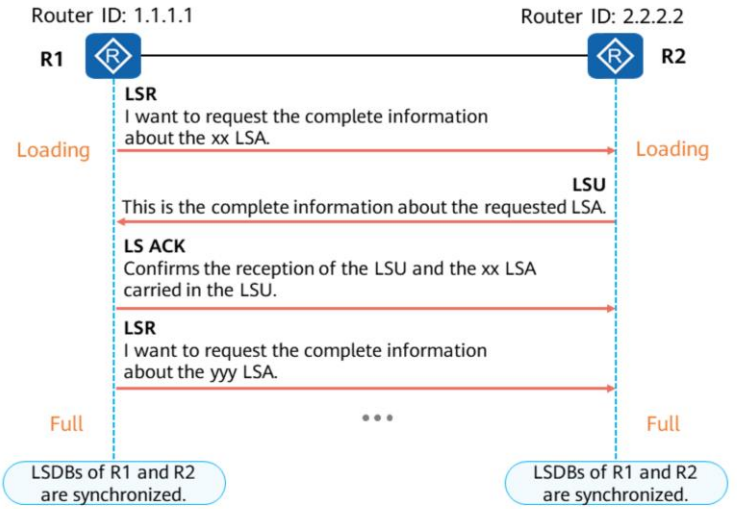


- When an OSPF router receives the first Hello packet from another router, the OSPF router changes from the Down state to the Init state.
- When an OSPF router receives a Hello packet in which the neighbor field contains its router ID, the OSPF router changes from the Init state to the 2-way state.



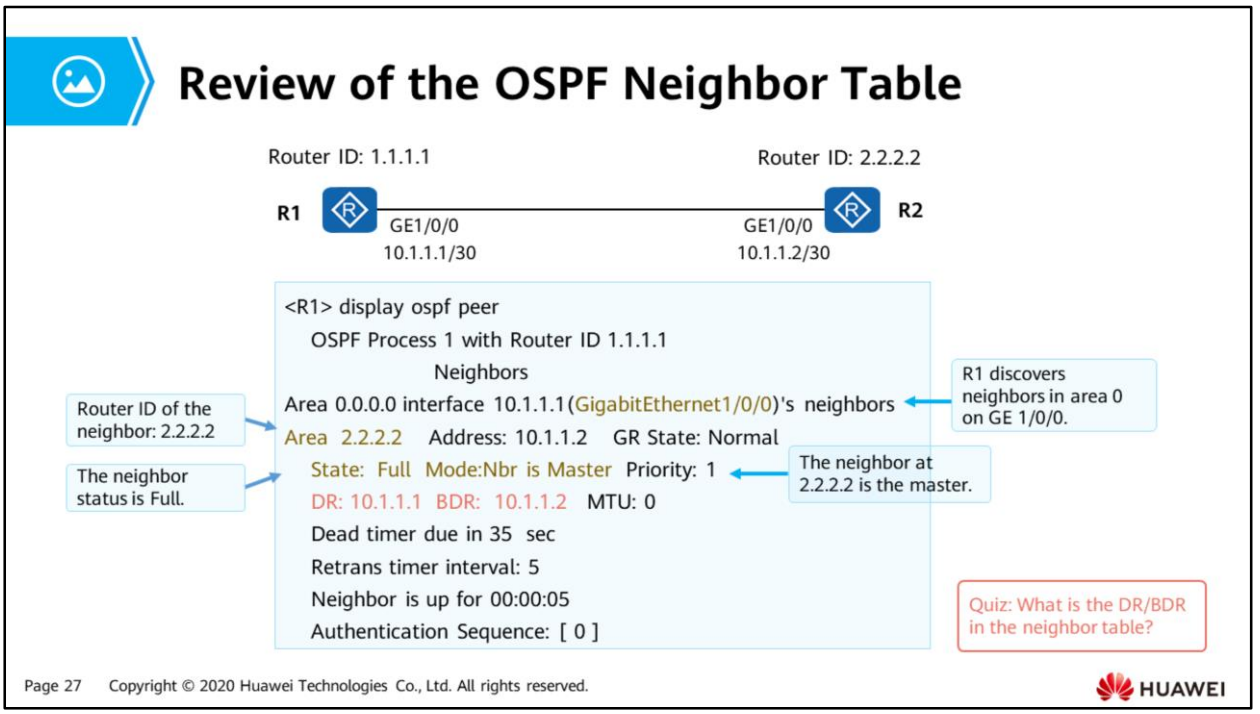
- After the neighbor state machine changes from 2-way to Exstart, the master/slave election starts.
    - The first DD packet sent from R1 to R2 is empty, and its sequence number is assumed to be X.
    - R2 also sends the first DD packet to R1. In the examples provided in this presentation, the sequence number of the first DD packet is Y.
    - The master/slave relationship is selected based on the router ID. A larger router ID indicates a higher priority. The router ID of R2 is greater than that of R1. Therefore, R2 becomes the master device. After the master/slave role negotiation is complete, R1's status changes from Exstart to Exchange.
- After the neighbor status of R1 changes to Exchange, R1 sends a new DD packet containing its own LSDB description. The sequence number of the DD packet is the same as that of R2. After R2 receives the packet, the neighbor status changes from Exstart to Exchange.
- R2 sends a new DD packet to R1. The DD packet contains the description of its own LSDB and the sequence number of the DD packet is Y + 1.
- As a backup router, R1 needs to acknowledge each DD packet sent by R2. The sequence number of the response packet is the same as that of the DD packet sent by R2.
- After sending the last DD packet, R1 changes the neighbor status to Loading.

Process of Establishing an OSPF Adjacency - Step 4



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

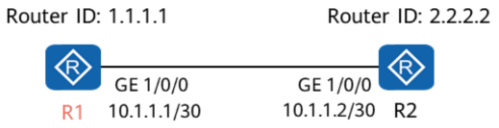
- After the neighbor status changes to Loading, R1 sends an LSR to R2 to request the LSAs that are discovered through DD packets in the Exchange state but do not exist in the local LSDB.
- After receiving the LSU, R2 sends an LSU to R1. The LSU contains detailed information about the requested LSAs.
- After R1 receives the LSU, R1 replies with an LSAck to R2.
- During this process, R2 also sends an LSA request to R1. When the LSDBs on both ends are the same, the neighbor status changes to Full, indicating that the adjacency has been established successfully.



- Fields displayed in the **display ospf peer** command output are as follows:
  - OSPF Process 1 with Router ID 1.1.1.1: The local OSPF process ID is 1, and the local OSPF router ID is 1.1.1.1.
  - Area ID of the neighboring OSPF router.
  - Address: address of the neighbor interface.
  - GR State: GR status after OSPF GR is enabled. GR is an optimized function. The default value is Normal.
  - State: neighbor status. In normal cases, after LSDB synchronization is complete, the neighbor stably stays in the Full state.
  - Mode: whether the local device is the master or backup device during link status information exchange.
  - Priority: priority of the neighboring router. The priority is used for DR election.
  - DR: designated router.
  - BDR: backup designated router.
  - MTU: MTU of a neighbor interface.
  - Retrans timer interval: interval (in seconds) at which LSAs are retransmitted.
  - Authentication Sequence: authentication sequence number.

OSPF Network Types

- Before learning concepts of the DR and BDR, understand OSPF network types.
- The OSPF network type is a very important interface variable. This variable affects OSPF operations on interfaces. For example, it determines how to send OSPF packets and whether to elect a DR or BDR.
- The default OSPF network type of an interface depends on the data link layer encapsulation used by the interface.
- As shown in the figure, OSPF has four network types: broadcast, NBMA, P2MP, and P2P.



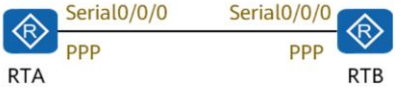

```
[R1-GigabitEthernet1/0/0] ospf network-type ?
  broadcast  Specify OSPF broadcast network
  nbma       Specify OSPF NBMA network
  p2mp       Specify OSPF point-to-multipoint network
  p2p        Specify OSPF point-to-point network
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

OSPF Network Types (1)

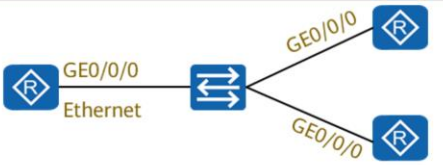
- Generally, the network types of OSPF interfaces at both ends of a link must be the same. Otherwise, the two interfaces cannot establish a neighbor relationship.
- An OSPF network type can be manually changed on an interface to adapt to different network scenarios. For example, you can change the BMA network type to P2P.

Point-to-Point (P2P)



- P2P indicates that only two network devices can be connected on a link.
- A typical example is a PPP link. When an interface uses PPP encapsulation, the default network type of the OSPF interface is P2P.

Broadcast Multiple Access (BMA)



- BMA is also called broadcast. It refers to an environment that allows multiple devices to access and supports broadcast.
- A typical example is an Ethernet network. When an interface uses Ethernet encapsulation, the default network type of the OSPF interface is BMA.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

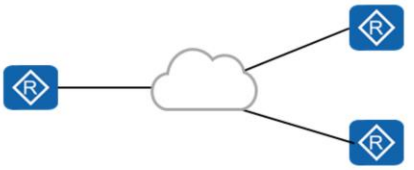
OSPF Network Types (2)

Non-Broadcast Multiple Access (NBMA)



- NBMA refers to an environment that allows multiple network devices to access but does not support broadcast.
- A typical example is a Frame Relay (FR) network.

Point-to-Multipoint (P2MP)

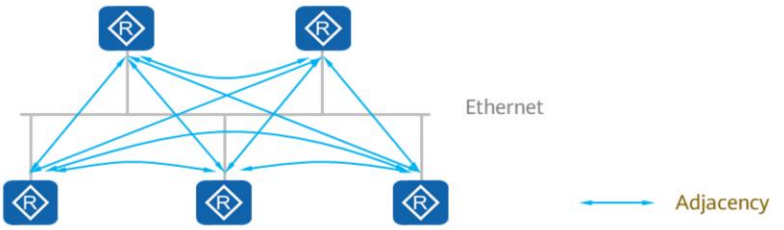


- A P2MP network is formed by bundling endpoints of multiple P2P links.
- No link layer protocol is considered as a P2MP network by default. This type must be manually changed from another network type.
- For example, a non-full-mesh NBMA network can be changed to a P2MP network.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Background of DR and BDR

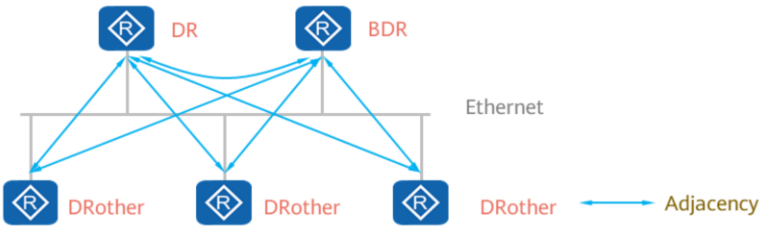
- Multi-access (MA) networks are classified into BMA and NBMA networks. Ethernet is a typical broadcast multi-access network.
- On an MA network, if each OSPF router establishes OSPF adjacencies with all the other routers, excessive OSPF adjacencies exist on the network, which increases the load on the devices and the number of OSPF packets flooded on the network.
- Once the network topology changes, LSA flooding on the network may waste bandwidth and device resources.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

DR and BDR

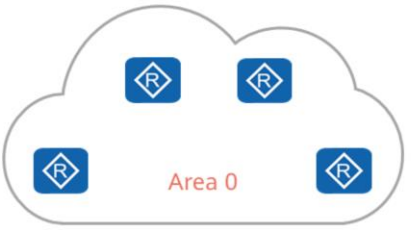
- To optimize OSPF neighbor relationships on an MA network, the OSPF protocol specifies three types of OSPF routers: DR, BDR, and DRother.
- Only the DR and BDR can establish adjacencies with other OSPF routers. DRothers do not establish OSPF adjacencies with one another, and their relationship is in the 2-way state.
- The BDR monitors the status of the DR and takes over the role of the DR if the existing DR fails.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Election rule: The interface with a higher OSPF DR priority becomes the DR of the MA. If the priorities (default value of 1) are the same, the router (interface) with a higher OSPF router ID is elected as the DR, and the DR is non-preemption.

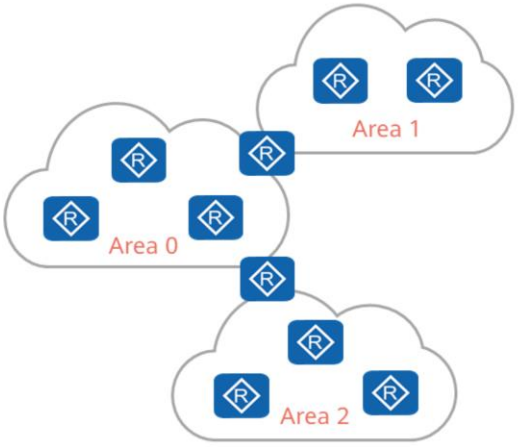
OSPF Domain and Single Area



- An OSPF domain is a network that consists of a series of contiguous OSPF network devices that use the same policy.
- An OSPF router floods LSAs in the same area. To ensure that all routers have the same understanding of the network topology, LSDBs need to be synchronized within an area.
- If there is only one OSPF area, the number of OSPF routers increases with the network scale. This causes the following problems:
  - The LSDB becomes larger and larger, and the size of the OSPF routing table increases. A large number of router resources are consumed, device performance deteriorates, and data forwarding is affected.
  - It is difficult to calculate routes based on a large LSDB.
  - When the network topology changes, LSA flooding and SPF recalculation on the entire network bring heavy loads.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Multi-Area OSPF



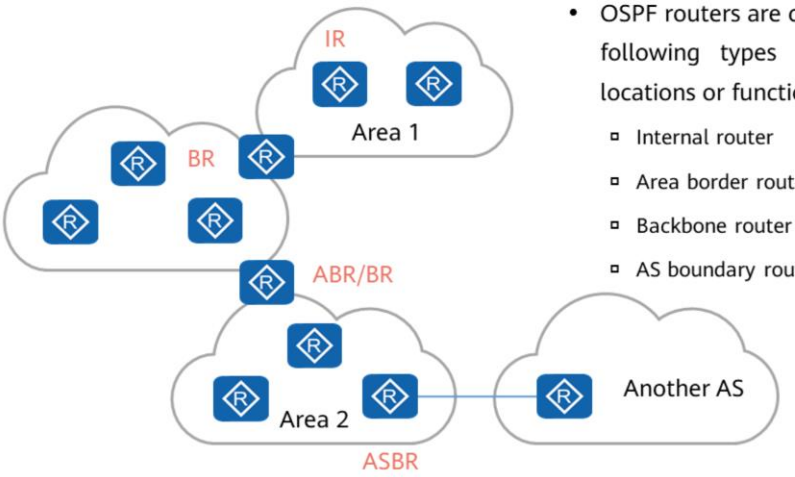
- OSPF introduces the concept of area. An OSPF domain is divided into multiple areas to support larger-scale networking.
- The OSPF multi-area design reduces the flooding scope of LSAs and effectively controls the impact of topology changes within an area, optimizing the network.
- Routes can be summarized at the area border to reduce the size of the routing table.
- Multi-area improves network scalability and facilitates large-scale network construction.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Types of areas: Areas can be classified into backbone areas and non-backbone areas. Area 0 is a backbone area. All areas except area 0 are called non-backbone areas.
- Multi-area interconnection: To prevent inter-area loops, non-backbone areas cannot be directly connected to each other. All non-backbone areas must be connected to a backbone area.

Types of OSPF Routers



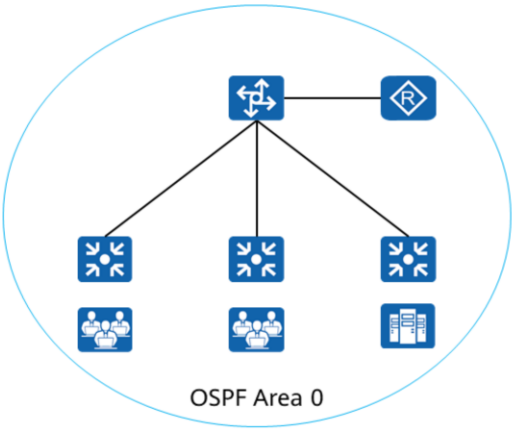
- OSPF routers are classified into the following types based on their locations or functions:
  - Internal router
  - Area border router (ABR)
  - Backbone router
  - AS boundary router (ASBR)

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

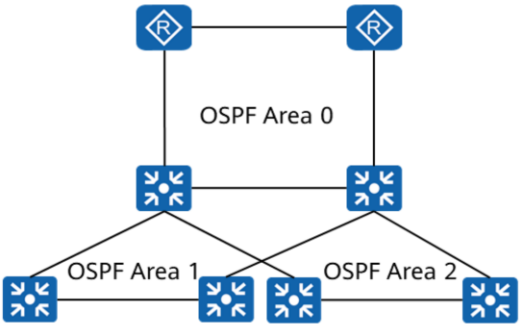
HUAWEI

- Internal router: All interfaces of an internal router belong to the same OSPF area.
- ABR: An interface of an ABR belongs to two or more areas, but at least one interface belongs to the backbone area.
- Backbone router: At least one interface of a backbone router belongs to the backbone area.
- ASBR: exchanges routing information with other ASs. If an OSPF router imports external routes, the router is an ASBR.

Typical OSPF Single-Area and Multi-Area Networking



Small- and medium-sized enterprise network (single area)



Large enterprise network (multiple areas)

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

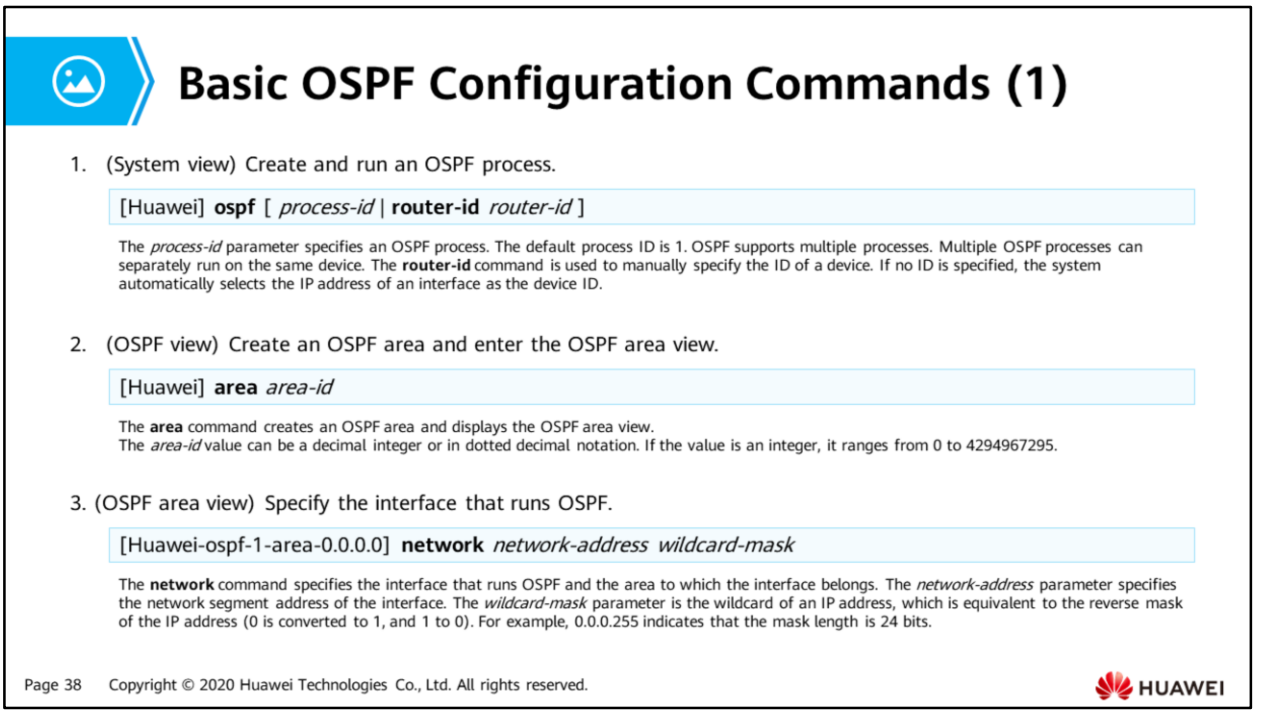
- Small- and medium-sized enterprise networks have a small scale and a limited number of routing devices. All devices can be deployed in the same OSPF area.
- A large-scale enterprise network has a large number of routing devices and is hierarchical. Therefore, OSPF multi-area deployment is recommended.

Contents

1. OSPF Overview
2. OSPF Working Mechanism
3. **Typical OSPF Configuration**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI



- A router ID is selected in the following order: The largest IP address among Loopback addresses is preferentially selected as a router ID. If no Loopback interface is configured, the largest IP address among interface addresses is selected as a router ID.

Basic OSPF Configuration Commands (2)

4. (Interface view) Set an OSPF interface cost.

```
[Huawei-GE1/0/1] ospf cost cost
```

The **ospf cost** command sets a cost for an OSPF interface. By default, OSPF automatically calculates the cost of an interface based on the interface bandwidth. The cost value is an integer ranging from 1 to 65535.

5. (OSPF view) Set an OSPF bandwidth reference value.

```
[Huawei-ospf-1] bandwidth-reference value
```

The **bandwidth-reference** command sets a bandwidth reference value that is used to calculate interface costs. The value ranges from 1 to 2147483648, in Mbit/s. The default value is 100 Mbit/s.

6. (Interface view) Set the priority of an interface for DR election.

```
[Huawei-GigabitEthernet0/0/0] ospf dr-priority priority
```

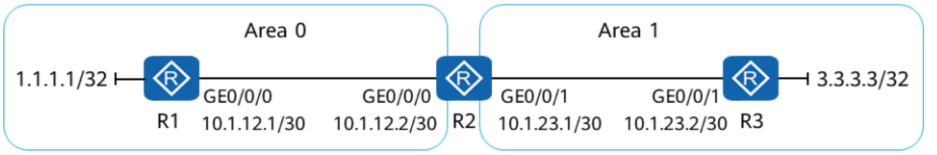
The **ospf dr-priority** command sets a priority for an interface that participates in DR election. A larger value indicates a higher priority. The value ranges from 0 to 255.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

OSPF Configuration Example

Description:

- There are three routers, R1, R2, and R3. R1 and R3 are connected to networks 1.1.1.1/32 and 3.3.3.3/32 (simulated by Loopback 0), respectively. OSPF needs to be used to implement interworking between the two networks. Detailed topology was as follows:

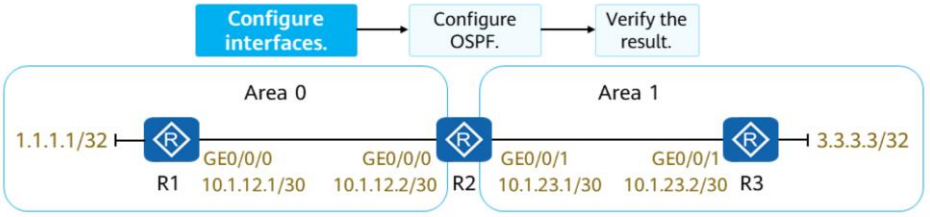




- The configuration process consists of three steps: configuring device interfaces, configuring OSPF, and verifying the result.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

OSPF Configuration Example - Configuring Interfaces



- Set IP addresses for R1's, R2's, and R3's interfaces according to the plan.

```
# Configure interfaces of R1.
[R1] interface LoopBack 0
[R1-LoopBack0] ip address 1.1.1.1 32
[R1-LoopBack0] interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0] ip address 10.1.12.1 30
```

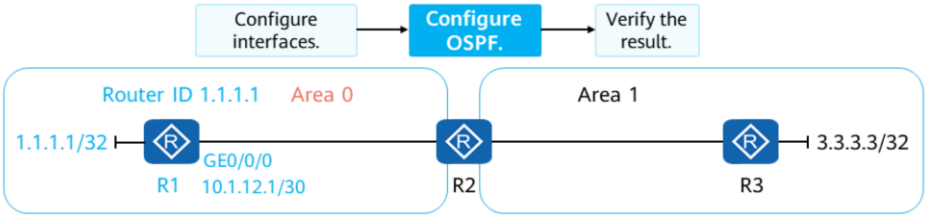
```
# Configure interfaces of R3.
[R3] interface LoopBack 0
[R3-LoopBack0] ip address 3.3.3.3 32
[R3-LoopBack0] interface GigabitEthernet 0/0/1
[R3-GigabitEthernet0/0/1] ip address 10.1.23.2 30
```

Assign IP addresses for GE0/0/0 and GE0/0/1 on R2. For details, see comment in this slide.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Configure interfaces of R2.
  - [R2] interface GigabitEthernet 0/0/0
    [R2-GigabitEthernet0/0/0] ip address 10.1.12.2 30
    [R2-GigabitEthernet0/0/0] interface GigabitEthernet 0/0/1
    [R2-GigabitEthernet0/0/1] ip address 10.1.23.1 30

OSPF Configuration Example - Configuring OSPF (1)



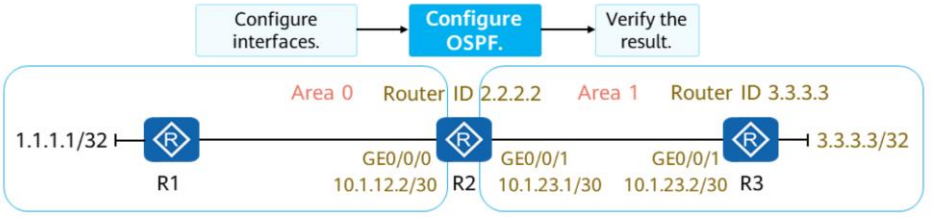
- Planned OSPF parameters: The OSPF process ID is 1. Router IDs of R1, R2, and R3 are 1.1.1.1, 2.2.2.2, and 3.3.3.3 respectively.
- Procedure:
  - Create and run an OSPF process.
  - Create an OSPF area and enter the OSPF area view.
  - Specify the interface that runs OSPF..

```
# Configure OSPF on R1.
[R1] ospf 1 router-id 1.1.1.1
[R1-ospf-1] area 0
[R1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[R1-ospf-1-area-0.0.0.0] network 10.1.12.0 0.0.0.3
```

An inverse mask is specified here.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

OSPF Configuration Example - Configuring OSPF (2)



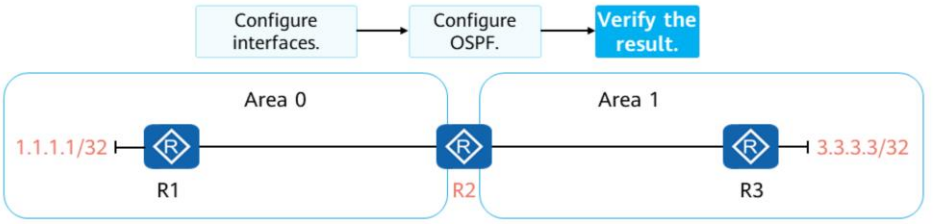
- When configuring OSPF multi-area, be sure to advertise the route destined for a network segment that responds to a specified area.

```
# Configure OSPF on R2.
[R2] ospf 1 router-id 2.2.2.2
[R2-ospf-1] area 0
[R2-ospf-1-area-0.0.0.0] network 10.1.12.0 0.0.0.3
[R2-ospf-1-area-0.0.0.0] area 1
[R2-ospf-1-area-0.0.0.1] network 10.1.23.0 0.0.0.3
```

```
# Configure OSPF on R3.
[R3] ospf 1 router-id 3.3.3.3
[R3-ospf-1] area 1
[R3-ospf-1-area-0.0.0.1] network 3.3.3.3 0.0.0.0
[R3-ospf-1-area-0.0.0.1] network 10.1.23.0 0.0.0.3
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

OSPF Configuration Example - Verification (1)



- Check the OSPF neighbor table on R2.

```
<R2> display ospf peer brief
        OSPF Process 1 with Router ID 2.2.2.2
                Peer Statistic Information
 ----------------------------------------------------------------------------
 Area Id          Interface                     Neighbor id      State
 0.0.0.0          GigabitEthernet0/0/0          1.1.1.1          Full
 0.0.0.1          GigabitEthernet0/0/1          3.3.3.3          Full
 ----------------------------------------------------------------------------
```

Area ID of a neighbor

Neighbor status
Verify that the neighbor status is Full, indicating that the adjacency has been established successfully.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

OSPF Configuration Example - Verification (2)

- Check the routing table on R1 and ping 3.3.3.3 from 1.1.1.1.

Route to 3.3.3.3/32 learned using OSPF

Set the source IP address to 1.1.1.1 and ping 3.3.3.3.

```
<R1>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing tables: Public
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        3.3.3.3/32  OSPF    10   2           D   10.1.12.2       GigabitEthernet 0/0/0
       10.1.12.0/30 Direct  0    0           D   10.1.12.1       GigabitEthernet 0/0/0

...
<R1>ping -a 1.1.1.1 3.3.3.3
  PING 3.3.3.3: 56  data bytes, press CTRL_C to break
    Reply from 3.3.3.3: bytes = 56 Sequence = 1 ttl = 254 time = 50 ms
...
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Quiz

1. (Multiple) In the process of establishing OSPF neighbor relationships and adjacencies, which of the following states are stable? ( )
   A. Exstart
   B. Two-way
   C. Exchange
   D. Full
2. (Multiple) In which of the following situation will the establishment of adjacencies between routers be triggered? ( )
   A. Two routers on a point-to-point link
   B. DR and BDR on a broadcast network
   C. DRother and DRother on an NBMA network
   D. BDR and DRother on a broadcast network

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

1. BD
2. ABD

Summary

- OSPF is a widely used routing protocol on the live network. This presentation describes basic concepts, application scenarios, and basic configurations of OSPF.
- The router ID, area, OSPF neighbor table, LSDB table, and OSPF routing table are basic OSPF concepts. Describe the establishment of OSPF neighbor relationships and adjacencies, which helps you better understand the link-state routing protocol.
- OSPF has more interesting details, such as LSA types, the SPF calculation process, and the OSPF special area. For more OSPF information, please continue your Huawei HCIP-Datacom certification courses.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Ethernet Switching Basics

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- Data transmission on networks must comply with certain standards. Ethernet protocols define how data frames are transmitted over an Ethernet network. Understanding Ethernet protocols is the basis for fully understanding communication at the data link layer. An Ethernet switch is the main device for implementing data link layer communication. It is essential to understand how an Ethernet switch works.
- This course describes the concepts related to Ethernet protocols, MAC address types, and working process and mechanism of Layer 2 switches.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Describe the basic concepts of an Ethernet network.
  - Distinguish MAC address types.
  - Get familiar with the working process of a Layer 2 switch.
  - Get familiar with the structure and generation process of a MAC address table.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

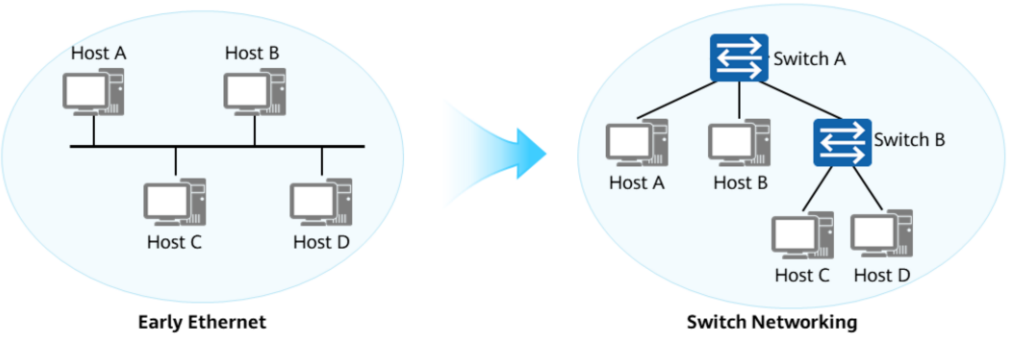
1. **Overview of Ethernet Protocols**
2. Overview of Ethernet Frames
3. Overview of Ethernet Switches
4. Process of Data Communication Within a Network Segment

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Ethernet Protocols

- Ethernet is the most common communication protocol standard used by existing local area networks (LANs). It defines the cable types and signal processing methods that are used on a LAN.
- An Ethernet network is a broadcast network built based on the carrier sense multiple access/collision detection (CSMA/CD) mechanism.

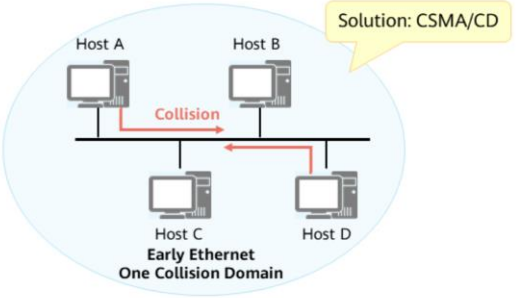


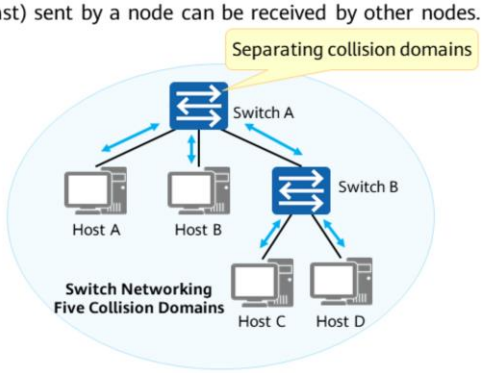
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Early Ethernet:
  - Ethernet networks are broadcast networks established based on the CSMA/CD mechanism. Collisions restrict Ethernet performance. Early Ethernet devices such as hubs work at the physical layer, and cannot confine collisions to a particular scope. This restricts network performance improvement.
- Switch networking:
  - Working at the data link layer, switches are able to confine collisions to a particular scope. Switches help improve Ethernet performance and have replaced hubs as mainstream Ethernet devices. However, switches do not restrict broadcast traffic on the Ethernet. This affects Ethernet performance.

Collision Domain

- A collision domain is a set of nodes connected to the same shared medium. All nodes in a collision domain compete for the same bandwidth. Packets (unicast, multicast, or broadcast) sent by a node can be received by other nodes.





- On a traditional Ethernet network, multiple nodes on the same medium share the link bandwidth and compete for the right to use the link. As a result, collision occurs.
- The probability that collision occurs increases when more nodes are deployed on a shared medium.

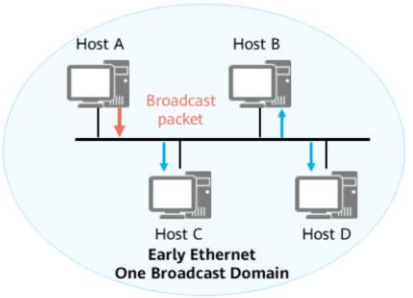
The switch interfaces used to send and receive data are independent of each other and belong to different collision domains. Therefore, collisions do not occur between hosts (or networks) connected through switch interfaces.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

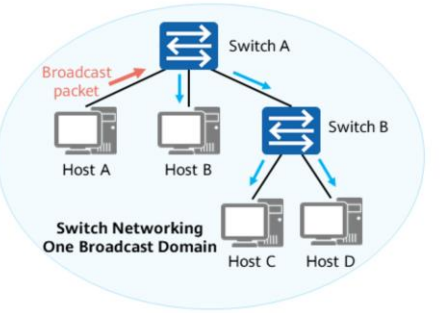
- On a shared network, the Ethernet uses the CSMA/CD technology to avoid collisions. The CSMA/CD process is as follows:
  - A terminal continuously detects whether the shared line is idle.
    - If the line is idle, the terminal sends data.
    - If the line is in use, the terminal waits until the line becomes idle.
  - If two terminals send data at the same time, a collision occurs on the line, and signals on the line become unstable.
  - After detecting the instability, the terminal immediately stops sending data.
  - The terminal sends a series of disturbing pulses. After a period of time, the terminal resumes the data transmission. The terminal sends disturbing pulses to inform other terminals, especially the terminal that sends data at the same time, that a collision occurred on the line.
- The working principle of CSMA/CD can be summarized as follows: listen before send, listen while sending, stop sending due to collision, and resend after random delay.

Broadcast Domain

- The entire access scope of broadcast packets is called a Layer 2 broadcast domain, which is also called a broadcast domain. All hosts in the same broadcast domain can receive broadcast packets.



On a traditional Ethernet network, multiple nodes on the same medium share a link. The broadcast packets sent by a device can be received by all the other devices.



A switch forwards broadcast packets to all interfaces. Therefore, the nodes connected to all interfaces of the switch belong to the same broadcast domain.

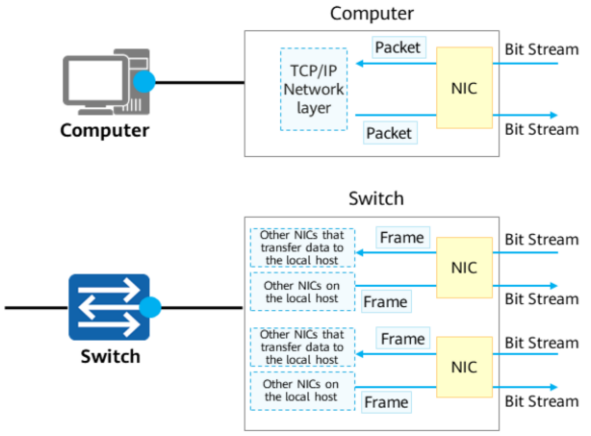
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- An all-1 MAC address (FF-FF-FF-FF-FF-FF) is a broadcast address. All nodes process data frames with the destination address being a broadcast address. The entire access range of the data frames is called a Layer 2 broadcast domain, which is also called a broadcast domain.

- Note that a MAC address uniquely identifies a network interface card (NIC). Each network adapter requires a unique MAC address.

Ethernet NIC

- A network interface card (NIC) is a key component that connects a network device (such as a computer, a switch, or a router) to an external network.



- **Network Port**
  - A network port is also called a network interface, interface, or port.
- **NIC**
  - Each network port corresponds to a NIC.
  - A computer or switch forwards data through a NIC.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- There are many types of NICs. In this document, all the NICs mentioned are Ethernet NICs.
- The switches mentioned in this document are Ethernet switches. The NICs used by each network port on a switch are Ethernet NICs.

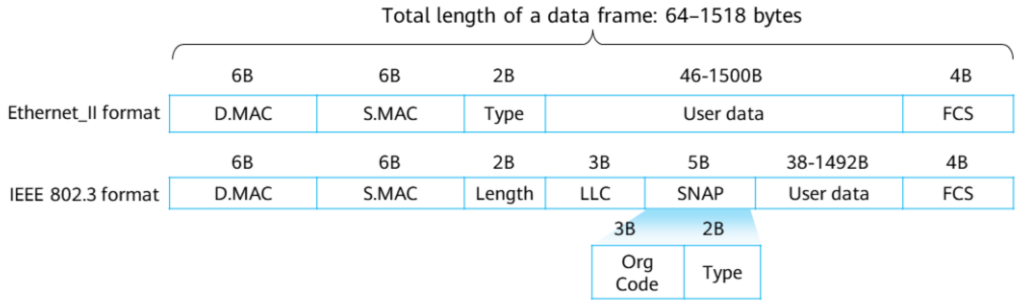
Contents

1. Overview of Ethernet Protocols
2. **Overview of Ethernet Frames**
3. Overview of Ethernet Switches
4. Process of Data Communication Within a Network Segment

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Ethernet Frame Format

- The frames used by Ethernet technology are referred to as Ethernet frames.
- Ethernet frames are in two formats: Ethernet_II and IEEE 802.3.



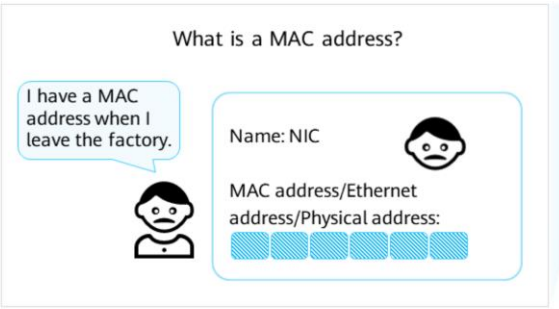
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Frame is the unit of data that is transmitted between network nodes on an Ethernet network. Ethernet frames are in two formats, namely, Ethernet_II and IEEE 802.3, as illustrated in the figure shown in this slide.
- Ethernet II frame:
  - DMAC: 6 bytes, destination MAC address. This field identifies which MAC address should receive the frame.
  - SMAC: 6 bytes, source MAC address. This field identifies which MAC address should send the frame.
  - Type: 2 bytes, protocol type. Common values are as follows:
    - 0x0800: Internet Protocol Version 4 (IPv4)
    - 0x0806: Address Resolution Protocol (ARP)
- IEEE 802.3 LLC Ethernet frame:
  - Logical link control (LLC) consists of the destination service access point (DSAP), source service access point (SSAP), and Control field.
    - DSAP: 1 byte, destination service access point. If the subsequent type is IP, the value is set to 0x06. The function of a service access point is similar to the Type field in an Ethernet II frame or the port number in TCP/UDP.
    - SSAP: 1 byte, source service access point. If the subsequent type is IP, the value is set to 0x06.
    - Ctrl: 1 byte. This field is usually set to 0x03, indicating unnumbered IEEE 802.2 information of a connectionless service.

    - The Subnetwork Access Protocol (SNAP) field consists of the Org Code field and the Type field.
        - The three bytes of the Org Code field are all 0s.
        - The Type field functions the same as that in Ethernet_II frames.
- The total length of a data frame ranges from 64 bytes to 1518 bytes. What is the reason for this design? (In addition, the MTU of an Ethernet interface is 1500 bytes.)
    - On an Ethernet network, the minimum frame length is 64 bytes, which is determined jointly by the maximum transmission distance and the CSMA/CD mechanism.
        - The use of minimum frame length can prevent the following situation: station A finishes sending the last bit, but the first bit does not arrive at station B, which is far from station A. Station B considers that the line is idle and begins to send data, leading to a collision.
        - An upper-layer protocol must ensure that the Data field contains at least 46 bytes. In this way, the 14-byte Ethernet frame header and 4-byte check code at the frame tail can meet the minimum frame length of 64 bytes. If the actual data is less than 46 bytes, the upper-layer protocol must fill in certain data units.
    - To achieve a tradeoff between transmission efficiency and transmission reliability, the maximum length of an Ethernet frame is 1518 bytes, and the corresponding IP data packet is 1500 bytes.
        - A large frame length improves the data transmission efficiency. However, if the data frame is too long, the transmission over the shared link takes a long time, which greatly affects delay-sensitive applications.
        - As such, a compromise data frame length of 1518 bytes is used, which corresponds to an IP data packet length of 1500 bytes. This is where the concept of MTU comes from.

What Is a MAC Address?

- A media access control (MAC) address uniquely identifies a NIC on a network. Each NIC must have a globally unique MAC address.



MAC Address

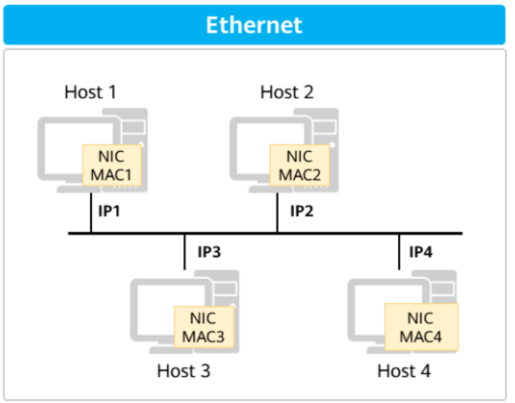
Each NIC has a number, that is, a MAC address, to identify itself, just as each person has an ID card number to identify himself/herself.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A MAC address, as defined and standardized in IEEE 802, indicates the position of a network device. All Ethernet NICs that comply with the IEEE 802 standard must have a MAC address. The MAC address varies according to the NIC.

IP Address Vs. MAC Address

- Each Ethernet device has a unique MAC address before delivery. When the device accesses the network, it assigns an IP address to each host. Why?



Characteristics of IP addresses:
- IP addresses are unique.
- IP addresses are changeable.
- IP addresses are assigned based on network topology.

Characteristics of MAC addresses:
- MAC addresses are unique.
- MAC addresses cannot be changed.
- MAC addresses are assigned based on the manufacturer.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Each Ethernet device has a unique MAC address before delivery. Then, why is an IP address assigned to each host? In other words, if each host is assigned a unique IP address, why does a unique MAC address need to be embedded in a network device (such as a NIC) during production?
- The main causes are as follows:
  - IP addresses are assigned based on the network topology, and MAC addresses are assigned based on the manufacturer. If route selection is based on the manufacturer, this solution is not feasible.
  - When two-layer addressing is used, devices are more flexible and easy to maintain.
    - For example, if an Ethernet NIC is faulty, you can replace it without changing its IP address. If an IP host is moved from one network to another, a new IP address can be assigned to the IP host with no need for replacing the NIC with a new one.
- Conclusion:
  - An IP address uniquely identifies a network node. Data on different network segments can be accessed using IP addresses.
  - A MAC address uniquely identifies a NIC. Data on a single network segment can be accessed using MAC addresses.

MAC Address Presentation

- A MAC address is 48 bits (6 bytes) in length.
- As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator.

For example, 00-1E-10-DD-DD-02 or 001E-10DD-DD02

Hexadecimal	00	1E	10	DD	DD	02	6-byte
Binary	0000 0000	0001 1110	0001 0000	1101 1101	1101 1101	0000 0010	48-bit

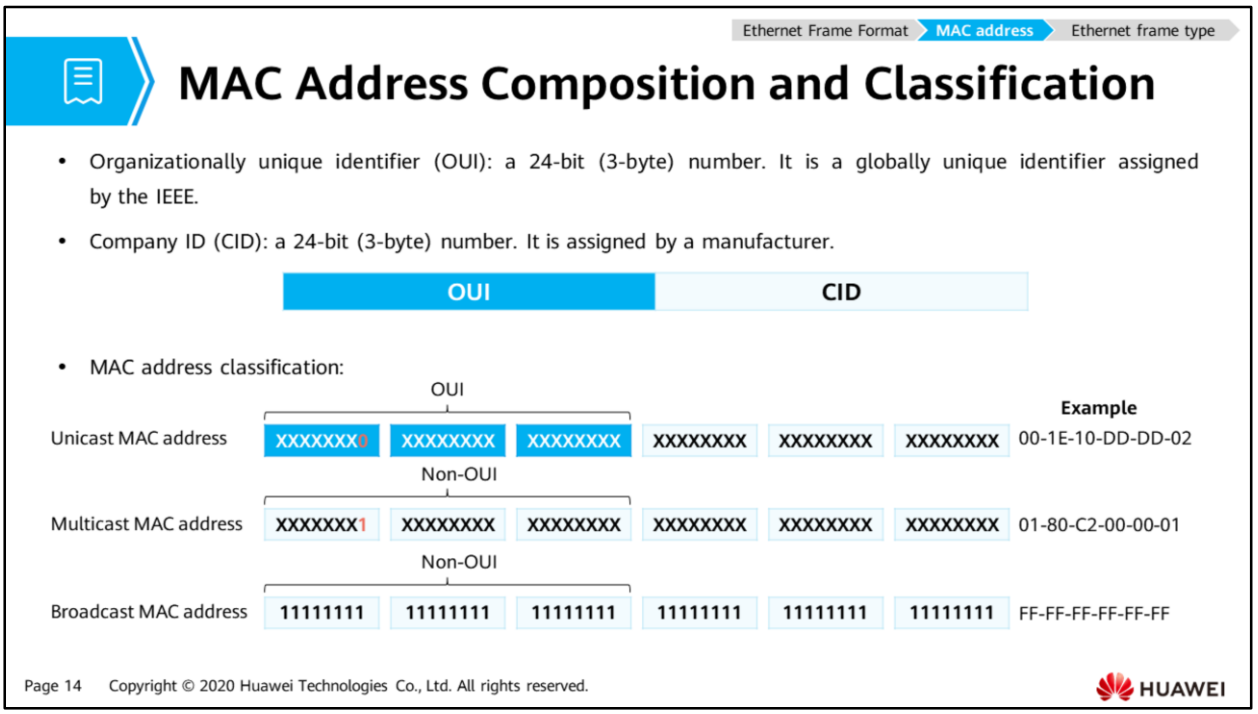
Conversion between hexadecimal and binary digits

Power	2^3	2^2	2^1	2^0	2^3	2^2	2^1	2^0
	8	4	2	1	8	4	2	1
Bit	0	0	0	1	1	1	1	0
	= 1				= 8+4+2=14=E			

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- A MAC Address, which is 48 bits (6 bytes) in length, is a 12-digit hexadecimal number.

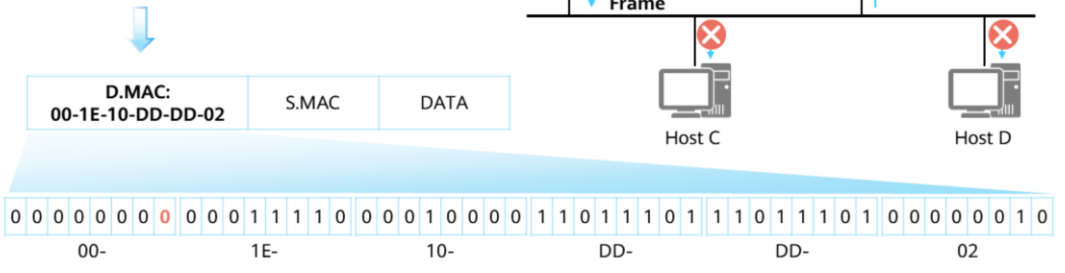


- A manufacturer must register with the IEEE to obtain a 24-bit (3-byte) vendor code, which is also called OUI, before producing a NIC.
- The last 24 bits are assigned by a vendor and uniquely identify a NIC produced by the vendor.
- MAC addresses fall into the following types:
  - Unicast MAC address: is also called the physical MAC address. A unicast MAC address uniquely identifies a terminal on an Ethernet network and is a globally unique hardware address.
    - A unicast MAC address identifies a single node on a link.
    - A frame whose destination MAC address is a unicast MAC address is sent to a single node.
    - A unicast MAC address can be used as either the source or destination address.
    - Note that unicast MAC addresses are globally unique. When two terminals with the same MAC address are connected to a Layer 2 network (for example, due to incorrect operations), a communication failure occurs (for example, the two terminals fail to communicate with each other). The communication between the two terminals and other devices may also fail.

- Broadcast MAC address: an all-1 MAC address (FF-FF-FF-FF-FF-FF), which indicates all terminals on a LAN.
  - A broadcast MAC address can be considered as a special multicast MAC address.
  - The format of a broadcast MAC address is FFFF-FFFF-FFFF.
  - The frame whose destination MAC address is a broadcast MAC address is sent to all nodes on a link.
- Multicast MAC address: indicates a group of terminals on a LAN. Except for broadcast MAC addresses, all the MAC addresses with the eighth bit as 1 are multicast MAC addresses (for example, 01-00-00-00-00-00).
  - A multicast MAC address identifies a group of nodes on a link.
  - A frame whose destination MAC address is a multicast MAC address is sent to a group of nodes.
  - A multicast MAC address can only be used as the destination address but not the source address.

Unicast Ethernet Frame

- A unicast Ethernet frame is also called a unicast frame.
- The destination MAC address of a unicast frame is a unicast MAC address.

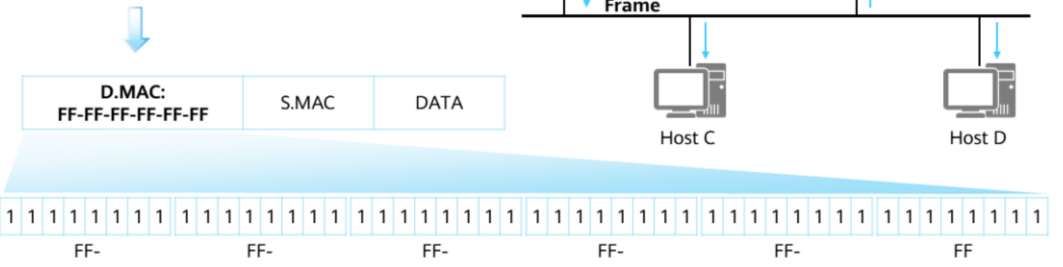


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Frames on a LAN can be sent in three modes: unicast, broadcast, and multicast.
- In unicast mode, frames are sent from a single source to a single destination.
  - Each host interface is uniquely identified by a MAC address. In the OUI of a MAC address, the eighth bit of the first byte indicates the address type. For a host MAC address, this bit is fixed at 0, indicating that all frames with this MAC address as the destination MAC address are sent to a unique destination.

Broadcast Ethernet Frame

- A broadcast Ethernet frame ia also called a broadcast frame.
- The destination MAC address of a broadcast frame is a broadcast MAC address.

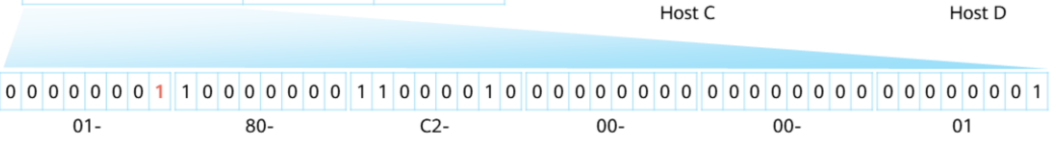


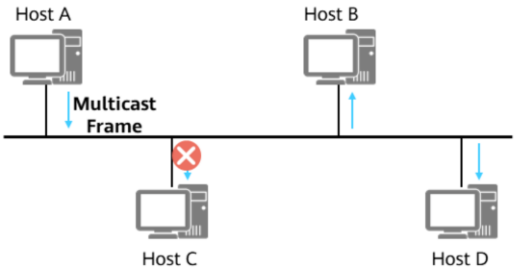
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In broadcast mode, frames are sent from a single source to all hosts on the shared Ethernet.
  - The destination MAC address of a broadcast frame is a hexadecimal address in the format of FF-FF-FF-FF-FF-FF. All hosts that receive the broadcast frame must receive and process the frame.
  - In broadcast mode, a large amount of traffic is generated, which decreases the bandwidth utilization and affects the performance of the entire network.
  - The broadcast mode is usually used when all hosts on a network need to receive and process the same information.

Multicast Ethernet Frame

- A multicast Ethernet frame is also called a multicast frame.
- The destination MAC address of a multicast frame is a unicast MAC address.





 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

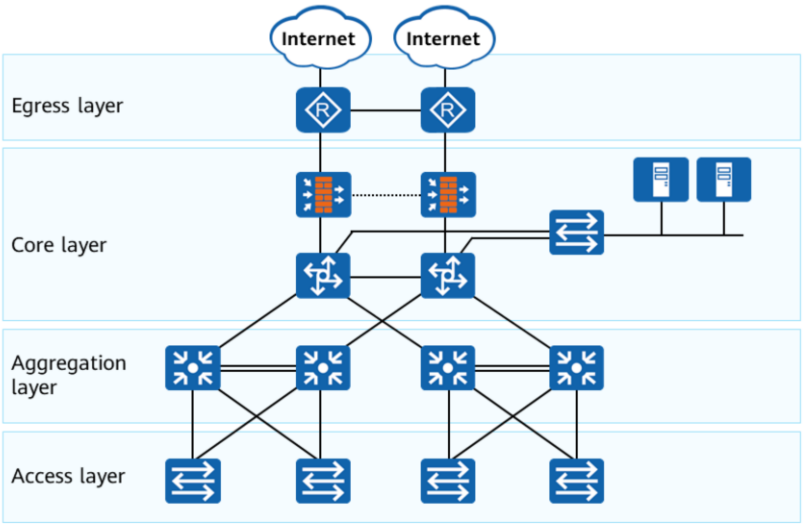
- The multicast mode is more efficient than the broadcast mode.
  - Multicast forwarding can be considered as selective broadcast forwarding. Specifically, a host listens for a specific multicast address, and receives and processes frames whose destination MAC address is the multicast MAC address.
  - A multicast MAC address and a unicast MAC address are distinguished by the eighth bit in the first byte. The eighth bit of a multicast MAC address is 1.
  - The multicast mode is used when a group of hosts (not all hosts) on the network need to receive the same information and other hosts are not affected.

Contents

1. Overview of Ethernet Protocols
2. Overview of Ethernet Frames
3. **Overview of Ethernet Switches**
4. Process of Data Communication Within a Network Segment

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Typical Architecture of a Campus Network

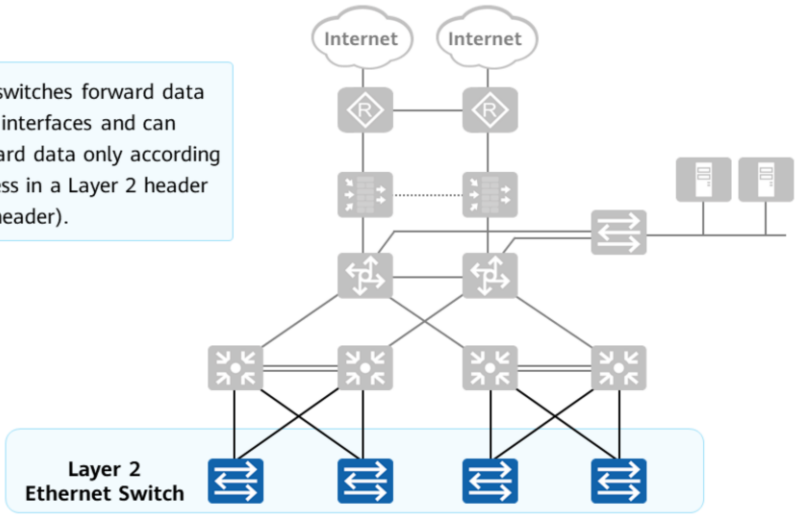


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A typical campus network consists of different devices, such as routers, switches, and firewalls. Generally, a campus network adopts the multi-layer architecture which includes the access layer, aggregation layer, core layer, and egress layer.

Layer 2 Ethernet switch

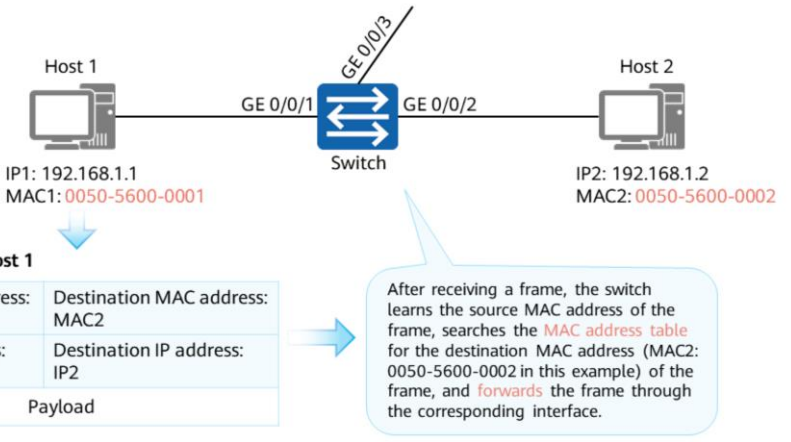
Layer 2 Ethernet switches forward data through Ethernet interfaces and can address and forward data only according to the MAC address in a Layer 2 header (Ethernet frame header).



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Layer 2 Ethernet switch:
  - On a campus network, a switch is the device closest to end users and is used to connect terminals to the campus network. Switches at the access layer are typically Layer 2 switches.
  - A Layer 2 switch works at the second layer of the TCP/IP model, which is the data link layer, and forwards data packets based on MAC addresses.
- Layer 3 Ethernet switch:
  - Routers are required to implement network communication between different LANs. As data communication networks expand and more services emerge on the networks, increasing traffic needs to be transmitted between networks. Routers cannot adapt to this development trend because of their high costs, low forwarding performance, and small interface quantities. New devices capable of high-speed Layer 3 forwarding are required. Layer 3 switches are such devices.
- Note that the switches involved in this course refer to Layer 2 Ethernet switches.

Working Principles of Switches

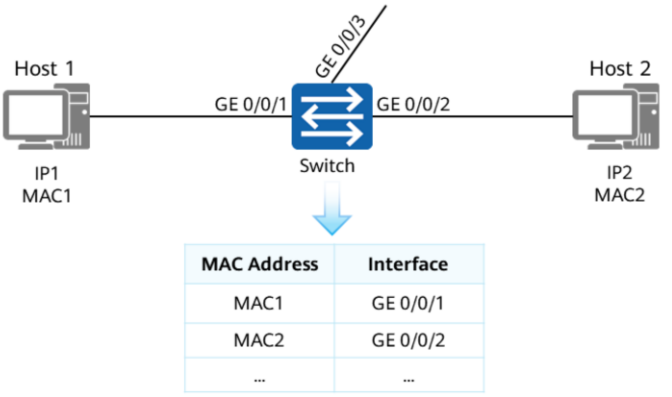


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Layer 2 switches work at the data link layer and forward frames based on MAC addresses. Switch interfaces used to send and receive data are independent of each other. Each interface belongs to a different collision domain, which effectively isolates collision domains on the network.
- Layer 2 switches maintain the mapping between MAC addresses and interfaces by learning the source MAC addresses of Ethernet frames. The table that stores the mapping between MAC addresses and interfaces is called a MAC address table. Layer 2 switches look up the MAC address table to determine the interface to which frames are forwarded based on the destination MAC address.

MAC Address Table

- Each switch has a MAC address table that stores the mapping between MAC addresses and switch interfaces.



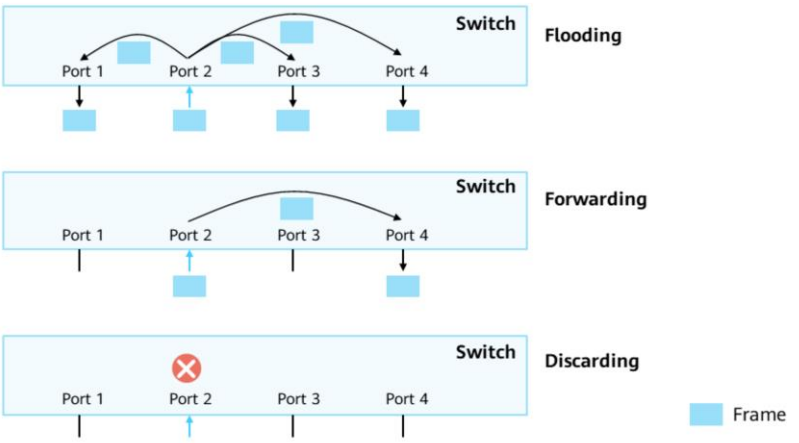
MAC Address	Interface
MAC1	GE 0/0/1
MAC2	GE 0/0/2
...	...

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- A MAC address table records the mapping between MAC addresses and interfaces of other devices learned by a switch. When forwarding a frame, the switch looks up the MAC address table based on the destination MAC address of the frame. If the MAC address table contains the entry corresponding to the destination MAC address of the frame, the frame is directly forwarded through the outbound interface in the entry. If the MAC address table does not contain the entry corresponding to the destination MAC address of the frame, the switch floods the frame on all interfaces except the interface that receives the frame.

Three Frame Processing Behaviors of a Switch

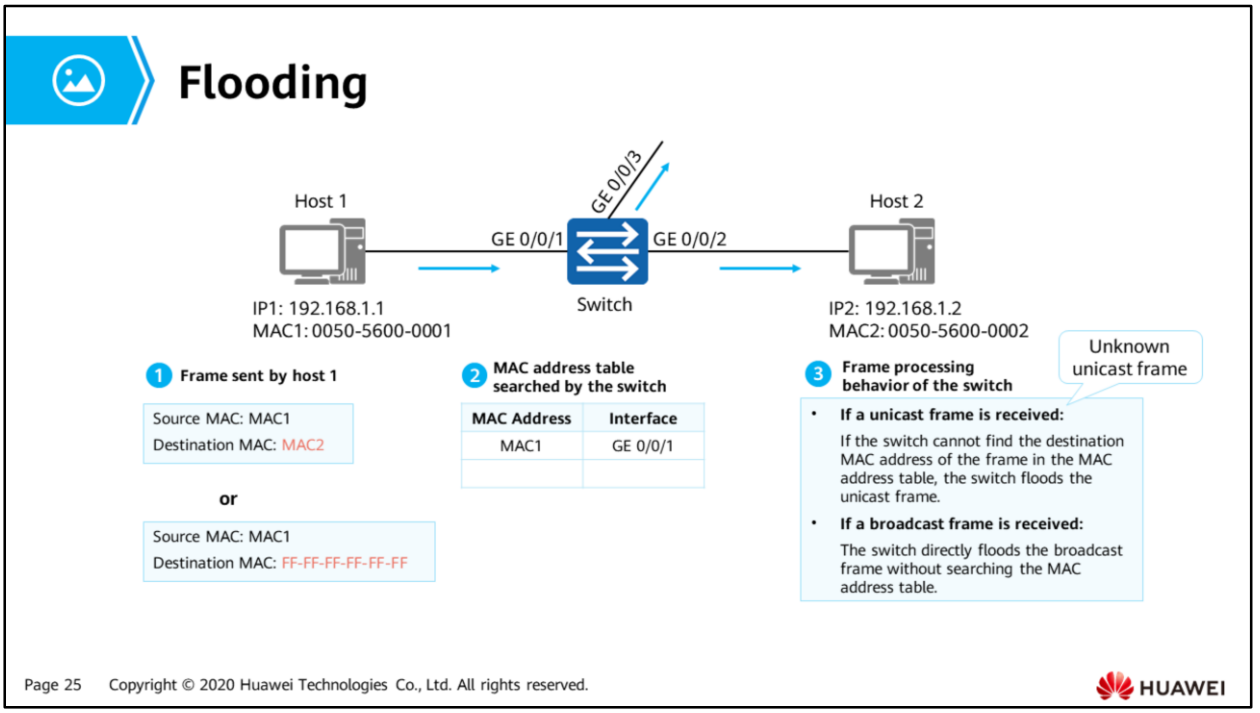
- A switch processes the frames entering an interface over a transmission medium in three ways:



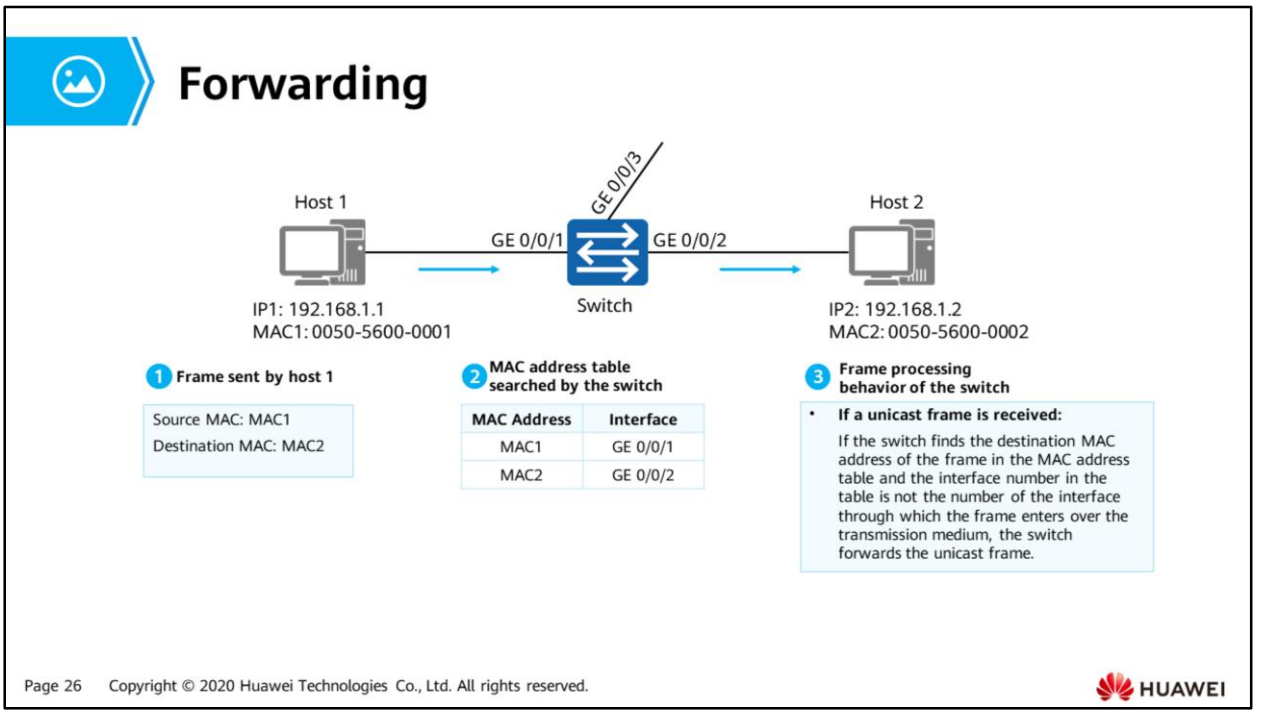
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

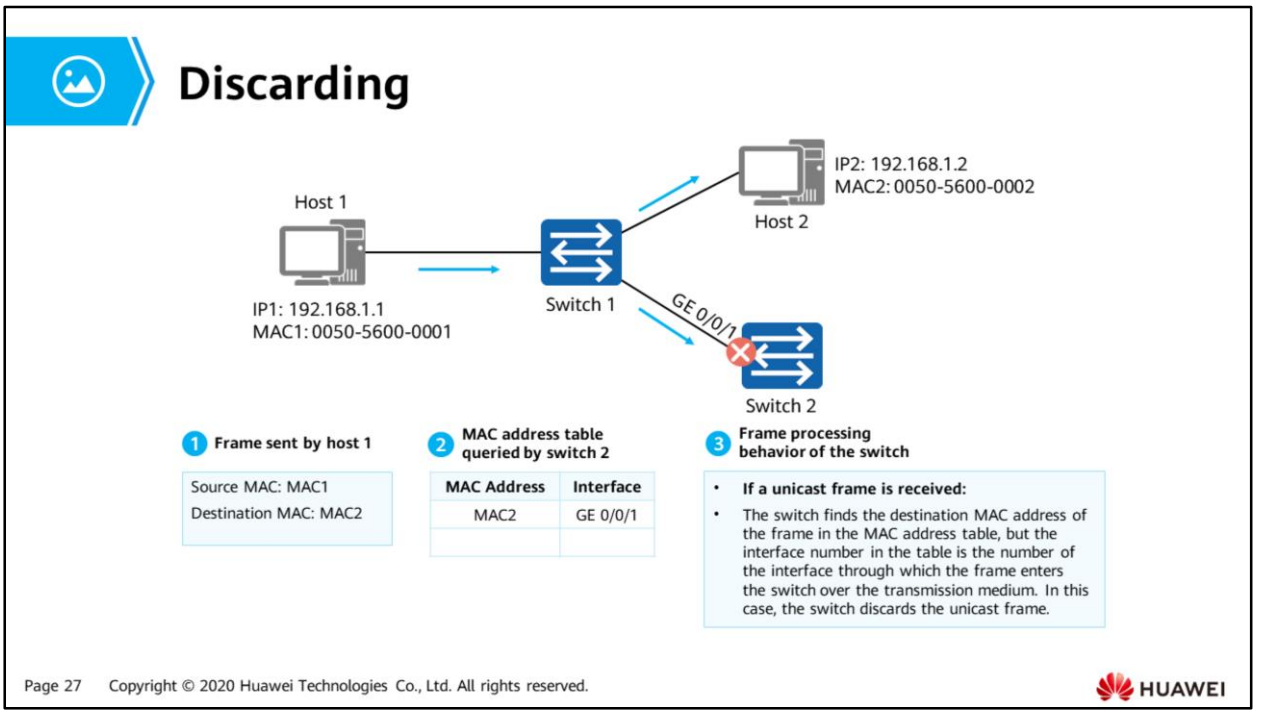
- A switch forwards each frame that enters an interface over a transmission medium. The basic function of a switch is to forward frames.
- A switch processes frames in three ways: flooding, forwarding, and discarding.
  - Flooding: The switch forwards the frames received from an interface to all other interfaces.
  - Forwarding: The switch forwards the frames received from an interface to another interface.
  - Discarding: The switch discards the frames received from an interface.



- If a unicast frame enters a switch interface over a transmission medium, the switch searches the MAC address table for the destination MAC address of the frame. If the MAC address cannot be found, the switch floods the unicast frame.
- If a broadcast frame enters a switch interface over a transmission medium, the switch directly floods the broadcast frame instead of searching the MAC address table for the destination MAC address of the frame.
- As shown in this figure:
    - Scenario 1: Host 1 wants to access host 2 and sends a unicast frame to the switch. After receiving the unicast frame, the switch searches the MAC address table for the destination MAC address of the frame. If the destination MAC address does not exist in the table, the switch floods the frame.
    - Scenario 2: Host 1 wants to access host 2 but does not know the MAC address of host 2. Host 1 sends an ARP Request packet, which is a broadcast frame to the switch. The switch then floods the broadcast frame.

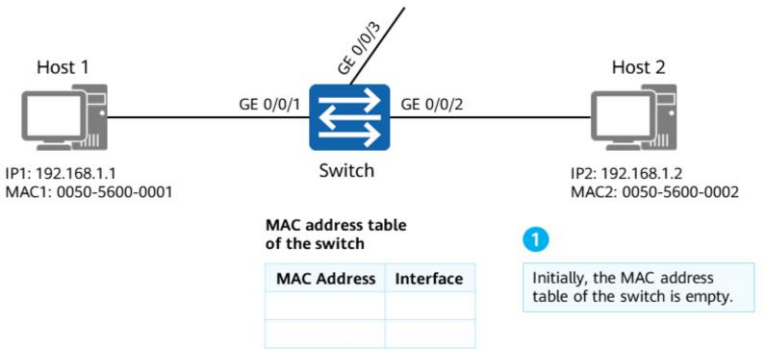


- If a unicast frame enters a switch interface over a transmission medium, the switch searches the MAC address table for the destination MAC address of the frame. If the corresponding entry is found in the MAC address table, the switch checks whether the interface number corresponding to the destination MAC address is the number of the interface through which the frame enters the switch over the transmission medium. If not, the switch forwards the frame to the interface corresponding to the destination MAC address of the frame in the MAC address table. The frame is then sent out from this interface.
- As shown in this figure,
    - host 1 wants to access host 2 and sends a unicast frame to the switch. After receiving the unicast frame, the switch finds the corresponding entry in the MAC address table and forwards the frame in point-to-point mode.



- If a unicast frame enters a switch interface over a transmission medium, the switch searches the MAC address table for the destination MAC address of the frame. If the corresponding entry is found in the MAC address table, the switch checks whether the interface number corresponding to the destination MAC address in the MAC address table is the number of the interface through which the frame enters the switch over the transmission medium. If yes, the switch discards the frame.
- As shown in this figure:
  - Host 1 wants to access host 2 and sends a unicast frame to switch 1. After receiving the unicast frame, switch 1 searches the MAC address table for the destination MAC address of the frame. If the destination MAC address does not exist in the table, switch 1 floods the frame.
  - After receiving the frame, switch 2 finds that the interface corresponding to the destination MAC address is the interface that receives the frame. In this case, switch 2 discards the frame.

MAC Address Learning on a Switch (1)



MAC address table of the switch

MAC Address	Interface

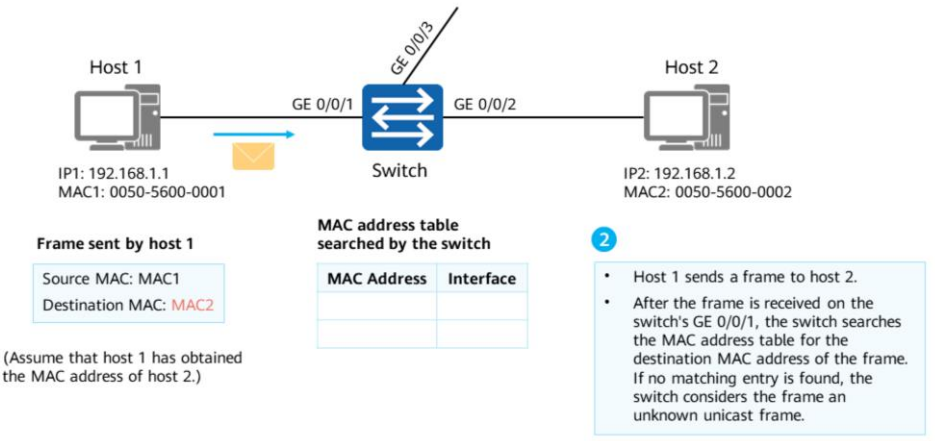
1

Initially, the MAC address table of the switch is empty.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In the initial state, a switch does not know the MAC address of a connected host. Therefore, the MAC address table is empty.

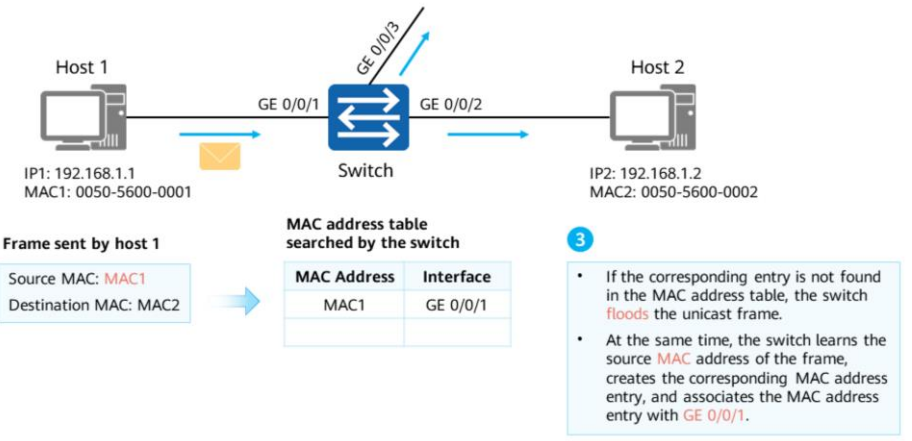
MAC Address Learning on a Switch (2)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- If host 1 wants to send data to host 2 (assume that host 1 has obtained the IP address and MAC address of host 2), host 1 encapsulates the frame with its own source IP address and source MAC address.
- After receiving the frame, the switch searches its own MAC address table. If no matching entry is found in the table, the switch considers the frame an unknown unicast frame.

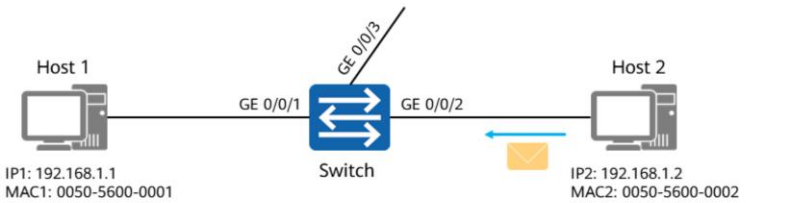
MAC Address Learning on a Switch (3)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- The switch floods the received frame because it is an unknown unicast frame.
- In addition, the switch records the source MAC address and interface number of the received frame in the MAC address table.
- Note that the dynamically learned entries in a MAC address table are not always valid. Each entry has a lifespan. If an entry is not updated within the lifespan, the entry will be deleted. This lifespan is called the aging time. For example, the default aging time of Huawei S series switches is 300s.

MAC Address Learning on a Switch (4)



4

- The frame is also received by the hosts connected to other interfaces on the switch. These hosts, however, discard the frame.
- Host 2 receives and processes the frame, responds to host 1, and sends the frame to the switch.

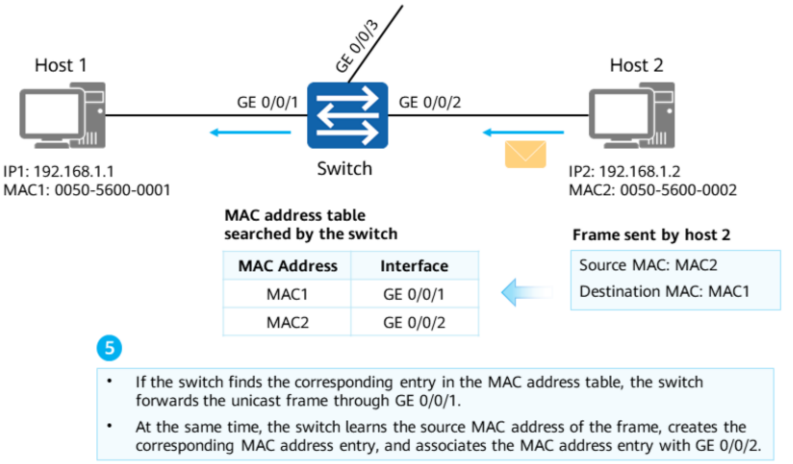
Frame sent by host 2

Source MAC: MAC2
Destination MAC: MAC1

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- All hosts on a broadcast network receive the frame, but only host 2 processes the frame because the destination MAC address is the MAC address of host 2.
- Host 2 sends a reply frame, which is also a unicast data frame, to host 1.

MAC Address Learning on a Switch (5)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- After receiving the unicast frame, the switch checks its MAC address table. If a matching entry is found, the switch forwards the frame through the corresponding interface.
- In addition, the switch records the source MAC address and interface number of the received frame in the MAC address table.

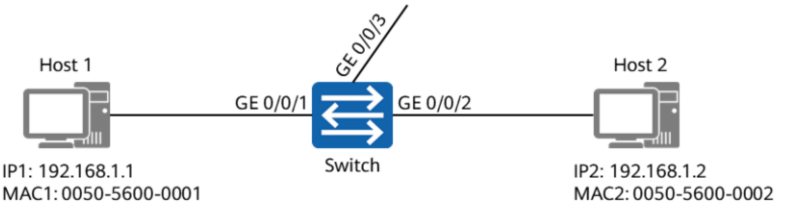
Contents

1. Overview of Ethernet Protocols
2. Overview of Ethernet Frames
3. Overview of Ethernet Switches
4. **Process of Data communication Within a Network Segment**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

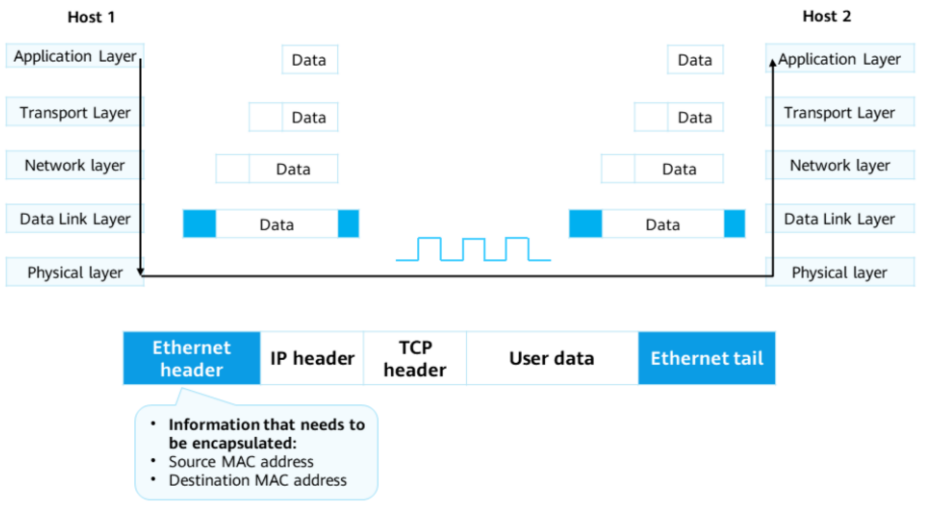
Process of Data Communication Within a Network Segment

- Scenario description:
  - Task: Host 1 wants to access host 2.
  - Host: The host is in the initialized state and only knows its own IP address and MAC address (assume that the IP address of the peer host has been obtained).
  - Switch: The switch is just powered on and in the initialized state.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

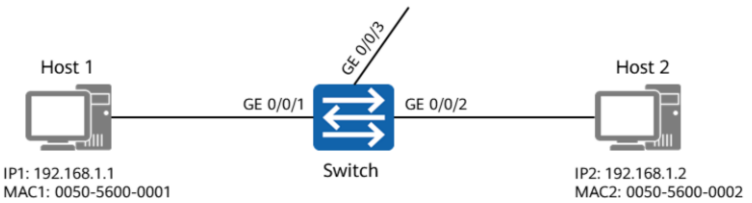
Data Encapsulation Process



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Before sending a packet, host 1 needs to encapsulate information, including the source and destination IP addresses and the source and destination MAC addresses, into the packet.

Initialization



ARP cache table of host 1

```
Host 1>arp -a
Internet Address    Physical Address   Type
```

MAC address table of the switch

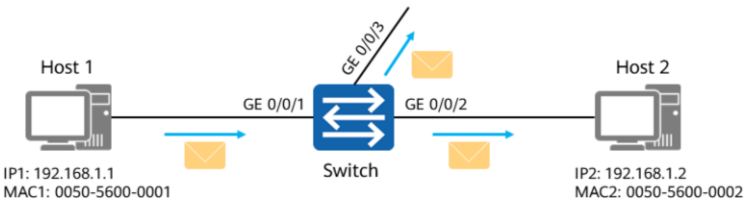
```
[Switch]display mac-address verbose
MAC address table of slot 0:
------------------------------------------------------------
MAC Address       Port        Type
------------------------------------------------------------

------------------------------------------------------------
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- To encapsulate packet, host 1 searches the local ARP cache table. In the initial state, the ARP cache table of host 1 is empty.
- For the switch that is just powered on, in the initial state, the MAC address table is also empty.

Flooding Frames



ARP Request packet sent by host 1

Source MAC address: MAC1	Destination MAC address: FF-FF-FF-FF-FF-FF
Source IP address: IP1	Destination IP address: IP2
Operation type: ARP Request Sender's MAC address: MAC1 Sender's IP address: IP1 Destination MAC address: 00-00-00-00-00-00 Destination IP address: IP2	

MAC address table of the switch

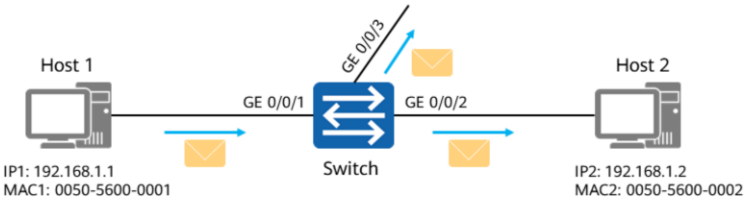
```
[Switch]display mac-address verbose
MAC address table of slot 0:
------------------------------------------------------------
MAC Address      Port        Type
------------------------------------------------------------


------------------------------------------------------------
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Host 1 sends an ARP Request packet to request for the destination MAC address.
- After receiving a frame, the switch searches the MAC address table. If no matching entry is found in the table, the switch floods the frame to other interfaces other than the interface receiving the frame.

MAC Address Learning



ARP Request packet sent by host 1

Source MAC address: MAC1	Destination MAC address: FF-FF-FF-FF-FF-FF
Source IP address: IP1	Destination IP address: IP2
Operation type: ARP Request Sender's MAC address: MAC1 Sender's IP address: IP1 Destination MAC address: 00-00-00-00-00-00 Destination IP address: IP2	

MAC address table of the switch

```
[Switch]display mac-address verbose
MAC address table of slot 0:
-------------------------------------------------------------
MAC Address      Port        Type
-------------------------------------------------------------
0050-5600-0001   GE0/0/1     dynamic

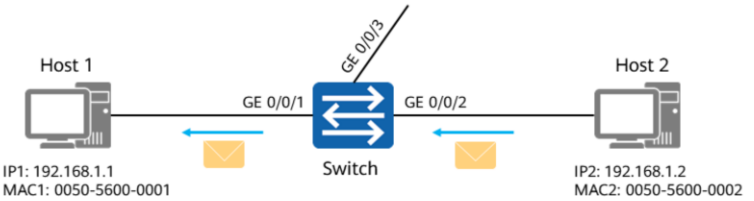
-------------------------------------------------------------
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- The switch records the source MAC address and interface number of the received frame in the MAC address table.

Reply of the Target Host



MAC address table of the switch

```
[Switch]display mac-address verbose
MAC address table of slot 0:
-------------------------------------------------------------
MAC Address     Port        Type
-------------------------------------------------------------
0050-5600-0001  GE0/0/1     dynamic
0050-5600-0002  GE0/0/2     dynamic
-------------------------------------------------------------
```

ARP Reply packet sent by host 2

Source MAC address: MAC2	Destination MAC address: MAC1
Source IP address: IP2	Destination IP address: IP1

Operation type: ARP Reply
Sender's MAC address: MAC2
Sender's IP address: IP2
Destination MAC address: MAC1
Destination IP address: IP1

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- After receiving the ARP Request packet, host 2 processes the packet and sends an ARP Reply packet to host 1.
- After receiving a frame, the switch searches the MAC address table. If the corresponding entry is found in the table, the switch forwards the frame to the corresponding interface and records the source MAC address and interface number of the received frame in the MAC address table.
- After receiving the ARP Reply packet from host 2, host 1 records the corresponding IP address and MAC address in its ARP cache table and encapsulates its packets to access host 2.

Quiz

1. (Single) A Layer 2 Ethernet switch generates a MAC address table entry based on the ( ) of the packet received by an interface.
   A. Source MAC address
   B. Destination MAC address
   C. Source IP address
   D. Destination IP address.
2. (Single) A switch has eight interfaces. A unicast frame enters the switch through one of the eight interfaces, but the switch cannot find the destination MAC address entry of the frame in the MAC address table. In this case, which of the following operations is performed by the switch? ( )
   A. Discarding
   B. Flooding
   C. Point-to-point forwarding

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. A
2. B

Summary

- This section describes the basic information about the Ethernet protocol, Ethernet frame formats, MAC address, and working principles of Layer 2 switches. Specifically, after receiving a frame, a switch learns the source MAC address of the frame and searches the destination MAC address of the frame in the MAC address table. If the destination MAC address exists in the table, the switch forwards the frame through the corresponding interface.
- This course also describes the whole process of data communication within the same network segment based on the working principles of switches.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



VLAN Principles and Configuration

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- Ethernet technology implements data communication over shared media based on carrier sense multiple access with collision detection (CSMA/CD). If there are a large number of PCs on the Ethernet, security risks and broadcast storms may occur, deteriorating network performance and even causing network breakdowns.
- The virtual local area network (VLAN) technology is therefore introduced to solve the preceding problem.
- This course describes basic VLAN principles, working principles of different Layer 2 interfaces, VLAN applications, data forwarding principles, and basic VLAN configuration methods.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand the background of the VLAN technology.
  - Identify the VLAN to which data belongs.
  - Master different VLAN assignment modes.
  - Describe how data communication is implemented through VLANs.
  - Master basic VLAN configuration methods.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

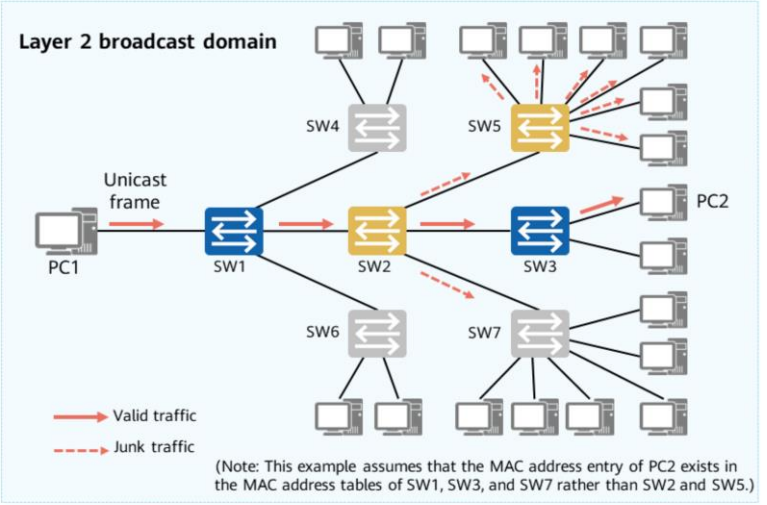
Contents

1. **What Is VLAN**
2. VLAN Principles
3. VLAN Applications
4. VLAN Configuration Examples

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Issues Facing a Traditional Ethernet

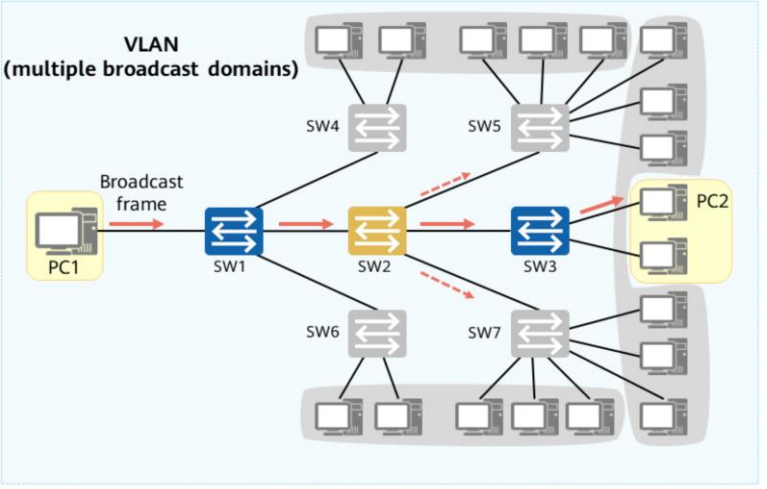


- On a typical switching network,broadcast frames or unknown unicast frames sent by a PC are flooded in the entire broadcast domain.
- The larger the broadcast domain is, the more serious network security and junk traffic problems are.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Broadcast domain:
  - The preceding figure shows a typical switching network with only PCs and switches. If PC1 sends a broadcast frame, the switches flood the frame on the network. As a result, all the other PCs receive the frame.
  - The range that broadcast frames can reach is called a Layer 2 broadcast domain (broadcast domain for short). A switching network is a broadcast domain.
- Network security and junk traffic problems:
  - Assume that PC1 sends a unicast frame to PC2. The MAC address entry of PC2 exists in the MAC address tables of SW1, SW3, and SW7 rather than SW2 and SW5. In this case, SW1 and SW3 forward the frame in point-to-point mode, SW7 discards the frame, and SW2 and SW5 flood the frame. As a result, although PC2 receives the unicast frame, other PCs on the network also receive the frame that should not be received.
- The larger the broadcast domain is, the more serious network security and junk traffic problems are.

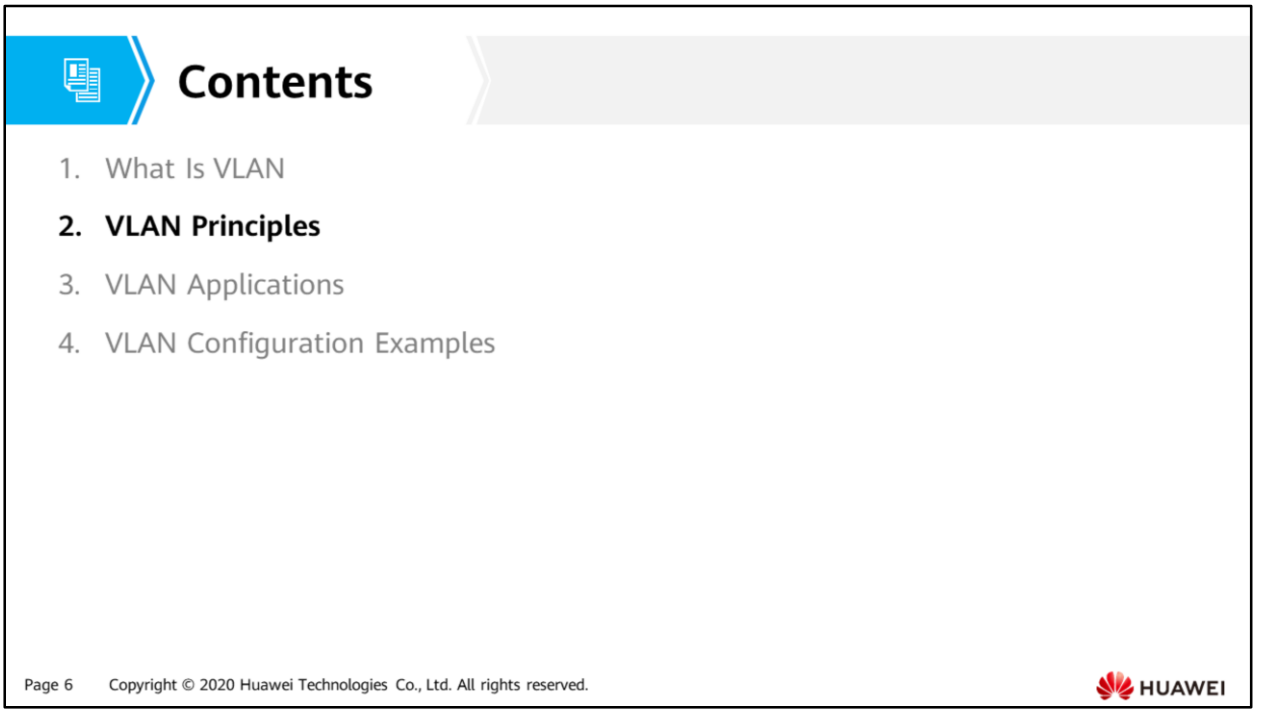
VLAN



- The VLAN technology isolates broadcast domains.
- Characteristics:
  - Geographically independent.
  - Only devices in the same VLAN can directly communicate at Layer 2.

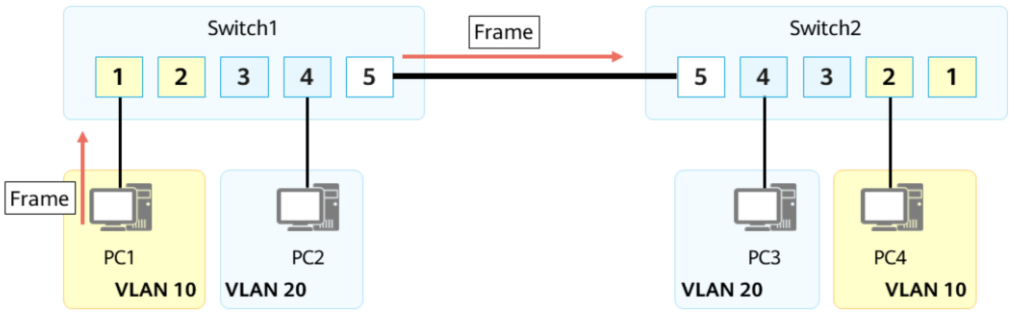
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- The VLAN technology is introduced to solve the problems caused by large broadcast domains.
  - By deploying VLANs on switches, you can logically divide a large broadcast domain into several small broadcast domains. This effectively improves network security, lowers junk traffic, and reduces the number of required network resources.
- VLAN characteristics:
  - Each VLAN is a broadcast domain. Therefore, PCs in the same VLAN can directly communicate at Layer 2. PCs in different VLANs, by contrast, can only communicate at Layer 3 instead of directly communicating at Layer 2. In this way, broadcast packets are confined to a VLAN.
  - VLAN assignment is geographically independent.
- Advantages of the VLAN technology:
  - Allows flexible setup of virtual groups. With the VLAN technology, terminals in different geographical locations can be grouped together, simplifying network construction and maintenance.
  - Confines each broadcast domain to a single VLAN, conserving bandwidth and improving network processing capabilities.
  - Enhances LAN security. Frames in different VLANs are separately transmitted, so that PCs in a VLAN cannot directly communicate with those in another VLAN.
  - Improves network robustness. Faults in a VLAN do not affect PCs in other VLANs.
- Note: Layer 2 refers to the data link layer.



- This part describes VLAN principles from the following three aspects: VLAN identification, VLAN assignment, and VLAN frame processing on switches.

VLAN Implementation

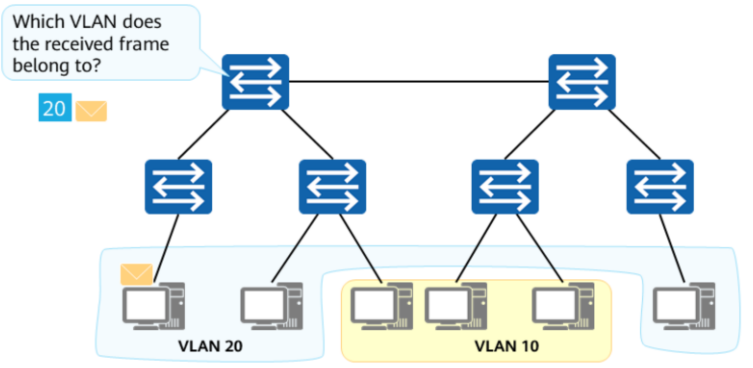


- Switch1 and Switch2 belong to the network of the same enterprise. VLANs are planned for the network, with VLAN 10 for department A and VLAN 20 for department B. Employees in departments A and B are connected to both Switch1 and Switch2.
- Assume that a frame sent from PC1 reaches Switch2 through the link between Switch1 and Switch2. If no processing is implemented, Switch2 can neither identify the VLAN to which the frame belongs nor determine the local VLAN to which the frame should be sent.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

VLAN Tag

- How does a switch identify the VLAN to which a received frame belongs?

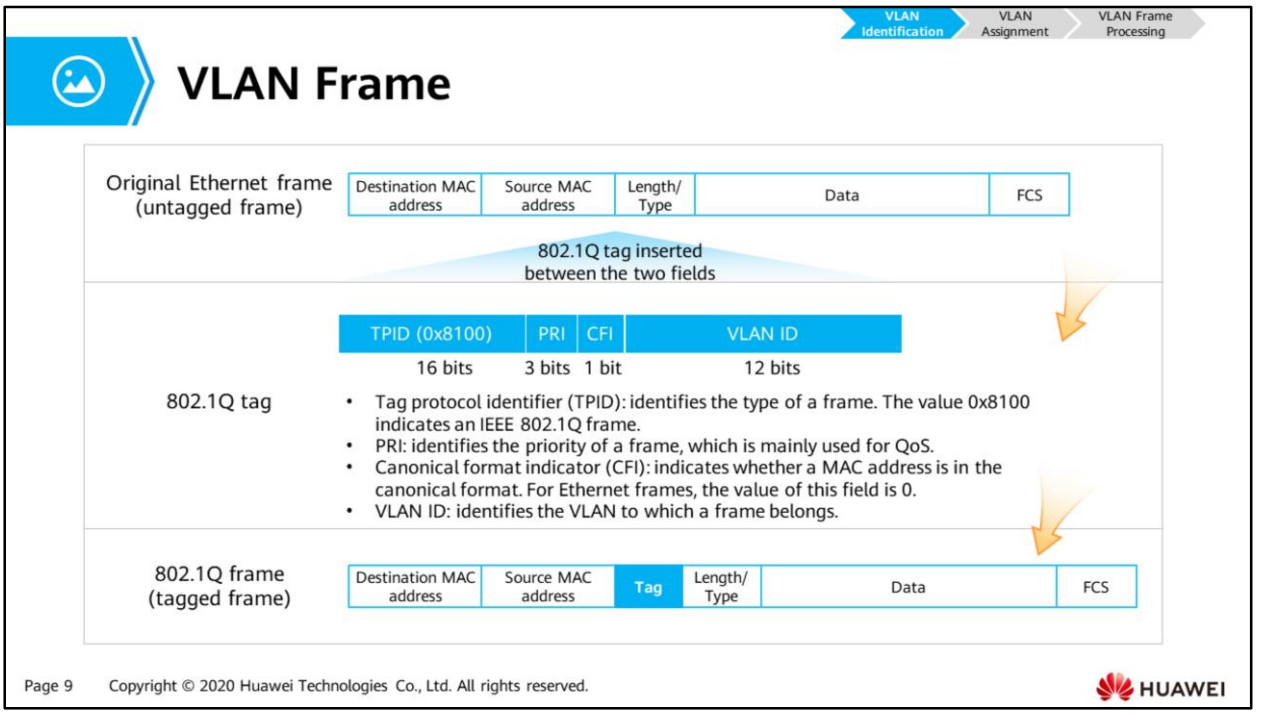


VLAN Tag

IEEE 802.1Q defines a 4-byte VLAN tag for Ethernet frames, enabling switches to identify the VLANs to which received frames belong.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

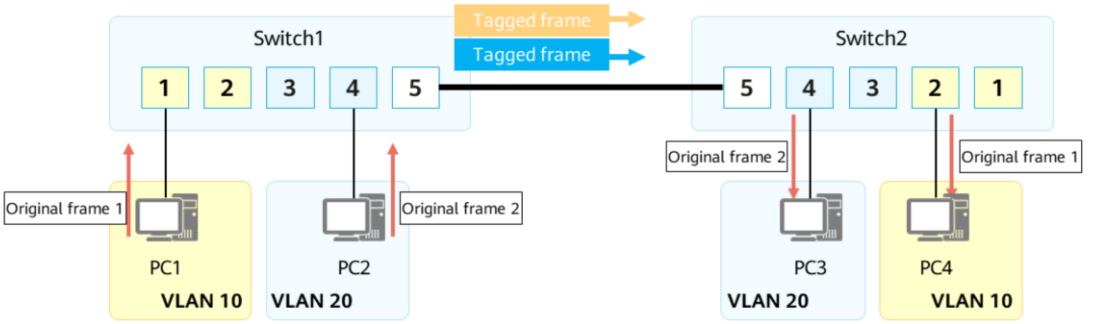
- As shown in the figure, after receiving a frame and identifying the VLAN to which the frame belongs, SW1 adds a VLAN tag to the frame to specify this VLAN. Then, after receiving the tagged frame sent from SW1, another switch, such as SW2, can easily identify the VLAN to which the frame belongs based on the VLAN tag.
- Frames with a 4-byte VLAN tag are called IEEE 802.1Q frames or VLAN frames.



- Ethernet frames in a VLAN are mainly classified into the following types:
  - Tagged frames: Ethernet frames for which a 4-byte VLAN tag is inserted between the source MAC address and length/type fields according to IEEE 802.1Q
  - Untagged frames: frames without a 4-byte VLAN tag
- Main fields in a VLAN frame:
  - TPID: a 16-bit field used to identify the type of a frame.
    - The value 0x8100 indicates an IEEE 802.1Q frame. A device that does not support 802.1Q discards 802.1Q frames.
    - Device vendors can define TPID values for devices. To enable a device to identify the non-802.1Q frames sent from another device, you can change the TPID on the device to be the same as that device.
  - PRI: a 3-bit field used to identify the priority of a frame. It is mainly used for QoS.
    - The value of this field is an integer ranging from 0 to 7. A larger value indicates a higher priority. If congestion occurs, a switch preferentially sends frames with the highest priority.

    - CFI: a 1-bit field indicating whether a MAC address is encapsulated in the canonical format. This field is mainly used to differentiate Ethernet frames, fiber distributed digital interface (FDDI) frames, and token ring frames.
        - The value 0 indicates that the MAC address is encapsulated in the canonical format, and the value 1 indicates that the MAC address is encapsulated in a non-canonical format.
        - For Ethernet frames, the value of this field is 0.
    - VLAN ID: also called VID, a 12-bit field used to identify the VLAN to which a frame belongs.
        - The value of this field is an integer ranging from 0 to 4095. Values 0 and 4095 are reserved. Therefore, only VLAN IDs from 1 to 4094 can be used.
        - A switch uses the VID contained in the VLAN tag to identify the VLAN that a frame belongs. Broadcast frames are forwarded only in the local VLAN.
- Method of identifying frames with VLAN tags:
    - Value of the Length/Type field of frames = 0x8100
- Note: PCs cannot identify tagged frames and therefore can send or process only untagged frames. By contrast, all frames processed by switches are tagged ones, improving processing efficiency.

VLAN Implementation

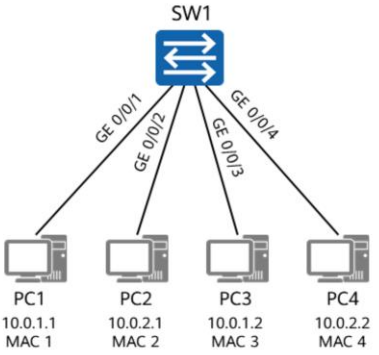


- The link between Switch1 and Switch2 carries data of multiple VLANs. In this situation, a VLAN-based data tagging method is required to distinguish the frames of different VLANs.
- IEEE 802.1Q, often referred to as Dot1q, defines a system of VLAN tagging for Ethernet frames by inserting an 802.1Q tag into the frame header to carry VLAN information.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

VLAN Assignment Methods

- How are VLANs assigned on a network?



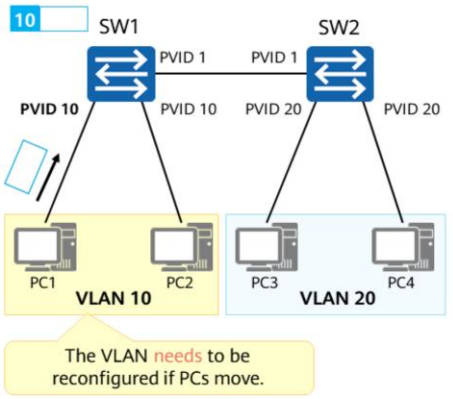
VLAN Assignment Method	VLAN 10	VLAN 20
Interface-based assignment	GE 0/0/1 and GE 0/0/3	GE 0/0/2 and GE 0/0/4
MAC address-based assignment	MAC 1 and MAC 3	MAC 2 and MAC 4
IP subnet-based assignment	10.0.1.*	10.0.2.*
Protocol-based assignment	IP	IPv6
Policy-based assignment	10.0.1.* + GE 0/0/1 + MAC 1	10.0.2.* + GE 0/0/2 + MAC 2

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- PCs send only untagged frames. After receiving such an untagged frame, a switch that supports the VLAN technology needs to assign the frame to a specific VLAN based on certain rules.
- Available VLAN assignment methods are as follows:
  - Interface-based assignment: assigns VLANs based on switch interfaces.
    - A network administrator preconfigures a port VLAN ID (PVID) for each switch interface. When an untagged frame arrives at an interface of a switch, the switch adds a tag carrying the PVID of the interface to the frame. The frame is then transmitted in the specified VLAN.
  - MAC address-based assignment: assigns VLANs based on the source MAC addresses of frames.
    - A network administrator preconfigures the mapping between MAC addresses and VLAN IDs. After receiving an untagged frame, a switch adds the VLAN tag mapping the source MAC address of the frame to the frame. The frame is then transmitted in the specified VLAN.

- IP subnet-based assignment: assigns VLANs based on the source IP addresses and subnet masks of frames.
  - A network administrator preconfigures the mapping between IP addresses and VLAN IDs. After receiving an untagged frame, a switch adds the VLAN tag mapping the source IP address of the frame to the frame. The frame is then transmitted in the specified VLAN.
- Protocol-based assignment: assigns VLANs based on the protocol (suite) types and encapsulation formats of frames.
  - A network administrator preconfigures the mapping between protocol (suite) types and VLAN IDs. After receiving an untagged frame, a switch adds the VLAN tag mapping the protocol (suite) type of the frame to the frame. The frame is then transmitted in the specified VLAN.
- Policy-based assignment: assigns VLANs based on a specified policy, such as a policy combining the preceding methods.
  - A network administrator preconfigures a policy. After receiving an untagged frame that matches the policy, a switch adds a specified VLAN tag to the frame. The frame is then transmitted in the specified VLAN.

Interface-based VLAN Assignment



Interface-based VLAN Assignment

- **Principles**
  - VLANs are assigned based on interfaces.
  - A network administrator preconfigures a PVID for each switch interface and assigns each interface to a VLAN corresponding to the PVID.
  - After an interface receives an untagged frame, the switch adds a tag carrying the PVID of the interface to the frame. The frame is then transmitted in the specified VLAN.
- **Port Default VLAN ID: PVID**
  - Default VLAN ID for an interface
  - Value range: 1–4094

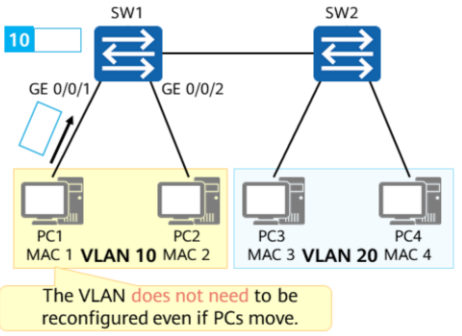
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Assignment rules:
  - VLAN IDs are configured on physical interfaces of a switch. All PC-sent untagged frames arriving at a physical interface are assigned to the VLAN corresponding to the PVID configured for the interface.
- Characteristics:
  - VLAN assignment is simple, intuitive, and easy to implement. Currently, it is the most widely used VLAN assignment method.
  - If the switch interface to which a PC is connected changes, the VLAN to which frames sent from the PC to the interface are assigned may also change.
- Port Default VLAN ID: PVID
  - A PVID needs to be configured for each switch interface. All untagged frames arriving at an interface are assigned to the VLAN corresponding to the PVID configured for the interface.
  - The default PVID is 1.

MAC Address-based VLAN Assignment

Mapping Between MAC Addresses and VLAN IDs on SW1

MAC Address	VLAN ID
MAC 1	10
MAC 2	10
...	...



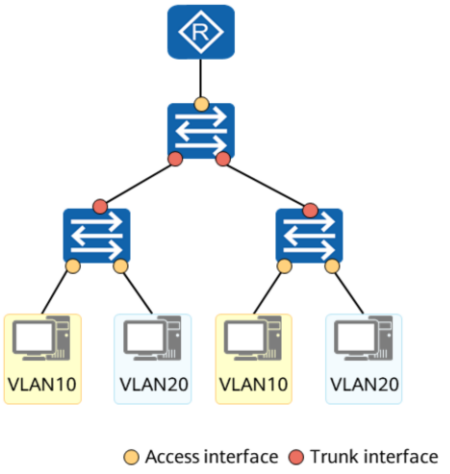
MAC Address-based VLAN Assignment

- **Principles**
  - VLANs are assigned based on the source MAC addresses of frames.
  - A network administrator preconfigures the mapping between MAC addresses and VLAN IDs.
  - After receiving an untagged frame, a switch adds the VLAN tag mapping the source MAC address of the frame to the frame. The frame is then transmitted in the specified VLAN.
- **Mapping table**
  - Records the mapping between MAC addresses and VLAN IDs.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Assignment rules:
  - Each switch maintains a table recording the mapping between MAC addresses and VLAN IDs. After receiving a PC-sent untagged frame, a switch analyzes the source MAC address of the frame, searches the mapping table for the VLAN ID mapping the MAC address, and assigns the frame to the corresponding VLAN according to the mapping.
- Characteristics:
  - This assignment method is a bit complex but more flexible.
  - If the switch interface to which a PC is connected changes, the VLAN to which frames sent from the PC to the interface are assigned remains unchanged because the PC's MAC address does not change.
  - However, as malicious PCs can easily forge MAC addresses, this assignment method is prone to security risks.

Layer 2 Ethernet Interface Types

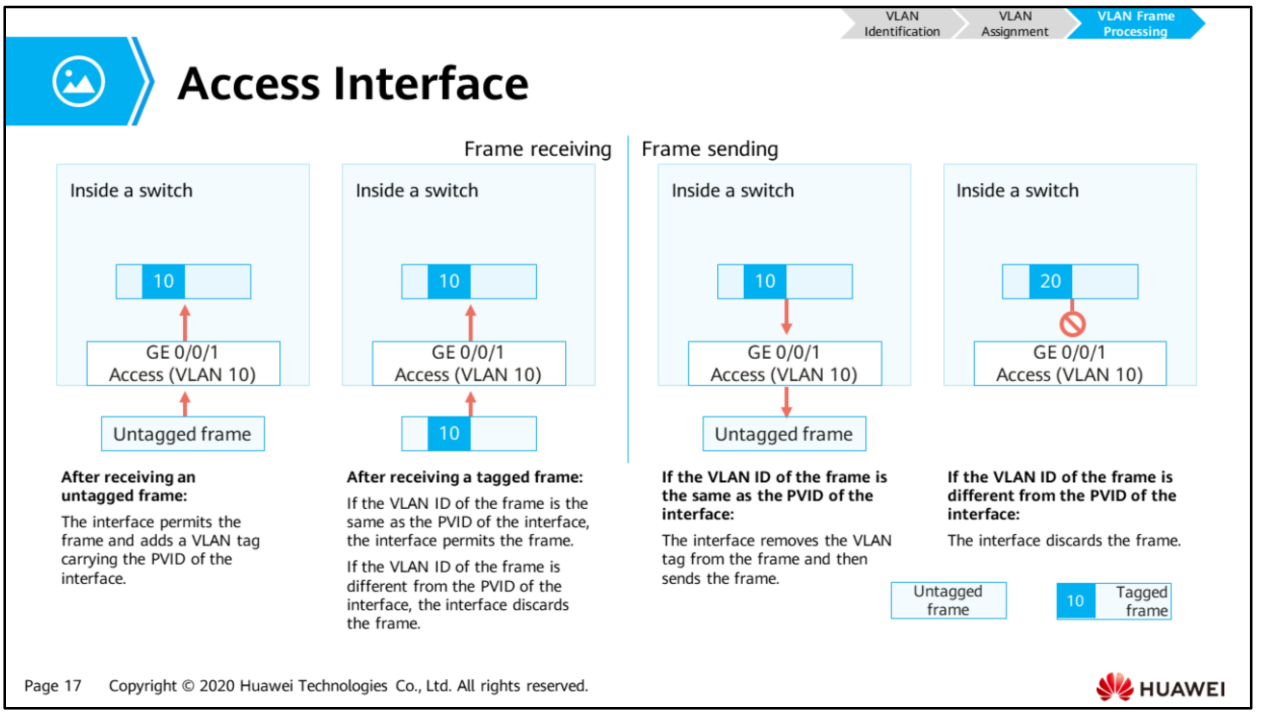


Interface Types

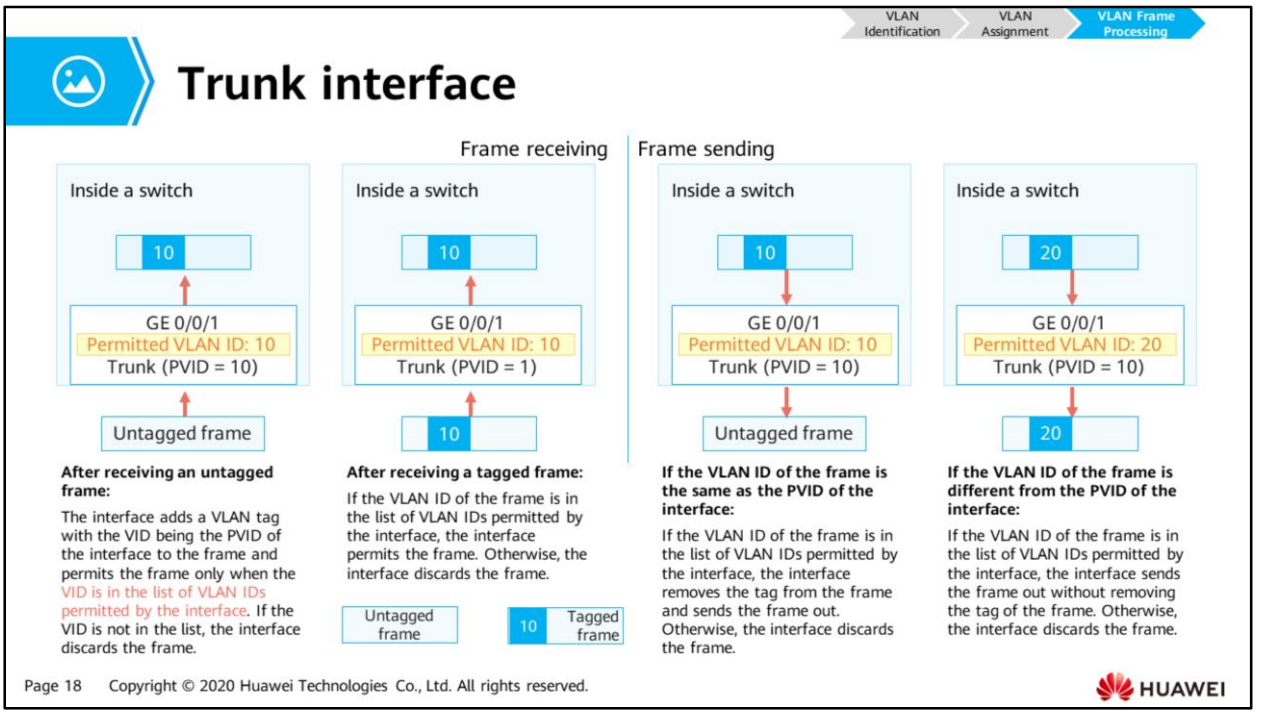
- **Access interface**
  An access interface is used to connect a switch to a terminal, such as a PC or server. In general, the NICs on such a terminal receive and send only untagged frames. An access interface can be added to only one VLAN.
- **Trunk interface**
  A trunk interface allows frames that belong to multiple VLANs to pass through and differentiates the frames using the 802.1Q tag. This type of interface is used to connect a switch to another switch or a sub-interface on a device, such as a router or firewall.
- **Hybrid interface**
  Similar to a trunk interface, a hybrid interface also allows frames that belong to multiple VLANs to pass through and differentiates the frames using the 802.1Q tag. You can determine whether to allow a hybrid interface to carry VLAN tags when sending the frames of one or more VLANs.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- The interface-based VLAN assignment method varies according to the switch interface type.
- Access interface
  - An access interface often connects to a terminal (such as a PC or server) that cannot identify VLAN tags, or is used when VLANs do not need to be differentiated.
- Trunk interface
  - A trunk interface often connects to a switch, router, AP, or voice terminal that can receive and send both tagged and untagged frames.
- Hybrid interface
  - A hybrid interface can connect to a user terminal (such as a PC or server) that cannot identify VLAN tags or to a switch, router, AP, or voice terminal that can receive and send both tagged and untagged frames.
  - By default, hybrid interfaces are used on Huawei devices.



- How do switch interfaces process tagged and untagged frames? First, let's have a look at access interfaces.
- Characteristics of access interfaces:
  - An access interface permits only frames whose VLAN ID is the same as the PVID of the interface.
- Frame receiving through an access interface:
  - After receiving an untagged frame, the access interface adds a tag with the VID being the PVID of the interface to the frame and then floods, forwards, or discards the tagged frame.
  - After receiving a tagged frame, the access interface checks whether the VID in the tag of the frame is the same as the PVID. If they are the same, the interface forwards the tagged frame. Otherwise, the interface directly discards the tagged frame.
- Frame sending through an access interface:
  - After receiving a tagged frame sent from another interface on the same switch, the access interface checks whether the VID in the tag of the frame is the same as the PVID.
    - If they are the same, the interface removes the tag from the frame and sends the untagged frame out.
    - Otherwise, the interface directly discards the tagged frame.

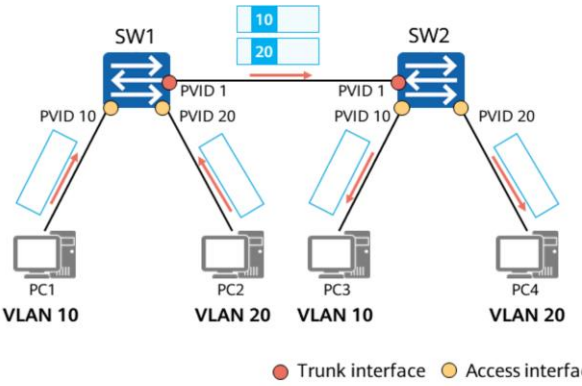


- For a trunk interface, you need to configure not only a PVID but also a list of VLAN IDs permitted by the interface. By default, VLAN 1 exists in the list.
- Characteristics of trunk interfaces:
  - A trunk interface allows only frames whose VLAN IDs are in the list of VLAN IDs permitted by the interface to pass through.
  - It allows tagged frames from multiple VLANs but untagged frames from only one VLAN to pass through.
- Frame receiving through a trunk interface:
  - After receiving an untagged frame, the trunk interface adds a tag with the VID being the PVID of the interface to the frame and then checks whether the VID is in the list of VLAN IDs permitted by the interface. If the VID is in the list, the interface forwards the tagged frame. Otherwise, the interface directly discards the tagged frame.
  - After receiving a tagged frame, the trunk interface checks whether the VID in the tag of the frame is in the list of VLAN IDs permitted by the interface. If the VID is in the list, the interface forwards the tagged frame. Otherwise, the interface directly discards the tagged frame.

- Frame sending through a trunk interface:
  - After receiving a tagged frame sent from another interface on the same switch, the trunk interface checks whether the VID in the tag of the frame is in the list of VLAN IDs permitted by the interface. If the VID is not in the list, the interface directly discards the frame.
  - After receiving a tagged frame sent from another interface on the same switch, the trunk interface checks whether the VID in the tag of the frame is in the list of VLAN IDs permitted by the interface. If the VID is in the list, the interface checks whether the VID is the same as the PVID of the interface.
    - If they are the same, the interface removes the tag from the frame and sends the untagged frame out.
    - If they are different, the interface directly sends the frame out without removing the tag from the frame.

Example for Frame Processing on Access and Trunk Interfaces

- Describe how inter-PC access is implemented in this example.

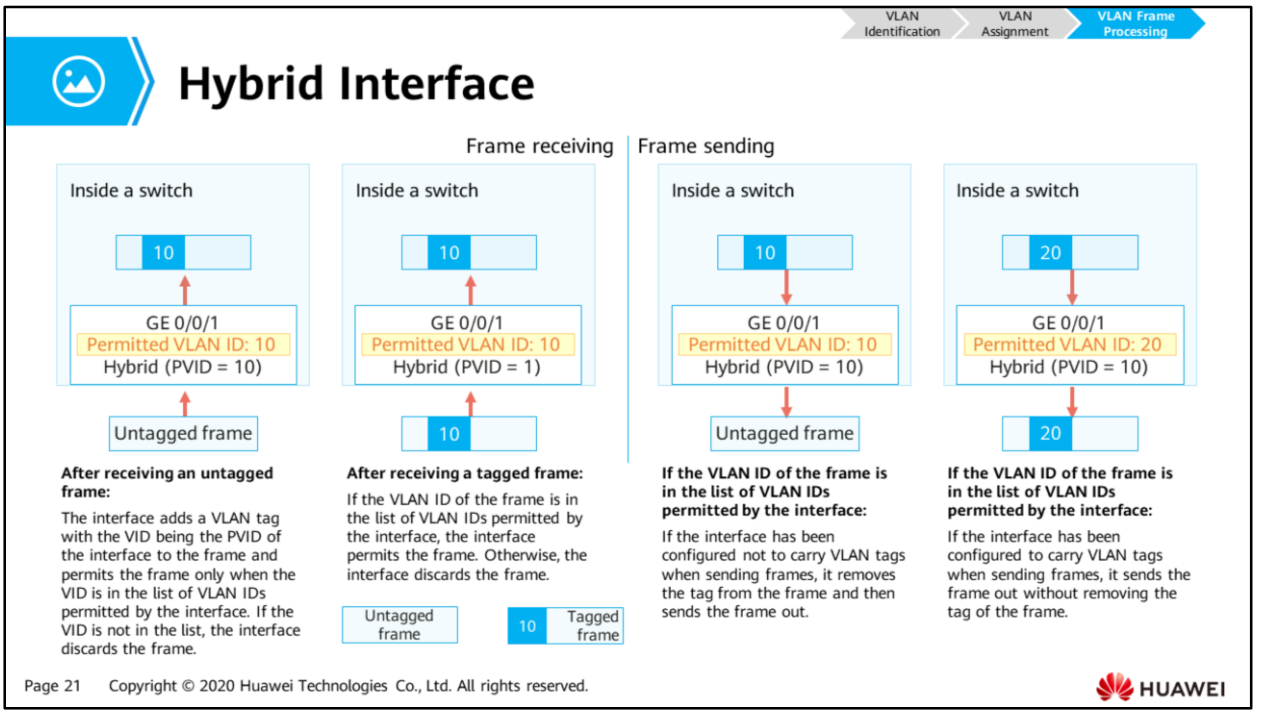


Trunk Interfaces on SW1 and SW2

List of Permitted VLAN IDs	
VLAN ID	1
	10
	20

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In this example, SW1 and SW2 connect to PCs through access interfaces. PVIDs are configured for the interfaces, as shown in the figure. SW1 and SW2 are connected through trunk interfaces whose PVIDs are all set to 1. The table lists the VLAN IDs permitted by the trunk interfaces.
- Describe how inter-PC access is implemented in this example.

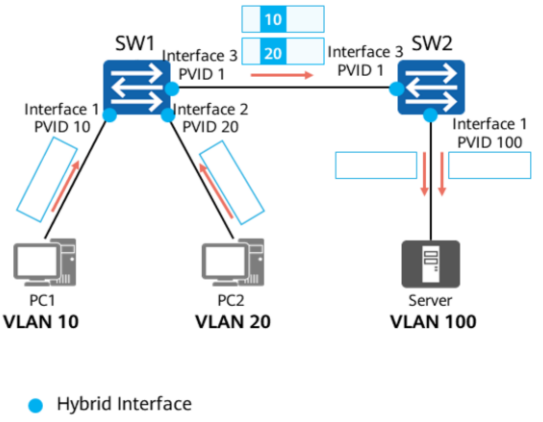


- For a hybrid interface, you need to configure not only a PVID but also two lists of VLAN IDs permitted by the interface: one untagged VLAN ID list and one tagged VLAN ID list. By default, VLAN 1 is in the untagged VLAN ID list. Frames from all the VLANs in the two lists are allowed to pass through the hybrid interface.
- Characteristics of hybrid interfaces:
  - A hybrid interface allows only frames whose VLAN IDs are in the lists of VLAN IDs permitted by the interface to pass through.
  - It allows tagged frames from multiple VLANs to pass through. Frames sent out from a hybrid interface can be either tagged or untagged, depending on the VLAN configuration.
  - Different from a trunk interface, a hybrid interface allows untagged frames from multiple VLANs to pass through.

- Frame receiving through a hybrid interface:
  - After receiving an untagged frame, the hybrid interface adds a tag with the VID being the PVID of the interface to the frame and then checks whether the VID is in the tagged or untagged VLAN ID list. If the VID is in the list, the interface forwards the tagged frame. Otherwise, the interface directly discards the tagged frame.
  - After receiving a tagged frame, the hybrid interface checks whether the VID in the tag of the frame is in the tagged or untagged VLAN ID list. If the VID is in the tagged or untagged VLAN ID list, the interface forwards the tagged frame. Otherwise, the interface directly discards the tagged frame.
- Frame sending through a hybrid interface:
  - After receiving a tagged frame sent from another interface on the same switch, the hybrid interface checks whether the VID in the tag of the frame is in the tagged or untagged VLAN ID list. If the VID is not in any of the two lists, the interface directly discards the frame.
  - After receiving a tagged frame sent from another interface on the same switch, the hybrid interface checks whether the VID in the tag of the frame is in the tagged or untagged VLAN ID list. If the VID is in the untagged VLAN ID list, the interface removes the tag from the frame and then sends the untagged frame out.
  - After receiving a tagged frame sent from another interface on the same switch, the hybrid interface checks whether the VID in the tag of the frame is in the tagged or untagged VLAN ID list. If the VID is in the tagged VLAN ID list, the interface directly sends the frame out without removing the tag from the frame.

Example for Frame Processing on Hybrid Interfaces

- Describe how PCs access the server in this example.



List of VLAN IDs Permitted by Interfaces on SW1

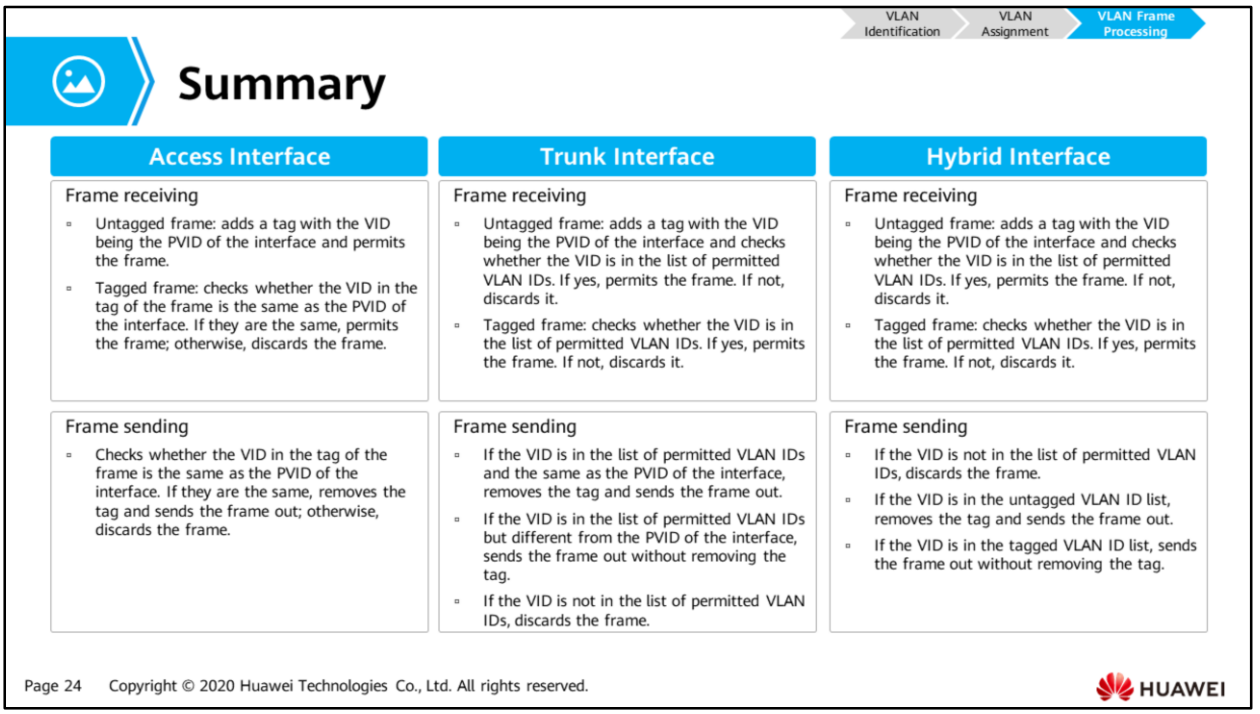
	Interface 1	Interface 2	Interface 3
	Untagged	Untagged	Tagged
VLAN ID	1	1	10
	10	20	10
	100	100	100

List of VLAN IDs Permitted by Interfaces on SW2

	Interface 1	Interface 3
	Untagged	Tagged
VLAN ID	1	10
	10	20
	20	100
	100	

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In this example, SW1 and SW2 connect to PCs through hybrid interfaces. The two switches are connected also through this type of interface. PVIDs are configured for the interfaces, as shown in the figure. The tables list the VLAN IDs permitted by the interfaces.
- Describe how PCs access the server in this example.



- The processes of adding and removing VLAN tags on interfaces are as follows:
  - Frame receiving:
    - After receiving an untagged frame, access, trunk, and hybrid interfaces all add a VLAN tag to the frame. Then, trunk and hybrid interfaces determine whether to permit the frame based on the VID of the frame (the frame is permitted only when the VID is a permitted VLAN ID), whereas an access interface permits the frame unconditionally.
    - After receiving a tagged frame, an access interface permits the frame only when the VID in the tag of the frame is the same as the PVID configured for the interface, while trunk and hybrid interfaces permit the frame only when the VID in the tag of the frame is in the list of permitted VLANs.
  - Frame sending:
    - Access interface: directly removes VLAN tags from frames before sending the frames.
    - Trunk interface: removes VLAN tags from frames only when the VIDs in the tags are the same as the PVID of the interface.
    - Hybrid interface: determines whether to remove VLAN tags from frames based on the interface configuration.
- Frames sent by an access interface are all untagged. On a trunk interface, only frames of one VLAN are sent without tags, and frames of other VLANs are all sent with tags. On a hybrid interface, you can specify the VLANs of which frames are sent with or without tags.

Contents

1. What Is VLAN
2. VLAN Principles
3. **VLAN Applications**
4. VLAN Configuration Examples

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

VLAN Planning

- **VLAN assignment rules**
  - By service: voice, video, and data VLANs
  - By department: e.g. VLANs for engineering, marketing, and financing departments
  - By application: e.g. VLANs for servers, offices, and classrooms
- **Tips for VLAN assignment**

  VLAN IDs can be randomly assigned within the supported range. To improve VLAN ID continuity, you can associate VLAN IDs with subnets during VLAN assignment.
- **Example for VLAN planning**
  - Assume that there are three buildings: administrative building with offices, classrooms, and financing sections, teaching building with offices and classrooms, and office building with offices and financing sections. Each building has one access switch, and the core switch is deployed in the administrative building.
  - The following table describes the VLAN plan.

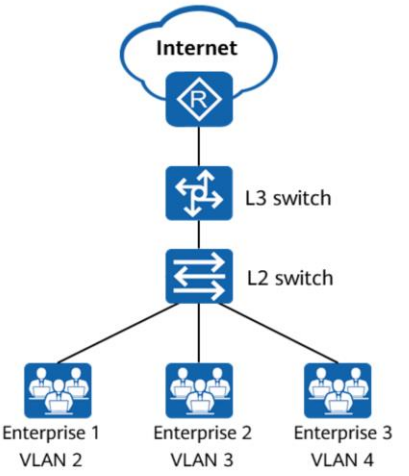
VLAN ID	IP Address Segment	Description
1	X.16.10.0/24	VLAN to which office users belong
2	X.16.20.0/24	VLAN to which the users of the financing department belong
3	X.16.30.0/24	VLAN to which classroom users belong
100	Y.16.100.0/24	VLAN to which the device management function belongs

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- You are advised to assign consecutive VLAN IDs to ensure proper use of VLAN resources. The most common method is interface-based VLAN assignment.

Interface-based VLAN Assignment

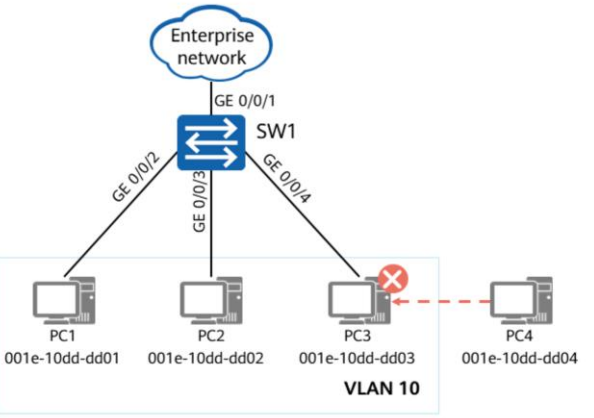
- Applicable scenario:
  - There are multiple enterprises in a building. These enterprises share network resources to reduce costs. Networks of the enterprises connect to different interfaces of the same Layer 2 switch and access the Internet through the same egress device.
- VLAN assignment:
  - To isolate the services of different enterprises and ensure service security, assign interfaces connected to the enterprises' networks to different VLANs. In this way, each enterprise has an independent network, and each VLAN works as a virtual work group.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

MAC Address-based VLAN Assignment

- Applicable scenario:
  - The network administrator of an enterprise assigns PCs in the same department to the same VLAN. To improve information security, the enterprise requires that only employees in the specified department be allowed to access specific network resources.
- VLAN assignment:
  - To meet the preceding requirement, configure MAC address-based VLAN assignment on SW1, preventing new PCs connected to the network from accessing the network resources.



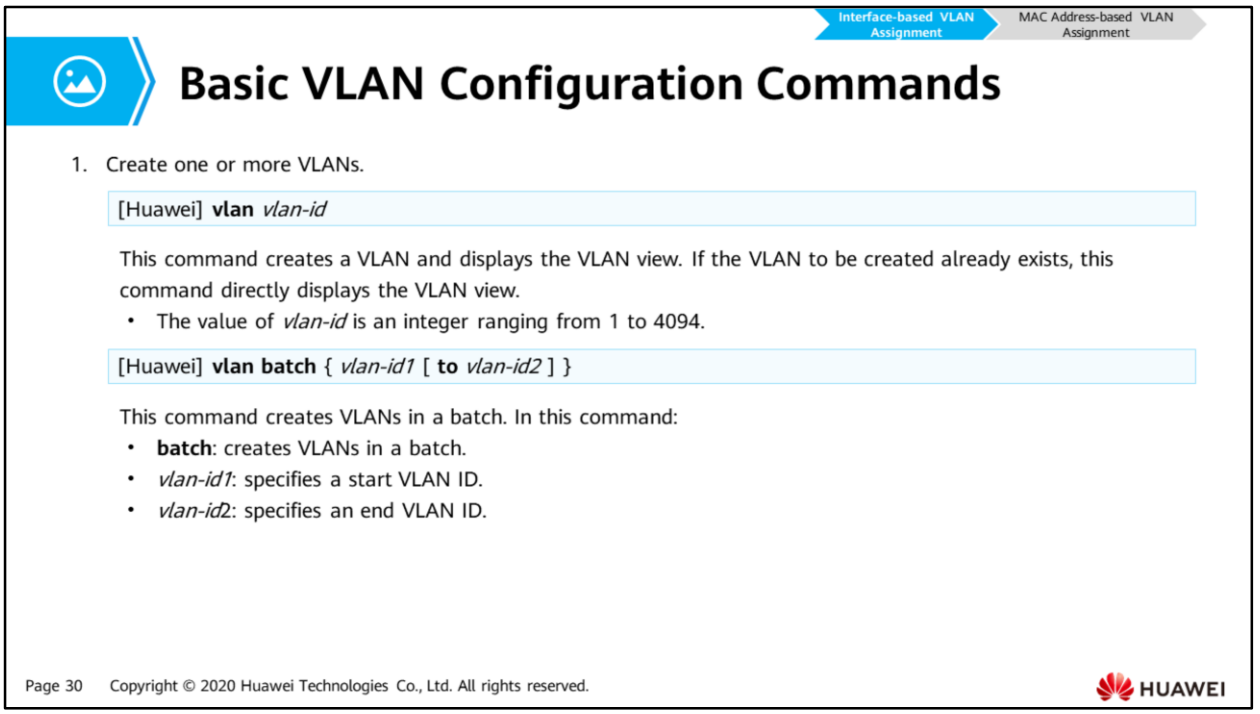
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Contents

1. What Is VLAN
2. VLAN Principles
3. VLAN Applications
4. **VLAN Configuration Examples**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI



- The **vlan** command creates a VLAN and displays the VLAN view. If the VLAN to be created already exists, this command directly displays the VLAN view.
- The **undo vlan** command deletes a VLAN.
- By default, all interfaces are added to the default VLAN with the ID of 1.
- Commands:
  - **vlan** *vlan-id*
    - *vlan-id*: specifies a VLAN ID. The value is an integer ranging from 1 to 4094.
  - **vlan batch** { *vlan-id1* [**to** v*lan-id2*] }
    - **batch**: creates VLANs in a batch.
    - *vlan-id1* [**to** v*lan-id2*]: specifies the IDs of VLANs to be created in a batch.
      - *vlan-id1*: specifies a start VLAN ID.
      - *vlan-id2*: specifies an end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*. The two parameters work together to define a VLAN range.
    - If you do not specify **to** v*lan-id2*, the command creates only one VLAN with the ID being specified using *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are both integers ranging from 1 to 4094.

Basic Access Interface Configuration Commands

1. Set the link type of an interface.

```
[Huawei-GigabitEthernet0/0/1] port link-type access
```

In the interface view, set the link type of the interface to access.

2. Configure a default VLAN for the access interface.

```
[Huawei-GigabitEthernet0/0/1] port default vlan vlan-id
```

In the interface view, configure a default VLAN for the interface and add the interface to the VLAN.

- *vlan-id:* specifies an ID for the default VLAN. The value is an integer ranging from 1 to 4094.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Basic Trunk Interface Configuration Commands

1. Set the link type of an interface.

   ```
   [Huawei-GigabitEthernet0/0/1] port link-type trunk
   ```

   In the interface view, set the link type of the interface to trunk.

2. Add the trunk interface to specified VLANs.

   ```
   [Huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan { { vlan-id1 [ to vlan-id2 ] } | all }
   ```

   In the interface view, add the trunk interface to specified VLANs.

3. (Optional) Configure a default VLAN for the trunk interface.

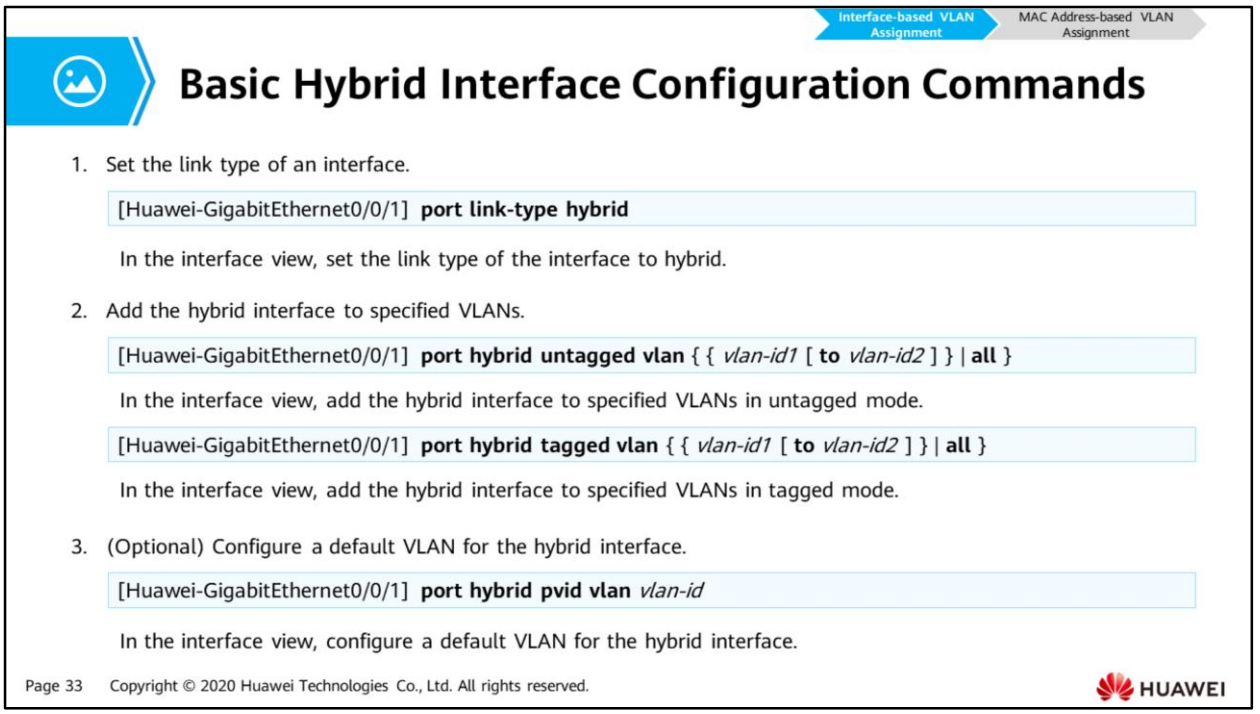
   ```
   [Huawei-GigabitEthernet0/0/1] port trunk pvid vlan vlan-id
   ```

   In the interface view, configure a default VLAN for the trunk interface.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

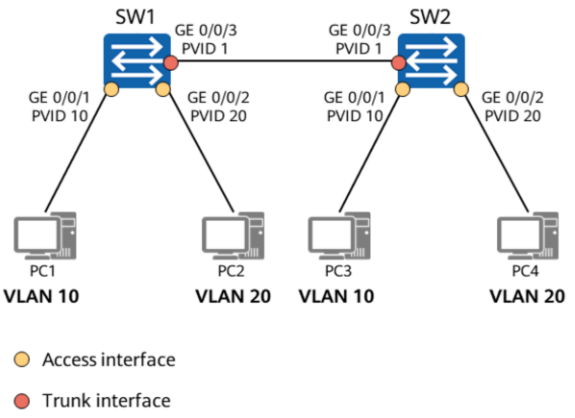
HUAWEI

- Command: **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] | **all** }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the IDs of VLANs to which a trunk interface needs to be added.
    - *vlan-id1*: specifies a start VLAN ID.
    - *vlan-id2*: specifies an end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are both integers ranging from 1 to 4094.
  - **all**: adds a trunk interface to all VLANs.
- The **port trunk pvid vlan** *vlan-id* command configures a default VLAN for a trunk interface.
  - *vlan-id*: specifies the ID of the default VLAN to be created for a trunk interface. The value is an integer ranging from 1 to 4094.



- Command: **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the IDs of VLANs to which a hybrid interface needs to be added.
    - *vlan-id1*: specifies a start VLAN ID.
    - vlan-id2: specifies an end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are both integers ranging from 1 to 4094.
  - **all**: adds a hybrid interface to all VLANs.
- Command: **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } | **all** }
  - *vlan-id1* [**to** *vlan-id2*]: specifies the IDs of VLANs to which a hybrid interface needs to be added.
    - *vlan-id1*: specifies a start VLAN ID.
    - vlan-id2: specifies an end VLAN ID. The value of *vlan-id2* must be greater than or equal to that of *vlan-id1*.
    - The values of *vlan-id1* and *vlan-id2* are both integers ranging from 1 to 4094.
  - **all**: adds a hybrid interface to all VLANs.
- The **port hybrid pvid vlan** *vlan-id* command configures a default VLAN for a hybrid interface.
  - *vlan-id*: specifies the ID of the default VLAN to be created for a hybrid interface. The value is an integer ranging from 1 to 4094.

Case1:Configuring Interface-based VLAN Assignment



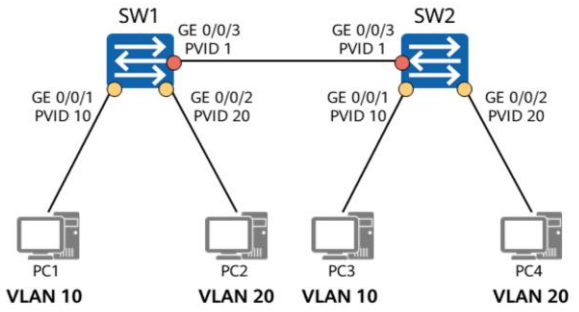
- Networking requirements:
  - On the network shown in the left figure, the switches (SW1 and SW2) of an enterprise are connected to multiple PCs, and PCs with the same services access the network using different devices. To ensure communication security, the enterprise requires that only PCs with the same service can directly communicate.
  - To meet this requirement, configure interface-based VLAN assignment on the switches and add interfaces connected to PCs with the same service to the same VLAN. In this way, PCs in different VLANs cannot directly communicate at Layer 2, but PCs in the same VLAN can directly communicate.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration roadmap:

- Create VLANs and add interfaces connected to PCs to the VLANs to isolate Layer 2 traffic between PCs with different services.
- Configure interface types and specify permitted VLANs for SW1 and SW2 to allow PCs with the same service to communicate through SW1 and SW2.

Creating VLANs



Create VLANs.

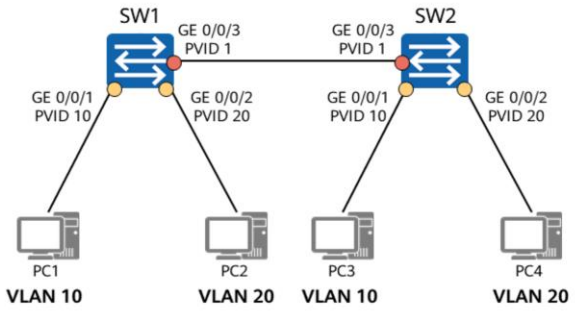
```
[SW1] vlan 10
[SW1-vlan10] quit
[SW1] vlan 20
[SW1-vlan20] quit
```

```
[SW2] vlan batch 10 20
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Configuring Access and Trunk Interfaces



Configure access interfaces and add the interfaces to corresponding VLANs.

```
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 10
```

```
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type access
[SW1] vlan 20
[SW1-vlan20] port GigabitEthernet0/0/2
[SW1-vlan20] quit
```

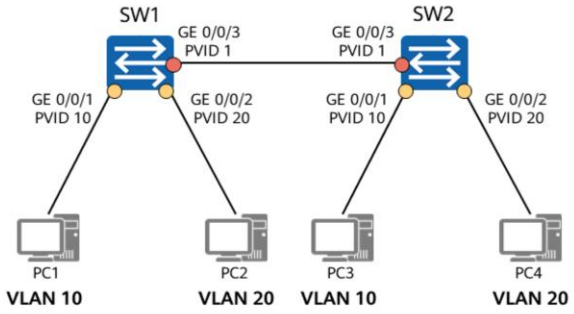
Configure a trunk interface and specify a list of VLAN IDs permitted by the interface.

```
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type trunk
[SW1-GigabitEthernet0/0/3] port trunk pvid vlan 1
[SW1-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
```

Note: The configuration on SW2 is similar to that on SW1.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Verifying the Configuration

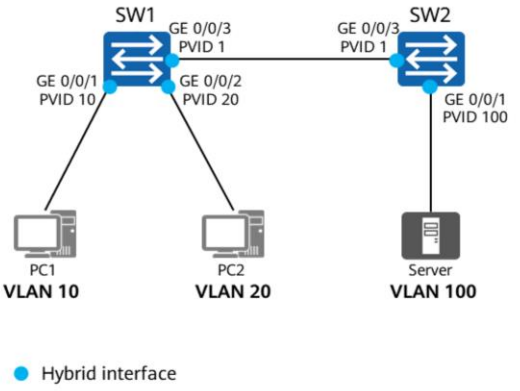



```
[SW1]display vlan
The total number of vlans is : 3
--------------------------------------------------------------------------------
U: Up;          D: Down;                TG: Tagged;  UT: Untagged;
MP: Vlan-mapping;                       ST: Vlan-stacking;
#: ProtocolTransparent-vlan;            *: Management-vlan;
--------------------------------------------------------------------------------
VID         Type        Ports
--------------------------------------------------------------------------------
1           common      UT:GE0/0/3(U)                    .....
10          common      UT:GE0/0/1(U)
                        TG:GE0/0/3(U)
20          common      UT:GE0/0/2(U)
                        TG:GE0/0/3(U)
.....
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Command: The **display vlan** command displays VLAN information.
- Command output:
  - **Tagged/Untagged**: Interfaces are manually added to VLANs in tagged or untagged mode.
  - **VID** or **VLAN ID**: VLAN ID.
  - **Type** or **VLAN Type**: VLAN type. The value **common** indicates a common VLAN.
  - **Ports**: interfaces added to VLANs.

Case2:Configuring Interface-based VLAN Assignment



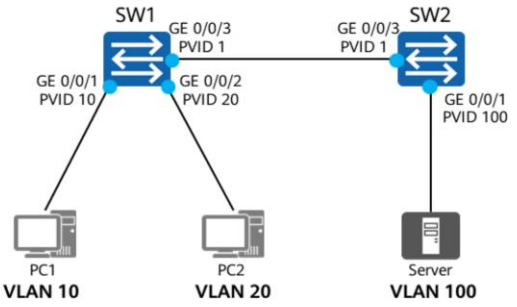
- Networking requirements:
  - On the network shown in the left figure, the switches (SW1 and SW2) of an enterprise are connected to multiple PCs, and PCs in different departments need to access the server of the enterprise. To ensure communication security, the enterprise requires that PCs in different departments cannot directly communicate.
  - To meet this requirement, configure interface-based VLAN assignment and hybrid interfaces on the switches to enable PCs in different departments to access the server but disable them from directly communicating at Layer 2.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Configuration roadmap:
  - Create VLANs and add interfaces connected to PCs to the VLANs to isolate Layer 2 traffic between PCs with different services.
  - Configure interface types and specify permitted VLANs for SW1 and SW2 to allow PCs to communicate with the server through SW1 and SW2.

Configuring Hybrid Interfaces (1)

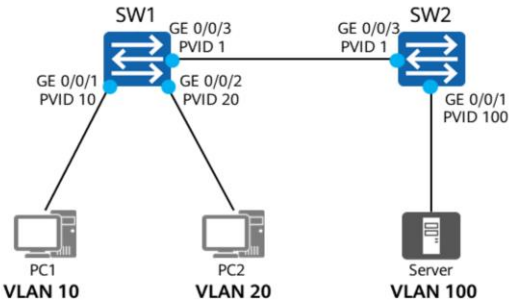


SW1 configuration:

```
[SW1] vlan batch 10 20 100
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type hybrid
[SW1-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[SW1-GigabitEthernet0/0/1] port hybrid untagged vlan 10 100
[SW1-GigabitEthernet0/0/1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type hybrid
[SW1-GigabitEthernet0/0/2] port hybrid pvid vlan 20
[SW1-GigabitEthernet0/0/2] port hybrid untagged vlan 20 100
[SW1-GigabitEthernet0/0/2] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type hybrid
[SW1-GigabitEthernet0/0/3] port hybrid tagged vlan 10 20 100
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuring Hybrid Interfaces (2)

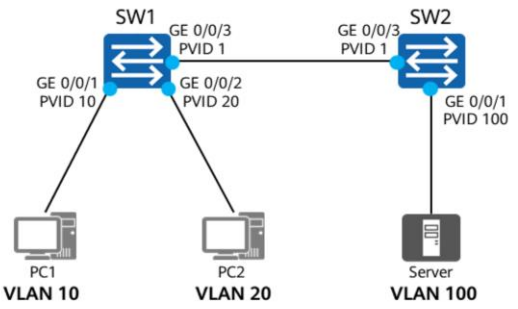


SW2 configuration:

```
[SW2] vlan batch 10 20 100
[SW2] interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1] port link-type hybrid
[SW2-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[SW2-GigabitEthernet0/0/1] port hybrid untagged vlan 10  20 100
[SW2-GigabitEthernet0/0/1] interface GigabitEthernet 0/0/3
[SW2-GigabitEthernet0/0/3] port link-type hybrid
[SW2-GigabitEthernet0/0/3] port hybrid tagged vlan 10 20 100
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Verifying the Configuration




```
[SW1]display vlan
The total number of vlans is : 4
--------------------------------------------------------------------------------
U: Up;         D: Down;                TG: Tagged;  UT: Untagged;
MP: Vlan-mapping;                      ST: Vlan-stacking;
#: ProtocolTransparent-vlan;           *: Management-vlan;
--------------------------------------------------------------------------------
VID         Type        Ports
--------------------------------------------------------------------------------
1           common      UT:GE0/0/1(U)     GE0/0/2(U)     GE0/0/3(U) .....
10          common      UT:GE0/0/1(U)
                        TG:GE0/0/3(U)
20          common      UT:GE0/0/2(U)
                        TG:GE0/0/3(U)
100         common      UT:GE0/0/1(U)     GE0/0/2(U)
                        TG:GE0/0/3(U)
.....
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Basic VLAN Configuration Commands

1. Associate a MAC address with a VLAN.

   [Huawei-vlan10] **mac-vlan mac-address** *mac-address* [*mac-address-mask* | *mac-address-mask-length*]

   This command associates a MAC address with a VLAN.
   - *mac-address*: specifies the MAC address to be associated with a VLAN. The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits, such as 00e0 or fc01. If an H contains less than four digits, the left-most digits are padded with zeros. For example, e0 is displayed as 00e0. The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or any multicast address.
   - *mac-address-mask*: specifies the mask of a MAC address. The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
   - *mac-address-mask-length*: specifies the mask length of a MAC address. The value is an integer ranging from 1 to 48.

2. Enable MAC address-based VLAN assignment on an interface.

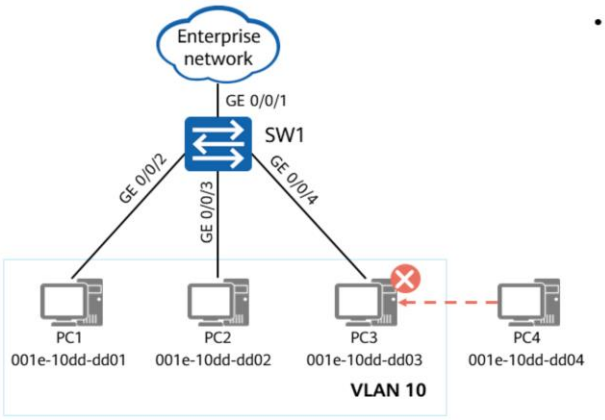
   [Huawei-GigabitEthernet0/0/1] **mac-vlan enable**

   This command enables MAC address-based VLAN assignment on an interface.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Command: **mac-vlan mac-address** *mac-address* [*mac-address-mask* | *mac-address-mask-length*]
  - *mac-address*: specifies the MAC address to be associated with a VLAN.
    - The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits, such as 00e0 or fc01. If an H contains less than four digits, the left-most digits are padded with zeros. For example, e0 is displayed as 00e0.
    - The MAC address cannot be 0000-0000-0000, FFFF-FFFF-FFFF, or any multicast address.
  - *mac-address-mask*: specifies the mask of a MAC address.
    - The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
  - *mac-address-mask-length*: specifies the mask length of a MAC address.
    - The value is an integer ranging from 1 to 48.
- The **mac-vlan enable** command enables MAC address-based VLAN assignment on an interface.

Example for Configuring MAC Address-based VLAN Assignment

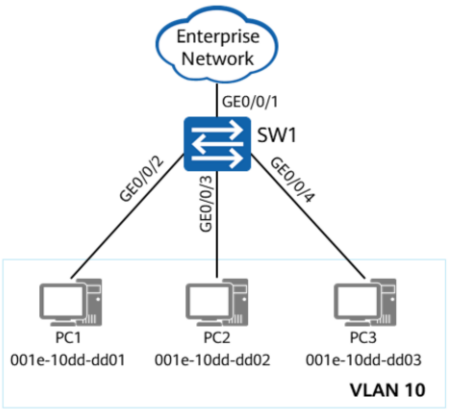


- Networking requirements:
  - The network administrator of an enterprise assigns PCs in the same department to the same VLAN. To improve information security, the enterprise requires that only employees in the department be allowed to access the network resources of the enterprise.
  - PCs 1 through 3 belong to the same department. According to the enterprise' requirement, only the three PCs can access the enterprise network through SW1.
  - To meet this requirement, configure MAC address-based VLAN assignment and associate the MAC addresses of the three PCs with the specified VLAN.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Configuration roadmap:
  - Create a VLAN, for example, VLAN 10.
  - Add Ethernet interfaces on SW1 to the VLAN.
  - Associate the MAC addresses of PCs 1 through 3 with the VLAN.

Creating a VLAN and Associating MAC Addresses with the VLAN



Create a VLAN.

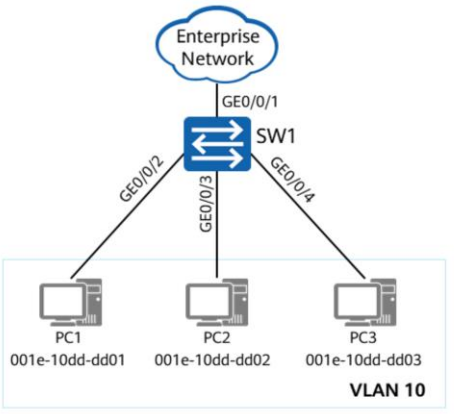
```
[SW1] vlan 10
[SW1-vlan10] quit
```

Associate MAC addresses with the VLAN.

```
[SW1] vlan 10
[SW1-vlan10] mac-vlan mac-address 001e-10dd-dd01
[SW1-vlan10] mac-vlan mac-address 001e-10dd-dd02
[SW1-vlan10] mac-vlan mac-address 001e-10dd-dd03
[SW1-vlan10] quit
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Adding Interfaces to the VLAN and Enabling MAC Address-based VLAN Assignment



Add interfaces to the VLAN.

```
[SW1] interface gigabitethernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type hybrid
[SW1-GigabitEthernet0/0/1] port hybrid tagged vlan 10

[SW1] interface gigabitethernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type hybrid
[SW1-GigabitEthernet0/0/2] port hybrid untagged vlan 10
```

Enable MAC address-based VLAN assignment on the specified interface.

```
[SW1] interface gigabitethernet 0/0/2
[SW1-GigabitEthernet0/0/2] mac-vlan enable
[SW1-GigabitEthernet0/0/2] quit
```

Note: The configuration of GE 0/0/3 and GE 0/0/4 is similar to that of GE 0/0/2.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- On access and trunk interfaces, MAC address-based VLAN assignment can be used only when the MAC address-based VLAN is the same as the PVID. It is recommended that MAC address-based VLAN assignment be configured on hybrid interfaces.



Verifying the Configuration

```
[SW1]display vlan
The total number of vlans is : 2
--------------------------------------------------------------------------------
U: Up;         D: Down;         TG: Tagged;  UT: Untagged;
MP: Vlan-mapping;               ST: Vlan-stacking;
#: ProtocolTransparent-vlan;    *: Management-vlan;
--------------------------------------------------------------------------------
VID        Type        Ports
--------------------------------------------------------------------------------
1          common      UT:GE0/0/1(U)          GE0/0/2(U)  GE0/0/3(U) .....
10         common      UT:GE0/0/2(U)          GE0/0/3(U)  GE0/0/4(U)
                       TG:GE0/0/1(U)
.....
```

```
[SW1]display mac-vlan mac-address all
--------------------------------------------------------------------------------
MAC Address          MASK          VLAN       Priority
--------------------------------------------------------------------------------
001e-10dd-dd01       ffff-ffff-ffff  10       0
001e-10dd-dd02       ffff-ffff-ffff  10       0
001e-10dd-dd03       ffff-ffff-ffff  10       0

Total MAC VLAN address count: 3
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Command: The **display mac-vlan** { **mac-address** { **all** | *mac-address* [*mac-address-mask* | *mac-address-mask-length*] } | **vlan** *vlan-id* } command displays the configuration of MAC address-based VLAN assignment.
  - **all**: displays all VLANs associated with MAC addresses.
  - **mac-address** *mac-address*: displays the VLAN associated with a specified MAC address.
    - The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
  - *mac-address-mask*: specifies the mask of a MAC address.
    - The value is a hexadecimal number in the format of H-H-H. Each H contains one to four digits.
  - *mac-address-mask-length*: specifies the mask length of a MAC address.
    - The value is an integer ranging from 1 to 48.
  - **vlan** *vlan-id*: specifies a VLAN ID.
    - The value is an integer ranging from 1 to 4094.
- Command output:
  - **MAC Address**: MAC address
  - **MASK**: mask of a MAC address
  - **VLAN**: ID of the VLAN associated with a MAC address
  - **Priority**: 802.1p priority of the VLAN associated with a MAC address

Quiz

1. (Multiple) Which of the following statements about the VLAN technology are incorrect? ( )
   A. The VLAN technology can isolate a large collision domain into several small collision domains.
   B. The VLAN technology can isolate a large Layer 2 broadcast domain into several small Layer 2 broadcast domains.
   C. PCs in different VLANs cannot communicate.
   D. PCs in the same VLAN can communicate at Layer 2.
2. If the PVID of a trunk interface is 5 and the port trunk allow-pass vlan 2 3 command is run on the interface, which VLANs' frames can be transmitted through the trunk interface?

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. AC
2. After the **port trunk allow-pass vlan 2 3** command is run, the frames of VLAN 5 cannot be transmitted through the trunk interface. By default, the frames of VLAN 1 can be transmitted through the trunk interface. Therefore, the frames of VLANs 1 through 3 can all be transmitted through the interface.

Summary

- This course describes the VLAN technology, including the functions, identification, assignment, data exchange, planning, application, and basic configuration of VLANs.
- The VLAN technology can divide a physical LAN into multiple broadcast domains so that network devices in the same VLAN can directly communicate at Layer 2, while devices in different VLANs cannot.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



STP Principles and Configuration

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- On an Ethernet switching network, redundant links are used to implement link backup and enhance network reliability. However, the use of redundant links may produce loops, leading to broadcast storms and an unstable MAC address table. As a result, communication on the network may deteriorate or even be interrupted. To prevent loops, IEEE introduced the Spanning Tree Protocol (STP).
- Devices running STP exchange STP Bridge Protocol Data Units (BPDUs) to discover loops on the network and block appropriate ports. This enables a ring topology to be trimmed into a loop-free tree topology, preventing infinite looping of packets and ensuring packet processing capabilities of devices.
- IEEE introduced the Rapid Spanning Tree Protocol (RSTP) to improve the network convergence speed.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

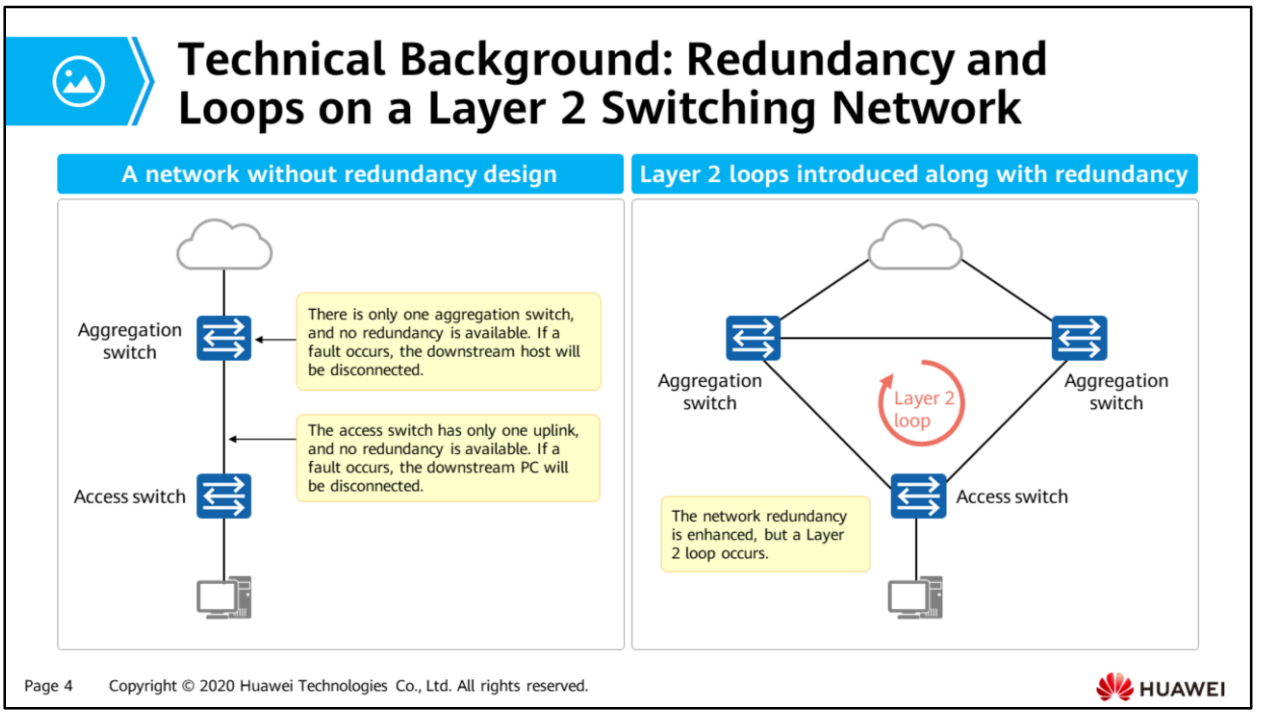
- Upon completion of this course, you will be able to:
  - Describe the causes and problems of Layer 2 loops on a campus switching network.
  - Describe basic concepts and working mechanism of STP.
  - Distinguish STP from RSTP and describe the improvement of RSTP on STP.
  - Complete basic STP configurations.
  - Understand other methods to eliminate Layer 2 loops on the switching network except STP.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

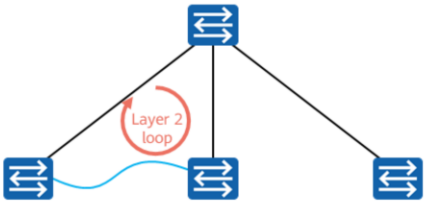
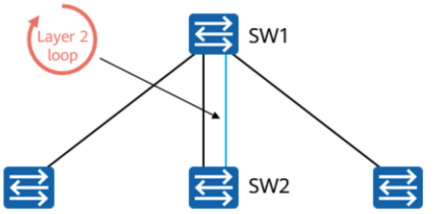
1. **STP Overview**
2. Basic Concepts and Working Mechanism of STP
3. Basic STP Configurations
4. Improvements Made in RSTP
5. STP Advancement

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



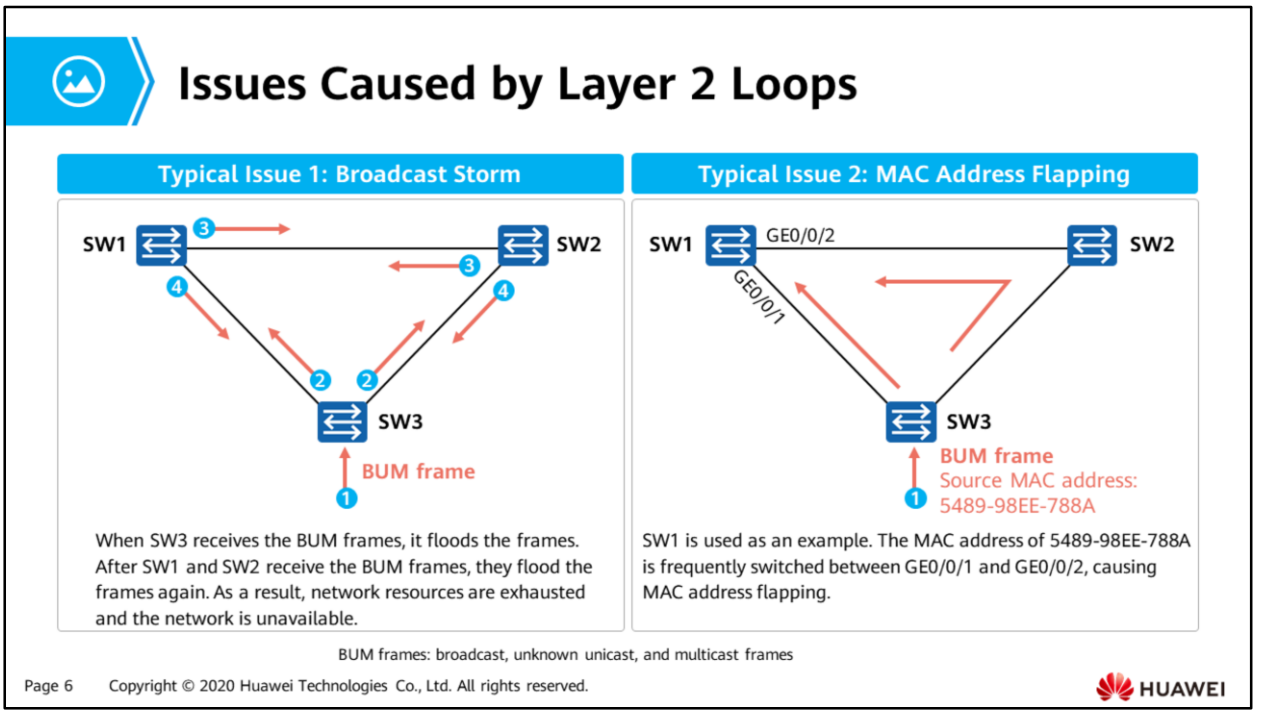
- As LANs increase, more and more switches are used to implement interconnection between hosts. As shown in the figure, the access switch is connected to the upstream device through a single link. If the uplink fails, the host connected to the access switch is disconnected from the network. Another problem is the single point of failure (SPOF). That is, if the switch breaks down, the host connected to the access switch is also disconnected.
- To solve this problem, switches use redundant links to implement backup. Although redundant links improve network reliability, loops may occur. Loops cause many problems, such as communication quality deterioration and communication service interruption.

Technical Background: Layer 2 Loops Caused by Human Errors

Case 1	Case 2
	
Incorrect operations: For example, connections of cables between devices are incorrect.	Incorrect manual configurations: For example, the network administrator does not bind the link between SW1 and SW2 to a logical link (aggregation link), causing Layer 2 loops.

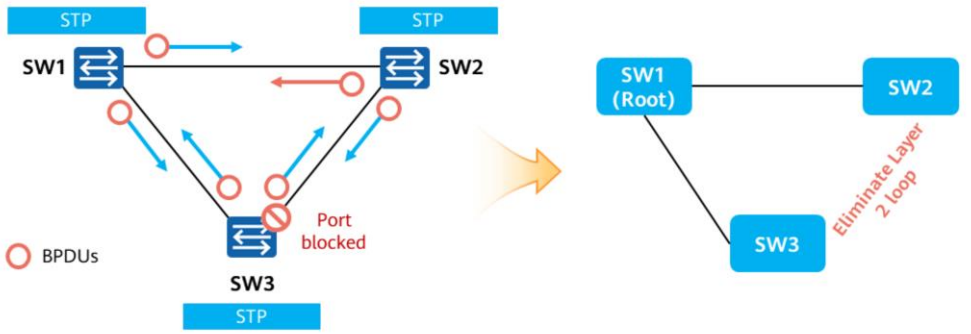
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In practice, redundant links may cause loops, and some loops may be caused by human errors.



- Issue 1: Broadcast storm
  - According to the forwarding principle of switches, if a switch receives a broadcast frame or a unicast frame with an unknown destination MAC address from an interface, the switch forwards the frame to all other interfaces except the source interface. If a loop exists on the switching network, the frame is forwarded infinitely. In this case, a broadcast storm occurs and repeated data frames are flooded on the network.
  - In this example, SW3 receives a broadcast frame and floods it. SW1 and SW2 also forward the frame to all interfaces except the interface that receives the frame. As a result, the frame is forwarded to SW3 again. This process continues, causing a broadcast storm. The switch performance deteriorates rapidly and services are interrupted.
- Issue 2: MAC address flapping
  - A switch generates a MAC address table based on source addresses of received data frames and receive interfaces.
  - In this example, SW1 learns and floods the broadcast frame after receiving it from GE0/0/1, forming the mapping between the MAC address 5489-98EE-788A and GE0/0/1. SW2 learns and floods the received broadcast frame. SW1 receives the broadcast frame with the source MAC address 5489-98EE-788A from GE0/0/2 and learns the MAC address again. Then, the MAC address 5489-98EE-788A is switched between GE0/0/1 and GE0/0/2 repeatedly, causing MAC address flapping.

Introduction to STP

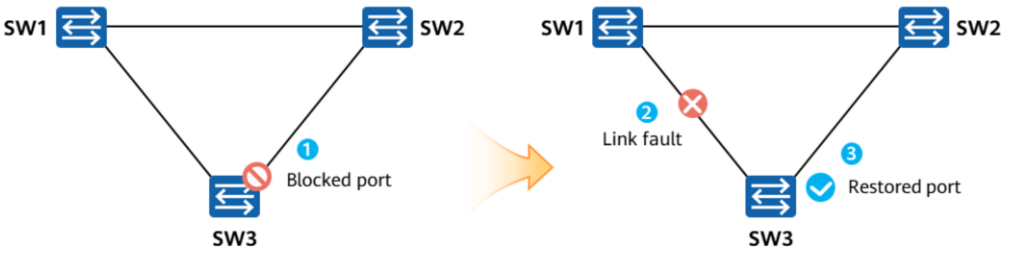


When STP is deployed on a network, switches exchange STP BPDUs and calculate a loop-free topology. Finally, one or more ports on the network are blocked to eliminate loops.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- On an Ethernet network, loops on a Layer 2 network may cause broadcast storms, MAC address flapping, and duplicate data frames. STP is used to prevent loops on a switching network.
- STP constructs a tree to eliminate loops on the switching network.
- The STP algorithm is used to detect loops on the network, block redundant links, and prune the loop network into a loop-free tree network. In this way, proliferation and infinite loops of data frames are avoided on the loop network.

STP Can Dynamically Respond to Network Topology Changes and Adjust Blocked Ports



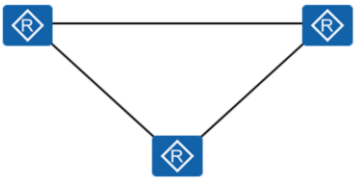
STP running on a switch continuously monitors the network topology. When the network topology changes, STP can detect the changes and automatically adjust the network topology.
Therefore, STP can solve the Layer 2 loop problem and provide a solution for network redundancy.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- As shown in the preceding figure, switches run STP and exchange STP BPDUs to monitor the network topology. Normally, a port on SW3 is blocked to prevent the loop. When the link between SW1 and SW3 is faulty, the blocked port is unblocked and enters the forwarding state.

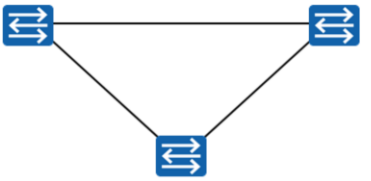
Q&A: Layer 2 and Layer 3 loops

Layer 3 loop



- Common root cause: routing loop
- Dynamic routing protocols have certain loop prevention capabilities.
- The TTL field in the IP packet header can be used to prevent infinite packet forwarding.

Layer 2 loop

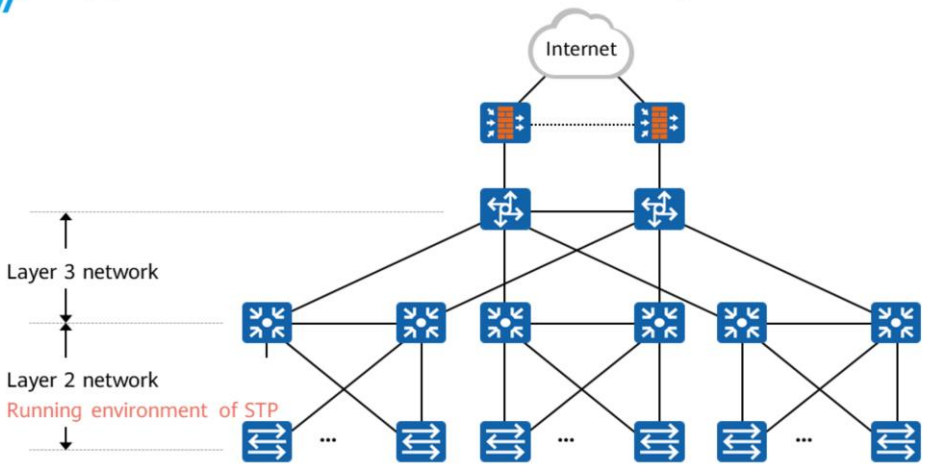


- Common root cause: Layer 2 redundancy is deployed on the network, or cables are incorrectly connected.
- Specific protocols or mechanisms are required to implement Layer 2 loop prevention.
- The Layer 2 frame header does not contain any information to prevent data frames from being forwarded infinitely.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Common loops are classified into Layer 2 and Layer 3 loops.
- Layer 2 loops are caused by Layer 2 redundancy or incorrect cable connections. You can use a specific protocol or mechanism to prevent Layer 2 loops.
- Layer 3 loops are mainly caused by routing loops. Dynamic routing protocols can be used to prevent loops and the TTL field in the IP packet header can be used to prevent packets from being forwarded infinitely.

Application of STP on a Campus Network



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- STP is used on Layer 2 networks of campus networks to implement link backup and eliminate loops.

STP Overview

- STP is used on a LAN to prevent loops.
- Devices running STP exchange information with one another to discover loops on the network, and block certain ports to eliminate loops.
- After running on a network, STP continuously monitors the network status. When the network topology changes, STP can detect the change and automatically respond to the change. In this way, the network status can adapt to the new topology, ensuring network reliability.
- With the growth in scale of LANs, STP has become an important protocol for a LAN.

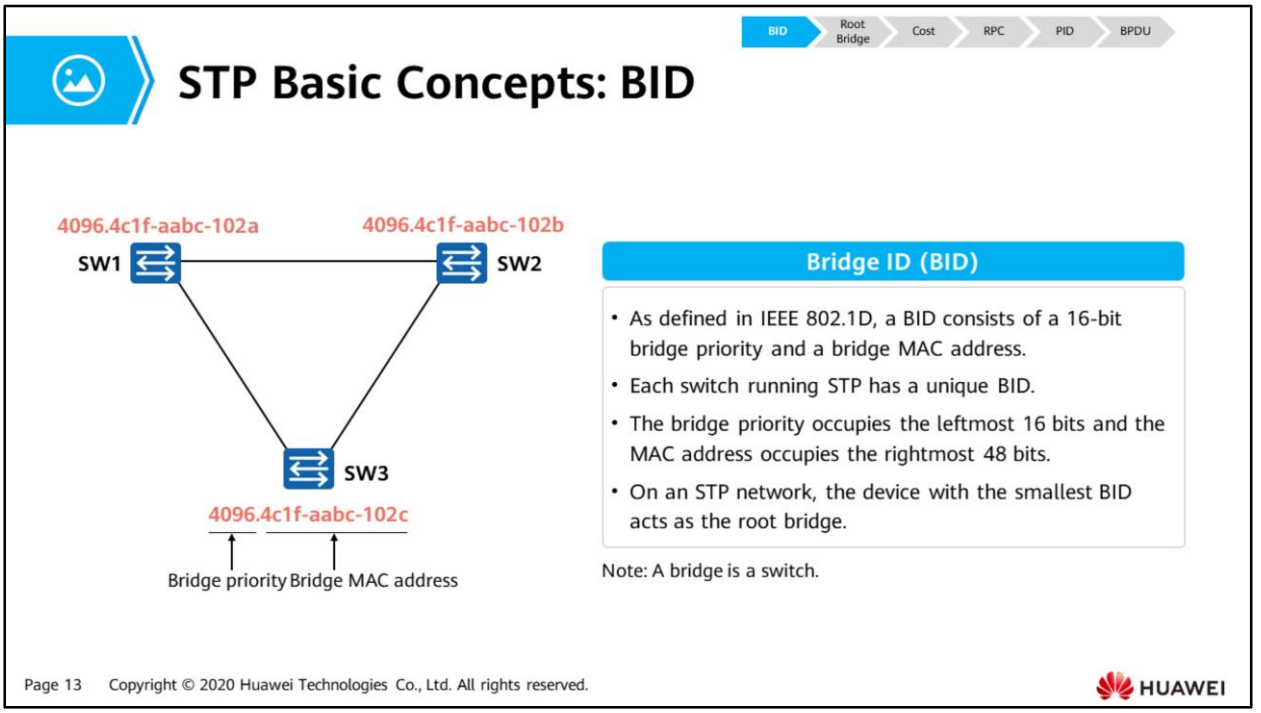
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. STP Overview
2. **Basic Concepts and Working Mechanism of STP**
3. Basic STP Configurations
4. Improvements Made in RSTP
5. STP Advancement

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

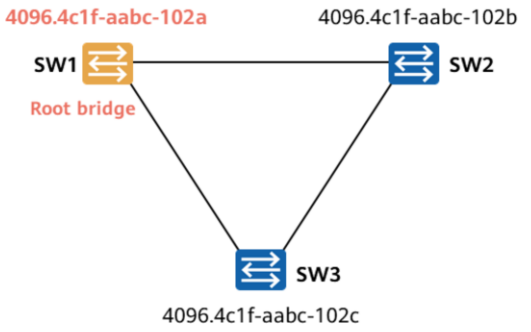
HUAWEI



- In STP, each switch has a bridge ID (BID), which consists of a 16-bit bridge priority and a 48-bit MAC address. On an STP network, the bridge priority is configurable and ranges from 0 to 65535. The default bridge priority is 32768. The bridge priority can be changed but must be a multiple of 4096. The device with the highest priority (a smaller value indicates a higher priority) is selected as the root bridge. If the priorities are the same, devices compare MAC addresses. A smaller MAC address indicates a higher priority.
- As shown in the figure, the root bridge needs to be selected on the network. The three switches first compare bridge priorities. The bridge priorities of the three switches are 4096. Then the three switches compare MAC addresses. The switch with the smallest MAC address is selected as the root bridge.

BID | Root Bridge | Cost | RPC | PID | BPDU

STP Basic Concepts: Root Bridge



Root Bridge

- One of the main functions of STP is to calculate a loop-free STP tree on the entire switching network.
- The root bridge is the root of an STP network.
- After STP starts to work, it elects a root bridge on the switching network. The root bridge is the key for topology calculation of the spanning tree and is the root of the loop-free topology calculated by STP.
- On an STP network, the device with the smallest BID acts as the root bridge.

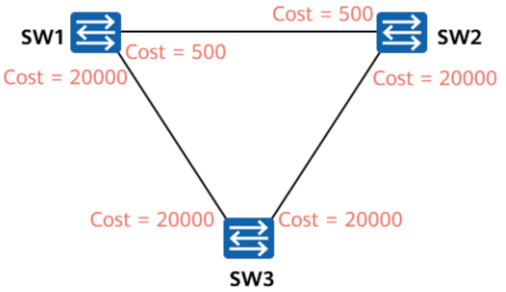
  During BID comparison, devices first compare bridge priorities. A smaller priority value indicates a higher priority of a device. The switch with the smallest priority value becomes the root bridge. If priority values are the same, the switch with the smallest MAC address becomes the root bridge.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- The root bridge functions as the root of a tree network.
- It is the logical center, but not necessarily the physical center, of the network. The root bridge changes dynamically with the network topology.
- After network convergence is completed, the root bridge generates and sends configuration BPDUs to other devices at specific intervals. Other devices process and forward the configuration BPDUs to notify downstream devices of topology changes, ensuring that the network topology is stable.

BID | Root Bridge | Cost | RPC | PID | BPDU

STP Basic Concepts: Cost



Cost

- Each STP-enabled port maintains a cost. The cost of a port is used to calculate the root path cost (RPC), that is, the cost of the path to the root.
- The default cost of a port is related to the rate, working mode, and STP cost calculation method used by a switch.
- A higher port bandwidth indicates a smaller cost.
- You can also run commands to adjust the cost of a port as required.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Each port on a switch has a cost in STP. By default, a higher port bandwidth indicates a smaller port cost.
- Huawei switches support multiple STP path cost calculation standards to provide better compatibility in scenarios where devices from multiple vendors are deployed. By default, Huawei switches use IEEE 802.1t to calculate the path cost.

STP Basic Concepts: Cost Calculation Methods

Port Rate	Port Mode	Recommended STP Cost		
		IEEE 802.1d-1998	IEEE 802.1t	Huawei Legacy Standard
100 Mbit/s	Half-duplex	19	200,000	200
	Full-duplex	18	199,999	199
	Aggregated link: two ports	15	100,000	180
1000 Mbit/s	Full-duplex	4	20,000	20
	Aggregated link: two ports	3	10,000	18
10 Gbit/s	Full-duplex	2	2000	2
	Aggregated link: two ports	1	1000	1
40 Gbit/s	Full-duplex	1	500	1
	Aggregated link: two ports	1	250	1
100 Gbit/s	Full-duplex	1	200	1
	Aggregated link: two ports	1	100	1
...				

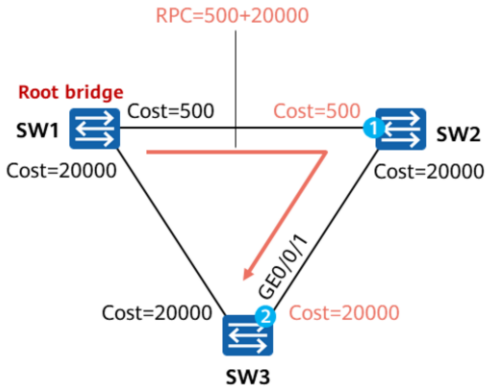
The cost has a default value and is associated with the port rate. When the device uses different algorithms, the same port rate corresponds to different cost values.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

BID | Root Bridge | Cost | RPC | PID | BPDU

STP Basic Concepts: RPC



RPC

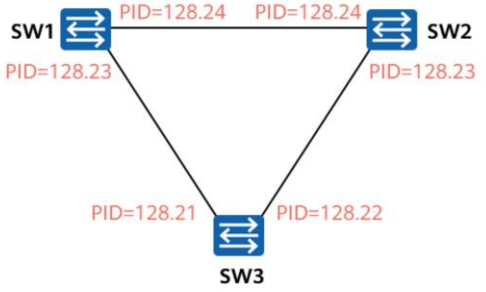
- The cost from a switch port to the root bridge, that is, RPC, is important during STP topology calculation.
- The RPC from a port to the root bridge is the sum of costs of all inbound ports along the path from the root bridge to the device.
- In this example, the RPC for SW3 to reach the root bridge through GE0/0/1 is equal to the cost of port 1 plus the cost of port 2.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- There may be multiple paths from a non-root bridge to the root bridge. Each path has a total cost, which is the sum of all port costs on this path. A non-root bridge compares the costs of multiple paths to select the shortest path to the root bridge. The path cost of the shortest path is called the root path cost (RPC), and a loop-free tree network is generated. The RPC of the root bridge is 0.

BID | Root Bridge | Cost | RPC | PID | BPDU

STP Basic Concepts: PID

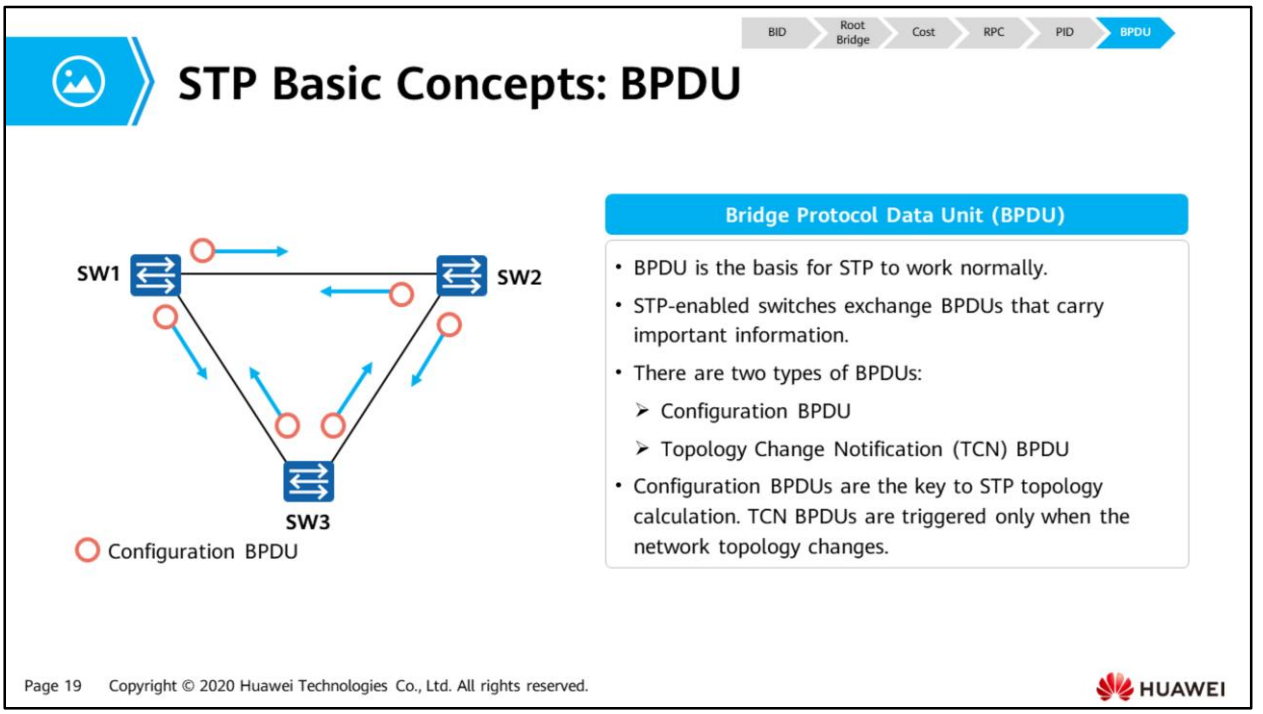


Port ID (PID)

- An STP-enabled switch uses PIDs to identify ports. A PID is used to elect a designated port in a specific scenario.
- A PID consists of the leftmost four bits (port priority) and the rightmost 12 bits (port number).
- An STP-enabled port maintains a default port priority, which is 128 on Huawei switches. You can run a command to change the priority as required.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Each port on an STP-enabled switch has a port ID, which consists of the port priority and port number. The value of the port priority ranges from 0 to 240, with an increment of 16. That is, the value must be an integer multiple of 16. By default, the port priority is 128. The PID is used to determine the port role.



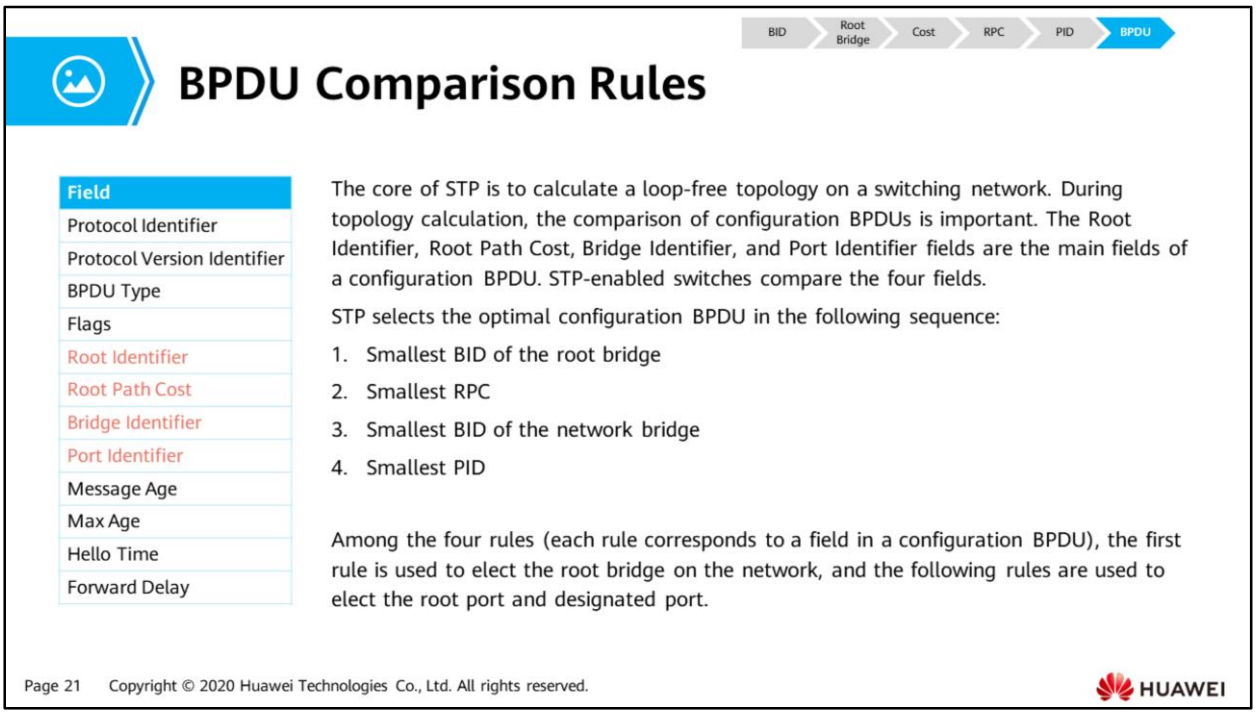
- Switches exchange BPDUs where information and parameters are encapsulated to calculate spanning trees.
- BPDUs are classified into configuration BPDUs and TCN BPDUs.
- A configuration BPDU contains parameters such as the BID, path cost, and PID. STP selects the root bridge by transmitting configuration BPDUs between switches and determines the role and status of each switch port. Each bridge proactively sends configuration BPDUs during initialization. After the network topology becomes stable, only the root bridge proactively sends configuration BPDUs. Other bridges send configuration BPDUs only after receiving configuration BPDUs from upstream devices.
- A TCN BPDU is sent by a downstream switch to an upstream switch when the downstream switch detects a topology change.

Format of Configuration BPDUs



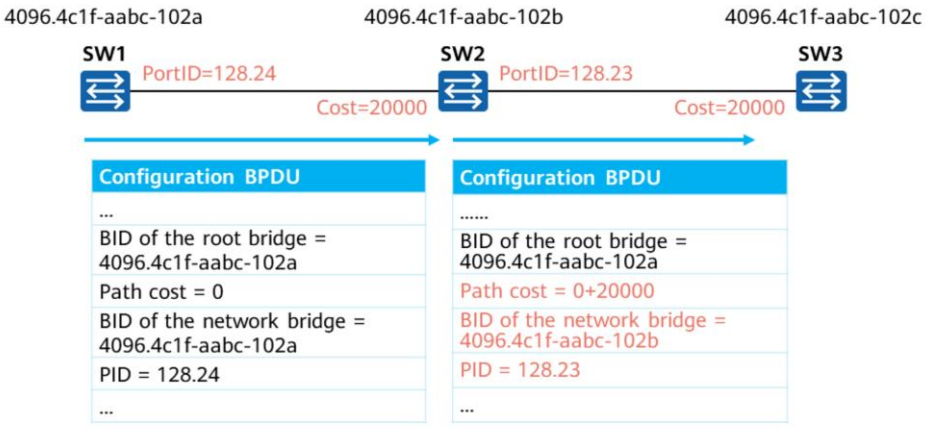
Byte	Field	Description
2	PID	For STP, the value of this field is always 0.
1	PVI	For STP, the value of this field is always 0.
1	BPDU Type	Type of BPDUs. The value 0x00 indicates a configuration BPDU and the value 0x80 indicates a TCN BPDU.
1	Flags	STP uses only the leftmost two bits and the rightmost two bits: Topology Change Acknowledgment (TCA) and Topology Change (TC).
8	Root D	BID of the root bridge.
4	RPC	STP cost of the path from the current port to the root bridge.
8	Bridge ID	BID of the sender.
2	Port ID	ID of the port that sends this BPDU, which consists of the port priority and port number.
2	Message Age	Number of seconds after a BPDU is sent from the root bridge. The value increases by 1 each time the BPDU passes through a network bridge. It refers to the number of hops to the root bridge.
2	Max Age	If the bridge does not receive any BPDU for a period of time and the lifetime of the network bridge reaches the maximum, the network bridge considers that the link connected to the port is faulty. The default value is 20s.
2	Hello Time	Interval at which the root bridge sends configuration BPDUs. The default value is 2s.
2	Forward Delay	Time that is spent in Listening or Learning state. The default value is 15s.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



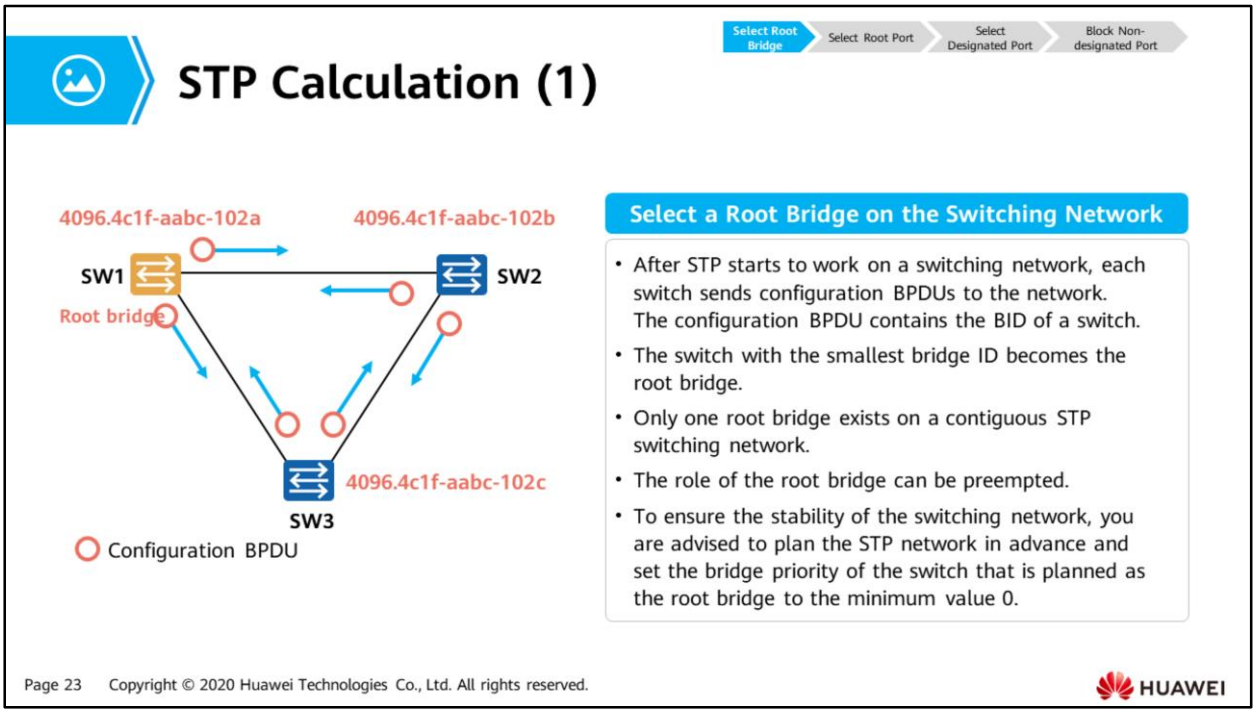
- STP operations:
    1. Selects a root bridge.
    2. Each non-root switch elects a root port.
    3. Select a designated port for each network segment.
    4. Blocks non-root and non-designated ports.
- STP defines three port roles: designated port, root port, and alternate port.
- A designated port is used by a switch to forward configuration BPDUs to the connected network segment. Each network segment has only one designated port. In most cases, each port of the root bridge is a designated port.
- The root port is the port on the non-root bridge that has the optimal path to the root bridge. A switch running STP can have only one root port, but the root bridge does not have any root port.
- If a port is neither a designated port nor a root port, the port is an alternate port. The alternate port is blocked.

Configuration BPDU Forwarding Process



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

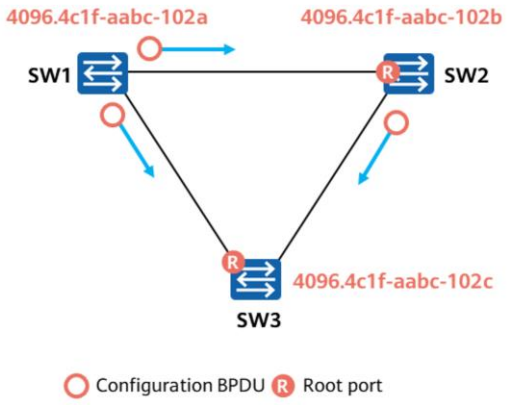
- When a switch starts, it considers itself as the root bridge and sends configuration BPDUs to each other for STP calculation.



- What is a root bridge?
  - The root bridge is the root node of an STP tree.
  - To generate an STP tree, first determine a root bridge.
  - It is the logical center, but not necessarily the physical center, of the network.
  - When the network topology changes, the root bridge may also change. (The role of the root bridge can be preempted.)
- Election process:
  1. When an STP-enabled switch is started, it considers itself as the root bridge and declares itself as the root bridge in the BPDUs sent to other switches. In this case, the BID in the BPDU is the BID of each device.
  2. When a switch receives a BPDU from another device on the network, it compares the BID in the BPDU with its own BID.
  3. Switches exchange BPDUs continuously and compare BIDs. The switch with the smallest BID is selected as the root bridge, and other switches are non-root bridges.
  4. As shown in the figure, the priorities of SW1, SW2, and SW3 are compared first. If the priorities of SW1, SW2, and SW3 are the same, MAC addresses are compared. The BID of SW1 is the smallest, so SW1 is the root bridge, and SW2 and SW3 are non-root bridges.
- Note:
  - The role of the root bridge can be preempted. When a switch with a smaller BID joins the network, the network performs STP calculation again to select a new root bridge.

Select Root Bridge > Select Root Port > Select Designated Port > Block Non-designated Port

STP Calculation (2)



Select a Root Port on Each Non-root Bridge

- Each non-root bridge selects a root port from its ports.
- A non-root bridge has only one root port.
- When a non-root-bridge switch has multiple ports connected to the network, the root port receives the optimal configuration BPDU.
- The root port is located on each non-root bridge and has the shortest distance away from the root bridge.

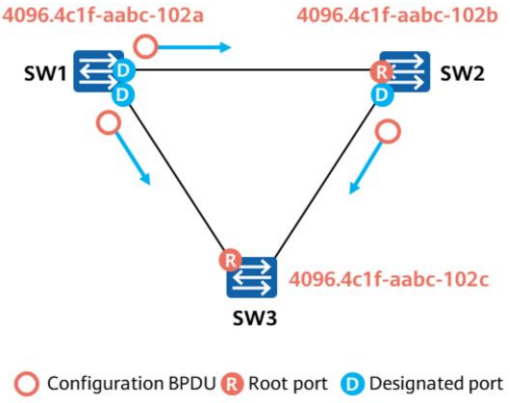
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- What is a root port?
  - A non-root bridge may have multiple ports connected to a network. To ensure that a working path from a non-root bridge to a root bridge is optimal and unique, the root port needs to be determined among ports of the non-root bridge. The root port is used for packet exchange between the non-root bridge and the root bridge.
  - After the root bridge is elected, the root bridge still continuously sends BPDUs, and the non-root bridge continuously receives BPDUs from the root bridge. Therefore, the root port closest to the root bridge is selected on all non-root bridges. After network convergence, the root port continuously receives BPDUs from the root bridge.
  - That is, the root port ensures the unique and optimal working path between the non-root bridge and the root bridge.
- Note: A non-root bridge can have only one root port.

- Election process:
    1. A switch has multiple ports connected to a network. Each port receives a BPDU carrying main fields such as RootID, RPC, BID, and PID. The ports compare these fields.
    2. First, RPCs are compared.STP uses the RPC as an important basis to determine the root port. A smaller RPC indicates a higher priority of selecting the root port. Therefore, the switch selects the port with the smallest RPC as the root port.
    3. When the RPCs are the same, BIDs in the BPDUs received by ports of a switch are compared. A smaller BID indicates a higher priority of electing the root port, so the switch selects the port with the smallest BID as the root port.
    4. When the BIDs are the same, PIDs in the BPDUs received by ports of a switch are compared. A smaller PID indicates a higher priority of electing the root port, so the switch selects the port with the smallest PID as the root port.
    5. When the PIDs are the same, PIDs of ports on the local switch are compared. A smaller PID indicates a higher priority of electing the root port, so the switch selects the port with the smallest PID as the root port.

Select Root Bridge | Select Root Port | Select Designated Port | Block Non-designated Port

STP Calculation (3)

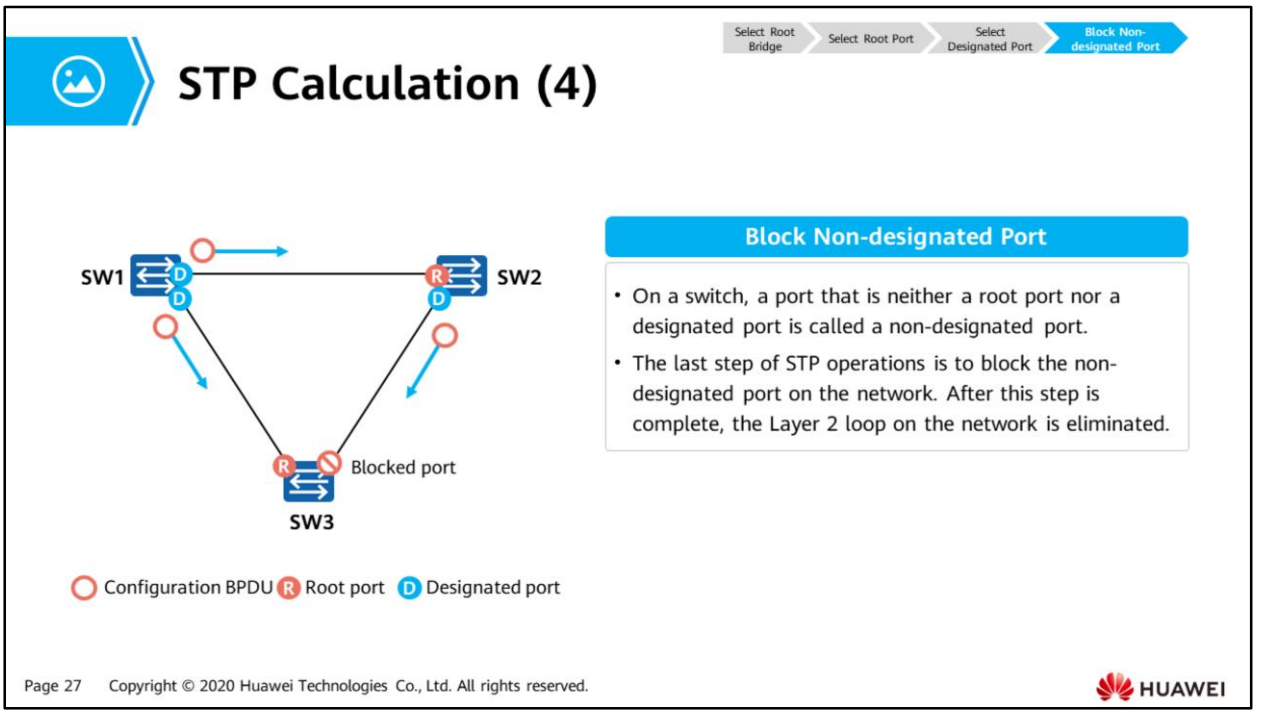


A designated port is elected on each link.

- After the root port is elected, the non-root bridge uses the optimal BPDU received on the port to calculate the configuration BPDU and compares the calculated configuration BPDU with the configuration BPDUs received by all ports except the root port.
  - If the former is better, the port is a designated port.
  - If the latter is better, the port is not a designated port.
- In most cases, all ports on the root bridge are designated ports.

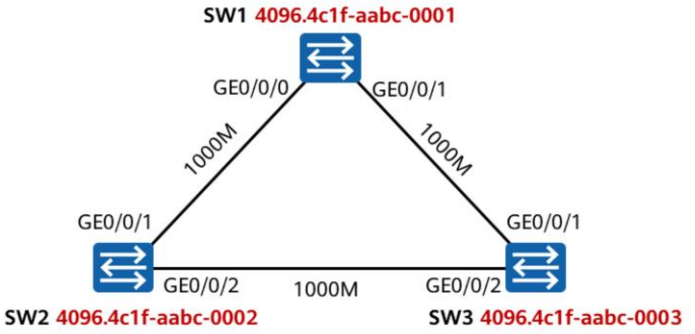
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- What is a designated port?
  - The working path between each link and the root bridge must be unique and optimal. When a link has two or more paths to the root bridge (the link is connected to different switches, or the link is connected to different ports of a switch), the switch (may be more than one) connected to the link must determine a unique designated port.
  - Therefore, a designated port is selected for each link to send BPDUs along the link.
- Note: Generally, the root bridge has only designated ports.
- Election process:
  1. The designated port is also determined by comparing RPCs. The port with the smallest RPC is selected as the designated port. If the RPCs are the same, the BID and PID are compared.
  2. First, RPCs are compared.A smaller value indicates a higher priority of electing the designated port, so the switch selects the port with the smallest RPC as the designated port.
  3. If the RPCs are the same, BIDs of switches at both ends of the link are compared. A smaller BID indicates a higher priority of electing the designated port, so the switch selects the port with the smallest BID as the designated port.
  4. If the BIDs are the same, PIDs of switches at both ends of the link are compared. A smaller PID indicates a higher priority of electing the designated port, so the switch selects the port with the smallest PID as the designated port.



- What is a non-designated port (alternate port)?
  - After the root port and designated port are determined, all the remaining non-root ports and non-designated ports on the switch are called alternate ports.
- Blocking alternate ports
  - STP logically blocks the alternate ports. That is, the ports cannot forward the frames (user data frames) generated and sent by terminal computers.
  - Once the alternate port is logically blocked, the STP tree (loop-free topology) is generated.
- Note:
  - The blocked port can receive and process BPDUs.
  - The root port and designated port can receive and send BPDUs and forward user data frames.

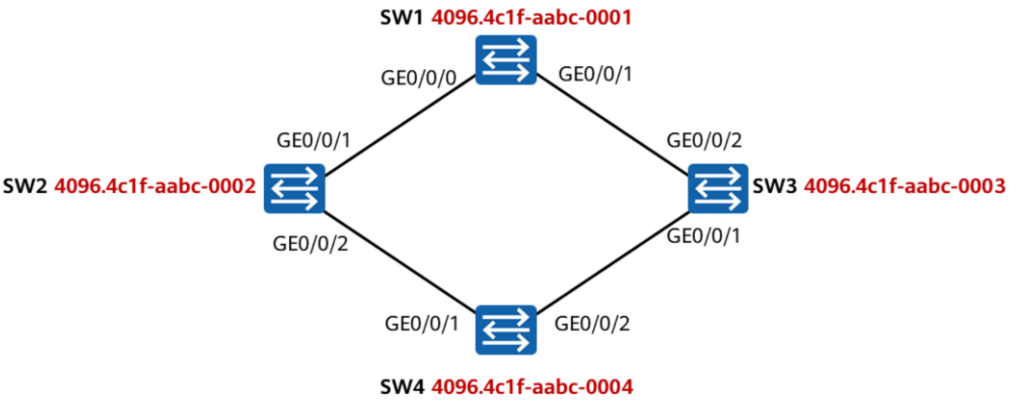
Quiz 1: Identify the Root Bridge and Port Roles



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- As shown in the figure, the root bridge is selected first. If the three switches have the same bridge priority, the switch with the smallest MAC address is selected as the root bridge.
- GE0/0/1 on SW2 is closest to the root bridge and has the smallest RPC, so GE0/0/1 on SW2 is the root port. Similarly, GE0/0/1 on SW3 is also the root port.
- Then designated ports are selected. SW1 is elected as the root bridge, so GE0/0/0 and GE0/0/1 on SW1 are designated ports. GE0/0/2 on SW2 receives configuration BPDUs from SW3 and compares the BIDs of SW2 and SW3. SW2 has a higher BID than SW3, so GE0/0/2 on SW2 is the designated port.
- GE0/0/2 on SW3 is the alternate port.

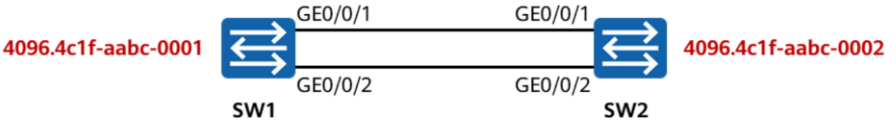
Quiz 2: Identify the Root Bridge and Port Roles in the Following Topology



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- As shown in the figure, the root bridge is selected first. If the four switches have the same bridge priority, the switch with the smallest MAC address is selected as the root bridge.
- GE0/0/1 on SW2 is closest to the root bridge and has the smallest RPC. Therefore, GE0/0/1 on SW2 is the root port. Similarly, GE0/0/2 on SW3 is the root port. The two ports on SW4 have the same RPC. The BID of SW2 connected to GE0/0/1 on SW4 and the BID of SW3 connected to GE0/0/2 on SW4 are compared. The smaller the BID, the higher the priority. Given this, GE0/0/1 on SW4 is selected as the root port.
- Then designated ports are selected. SW1 is elected as the root bridge, so GE0/0/0 and GE0/0/1 on SW1 are designated ports. GE0/0/2 on SW2 receives configuration BPDUs from SW4 and compares the BIDs of SW2 and SW4. SW2 has a higher BID than SW4, so GE0/0/2 on SW2 is the designated port, and GE0/0/1 on SW3 is the designated port.
- GE0/0/2 on SW4 is the alternate port.

Quiz 3: Identify the Root Bridge and Port Roles in the Following Topology



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

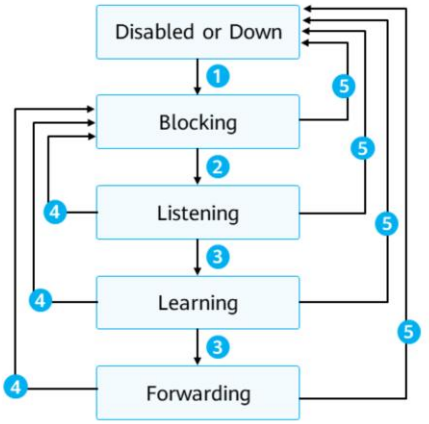
- As shown in the figure, the root bridge is selected first. If the two switches have the same bridge priority, the switch with a smaller MAC address is selected as the root bridge. SW1 is selected as the root bridge.
- Then the root port is selected. The two ports on SW2 have the same RPC and BID. The PIDs of the two ports are compared. The PID of G0/0/1 on SW2 is 128.1, and the PID of G0/0/2 on SW2 is 128.2. The smaller the PID, the higher the priority. Therefore, G0/0/1 of SW2 is the root port.
- SW1 is the root bridge, so GE0/0/1 and GE0/0/2 on SW1 are designated ports.
- GE0/0/2 on SW2 is the alternate port.

STP Port States

Port State	Description
Disabled	The port cannot send or receive BPDUs or service data frames. That is, the port is Down.
Blocking	The port is blocked by STP. A blocked port cannot send BPDUs but listens to BPDUs. In addition, the blocked port cannot send or receive service data frames or learn MAC addresses.
Listening	STP considers the port in Listening state as the root port or designated port, but the port is still in the STP calculation process. In this case, the port can send and receive BPDUs but cannot send or receive service data frames or learn MAC addresses.
Learning	A port in Learning state listens to service data frames but cannot forward them. After receiving service data frames, the port learns MAC addresses.
Forwarding	A port in Forwarding state can send and receive service data frames and process BPDUs. Only the root port or designated port can enter the Forwarding state.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

STP Port State Transition

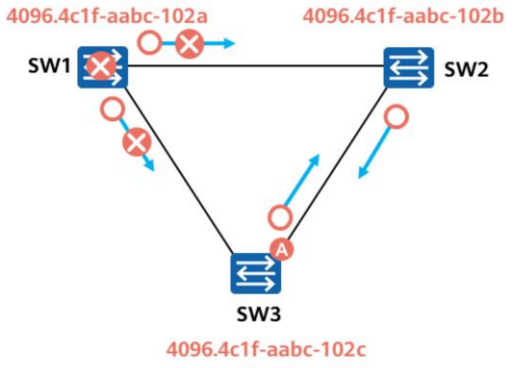


1. When a port is initialized or activated, it automatically enters the blocking state.
2. The port is elected as the root port or designated port and automatically enters the Listening state.
3. The Forward Delay timer expires and the port is still the root port or designated port.
4. The port is no longer the root port or designated port.
5. The port is disabled or the link fails.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- The figure shows the STP port state transition. The STP-enabled device has the following five port states:
- Forwarding: A port can forward user traffic and BPDUs. Only the root port or designated port can enter the Forwarding state.
- Learning: When a port is in Learning state, a device creates MAC address entries based on user traffic received on the port but does not forward user traffic through the port. The Learning state is added to prevent temporary loops.
- Listening: A port in Listening state can forward BPDUs, but cannot forward user traffic.
- Blocking: A port in Blocking state can only receive and process BPDUs, but cannot forward BPDUs or user traffic. The alternate port is in Blocking state.
- Disabled: A port in Disabled state does not forward BPDUs or user traffic.

Topology Change: Root Bridge Fault



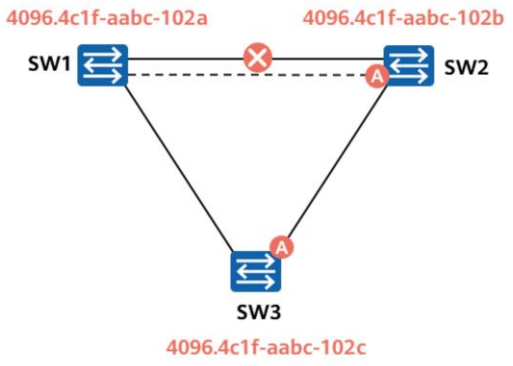
Root Bridge Fault Rectification Process

1. SW1 (root bridge) is faulty and stops sending BPDUs.
2. SW2 waits for the Max Age timer (20s) to expire. In this case, the record about the received BPDUs becomes invalid, and SW2 cannot receive new BPDUs from the root bridge. SW2 learns that the upstream device is faulty.
3. Non-root bridges send configuration BPDUs to each other to elect a new root bridge.
4. After re-election, port A of SW3 transitions to the Forwarding state after two intervals of the Forward Delay timer (the default interval is 15s).
   - A non-root bridge starts root bridge re-election after BPDUs age.
   - Due to the root bridge failure, it takes about 50s to recover from a root bridge failure.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Root bridge fault:
  - On a stable STP network, a non-root bridge periodically receives BPDUs from the root bridge.
  - If the root bridge fails, the downstream switch stops sending BPDUs. As a result, the downstream switch cannot receive BPDUs from the root bridge.
  - If the downstream switch does not receive BPDUs, the Max Age timer (the default value is 20s) expires. As a result, the record about the received BPDUs becomes invalid. In this case, the non-root bridges send configuration BPDUs to each other to elect a new root bridge.
- Port state:
  - The alternate port of SW3 enters the Listening state from the Blocking state after 20s and then enters the Learning state. Finally, the port enters the Forwarding state to forward user traffic.
- Convergence time:
  - It takes about 50s to recover from a root bridge failure, which is equal to the value of the Max Age timer plus twice the value of the Forward Delay timer.

Topology Change: Direct Link Fault



Direct Link Fault Rectification Process

On a stable network, when SW2 detects that the link of the root port is faulty, the alternate port of SW2 enters the Forwarding state after twice the value of the Forward Delay timer (the default value is 15s).

- After SW2 detects a fault on the direct link, it switches the alternate port to the root port.
- If a direct link fails, the alternate port restores to the Forwarding state after 30s.

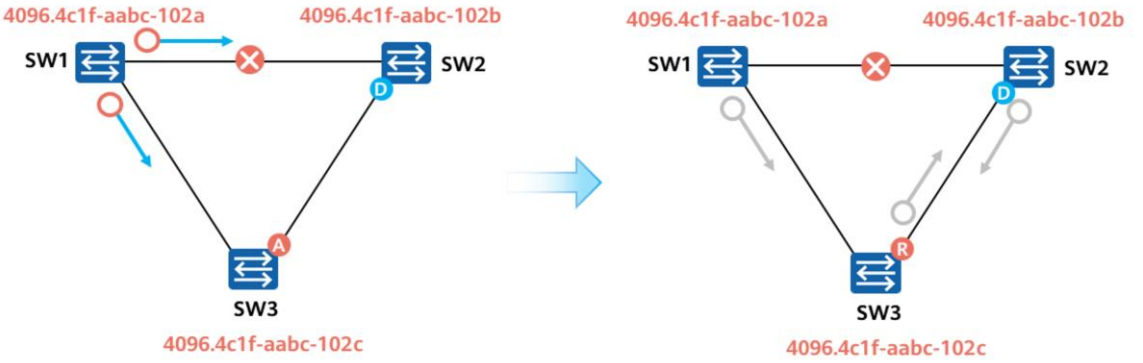
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Direct link fault:
  - When two switches are connected through two links, one is the active link and the other is the standby link.
  - When the network is stable, SW2 detects that the link of the root port is faulty, and the alternate port enters the Forwarding state.
- Port state:
  - The alternate port transitions from the Blocking state to the Listening, Learning, Forwarding states in sequence.
- Convergence speed:
  - If a direct link fails, the alternate port restores to the Forwarding state after 30s.

Topology Change: Indirect Link Fault

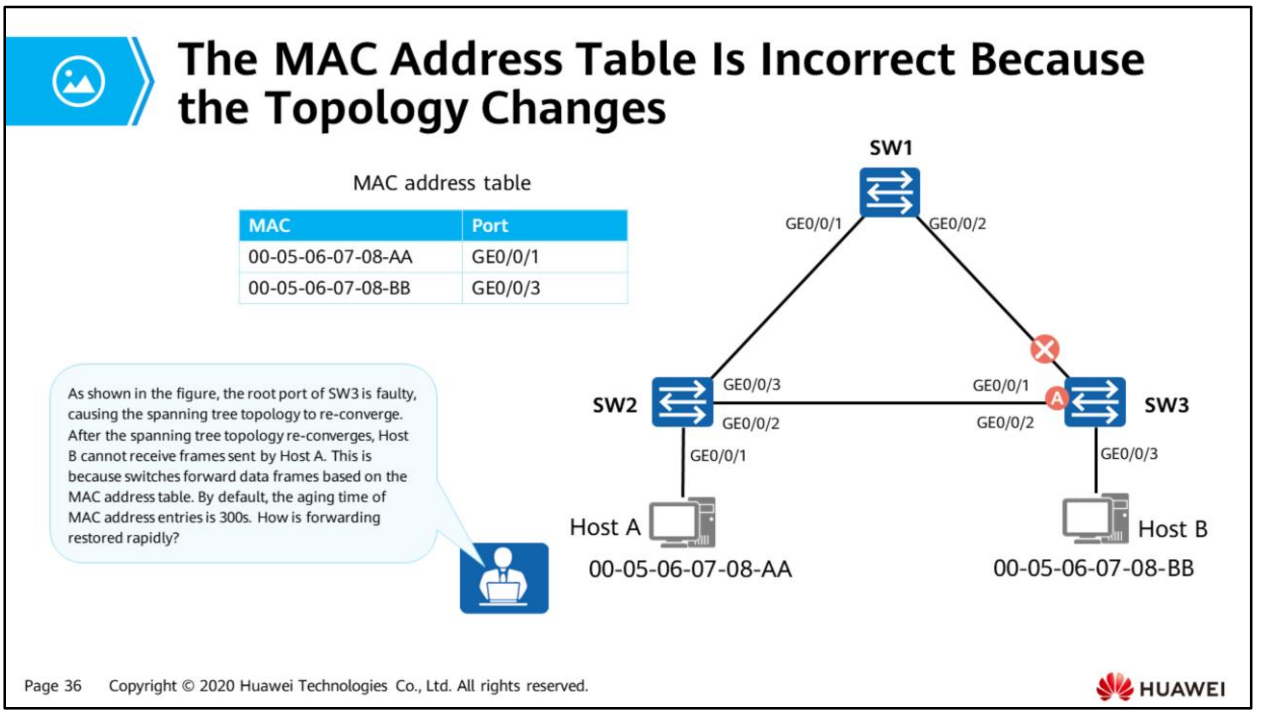
- When the indirect link fails, the alternate port on SW3 restores to the Forwarding state. It takes about 50s to recover from an indirect link failure.



Page 35 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Indirect link fault:
  - On a stable STP network, a non-root bridge periodically receives BPDUs from the root bridge.
  - If the link between SW1 and SW2 is faulty (not a physical fault), SW2 cannot receive BPDUs from SW1. The Max Age timer (the default value is 20s) expires. As a result, the record about the received BPDUs becomes invalid.
  - In this case, the non-root bridge SW2 considers that the root bridge fails and considers itself as the root bridge. Then SW2 sends its own configuration BPDU to SW3 to notify SW3 that it is the new root bridge.
  - During this period, the alternate port of SW3 does not receive any BPDU that contains the root bridge ID. After the Max Age timer expires, the port enters the Listening state and starts to forward the BPDU that contains the root bridge ID from the upstream device to SW2.
  - After the Max Age timer expires, SW2 and SW3 receive BPDUs from each other almost at the same time and perform STP recalculation. SW2 finds that the BPDU sent by SW3 is superior, so it does not declare itself as the root bridge and re-determines the port role.
- Port state:
  - The alternate port of SW3 enters the Listening state from the Blocking state after 20s and then enters the Learning state. Finally, the port enters the Forwarding state to forward user traffic.
- Convergence time:
  - It takes about 50s to recover from an indirect link failure, which is equal to the value of the Max Age timer plus twice the value of the Forward Delay timer.



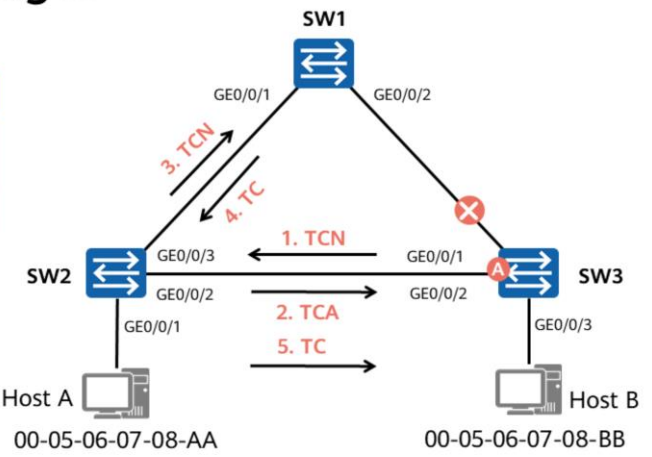
- On a switching network, a switch forwards data frames based on the MAC address table. By default, the aging time of MAC address entries is 300 seconds. If the spanning tree topology changes, the forwarding path of the switch also changes. In this case, the entries that are not aged in a timely manner in the MAC address table may cause data forwarding errors. Therefore, the switch needs to update the MAC address entries in a timely manner after the topology changes.
- In this example, the MAC address entry on SW2 defines that packets can reach Host A through GE0/0/1 and reach Host B through GE0/0/3. The root port of SW3 is faulty, causing the spanning tree topology to re-converge. After the spanning tree topology re-converges, Host B cannot receive frames sent by Host A. This is because the aging time of MAC address entries is 300s. After a frame sent from Host A to Host B reaches SW2, SW2 forwards the frame through GE0/0/3.

The MAC Address Table Is Incorrect Because the Topology Changes

MAC address table

MAC	Port
00-05-06-07-08-AA	GE0/0/3
00-05-06-07-08-BB	GE0/0/1
00-05-06-07-08-BB	GE0/0/2

- TCN BPDUs are generated when the network topology changes.
- Packet format: protocol identifier, version number, and type
- Topology change: The TCA and TC bits in the Flags field of configuration BPDUs are used.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- When the network topology changes, the root bridge sends TCN BPDUs to notify other devices of the topology change. The root bridge generates TCs to instruct other switches to age existing MAC address entries.
- The process of topology change and MAC address entry update is as follows:
    1. After SW3 detects the network topology change, it continuously sends TCN BPDUs to SWB.
    2. After SW2 receives the TCN BPDUs from SW3, it sets the TCA bit in the Flags field of the BPDUs to 1 and sends the BPDUs to SW3, instructing SW3 to stop sending TCN BPDUs.
    3. SW2 forwards the TCN BPDUs to the root bridge.
    4. SW1 sets the TC bit in the Flags field of the configuration BPDU to 1 and sends the configuration BPDU to instruct the downstream device to change the aging time of MAC address entries from 300s to the value of the Forward Delay timer (15s by default).
    5. The incorrect MAC address entries on SW2 are automatically deleted after 15s at most. Then, SW2 starts to learn MAC address entries again and forwards packets based on the learned MAC address entries.

Contents

1. STP Overview
2. Basic Concepts and Working Mechanism of STP
3. **Basic STP Configurations**
4. Improvements Made in RSTP
5. STP Advancement

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic STP Configuration Commands (1)

1. Configure a working mode.

   [Huawei] **stp mode** { **stp** | **rstp** | **mstp** }

   The switch supports three working modes: STP, RSTP, and Multiple Spanning Tree Protocol (MSTP). By default, a switch works in MSTP mode. On a ring network running only STP, the working mode of a switch is configured as STP; on a ring network running RSTP, the working mode of a switch is configured as RSTP.

2. (Optional) Configure the root bridge.

   [Huawei] **stp root primary**

   Configure the switch as the root bridge. By default, a switch does not function as the root bridge of any spanning tree. After you run this command, the priority value of the switch is set to 0 and cannot be changed.

3. (Optional) Configure the switch as the secondary root bridge.

   [Huawei] **stp root secondary**

   Configure the switch as the secondary root bridge. By default, a switch does not function as the secondary root bridge of any spanning tree. After you run this command, the priority value of the switch is set to 4096 and cannot be changed.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic STP Configuration Commands (2)

1. (Optional) Configure the STP priority of a switch.

   [Huawei] **stp priority** *priority*

   By default, the priority value of a switch is 32768.

2. (Optional) Configure a path cost for a port.

   [Huawei] **stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }

   Configure a path cost calculation method. By default, the IEEE 802.1t standard (**dot1t**) is used to calculate path costs.
   All switches on a network must use the same path cost calculation method.

   [Huawei-GigabitEthernet0/0/1] **stp cost** *cost*

   Set the path cost of the port.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic STP Configuration Commands (3)

1. (Optional) Configure a priority for a port.

   [Huawei-GigabitEthernet0/0/1] **stp priority** *priority*

   Configure a priority for a port. By default, the priority of a switch port is 128.

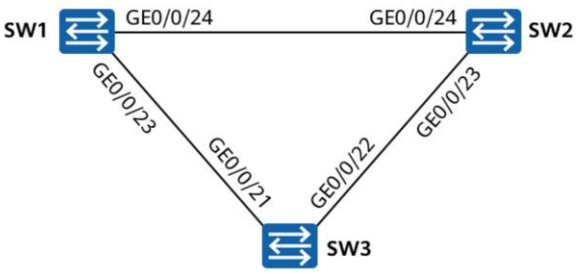
2. Enable STP, RSTP, or MSTP.

   [Huawei] **stp enable**

   Enable STP, RSTP, or MSTP on a switch. By default, STP, RSTP, or MSTP is enabled on a switch.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case 1: Basic STP Configurations



- Deploy STP on the three switches to eliminate Layer 2 loops on the network.
- Configure SW1 as the root bridge and block GE0/0/22 on SW3.

SW1 configuration:

```
[SW1] stp mode stp
[SW1] stp enable
[SW1] stp priority 0
```

SW2 configuration:

```
[SW2] stp mode stp
[SW2] stp enable
[SW2] stp priority 4096
```

SW3 configuration:

```
[SW3] stp mode stp
[SW3] stp enable
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case 1: Basic STP Configurations

Check brief information about STP states of ports on SW3.

<SW3> **display stp brief**

MSTID	Port	Role	STP State	Protection
0	GigabitEthernet0/0/21	ROOT	FORWARDING	NONE
0	GigabitEthernet0/0/22	ALTE	DISCARDING	NONE

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. STP Overview
2. Basic Concepts and Working Mechanism of STP
3. Basic STP Configurations
4. **Improvements Made in RSTP**
5. STP Advancement

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Disadvantages of STP

- STP ensures a loop-free network but is slow to converge, leading to service quality deterioration. If the network topology changes frequently, connections on the STP network are frequently torn down, causing frequent service interruption.
- STP does not differentiate between port roles according to their states, making it difficult for less experienced administrators to learn about and deploy this protocol.
  - Ports in Listening, Learning, and Blocking states are the same for users because none of these ports forwards service traffic.
  - In terms of port use and configuration, the essential differences between ports lie in the port roles but not port states.
  - Both root and designated ports can be in Listening state or Forwarding state, so the port roles cannot be differentiated according to their states.
- The STP algorithm does not determine topology changes until the timer expires, delaying network convergence.
- The STP algorithm requires the root bridge to send configuration BPDUs after the network topology becomes stable, and other devices process and spread the configuration BPDUs through the entire network. This also delays convergence.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



RSTP Overview

- RSTP defined in IEEE 802.1w is an enhancement to STP. RSTP optimizes STP in many aspects, provides faster convergence, and is compatible with STP.
- RSTP introduces new port roles. When the root port fails, the switch can enable the alternate port to obtain an alternate path from the designated bridge to the root bridge. RSTP defines three states for a port based on whether the port forwards user traffic and learns MAC addresses. In addition, RSTP introduces the edge port. The port connecting a switch to a terminal is configured as an edge port that enters the Forwarding state immediately after initialization, thus improving the working efficiency.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- The IEEE 802.1w standard released in 2001 defines RSTP. RSTP is an improvement on STP and implements fast network topology convergence.
- RSTP is evolved from STP and has the same working mechanism as STP. When the topology of a switching network changes, RSTP can use the Proposal/Agreement mechanism to quickly restore network connectivity.
- RSTP removes three port states, defines two new port roles, and distinguishes port attributes based on port states and roles. In addition, RSTP provides enhanced features and protection measures to ensure network stability and fast convergence.
- RSTP is backward compatible with STP, which is not recommended because STP slow convergence is exposed.
- Improvements made in RSTP:
  - RSTP processes configuration BPDUs differently from STP.
    - When the topology becomes stable, the mode of sending configuration BPDUs is optimized.
    - RSTP uses a shorter timeout interval of BPDUs.
    - RSTP optimizes the method of processing inferior BPDUs.
  - RSTP changes the configuration BPDU format and uses the Flags field to describe port roles.
  - RSTP topology change processing: Compared with STP, RSTP is optimized to accelerate the response to topology changes.

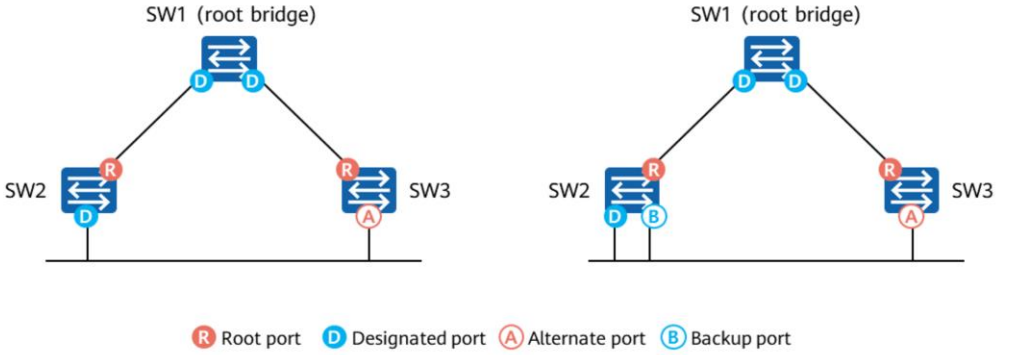
Improvements Made in RSTP

- RSTP processes configuration BPDUs differently from STP.
  - When the topology becomes stable, the mode of sending configuration BPDUs is optimized.
  - RSTP uses a shorter timeout interval of BPDUs.
  - RSTP optimizes the method of processing inferior BPDUs.
- RSTP changes the configuration BPDU format and uses the Flags field to describe port roles.
- RSTP topology change processing: Compared with STP, RSTP is optimized to accelerate the response to topology changes.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Port Roles in RSTP

- RSTP adds port roles to help understand RSTP and simplify RSTP deployment.



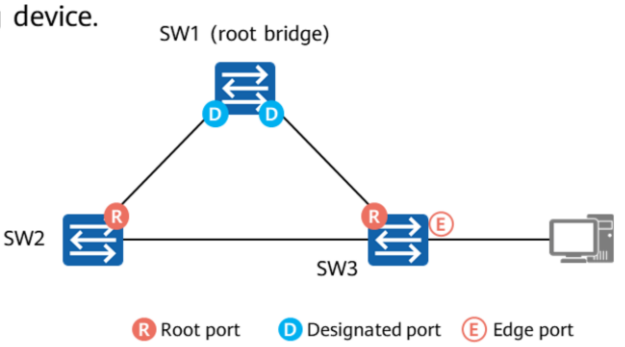
RSTP defines four port roles: root port, designated port, alternate port, and backup port.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- From the perspective of configuration BPDU transmission:
  - An alternate port is blocked after learning a configuration BPDU sent from another network bridge.
  - A backup port is blocked after learning a configuration BPDU sent from itself.
- From the perspective of user traffic:
  - An alternate port acts as a backup of the root port and provides an alternate path from the designated bridge to the root bridge.
  - A backup port backs up a designated port and provides a backup path from the root bridge to the related network segment.

Edge Port

- An edge port is located at the edge of a region and does not connect to any switching device.



Generally, an edge port is directly connected to a user terminal. The edge port can transition from the Disabled state to the Forwarding state.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- In STP, it takes 15 seconds for the port of a switch connected to a user terminal to transition from Disabled to Forwarding. During this period, the user terminal cannot access the Internet. If the network changes frequently, the Internet access status of the user terminal is unstable.
- An edge port is directly connected to a user terminal and is not connected to any switching device. An edge port does not receive or process configuration BPDUs and does not participate in RSTP calculation. It can transition from Disabled to Forwarding without any delay. An edge port becomes a common STP port once it receives a configuration BPDU. The spanning tree needs to be recalculated, which leads to network flapping.

Port States in RSTP

- RSTP deletes two port states defined in STP, reducing the number of port states to three.
  - If the port does not forward user traffic or learn MAC addresses, it is in Discarding state.
  - If the port does not forward user traffic but learns MAC addresses, it is in Learning state.
  - If the port forwards user traffic and learns MAC addresses, it is in Forwarding state.

STP Port State	RSTP Port State	Port Role
Forwarding	Forwarding	Root port or designated port
Learning	Learning	Root port or designated port
Listening	Discarding	Root port or designated port
Blocking	Discarding	Alternate port or backup port
Disabled	Discarding	Disabled port

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- RSTP deletes two port states defined in STP, reducing the number of port states to three.
  1. A port in Discarding state does not forward user traffic or learn MAC addresses.
  2. A port in Learning state does not forward user traffic but learns MAC addresses.
  3. A port in Forwarding state forwards user traffic and learns MAC addresses.

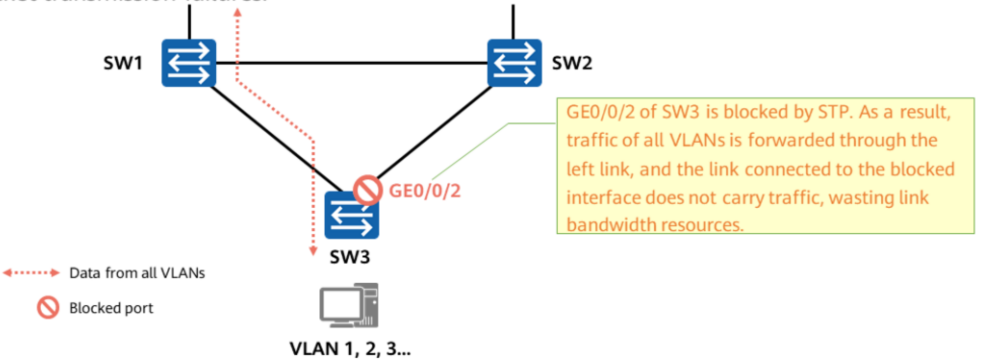
Contents

1. STP Overview
2. Basic Concepts and Working Mechanism of STP
3. Basic STP Configurations
4. Improvements Made in RSTP
5. **STP Advancement**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Defects of STP/RSTP: All VLANs Share One Spanning Tree

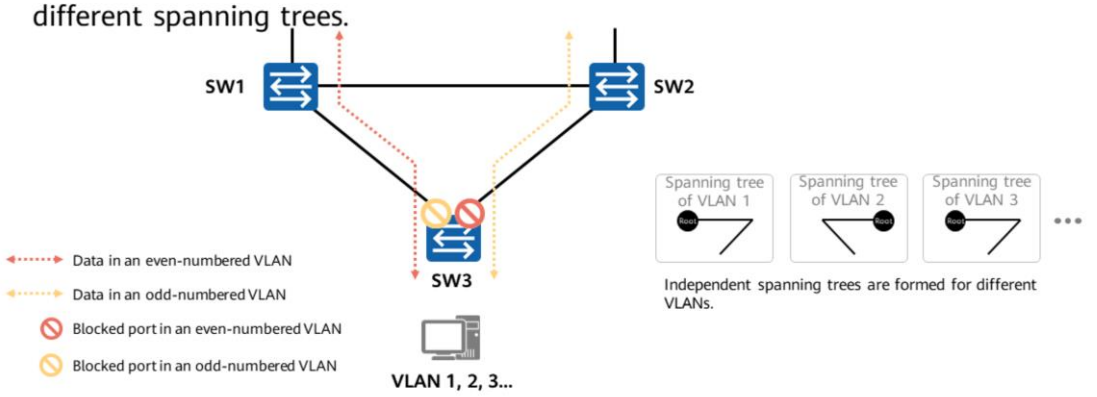
- RSTP, an enhancement to STP, allows for fast network topology convergence.
- STP and RSTP both have a defect: All VLANs on a LAN share one spanning tree. As a result, inter-VLAN load balancing cannot be performed, and blocked links cannot transmit any traffic, which may lead to VLAN packet transmission failures.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

VBST

- Huawei provides the VLAN-based Spanning Tree (VBST). VBST constructs a spanning tree in each VLAN so that traffic from different VLANs is load balanced along different spanning trees.

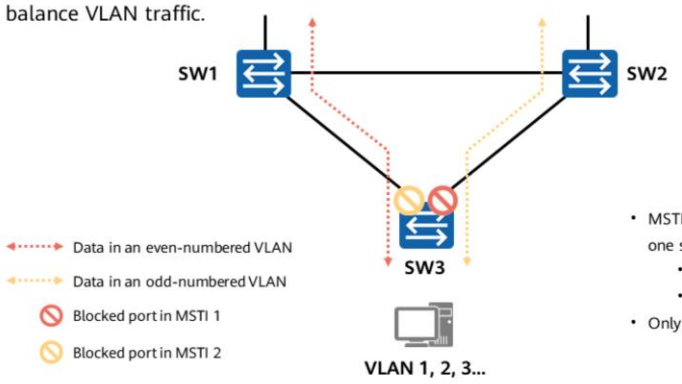


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- VBST brings in the following benefits:
  - Eliminates loops.
  - Implements link multiplexing and load balancing, and therefore improves link use efficiency.
  - Reduces configuration and maintenance costs.
- If a great number of VLANs exist on a network, spanning tree computation for each VPN consumes a huge number of switch processor resources.

MSTP

- To fix the defects, the IEEE released the 802.1s standard that defines the Multiple Spanning Tree Protocol (MSTP) in 2002.
- MSTP is compatible with STP and RSTP, and can rapidly converge traffic and provides multiple paths to load balance VLAN traffic.





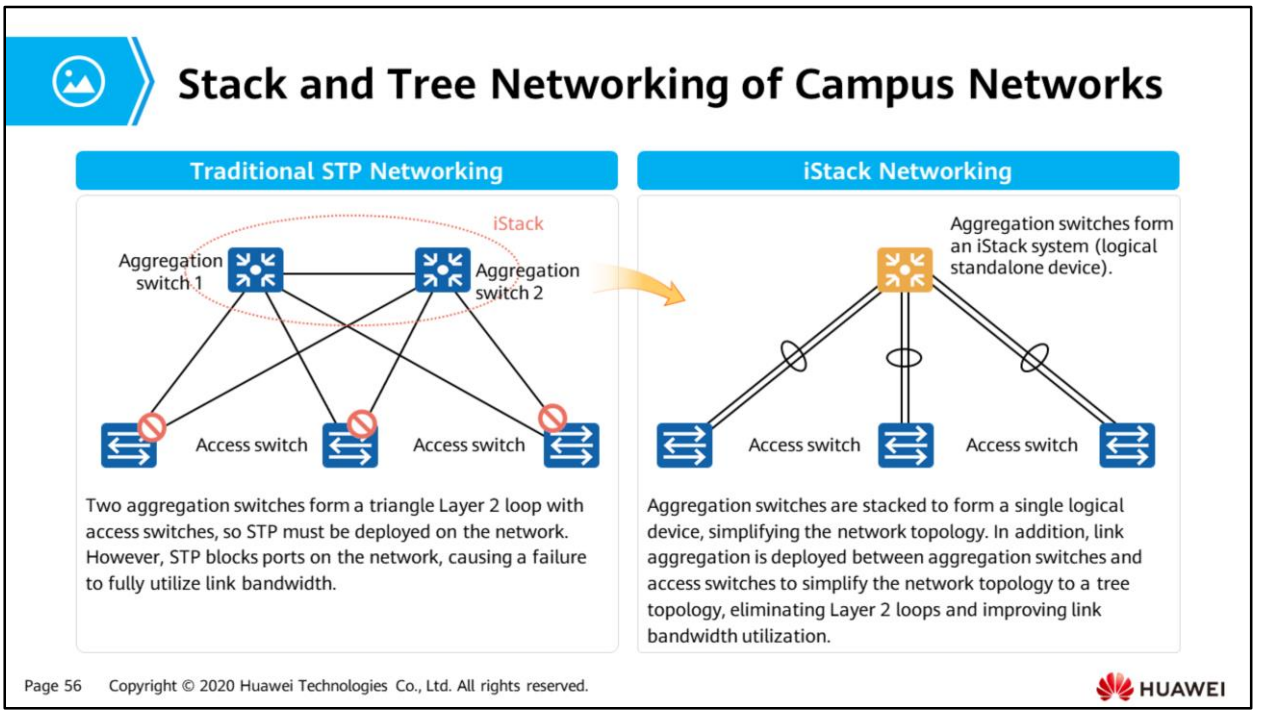
- MSTP maps VLANs to an MSTI. Multiple VLANs can share one spanning tree. For example:
  - Even-numbered VLANs are mapped to MSTI 1.
  - Odd-numbered VLANs are mapped to MSTI 2.
- Only two spanning trees are maintained on the network.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

MSTP Overview

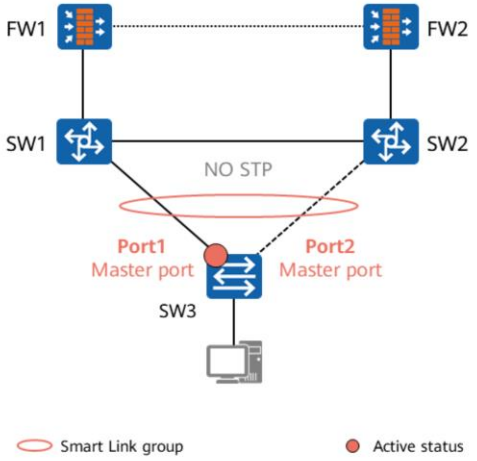
- MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other.
- Each spanning tree is called a multiple spanning tree instance (MSTI).
- An MSTI is the spanning tree corresponding to a set of VLANs.
- Binding multiple VLANs to a single MSTI reduces communication costs and resource usage.
- The topology of each MSTI is calculated independently, and traffic can be balanced among MSTIs.
- Multiple VLANs with the same topology can be mapped to a single MSTI. The forwarding state of the VLANs for an interface is determined by the interface state in the MSTI.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Intelligent Stack (iStack) enables multiple iStack-capable switches to function as a logical device.
- Before an iStack system is set up, each switch is an independent entity and has its own IP address and MAC address. You need to manage the switches separately. After an iStack system is set up, switches in the iStack system form a logical entity and can be managed and maintained using a single IP address. iStack technology improves forwarding performance and network reliability, and simplifies network management.

Smart Link



Smart Link is tailored for dual-uplink networking.

- Smart Link is deployed on two switches where a host is dual-homed. When the network is normal, one of the two uplinks is active, and the other is in standby state (does not carry service traffic). In this way, a Layer 2 loop is eliminated.
- When the active link is faulty, traffic is switched to the standby link in milliseconds. This ensures proper data forwarding.
- Smart Link is easy to configure.
- Smart Link does not involve protocol packet exchange, therefore greatly improving speed and reliability.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- As shown in the figure, SW3 is connected to FW1 and FW2 through dual uplinks. In this way, Switch3 has two uplinks to the uplink device. Smart Link can be configured on SW3. In normal situations, the link on Port2 functions as a backup link. If the link on Port1 fails, Smart Link automatically switches data traffic to the link on Port2 to ensure service continuity.

Quiz

1. (Single Choice) Which statement about the STP port state is false? ()

   A. The blocked port does not listen to or send BPDUs.

   B. A port in Learning state learns MAC addresses but does not forward data.

   C. A port in Listening state keeps listening to BPDUs.

   D. If a blocked port does not receive BPDUs within a specified period, the port automatically switches to the Listening state.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Answer: A

Summary

- STP prevents loops on a LAN. Devices running STP exchange information with one another to discover loops on the network, and block certain ports to eliminate loops. With the growth in scale of LANs, STP has become an important protocol for a LAN.
- After STP is configured on an Ethernet switching network, the protocol calculates the network topology to implement the following functions:
  - Loop prevention: The spanning tree protocol blocks redundant links to prevent potential loops on the network.
  - Link redundancy: If an active link fails and a redundant link exists, the spanning tree protocol activates the redundant link to ensure network connectivity.
- STP cannot meet requirements of modern campus networks. However, understanding the working mechanism of STP helps you better understand the working mechanism and deployment of RSTP and MSTP.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Inter-VLAN Communication

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- By default, a Layer 2 switching network is a broadcast domain, which brings many problems. Virtual local area network (VLAN) technology isolates such broadcast domains, preventing users in different VLANs from communicating with each other. However, such users sometimes need to communicate.
- This course describes how to implement inter-VLAN communication.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to understand:
  - Methods of implementing inter-VLAN communication.
  - How to use routers (physical interfaces or sub-interfaces) to implement inter-VLAN communication.
  - How to use Layer 3 switches to implement inter-VLAN communication.
  - How Layer 3 packets are forwarded.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

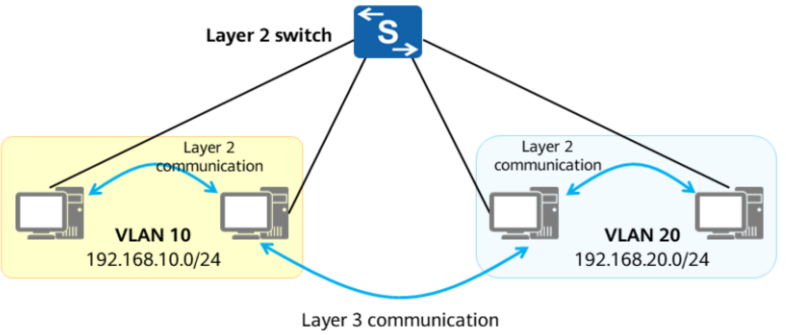
Contents

1. **Background**
2. Using Routers' Physical Interfaces or Sub-interfaces to Implement Inter-VLAN Communication
3. Using VLANIF Interfaces to Implement Inter-VLAN Communication
4. Layer 3 Communication Process

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Inter-VLAN Communication (1)

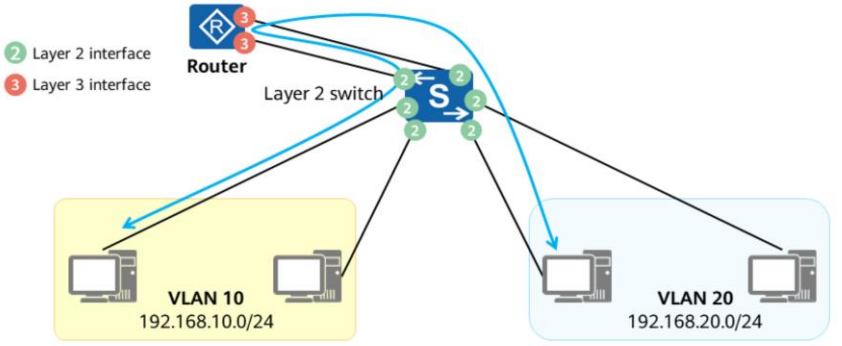
- In real-world network deployments, different IP address segments are assigned to different VLANs.
- PCs on the same network segment in the same VLAN can directly communicate with each other without the need for Layer 3 forwarding devices. This communication mode is called Layer 2 communication.
- Inter-VLAN communication belongs to Layer 3 communication, which requires Layer 3 devices.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Inter-VLAN Communication (2)

- Common Layer 3 devices: routers, Layer 3 switches, firewalls, etc.
- Inter-VLAN communication is implemented by connecting a Layer 2 switch to a Layer 3 interface of a Layer 3 device. The communication packets are routed by the Layer 3 device.



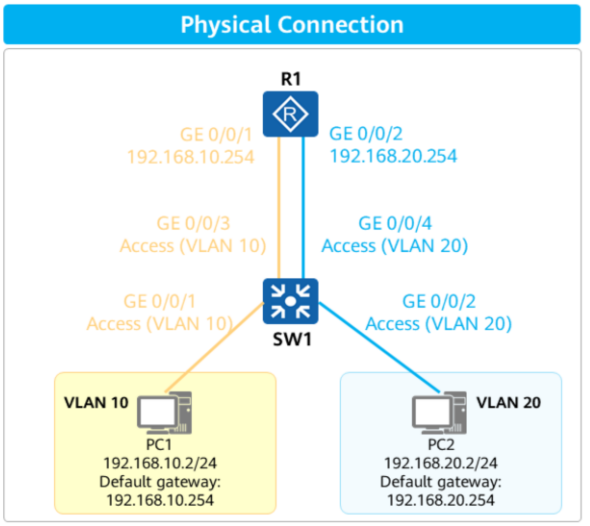
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. Background
2. **Using Routers' Physical Interfaces or Sub-interfaces to Implement Inter-VLAN Communication**
3. Using VLANIF Interfaces to Implement Inter-VLAN Communication
4. Layer 3 Communication Process

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Using a Router's Physical Interfaces

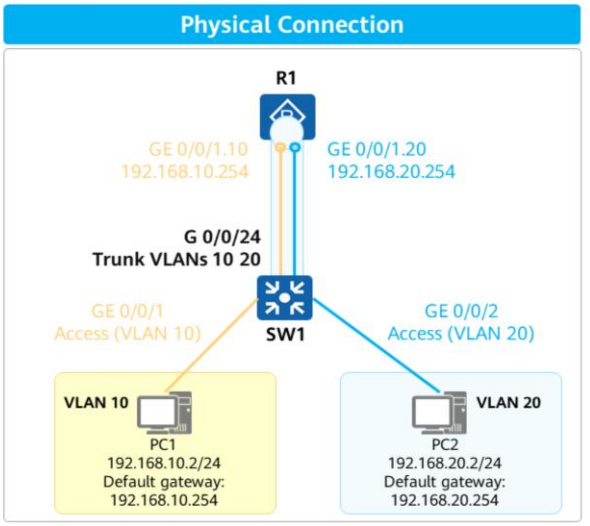


- The Layer 3 interfaces of the router function as gateways to forward traffic from the local network segment to other network segments.
- The Layer 3 interfaces of the router cannot process data frames with VLAN tags. Therefore, the interfaces of the switch connected to the router must be set to the access type.
- One physical interface of the router can function as the gateway of only one VLAN, meaning that the number of required physical interfaces are determined by the quantity of the deployed VLANs.
- A router, mainly forwarding packets at Layer 3, provides only a small number of physical interfaces. Therefore, the scalability of this solution is poor.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Configure VLANs on the Layer 2 switch. Each VLAN uses an independent switch interface to connect to the router.
- The router provides two physical interfaces as the default gateways of PCs in VLAN 10 and VLAN 20, respectively, for the PCs to communicate with each other.

Using a Router's Sub-interfaces



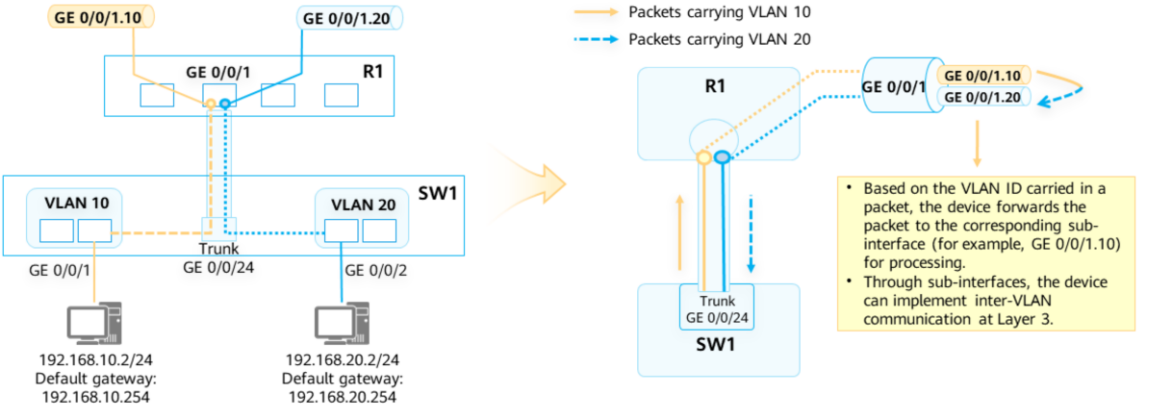
- A sub-interface is a logical interface created on a router's Ethernet interface and is identified by a physical interface number and a sub-interface number. Similar to a physical interface, a sub-interface can perform Layer 3 forwarding.
- Different from a physical interface, a sub-interface can terminate data frames with VLAN tags.
- You can create multiple sub-interfaces on one physical interface. After connecting the physical interface to the trunk interface of the switch, the physical interface can provide Layer 3 forwarding services for multiple VLANs.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- R1 connects to SW1 through a physical interface (GE 0/0/1). Two sub-interfaces (GE 0/0/1.10 and GE 0/0/1.20) are created on the physical interface and used as the default gateways of VLAN 10 and VLAN 20, respectively.
- Layer 3 sub-interfaces do not support VLAN packets and discard them once received. To prevent this issue, the VLAN tags need to be removed from the packets on the sub-interfaces. That is, VLAN tag termination is required.

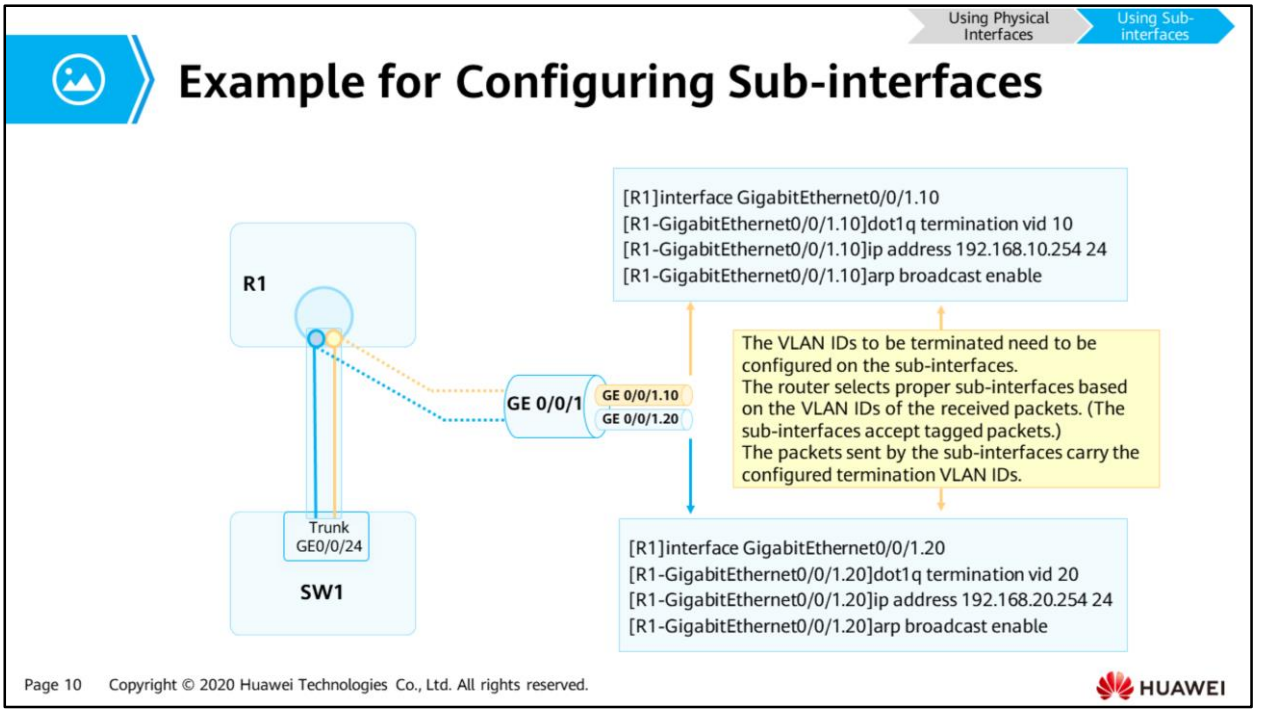
Sub-Interface Processing

- The interface connecting the switch to the router is set to a trunk interface. The router forwards the received packets to the corresponding sub-interfaces according to the VLAN tags in the packets.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A sub-interface implements VLAN tag termination as follows:
  - Removes VLAN tags from the received packets before forwarding or processing the packets.
  - Adds VLAN tags to the packets before forwarding the packets.



- The **interface** *interface-type interface-number.sub-interface number* command creates a sub-interface. *sub-interface number* specifies the number of a sub-interface on a physical interface. For easy memorization, a sub-interface number is generally the same as the VLAN ID to be terminated on the sub-interface.
- The **dot1q termination vid** command enables Dot1q VLAN tag termination for single-tagged packets on a sub-interface. By default, Dot1q VLAN tag termination for single-tagged packets is not enabled on sub-interfaces. The **arp broadcast enable** command enables ARP broadcast on a VLAN tag termination sub-interface. By default, ARP broadcast is not enabled on VLAN tag termination sub-interfaces. VLAN tag termination sub-interfaces cannot forward broadcast packets and automatically discard received ones. To allow a VLAN tag termination sub-interface to forward broadcast packets, run the **arp broadcast enable** command.

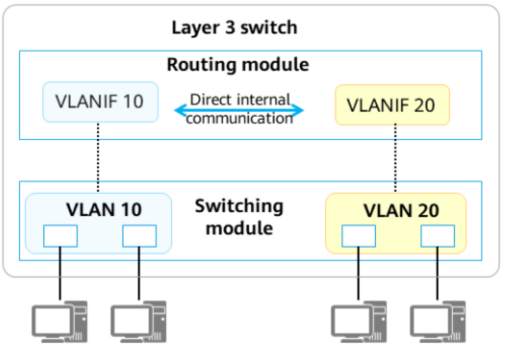
Contents

1. Background
2. Using Routers' Physical Interfaces or Sub-interfaces to Implement Inter-VLAN Communication
3. **Using VLANIF Interfaces to Implement Inter-VLAN Communication**
4. Layer 3 Communication Process

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

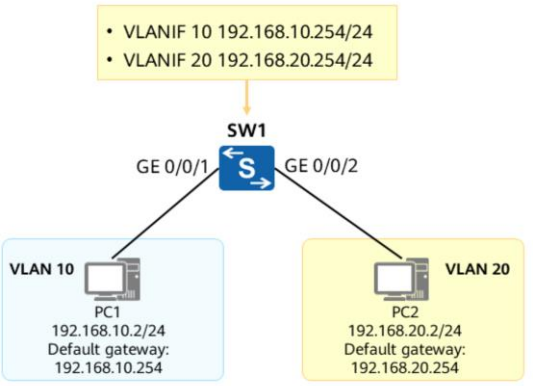
Layer 3 Switch and VLANIF Interfaces



- A Layer 2 switch provides only Layer 2 switching functions.
- A Layer 3 switch provides routing functions through Layer 3 interfaces (such as VLANIF interfaces) as well as the functions of a Layer 2 switch.
- A VLANIF interface is a Layer 3 logical interface that can remove and add VLAN tags. VLANIF interfaces therefore can be used to implement inter-VLAN communication.
- A VLANIF interface number is the same as the ID of its corresponding VLAN. For example, VLANIF 10 is created based on VLAN 10.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring VLANIF Interfaces



Basic configurations:

```
[SW1]vlan batch 10 20
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 10
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type access
[SW1-GigabitEthernet0/0/2] port default vlan 20
```

Configure VLANIF interfaces:

```
[SW1]interface Vlanif 10
[SW1-Vlanif10]ip address 192.168.10.254 24
[SW1]interface Vlanif 20
[SW1-Vlanif20]ip address 192.168.20.254 24
```

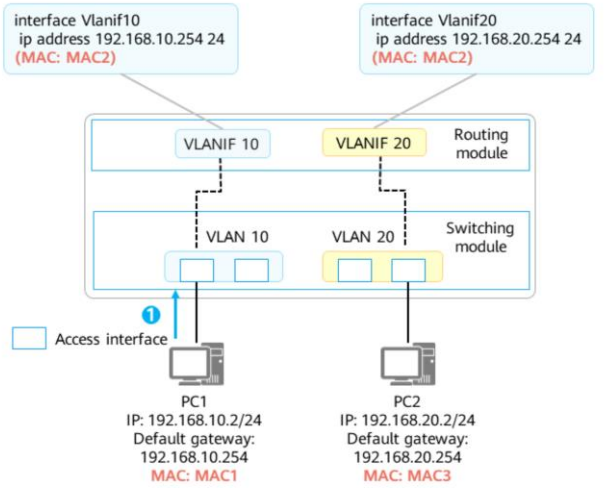
- Configuration Requirements
  Configure VLANs 10 and 20 for the interfaces connecting to PC1 and PC2, respectively. Configure the Layer 3 switch to allow the two PCs to communicate with each other.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- The **interface vlanif** *vlan-id* command creates a VLANIF interface and displays the VLANIF interface view. *vlan-id* specifies the ID of the VLAN associated with the VLANIF interface. The IP address of a VLANIF interface is used as the gateway IP address of a PC and must be on the same network segment as the IP address of the PC.

VLANIF Forwarding Process (1)



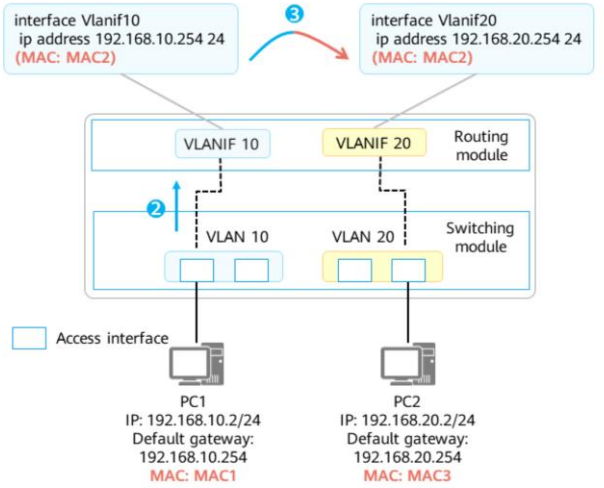
This example assumes that the required ARP or MAC address entries already exist on the PCs and the Layer 3 switch.

The communication process between PC1 and PC2 is as follows:

1. PC1 performs calculation based on its local IP address, local subnet mask, and destination IP address, and finds that the destination device PC2 is not on its network segment. PC1 then determines that Layer 3 communication is required and sends the traffic destined for PC2 to its gateway. Data frame sent by PC1: source MAC = MAC1, destination MAC = MAC2

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

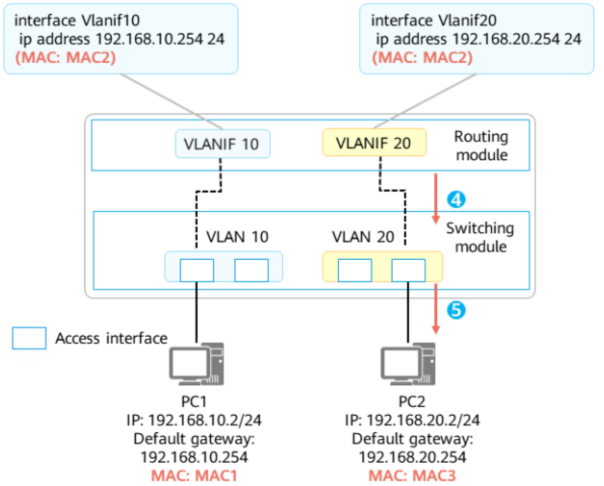
VLANIF Forwarding Process (2)



2. After receiving the packet sent from PC1 to PC2, the switch decapsulates the packet and finds that the destination MAC address is the MAC address of VLANIF 10. The switch then sends the packet to the routing module for further processing.
3. The routing module finds that the destination IP address is 192.168.20.2, which is not the IP address of its local interface, and determines that this packet needs to be forwarded at Layer 3. By searching the routing table, the routing module finds a matching route – the direct route generated by VLANIF 20 – for this packet.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

VLANIF Forwarding Process (3)



4. Because the matching route is a direct route, the switch determines that the packet has reached the last hop. It searches its ARP table for 192.168.20.2, obtains the corresponding MAC address, and sends the packet to the switching module for re-encapsulation.
5. The switching module searches its MAC address table to determine the outbound interface of the frame and whether the frame needs to carry a VLAN tag. Data frame sent by the switching module: source MAC = MAC2, destination MAC = MAC3, VLAN tag = None

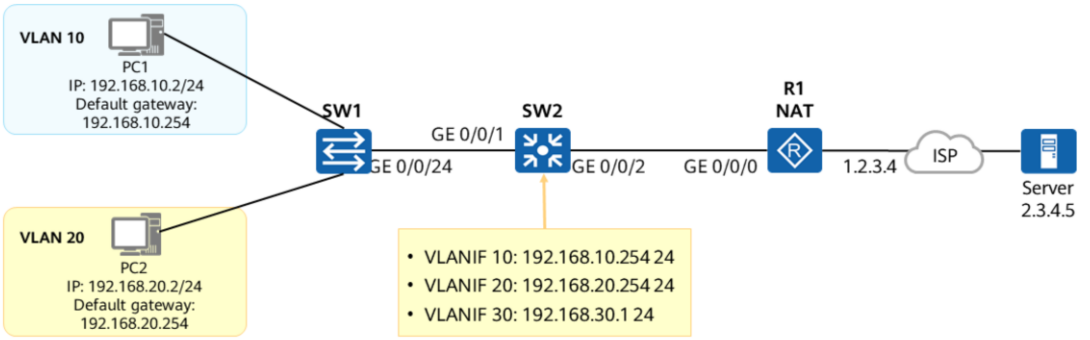
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. Background
2. Using Routers' Physical Interfaces or Sub-interfaces to Implement Inter-VLAN Communication
3. Using VLANIF Interfaces to Implement Inter-VLAN Communication
4. **Layer 3 Communication Process**

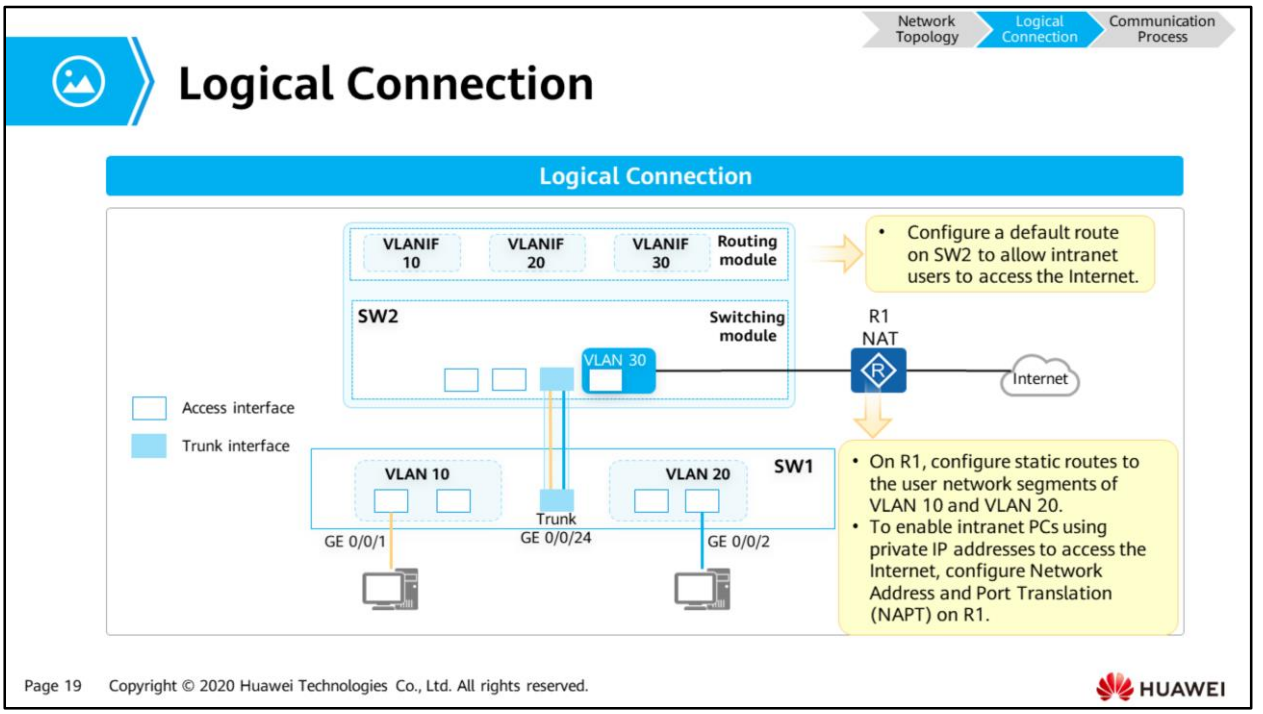
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Network Topology

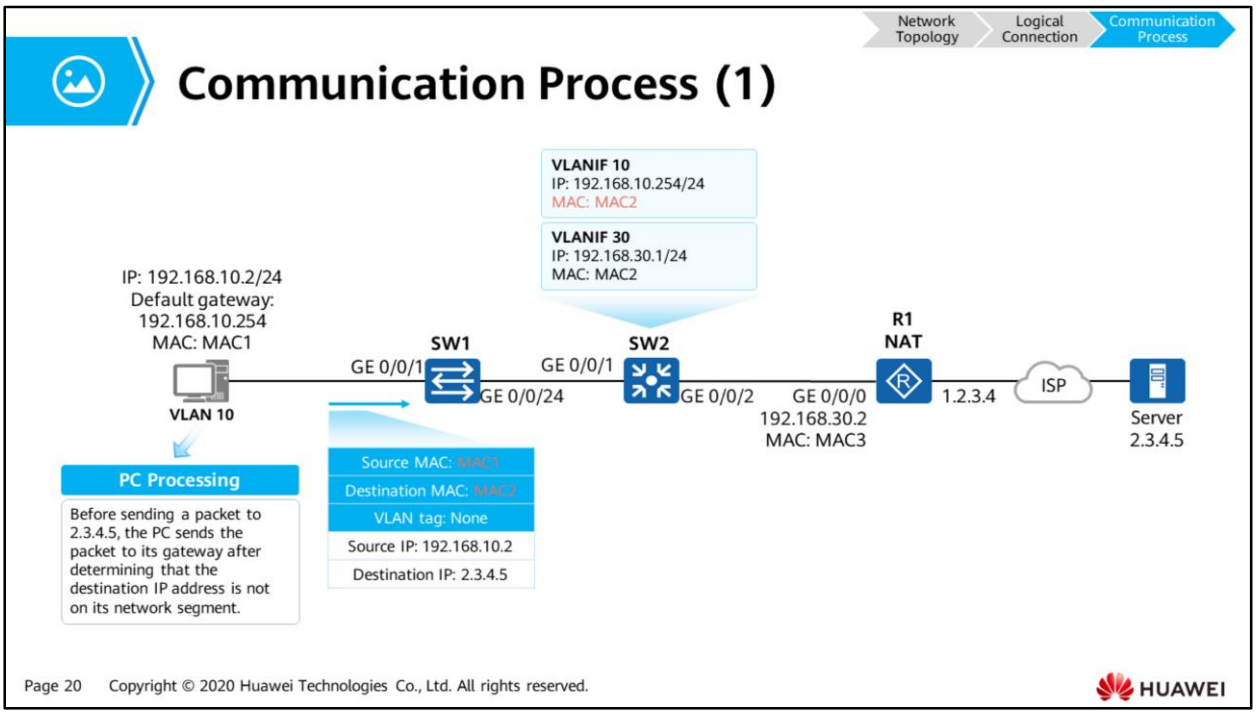


This topology is used as an example to describe the communication process from PC1 in VLAN 10 to the server (2.3.4.5) on the Internet.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

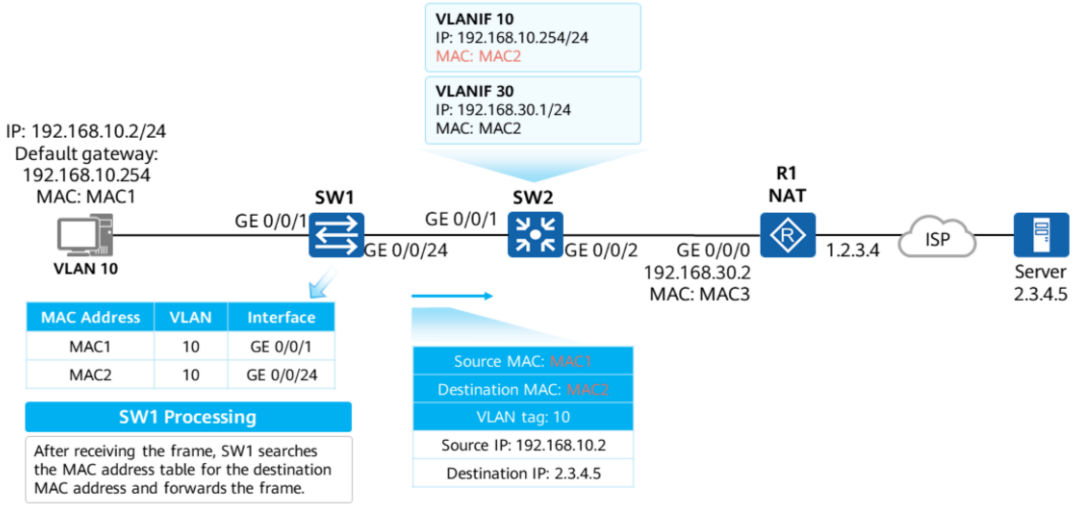


- NAPT: translates the IP address and port number in an IP packet header to another IP address and port number. NAPT is mainly used to enable devices on an internal network (private IP addresses) to access an external network (public IP addresses). NAPT allows multiple private IP addresses to be mapped to the same public IP address. In this way, multiple private IP addresses can access the Internet at the same time using the same public IP address.



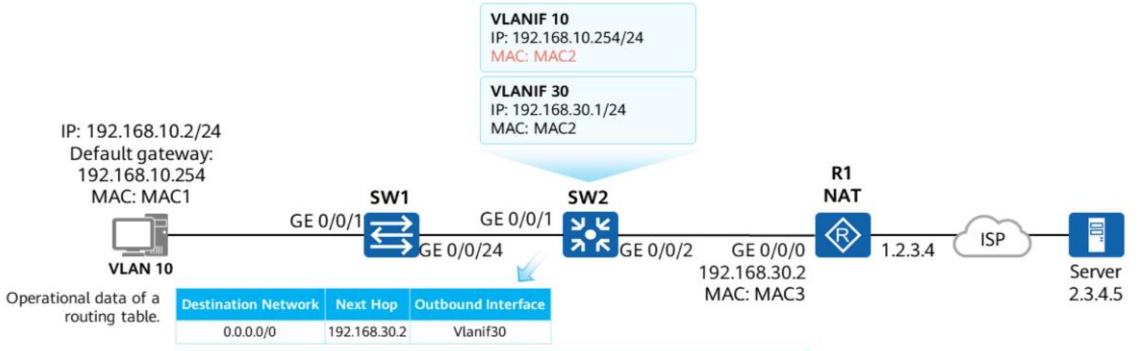
- This example assumes that the required ARP or MAC address entries already exist on all devices.

Communication Process (2)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Communication Process (3)



Operational data of a routing table.

Destination Network	Next Hop	Outbound Interface
0.0.0.0/0	192.168.30.2	Vlanif30

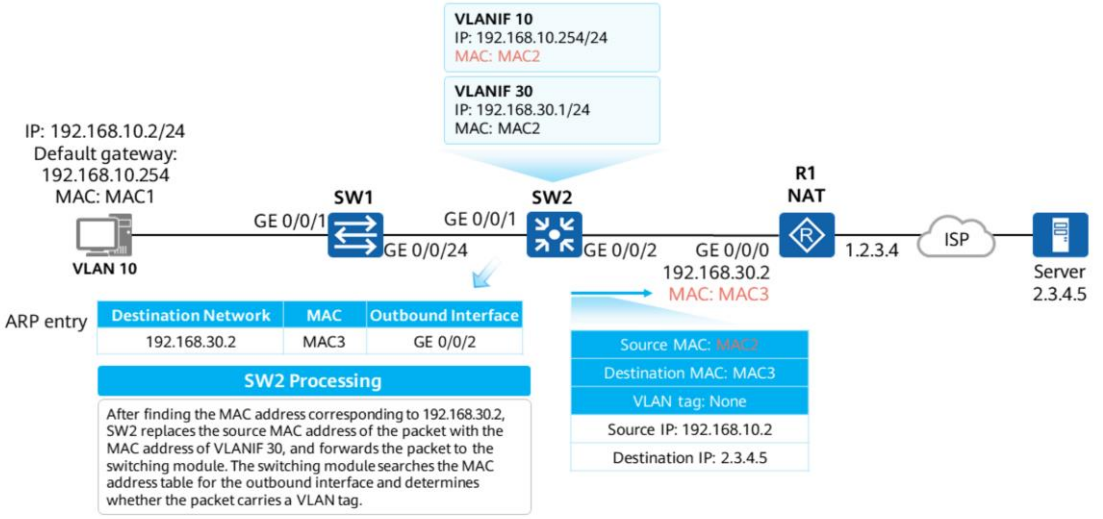
SW2 Processing

After SW2 receives the frame, it finds that the destination MAC address is the MAC address of its VLANIF 10 and sends the frame to the routing module, which then searches the routing table for a route matching the destination IP address 2.3.4.5.

After finding that the matching route is a default route, the outbound interface is VLANIF 30, and the next hop is 192.168.30.2, SW2 searches its ARP table to obtain the MAC address corresponding to 192.168.30.2.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Communication Process (4)

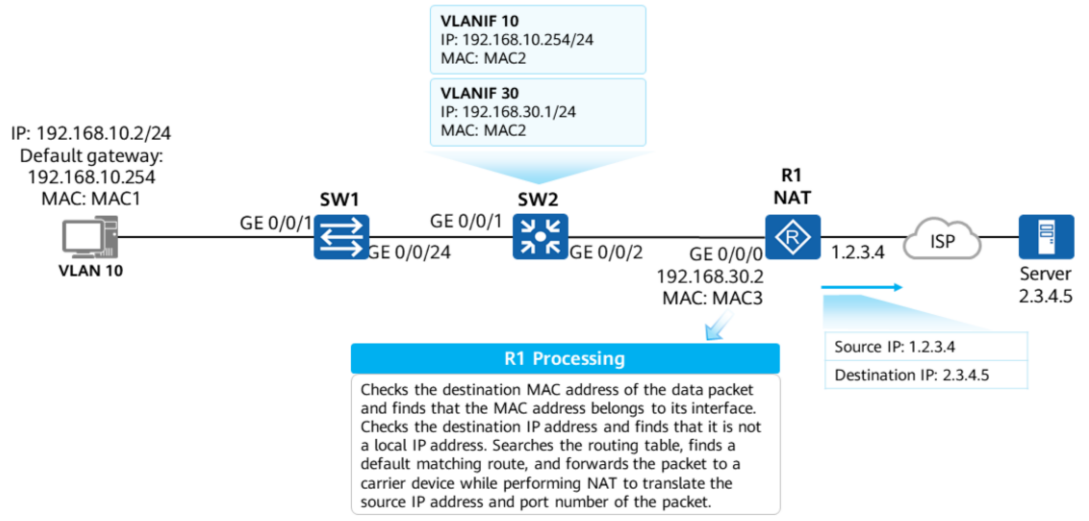


SW2 Processing

After finding the MAC address corresponding to 192.168.30.2, SW2 replaces the source MAC address of the packet with the MAC address of VLANIF 30, and forwards the packet to the switching module. The switching module searches the MAC address table for the outbound interface and determines whether the packet carries a VLAN tag.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Communication Process (5)



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Network Address Translation (NAT) translates the IP addresses in IP packet headers to other IP addresses.

Quiz

1. When a sub-interface is used to implement inter-VLAN communication, how does the switch interface connected to the router need to be configured?
2. How are packets changed when being forwarded at Layer 3?

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. Configure the interface as a trunk or hybrid interface to permit packets carrying VLAN tags corresponding to terminals.
2. The source and destination IP addresses remain unchanged during packet forwarding (without NAT), but the source and destination MAC addresses change. Each time a packet passes through a Layer 3 device, its source and destination MAC addresses change.

Summary

- This course describes three methods of implementing inter-VLAN communication: through physical interfaces, sub-interfaces, and VLANIF interfaces.
- It also elaborates the Layer 3 communication process, and device processing mechanism and packet header changes during the communication.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

More Information

- Comparison between Layer 2 and Layer 3 interfaces

Layer 2 Interface	Layer 3 Interface
An IP address cannot be configured for a Layer 2 interface.	An IP address can be configured for a Layer 3 interface
A Layer 2 interface does not have a MAC address.	A Layer 3 interface has a MAC address.
After a Layer 2 interface receives a data frame, it searches its MAC address table for the destination MAC address of the frame. If a matching MAC address entry is found, it forwards the frame according to the entry. If no matching MAC address entry is found, it floods the frame.	After a Layer 3 interface receives a data frame, if the destination MAC address of the data frame is the same as the local MAC address, it decapsulates the data frame and looks up the destination IP address of the data packet in the routing table. If a matching route is found, it forwards the data frame according to the instruction of the route. If no matching route is found, it discards the packet.
A physical interface on a Layer 2 switch (has only Layer 2 switching capabilities) is a typical Layer 2 interface. By default, the physical interfaces of most Layer 3 switches (have both Layer 2 and Layer 3 switching capabilities) work at Layer 2.	A Layer 3 interface on a router is a typical Layer 3 interface. Physical interfaces on some Layer 3 switches can be switched to Layer 3 mode. In addition to Layer 3 physical interfaces, there are Layer 3 logical interfaces, such as VLANIF interfaces on switches or logical sub-interfaces on other network devices, such as GE 0/0/1.10.
Layer 2 interfaces do not isolate broadcast domains. They flood received broadcast frames.	Layer 3 interfaces isolate broadcast domains. They directly terminate received broadcast frames instead of flooding them.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Eth-Trunk, iStack, and CSS

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- As services develop and the campus network scale expands, users have increasingly demanding requirements on network bandwidth and reliability. Traditional solutions improve network bandwidth by upgrading devices and implement high reliability by deploying redundant links and using the Spanning Tree Protocol (STP), leading to low flexibility, time-consuming troubleshooting, and complex configuration.
- This chapter describes how to use Eth-Trunk, intelligent stack (iStack), and cluster switch system (CSS) technologies to improve network bandwidth and reliability.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand the functions of link aggregation.
  - Understand the link aggregation types.
  - Understand the link aggregation negotiation process in Link Aggregation Control Protocol (LACP) mode.
  - Understand the advantages and principles of iStack and CSS.
  - Understand the common applications and networking of link aggregation and stacking technologies.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

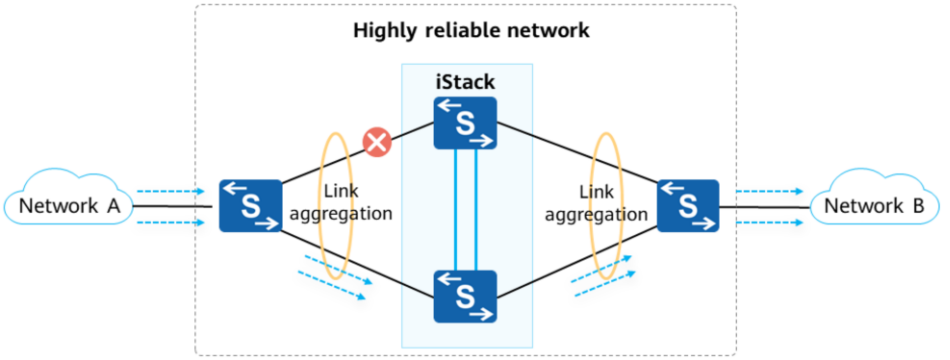
Contents

1. **Network Reliability Requirements**
2. Principle and Configuration of Link Aggregation
3. Overview of iStack and CSS

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Network Reliability

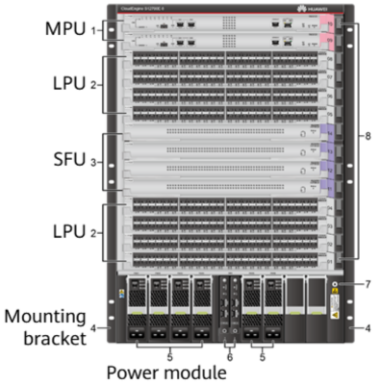
- Network reliability refers to the capability of ensuring nonstop network services when a single point or multiple points of failure occur on a device or link.
- Network reliability can be implemented at the card, device, and link levels.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- As networks rapidly develop and applications become more and more diversified, various value-added services (VASs) are widely deployed. Network interruption may cause many service exceptions and huge economic losses. Therefore, the reliability of networks has become a focus.

Card Reliability (1)

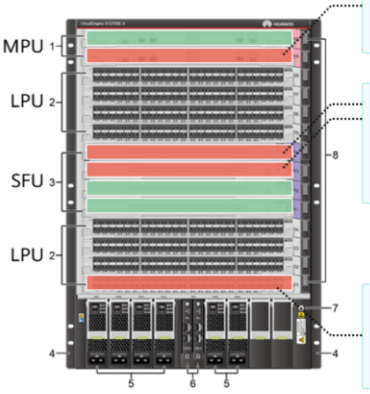


Front view of the S12700E-8 chassis

- A modular switch consists of a chassis, power modules, fan modules, main processing units (MPUs), switch fabric units (SFUs), and line processing units (LPUs).
- Chassis: provides slots for various cards and modules to implement inter-card communication.
- Power module: power supply system of the device
- Fan module: heat dissipation system
- MPU: responsible for the control plane and management plane of the entire system.
- SFU: responsible for the data plane of the entire system. The data plane provides high-speed non-blocking data channels for data switching between service modules.
- LPU: provides data forwarding functions on a physical device and provides optical and electrical interfaces of different rates.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Card Reliability (2)



The failure of a single MPU does not affect the normal operation of the control platform.

If some SFUs are faulty, the data plane can still forward data properly.

If the LPU is faulty, the interfaces on the LPU are affected.

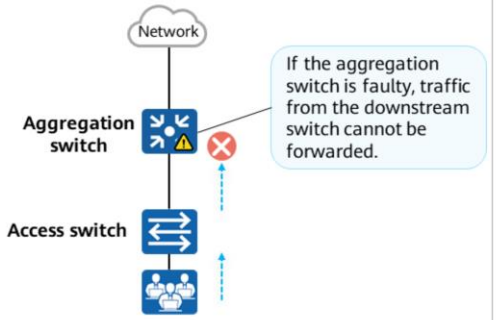
Front view of the S12700E-8 chassis

- For example, the S12700E-8 provides eight LPU slots, four SFU slots, two MPU slots, six power module slots, and four fan module slots.
- A modular switch can be configured with multiple MPUs and SFUs to ensure device reliability. If an SFU or MPU in a single slot is faulty, the switch can still run properly.
- After an LPU of a modular switch is damaged, interfaces on the LPU cannot forward data.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

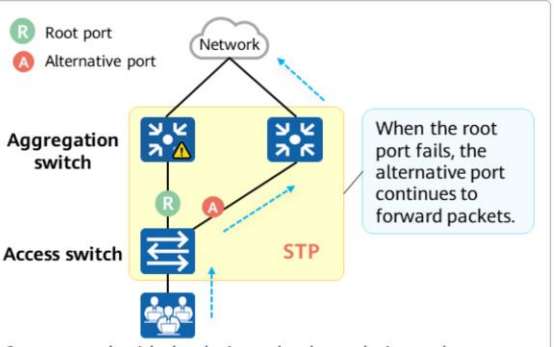
Device Reliability

No backup



On a network without the device redundancy design, a downstream switch uses a single uplink. If the upstream switch or its interfaces fail, all downstream networks are interrupted.

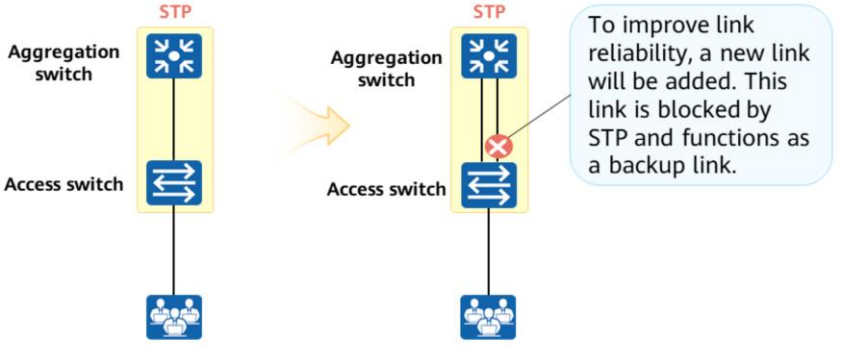
Master/Backup mode



On a network with the device redundancy design, a downstream switch is dual-homed to two upstream switches. The links work in active/backup mode. If the active link or upstream switch fails, traffic is switched to the backup link and forwarded through the backup device.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Link Reliability



- To ensure link reliability, deploy multiple physical links between devices. To prevent loops, configure STP to ensure that traffic is forwarded on only one link, and other links function as backup links.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

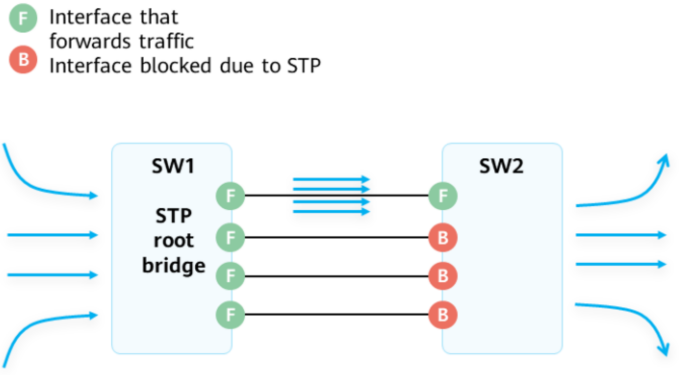
Contents

1. Network Reliability Requirements
2. **Principle and Configuration of Link Aggregation**
   - **Principle**
   - Manual Mode
   - LACP Mode
   - Typical Application Scenarios
   - Configuration Example
3. Overview of iStack and CSS

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Increasing Link Bandwidth

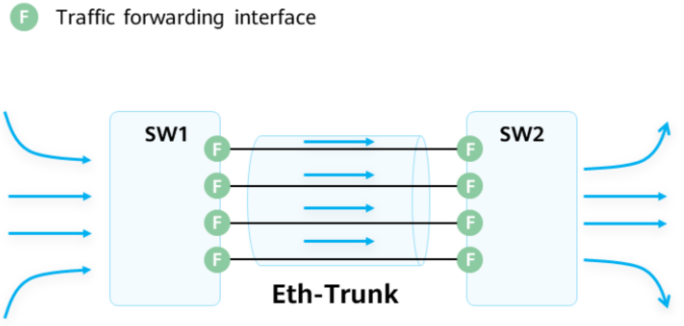
- When multiple links exist between devices, traffic is forwarded on only one link due to STP. In this case, the inter-device link bandwidth remains unchanged.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

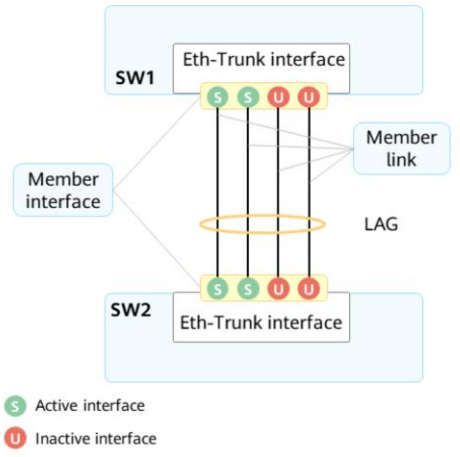
Eth-Trunk

- Ethernet link aggregation, also called Eth-Trunk, bundles multiple physical links into a logical link to increase link bandwidth, without having to upgrade hardware.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic Concepts of Eth-Trunk



- A link aggregation group (LAG) is a logical link formed by bundling several links. Each LAG has one logical interface, known as an LAG interface or Eth-Trunk interface.
- Member interface and member link: Physical interfaces that constitute an Eth-Trunk interface are called member interfaces, and the link corresponding to a member interface is known as a member link.
- Active interface and active link: An active interface is also called a selected interface and is a member interface that participates in data forwarding. The link corresponding to an active interface is called an active link.
- Inactive interface and inactive link: An inactive interface is also called an unselected interface and is a member interface that does not participate in data forwarding. A link corresponding to an inactive interface is referred to as an inactive link.
- Link aggregation mode: Based on whether the Link Aggregation Control Protocol (LACP) is enabled, link aggregation can be classified into manual mode and LACP mode.
- Other concepts: upper and lower thresholds for the number of active interfaces

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

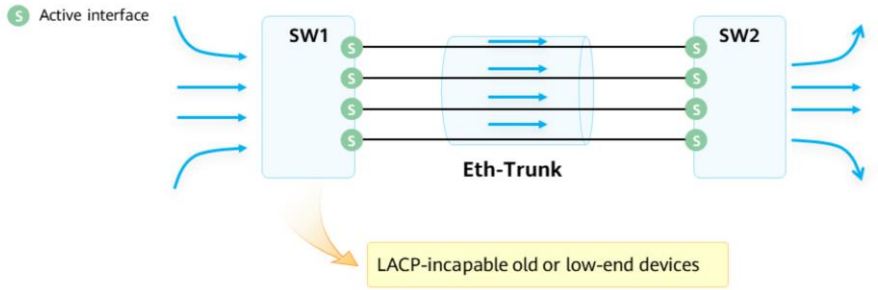
- An Eth-Trunk can be treated as a physical Ethernet interface. The only difference between the Eth-Trunk and physical Ethernet interface is that the Eth-Trunk needs to select one or more member interfaces to forward traffic.
- The following parameters must be the same for member interfaces in an Eth-Trunk:
  - Interface rate
  - Duplex mode
  - VLAN configurations: The interface type must be the same (access, trunk, or hybrid). For access interfaces, the default VLAN of the member interfaces must be the same. For trunk interfaces, the allowed VLANs and the default VLAN of the member interfaces must be the same.

Contents

1. Network Reliability Requirements
2. **Principle and Configuration of Link Aggregation**
   - Principle
   - **Manual Mode**
   - LACP Mode
   - Typical Application Scenarios
   - Configuration Example
3. Overview of iStack and CSS

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

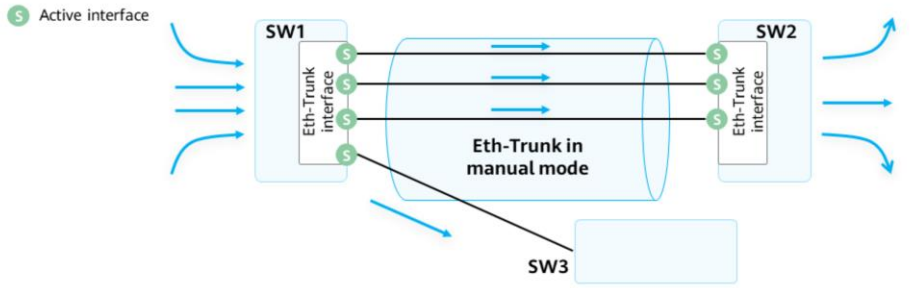
Manual Mode



- Manual mode: An Eth-Trunk is manually created, and its member interfaces are manually configured. LACP is not used for negotiation between the two systems.
- In most cases, all links are active links. In this mode, all active links forward data and evenly share traffic. If an active link is faulty, the LAG automatically evenly shares traffic among the remaining active links.
- If one of the devices at both ends of an LAG does not support LACP, you can use the manual mode.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Defects of the Manual Mode (1)

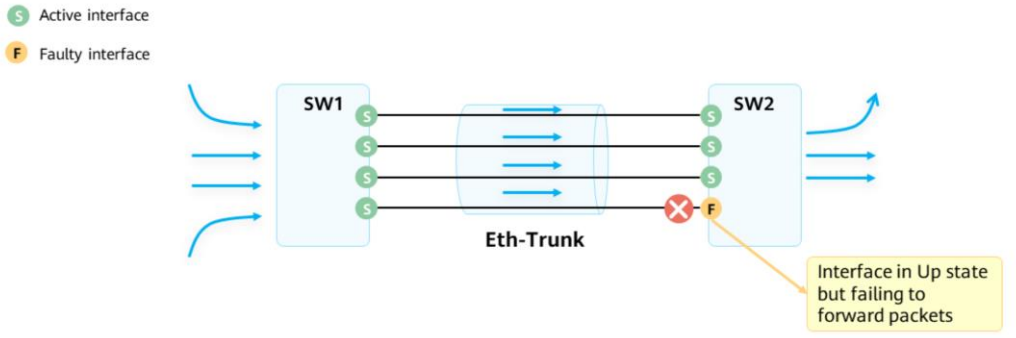


- To ensure that the Eth-Trunk works properly, ensure that the peer interfaces of all member interfaces in the Eth-Trunk meet the following requirements:
  - The peer interfaces reside on the same device.
  - The peer interfaces are added to the same Eth-Trunk.
- In manual mode, devices do not exchange packets. Therefore, the configuration needs to be manually confirmed.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- As shown in the preceding figure, four interfaces of SW1 are added to an Eth-Trunk, but the peer end of one interface is SW3 instead of SW2. In this case, some traffic is load balanced to SW3, causing communication exceptions.

Defects of the Manual Mode (2)



- In manual mode, the device can determine whether the peer interface is working properly based only on the physical layer status.

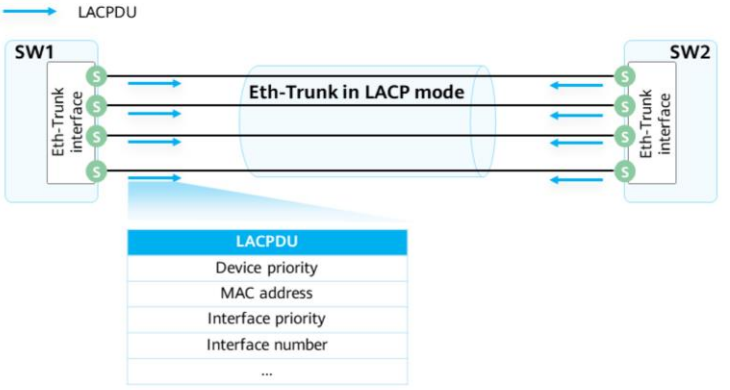
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. Network Reliability Requirements
2. **Principle and Configuration of Link Aggregation**
   - Principle
   - Manual Mode
   - **LACP Mode**
   - Typical Application Scenarios
   - Configuration Example
3. Overview of iStack and CSS

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

LACPDU



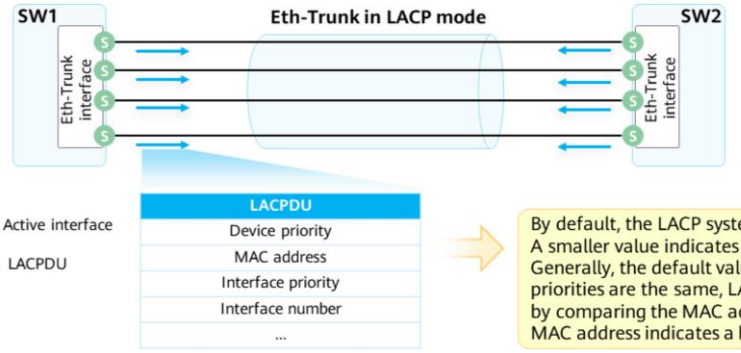
LACPDU
Device priority
MAC address
Interface priority
Interface number
...

- LACP mode: A link aggregation mode that uses the LACP protocol. Devices exchange Link Aggregation Control Protocol Data Units (LACPDUs) to ensure that the peer interfaces are member interfaces that belong to the same Eth-Trunk and are on the same device.
- An LACPDU contains the device priority, MAC address, interface priority, and interface number.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

System Priority

- In LACP mode, the number of active interfaces selected by devices at both ends must be consistent; otherwise, the Eth-Trunk cannot be set up. In this case, configure one end as the Actor. Then the other end selects active interfaces according to the Actor.
- The Actor is determined based on the LACP system priority. A smaller value indicates a higher priority.

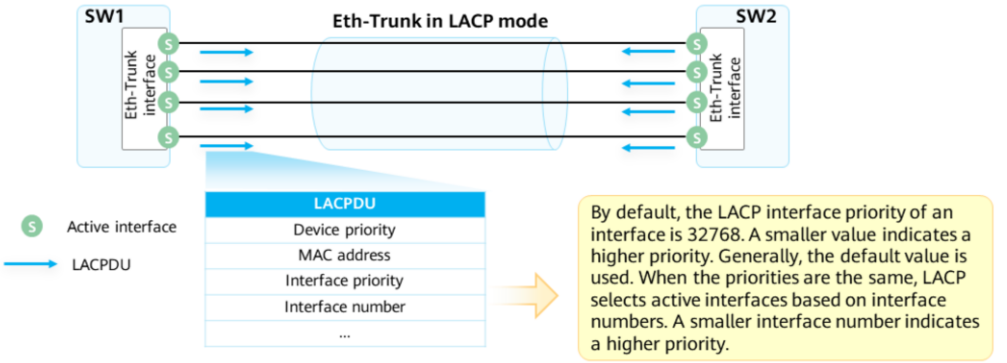


By default, the LACP system priority is 32768. A smaller value indicates a higher priority. Generally, the default value is used. When the priorities are the same, LACP selects the Actor by comparing the MAC addresses. A smaller MAC address indicates a higher priority.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Interface Priority

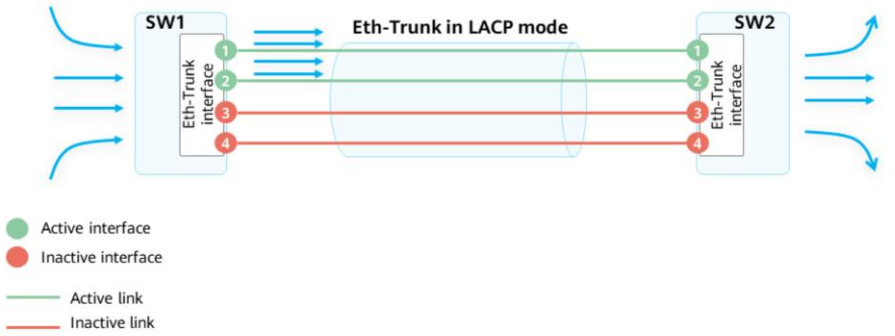
- After the Actor is selected, both devices select active interfaces based on the interface priorities of the Actor. A smaller LACP interface priority value indicates a higher priority.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Maximum Number of Active Interfaces (1)

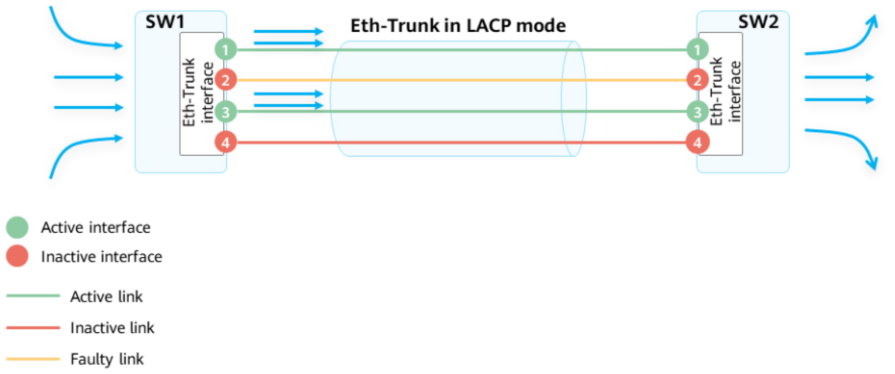
- In LACP mode, the maximum number of active interfaces can be configured. When the number of member interfaces exceeds the maximum number of active interfaces, the interfaces with higher priorities and smaller interface numbers are selected as active interfaces, and the other interfaces function as backup interfaces (inactive interfaces). In addition, the links corresponding to active interfaces become active links, and the links corresponding to inactive interfaces become inactive links. The switch sends and receives packets only through active interfaces.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

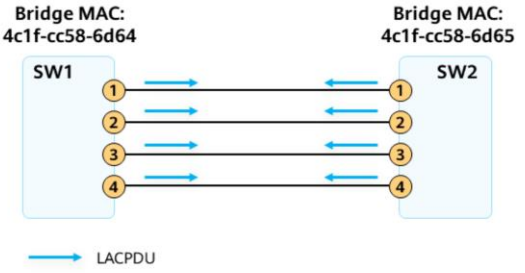
Maximum Number of Active Interfaces (2)

- If an active link fails, an inactive link with the highest priority (based on the interface priority and interface number) is selected to replace the faulty link. This ensures that the overall bandwidth does not change and services are not interrupted.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Active Link Election (1)



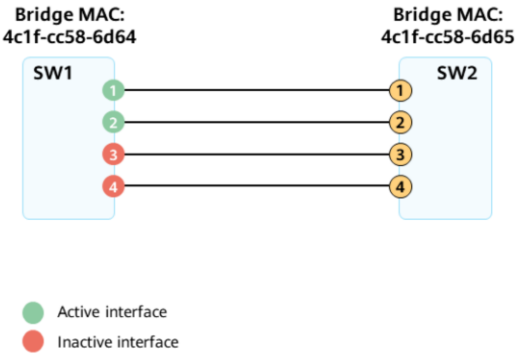
- An Eth-Trunk in LACP mode is set up between SW1 and SW2. The maximum number of active interfaces is set to 2 on SW1 and SW2.
- SW1 with a higher priority is elected as the Actor through LACPDUs.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Configure an Eth-Trunk in LACP mode between SW1 and SW2 and add four interfaces to an Eth-Trunk. The four interfaces are numbered 1, 2, 3, and 4. On SW1 and SW2, set the maximum number of active interfaces in the Eth-Trunk to 2 and retain the default settings for the other parameters (system priority and interface priority).
- SW1 and SW2 send LACPDUs through member interfaces 1, 2, 3, and 4.
- When receiving LACPDUs from the peer end, SW1 and SW2 compare the system priorities, which use the default value 32768 and are the same. Then they compare MAC addresses. The MAC address of SW1 is 4c1f-cc58-6d64, and the MAC address of SW2 is 4c1f-cc58-6d65. SW1 has a smaller MAC address and is preferentially elected as the Actor.

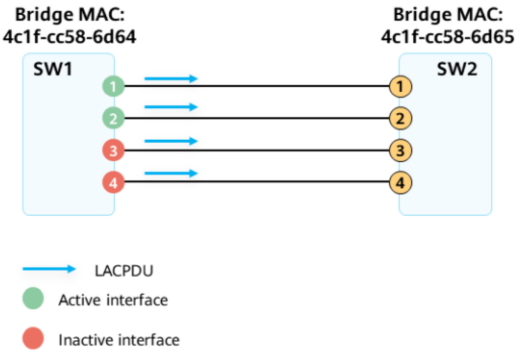
Active Link Election (2)



- SW1 compares the interface priorities and interface numbers to select active interfaces. Under the same interface priority, interfaces 1 and 2 have smaller interface numbers and are elected as active interfaces.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Active Link Election (3)

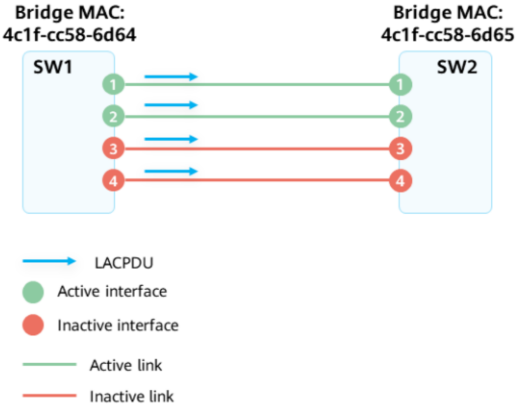


- SW1 notifies the peer end of the elected active interfaces through LACPDUs.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- LACP uses the following flags in an LACPDU to identify the interface status. If the three flags are set to 1, the interface is an active interface.
  - Synchronization
  - Collecting
  - Distributing
- If the three flags are set to 0, the interface is an inactive interface.

Active Link Election (4)



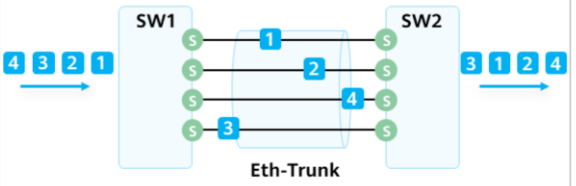
- SW2 determines the local active interfaces based on the election result of SW1 and the corresponding links become active links.
- In this way, the election of active links is complete.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Load Balancing

Per-packet load balancing

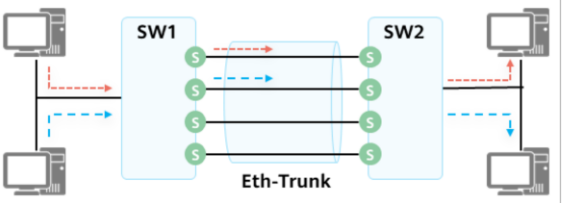
Active interface



When an Eth-Trunk is used to forward data, there are multiple physical links between devices at both ends of the Eth-Trunk. If data frames are forwarded on different links, data frames may arrive at the peer end in a different order in which they were transmitted, resulting in out-of-order packets.

Per-flow load balancing

Active interface

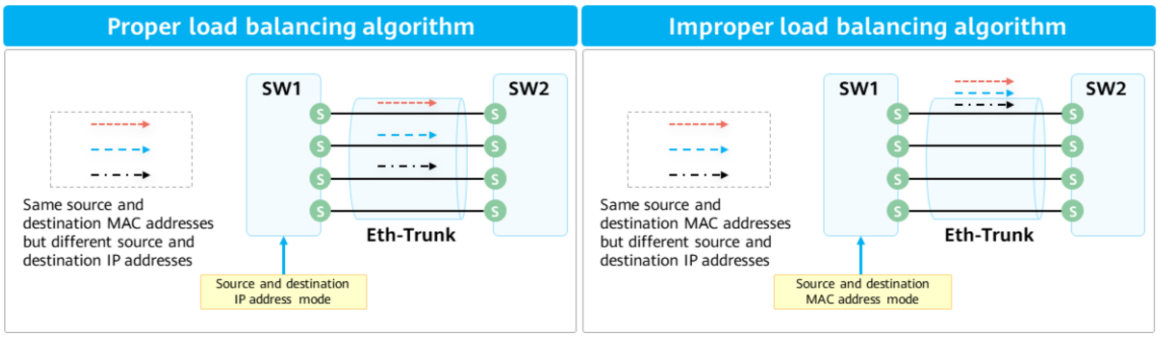


Load balancing based on flows is recommended for an Eth-Trunk. In this mode, a flow is load balanced to the same link. This ensures that frames of the same flow are transmitted over the same physical link and implements load balancing among physical links in an Eth-Trunk.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Load Balancing Mode

- An Eth-Trunk can load balance traffic based on IP addresses or MAC addresses of packets. You can configure different load balancing modes (valid locally only for outgoing packets) to distribute data flows to different member interfaces.
- Traffic can be load balanced based on: source IP address, source MAC address, destination IP address, destination MAC address, source and destination IP addresses, and source and destination MAC addresses.
- For actual services, you need to configure a proper load balancing mode based on traffic characteristics. If a service traffic parameter changes frequently, it is easier to load balance traffic if you use the load balancing mode based on this frequently-changing parameter.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

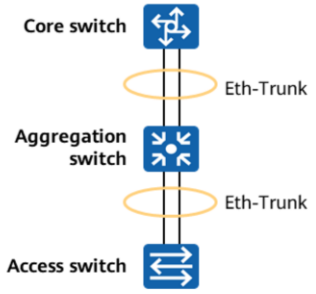
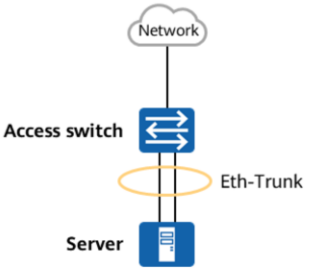
- If the IP addresses of packets change frequently, load balancing based on the source IP address, destination IP address, or source and destination IP addresses is more suitable for load balancing among physical links.
- If MAC addresses of packets change frequently and IP addresses are fixed, load balancing based on the source MAC address, destination MAC address, or source and destination MAC addresses is more suitable for load balancing among physical links.
- If the selected load balancing mode is unsuitable for the actual service characteristics, traffic may be unevenly load balanced. Some member links have high load, but other member links are idle. For example, if the source and destination IP addresses of packets change frequently but the source and destination MAC addresses are fixed and traffic is load balanced based on the source and destination MAC addresses, all traffic is transmitted over one member link.

Contents

1. Network Reliability Requirements
2. **Principle and Configuration of Link Aggregation**
   - Principle
   - Manual Mode
   - LACP Mode
   - **Typical Application Scenarios**
   - Configuration Example
3. Overview of iStack and CSS

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

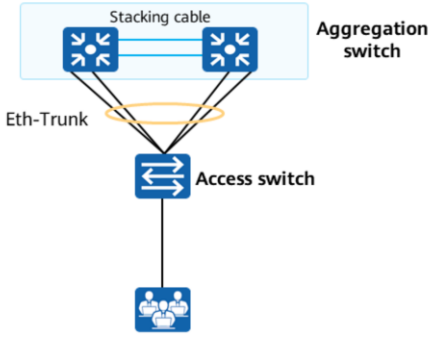
Typical Application Scenario (1)

Between switches	Between the switch and server
	
To ensure the bandwidth and reliability of links between switches, deploy multiple physical links between switches and add them to an Eth-Trunk.	To improve the access bandwidth and reliability of the server, bind two or more physical NICs into a NIC group and establish an Eth-Trunk with the switch.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

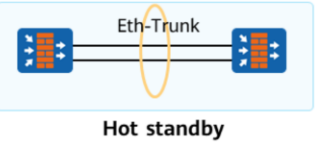
Typical Application Scenario (2)

Between a switch and stack



An iStack is a logical device consisting of two switches. A switch can be connected to the iStack through an Eth-Trunk to form a highly reliable loop-free network.

Heartbeat link of firewalls in hot standby mode



If two firewalls are deployed in hot standby mode, the heartbeat link is used to detect the status of the peer device. To prevent status detection errors caused by single-interface or single-link faults, you can create an Eth-Trunk and use it as the heartbeat link for status detection.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. Network Reliability Requirements
2. **Principle and Configuration of Link Aggregation**
   - Principle
   - Manual Mode
   - LACP Mode
   - Typical Application Scenarios
   - **Configuration Example**
3. Overview of iStack and CSS

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Commands (1)

1. Create an Eth-Trunk.

   ```
   [Huawei] interface eth-trunk trunk-id
   ```

   An Eth-Trunk interface is created, and the Eth-Trunk interface view is displayed.

2. Configure a link aggregation mode.

   ```
   [Huawei-Eth-Trunk1] mode {lacp | manual load-balance }
   ```

   To enable the LACP mode, run **mode lacp**. To enable the manual mode, run **mode manual load-balance**.
   Note: The link aggregation modes at both ends must be the same.

3. Add an interface to the Eth-Trunk (Ethernet interface view).

   ```
   [Huawei-GigabitEthernet0/0/1] eth-trunk trunk-id
   ```

   In the interface view, the interface is added to the Eth-Trunk.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Commands (2)

4. Add an interface to the Eth-Trunk (Eth-Trunk view).

   [Huawei-Eth-Trunk1] **trunkport** *interface-type { interface-number}*

   In the Eth-Trunk view, the interface is added to the Eth-Trunk. You can use either of the preceding commands to add an interface to an Eth-Trunk.
5. Enable interfaces at different rates to join the same Eth-Trunk interface.

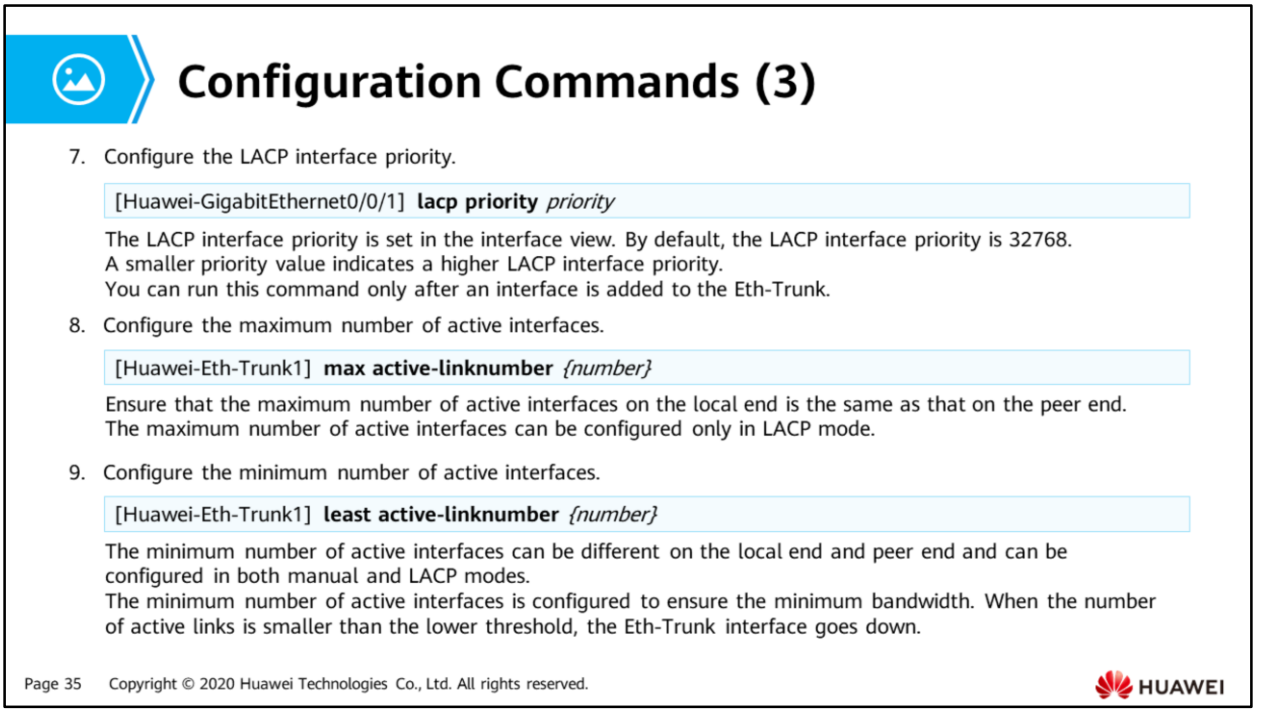
   [Huawei-Eth-Trunk1] **mixed-rate link enable**

   By default, interfaces at different rates are not allowed to join the same Eth-Trunk, and only interfaces at the same rate can be added to the same Eth-Trunk.
6. Configure the LACP system priority.

   [Huawei] **lacp priority** *priority*

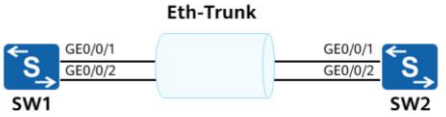
   A smaller priority value indicates a higher LACP system priority. By default, the LACP priority is 32768.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The maximum number of active interfaces varies according to switch models. For example, the maximum number of active interfaces in an Eth-Trunk is 32 on the S6720HI, S6730H, S6730S, and S6730S-S, and is 16 on the S6720LI, S6720S-LI, S6720SI, and S6720S-SI. For details, see the product manual.
- The minimum number of active interfaces is configured to ensure the minimum bandwidth. If the bandwidth is too small, services that require high link bandwidth may be abnormal. In this case, you can disconnect the Eth-Trunk interface to switch services to other paths through the high reliability mechanism of the network, ensuring normal service running.

Example for Configuring an Eth-Trunk in Manual Mode



- Requirement description:
  - SW1 and SW2 are connected to the networks of VLAN 10 and VLAN 20.
  - SW1 and SW2 are connected through two Ethernet links. To provide link redundancy and enhance transmission reliability, configure an Eth-Trunk in manual mode between SW1 and SW2.

SW1 configuration:

```
[SW1] interface eth-trunk 1
[SW1-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/2
[SW1-Eth-Trunk1] port link-type trunk
[SW1-Eth-Trunk1] port trunk allow-pass vlan 10 20
```

SW2 configuration:

```
[SW2] interface eth-trunk 1
[SW2-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/2
[SW2-Eth-Trunk1] port link-type trunk
[SW2-Eth-Trunk1] port trunk allow-pass vlan 10 20
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring an Eth-Trunk in LACP Mode (1)



- Requirement description:
  - SW1 and SW2 are connected to the networks of VLAN 10 and VLAN 20.
  - SW1 and SW2 are connected through three Ethernet links. To provide link redundancy and enhance transmission reliability, configure an Eth-Trunk in LACP mode between SW1 and SW2, manually adjust the priority to configure SW1 as the Actor, and set the maximum number of active interfaces to 2. The other link functions as the backup link.

SW1 configuration:

```
[SW1] interface eth-trunk 1
[SW1-Eth-Trunk1] mode lacp
[SW1-Eth-Trunk1] max active-linknumber 2
[SW1-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/3
[SW1-Eth-Trunk1] port link-type trunk
[SW1-Eth-Trunk1] port trunk allow-pass vlan 10 20
[SW1-Eth-Trunk1] quit
[SW1] lacp priority 30000
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring an Eth-Trunk in LACP Mode (2)



- Requirement description:
  - SW1 and SW2 are connected to the networks of VLAN 10 and VLAN 20.
  - SW1 and SW2 are connected through three Ethernet links. To provide link redundancy and enhance transmission reliability, configure an Eth-Trunk in LACP mode between SW1 and SW2, manually adjust the priority to configure SW1 as the Actor, and set the maximum number of active interfaces to 2. The other link functions as the backup link.

SW1 configuration:

```
[SW2] interface eth-trunk 1
[SW2-Eth-Trunk1] mode lacp
[SW2-Eth-Trunk1] max active-linknumber 2
[SW2-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/3
[SW2-Eth-Trunk1] port link-type trunk
[SW2-Eth-Trunk1] port trunk allow-pass vlan 10 20
[SW2-Eth-Trunk1] quit
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

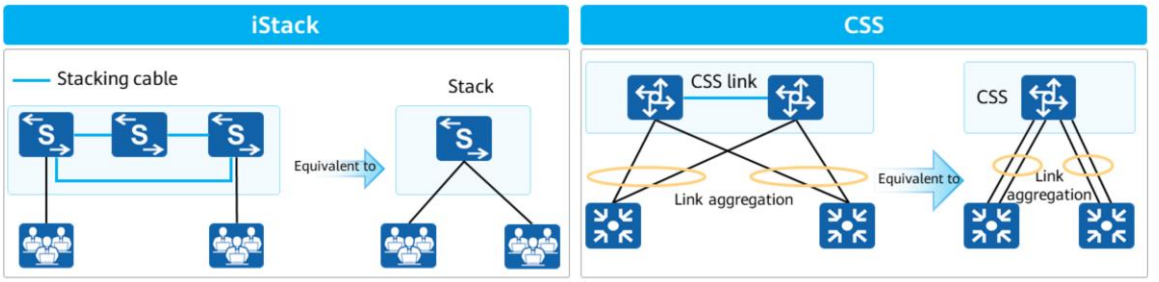
Contents

1. Network Reliability Requirements
2. Principle and Configuration of Link Aggregation
3. **Overview of iStack and CSS**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

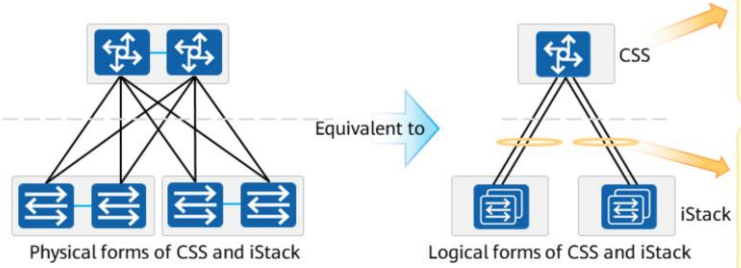
Introduction to iStack and CSS



- iStack: Multiple iStack-capable switches are connected using stacking cables to form a logical switch that participates in data forwarding.
- Cluster switch system (CSS): Two CSS-capable switches are bundled into one logical switch.
- A CSS consists of only two switches. Generally, modular switches support CSS, and fixed switches support iStack.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Advantages of iStack and CSS



- One logical device simplifies O&M and facilitates management.
- If a physical device fails, the other device can take over the forwarding and control functions, preventing single points of failure.

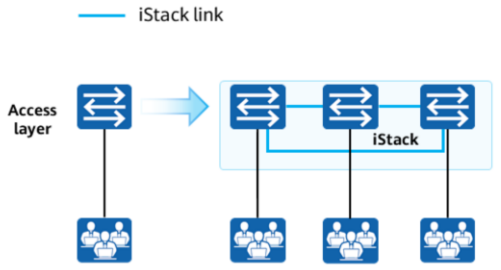
- Inter-device link aggregation is implemented on a loop-free physical network, so STP does not need to be deployed.
- All links in the Eth-Trunk are used, and the link usage is 100%.

- Many-to-one virtualization: Switches can be virtualized into one logical switch (CSS) that has a unified control plane for unified management.
- Unified forwarding plane: Physical switches in a CSS use a unified forwarding plane, and share and synchronize forwarding information in real time.
- Inter-device link aggregation: Links between physical switches are aggregated into a single Eth-Trunk interface to interconnect with downstream devices.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

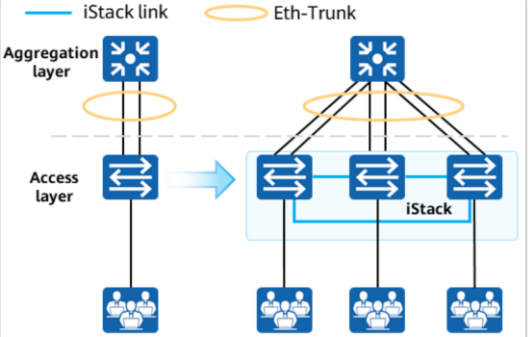
Application (1)

Extending the port quantity



- When the port density of a switch cannot meet the access requirements, add new switches to set up an iStack to increase the number of ports.

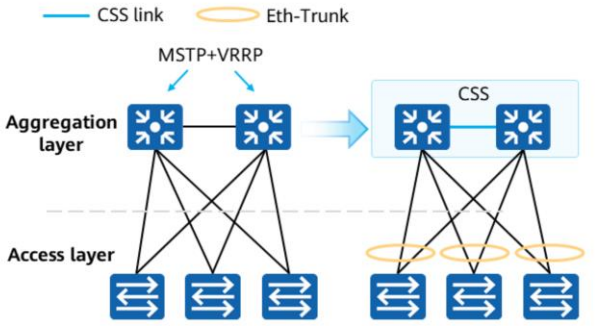
Extending the bandwidth and implementing redundancy backup



- To increase the uplink bandwidth, add new switches to set up an iStack and add multiple physical links of the member switches to an Eth-Trunk. This increases the uplink bandwidth, implements inter-device backup and inter-device link redundancy, and improves reliability.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

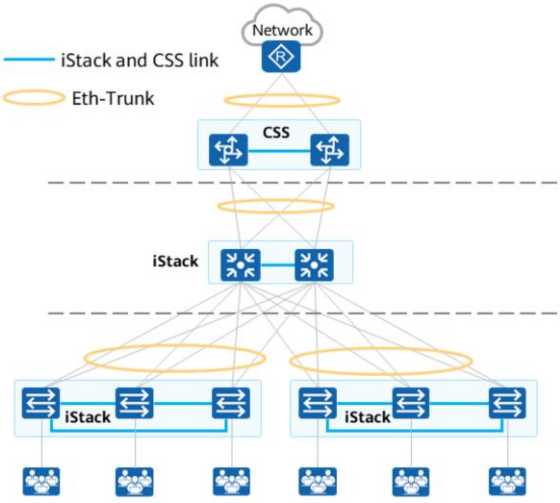
Application (2)



- Two devices form a CSS and are virtualized into a single logical device. This simplified network does not require Multiple Spanning Tree Protocol (MSTP) or Virtual Router Redundancy Protocol (VRRP), so network configuration is much simpler. Additionally, inter-device link aggregation speeds up network convergence and improves network reliability.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Recommended Architecture



Core layer

- Core switches set up a CSS and use Eth-Trunks to connect to uplink and downlink devices, building a highly reliable and loop-free network.

Aggregation layer

- Aggregation switches set up an iStack and use Eth-Trunks to connect to uplink and downlink devices, building a highly reliable loop-free network.

Access layer

- Access devices that are geographically close to each other (such as access switches in a building) are virtualized into one logical device using iStack. This adds interfaces and simplifies management.
- An Eth-Trunk is used to connect to the aggregation layer. The logical network architecture is simple, and STP and VRRP are not required. This networking offers high reliability, high uplink bandwidth, and fast convergence.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Quiz

1. What are the differences between per-packet load balancing and per-flow load balancing?
2. How does an Actor be elected in LACP mode?
3. What are the advantages of CSS and iStack?

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. Packet disorder may occur if packets are load balanced to different links based on packets. If packets are load balanced to the same link based on flows, packet disorder will not occur. However, a single flow cannot make full use of the bandwidth of the entire Eth-Trunk.
2. Switches compare system priorities. A smaller value indicates a higher priority. If the system priorities are the same, the bridge MAC addresses are compared. A smaller bridge MAC address indicates a higher priority. The device with a higher priority becomes the Actor.
3. CSS and iStack simplify network management, improve network reliability, make full use of network link bandwidth, and use inter-device Eth-Trunk to construct a loop-free physical network.

Summary

- Link aggregation can be used to improve link reliability, utilization, and bandwidth. Link aggregation can be classified into static and LACP aggregation based on the aggregation mode.
- LACP uses packet negotiation to implement backup for active links. When a link fails, the backup link is elected as the active link to forward packets.
- To ensure the sequence in which packets arrive, link aggregation uses per-flow load balancing.
- iStack and CSS simplify network management and network structure, and improve network reliability.

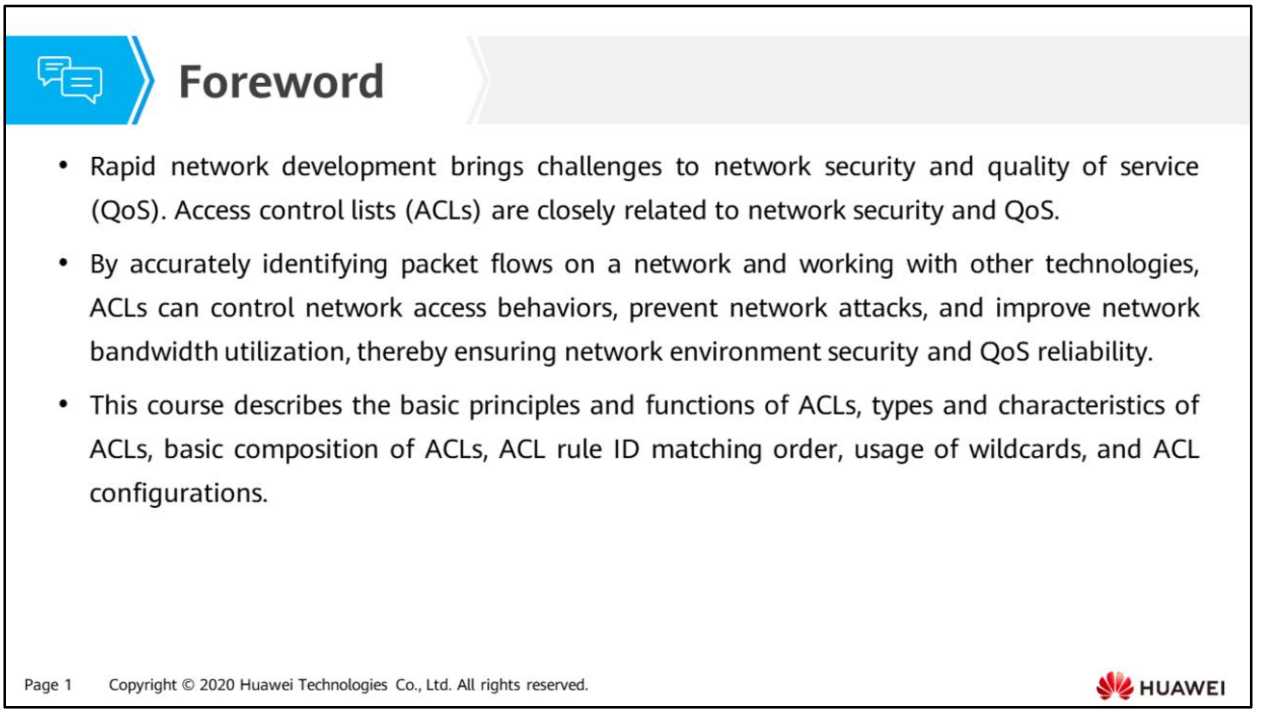
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



ACL Principles and Configuration

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Note:
  - The implementation of ACLs varies with vendors. This course describes the ACL technology implemented on Huawei devices.
  - A local area network (LAN) is a computer network that connects computers in a limited area, such as a residential area, a school, a lab, a college campus, or an office building.

Objectives

- On completion of this course, you will be able to:
  - Describe the basic principles and functions of ACLs.
  - Understand the types and characteristics of ACLs.
  - Describe the basic composition of ACLs and ACL rule ID matching order.
  - Understand how to use wildcards in ACLs.
  - Complete the basic configurations of ACLs.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

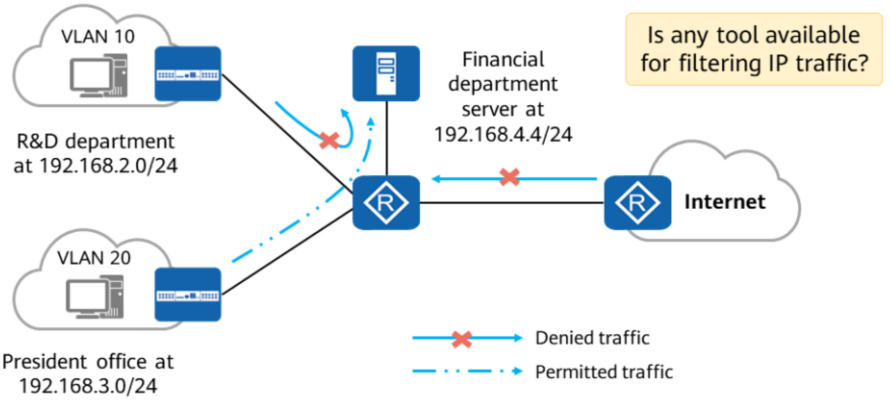
Contents

1. **ACL Overview**
2. Basic Concepts and Working Mechanism of ACLs
3. Basic Configurations and Applications of ACLs

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Background: A Tool Is Required to Filter Traffic



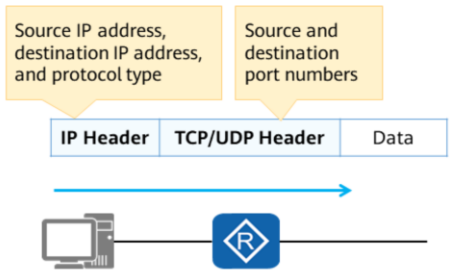
- To ensure financial data security, an enterprise prohibits the R&D department's access to the financial department server but allows the president office's access to the financial department server.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Rapid network development brings the following issues to network security and QoS:
  - Resources on the key servers of an enterprise are obtained without permission, and confidential information of the enterprise leaks, causing a potential security risk to the enterprise.
  - The virus on the Internet spreads to the enterprise intranet, threatening intranet security.
  - Network bandwidth is occupied by services randomly, and bandwidth for delay-sensitive services such as voice and video cannot be guaranteed, lowering user experience.
- These issues seriously affect network communication, so network security and QoS need to be improved urgently. For example, a tool is required to filter traffic.

ACL Overview

- An ACL is a set of sequential rules composed of permit or deny statements.
- An ACL matches and distinguishes packets.



ACL Application

- Matching IP traffic
- Invoked in a traffic filter
- Invoked in network address translation (NAT)
- Invoked in a routing policy
- Invoked in a firewall policy
- Invoked in QoS
- Others

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- ACLs accurately identify and control packets on a network to manage network access behaviors, prevent network attacks, and improve bandwidth utilization. In this way, ACLs ensure security and QoS.
  - An ACL is a set of sequential rules composed of permit or deny statements. It classifies packets by matching fields in packets.
  - An ACL can match elements such as source and destination IP addresses, source and destination port numbers, and protocol types in IP datagrams. It can also match routes.
- In this course, traffic filtering is used to describe ACLs.

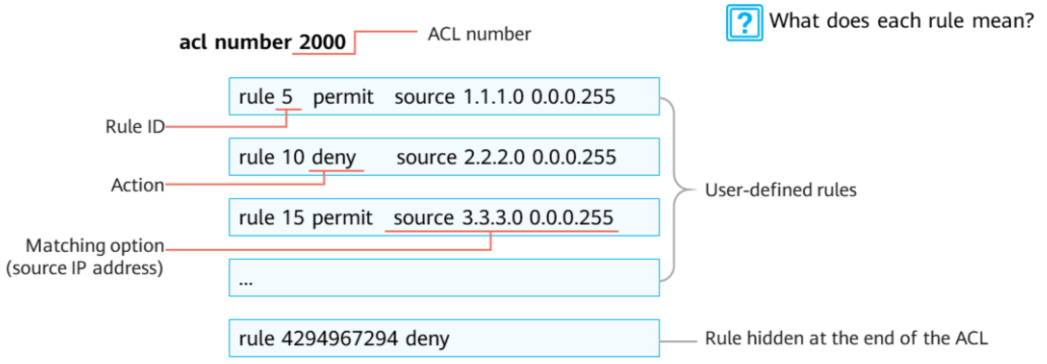
Contents

1. ACL Overview
2. **Basic Concepts and Working Mechanism of ACLs**
3. Basic Configurations and Applications of ACLs

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

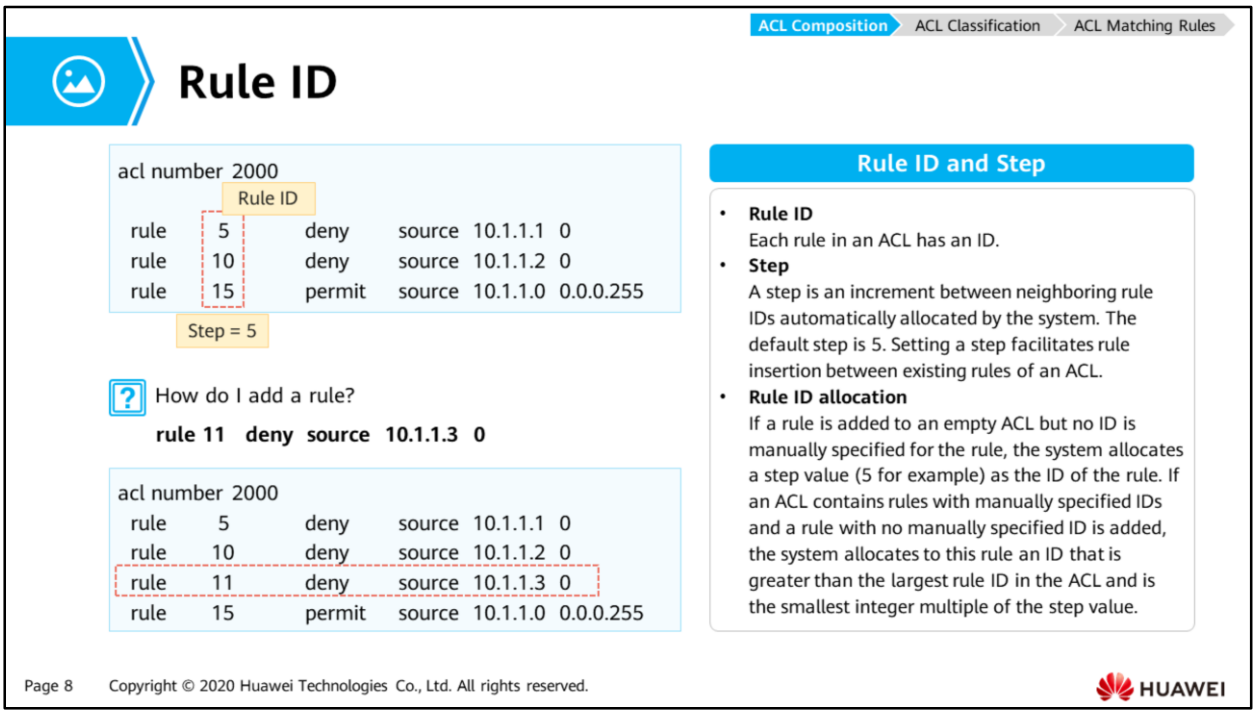
ACL Composition

- An ACL consists of several permit or deny statements. Each statement is a rule of the ACL, and permit or deny in each statement is the action corresponding to the rule.

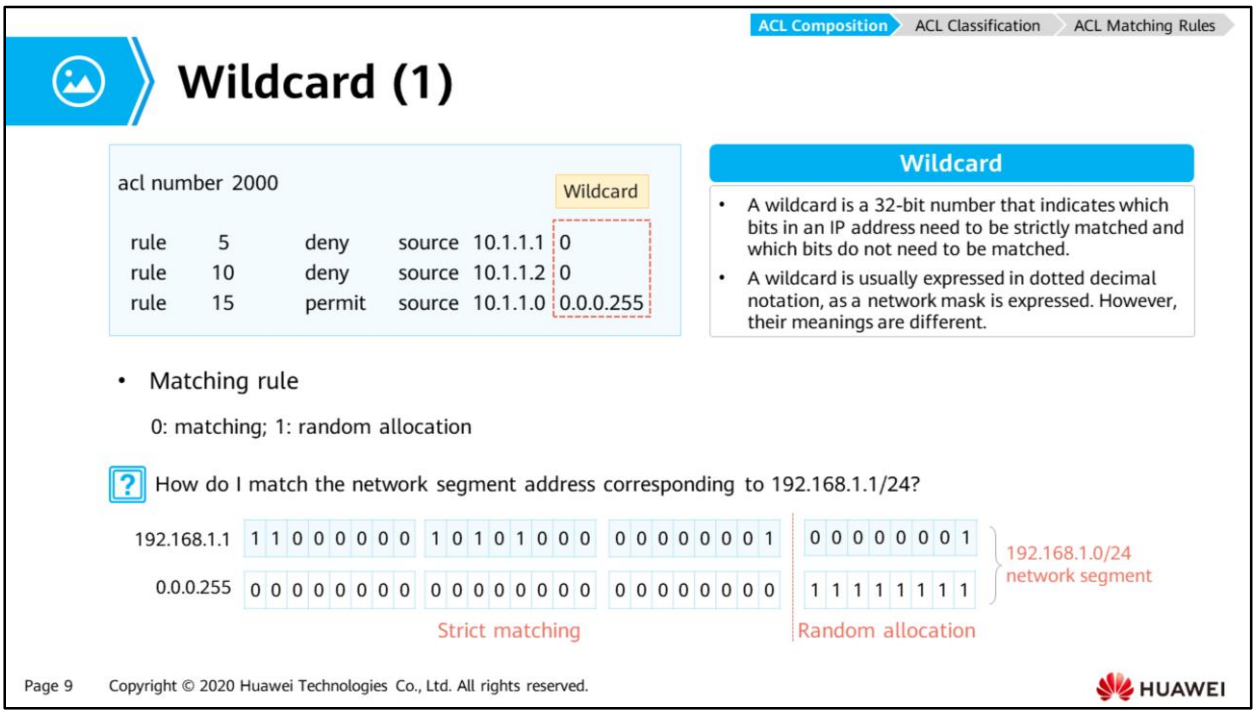


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

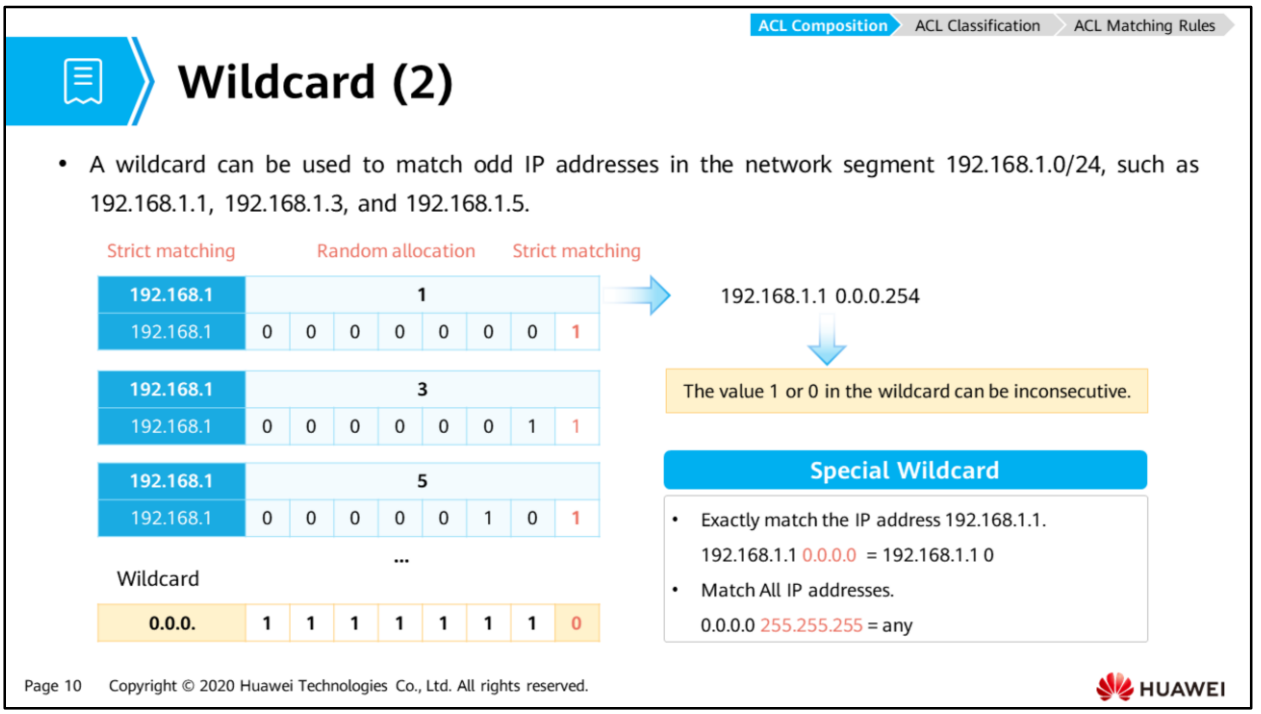
- ACL composition:
  - ACL number: An ACL is identified by an ACL number. Each ACL needs to allocated an ACL number. The ACL number range varies according to the ACL type, which will be described later.
  - Rule: As mentioned above, an ACL consists of several permit/deny statements, and each statement is a rule of the ACL.
  - Rule ID: Each ACL rule has an ID, which identifies the rule. Rule IDs can be manually defined or automatically allocated by the system. A rule ID ranges from 0 to 4294967294. All rules are arranged in the ascending order of rule ID.
  - Action: Each rule contains a permit or deny action. ACLs are usually used together with other technologies, and the meanings of the permit and deny actions may vary according to scenarios.
    - For example, if an ACL is used together with traffic filtering technology (that is, the ACL is invoked in traffic filtering), the permit action allows traffic to pass and the deny action rejects traffic.
  - Matching option: ACLs support various matching options. In this example, the matching option is a source IP address. The ACL also supports other matching options, such as Layer 2 Ethernet frame header information (including source and destination MAC addresses and Ethernet frame protocol type), Layer 3 packet information (including destination address and protocol type), and Layer 4 packet information (including TCP/UDP port number).
- Question: What does rule 5 permit source 1.1.1.0 0.0.0.255 mean? This will be introduced later.



- Rule ID and step:
  - Rule ID: Each ACL rule has an ID, which identifies the rule. Rule IDs can be manually defined or automatically allocated by the system.
  - Step: When the system automatically allocates IDs to ACL rules, the increment between neighboring rule IDs is called a step. The default step is 5. Therefore, rule IDs are 5, 10, 15, and so on.
    - If a rule is manually added to an ACL but no ID is specified, the system allocates to this rule an ID that is greater than the largest rule ID in the ACL and is the smallest integer multiple of the step value.
    - The step can be changed. For example, if the step is changed to 2, the system automatically renumbers the rule IDs as 2, 4, 6...
- What is the function of a step? Why can't rules 1, 2, 3, and 4 be directly used?
  - First, let's look at a question. How do I add a rule?
  - We can manually add rule 11 between rules 10 and 15.
  - Therefore, setting a step of a certain length facilitates rule insertion between existing rules.



- When an IP address is matched, a 32-bit mask is followed. The 32-bit mask is called a wildcard.
- A wildcard is also expressed in dotted decimal notation. After the value is converted to a binary number, the value 0 indicates that the equivalent bit must match and the value 1 indicates that the equivalent bit does not matter.
- Let's look at two rules:
  - rule 5: denies the packets with the source IP address 10.1.1.1. Because the wildcard comprises all 0s, each bit must be strictly matched. Specifically, the host IP address 10.1.1.1 is matched.
  - rule 15: permits the packets with the source IP address on the network segment 10.1.1.0/24. The wildcard is 0.0.0.11111111, and the last eight bits are 1s, indicating that the bits do not matter. Therefore, the last eight bits of 10.1.1.xxxxxxxx can be any value, and the 10.1.1.0/24 network segment is matched.
- For example, if we want to exactly match the network segment address corresponding to 192.168.1.1/24, what is the wildcard?
  - It can be concluded that the network bits must be strictly matched and the host bits do not matter. Therefore, the wildcard is 0.0.0.255.



- How do I set the wildcard to match the odd IP addresses in the network segment 192.168.1.0/24?
  - First, let's look at the odd IP addresses, such as 192.168.1.1, 192.168.1.5, and 192.168.1.11.
  - After the last eight bits are converted into binary numbers, the corresponding addresses are 192.168.1.00000001, 192.168.1.00000101, and 192.168.1.00001011.
  - We can see the common points. The seven most significant bits of the last eight bits can be any value, and the least significant bit is fixed to 1. Therefore, the answer is 192.168.1.1 0.0.0.254 (0.0.0.11111110).
- In conclusion, 1 or 0 in a wildcard can be inconsecutive.

- There are two special wildcards.
  - If a wildcard comprising all 0s is used to match an IP address, the address is exactly matched.
  - If a wildcard comprising all 1s is used to match 0.0.0.0, all IP addresses are matched.

ACL Classification and Identification

- ACL classification based on ACL rule definition methods

Category	Number Range	Description
Basic ACL	2000 to 2999	Defines rules based on source IPv4 addresses, fragmentation information, and effective time ranges.
Advanced ACL	3000 to 3999	Defines rules based on source and destination IPv4 addresses, IPv4 protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and effective time ranges.
Layer 2 ACL	4000 to 4999	Defines rules based on information in Ethernet frame headers of packets, such as source and destination MAC addresses and Layer 2 protocol types.
User-defined ACL	5000 to 5999	Defines rules based on packet headers, offsets, character string masks, and user-defined character strings.
User ACL	6000 to 6999	Defines rules based on source IPv4 addresses or user control list (UCL) groups, destination IPv4 addresses or destination UCL groups, IPv4 protocol types, ICMP types, TCP source/destination port numbers, and UDP source/destination port numbers.

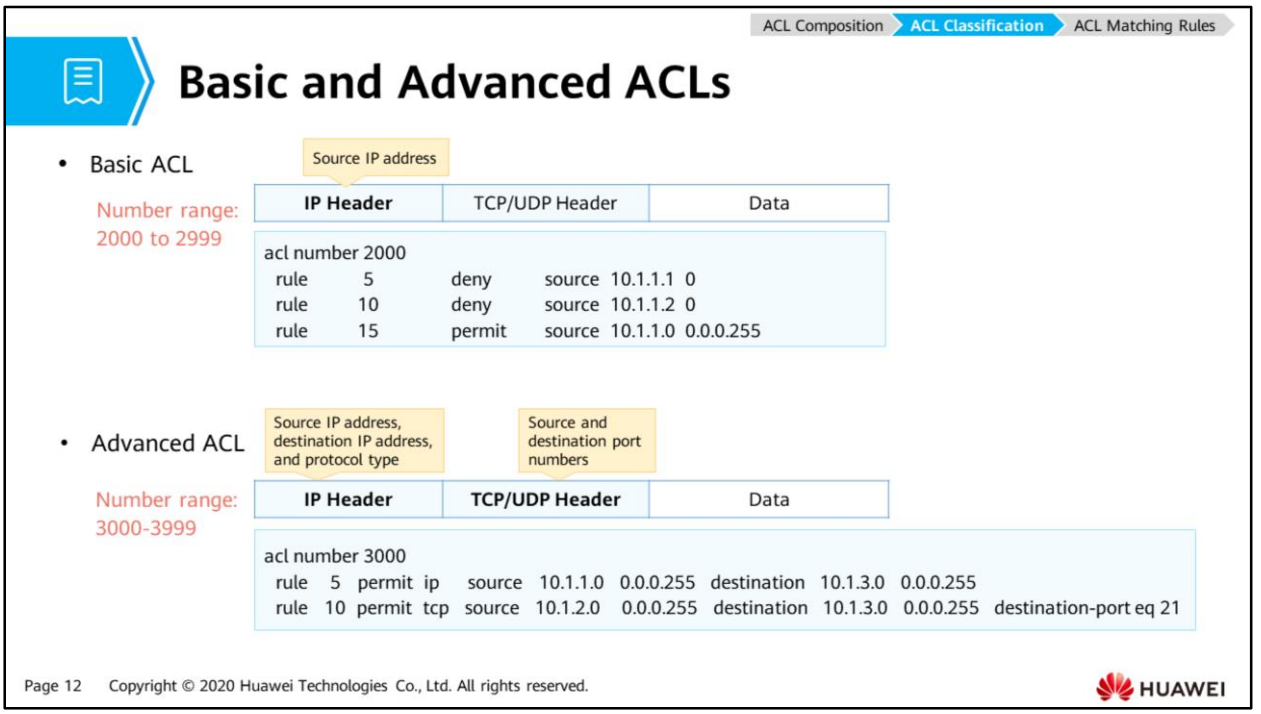
- ACL classification based on ACL identification methods

Category	Description
Numbered ACL	Traditional ACL identification method. A numbered ACL is identified by a number.
Named ACL	A named ACL is identified by a name.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

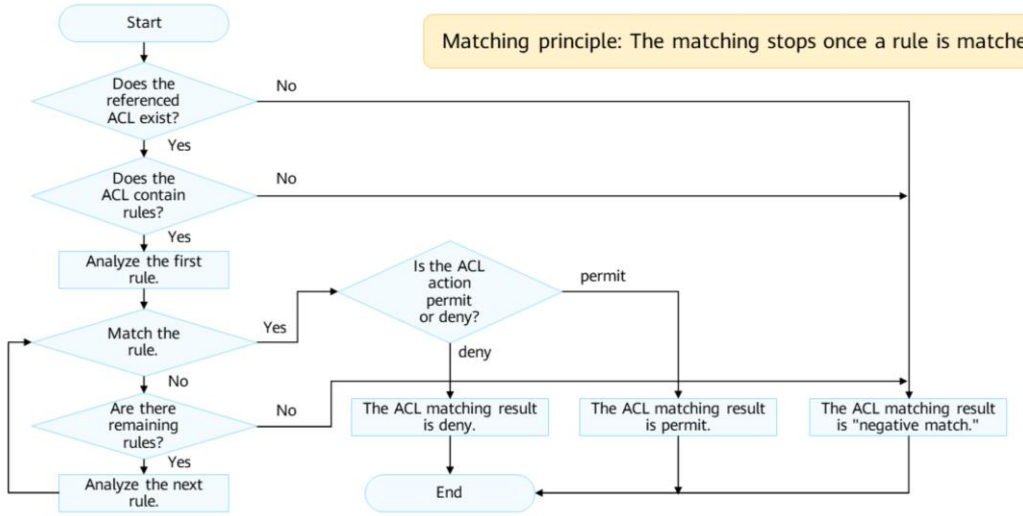
- Based on ACL rule definition methods, ACLs can be classified into the following types:
  - Basic ACL, advanced ACL, Layer 2 ACL, user-defined ACL, and user ACL
- Based on ACL identification methods, ACLs can be classified into the following types:
  - Numbered ACL and named ACL

- Note: You can specify a number for an ACL. The ACLs of different types have different number ranges. You can also specify a name for an ACL to help you remember the ACL's purpose. A named ACL consists of a name and number. That is, you can specify an ACL number when you define an ACL name. If you do not specify a number for a named ACL, the system automatically allocates a number to it.



- Basic ACL:
  - A basic ACL is used to match the source IP address of an IP packet. The number of a basic ACL ranges from 2000 to 2999.
  - In this example, ACL 2000 is created. This ACL is a basic ACL.
- Advanced ACL:
  - An advanced ACL can be matched based on elements such as the source IP address, destination IP address, protocol type, and TCP or UDP source and destination port numbers in an IP packet. A basic ACL can be regarded as a subset of an advanced ACL. Compared with a basic ACL, an advanced ACL defines more accurate, complex, and flexible rules.

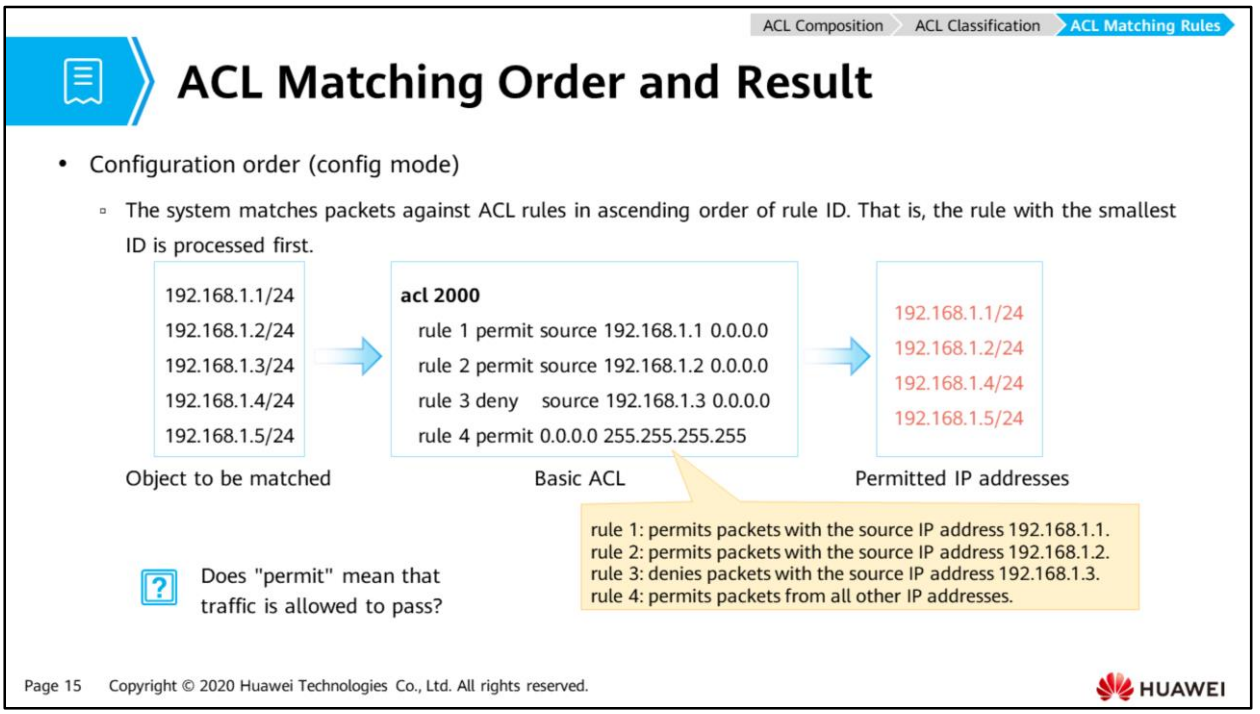
ACL Matching Mechanism



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The ACL matching mechanism is as follows:
  - After receiving a packet, the device configured with an ACL matches the packet against ACL rules one by one. If the packet does not match any ACL rule, the device attempts to match the packet against the next ACL rule.
  - If the packet matches an ACL rule, the device performs the action defined in the rule and stops the matching.
- Matching process: The device checks whether an ACL is configured.
  - If no ACL is configured, the device returns the result "negative match."
  - If an ACL is configured, the device checks whether the ACL contains rules.
    - If the ACL does not contain rules, the device returns the result "negative match."
    - If the ACL contains rules, the device matches the packet against the rules in ascending order of rule ID.
      - If the packet matches a permit rule, the device stops matching and returns the result "positive match (permit)."
      - If the packet matches a deny rule, the device stops matching and returns the result "positive match (deny)."
      - If the packet does not match any rule in the ACL, the device returns the result "negative match."

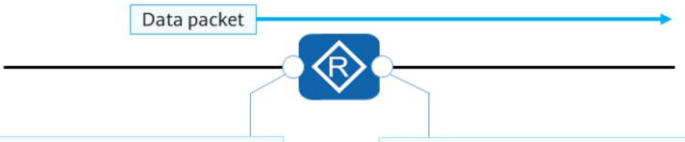
- The ACL matching results include "positive match" and "negative match."
  - Positive match: Packets match a rule in an ACL. The result is "positive match" regardless of whether packets match a permit or deny rule in an ACL.
  - Negative match: No ACL exists, the ACL does not contain rules, or packets do not match any rule in an ACL.
- Matching principle: The matching stops once a rule is matched.



- An ACL can consist of multiple deny or permit statements. Each statement describes a rule. Rules may overlap or conflict. Therefore, the ACL matching order is very important.
- Huawei devices support two matching orders: automatic order (auto) and configuration order (config). The default matching order is config.
    - auto: The system arranges rules according to the precision of the rules ("depth first" principle), and matches packets against the rules in descending order of precision. ––This is complicated and is not detailed here. If you are interested in it, you can view related materials after class.
    - config: The system matches packets against ACL rules in ascending order of rule ID. That is, the rule with the smallest ID is processed first. ––This is the matching order mentioned above.
        - If another rule is added, the rule is added to the corresponding position, and packets are still matched in ascending order.
- Matching result:
    - First, let's understand the meaning of ACL 2000.
        - rule 1: permits packets with the source IP address 192.168.1.1.
        - rule 2: permits packets with the source IP address 192.168.1.2.
        - rule 3: denies packets with the source IP address 192.168.1.3.
        - rule 4: permits packets from all other IP addresses.

    - When packets with the source IP address 192.168.1.3 pass through the device configured with the ACL:
        - The device matches the packets against rule 1. The matching result is "negative match."
        - The device continues to match the packets against rule 2. The matching result is still "negative match."
        - The device continues to match the packets against rule 3. The matching result is "positive match," and the action is deny.
- Note: ACLs are usually used together with other technologies, and the meanings of the permit and deny actions may vary according to scenarios.For example, if an ACL is used together with traffic filtering technology (that is, the ACL is invoked in traffic filtering), the permit action allows traffic to pass and the deny action rejects traffic.

ACL Matching Position

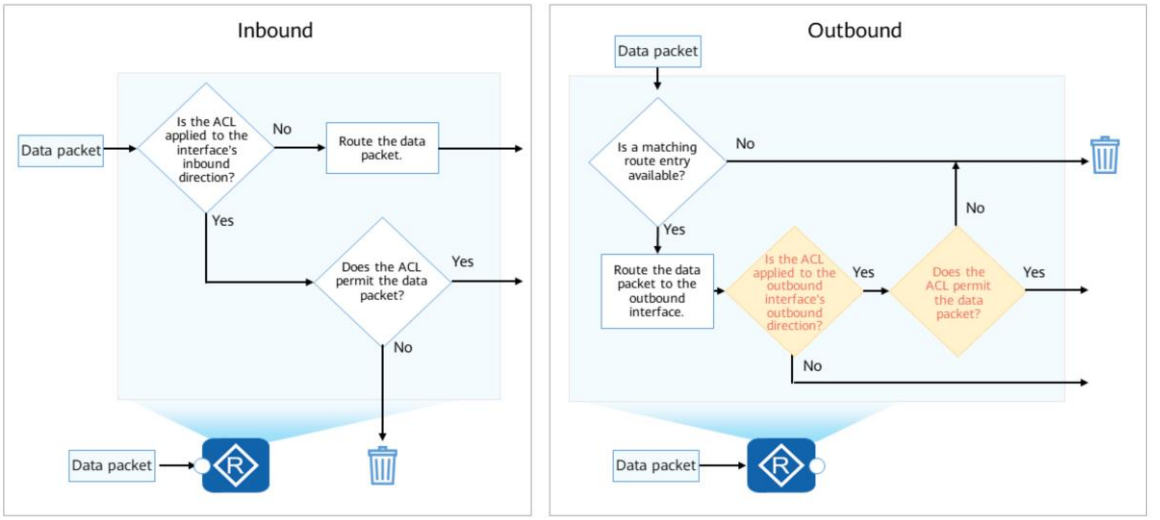


Configure an ACL on the interface. To enable the ACL to take effect for the data packet shown in the figure, apply the ACL to the inbound direction.

Configure an ACL on the interface. To enable the ACL to take effect for the data packet shown in the figure, apply the ACL to the outbound direction.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Inbound and Outbound Directions



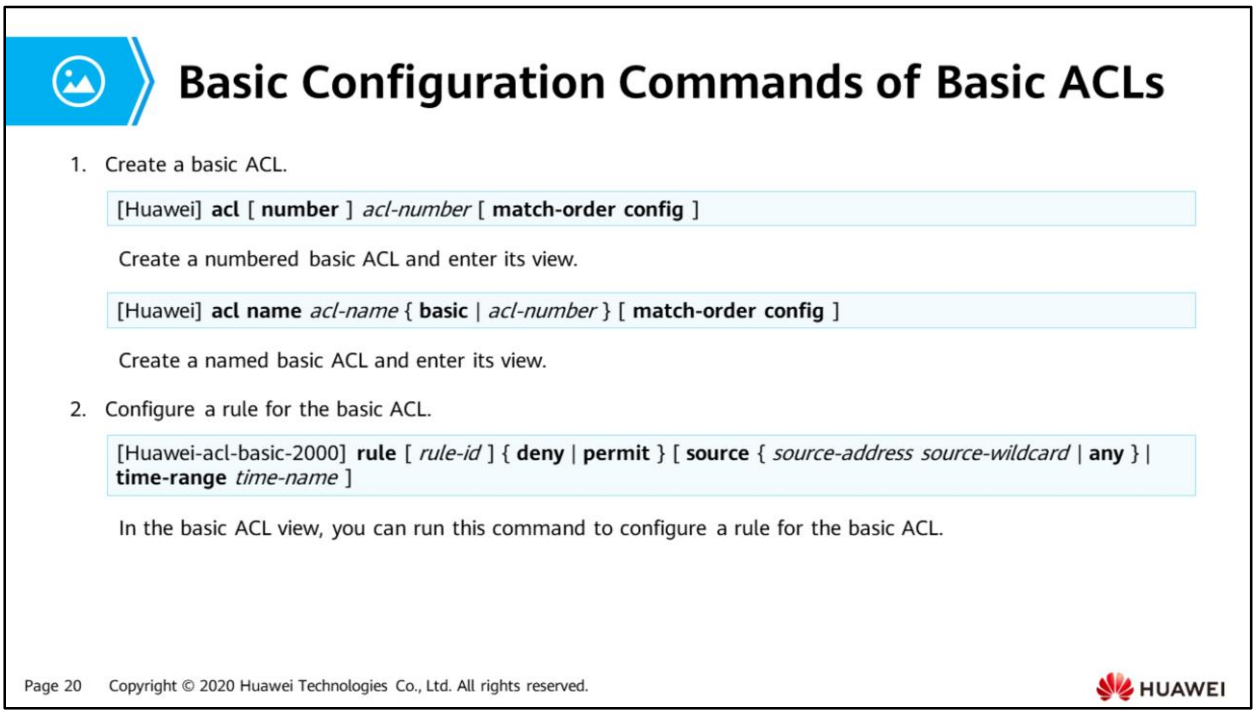
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. ACL Overview
2. Basic Concepts and Working Mechanism of ACLs
3. **Basic Configurations and Applications of ACLs**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

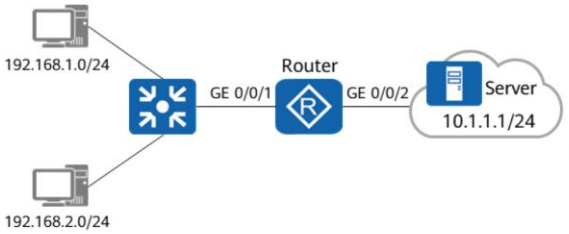
HUAWEI



- Create a basic ACL.
- [Huawei] **acl** [**number**] *acl-number* [**match-order config**]
  - *acl-number*: specifies the number of an ACL.
  - **match-order config**: indicates the matching order of ACL rules. config indicates the configuration order.
- [Huawei] **acl name** *acl-name* { **basic** | *acl-number* } [**match-order config**]
  - *acl-name*: specifies the name of an ACL.
  - **basic**: indicates a basic ACL.
- Configure a rule for the basic ACL.
- [Huawei-acl-basic-2000] **rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*]
  - *rule-id*: specifies the ID of an ACL rule.
  - **deny**: denies the packets that match the rule.
  - **permit**: permits the packets that match the rule.

- **source** { *source-address source-wildcard* | **any** }: specifies the source IP address of packets that match the ACL rule. If no source address is specified, packets with any source addresses are matched.
  - *source-address*: specifies the source IP address of packets.
  - *source-wildcard*: specifies the wildcard of the source IP address.
  - **any**: indicates any source IP address of packets. That is, the value of source-address is 0.0.0.0 or the value of source-wildcard is 255.255.255.255.
- **time-range** *time-name*: specifies a time range in which the ACL rule takes effect. time-name specifies the name of a time range. If no time range is specified, the ACL rule is always valid.

Case: Use a Basic ACL to Filter Data Traffic



- Requirements:

  To prevent the user host on the network segment 192.168.1.0/24 from accessing the network where the server resides, configure a basic ACL on the router. After the configuration is complete, the ACL filters out the data packets whose source IP addresses are on the network segment 192.168.1.0/24 and permits other data packets.

1. Configure IP addresses and routes on the router.

2. Create a basic ACL on the router to prevent the network segment 192.168.1.0/24 from accessing the network where the server resides.

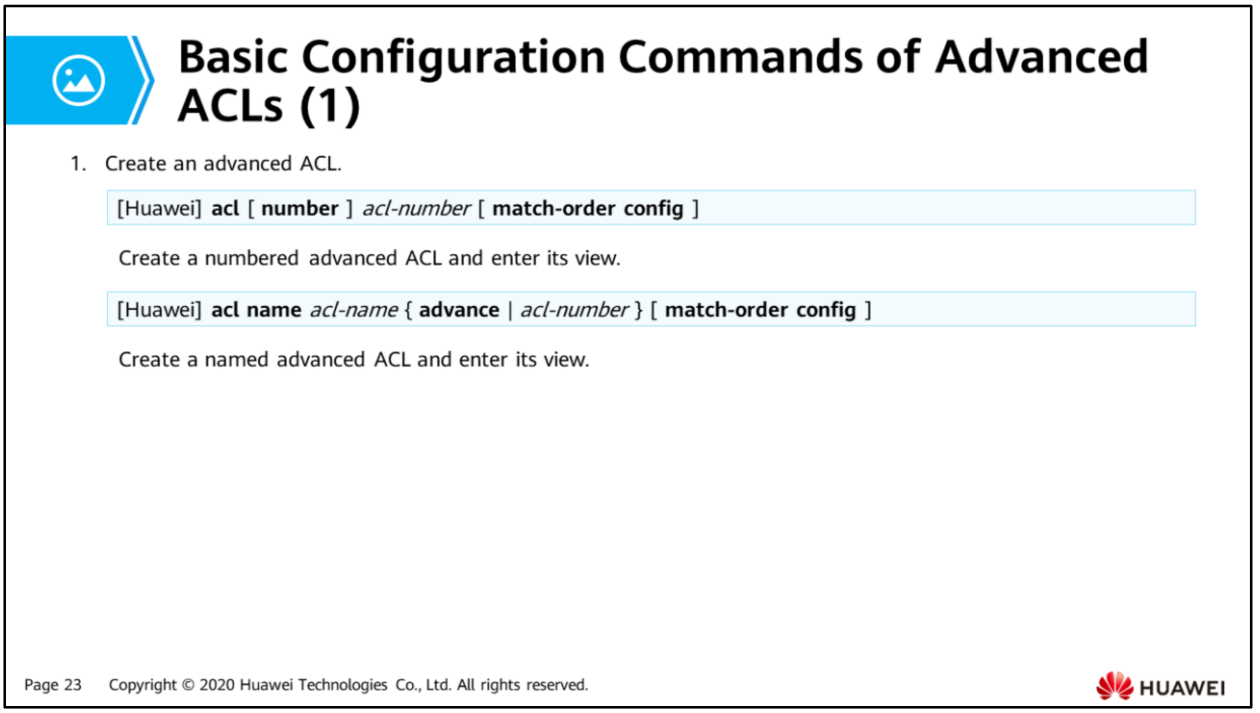
```
[Router] acl 2000
[Router-acl-basic-2000] rule deny source 192.168.1.0  0.0.0.255
[Router-acl-basic-2000] rule permit source any
```

3. Configure traffic filtering in the inbound direction of GE 0/0/1.

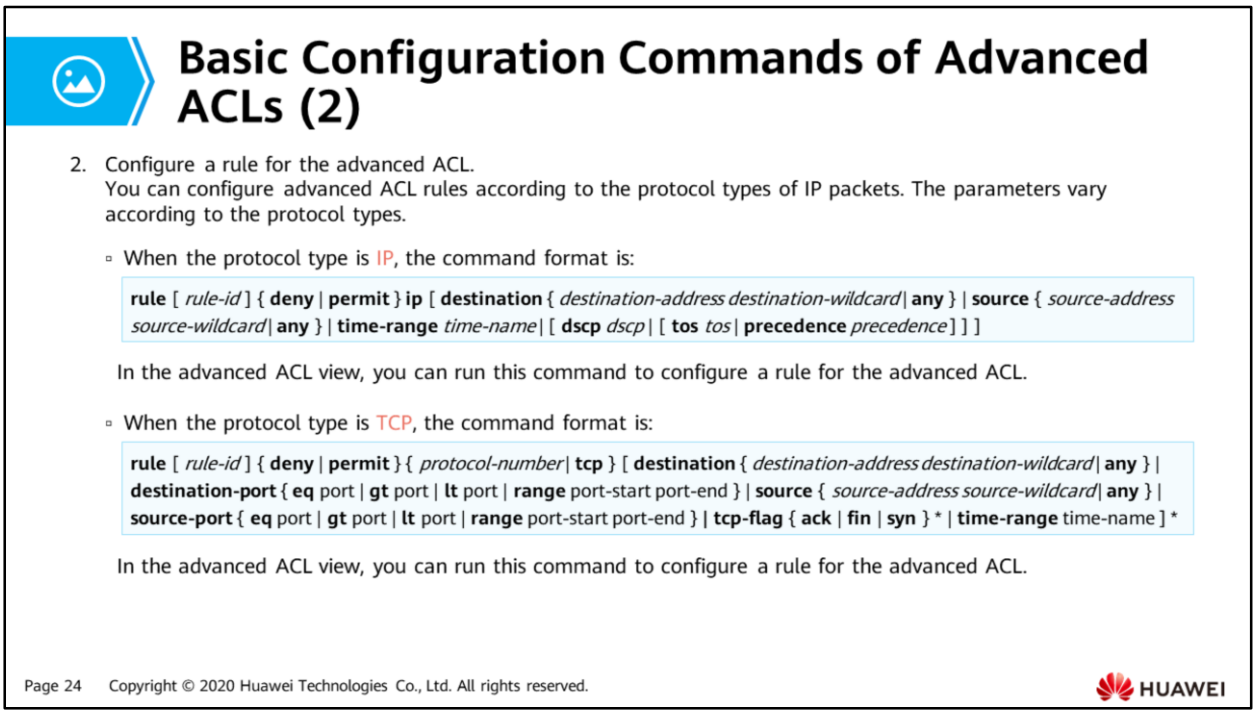
```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-filter inbound acl 2000
[Router-GigabitEthernet0/0/1] quit
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Configuration roadmap:
  - Configure a basic ACL and traffic filtering to filter packets from a specified network segment.
- Procedure:
  1. Configure IP addresses and routes on the router.
  2. Create ACL 2000 and configure ACL rules to deny packets from the network segment 192.168.1.0/24 and permit packets from other network segments.
  3. Configure traffic filtering.
- Note:
  - The **traffic-filter** command applies an ACL to an interface to filter packets on the interface.
  - Command format: **traffic-filter** { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }
    - **inbound**: configures ACL-based packet filtering in the inbound direction of an interface.
    - **outbound**: configures ACL-based packet filtering in the outbound direction of an interface.
    - **acl**: filters packets based on an IPv4 ACL.



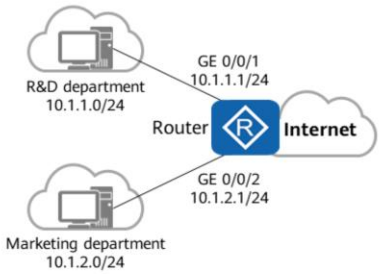
- Create an advanced ACL.
- [Huawei] **acl** [**number**] *acl-number* [**match-order config**]
  - *acl-number*: specifies the number of an ACL.
  - **match-order config**: indicates the matching order of ACL rules. config indicates the configuration order.
- [Huawei] **acl name** *acl-name* { **advance** | *acl-number* } [**match-order config**]
  - *acl-name*: specifies the name of an ACL.
  - **advance**: indicates an advanced ACL.



- Configure a rule for the advanced ACL.
- When the protocol type is IP:
  - **rule** [*rule-id*] { **deny** | **permit** } **ip** [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*]]]
    - **ip**: indicates that the protocol type is IP.
    - **destination** { *destination-address destination-wildcard* | any }: specifies the destination IP address of packets that match the ACL rule. If no destination address is specified, packets with any destination addresses are matched.
    - **dscp** *dscp*: specifies the differentiated services code point (DSCP) of packets that match the ACL rule. The value ranges from 0 to 63.
    - **tos** *tos*: specifies the ToS of packets that match the ACL rule. The value ranges from 0 to 15.
    - **precedence** *precedence*: specifies the precedence of packets that match the ACL rule. The value ranges from 0 to 7.

- When the protocol type is TCP:
  - **rule** [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **syn** } * | **time-range** *time-name*] *
    - **tcp**: indicates that the protocol type is TCP. You can set protocol-number to 6 to indicate TCP.
    - **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }: specifies the TCP destination port number of packets that match the ACL rule. The value is valid only when the protocol type is TCP. If no destination port number is specified, packets with any TCP destination port numbers are matched.
      - **eq** *port*: equal to the destination port number
      - **gt** *port*: greater than the destination port number
      - **lt** *port*: less than the destination port number
      - **range** *port-start port-end*: specifies a source port number range.
    - **tcp-flag**: indicates the SYN Flag in the TCP packet header.

Case: Use Advanced ACLs to Prevent User Hosts on Different Network Segments from Communicating (1)



Requirements:

- The departments of a company are connected through the router. To facilitate network management, the administrator allocates IP addresses of different network segments to the R&D and marketing departments.
- The company requires that the router prevent the user hosts on different network segments from communicating to ensure information security.

1. Configure IP addresses and routes on the router.

2. Create ACL 3001 and configure rules for the ACL to deny packets from the R&D department to the marketing department.

```
[Router] acl 3001
[Router-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255
destination 10.1.2.0 0.0.0.255
[Router-acl-adv-3001] quit
```

3. Create ACL 3002 and configure rules for the ACL to deny packets from the marketing department to the R&D department.

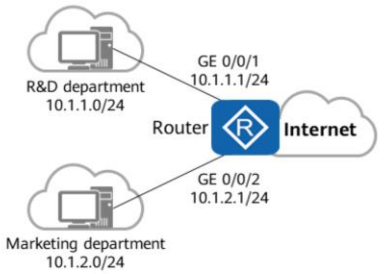
```
[Router] acl 3002
[Router-acl-adv-3002] rule deny ip source 10.1.2.0 0.0.0.255
destination 10.1.1.0 0.0.0.255
[Router-acl-adv-3002] quit
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Configuration roadmap:
  - Configure an advanced ACL and traffic filtering to filter the packets exchanged between the R&D and marketing departments.
- Procedure:
  1. Configure IP addresses and routes on the router.
  2. Create ACL 3001 and configure rules for the ACL to deny packets from the R&D department to the marketing department.
  3. Create ACL 3002 and configure rules for the ACL to deny packets from the marketing department to the R&D department.

Case: Use Advanced ACLs to Prevent User Hosts on Different Network Segments from Communicating (2)



Requirements:

- The departments of a company are connected through the router. To facilitate network management, the administrator allocates IP addresses of different network segments to the R&D and marketing departments.
- The company requires that the router prevent the user hosts on different network segments from communicating to ensure information security.

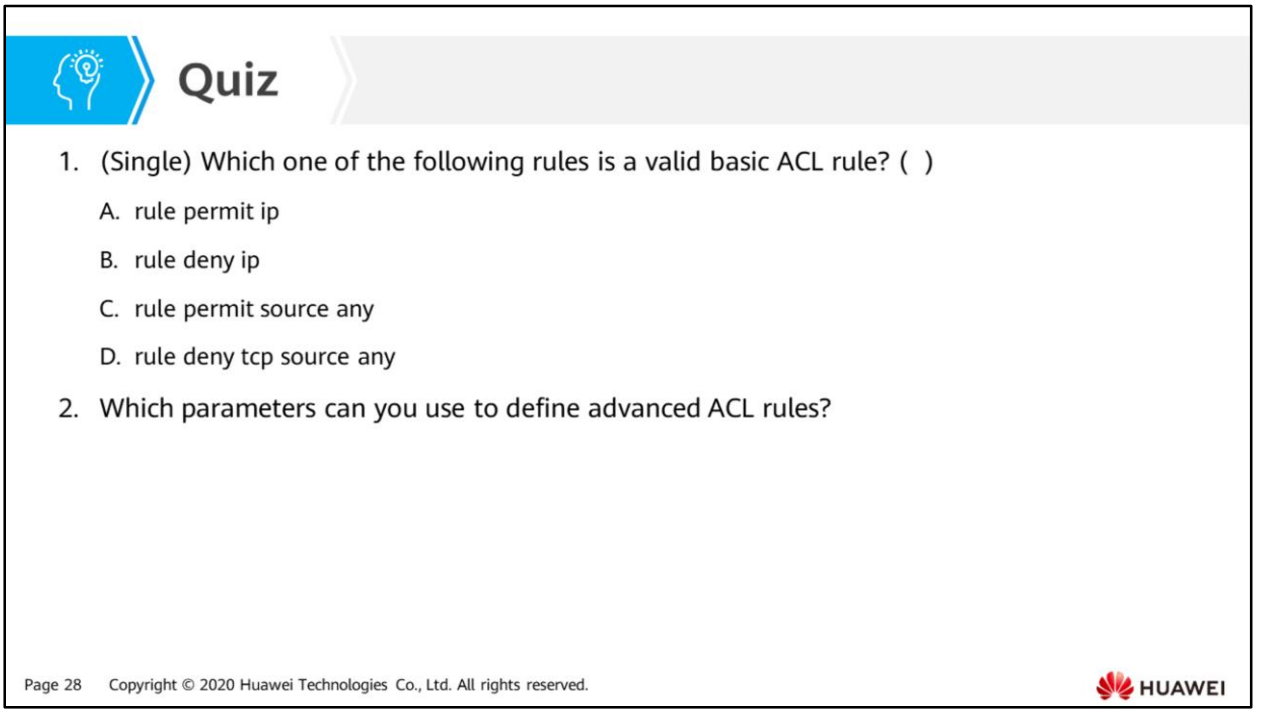
4. Configure traffic filtering in the inbound direction of GE 0/0/1 and GE 0/0/2.

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-filter inbound acl 3001
[Router-GigabitEthernet0/0/1] quit

[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-filter inbound acl 3002
[Router-GigabitEthernet0/0/2] quit
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Procedure:
  4. Configure traffic filtering in the inbound direction of GE 0/0/1 and GE 0/0/2.
- Note:
  - The **traffic-filter** command applies an ACL to an interface to filter packets on the interface.
  - Command format: **traffic-filter** { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }
    - **inbound**: configures ACL-based packet filtering in the inbound direction of an interface.
    - **outbound**: configures ACL-based packet filtering in the outbound direction of an interface.
    - **acl**: filters packets based on an IPv4 ACL.



1. C
2. parameters such as the source/destination IP address, source/destination port number, protocol type, and TCP flag (SYN, ACK, or FIN).

Summary

- ACL is a widely used network technology. Its principle is as follows: packets are matched against configured ACL rules and actions are taken on the packets as configured in the ACL rules. The matching rules and actions are configured based on network requirements. Due to the variety of matching rules and actions, ACLs can implement a lot of functions.
- ACLs are often used with other technologies, such as firewall, routing policy, QoS, and traffic filtering.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



AAA Principles and Configuration

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- User management is one of the most basic security management requirements for any network.
- Authentication, authorization, and accounting (AAA) is a management framework that provides a security mechanism for authorizing some users to access specified resources and recording the operations of these users. AAA is widely used because of its good scalability and easy implementation of centralized management of user information. AAA can be implemented through multiple protocols. In actual applications, the Remote Authentication Dial-In User Service (RADIUS) protocol is the most commonly used to implement AAA.
- This course describes the basic concepts, implementation, basic configurations, and typical application scenarios of AAA.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- Upon completion of this course, you will be able to:
  - Understand the fundamentals of AAA.
  - Describe the application scenarios of AAA.
  - Understand the fundamentals of RADIUS.
  - Get familiar with the basic configurations of AAA.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

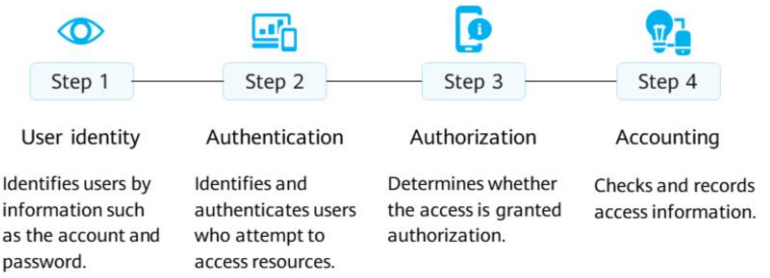
Contents

1. **AAA Overview**
2. AAA Configuration

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic Concepts of AAA

- Authentication, authorization, and accounting (AAA) provides a management mechanism for network security.

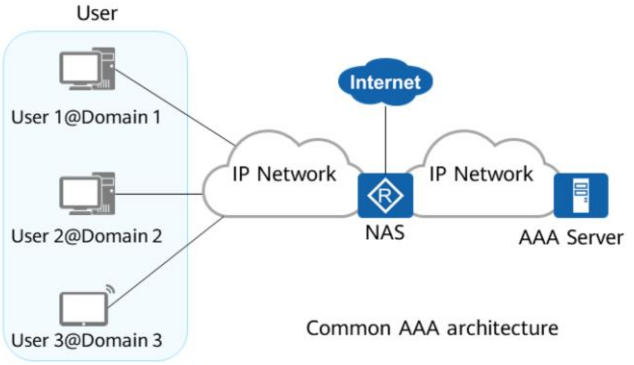


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Authentication: determines which users can access the network.
- Authorization: authorizes users to access specific services.
- Accounting: records network resource utilization.
- The Internet service provider (ISP) needs to authenticate the account and password of a home broadband user before allowing the user to access the Internet. In addition, the ISP records the online duration or traffic of the user. This is the most common application scenario of the AAA technology.

Common AAA Architecture

- A common AAA architecture includes the user, network access server (NAS), and AAA server.



Common AAA architecture

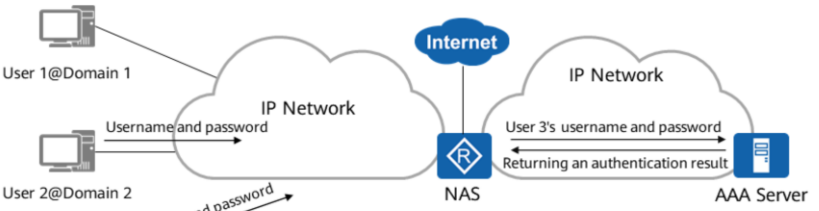
- The NAS collects and manages user access requests in a centralized manner.
- Multiple domains are created on the NAS to manage users. Different domains can be associated with different AAA schemes, which include the authentication scheme, authorization scheme, and accounting scheme.
- When receiving a user access request, the NAS determines the domain to which the user belongs based on the username and performs user management and control based on the AAA schemes configured for the domain.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The NAS manages users based on domains. Each domain can be configured with different authentication, authorization, and accounting schemes to perform authentication, authorization, and accounting for users in the domain.
- Each user belongs to a domain. The domain to which a user belongs is determined by the character string following the domain name delimiter @ in the user name. For example, if the user name is user 1@domain 1, the user belongs to domain 1. If the user name does not end with @, the user belongs to the default domain.

Authentication

- AAA supports the following authentication modes: non-authentication, local authentication, and remote authentication.



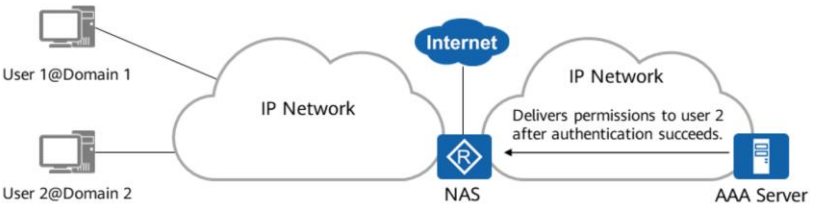
User	Domain	Authentication Mode
User 1@Domain 1	Domain 1	Non-authentication
User 2@Domain 2	Domain 2	Local authentication
User 3@Domain 3	Domain 3	Remote authentication

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- AAA supports three authentication modes:
  - Non-authentication: Users are fully trusted and their identities are not checked. This authentication mode is seldom used for security purposes.
  - Local authentication: Local user information (including the username, password, and attributes) is configured on the NAS. In this case, the NAS functions as the AAA server. Local authentication features fast processing and low operational costs. The disadvantage is that the amount of stored information is limited by device hardware. This authentication mode is often used to manage login users, such as Telnet and FTP users.
  - Remote authentication: User information (including the username, password, and attributes) is configured on the authentication server. Remote authentication can be implemented through RADIUS or HWTACACS. The NAS functions as a client to communicate with the RADIUS or HWTACACS server.

Authorization

- AAA supports the following authorization modes: non-authorization, local authorization, and remote authorization.
- Authorization information includes the user group, VLAN ID, and ACL number.



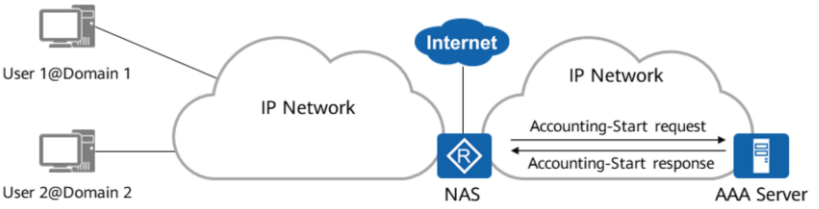
User	Domain	Authorization Mode	Authorization Content
User 1@Domain 1	Domain 1	Non-authorization	None
User 2@Domain 2	Domain 2	Local authorization	Internet access is allowed.
User 3@Domain 3	Domain 3	Remote authorization	Authorization is granted by a remote server.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- The AAA authorization function grants users the permission to access specific networks or devices. AAA supports the following authorization modes:
  - Non-authorization: Authenticated users have unrestricted access rights on a network.
  - Local authorization: Users are authorized based on the domain configuration on the NAS.
  - Remote authorization: The RADIUS or HWTACACS server authorizes users.
    - In HWTACACS authorization, all users can be authorized by the HWTACACS server.
    - RADIUS authorization applies only to the users authenticated by the RADIUS server. RADIUS integrates authentication and authorization. Therefore, RADIUS authorization cannot be performed singly.
- When remote authorization is used, users can obtain authorization information from both the authorization server and NAS. The priority of the authorization information configured on the NAS is lower than that delivered by the authorization server.

Accouting

- The accounting function monitors the network behavior and network resource utilization of authorized users.
- AAA supports two accounting modes: non-accounting and remote accounting.



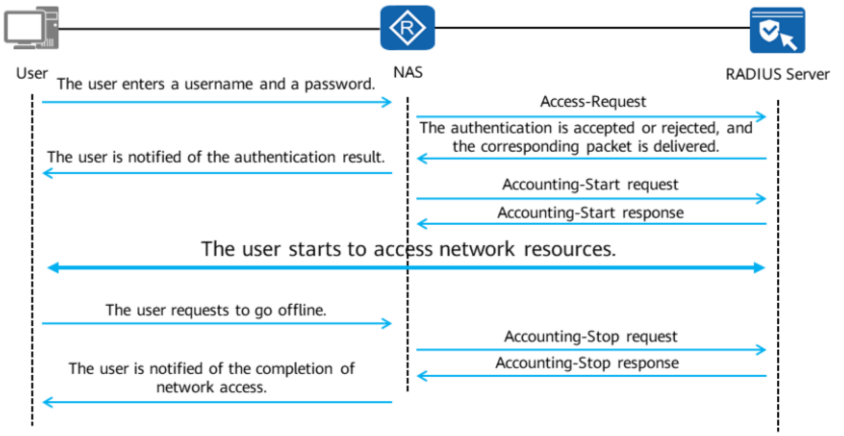
User	Domain	Accounting Mode
User 1@Domain 1	Domain 1	Non-accounting
User 2@Domain 2	Domain 2	Non-accounting
User 3@Domain 3	Domain 3	Remote accounting

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- AAA supports the following accounting modes:
  - Non-accounting: Users can access the Internet for free, and no activity log is generated.
  - Remote accounting: Remote accounting is performed through the RADIUS server or HWTACACS server.

AAA Implementation Protocol - RADIUS

- Of the protocols that are used to implement AAA, RADIUS is the most commonly used.



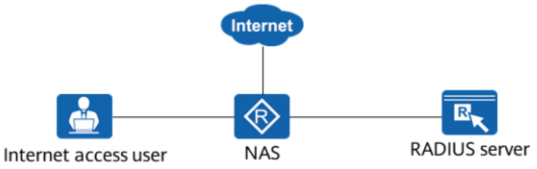
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Of the protocols that are used to implement AAA, RADIUS is the most commonly used. RADIUS is a distributed information exchange protocol based on the client/server structure. It implements user authentication, accounting, and authorization.
- Generally, the NAS functions as a RADIUS client to transmit user information to a specified RADIUS server and performs operations (for example, accepting or rejecting user access) based on the information returned by the RADIUS server.
- RADIUS servers run on central computers and workstations to maintain user authentication and network service access information. The servers receive connection requests from users, authenticate the users, and send the responses (indicating that the requests are accepted or rejected) to the clients. RADIUS uses the User Datagram Protocol (UDP) as the transmission protocol and uses UDP ports 1812 and 1813 as the authentication and accounting ports, respectively. RADIUS features high real-time performance. In addition, the retransmission mechanism and standby server mechanism are also supported, providing good reliability.
- The message exchange process between the RADIUS server and client is as follows:
    1. When a user accesses the network, the user initiates a connection request and sends the username and password to the RADIUS client (NAS).
    2. The RADIUS client sends an authentication request packet containing the username and password to the RADIUS server.

3. If the request is valid, the RADIUS server completes authentication and sends the required authorization information to the RADIUS client. If the request is invalid, the RADIUS server sends the authorization failure information to the RADIUS client.
4. The RADIUS client notifies the user of whether authentication is successful.
5. The RADIUS client permits or rejects the user according to the authentication result. If the user is permitted, the RADIUS client sends an Accounting-Request (Start) packet to the RADIUS server.
6. The RADIUS server sends an Accounting-Response (Start) packet to the RADIUS client and starts accounting.
7. The user starts to access network resources.
8. When a user does not want to access network resources, the user sends a logout request to stop accessing network resources.
9. The RADIUS client sends an Accounting-Request (Stop) packet to the RADIUS server.
10. The RADIUS server sends an Accounting-Response (Stop) packet to the RADIUS client and stops accounting.
11. The RADIUS client notifies the user of the processing result, and the user stops accessing network resources.

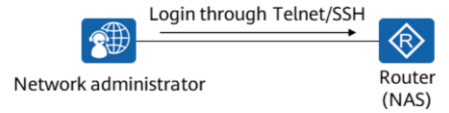
Common AAA Application Scenarios

AAA for Internet Access Users Through RADIUS



- AAA schemes are configured on the NAS to implement interworking between the NAS and RADIUS server.
- After the user enters a username and a password on the client, the NAS sends the username and password to the RADIUS server for authentication.
- If the authentication succeeds, the user is granted the Internet access permission.
- The RADIUS server can record the user's network resource utilization during Internet access.

Local Authentication and Authorization for Administrative Users



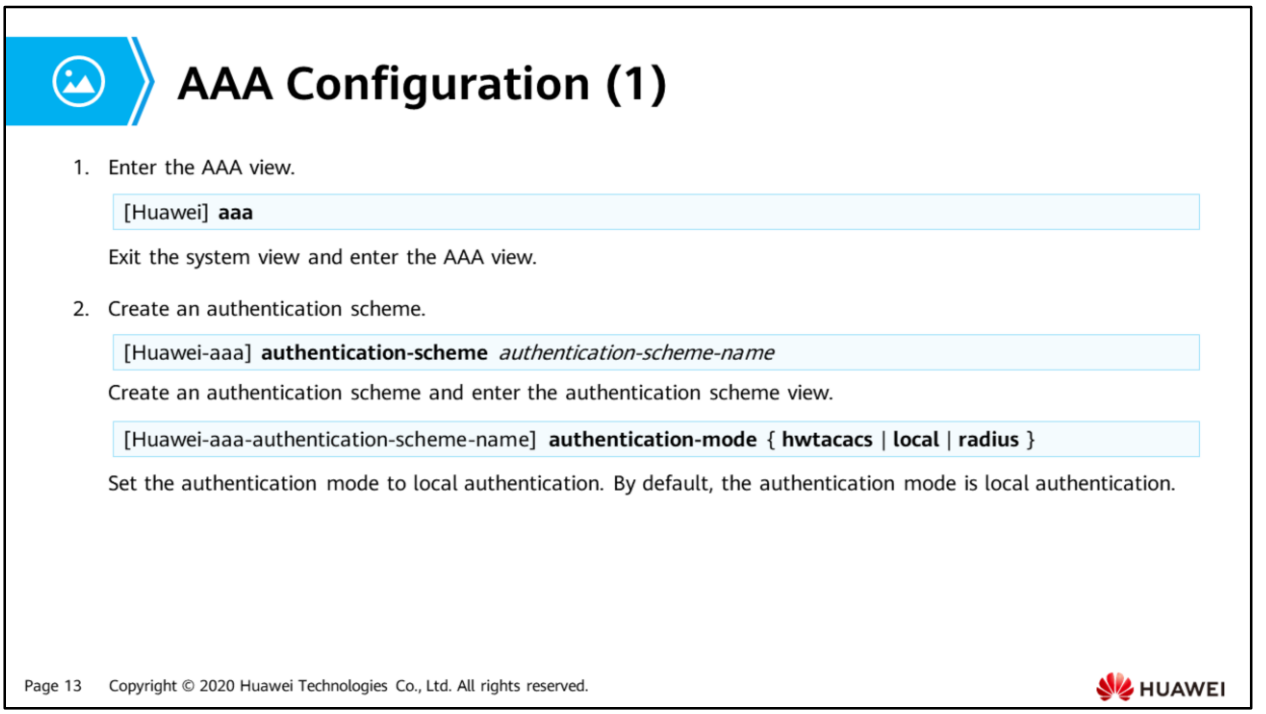
- After local AAA schemes are configured on Router, Router compares the username and password of the network administrator with the locally configured username and password when the network administrator logs in to Router.
- After the authentication succeeds, Router grants certain administrator permissions to the network administrator.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. AAA Overview
2. **AAA Configuration**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The **authorization-scheme** *authorization-scheme-name* command configures an authorization scheme for a domain. By default, no authorization scheme is applied to a domain.
- The **authentication-mode** { **hwtacacs** | **local** | **radius** } command configures an authentication mode for the current authentication scheme. By default, local authentication is used.

AAA Configuration (2)

3. Create a domain and bind an authentication scheme to the domain.

   [Huawei-aaa] **domain** *domain-name*

   Create a domain and enter the domain view.

   [Huawei-aaa-domain-name] **authentication-scheme** *authentication-scheme-name*

   Bind the authentication scheme to the domain.

4. Create a user.

   [Huawei-aaa] **local-user** *user-name* **password cipher** *password*

   Create a local user and configure a password for the local user.

   - If the username contains a delimiter "@", the character before "@" is the username and the character after "@" is the domain name.
   - If the value does not contain "@", the entire character string represents the username and the domain name is the default one.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

AAA Configuration (3)

5. Configure a user access type.

   [Huawei-aaa] **local-user user-name service-type { { terminal | telnet | ftp | ssh | snmp | http } | ppp | none }**

   Configure the access type of the local user. By default, all access types are disabled for a local user.

6. Configure a user level.

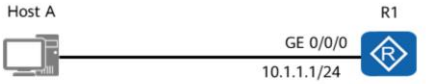
   [Huawei-aaa] **local-user** *user-name* **privilege level** *level*

   Specify the permission level of the local user.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

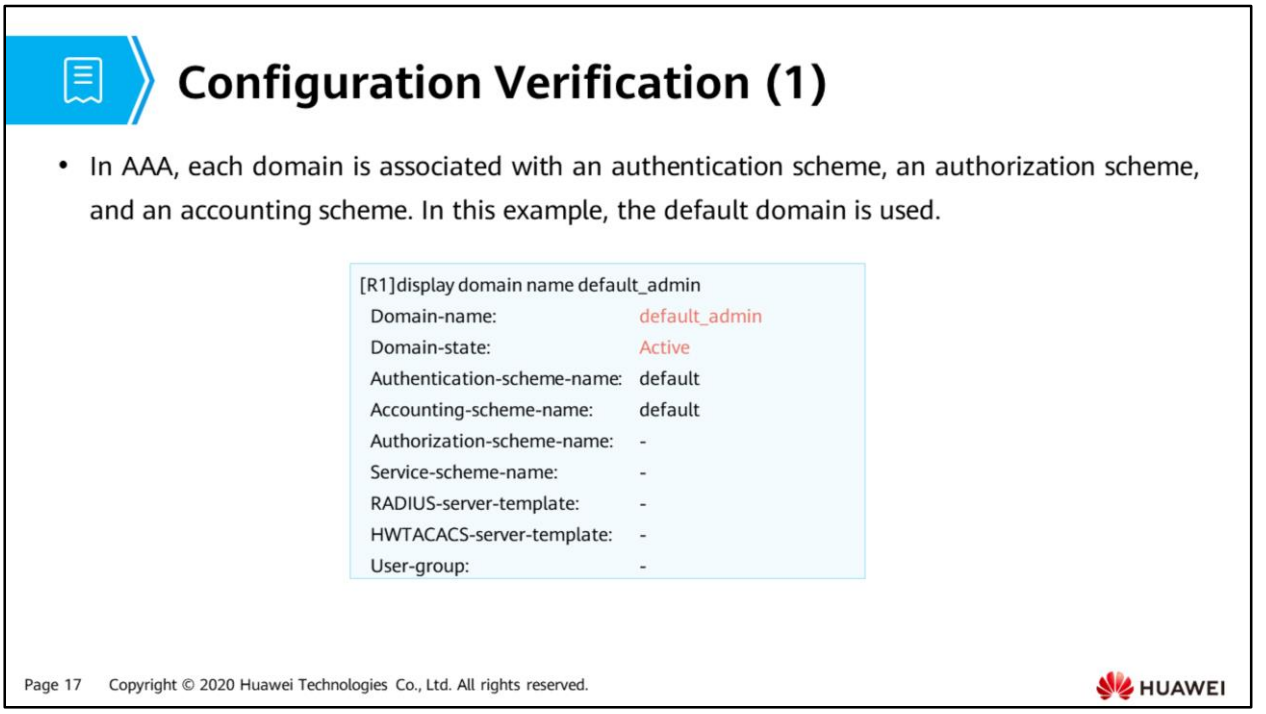
AAA Configuration Examples

- After a user password and a user level are configured on R1, host A can use the configured username and password to remotely log in to R1.




```
[R1]aaa
[R1-aaa]local-user huawei password cipher huawei123
[R1-aaa]local-user huawei service-type telnet
[R1-aaa]local-user huawei privilege level 0
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The **display domain** [**name** *domain-name*]command displays the configuration of a domain.
- If the value of **Domain-state** is Active, the domain is activated.
- If the username does not end with @, the user belongs to the default domain. Huawei devices support the following default domains:
  - The **default** domain is for common users.
  - The **default_admin** domain is the default domain for administrators.

Configuration Verification (2)

- After the user properly logs in and logs out, you can view the user record.

```
[R1]display aaa offline-record all
------------------------------------------------------------------------------
User name:              huawei
Domain name:            default_admin
User MAC:               00e0-fc12-3456
User access type:       telnet
User IP address:        10.1.1.2
User ID:                1
User login time:        2019/12/28 17:59:10
User offline time:      2019/12/28 18:00:04
User offline reason:    user request to offline
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The **display aaa offline-record** command displays user offline records.



Quiz

1. What authentication, authorization, and accounting modes are supported by AAA?
2. When a new common user is configured with local authentication but is not associated with a user-defined domain, which domain does the user belong to?

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

1. AAA supports the following authentication modes: non-authentication, local authentication, and remote authentication. AAA supports the following authorization modes: non-authorization, local authorization, and remote authorization. AAA supports two accounting modes: non-accounting and remote accounting.
2. If the domain to which a user belongs is not specified when the user is created, the user is automatically associated with the **default** domain (the administrator is associated with the **default_admin** domain).

Summary

- AAA improves enterprise network security and prevents unauthorized users from logging in to enterprise networks by authenticating the identities of enterprise employees and external users, authorizing accessible resources, and monitoring Internet access behavior.
  - Authentication: determines which users can access the network.
  - Authorization: authorizes users to access specific services.
  - Accounting: records network resource utilization.
- AAA technology can be implemented either locally or through a remote server.
- Of the protocols that are used to implement AAA, RADIUS is the most commonly used.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Network Address Translation

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- With the development of the Internet and the increase of network applications, limited public IPv4 addresses have become the bottleneck of network development. To solve this problem, Network Address Translation (NAT) was introduced.
- NAT enables hosts on an internal network to access an external network. It not only helps alleviate IPv4 address shortage but also improves the security of the internal network as NAT prevents devices on the external network from directly communicating with hosts on the internal network that uses private addresses.
- This course describes the motivation behind NAT, and implementations and application scenarios of different types of NAT.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand the motivation behind NAT.
  - Master NAT classification and implementations.
  - Master NAT selection in different scenarios.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. **NAT Overview**
2. Static NAT
3. Dynamic NAT
4. NAPT and Easy IP
5. NAT Server

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Motivation Behind NAT

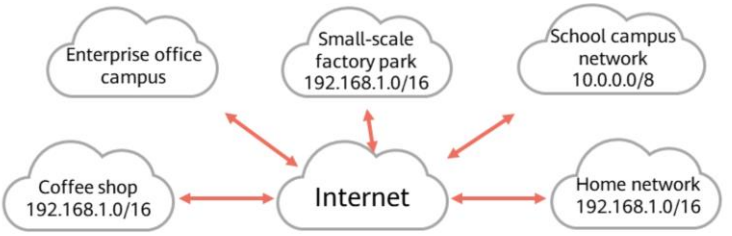
- As the number of Internet users increases, public IPv4 addresses become scarcer.
- What's worse, uneven allocation of these addresses has resulted in a severe shortage of available public IPv4 addresses in some areas.
- To overcome public IPv4 address shortage, it is necessary to use transition technologies.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Private IP Addresses

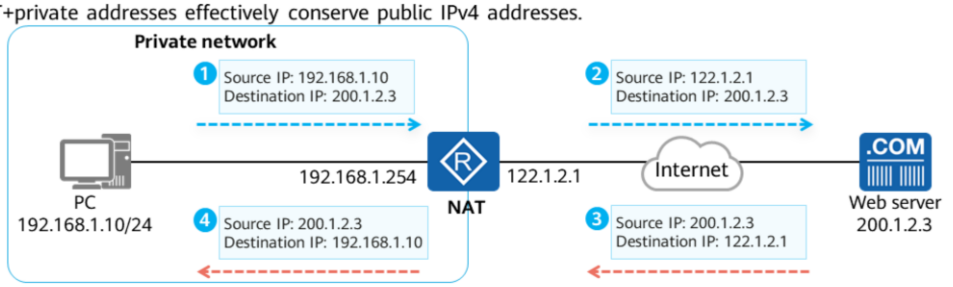
- Public IP addresses: managed and allocated by a dedicated organization and can be used for direct communication on the Internet
- Private IP addresses: can be used by organizations or individuals randomly on internal networks, but cannot be used for direct communication on the Internet
- The following Class A, B, and C addresses are reserved as private IP addresses:
  - Class A: 10.0.0.0–10.255.255.255
  - Class B: 172.16.0.0–172.31.255.255
  - Class C: 192.168.0.0–192.168.255.255



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

NAT Implementation

- NAT: translates IP addresses in IP data packets. It is widely used on live networks and is usually deployed on network egress devices, such as routers or firewalls.
- Typical NAT application scenario: Private addresses are used on private networks (enterprises or homes), and NAT is deployed on egress devices. For traffic from an internal network to an external network, NAT translates the source addresses of the data packets into specific public addresses. For traffic from an external network to an internal network, NAT translates the destination address of the data packets.
- NAT+private addresses effectively conserve public IPv4 addresses.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Because packets with private IP addresses cannot be routed and forwarded on the Internet, IP packets destined for the Internet cannot reach the egress device of the private network due to lack of routes.
- If a host that uses a private IP address needs to access the Internet, NAT must be configured on the network egress device to translate the private source address in the IP data packet into a public source address.

Contents

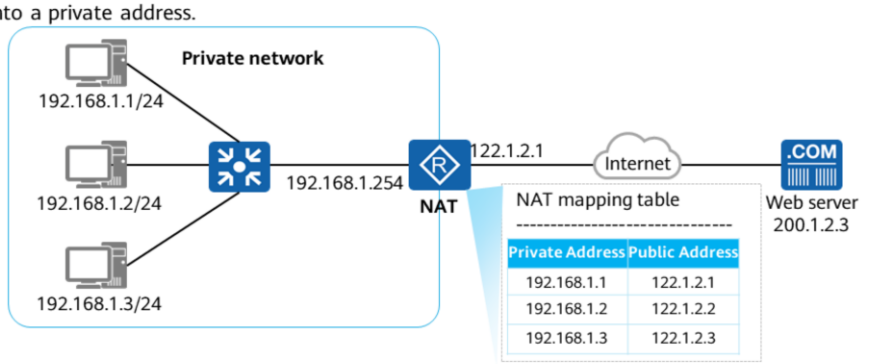
1. NAT Overview
2. **Static NAT**
3. Dynamic NAT
4. NAPT and Easy IP
5. NAT Server

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

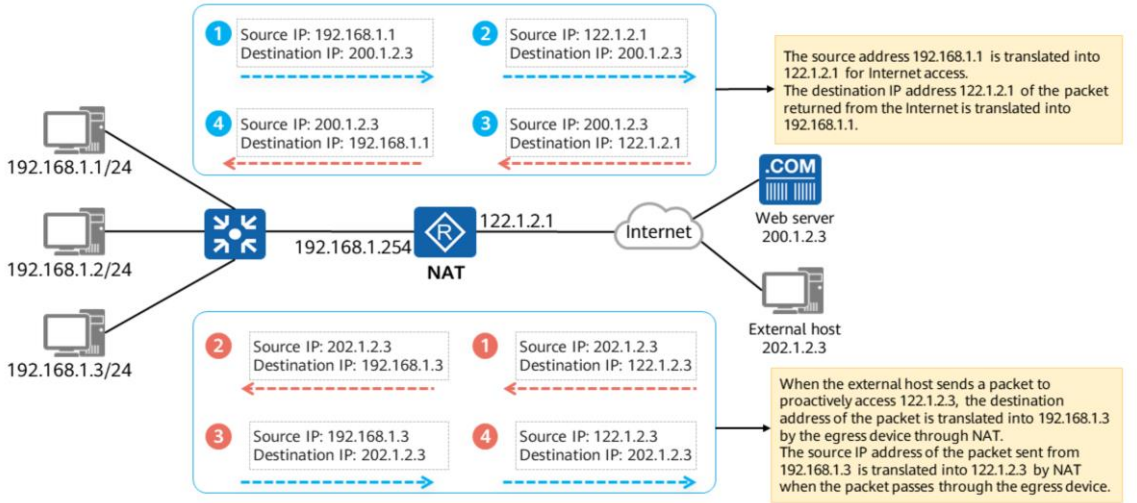
Static NAT Implementation

- Static NAT: A private IP address is mapped to a fixed public IP address.
- Bidirectional access: When an internal host with a private IP address accesses the Internet, the egress NAT device translates the private IP address into a public IP address. Similarly, when an external network device sends packets to access an internal network, the NAT device translates the public address (destination address) carried in the packets into a private address.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Static NAT Example



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Configuring Static NAT

1. Method 1: Configure static NAT in the interface view.

   [Huawei-GigabitEthernet0/0/0] **nat static global** *{ global-address}* **inside** *{host-address }*

   global *{ global-address}* is used to configure an external public IP address, and **inside** *{host-address }* is used to configure an internal private IP address.

2. Method 2: Configure static NAT in the system view.

   [Huawei] **nat static global** *{ global-address}* **inside** *{host-address }*

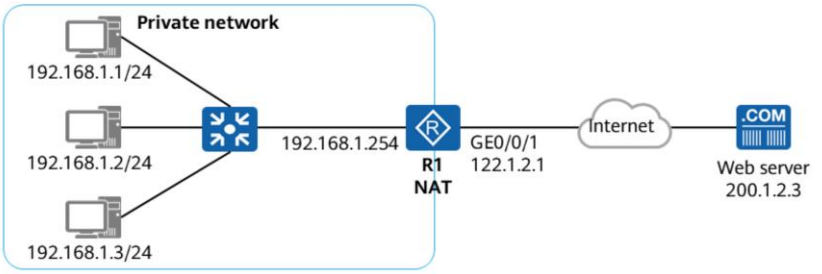
   The command format in the system view is the same as that in the interface view. After this configuration, enable static NAT on a specific interface.

   [Huawei-GigabitEthernet0/0/0] **nat static enable**

   This command enables static NAT on the interface.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring Static NAT



- Configure static NAT on R1 to map private addresses of internal hosts to public addresses in one-to-one mode.

```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 122.1.2.1 24
[R1-GigabitEthernet0/0/1]nat static global 122.1.2.1 inside 192.168.1.1
[R1-GigabitEthernet0/0/1]nat static global 122.1.2.2 inside 192.168.1.2
[R1-GigabitEthernet0/0/1]nat static global 122.1.2.3 inside 192.168.1.3
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

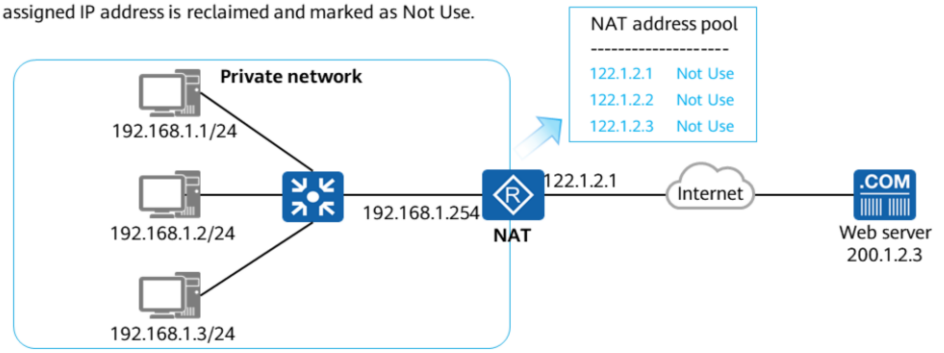
1. NAT Overview
2. Static NAT
3. **Dynamic NAT**
4. NAPT and Easy IP
5. NAT Server

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

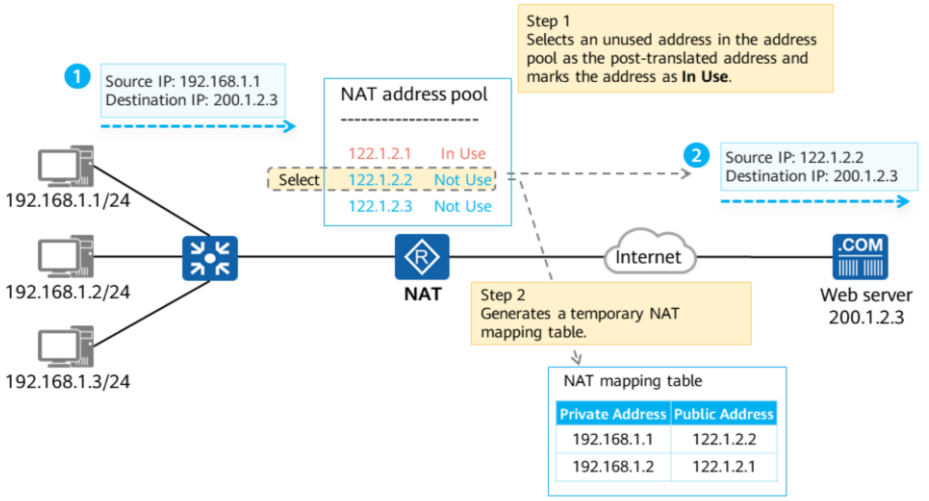
Dynamic NAT Implementation

- Dynamic NAT: A private IP address is mapped to a public IP address from a NAT address pool containing a group of public IP addresses. Static NAT strictly maps addresses in one-to-one mode. As a result, even if an internal host is offline for a long time or does not send data, the public address is still occupied by the host.
- Dynamic NAT prevents such address wastes. When an internal host accesses an external network, an available IP address in a NAT address pool is temporarily assigned to the host and marked as In Use. When the host no longer accesses the external network, the assigned IP address is reclaimed and marked as Not Use.



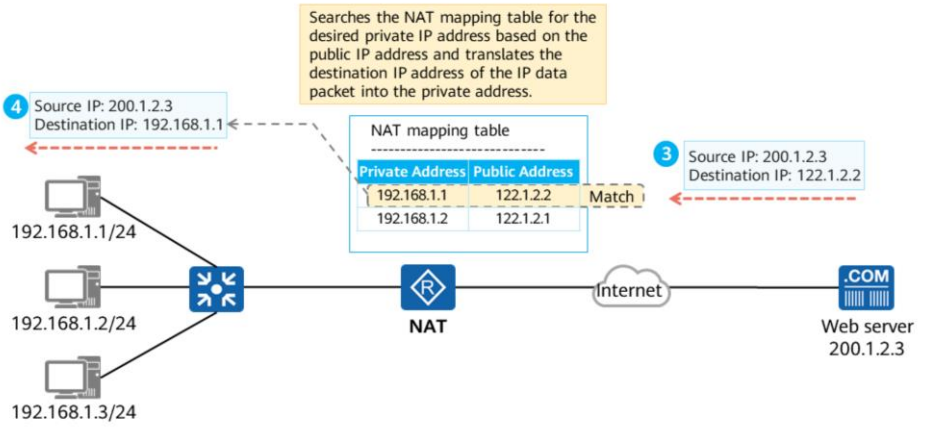
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Dynamic NAT Example (1)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Dynamic NAT Example (2)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuring Dynamic NAT

1. Create an address pool.

   [Huawei] **nat address-group** *group-index start-address end-address*

   Configure a public address range. *group-index* specifies the address pool ID, and *start-address* and *end-address* specify the start and end addresses of the address pool, respectively.

2. Configure an ACL rule for NAT.

   [Huawei] **acl** *number*
   [Huawei-acl-basic-*number*] **rule permit source** *source-address source-wildcard*

   Configure a basic ACL to match the source address range that requires dynamic NAT.

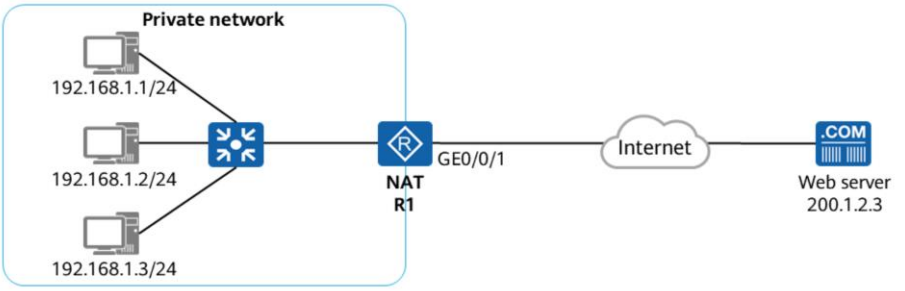
3. Configure outbound NAT with the address pool in the interface view.

   [Huawei-GigabitEthernet0/0/0] **nat outbound** *acl-number* **address-group** *group-index* [**no-pat**]

   Associate the ACL rule with the address pool for dynamic NAT on the interface. The **no-pat** parameter specifies that port translation is not performed.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring Dynamic NAT



- Configure dynamic NAT on R1 to dynamically map private addresses of internal hosts to public addresses.

```
[R1]nat address-group 1 122.1.2.1 122.1.2.3
[R1]acl 2000
[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000]quit
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1 no-pat
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

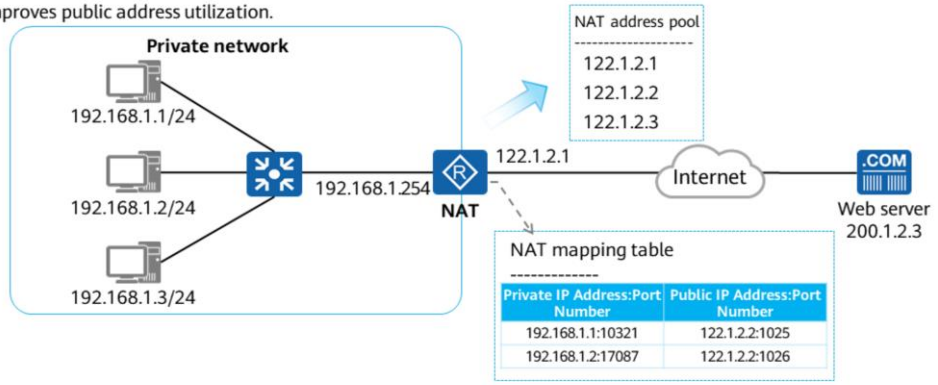
1. NAT Overview
2. Static NAT
3. Dynamic NAT
4. **NAPT and Easy IP**
5. NAT Server

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

NAPT Implementation

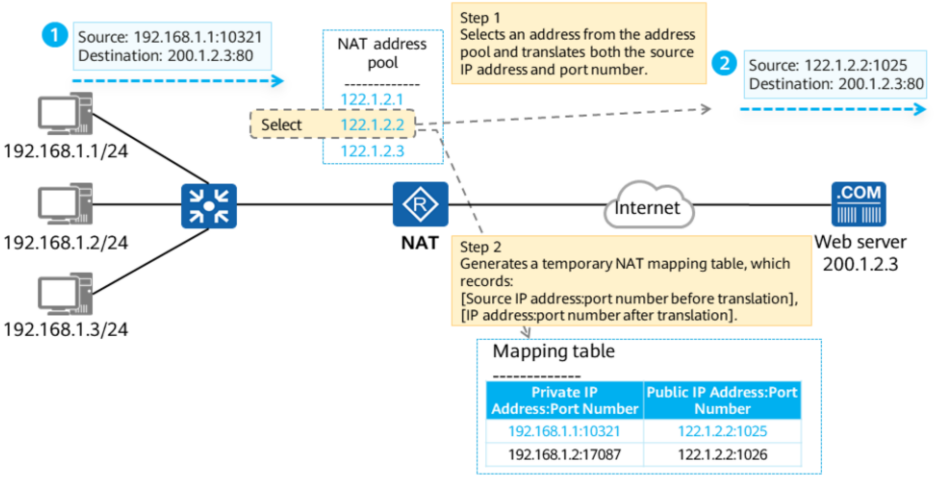
- Dynamic NAT does not translate port numbers. It belongs to No-Port Address Translation (No-PAT). In this mode, the mapping between public and private addresses is still 1:1, which cannot improve public address utilization.
- Network Address and Port Translation (NAPT): translates both IP addresses and port numbers from multiple internal hosts to one public IP address in an address pool. In this way, 1:n mapping between public and private addresses is implemented, which effectively improves public address utilization.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

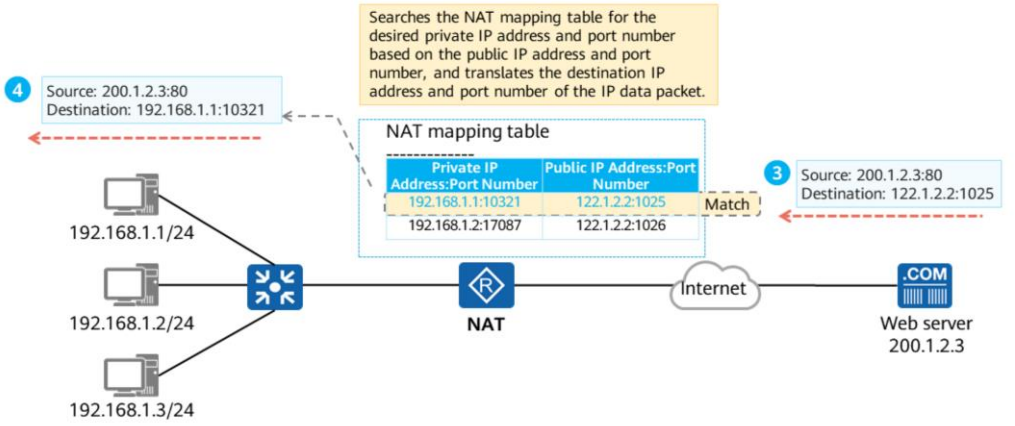
- NAPT enables a public IP address to map multiple private IP addresses through ports. In this mode, both IP addresses and transport-layer ports are translated so that different private addresses with different source port numbers are mapped to the same public address with different source port numbers.

NAPT Example (1)



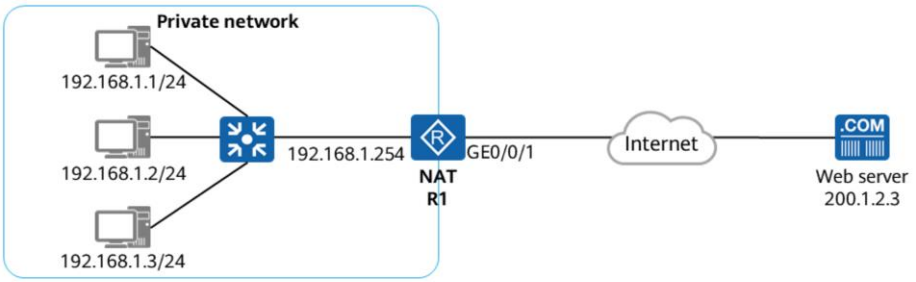
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

NAPT Example (2)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring NAPT



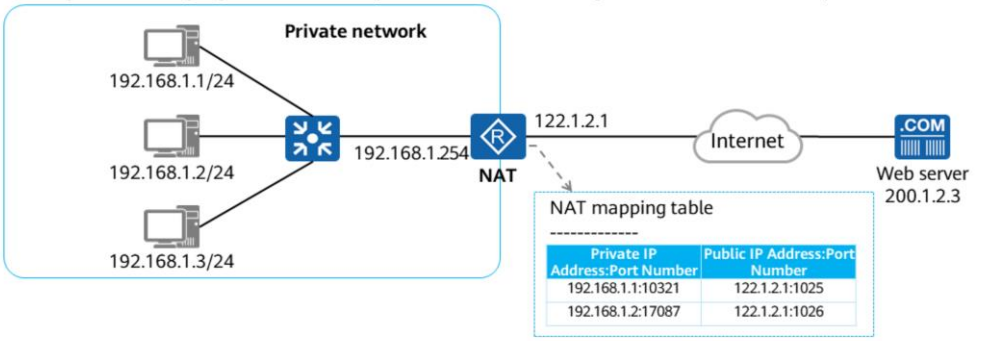
- Configure NAPT on R1 to allow all hosts with private IP addresses on the internal network to access the public network through 122.1.2.1.

```
[R1]nat address-group 1 122.1.2.1 122.1.2.1
[R1]acl 2000
[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000]quit
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Easy IP

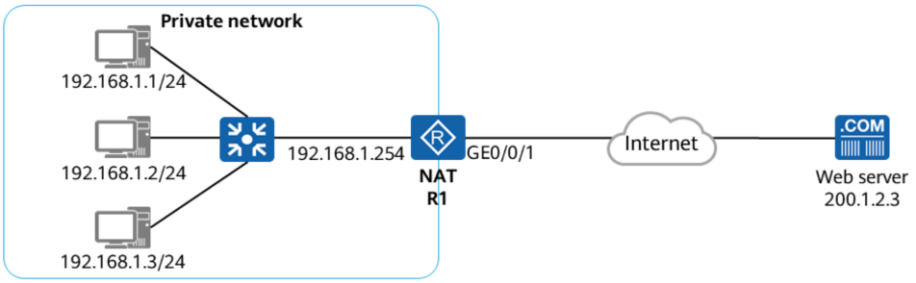
- Easy IP: translates both IP addresses and transport-layer port numbers. The implementation of Easy IP is the same as that of NAPT. The difference is that Easy IP does not involve address pools. It uses an interface address as a public address for NAT.
- Easy IP applies to scenarios where public IP addresses are not fixed, such as scenarios where public IP addresses are dynamically obtained by egress devices on private networks through DHCP or PPPoE dialup.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- DHCP: Dynamic Host Configuration Protocol
- PPPoE: Point-to-Point Protocol over Ethernet

Example for Configuring Easy IP



- Configure Easy IP on R1 to allow all hosts with private IP addresses on the internal network to access the public network through 122.1.2.1.

```
[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000]quit
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]nat outbound 2000
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

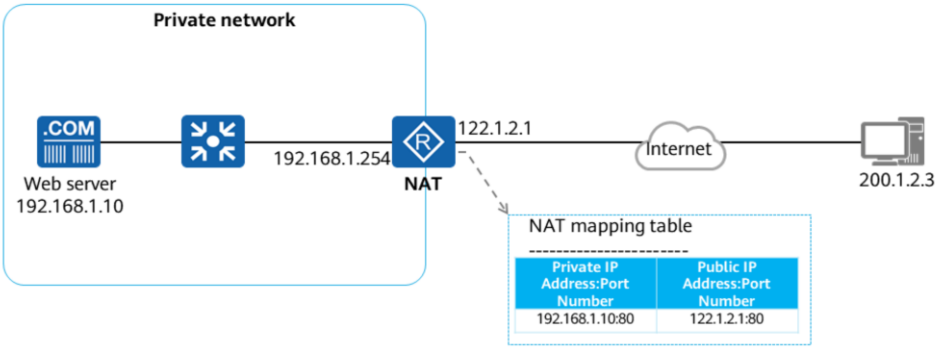
Contents

1. NAT Overview
2. Static NAT
3. Dynamic NAT
4. NAPT and Easy IP
5. **NAT Server**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

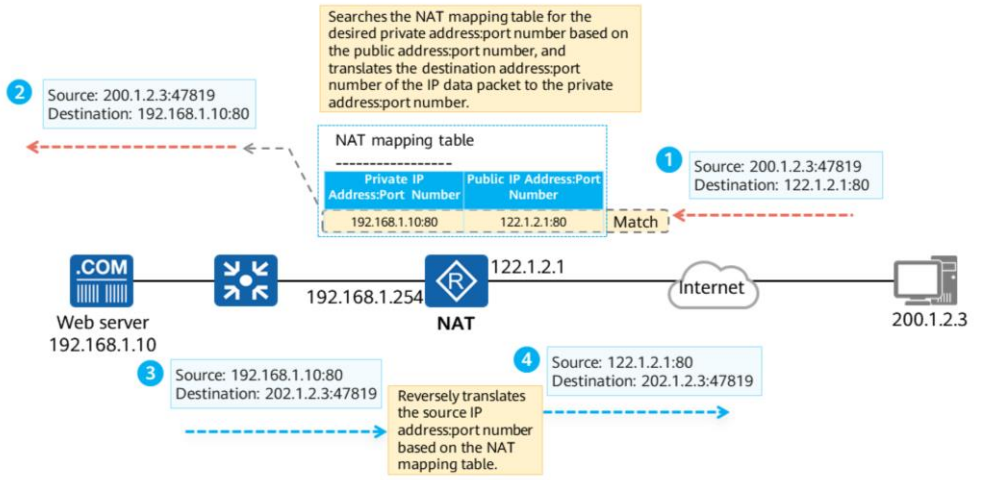
NAT Server

- NAT Server: maps an internal server to a public network through a one-to-one mapping between a [**public IP address:port number**] and a [**private IP address:port number**]. This function is used when the internal server needs to provide services for the public network.
- An external host proactively accesses the [**public IP address:port number**] to communicate with the internal server.



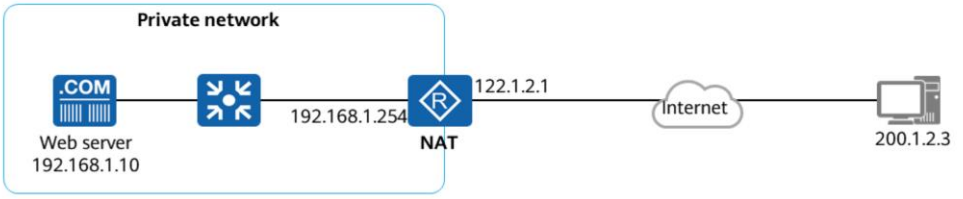
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

NAT Server Example



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Example for Configuring NAT Server



- Configure NAT Server on R1 to map the internal server's IP address 192.168.1.10 and port number 80 to the public IP address 122.1.2.1 and port number 8080.

```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 122.1.2.1 24
[R1-GigabitEthernet0/0/1]nat server protocol tcp global 122.1.2.1 www inside 192.168.1.10 8080
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Quiz

1. What types of NAT can enable external devices to proactively access an internal server?
2. What are the advantages of NAPT over No-PAT?

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. Static NAT and NAT Server Static NAT implements bidirectional communication, meaning that external devices are allowed to access an internal server. NAT Server is designed to allow external devices to proactively access an internal server.
2. NAPT can translate multiple private IP addresses into one public IP address, improving public IP address utilization.

Summary

- Using private addresses on private networks and using NAT at the network egress effectively reduce the number of required public IPv4 addresses. NAT effectively alleviates the shortage of public IPv4 addresses.
- Dynamic NAT, NAPT, and Easy IP provide source address translation for private network hosts to access the public network.
- NAT Server enables internal servers to provide services for public networks.
- Static NAT provides one-to-one mapping and supports bidirectional communication.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Network Services and Applications

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- The Internet has become an integral part of our lives, with a wide range of applications such as file transfer, email sending, online video, web browsing, and online gaming. Because of the layered network model, common users can use various services provided by the application layer, without knowing technical details such as communication technology implementations.
- In previous courses, we have learned technologies related to the data link layer, network layer, and transport layer. This chapter will describe common network services and applications such as FTP, DHCP, and HTTP.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand FTP fundamentals.
  - Understand TFTP fundamentals.
  - Understand DHCP fundamentals.
  - Understand Telnet fundamentals.
  - Understand HTTP fundamentals.
  - Understand DNS fundamentals.
  - Understand NTP fundamentals.

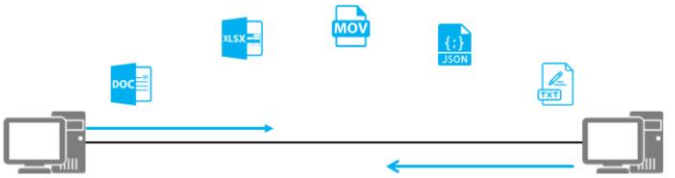
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. **File Transfer**
   - **FTP**
   - TFTP
2. Telnet
3. DHCP
4. HTTP
5. DNS
6. NTP

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

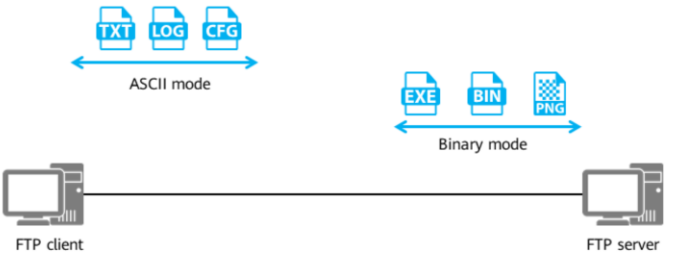
File Transfer Protocols



- File transfer between hosts is an important function of IP networks. Nowadays, people can conveniently transfer files using web pages and mailboxes.
- However, in the early Internet era when the World Wide Web (WWW) did not come into being and operating systems used command-line interfaces, people transferred files via command-line tools. The most commonly used protocols for transferring files at that time are File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP).

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

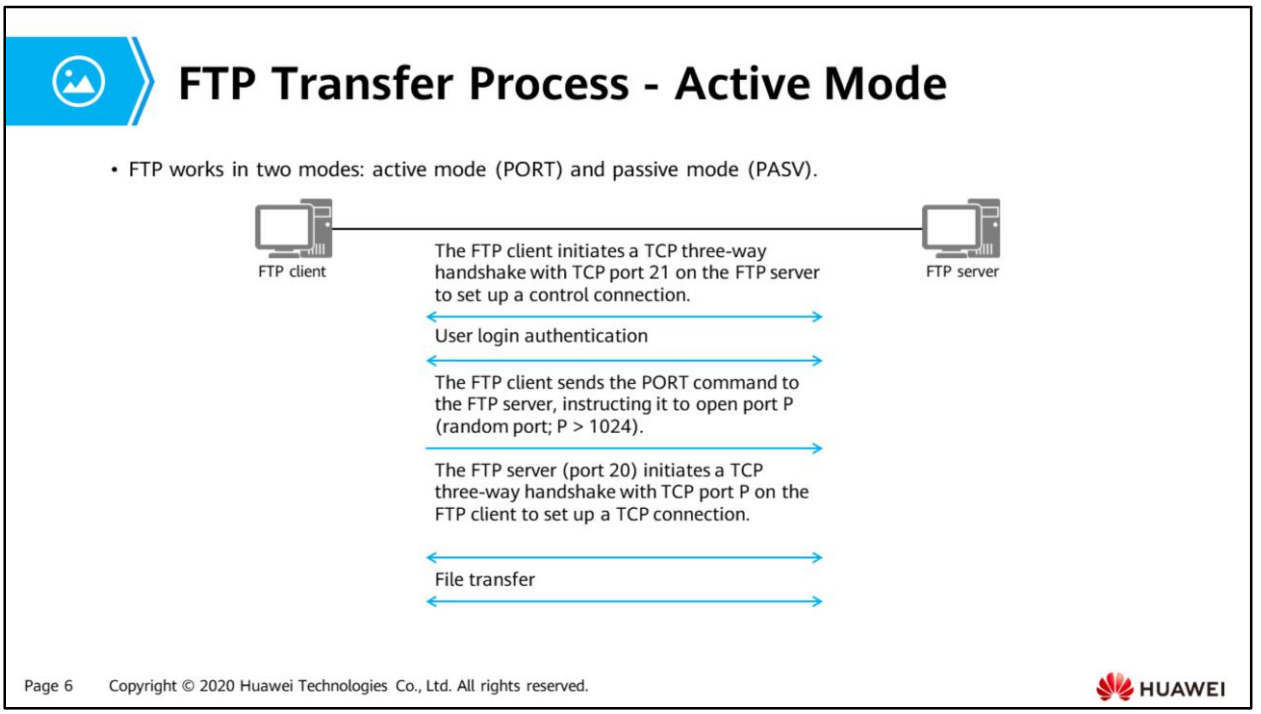
Basic Concepts of FTP



- FTP adopts the typical client/server (C/S) architecture. After an FTP client establishes a TCP connection with an FTP server, files can be uploaded and downloaded.
- FTP uses different transfer modes based on the file type:
  - **ASCII mode**: When a text file (in TXT, LOG, or CFG format) is transferred, the encoding mode of the text content is converted to improve the transfer efficiency. This mode is recommended for transferring configuration files and log files of network devices.
  - **Binary mode**: Non-text files (in CC, BIN, EXE, or PNG format), such as images and executable programs, are transferred in binary mode. This mode is recommended for transferring version files of network devices.

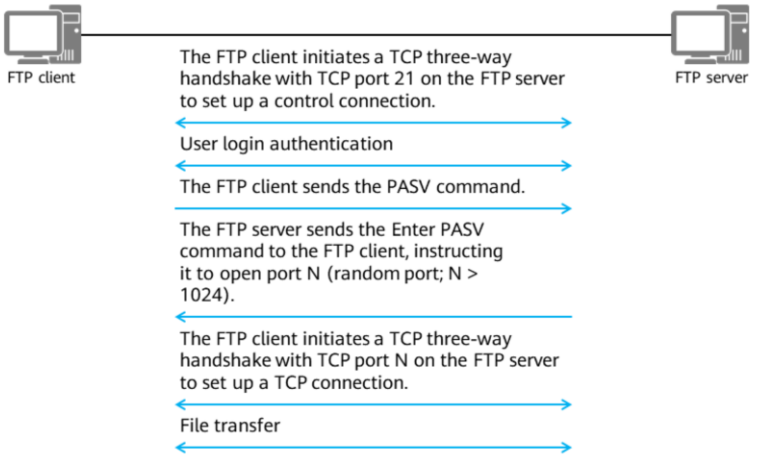
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- FTP supports two transfer modes: ASCII and binary.
- The ASCII mode is used to transfer text files. In this mode, the sender converts characters into the ASCII code format before sending them. After receiving the converted data, the receiver converts it back into characters. The binary mode is usually used to send image files and program files. In this mode, the sender can transfer files without converting the file format.
- CC: VRP system file extension



- In active mode, the FTP client uses a random port (with the number greater than 1024) to send a connection request to port 21 of the FTP server. After receiving the request, the FTP server sets up a control connection with the FTP client to transmit control messages. In the meantime, the FTP client starts to listen on port P (another random port with the number greater than 1024) and uses the PORT command to notify the FTP server. When data needs to be transmitted, the FTP server sends a connection request from port 20 to port P of the FTP client to establish a TCP connection for data transmission.

FTP Transfer Process - Passive Mode



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- In passive mode, the FTP client uses a random port (with the number greater than 1024) to send a connection request to port 21 of the FTP server. After receiving the request, the FTP server sets up a control connection with the FTP client to transmit control messages. In the meantime, the FTP client starts to listen on port P (another random port with the number greater than 1024) and uses the PASV command to notify the FTP server. After receiving the PASV command, the FTP server enables port N (a random port with the number greater than 1024) and uses the Enter PASV command to notify the FTP client of the opened port number. When data needs to be transmitted, the FTP client sends a connection request from port P to port N on the FTP server to establish a transmission connection for data transmission.
- The active mode and passive mode differ in data connection methods and have their own advantages and disadvantages.
    - In active mode, if the FTP client is on a private network and a NAT device is deployed between the FTP client and the FTP server, the port number and IP address carried in the PORT packet received by the FTP server are not those of the FTP client converted using NAT. Therefore, the FTP server cannot initiate a TCP connection to the private IP address carried in the PORT packet. In this case, the private IP address of the FTP client is not accessible on the public network.
    - In passive mode, the FTP client initiates a connection to an open port on the FTP server. If the FTP server lives in the internal zone of a firewall and inter-zone communication between this internal zone and the zone where the FTP client resides is not allowed, the client-server connection cannot be set up. As a result, FTP transfer fails.

Configuration Commands (Device as FTP Server)

A user accesses a device through FTP.

1. Enable the FTP server function.

   [Huawei]**ftp** [**ipv6**] **server enable**

   By default, the FTP server function is disabled.

2. Configure a local FTP user.

   [Huawei]**aaa**
   [Huawei]**local-user** *user-name* **password irreversible-cipher** *password*
   [Huawei]**local-user** *user-name* **privilege level** *level*
   [Huawei]**local-user** *user-name* **service-type ftp**
   [Huawei]**local-user** *user-name* **ftp-directory** *directory*

   The privilege level must be set to level 3 or higher. Otherwise, the FTP connection fails.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Commands (Device as FTP Client)

1. A VRP device that functions as an FTP client accesses an FTP server.

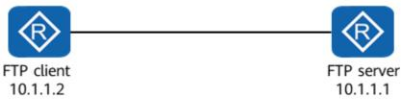
```
<FTP Client>ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):ftp
331 Password required for ftp.
Enter password:
230 User logged in.
```

2. Common commands used when the VRP device functions as an FTP client.

```
ascii     Set the file transfer type to ASCII, and it is the default type
binary    Set the file transfer type to support the binary image
ls        List the contents of the current or remote directory
passive   Set the toggle passive mode, the default is on
get       Download the remote file to the local host
put       Upload a local file to the remote host
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Example



- One router functions as the FTP server, and the other as the FTP client.
- Enable the FTP service on the FTP server and create an FTP login account. Then, the FTP client logs in to the FTP server and runs the **get** command to download a file.

Configurations on the FTP server:

```
<Huawei> system-view
[Huawei] sysname FTP_Server
[FTP_Server] ftp server enable
[FTP_Server] aaa
[FTP_Server-aaa] local-user admin1234 password irreversible-cipher
Helloworld@6789
[FTP_Server-aaa] local-user admin1234 privilege level 15
[FTP_Server-aaa] local-user admin1234 service-type ftp
[FTP_Server-aaa] local-user admin1234 ftp-directory flash:
```

Operations on the FTP client:

```
<FTP Client>ftp 10.1.1.1
[FTP Client-ftp]get sslvpn.zip
200 Port command okay.
FTP: 828482 byte(s) received in 2.990 second(s) 277.08Kbyte(s)/sec.
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

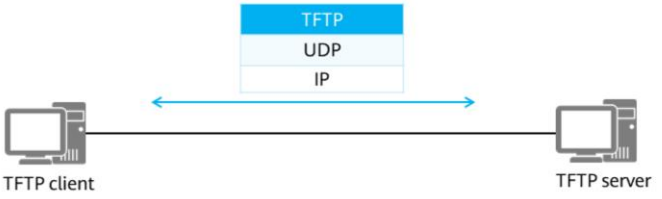
1. **File Transfer**
   - FTP
   - **TFTP**
2. Telnet
3. DHCP
4. HTTP
5. DNS
6. NTP

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

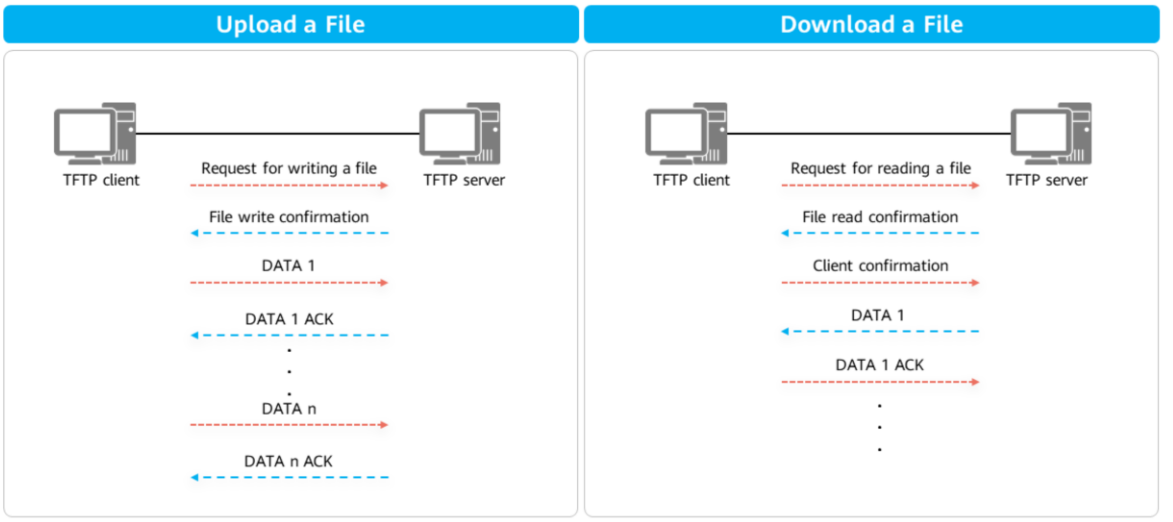
Basic Concepts of TFTP

- Compared with FTP, TFTP is designed to transfer small files and is easier to implement.
  - Using UDP (port 69) for transmission
  - Authentication not required
  - You can only request a file from or upload a file to the server, but cannot view the file directory on the server.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

TFTP Transfer Example



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- TFTP supports five packet formats:
  - RRQ: read request packet
  - WRQ: write request packet
  - DATA: data transmission packet
  - ACK: acknowledgment packet, which is used to acknowledge the receipt of a packet from the peer end
  - ERROR: error control packet

Configuration Commands (Device as TFTP Client)

1. Download a file (VRP device functioning as a TFTP client).

   <HUAWEI> **tftp** *tftp_server* **get** *filename*

   You do not need to log in to the TFTP server, and only need to enter the IP address of the TFTP server and the corresponding command.

2. Upload a file (VRP device functioning as a TFTP client).

   <HUAWEI> **tftp** *tftp_server* **put** *filename*

   You do not need to log in to the TFTP server, and only need to enter the IP address of the TFTP server and the corresponding command.

   Currently, VRP devices can function only as TFTP clients.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

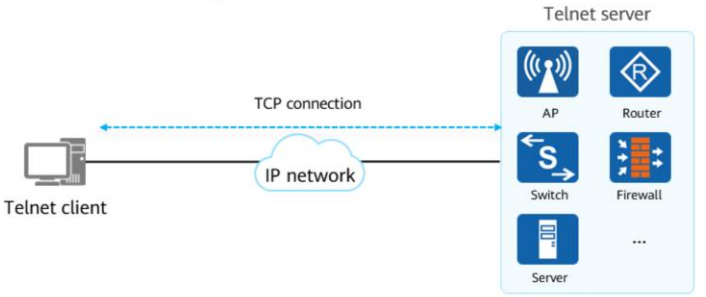
Contents

1. File Transfer
2. **Telnet**
3. DHCP
4. HTTP
5. DNS
6. NTP

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Application Scenario of Telnet

- To facilitate device management using commands, you can use Telnet to manage devices.
- Device management through Telnet is different from that using the console port. In Telnet-based device management mode, no dedicated cable is required to directly connect to the console port of the Telnet server, as long as the Telnet server's IP address is reachable and Telnet clients can communicate with the Telnet server's TCP port 23.
- The device that can be managed through Telnet is called the Telnet server, and the device connecting to the Telnet server is called the Telnet client. Many network devices can act as both the Telnet server and Telnet client.

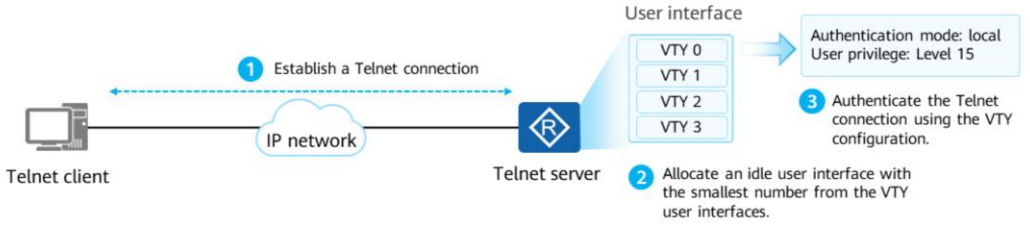


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Currently, mainstream network devices, such as access controllers (ACs), access points (APs), firewalls, routers, switches, and servers, can function as both the Telnet server and Telnet client.

VTY User Interface

- When a user logs in to a device using the console port or Telnet, the system allocates a user interface to manage and monitor the current session between the device and the user. A series of parameters can be set in each user interface view to specify the authentication mode and user privilege level after login. After a user logs in to a device, user operations that can be performed depend on the configured parameters.
- The user interface type of Telnet is virtual type terminal (VTY) user interface.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Commands (1)

1. Enable the Telnet server function.

   [Huawei] **telnet server enable**

   The Telnet server function is enabled on the device (disabled by default). To disable this function, run the **undo telnet server enable** command.

2. Enter the user view.

   [Huawei] **user-interface vty** *first-ui-number [last-ui-number]*

   The VTY user interface view is displayed. VTY user interfaces may vary according to device models.

3. Configure protocols supported by the VTY user interface.

   [Huawei-ui-vty0-4]] **protocol inbound** { **all** | **telnet** | **ssh**}

   By default, the VTY user interface supports Secure Shell (SSH) and Telnet.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Commands (2)

4. Configure the authentication mode and the authentication password in password authentication mode.

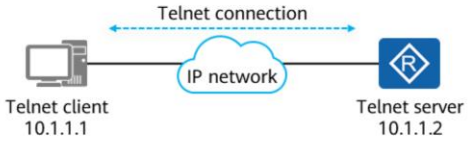
```
[Huawei-ui-vty0-4] authentication-mode {aaa | none | password}
[Huawei-ui-vty0-4] set authentication password cipher
```

By default, no default authentication mode is available. You need to manually configure an authentication mode.

The **set authentication password cipher** command implementation varies according to VRP versions. In some versions, you need to press **Enter** and then enter the password. In other versions, you can directly enter the password after the command.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Example (1)



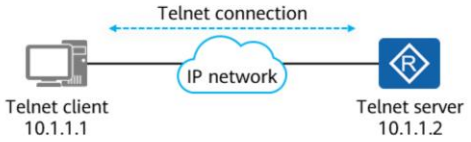
- Configure the router at 10.1.1.2 as the Telnet server and set the authentication mode to AAA local authentication. Create an account named **huawei**, set the password to **Huawei@123**, and set the privilege level to 15.
- Log in to and manage the Telnet server through the Telnet client.

Configurations on the Telnet server:

```
<Huawei> system-view
[Huawei] telnet server enable
[Huawei] aaa
[Huawei-aaa] local-user huawei password irreversible-cipher
Huawei@123
[Huawei-aaa] local-user huawei privilege level 15
[Huawei-aaa] local-user huawei service-type telnet
[Huawei-aaa] quit
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode aaa
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Example (2)



- Configure the router at 10.1.1.2 as the Telnet server and set the authentication mode to AAA local authentication. Create an account named **huawei**, set the password to **Huawei@123**, and set the privilege level to 15.
- Log in to and manage the Telnet server through the Telnet client.

Operations on the Telnet client:

```
<Host>telnet 10.1.1.2
Login authentication

Username:huawei
Password:
Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 1.
      The current login time is 2020-01-08 15:37:25.
<Huawei>
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. File Transfer
2. Telnet
3. **DHCP**
4. HTTP
5. DNS
6. NTP

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

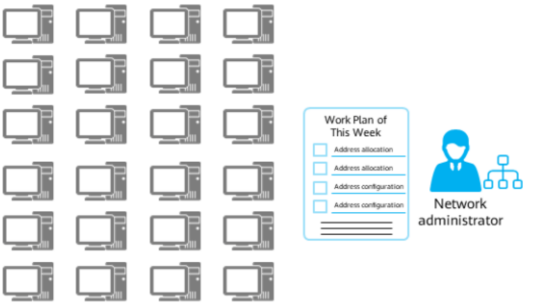
Issues Faced by Manual Network Parameter Configuration (1)

Too Many Hard-to-Understand Parameters



- Common users are not familiar with network parameters and misconfiguration often occurs, resulting in network access failure. Random IP address configuration may cause IP address conflicts.

Huge Workload

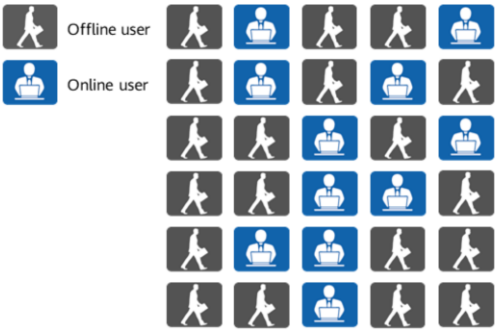


- Network administrators centrally configure network parameters, with heavy workloads and repetitive tasks.
- Network administrators need to plan and allocate IP addresses to users in advance.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

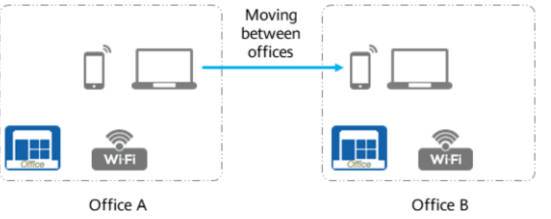
Issues Faced by Manual Network Parameter Configuration (2)

Low Utilization



- On an enterprise network, each user uses a fixed IP address. As a result, the IP address utilization is low, and some IP addresses may remain unused for a long time.

Poor Flexibility



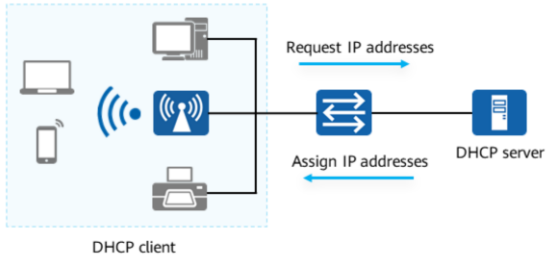
Office A Office B

- Wireless local area networks (WLANs) allow for flexible station (STA) access locations. When a STA moves from one wireless coverage area to another, the IP address of the STA may need to be reconfigured.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

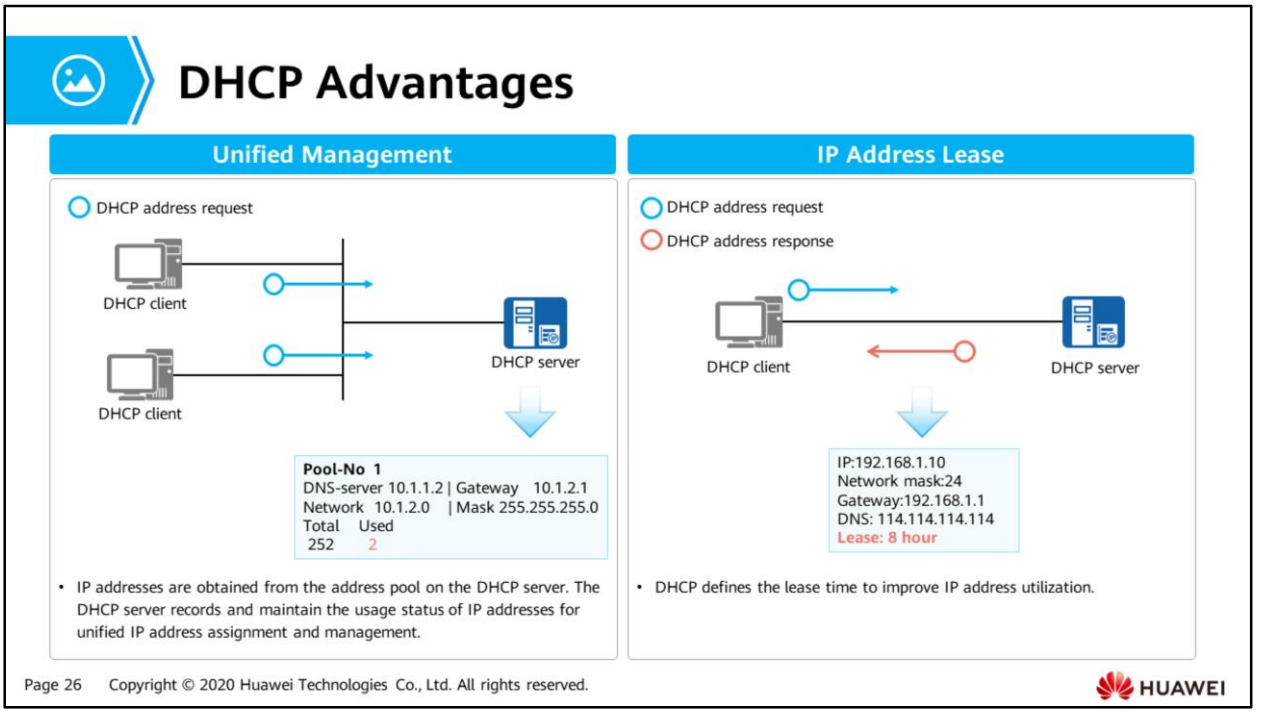
Basic Concepts of DHCP

DHCP Working Principle



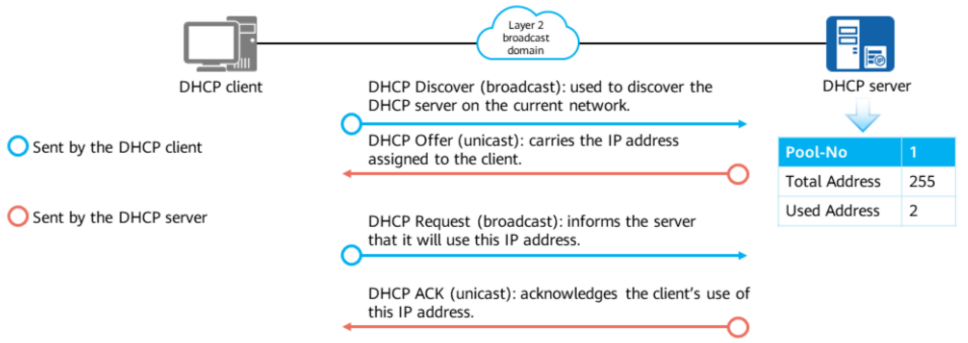
- To overcome the disadvantages of the traditional static IP configuration mode, the Dynamic Host Configuration Protocol (DHCP) is developed to dynamically assign suitable IP addresses to hosts.
- DHCP adopts the client/server (C/S) architecture. Hosts do not need to be configured and can automatically obtain IP addresses from a DHCP server. DHCP enables host plug-and-play after they are connected to the network.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- If a DHCP client does not renew the lease of an assigned IP address after the lease expires, the DHCP server determines that the DHCP client no longer needs to use this IP address, reclaims it, and may assign it to another client.

DHCP Working Principle

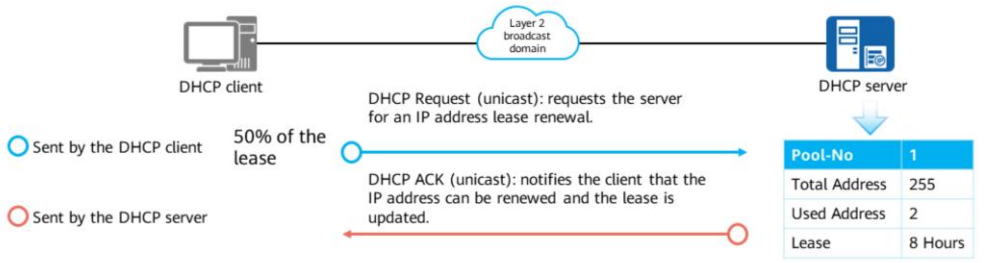


- Question: Why does a DHCP client need to send a DHCP Request packet to the DHCP server to notify its use of a particular IP address after receiving a DHCP Offer packet?

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- A client's DHCP Request packet is broadcast, so other DHCP servers on the network know that the client has selected a particular IP address assigned by the DHCP server. This ensures that other DHCP servers can release this IP address assigned to the client through the unicast DHCP Offer packet.

DHCP Lease Renewal



- If the DHCP client fails to receive a response from the original DHCP server at 50% of the lease (known as T1), the DHCP client waits until 87.5% of the lease (known as T2) has passed. At T2, the client enters the rebinding state, and broadcasts a DHCP Request packet, to which any DHCP server can respond.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Commands (1)

1. Enable DHCP.

   [Huawei] **dhcp enable**

2. Enable the interface to use the interface address pool to provide the DHCP server function.

   [Huawei-Gigabitthernet0/0/0]**dhcp select interface**

3. Specify a DNS server IP address for the interface address pool.

   [Huawei-Gigabitthernet0/0/0]**dhcp server dns-list** *ip-address*

4. Configure the range of IP addresses that cannot be automatically assigned to clients from the interface address pool.

   [Huawei-Gigabitthernet0/0/0]**dhcp server excluded-ip-address** *start-ip-address [end-ip-address]*

5. Configure the lease of IP addresses in the interface address pool of the DHCP server.

   [Huawei-Gigabitthernet0/0/0]**dhcp server lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

   By default, the IP address lease is one day.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Commands (2)

6. Create a global address pool.

   [Huawei]**ip pool** *ip-pool-name*

7. Specify the range of IP addresses that can be assigned dynamically in the global address pool.

   [Huawei-ip-pool-2]**network ip-address [mask {** *mask* | *mask-length* **}]**

8. Configure the gateway address for DHCP clients.

   [Huawei-ip-pool-2]**gateway-list** *ip-address*

9. Specify the DNS server IP address that the DHCP server delivers to DHCP clients.

   [Huawei-ip-pool-2]**dns-list** *ip-address*

10. Set the IP address lease.

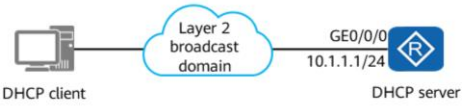
    [Huawei-ip-pool-2] **lease { day** *day* **[hour** *hour* **[minute** *minute* **]] | unlimited }**

11. Enable the DHCP server function on the interface.

    [Huawei-Gigabitthernet0/0/0]**dhcp select global**

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

DHCP Interface Address Pool Configuration



Requirement:

- Configure a router as the DHCP server, configure the subnet to which GE0/0/0 belongs as the address pool of DHCP clients, set the IP address of GE0/0/0 to that of the DNS server, and set the lease to three days.

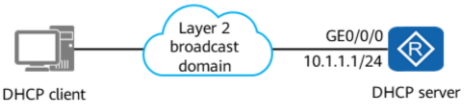
Configuration on the DHCP server:

```
[Huawei]dhcp enable
[Huawei]interface GigabitEthernet0/0/0
[Huawei-GigabitEthernet0/0/0]dhcp select interface
[Huawei-GigabitEthernet0/0/0]dhcp server dns-list 10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server excluded-ip-address 10.1.1.2
[Huawei-GigabitEthernet0/0/0]dhcp server lease day 3
```

Enable the DHCP service globally, enter the interface view, associate the current interface with the DHCP address pool, configure the DNS address and excluded IP address (excluding the interface IP address) in the interface view, and configure the lease of the IP addresses assigned to clients.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

DHCP Global Address Pool Configuration



Requirement:

- Configure a router as the DHCP server and configure the global address pool **pool2** to assign IP addresses (on the subnet 1.1.1.0/24) to DHCP clients. Set both the gateway address and DNS address to 1.1.1.1, set the lease to 10 days, and enable GE0/0/0 to use the global address pool.

Configuration on the DHCP server:

```
[Huawei]dhcp enable
[Huawei]ip pool pool2
Info: It's successful to create an IP address pool.
[Huawei-ip-pool-pool2]network 1.1.1.0 mask 24
[Huawei-ip-pool-pool2]gateway-list 1.1.1.1
[Huawei-ip-pool-pool2]dns-list 1.1.1.1
[Huawei-ip-pool-pool2]lease day 10
[Huawei-ip-pool-pool2]quit
[Huawei]interface GigabitEthernet0/0/0
[Huawei-GigabitEthernet0/0/1]dhcp select global
```

- Enable the DHCP service globally and configure the global address pool **pool2**. Configure the address range, gateway address, DNS address, and lease for **pool2**.
- Select the global address pool on a specific interface (GE0/0/0). When GE0/0/0 receives a DHCP request, it assigns an IP address from the global address pool.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

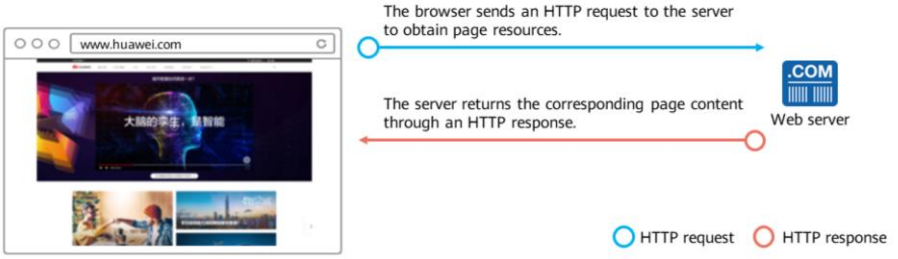
Contents

1. File Transfer
2. Telnet
3. DHCP
4. **HTTP**
5. DNS
6. NTP

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Web Page Access Using a Browser

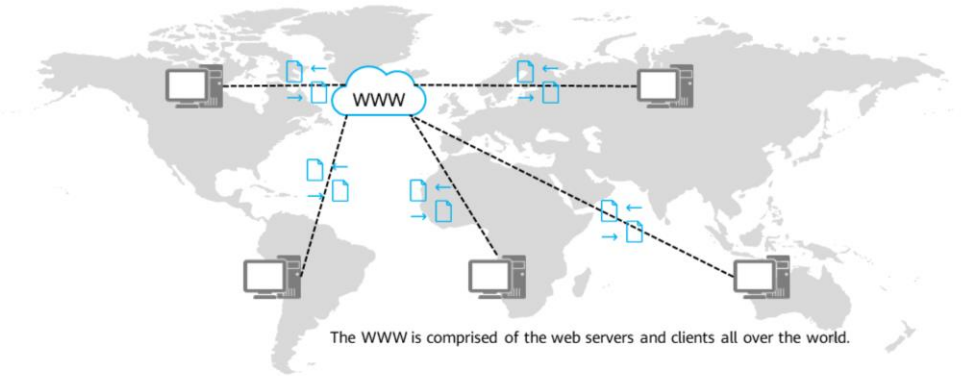


- When you enter a uniform resource locator (URL) in a browser, the browser can obtain data from a web server and display the content on the page.
- Hypertext Transfer Protocol (HTTP): an application layer protocol for communication between a client browser or another program and a web server
- HTTP adopts the typical C/S architecture, and uses TCP for transmission.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- URL: uniquely identifies the location of a web page or other resources on the Internet. A URL can contain more detail, such as the name of a page of hypertext, usually identified by the file name extension .html or .htm.

Background

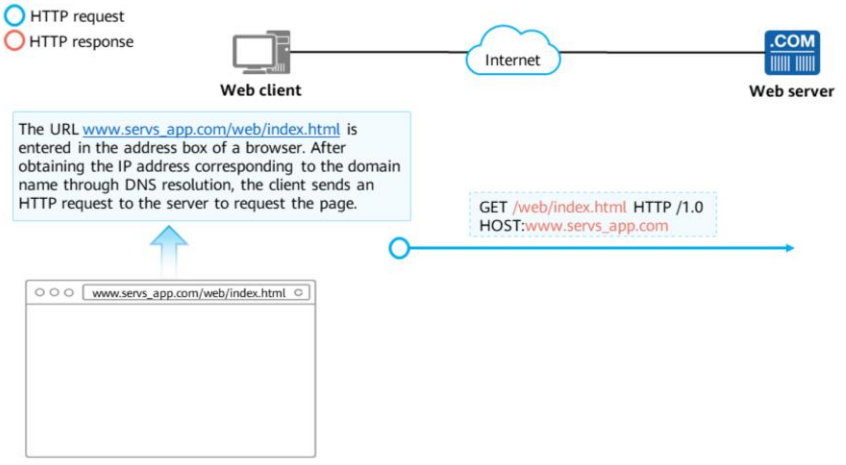


The WWW is comprised of the web servers and clients all over the world.

- In the early days of the Internet, World Wide Web (WWW) was proposed to share documents.
- The WWW consists of three parts: Hypertext Markup Language (HTML) for displaying document content in a browser, HTTP for transmitting documents on the network, and URLs for specifying document locations on the network.
- WWW was actually the name of a client application for browsing HTML documents, and now represents a collection of technologies (HTML + HTTP + URL) and is commonly known as the Web.

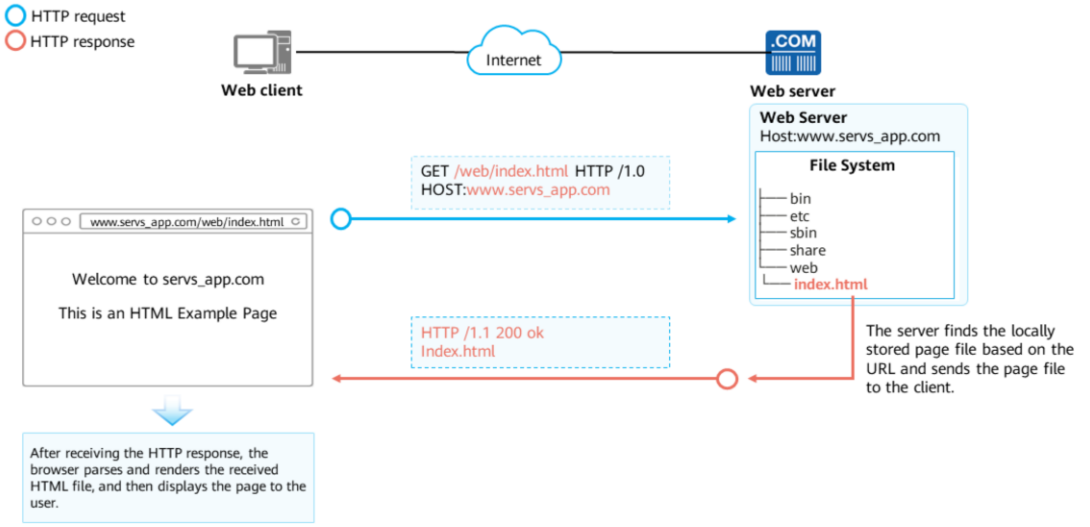
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Transfer Example (1)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Transfer Example (2)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

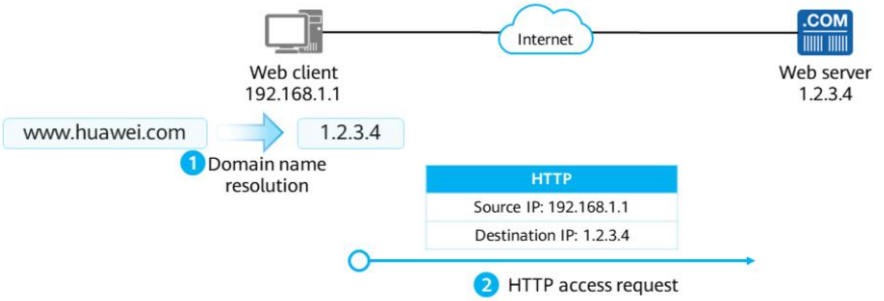
1. File Transfer
2. Telnet
3. DHCP
4. HTTP
5. **DNS**
6. NTP

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Birth of DNS

- When you enter a domain name in your browser to access a website, the domain name is resolved to an IP address. The browser actually communicates with this IP address.
- The protocol used for resolving domain names to IP addresses is Domain Name System (DNS).
- Each node on the network has a unique IP address, and nodes can communicate with one another through IP addresses. However, if all nodes communicate through IP addresses, it is difficult to remember so many IP addresses. Therefore, DNS is proposed to map IP addresses to alphanumeric character strings (domain names).



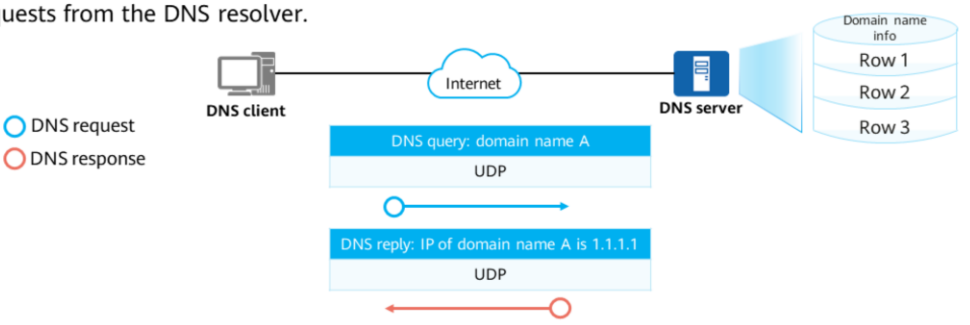
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Advanced Research Projects Agency Network (ARPANET), the predecessor of the Internet, provides the mappings between host names and IP addresses. However, the number of hosts was small at that time. Only one file (HOSTS.txt) is required to maintain the name-to-address mapping. The HOSTS.txt file is maintained by the network information center (NIC). Users who change their host names send their changes to the NIC by email, and the NIC periodically updates the HOSTS.txt file.
- However, after ARPANET uses TCP/IP, the number of network users increases sharply, and it seems difficult to manually maintain the HOSTS.txt file. The following issues may occur:
  - **Name conflict**: Although the NIC can ensure the consistency of host names that it manages, it is difficult to ensure that the host names are not randomly changed to be the same as those being used by others.
  - **Consistency**: As the network scale expands, it is hard to keep the HOSTS.txt file consistent. The names of other hosts may have been changed several times before the HOSTS.txt file of the current host is updated.
- Therefore, DNS is introduced.

DNS Components

- **Domain name**: a sequence of characters to identify hosts. In most cases, the URL entered in the browser when you visit a website is the domain name of the website.
- **DNS server**: maintains the mappings between domain names and IP addresses and responds to requests from the DNS resolver.

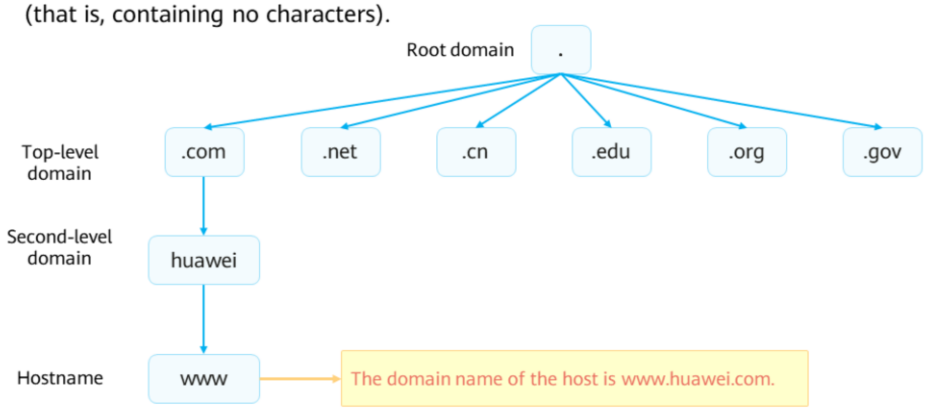


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The DNS adopts a distributed architecture. The database on each server stores only the mapping between some domain names and IP addresses.

Domain Name Format

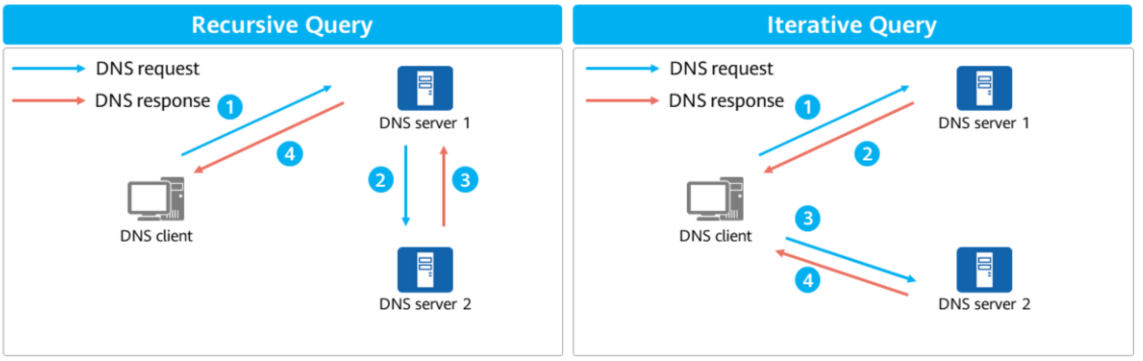
- The domain name is in the format of *hostname.second-level domain.top-level domain.root domain*. The root domain is represented by a dot (.). Generally, the root domain is denoted by an empty name (that is, containing no characters).



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

DNS Query Modes

- The DNS is a distributed system. The database of most DNS servers does not have all domain name records. When a client queries a domain name from a DNS server but the DNS server does not have the record of the domain name, the client can continue the query in either of the following ways:
  - **Recursive query**: The DNS server queries other DNS servers and returns the query result to the DNS client.
  - **Iterative query**: The DNS server informs the DNS client of the IP address of another DNS server, from which the DNS client queries the domain name.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The iterative query is different from the recursive query in that the DNS response returned by DNS server 1 contains the IP address of another DNS server (DNS server 2).

Contents

1. File Transfer
2. Telnet
3. DHCP
4. HTTP
5. DNS
6. **NTP**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

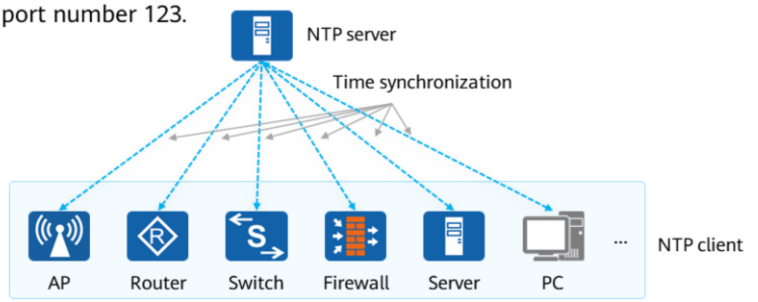
Time Synchronization Requirements

- Consistent clock of all devices is required in many scenarios on enterprise campus networks:
  - Network management: Analysis of logs or debugging messages collected from different routers needs time for reference.
  - Charging system: The clocks of all devices must be consistent.
  - Several systems working together on the same complicate event: Systems have to take the same clock for reference to ensure a proper sequence of implementation.
  - Incremental backup between a backup server and clients: Clocks on the backup server and clients should be synchronized.
  - System time: Some applications need to know the time when users log in to the system and the time when files are modified.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

NTP Overview

- If the administrator manually enters commands to change the system time for time synchronization, the workload is heavy and the accuracy cannot be ensured. Therefore, the Network Time Protocol (NTP) is designed to synchronize the clocks of devices.
- NTP is an application layer protocol belonging to the TCP/IP suite and synchronizes time between a group of distributed time servers and clients. NTP is based on IP and UDP, and NTP packets are transmitted using UDP on port number 123.

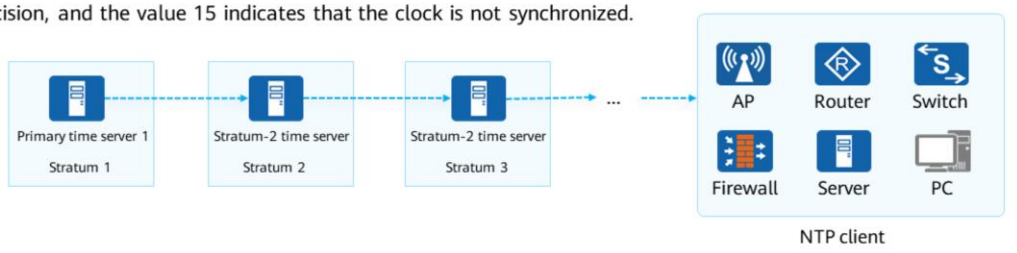


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Currently, mainstream network devices, such as access controllers (ACs), access points (APs), firewalls, routers, switches, and servers, basically serve as NTP clients, and some of the network devices can also serve as NTP servers.

NTP Network Structure

- **Primary time server**: directly synchronizes its clock with a standard reference clock through a cable or radio. Typically, the standard reference clock is either a radio clock or the Global Positioning System (GPS).
- **Stratum-2 time server**: synchronizes its clock with either the primary time server or other stratum-2 time servers within the network. Stratum-2 time servers use NTP to send time information to other hosts in a Local Area Network (LAN).
- **Stratum**: is a hierarchical standard for clock synchronization. It represents the precision of a clock. The value of a stratum ranges from 1 to 15. A smaller value indicates higher precision. The value 1 indicates the highest clock precision, and the value 15 indicates that the clock is not synchronized.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Quiz

1. Which FTP mode is recommended for transferring log and configuration files on network devices? Why?
2. Why does a DHCP client need to send a DHCP Request packet to the DHCP server to notify its use of a particular IP address after receiving a DHCP Offer packet?
3. What are the functions of HTML, URL, and HTTP?

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

1. ASCII mode; The binary mode is more applicable to the transmission of non-text files that cannot be converted, such as EXE, BIN, and CC (VRP version file extension) files.
2. A client's DHCP Request packet is broadcast, so other DHCP servers on the network know that the client has selected a particular IP address assigned by the DHCP server. This ensures that other DHCP servers can release this IP address assigned to the client through the unicast DHCP Offer packet.
3. HTML is used to display page content, URL is used to locate the network location of a document or file, and HTTP is used for requesting and transferring files.

Summary

- FTP is used to transfer files. You are advised to use different transfer modes for different files. FTP is based on TCP and therefore can ensure the reliability and efficiency of file transfer.
- Dynamically assigning IP addresses through DHCP reduces the workload of the administrator and avoids IP address conflicts caused by manual configuration of network parameters.
- As the document transfer protocol of WWW, HTTP is widely used in today's network for encoding and transporting information between a client (such as a web browser) and a web server.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



WLAN Overview

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- Wired LANs are expensive and lack mobility. The increasing demand for portability and mobility requires wireless local area network (WLAN) technologies.
- WLAN is now the most cost-efficient and convenient network access mode.
- This course introduces the development of WLAN in different phases, concepts related to WLAN technologies, implementation and basic configurations of common WLAN networking architectures, and WLAN development trends.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand basic concepts of WLAN and the history of the 802.11 protocol family.
  - Learn about different WLAN devices.
  - Distinguish between different WLAN networking architectures.
  - Understand the WLAN working process.
  - Complete basic WLAN configurations.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

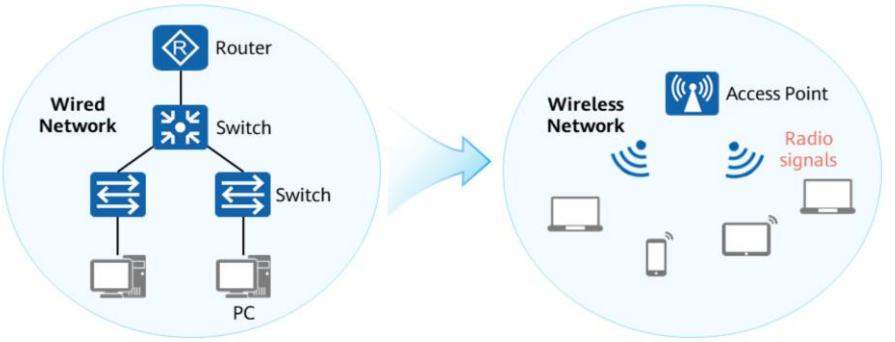
Contents

1. **WLAN Overview**
2. Basic Concepts of WLAN
3. WLAN Fundamentals
4. WLAN Configuration Implementation
5. Next-Generation WLAN Solutions

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Introduction to WLAN

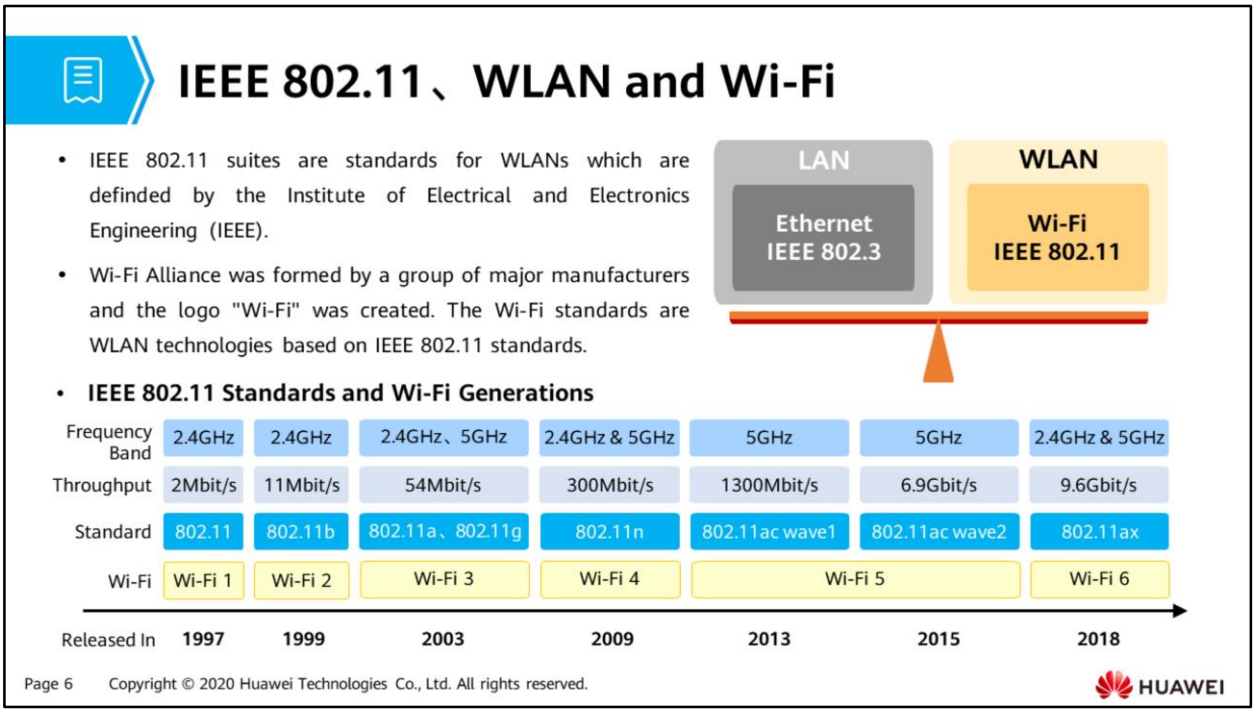
- A wireless local area network (WLAN) is constructed using wireless technologies. It uses high-frequency (2.4 GHz or 5 GHz) signals such as radio waves, lasers, and infrared rays to replace the traditional media used for transmission on a wired LAN.
- WLAN technology allows users to easily access a wireless network and move around within the coverage of the wireless network.



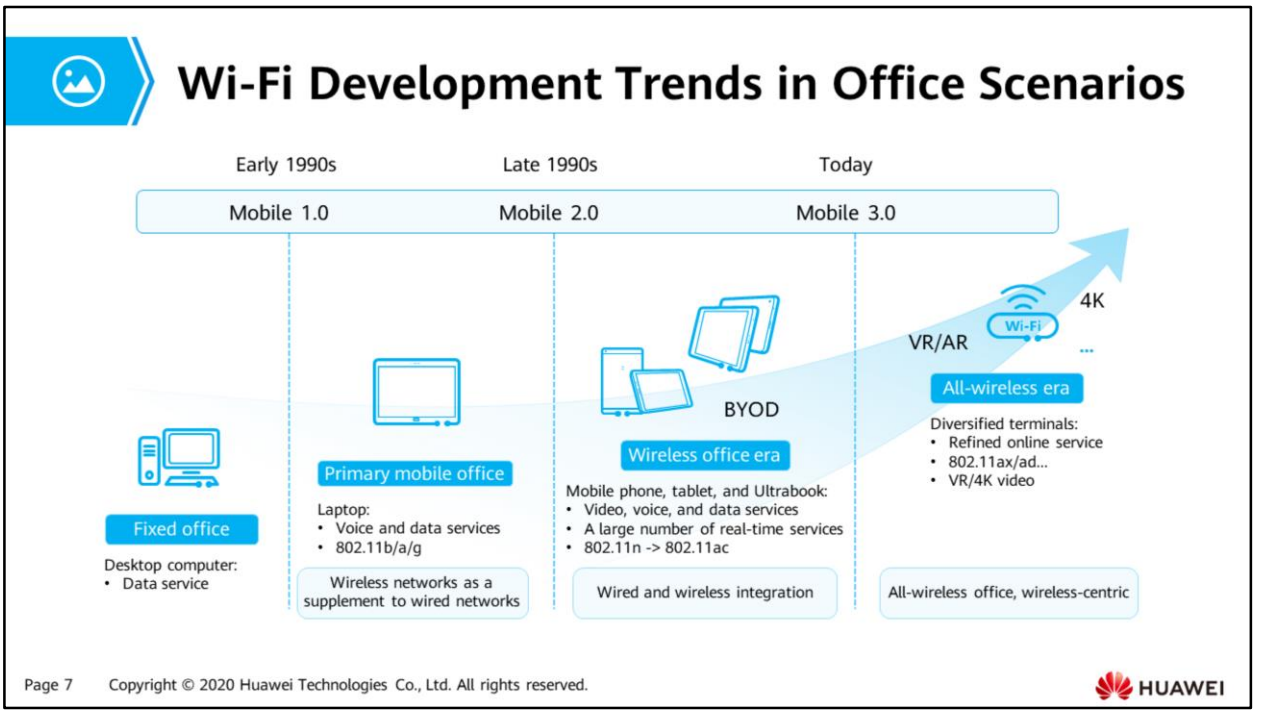
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A wireless local area network (WLAN) is constructed using wireless technologies.
  - Wireless technologies mentioned here include not only Wi-Fi, but also infrared, Bluetooth, and ZigBee.
  - WLAN technology allows users to easily access a wireless network and move around within the coverage of the wireless network.
- Wireless networks can be classified into WPAN, WLAN, WMAN, and WWAN based on the application scope.
  - Wireless personal area network (WPAN): Bluetooth, ZigBee, NFC, HomeRF, and UWB technologies are commonly used.
  - Wireless local area network (WLAN): The commonly used technology is Wi-Fi. WPAN-related technologies may also be used in WLANs.
  - Wireless metropolitan area network (WMAN): Worldwide Interoperability for Microwave Access (WiMAX) is commonly used.
  - Wireless wide area network (WWAN): GSM, CDMA, WCDMA, TD-SCDMA, LTE, and 5G technologies are commonly used.

- Advantages of WLAN:
    - High network mobility: WLANs are easily connected, and are not limited by cable and port positions. This makes WLANs most suitable for scenarios where users are often moving, such as in office buildings, airport halls, resorts, hotels, stadiums, and cafes.
    - Flexible network deployment: WLANs provide wireless network coverage in places where cables are difficult to deploy, such as subways and highways. WLANs reduce the number of required cables, offer low-cost, simplify deployment, and have high scalability.
- Note: WLAN technology described in this document is implemented based on 802.11 standards. That is, a WLAN uses high-frequency (2.4 GHz or 5 GHz) signals as transmission media.



- IEEE 802.11 standards are located on the lower two layers of the equivalent TCP/IP model.
  - Data link layer: provides channel access, addressing, data frame check, error detection, and security mechanisms.
  - Physical layer: transmits bit streams over an air interface, for example, specifying the frequency band.
- When created in 1999, the Wi-Fi Alliance was called the Wireless Ethernet Compatibility Alliance (WECA) at that time. In October 2002, the WECA was renamed Wi-Fi Alliance.
- The first version of IEEE 802.11 was released in 1997. Since then, more IEEE 802.11-based supplementary standards have been gradually defined. The most well-known standards that affect the evolution of Wi-Fi are 802.11b, 802.11a, 802.11g, 802.11n, and 802.11ac.
- When the IEEE 802.11ax standard is released, the Wi-Fi Alliance renames the new Wi-Fi specification to Wi-Fi 6, the mainstream IEEE 802.11ac to Wi-Fi 5, and IEEE 802.11n to Wi-Fi 4. The same naming convention applies to other generations.



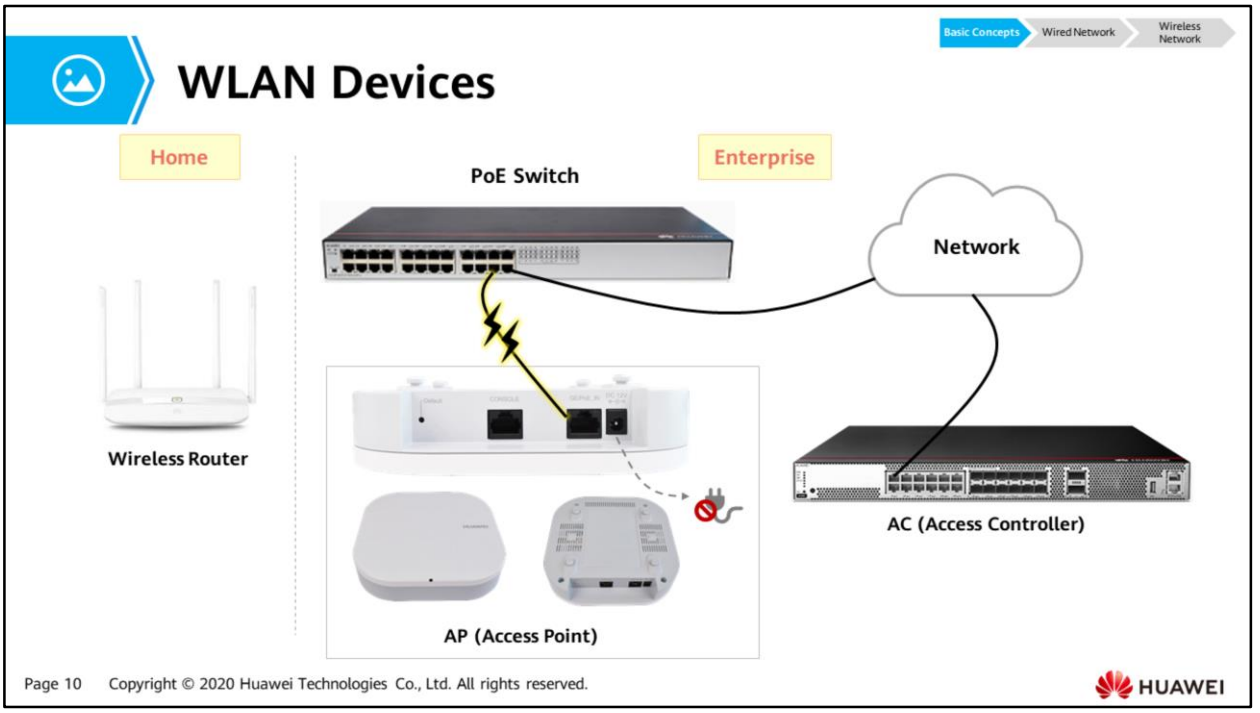
- Phase 1: Initial Mobile Office Era — Wireless Networks as a Supplement to Wired Networks
    - WaveLAN technology is considered as the prototype of enterprise WLAN. Early Wi-Fi technologies were mainly applied to IoT devices such as wireless cash registers. However, with the release of 802.11a/b/g standards, wireless connections have become increasingly advantageous. Enterprises and consumers are beginning to realize the potential of Wi-Fi technologies, and wireless hotspots are found to be deployed in cafeterias, airports, and hotels.
    - The name Wi-Fi was also created during this period. It is the trademark of the Wi-Fi Alliance. The original goal of the alliance was to promote the formulation of the 802.11b standard as well as the compatibility certification of Wi-Fi products worldwide. With the evolution of standards and the popularization of standard-compliant products, people tend to equate Wi-Fi with the 802.11 standard.
    - The 802.11 standard is one of many WLAN technologies, and yet it has become a mainstream standard in the industry. When a WLAN is mentioned, it usually is a WLAN using the Wi-Fi technology.
    - The first phase of WLAN application eliminated the limitation of wired access, with the goal to enable devices to move around freely within a certain range. That is, WLAN extends wired networks with the utilization of wireless networks. In this phase, WLANs do not have specific requirements on security, capacity, and roaming capabilities. APs are still single access points used for wireless coverage in single-point networking. Generally, an AP using a single access point architecture is called a Fat AP.

- Phase 2: Wireless Office Era — Integration of Wired and Wireless Networks
    - With the increasing popularity of wireless devices, WLANs have evolved from the supplement of wired networks to necessities.
    - In this phase, a WLAN, as a part of the network, needs to provide network access for enterprise guests.
    - Numerous large-bandwidth services, such as video and voice, are required in office scenarios, thereby imposing higher bandwidth requirements on WLANs. Since 2012, the 802.11ac standard has become mature and implemented many improvements in the working frequency bands, channel bandwidths, as well as modulation and coding schemes (MCSs). Compared with earlier 802.11 standards, the 802.11ac standard includes higher traffic volumes and less interference, and it allows more users to access networks.
- Phase 3: All-Wireless Office Era, Wireless-Centric
    - Currently, WLANs have entered the third phase. In office environments, wireless networks are used in preference to wired networks, and each office area is covered entirely by Wi-Fi. Furthermore, office areas do not include a wired network port, making the office environment more open and intelligent.
    - In the future, high-bandwidth services, including cloud desktop office, telepresence conference, and 4K video, will be migrated from wired to wireless networks. Likewise, new technologies such as virtual reality (VR)/augmented reality (AR) will be directly deployed on wireless networks. These new application scenarios pose higher requirements on WLAN design and planning.
    - The year 2018 marked the release of the next-generation Wi-Fi standard, referred to as Wi-Fi 6 and 802.11ax by the Wi-Fi Alliance and IEEE, respectively. This represents another milestone in Wi-Fi development. In that regard, the core value of Wi-Fi 6 is further improvements in capacity, leading wireless communications into the 10-gigabit era. The concurrent performance has improved fourfold, ensuring excellent service capabilities in high-density access and heavy-load scenarios.

Contents

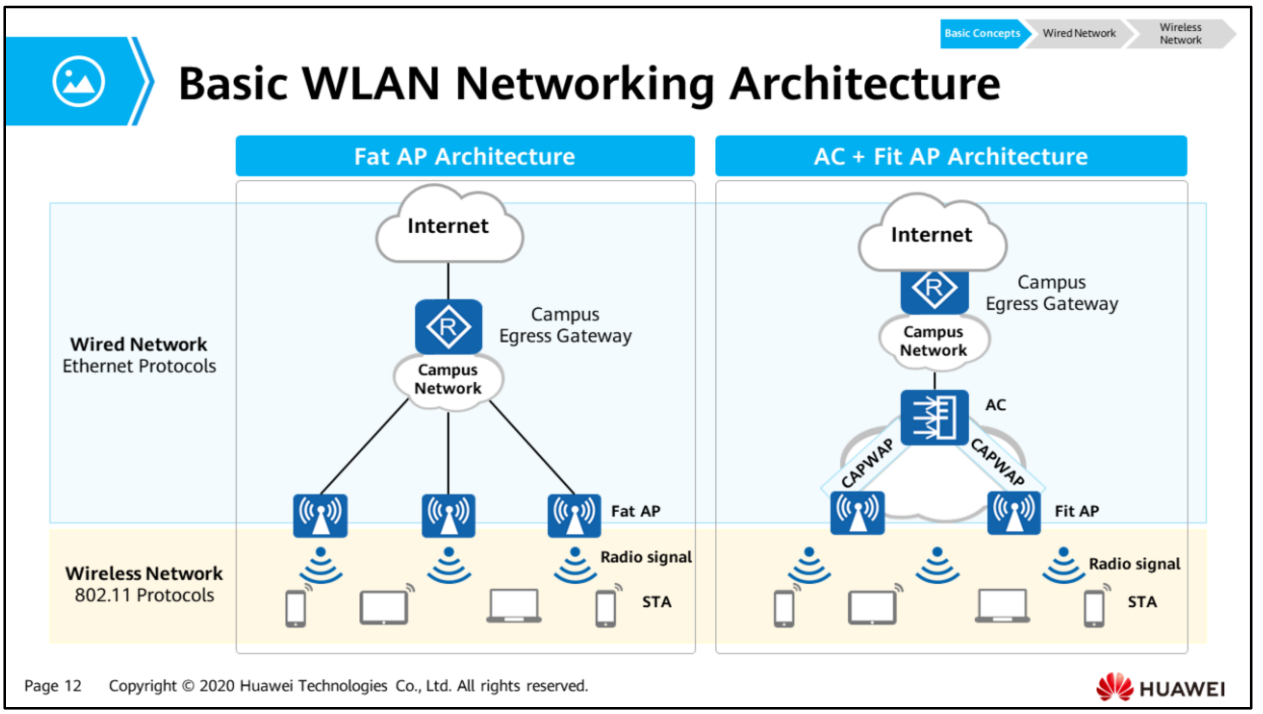
1. WLAN Overview
2. **Basic Concepts of WLAN**
3. WLAN Fundamentals
4. WLAN Configuration Implementation
5. Next-Generation WLAN Solutions

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Huawei WLAN products provide high-speed, secure, and reliable wireless network connections in various scenarios, such as indoor and outdoor scenarios and home and enterprise scenarios.
- Wireless routers are Fat APs in most cases.
  - A wireless router converts wired network signals into wireless signals to be received by devices such as home computers and mobile phones so that they can access the Internet in wireless mode.
- Enterprise WLAN products:
  - AP
    - The AP can switch flexibly among the Fat, Fit, and cloud modes based on the network plan.
    - Fat AP: applies to home WLANs. A Fat AP works independently and requires separate configurations. It provides only simple functions and is cost-effective. The Fat AP independently implements functions such as user access, authentication, data security, service forwarding, and QoS.
    - Fit AP: applies to medium- and large-sized enterprises. Fit APs are managed and configured by the AC in a unified manner, provide various functions, and have high requirements on network maintenance personnel's skills. Fit APs must work with an AC for user access, AP going-online, authentication, routing, AP management, security, and QoS.
    - Cloud AP: applies to small- and medium-sized enterprises. Cloud APs are managed and configured by a cloud management platform in a unified manner, provide various functions, support plug-and-play, and have low requirements on network maintenance personnel's skills.

- AC
  - An AC is usually deployed at the aggregation layer of a network to provide high-speed, secure, and reliable WLAN services.
  - Huawei ACs provide a large capacity and high performance. They are highly reliable, easy to install and maintain, and feature such advantages as flexible networking and energy conservation.
- PoE Switch
  - Power over Ethernet (PoE) provides electrical power through the Ethernet. It is also called Power over LAN (PoL) or active Ethernet.
  - PoE transmits power to terminals through data transmission lines or idle lines.
  - On a WLAN, a PoE switch can be used to supply power to APs.
  - PoE can be used to effectively provide centralized power for terminals such as IP phones, APs, portable device chargers, POS machines, cameras, and data collection devices. With PoE, terminals are provided with power when they access the network. Therefore, indoor cabling of power supply is not required.

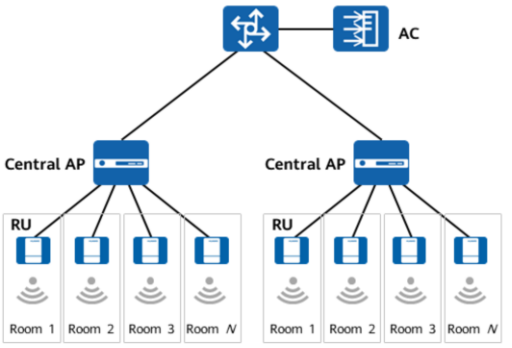


- A WLAN involves both wired and wireless sides. On the wired side, APs connect to the Internet using Ethernet. On the wireless side, STAs communicate with APs using 802.11 standards.
- The wireless side uses the centralized architecture. The original Fat AP architecture evolves to the AC + Fit AP architecture.
    - Fat AP architecture
        - This architecture is also called autonomous network architecture because it does not require a dedicated device for centralized control. It can implement functions such as connecting wireless users, encrypting service data, and forwarding service data packets.
        - Applicable scope: home and small-sized enterprises
        - Characteristics: A Fat AP works independently and is configured separately. It provides only simple functions and is cost-effective.
        - Disadvantages: The increase in the WLAN coverage area and the number of access users requires more and more Fat APs. No unified control device is available for these independently working Fat APs. Therefore, it is difficult to manage and maintain the Fat APs.

    - AC + Fit AP architecture
        - In this architecture, an AC is responsible for WLAN access control, forwarding and statistics collection, AP configuration monitoring, roaming management, AP network management agent, and security control. A Fit AP encrypts and decrypts 802.11 packets, provides 802.11 physical layer functions, and is managed by an AC.
        - Applicable scope: medium- and large-sized enterprises
        - Characteristics: Fit APs are managed and configured by the AC in a unified manner, provide various functions, and have high requirements on network maintenance personnel's skills.
- Note: This course uses the AC + Fit AP architecture as an example.

- Basic WLAN Concepts
    - Station (STA)
        - 802.11-compliant terminal, for example, PC with wireless network interface cards (NICs) or mobile phone that supports WLAN
    - AC
        - Controls and manages all Fit APs on an AC + Fit AP network. For example, an AC can connect to an authentication server to authenticate WLAN users.
    - AP
        - Provides 802.11-compliant wireless access for STAs. APs connect wired networks to wireless networks.
    - Control And Provisioning of Wireless Access Points (CAPWAP)
        - An encapsulation and transmission mechanism defined in RFC 5415 to implement communication between APs and ACs.
    - Radio signal (radio electromagnetic wave)
        - High-frequency electromagnetic wave that has long-distance transmission capabilities. Radio signals provide transmission media for 802.11-compliant WLANs. Radio signals described in this course are electromagnetic waves on the 2.4 GHz or 5 GHz frequency band.

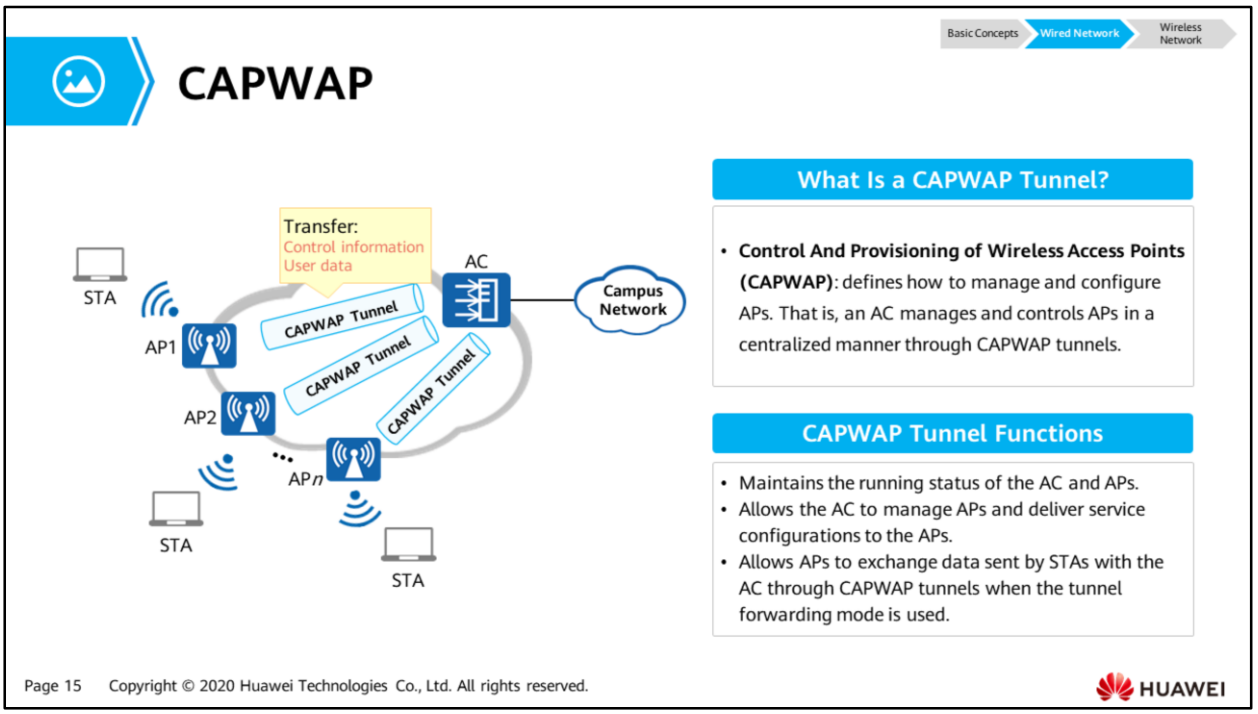
Agile Distributed Architecture



Architecture Characteristics

- The agile distributed architecture divides an AP into a central AP and remote units (RUs). The central AP can manage multiple RUs, which provides good coverage and reduces costs. RUs can be used in the Fat AP, AC + Fit AP, and cloud management architectures.
- Application scope: densely distributed rooms

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

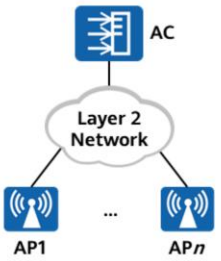


- To meet the requirements of large-scale networking and unified management of APs on the network, the Internet Engineering Task Force (IETF) sets up a CAPWAP Working Group and formulates the CAPWAP protocol. This protocol defines how an AC manages and configures APs. That is, CAPWAP tunnels are established between the AC and APs, through which the AC manages and controls the APs.
- CAPWAP is an application-layer protocol based on UDP transmission.
    - CAPWAP functions in the transmission of two types of messages:
        - Data messages, which encapsulate wireless data frames through the CAPWAP data tunnel.
        - Control messages, which are exchanged for AP management through the CAPWAP control tunnel.
    - CAPWAP data and control packets are transmitted on different UDP ports:
        - UDP port 5246 for transmitting control packets
        - UDP port 5247 for transmitting data packets

AP-AC Networking

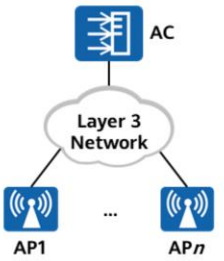
- The AP-AC networking modes are classified into Layer 2 networking and Layer 3 networking.

Layer 2 Networking



- Layer 2 networking: APs are connected to an AC directly or across a Layer 2 network.
- The Layer 2 networking features quick deployment. It is applicable to simple or temporary networking but not to large networking.

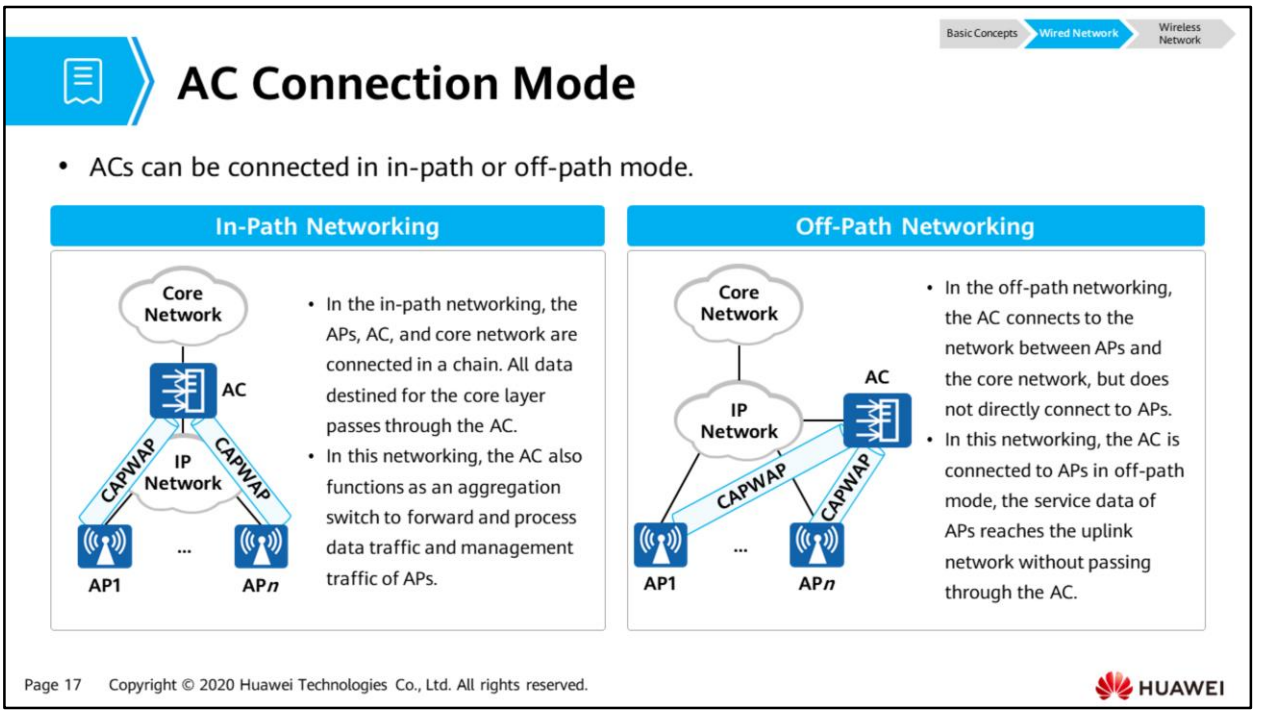
Layer 3 Networking



- Layer 3 networking: APs are connected to an AC across a Layer 3 network.
- In the actual networking, an AC can connect to dozens or even hundreds of APs, which is usually complex. In most cases, the Layer 3 networking is used on a large network.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

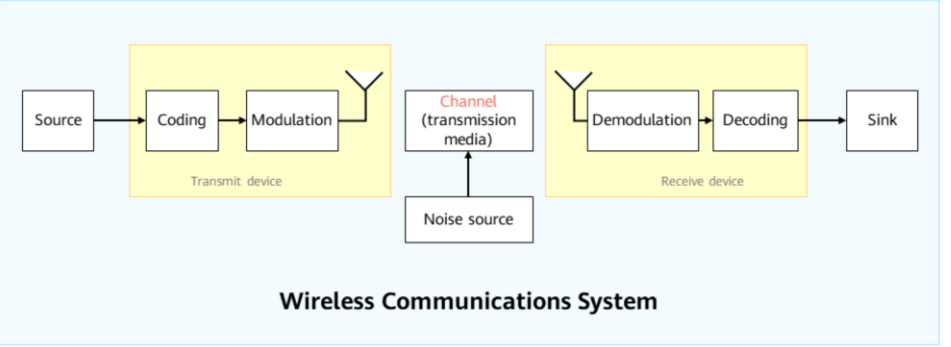
- AP-AC networking: The Layer 2 or Layer 3 networking can be used between the AC and APs. In the Layer 2 networking, APs can go online in plug-and-play mode through Layer 2 broadcast or DHCP. In the Layer 3 networking, APs cannot directly discover an AC. We need to deploy DHCP or DNS, or manually specify the AC's IP address.
- In the actual networking, an AC may connect to dozens or even hundreds of APs, which is complex. For example, on an enterprise network, APs can be deployed in offices, meeting rooms, and guest rooms, and the AC can be deployed in the equipment room. This constructs a complex Layer 3 network between the AC and APs. Therefore, the Layer 3 networking is often used on large-scale networks.



- AC connection mode: In in-path mode, the AC is deployed on the traffic forwarding path, and user traffic passes through the AC. This consumes the AC's forwarding capability. In off-path mode, traffic does not pass through the AC.
- In-path networking:
  - In the in-path networking, the AC must be powerful in throughput and processing capabilities, or the AC becomes the bandwidth bottleneck.
  - This networking has a clear architecture and is easy to deploy.
- Off-path networking:
  - Most wireless networks are deployed after wired networks are constructed and are not planned in early stage of network construction. The off-path networking makes it easy to expand the wireless network. Customers only need to connect an AC to a network device, for example, an aggregation switch, to manage APs. Therefore, the off-path networking is used more often.
  - In the off-path networking, the AC only manages APs, and management flows are encapsulated and transmitted in CAPWAP tunnels. Data flows can be forwarded to the AC over CAPWAP tunnels, or forwarded to the uplink network by the aggregation switch and do not pass through the AC.

Wireless Communications System

- In a wireless communications system, information may be an image, a text, a sound, or the like. The transmit device first applies source coding to convert information into digital signals that allow for circuit calculation and processing, and then into radio waves by means of channel coding and modulation.



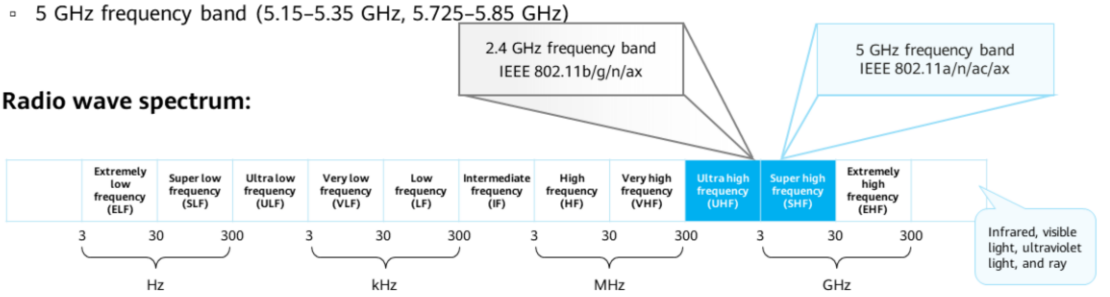
Wireless Communications System

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Coding
  - Source coding is a process of converting raw information into digital signals by using a coding scheme.
  - Channel coding is a technology for correcting and detecting information errors to improve channel transmission reliability. With wireless transmission that is prone to noise interference, information arriving at the receive device may be erroneous. Channel coding is introduced to restore information to the maximum extent on the receive device, thereby reducing the bit error rate.
- Modulation is a process of superimposing digital signals on high-frequency signals generated by high-frequency oscillation circuits so that the digital signals be converted into radio waves over antennas and then transmitted.
- A channel transmits information, and a radio channel is a radio wave in space.
- The air interface is used by radio channels. The transmit device and receive device are connected through the air interfaces and channels. The air interfaces in wireless communication are invisible and connected over the air.

Radio Wave

- A radio wave is an electromagnetic wave whose frequency is between 3 Hz and about 300 GHz. Radio technology converts sound signals or other signals and transmits them by using radio waves.
- WLAN technology enables transmission of information by radio waves over the air. Currently, the WLAN uses the following frequency bands:
  - 2.4 GHz frequency band (2.4–2.4835 GHz)
  - 5 GHz frequency band (5.15–5.35 GHz, 5.725–5.85 GHz)
- **Radio wave spectrum:**



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- ELF (3 Hz to 30 Hz): Used for submarine communication or directly converted into sound
- SLF (30 Hz to 300 Hz): Directly converted into sound or used for AC transmission system (50–60 Hz)
- ULF (300 Hz to 3 kHz): Used for communications in mining farms or directly converted into sound
- VLF (3 kHz to 30 kHz): Directly converted into sound and ultrasound or used for geophysics
- LF (30 kHz to 300 kHz): Used for international broadcasting
- IF (300 kHz to 3 MHz): Used for amplitude modulation (AM) broadcasting, maritime communications, and aeronautical communications
- HF (3 MHz to 30 MHz): Used for short-wave and civil radios
- VHF (30 MHz to 300 MHz): Used for frequency modulation (FM) broadcasting, television broadcasting, and aeronautical communications
- UHF (300 MHz to 3 GHz): Used for television broadcasting, radio telephone communications, wireless network, and microwave oven
- SHF (3 GHz to 30 GHz): Used for wireless network, radar, and artificial satellite
- EHF (30 GHz to 300 GHz): Used for radio astronomy, remote sensing, and millimeter wave scanner
- Higher than 300 GHz: Infrared, visible light, ultraviolet light, and ray

Radio Channel

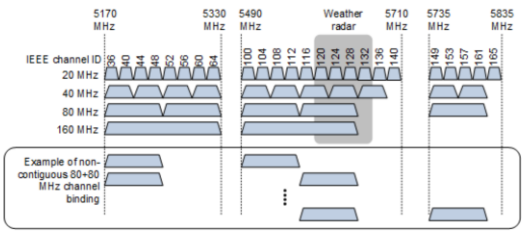
- A channel transmits information, and a radio channel is a radio wave in space. Given that radio waves are ubiquitous, the random use of spectrum resources will cause endless interference issues. Therefore, in addition to defining the usable frequency bands, wireless communication protocols must also accurately divide the frequency ranges. Each frequency range is a channel.

2.4 GHz Frequency Band



- The 2.4 GHz frequency band is divided into 14 channels with overlapping or non-overlapping relationships, each with a bandwidth of 20 MHz.
  - Overlapping channels, such as channels 1 and 2, interfere with each other.
  - Non-overlapping channels, such as channels 1 and 6, do not interfere with each other.

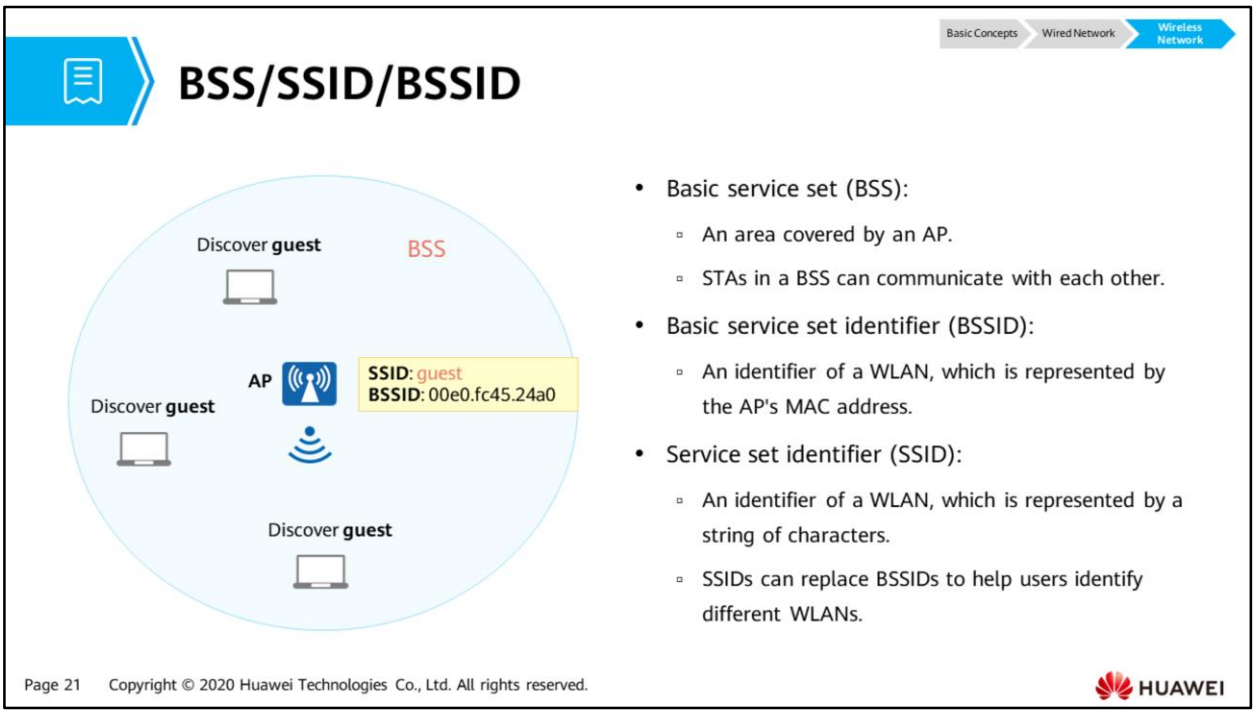
5 GHz Frequency Band



- The 5 GHz frequency band has richer spectrum resources. In addition to 20 MHz channels, APs working on the 5 GHz frequency band support 40 MHz, 80 MHz, and higher-bandwidth channels.

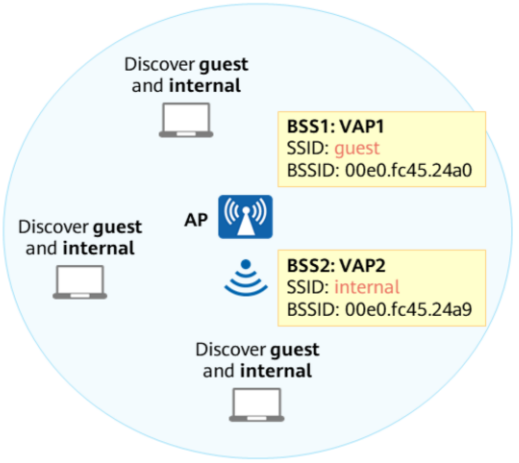
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- On a WLAN, the operating status of APs is affected by the radio environment. For example, a high-power AP can interfere with adjacent APs if they work on overlapping channels.
- In this case, the radio calibration function can be deployed to dynamically adjust channels and power of APs managed by the same AC to ensure that the APs work at the optimal performance.



- BSS:
  - A BSS, the basic service unit of a WLAN, consists of an AP and multiple STAs. The BSS is the basic structure of an 802.11 network. Wireless media can be shared, and therefore packets sent and received in a BSS must carry the BSSID (AP's MAC address).
- BSSID:
  - AP's MAC address on the data link layer.
  - STAs can discover and find an AP based on the BSSID.
  - Each BSS must have a unique BSSID. Therefore, the AP's MAC address is used to ensure the uniqueness of the BSSID.
- SSID:
  - A unique identifier that identifies a wireless network. When you search for available wireless networks on your laptop, SSIDs are displayed to identify the available wireless networks.
  - If multiple BSSs are deployed in a space, the STA may discover not only one BSSID. You only need to select a BSSID as required. For easier AP identification, a string of characters is configured as the AP name. This character string is the SSID.

VAP



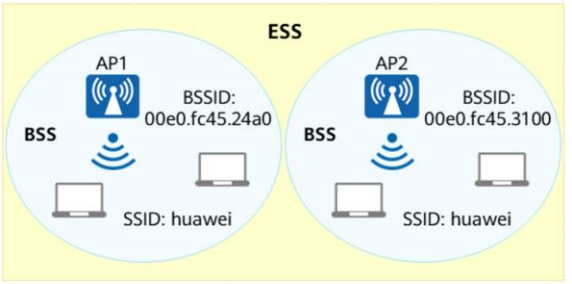
- In the early stage, APs support only one BSS. If multiple BSSs are deployed in a space, we must also deploy multiple APs, which increases costs and occupies channel resources. To resolve this problem, APs now support creation of multiple virtual access points (VAPs).
- VAP:
  - A physical AP can be virtualized into multiple VAPs, each of which provides the same functions as the physical AP.
  - Each VAP corresponds to one BSS. In this way, one AP may provide multiple BSSs that can have different SSIDs specified.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- VAP:
  - A VAP is a functional entity virtualized on a physical AP. You can create different VAPs on an AP to provide the wireless access service for different user groups.
- The use of VAPs simplifies WLAN deployment, but it does not mean that we need to configure as many as VAPs. VAPs must be planned based on actual requirements. Simply increasing the number of VAPs will increase the time for STAs to find SSIDs and make AP configuration more complex. Additionally, a VAP is not equivalent to a real AP. All VAPs virtualized from a physical AP share software and hardware resources of the AP, and all users associated with these VAPs share same channel resources. The capacity of an AP will not change or multiply with the increasing number of VAPs.

ESS



- The coverage of a BSS is limited. An extended service set (ESS) can be used to expand the coverage. When a STA moves from one BSS to another BSS, an ESS ensures that the STA does not sense the change of the SSID.
- ESS:
  - A larger-scale virtual BSS that consists of multiple BSSs with the same SSID.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- ESS:
  - A large-scale virtual BSS consisting of multiple BSSs with the same SSID.
  - A STA can move and roam within an ESS and considers that it is within the same WLAN regardless of its location.
- WLAN roaming:
  - WLAN roaming allows STAs to move within the coverage areas of APs belonging to the same ESS with nonstop service transmission.
  - The most obvious advantage of the WLAN is that a STA can move within a WLAN without physical media restrictions. WLAN roaming allows the STA to move within a WLAN without service interruption. Multiple APs are located within an ESS. When a STA moves from an AP to another, WLAN roaming ensures seamless transition of STA services between APs.

Contents

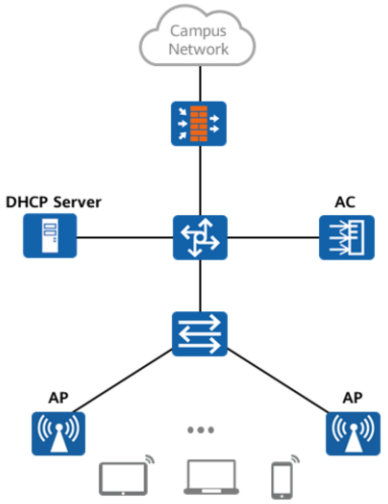
1. WLAN Overview
2. Basic Concepts of WLAN
3. **WLAN Fundamentals**
4. WLAN Configuration Implementation
5. Next-Generation WLAN Solutions

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

AP Onboarding | Configuration Delivery | STA Access | Data Forwarding

WLAN Working Process Overview



WLAN Working Process

1. AP onboarding

An AP obtains an IP address, discovers an AC, and sets up a connection with the AC.

2. WLAN service configuration delivery

The AC delivers WLAN service configurations to the AP.

3. STA access

STAs find the SSID transmitted by the AP, connect to the network, and go online.

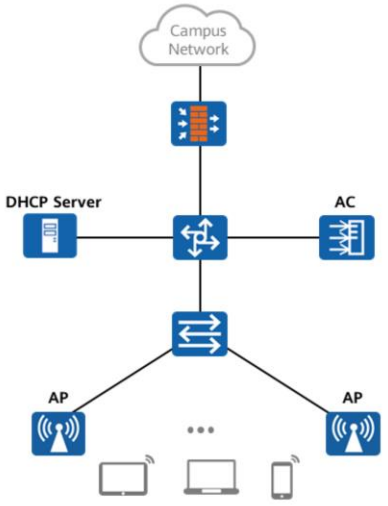
4. WLAN service data forwarding

The WLAN starts to forward service data.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- In the AC + Fit AP networking architecture, the AC manages APs in a unified manner. Therefore, all configurations are performed on the AC.

WLAN Working Process: Step 1



WLAN Working Process

1. AP onboarding

The AC can manage and control Fit APs in a centralized manner and deliver services only after they go online. The procedure is as follows:

1. An AP obtains an IP address.
2. The AP discovers the AC and establishes a CAPWAP tunnel with it.
3. AP access control
4. AP upgrade
5. CAPWAP tunnel maintenance

2. WLAN service configuration delivery
3. STA access
4. WLAN service data forwarding

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

APs Obtain IP Addresses

IP address allocation
CAPWAP tunnel establishment
AP access control
AP upgrade (Optional)
CAPWAP tunnel maintenance

- An AP can communicate with an AC only after obtaining an IP address.

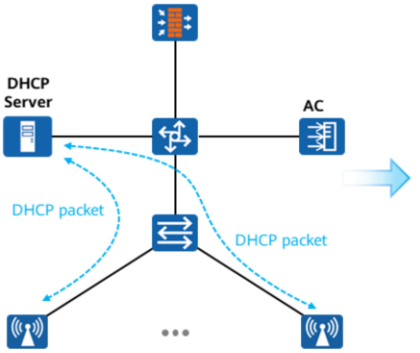
IP Address Allocation

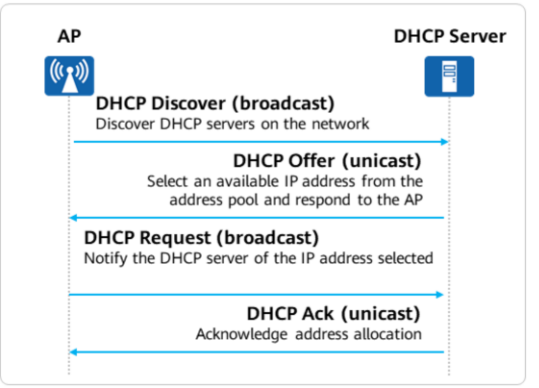
- An AP can obtain an IP address in either of the following modes:
  - Static mode: A user logs in to the AP and configures its IP address.
  - DHCP mode: The AP serves as a DHCP client and requests an IP address from a DHCP server.
- Typical solutions:
  - Deploy a dedicated DHCP server to assign IP addresses to APs.
  - Configure the AC to assign IP addresses to APs.
  - Use a device on the network, such as a core switch, to assign IP addresses to APs.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

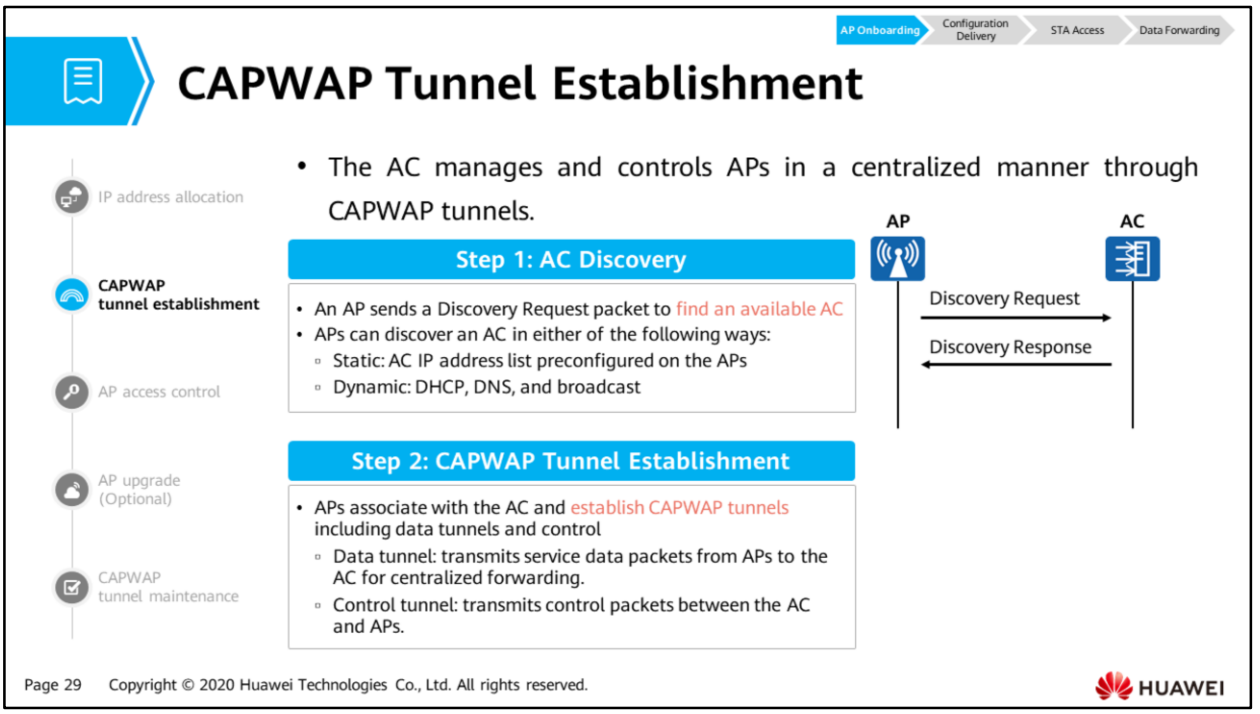
DHCP IP Address Allocation

- IP address allocation
- CAPWAP tunnel establishment
- AP access control
- AP upgrade (Optional)
- CAPWAP tunnel maintenance

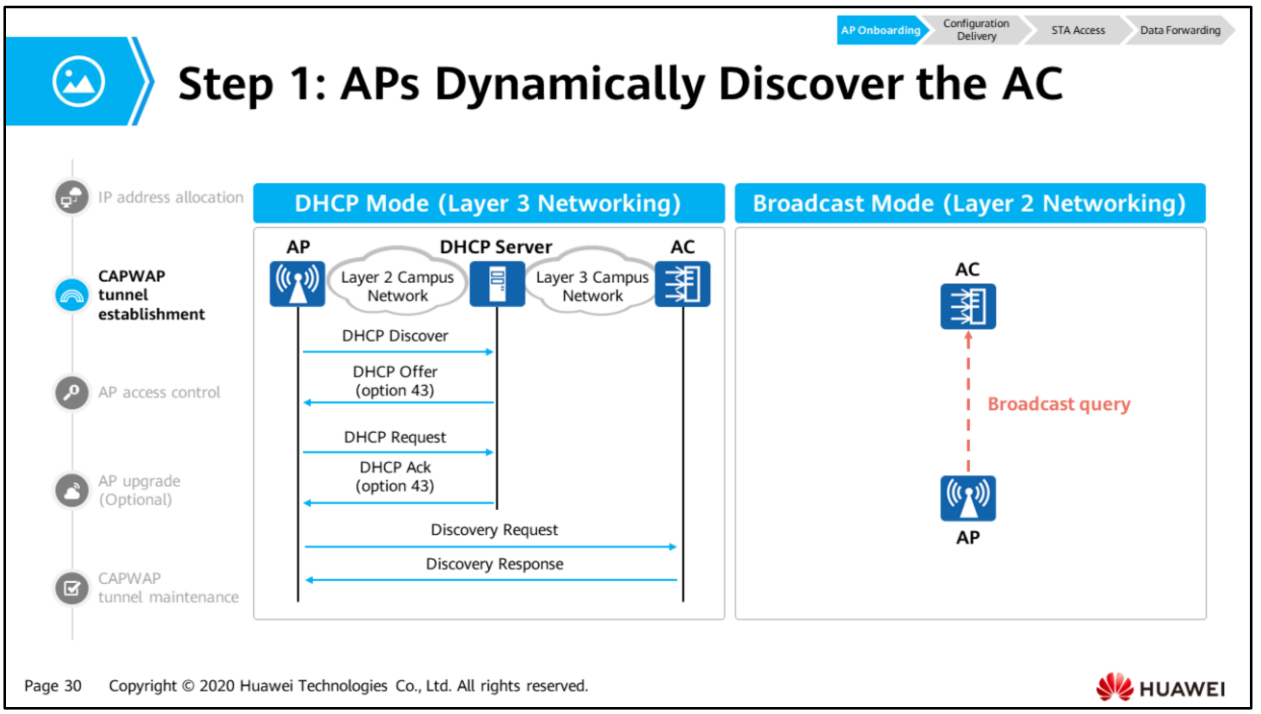




Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- CAPWAP tunnels provide the following functions:
  - Maintains the running status of the AC and APs.
  - Allows the AC to manage APs and deliver configurations to APs.
  - Transmits service data to the AC for centralized forwarding.
- AC discovery phase:
  - Static: An AC IP address list is preconfigured on the APs. When an AP goes online, the AP unicasts a Discovery Request packet to each AC whose IP address is specified in the preconfigured AC IP address list. After receiving the Discovery Request packet, the ACs send Discovery Response packets to the AP. The AP then selects an AC to establish a CAPWAP tunnel according to the received Discovery Request packets.
  - Dynamic: DHCP, DNS, and broadcast. This course describes DHCP and broadcast modes.

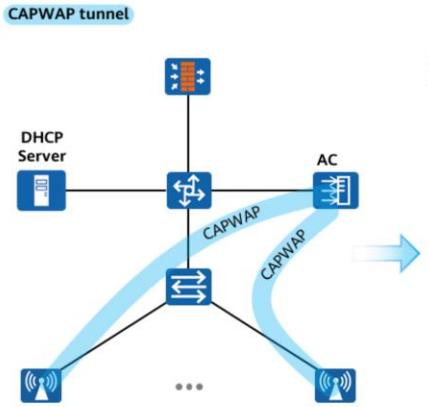


- DHCP mode:
  - Obtain the AC IP address through a four-way DHCP handshake process.
    - When no AC IP address list is preconfigured, the AP starts the dynamic AC auto-discovery process. The AP obtains an IP address through DHCP and the AC address list through the Option field in the DHCP packets. (The DHCP server is configured to carry Option 43 in the DHCP Offer packet, and Option 43 contains the AC IP address list.)
    - First, the AP sends a DHCP Discover packet to the DHCP server in broadcast mode. When receiving the DHCP Discover packet, the DHCP server encapsulates the first free IP address and other TCP/IP configuration in a DHCP Offer packet containing the lease duration, and sends the packet to the AP.
    - A DHCP Offer packet can be a unicast or broadcast packet. When the AP receives DHCP Offer packets from multiple DHCP servers, it selects only one DHCP Offer packet (usually the first DHCP Offer packet) and broadcasts a DHCP Request packet to all DHCP servers. Then, the AP sends a DHCP Request packet to the specified server from which will allocate an IP address.
    - When the DHCP server receives the DHCP Request packet, it responds with a DHCP Ack packet, which contains the IP address for the AP, lease duration, gateway information, and DNS server IP address. By now, the lease contract takes effect and the DHCP four-way handshake is completed.

    - The AC discovery mechanism allows APs to associate with the AC.
        - After obtaining the AC's IP address from the DHCP server, the AP finds available ACs through the AC discovery mechanism and decides to associate with the optimal AC and establish CAPWAP tunnels.
        - The AP starts the CAPWAP protocol discovery mechanism and sends unicast or broadcast request packets to attempt to associate with an AC. The ACs respond to the Discovery Request packets with unicast discovery response packets, containing the AC priority and the number of APs. The AP determines to associate with the appropriate AC based on the AC priority and the number of APs.
- Broadcast mode:
    - After an AP is started, if DHCP-based and DNS-based AC discovery procedures fail, the AP initiates a broadcast AC discovery procedure and broadcasts an AC discovery request.
    - The AC receiving discovery request packets checks whether the AP is authorized to access (or whether the AP has authorized MAC addresses or sequence numbers). If so, the AC returns a discovery response to the AP. If not, the AC rejects its discovery request.
    - Broadcast AC discovery is applicable to a Layer 2 network between the AP and the AC.

Step 2: CAPWAP Tunnel Establishment

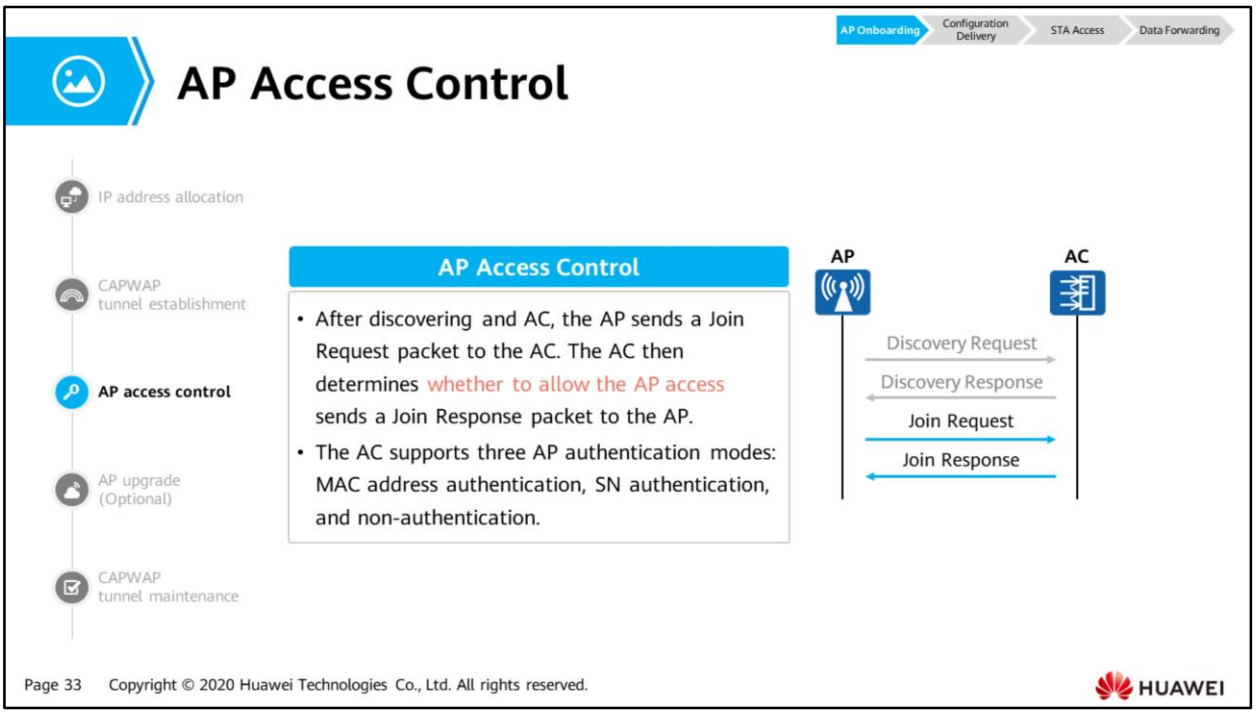
- IP address allocation
- **CAPWAP tunnel establishment**
- AP access control
- AP upgrade (Optional)
- CAPWAP tunnel maintenance



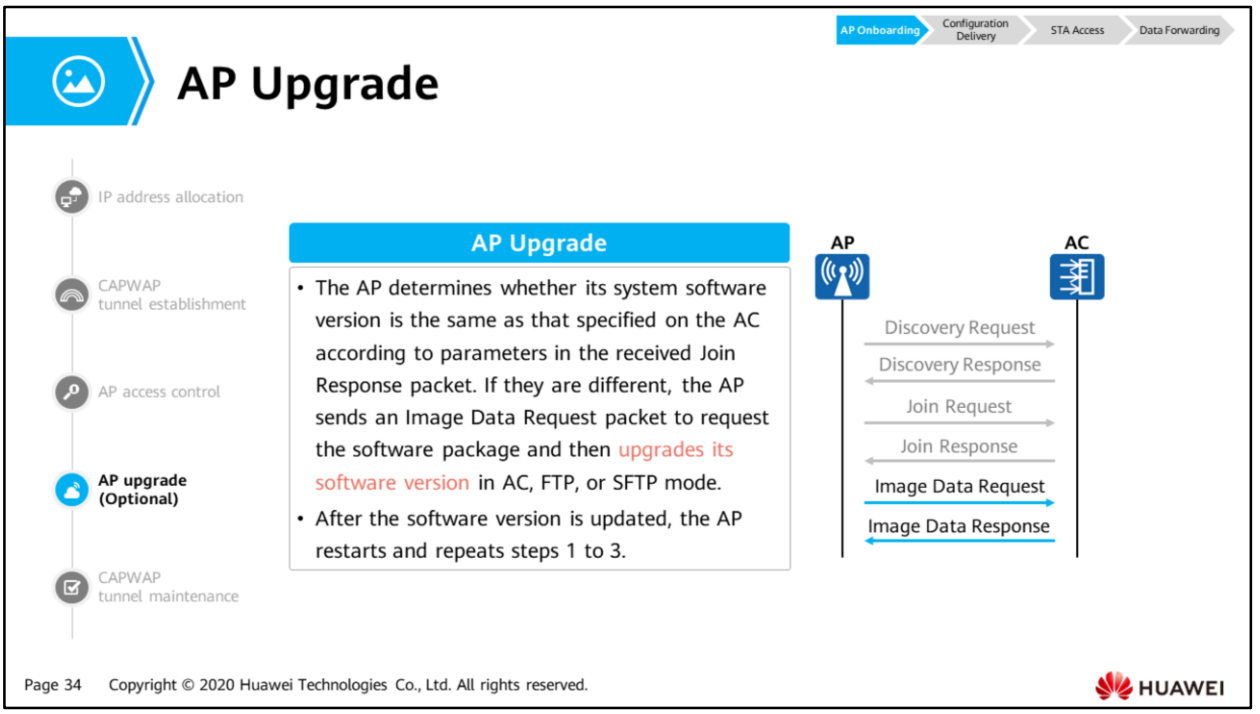
Step 2: CAPWAP Tunnel Establishment

- APs associate with the AC and establish CAPWAP tunnels, including data tunnels and control tunnels.
  - Data tunnel: transmits service data packets from APs to the AC for centralized forwarding. Datagram Transport Layer Security (DTLS) encryption can be enabled over the data tunnel to ensure security of CAPWAP data packets. Subsequently, CAPWAP data packets will be encrypted and decrypted using DTLS.
  - Control tunnel: transmits control packets between the AC and APs. DTLS encryption can be enabled over the control tunnel to ensure security of CAPWAP control packets. Subsequently, CAPWAP control packets will be encrypted and decrypted using DTLS.

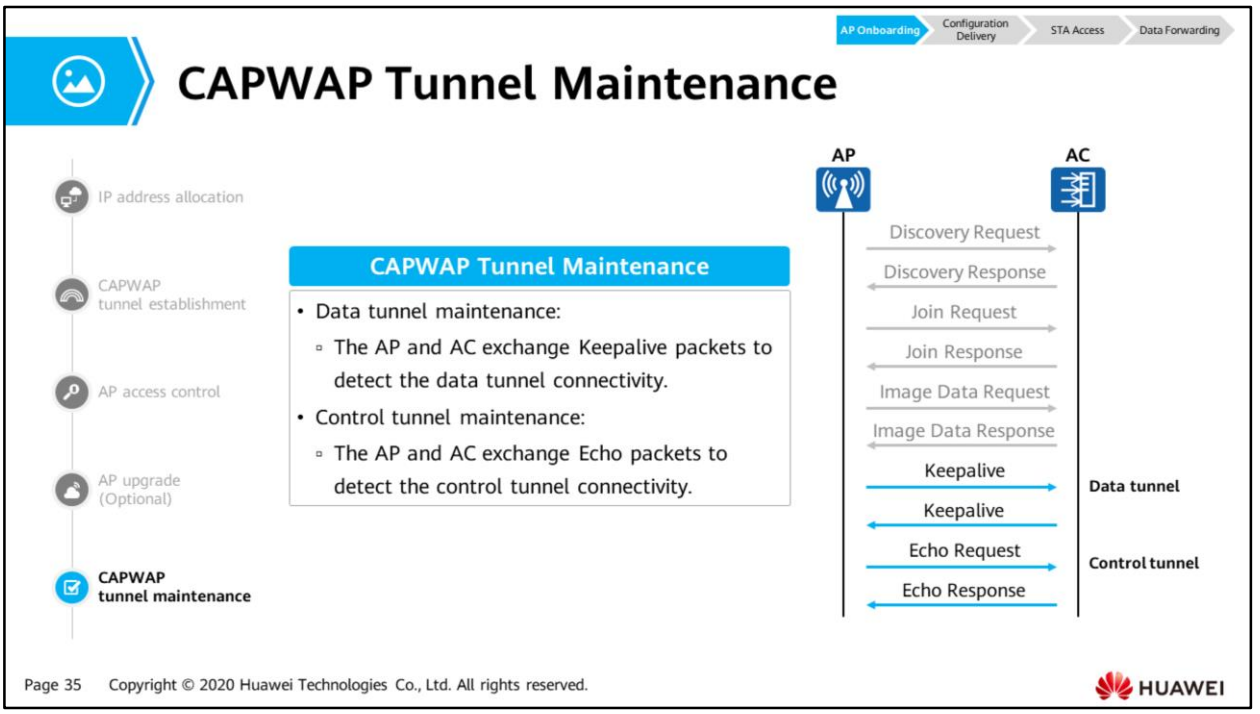
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



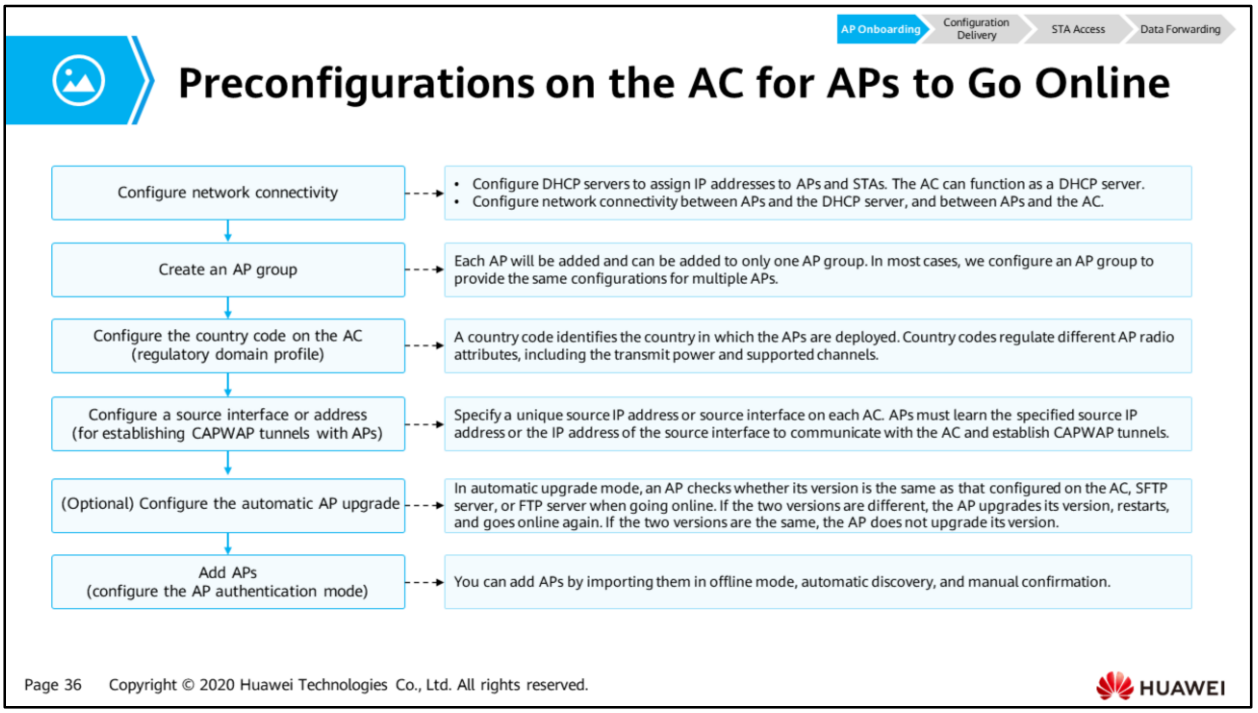
- After receiving the Join Request packet from an AP, an AC authenticates the AP. If authentication is successful, the AC adds the AP.
- The AC supports the following AP authentication modes:
  - MAC address authentication
  - SN authentication
  - Non-authentication
- APs can be added to an AC in the following ways:
  - Manual configuration: Specify the MAC addresses and SNs of APs in offline mode on the AC in advance. When APs are connected the AC, the AC finds that their MAC addresses and SNs match the preconfigured ones and establish connections with them.
  - Automatic discovery: If the AP authentication mode is set to non-authentication, or the AP authentication mode is set to MAC or SN authentication and the AP is whitelisted, the AC automatically discovers connected APs and establish connections with them.
  - Manual confirmation: If the AP authentication mode is set to MAC or SN authentication and the AP is not imported offline or whitelisted, the AC adds the AP to the list of unauthorized APs. You can manually confirm the identity of such an AP to bring it online.



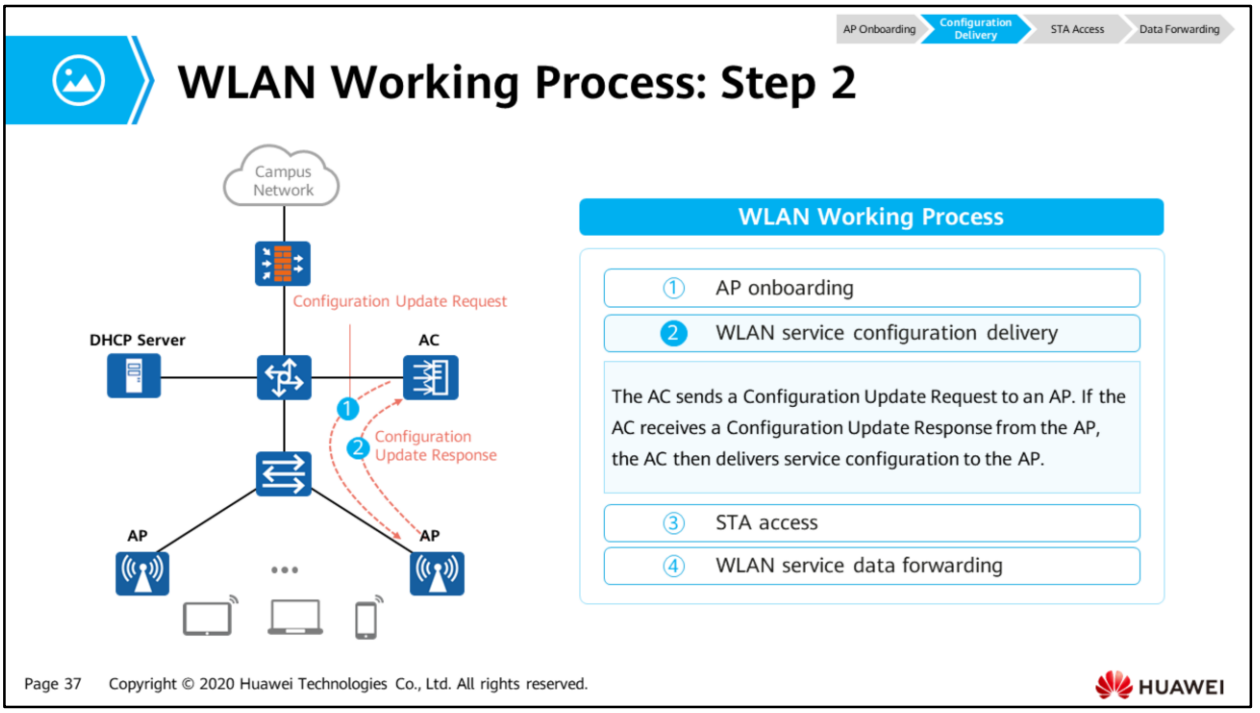
- APs can be upgraded on an AC in the following modes:
  - Automatic upgrade: mainly used when APs have not gone online on an AC. In this mode, we need to configure the automatic upgrade parameters for APs to go online before configuring AP access. Then the APs are automatically upgraded when they go online. An online AP will be automatically upgraded after the automatic upgrade parameters are configured and the AP is restarted in any mode. Compared with the automatic upgrade mode, the in-service upgrade mode reduces the service interruption time.
    - AC mode: applies when a small number of APs are deployed. APs download the upgrade file from the AC during the upgrade.
    - FTP mode: applies to file transfer without high network security requirements. APs download the upgrade file from an FTP server during the upgrade. In this mode, data is transmitted in clear text, which brings security risks.
    - SFTP mode: applies to scenarios that require high network security and provides strict encryption and integrity protection for data transmission. APs download the upgrade file from an SFTP server during an upgrade.
  - In-service upgrade: mainly used when APs are already online on the AC and carry WLAN services.
  - Scheduled upgrade: mainly used when APs are already online on the AC and carry WLAN services. The scheduled upgrade is usually performed during off-peak hours.



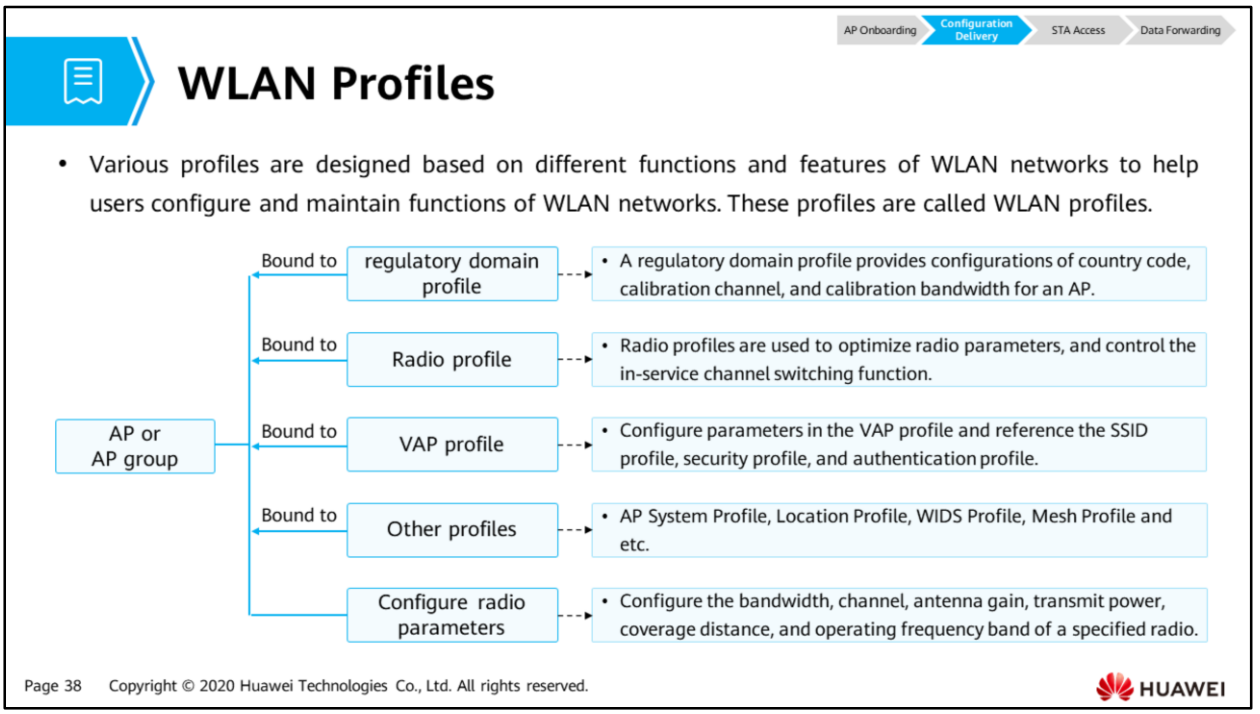
- Data tunnel maintenance:
  - The AP and AC exchange Keepalive packets (through the UDP port 5247) to detect the data tunnel connectivity.
- Control tunnel maintenance:
  - The AP and AC exchange Echo packets (through the UDP port 5246) to detect the control tunnel connectivity.



- Regulatory domain profile:
  - A regulatory domain profile provides configurations of the country code, calibration channel, and calibration bandwidth for an AP.
  - A country code identifies the country in which the APs are deployed. Country codes regulate different AP radio attributes, including the transmit power and supported channels. Correct country code configuration ensures that radio attributes of APs comply with local laws and regulations.
- Configure a source interface or address on the AC.
  - Specify a unique IP address, VLANIF interface, or Loopback interface on an AC. In this manner, APs connected to the AC can learn the specified IP address or the IP address of the specified interface to establish CAPWAP tunnels with the AC. This specified IP address or interface is called the source address or interface.
  - Only after the unique source interface or address is specified on an AC, can APs establish CAPWAP tunnels with the AC.
  - A VLANIF or Loopback interface can be used as the source interface, and their IP addresses can be configured as the source address.
- Add APs: Configure the AP authentication mode and enable APs to go online.
  - You can add APs by importing them in offline mode, automatic discovery, and manual confirmation.

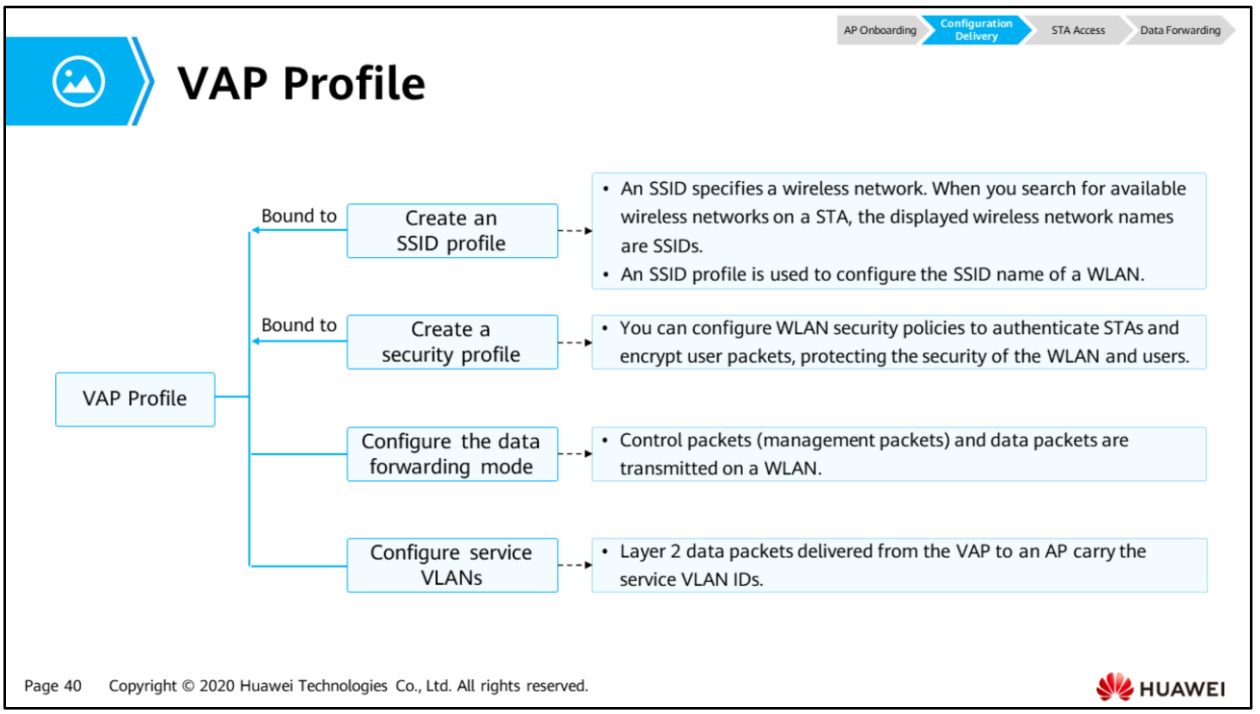


- After an AP goes online, it sends a Configuration Status Request containing its running configuration to the AC. The AC then compares the AP's running configuration with the local AP configuration. If they are inconsistent, the AC sends a Configuration Status Response message to the AP.
- Note: After an AP goes online, it obtains the existing configuration from the AC. The AC then manages the AP and delivers service configurations to the AP.



- To simplify the configuration of a large number of APs, you can add them to an AP group and perform centralized configuration.However, APs may have different configurations. These configurations cannot be uniformly performed but can be directly performed on each AP.Each AP must and can only join one AP group when going online. If an AP obtains both AP group and specific configurations from an AC, the AP specific configurations are preferentially used.
- Various profiles can be bound to the AP group and AP: regulatory domain profile, radio profile, VAP profile, Location profile, AP system profile, WIDS profile, AP wired port profile, WDS profile, and Mesh profile. Some of the listed profiles can further reference other profiles.
    - Regulatory domain profile
        - A country code identifies the country to which AP radios belong. Different countries support different AP radio attributes, including the transmit power and supported channels. Correct country code configuration ensures that radio attributes of APs comply with laws and regulations of countries and regions to which the APs are delivered.
        - A calibration channel set limits the dynamic AP channel adjustment range when the radio calibration function is configured. Radar channels and the channels that are not supported by STAs are avoided.

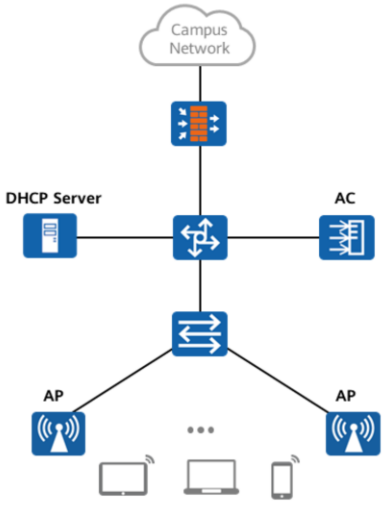
- Radio profile
  - You can adjust and optimize radio parameters to adapt to different network environments, enabling APs to provide required radio capabilities and improving signal quality of WLANs. After parameters in a radio profile are delivered to an AP, only the parameters supported by the AP can take effect.
  - Parameters that can be configured include the radio type, radio rate, multicast rate of radio packets, and interval at which an AP sends Beacon frames.
- VAP profile
  - After parameters in a VAP profile are configured, and the VAP profile is bound to an AP group or AP, virtual access points (VAPs) are created on APs. VAPs provide wireless access services for STAs. You can configure parameters in the VAP profile to enable APs to provide different wireless services.
  - A VAP profile can also reference an SSID profile, a security profile, a traffic profile and etc.
- Configure radio parameters:
  - Configure different radio parameters for AP radios based on actual WLAN environments, so that the AP radios can work at the optimal performance.
  - If working channels of adjacent APs have overlapping frequencies, signal interference occurs and affects AP working status. To prevent signal interference and enable APs to work at the optimal performance with higher WLAN quality, configure any two adjacent APs to work on non-overlapping channels.
  - Configure the transmit power and antenna gain for radios according to actual network environments so that the radios provide sufficient signal strength, improving signal quality of WLANs.
  - In actual application scenarios, two APs may be connected over dozens of meters to dozens of kilometers. Due to different AP distances, the time to wait for ACK packets from the peer AP varies. A proper timeout value can improve data transmission efficiency between APs.



- An SSID profile is used to configure the SSID name and other access parameters of a WLAN. The following parameters are set in an SSID profile:
  - SSID hiding: This functions enables an AP to hide the SSID of a WLAN. Only the users who know the SSID can connect to the WLAN, improving security.
  - Maximum number of STAs on a VAP: More access users on a VAP indicate fewer network resources that are available to each user. To ensure Internet experience of users, you can configure a proper maximum number of access users on a VAP according to actual network situations.
  - SSID hiding when the number of STAs reaches the maximum: When this function is enabled and the number of access users on a WLAN reaches the maximum, the SSID of the WLAN is hidden and new users cannot find the SSID.
- Security profile: You can configure WLAN security policies to authenticate STAs and encrypt user packets, protecting the security of the WLAN and users.
  - The supported WLAN security policies include open system authentication, WEP, WPA/WPA2-PSK, and WPA/WPA2-802.1X. You can configure one of them in a security profile.
- Data forwarding mode:
  - Control packets are forwarded through CAPWAP control tunnels. Data packets are forwarded in tunnel forwarding (centralized forwarding) or direct forwarding (local forwarding) mode. The data forwarding modes will be detailed later in the course.

- Service VLAN:
    - Since WLANs provide flexible access modes, STAs may connect to the same WLAN at the office entrance or stadium entrance, and then roam to different APs.
        - If a single VLAN is configured as the service VLAN, IP address resources may become insufficient in areas where many STAs access the WLAN, and IP addresses in the other areas are wasted.
        - After a VLAN pool is created, add multiple VLANs to the VLAN pool and configure the VLANs as service VLANs. In this way, an SSID can use multiple service VLANs to provide wireless access services. Newly connected STAs are dynamically assigned to VLANs in the VLAN pool, which reduces the number of STAs in each VLAN and also the size of the broadcast domain. Additionally, IP addresses are evenly allocated, preventing IP address waste.

WLAN Working Process: Step 3



WLAN Working Process

① AP onboarding

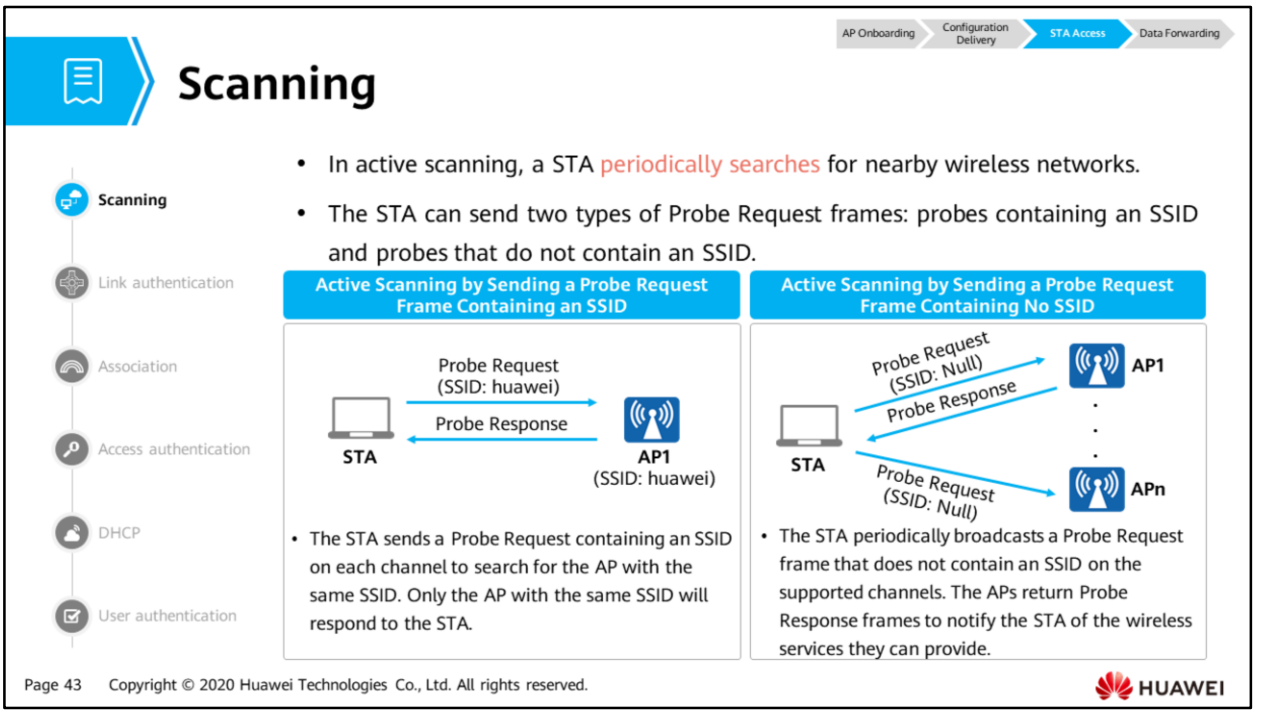
② WLAN service configuration delivery

③ STA access

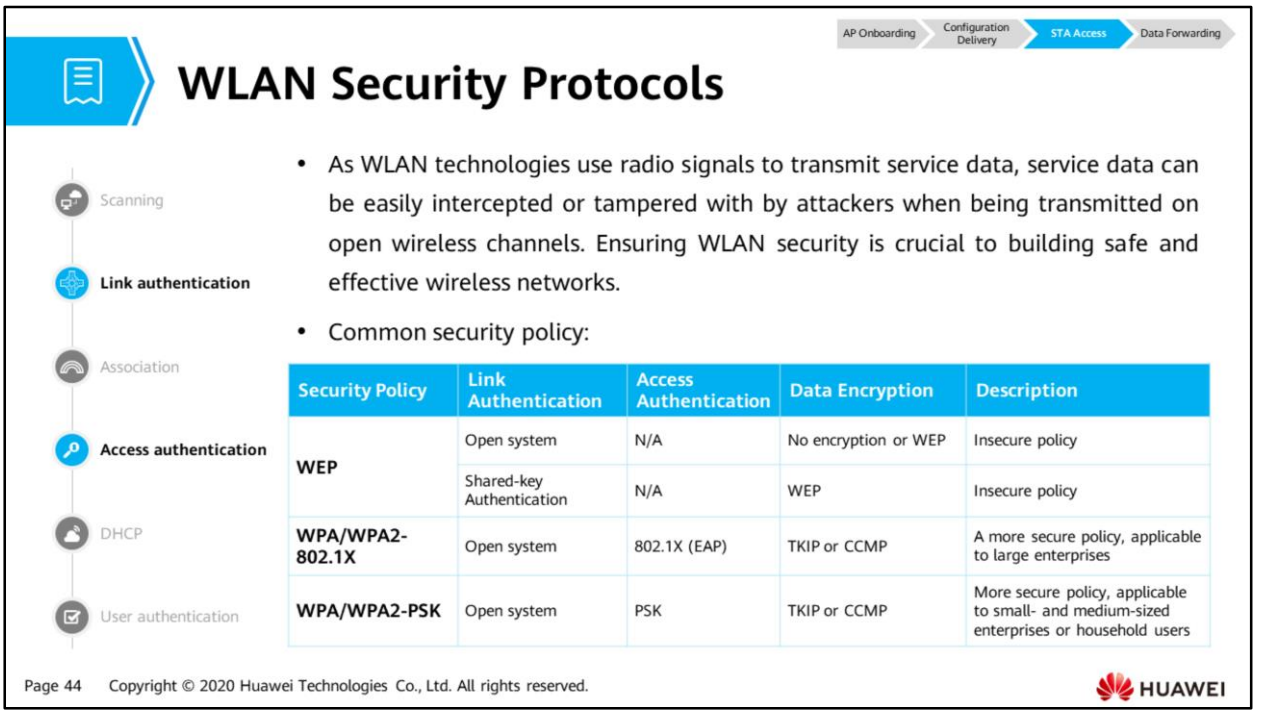
STAs can access a WLAN after CAPWAP tunnels are established.
The STA access process consists of six phases: scanning, link authentication, association, access authentication, DHCP, and user authentication.

④ WLAN service data forwarding

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

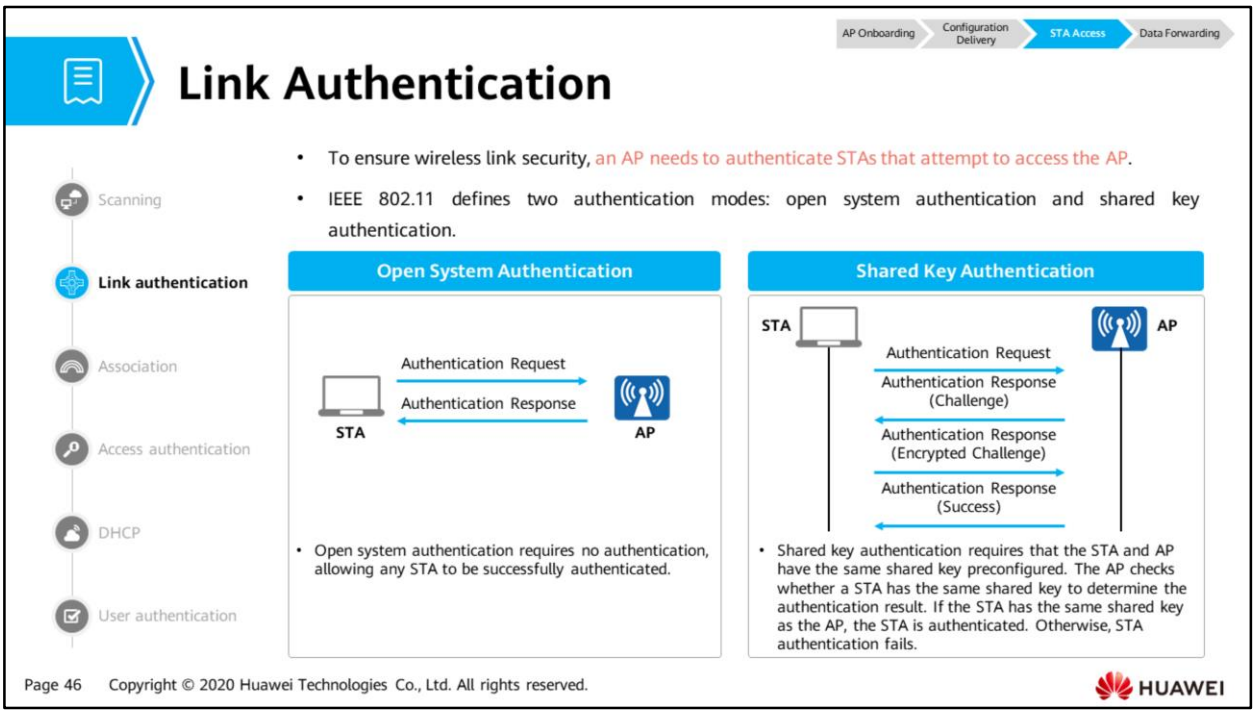


- Active scanning:
  - Probes containing an SSID: applies when a STA actively scans wireless networks to access a specified wireless network.
  - Probes that do not contain an SSID: applies when a STA actively scans wireless networks to determine whether wireless services are available.
- Passive scanning:
  - STAs can passively scan wireless networks.
  - In passive scanning mode, a STA listens to Beacon frames (containing the SSID and supported rate) periodically sent by an AP to discover surrounding wireless networks. By default, an AP sends Beacon frames at an interval of 100 TUs (1 TU = 1024 us).

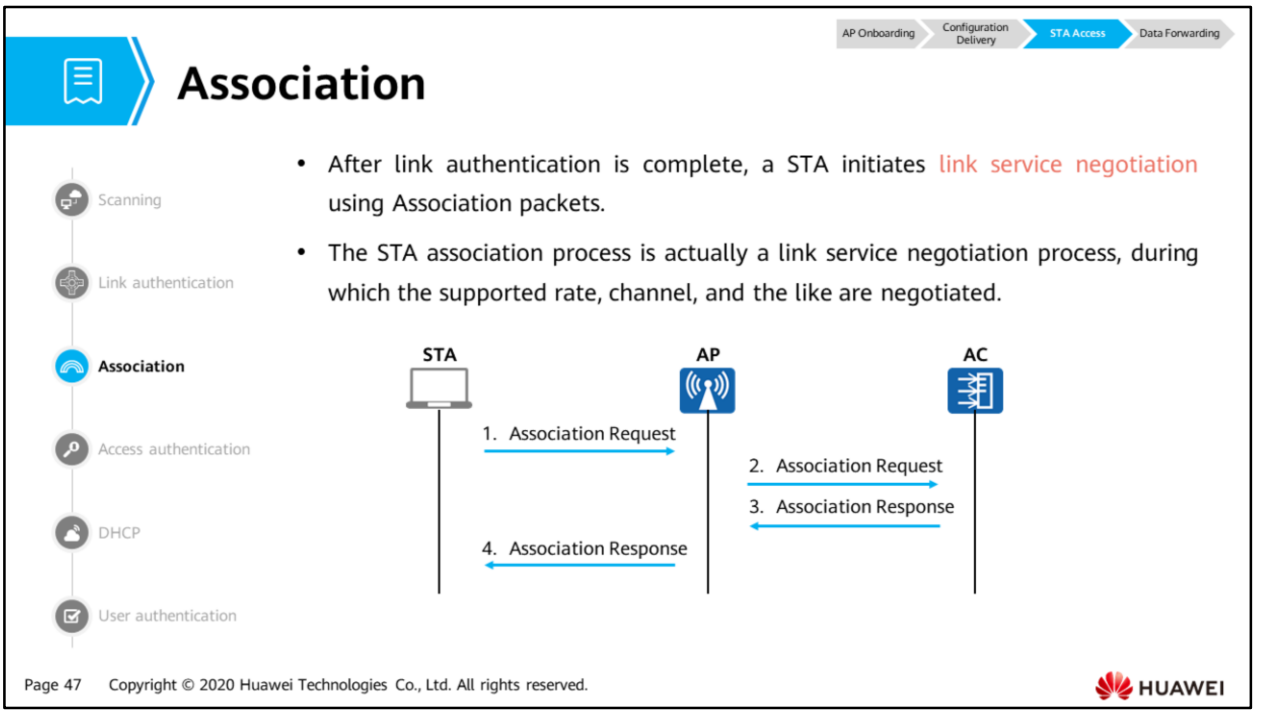


- Three WLAN security policies are available: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2. Each security policy has a series of security mechanisms, including link authentication used to establish a wireless link, user authentication used when users attempt to connect to a wireless network, and data encryption used during data transmission.
- WEP
    - WEP, defined in IEEE 802.11, is used to protect data of authorized users from being intercepted during transmission on a WLAN. WEP uses the RC4 algorithm to encrypt data through a 64-bit, 128-bit, or 152-bit key. Each encryption key contains a 24-bit initialization vector (IV) generated by the system. Therefore, the length of the key configured on the WLAN server and client is 40 bits, 104 bits, or 128 bits. WEP uses a static encryption key. All STAs associating with the same SSID use the same key to connect to the WLAN.

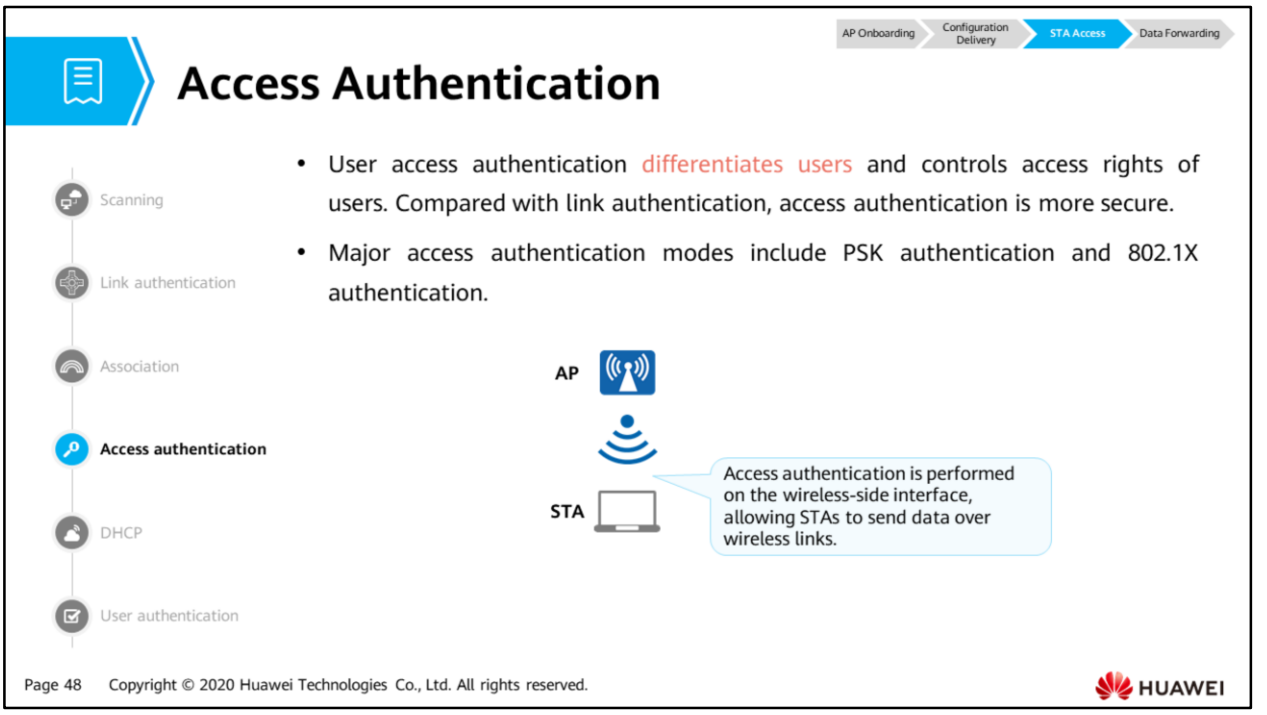
- WPA/WPA2
  - WEP shared key authentication uses the Rivest Cipher 4 (RC4) symmetric stream cipher to encrypt data. Therefore, the same static key must be preconfigured on the server and clients. Both the encryption mechanism and algorithm, however, are prone to security threats. To address this challenge, the Wi-Fi Alliance developed WPA to overcome WEP defects. In addition to the RC4 algorithm, WPA defines the Temporal Key Integrity Protocol (TKIP) encryption algorithm on the basis of WEP, uses the 802.1X identity authentication framework, and supports Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) and EAP-Transport Layer Security (EAP-TLS) authentication. Later, 802.11i defined WPA2. WPA2 uses a more secure encryption algorithm, that is, Counter Mode with CBC-MAC Protocol (CCMP).
  - Both WPA and WPA2 can use 802.1X access authentication and the TKIP or CCMP encryption algorithm, giving better compatibility. WPA and WPA2 provide almost the same security level, with the only difference being the protocol packet format.
  - The WPA/WPA2 security policy involves four phases: link authentication, access authentication, key negotiation, and data encryption.



- A WLAN needs to ensure validity and security of STA access. To achieve this, STAs need to be authenticated before accessing the WLAN. This process is known as link authentication, which is usually considered the beginning of STA access.
- Shared key authentication:
  - The same shared key is configured for STAs and APs in advance. The AP checks whether the STA has the same shared key during link authentication. If so, the STA is successfully authenticated. Otherwise, STA authentication fails.
  - Authentication process:
    1. The STA sends an Authentication Request packet to the AP.
    2. The AP generates a challenge and sends it to the STA.
    3. The STA uses the preconfigured key to encrypt the challenge and sends the encrypted challenge to the AP.
    4. The AP uses the preconfigured key to decrypt the encrypted challenge and compares the decrypted challenge with the challenge sent to the STA. If the two challenges are the same, the STA is successfully authenticated. Otherwise, STA authentication fails.



- STA association in the Fit AP architecture consists of the following steps:
    1. The STA sends an Association Request packet to the AP. The Association Request packet carries the STA's parameters and the parameters selected by the STA according to the service configuration, including the transmission rate, channel, and QoS capabilities.
    2. After receiving the Association Request packet, the AP encapsulates the packet into a CAPWAP packet and sends the CAPWAP packet to the AC.
    3. The AC determines whether to permit the STA access according to the received Association Request packet and replies with a CAPWAP packet containing an Association Response.
    4. The AP decapsulates the CAPWAP packet to obtain the Association Response, and sends the Association Response to the STA.

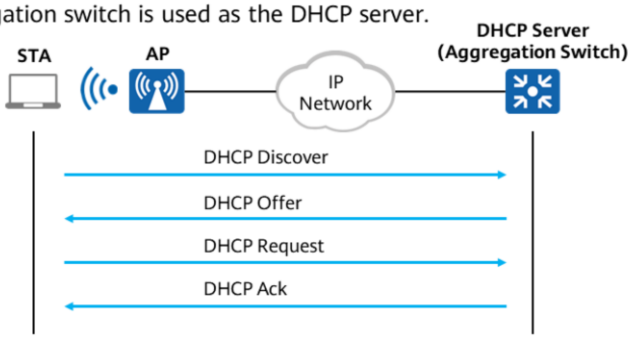


- Data encryption:
  - In addition to user access authentication, data packets need to be encrypted to ensure data security, which is also implemented in the access authentication phase. After a data packet is encrypted, only the device that holds the key can decrypt the packet. Other devices cannot decrypt the packet even if they receive the packet because they do not have the corresponding key.

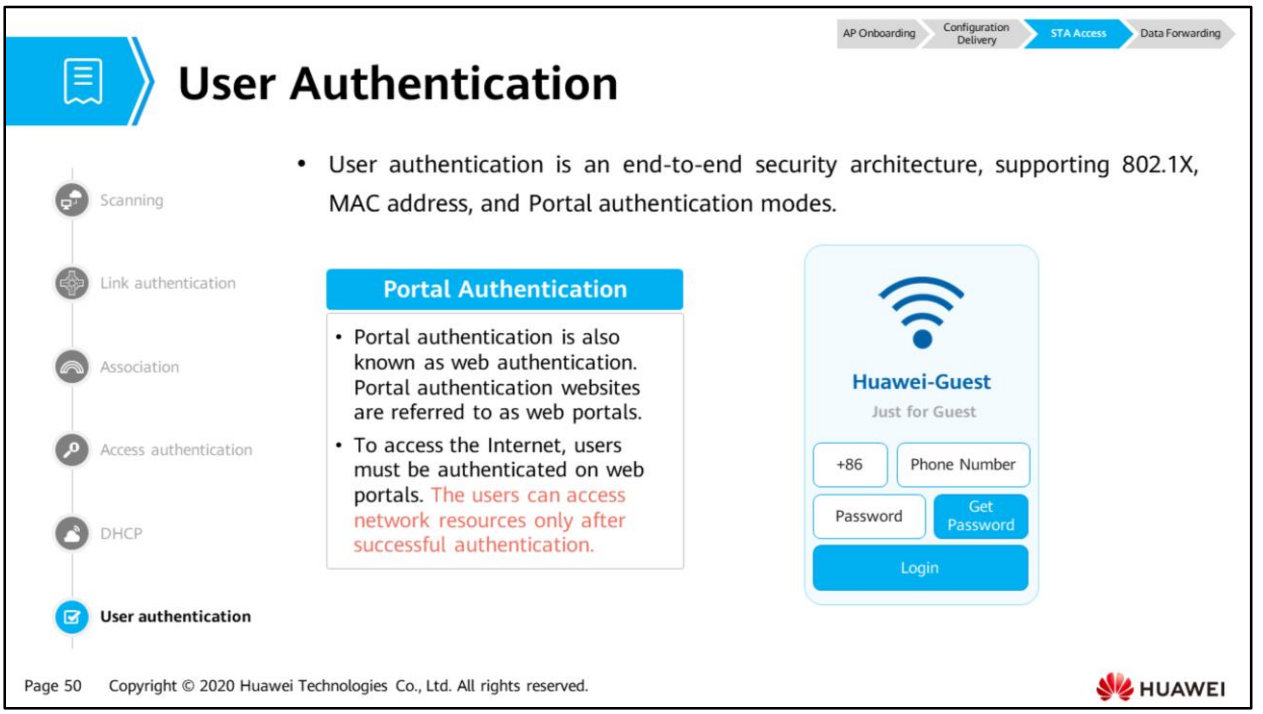
STA Address Allocation

Scanning
Link authentication
Association
Access authentication
DHCP
User authentication

- The prerequisite for APs and STAs to go online properly is that they have obtained IP addresses.
- If STAs obtain IP addresses through DHCP, the AC or aggregation switch can function as a DHCP server to assign IP addresses to the STAs. In most cases, the aggregation switch is used as the DHCP server.

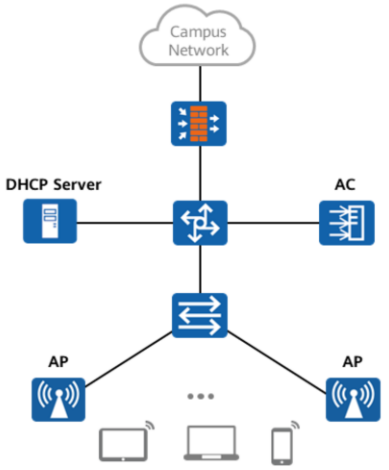


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- With the application and development of enterprise networks, threats increasingly bring risks, such as viruses, Trojan horses, spyware, and malicious network attacks. On a traditional enterprise network, the intranet is considered secure and threats come from the extranet. However, research shows that 80% of cyber security vulnerabilities come from inside the network. The network security threats and viruses affect the network seriously, leading to system or network crashes. In addition, when intranet users browse websites on the external network, the spyware and Trojan horse software may be automatically installed on users' computers, which cannot be sensed by the users. The malicious software may spread on the intranet.
- Therefore, as security challenges keep escalating, traditional security measures are far from enough. The security model needs to be changed from the passive mode to active mode. Thoroughly solving network security problems from the root (terminal) can improve the information security level of the entire enterprise.

WLAN Working Process: Step 4



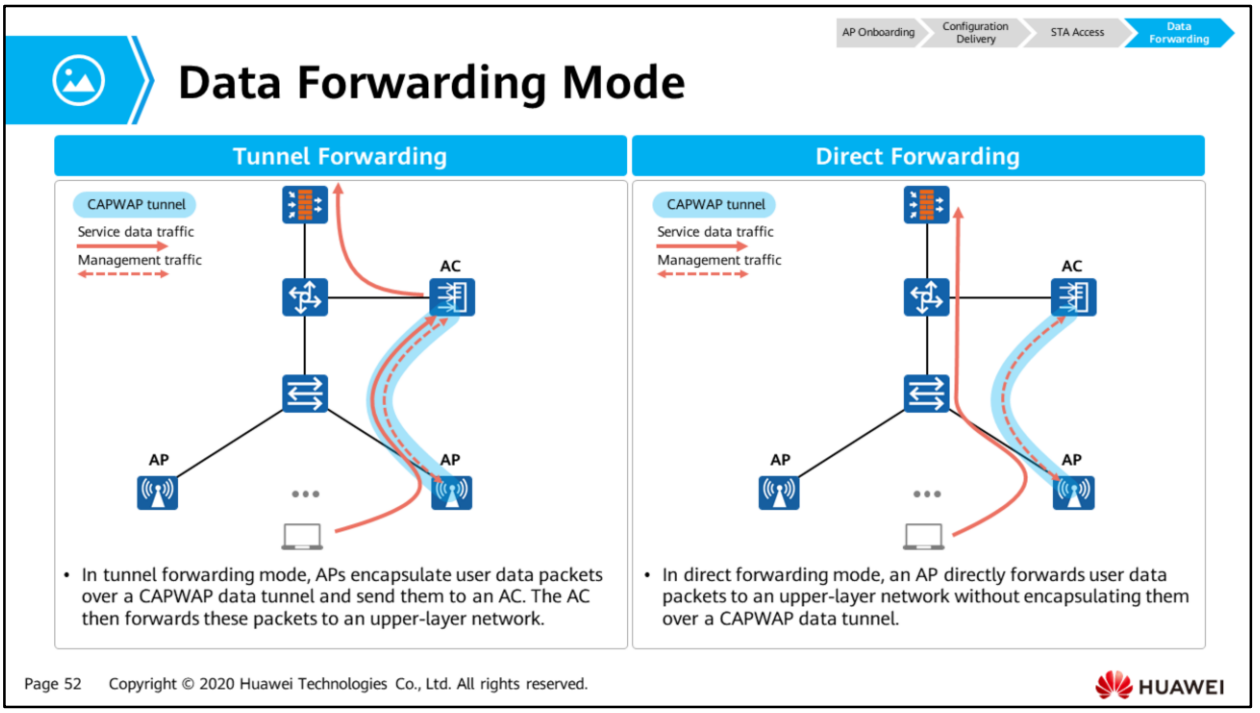
WLAN Working Process

1. AP onboarding
2. WLAN service configuration delivery
3. STA access
4. WLAN service data forwarding

Control packets (management packets) and data packets are transmitted over CAPWAP tunnels.

- Control packets are forwarded through the CAPWAP control tunnel.
- User data packets can be forwarded in tunnel forwarding (centralized forwarding) or direct forwarding (local forwarding) mode.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



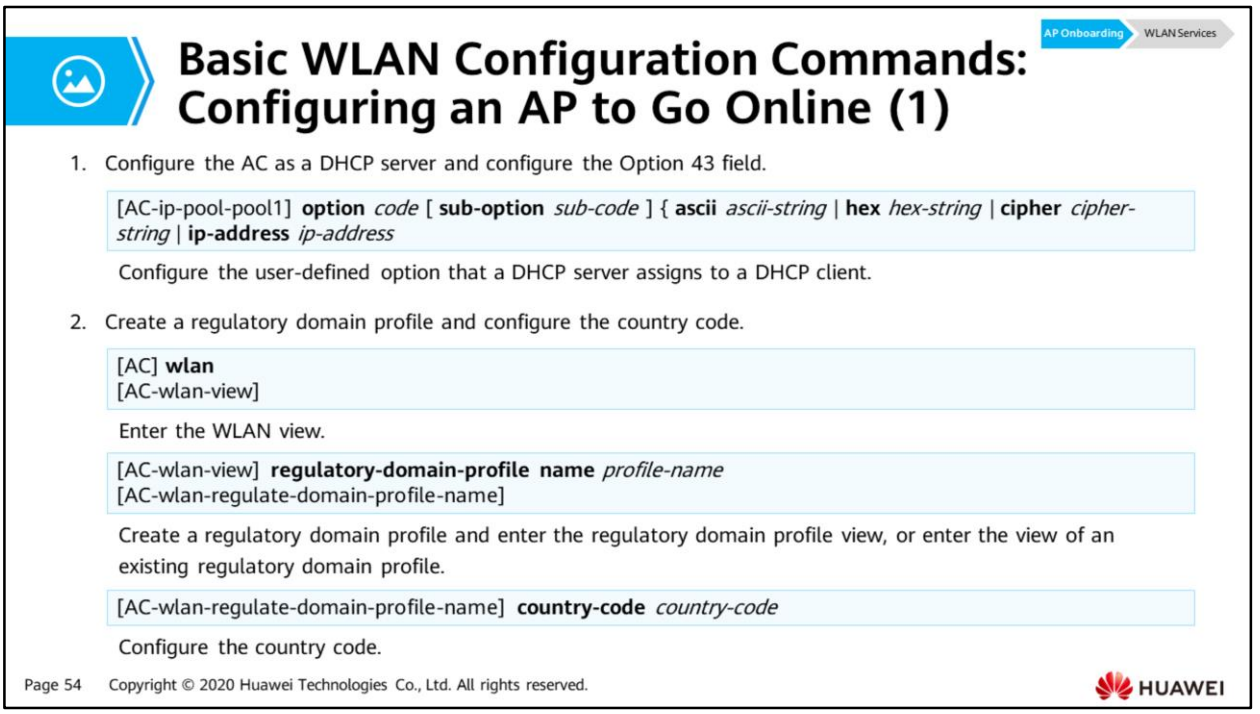
- Tunnel forwarding mode:
  - Advantages: An AC forwards all data packets, ensuring security and facilitating centralized management and control.
  - Disadvantages: Service data must be forwarded by an AC, which is inefficient and increases the load on the AC.
- Direct forwarding mode:
  - Advantages: Service data packets do not need to be forwarded by an AC, improving packet forwarding efficiency and reducing the burden on the AC.
  - Disadvantages: Service data is difficult to manage and control in a centralized manner.

Contents

1. WLAN Overview
2. Basic Concepts of WLAN
3. WLAN Fundamentals
4. **WLAN Configuration Implementation**
5. Next-Generation WLAN Solutions

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI



- Command: **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* }
  - *code*: specifies the code of a user-defined option. The value is an integer that ranges from 1 to 254, except values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 121 and 184.
  - **sub-option** *sub-code*: specifies the code of a user-defined sub-option. The value is an integer ranging from 1 to 254. For details about well-known options, see RFC 2132.
  - **ascii** | **hex** | **cipher**: specifies the user-defined option code as an ASCII character string, hexadecimal character string, or ciphertext character string.
  - **ip-address** *ip-address*: specifies the user-defined option code as an IP address.
- Command: **regulatory-domain-profile name** *profile-name*
  - **name** *profile-name*: specifies the name of a regulatory domain profile. The value is a string of 1 to 35 case-insensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").

- Command: **country-code** *country-code*
  - *country-code*: specifies a country code. The value is a string of characters in enumerated type.
  - The AC supports multiple country codes, such as:
    - CN (default value): China
    - AU: Australia
    - CA: Canada
    - DE: Germany
    - FR: France
    - US: United States
    - ...

Basic WLAN Configuration Commands: Configuring an AP to Go Online (2)

[AC-wlan-view] **ap-group name** *group-name*
[AC-wlan-ap-group-group-name]

Create an AP group and enter the AP group view, or enter the view of an existing AP group.

[AC-wlan-ap-group-group-name] **regulatory-domain-profile** *profile-name*

Bind the regulatory domain profile to an AP or AP group.

3. Configure a source interface or address.

[AC] **capwap source interface** { **loopback** *loopback-number* | **vlanif** *vlan-id* }

Specify a source interface on the AC for establishing CAPWAP tunnels with APs.

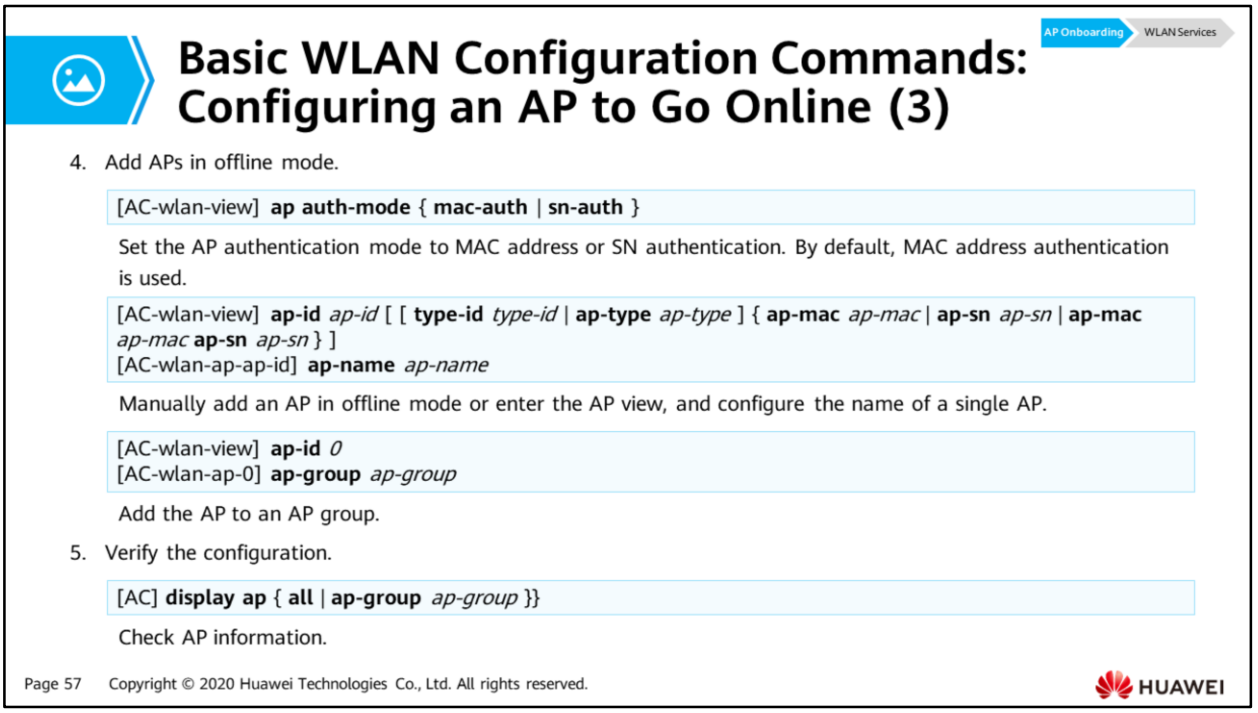
[AC] **capwap source ip-address** *ip-address*

Configure the source IP address on the AC.

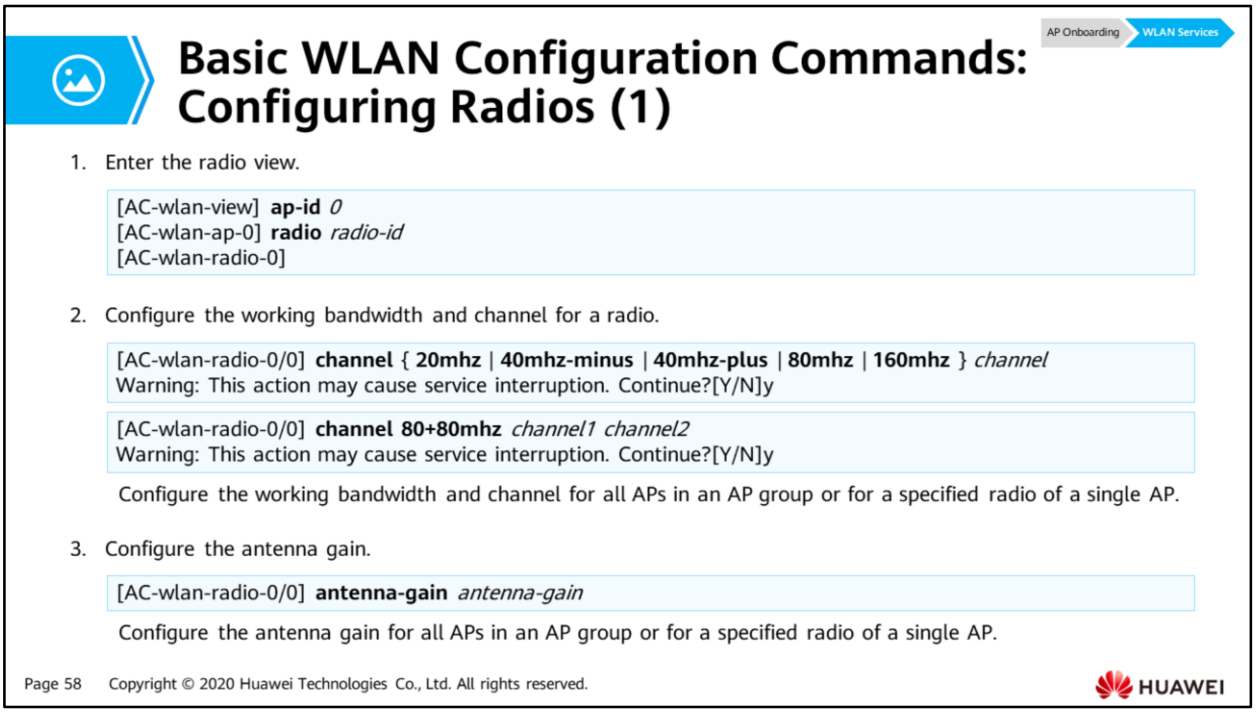
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

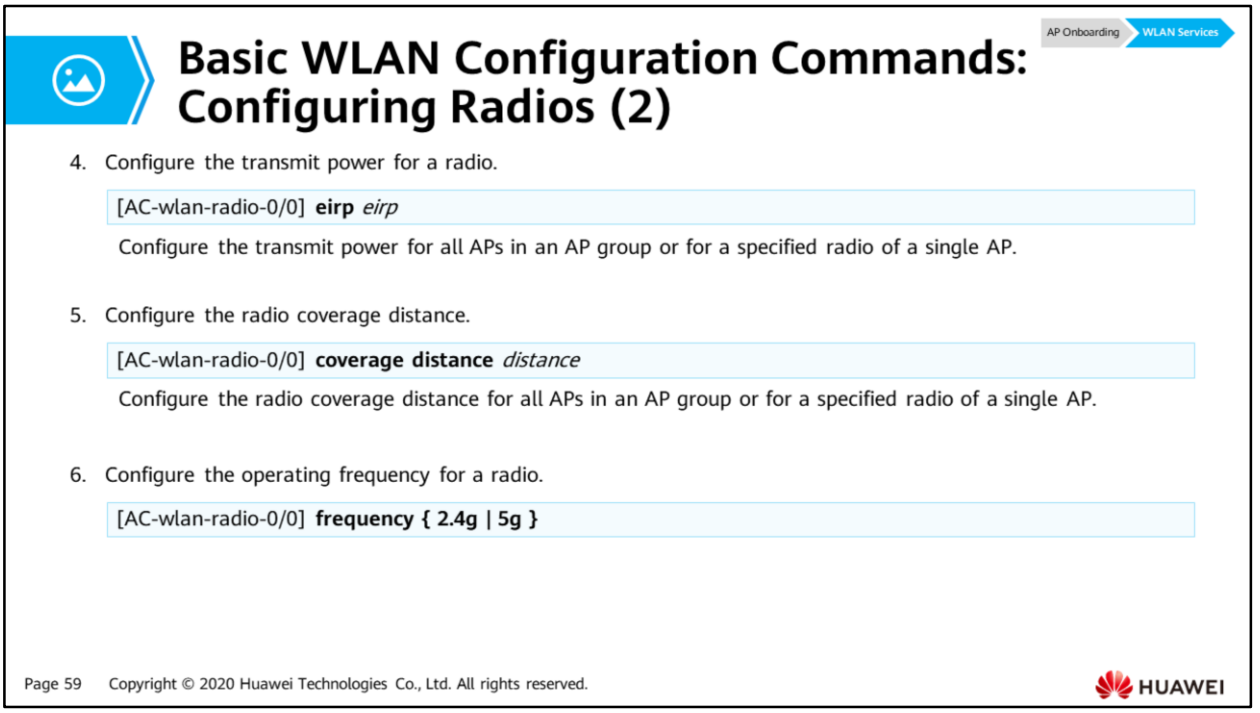
- Command: **ap-group name** *group-name*
  - **name** *group-name*: specifies the name of an AP group. The value is a string of 1 to 35 characters. It cannot contain question marks (?), slashes (/), or spaces, and cannot start or end with double quotation marks (").



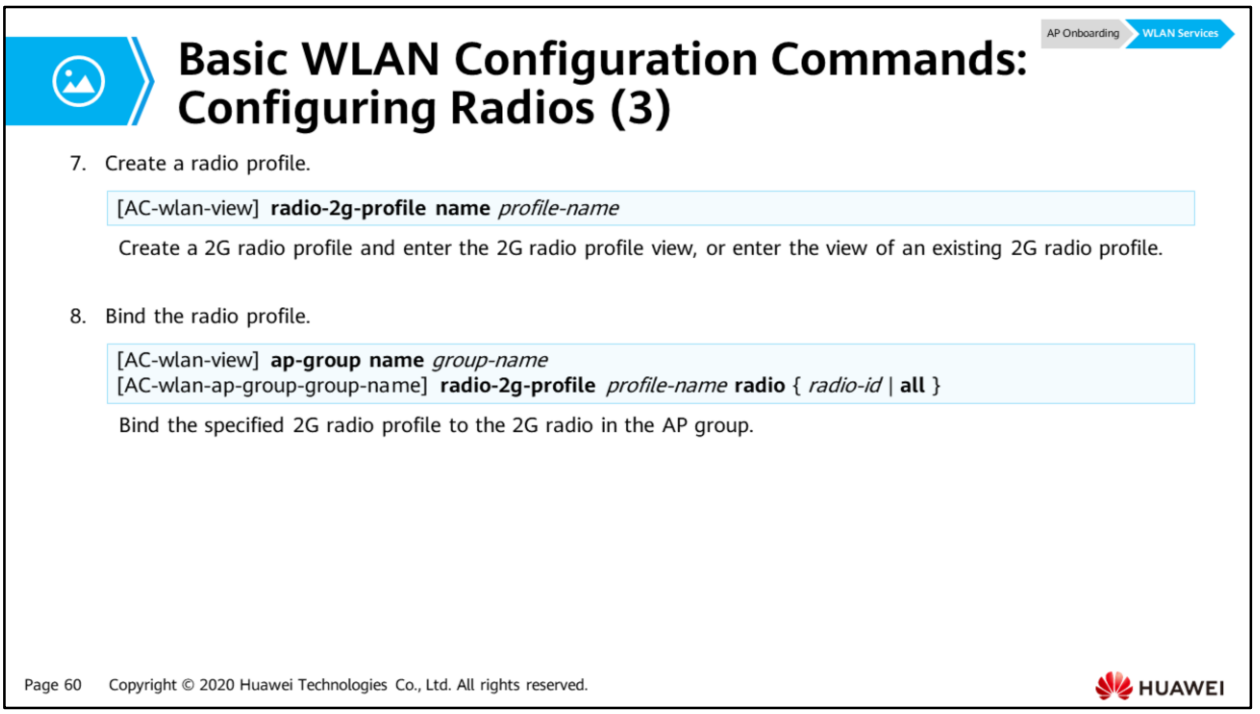
- Command: **ap-id** *ap-id* [**[type-id** *type-id* | **ap-type** *ap-type*] { **ap-mac** *ap-mac* | **ap-sn** *ap-sn* | **ap-mac** *ap-mac* **ap-sn** *ap-sn* }]
  - *ap-id*: specifies the ID of an AP. The value is an integer that ranges from 0 to 8191.
  - *type-id:* specifies the ID of an AP type. The value is an integer that ranges from 0 to 255.
  - *ap-type*: specifies the type of an AP. The value is a string of 1 to 31 characters.
  - *ap-mac:* specifies the MAC address of an AP. The value is in H-H-H format. An H is a 4-digit hexadecimal number.
  - *ap-sn:* specifies the SN of an AP. The value is a string of 1 to 31 characters, and can contain only letters and digits.



- Command: **radio** *radio-id*
  - *radio-id*: specifies the ID of a radio. The radio ID must exist.
- Commands:
  - **channel { 20mhz | 40mhz-minus | 40mhz-plus | 80mhz | 160mhz }** *channel*
  - **channel 80+80mhz** *channel1 channel2*
  - **20mhz**: sets the working bandwidth of a radio to 20 MHz.
  - **40mhz-minus:** sets the working bandwidth of a radio to 40 MHz Minus.
  - **40mhz-plus:** sets the working bandwidth of a radio to 40 MHz Plus.
  - **80mhz:** sets the working bandwidth of a radio to 80 MHz.
  - **160mhz:** sets the working bandwidth of a radio to 160 MHz.
  - **80+80mhz:** sets the working bandwidth of a radio to 80+80 MHz.
  - *channel/channel1/channel2:* specifies the working channel for a radio. The channel is selected based on the country code and radio mode. The parameter is an enumeration value. The value range is determined according to the country code and radio mode.
- Command: **antenna-gain** *antenna-gain*
  - *antenna-gain:* specifies the antenna gain. The value is an integer that ranges from 0 to 30, in dB.



- Command: **eirp** *eirp*
  - *eirp*: specifies the transmit power. The value is an integer that ranges from 1 to 127, in dBm.
- Command: **coverage distance** *distance*
  - *distance*: specifies the radio coverage distance. Each distance corresponds to a group of slottime, acktimeout, and ctstimeout values. You can configure the radio coverage distance based on the AP distance, so that APs adjust the values of slottime, acktimeout, and ctstimeout values accordingly. The value is an integer that ranges from 1 to 400, in 100 meters.
- Command: **frequency { 2.4g | 5g }**
  - By default, radio 0 works on the 2.4 GHz frequency band, and radio 2 works on the 5 GHz frequency band.



- Command: **radio-2g-profile name** *profile-name*
  - **name** *profile-name*: specifies the name of a 2G radio profile. The value is a string of 1 to 35 case-insensitive characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (").
  - By default, the system provides the 2G radio profile default.
- Command: **radio-2g-profile** *profile-name* **radio** { *radio-id* | **all** }
  - *profile-name*: specifies the name of a 2G radio profile. The 2G radio profile must exist.
  - **radio** *radio-id*: specifies the ID of a radio. The value is an integer that can be 0 or 2.
  - **radio all**: specifies all radios.

Basic WLAN Configuration Commands: Configuring VAPs (1)

1. Create a VAP profile.

```
[AC-wlan-view] vap-profile name profile-name
[AC-wlan-vap-prof-profile-name]
```

Create a VAP profile and enter the VAP profile view, or enter the view of an existing VAP profile.

2. Configure the data forwarding mode.

```
[AC-wlan-vap-prof-profile-name] forward-mode { direct-forward | tunnel }
```

Set the data forwarding mode in the VAP profile to direct or tunnel.

3. Configure service VLANs.

```
[AC-wlan-vap-prof-profile-name] service-vlan { vlan-id vlan-id | vlan-pool pool-name }
```

Configure service VLANs configured for the VAP.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic WLAN Configuration Commands: Configuring VAPs (2)

4. Configure a security profile.

```
[AC-wlan-view] security-profile name profile-name
[AC-wlan-sec-prof-profile-name]
```

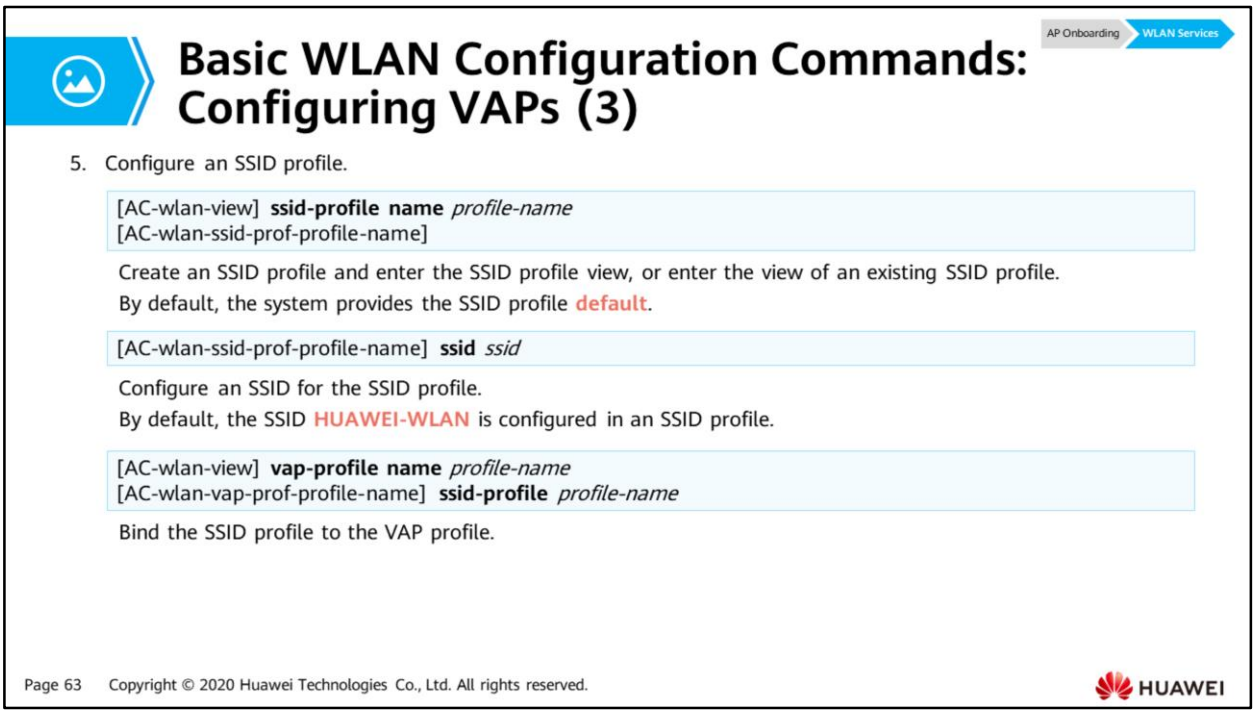
Create a security profile and enter the security profile view.

By default, security profiles **default, default-wds**, and **default-mesh** are available in the system.

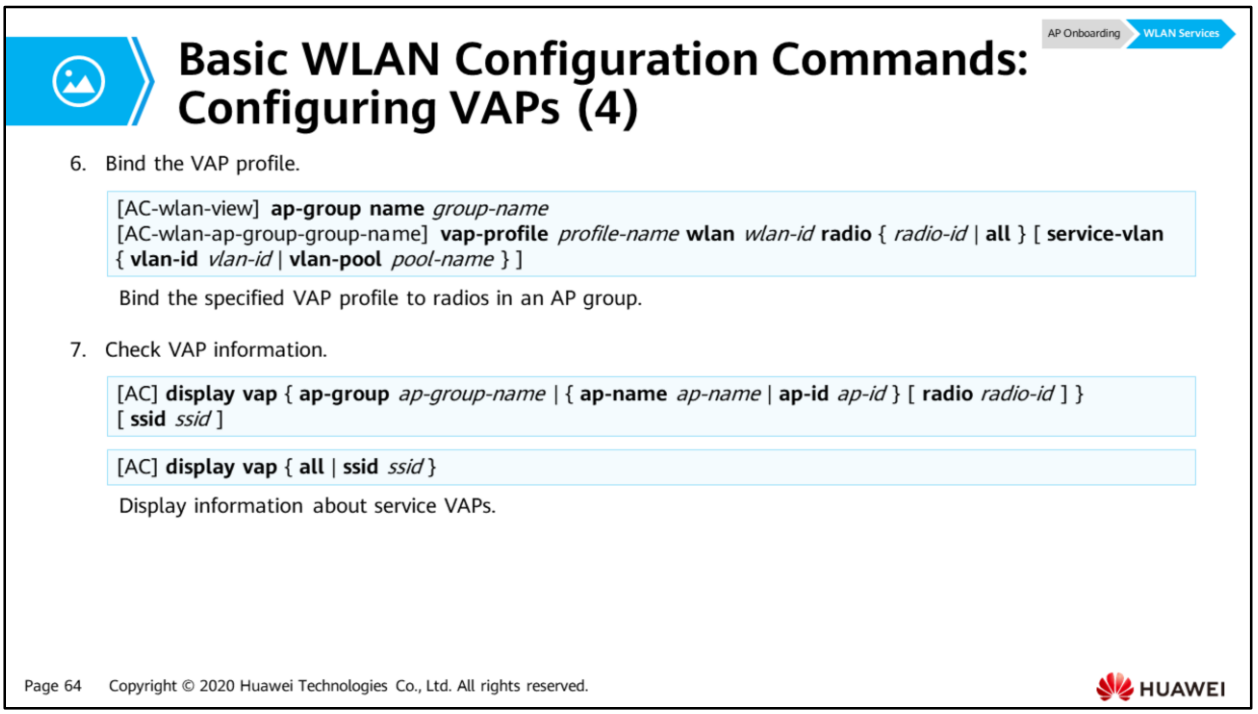
```
[AC-wlan-view] vap-profile name profile-name
[AC-wlan-vap-prof-profile-name] security-profile profile-name
```

Bind the security profile to the VAP profile.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

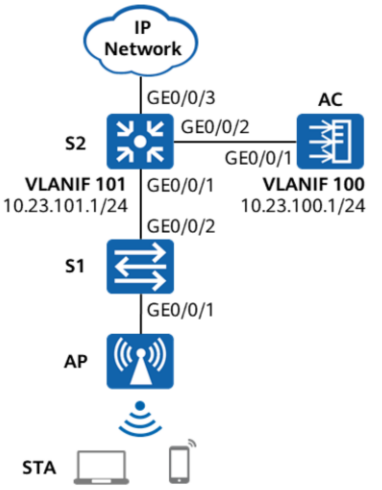


- Command: **ssid** *ssid*
  - *ssid*: specifies an SSID. The value is a string of 1 to 32 case-sensitive characters. It supports Chinese characters or Chinese + English characters, without tab characters.
  - To start an SSID with a space, you need to encompass the SSID with double quotation marks ("), for example, " hello". The double quotation marks occupy two characters. To start an SSID with a double quotation mark, you need to add a backslash (\) before the double quotation mark, for example, \"hello. The backslash occupies one character.



- Command: **display vap** { **ap-group** *ap-group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] } [**ssid** *ssid*]
  - *ap-group-name*: displays information about all service VAPs in a specified AP group. The AP group must exist.
  - *ap-name*: displays information about service VAPs on the AP with a specified name. The AP name must exist.
  - *ap-id*: displays information about service VAPs on the AP with a specified ID. The AP ID must exist.
  - *radio-id*: Displays information about service VAPs of a specified radio. The value is an integer that ranges from 0 to 2.
  - *ssid*: Displays information about service VAPs of a specified SSID. The SSID must exist.
- Command: **display vap** { **all** | **ssid** *ssid* }
  - **all:** displays information about all service VAPs.

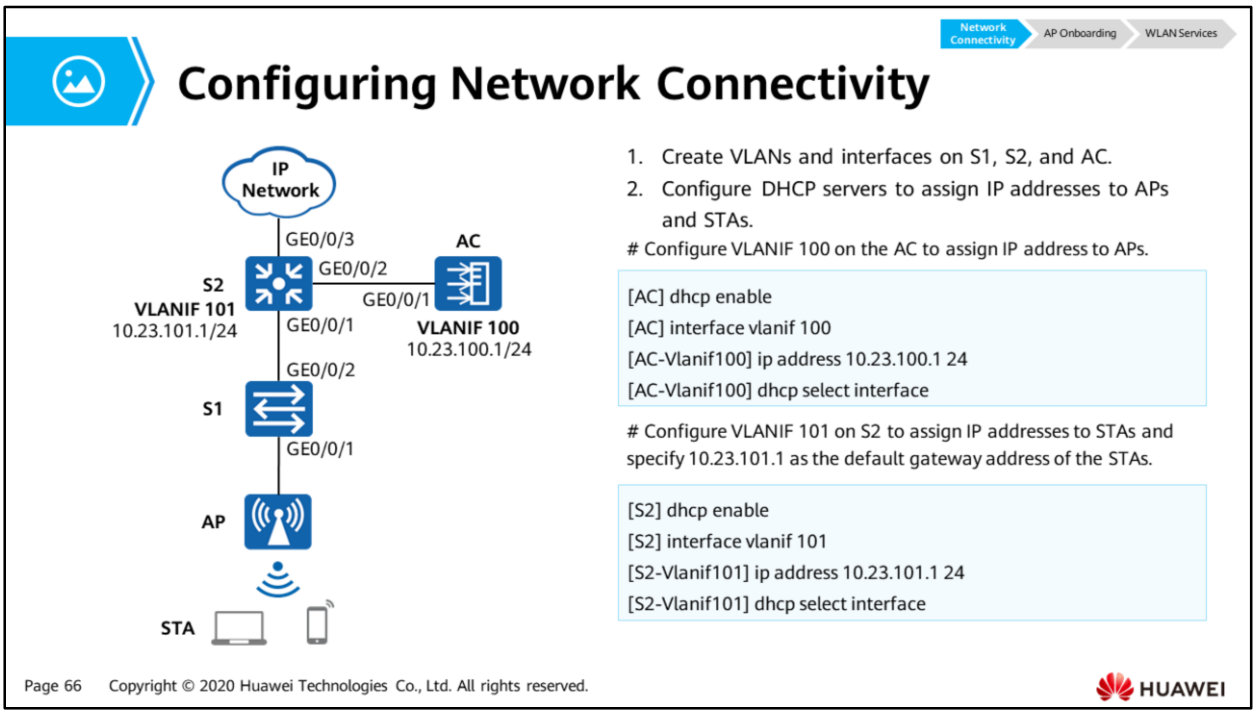
Example for Configuring Layer 2 Tunnel Forwarding in Off-Path Mode



Data	Configuration
Management VLAN for APs	VLAN 100
Service VLAN for STAs	VLAN 101
DHCP server	The AC functions as a DHCP server to assign IP addresses to APs. The aggregation switch S2 functions as a DHCP server to assign IP addresses to STAs. The default gateway address of STAs is 10.23.101.1.
IP address pool for APs	10.23.100.2–10.23.100.254/24
IP address pool for STAs	10.23.101.2–10.23.101.254/24
IP address of the AC's source interface	VLANIF 100: 10.23.100.1/24
AP group	Name: ap-group1 Referenced profiles: VAP profile **wlan-net** and regulatory domain profile
Regulatory domain profile	Name: default Country code: CN
SSID profile	Name: wlan-net SSID name: wlan-net
Security profile	Name: wlan-net Security policy: WPA-WPA2+PSK+AES Password: a1234567
VAP profile	Name: wlan-net Forwarding mode: tunnel forwarding Service VLAN: VLAN 101 Referenced profiles: SSID profile **wlan-net** and security profile **wlan-net**

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Service requirements
  - An enterprise wants to enable users to access the Internet through a WLAN, meeting the basic mobile office requirements.
- Networking requirements
  - AC networking mode: Layer 2 networking in off-path mode
  - DHCP deployment mode:
    - The AC functions as a DHCP server to assign IP addresses to APs.
    - The aggregation switch S2 functions as a DHCP server to assign IP addresses to STAs.
  - Service data forwarding mode: tunnel forwarding
- Configuration roadmap
  - Configure network connectivity between the AC, APs, and other network devices.
  - Configure the APs to go online.
    - Create an AP group and add APs that require the same configuration to the group for unified configuration.
    - Configure AC system parameters, including the country code and source interface used by the AC to communicate with the APs.
    - Configure the AP authentication mode and imports the APs in offline mode for them to go online.
  - Configure WLAN service parameters for STAs to access the WLAN.



- 1. Create VLANs and interfaces on S1, S2, and AC.
  - S1 configuration:

    [S1] vlan batch 100

    [S1] interface gigabitethernet 0/0/1

    [S1-GigabitEthernet0/0/1] port link-type trunk

    [S1-GigabitEthernet0/0/1] port trunk pvid vlan 100

    [S1-GigabitEthernet0/0/1] port trunk allow-pass vlan 100

    [S1-GigabitEthernet0/0/1] quit

    [S1] interface gigabitethernet 0/0/2

    [S1-GigabitEthernet0/0/2] port link-type trunk

    [S1-GigabitEthernet0/0/2] port trunk allow-pass vlan 100

    [S1-GigabitEthernet0/0/2] quit

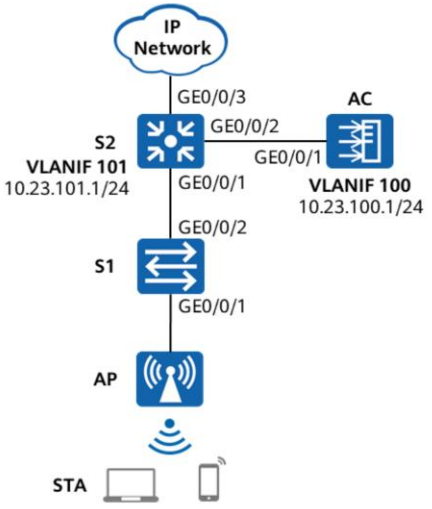
- S2 configuration:

  ```
  [S2] vlan batch 100 101
  [S2] interface gigabitethernet 0/0/1
  [S2-GigabitEthernet0/0/1] port link-type trunk
  [S2-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
  [S2-GigabitEthernet0/0/1] quit
  [S2] interface gigabitethernet 0/0/2
  [S2-GigabitEthernet0/0/2] port link-type trunk
  [S2-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 101
  [S2-GigabitEthernet0/0/2] quit
  [S2] interface gigabitethernet 0/0/3
  [S2-GigabitEthernet0/0/3] port link-type trunk
  [S2-GigabitEthernet0/0/3] port trunk allow-pass vlan 101
  [S2-GigabitEthernet0/0/3] quit
  ```

- AC configuration:

  ```
  [AC] vlan batch 100 101
  [AC] interface gigabitethernet 0/0/1
  [AC-GigabitEthernet0/0/1] port link-type trunk
  [AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 101
  [AC-GigabitEthernet0/0/1] quit
  ```

Configuring APs to Go Online (1)



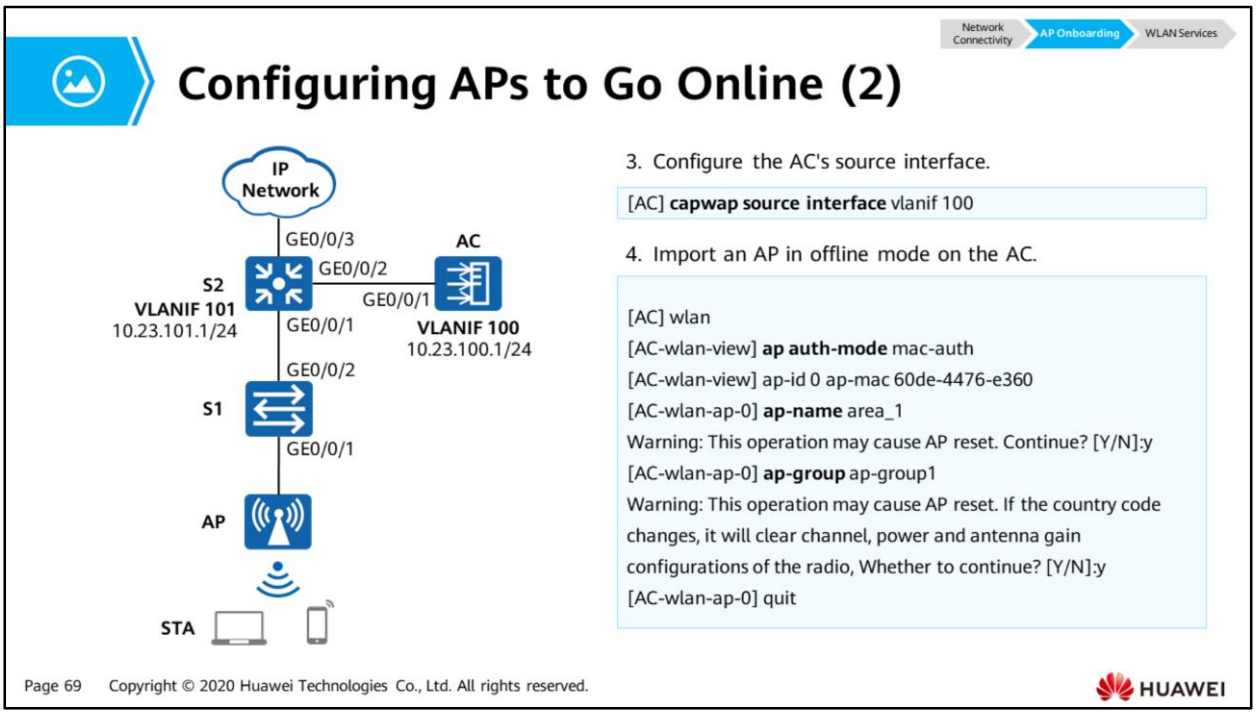
1. Create an AP group.

```
[AC] wlan
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] quit
```

2. Create a regulatory domain profile and configure the country code.

```
AC-wlan-view] regulatory-domain-profile name default
[AC-wlan-regulate-domain-default] country-code cn
[AC-wlan-regulate-domain-default] quit
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and
antenna gain configurations of the radio and reset the AP. Continu
e?[Y/N]:y
[AC-wlan-ap-group-ap-group1] quit
[AC-wlan-view] quit
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Import an AP in offline mode on the AC.
  - Add the AP to the AP group **ap-group1**. Assume that an AP's MAC address is 60de-4476-e360. Configure a name for the AP based on the AP's deployment location, so that you can know where the AP is deployed from its name. For example, name the AP **area_1** if it is deployed in area 1.

Verifying the AP Onboarding Configuration

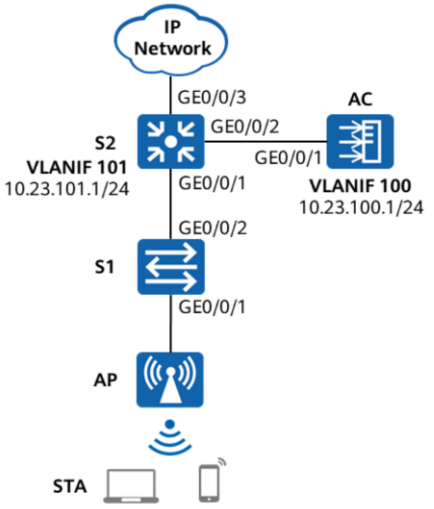
- After the AP is powered on, run the **display ap all** command to check the AP state. If the **State** field displays **nor**, the AP has gone online.

```
[AC-wlan-view] display ap all
Total AP information:
nor  : normal          [1]
Extra information:
P  : insufficient power supply
--------------------------------------------------------------------------------
ID  MAC             Name      Group      IP             Type        State STA Uptime    ExtraInfo
--------------------------------------------------------------------------------
0   60de-4476-e360  area_1    ap-group1  10.23.100.254  AP5030DN    nor   0   10S       -
--------------------------------------------------------------------------------
Total: 1
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Description of the **display ap** command output:
  - ID: AP ID.
  - MAC: AP MAC address.
  - Name: AP name.
  - Group: Name of the AP group to which an AP belongs.
  - IP: IP address of an AP. In NAT scenarios, APs are on the private network and the AC on the public network. This value is an AP's private IP address. To check the public IP address of an AP, run the **display ap run-info** command.
  - Type: AP type.
  - State: AP state.
    - normal: An AP has gone online on an AC and is working properly.
    - commit-failed: WLAN service configurations fail to be delivered to an AP after it goes online on an AC.
    - download: An AP is in upgrade state.
    - fault: An AP fails to go online.
    - idle: It is the initialization state of an AP before it establishes a link with the AC for the first time.
  - STA: Number of STAs connected to an AP.
  - Uptime: Online duration of an AP.
  - ExtraInfo: Extra information. The value P indicates an AP has no sufficient power supply.

Configuring WLAN Service Parameters (1)



1. Create security profile **wlan-net** and configure a security policy.

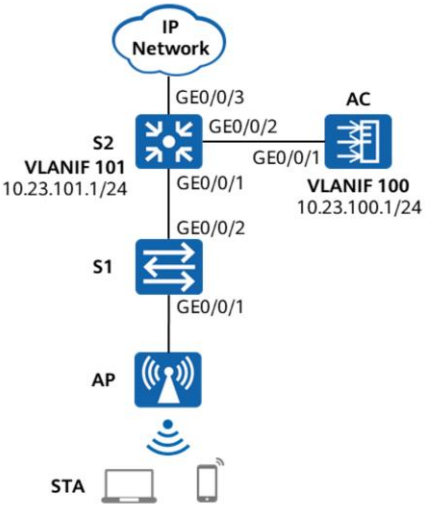
```
[AC-wlan-view] security-profile name wlan-net
[AC-wlan-sec-prof-wlan-net] security wpa-wpa2 psk pass-phrase a1234567 aes
[AC-wlan-sec-prof-wlan-net] quit
```

2. Create SSID profile **wlan-net** and set the SSID name to **wlan-net**.

```
[AC-wlan-view] ssid-profile name wlan-net
[AC-wlan-ssid-prof-wlan-net] ssid wlan-net
[AC-wlan-ssid-prof-wlan-net] quit
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuring WLAN Service Parameters (2)



3. Create VAP profile **wlan-net**, set the data forwarding mode and service VLAN, and bind the security profile and SSID profile to the VAP profile.

```
[AC-wlan-view] vap-profile name wlan-net
[AC-wlan-vap-prof-wlan-net] forward-mode tunnel
[AC-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
[AC-wlan-vap-prof-wlan-net] security-profile wlan-net
[AC-wlan-vap-prof-wlan-net] ssid-profile wlan-net
[AC-wlan-vap-prof-wlan-net] quit
```

4. Bind the VAP profile to the AP group and apply configurations in VAP profile **wlan-net** to radio 0 and radio 1 of the APs in the AP group.

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[AC-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[AC-wlan-ap-group-ap-group1] quit
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Checking VAP Profile Information

- The AC automatically delivers WLAN service configuration to the AP. After the service configuration is complete, run the **display vap ssid wlan-net** command. If **Status** in the command output is displayed as **ON**, the VAPs have been successfully created on AP radios.

```
[AC-wlan-view] display vap ssid wlan-net
WID : WLAN ID
------------------------------------------------------------------------------------------------------
AP ID     AP name   RfID WID  BSSID           Status Auth type        STA  SSID
------------------------------------------------------------------------------------------------------
0         area_1    0    1    60DE-4476-E360  ON     WPA/WPA2-PSK     0    wlan-net
0         area_1    1    1    60DE-4476-E370  ON     WPA/WPA2-PSK     0    wlan-net
------------------------------------------------------------------------------------------------------
Total: 2
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Description of the **display vap** command output:
  - AP ID: AP ID.
  - AP name: AP name.
  - RfID: Radio ID.
  - WID: VAP ID.
  - SSID: SSID name.
  - BSSID: MAC address of a VAP.
  - Status: Current status of a VAP.
    - ON: The VAP service is enabled.
    - OFF: The VAP service is disabled.
  - Auth type: VAP authentication mode.
  - STA: Number of STAs connected to a VAP.

Contents

1. WLAN Overview
2. Basic Concepts of WLAN
3. WLAN Fundamentals
4. WLAN Configuration Implementation
5. **Next-Generation WLAN Solutions**

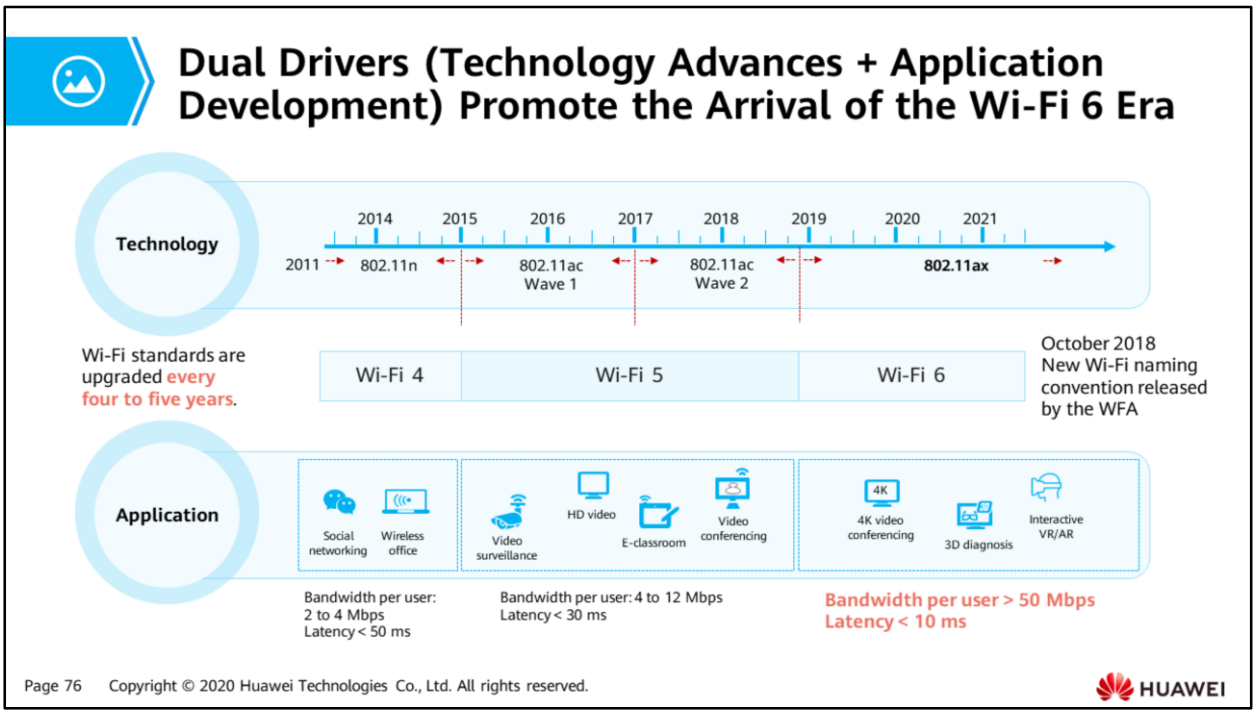
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

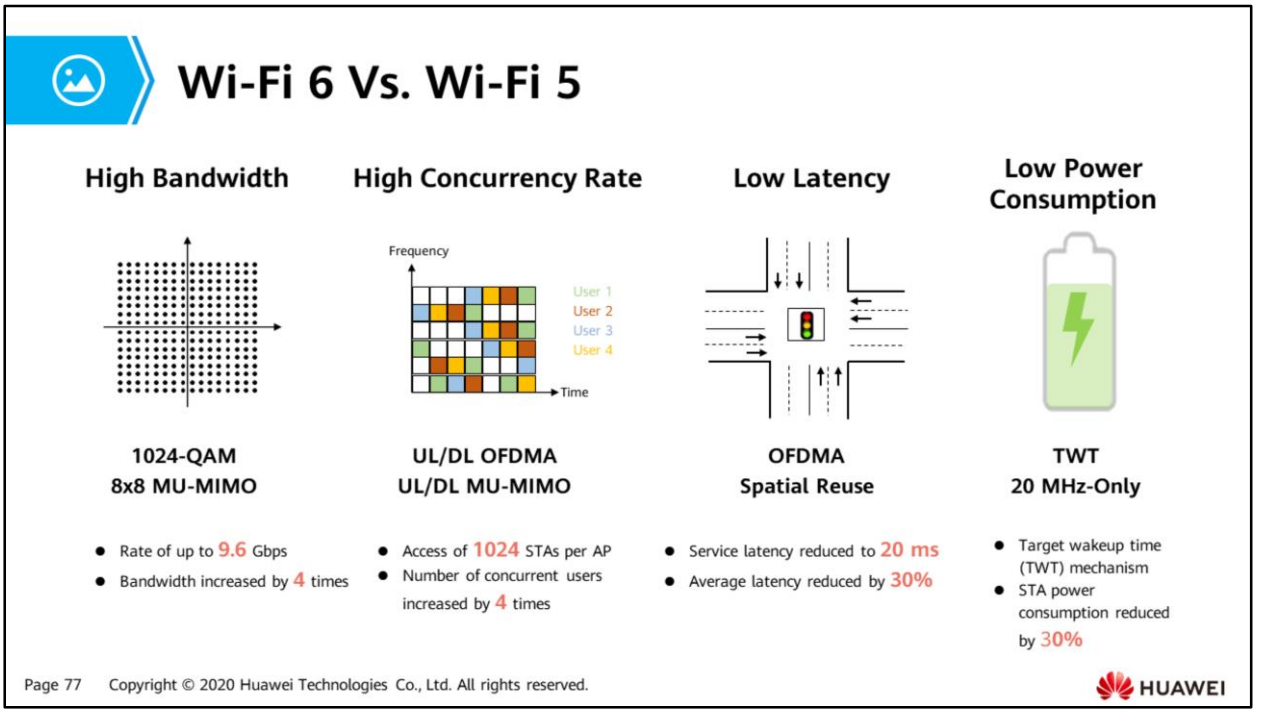
Huawei WLAN Solutions Meet Future Wireless Network Construction Requirements

All-scenario	• Use scenario-based customized solutions for complex and diversified application scenarios • Complete WLAN deployment and management solutions for campus networks and branch networks
High bandwidth	• 802.11ac Wave 2 protocol, dual-5G radio coverage, and up to 3.46 Gbps wireless access bandwidth • Huawei is a key contributor to the next-generation 802.11ax standard (Wi-Fi 6) with a single 5 GHz radio rate of up to 9.6 Gbps. • Roaming and multiple wireless QoS protocols such as Wi-Fi multimedia (WMM) to ensure QoS
High security	• Mainstream authentication and encryption modes, such as WPA, WPA2, WPA3, and WAPI • Wireless intrusion detection • Portal and 802.1X authentication, protecting intranet security
Easy deployment	• APs support plug-and-play, automatic upgrade, automatic channel selection, dynamic rate and power adjustment, and load balancing. • IoT APs and APs with built-in high-density antennas, simplifying installation and enabling fast deployment • APs support cloud management and can work in dual-stack mode to smoothly switch between the cloud and local management modes.

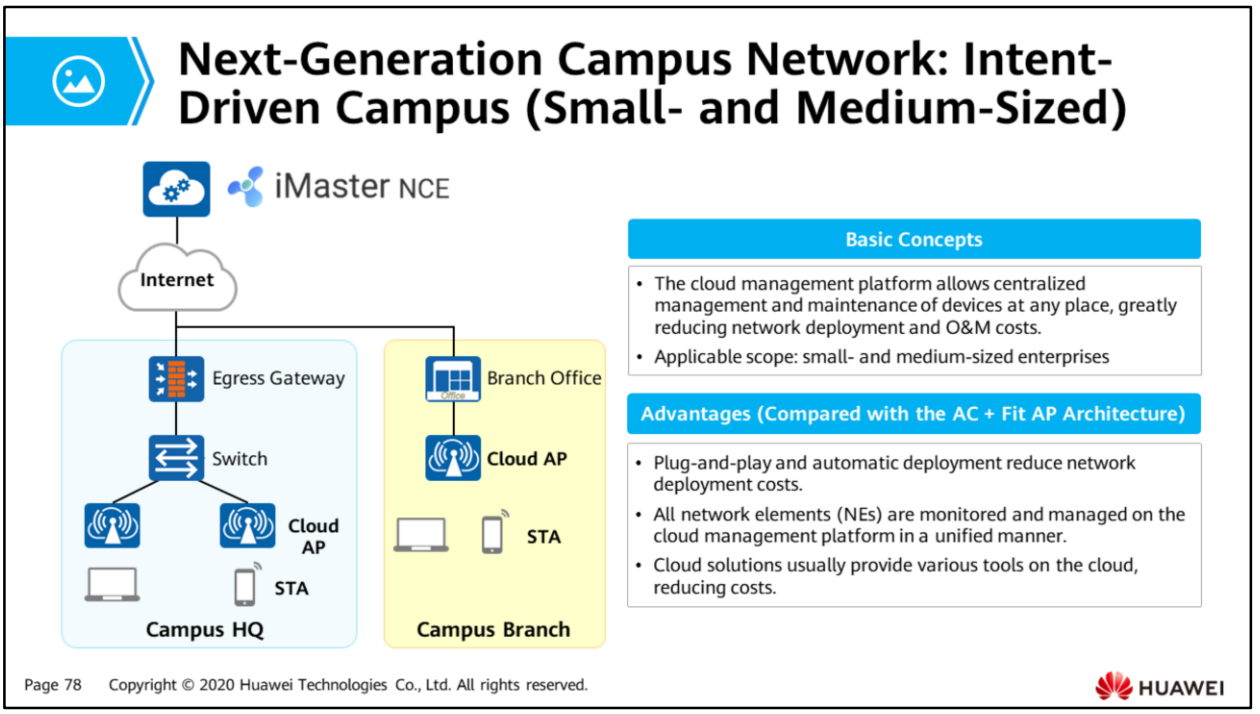
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Wi-Fi 5 cannot meet the low service latency and high bandwidth requirements of 4K/8K video conferencing scenarios.
- Powered by Huawei SmartRadio intelligent application acceleration, Wi-Fi 6 achieves a latency of as low as 10 ms.

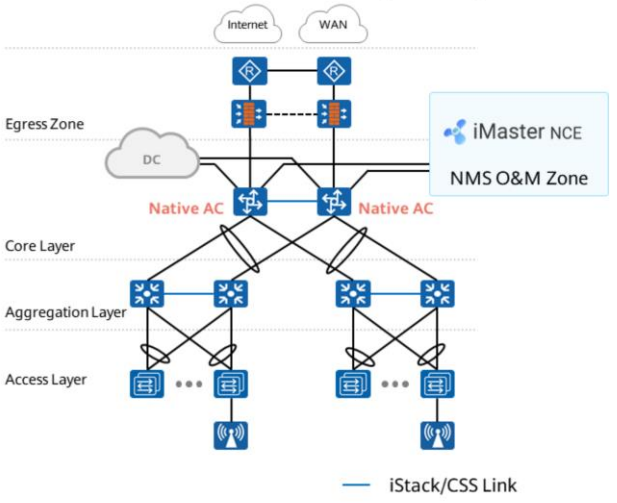


- Currently, the theoretical rate of all Wi-Fi 5 products (Wave 2) is 2.5 Gbit/s, and that of Wi-Fi 6 products is 9.6 Gbit/s. Therefore, Wi-Fi 6 increases the rate by four folds compared with Wi-Fi 5.
- Wi-Fi 6 increases the number of concurrent users by four folds compared with Wi-Fi 5. In the actual test, at a per user bandwidth of 2 Mbit/s, the concurrent number of users supported by Wi-Fi 5 is 100, and that supported by Wi-Fi 6 is 400.
- The average latency supported by Wi-Fi 6 is about 20 ms (about 30 ms in Wi-Fi 5). Huawei SmartRadio intelligent application acceleration technology further reduces the service latency to as low as 10 ms.
- TWT is not supported by Wi-Fi 5.



- Disadvantages of traditional network solutions:
  - Traditional network solutions have many network deployment problems, such as high deployment costs and O&M difficulties. These problems are obvious in enterprises with many branches or geographically dispersed branches.
- Cloud management architecture:
  - The cloud management architecture can solve the problems faced by traditional network solutions. The cloud management platform can manage and maintain devices in a centralized manner at any place, greatly reducing network deployment and O&M costs.
  - After a cloud AP is deployed, the network administrator does not need to go to the site for cloud AP software commissioning. After power-on, the cloud AP automatically connects to the specified cloud management platform to load system files such as the configuration file, software package, and patch file. In this manner, the cloud AP can go online with zero touch configuration. The network administrator can deliver configurations to the cloud APs through the cloud management platform at anytime and anywhere, facilitating batch service configurations.

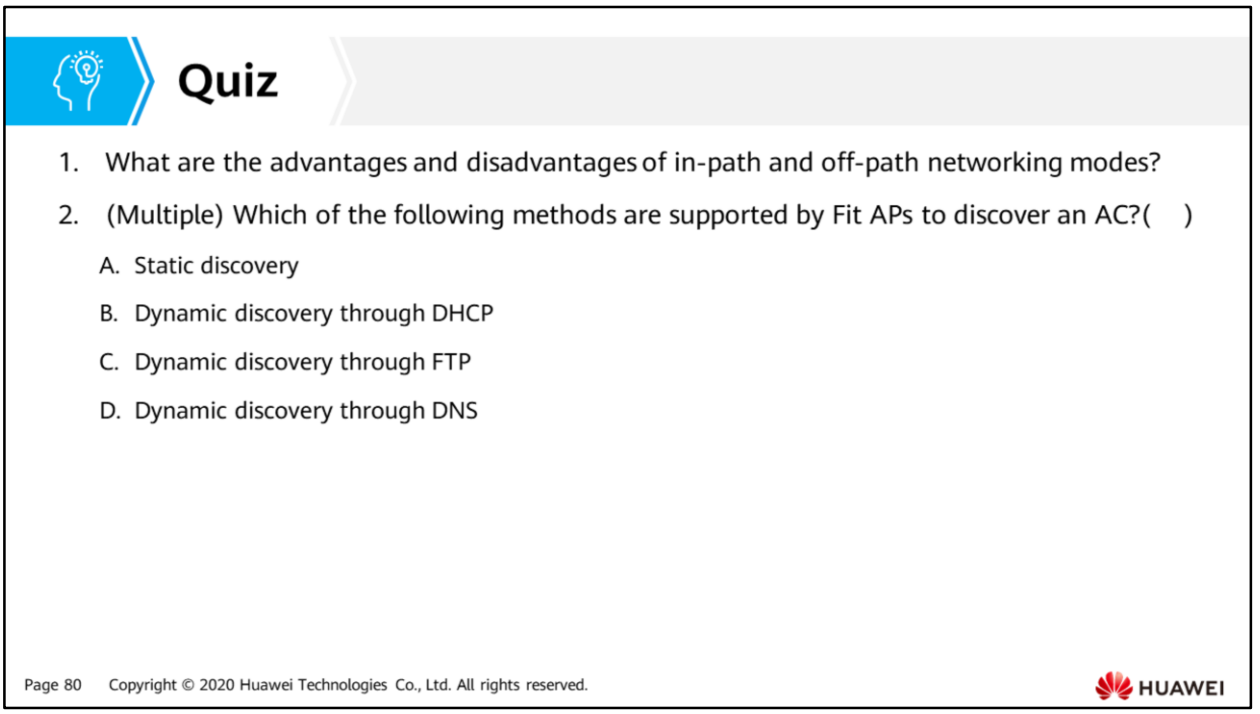
Next-Generation Campus Network: Intent-Driven Campus (Medium- and Large-Sized)



Architecture Characteristics

- iMaster NCE manages and configures APs in a unified manner and provides various functions. By further integrating with wired networks and leveraging Big Data and AI technologies, this architecture implements simplified, intelligent, and secure campus networks.
- Applicable scope: medium- and large-sized enterprises

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



1. Answer:
   - In-path networking advantages: Direct forwarding is often used on an in-path network. This networking mode simplifies the network architecture and applies to large-scale centralized WLANs.
   - Off-path networking advantages: The off-path networking mode is commonly used. Wireless user service data does not need to be processed by an AC, eliminating the bandwidth bottleneck and facilitating the usage of existing security policies. Therefore, this networking mode is recommended.
2. ABD

Summary

- WLAN technology allows users to easily access a wireless network and freely move around within the coverage of the wireless network, eliminating the constraints of wired networks.
- In this course, we have learned WLAN technologies on enterprise networks, including the basic concepts, fundamentals, network architectures, configuration implementation, and development trend of WLAN technologies.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



WAN Technologies

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- As economic globalization and digital transformation accelerate, enterprises keep expanding their scales. More and more branches locate in different regions, with each branch network being considered as a local area network (LAN). The headquarters and branches need to cross geographical locations to communicate with each other. To better carry out services, an enterprise needs to connect these geographically dispersed branches through a wide area network (WAN).
- The development of the WAN technologies is accompanied by the continuously increased bandwidth. In the early stage, X.25 provided only the bandwidth of 64 kbit/s. Later, the digital data network (DDN) and Frame Relay (FR) increased the bandwidth to 2 Mbit/s. Synchronous digital hierarchy (SDH) and asynchronous transfer mode (ATM) further increased the bandwidth to 10 Gbit/s. Now, the current IP-based WANs provide 10 Gbit/s or even higher bandwidth.
- This course describes the development history of WAN technologies, especially the implementations and configurations of Point-to-Point Protocol (PPP) and Point-to-Point Protocol over Ethernet (PPPoE).

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand the basic concepts and development history of WANs.
  - Understand PPP and PPPoE implementations.
  - Master basic PPP and PPPoE configurations.
  - Understand basic MPLS/SR concepts.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

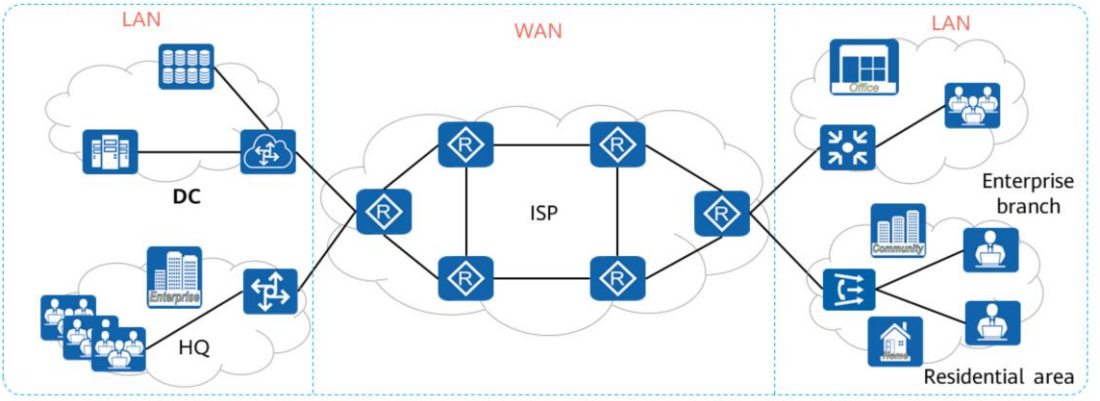
Contents

1. **Overview of Early WAN Technologies**
2. PPP Implementation and Configuration
3. PPPoE Implementation and Configuration
4. Development of WAN Technologies

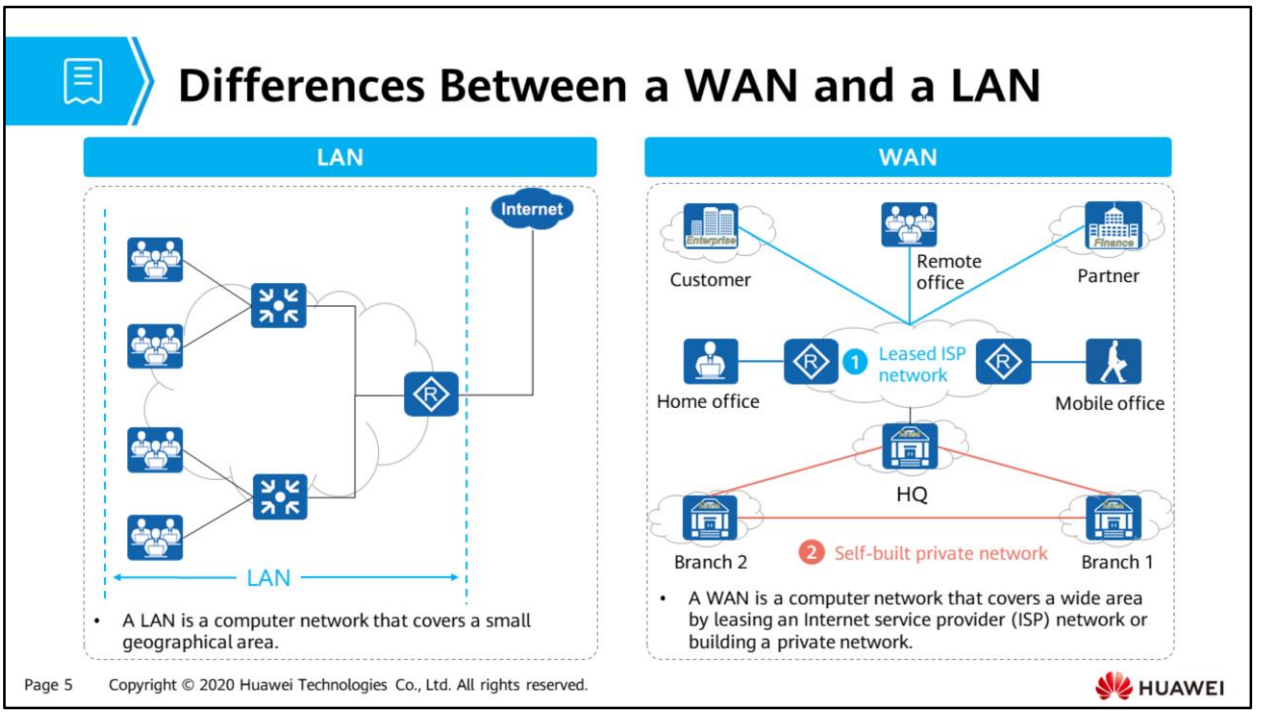
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

What Is a WAN?

- A **WAN** is a network that connects LANs in different areas. A WAN generally covers tens of kilometers to thousands of kilometers. It can connect multiple regions, cities, and countries, or provide long-distance communication across several continents, forming an international remote network.



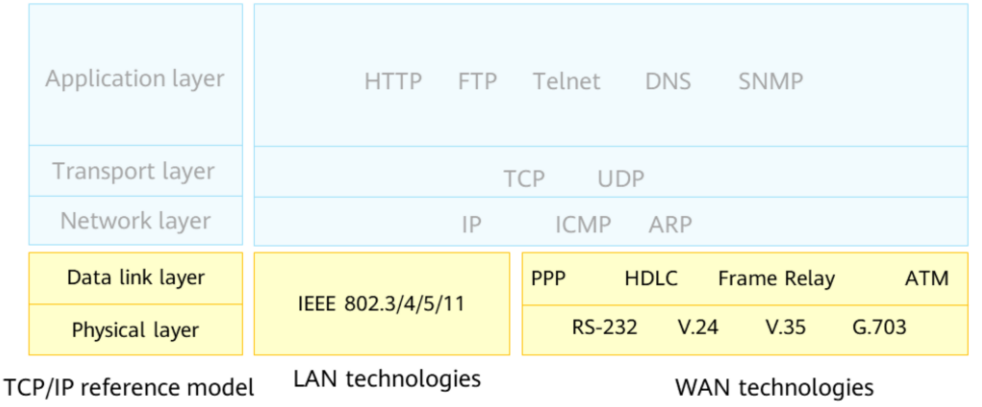
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The main differences between a WAN and a LAN are as follows:
  - A LAN provides high bandwidth but supports only a short transmission distance, which cannot meet the long-distance transmission requirements of a WAN.
  - LAN devices are usually switches, whereas WAN devices are mostly routers.
  - A LAN belongs to an institute or organization, whereas most WAN services are provided by ISPs.
  - WANs and LANs usually use different protocols or technologies only at the physical layer and data link layer. They do not have notable differences in the other layers.
  - The private networks of banks, governments, military, and large companies are also WANs and physically isolated from the Internet.
  - The Internet is only a type of WAN. Small enterprises use the Internet as the WAN connection.

Overview of Early WAN Technologies

- The early WANs and LANs differ in the data link layer and physical layer and are the same in the other layers in the TCP/IP reference model.

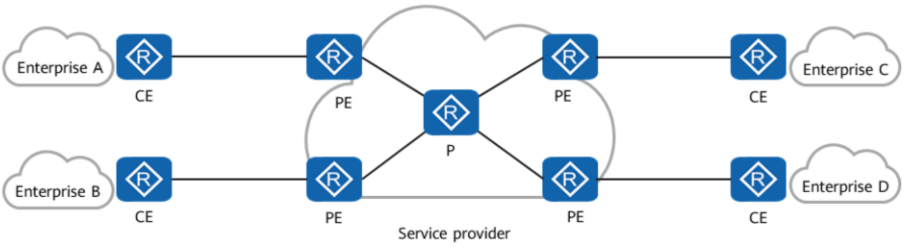


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- At the early stage, the common physical layer standards of WANs include common interface standards EIA/TIA-232 (RS-232) formulated by the Electronic Industries Alliance (EIA), and Telecommunications Industry Association (TIA), serial line interface standards V.24 and V.35 formulated by the International Telecommunication Union (ITU), and the G.703 standards related to the physical and electrical features of various digital interfaces.
- The common data link layer standards of WANs include High-Level Data Link Control (HDLC), PPP, FR, and ATM.
    - HDLC is a universal protocol running at the data link layer. Data packets are encapsulated into HDLC frames with the header and tail overheads added. The HDLC frames can be transmitted only on P2P synchronous links and do not support IP address negotiation and authentication. HDLC seeks high reliability by introducing a high overhead, leading to low transmission efficiency.
    - PPP runs at the data link layer for P2P data transmission over full-duplex synchronous and asynchronous links. PPP is widely used because it provides user authentication, supports synchronous and asynchronous communication, and is easy to extend.
    - FR is an industry-standard and switched data link protocol. It uses the error-free check mechanism to speed up data forwarding.
    - ATM is a connection-oriented switching technology based on circuit switching and packet switching. It uses 53-byte ATM cells to transmit information.

WAN Device Roles

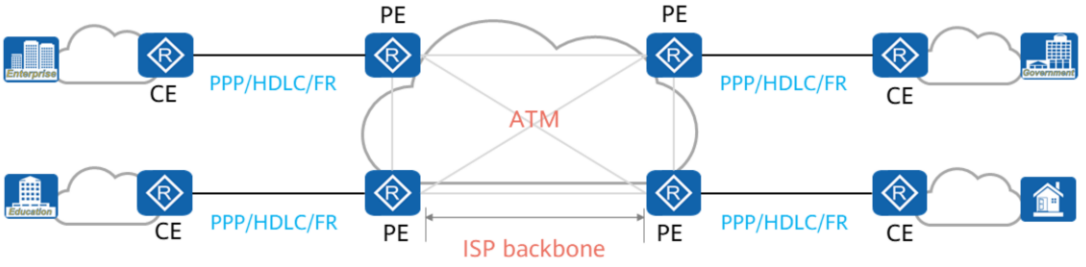
- There are three basic roles of WAN devices: customer edge (CE), provider edge (PE), and provider (P). They are defined as follows:
  - CE: a device located at the customer premises and connected to one or more PEs for user access.
  - PE: a service provider's important edge device that is connected to both a CE and a P.
  - P: a service provider's device that is not connected to any CE.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Application of Early WAN Technologies

- The early WAN technologies perform different Layer 2 encapsulation at the data link layer for different types of physical links. PPP, HDLC, and FR are commonly used between CEs and PEs to implement long-distance transmission of user access packets over a WAN. ATM is commonly used on ISP backbone networks for high-speed forwarding.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. Overview of Early WAN Technologies
2. **PPP Implementation and Configuration**
   - **PPP Implementation**
   - PPP Configuration
3. PPPoE Implementation and Configuration
4. Development of WAN Technologies

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

PPP Introduction

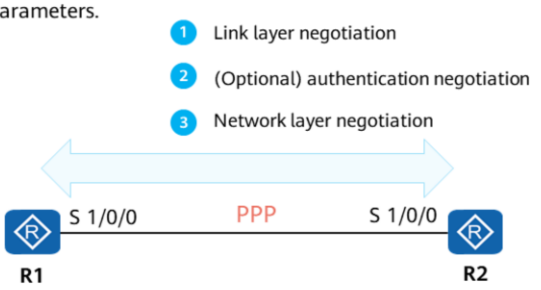
- PPP is a common WAN data link layer protocol. It is used for P2P data encapsulation and transmission on full-duplex links.
- PPP provides the Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).
- PPP features high extensibility. For example, PPP can be extended as Point-to-Point Protocol over Ethernet (PPPoE) when PPP packets need to be transmitted over an Ethernet.
- PPP provides the Link Control Protocol (LCP), which is used to negotiate link layer parameters, such as the maximum receive unit (MRU) and authentication mode.
- PPP provides various Network Control Protocols (NCPs), such as IP Control Protocol (IPCP), for negotiation of network layer parameters and better support for network layer protocols.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

PPP Link Setup Process

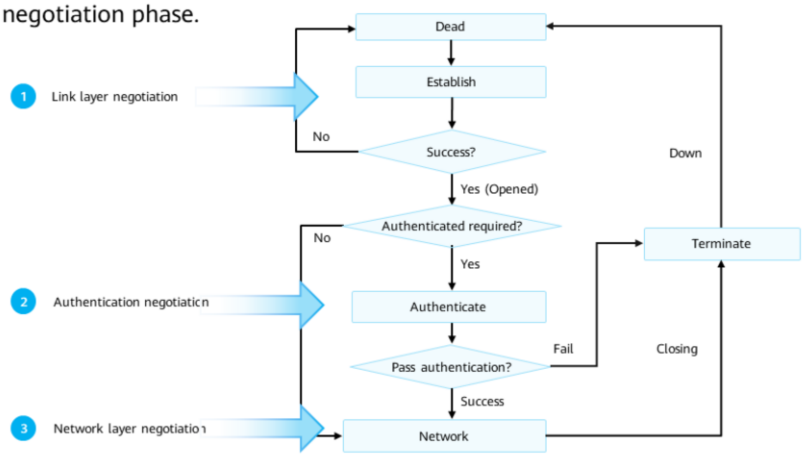
- PPP link setup involves link layer negotiation, optional authentication negotiation, and network layer negotiation.
  - Link layer negotiation: LCP packets are used to negotiate link parameters and establish link layer connections.
  - (Optional) authentication negotiation: The authentication mode negotiated during link layer negotiation is used for link authentication.
  - Network layer negotiation: NCP negotiation is used to select and configure a network layer protocol and negotiate network layer parameters.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

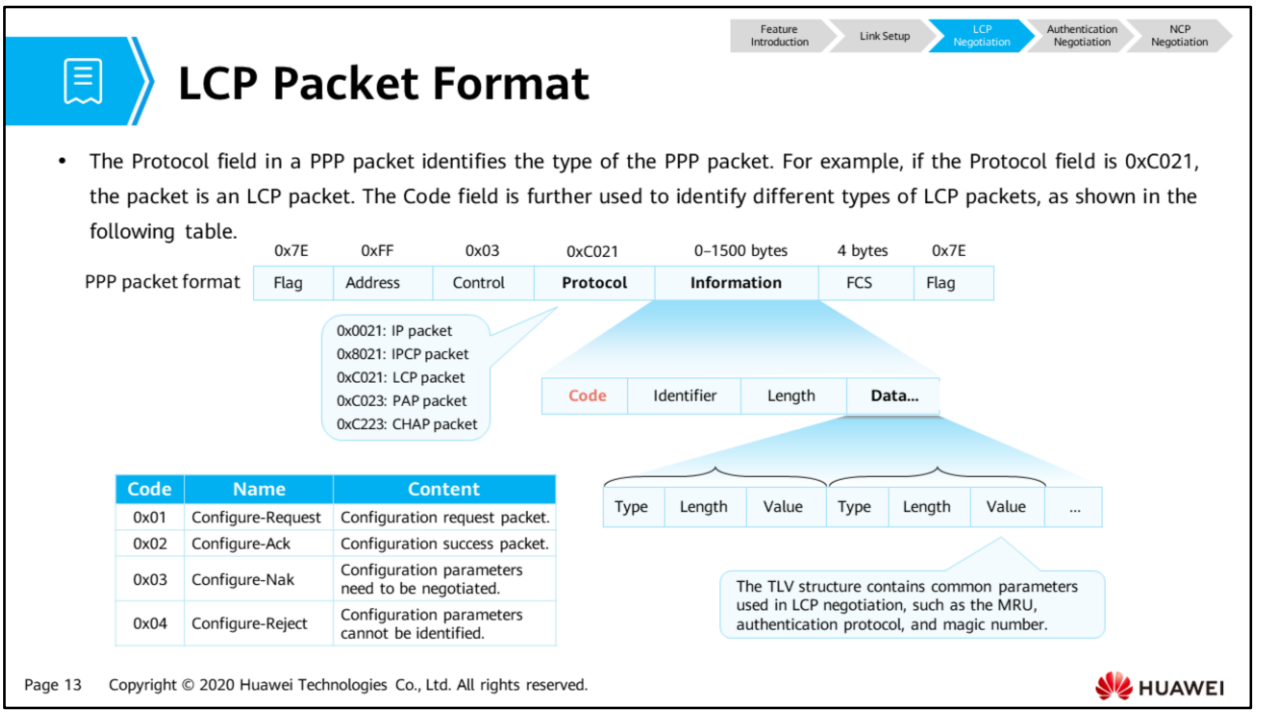
State Machine of the PPP Link Interface

- PPP negotiation is performed by the interfaces at both ends of a link. The interface status indicates the protocol negotiation phase.



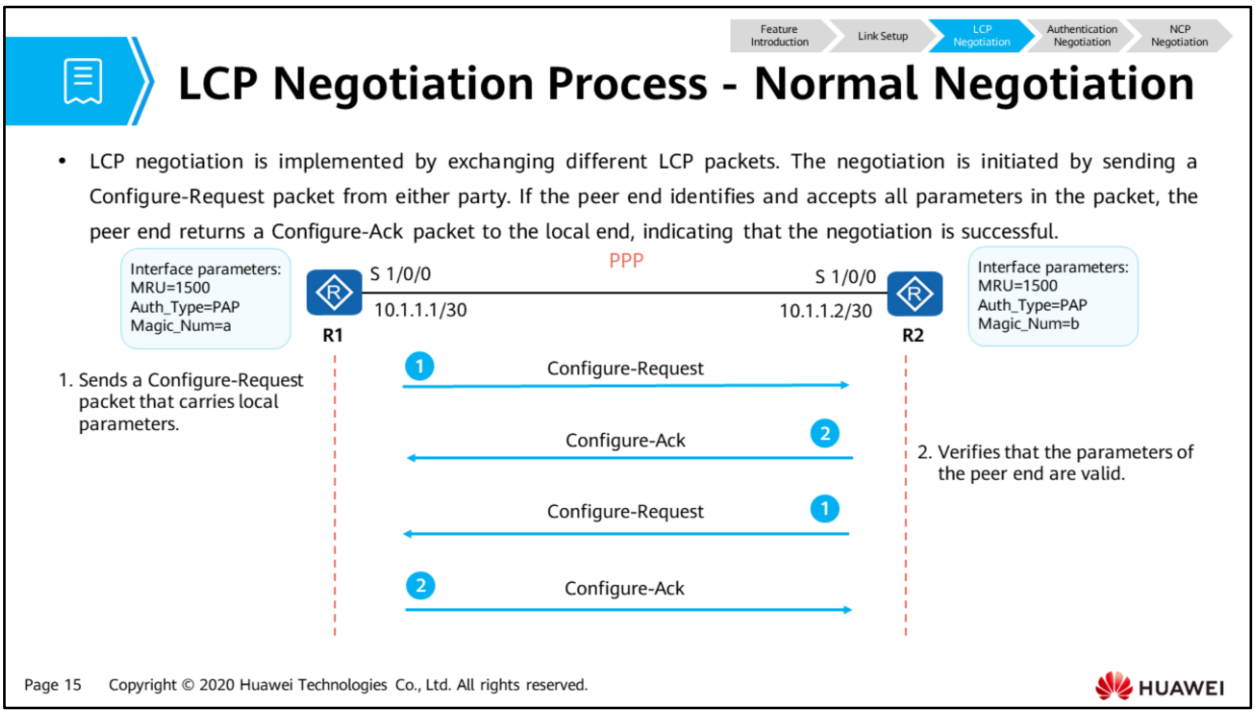
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- A PPP link can be set up after going through the link establishment, authentication, and network layer negotiation phases. The details are as follows:
  1. Two communicating devices enter the Establish phase when starting to set up a PPP connection.
  2. In the Establish phase, they perform LCP negotiation to negotiate an MRU, authentication mode, magic number, and other options. If the negotiation is successful, the devices enter the Opened state, indicating that the lower-layer link has been established.
  3. If authentication is configured, the devices enter the Authenticate phase. Otherwise, the devices directly enter the Network phase.
  4. In the Authenticate phase, link authentication is performed based on the authentication mode negotiated in the link establishment phase. Two authentication modes are available: PAP and CHAP. If the authentication succeeds, the devices enter the Network phase. Otherwise, the devices enter the Terminate phase, tear down the link, and set the LCP status to Down.
  5. In the Network phase, NCP negotiation is performed on the PPP link to select and configure a network layer protocol and to negotiate network layer parameters. The most common NCP protocol is IPCP, which is used to negotiate IP parameters.
  6. In the Terminate phase, if all resources are released, the two communicating devices return to the Dead phase.
- During the PPP operation, the PPP connection can be terminated at any time. A physical link disconnection, authentication failure, timeout timer expiry, and connection close by administrators through configuration can all cause a PPP connection to enter the Terminate phase.

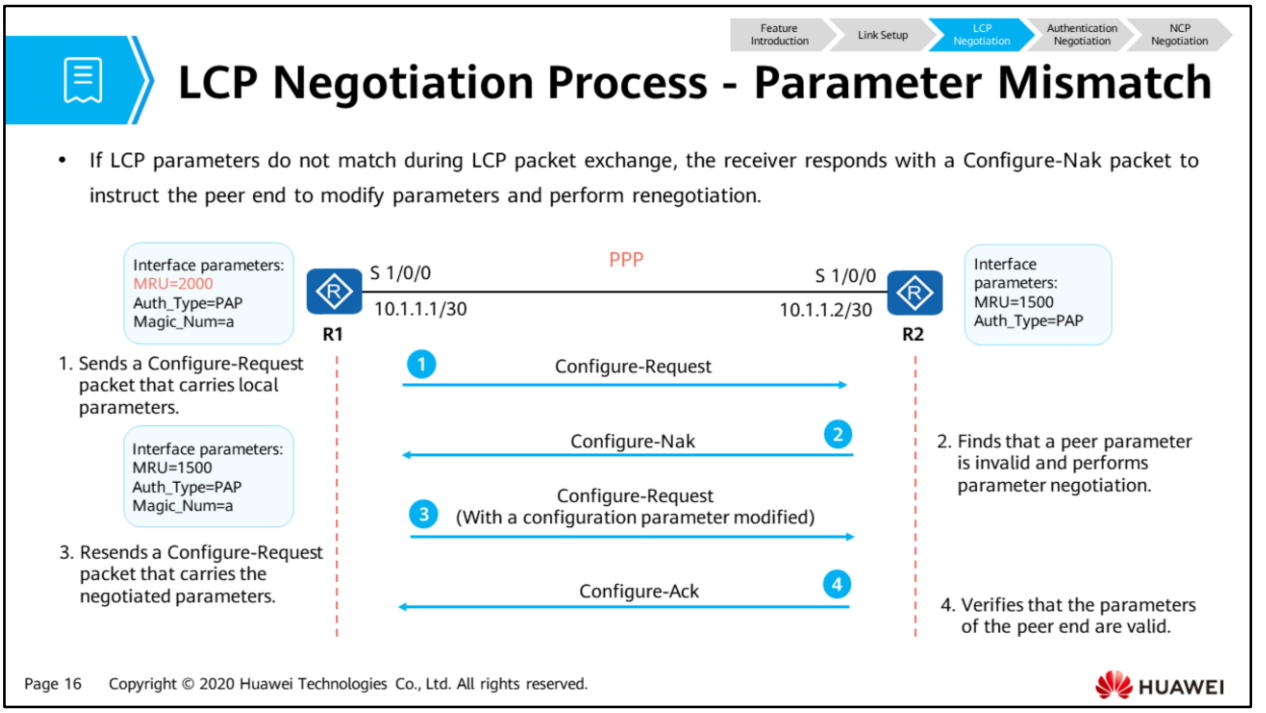


- PPP frame format:
  - The Flag field identifies the start and end of a physical frame and is a binary sequence 01111110 (0X7E).
  - The Address field in a PPP frame represents a broadcast address and has a fixed value of 11111111(0XFF).
  - The Control field of a PPP data frame is 00000011 (0X03) by default, indicating that the frame is an unordered frame.
  - The FCS field is a 16-bit checksum used to check the integrity of PPP frames.
  - The Protocol field indicates the type of protocol packets encapsulated using PPP. 0XC021, 0XC023, and 0XC223 indicate LCP, PAP, and CHAP packets, respectively.
  - The Information field specifies the content of a protocol specified by the Protocol field. The maximum length of this field is called the MRU. The default value is 1500 bytes.
  - When the Protocol field is 0XC021, the Information field structure is as follows:
    - The Identifier field is one byte and is used to match requests and responses.
    - The Length field specifies the total number of bytes in the LCP packet.
    - The Data field carries various TLV parameters for negotiating configuration options, including an MRU, authentication protocol, and the like.

- Common configuration parameters carried by LCP packets include the MRU, authentication protocol, and magic number.
    - On the versatile routing platform (VRP), the MRU is represented by the maximum transmission unit (MTU) configured on an interface.
    - The common PPP authentication protocols are PAP and CHAP. The two ends of a PPP link can use different authentication protocols to authenticate each other. However, the authenticated end must support the authentication protocol required by the authenticating end and be configured with correct authentication information such as the username and password.
    - LCP uses magic numbers to detect link loops and other exceptions. A magic number is a random number. The random mechanism must ensure that the probability of generating the same magic number at both ends is almost 0.



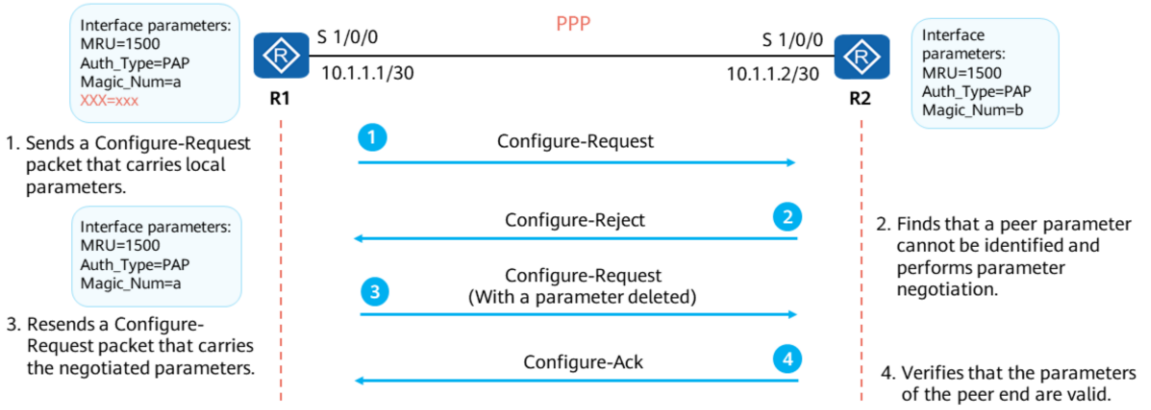
- R1 and R2 are connected through a serial link and run the PPP protocol. After the physical link becomes available, R1 and R2 use LCP to negotiate link parameters.
- In this example, R1 sends a Configure-Request packet that carries link layer parameters configured on R1. After receiving the Configure-Request packet, R2 returns a Configure-Ack packet to R1 if R2 can identify and accept all parameters in the packet. Similarly, R2 also sends a Configure-Request packet to R1, so that R1 checks whether the parameters on R2 are acceptable.
- If R1 does not receive any Configure-Ack packet, it retransmits a Configure-Request packet every 3s. If R1 does not receive any Configure-Ack packet after sending 10 Configure-Request packets consecutively, it considers the peer end unavailable and stops sending Configure-Request packets.



- After R2 receives the Configure-Request packet from R1, if R2 can identify all link layer parameters carried in the packet but considers that some or all parameter values are unacceptable (parameter value negotiation fails), R2 returns a Configure-Nak packet to R1.
- The Configure-Nak packet contains only unacceptable link layer parameters, with values (or value ranges) changed to those that can be accepted by R2.
- After receiving the Configure-Nak packet, R1 re-selects other locally configured parameters according to the link layer parameters in the packet and resends a Configure-Request packet.

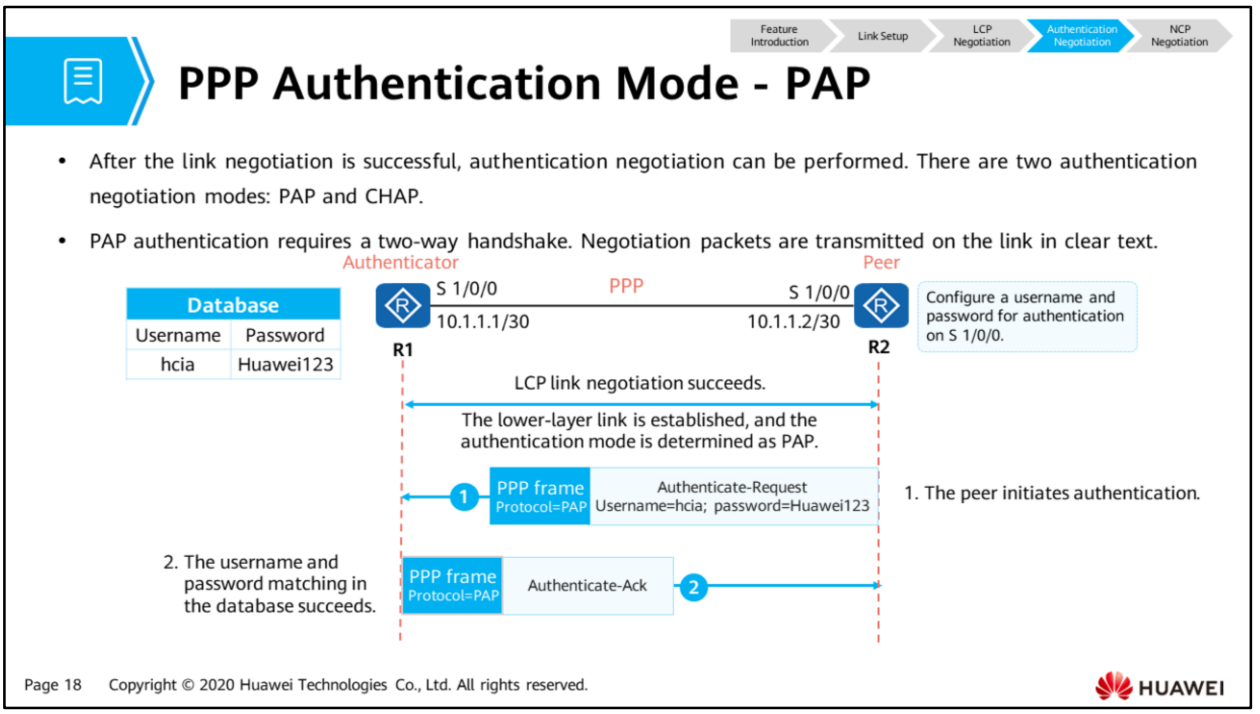
LCP Negotiation - Unrecognized Parameters

- If LCP parameters cannot be identified during LCP packet exchange, the receiver responds with a Configure-Reject packet to instruct the peer end to delete the unidentifiable parameters and renegotiates with the peer end.

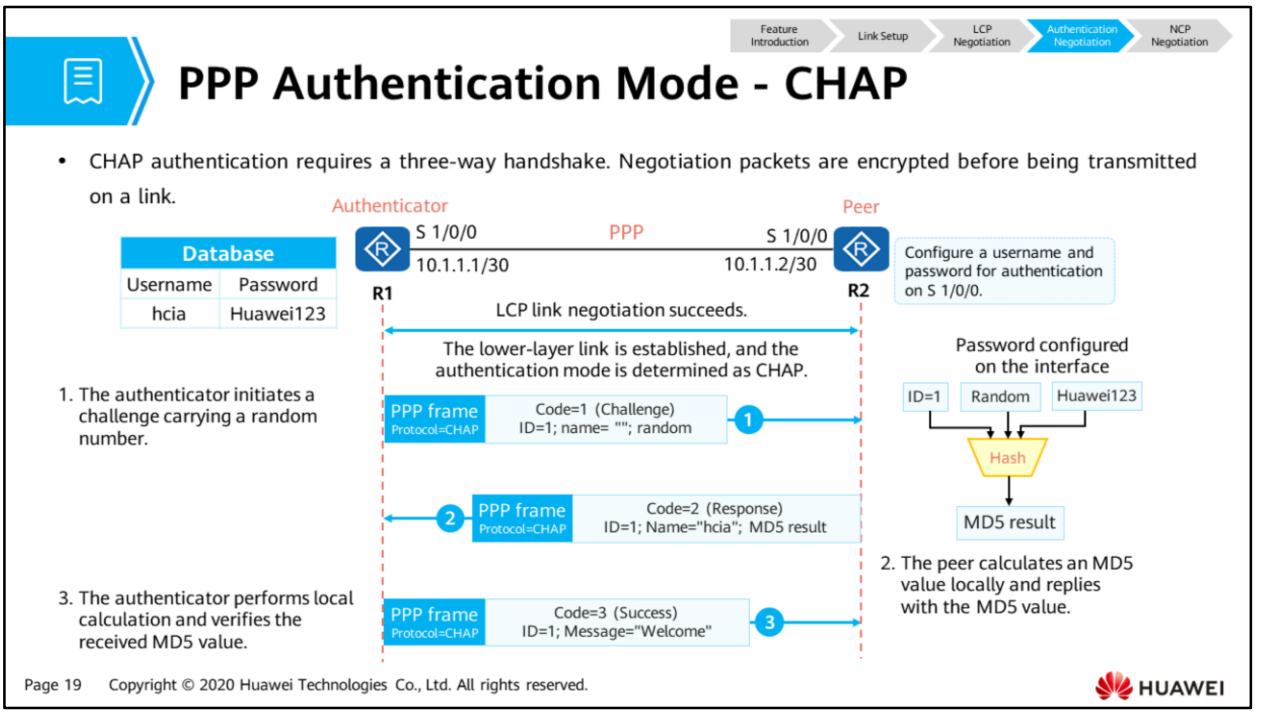


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- After receiving a Configure-Request packet from R1, R2 returns a Configure-Reject packet to R1 if R2 cannot identify some or all link layer parameters carried in the packet. The Configure-Reject packet contains only the link layer parameters that cannot be identified.
- After receiving the Configure-Reject packet, R1 resends a Configure-Request packet to R2. This packet contains only parameters that can be identified by R2.



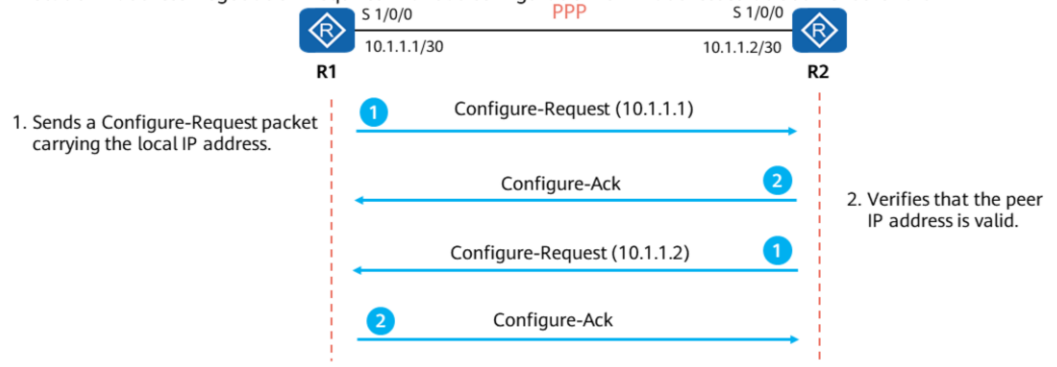
- After LCP negotiation is complete, the authenticator requires the peer to use PAP for authentication.
- PAP is a two-way handshake authentication protocol. The password is transmitted in clear text on the link. The process is as follows:
  - The peer sends the configured username and password to the authenticator in clear text through an Authenticate-Request packet.
  - After receiving the username and password from the peer, the authenticator checks whether the username and password match those in the locally configured database. If they match, the authenticator returns an Authenticate-Ack packet, indicating that the authentication is successful. If they do not match, the authenticator returns an Authenticate-Nak packet, indicating that the authentication is unsuccessful.



- After LCP negotiation is complete, the authenticator requires the peer to use CHAP for authentication.
- CHAP authentication requires three packet exchanges. The process is as follows:
  - The authenticator initiates an authentication request and sends a Challenge packet to the peer. The Challenge packet contains a random number and an ID.
  - After receiving the Challenge packet, the peer performs encryption calculation using the formula MD5{ID+random number+password}. The formula means that the authenticator combines the identifier, random number, and password into a character string and performs an MD5 operation on the character string to obtain a 16-byte digest. The peer then encapsulates the digest and the CHAP username configured on the interface into a Response packet and sends the Response packet to the authenticator.
  - After receiving the Response packet, the authenticator locally searches for the password corresponding to the username in the Response packet. After obtaining the password, the authenticator encrypts the password using the same formula as that used by the peer. Then, the authenticator compares the digest obtained through encryption with that in the Response packet. If they are the same, the authentication succeeds. If they are different, the authentication fails.
- In CHAP authentication, the password of the peer is encrypted before being transmitted, which greatly improves security.
- Notices About Encryption Algorithms
  - The MD5 (digital signature scenario and password encryption) encryption algorithm has security risks. You are advised to use more secure encryption algorithms, such as AES, RSA (2048 bits or above), SHA2, and HMAC-SHA2.

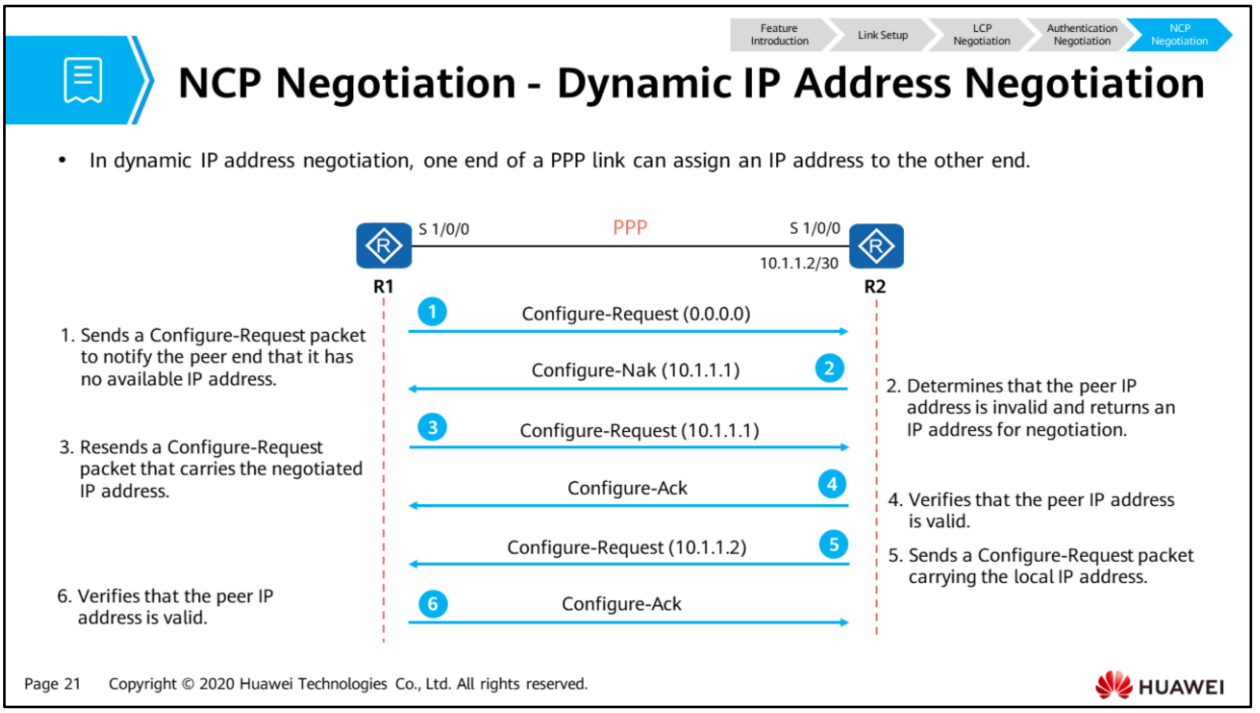
NCP Negotiation - Static IP Address Negotiation

- After PPP authentication negotiation, the two ends enter the NCP negotiation phase to negotiate the format and type of data packets transmitted on the data link. IPCP, for example, is classified into static and dynamic IP address negotiation.
- Static IP address negotiation requires manual configuration of IP addresses at both ends of a link.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- NCP is used to establish and configure different network layer protocols and negotiate the format and type of data packets transmitted on a data link. IPCP is a commonly used NCP.
- The static IP address negotiation process is as follows:
  - Each end sends a Configure-Request packet carrying the locally configured IP address.
  - After receiving the packet from the peer end, the local end checks the IP address in the packet. If the IP address is a valid unicast IP address and is different from the locally configured IP address (no IP address conflict), the local end considers that the peer end can use this address and responds with a Configure-Ack packet.



- The dynamic IP address negotiation process is as follows:
  - R1 sends a Configure-Request packet to R2. The packet contains an IP address 0.0.0.0, indicating that R1 requests an IP address from R2.
  - After receiving the Configure-Request packet, R2 considers the IP address 0.0.0.0 invalid and replies with a Configure-Nak packet carrying a new IP address 10.1.1.1.
  - After receiving the Configure-Nak packet, R1 updates its local IP address and resends a Configure-Request packet carrying the new IP address 10.1.1.1.
  - After receiving the Configure-Request packet, R2 considers the IP address contained in the packet valid and returns a Configure-Ack packet.
  - R2 also sends a Configure-Request packet to R1 to request use of IP address 10.1.1.2. R1 considers the IP address valid and replies with a Configure-Ack packet.

Contents

1. Overview of Early WAN Technologies
2. **PPP Implementation and Configuration**
   - PPP Implementation
   - **PPP Configuration**
3. PPPoE Implementation and Configuration
4. Development of WAN Technologies

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuring Basic PPP Functions

1. Encapsulate an interface with PPP.

   [Huawei-Serial0/0/0] **link-protocol ppp**

   In the interface view, change the interface encapsulation protocol to PPP. The default encapsulation protocol of Huawei devices' serial interfaces is PPP.

2. Configure a negotiation timeout period.

   [Huawei-Serial0/0/0] **ppp timer negotiate** *seconds*

   During LCP negotiation, the local end sends an LCP negotiation packet to the peer end. If the local end does not receive a reply packet from the peer end within the specified negotiation timeout period, the local end resends an LCP negotiation packet.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuring PAP Authentication

1. Configure an authenticator to authenticate a peer using the PAP mode.

```
[Huawei-aaa] local-user user-name password { cipher | irreversible-cipher } password
[Huawei-aaa] local-user user-name service-type ppp
```

```
[Huawei-Serial0/0/0] ppp authentication-mode pap
```

Before configuring the authenticator to authenticate a peer using the PAP mode, add the username and password of the peer to the local user list in the AAA view. Then select the PAP authentication mode.

2. Configure the peer to be authenticated by the authenticator in PAP mode.

```
[Huawei-Serial0/0/0] ppp pap local-user user-name password { cipher | simple } password
```

This command configures the peer to send its username and password to the authenticator.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuring CHAP Authentication

1. Configure an authenticator to authenticate a peer using CHAP mode.

```
[Huawei-aaa] local-user user-name password { cipher | irreversible-cipher } password
[Huawei-aaa] local-user user-name service-type ppp
```

```
[Huawei-Serial0/0/0] ppp authentication-mode chap
```

2. Configure the peer to be authenticated by the authenticator in CHAP mode.

```
[Huawei-Serial0/0/0] ppp chap user user-name
```

```
[Huawei-Serial0/0/0] ppp chap password { cipher | simple } password
```

This command configures a local username and a password for CHAP authentication.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring PAP Authentication



- Experiment requirements:
  1. Enable PAP authentication on the PPP link between R1 and R2.
  2. Configure R1 as the authenticator.
  3. Configure R2 as the peer.

Configurations on R1

```
[R1]aaa # Add information about the user to be authenticated.
[R1-aaa]local-user huawei password cipher huawei123
[R1-aaa]local-user huawei service-type ppp
# Specify the service type of the user to be authenticated.
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]link-protocol ppp
[R1-Serial1/0/0]ppp authentication-mode pap
# Set the authentication mode to PAP.
[R1-Serial1/0/0]ip address 10.1.1.1 30
```

Configurations on R2

```
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]link-protocol ppp
[R2-Serial1/0/0]ppp pap local-user huawei password cipher
huawei123 # Add user information for PPP authentication.
[R2-Serial1/0/0]ip address 10.1.1.2 30
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring CHAP Authentication



- Experiment requirements:
  1. Enable CHAP authentication on the PPP link between R1 and R2.
  2. Configure R1 as the authenticator.
  3. Configure R2 as the peer.

Configurations on R1

```
[R1]aaa # Add information about the user to be authenticated.
[R1-aaa]local-user huawei password cipher huawei123
[R1-aaa]local-user huawei service-type ppp
# Specify the service type of the user to be authenticated.
[R1]interface Serial 1/0/0
[R1-Serial1/0/0]link-protocol ppp
[R1-Serial1/0/0]ppp authentication-mode chap
# Set the authentication mode to CHAP.
```

Configurations on R2

```
[R2]interface Serial 1/0/0
[R2-Serial1/0/0]link-protocol ppp
[R2-Serial1/0/0]ppp chap user huawei
[R2-Serial1/0/0]ppp chap password cipher huawei123
# Add user information for PPP authentication.
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

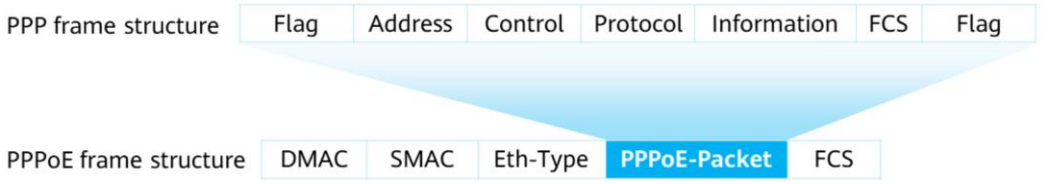
1. Overview of Early WAN Technologies
2. PPP Implementation and Configuration
3. **PPPoE Implementation and Configuration**
   - **PPPoE Overview**
   - Basic PPPoE Configuration
4. Development of WAN Technologies

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

What Is PPPoE?

- PPP over Ethernet (PPPoE) is a link layer protocol that encapsulates PPP frames into Ethernet frames. PPPoE enables multiple hosts on an Ethernet to connect to a broadband remote access server (BRAS).
- PPPoE integrates the advantages of Ethernet and PPP. It has the flexible networking advantage of Ethernet and can use PPP to implement authentication and accounting.

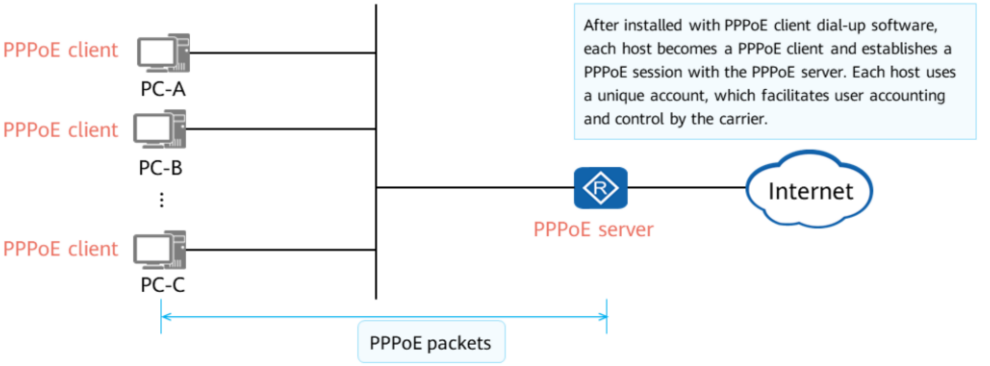


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Carriers want to connect multiple hosts at a site to a remote access device, which can provide access control and accounting for these hosts in a manner similar to dial-up access. Ethernet is the most cost-effective technology among all access technologies that connect multiple hosts to an access device. PPP provides good access control and accounting functions. PPPoE therefore was introduced to transmit PPP packets on the Ethernet.
- PPPoE uses Ethernet to connect a large number of hosts to the Internet through a remote access device and uses PPP to control each host. PPPoE applies to various scenarios, and provides high security as well as convenient accounting.

PPPoE Application Scenarios

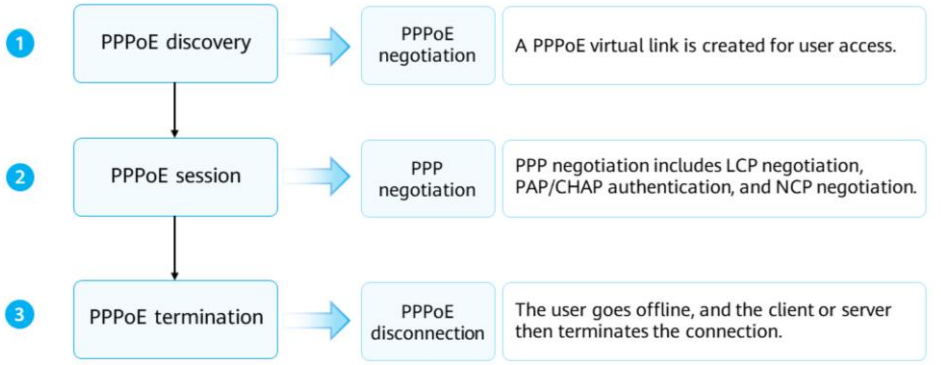
- PPPoE provides P2P connections on an Ethernet. A PPPoE client and a PPPoE server establish a PPP session to encapsulate PPP data packets and provide access services for hosts on the Ethernet, implementing user control and accounting. PPPoE is widely used on enterprise and carrier networks.
- PPPoE is usually used by home users and enterprise users to dial up to access the Internet.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

PPPoE Session Establishment

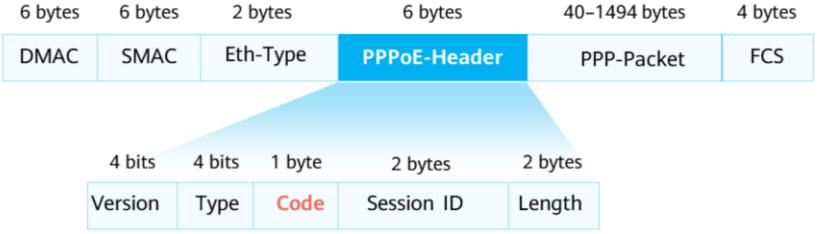
- PPPoE session establishment involves three stages: PPPoE discovery, session, and termination stages.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

PPPoE Packets

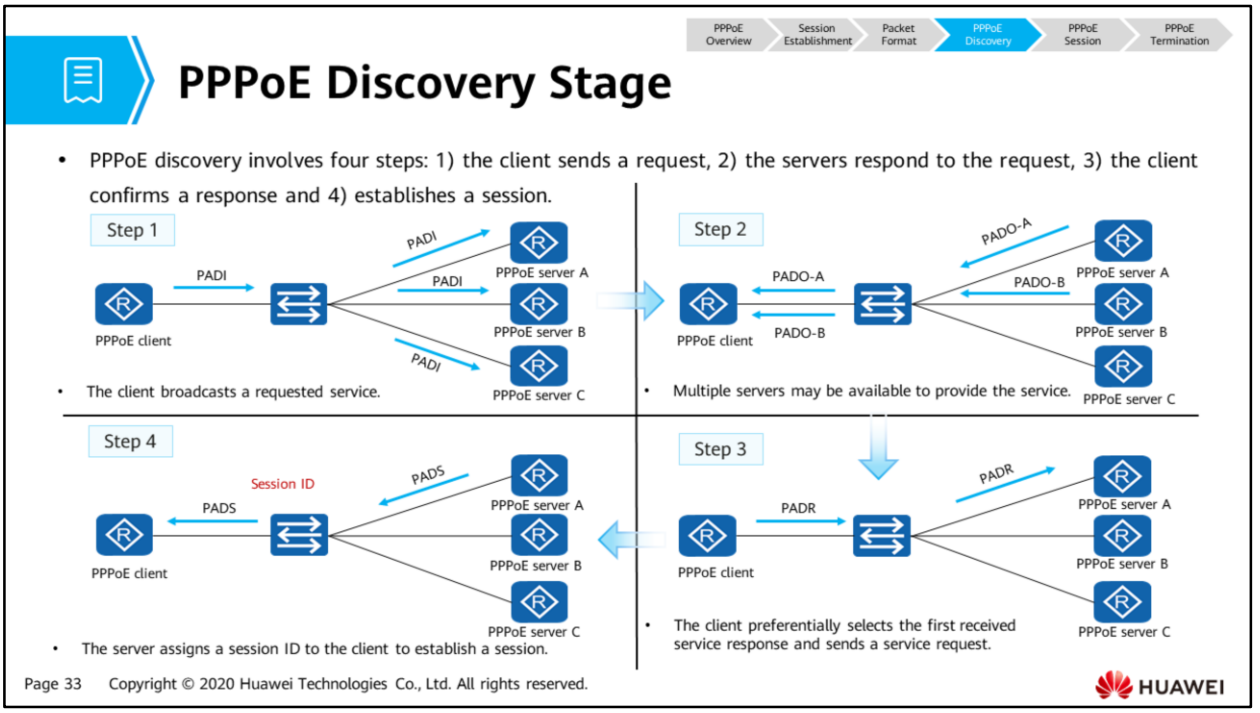
- A PPPoE session is established by exchanging different PPPoE packets. The PPPoE packet structure and common packet types are as follows.



Code	Name	Content
0x09	PADI	PPPoE Active Discovery Initiation packet
0x07	PADO	PPPoE Active Discovery Offer packet
0x19	PADR	PPPoE Active Discovery Request packet
0x65	PADS	PPPoE Active Discovery Session-confirmation packet
0xa7	PADT	PPPoE Active Discovery Terminate packet

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- PPPoE packets are encapsulated in Ethernet frames. The fields in an Ethernet frame are described as follows:
- DMAC: indicates the MAC address of a destination device, which is usually an Ethernet unicast or broadcast address (0xFFFFFFFF).
- SMAC: indicates the MAC address of a source device.
- Eth-Type: indicates the protocol type. The value 0x8863 indicates that PPPoE discovery packets are carried. The value 0x8864 indicates that PPPoE session packets are carried.
- The fields in a PPPoE packet are described as follows:
  - VER: indicates a PPPoE version. The value is 0x01.
  - Type: indicates the PPPoE type. The value is 0x01.
  - Code: indicates a PPPoE packet type. Different values indicate different PPPoE packet types.
  - Session ID: indicates a PPPoE session ID. This field defines a PPPoE session, together with the Ethernet SMAC and DMAC fields.
  - Length: indicates the length of a PPPoE packet.

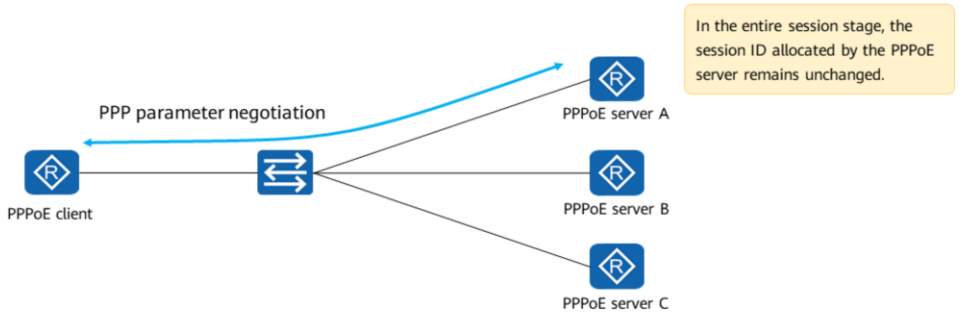


1. The PPPoE client broadcasts a PADI packet that contains the required service information on the local Ethernet.
    - The destination MAC address of the PADI packet is a broadcast address, the Code field is set to 0x09, and the Session ID field is set to 0x0000.
    - After receiving the PADI packet, all PPPoE servers compare the requested services with the services that they can provide.
2. If a server can provide the requested service, it replies with a PADO packet.
    - The destination address of the PADO packet is the MAC address of the client that sends the PADI packet. The Code field is set to 0x07 and the Session ID field is set to 0x0000.
3. The PPPoE client may receive multiple PADO packets. In this case, the PPPoE client selects the PPPoE server whose PADO packet is first received by the client and sends a PADR packet to the PPPoE server.
    - The destination address of the PADR packet is the MAC address of the selected server, the Code field is set to 0x19, and the Session ID field is set to 0x0000.
4. After receiving the PADR packet, the PPPoE server generates a unique session ID to identify the session with the PPPoE client and sends a PADS packet.
    - The destination address of the PADS packet is the MAC address of the PPPoE client, the Code field is set to 0x65, and the Session ID field is set to the uniquely generated session ID.

- After a PPPoE session is established, the PPPoE client and server enter the PPPoE session stage.

PPPoE Session Stage

- In the PPPoE session stage, PPP negotiation, including LCP, authentication, and NCP negotiation, is performed.

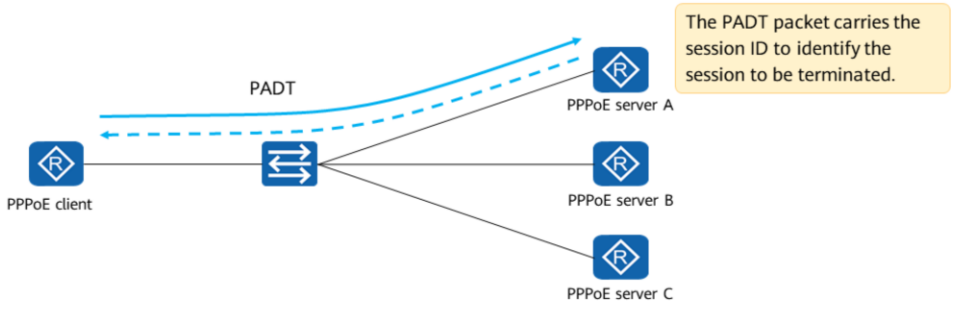


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In the PPPoE session stage, PPP negotiation and PPP packet transmission are performed.
- PPP negotiation in the PPPoE session stage is the same as common PPP negotiation, which includes the LCP, authentication, and NCP negotiation phases.
  - In the LCP phase, the PPPoE server and PPPoE client establish and configure a data link, and verify the data link status.
  - After LCP negotiation succeeds, authentication starts. The authentication protocol type is determined by the LCP negotiation result.
  - After authentication succeeds, PPP enters the NCP negotiation phase. NCP is a protocol suite used to configure different network layer protocols. A commonly used network-layer protocol is IPCP, which is responsible for configuring IP addresses for users and domain name servers (DNSs).
- After PPP negotiation succeeds, PPP data packets can be forwarded over the established PPP link. The data packets transmitted in this phase must contain the session ID determined in the discovery stage, and the session ID must remain unchanged.

PPPoE Session Termination Stage

- If the PPPoE client wants to terminate the session, it sends a PADT packet to the PPPoE server.
- Similarly, if the PPPoE server wants to terminate the session, it sends a PADT packet to the PPPoE client.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In a PADT packet, the destination MAC address is a unicast address, and the session ID is the ID of the session to be closed. Once a PADT packet is received, the session is closed.

Contents

1. Overview of Early WAN Technologies
2. PPP Implementation and Configuration
3. **PPPoE Implementation and Configuration**
   - PPPoE Overview
   - **Basic PPPoE Configuration**
4. Development of WAN Technologies

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Configuring Basic PPPoE Functions

1. Configure a dialer rule and set conditions for initiating a PPPoE session under the rule.

   ```
   [Huawei] dialer-rule
   ```

   Configure a username on the dialer interface. The username must be the same as that of the peer server.

   ```
   [Huawei-Dialer1]dialer user username
   ```

3. Add the interface to a dialer group.

   ```
   [Huawei-Dialer1]dialer-group group-number
   ```

4. Specify a dialer bundle for the interface.

   ```
   [Huawei-Dialer1]dialer-bundle number
   ```

5. Bind a physical interface to the dialer bundle.

   ```
   [Huawei-Ethernet0/0/0]pppoe-client dial-bundle-number number
   ```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example for Configuring a PPPoE Client (1)



- Experiment requirements:
  1. Configure R1 as a PPPoE client and R2 as a PPPoE server.
  2. Configure a dialer interface for the PPPoE client on R1.
  3. Configure the authentication function on the dialer interface on R1.
  4. The dialer interface on R1 can obtain the IP address allocated by the PPPoE server.
  5. R1 can access the server through the dialer interface.

1. Create a dialer interface and configure a username and password for authentication.

```
[R1]dialer-rule
[R1-dialer-rule]dialer-rule 1 ip permit
[R1-dialer-rule]quit
[R1]interface dialer 1
[R1-Dialer1] dialer user enterprise
[R1-Dialer1] dialer-group 1
[R1-Dialer1] dialer bundle 1
[R1-Dialer1] ppp chap user huawei1
[R1-Dialer1] ppp chap password cipher huawei123
[R1-Dialer1] ip address ppp-negotiate
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- The configuration of the PPPoE client includes three steps:
- Step 1: Configure a dialer interface.
  - The **dialer-rule** command displays the dialer rule view. In this view, you can configure the conditions for initiating a PPPoE session.
  - The **interface dialer** *number* command creates a dialer interface and displays the dialer interface view.
  - The **dialer user** *user-name* command configures a username for the peer end. This username must be the same as the PPP username on the peer server.
  - The **dialer-group** *group-number* command adds an interface to a dialer group.
  - The **dialer bundle** *number* command specifies a dialer bundle for the dialer interface. The device associates a physical interface with the dialer interface through the dialer bundle.
- Note: Ensure that the *group-number* parameter in the **dialer-group** command is the same as the *dialer-rule-number* parameter in the **dialer-rule** command.

Example for Configuring a PPPoE Client (2)



- Experiment requirements:
  1. Configure R1 as a PPPoE client and R2 as a PPPoE server.
  2. Configure a dialer interface for the PPPoE client on R1.
  3. Configure the authentication function on the dialer interface on R1.
  4. The dialer interface on R1 can obtain the IP address allocated by the PPPoE server.
  5. R1 can access the server through the dialer interface.

2. Bind the dialer interface to an outbound interface.

```
[R1]interface GigabitEthernet 0/0/1
[R1-GigabitEthernet0/0/1]pppoe-client dial-bundle-number 1
[R1-GigabitEthernet0/0/1]quit
```

3. Configure a default route from the PPPoE client to the server.

```
[R1]ip route-static 0.0.0.0  0.0.0.0  dialer 1
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Step 2: Bind the dialer bundle to a physical interface.
  - The **pppoe-client dial-bundle-number** *number* command binds the dialer bundle to a physical interface and specifies the dialer bundle for the PPPoE session. number specifies the dialer bundle number corresponding to the PPPoE session.
- Step 3: Configure a default static route. This route allows the traffic that does not match any entry in the routing table to initiate a PPPoE session through the dialer interface.

Example for Configuring a PPPoE Server



- Experiment requirements:
  1. Create an address pool on the PPPoE server for address allocation to the PPPoE client.
  2. The PPPoE server authenticates the PPPoE client and assigns a valid IP address to the client.

1. Create an address pool and a virtual template.

```
[R2]ip pool pool1 # Create an address pool and specify the range of the IP addresses to be allocated and a gateway.
[R2-ip-pool-pool1]network 192.168.1.0 mask 255.255.255.0
[R2-ip-pool-pool1]gateway-list 192.168.1.254
[R2]interface Virtual-Template 1 # Create a virtual template interface.
[R2-Virtual-Template1]ppp authentication-mode chap
[R2-Virtual-Template1]ip address 192.168.1.254 255.255.255.0
[R2-Virtual-Template1]remote address pool pool1
```

2. Bind a physical interface to the virtual template.

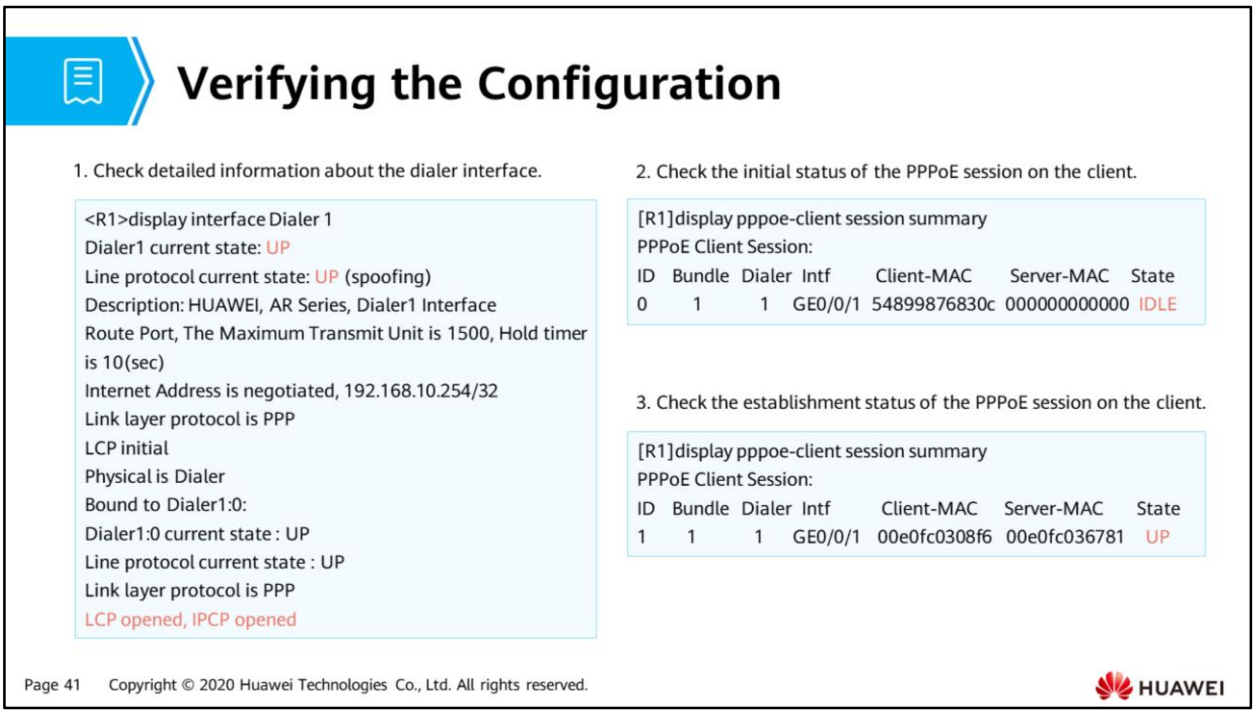
```
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]pppoe-server bind virtual-template 1
[R2-GigabitEthernet0/0/0]quit
```

3. Create an access user.

```
[R2]aaa # Add information about the user to be authenticated.
[R2-aaa]local-user huawei1 password cipher huawei123
[R2-aaa]local-user huawei1 service-type ppp
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- PPPoE Server Configurations
  - The **interface virtual-template** command creates a virtual template interface or displays the view of an existing virtual template interface.
  - The **pppoe-server bind** command binds an interface to the virtual template interface for PPPoE access.



- The **display interface dialer** *number* command displays the configuration of the dialer interface. The command output helps locate faults on the dialer interface.
- LCP opened, IPCP opened indicates that the link is working properly.
- The **display pppoe-client session summary** command displays the PPPoE session status and statistics on the PPPoE client.
    - **ID** indicates a PPPoE session ID. The values of the bundle ID and dialer ID are determined by the configured dialer parameters.
    - **Intf** indicates the physical interface used for negotiation on the PPPoE client.
    - **State** indicates the status of a PPPoE session, which can be:
        1. IDLE: The current session is idle.
        2. PADI: The current session is in the discovery stage, and a PADI packet has been sent.
        3. PADR: The current session is in the discovery stage, and a PADR packet has been sent.
        4. UP: The current session is set up successfully.

Contents

1. Overview of Early WAN Technologies
2. PPP Implementation and Configuration
3. PPPoE Implementation and Configuration
4. **Development of WAN Technologies**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

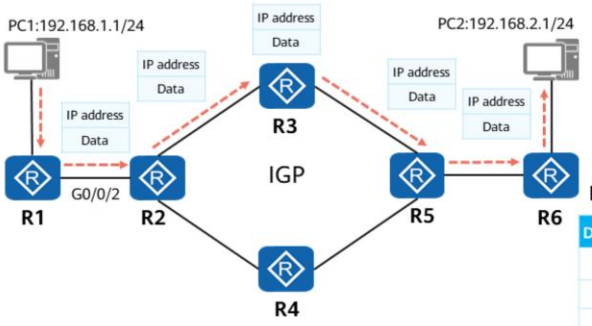
Evolution of WAN Technologies

- The data link layer protocols commonly used on early WANs include PPP, HDLC, and ATM. With the network evolution towards all-IP, the IP-based Internet becomes popular. However, the IP technology based on the longest match rule must use software to search for routes, resulting in low forwarding performance, which has become the bottleneck that restricts the network development.
- Multiprotocol Label Switching (MPLS) was originally proposed to improve the forwarding speeds of routers. Compared with the traditional IP routing mode, MPLS parses IP packet headers only at the network edges during data forwarding. Transit nodes forward packets based on labels, without the need to parse IP packet headers. This speeds up software processing.
- With the improvement of router performance, the route search speed is no longer a bottleneck for network development. Thus, MPLS loses its advantage in fast forwarding speed. However, leveraging support for multi-layer labels and a connection-oriented forwarding plane, MPLS is widely applied in various scenarios, such as virtual private network (VPN), traffic engineering (TE), and quality of service (QoS) scenarios.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Traditional IP Routing and Forwarding

- Traditional IP forwarding uses hop-by-hop forwarding. Each time a data packet passes through a router, the router decapsulates the packet to check the network layer information and searches its routing table based on the longest match rule to guide packet forwarding. The repeat process of decapsulating packets, searching routing tables, and re-encapsulating the packets on routers lead to low forwarding performance.



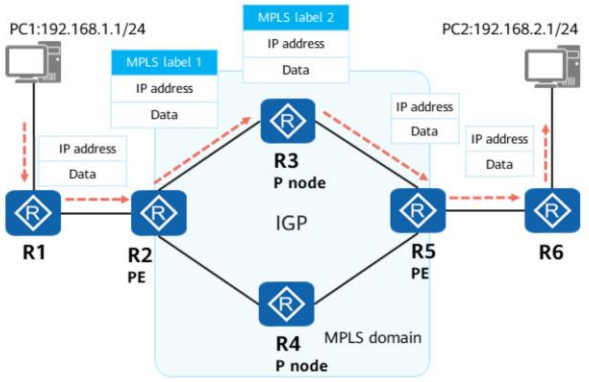
- Characteristics of traditional IP routing and forwarding:
  - All routers need to know the network-wide routes.
  - Traditional IP forwarding is connectionless-oriented and cannot provide good end-to-end QoS guarantee.

R1 routing table

Destination/Mask	Protocol	Preference	Cost	NextHop	Interface
192.168.1.0/24	Direct	0	0	192.168.1.254	GE 0/0/0
192.168.12.0/24	Direct	0	0	192.168.12.1	GE 0/0/2
192.168.2.0/24	OSPF	10	3	192.168.12.2	GE 0/0/2

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

MPLS Label-based Forwarding

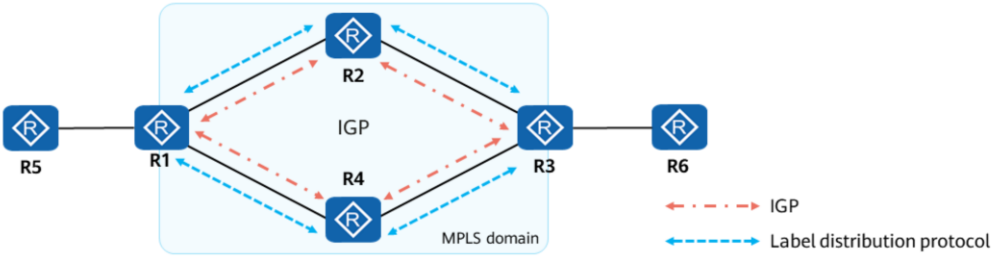


- MPLS is used on IP backbone networks.
- MPLS is a tunneling technology that provides connection-oriented switching for the network layer based on IP routing and control protocols. It provides better QoS guarantee.
- MPLS labels, instead of IP routes, are searched for to forward packets, which greatly improves forwarding efficiency.
- Labels used in MPLS forwarding can be manually configured or dynamically allocated using a label distribution protocol.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

MPLS Forwarding Problems

- MPLS labels can be statically or dynamically distributed. The involved problems are as follows:
  - Static label distribution requires manual configuration. As the network scale expands, network topologies are prone to change. Static label configuration cannot meet the requirements of large-scale networks.
  - Some dynamic label distribution protocols do not have the path computation capability and need to use IGPs to compute paths. In addition, the control planes of these protocols are complex, requiring devices to send a large number of messages to maintain peer and path status, wasting link bandwidth and device resources. What is more, despite supporting TE, some label distribution protocols require complex configurations and do not support load balancing. Devices have to send a large number of protocol packets to maintain proper paths. In addition, as devices are independent and know only their own status, they need to exchange signaling packets, which also waste link bandwidth and device resources.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

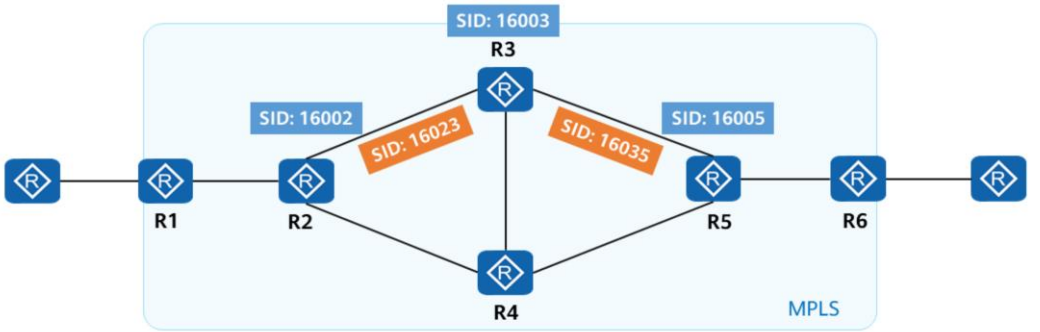
Introduction to Segment Routing

- To solve the problems facing traditional IP forwarding and MPLS forwarding, the industry proposed Segment Routing (SR). SR makes the following improvements:
  1. Extends the existing protocols.
     - The extended IGPs and BGP have the label distribution capability, eliminating the need for other label distribution protocols on networks, and thereby simplifying protocols.
  2. Introduces the source routing mechanism.
     - Using the source routing mechanism, controllers can centrally calculate paths.
  3. Allows networks to be defined by services.
     - Networks are driven by services. After service requirements, such as latency, bandwidth, and packet loss rate requirements, are raised by applications, a controller can collect information such as the network topology, bandwidth usage, and latency, and calculate explicit paths based on these requirements.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

SR Forwarding Implementation (1)

- SR divides a network path into segments and assigns segment IDs (SIDs) to these segments.
- SIDs are allocated to forwarding nodes or adjacency links. In this example, SIDs of the forwarding nodes are expressed in 1600X, where X is a node ID; SIDs of the adjacency links are expressed in 160XX, where XX indicates the node IDs at both ends of a link.

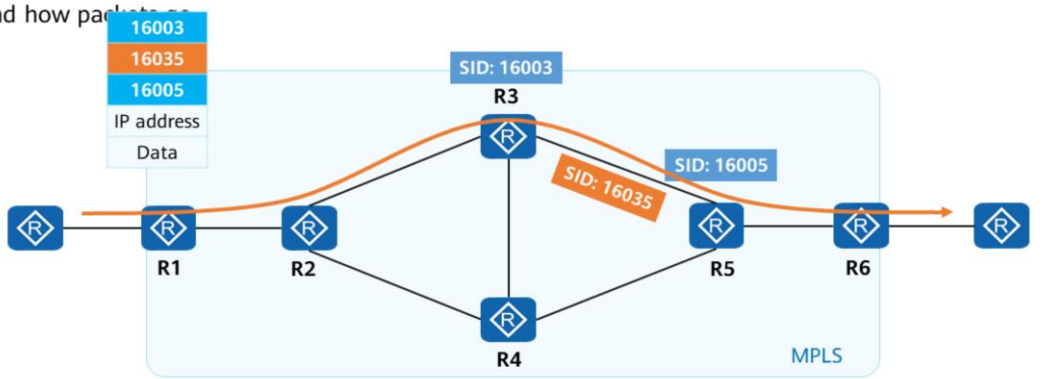


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- SIDs are used to identify segments. The format of SIDs depends on the implementation of technologies. For example, SIDs can be MPLS labels, indexes in an MPLS label space, or IPv6 packet headers. SR using MPLS labels is called SR-MPLS and using IPv6 is called SRv6.

SR Forwarding Implementation (2)

- SIDs of adjacency links and network nodes are arranged in order to form a segment list, which represents a forwarding path. The segment list is encoded by the source node in a header of a data packet, and is transmitted with the data packet. The essence of SR is instructions, which guide where and how pa

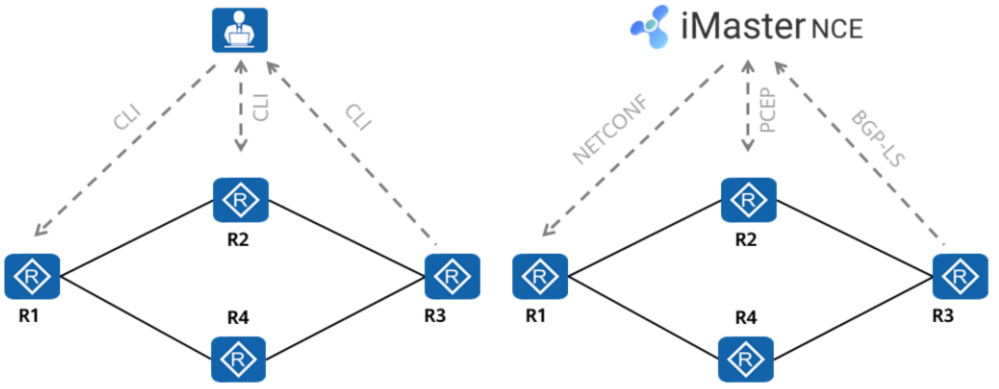


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- After receiving a packet, the receive end parses the segment list. If the top SID in the segment list identifies the local node, the node removes the SID and proceeds with the follow-up procedures. If the top SID does not identify the local node, the node forwards the packet to a next node in equal cost multiple path (ECMP) mode.

SR Deployment Modes

- SR can be deployed with or without a controller. If a controller is used, the controller collects information, reserves path resources, computes paths, and delivers the results to the source node. This mode is preferred.

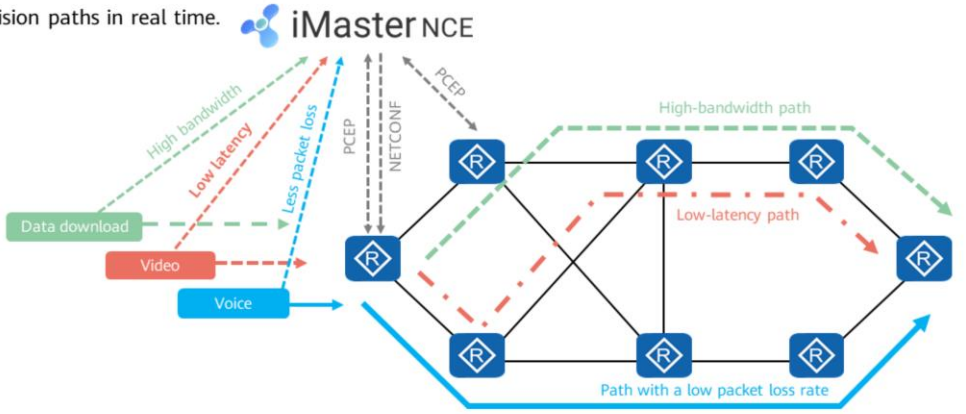


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- PCEP: Path Computation Element Communication Protocol
- NETCONF: Network Configuration Protocol

SR Application

- SR can be used to easily specify packet forwarding paths. On a live network, different paths can be defined for different services. In this example, three explicit paths are defined to implement the service-driven network: one each for data download, video, and voice services. Devices are managed by the controller, which can quickly provision paths in real time.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Quiz

1. (Multiple) Which of the following statements about PPP are true?
   A. PPP supports the bundling of multiple physical links into a logical link to increase the bandwidth.
   B. PPP supports cleartext and ciphertext authentication.
   C. PPP cannot be deployed on Ethernet links because of its poor scalability.
   D. PPP supports asynchronous and synchronous links for the physical layer.
   E. PPP supports multiple network layer protocols, such as IPCP.
2. (Single) After a PPPoE client sends a PADI packet to PPPoE servers, the PPPoE servers reply with a PADO packet. Which kind of frame is the PADO packet?
   A. A. Multicast B. Broadcast C. Unicast D. Anycast
3. (Single) Which of the following values of the Length/Type field in an Ethernet data frame indicates that the Ethernet data frame carries PPPoE discovery packets?
   A. A. 0x0800 B. 0x8864 C. 0x8863 D. 0x0806

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

1. ABDE
2. B
3. C

Summary

- This course reviews the types and applications of early WAN technologies and describes the evolution of WANs from the early circuit switching networks to IP networks, MPLS label switching network, and finally to SR networks. With the development of network technologies, networks become more efficient and intelligent.
- The course also describes the implementation of PPP, including parameter negotiation during PPP link establishment, authentication negotiation, and network layer negotiation. It analyzes in detail two PPP authentication protocols – PAP and CHAP, and describes their working processes and differences.
- PPPoE is the most widely used PPP application. By analyzing how a PPPoE session is discovered, negotiated, established, and torn down, this course help you better understand the working mechanism and configuration of PPPoE.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

More Information

- (Multimedia) Segment Routing MPLS Advanced Series
  - https://support.huawei.com/carrier/docview?nid=DOC1100645168&path=PBI1-7275726/PBI1-21782273/PBI1-7275849/PBI1-7276518/PBI1-15837
- (Multimedia) Segment Routing IPv6 Advanced Series
  - https://support.huawei.com/enterprise/en/doc/EDOC1100133514?idPath=24030814%7C9856750%7C22715517%7C9858933%7C15837

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Network Management and O&M

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- The ever expanding network and increasing network devices present a significant challenge in managing networks effectively and providing high-quality network services.
- There are many network management and O&M methods, of which this course describes some of the most common.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Understand basic concepts of network management and O&M.
  - Master common network management and O&M methods.
  - Describe basic functions of network management and O&M.
  - Understand the fundamentals of SNMP.
  - Understand Huawei iMaster NCE and related technologies.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

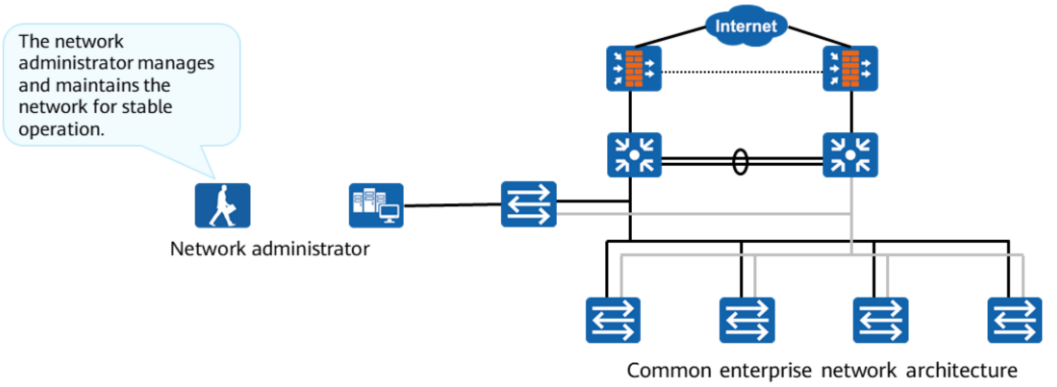
1. **Basic Concepts of Network Management and O&M**
2. SNMP Fundamentals and Configuration
3. Network Management Based on Huawei iMaster NCE

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

What Is Network Management and O&M?

- Network management and O&M plays an important role on a communications network. It ensures that devices work properly and the communications network runs properly to provide efficient, reliable, and secure communications services.



Common enterprise network architecture

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Network management and O&M is classified as software management or hardware management.
  - Software management: management of network applications, user accounts (such as accounts for using files), and read and write permissions. This course does not describe software management in detail.
  - Hardware management: management of network elements (NEs) that constitute the network, including firewalls, switches, routers, and other devices. This course mainly describes hardware management.
- Generally, an enterprise network has dedicated departments or personnel responsible for network management and O&M.
- Note:
  - A network element (NE) refers to a hardware device and software running on the hardware device. An NE has at least one main control board that manages and monitors the entire NE. The NE software runs on the main control board.

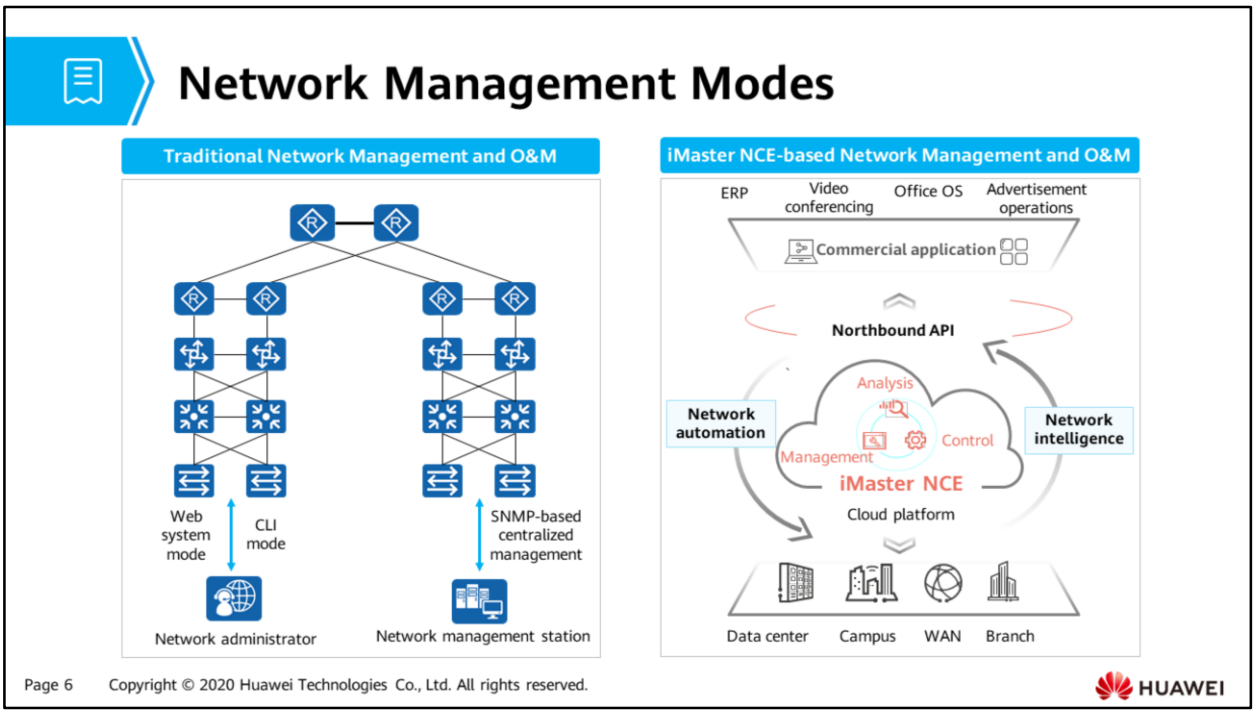
Basic Network Management Functions



OSI defines five functional models for network management:

- Configuration management: monitors network configuration information so that network administrators can generate, query, and modify hardware and software running parameters and conditions, and configure services.
- Performance management: manages network performance so that the network can provide reliable, continuous, and low-latency communication capabilities with as few network resources as possible.
- Fault management: ensures that the network is always available and rectifies faults as soon as possible.
- Security management: protects networks and systems from unauthorized access and attacks.
- Accounting management: records the network resource usage of users, charges users, and collects statistics on network resource usage.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Traditional network management:
  - Web system: The built-in web server of the device provides a graphical user interface (GUI). You need to log in to the device to be managed from a terminal through Hypertext Transfer Protocol Secure (HTTPS).
  - CLI mode: You can log in to a device through the console port, Telnet, or SSH to manage and maintain the device. This mode provides refined device management but requires that users be familiar with command lines.
  - SNMP-based centralized management: The Simple Network Management Protocol (SNMP) provides a method for managing NEs (such as routers and switches) by using a central computer (that is, a network management station) that runs network management software. This mode provides centralized and unified management of devices on the entire network, greatly improving management efficiency.
- iMaster NCE-based network management:
  - iMaster NCE is a network automation and intelligence platform that integrates management, control, analysis, and AI functions. It provides four key capabilities: full-lifecycle automation, intelligent closed-loop management based on big data and AI, scenario-specific app ecosystem enabled by open programmability, and all-cloud platform with ultra-large system capacity.
  - iMaster NCE uses protocols such as Network Configuration Protocol (NETCONF) and RESTCONF to deliver configurations to devices and uses telemetry to monitor network traffic.

Contents

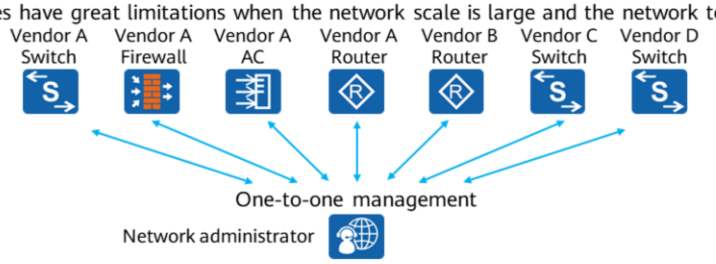
1. Basic Concepts of Network Management and O&M
2. **Traditional Network Management**
3. Network Management Based on Huawei iMaster NCE

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Management Through the CLI or Web System

- When the network scale is small, the CLI and web system are generally used for network management.
  - Network administrators can log in to a device through HTTPS, Telnet, or the console port to manage the device.
  - These network management modes do not require any program or server to be installed on the network, and the cost is low.
  - Network administrators must have a good master of network knowledge and vendor-specific network configuration commands.
  - These modes have great limitations when the network scale is large and the network topology is complex.

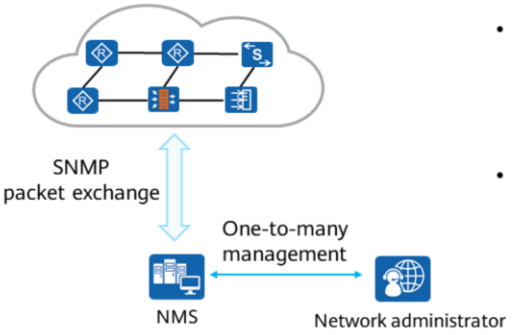


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- As networks rapidly expand and applications become more diversified, network administrators face the following problems:
  - The fast growth of network devices increases network administrators' workloads. In addition, networks' coverage areas are constantly being expanded, making real-time monitoring and fault locating of network devices difficult.
  - There are various types of network devices and the management interfaces (such as command line interfaces) provided by different vendors vary from each other, making network management more complex.

SNMP-based Centralized Management

- SNMP is a standard network management protocol widely used on TCP/IP networks. It provides a method for managing NEs through a central computer that runs network management software, that is, a network management station.

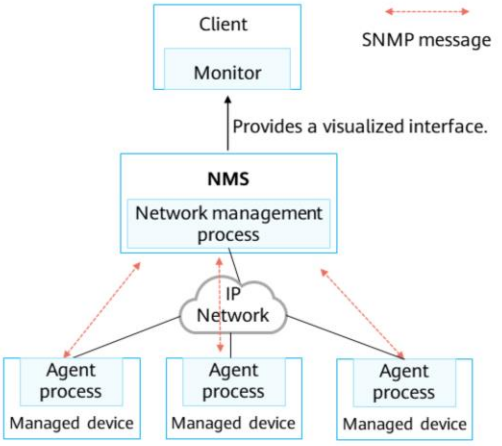


- Network administrators can use the NMS to query information, modify information, and troubleshoot faults on any node on the network, improving work efficiency.
- Network devices of different types and vendors are managed in a unified manner.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- There are three SNMP versions: SNMPv1, SNMPv2c, and SNMPv3.
  - In May 1990, RFC 1157 defined the first SNMP version: SNMPv1. RFC 1157 provides a systematic method for monitoring and managing networks. SNMPv1 implements community name-based authentication, failing to provide high security. In addition, only a few error codes are returned in SNMPv1 packets.
  - In 1996, the Internet Engineering Task Force (IETF) released RFC 1901 in which SNMPv2c is defined. SNMPv2c provides enhancements to standard error codes, data types (Counter 64 and Counter 32), and operations including GetBulk and Inform.
  - SNMPv2c still lacks security protection measures, so IETF released SNMPv3. SNMPv3 provides user security module (USM)-based encryption and authentication and a view-based access control model (VACM).

Typical SNMP Architecture

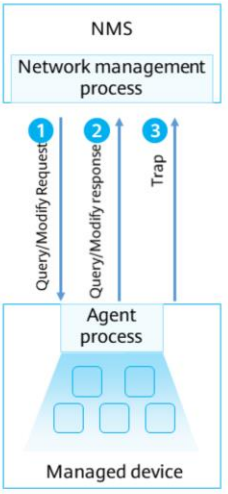


- On a network where SNMP is used for network management, a network management system (NMS) functions as a network management center and runs management processes. Each managed device needs to run an agent process. The management process and agent process communicate with each other through SNMP messages.
- An NMS is a system that uses SNMP to manage and monitor network devices. The NMS software runs on NMS servers.
- Managed devices are devices that are managed by the NMS on the network.
- The agent process runs on managed devices to maintain the information data of the managed devices, respond to the request from the NMS, and report the management data to the NMS that sends the request.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- An NMS is an independent device that runs network management programs. The network management programs provide at least one man-machine interface for network administrators to perform network management operations. Web page interaction is a common man-machine interaction mode. That is, a network administrator uses a terminal with a monitor to access the web page provided by the NMS through HTTP/HTTPS.

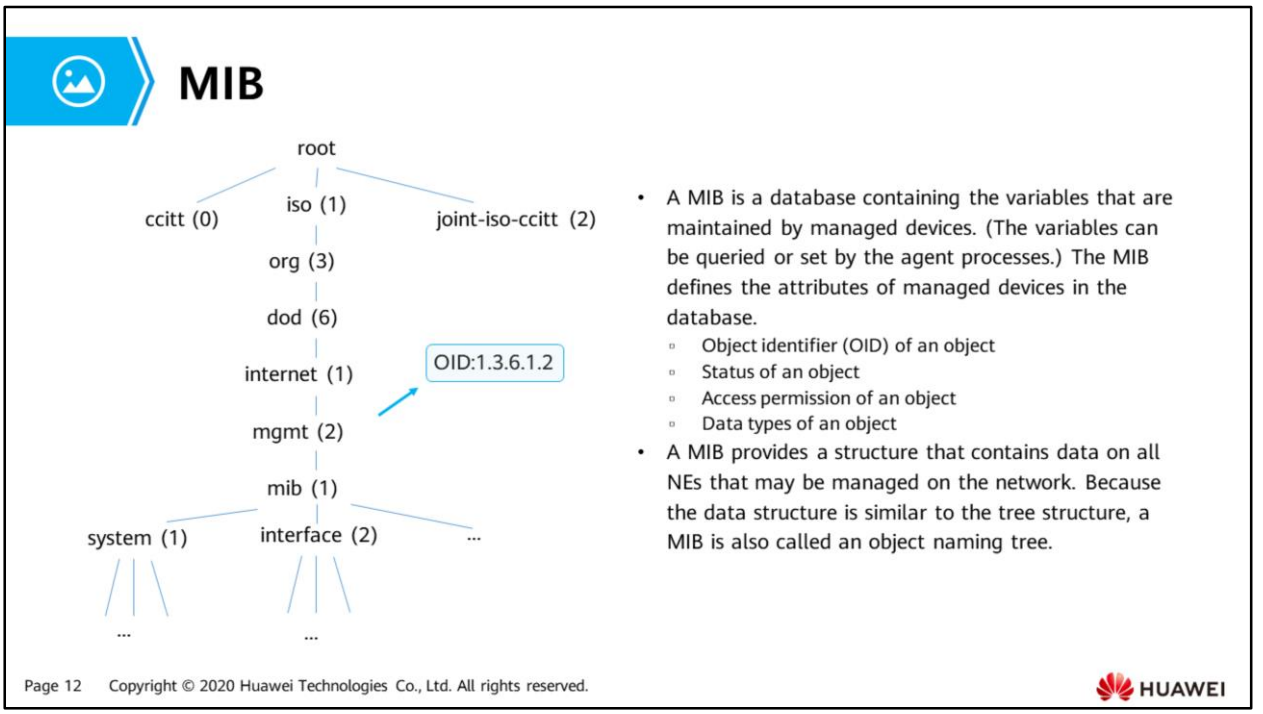
SNMP Message Exchange



Managed object

- The NMS and managed devices exchange messages in the following modes:
  - The NMS sends a request for modifying or querying configuration information to a managed device through SNMP. The agent process running on the managed device responds to the request from the NMS.
  - The managed device can proactively report traps to the NMS so that the network administrator can detect faults in a timely manner.
- Managed object: Each device may contain multiple managed objects. A managed object can be a hardware component or a set of parameters configured on the hardware or software (such as a routing protocol).
- SNMP uses management information bases (MIBs) to describe a group of objects of a manageable entity.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- MIB is defined independently of a network management protocol. Device vendors can integrate SNMP agent software into their products (for example, routers), but they must ensure that this software complies with relevant standards after new MIBs are defined. You can use the same network management software to manage routers containing MIBs of different versions. However, the network management software cannot manage a router that does not support the MIB function.
- There are public MIBs and private MIBs.
  - Public MIBs: defined by RFCs and used for structure design of public protocols and standardization of interfaces. Most vendors need to provide SNMP interfaces according to the specifications defined in RFCs.
  - Private MIBs: They are the supplement of the public MIBs. Some enterprises need to develop private protocols or special functions. The private MIBs are designed to enable the SNMP interface to manage such protocols or functions. They also help the NMS provided by the third party to manage devices. For example, the MIB object of Huawei is 1.3.6.1.4.1.2011.

Common MIB Objects

- Objects used for query or modification:

OID	Object Name	Data Type	Maximum Access	Description
1.3.6.1.2.1.2.1	ifNumber	Integer	read-only	Number of network interfaces in the system (regardless of the current interface status)
1.3.6.1.4.1.2011.5.25.41.1.2.1.1.3	hwIpAdEntNetMask	IpAddress	read-create	Subnet mask of an IP address

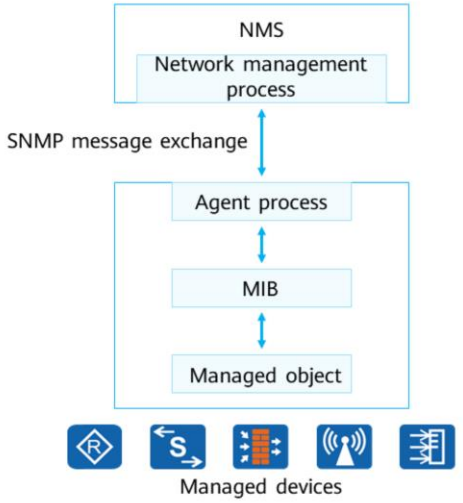
- Objects used for alarm notification:

OID	Object Name	Bound Variable	Description
3.6.1.6.3.1.1.5.3	linkDown	ifIndex ifAdminStatus ifOperStatus ifDesc	It is detected that one of the communication links in the ifOperStatus object has entered the down state from another state (but not the notPresent state). The original state is indicated by the value of ifOperStatus.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

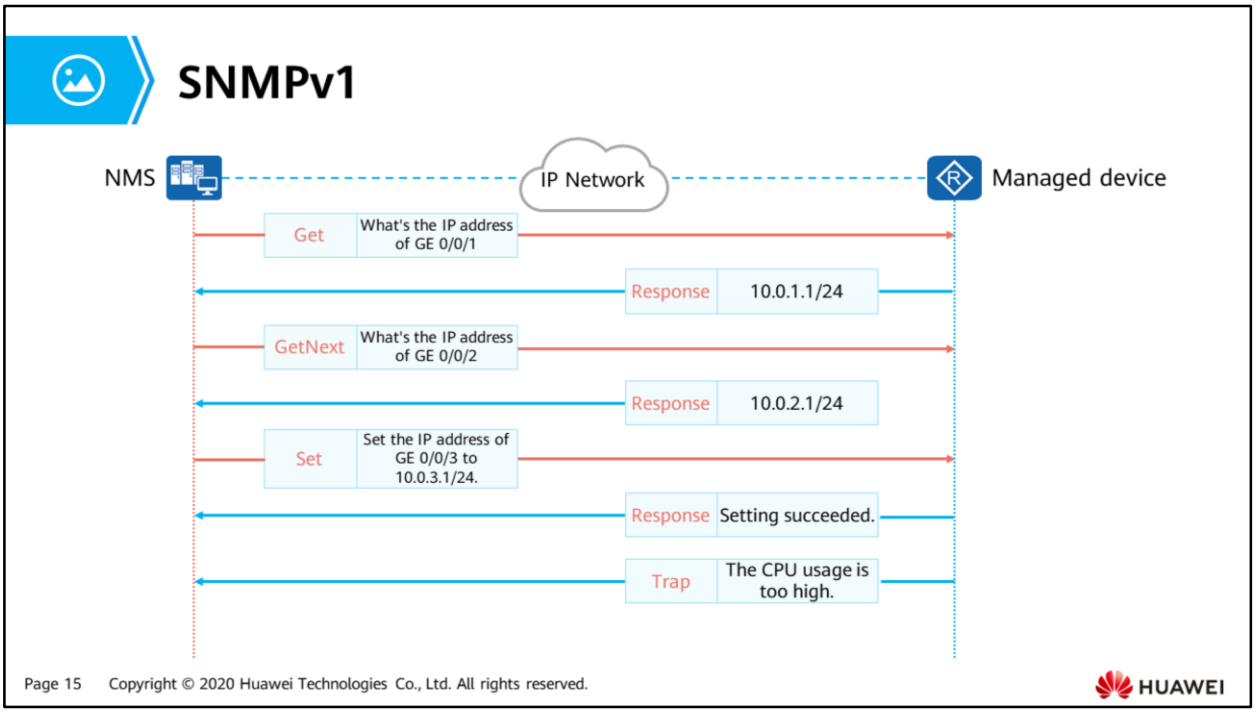
- The maximum access permission of a MIB object indicates the operations that the NMS can perform on the device through the MIB object.
  - not-accessible: No operation can be performed.
  - read-only: reads information.
  - read-write: reads information and modifies configurations.
  - read-create: reads information, modifies configurations, adds configurations, and deletes configurations.
- When generating a trap, the device reports the type of the current trap together with some variables. For example, when sending a linkDown trap, the device also sends variables such as the interface index and current configuration status of the involved interface.
  - ifIndex: interface index (number)
  - ifAdminStatus: indicates the administrative status, that is, whether the interface is shut down. 1 indicates that the interface is not shut down, and 2 indicates that the interface is shut down.
  - ifOperStasuts: indicates the current operating status of the interface, that is, the link layer protocol status of the interface. The value 1 indicates Up, 2 indicates Down.
  - ifDesc: interface description

SNMP Management Model

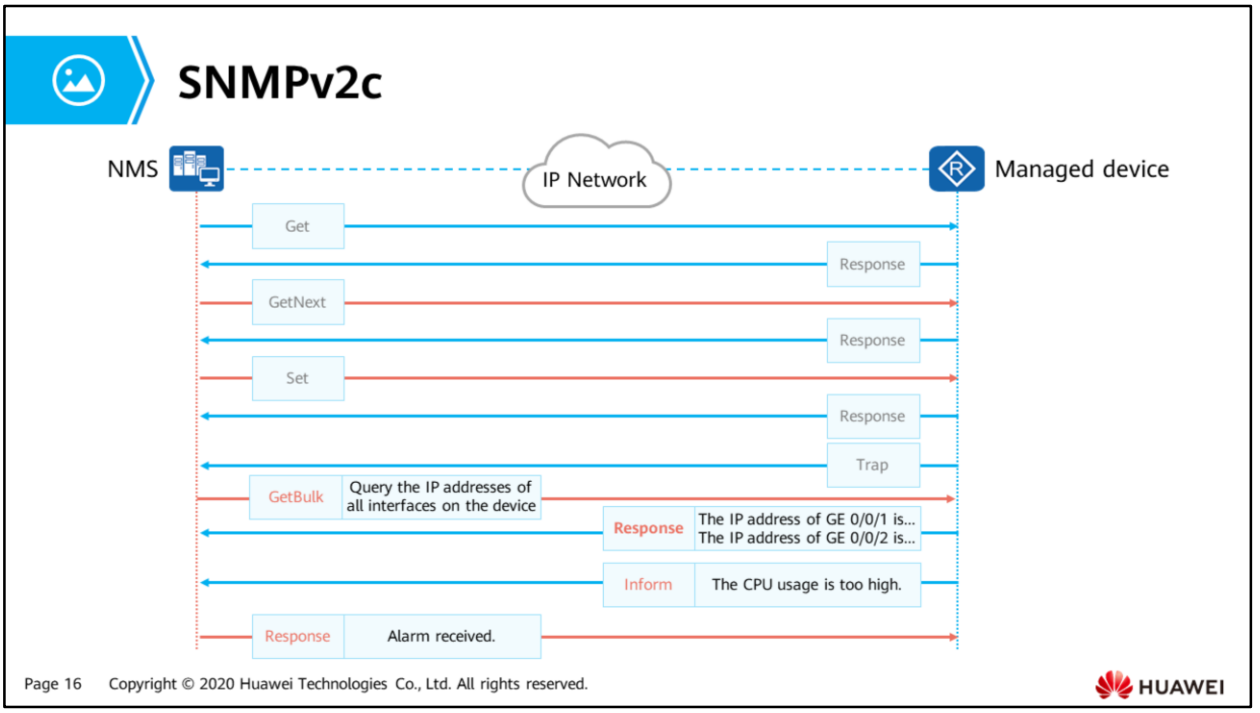


- Query/Modify operation:
  - The NMS sends an SNMP request message to an agent process.
  - The agent process searches the MIB on the device for information to be queried or modified and sends an SNMP response message to the NMS.
- Trap operation:
  - If the trap triggering conditions defined for a module are met, the agent process sends a message to notify the NMS that an event or trap has occurred on a managed object. This helps network administrators promptly process network faults.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



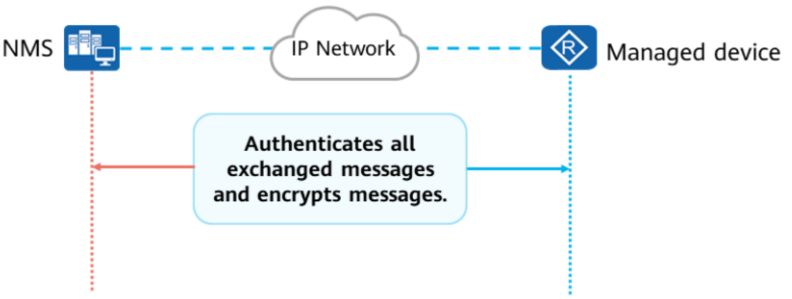
- SNMPv1 defines five protocol operations.
  - Get-Request: The NMS extracts one or more parameter values from the MIB of the agent process on the managed device.
  - Get-Next-Request: The NMS obtains the next parameter value from the MIB of the agent process in lexicographical order.
  - Set-Request: The NMS sets one or more parameter values in the MIB of the agent process.
  - Response: The agent process returns one or more parameter values. It is the response to the first three operations.
  - Trap: The agent process sends messages to the NMS to notify the NMS of critical or major events.



- SNMPv2c supports the following operations:
  - GetBulk: equals to multiple GetNext operations. You can set the number of GetNext operations to be included in one GetBulk operation.
  - Inform: A managed device proactively sends traps to the NMS. In contrast to the trap operation, the inform operation requires an acknowledgement. After a managed device sends an InformRequest message to the NMS, the NMS returns an InformResponse message. If the managed device does not receive the acknowledgment message, it temporarily saves the trap in the Inform buffer and resends the trap until the NMS receives the trap or the number of retransmission times reaches the maximum.

SNMPv3

- SNMPv3 has the same working mechanism as SNMPv1 and SNMPv2c, but adds header data and security parameters.
- SNMPv3 messages can be authenticated and encrypted.
- SNMPv3 is applicable to networks of various scales and has high security.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- SNMPv3 supports identity authentication and encryption.
  - Identity authentication: A process in which the agent process (or NMS) confirms whether the received message is from an authorized NMS (or agent process) and whether the message is changed during transmission.
  - Encryption: The header data and security parameter fields are added to SNMPv3 messages. For example, when the management process sends an SNMPv3 Get-Request message carrying security parameters such as the username, key, and encryption parameters, the agent process also uses an encrypted response message to respond to the Get-Request message. This security encryption mechanism is especially applicable to a scenario in which data needs to be transmitted through a public network between the management process and agent process.

SNMP Summary

- SNMP has the following advantages:
  - Simplicity: SNMP is applicable to networks that require high speed and low cost because it uses a polling mechanism and provides basic network management functions. Moreover, SNMP uses UDP to exchange data and therefore is supported by most products.
  - Convenience: SNMP allows management information exchange between arbitrary devices on a network, so that a network administrator can query information and locate faults on any device.
- SNMPv1 applies to small-scale networks where security requirements are not high or the network environment is safe and stable, such as campus networks and small-sized enterprise networks.
- SNMPv2c applies to medium- and large-sized networks where security requirements are not high or the network environment is safe, but a large volume of traffic exists and traffic congestion may occur.
- SNMPv3 is the recommended version and applies to networks of various scales, especially those networks that have high security requirements and allow only authorized administrators to manage network devices.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic SNMP Configuration (1)

1. Enable the SNMP agent function.

   [Huawei] **snmp-agent**

2. Set the SNMP version.

   [Huawei] **snmp-agent sys-info version [v1 | v2c | v3]**

   You can configure the SNMP version as required. However, the protocol version used on the device must be the same as that used on the NMS.

3. Create or update MIB view information.

   [Huawei] **snmp-agent mib-view** *view-name* { **exclude** | **include** } *subtree-name* [**mask** *mask*]

4. Add a new SNMP group and map users in this group to the SNMP view.

   [Huawei] **snmp-agent group v3** *group-name* **{ authentication | noauth | privacy } [read-view** *view-name* **| write-view** *view-name* **| notify-view** *view-name* **]**

   This command is used to create an SNMP group of the SNMPv3 version and specify the authentication and encryption mode and one or more of read-only view, read-write view, and notification view. It is a mandatory command on networks that require high security.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic SNMP Configuration (2)

5. Add a user to the SNMP group.

```
[Huawei] snmp-agent usm-user v3 user-name group group-name
```

6. Configure an authentication password for an SNMPv3 user.

```
[Huawei] snmp-agent usm-user v3 user-name  authentication-mode { md5 | sha | sha2-256 }
```

7. Configure the SNMPv3 user encryption password.

```
[Huawei] snmp-agent usm-user v3 user-name privacy-mode { aes128 | des56 }
```

8. Set parameters for the device to send traps.

```
[Huawei] snmp-agent target-host trap-paramsname paramsname v3 securityname securityname {
authentication | noauthnopriv | privacy }
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic SNMP Configuration (3)

9. Configure the target host of traps.

```
[Huawei] snmp-agent target-host trap-hostname hostname address ipv4-address trap-paramsname paramsname
```

10. Enable all trap functions.

```
[Huawei] snmp-agent trap enable
```

Note that this command is used only to enable the device to send traps. This command must be used together with the **snmp-agent target-host** command. The **snmp-agent target-host** command specifies the device to which traps are sent.

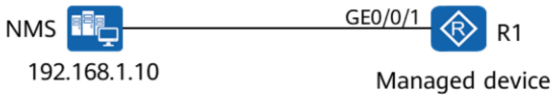
11. Configure the source interface that sends traps.

```
[Huawei] snmp-agent trap source interface-type interface-number
```

Note that a source IP address must have been configured for the interface that sends traps.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

SNMP Configuration Example (Network Device Side)



- Enable SNMP on R1and set the SNMP version to SNMPv3.
- Set the SNMPv3 group name to **test** and encryption authentication mode to **privacy**.
- Create an SNMPv3 user named **R1** and set the authentication and encryption passwords to **HCIA-Datacom123**.
- Create a trap parameter named **param** and set securityname to **sec**.
- Set the IP address of the SNMP target host to 192.168.1.10.
- Enable the trap function and specify GE 0/0/1 as the source interface that sends traps.

```
R1configuration:
[R1]snmp-agent
[R1]snmp-agent sys-info version v3
[R1]snmp-agent group v3 test privacy
[R1]snmp-agent usm-user v3 R1 test authentication-
mode md5 HCIA@Datacom123 privacy-mode aes128
HCIA-Datacom123
[R1]snmp-agent target-host trap-paramsname param v3
securityname sec privacy
[R1]snmp-agent target-host trap-hostname nms address
192.168.1.10 trap-paramsname param
[R1]snmp-agent trap source GigabitEthernet 0/0/1
[R1]snmp-agent trap enable
Info: All switches of SNMP trap/notification will be open.
Continue? [Y/N]:y
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

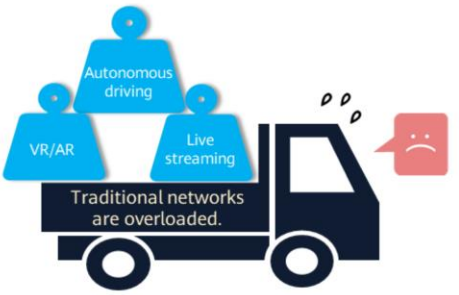
1. Basic Concepts of Network Management and O&M
2. Traditional Network Management
3. **Network Management Based on Huawei iMaster NCE**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Transformation and Challenges of the Network Industry

- With the advent of the 5G and cloud era, innovative services such as VR/AR, live streaming, and autonomous driving are emerging, and the entire ICT industry is booming. At the same time, the traffic of the entire network also increases explosively. Huawei Global Industry Vision (GIV) predicts that the amount of new data will reach 180 ZB by 2025. Moreover, the dynamic complexity of services makes the entire network more complex.
- Such challenges can only be overcome by constructing automated and intelligent network systems centered on user experience.

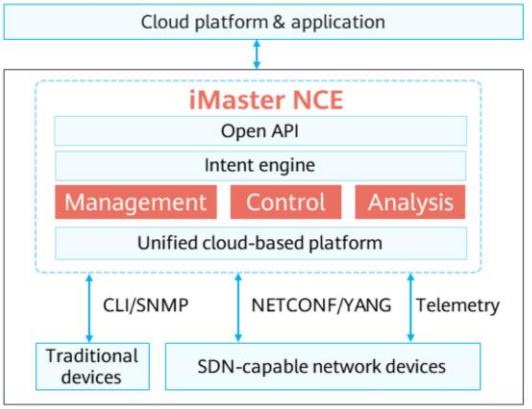


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- One zettabyte (abbreviated "ZB") is equal to 10^{12} GB.

Huawei iMaster NCE

- Huawei iMaster NCE is a network automation and intelligence platform that integrates management, control, analysis, and AI functions.



- In terms of management and control, iMaster NCE allows you to:
  - Manage and control traditional devices through traditional technologies such as CLI and SNMP.
  - Manage and control SDN-capable networks through NETCONF (based on the YANG model).
- iMaster NCE collects network data through protocols such as SNMP and telemetry, performs intelligent big data analysis based on AI algorithms, and displays device and network status in multiple dimensions through dashboards and reports, helping O&M personnel quickly detect and handle device and network exceptions and ensuring normal running of devices and networks.

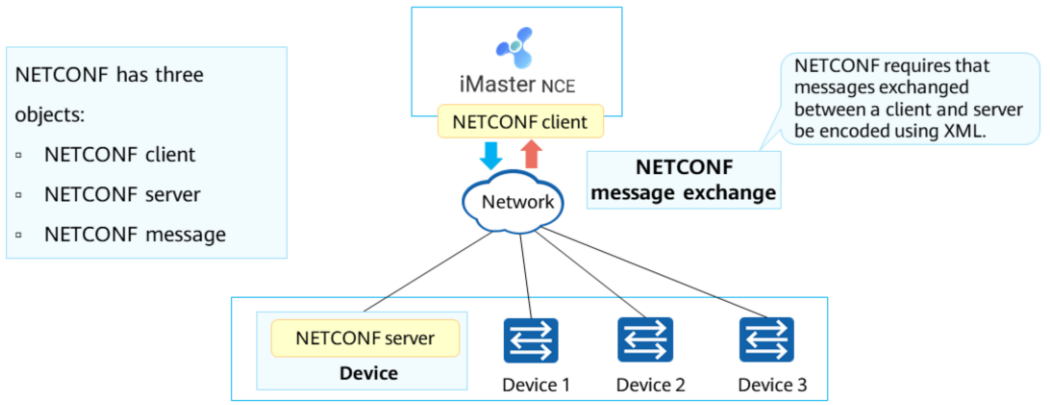
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- iMaster NCE provides the following key capabilities:
  - Full-lifecycle automation: iMaster NCE provides full-lifecycle automation across multiple network technologies and domains based on unified resource modeling and data sharing, enabling device plug-and-play, immediate network availability after migration, on-demand service provisioning, fault self-healing, and risk warning.
  - Intelligent closed-loop management based on big data and AI: iMaster NCE constructs a complete intelligent closed-loop system based on its intent engine, automation engine, analytics engine, and intelligence engine. It also uses telemetry to collect and aggregate massive volumes of network data. This allows it to determine the network status in real time. iMaster NCE provides big data-based global network analysis and insights through unified data modeling, and is equipped with Huawei's sophisticated AI algorithms accumulated during its 30 years in the telecom industry. It provides automated closed-loop analysis, forecast, and decision-making based on customers' intents. This helps improve user experience and continuously enhance network intelligence.

- Open programmability-enabled scenario-based application ecosystem: In the southbound direction, iMaster NCE provides a programmable integrated development environment — Design Studio — and a developer community for integration with third-party network controllers and devices; in the northbound direction, it provides cloud-based AI training platforms and IT applications. iMaster NCE allows customers to purchase Huawei native apps on demand, develop their own apps, and turn to third-party system integrators for app development.
- Large-capacity cloud platform: iMaster NCE, with cloud-native architecture, supports both on-premises deployment and cloud-based deployment. With elastic scalability, it can provide large system capacity to allow a large number of access users. With online data sharing and process streamlining, it avoids scattered data distribution and multi-level O&M in offline mode.

NETCONF Overview

- NETCONF provides a network device management mechanism. You can use NETCONF to add, modify, or delete configurations of network devices, and obtain configurations and status of network devices.



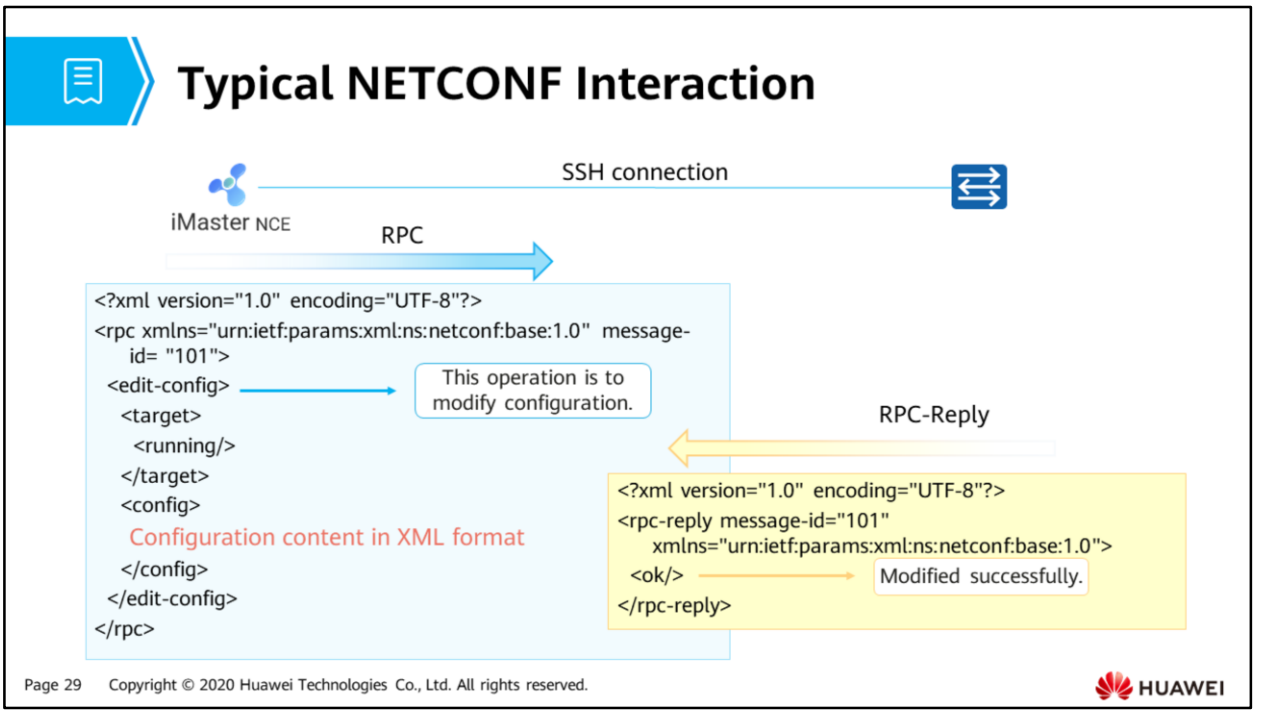
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- NETCONF client: manages network devices using NETCONF. Generally, the NMS functions as the NETCONF client. It sends <rpc> elements to a NETCONF server to query or modify configuration data. The client can learn the status of a managed device based on the traps and events reported by the server.
- NETCONF server: maintains information about managed devices, responds to requests from clients, and reports management data to the clients. NETCONF servers are typically network devices, for example, switches and routers. After receiving a request from a client, a server parses data, processes the request with the assistance of the Configuration Manager Frame (CMF), and then returns a response to the client. If a trap is generated or an event occurs on a managed device, the NETCONF server reports the trap or event to the client through the Notification mechanism, so the client can learn the status change of the managed device.
- A client and a server establish a connection based on a secure transmission protocol such as Secure Shell (SSH) or Transport Layer Security (TLS), and establish a NETCONF session after exchanging capabilities supported by the two parties using Hello packets. In this way, the client and the server can exchange messages. A network device must support at least one NETCONF session. The data that a NETCONF client obtains from a NETCONF server can be configuration data or status data.

NETCONF Advantages

Function	NETCONF	SNMP	CLI
Interface type	Machine-machine interface: The interface definition is complete and standard, and the interface is easy to control and use.	Machine-to-machine interface	Man-machine interface
Operation efficiency	High: Object-based modeling is supported. Only one interaction is required for object operations. Operations such as filtering and batch processing are supported.	Medium	Low
Scalability	Proprietary protocol capabilities can be extended.	Weak	Moderate
Transaction	Supports transaction processing mechanisms such as trial running, rollback upon errors, and configuration rollback.	Not supported	Partially supported
Secure transmission	Multiple security protocols: SSH, TLS, BEEP/TLS, and SOAP/HTTP/TLS	Only SNMPv3 supports secure transmission.	SSH

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- NETCONF uses SSH to implement secure transmission and uses Remote Procedure Call (RPC) to implement communication between the client and server.

YANG Language Overview

- Yet Another Next Generation (YANG) is a data modeling language that standardizes NETCONF data content.
- The YANG model defines the hierarchical structure of data and can be used for NETCONF-based operations. Modeling objects include configuration, status data, remote procedure calls, and notifications. This allows a complete description of all data exchanged between a NETCONF client and server.

A model is an abstraction and expression of things.

A data model is an abstraction and expression of data features.

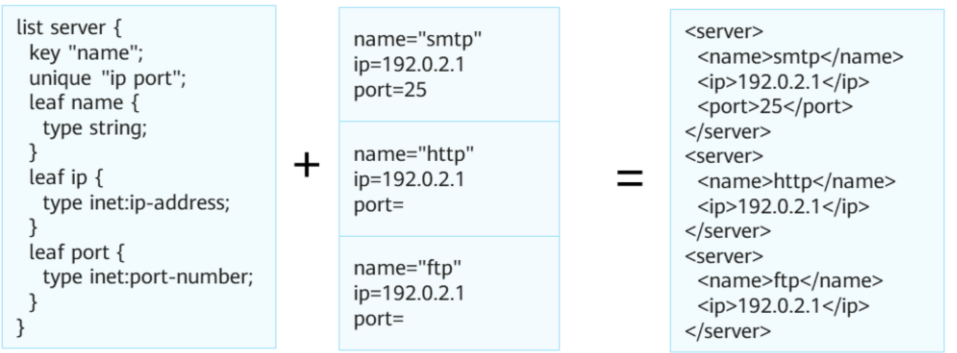


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- YANG originates from NETCONF but is not only used for NETCONF. Although the YANG modeling language is unified, YANG files are not unified.
- YANG files can be classified into the following types:
  - Vendor's proprietary YANG file
  - IETF standard YANG
  - OpenConfig YANG
- The YANG model is presented as a **.yang** file.
- The YANG model has the following characteristics:
  - Hierarchical tree-like structure modeling.
  - Data models are presented as modules and sub-modules.
  - It can be converted to the YANG Independent Notation (YIN) model based on the XML syntax without any loss.
  - Defines built-in data types and extensible types.

YANG and XML (1)

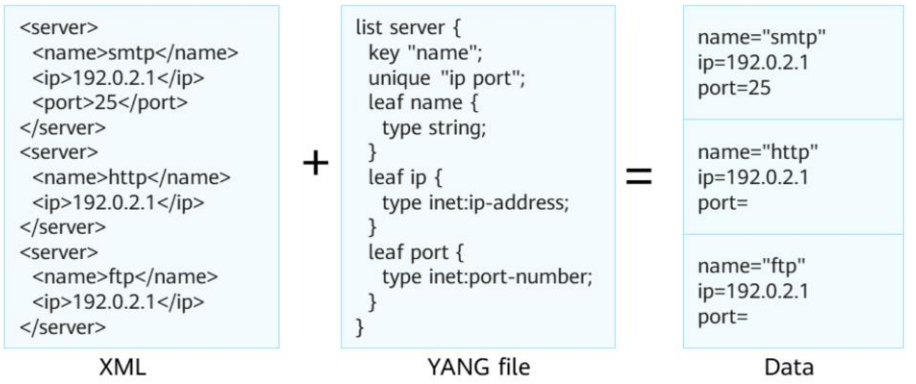
- A YANG file is loaded on the NETCONF client (such as the NMS or SDN controller).
- The YANG file is used to convert data into XML-format NETCONF messages before they are sent to the device.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

YANG and XML (2)

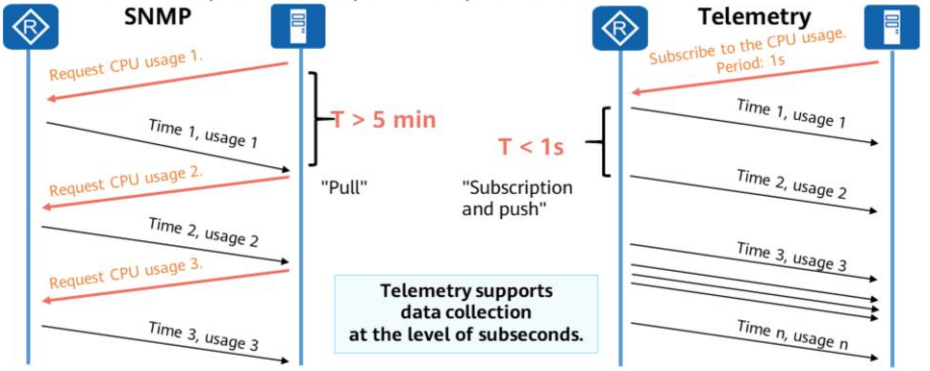
- A YANG file is loaded on the NETCONF server (such as a router or switch).
- The YANG file is used to convert received XML-format NETCONF messages into data for subsequent processing.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Telemetry Overview

- Telemetry, also called network telemetry, is a technology that remotely collects data from physical or virtual devices at a high speed.
- Devices periodically send interface traffic statistics, CPU usage, and memory usage to collectors in push mode. Compared with the traditional pull mode, the push mode provides faster and more real-time data collection.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- There is also a view in the industry that SNMP is considered as a traditional telemetry technology, and the current telemetry is referred to as streaming telemetry or model-driven telemetry.
- Telemetry packs the data to be sent, improving transmission efficiency.

Quiz

1. (Single) On an SNMP-based network, which of the following runs the management process to manage the managed devices? ( )
   A. NMS
   B. Agent process
   C. MIB
   D. SNMP
2. (Single) In SNMPv1, which of the following operations is used by a managed device to report traps? ( )
   A. Get-Request
   B. Set-Request
   C. Trap
   D. Response

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. A
2. C

Quiz

3. YANG is a data modeling language. ( )
   A. True
   B. False
4. Telemetry supports data collection at the level of subseconds. ( )
   A. True
   B. False

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

3. A
4. A

Summary

- With the development of network technologies, more and more network management and O&M methods are available. The common methods are as follows:
  - CLI mode or web system
  - SNMP
  - Huawei iMaster NCE's intelligent O&M platform (covering management, control, and analysis)

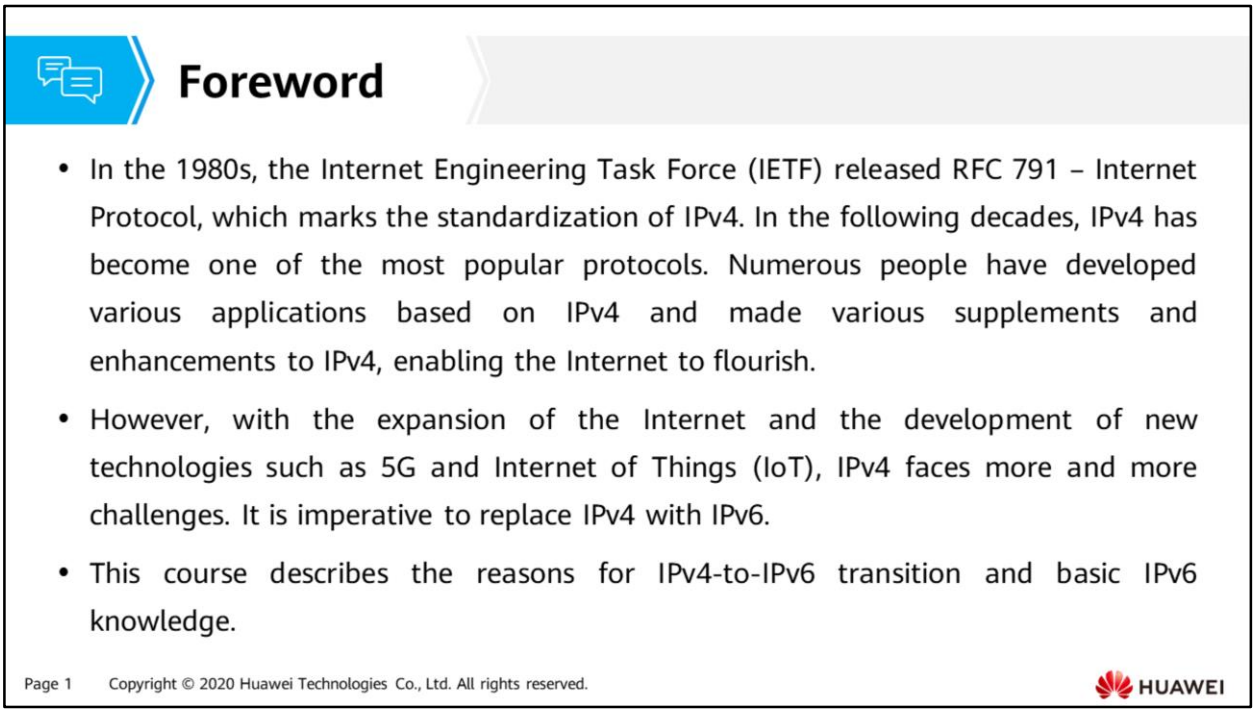
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



IPv6 Basics

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Internet Protocol version 4 (IPv4): a current IP version. An IPv4 address is 32 bits in length and is usually represented by four octets written in dotted decimal notation. Each IPv4 address consists of a network number, an optional subnet number, and a host number. The network and subnet numbers together are used for routing, and the host number is used to address an individual host within a network or subnet.
- Internet Protocol version 6 (IPv6): a set of specifications designed by the IETF. It is an upgraded version of IPv4. IPv6 is also called IP Next Generation (IPng). IPv6 addresses are extended to 128 bits in length.

Objectives

- On completion of this course, you will be able to:
  - Summarize the advantages of IPv6 over IPv4.
  - Describe the basic concepts of IPv6.
  - Describe the formats and functions of IPv6 packet headers.
  - Describe the IPv6 address format and address types.
  - Describe the method and basic procedure for configuring IPv6 addresses.
  - Configure IPv6 addresses and IPv6 static routes.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

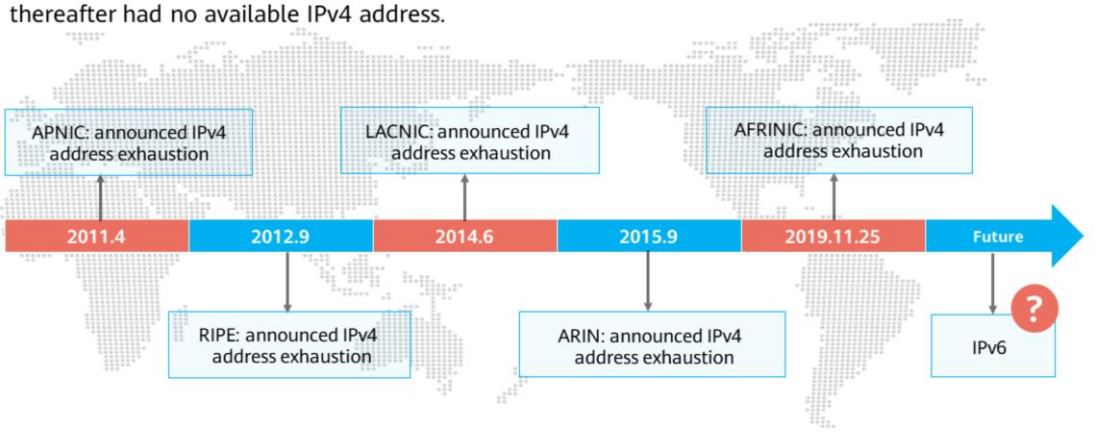
1. **IPv6 Overview**
2. IPv6 Address Configuration
3. Typical IPv6 Configuration Examples

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

IPv4 Status

- On February 3, 2011, the Internet Assigned Numbers Authority (IANA) announced even allocation of its last 4.68 million IPv4 addresses to five Regional Internet Registries (RIRs) around the world. The IANA thereafter had no available IPv4 address.



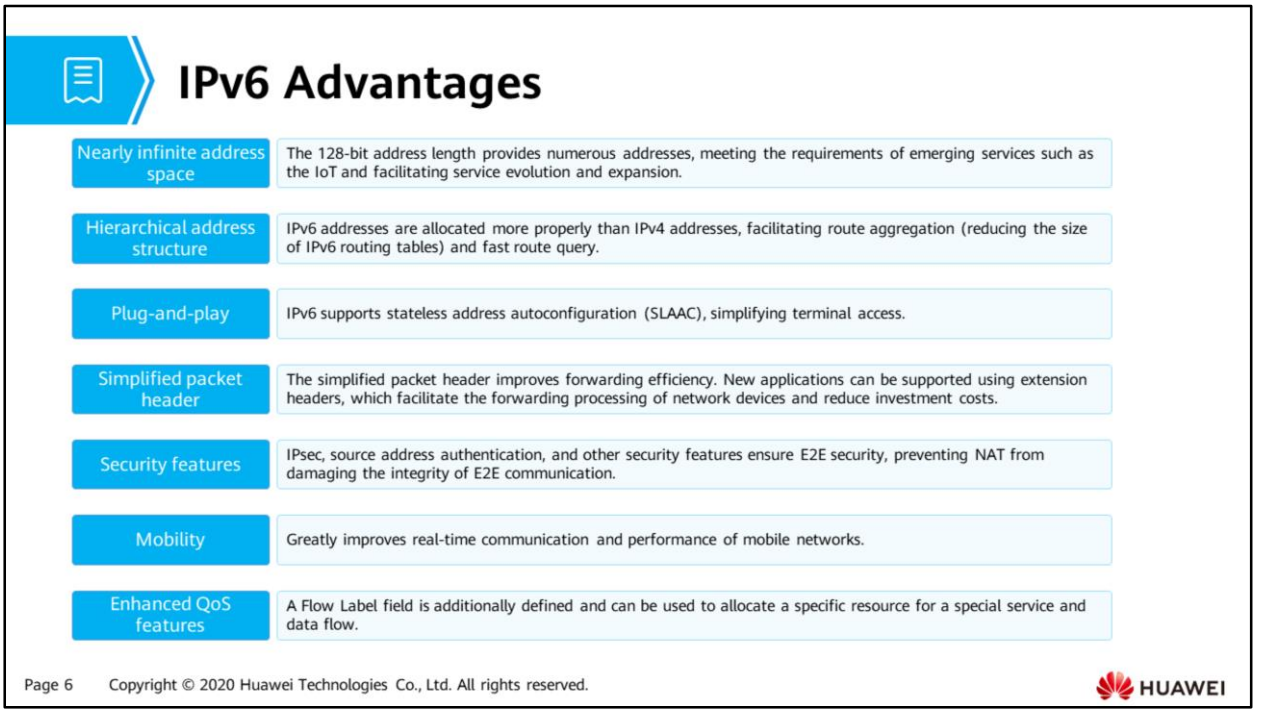
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- The IANA is responsible for assigning global Internet IP addresses. The IANA assigns some IPv4 addresses to continent-level RIRs, and then each RIR assigns addresses in its regions. The five RIRs are as follows:
  - RIPE: Reseaux IP Europeans, which serves Europe, Middle East, and Central Asia.
  - LACNIC: Latin American and Caribbean Internet Address Registry, which serves the Central America, South America, and the Caribbean.
  - ARIN: American Registry for Internet Numbers, which serves North America and some Caribbean regions.
  - AFRINIC: Africa Network Information Center, which serves Africa.
  - APNIC: Asia Pacific Network Information Centre, which serves Asia and the Pacific.
- IPv4 has proven to be a very successful protocol. It has survived the development of the Internet from a small number of computers to hundreds of millions of computers. But the protocol was designed decades ago based on the size of the networks at that time. With the expansion of the Internet and the launch of new applications, IPv4 has shown more and more limitations.
- The rapid expansion of the Internet scale was unforeseen at that time. Especially over the past decade, the Internet has experienced explosive growth and has been accessed by numerous households. It has become a necessity in people's daily life. Against the Internet's rapid development, IP address depletion becomes a pressing issue.
- In the 1990s, the IETF launched technologies such as Network Address Translation (NAT) and Classless Inter-Domain Routing (CIDR) to delay IPv4 address exhaustion. However, these transition solutions can only slow down the speed of address exhaustion, but cannot fundamentally solve the problem.

Why IPv6?

IPv4		IPv6
Exhausted public IP addresses		Nearly infinite address space
Improper packet header design		Hierarchical address allocation
Large routing table, leading to inefficient table query	VS.	Plug-and-play
Dependency on ARP causes broadcast storms		Simplified packet header
...		IPv6 security features
		Integrity of E2E communication
		Support for mobility
		Enhanced QoS features
		...

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



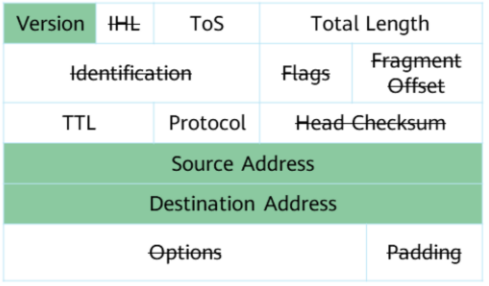
- Nearly infinite address space: This is the most obvious advantage over IPv4. An IPv6 address consists of 128 bits. The address space of IPv6 is about 8×10^{28} times that of IPv4. It is claimed that IPv6 can allocate a network address to each grain of sand in the world. This makes it possible for a large number of terminals to be online at the same time and unified addressing management, providing strong support for the interconnection of everything.
- Hierarchical address structure: IPv6 addresses are divided into different address segments based on application scenarios thanks to the nearly infinite address space. In addition, the continuity of unicast IPv6 address segments is strictly required to prevent "holes" in IPv6 address ranges, which facilitates IPv6 route aggregation to reduce the size of IPv6 address tables.
- Plug-and-play: Any host or terminal must have a specific IP address to obtain network resources and transmit data. Traditionally, IP addresses are assigned manually or automatically using DHCP. In addition to the preceding two methods, IPv6 supports SLAAC.
- E2E network integrity: NAT used on IPv4 networks damages the integrity of E2E connections. After IPv6 is used, NAT devices are no longer required, and online behavior management and network monitoring become simple. In addition, applications do not need complex NAT adaptation code.
- Enhanced security: IPsec was initially designed for IPv6. Therefore, IPv6-based protocol packets (such as routing protocol packets and neighbor discovery packets) can be encrypted in E2E mode, despite the fact that this function is not widely used currently. The security capability of IPv6 data plane packets is similar to that of IPv4+IPsec.

- High scalability: IPv6 extension headers are not a part of the main data packet. However, if necessary, the extension headers can be inserted between the basic IPv6 header and the valid payload to assist IPv6 in encryption, mobility, optimal path selection, and QoS, improving packet forwarding efficiency.
- Improved mobility: When a user moves from one network segment to another on a traditional network, a typical triangle route is generated. On an IPv6 network, the communication traffic of such mobile devices can be directly routed without the need of the original triangle route. This feature reduces traffic forwarding costs and improves network performance and reliability.
- Enhanced QoS: IPv6 reserves all QoS attributes of IPv4 and additionally defines a 20-byte Flow Label field for applications or terminals. This field can be used to allocate specific resources to special services and data flows. Currently, this mechanism has not been fully developed and applied yet.

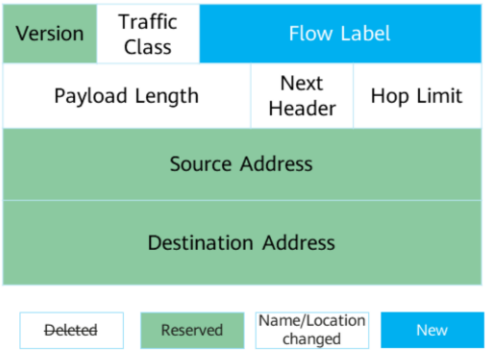
Basic IPv6 Header

- An IPv6 header consists of a mandatory basic IPv6 header and optional extension headers.
- The basic header provides basic information for packet forwarding and is parsed by all devices on a forwarding path.

IPv4 packet header (20–60 bytes)

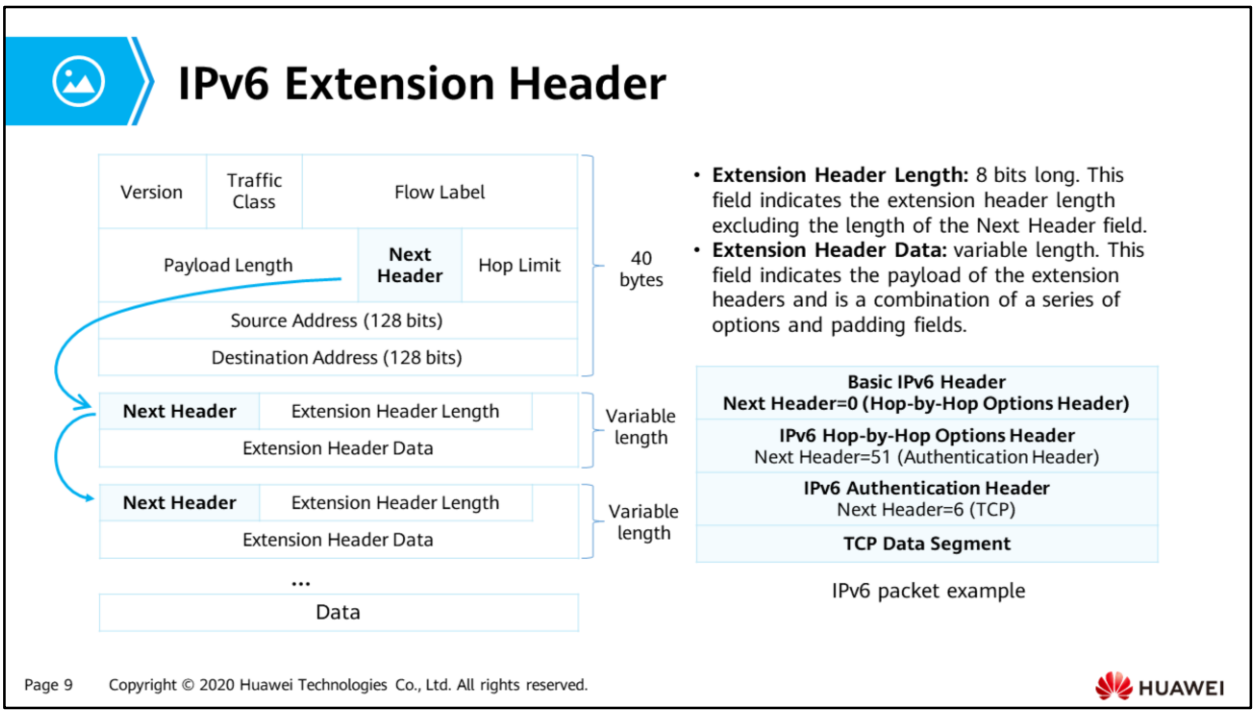


Basic IPv6 header (40 bytes)



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

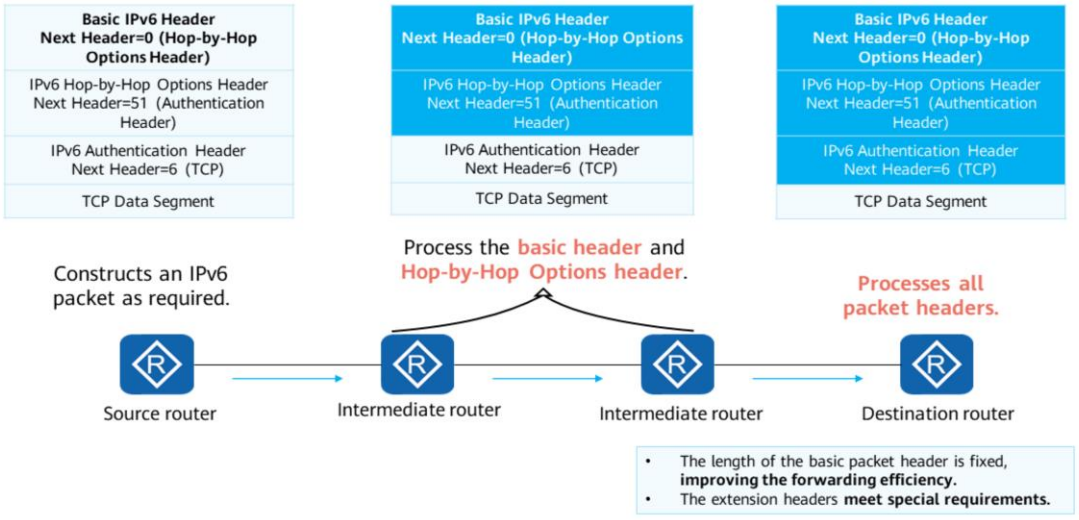
- The fields in a basic IPv6 header are described as follows:
  - Version: 4 bits long. In IPv6, the value is 6.
  - Traffic Class: 8 bits long. This field indicates the class or priority of an IPv6 packet. It is similar to the TOS field in an IPv4 packet and is mainly used in QoS control.
  - Flow Label: 20 bits long. This field was added in IPv6 to differentiate real-time traffic. A flow label and a source IP address together can identify a unique data flow. Intermediate network devices can effectively differentiate data flows based on this field.
  - Payload Length: 16 bits long. This field indicates the length of the part (namely, extension headers and upper-layer PDU) in an IPv6 packet following the IPv6 basic header.
  - Next Header: 8 bits long. This field defines the type of the first extension header (if any) following a basic IPv6 header or the protocol type in an upper-layer PDU (similar to the Protocol field in IPv4).
  - Hop Limit: 8 bits long. This field is similar to the Time to Live field in an IPv4 packet. It defines the maximum number of hops that an IP packet can pass through. The value is decreased by 1 each time an IP packet passes through a node. The packet is discarded if Hop Limit is decreased to zero.
  - Source Address: 128 bits long. This field indicates the address of the packet sender.
  - Destination Address: 128 bits long. This field indicates the address of the packet receiver.



- An IPv4 packet header carries the optional Options field, which can represent security, timestamp, or record route options. The Options field extends the IPv4 packet header from 20 bytes to 60 bytes. The Options field needs to be processed by all the intermediate devices, consuming a large number of resources. For this reason, this field is seldom used in practice.
- IPv6 removes the Options field from the basic header and puts it in the extension headers, which are placed between a basic IPv6 header and upper-layer PDU. An IPv6 packet may carry zero, one, or more extension headers. A sender adds one or more extension headers to a packet only when the sender requests the destination device or other devices to perform special handling. The length of IPv6 extension headers is not limited to 40 bytes so that new options can be added later. This feature together with the option processing modes enables the IPv6 options to be leveraged. To improve extension header processing efficiency and transport protocol performance, the extension header length, however, is always an integer multiple of 8 bytes.
- When multiple extension headers are used, the Next Header field of the preceding header indicates the type of the current extension header. In this way, a chained packet header list is formed.

- When more than one extension header is used in the same IPv6 packet, those headers must appear in the following order:
    1. Hop-by-Hop Options header: carries optional information that must be examined by every node along a packet's delivery path.
    2. Destination Options header: carries optional information that needs to be examined only by a packet's destination node.
    3. Routing header: used by an IPv6 source to list one or more intermediate nodes to be "visited" on the way to a packet's destination.
    4. Fragment header: used by an IPv6 source to send a packet longer than the path MTU to its destination.
    5. Authentication header (AH): used by IPsec to provide authentication, data integrity, and replay protection.
    6. Encapsulating Security Payload (ESP) header: used by IPsec to provide authentication, data integrity, replay protection, and confidentiality of IPv6 packets.

IPv6 Packet Processing Mechanism

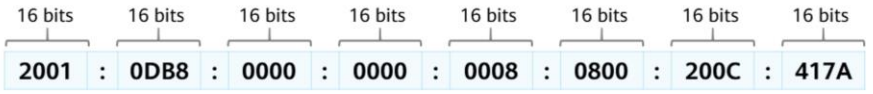


- The length of the basic packet header is fixed, **improving the forwarding efficiency.**
- The extension headers **meet special requirements.**

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

IPv6 Address

- The length of an IPv6 address is 128 bits. Colons are generally used to divide the IPv6 address into eight segments. Each segment contains 16 bits and is expressed in hexadecimal notation.



The letters in an IPv6 address are case insensitive. For example, **A** is equivalent to **a**.

- Similar to an IPv4 address, an IPv6 address is expressed in the format of IPv6 address/mask length.
  - Example: 2001:0DB8:2345:CD30:1230:4567:89AB:CDEF/64

    IPv6 address: 2001:0DB8:2345:CD30:1230:4567:89AB:CDEF

    Subnet number: 2001:0DB8:2345:CD30::/64

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

IPv6 Address Abbreviation Specifications

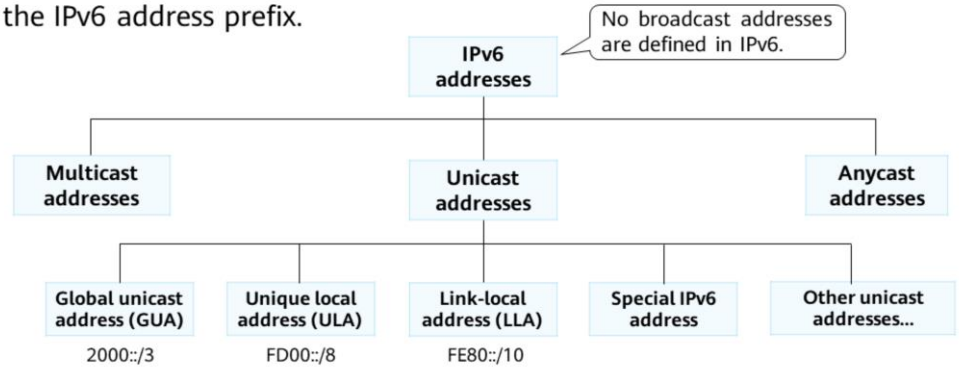
- For convenience, IPv6 can be abbreviated according to the following rules.

Abbreviation Specifications	Abbreviation Examples
2001 : 0DB8 : 0000 : 0000 : 0008 : 0800 : 200C : 417A The leading 0s in each 16-bit segment can be omitted. However, if all bits in a 16-bit segment are 0s, at least one 0 must be reserved. The tailing 0s cannot be omitted. **2001 : DB8 : 0 : 0 : 8 : 800 : 200C : 417A** If one or more consecutive 16-bit segments contain only 0s, a double colon (::) can be used to represent them, but only one :: is allowed in an entire IPv6 address. **2001 : DB8 :: 8 : 800 : 200C : 417A** If an abbreviated IPv6 address contains two double colons (::), the IPv6 address cannot be restored to the original one.	Before 0000:0000:0000:0000:0000:0000:0000:0001 After ::1 Before 2001:0DB8:0000:0000:FB00:1400:5000:45FF After 2001:DB8::FB00:1400:5000:45FF Before 2001:0DB8:0000:0000:0000:2A2A:0000:0001 After 2001:DB8::2A2A:0:1 Before 2001:0DB8:0000:1234:FB00:0000:5000:45FF After 2001:DB8::1234:FB00:0:5000:45FF or 2001:DB8:0:1234:FB00::5000:45FF

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

IPv6 Address Classification

- IPv6 addresses are classified into unicast, multicast, and anycast addresses according to the IPv6 address prefix.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Unicast address: identifies an interface. A packet destined for a unicast address is sent to the interface having that unicast address. In IPv6, an interface may have multiple IPv6 addresses. In addition to GUAs, ULAs, and LLAs, IPv6 has the following special unicast addresses:
  - Unspecified address: 0:0:0:0:0:0:0:0/128, or ::/128. The address is used as the source address of some packets, for example, Neighbor Solicitation (NS) messages sent during DAD or request packets sent by a client during DHCPv6 initialization.
  - Loopback address: 0:0:0:0:0:0:0:1/128, or ::1/128, which is used for local loopback (same function as 127.0.0.1 in IPv4). The data packets sent to ::/1 are actually sent to the local end and can be used for loopback tests of local protocol stacks.
- Multicast address: identifies multiple interfaces. A packet destined for a multicast address is sent to all the interfaces joining in the corresponding multicast group. Only the interfaces that join a multicast group listen to the packets destined for the corresponding multicast address.
- Anycast address: identifies a group of network interfaces (usually on different nodes). A packet sent to an anycast address is routed to the nearest interface having that address, according to the router's routing table.
- IPv6 does not define any broadcast address. On an IPv6 network, all broadcast application scenarios are served by IPv6 multicast.

IPv6 Unicast Address Format

- An IPv6 unicast address is composed of two parts:
  - Network prefix: consists of n bits and is parallel to the network ID of an IPv4 address.
  - Interface ID: consists of (128 – n) bits and is parallel to the host ID of an IPv4 address.
- Common IPv6 unicast addresses, such as GUAs and LLAs, require that the network prefix and interface ID be 64 bits.

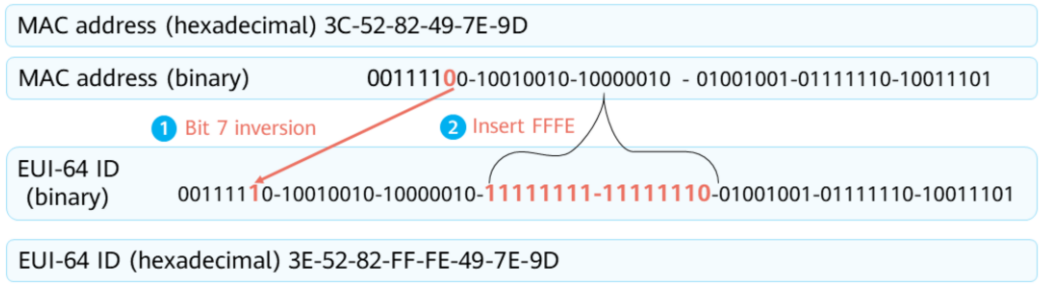


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Global unicast addresses that start with binary value 000 can use a non-64-bit network prefix. Such addresses are not covered in this course.

Interface ID of an IPv6 Unicast Address

- 3 methods to generate an interface ID:
  - Manual configuration
  - Automatic generation by the system
  - Using the IEEE 64-bit extended unique identifier (EUI-64) standard
- EUI-64 is most commonly used. It converts the MAC address of an interface into an IPv6 interface ID.

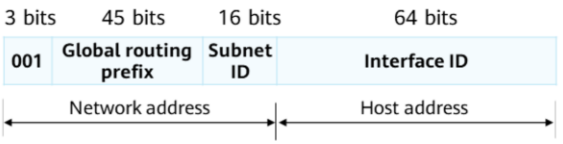


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

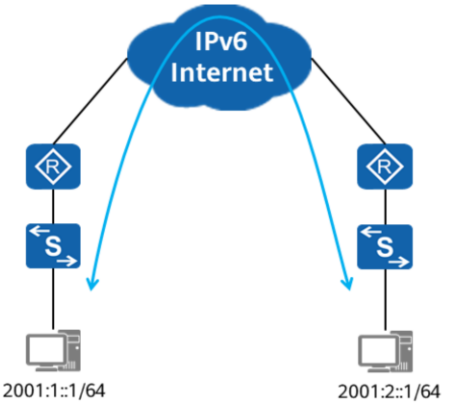
- An interface ID is 64 bits long and is used to identify an interface on a link. The interface ID must be unique on each link. The interface ID is used for many purposes. Most commonly, an interface ID is attached to a link-local address prefix to form the link-local address of the interface. It can also be attached to an IPv6 global unicast address prefix in SLAAC to form the global unicast address of the interface.
- IEEE EUI-64 standard
  - Converting MAC addresses into IPv6 interface IDs reduces the configuration workload. Especially, you only need an IPv6 network prefix in SLAAC to form an IPv6 address.
  - The defect of this method is that IPv6 addresses can be deducted by attackers based on MAC addresses.

Common IPv6 Unicast Address - GUA

- A GUA is also called an aggregatable GUA. This type of address is globally unique and is used by hosts that need to access the Internet. It is equivalent to a public IPv4 address.



- The network address and interface ID of a GUA are each generally 64 bits long.
- Global routing prefix: is assigned by a provider to an organization and is generally at least 45 bits.
- Subnet ID: An organization can divide subnets based on network requirements.
- Interface ID: identifies a device's interface.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- You can apply for a GUA from a carrier or the local IPv6 address management organization.

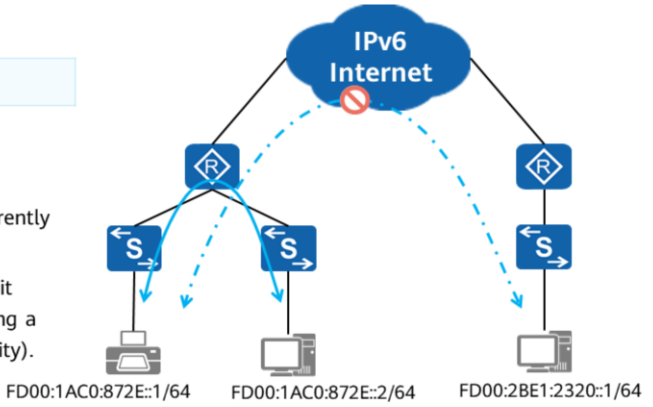
Common IPv6 Unicast Address - ULA

- A ULA is a private IPv6 address that can be used only on an intranet. This type of address cannot be routed on an IPv6 public network and therefore cannot be used to directly access a public network.

8 bits	40 bits	16 bits	64 bits
1111 1101	Global ID	Subnet ID	Interface ID

Generated using a pseudo-random algorithm

- ULAs use the FC00::/7 address segment, among which, only the FD00::/8 address segment is currently used. FC00::/8 is reserved for future expansion.
- Although a ULA is valid only in a limited range, it also has a globally unique prefix (generated using a pseudo-random algorithm, low conflict probability).



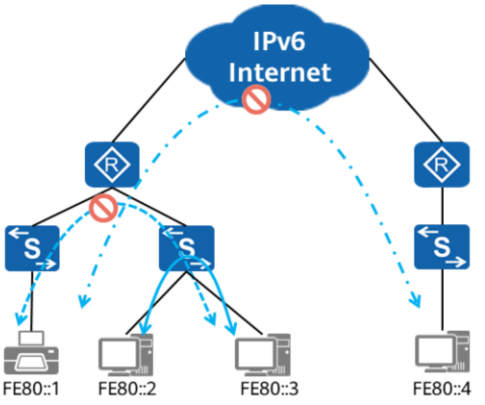
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Common IPv6 Unicast Address - LLA

- An LLA is another type of IPv6 address with limited application scope. The valid range of the LLA is the local link, with the prefix of FE80::/10.

10 bit	54 bit	64 bit
1111 1110 10	**0**	**Interface ID**
	Fixed at 0	

- An LLA is used for communication on a single link, such as during IPv6 SLAAC and IPv6 neighbor discovery.
- Data packets with the source or destination IPv6 address being an LLA are not forwarded out of the originating link. In other words, the valid scope of an LLA is the local link.
- Each IPv6 interface must have an LLA. Huawei devices support automatic generation and manual configuration of LLAs.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

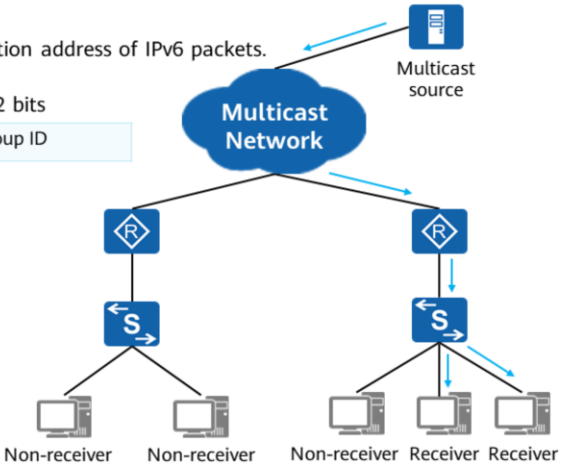
IPv6 Unicast Address | IPv6 Multicast Address | IPv6 Anycast Address

IPv6 Multicast Address

- An IPv6 multicast address identifies multiple interfaces and is generally used in one-to-many communication scenarios.
- An IPv6 multicast address can be used only as the destination address of IPv6 packets.

8 bits	4 bits	4 bits	80 bits	32 bits
11111111	Flags	Scope	Reserved (must be 0)	Group ID

- **Flags**: indicates a permanent or transient multicast group.
- **Scope**: indicates the multicast group scope.
- **Group ID**: indicates a multicast group ID.

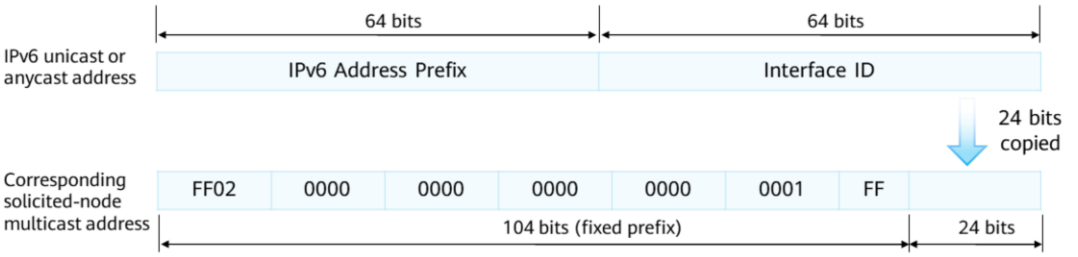


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Types and scope of IPv6 multicast groups:
  - Flags:
    - 0000: permanent or well-known multicast group
    - 0001: transient multicast group
  - Scope:
    - 0: reserved
    - 1: interface-local scope, which spans only a single interface on a node and is useful only for loopback transmission of multicast
    - 2: link-local scope (for example, FF02::1)
    - 5: site-local scope
    - 8: organization-local scope
    - E: global scope
    - F: reserved

Solicited-Node Multicast Address

- If a node has an IPv6 unicast or anycast address, a solicited-node multicast address is generated for the address, and the node joins the corresponding multicast group. This address is used for **neighbor discovery** and **duplicate address detection (DAD)**. A solicited-node multicast address is **valid only on the local link**.

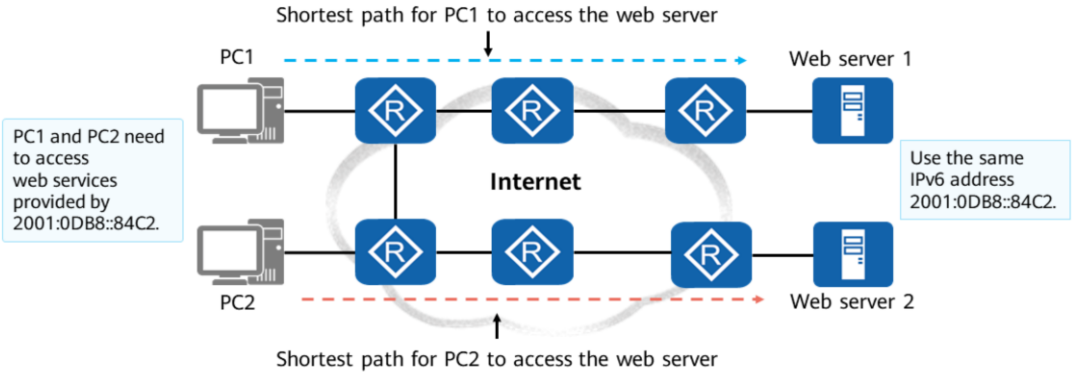


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- An application scenario example of a solicited-node multicast group address is as follows: In IPv6, ARP and broadcast addresses are canceled. When a device needs to request the MAC address corresponding to an IPv6 address, the device still needs to send a request packet, which is a multicast packet. The destination IPv6 address of the packet is the solicited-node multicast address corresponding to the target IPv6 unicast address. Because only the target node listens to the solicited-node multicast address, the multicast packet is received only by the target node, without affecting the network performance of other non-target nodes.

IPv6 Anycast Address

- An anycast address identifies a group of network interfaces, which usually belong to different nodes. An anycast address can be used as the source or destination address of IPv6 packets.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- The anycast process involves an anycast packet initiator and one or more responders.
  - An initiator of an anycast packet is usually a host requesting a service (for example, a web service).
  - The format of an anycast address is the same as that of a unicast address. A device, however, can send packets to multiple devices with the same anycast address.
- Anycast addresses have the following advantages:
  - Provide service redundancy. For example, a user can obtain the same service (for example, a web service) from multiple servers that use the same anycast address. These servers are all responders of anycast packets. If no anycast address is used and one server fails, the user needs to obtain the address of another server to establish communication again. If an anycast address is used and one server fails, the user can automatically communicate with another server that uses the same address, implementing service redundancy.
  - Provide better services. For example, a company deploys two servers – one in province A and the other in province B – to provide the same web service. Based on the optimal route selection rule, users in province A preferentially access the server deployed in province A when accessing the web service provided by the company. This improves the access speed, reduces the access delay, and greatly improves user experience.

Contents

1. IPv6 Overview
2. **IPv6 Address Configuration**
3. Typical IPv6 Configuration Examples

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

IPv6 Addresses of Hosts and Routers

- The unicast IPv6 addresses and multicast addresses of hosts and routers are typically as follows:



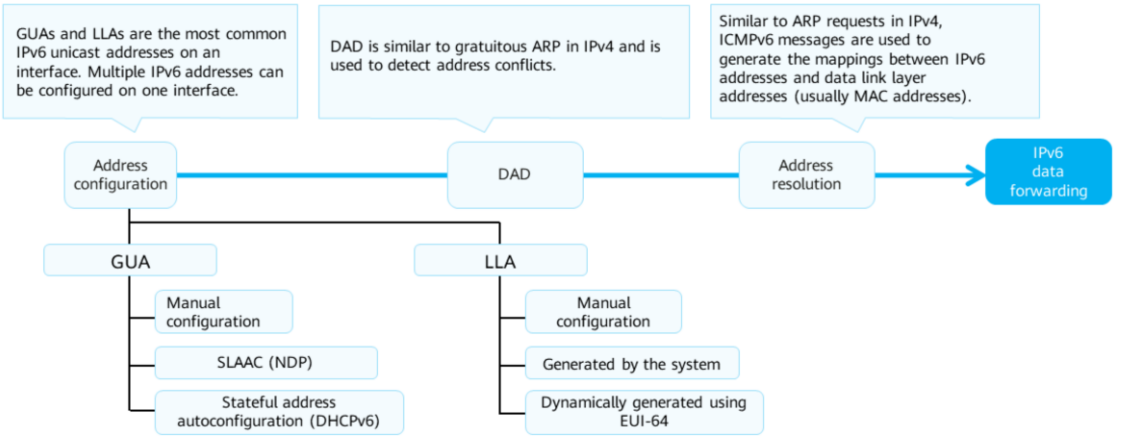
LLA of the network adapter	FE80::2E0:FCFF:FE35:7287
GUA assigned by an administrator	2001::1
Loopback address	::1
Multicast addresses of all nodes	FF01::1 and FF02::1
Solicited-node multicast address corresponding to each unicast address of the network adapter	FF02::1:FF35:7287 FF02::1:FF00:1

LLA of the network adapter	FE80::2E0:FCFF:FE99:1285
GUA assigned by an administrator	2001::2
Loopback address	::1
Multicast addresses of all nodes	FF01::1 and FF02::1
Multicast addresses of all routers	FF01::2 and FF02::2
Solicited-node multicast address corresponding to each unicast address of the network adapter	FF02::1:FF99:1285 FF02::1:FF00:2

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Service Process of IPv6 Unicast Addresses

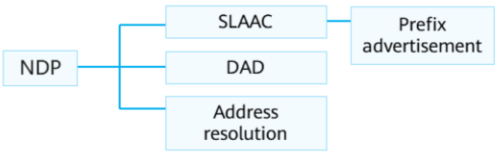
- Before sending IPv6 packets, an interface undergoes address configuration, DAD, and address resolution. During this process, the Neighbor Discovery Protocol (NDP) plays an important role.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

NDP

- NDP is defined in RFC 2461, which was replaced by RFC 4861.
- NDP uses ICMPv6 messages to implement its functions.



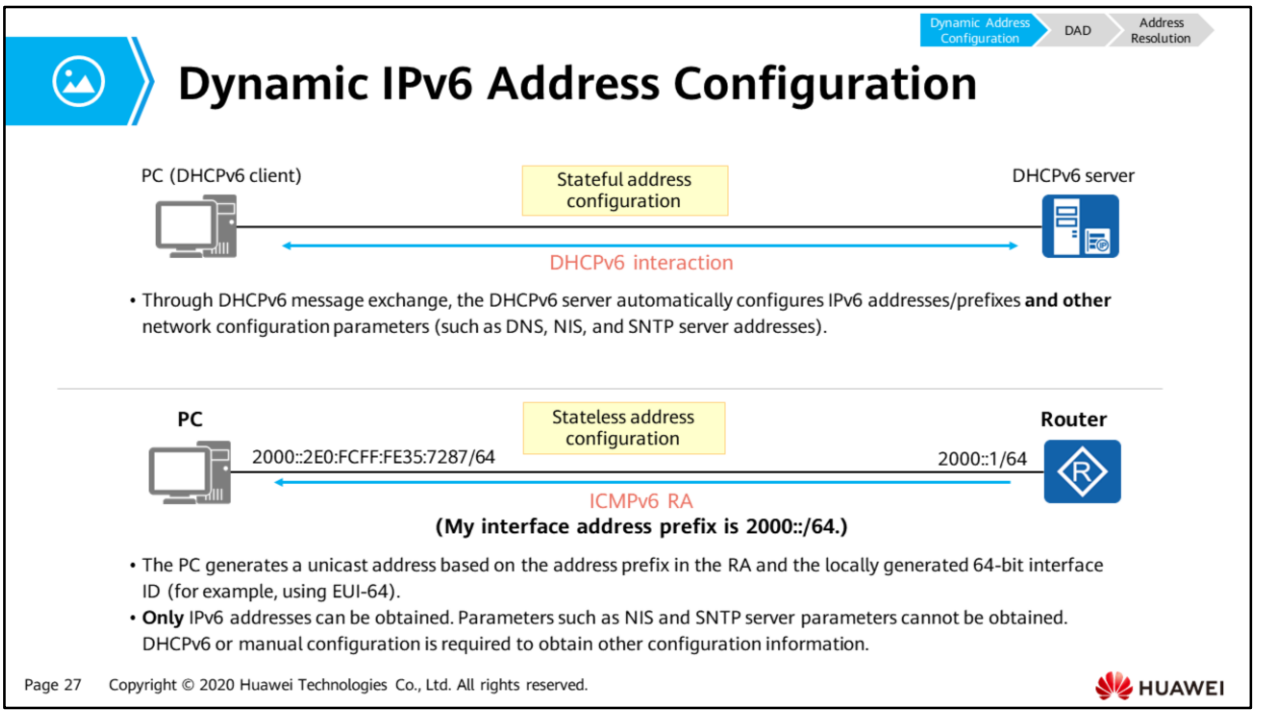
ICMPv6 messages used by NDP

ICMPv6 Type	Message Name
133	Router Solicitation (RS)
134	Router Advertisement (RA)
135	Neighbor Solicitation (NS)
136	Neighbor Advertisement (NA)

Mechanism	RS 133	RA 134	NS 135	NA 136
Address resolution			√	√
Prefix advertisement	√	√		
DAD			√	√

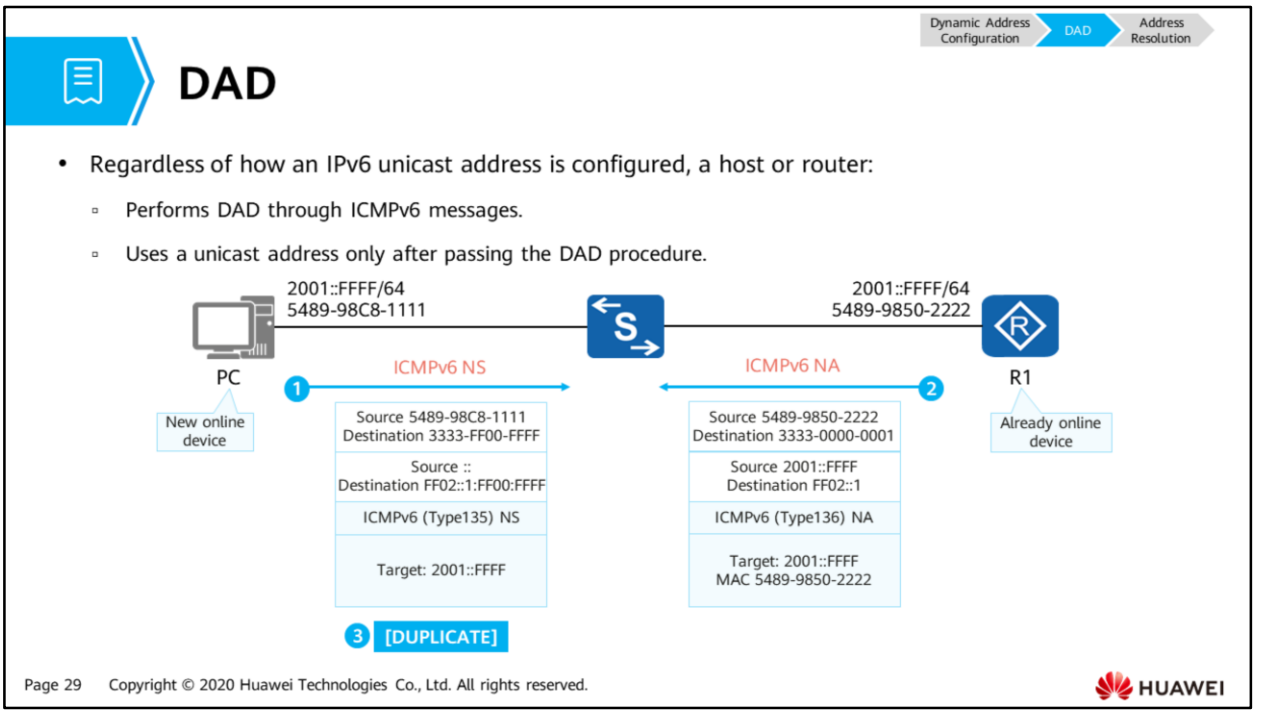
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- SLAAC is a highlight of IPv6. It enables IPv6 hosts to be easily connected to IPv6 networks, without the need to manually configure IPv6 addresses and to deploy application servers (such as DHCP servers) to assign addresses to hosts. SLAAC uses ICMPv6 RS and RA messages.
- Address resolution uses ICMPv6 NS and NA messages.
- DAD uses ICMPv6 NS and NA messages to ensure that no two identical unicast addresses exist on the network. DAD must be performed on all interfaces before they use unicast addresses.

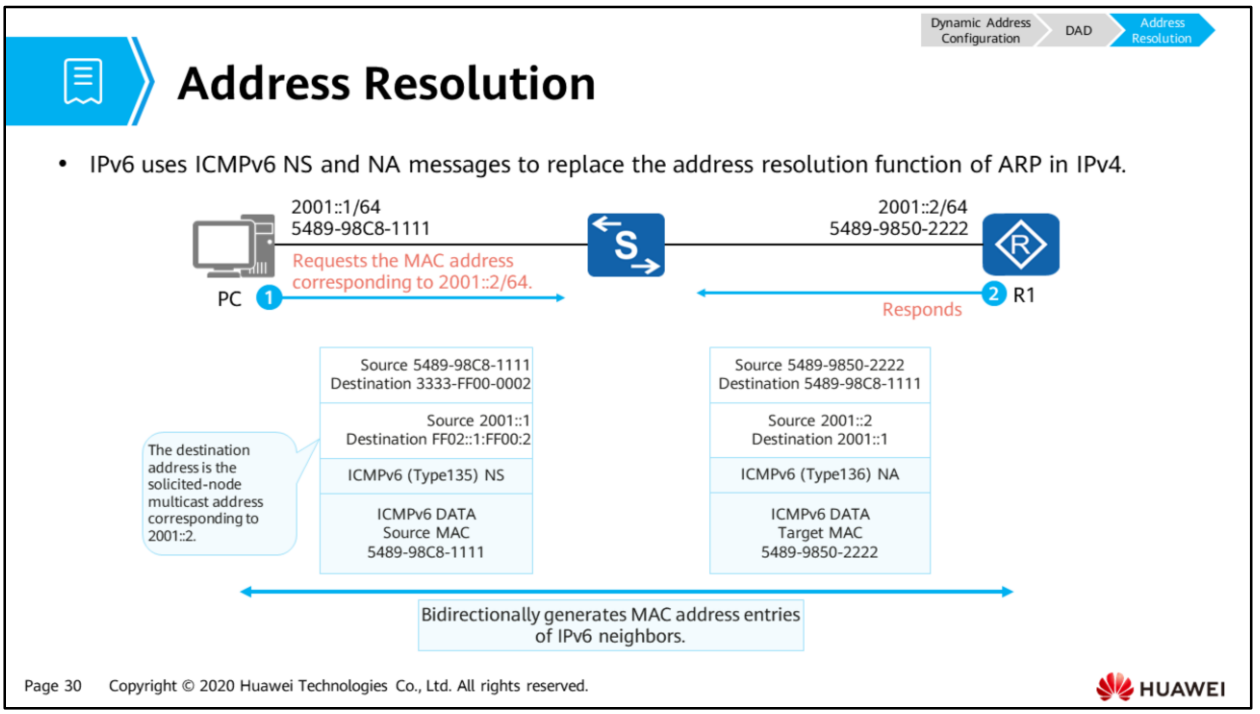


- IPv6 supports stateful and stateless address autoconfiguration. The managed address configuration flag (M flag) and other stateful configuration flag (O flag) in ICMPv6 RA messages are used to control the mode in which terminals automatically obtain addresses.
- For stateful address configuration (DHCPv6), M = 1, O = 1:
  - DHCPv6 is used. An IPv6 client obtains a complete 128-bit IPv6 address, as well as other address parameters, such as DNS and SNTP server address parameter, from a DHCPv6 server.
  - The DHCPv6 server records the allocation of the IPv6 address (this is where stateful comes).
  - This method is complex and requires high performance of the DHCPv6 server.
  - Stateful address configuration is mainly used to assign IP addresses to wired terminals in an enterprise, facilitating address management.
- For SLAAC, M = 0, O = 0:
  - ICMPv6 is used.
    - The router enabled with ICMPv6 RA periodically advertises the IPv6 address prefix of the link connected to a host.
    - Alternatively, the host sends an ICMPv6 RS message, and the router replies with an RA message to notify the link's IPv6 address prefix.

    - The host obtains the IPv6 address prefix from the RA message returned by the router and combines the prefix with the local interface ID to form a unicast IPv6 address.
    - If the host wants to obtain other configuration information, it can use DHCPv6. When DHCPv6 is used, M = 0, and O = 1.
    - In SLAAC, routers do not care about the status of hosts or whether hosts are online.
    - SLAAC applies to scenarios where there are a large number of terminals that do not need other parameters except addresses. IoT is such a scenario.
- Domain name system (DNS): a mechanism that maps easy-to-remember domain names to IPv6 addresses that can be identified by network devices
- Network information system (NIS): a system manages all configuration files related to computer system management on computer networks
- Simple Network Time Protocol (SNTP): adapted from NTP and is used to synchronize the clocks of computers on the Internet



- Assume that R1 is an online device with an IPv6 address 2001::FFFF/64. After the PC goes online, it is configured with the same IPv6 address. Before the IPv6 address is used, the PC performs DAD for the IPv6 address. The process is as follows:
    1. The PC sends an NS message to the link in multicast mode. The source IPv6 address of the NS message is ::, and the destination IPv6 address is the solicited-node multicast address corresponding to 2001::FFFF for DAD, that is, FF02::1:FF00:FFFF. The NS message contains the destination address 2001::FFFF for DAD.
    2. All nodes on the link receive the multicast NS message. The node interfaces that are not configured with 2001::FFFF are not added to the solicited-node multicast group corresponding to 2001::FFFF. Therefore, these node interfaces discard the received NS message. R1's interface is configured with 2001::FFFF and joins the multicast group FF02::1:FF00:FFFF. After receiving the NS message with 2001::FFFF as the destination IP address, R1 parses the message and finds that the destination address of DAD is the same as its local interface address. R1 then immediately returns an NA message. The destination address of the NA message is FF02::1, that is, the multicast address of all nodes. In addition, the destination address 2001::FFFF and the MAC address of the interface are filled in the NA message.
    3. After the PC receives the NA message, it knows that 2001::FFFF is already in use on the link. The PC then marks the address as duplicate. This IP address cannot be used for communication. If no NA message is received, the PC determines that the IPv6 address can be used. The DAD mechanism is similar to gratuitous ARP in IPv4.



- IPv6 address resolution does not use ARP or broadcast. Instead, IPv6 uses the same NS and NA messages as those in DAD to resolve data link layer addresses.
- Assume that a PC needs to parse the MAC address corresponding to 2001::2 of R1. The detailed process is as follows:
    1. The PC sends an NS message to 2001::2. The source address of the NS message is 2001::1, and the destination address is the solicited-node multicast address corresponding to 2001::2.
    2. After receiving the NS message, R1 records the source IPv6 address and source MAC address of the PC, and replies with a unicast NA message that contains its own IPv6 address and MAC address.
    3. After receiving the NA message, the PC obtains the source IPv6 address and source MAC address from the message. In this way, both ends create a neighbor entry about each other.

Contents

1. IPv6 Overview
2. IPv6 Address Configuration
3. **Typical IPv6 Configuration Examples**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Basic IPv6 Configurations (1)

1. Enable IPv6.

   [Huawei] **ipv6**

   Enable the device to send and receive IPv6 unicast packets, including local IPv6 packets.

   [Huawei-GigabitEthernet0/0/0] **ipv6 enable**

   Enable IPv6 on the interface in the interface view.

2. Configure an LLA for the interface.

   [Huawei-GigabitEthernet0/0/0] **ipv6 address** *ipv6-address* **link-local**

   [Huawei-GigabitEthernet0/0/0] **ipv6 address auto link-local**

   Configure an LLA for the interface manually or automatically in the interface view.

3. Configure a GUA for the interface.

   [Huawei-GigabitEthernet0/0/0] **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* }

   [Huawei-GigabitEthernet0/0/0] **ipv6 address auto** { **global** | **dhcp** }

   Configure a GUA for the interface manually or automatically (stateful or stateless) in the interface view.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic IPv6 Configurations (2)

4. Configure an IPv6 static route.

   [Huawei] **ipv6 route-static** *dest-ipv6-address prefix-length* { *interface-type interface-number* [*nexthop-ipv6-address*] | *nexthop-ipv6-address* } [**preference** *preference*]

5. Display IPv6 information on an interface.

   [Huawei] **display ipv6 interface** [*interface-type interface-number* | **brief**]

6. Display neighbor entry information.

   [Huawei] **display ipv6 neighbors**

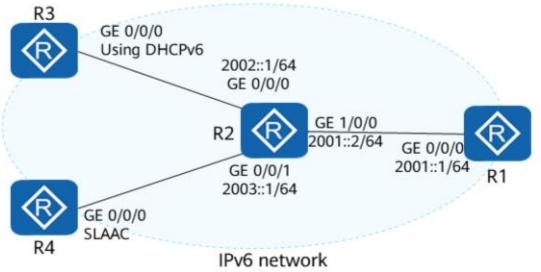
7. Enable an interface to send RA messages.

   [Huawei-GigabitEthernet0/0/0] **undo ipv6 nd ra halt**

   By default, a Huawei router's interfaces do not send ICMPv6 RA messages. In this situation, other devices on the links connected to the interfaces cannot perform SLAAC.
   To perform SLAAC, you need to manually enable the function of sending RA messages.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example: Configuring a Small IPv6 Network (1)



- Configuration Requirements
  - Connect R1 and R2 through interfaces with static IPv6 addresses.
  - Configure R2 as a DHCPv6 server to assign a GUA to GE 0/0/0 of R3.
  - Enable R2 to send RA messages, and configure GE 0/0/0 of R4 to automatically perform SLAAC based on the RA messages sent by R2.
  - Configure static routes to implement mutual access between the devices.

1. Enable IPv6 globally and on related interfaces of R1, R2, R3, and R4, and enable the interfaces to automatically generate LLAs. The following uses R1 configurations as an example.

```
[R1]ipv6
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ipv6 enable
[R1-GigabitEthernet0/0/0]ipv6 address auto link-local
```

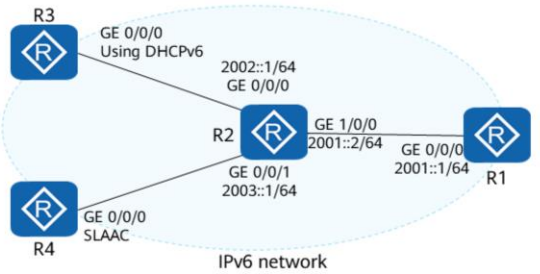
2. Configure static IPv6 GUAs on the related interfaces of R1 and R2.

```
[R1]interface GigabitEthernet 0/0/0
[R1-GigabitEthernet0/0/0]ipv6 address 2001::1 64
```

```
[R2]interface GigabitEthernet 1/0/0
[R2-GigabitEthernet1/0/0]ipv6 address 2001::2 64
[R2-GigabitEthernet1/0/0]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]ipv6 address 2002::1 64
[R2-GigabitEthernet0/0/0]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]ipv6 address 2003::1 64
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Example: Configuring a Small IPv6 Network (2)



- Configuration Requirements
  - Connect R1 and R2 through interfaces with static IPv6 addresses.
  - Configure R2 as a DHCPv6 server to assign a GUA to GE 0/0/0 of R3.
  - Enable R2 to send RA messages, and configure GE 0/0/0 of R4 to automatically perform SLAAC based on the RA messages sent by R2.
  - Configure static routes to implement mutual access between the devices.

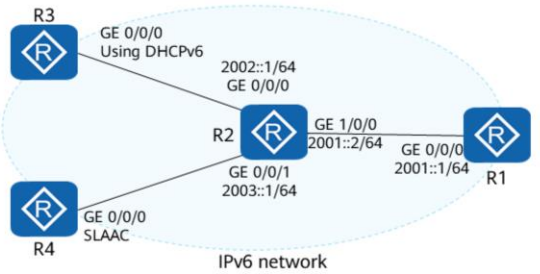
3. Configure R2 as a DHCPv6 server. Configure the related interface of R3 to obtain a GUA using DHCPv6.

```
[R2]dhcp enable
[R2]dhcpv6 pool pool1
[R2-dhcpv6-pool-pool1]address prefix 2002::/64
[R2]interface GigabitEthernet 0/0/0
[R2-GigabitEthernet0/0/0]dhcpv6 server pool1
```

```
[R3]dhcp enable
[R3]interface GigabitEthernet 0/0/0
[R3-GigabitEthernet0/0/0]ipv6 address auto dhcp
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Example: Configuring a Small IPv6 Network (3)



- Configuration Requirements
  - Connect R1 and R2 through interfaces with static IPv6 addresses.
  - Configure R2 as a DHCPv6 server to assign a GUA to GE 0/0/0 of R3.
  - Enable R2 to send RA messages, and configure GE 0/0/0 of R4 to automatically perform SLAAC based on the RA messages sent by R2.
  - Configure static routes to implement mutual access between the devices.

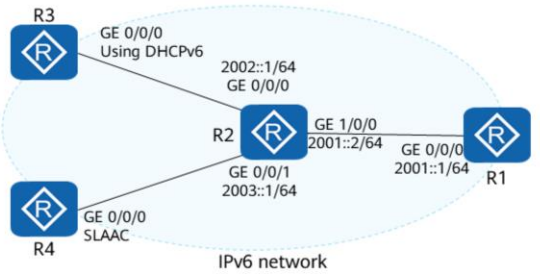
4. Enable R2 to advertise RA messages. Enable R4 to obtain an address through SLAAC based on the RA messages sent by R2.

```
[R2]interface GigabitEthernet 0/0/1
[R2-GigabitEthernet0/0/1]undo ipv6 nd ra halt
```

```
[R4]interface GigabitEthernet 0/0/0
[R4-GigabitEthernet0/0/0]ipv6 address auto global
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Example: Configuring a Small IPv6 Network (4)



- Configuration Requirements
  - Connect R1 and R2 through interfaces with static IPv6 addresses.
  - Configure R2 as a DHCPv6 server to assign a GUA to GE 0/0/0 of R3.
  - Enable R2 to send RA messages, and configure GE 0/0/0 of R4 to automatically perform SLAAC based on the RA messages sent by R2.
  - Configure static routes to implement mutual access between the devices.

5. Configure static routes on R4.

```
[R4]ipv6 route-static 2001:: 64 2003::1
[R4]ipv6 route-static 2002:: 64 2003::1
```

6. Configure an aggregated static route on R1.

```
[R1]ipv6 route-static  2002:: 15 2001::2
```

7. Configure a default route on R3.

```
[R3]ipv6 route-static :: 0 2002::1
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Quiz

1. What is the most abbreviated form of the IPv6 address 2001:0DB8:0000:0000:032A:0000:0000:2D70?
2. What is the process of SLAAC for IPv6 hosts?

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

1. 2001:DB8::32A:0:0:2D70 or 2001:DBB:0:0:32A::2D70
2. An IPv6 host obtains an address prefix from the RA message sent by the related router interface, and then generates an interface ID by inserting a 16-bit FFFE into the existing 48-bit MAC address of the host's interface. After generating an IPv6 address, the IPv6 host checks whether the address is unique through DAD.

Summary

Comparison	IPv6	IPv4
Address length	128 bits	32 bits
Packet format	A fixed 40-byte basic packet header+variable-length extension headers	A basic header containing the Options field to support extended features
Address type	Unicast, multicast, and anycast	Unicast, multicast, and broadcast
Address configuration	Static, DHCP, and SLAAC	Static and DHCP
DAD	ICMPv6	Gratuitous ARP
Address resolution	ICMPv6	ARP

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



SDN and NFV Overview

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- The open ecosystem of the computing industry brings booming development of multiple fields, such as Commercial Off-the-Shelf (COTS), operating system, virtualization, middleware, cloud computing, and software applications. The network industry is also seeking transformation and development. Software Defined Networking (SDN) and Network Functions Virtualization (NFV) are mainly used.
- This course aims to help engineers understand the development of SDN and NFV and introduce Huawei SDN and NFV solutions.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

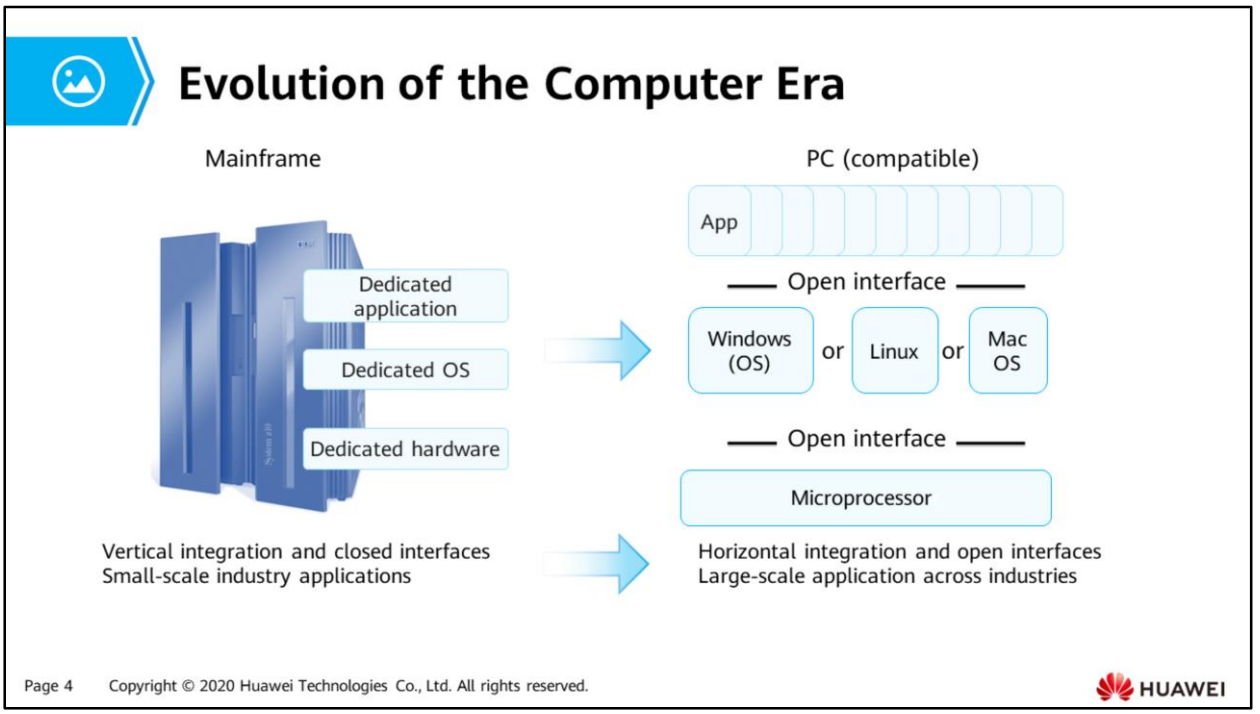
- Upon completion of this course, you will be able to:
  - Describe the development of SDN and NFV.
  - Understand basic principles of OpenFlow.
  - Understand Huawei SDN solution.
  - Understand the standard NFV architecture.
  - Understand Huawei NFV solution.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. **SDN Overview**
2. NFV Overview

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

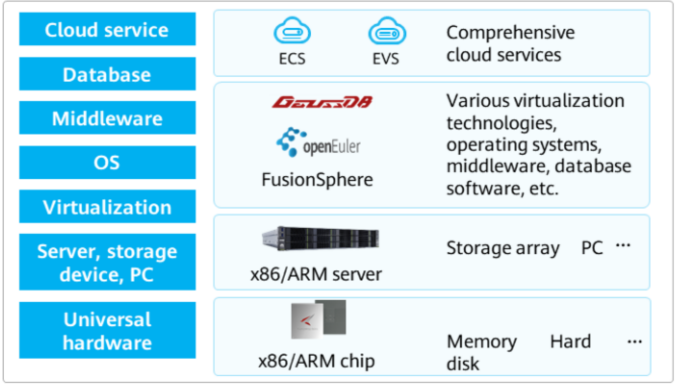


- In 1964, IBM spent US$5 billion on developing IBM System/360 (S/360), which started the history of mainframes. Mainframes typically use the centralized architecture. The architecture features excellent I/O processing capability and is the most suitable for processing large-scale transaction data. Compared with PCs, mainframes have dedicated hardware, operating systems, and applications.
- PCs have undergone multiple innovations from hardware, operating systems, to applications. Every innovation has brought about great changes and development. The following three factors support rapid innovation of the entire PC ecosystem:
    - Hardware substrate: The PC industry has adapted a simple and universal hardware base, x86 instruction set.
    - Software-defined: The upper-layer applications and lower-layer basic software (OS and virtualization) are greatly innovated.
    - Open-source: The flourishing development of Linux has verified the correctness of open source and bazaar model. Thousands of developers can quickly formulate standards to accelerate innovation.

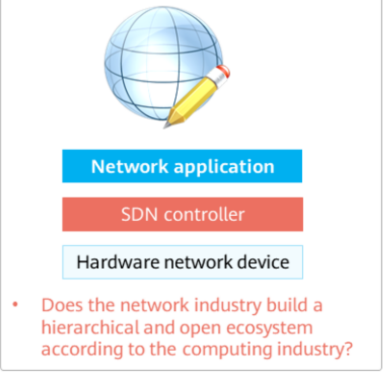
Network Industry Development: Implications from the IT Industry

- The transformation of the IT industry has triggered the thinking of the network industry. The industry has proposed the SDN concept and has made attempts to put SDN into commercial use, aiming to make networks more open, flexible, and simple.

Computing Industry Openness Promotes Ecosystem Development



What About Network Industry Changes

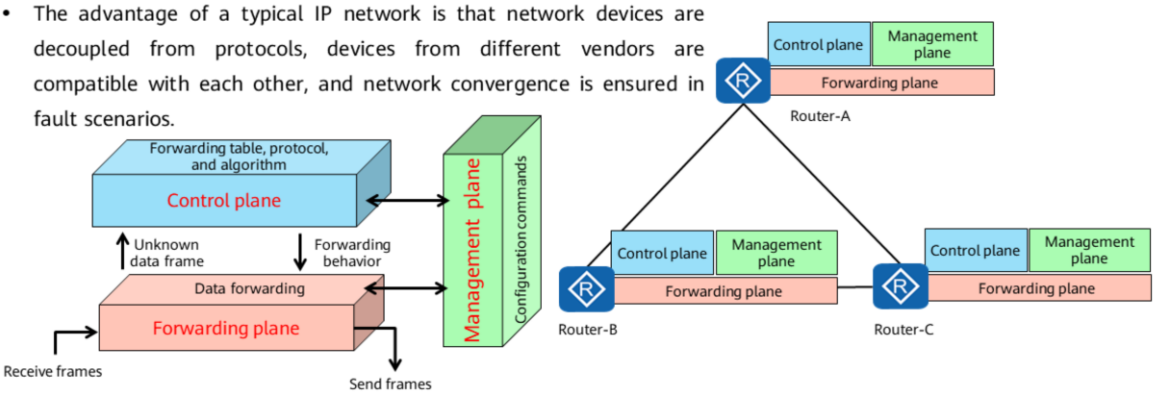


- Does the network industry build a hierarchical and open ecosystem according to the computing industry?

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Current Situation of the Network Industry: Typical IP Network - Distributed Network

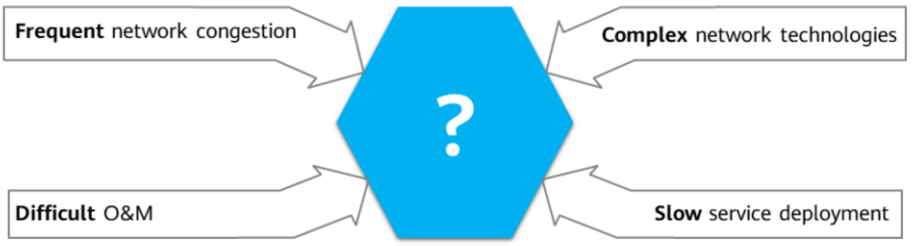
- The typical IP network is a distributed network with peer-to-peer control. Each network device has independent forwarding, control, and management planes. The control plane of a network device exchanges packets of a routing protocol to generate an independent data plane to guide packet forwarding.
- The advantage of a typical IP network is that network devices are decoupled from protocols, devices from different vendors are compatible with each other, and network convergence is ensured in fault scenarios.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- The switch is used as an example to describe the forwarding plane, control plane, and management plane.
- Forwarding plane: provides high-speed, non-blocking data channels for service switching between service modules. The basic task of a switch is to process and forward various types of data on its interfaces. Specific data processing and forwarding, such as Layer 2, Layer 3, ACL, QoS, multicast, and security protection, occur on the forwarding plane.
- Control plane: provides functions such as protocol processing, service processing, route calculation, forwarding control, service scheduling, traffic statistics collection, and system security. The control plane of a switch is used to control and manage the running of all network protocols. The control plane provides various network information and forwarding query entries required for data processing and forwarding on the data plane.
- Management plane: provides functions such as system monitoring, environment monitoring, log and alarm processing, system software loading, and system upgrade. The management plane of a switch provides network management personnel with Telnet, web, SSH, SNMP, and RMON to manage devices, and supports, parses, and executes the commands for setting network protocols. On the management plane, parameters related to various protocols on the control plane must be pre-configured, and the running of the control plane can be intervened if necessary.
- Some Huawei series products are divided into the data plane, management plane, and monitoring plane.

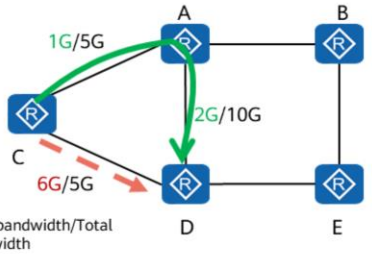
Thinking in the Network Field: Problems Faced by Typical Networks



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Frequent Network Congestion

Problem and Solution of Bandwidth-based Route Selection

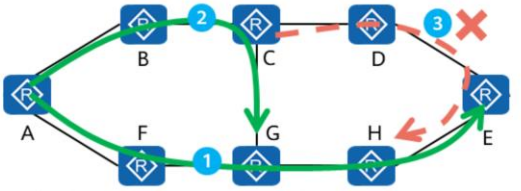


Used bandwidth/Total bandwidth

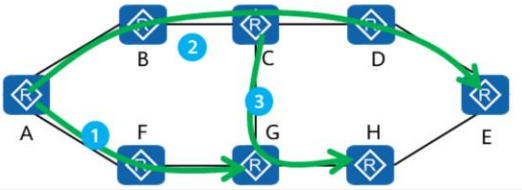
The network computes forwarding paths based on bandwidth. The link from router C to router D is the shortest forwarding path. The volume of service traffic from router C to router D exceeds the bandwidth, causing packet loss. Although other links are idle, the algorithm still selects the shortest path for forwarding. The optimal traffic forwarding path is C-A-D.

Problem and Solution of Tunnel Establishment Based on Fixed Sequence

Tunnels are established in sequence: 1. A-E; 2. A-G; 3. C-H. Tunnel 3 fails to be established due to insufficient bandwidth.



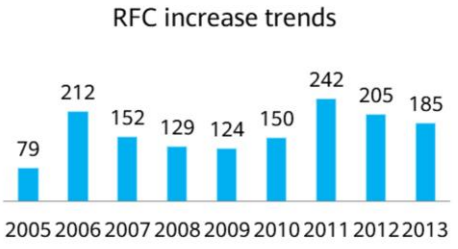
Global path calculation and optimal tunnel path adjustment:



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Complex Network Technologies

Many network protocols: Network technology experts need to learn many RFCs related to network devices. Understanding the RFCs takes a long time, and the number of RFCs is still increasing.



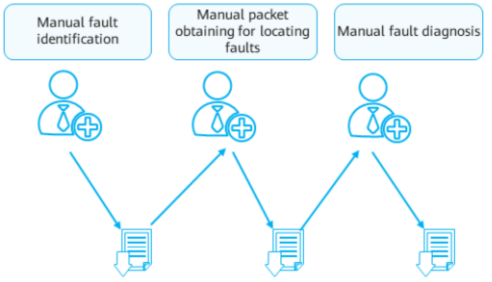
Difficult network configuration: To be familiar with devices of a specific vendor, you need to master tens of thousands of commands. Additionally, the number of commands is still increasing.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Difficulty in Locating and Analyzing Network Faults

Difficult to Spot Faults



- Traditional O&M networks rely on manual fault identification, location, and diagnosis.
- More than 85% of network faults are found only after service complaints. Problems cannot be proactively identified or analyzed.

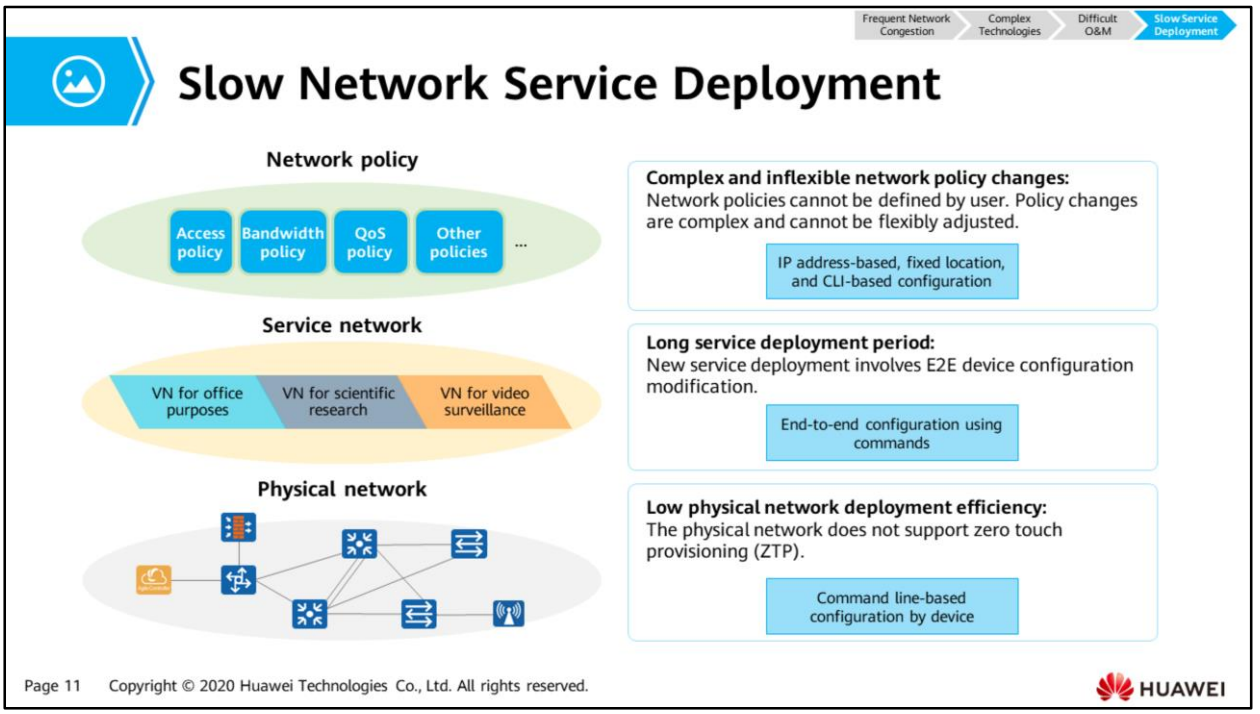
Difficult to Locate Faults

Abnormal flows account for 3.65% of all flows on the network.



- Traditional O&M only monitors device indicators. Some indicators are normal, but user experience is poor. There is no correlated analysis of users and networks.
- According to data center network (DCN) statistics, it takes 76 minutes to locate a fault on average.

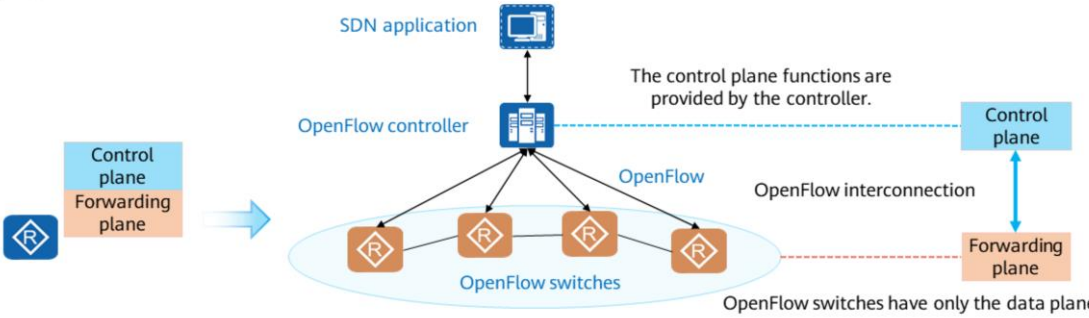
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Vision of network service deployment:
  - Free mobility based on network policies, regardless of physical locations
  - Quick deployment of new service
  - ZTP deployment on the physical network
  - Plug-and-play of devices

SDN Origin

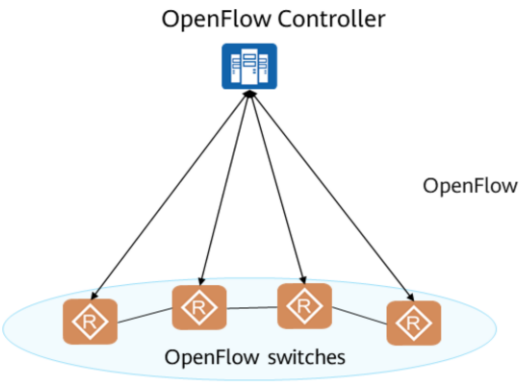
- SDN was developed by the Clean Slate Program at Stanford University as an innovative new network architecture. The core of SDN is to separate the control plane from the data plane of network devices to implement centralized control of the network control plane and provide good support for network application innovation.
- SDN has three characteristics in initial phase: forwarding-control separation, centralized control, and open programmable interfaces.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic Concepts of OpenFlow

- OpenFlow is an SBI protocol between a controller and a switch. It defines three types of messages: Controller-to-Switch, Asynchronous, and Symmetric. Each message contains more subtypes.



OpenFlow

Controller-to-Switch

This message is sent by the controller. It is used to manage and query switch information.

Asynchronous

This message is initiated by a switch. When the status of the switch changes, the switch sends this message to notify the controller of the status change.

Symmetric

This message can be initiated by a switch or controller. Symmetric messages include Hello, Echo, and Error messages.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Controller-to-Switch messages:
  - Features message: After an SSL/TCP session is established, the controller sends Features messages to a switch to request switch information. The switch must send a response, including the interface name, MAC address, and interface rate.
  - Configuration message: The controller can set or query the switch status.
  - Modify-State message: The controller sends this message to a switch to manage the switch status, that is, to add, delete, or modify the flow table and set interface attributes of the switch.
  - Read-State message: The controller sends this message to collect statistics on the switch.
  - Send-Packet message: The controller sends the message to a specific interface of the switch.
- Asynchronous messages:
  - Packet-in message: If no matching entry exists in the flow table or the action "send-to-controller" is matched, the switch sends a packet-in message to the controller.
  - Packet-out message: The controller sends this message to respond to a switch.
  - Flow-Removed message: When an entry is added to a switch, the timeout interval is set. When the timeout interval is reached, the entry is deleted. The switch then sends a Flow-Removed message to the controller. When an entry in the flow table needs to be deleted, the switch also sends this message to the controller.
  - Port-status message: A switch sends this message to notify the controller when the interface configuration or state changes.

- Symmetric messages:
    - Hello message: When an OpenFlow connection is established, the controller and switch immediately send an OFPT_HELLO message to each other. The version field in the message is filled with the latest OpenFlow version supported by the sender. After receiving the message, the receiver calculates the protocol version number, that is, selects the smaller one between the versions supported by the sender and the receiver. If the receiver supports the version, connection requests are processed until the connection is successful. Otherwise, the receiver replies with an OFPT_ERROR message, in which the type field is filled with ofp_error_type.OFPET_HELLO_FAILED.
    - Echo message: Either a switch or controller can send an Echo Request message, but the receiver must reply with an Echo Reply message. This message can be used to measure the latency and connectivity between the controller and switch. That is, Echo messages are heartbeat messages.
    - Error message: When a switch needs to notify the controller of a fault or error, the switch sends an Error message to the controller.
- The OpenFlow protocol is still being updated. For more message types, see the OpenFlow Switch Specification released by Open Networking Foundation (ONF).

Flow Table Overview

- OpenFlow switches forward packets based on flow tables.
- Each flow entry includes the Match Fields, Priority, Counters, Instructions, Timeouts, Cookie, and Flags. The Match Fields and Instructions are key fields for packet forwarding.
  - The Match Fields is a field against which a packet is matched and can be customized.
  - The Instructions field indicates OpenFlow processing when a packet matches a flow entry.

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie	Flags

Flow table fields can be customized. The following table is an example.

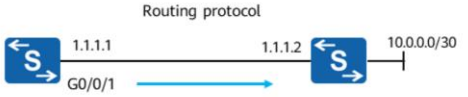
Ingress Port	Ether Source	Ether Dst	Ether Type	VLAN ID	VLAN Priority	IP Src	IP Dst	TCP Src Port	TCP Dst Port
3	MAC1	MAC2	0x8100	10	7	IP1	IP2	5321	8080

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Match Fields: a field against which a packet is matched. (OpenFlow 1.5.1 supports 45 options). It can contain the inbound interface, inter-flow table data, Layer 2 packet header, Layer 3 packet header, and Layer 4 port number.
- Priority: matching sequence of a flow entry. The flow entry with a higher priority is matched first.
- Counters: number of packets and bytes that match a flow entry.
- Instructions: OpenFlow processing when a packet matches a flow entry. When a packet matches a flow entry, an action defined in the Instructions field of each flow entry is executed. The Instructions field affects packets, action sets, and pipeline processing.
- Timeouts: aging time of flow entries, including Idle Time and Hard Time.
  - Idle Time: If no packet matches a flow entry after Idle Time expires, the flow entry is deleted.
  - Hard Time: After Hard Time expires, a flow entry is deleted regardless of whether a packet matches the flow entry.
- Cookie: identifier of a flow entry delivered by the controller.
- Flags: This field changes the management mode of flow entries.

Comparison Between Forwarding Modes

Typical Routing Protocol: Packet Forwarding Based on Routing Tables

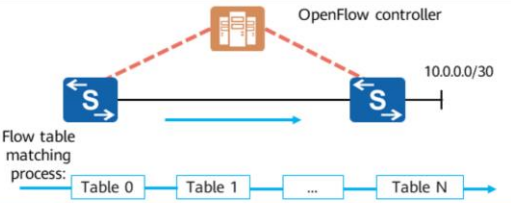


Routing table

Destination Network	Protocol	Next Hop	Outbound Interface
10.0.0.0/30	OSPF	1.1.1.2	G0/0/1

- In typical cases, network devices query routing tables to guide traffic forwarding.
- Entries in a routing table are calculated by running a routing protocol between network devices.
- The length of the routing table is fixed. Network devices forward packets based on the longest match rule. A network device has only one routing table.

OpenFlow: Packet Forwarding Based on Flow Tables



Flow table

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie

- OpenFlow is a network protocol. Switches running OpenFlow forward traffic based on flow tables.
- Flow tables are calculated by the OpenFlow controller and then delivered to switches.
- A flow table has variable length and defines various matching and forwarding rules. A network device has multiple flow tables.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- For tables 0-255, table 0 is first matched. In a flow table, flow entries are matched by priority. The flow entry with a higher priority is matched first.
- Currently, OpenFlow is mainly used on software switches, such as OVSs and CE1800Vs, in DCs, but not on physical switches to separate forwarding and control planes.

Essential Requirements of SDN

- The essence of SDN is to make networks more open, flexible, and simple. It builds a centralized brain for a network and implements fast service deployment, traffic optimization, or network service openness through centralized control in the global view.
- SDN has the following benefits:
  - Provides centralized management, simplifying network management and O&M.
  - Shields technical differences, simplifies network configuration, and reduces O&M costs.
  - Offers automatic optimization, improving network utilization.
  - Deploys services rapidly, shortening the service rollout time.
  - Builds an open network, supporting open and programmable third-party applications.

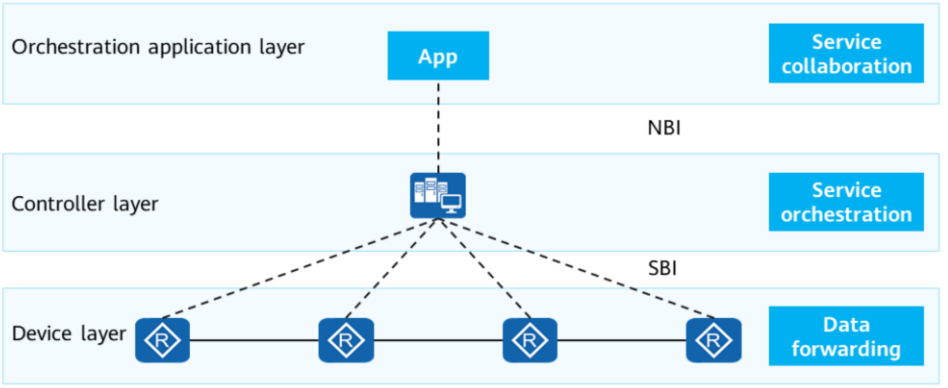
SDN transforms network architecture.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Forwarding-control separation is a method to implement SDN.

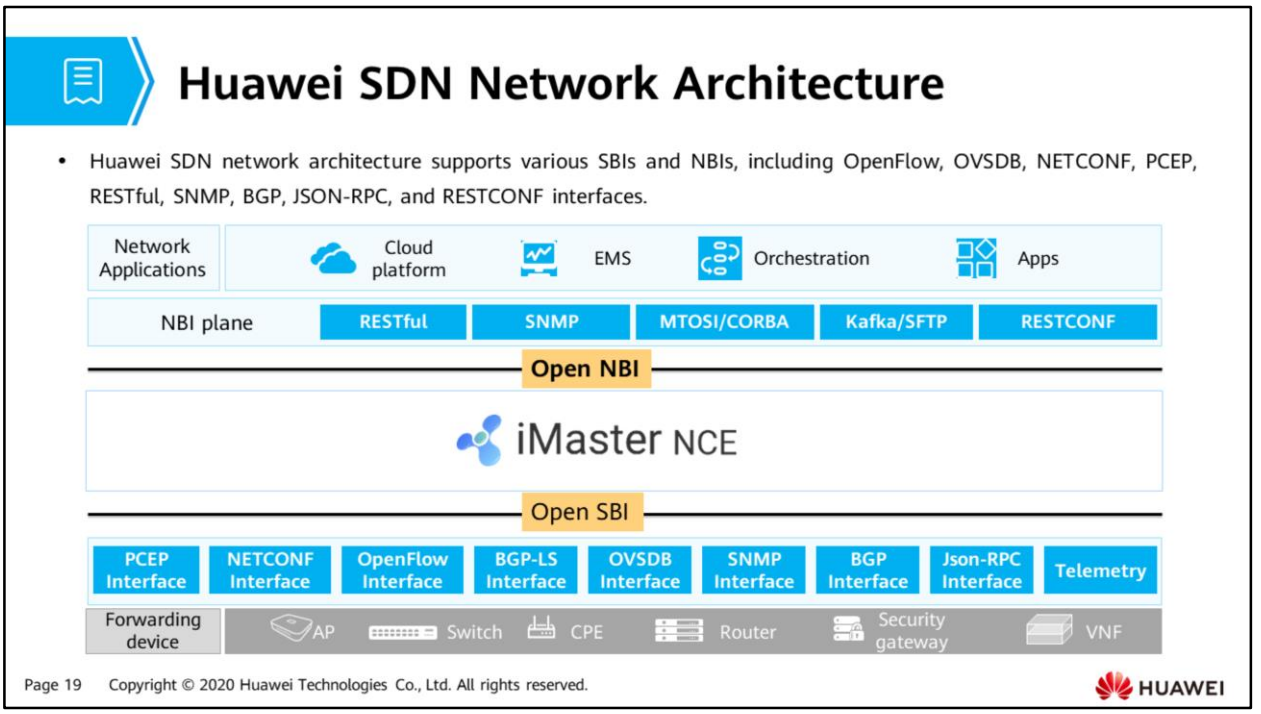
SDN Network Architecture

- The SDN network architecture consists of the orchestration application layer, controller layer, and device layer. Different layers are connected through open interfaces. From the perspective of the controller layer, SBIs oriented to the device layer and NBIs oriented to the orchestration application layer are distinguished. OpenFlow is one of SBI protocols.



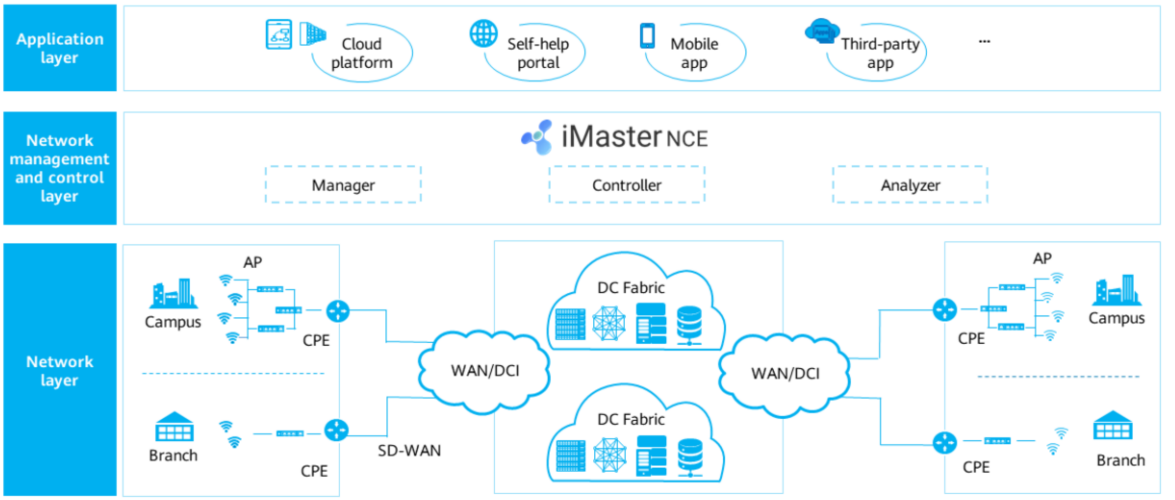
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Orchestration application layer: provides various upper-layer applications for service intents, such as OSS and OpenStack. The OSS is responsible for service orchestration of the entire network, and OpenStack is used for service orchestration of network, compute, and storage resources in a DC. There are other orchestration-layer applications. For example, a user wants to deploy a security app. The security app is irrelevant to the user host location but invokes NBIs of the controller. Then the controller delivers instructions to each network device. The command varies according to the SBI protocol.
- Controller layer: The SDN controller is deployed at this layer, which is the core of the SDN network architecture. The controller layer is the brain of the SDN system, and its core function is to implement network service orchestration.
- Device layer: A network device receives instructions from the controller and performs forwarding.
- NBI: NBIs are used by the controller to interconnect with the orchestration application layer, mainly RESTful.
- SBI: SBIs used by the controller to interact with devices through protocols such as NETCONF, SNMP, OpenFlow, and OVSDB.



- Cloud platform: resource management platform in a cloud DC. The cloud platform manages network, compute, and storage resources. OpenStack is the most mainstream open-source cloud platform.
- The Element Management System (EMS) manages one or more telecommunication network elements (NEs) of a specific type.
- Orchestration (container orchestration): The container orchestration tool can also provide the network service orchestration function. Kubernetes is a mainstream tool.
- MTOSI or CORBA is used to interconnect with the BSS or OSS. Kafka or SFTP can be used to connect to a big data platform.

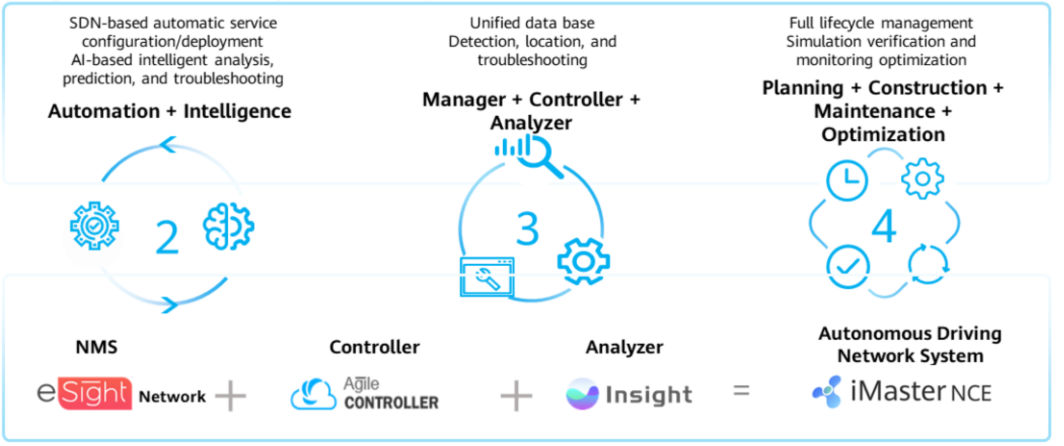
Huawei SDN Solution - Integrating Management, Control, and Analysis to Build an Intent-Driven Network



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Introduction to iMaster NCE

- Huawei iMaster NCE is the industry intelligent network automation platform that integrates management, control, analysis, and AI capabilities.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- iMaster NCE converts service intents into physical network configurations. It manages, controls, and analyzes global networks in a centralized manner in the southbound direction. It enables resource cloudification, full-lifecycle network automation, and intelligent closed-loop driven by data analysis for business and service intents. It provides northbound open APIs for quick integration with IT systems.
- iMaster NCE can be used in the enterprise data center network (DCN), enterprise campus, and enterprise branch interconnection (SD-WAN) scenarios to make enterprise networks simple, smart, open, and secure, accelerating enterprise service transformation and innovation.

iMaster NCE Application



iMaster NCE

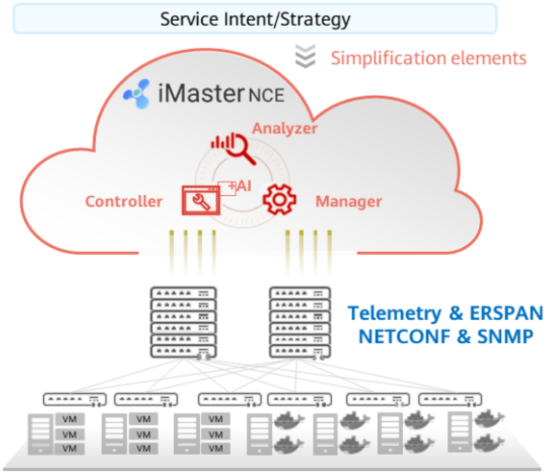
DC	iMaster NCE-Fabric *
Enterprise campus	iMaster NCE-Campus *
SD-WAN	iMaster NCE-WAN
IP WAN	iMaster NCE-IP
WAN transmission	iMaster NCE-T

* iMaster NCE-Fabric and iMaster NCE-Campus are introduced in this document.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Huawei CloudFabric DCN Autonomous Driving Network Solution

- Based on iMaster NCE-Fabric, DCNs provide full-lifecycle services from planning, construction, O&M, to optimization.



Integrated planning and construction:
- The planning tool interconnects with iMaster NCE-Fabric to implement integrated planning and construction.
- Zero Touch Provisioning (ZTP)

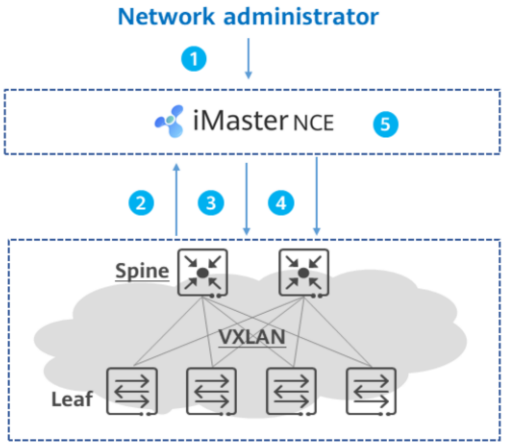
Simplified deployment
- Service intent self-understanding and conversion
- Network change simulation and evaluation, eliminating human errors

Intelligent O&M:
- Rapid fault detection and location based on knowledge graph and expert experience
- Fast fault rectification based on expert experiences and simulation analysis

Real-time optimization:
- AI-Fabric-oriented local traffic inference and online model training and optimization
- User behavior prediction and resource optimization suggestions

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Simplified ZTP Deployment

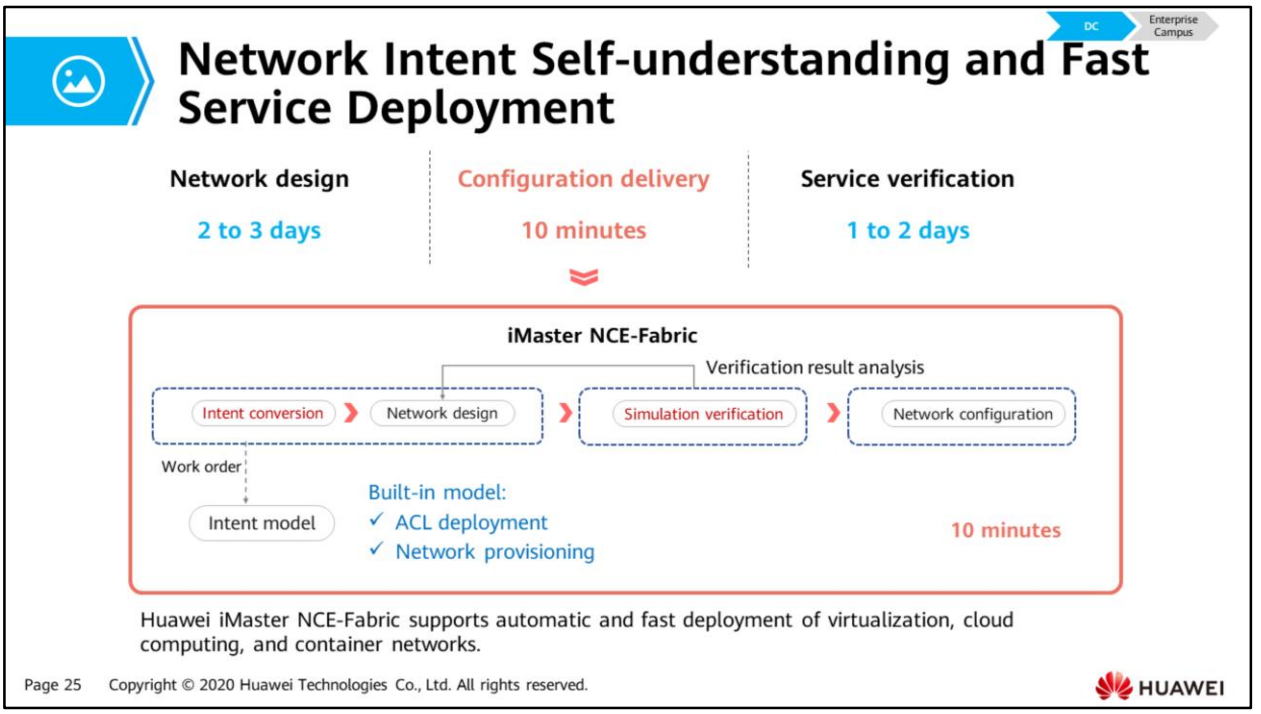


ZTP deployment process:

1. The network administrator clicks the icon on iMaster NCE to start the ZTP task.
2. A device automatically obtains an IP address to access iMaster NCE.
3. iMaster NCE determines the device role (spine or leaf node), delivers configurations such as the management IP address, SNMP configuration, and NETCONF configuration to online devices, and manages the devices through the management IP address.
4. iMaster NCE globally delivers interconnection configurations as well as OSPF or BGP configurations.
5. The device goes online successfully, and the administrator views network-wide information on iMaster NCE.

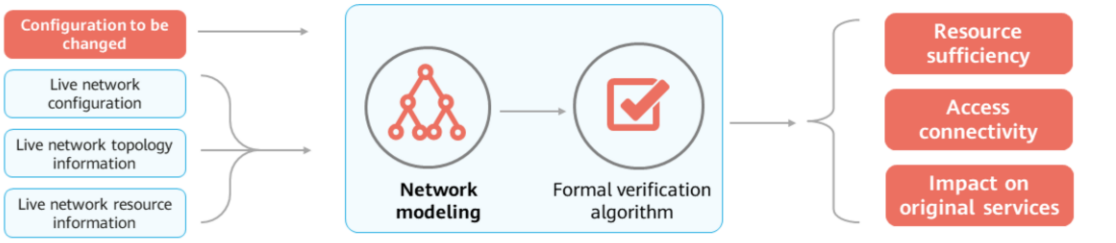
Note: The DC uses the spine-leaf architecture.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- iMaster NCE-Fabric can connect to a user's IT system to match the intent model for user intents and deliver configurations to devices through NETCONF to implement fast service deployment.
- iMaster NCE-Fabric can interconnect with the mainstream cloud platform (OpenStack), virtualization platform (vCenter/System Center), and container orchestration platforms (Kubernetes).

Network Change Simulation and Change Risk Prediction



Data collection/upload

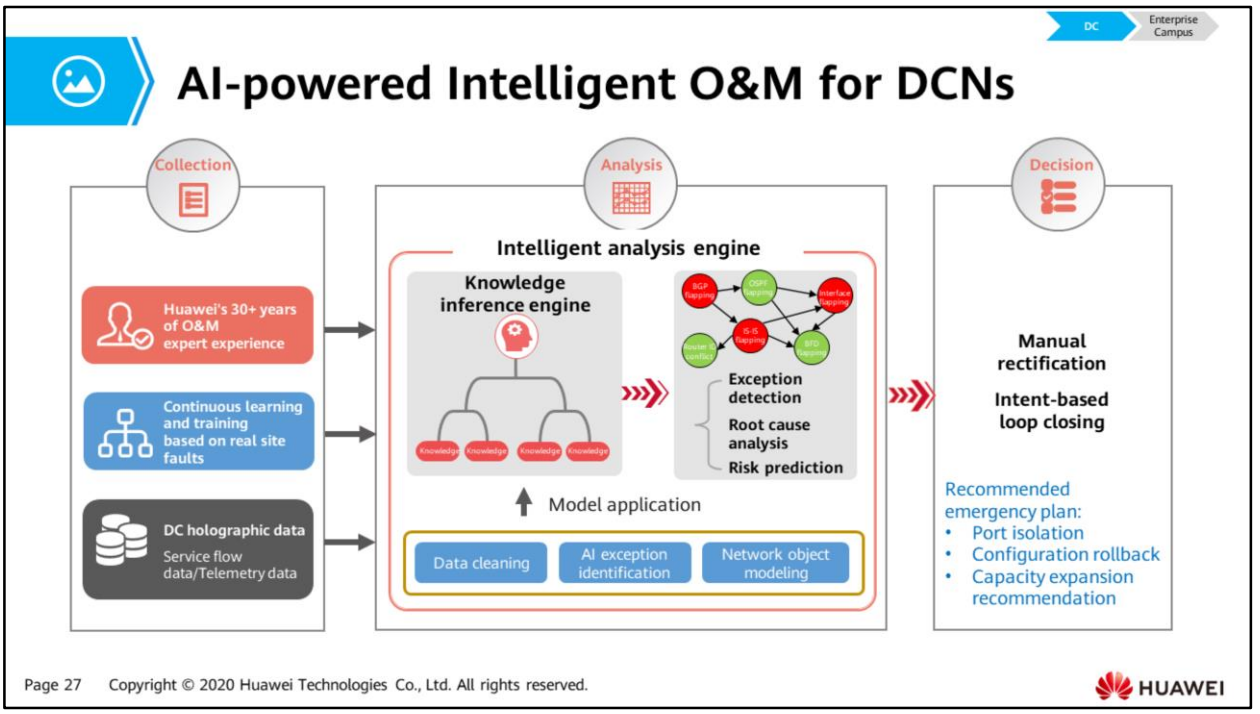
Modeling and Computing

- Establish physical, logical, and application network models.
- Use the formal verification algorithm for computing.

Verification result

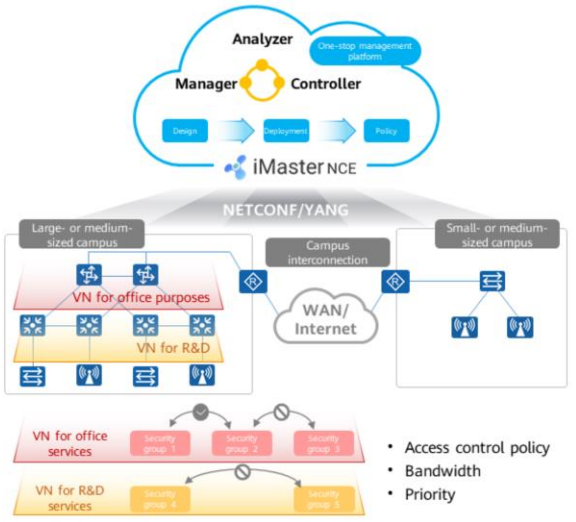
- Check whether resources on the live network are sufficient and whether the network is connected.
- Analyze and display the impact of changes on original services.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- iMaster NCE-FabricInsight provides AI-based intelligent O&M capabilities for DCs.

Huawei CloudCampus Autonomous Driving Network Solution



Fast network deployment, improving deployment efficiency by 600%

- Device plug-and-play: simplified device deployment, scenario navigation, and template-based configuration
- Simplified network deployment: Network resource pooling, multi-purpose network, and automatic service provisioning

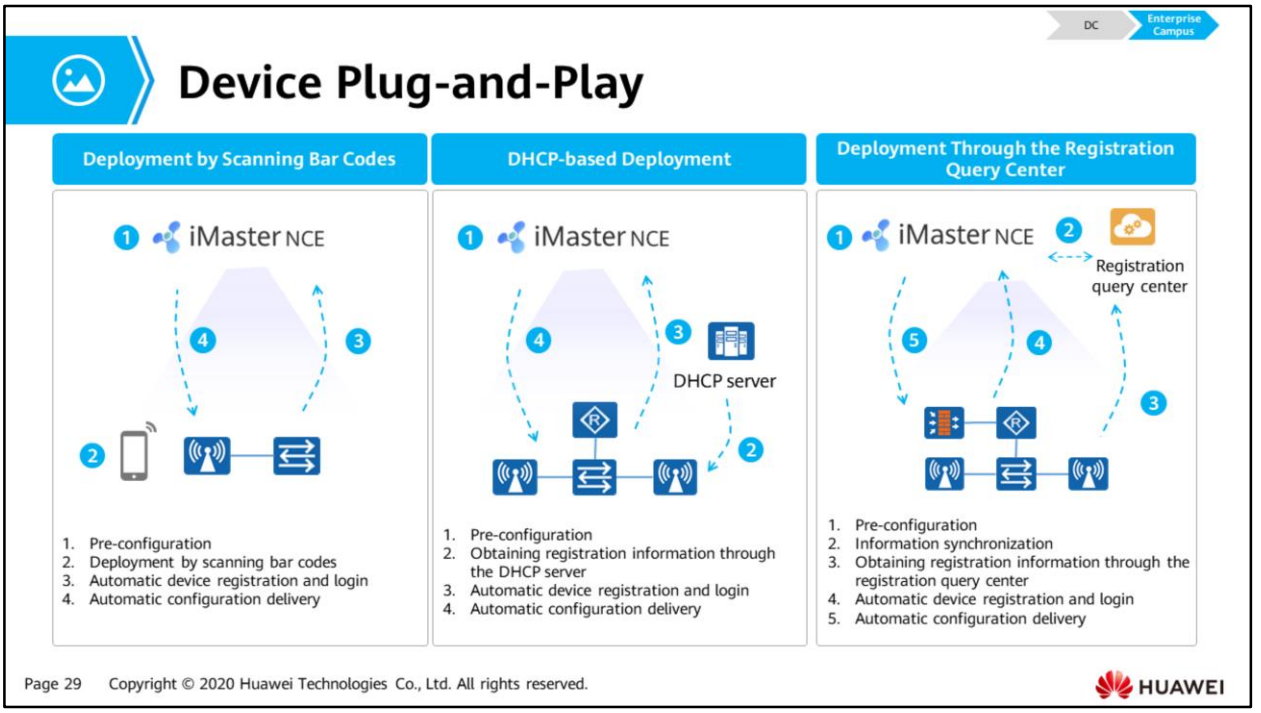
Fast service provisioning, improving user experience by 100%

- Free mobility: GUI-based policy configuration, allowing users to access the network anytime and anywhere without changing the roaming permission and user experience
- Intelligent terminal identification: Anti-spoofing for terminal access, with an intelligent terminal identification accuracy of over 95%
- Intelligent HQoS: Application-based scheduling and shaping, and refined bandwidth management, ensuring service experience of key users

Fast intelligent O&M, improving network performance by over 50%

- Real-time experience visualization: Telemetry-based network experience visualization at each moment, for each user, and in each area
- Precise fault analysis: Proactively identifying 85% of typical network issues and providing suggestions, and comparing and analyzing real-time data to predict faults
- Intelligent network optimization: Predictive optimization of wireless networks based on historical data, improving network-wide performance by over 50% (Source: Tolly Certification)

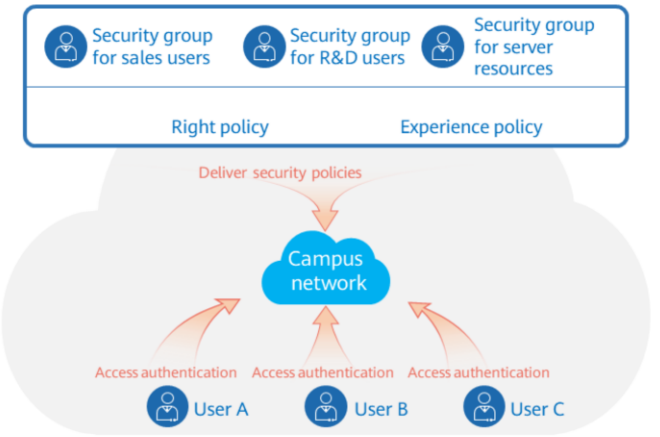
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Device plug-and-play includes but is not limited to deployment by scanning bar codes using an app, DHCP-based deployment, and deployment through the registration query center.
- Registration center: Huawei device registration query center, also called registration center, is one of the main components of Huawei CloudCampus solution. It is used to query the device management mode and registration ownership. A device determines whether to switch to the cloud-based management mode and which cloud management platform to register with based on the query result. The AP is used as an example. Huawei devices that support cloud-based management are pre-configured with the URL (register.naas.huawei.com) and port number (10020) of the Huawei device registration center.

Free Mobility: Policy Management Based on Security Groups

- Free mobility: Enables users to have consistent network rights and security policies regardless of their locations and IP addresses.

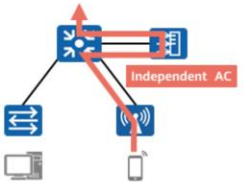


1. Use security groups. A security group is a group of users for which the same security policy is used.
2. Define security group-based permission control policies and user experience policies and deliver the policies to network devices.
3. A security group is authorized to a user after the user passes access authentication.
4. After user traffic enters a network, network devices enforce policies based on the source and destination security groups of the traffic.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

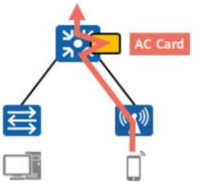
Wired and Wireless Convergence

WLAN Construction Mode 1: Standalone AC



- This mode poses a wireless traffic bottleneck and increases faulty nodes.
- Wired and wireless management is independent.
- Wired and wireless authentication points are separated.

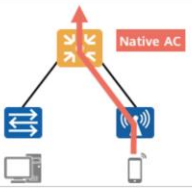
WLAN Construction Mode 2: AC Card



- An AC card is installed on a switch to provide AC functions.
- Hardware-level convergence.

Wired and wireless authentication point separation, distributed policy control, separation of control and data traffic forwarding, and troubleshooting and management difficulties.

Wired and Wireless Convergence (Native AC)



The switch integrates the AC function, eliminating wireless traffic forwarding bottlenecks and reducing fault nodes. Wired and wireless devices are centrally managed.

- Unified management and converged forwarding of wired and wireless services
- Converged management for wired and wireless users and gateway convergence
- Converged authentication points for wired and wireless access
- Unified wired and wireless policy execution

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Intelligent Terminal Identification, Ensuring Secure Access

Requirements and Challenges

A university

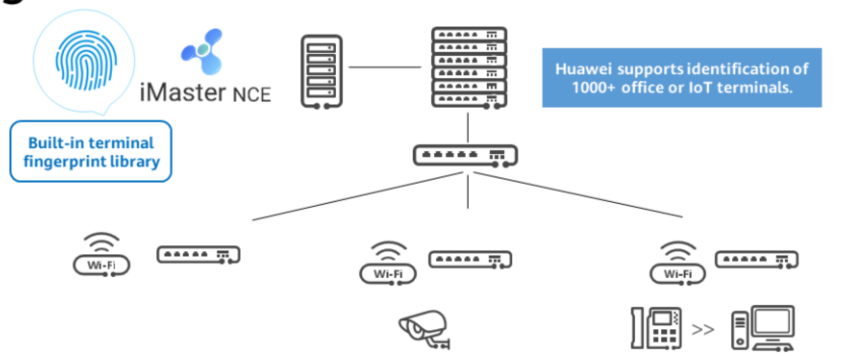
50+ types of smart terminals

Terminal information is collected by IT departments of colleges: MAC address collection is difficult and error-prone.

An enterprise

100+ authentication faults reported per day

It is difficult to locate access spoofing.



Terminal-type-based

Automatic authentication

Printer

- MAC address authentication, without entering any MAC address

Terminal-type-based

Automatic authorization

Camera

- Is automatically added to the video surveillance group.
- Is configured as the VIP user.

Terminal-type-based

Spoofing detection

IP phone and PC

- Report a terminal spoofing alarm.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HQoS: User- and Application-based QoS Policy

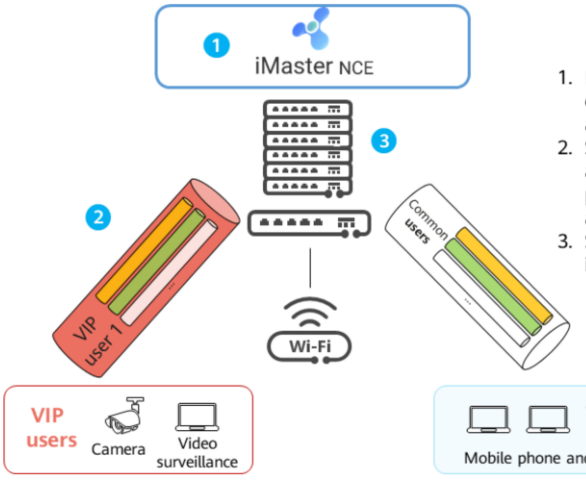
User- and application-based QoS policies ensure experience of high-priority users and applications

Requirements and Challenges

Traditional QoS policies are invalid for video services.

(Example) Building surveillance scenario: Wireless video services of common users increase, occupying a large number of network resources and causing network congestion.

>>

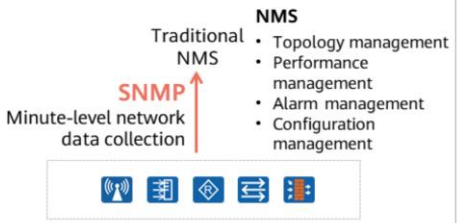


1. Define VIP users and common users, and application priorities.
2. Schedule users and application queues based on priorities of users and applications.
3. Support native AC or independent AC deployment.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

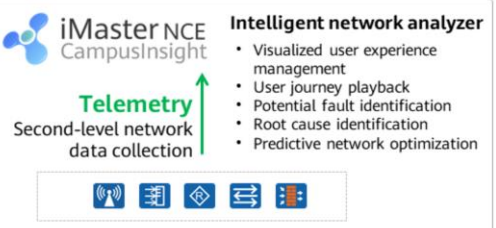
AI-Powered Intelligent O&M of Campus Networks

As-Is: Device-Centered Network Management



- **Device-centric O&M method**: User experience cannot be detected.
- **Fault-triggered responses**: Potential faults cannot be identified.
- Rely on professional engineers to **locate faults onsite**.

To-Be: User Experience-Centered AI-Powered Intelligent O&M



Experience visualization: Telemetry-based second-level data collection, visualized experience of each user and each application in real time

Minute-level potential fault identification and root cause location

- Identify potential faults based on dynamic baselines and big data correlation analysis.
- Accurately locate root causes of faults through KPI association analysis and protocol tracing.

Predictive network optimization: AI is used to intelligently analyze the AP load trend and implement predictive optimization on the wireless network.

The efficiency is improved by using algorithms. With scenario-based continuous learning and expert experience, intelligent O&M frees O&M personnel from complex alarms and noises, making O&M more automated and intelligent.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

AI-Powered Intelligent Radio Calibration

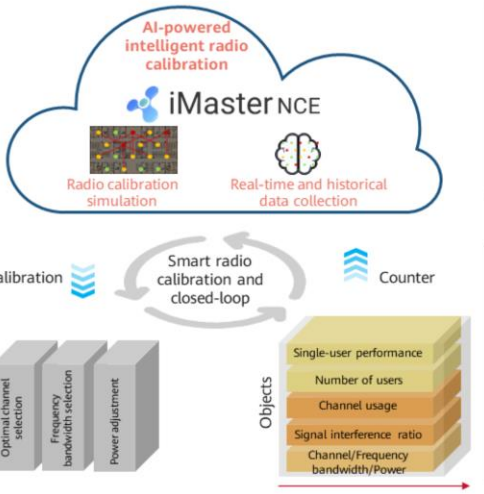
Traditional radio calibration cannot achieve expected results

Phase 1: Manual Calibration

Based on engineers' experience, the calibration is time-consuming and error-prone, and the calibration result is unstable.

Phase 2: Automatic Calibration

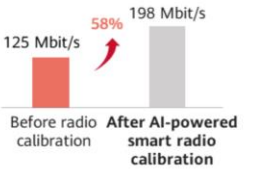
Calibration based on real-time radio interference does not consider device load changes, and the calibration result cannot be ensured.



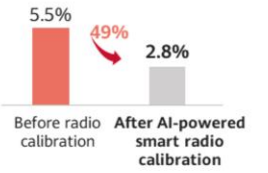
Tested and verified by authoritative organizations

Tolly.

Average downlink rate per terminal:



Average Wi-Fi channel interference



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Contents

1. SDN Overview
2. **NFV Overview**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

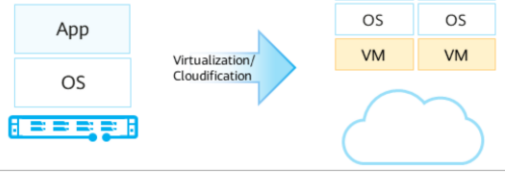
HUAWEI

NFV Background: Thinking from IT Industry Transformation

- The IT industry transformation brings thinking on network architecture and device architecture in the network industry. The network architecture layer involves the SDN controller and the device architecture layer involves the device deployment mode.

IT Industry Transformation

- In recent years, IT technologies such as virtualization and cloud computing have been booming, and applications deployed on hardware have been gradually migrated to the cloud. Applications are deployed on private clouds, public clouds, or hybrid clouds as software.





- Thinking about the network industry: Can network applications be deployed in a software-based manner?
- In the context, Network Functions Virtualization (NFV) is introduced.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Virtualized network functions (VNFs) are implemented by virtualizing traditional NEs such as IMSs and CPEs of carriers. After hardware is universalized, traditional NEs are no longer the products with embedded software and hardware. Instead, they are installed on universal hardware (NFVI) as software.

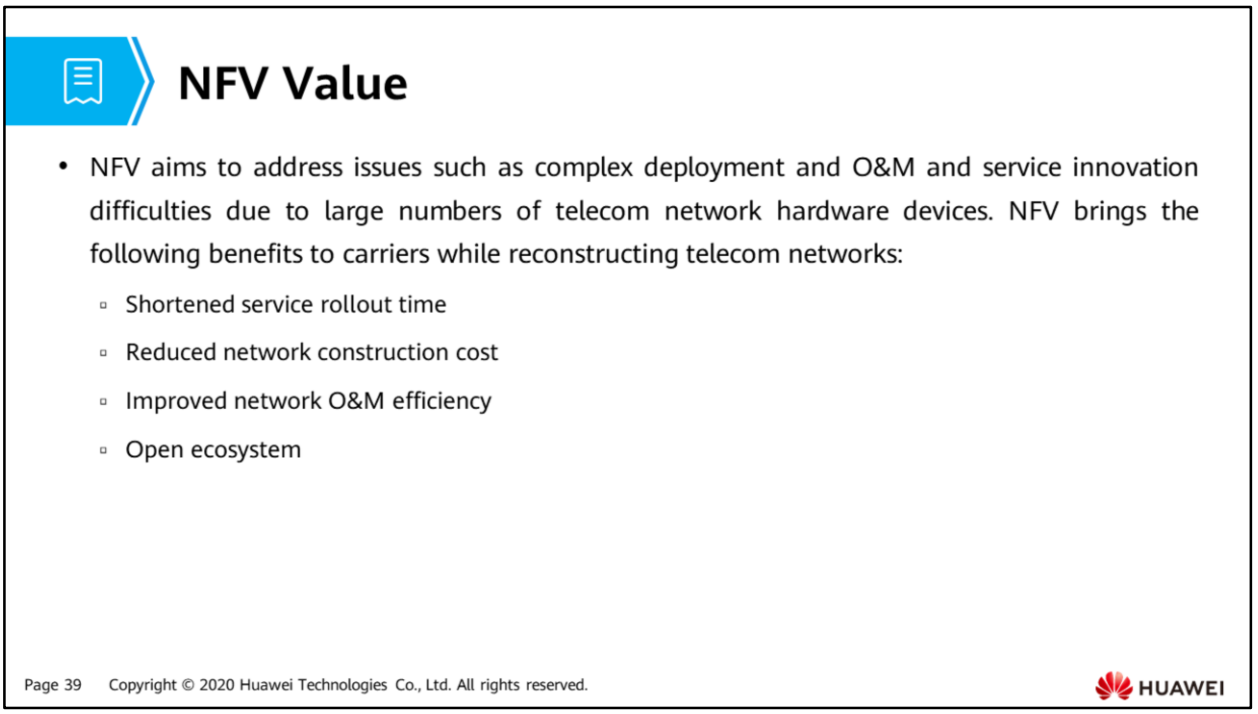
Origin of NFV

- In October 2012, 13 top carriers (including AT&T, Verizon, VDF, DT, T-Mobile, BT, and Telefonica) released the first version of NFV White Paper at the SDN and OpenFlow World Congress. In addition, the Industry Specification Group (ISG) was founded to promote the definition of network virtualization requirements and the formulation of the system architecture.
- In 2013, the ETSI NFV ISG conducted the first phase of research and completed the formulation of related standards. The ETSI NFV ISG defined NFV requirements and architecture and sorts out the standardization processes of different interfaces.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

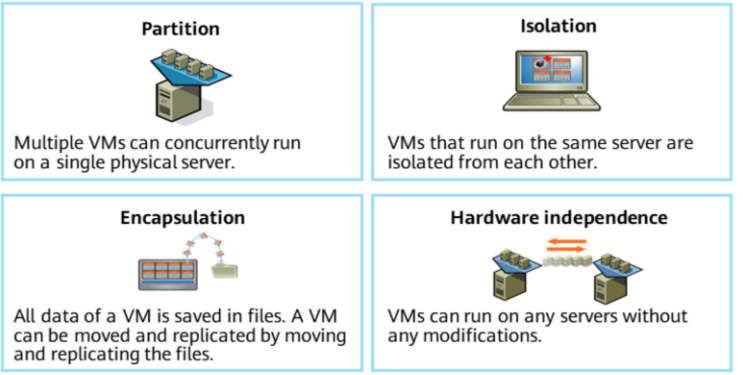
- In 2015, NFV research entered the second phase. The main research objective is to build an interoperable NFV ecosystem, promote wider industry participation, and ensure that the requirements defined in phase 1 are met. In addition, the ETSI NFV ISG specified the collaboration relationships between NFV and SDN standards and open source projects. Five working groups are involved in NFV phase 2: IFA (architecture and interface), EVE (ecosystem), REL (reliability), SEC (security), and TST (test, execution, and open source). Each working group mainly discusses the deliverable document framework and delivery plan.
- The ETSI NFV standard organization cooperates with the Linux Foundation to start the open source project OPNFV (NFV open source project, providing an integrated and open reference platform), integrate resources in the industry, and actively build the NFV industry ecosystem. In 2015, OPNFV released the first version, further promoting NFV commercial deployment.
- NFV-related standard organizations include:
  - ETSI NFV ISG: formulates NFV requirements and functional frameworks.
  - 3GPP SA5 working group: focuses on technical standards and specifications of 3GPP NE virtualization management (MANO-related).
  - OPNFV: provides an open-source platform project that accelerates NFV marketization.



- Shortened service rollout time: In the NFV architecture, adding new service nodes becomes simple. No complex site survey or hardware installation is required. For service deployment, you only need to request virtual resources (compute, storage, and network resources) and software loading, simplifying network deployment. To update service logic, you simply need to add new software or load new service modules to complete service orchestration. Service innovations become simple.
- Reduced network construction cost: Virtualized NEs can be integrated into COTS devices to reduce the cost. Enhancing network resource utilization and lowering power consumption can lower overall network costs. NFV uses cloud computing technologies and universal hardware to build a unified resource pool. Resources are dynamically allocated on demand based on service requirements, implementing resource sharing and improving resource utilization. For example, automatic scale-in and scale-out can be used to solve the resource usage problem in the tidal effect.
- Enhanced network O&M efficiency: Automated and centralized management improves the operation efficiency and reduces the O&M cost. Automation includes DC-based hardware unit management automation, MANO application service life management automation, NFV- or SDN-based coordinated network automation.
- Open ecosystem: The legacy telecom network exclusive software/hardware model defines a closed system. NFV-based telecom networks use an architecture based on standard hardware platforms and virtual software. The architecture easily provides open platforms and open interfaces for third-party developers, and allows carriers to build open ecosystems together with third-party partners.

Key NFV Technologies: Virtualization

- Virtualization is the foundation of NFV, and cloudification is the key.
- On traditional telecom networks, each NE is implemented by dedicated hardware, resulting in high costs and difficult O&M. Virtualization features partition, isolation, encapsulation, and independence from hardware, which can meet NFV requirements. Carriers use virtualization to run software-based NEs on universal infrastructures.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- On traditional telecom networks, each NE is implemented by dedicated hardware. A large number of hardware interoperability tests, installation, and configuration are required during network construction, which is time-consuming and labor-consuming. In addition, service innovation depends on the implementation of hardware vendors, which is time-consuming and cannot meet carriers' service innovation requirements. In this context, carriers want to introduce the virtualization mode to provide software NEs and run them on universal infrastructures (including universal servers, storage devices, and switches).
- Using universal hardware helps carriers reduce the cost of purchasing dedicated hardware. Service software can be rapidly developed through iteration, which enables carriers to innovate services quickly and improve their competitiveness. By dong this, carriers can enter the cloud computing market.

Key NFV Technology: Cloudification

- As defined by the National Institute of Standards and Technology (NIST), cloud computing is a model that allows users to obtain resources (for example, networks, servers, storage devices, applications, services) in a shared compute resource pool based on their needs anytime, anywhere. This model enables fast resource provisioning and release, and minimizes the resource management workload and interactions with service providers.
- Cloud computing has many advantages. Cloudification of network functions on carriers' networks mainly uses resource pooling and rapid elastic scaling.

Characteristics of Cloud Computing

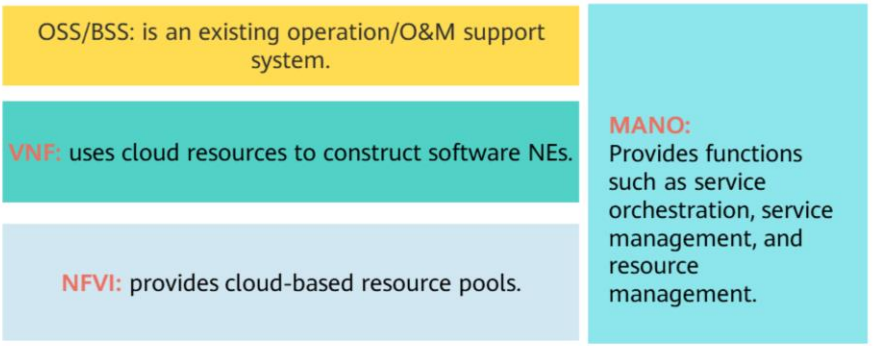


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- According to the NIST, cloud computing services have the following characteristics:
  - On-demand self-service: Cloud computing implements on-demand self-service of IT resources. Resources cna be requested and released without intervention of IT administrators.
  - Broad network access: Users can access networks anytime and anywhere.
  - Resource pooling: Resources including networks, servers, and storage devices in a resource pool can be provided for users.
  - Rapid elasticity: Resources can be quickly provisioned and released. The resource can be used immediately after being requested, and can be reclaimed immediately after being released.
  - Measured service: The charging basis is that used resources are measurable. For example, charging is based on the number of CPUs, storage space, and network bandwidth.

Introduction to the NFV Architecture

- The NFV architecture includes the network functions virtualization infrastructure (NFVI), a virtualized network function (VNF), and management and orchestration (MANO). In addition, the NFV architecture needs to support the existing business support system (BSS) or operations support system (OSS).

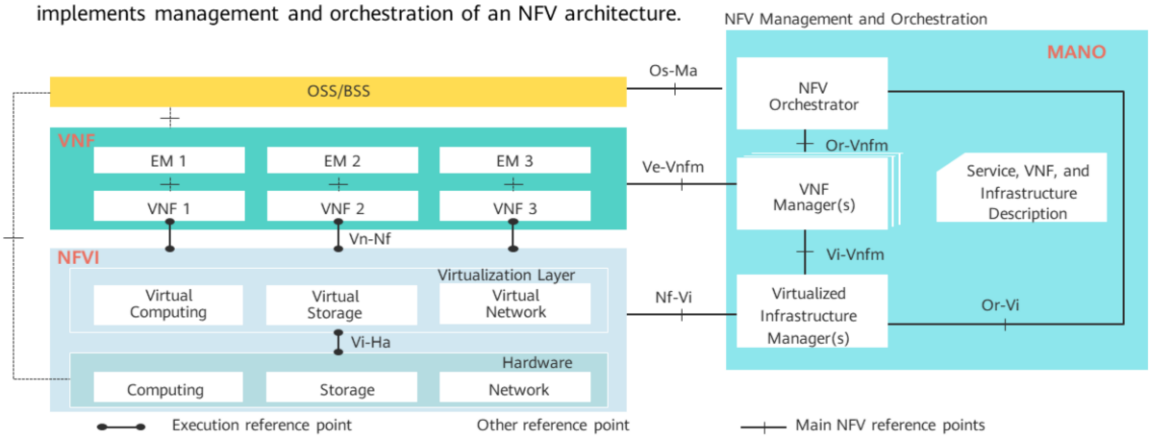


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

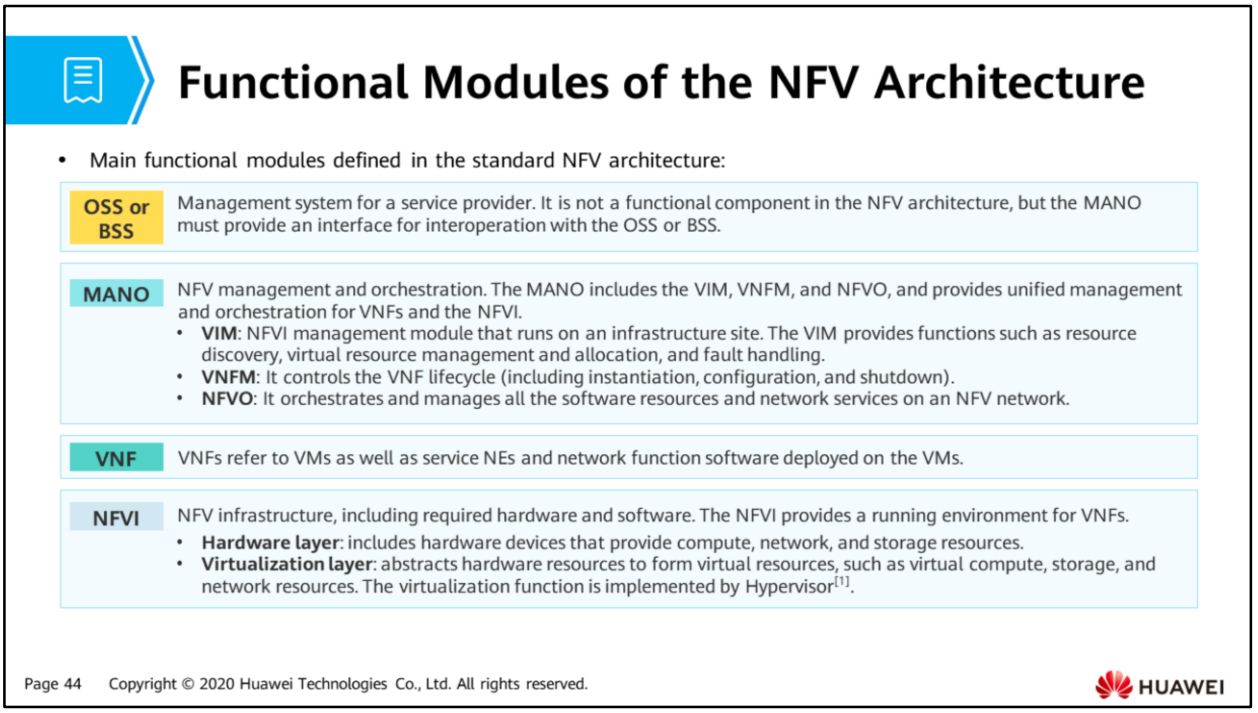
- Each layer of the NFV architecture can be provided by different vendors, which improves system development but increases system integration complexity.
- NFV implements efficient resource utilization through device normalization and software and hardware decoupling, reducing carriers' TCO, shortening service rollout time, and building an open industry ecosystem.
- The NFVI consists of the hardware layer and virtualization layer, which are also called COTS and CloudOS in the industry.
  - COTS: universal hardware, focusing on availability and universality, for example, Huawei FusionServer series hardware server.
  - CloudOS: cloud-based platform software, which can be regarded as the operating system of the telecom industry. CloudOS virtualizes physical compute, storage, and network resources into virtual resources for upper-layer software to use, for example, Huawei FusionSphere.
- VNF: A VNF can be considered as an app with different network functions and is implemented by software of traditional NEs (such as IMS, EPC, BRAS, and CPE) of carriers.
- MANO: MANO is introduced to provision network services in the NFV multi-CT or multi-IT vendor environment, including allocating physical and virtual resources, vertically streamlining management layers, and quickly adapting to and interconnecting with new vendors' NEs. The MANO includes the Network Functions Virtualization Orchestrator (NFVO, responsible for lifecycle management of network services), Virtualized Network Function Manager (VNFM, responsible for lifecycle management of VNFs), and Virtualized Infrastructure Manager (VIM, responsible for resource management of the NFVI).

Standard NFV Architecture

- ETSI defines the standard NFV architecture, which consists of the NFVI, VNF, and MANO. The NFVI includes the universal hardware layer and virtualization layer. The VNF is implemented using software, and the MANO implements management and orchestration of an NFV architecture.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- BSS: business support system
- OSS: operation support system
- A hypervisor is a software layer between physical servers and OSs. It allows multiple OSs and applications to share the same set of physical hardware. It can be regarded as a meta operating system in the virtual environment, and can coordinate all physical resources and VMs on the server. It is also called virtual machine monitor (VMM). The hypervisor is the core of all virtualization technologies. Mainstream hypervisors include KVM, VMWare ESXi, Xen, and Hyper-V.

NFV Architecture Interfaces

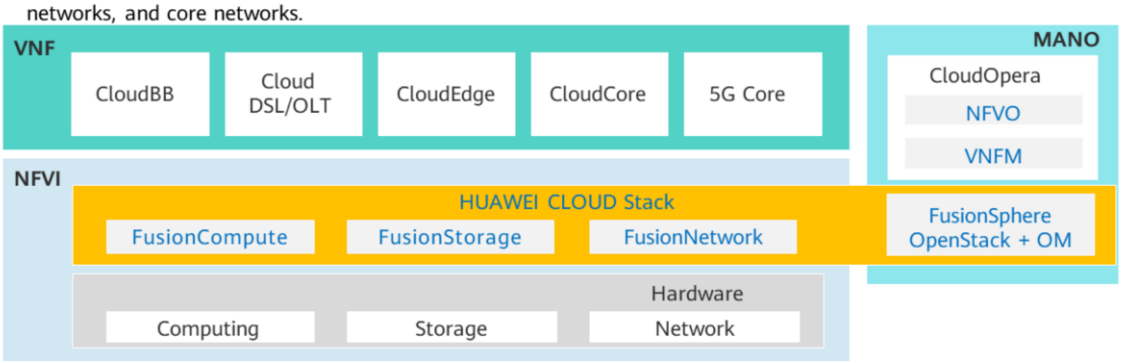
- Main interfaces of the standard NFV architecture:

Interface	Description
Vi-Ha	Is used between the virtualization layer and hardware layer. The virtualization layer meets basic hardware compatibility requirements.
Vn-Nf	Is used between a VM and the NFVI. It ensures that VMs can be deployed on the NFVI to meet performance, reliability, and scalability requirements. The NFVI meets VMs' OS compatibility requirements.
Nf-Vi	Is used between the virtualization layer management software and NFVI. It provides management of virtual computing, storage, and network systems of NFVI, virtual infrastructure configuration and connections, as well as system usage, performance monitoring, and fault management.
Ve-Vnfm	Is used between the VNFM and a VNF, implementing VNF lifecycle management, VNF configuration, VNF performance, and fault management.
OS-Ma	Manages lifecycles of network services and VNFs.
Vi-Vnfm	Is used for interaction between the service application management system or service orchestration system and virtualization layer management software.
Or-Vnfm	Sends configuration information to the VNFM, configures the VNFM, and connects the orchestrator and VNFM. It exchanges information with the NFVI resources allocated to VNFs and information between VNFs.
Or-Vi	Is used to send resource reservation and resource allocation requests required by the orchestrator and exchange virtual hardware resource configurations and status information.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Huawei's NFV Solution

- In the Huawei NFV architecture, functions of the virtualization layer and VIM are implemented by the HUAWEI CLOUD Stack NFVI platform. HUAWEI CLOUD Stack can virtualize compute, storage, and network resources and centrally manage, monitor, and optimize physical virtualization resources.
- Huawei provides cloud-based solutions for carriers' wireless networks, bearer networks, transport networks, access networks, and core networks.



 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- DSL: Digital Subscriber Line
- OLT: Optical Line Terminal

FAQ

- Q1: What is the relationship between SDN and NFV in the industry?
- A: Both SDN and NFV involve network transformation and the NFV concept was proposed at the SDN and OpenFlow World Congress. However, they are independent of each other. SDN mainly affects the network architecture, and NFV mainly affects the NE deployment mode.

- Q2: What is the relationship between SDN and NFV in Huawei solutions?
- A: Huawei provides different solutions for SDN and NFV, but they are associated. Huawei NFVI solution is provided by HUAWEI CLOUD Stack.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Quiz

1. (Multiple) Which of the following statements about Huawei SDN solution are true? ( )
   A. The solution supports various SBI protocols, such as RESTful, NETCONF, and OVSDB.
   B. OpenFlow can be used as the SBI protocol.
   C. The solution integrates management, control, and analysis to build a simplified network.
   D. The solution provides open and programmable network interfaces to support third-party application development and system interconnection.
2. Please briefly describe the benefits of NFV.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

1. BCD
2. NFV aims to address issues such as complex deployment and O&M and service innovation difficulties due to large numbers of telecom network hardware devices. NFV brings the following benefits to carriers while reconstructing telecom networks:
   - Shortened service rollout time
   - Reduced network construction cost
   - Improved network O&M efficiency
   - Open ecosystem

Summary

- With the transformation and development of the network industry, SDN and NFV are proposed.
- SDN is an innovation of network architecture. It uses a controller to make networks more open, flexible, and simple.
- NFV is an innovation in the deployment of telecom network devices. Based on virtualization and cloud computing, NFV helps reconstruct telecom networks.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

More Information

- For more information about OpenFlow, visit *https://www.opennetworking.org/* .
- For more information about Huawei SDN solution, see the HCIP course.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Network Programmability and Automation

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- New protocols, technologies, and delivery and O&M modes are emerging in the network engineering field. Conventional networks face challenges from new connection requirements, such as requirements for cloud computing and artificial intelligence (AI). Enterprises are also pursuing service agility, flexibility, and elasticity. Against this backdrop, network automation becomes increasingly important.
- Network programmability and automation is to simplify network configuration, management, monitoring, and operations for engineers and improve deployment and O&M efficiency. This course is to help network engineers understand Python programming and implement network automation.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- On completion of this course, you will be able to:
  - Describe the difficulties of conventional network O&M.
  - Understand the implementation of network automation.
  - Understand the classification of programming languages.
  - Describe the Python code style.
  - Describe the basic usage of Python telnetlib.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

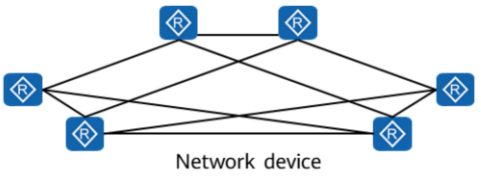
1. **Introduction to Network Programmability and Automation**
2. Overview of Programming Language and Python
3. Cases

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Background: Difficulties in Conventional Network O&M

- Conventional network O&M requires network engineers to manually log in to network devices, query and execute configuration commands, and filter command output. This highly human-dependent working mode is time-consuming, inefficient, and difficult to audit.

Numerous devices
Complex operations
Low efficiency



Network device

Typical O&M Scenarios

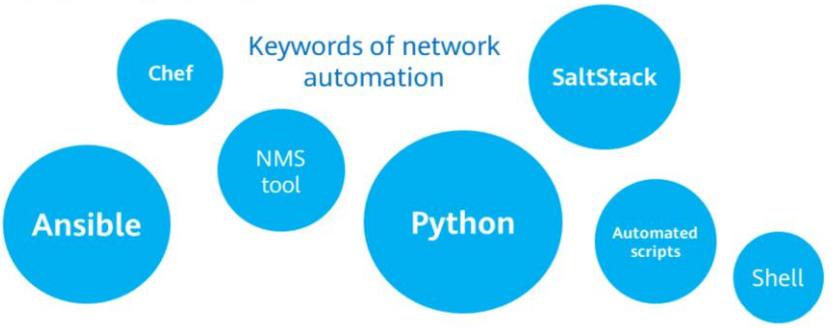
Are the following working scenes familiar to you?

1. Device upgrade: Thousands of network devices reside on a live network. You have to periodically upgrade the devices in batches.
2. Configuration audit: An enterprise needs to audit the configuration of devices every year. For example, the enterprise requires that STelnet be enabled on all devices and spanning tree security be configured on Ethernet switches. In this case, you have to quickly find out the devices that do not meet the requirements.
3. Configuration change: Due to network security requirements, device accounts and passwords need to be changed every three months. You have to delete the original account and create an account on thousands of network devices.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Network Automation

- Network automation: Tools are used to implement automated network deployment, operations, and O&M, gradually reducing dependency on human. This solves the conventional network O&M problems.
- Many open-source tools, such as Ansible, SaltStack, Puppet, and Chef, are available for network automation in the industry. From the perspective of network engineering capability construction, it is recommended that engineers acquire the code programming capability.

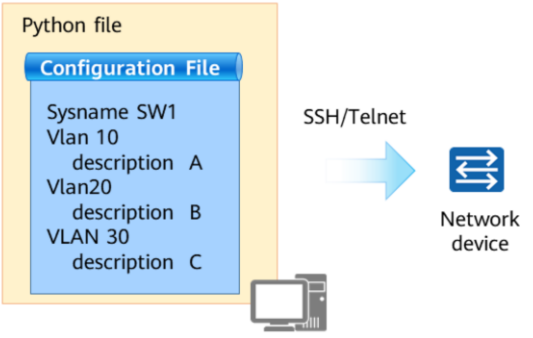


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Many network automation tools in the industry, such as Ansible, SaltStack, Puppet, and Chef, are derived from open-source tools. It is recommended that network engineers acquire the code programming capability.

Programming-based Network Automation

- In recent years, with the emergence of network automation technologies, Python-based programming capabilities have become a new skill requirement for network engineers.
- Automation script written in Python can execute repeated, time-consuming, and rule-based operations.



Example: Implementing automated device configuration using Python

- What can network automation do? The most intuitive example of network automation is automated device configuration. This process can be divided into two steps: writing a configuration file, and writing Python code to push the configuration file to a device.
- Write the configuration script in command line interface (CLI) mode, and then upload the script to the device using Telnet/SSH. This method is easy to understand for network engineers who are beginning to learn network programmability and automation. This presentation describes how to implement network automation.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

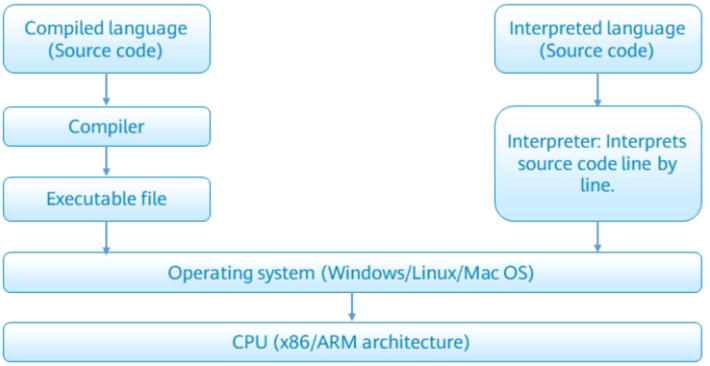
Contents

1. Introduction to Network Programmability and Automation
2. **Overview of Programming Language and Python**
3. Cases

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

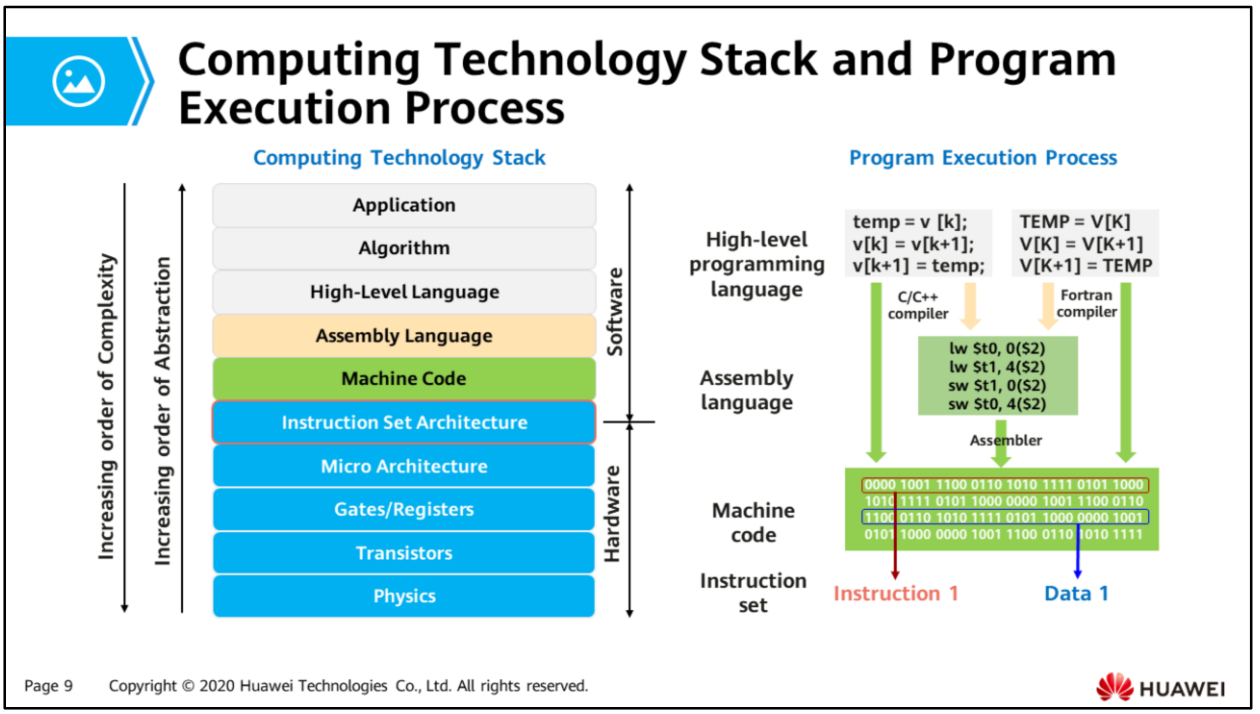
Programming Languages

- A programming language is used to write a computer program and control behavior of a computer.
- According to whether compilation is required before execution of a language, the programming language may be classified into the compiled language, and interpreted language that does not need to be compiled.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

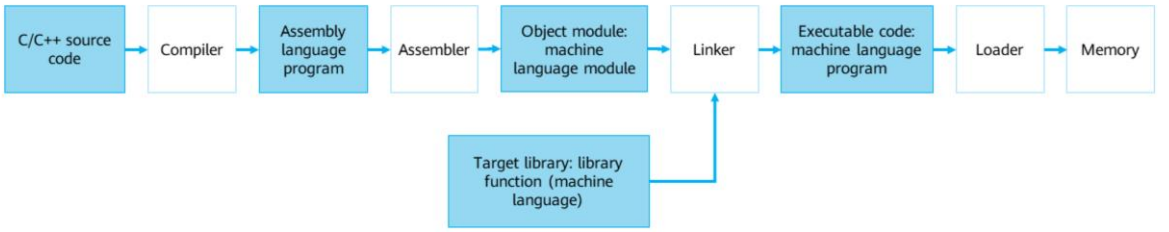
- Based on language levels, computer languages can also be classified into machine language, assembly language, and high-level language. The machine language consists of 0 and 1 instructions that can be directly identified by a machine. Because machine languages are obscure, hardware instructions 0 and 1 are encapsulated to facilitate identification and memory (such as MOV and ADD), which is assembly language. The two languages are low-level languages, and other languages are high-level languages, such as C, C++, Java, Python, Pascal, Lisp, Prolog, FoxPro, and Fortran. Programs written in high-level languages cannot be directly identified by computers. The programs must be converted into machine languages before being executed.



- A process of executing a computer's technology stack and programs. On the left is the computing technology stack. From the bottom layer of the hardware, physical materials and transistors are used to implement gate circuits and registers, and then the micro architecture of the CPU is formed. The instruction set of the CPU is an interface between hardware and software. An application drives hardware to complete calculation using an instruction defined in the instruction set.
- Applications use certain software algorithms to implement service functions. Programs are usually developed using high-level languages, such as C, C++, Java, Go, and Python. The high-level language needs to be compiled into an assembly language, and then the assembler converts the assembly language into binary machine code based on a CPU instruction set.
- A program on disk is a binary machine code consisting of a pile of instructions and data, that is, a binary file.

High-level Programming Language - Compiled Language

- Compiled language: Before a program in a compiled language is executed, a compilation process is performed to compile the program into a machine language file. The compilation result can be directly used without re-translation during running. Typical compiled languages include C/C++ and Go.
- From source code to program: The source code needs to be translated into machine instructions by the compiler and assembler, and then the linker uses the link library function to generate the machine language program. The machine language must match the instruction set of the CPU, which is loaded to the memory by the loader during running and executed by the CPU.

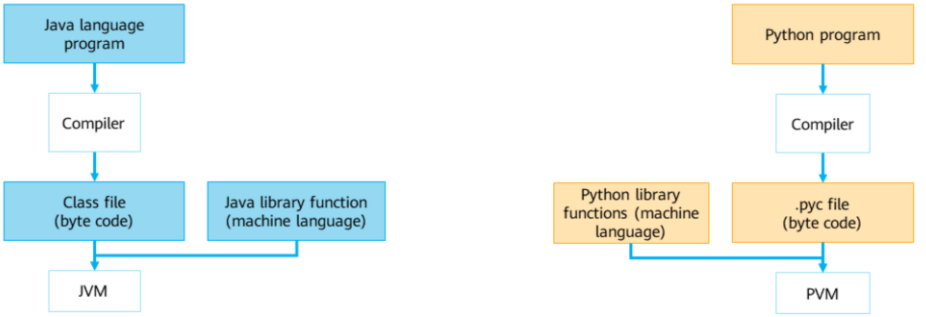


 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- Compiled languages are compiled into formats, such as .exe, .dll, and .ocx, that can be executed by machines. Compilation and execution are separated and cannot be performed across platforms. For example, x86 programs cannot run on ARM servers.

High-level Programming Language - Interpreted Language

- Interpreted language: Interpreted language programs do not need to be compiled before running. They are translated line by line when running. Typically, Java and Python are interpreted languages.
- Process from source code to programs: Source code of an interpreted language is generated by the compiler and then interpreted and executed by a virtual machine (VM) (for example, JVM/PVM). The VM shields the differences between CPU instruction sets. Therefore, portability of the interpreted language is relatively good.



Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- JVM: Java virtual machine
- PVM: Python VM



What Is Python?

- Python is a fully-open-source high-level programming language. Its author is Guido Van Rossum.

Advantages of Python:

- Is a dynamically typed interpreted language with elegant syntax. It allows learners to focus on program logic rather than syntax detail learning.
- Supports both process- and object-oriented programming.
- Provides abundant third-party libraries.
- Is nicknamed the glue language because it can call code written in other languages.

Disadvantages of Python:

- Runs slow. Is an interpreted language that runs without being compiled. Code is translated line by line at run time into machine code that the CPU can understand, which is time-consuming.

With support for abundant third-party libraries and advantages of the Python language, Python can be used in many fields, such as AI, data science, apps, and scripts for automated O&M.

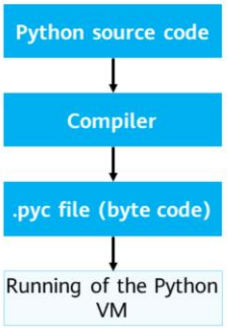
 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Python is also a dynamically typed language. The dynamically typed language automatically determines the type of variable during program running. The type of a variable does not need to be declared.

Python Code Execution Process

Process of compiling and running a Python program



Operation

1. Install Python and the running environment in an operating system.
2. Compile Python source code.
3. The compiler runs the Python source code and generates a .pyc file (byte code).
4. A Python VM converts the byte code into the machine language.
5. Hardware executes the machine language.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Python source code does not need to be compiled into binary code. Python can run programs directly from the source code. When Python code is run, the Python interpreter first converts the source code into byte code, and then the Python VM executes the byte code.
- The Python VM is not an independent program and does not need to be installed independently.

Getting Started with Python Code - Interactive Running

- Python runs in either interactive or script mode.
- Interactive programming does not require script files to be created, and code is written in the interactive mode of the Python interpreter.

```
C:\Users\Richard>python
Python 3.7.4 (default, Aug  9 2019, 18:34:13)  [MSC v.1915 64 bit (AMD64)] ::
Anaconda, Inc. on win32
Type "help", "copyright", "credits" or "license" for more information.
1. Input  -- >>> print ("hello world")
2. Output -- hello world
3. Input  -- >>> a = 1
4. Input  -- >>> b = 2
5. Input  -- >>> print ( a + b )
6. Output -- 3
>>>
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Getting Started with Python Code - Script-based Running

- Code in script mode can run on various Python compilers or in integrated development environments. For example, IDLE, Atom, Visual Studio, Pycharm, and Anaconda provided by Python can be used.

demo.py

```
print ("hello world")
a = 1
b = 2
print ( a + b )
```

1. Input --
2. Output --
3. Output --

```
C:\Users\Richard>python demo.py
hello world
3
```

1 Write a Python script file (.py).

2 Execute the script file.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Code Style Guide for Python

- Code style rules refer to naming rules, code indentation, and code and statement segmentation modes that must be complied with when Python is used to write code. Good style rules help improve code readability and facilitate code maintenance and modification.
- For example, the following rules for using semicolons, parentheses, blank lines, and spaces are recommended:

Semicolon

- A semicolon can be added at the end of a line in Python, but is not recommended to separate statements.
- It is recommended that each sentence be in a separate line.

Blank line

- Different functions or statement blocks can be separated by spaces. A blank line helps differentiate two segments of code, improving code readability.

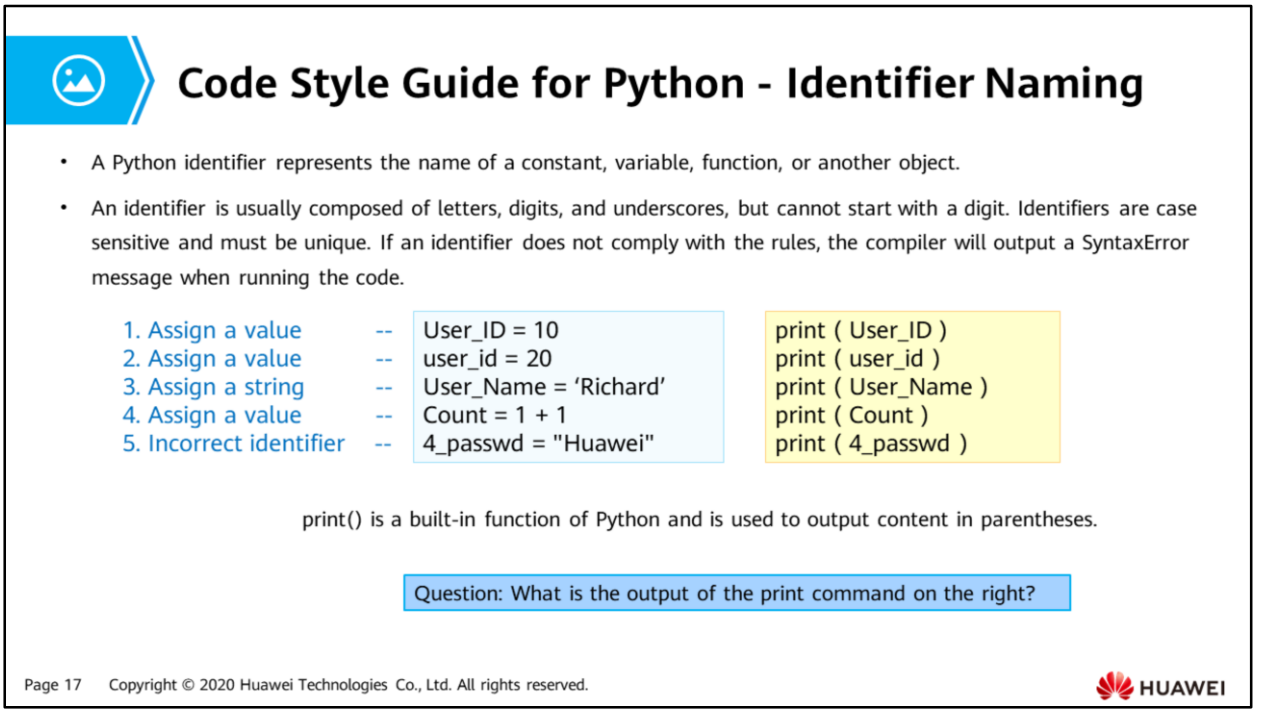
Parentheses

- Parentheses can be used for the continuation of long statements. Avoid unnecessary parentheses.

Space

- Spaces are not recommended in parentheses.
- You can determine whether to add spaces on both ends of an operator.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Basic data types of Python are Boolean (True/False), integer, floating point, and string. All data (Boolean values, integers, floating points, strings, and even large data structures, functions, and programs) in Python exists in the form of objects. This makes the Python language highly unified.
- The execution results are 10, 20, Richard, 2, and SyntaxError, respectively.
- This presentation does not describe Python syntax. For Python syntax details, see the HCIP course.

Code Style Guide for Python - Code Indentation

- In Python programs, code indentation represents the scope of a code block. If a code block contains two or more statements, the statements must have the same indentation. For Python, code indentation is a syntax rule that uses code indentation and colons to distinguish between layers of code.
- When writing code, you are advised to use four spaces for indentation. If incorrect indentation is used in the program code, an IndentationError error message is displayed during code running.

Correct indentation --
Correct indentation --
Incorrect indentation --

```
if True:
    print ("Hello")
else:
    print (0)

a = “Python”
    print (a)
```

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- if...else... is a complete block of code with the same indentation.
- print(a) calls parameter a, and it is in the same code block with if...else...clause.

Code Style Guide for Python - Using Comments

- Comments are explanations added to programs to improve program readability. In the Python program, comments are classified into single-line comments and multi-line comments.
- A single-line comment starts with a pound sign (#).
- A multi-line comment can contain multiple lines, which are enclosed in a pair of three quotation marks ('''...''' or """ ...""").

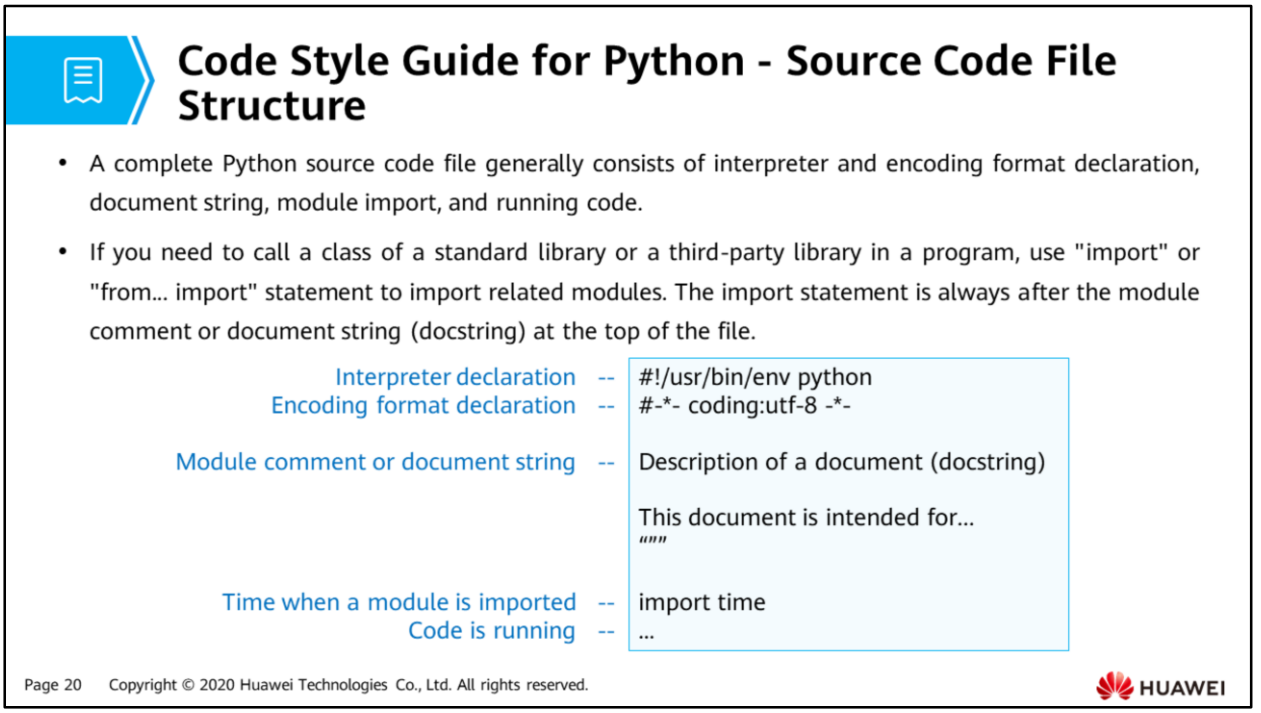
Single-line comment --

Multi-line comment --

```
# Assign a string to a.
a = “Python”
print (a)

“””
The output is Python.
“””
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The interpreter declaration is used to specify the path of the compiler that runs this file (the compiler is installed in a non-default path or there are multiple Python compilers). In the Windows , you can omit the first line of the interpreter declaration in the preceding example.
- The encoding format declaration is used to specify the encoding type used by the program to read the source code. By default, Python 2 uses ASCII code (Chinese is not supported), and Python 3 supports UTF-8 code (Chinese is supported).
- docstring is used to describe the functions of the program.
- time is a built-in module of Python and provides functions related to processing time.

Python Functions and Modules

- A function is a block of organized, reusable code that is used to perform a single, related action. It can improve the modularity of the program and code utilization. The function is defined using the def keyword.
- A module is a saved Python file. Modules can contain definitions of functions, classes, and variables that can then be utilized in other Python programs. The only difference between a module and a regular Python program is that the module is used for importing by other programs. Therefore, a module usually does not have a main function.

demo.py

```
def sit(): #Define a function.
    print ('A dog is now sitting')

sit() #Call a function.
```

Execution result:

```
A dog is now sitting.
```

1 Write a Python file (.py).

test.py

```
import demo #Import a module.

demo.sit()      #Call a function.
```

Execution result:

```
A dog is now sitting.
A dog is now sitting.
```

2 Import a module.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Python Classes and Methods

- A class is a collection of properties and methods that are the same. The class keyword is used to define a class.
- The function of an instantiated class is called a method. When you define a method, a class must carry the **self** keyword, which indicates the instance of the class.

demo.py

```
class Dog(): #Define a class.
    def sit(self):  #Define a method.
        print("A dog is now sitting.")

Richard = Dog() #The class is instantiated.
print (type(Richard.sit)) #The function of an instantiated type is called a method.
print (type(Dog.sit)) #The type is function.
```

Execution result:

```
<class 'method'>
<class 'function'>
```

1 Write a Python file (.py).

test.py

```
import demo

demo.Dog.sit
```

Execution result:

```
A dog is now sitting.
<class 'method'>
<class 'function'>
```

2 Import a module.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- Official definitions of functions and methods:
- A series of statements which returns some value to a caller. It can also be passed zero or more arguments which may be used in the execution of the body.
- A function which is defined inside a class body. If called as an attribute of an instance of that class, the method will get the instance object as its first argument (which is usually called self).
- For more information about classes, see https://docs.python.org/3/tutorial/classes.html.

Introduction to telnetlib

- telnetlib is a module in the standard Python library. It provides the telnetlib.Telnet class for implementing the Telnet function.
- Different methods in the telnetlib.Telnet class are called to implement different functions.

```
Import the Telnet class of the telnetlib module. --  from telnetlib import Telnet
Create a Telnet connection to a specified server. --  tn = Telnet(host=None, port=0[, timeout])
Invoke the read_all() method. --                      tn.read_all()
                                                      ...
```

Method	Function
Telnet.read_until (expected, timeout=None)	Read data until a given byte string, *expected*, is encountered or until *timeout* seconds have passed.
Telnet.read_all ()	Read all data until EOF as bytes; block until connection closed.
Telnet.read_very_eager()	Read everything that can be without blocking in I/O (eager). Raise EOFError if connection closed and no cooked data available. Return b'' if no cooked data available otherwise. Do not block unless in the midst of an IAC sequence.
Telnet.write(buffer)	Write a byte string to the socket, doubling any IAC characters.
Telnet.close()	Close the connection.

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved. HUAWEI

- Telnet defines the network virtual terminal (NVT). It describes the standard representation of data and sequences of commands transmitted over the Internet to shield the differences between platforms and operating systems. For example, different platforms have different line feed commands.
- Telnet communication adopts the inband signaling mode. That is, Telnet commands are transmitted in data streams. To distinguish Telnet commands from common data, Telnet uses escape sequences. Each escape sequence consists of 2 bytes. The first byte (0xFF) is called Interpret As Command (IAC), which indicates that the second byte is a command. EOF is also a Telnet command. Its decimal code is 236.
- A socket is an abstraction layer. Applications usually send requests or respond to network requests through sockets.
- For more information, see https://docs.python.org/3/library/telnetlib.html.

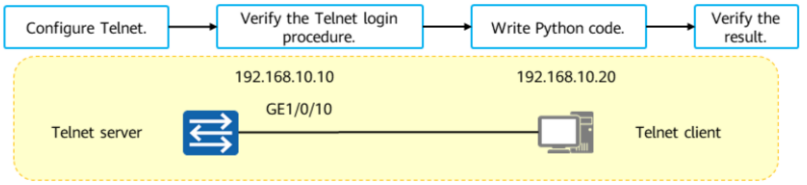
Contents

1. Introduction to Network Programmability and Automation
2. Overview of Programming Language and Python
3. **Cases**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case: Logging In to a Device Using telnetlib

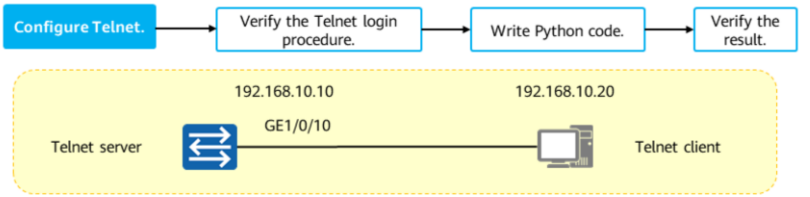
- Case description :
- A network device functions as a Telnet server, and the Python telnetlib needs to be used as a Telnet client to log in to the device.



- The implementation process is as follows :
- Configure the Telnet service.
- Manually verify and view the Telnet login procedure as a reference for code implementation.
- Compile and run Python code.
- Verify the result.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case: Logging In to a Device Using telnetlib



Configure the IP address of interface on the device:

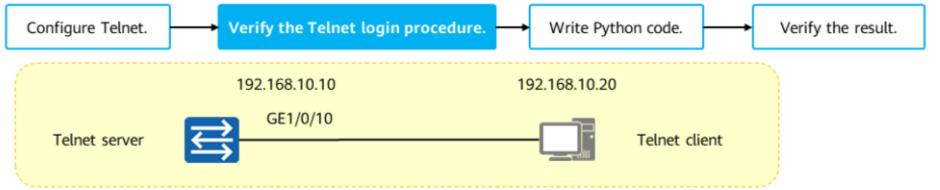
```
[Huawei] interface GE 1/0/0
[Huawei -GE1/0/0] ip add 192.168.10.10 24
[Huawei -GE1/0/0] quit
```

Configure the Telnet service:

```
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode password
[Huawei-ui-vty0-4] set authentication password simple Huawei@123
[Huawei-ui-vty0-4] protocol inbound telnet
[Huawei-ui-vty0-4] user privilege level 15
[Huawei-ui-vty0-4] quit
[Huawei] telnet server enable
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Case: Logging In to a Device Using telnetlib



Telnet login:

1. Run a login command. Command output
2. Enter a password. Command output

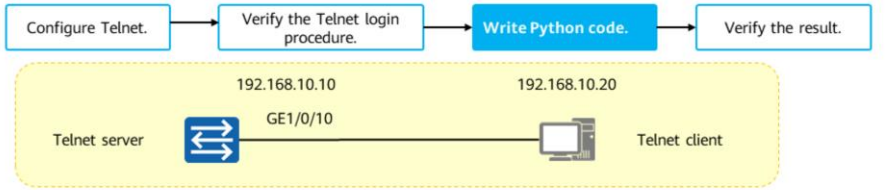
```
C:\Users\Richard>telnet 192.168.10.10
Login authentication

Password:
Info: The max number of VTY users is 5, and the number of current VTY users on line is 1.
The current login time is 2020-01-15 21:12:57.
<Huawei>
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

- In this case, the Windows operating system is used as an example. Run the telnet 192.168.10.10 command. In the preceding step, a Telnet login password is set. Therefore, the command output is
- Password:
- Enter the password Huawei@123 for authentication. The login is successful.

Case: Logging In to a Device Using telnetlib



Imports the module.	--	import telnetlib
Sets the IP address for a host.	--	**host** = '192.168.10.10'
Sets the password for logging in to the device.	--	**password** = 'Huawei@123'
Logs in to the host through Telnet.	--	tn = telnetlib.Telnet(**host**)
Prints data until **Password:** is displayed.	--	tn.read_until(b'Password:')
Sets an ASCII password and starts a new line.	--	tn.write(**password**.encode('ascii') + b"\n")
Prints data until **<Huawei>** is displayed.	--	print (tn.read_until(b'<Huawei>').decode('ascii'))
Closes the Telnet connection.	--	tn.close()

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

- In Python, the encode() and decode() functions are used to encode and decode strings in a specified format, respectively. In this example, password.encode('ascii') is to convert the string Huawei@123 into the ASCII format. The encoding format complies with the official requirements of the telnetlib module.
- Add a string b, b'str', indicating that the string is a bytes object. In this example, b'Password:' indicates that the string Password:' is converted into a string of the bytes type. The encoding format complies with the official requirements of the telnetlib module.
- For more information about Python objects, see https://docs.python.org/3/reference/datamodel.html#objects-values-and-types.

Case: Running Result Comparison



Manual Telnet login result:

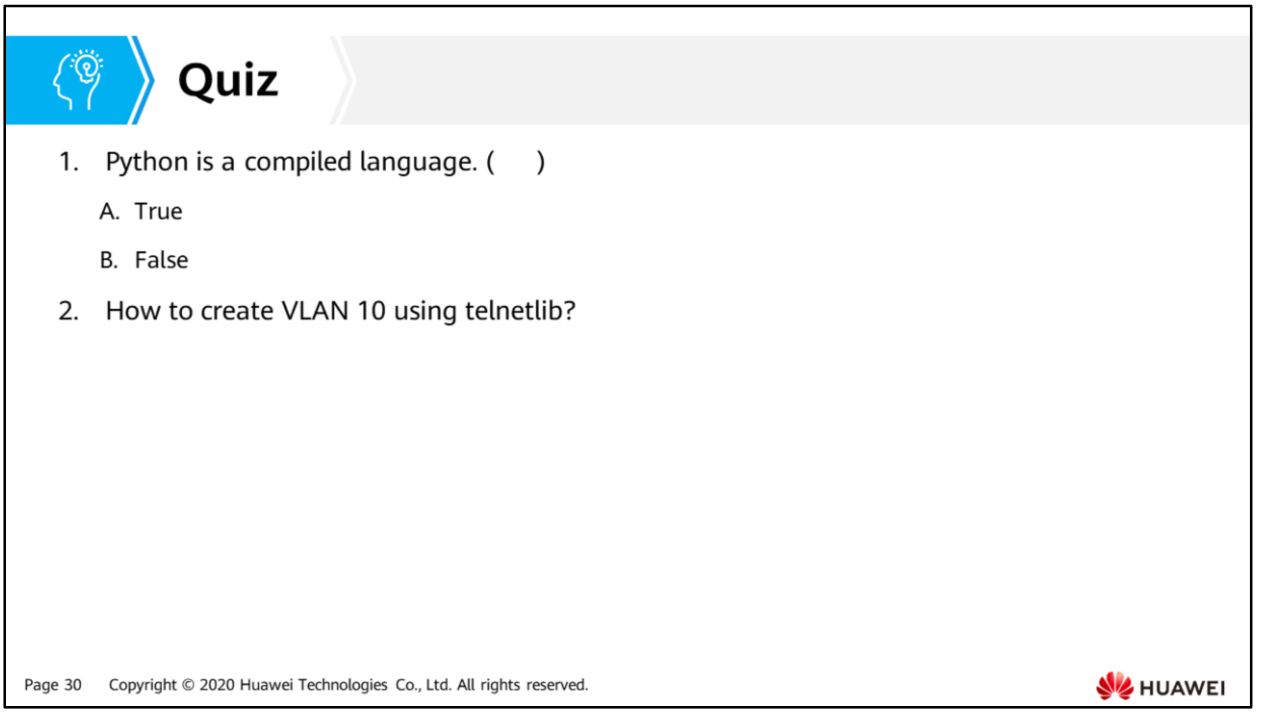
```
C:\Users\Richard>telnet 192.168.10.10
Login authentication

Password:
Info: The max number of VTY users is 5, and the number of current VTY users on line is 1.
The current login time is 2020-01-15 21:12:57.
<Huawei>
```

Python code execution result:

```
#Run Python code in the compiler.
Info: The max number of VTY users is 5, and the number
    of current VTY users on line is 1.
    The current login time is 2020-01-15 22:12:57.
<Huawei>
```


Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



1. B
2. You can use the telnetlib.write() method. After logging in to the device, issue the system-view command to access the system view, and then issue the vlan 10 command to create a VLAN. (For a device running the VRPv8, issue the system-view immediately command to access the system view.)

Summary

- Network automation uses tools to implement automated network deployment, operation, and O&M, gradually reducing dependency on people. You can use a programming language or tool to implement the network automation.
- Python is a fully-open-source high-level programming language that is simple syntax and is easy to learn. It has rich standard libraries and third-party libraries, which are applicable to the network engineering field.
- The telnetlib module of Python provides the telnetlib.Telnet class for implementing the Telnet function. It helps you enter the network programmability and automation world!

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

More Information

- For more information about Python, visit https://www.python.org/.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com



Typical Campus Network Architectures and Practices

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Foreword

- A broad range of places, such as campuses, office spaces, and shopping malls, are covered by networks. You can access internal resources of your school, access internal printers of your company to print documents, or access the Internet to browse news through the networks.
- These networks belong to campus networks and are generally constructed by enterprises or organizations. Campus networks not only improve the operational efficiency of enterprises, but also provide network access services for external users.
- This chapter describes the basic architecture of a campus network and details how to build a campus network.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- Upon completion of this course, you will be able to:
  - Understand the definition of campus networks.
  - Understand the typical networking architectures of campus networks.
  - Master the planning and design methods of small campus networks.
  - Master the deployment and implementation methods of small campus networks.
  - Understand the small campus network O&M concepts.
  - Understand the small campus network optimization concepts.
  - Independently complete a campus network project.

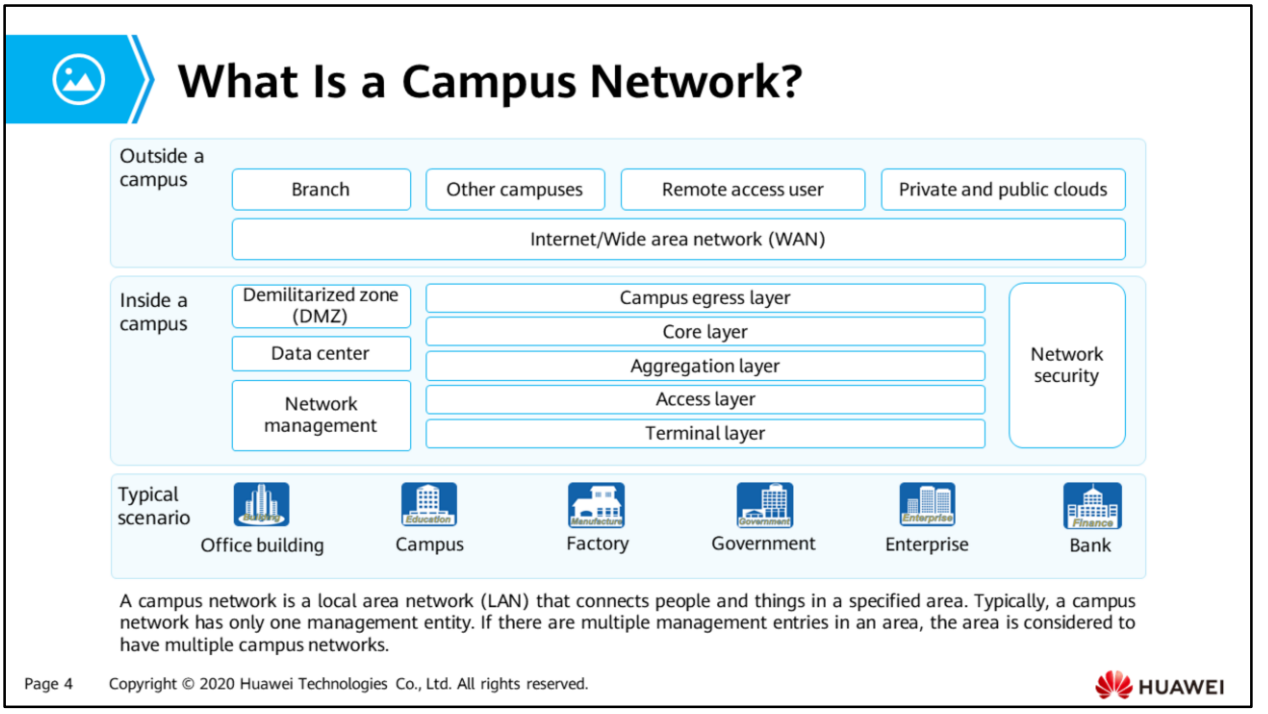
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

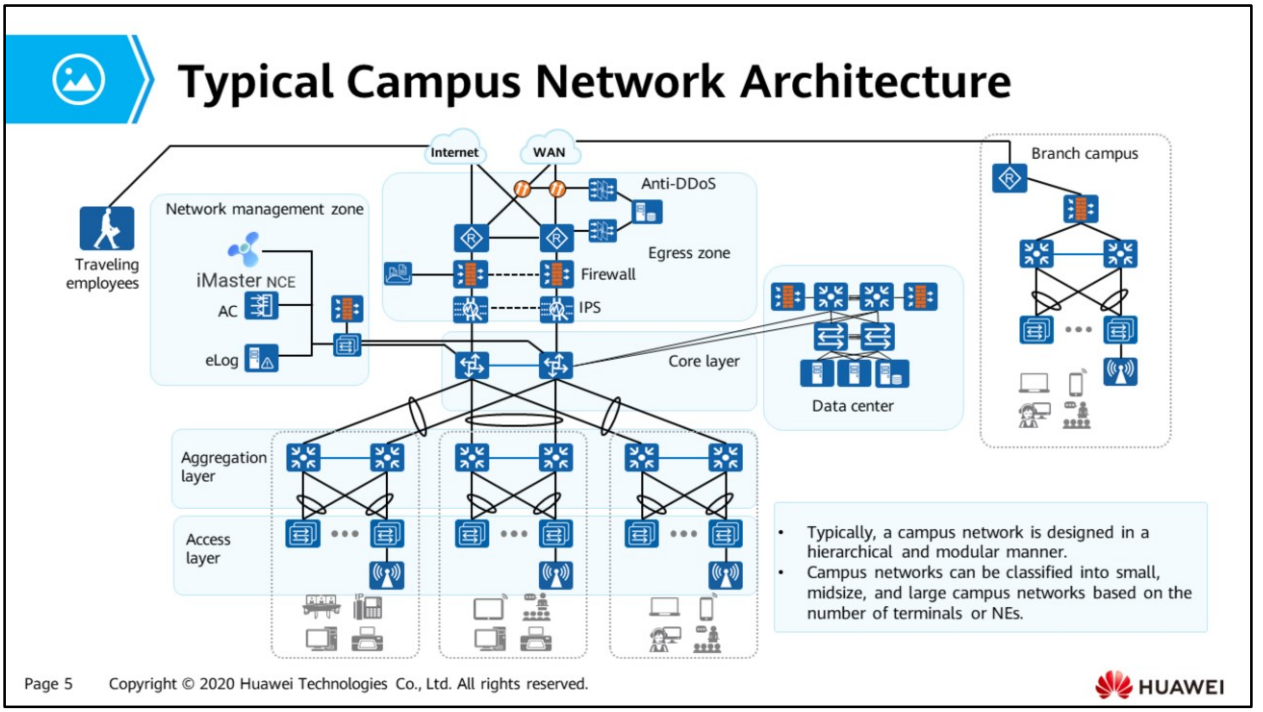
1. **Basic Concepts of Campus Networks**
2. Typical Campus Network Construction Process

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

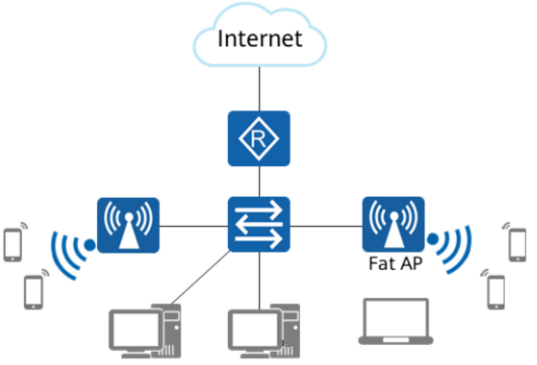


- The campus network scale is flexible depending on actual requirements. It can be a small office home office (SOHO), a school campus, enterprise campus, park, or shopping center. However, the campus network cannot be scaled out infinitely. Typically, large campuses, such as university campuses and industrial campuses, are limited within several square kilometers. Such campus networks can be constructed using local area network (LAN) technology. A campus network beyond this scope is usually considered as a metropolitan area network (MAN) and is constructed using the WAN technology.
- Typical LAN technologies used on campus networks include IEEE 802.3-compliant Ethernet (wired) technologies and IEEE 802.11-compliant Wi-Fi (wireless) technologies.



- Typical layers and areas of a campus network:
  - **Core layer**: is the backbone area of a campus network, which is the data switching core. It connects various parts of the campus network, such as the data center, management center, and campus egress.
  - **Aggregation layer**: is a middle layer of a campus network, and completes data aggregation or switching. Some fundamental network functions, such as routing, QoS, and security, are also provided at this layer.
  - **Access layer**: As the edge of a campus network, this layer connects end users to the campus network.
  - **Egress area**: As the edge that connects a campus network to an external network, this area enables mutual access between the two networks. Typically, a large number of network security devices, such as intrusion prevention system (IPS) devices, anti-DDoS devices, and firewalls, are deployed in this area to defend against attacks from external networks.
  - **Data center area**: has servers and application systems deployed to provide data and application services for internal and external users of an enterprise.
  - **Network management area**: Network management systems, including the SDN controller, WAC, and eLog (log server), are deployed in this area to manage and monitor the entire campus network.

Typical Architecture of Small Campus Networks



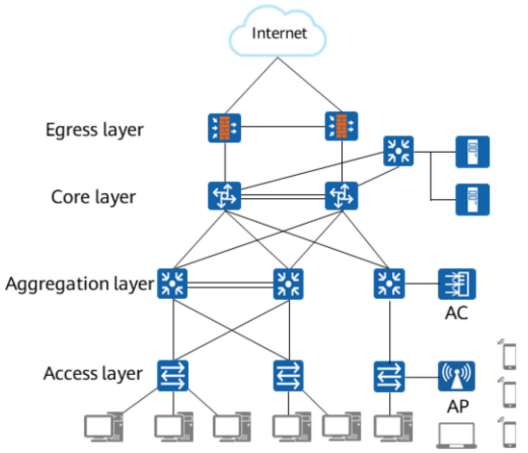
Network topology of a chain cafe

- Small campus networks are typically deployed in scenarios where the number of access users is small (several or dozens of users). A small campus network can cover only one location, has a simple architecture, and is constructed to enable mutual access between internal resources.
- Characteristics of small campus networks:
  - Small number of users
  - Only one location
  - Simple network architecture
  - Simple network requirements

Number of terminals	< 200
Number of NEs	< 25

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Typical Architecture of Midsize Campus Networks



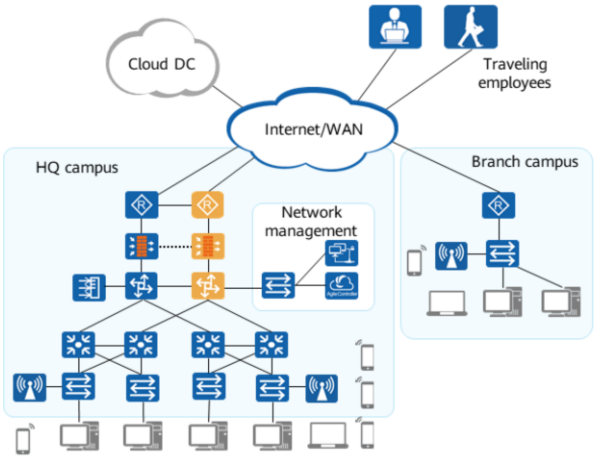
Network topology of a foreign trade company

- A midsize campus network supports access of hundreds to thousands of users.
- The modular design is introduced to midsize campus networks, that is, the networks can be partitioned by function. However, the number of function modules is small. In most cases, a midsize campus network is flexibly partitioned based on service requirements.
- Characteristics of midsize campus networks:
  - Midsize network scale
  - Most commonly used
  - Function partition
  - Typical three-layer network architecture: core, aggregation, and access

Number of terminals	200 to 2000
Number of NEs	25 to 100

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

Typical Architecture of Large Campus Networks



Network topology of a large enterprise

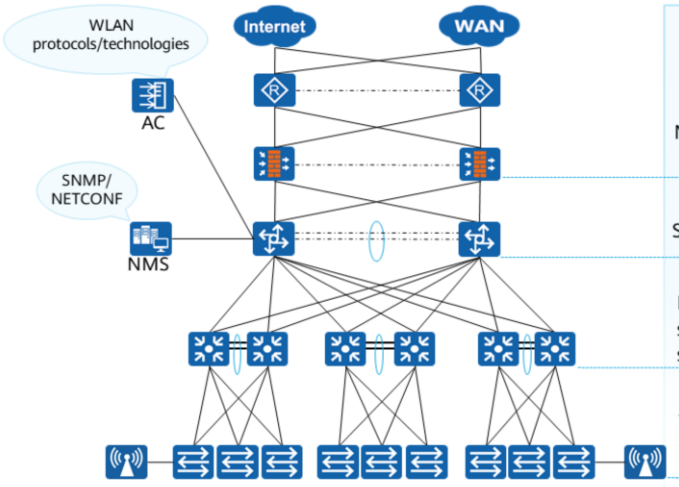
- A large campus network can cover multiple buildings and connect to multiple campuses in a city through WANs. Typically, a large campus network provides access services and allows traveling employees to access their company's internal network through technologies such as Virtual Private Network (VPN).
- Characteristics of large campus networks:
  - Wide coverage

Number of terminals	> 2000
Number of NEs	> 100

  - Large number of users
  - Complex network requirements
  - Comprehensive function modules
  - Complex network architecture

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Main Protocols and Technologies of Campus Networks



Common protocols/technologies	
NAT, OSPF, static routing, and PPPoE	Egress zone
Stacking, OSPF, static routing, and ACL	Core layer
DHCP, stacking, link aggregation, spanning tree protocol, OSPF, and static routing	Aggregation layer
VLAN, spanning tree, link aggregation, and AAA	Access layer

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Contents

1. Basic Concepts of Campus Networks
2. **Campus Network Project Practice**

 Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

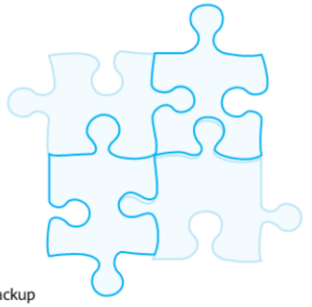
HUAWEI

Networking Requirements

- A company (with about 200 employees) plans to build a brand-new campus network to meet service development requirements. The network requirements are as follows:
  - Meet the current services requirements of the company.
  - Use a simple network topology for easy O&M.
  - Provide wired access for employees and wireless access for guests.
  - Implement simple network traffic management.
  - Ensure network security.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Campus Network Project Lifecycle



1 Planning and design

- Device model selection
- Physical topology
- Logical topology
- Technologies and protocols

2 Deployment and implementation

- Device installation
- Single UPS commissioning
- Joint commissioning test
- Network migration and integration

3 Network O&M

- Routine maintenance
- Software and configuration backup
- Centralized monitoring via the network management system (NMS)
- Software upgrade

4 Network optimization

- Network security improvement
- Software and configuration backup
- User experience improvement

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.
HUAWEI

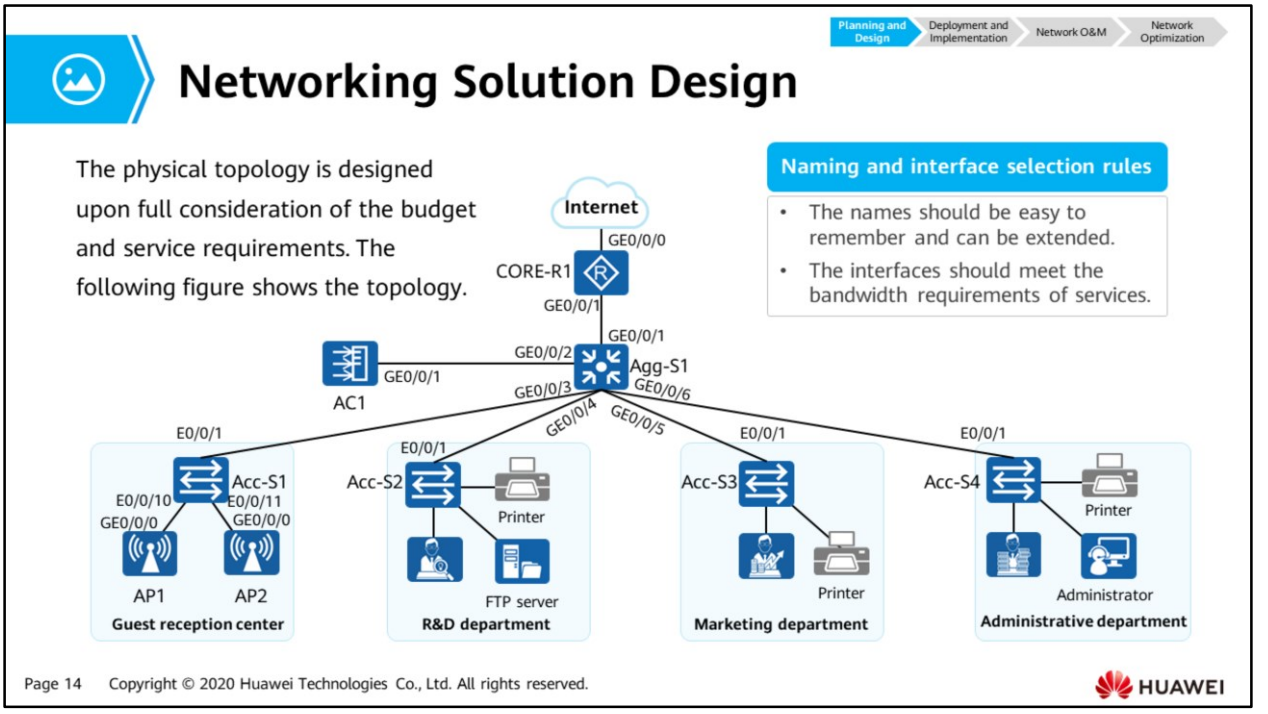
- A campus network project starts from network planning and design. Comprehensive and detailed network planning will lay a solid foundation for subsequent project implementation.
- Project implementation is a specific operation procedure for engineers to deliver projects. Systematic management and efficient process are critical to successful project implementation.
- Routine O&M and troubleshooting are required to ensure the normal running of network functions and support smooth provisioning of user services.
- As users' services develop, the users' requirements on network functions increase. If the current network cannot meet service requirements, or potential problems are found while the network is running, the network needs to be optimized.

Small Campus Network Design



1. Networking solution design	2. Network design	3. Security design	4. Network O&M and management design
Device model selection	Basic service	Egress security	Basic network management
Physical topology	WLAN	Intranet wired security	Intelligent O&M
	Layer 2 loop prevention	Intranet wireless security	
	Network reliability		

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The entire network uses a three-layer architecture.
  - The S3700 is deployed as the access switch to provide 100 Mbit/s network access for employees' PCs and printers.
  - The S5700 is deployed at the aggregation layer as the gateway of the Layer 2 network.
  - The AR2240 is deployed at the core and egress of a campus network.
- Note: Agg is short for aggregation, indicating a device at the aggregation layer. Acc is short for Access, indicating an access device.

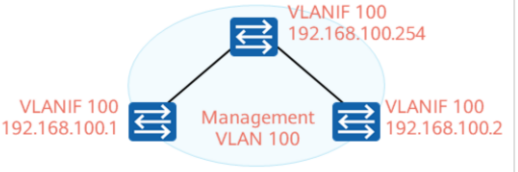
Basic Service Design: VLAN Design

- You are advised to assign consecutive VLAN IDs to ensure proper use of VLAN resources.
- VLANs can be classified into service VLANs, management VLANs, and interconnection VLANs as required.
- Typically, VLANs are assigned based on interfaces.

Service VLAN design

- VLAN assignment by geographic area
- VLAN assignment by logical area
- VLAN assignment by personnel structure
- VLAN assignment by service type

Management VLAN design



In most cases, Layer 2 switches use VLANIF interface addresses as management addresses. It is recommended that all switches on the same Layer 2 network use the same management VLAN and their management IP addresses be on the same network segment.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

VLAN Planning

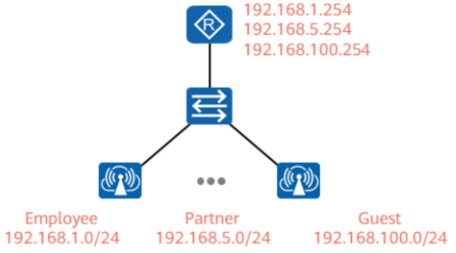
- A management VLAN is reserved for Layer 2 devices.
- VLANs are classified into the guest VLAN, R&D department VLAN, marketing department VLAN, and administrative department VLAN.
- Layer 3 switches need to be connected to routers through VLANIF interfaces. Therefore, interconnection VLANs need to be reserved.
- A VLAN is established for CAPWAP tunnels between APs and ACs.

VLAN ID	VLAN Description
1	Guest VLAN or WLAN service VLAN
2	R&D department VLAN
3	Marketing department VLAN
4	Administrative department VLAN
100	Management VLAN of Layer 2 devices
101	Management VLAN of WLAN services
102	Interconnection VLAN between Agg-S1 and CORE-R1

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Basic Service Design: IP Address Design

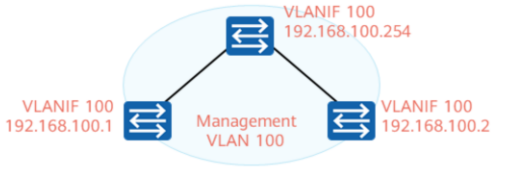
Service IP address



The service IP addresses are the IP addresses of servers, hosts, or gateways.

- It is recommended that the gateway IP addresses use the same rightmost digits, such as .254.
- The IP address ranges of different services must be clearly distinguished. The IP addresses of each type of service terminals must be continuous and can be aggregated.
- An IP address segment with a 24-bit mask is recommended.

Management IP address



Layer 2 devices use VLANIF interface IP addresses as the management IP addresses. It is recommended that all Layer 2 switches connected to a gateway use on the same network segment.

IP address for network device interconnection

It is recommended that the interconnection IP addresses use a 30-bit mask, and core devices use smaller host IP addresses.

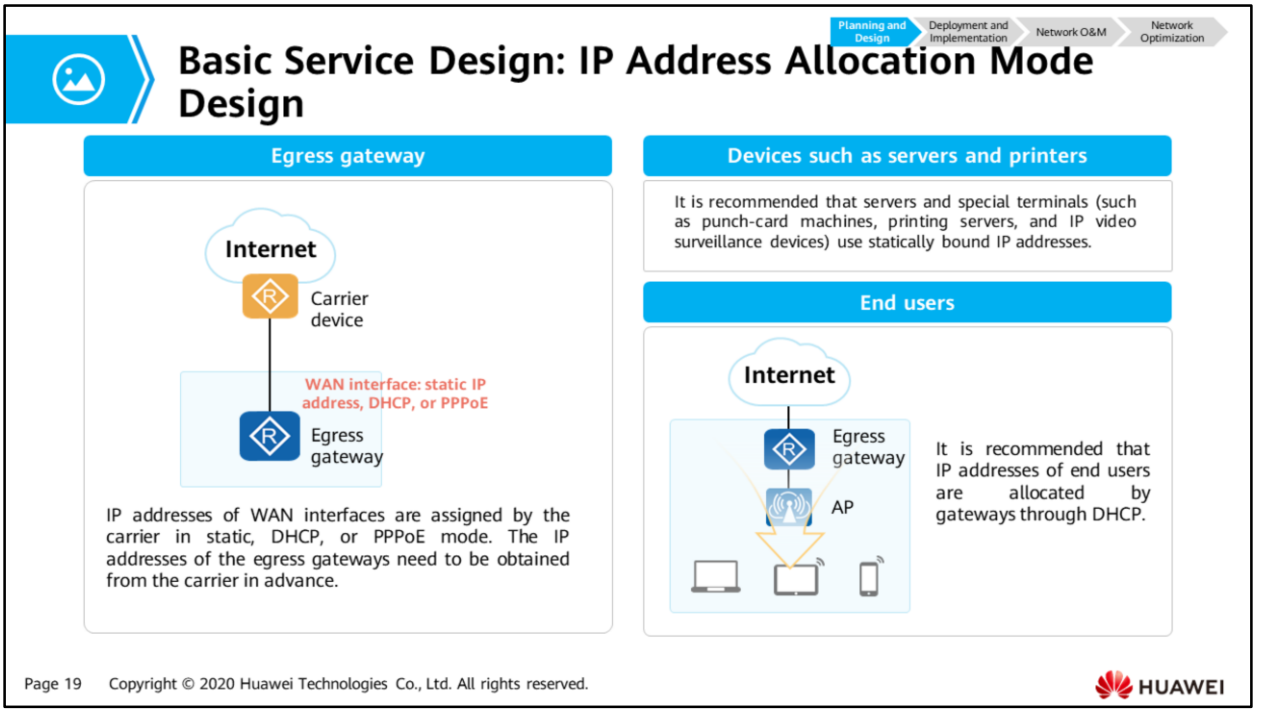
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

IP Address Planning

- Reserve sufficient IP addresses based on the number of clients to be accessed and plan network segments and gateway addresses for each type of service.
- Plan network segments for management IP addresses.
- Divide network segments for interconnection IP addresses.

IP Network Segment/Mask	Gateway Address	Network Segment Description
192.168.1.0/24	192.168.1.254	Network segment to which wireless access guests belong, with the gateway located on Agg-S1
192.168.2.0/24	192.168.2.254	Network segment to which the R&D department belongs, with the gateway located on Agg-S1
192.168.3.0/24	192.168.3.254	Network segment to which the marketing department belongs, with the gateway located on Agg-S1
192.168.4.0/24	192.168.4.254	Network segment to which the administrative department belongs, with the gateway located on Agg-S1
192.168.100.0/24	192.168.100.254	Management network segment of Layer 2 devices, with the gateway located on Agg-S1
192.168.101.0/24	N/A	Management network segment of WLAN services
192.168.102.0/30	N/A	Network segment between Agg-S1 and CORE-R1
1.1.1.1/32	N/A	Loopback interface address on CORE-R1, which is used as the management IP address

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



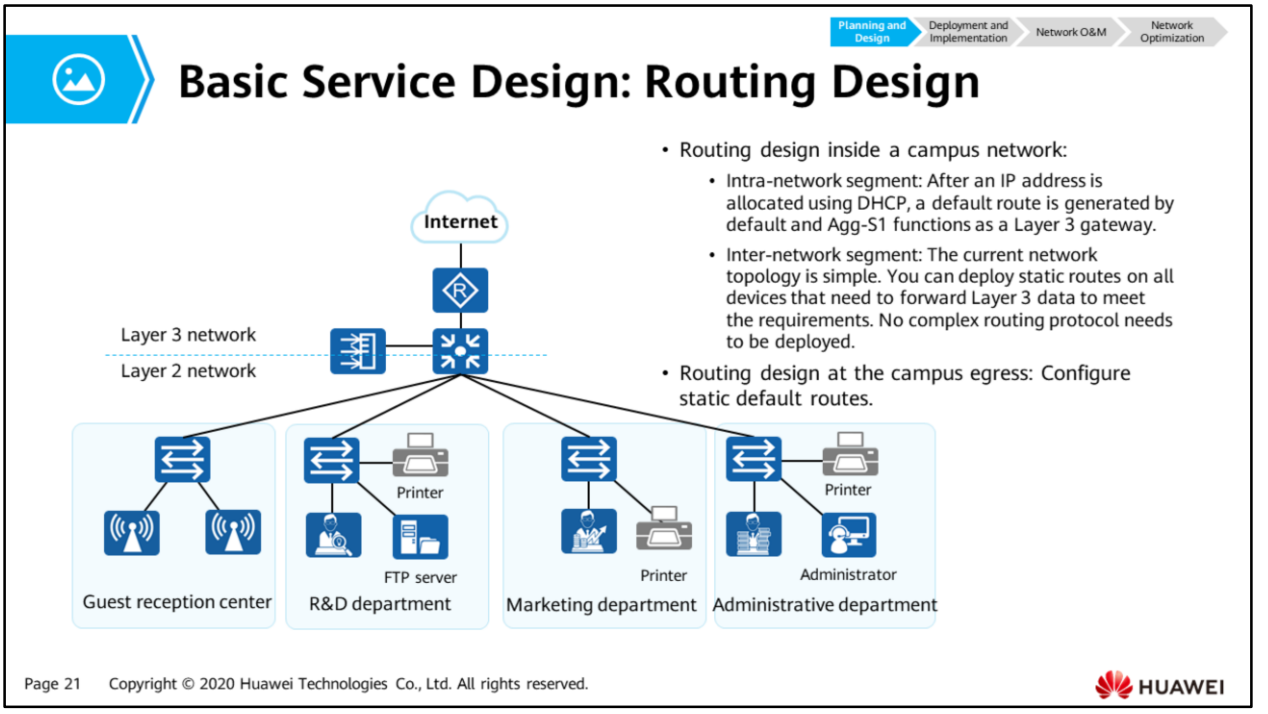
- Dynamic IP address assignment or static IP address binding can be used for IP address assignment. On a small or midsize campus network, IP addresses are assigned based on the following principles:
- IP addresses of WAN interfaces on egress gateways are assigned by the carrier in static, DHCP, or PPPoE mode. The IP addresses of the egress gateways need to be obtained from the carrier in advance.
- It is recommended that servers and special terminals (such as punch-card machines, printing servers, and IP video surveillance devices) use statically bound IP addresses.
- User terminal: It is recommended that the DHCP server be deployed on the gateway to dynamically assign IP addresses to user terminals such as PCs and IP phones using DHCP.

IP Address Allocation Mode Planning

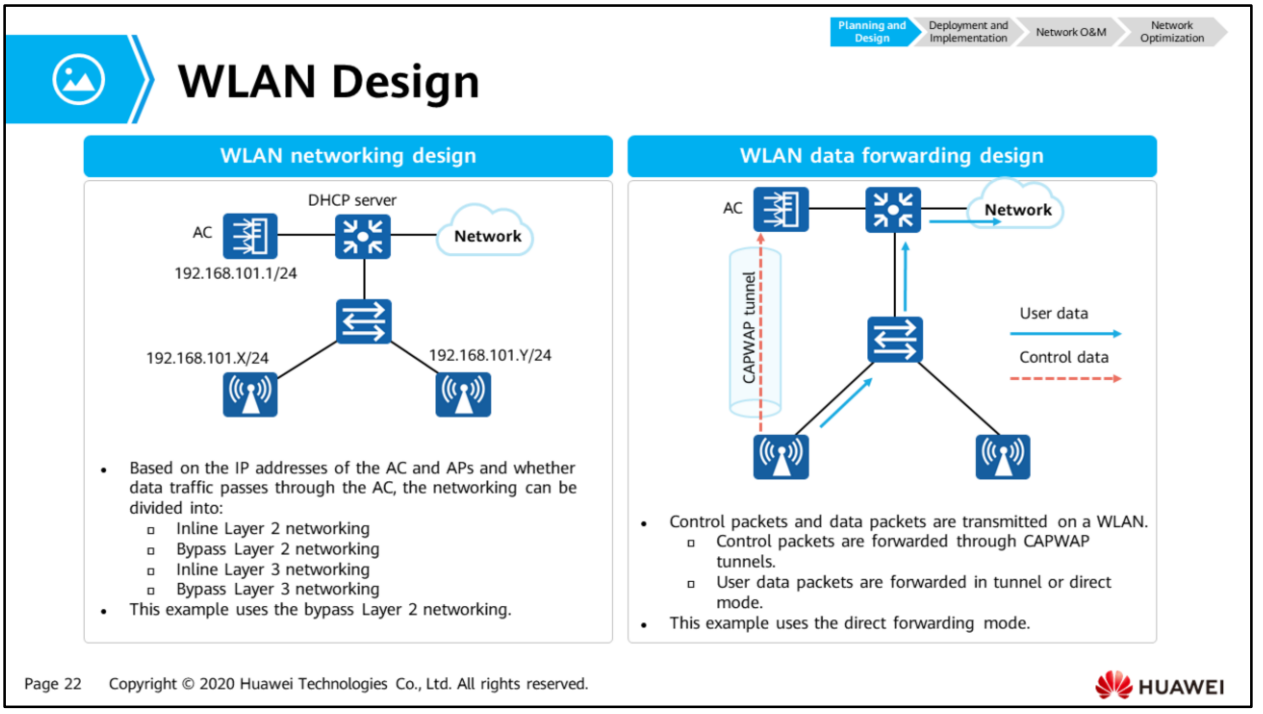
- The egress gateway obtains an IP address through PPPoE.
- All terminals obtain IP addresses through DHCP. The servers and printers are assigned fixed IP addresses.
- IP addresses of all network devices (except APs) are statically configured.

IP Network Segment/Interface	Allocation Mode	Allocation Mode Description
192.168.1.0/24 192.168.2.0/24 192.168.3.0/24 192.168.4.0/24	DHCP	Allocated by Agg-S1. Agg-S1 allocates fixed IP addresses to fixed devices such as servers and printers.
192.168.100.0/24	Static	Device management IP addresses, which are statically configured
192.168.101.0/24	DHCP	IP addresses of ACs are statically configured, and IP addresses of APs are allocated by Agg-S1.
192.168.102.0/30	Static	Interconnection IP address, which is statically configured
GE0/0/0 on CORE-R1	PPPoE	IP address assigned by the carrier

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- The routing design of a small or midsize campus network includes design of internal routes and the routes between the campus egress and the Internet or WAN devices.
- The internal routing design of a small or midsize campus network must meet the communication requirements of devices and terminals on the campus network and enable interaction with external routes. As the campus network is small in size, the network structure is simple.
    - AP: After an IP address is assigned through DHCP, a default route is generated by default.
    - Switch and gateway: Static routes can be used to meet requirements. No complex routing protocol needs to be deployed.
- The egress routing design meets the requirements of intranet users for accessing the Internet and WAN. When the egress device is connected to the Internet or WAN, you are advised to configure static routes on the egress device.



- In addition to planning the networking and data forwarding mode, you also need to perform the following operations:
  - **Network coverage design**: You need to design and plan areas covered by Wi-Fi signals to ensure that the signal strength in each area meets user requirements and to minimize co-channel interference between neighboring APs.
  - **Network capacity design**: You need to design the number of APs required based on the bandwidth requirements, number of terminals, user concurrency rate, and per-AP performance. This ensures that the WLAN performance can meet the Internet access requirements of all terminals.
  - **AP deployment design**: Based on the network coverage design, modify and confirm the actual AP deployment position, deployment mode, and power supply cabling principles based on the actual situation.
  - In addition, WLAN security design and roaming design are required.

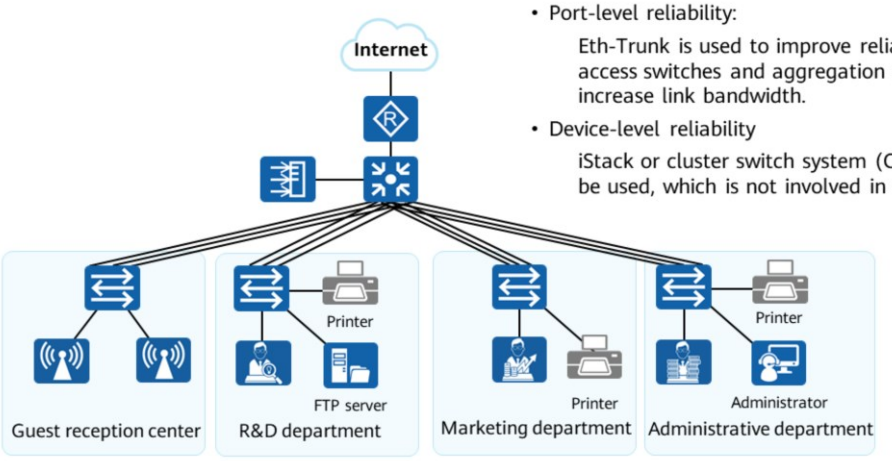


WLAN Data Plan

Item	Value
Management VLAN for APs	VLAN 101
Service VLAN for STAs	VLAN 1
DHCP server	Agg-S1 functions as a DHCP server to allocate IP addresses to APs and STAs. The default gateway address of STAs is 192.168.1.254.
IP address pool for APs	192.168.101.2 to 192.168.101.253/24
IP address pool for STAs	192.168.1.1 to 192.168.1.253/24
Source interface address of the AC	VLANIF 101: 192.168.101.1/24
AP group	Name: **ap-group1** Referenced profiles: VAP profile **WLAN-Guest** and regulatory domain profile **default**
Regulatory domain profile	Name: **default** Country code: CN
SSID profile	Name: **WLAN-Guest** SSID name: **WLAN-Guest**
Security profile	Name: **WLAN-Guest** Security policy: WPA-WPA2+PSK+AES Password: **WLAN@Guest123**
VAP profile	Name: **WLAN-Guest** Forwarding mode: direct forwarding Service VLAN: VLAN 1 Referenced profiles: SSID profile **WLAN-Guest** and security profile **WLAN-Guest**

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Reliability Design



- Port-level reliability:

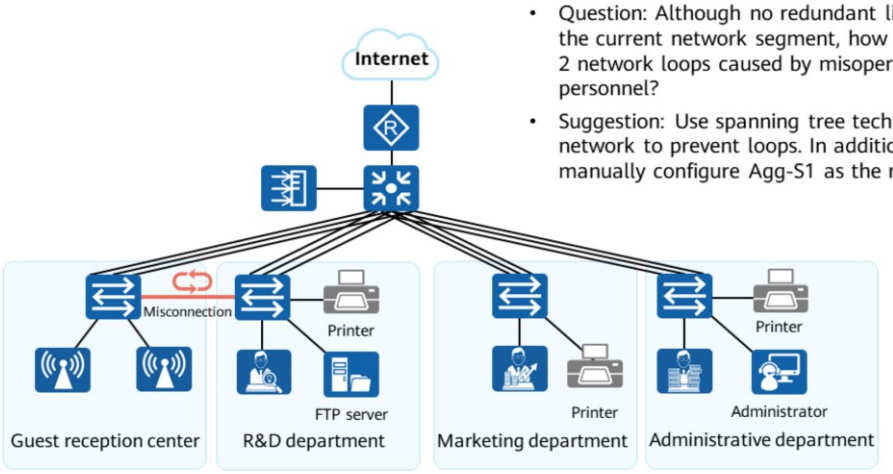
  Eth-Trunk is used to improve reliability between access switches and aggregation switches and increase link bandwidth.

- Device-level reliability

  iStack or cluster switch system (CSS) technology can be used, which is not involved in this networking.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Layer 2 Loop Prevention

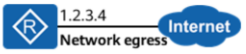


- Question: Although no redundant link is introduced to the current network segment, how can we prevent Layer 2 network loops caused by misoperations of office personnel?
- Suggestion: Use spanning tree technology on the Layer 2 network to prevent loops. In addition, you are advised to manually configure Agg-S1 as the root bridge.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Egress NAT Design

Static NAT

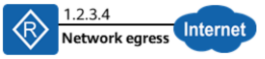


NAT mapping table

Private IP Address	Public IP Address
192.168.1.1	1.2.3.1
192.168.1.2	1.2.3.2

- Static NAT applies to scenarios where a large number of static IP addresses are configured and clients need to use fixed IP addresses.

Dynamic NAT

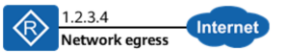


NAT address pool

1.2.3.1	Not in use
1.2.3.2	Not in use
1.3.3.3	Not in use

- Dynamic NAT introduces the address pool concept. Available IP addresses in the address pool are allocated to clients for Internet access.

NAPT and Easy IP



NAT mapping table

Private IP Address:Port Number	Public IP Address:Port Number
192.168.1.10:80	1.2.3.4:10335

- NAPT translates port numbers based on dynamic NAT to improve public address usage.
- Easy IP applies to scenarios where IP addresses of outbound network interfaces are dynamically allocated.

NAT Server

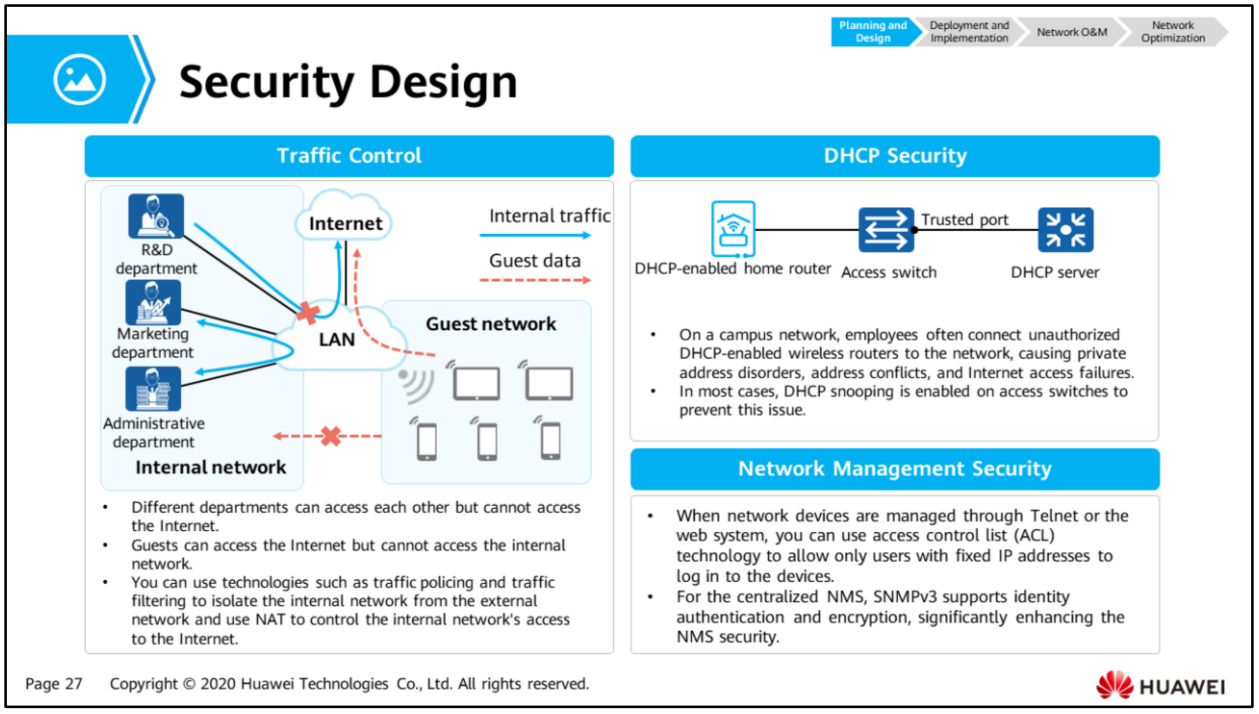


NAT mapping table

Private IP Address:Port Number	Public IP Address:Port Number
192.168.1.1:10321	1.2.3.4:1025
192.168.1.2:17087	1.2.3.4:1026

The NAT server applies to scenarios where a server on the intranet needs to externally provide services.

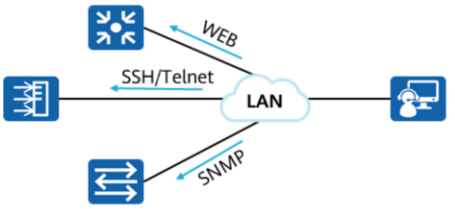
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



- Note: Security design in this case is implemented depending only on routers or switches.

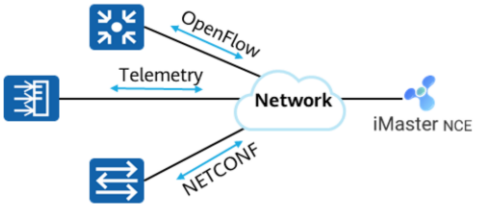
Network O&M and Management Design

Traditional Device Management



- When the network administrator and devices' IP addresses are routable to each other, you can manage the devices through Telnet, the web system, or SSH.
- When there are a large number of devices on a network, you can deploy an SNMP-based unified NMS for network O&M and management.

Management Based on iMaster NCE



- In addition to the SNMP-based traditional NMS, Huawei iMaster NCE can also be used for network management and O&M to implement autonomous network driving.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Small Campus Network Deployment and Implementation

- The project deployment and implementation process must include:
  - Solution formulation
  - Device installation
  - Network commissioning
  - Network migration and integration
  - Transfer-to-maintenance (ETM) training
  - Project acceptance
- The specific process is determined based on the actual situation.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Configuration Scheme (1)

1. Connect network devices using physical cables, configure link aggregation, and add interface description. For details, see the following two tables.

Device	Interface	Configuration
Acc-S1	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/1, GE0/0/2, GE0/0/3 Description: to Agg-S1's eth-trunk 1
	E0/0/10	Description: to AP1
	E0/0/11	Description: to AP2
Acc-S2	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/1, GE0/0/2, GE0/0/3 Description: to Agg-S1's eth-trunk 2
Acc-S3	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/1, GE0/0/2, GE0/0/3 Description: to Agg-S1's eth-trunk 3
Acc-S4	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/1, GE0/0/2, GE0/0/3 Description: to Agg-S1's eth-trunk 4
AC1	GE0/0/1	Description: to Agg-S1's GE0/0/2
CORE-R1	GE0/0/1	Description: to Agg-S1's GE0/0/1

Device	Interface	Configuration
Agg-S1	Eth-trunk 1	Mode: LACP-static Trunkport: GE0/0/3, GE0/0/7, GE0/0/8 Description: to Acc-S1's eth-trunk 1
	Eth-trunk 2	Mode: LACP-static Trunkport: GE0/0/4, GE0/0/9, GE0/0/10 Description: to Acc-S2's eth-trunk 1
	Eth-trunk 3	Mode: LACP-static Trunkport: GE0/0/5, GE0/0/11, GE0/0/12 Description: to Acc-S3's eth-trunk 1
	Eth-trunk 4	Mode: LACP-static Trunkport: GE0/0/6, GE0/0/13, GE0/0/14 Description: to Acc-S4's eth-trunk 1
	GE0/0/1	Description: to CORE-R1's GE0/0/1
	GE0/0/2	Description: to AC1's GE0/0/1

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Scheme (2)

2. Assign VLANs based on interfaces. For details, see the following two tables.

Device	Interface	Type	Configuration
Acc-S1	Eth-trunk 1	Trunk	PVID:100 Allow-pass VLAN 1, 100, 101
	E0/0/10		PVID:101 Allow-pass VLAN 1, 101
	E0/0/11		
Acc-S2	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 2, 100
	Other ports	Access	Default VLAN 2
Acc-S3	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 3, 100
	Other ports	Access	Default VLAN 3
Acc-S4	Eth-trunk 1	Trunk	PVID:100 Allow pass VLAN 4, 100
	Other ports	Access	Default VLAN 4

Device	Interface	Type	Configuration
Agg-S1	Eth-trunk 1	Trunk	PVID:100 Allow-pass VLAN 1, 100, 101
	Eth-trunk 2	Trunk	PVID:100 Allow pass VLAN 2, 100
	Eth-trunk 3	Trunk	PVID:100 Allow pass VLAN 3, 100
	Eth-trunk 4	Trunk	PVID:100 Allow pass VLAN 4, 100
	GE0/0/2	Access	Default VLAN 101
	GE0/0/1	Access	Default VLAN 102
AC1	GE0/0/1	Access	Default VLAN 101

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Scheme (3)

3. Allocate IP addresses to STAs and APs using DHCP and statically configure IP addresses for network devices. For details, see the following two tables.

Device	Interface	Address/Mask
Agg-S1	VLANIF 1	192.168.1.254/24
	VLANIF 2	192.168.2.254/24
	VLANIF 3	192.168.3.254/24
	VLANIF 4	192.168.4.254/24
	VLANIF 100	192.168.100.254/24
	VLANIF 101	192.168.101.254/24
	VLANIF 102	192.168.102.2/30
CORE-R1	GE0/0/1	192.168.102.1/30
	GE0/0/0	Automatic obtaining via PPPoE
	Loopback0	1.1.1.1/32

Device	Interface	Address/Mask
Acc-S1	VLANIF 100	192.168.100.1/24
Acc-S2	VLANIF 100	192.168.100.2/24
Acc-S3	VLANIF 100	192.168.100.3/24
Acc-S4	VLANIF 100	192.168.100.4/24
AC1	VLANIF 101	192.168.1.101/24

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Scheme (4)

4. Configure the IP address allocation mode. For details about DHCP, see the following table.

Network Segment	Other Parameters	Remarks
192.168.1.0/24	Gateway:192.168.1.254 DNS:192.168.1.254	Agg-S1 functions as a DHCP server.
192.168.2.0/24	Gateway:192.168.2.254 DNS:192.168.2.254	Agg-S1 functions as a DHCP server. Fixed IP addresses are allocated to printer (1) and the FTP server.
192.168.3.0/24	Gateway:192.168.3.254 DNS:192.168.3.254	Agg-S1 functions as a DHCP server. A fixed IP address is allocated to printer (2).
192.168.3.0/24	Gateway:192.168.4.254 DNS:192.168.4.254	Agg-S1 functions as a DHCP server. Fixed IP addresses are allocated to printer (3) and the network administrator.
192.168.101.0/24	N/A	Agg-S1 functions as a DHCP server. The IP address (192.168.101.1) occupied by the AC is not allocated.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Scheme (5)

5. Configure routes. Static routes are used because the network scale is small and the number of NEs is also small. For details, see the following table.

Device	Route Configuration	Remarks
Acc-S1	0.0.0.0 0 192.168.100.254	Route that enables the network administrator to access Layer 2 switches across network segments.
Acc-S2		
Acc-S3		
Acc-S4		
AC1	0.0.0.0 0 192.168.101.254	Route that enables the administrator to access AC1 across network segments.
Agg-S1	0.0.0.0 0 192.168.102.1	Route that matches the traffic destined for the Internet
CORE-R1	192.168.0.0 20 192.168.102.2	Aggregated route for the core router to access the intranet
	Default route	Route pointing to an interface on the external network

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Scheme (6)

6. Configure network management. Set the network management mode to Telnet-based remote management and authentication mode to Authentication, Authorization, and Accounting (AAA). For details, see the following table.

Device	Management Mode	Authentication Mode	Remarks
Acc-S1	Telnet	AAA	The user name and password must be complex and different. In addition, record them.
Acc-S2			
Acc-S3			
Acc-S4			
Agg-S1			
CORE-R1			
AC1			
AP1&AP2	Centralized control and management by the AC	N/A	N/A

7. Network egress configuration

Device	Interface	Access Mode	NAT Mode	Remarks
CORE-R1	GE0/0/0	PPPoE	Easy IP	User name: **PPPoEUser123** Password: **Huawei@123**

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Configuration Scheme (7)

8. Configure the WLAN as planned.
9. Perform security-related configurations. For details, see the following table.

Module	Related Technology	Configuration
Traffic monitoring	Traffic policy, NAT, and ACL	1. Configure an advanced ACL to block the traffic from 192.168.1.0/24 to the service network segment on the intranet and allow other traffic to pass through. Configure a traffic filtering policy to reference this ACL and apply the policy to an interface. 2. Configure a basic ACL to permit only the traffic from 192.168.1.0/24 and apply this ACL to the NAT configuration on an outbound network interface.
Network management security	AAA and ACL	Configure a basic ACL to permit only the packets whose source IP address is the administrator's IP address and wildcard mask is 0, and apply the ACL to the VTY interfaces of all managed devices.
DHCP security	DHCP snooping	Enable DHCP snooping on all access switches and configure the uplink interfaces as trusted interfaces.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Small Campus Network Commissioning

1. Connectivity Test	2. High Reliability Commissioning	3. Service Performance Test
Basic link interconnection test	Loop prevention function test	Service traffic test
Layer 2 interoperability test	Path switchover test	Access control test
Layer 3 interoperability test	Hot Standby (HSB) test	

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.

Small Campus Network O&M

- After a small campus network is provisioned, it enters the O&M phase. Common O&M methods include:
  - Device environment check
  - Basic device information check
  - Device running status check
  - Service check
  - Alarm handling
- When the network scale reaches a certain level, the network management software can be used for network management and O&M to improve efficiency.

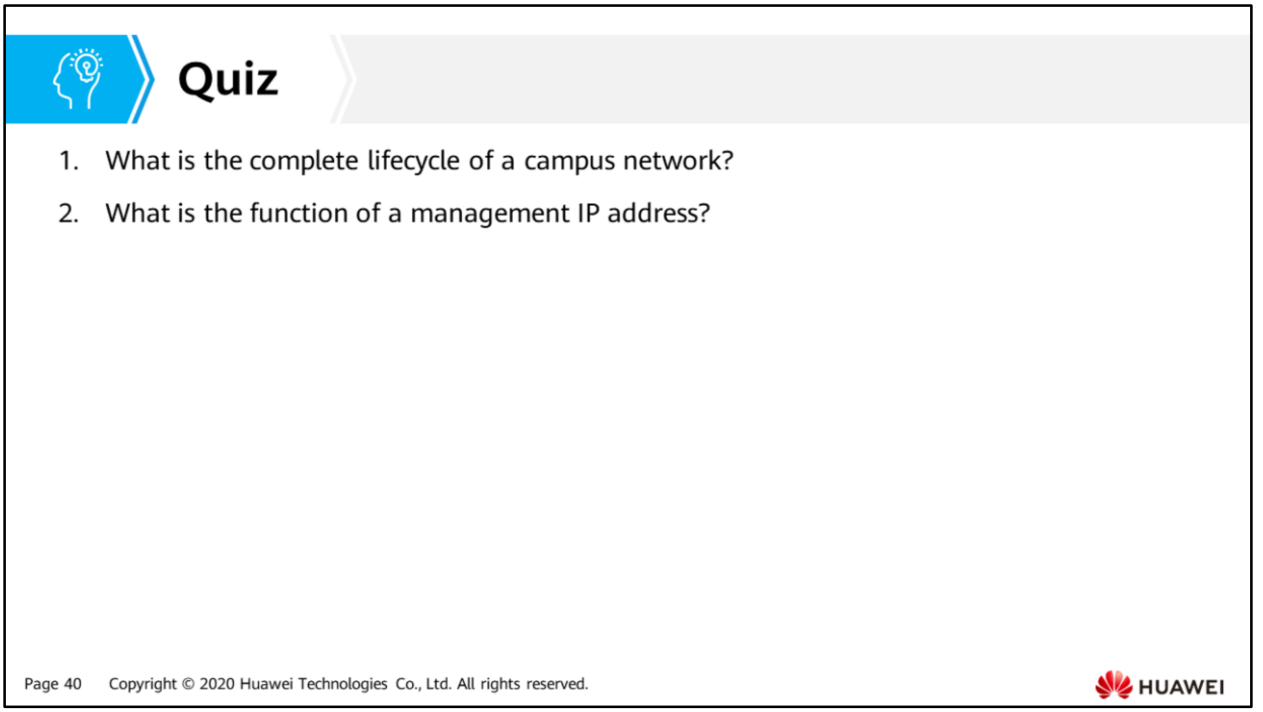
Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



Small Campus Network Optimization

- Network optimization can comprehensively improve the reliability and robustness of networks and better support the development of enterprise services. Common network optimization solutions include but are not limited to:
  - Device performance optimization, such as hardware upgrade and software version update
  - Basic network optimization, such as network architecture optimization and routing protocol adjustment
  - Service quality optimization, such as preferential forwarding of voice and video services
- Formulate an appropriate network optimization solution based on network requirements and actual conditions.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.



1. Network planning and design, deployment and implementation, O&M, and optimization
2. IP address used by the network administrator to manage a device

Summary

- This chapter describes the concepts, types, and common technologies of campus networks.
- Understand the lifecycle of campus networks:
  - Planning and design
  - Deployment and implementation
  - Network O&M
  - Network optimization
- Based on the previous courses, this course focuses on the planning, design, deployment, and implementation of campus networks and details how to establish a small campus network.

Copyright © 2020 Huawei Technologies Co., Ltd. All rights reserved.


Thank You
www.huawei.com