ENCOR v1.1

350-401

Implementing Cisco Enterprise Network Core Technologies

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Getting to Know You

What is your **First Name**?

What is your **Job Role**?

What is your **Cisco Experience** on a scale of 1 to 10 with 10 being an expert?

Why have you joined us in **ENCOR**?

Raymond, Instructor/Author/Network and Cloud dude, Because my Boss told me to be here. ☺

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Introduction to ENCOR Course and Exam Objectives

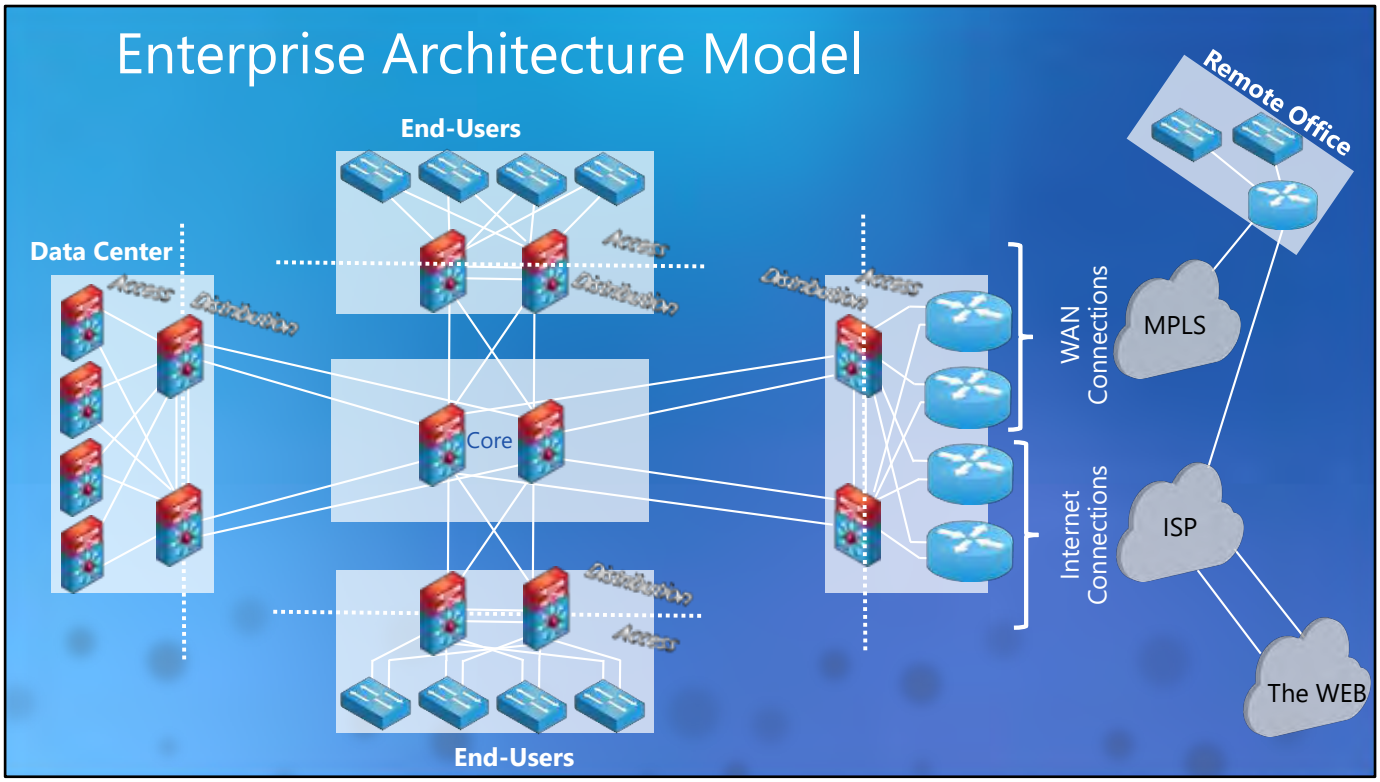
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Access and Distribution Layer Features and Services

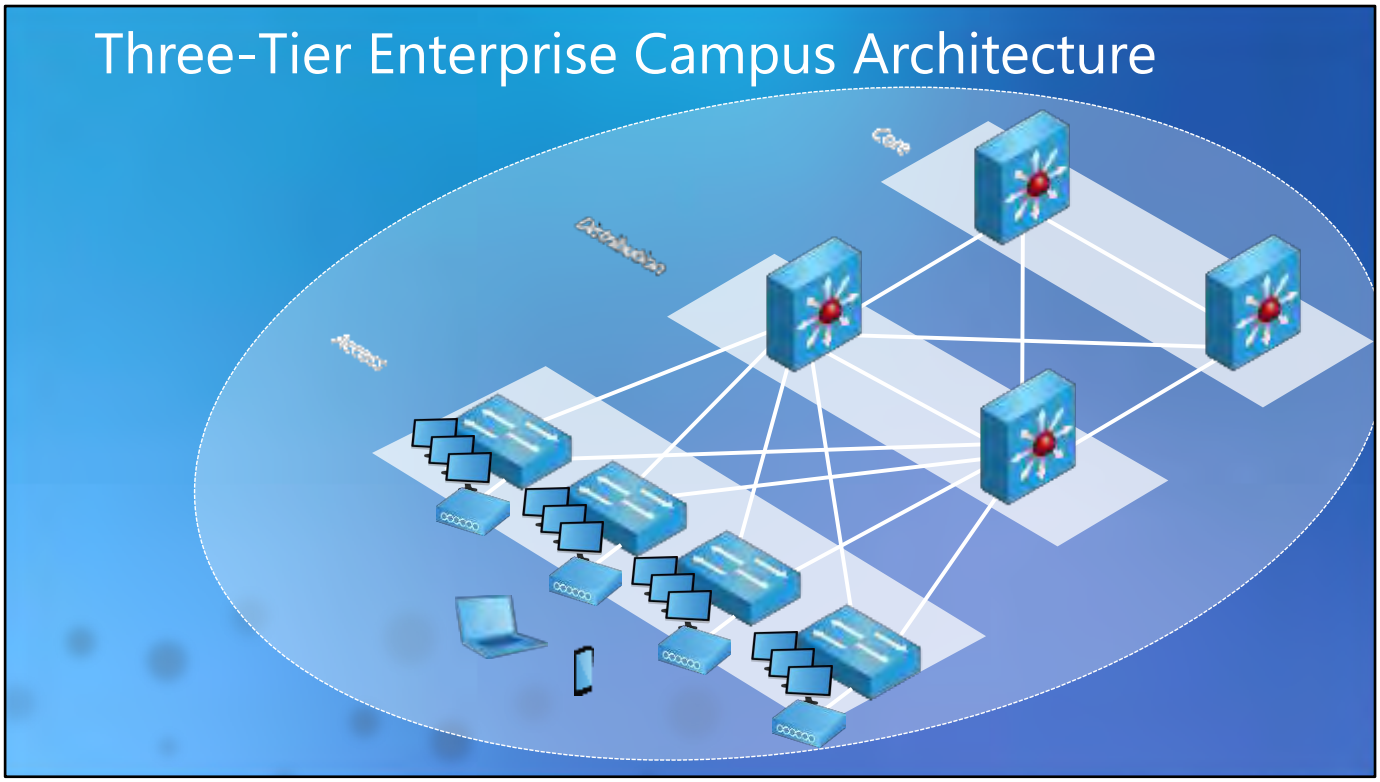
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Campus Architecture

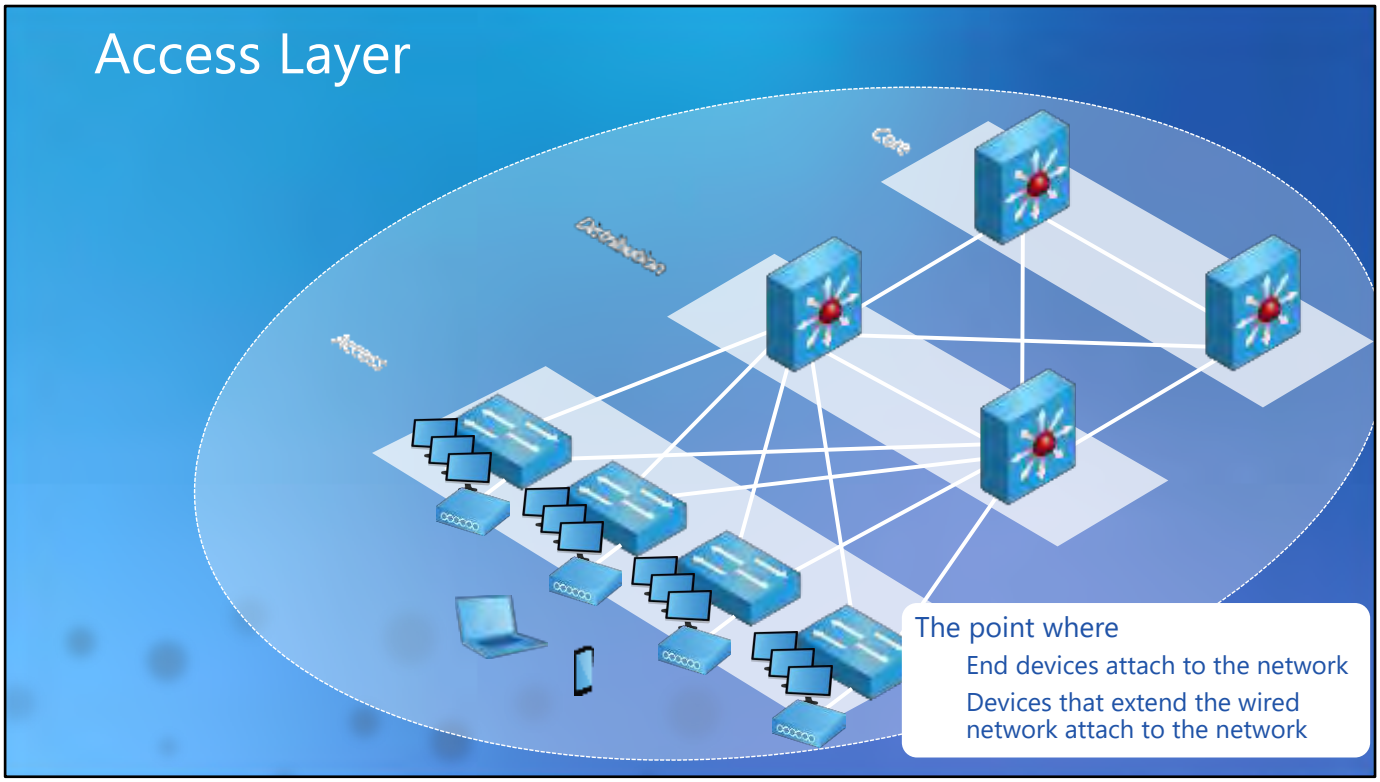
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



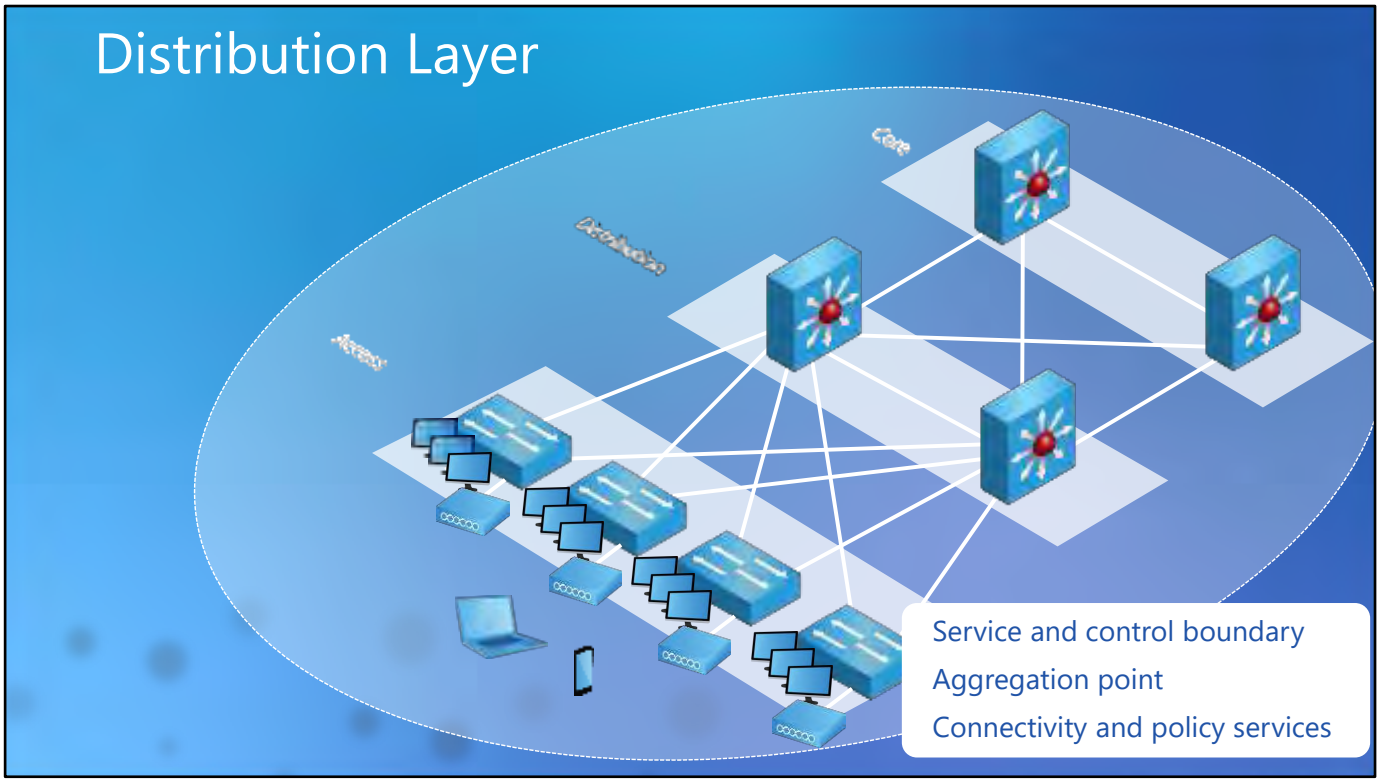
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



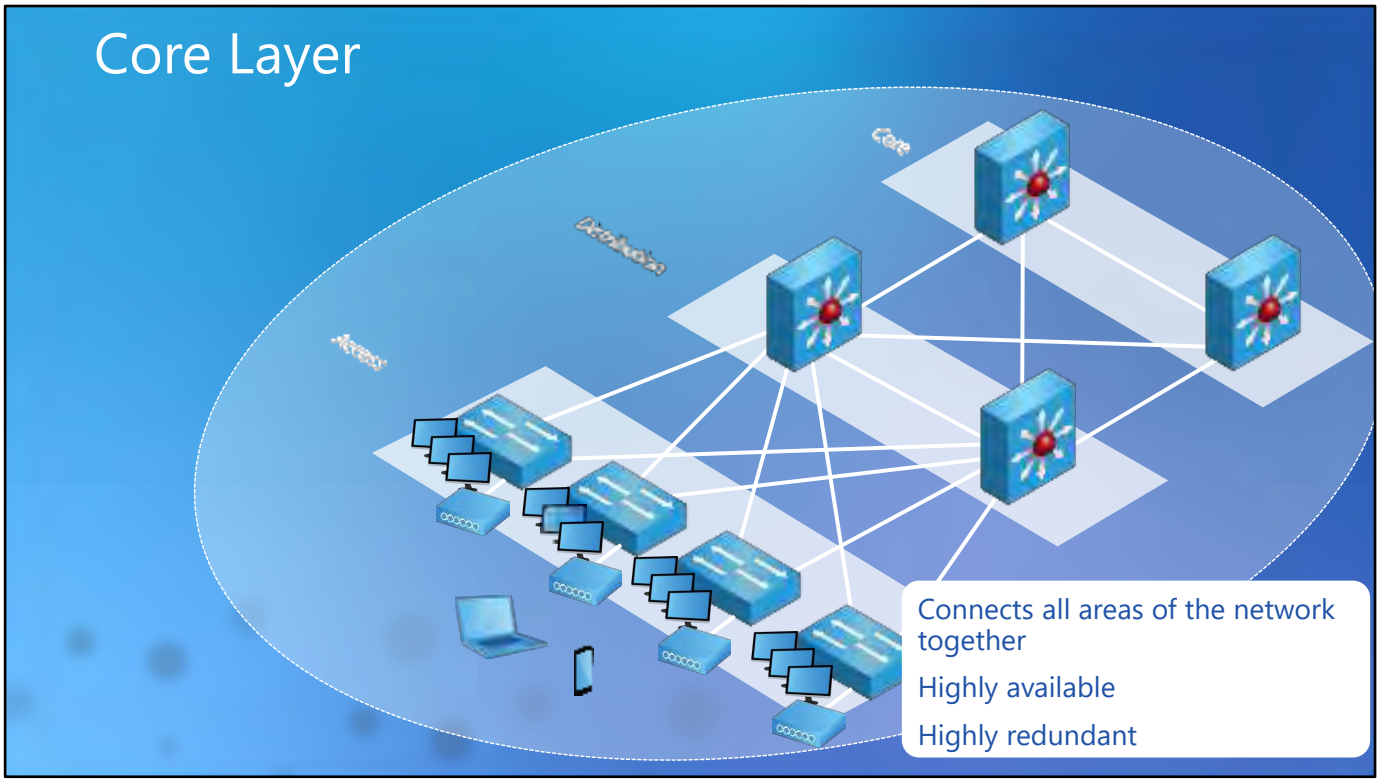
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



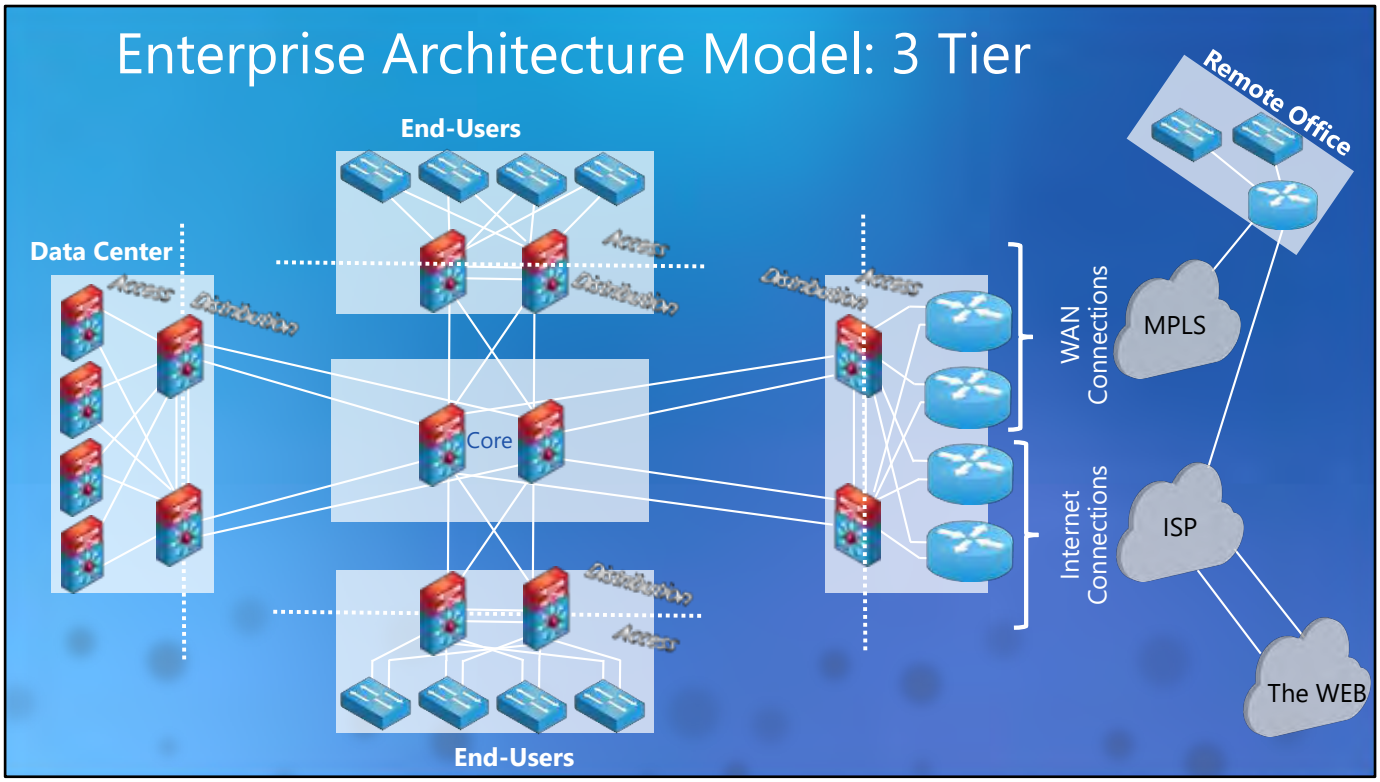
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



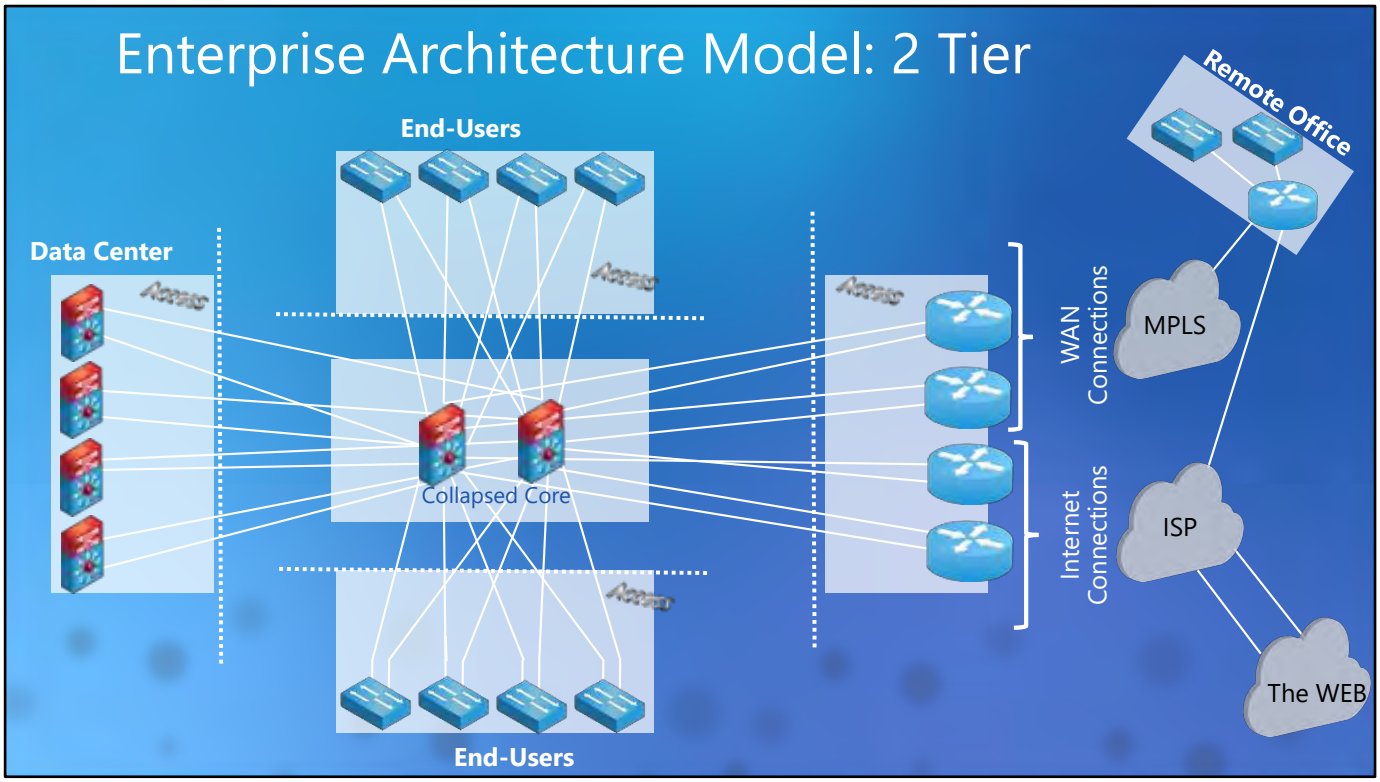
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



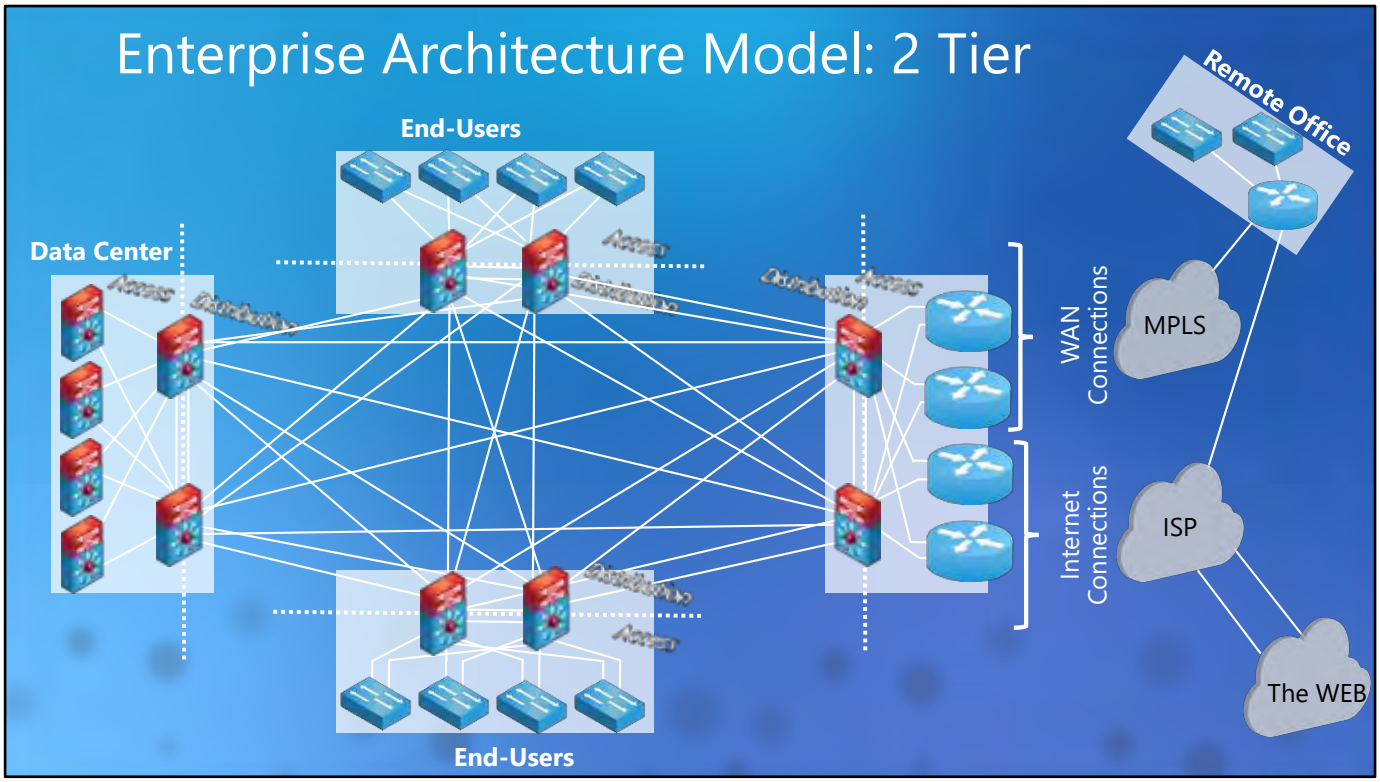
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



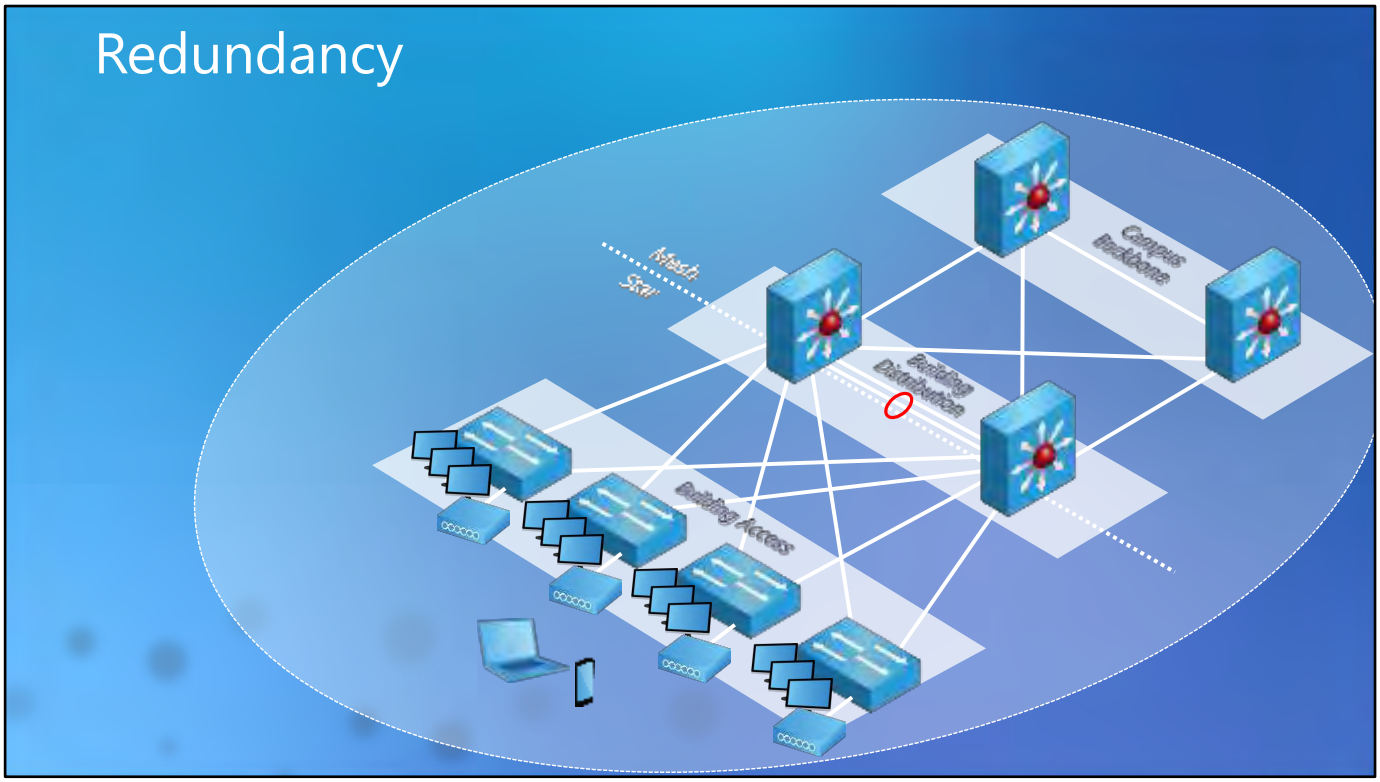
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



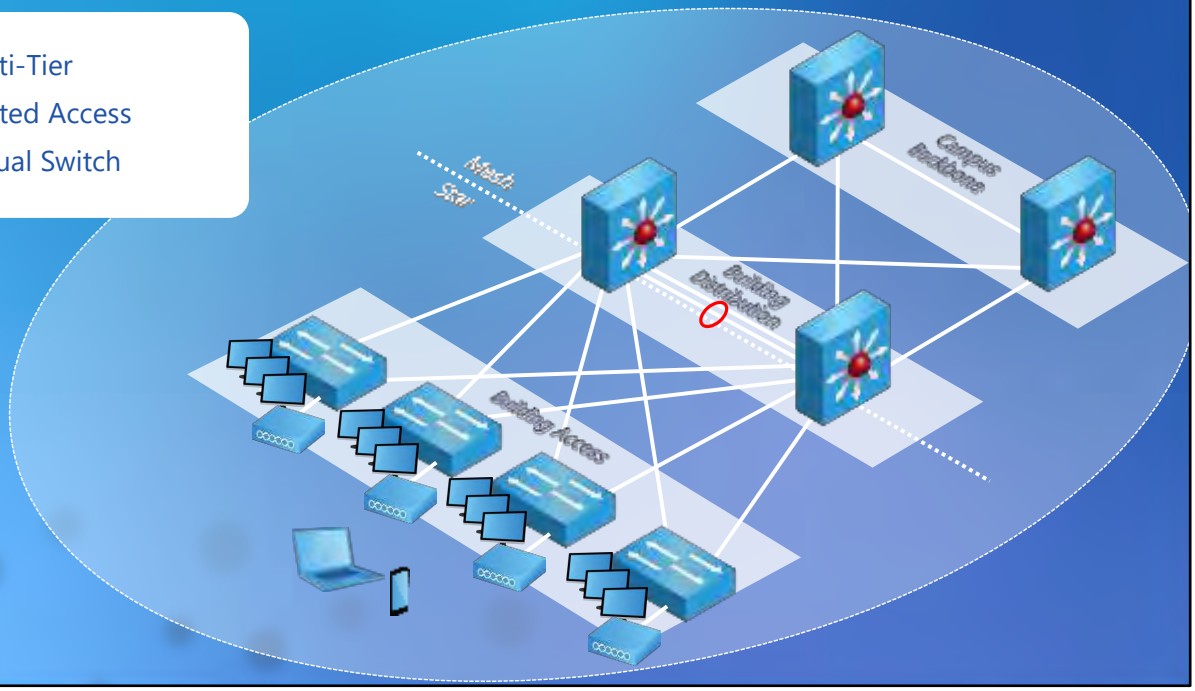
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



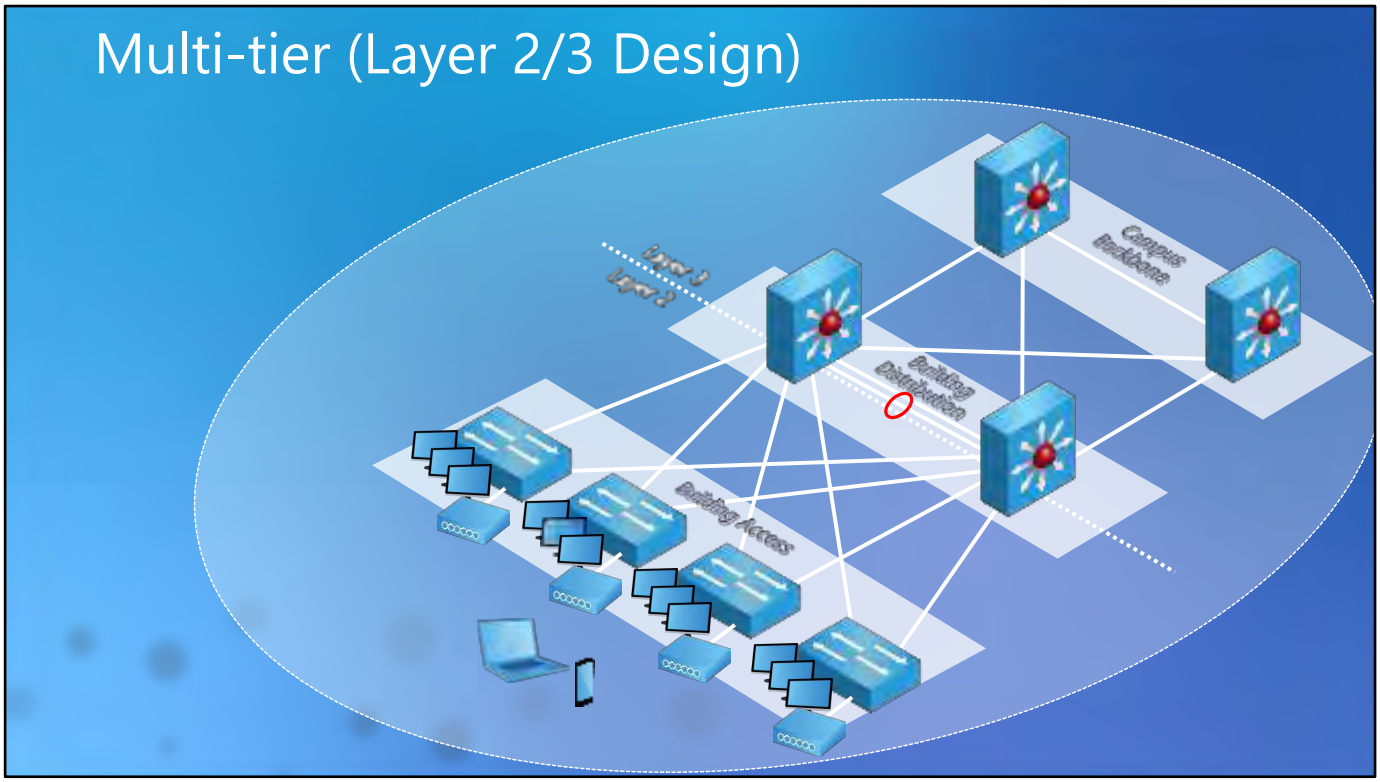
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Access – Distribution Design Options

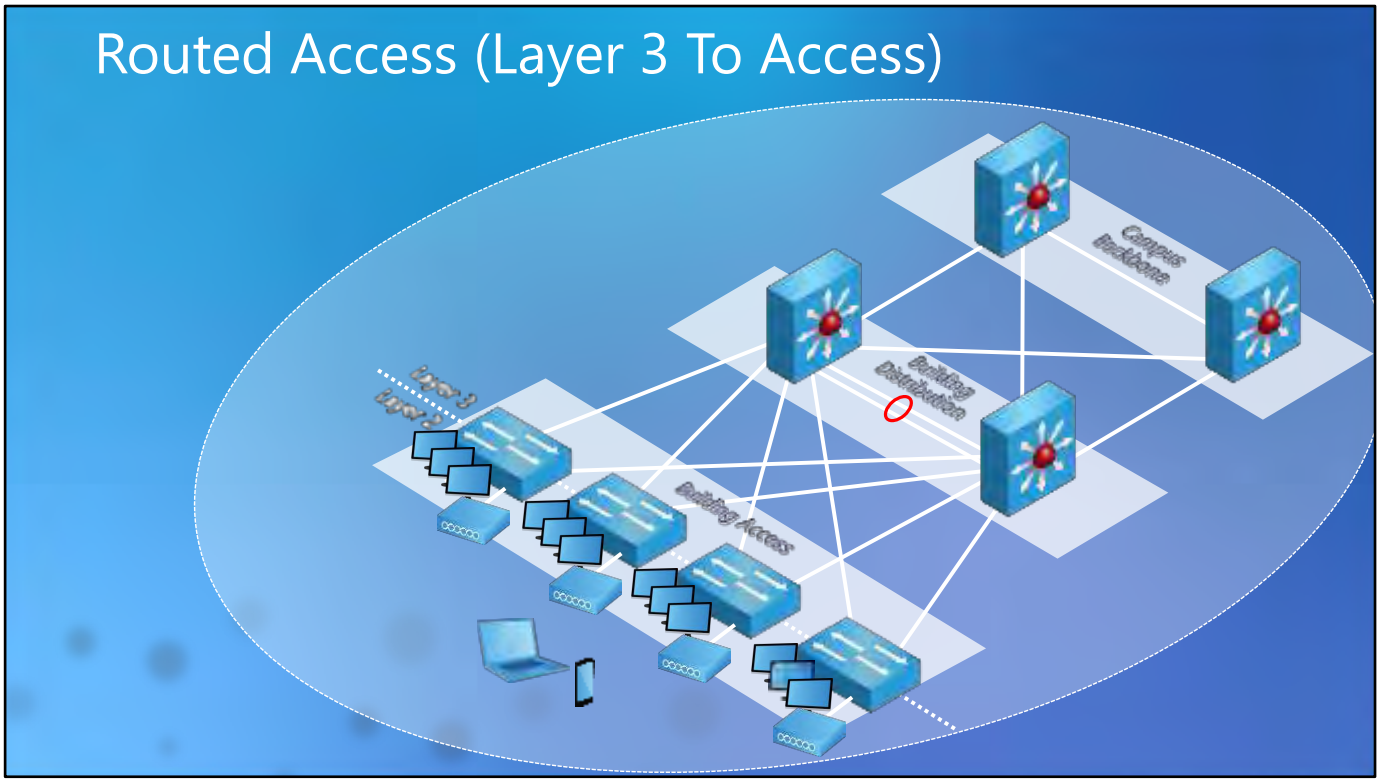
- Multi-Tier
- Routed Access
- Virtual Switch



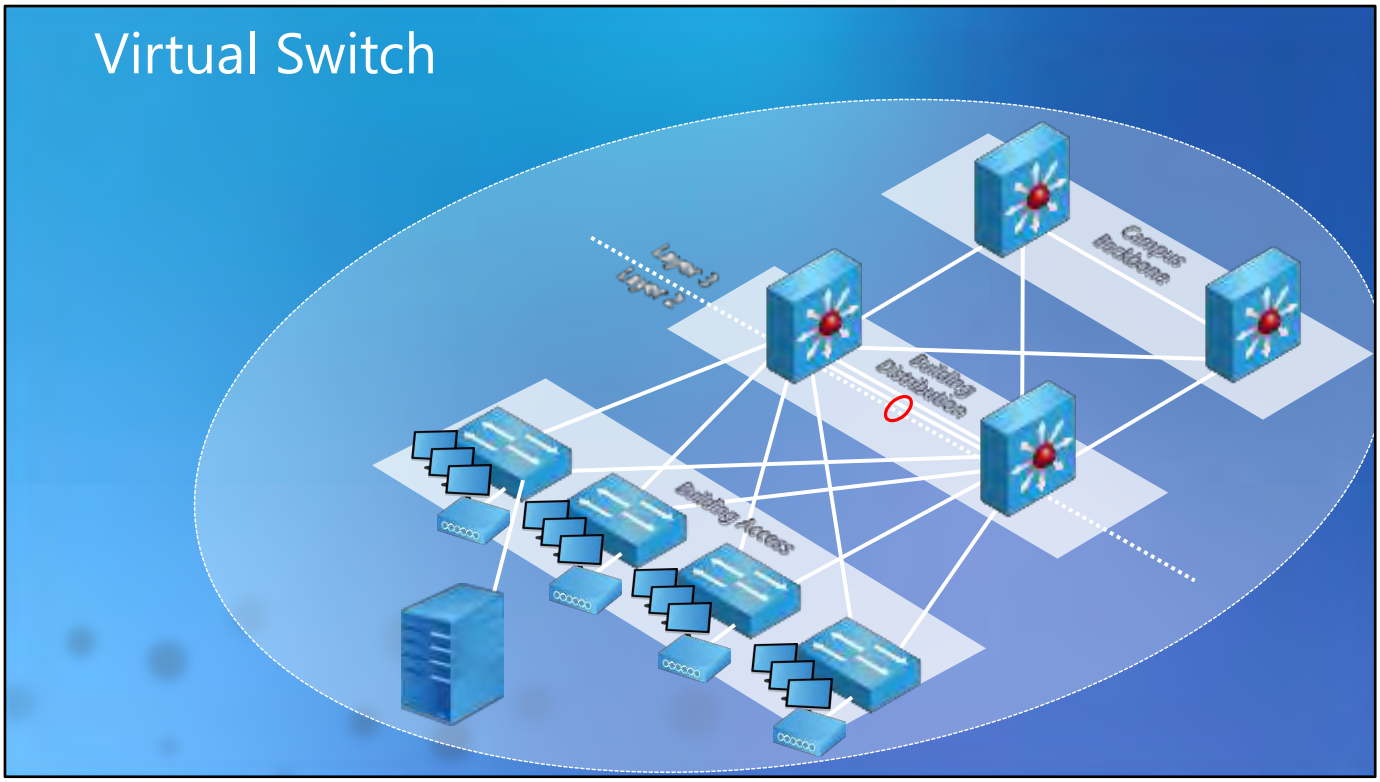
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



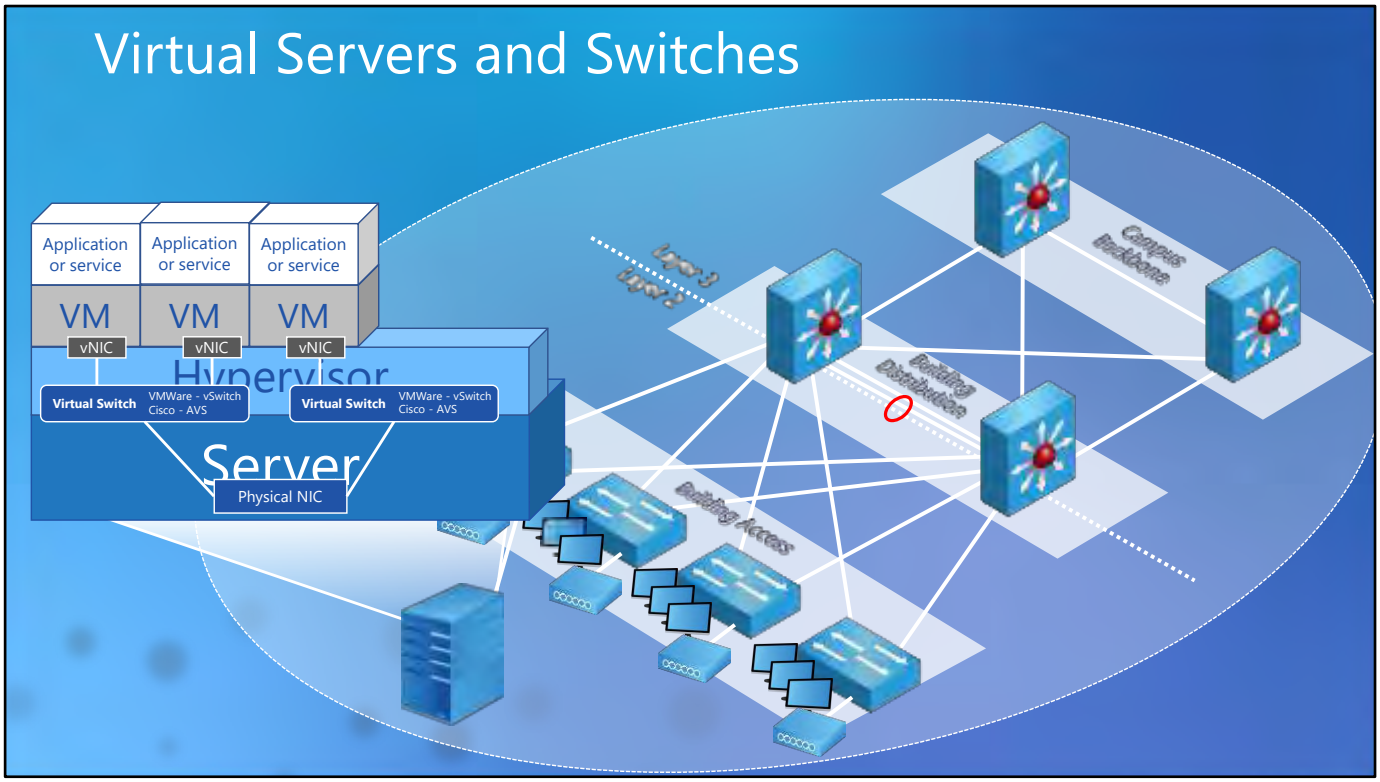
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



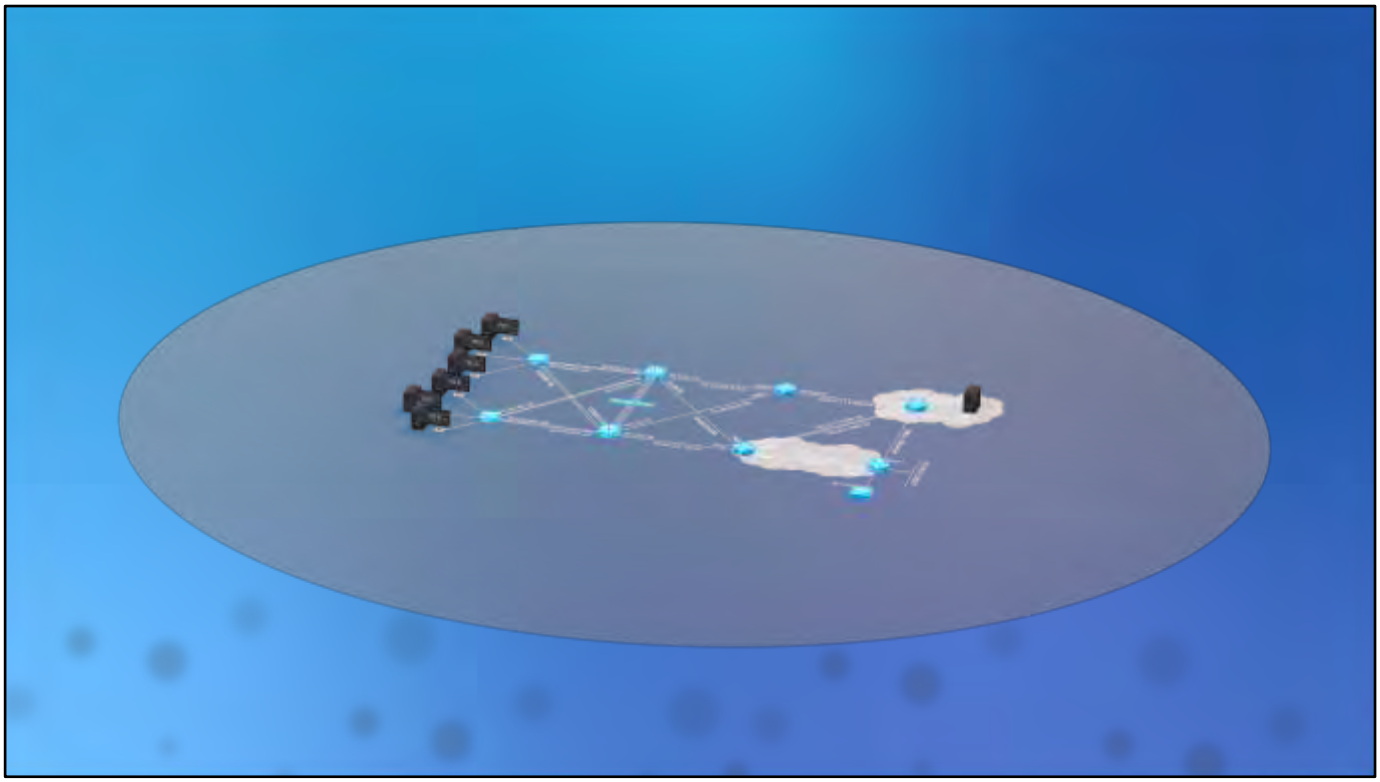
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

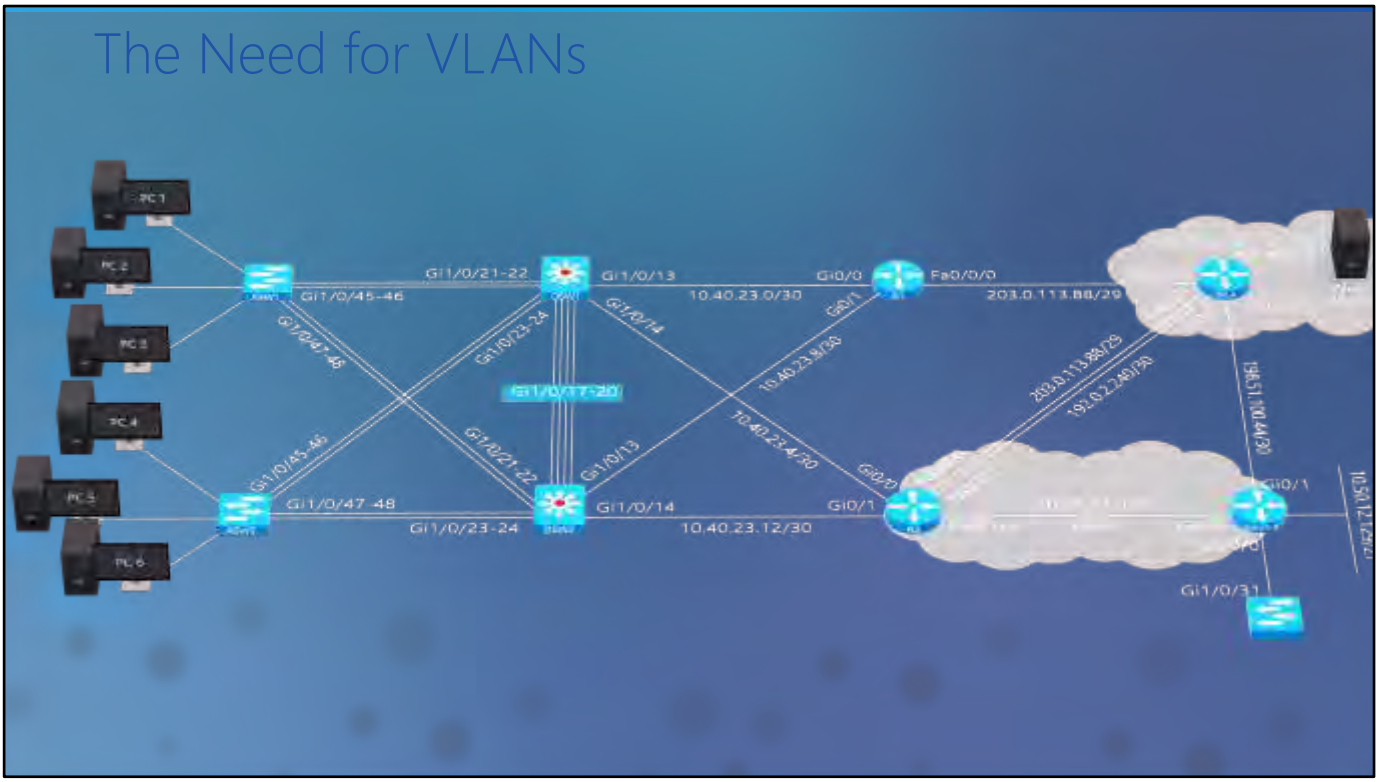
Configuring and Verifying VLANs

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



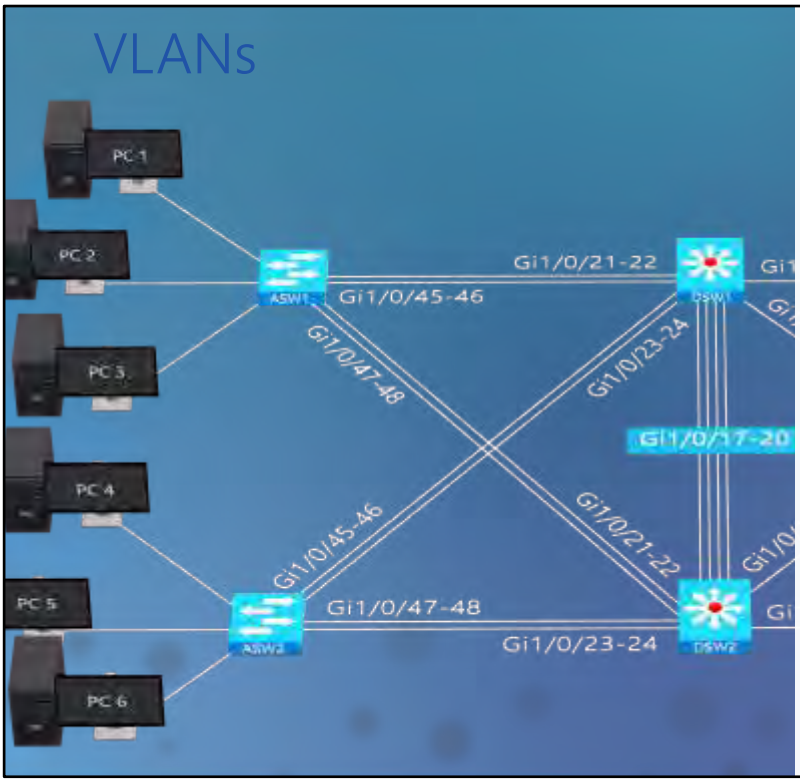
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

The Need for VLANs



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



VLAN is a virtual LAN

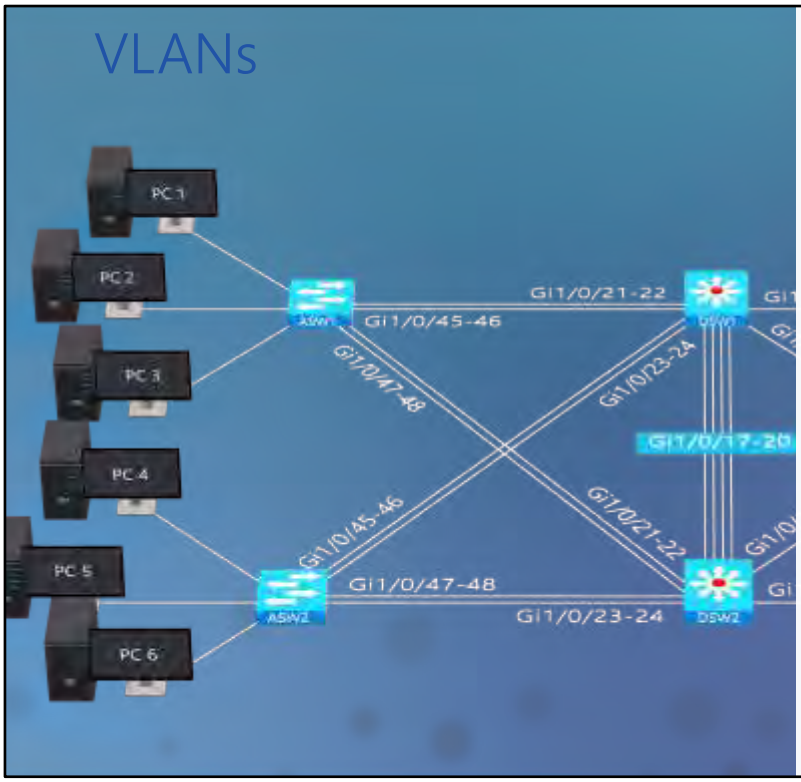
- VLAN = logical network (subnet)
- VLAN = broadcast domain

Each VLAN is its own Subnet

- Each Subnet is its own Broadcast Domain

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



Review:

1. What does a switch do first when it receives a frame?

Learns the source MAC address of the frame and populates the MAC address table with the:

MAC address

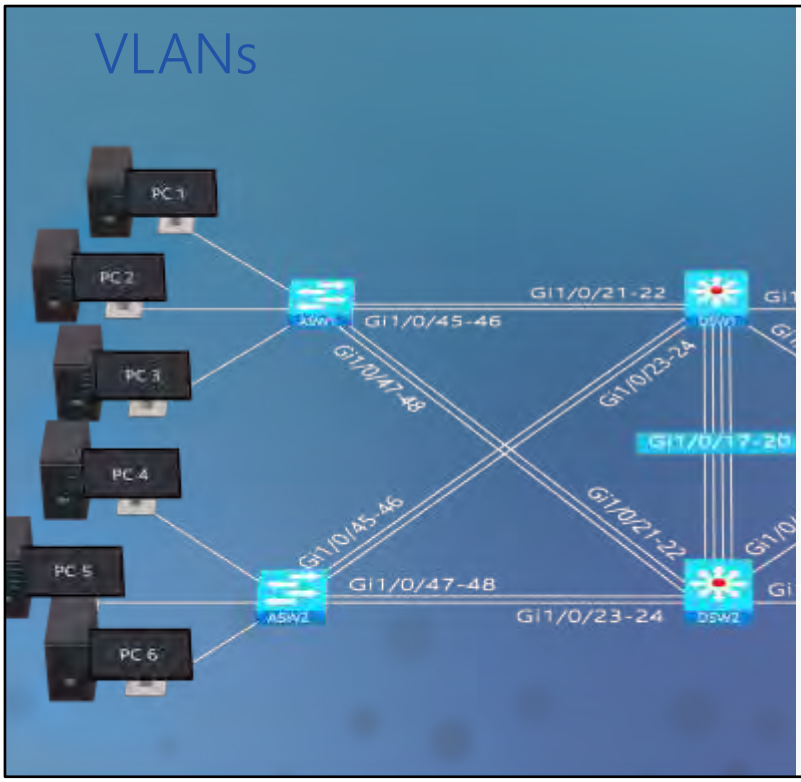
The Port the frame arrived in on

The VLAN ID of the port *

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



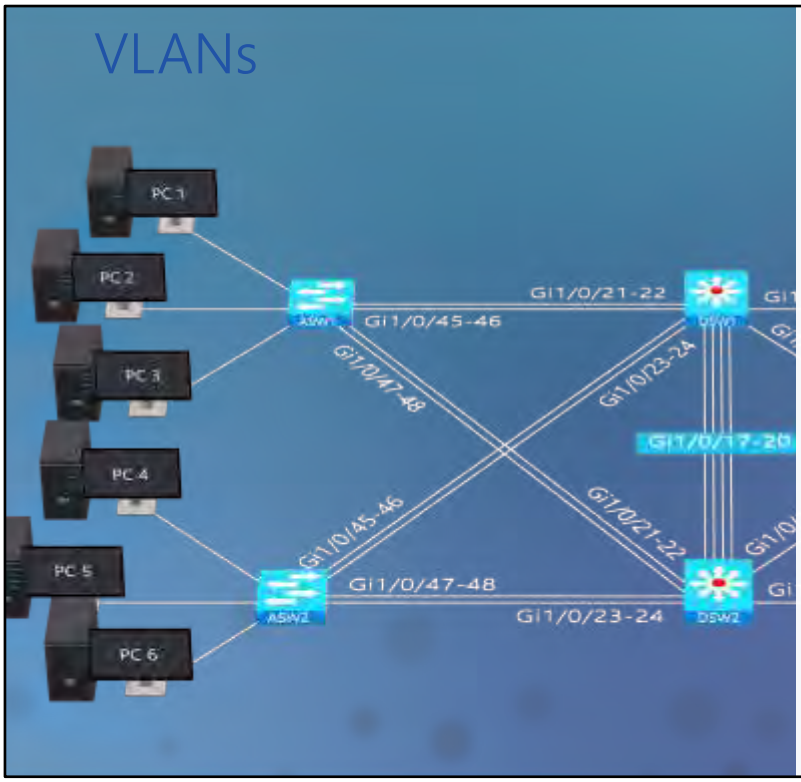
Review:

2 What part of the frame does a switch use to make a forwarding decision?

The destination MAC address

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



Review:

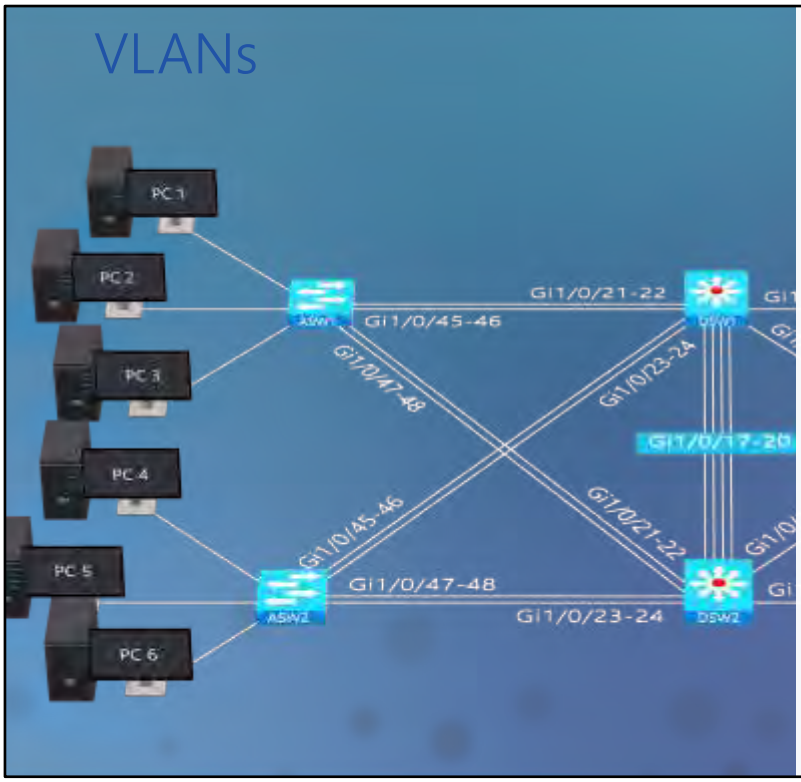
3. When will the switch forward a frame out a specific port?

When the destination MAC address is in the MAC address table…

And the destination is in the SAME VLAN!

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



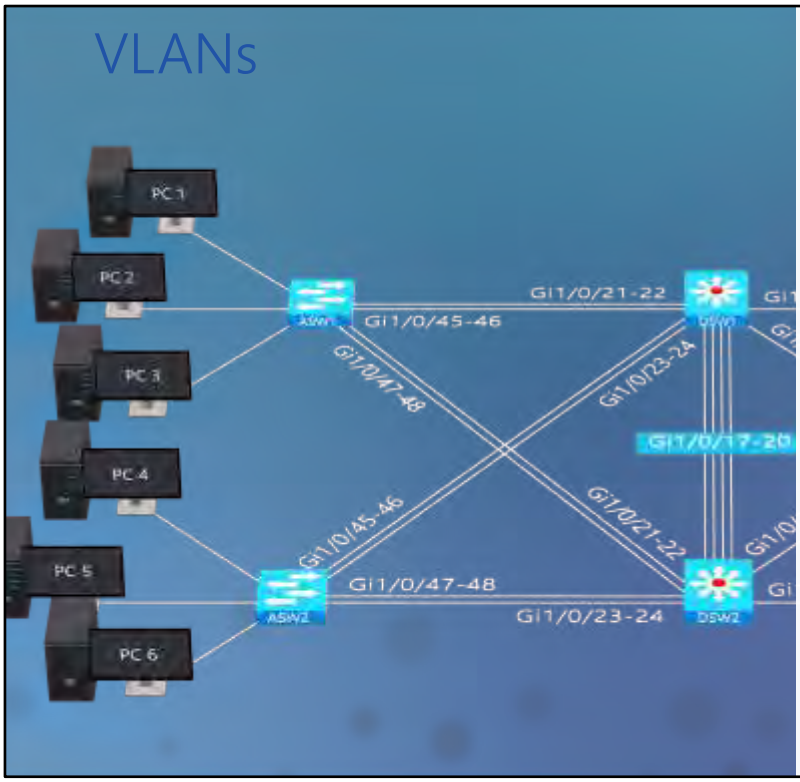
Review:

4 What happens when the destination MAC address is not in the same VLAN?

The frame is dropped!

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



Review:

5 When will the frame get flooded?

When the destination is FFFF:FFFF:FFFF (a broadcast frame)…

When the destination is not in the MAC address table

Sub-Question) What ports will the frame get flooded out?

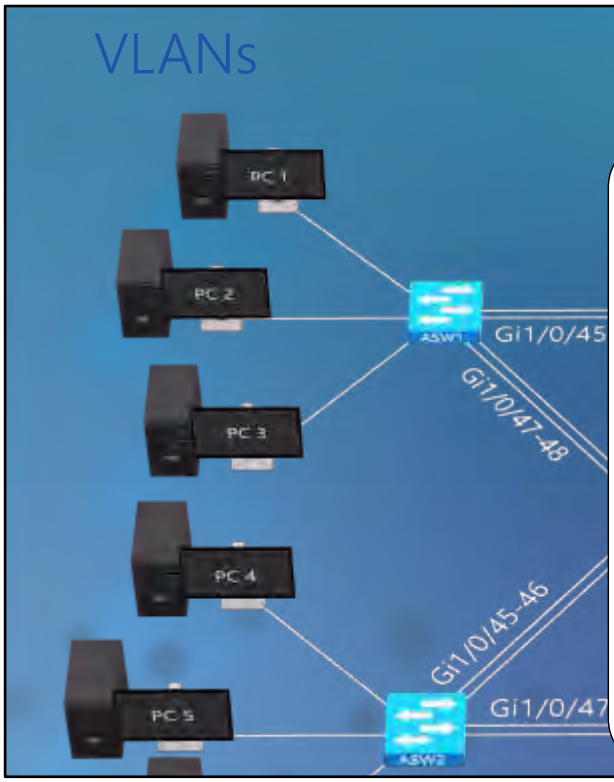
ONLY THE PORTS THAT ARE IN THE SAME VLAN AS THE SOURCE!!!

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

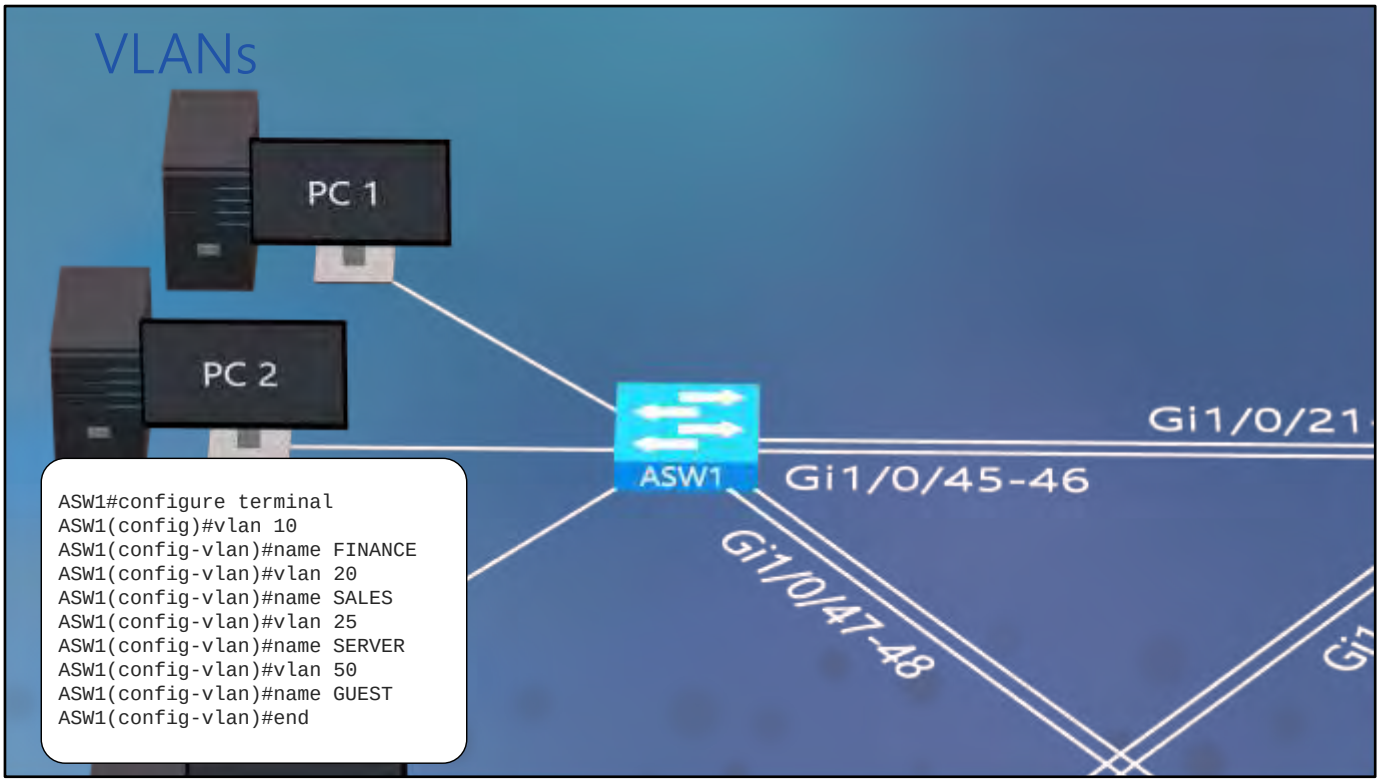
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



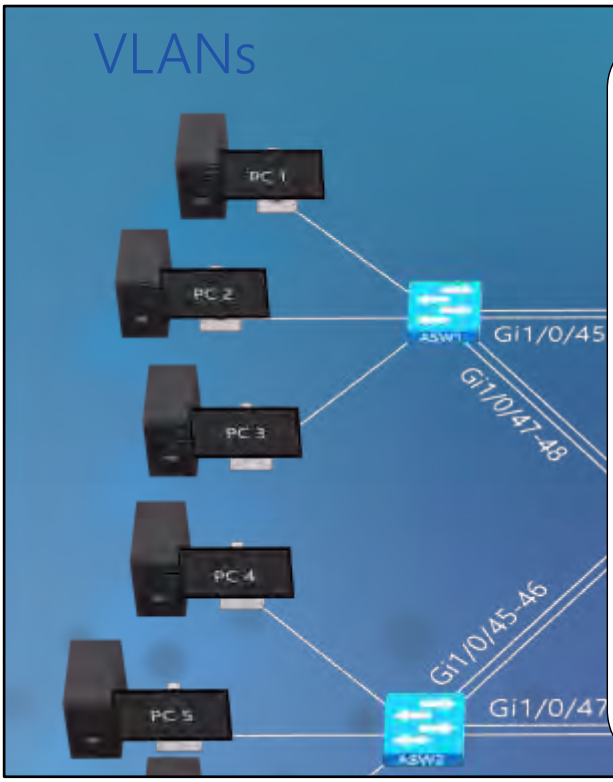

```
ASW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28, Gi1/0/29, Gi1/0/30
                                                Gi1/0/31, Gi1/0/32, Gi1/0/33
                                                Gi1/0/34, Gi1/0/35, Gi1/0/36
                                                Gi1/0/37, Gi1/0/38, Gi1/0/39
                                                Gi1/0/40, Gi1/0/41, Gi1/0/42
                                                Gi1/0/43, Gi1/0/44, Gi1/0/45
                                                Gi1/0/46, Gi1/0/47, Gi1/0/48
                                                Gi1/0/49, Gi1/0/50, Gi1/0/51
                                                Gi1/0/52
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

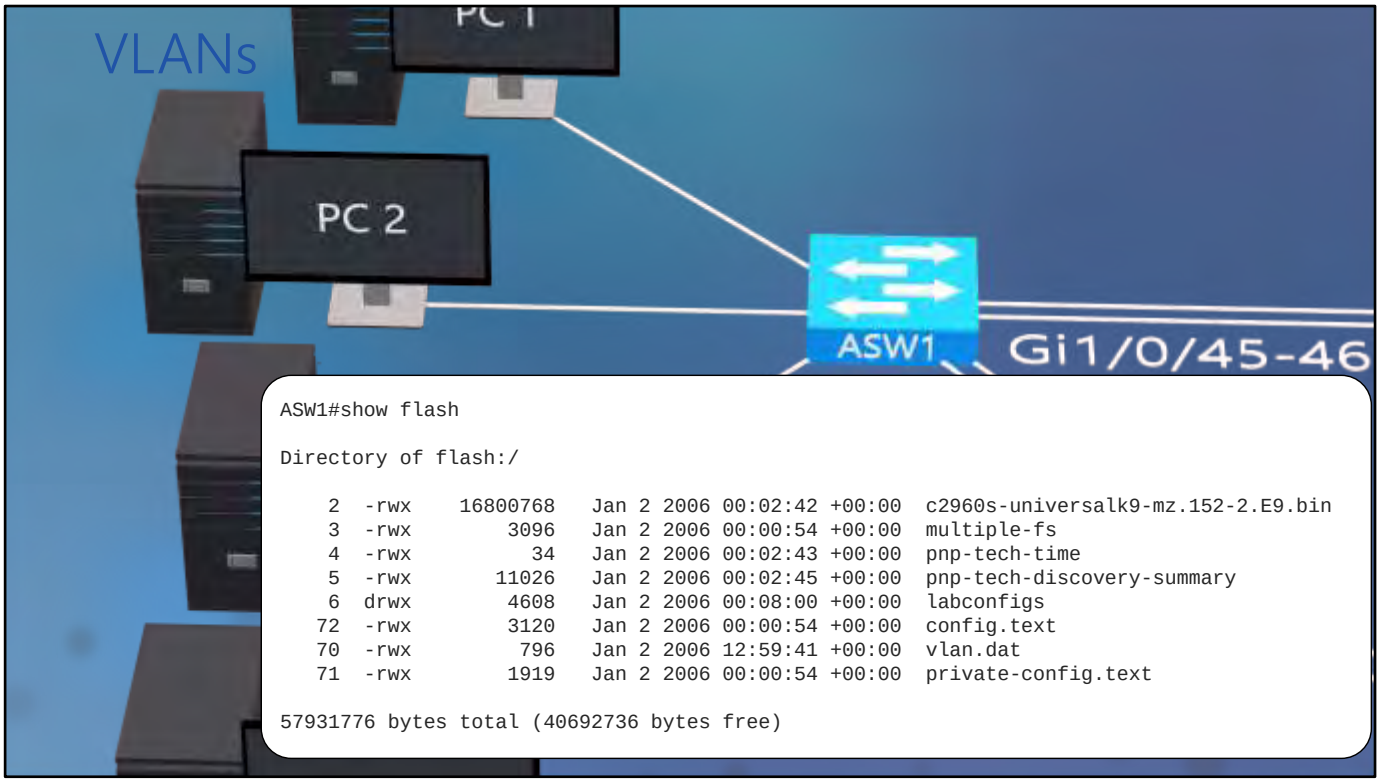
VLANs




```
ASW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28, Gi1/0/29, Gi1/0/30
                                                Gi1/0/31, Gi1/0/32, Gi1/0/33
                                                Gi1/0/34, Gi1/0/35, Gi1/0/36
                                                Gi1/0/37, Gi1/0/38, Gi1/0/39
                                                Gi1/0/40, Gi1/0/41, Gi1/0/42
                                                Gi1/0/43, Gi1/0/44, Gi1/0/45
                                                Gi1/0/46, Gi1/0/47, Gi1/0/48
                                                Gi1/0/49, Gi1/0/50, Gi1/0/51
                                                Gi1/0/52
10   FINANCE                          active
20   SALES                            active
25   SERVER                           active
50   GUEST                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

©2023 by StormWind LLC. All rights reserved.

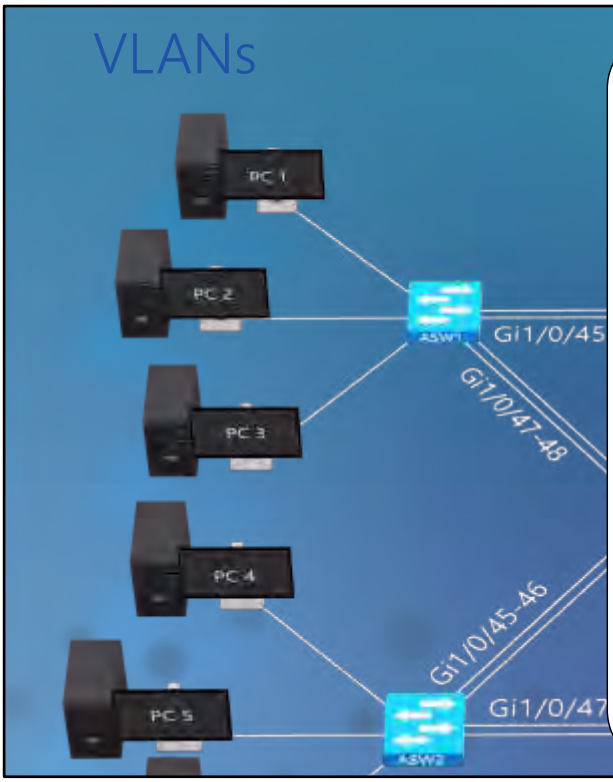
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
ASW1#show flash

Directory of flash:/

    2  -rwx    16800768   Jan 2 2006 00:02:42 +00:00  c2960s-universalk9-mz.152-2.E9.bin
    3  -rwx        3096   Jan 2 2006 00:00:54 +00:00  multiple-fs
    4  -rwx          34   Jan 2 2006 00:02:43 +00:00  pnp-tech-time
    5  -rwx       11026   Jan 2 2006 00:02:45 +00:00  pnp-tech-discovery-summary
    6  drwx        4608   Jan 2 2006 00:08:00 +00:00  labconfigs
   72  -rwx        3120   Jan 2 2006 00:00:54 +00:00  config.text
   70  -rwx         796   Jan 2 2006 12:59:41 +00:00  vlan.dat
   71  -rwx        1919   Jan 2 2006 00:00:54 +00:00  private-config.text

57931776 bytes total (40692736 bytes free)
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs

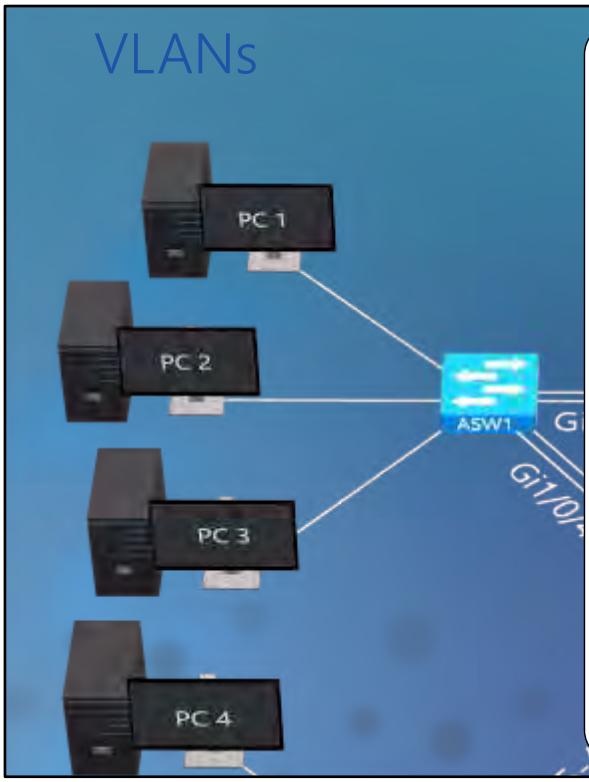



```
ASW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28, Gi1/0/29, Gi1/0/30
                                                Gi1/0/31, Gi1/0/32, Gi1/0/33
                                                Gi1/0/34, Gi1/0/35, Gi1/0/36
                                                Gi1/0/37, Gi1/0/38, Gi1/0/39
                                                Gi1/0/40, Gi1/0/41, Gi1/0/42
                                                Gi1/0/43, Gi1/0/44, Gi1/0/45
                                                Gi1/0/46, Gi1/0/47, Gi1/0/48
                                                Gi1/0/49, Gi1/0/50, Gi1/0/51
                                                Gi1/0/52
10   FINANCE                          active
20   SALES                            active
25   SERVER                           active
50   GUEST                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

©2023 by StormWind LLC. All rights reserved.

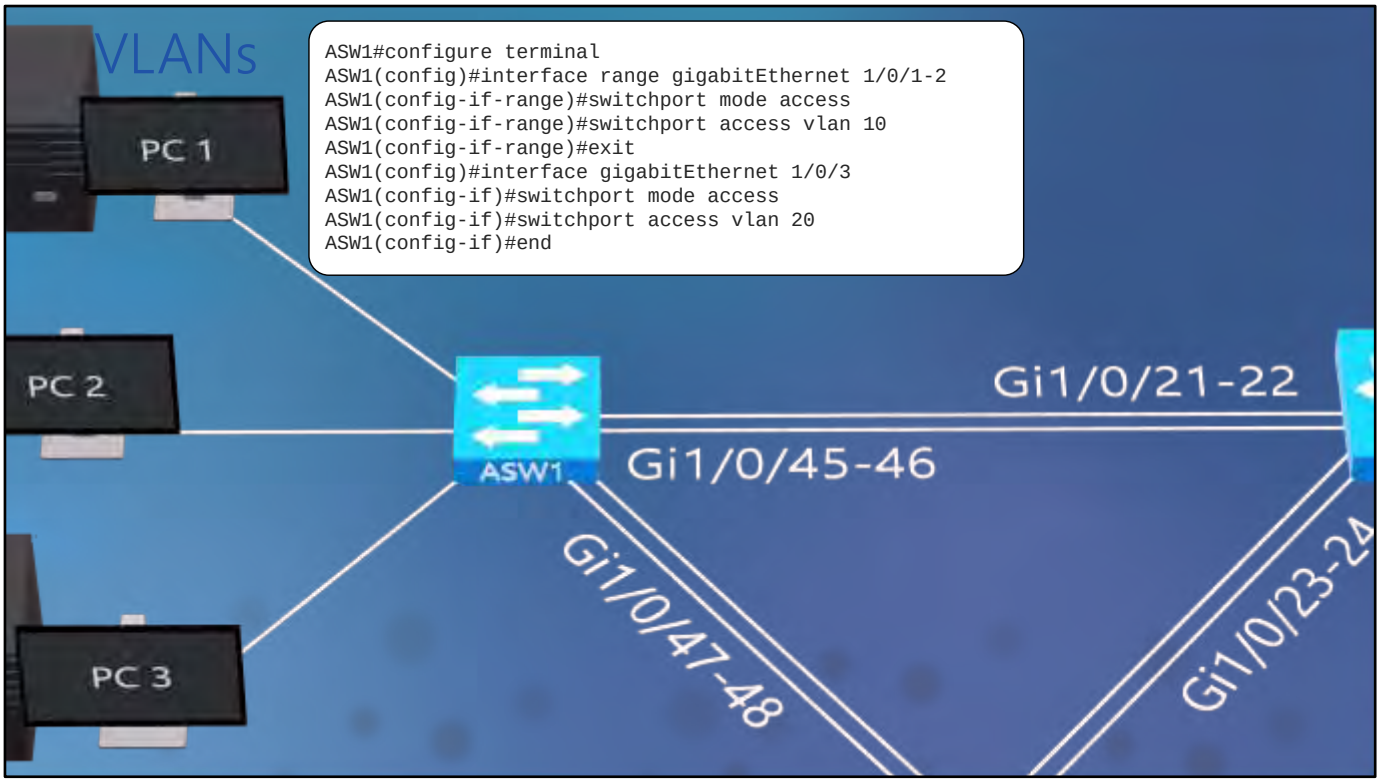
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs

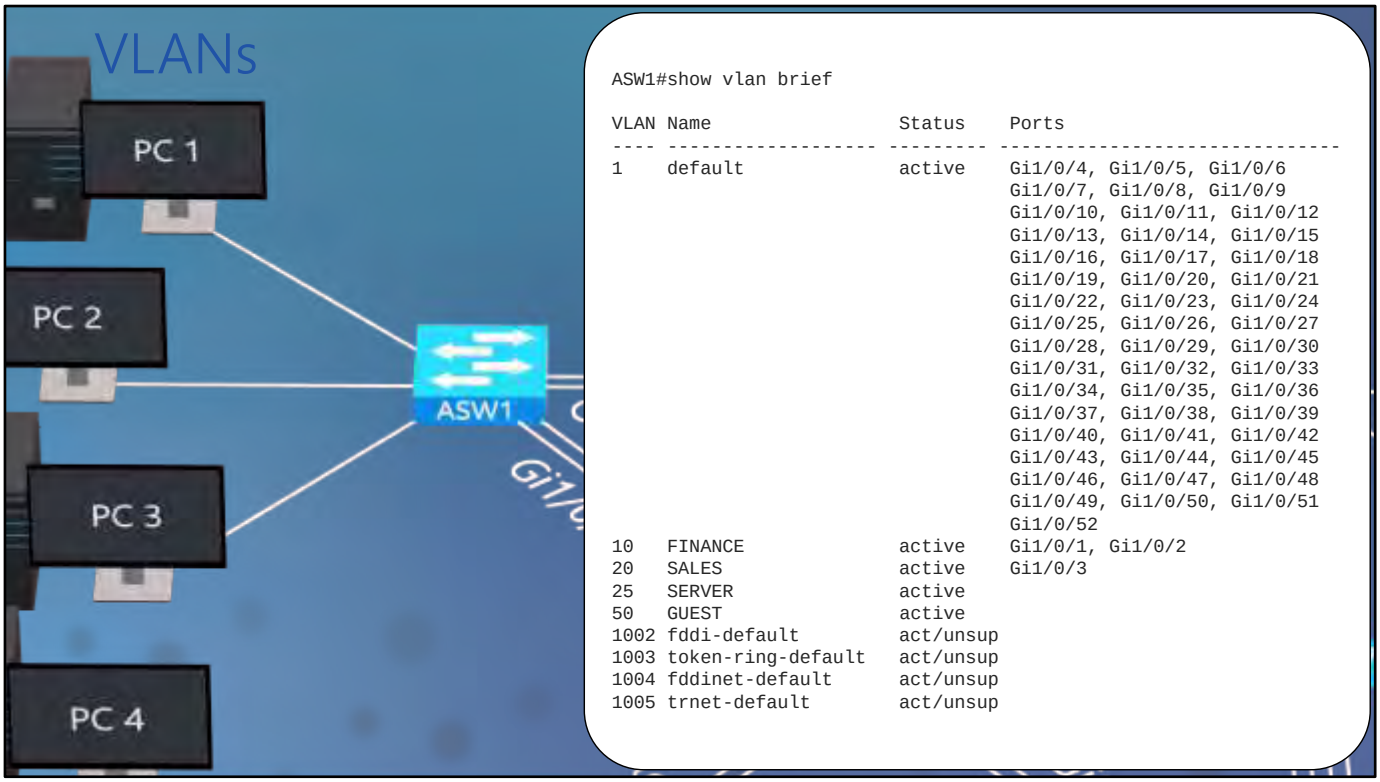



```
ASW1#show interfaces gigabitEthernet 1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



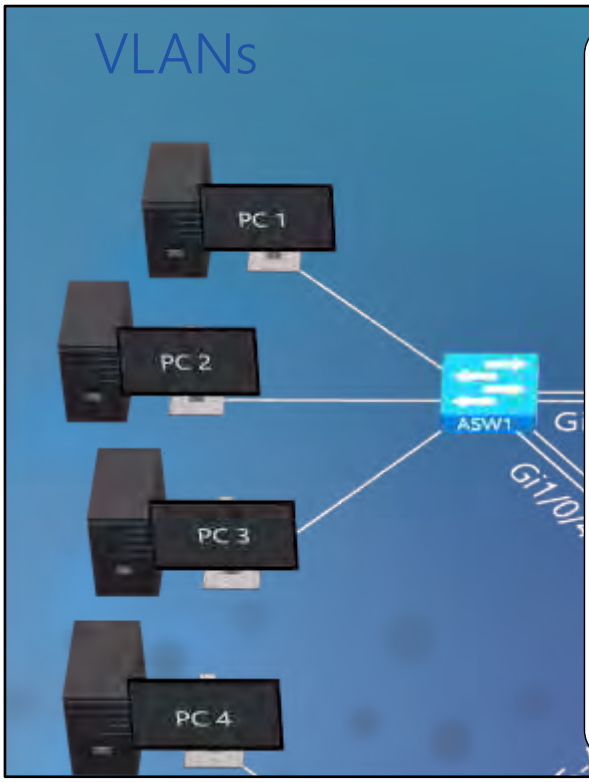
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
ASW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28, Gi1/0/29, Gi1/0/30
                                                Gi1/0/31, Gi1/0/32, Gi1/0/33
                                                Gi1/0/34, Gi1/0/35, Gi1/0/36
                                                Gi1/0/37, Gi1/0/38, Gi1/0/39
                                                Gi1/0/40, Gi1/0/41, Gi1/0/42
                                                Gi1/0/43, Gi1/0/44, Gi1/0/45
                                                Gi1/0/46, Gi1/0/47, Gi1/0/48
                                                Gi1/0/49, Gi1/0/50, Gi1/0/51
                                                Gi1/0/52
10   FINANCE                          active    Gi1/0/1, Gi1/0/2
20   SALES                            active    Gi1/0/3
25   SERVER                           active
50   GUEST                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs




```
ASW1#show interfaces gigabitEthernet 1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 10 (FINANCE)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

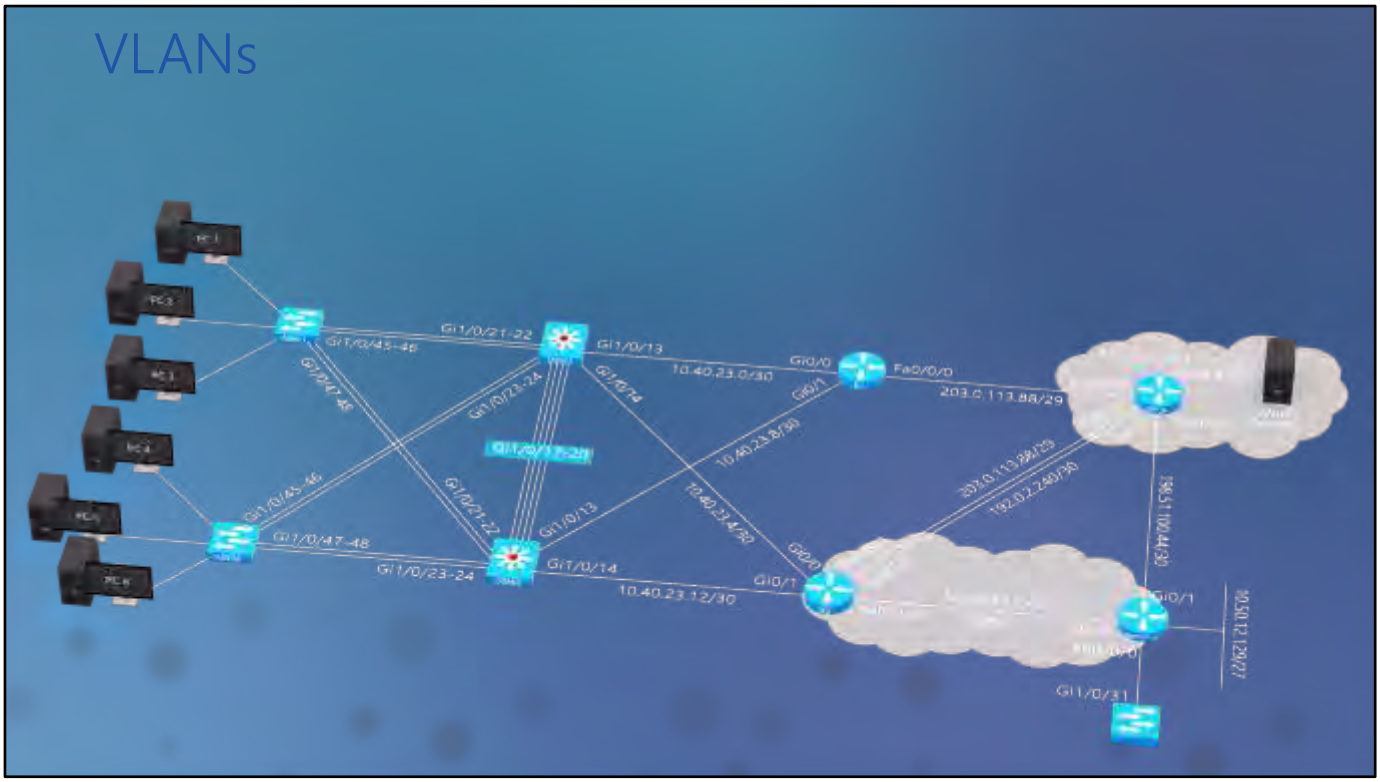
VLANs

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs

Voice Requirements

Bandwidth per call depends on codec, sampling rate, and Layer 2 media:

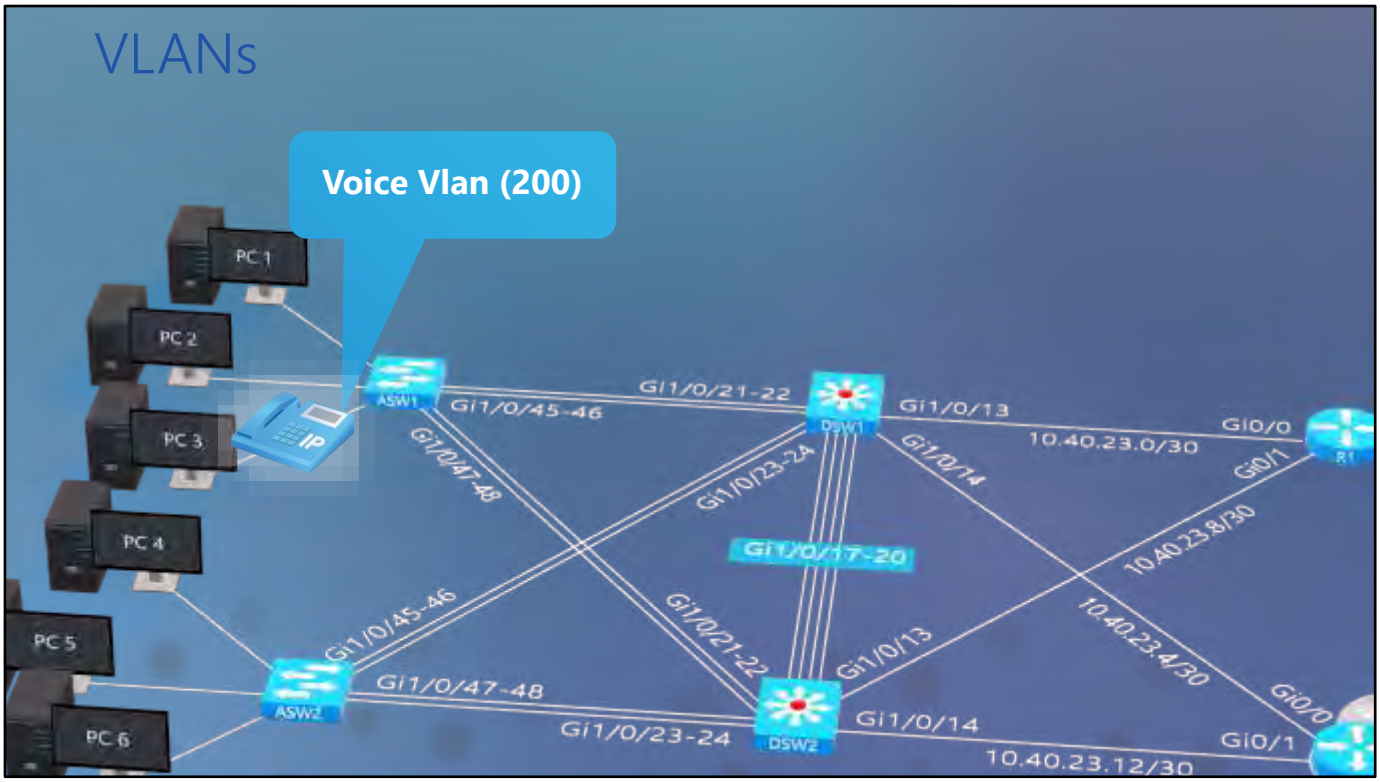
- Jitter less than 30 ms*
- Delay less than 150 ms*
- Packet loss that is less than 1 percent*
- Marked with 802.1p marking of 5

Voice

- Smooth
- Benign
- Drop-sensitive
- Delay-Sensitive
- UDP priority

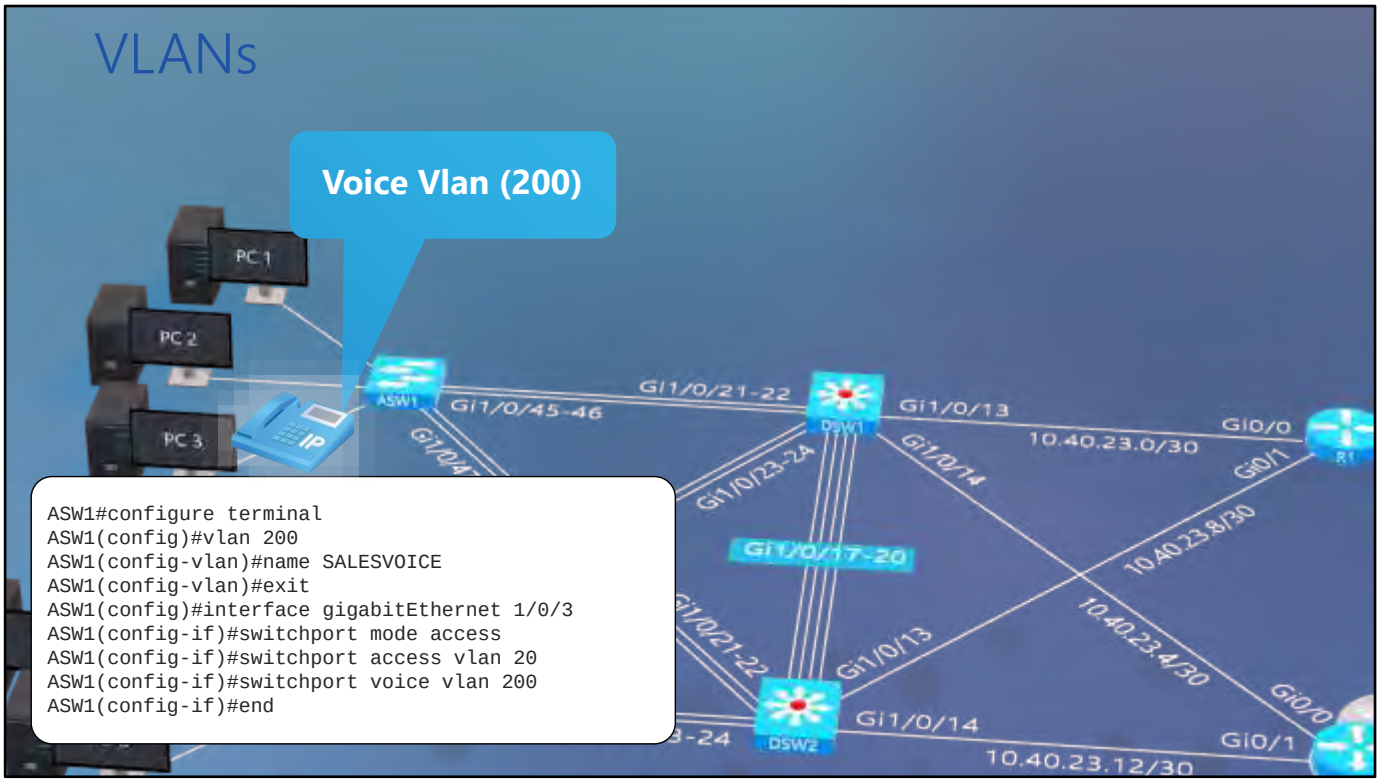
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

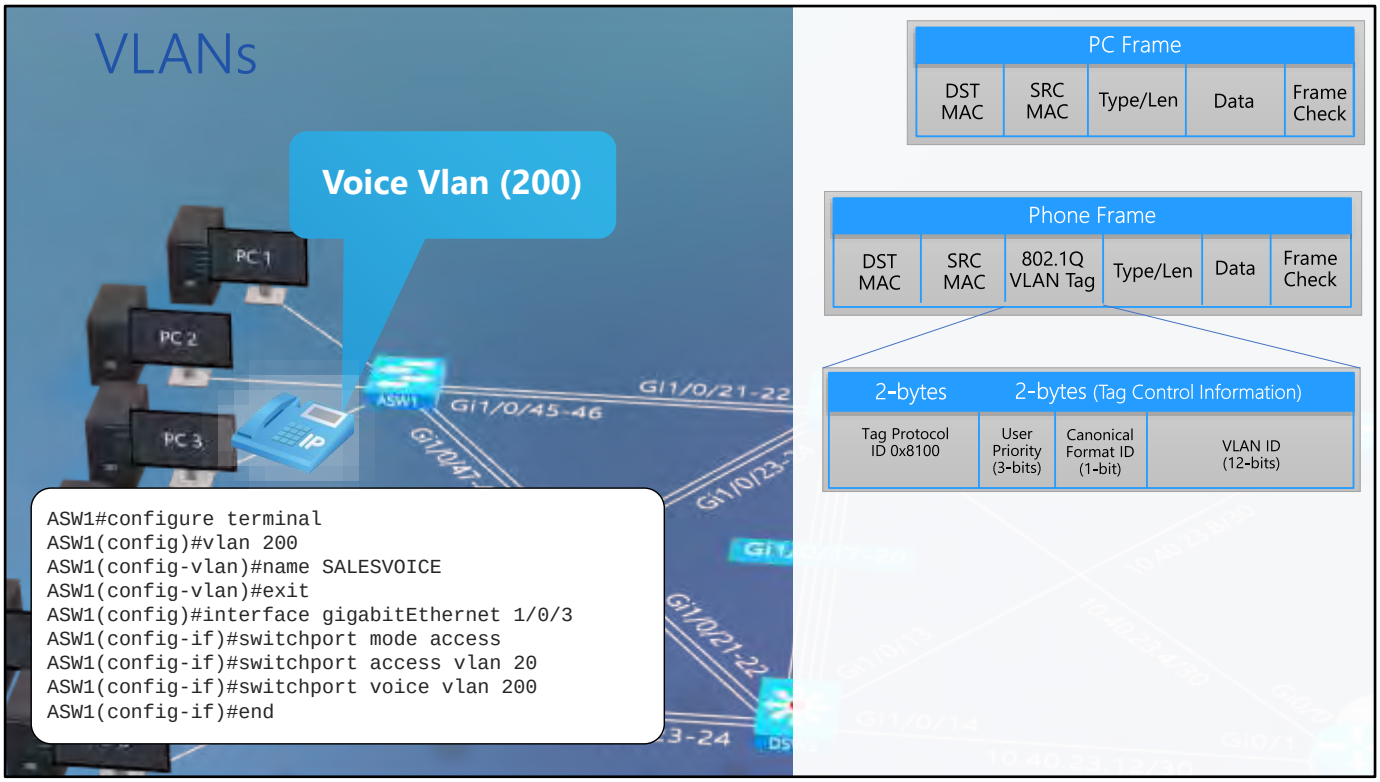
VLANs




```
ASW1#configure terminal
ASW1(config)#vlan 200
ASW1(config-vlan)#name SALESVOICE
ASW1(config-vlan)#exit
ASW1(config)#interface gigabitEthernet 1/0/3
ASW1(config-if)#switchport mode access
ASW1(config-if)#switchport access vlan 20
ASW1(config-if)#switchport voice vlan 200
ASW1(config-if)#end
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

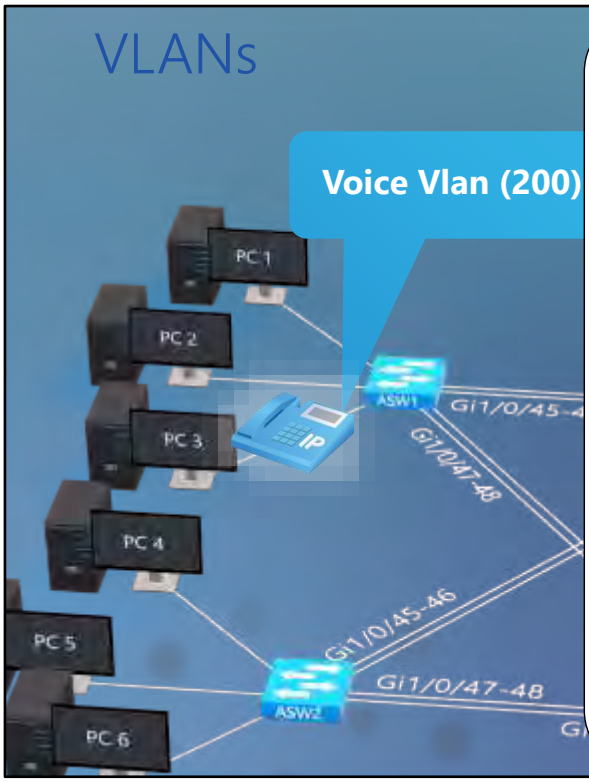
VLANs




```
ASW1#configure terminal
ASW1(config)#vlan 200
ASW1(config-vlan)#name SALESVOICE
ASW1(config-vlan)#exit
ASW1(config)#interface gigabitEthernet 1/0/3
ASW1(config-if)#switchport mode access
ASW1(config-if)#switchport access vlan 20
ASW1(config-if)#switchport voice vlan 200
ASW1(config-if)#end
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

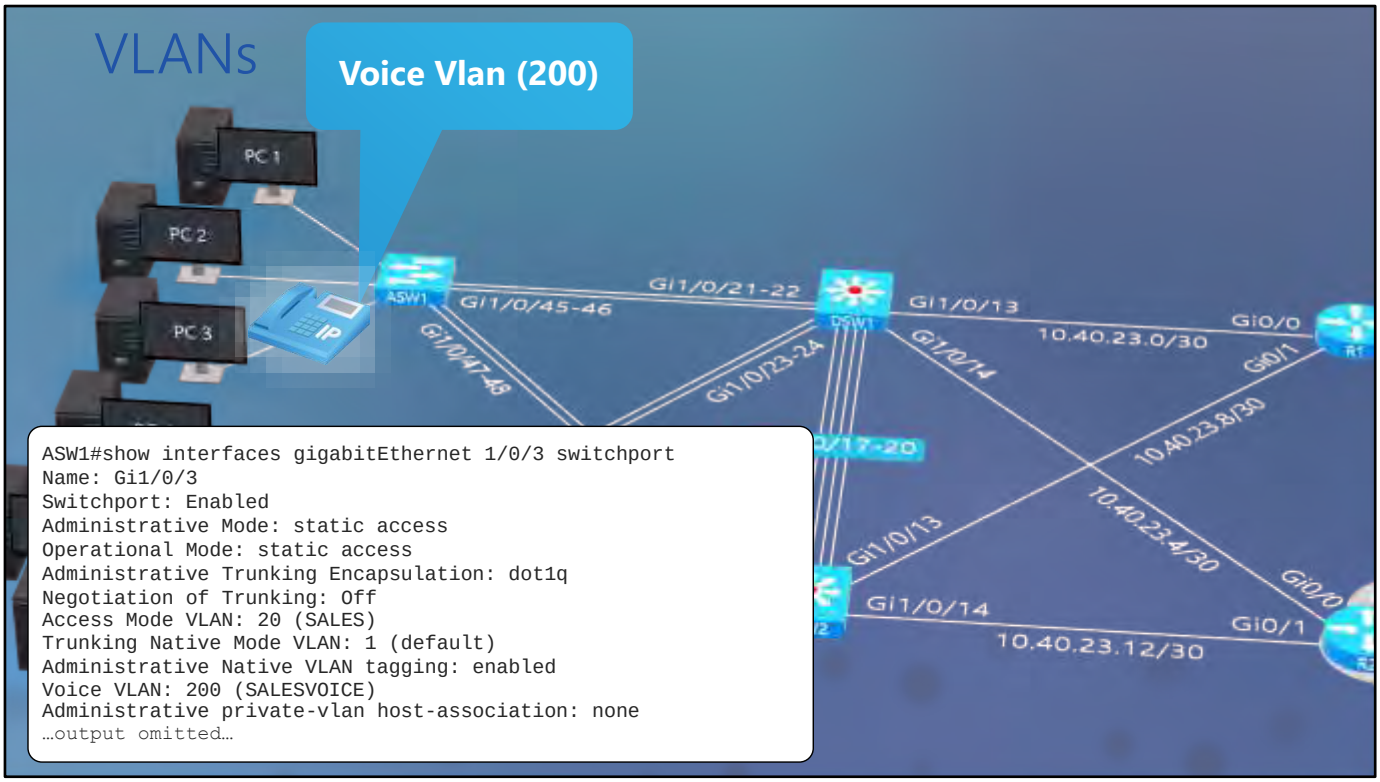
VLANs




```
ASW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28, Gi1/0/29, Gi1/0/30
                                                Gi1/0/31, Gi1/0/32, Gi1/0/33
                                                Gi1/0/34, Gi1/0/35, Gi1/0/36
                                                Gi1/0/37, Gi1/0/38, Gi1/0/39
                                                Gi1/0/40, Gi1/0/41, Gi1/0/42
                                                Gi1/0/43, Gi1/0/44, Gi1/0/45
                                                Gi1/0/46, Gi1/0/47, Gi1/0/48
                                                Gi1/0/49, Gi1/0/50, Gi1/0/51
                                                Gi1/0/52
10   FINANCE                          active    Gi1/0/1, Gi1/0/2
20   SALES                            active    Gi1/0/3
25   SERVER                           active
50   GUEST                            active
200  SALESVOICE                       active    Gi1/0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs




```
ASW1#show interfaces gigabitEthernet 1/0/3 switchport
Name: Gi1/0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (SALES)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 200 (SALESVOICE)
Administrative private-vlan host-association: none
…output omitted…
```

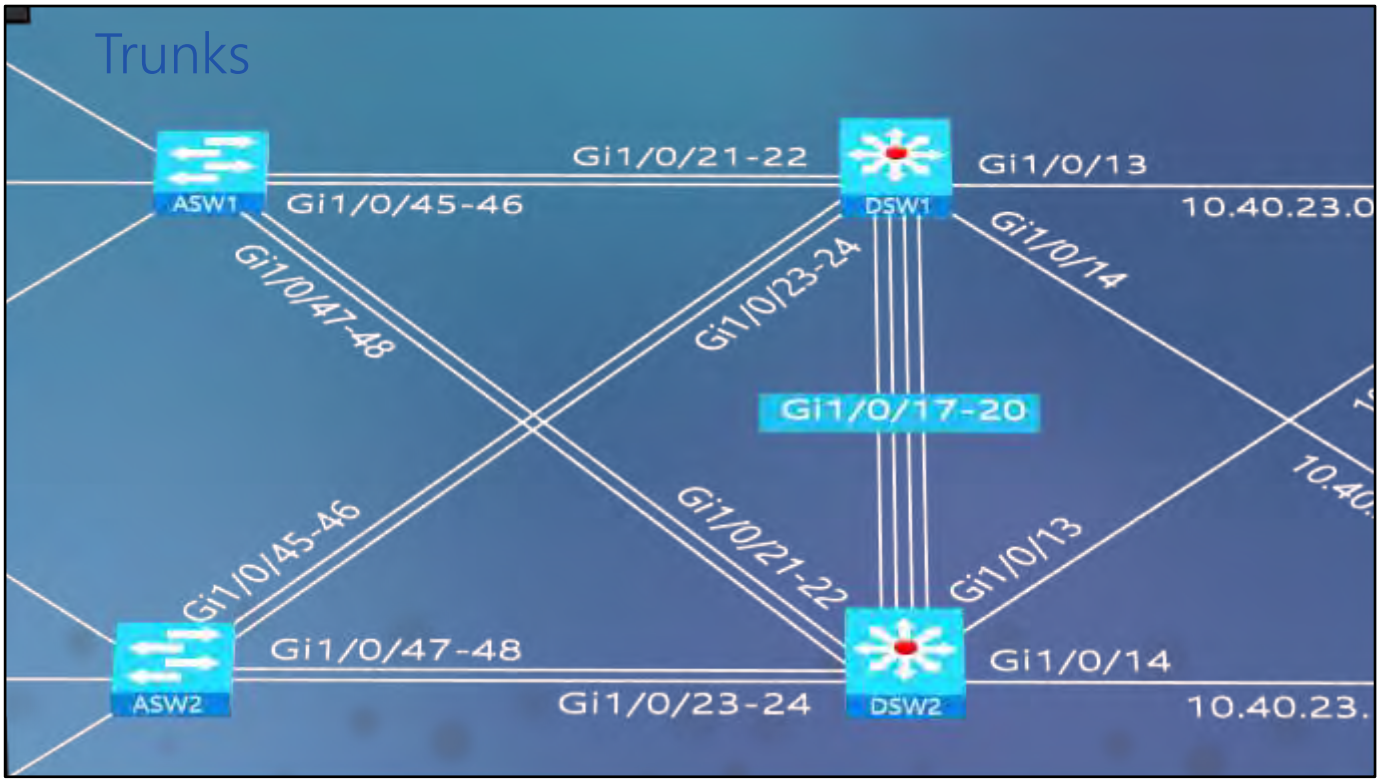
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring and Verifying Trunks

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



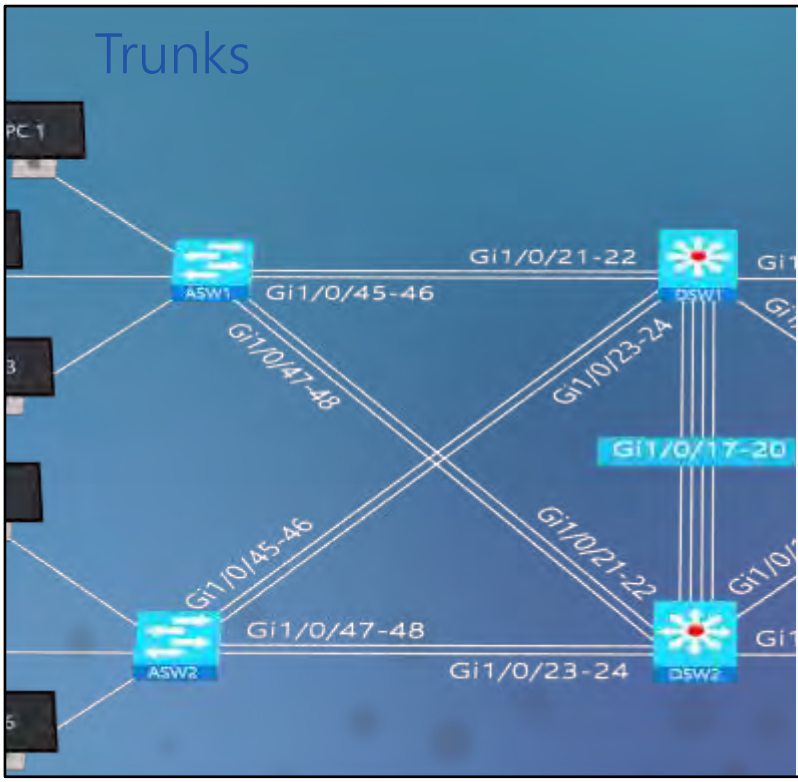
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trunks

```
ASW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
                                                Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28, Gi1/0/29, Gi1/0/30
                                                Gi1/0/31, Gi1/0/32, Gi1/0/33
                                                Gi1/0/34, Gi1/0/35, Gi1/0/36
                                                Gi1/0/37, Gi1/0/38, Gi1/0/39
                                                Gi1/0/40, Gi1/0/41, Gi1/0/42
                                                Gi1/0/43, Gi1/0/44, Gi1/0/45
                                                Gi1/0/46, Gi1/0/47, Gi1/0/48
                                                Gi1/0/49, Gi1/0/50, Gi1/0/51
                                                Gi1/0/52
10   FINANCE                          active    Gi1/0/1, Gi1/0/2
20   SALES                            active    Gi1/0/3
25   SERVER                           active
50   GUEST                            active
200  SALESVOICE                       active    Gi1/0/3
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trunks



What is a trunk?

A single physical link that can send and receive traffic for multiple VLANS.

A trunk can be formed:

- from a switch to a switch
- from a PC / Server to a switch
- from a switch to a router
- from an AP to a switch
- from a WLC to a switch

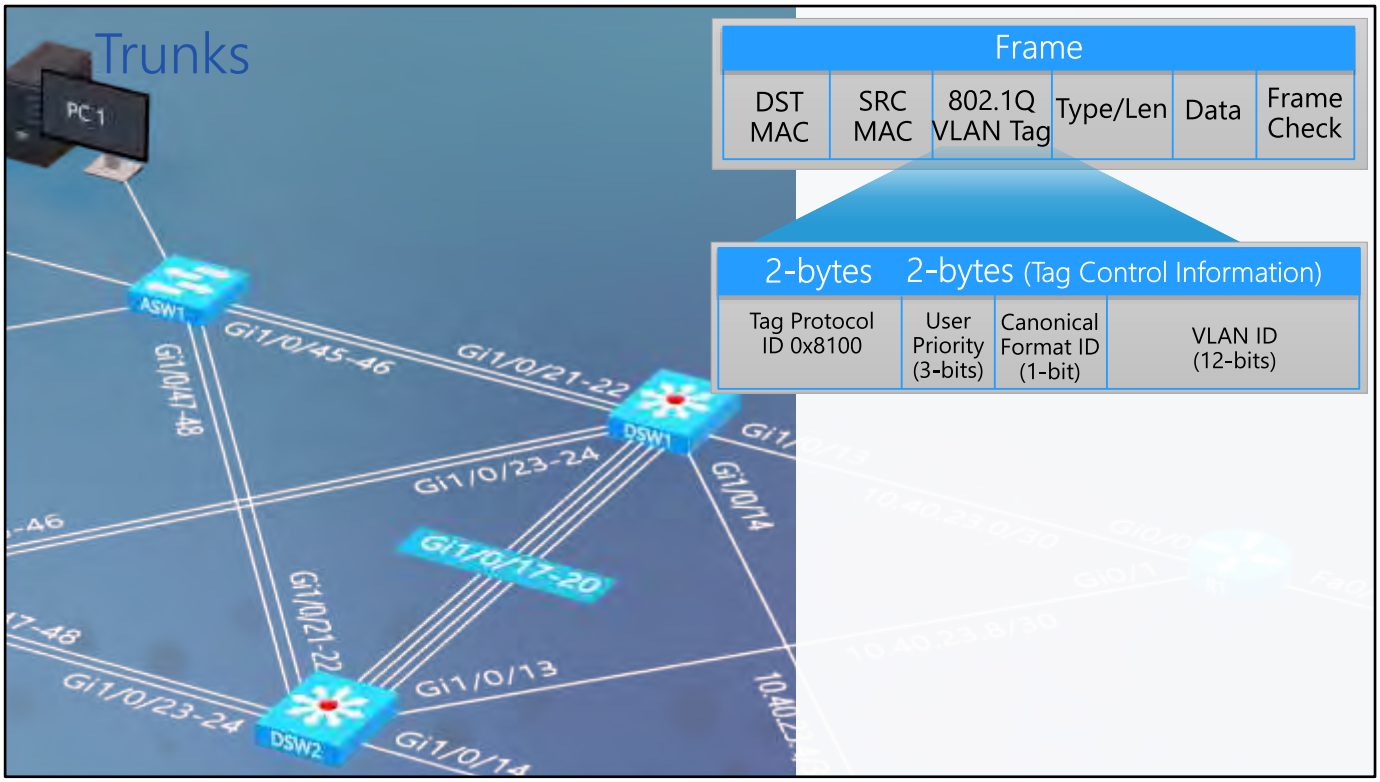
How is this done?

Configuring the port to be a trunk

Adding a tag to the frame that identifies the VLAN the frame belongs to

©2023 by StormWind LLC. All rights reserved.

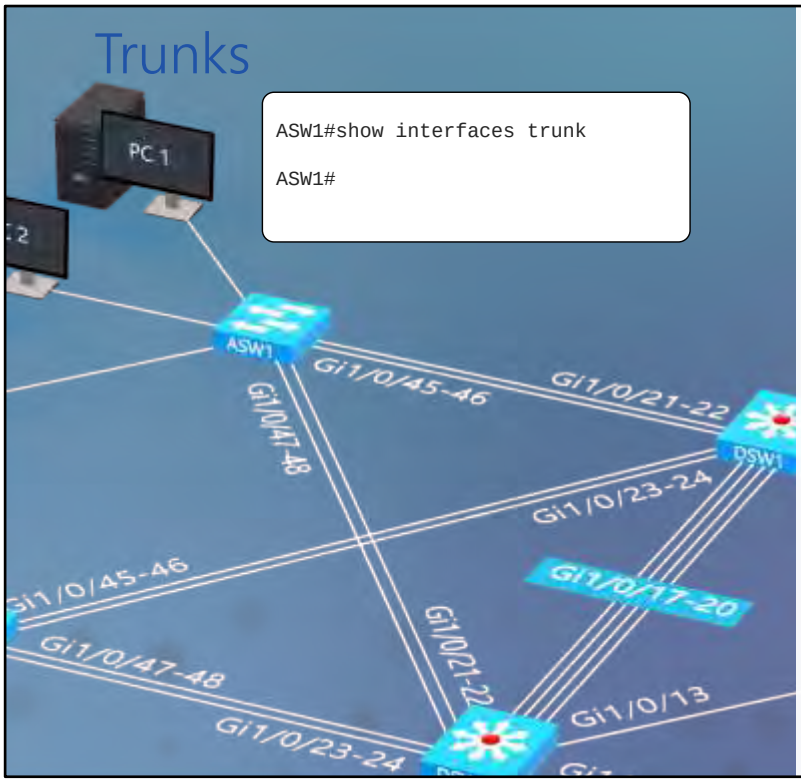
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

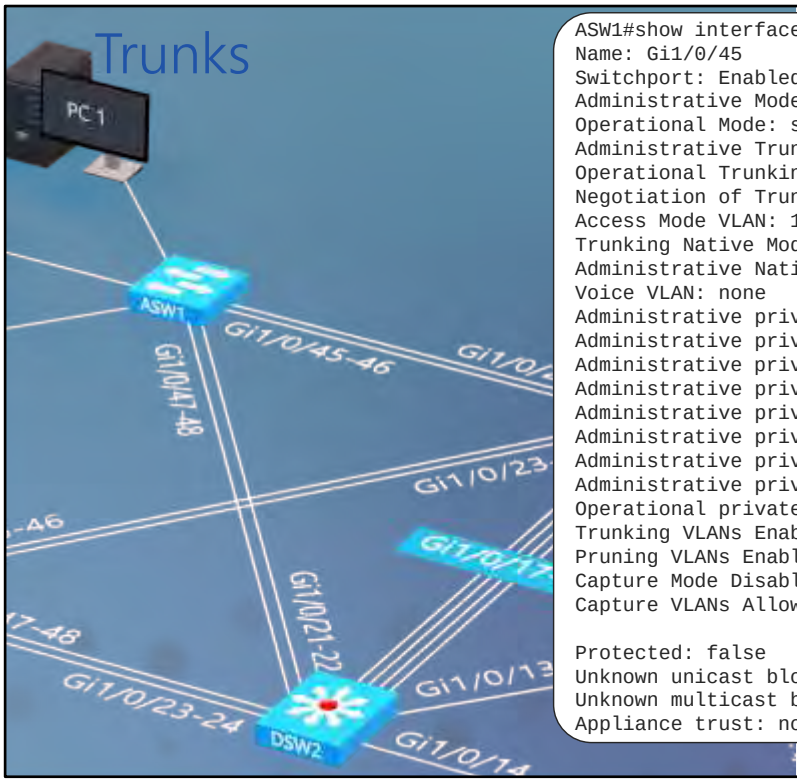
Trunks

```
ASW1#show interfaces trunk

ASW1#
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

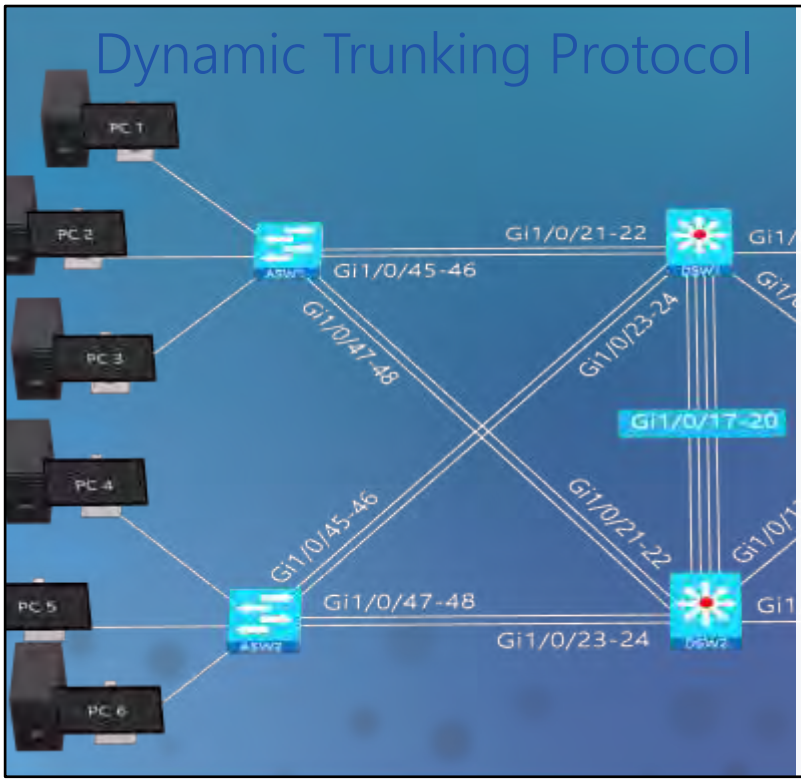
Trunks




```
ASW1#show interfaces gigabitEthernet 1/0/45 switchport
Name: Gi1/0/45
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Trunking Protocol



DTP allows for automatic trunk configuration

- Default modes vary on switch model

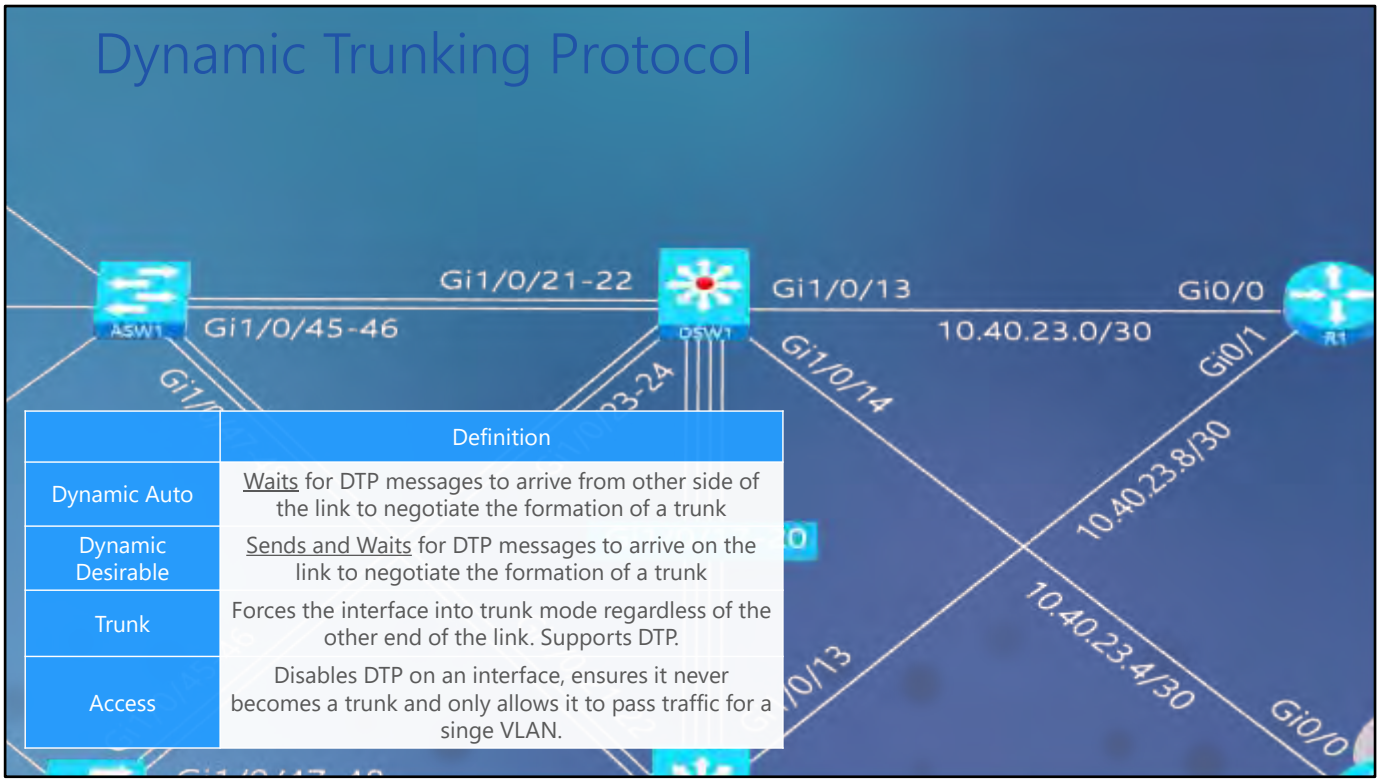
It is recommended to disable DTP and manually configure trunk links & manually configure all other links as access ports

The interface command `switchport nonegotiate` disables DTP

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

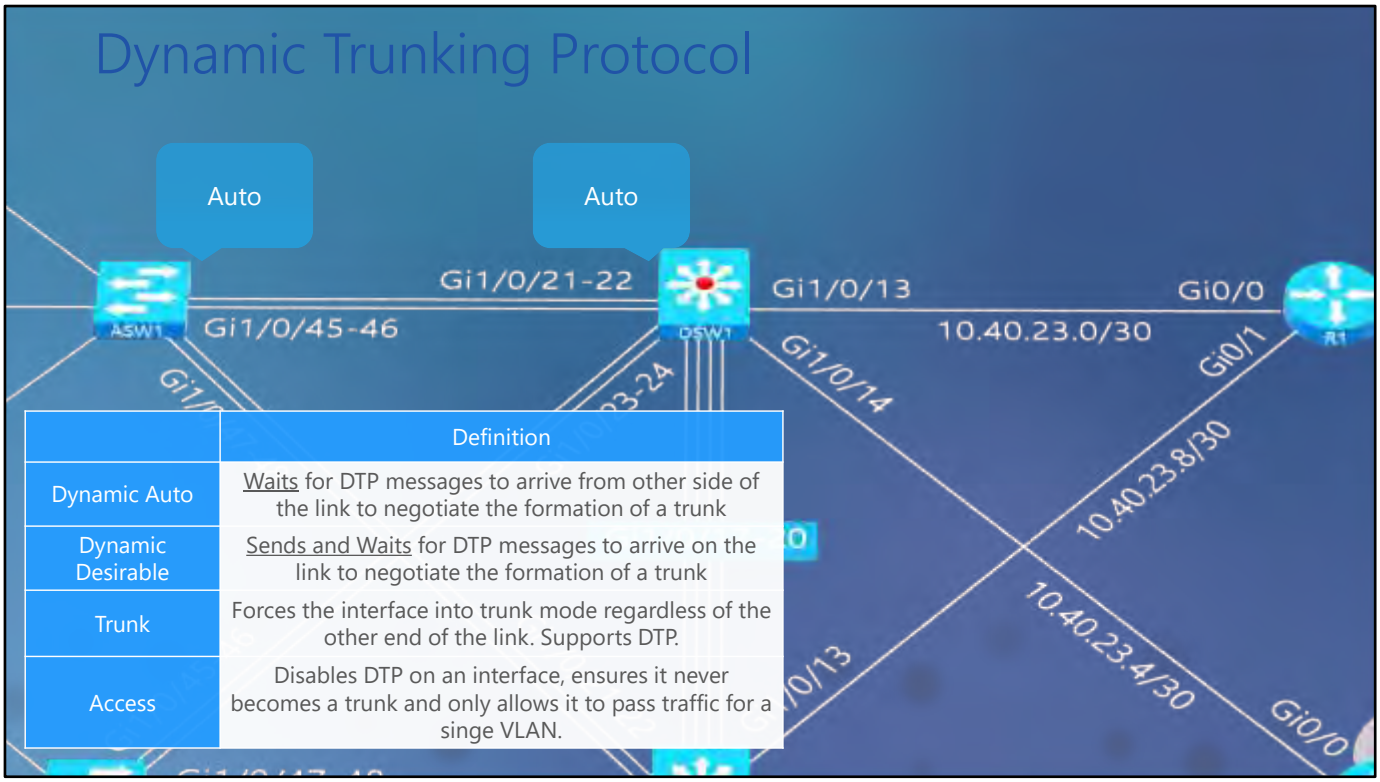
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

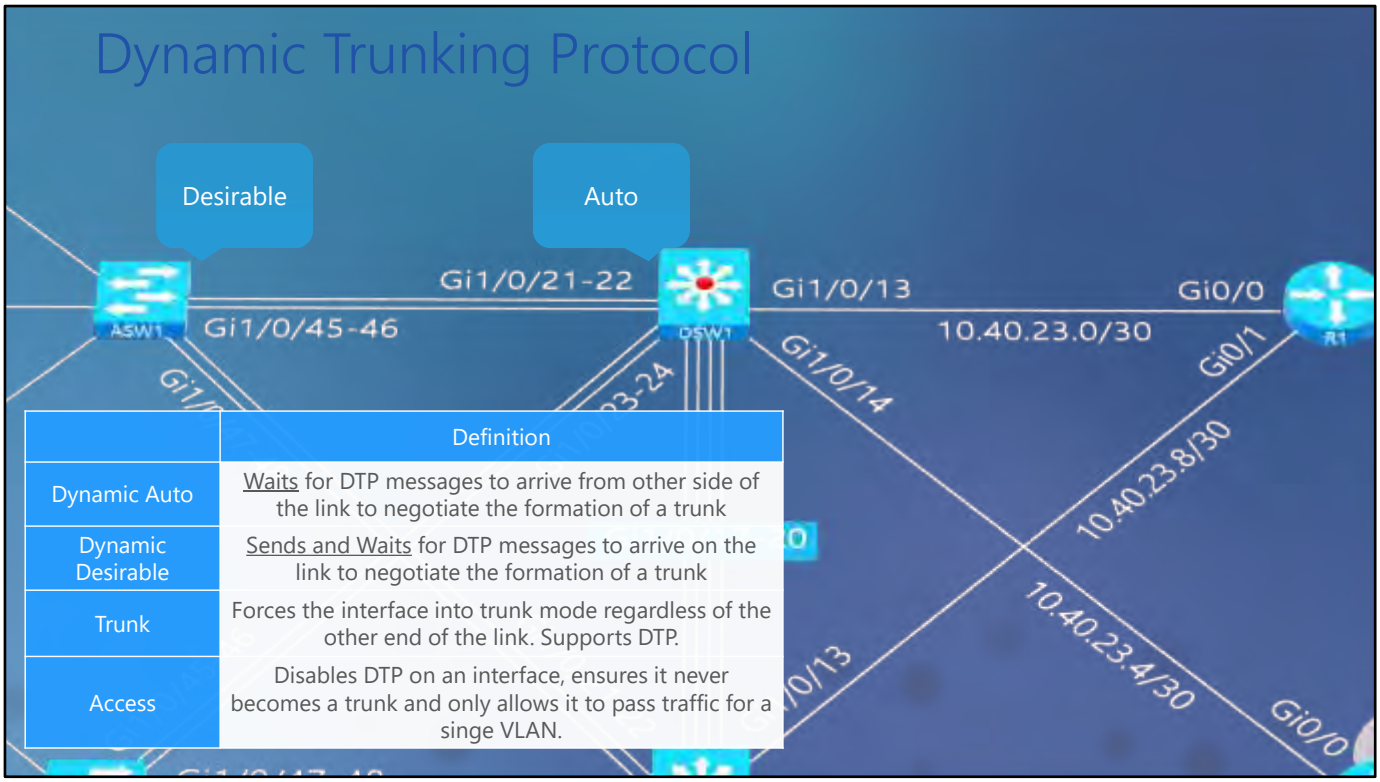
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

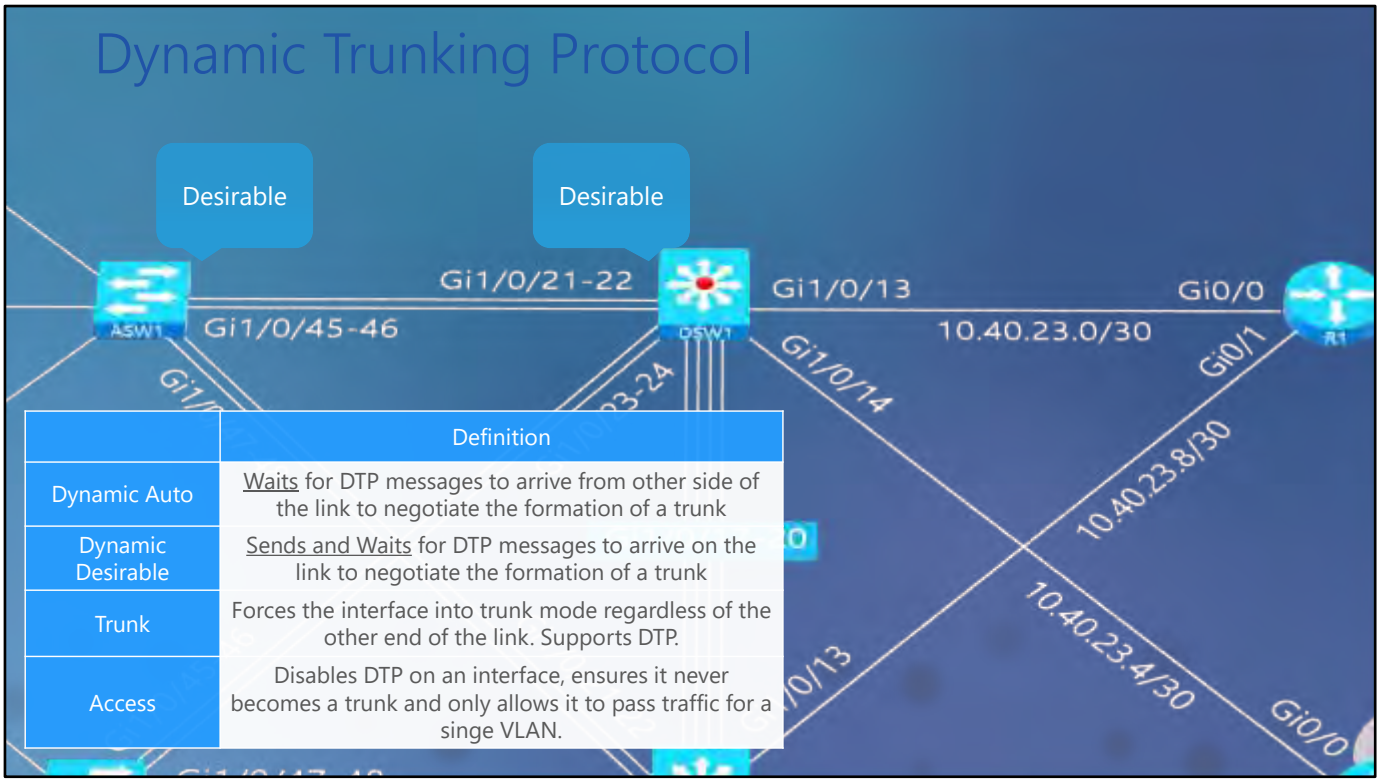
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

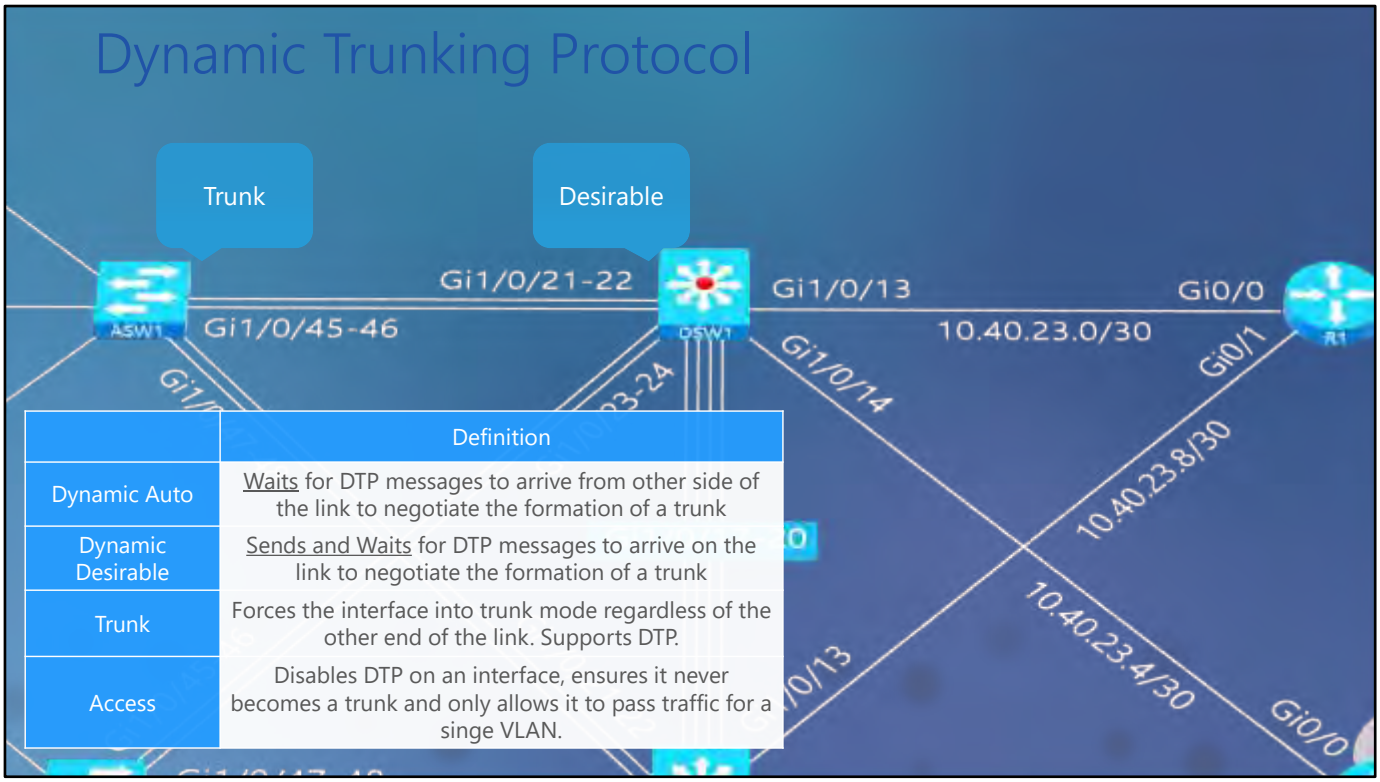
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

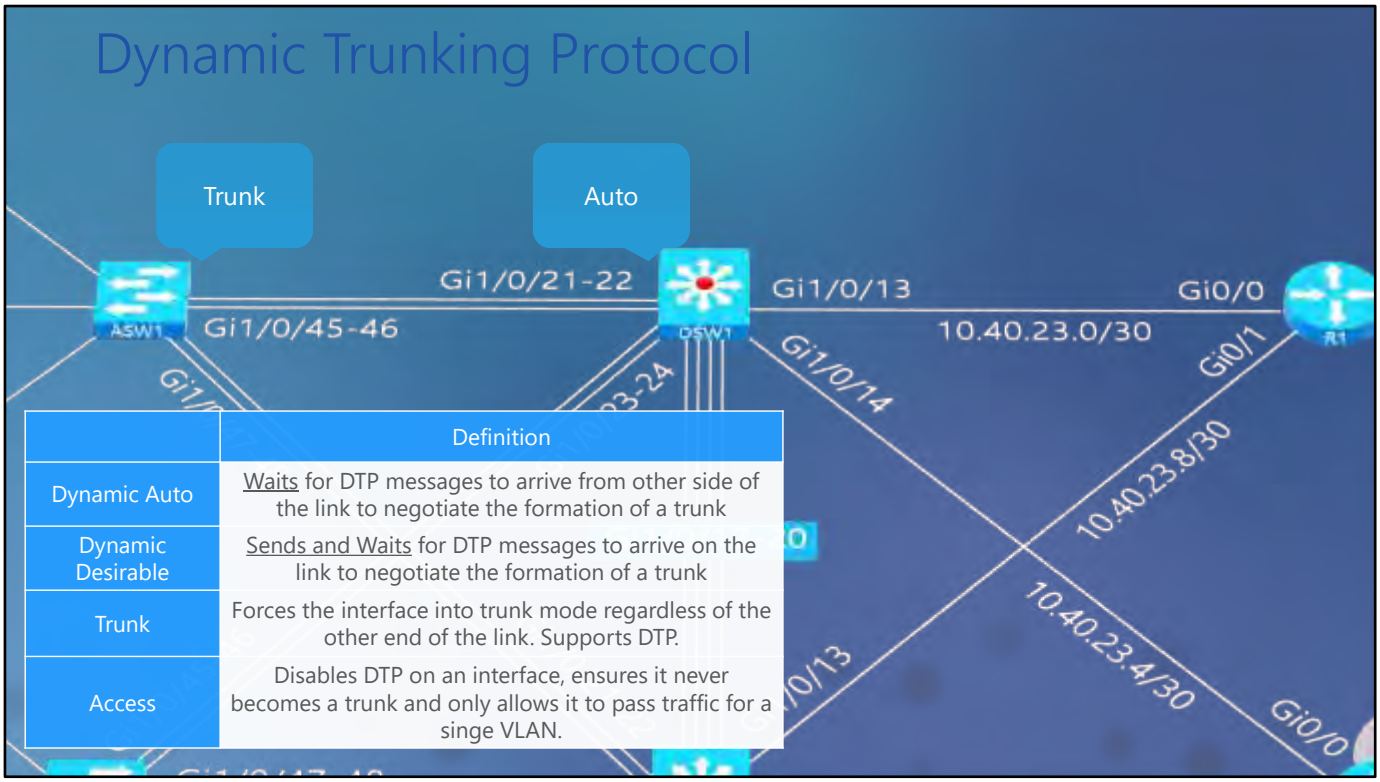
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

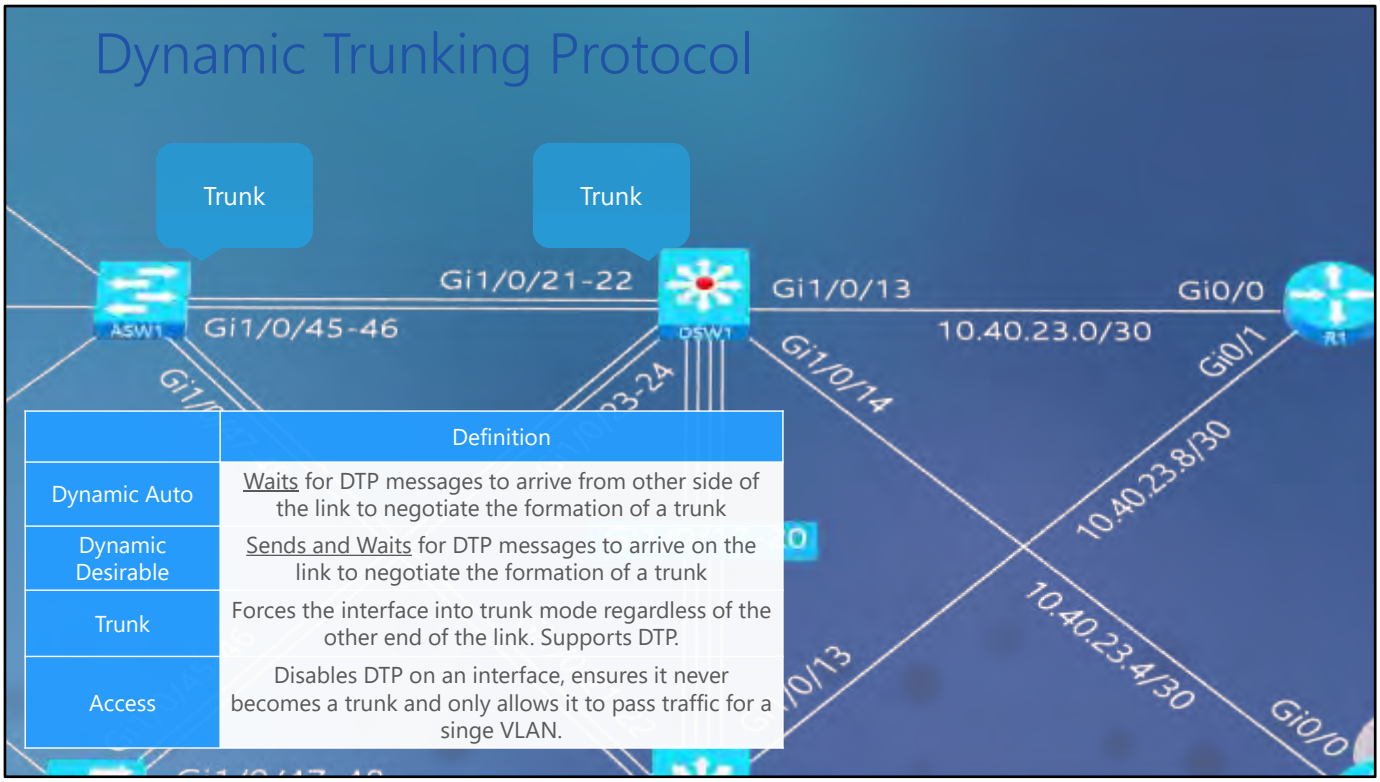
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

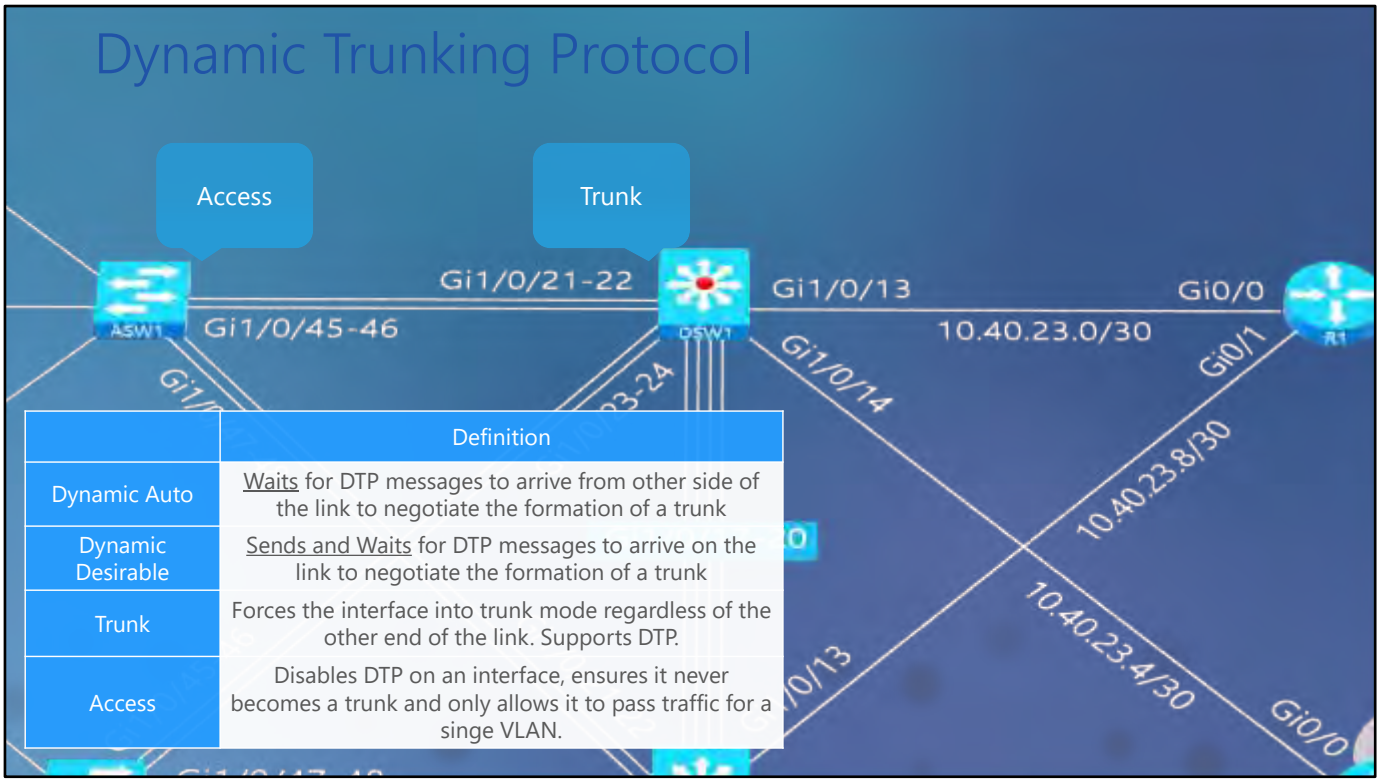
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

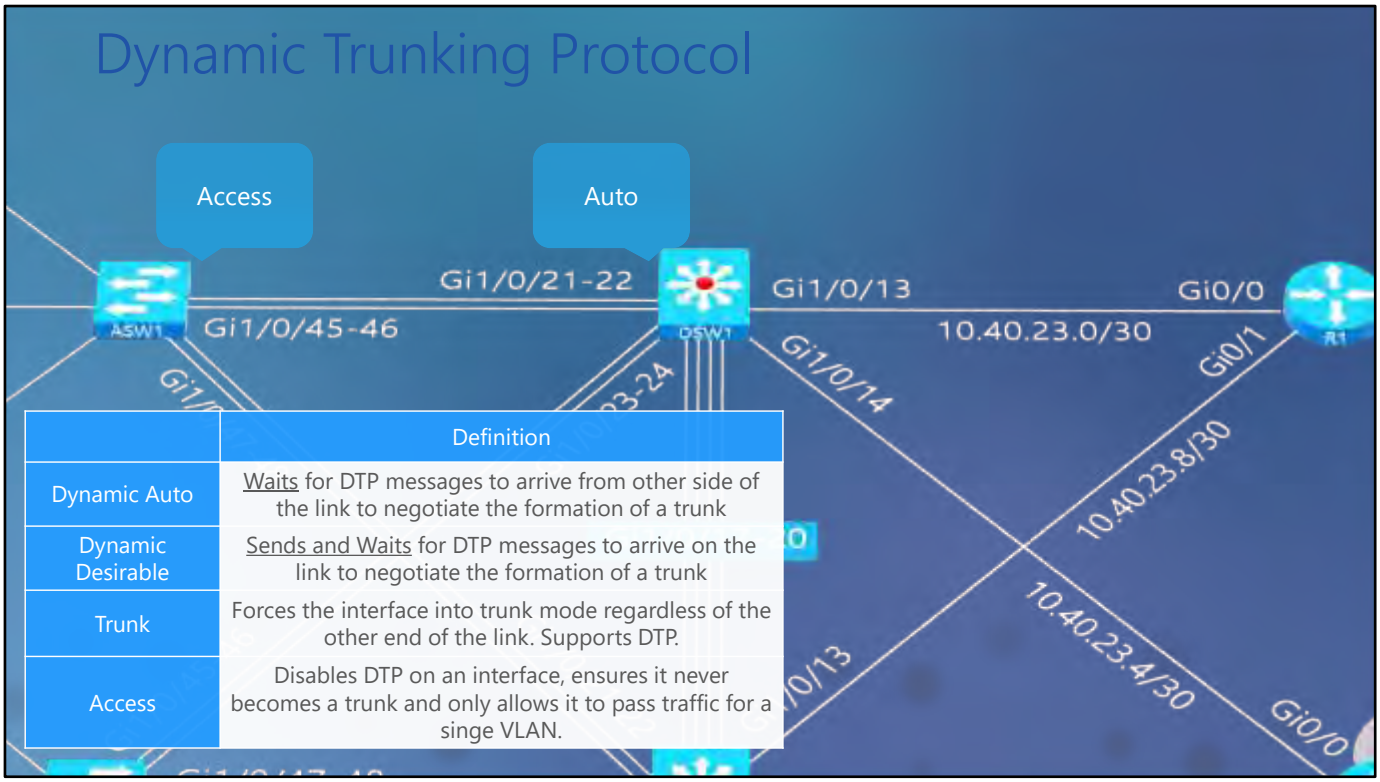
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

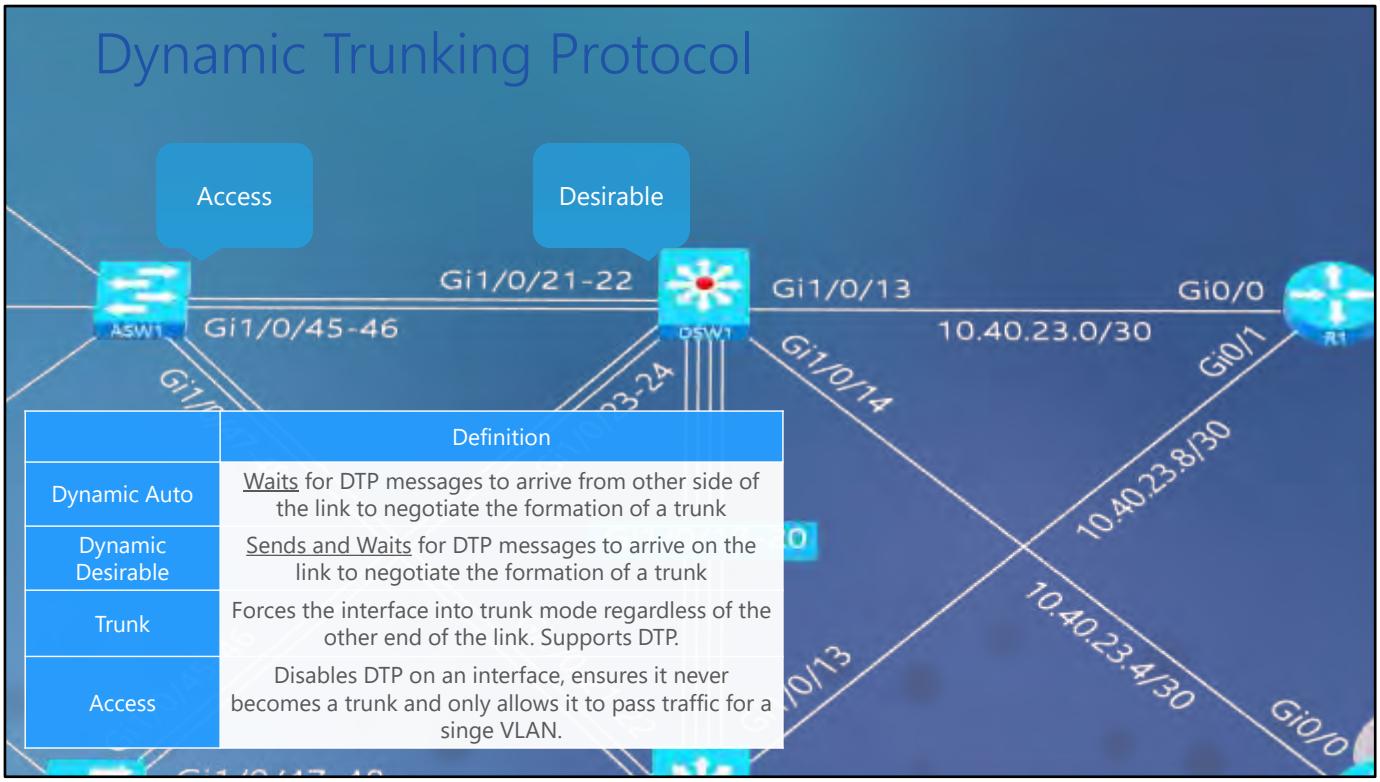
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

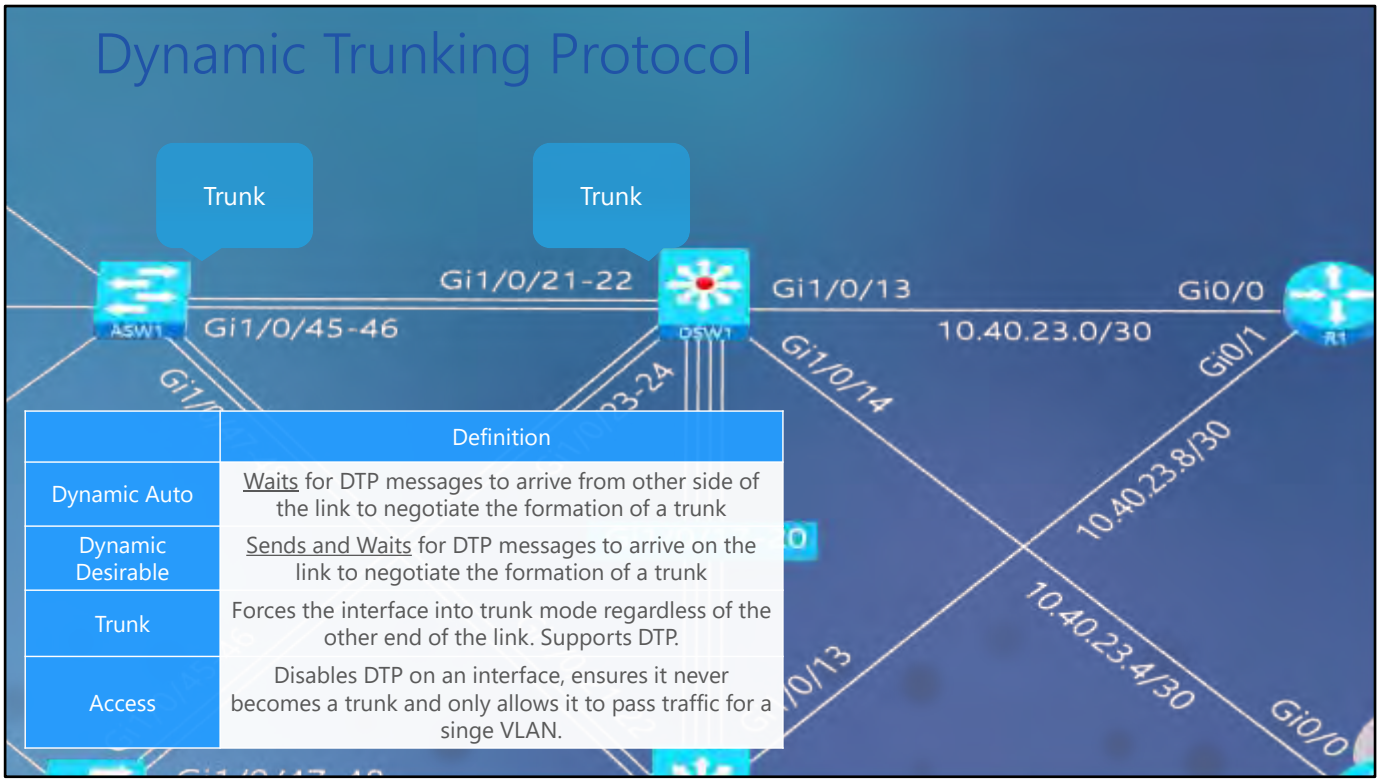
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

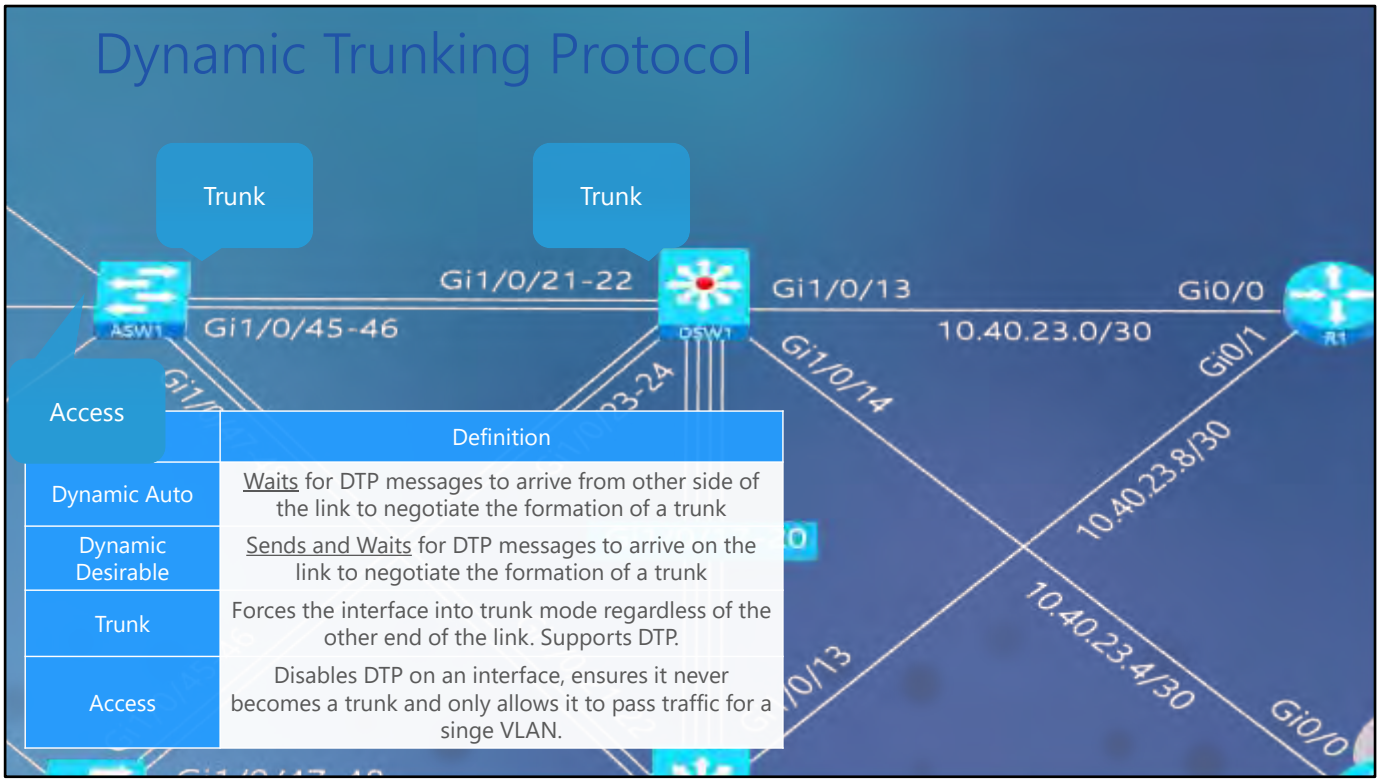
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

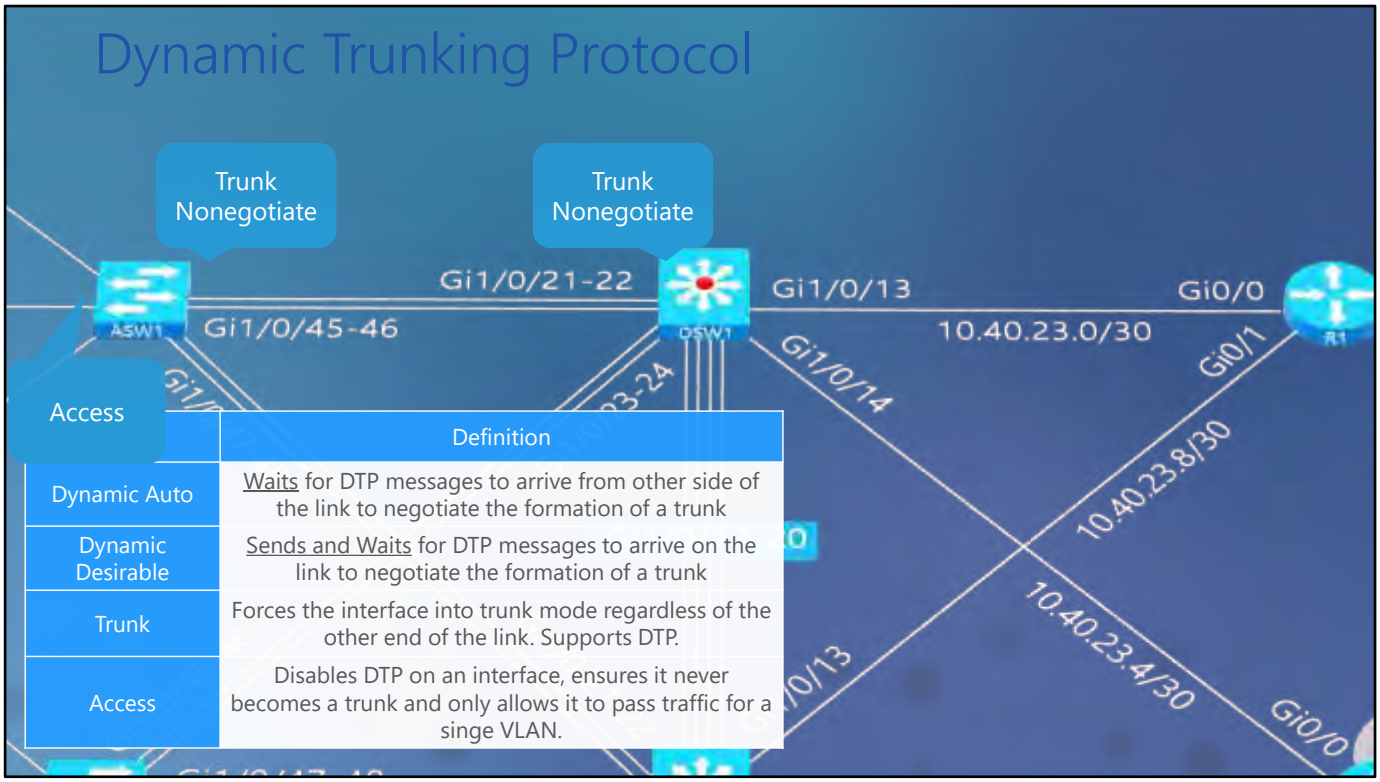
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

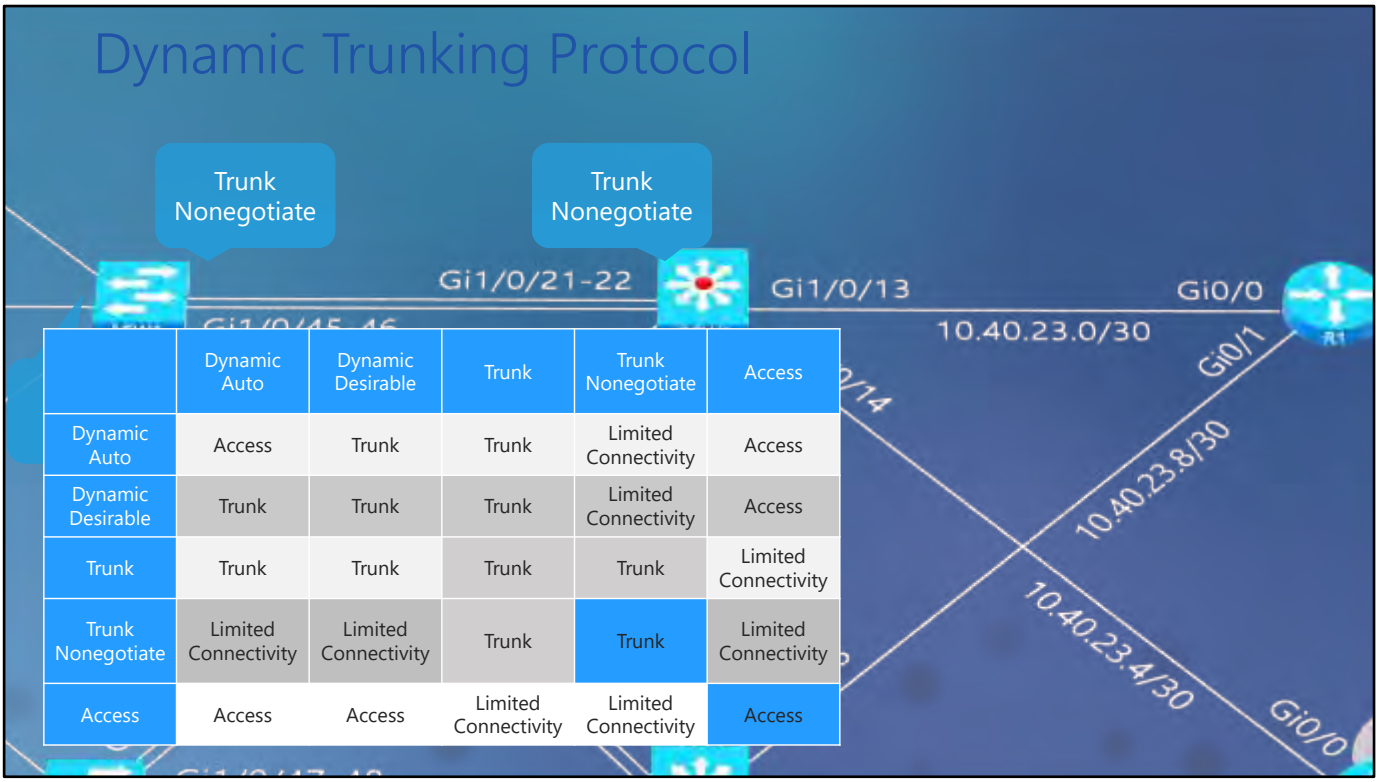
Dynamic Trunking Protocol



	Definition
Dynamic Auto	Waits for DTP messages to arrive from other side of the link to negotiate the formation of a trunk
Dynamic Desirable	Sends and Waits for DTP messages to arrive on the link to negotiate the formation of a trunk
Trunk	Forces the interface into trunk mode regardless of the other end of the link. Supports DTP.
Access	Disables DTP on an interface, ensures it never becomes a trunk and only allows it to pass traffic for a singe VLAN.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

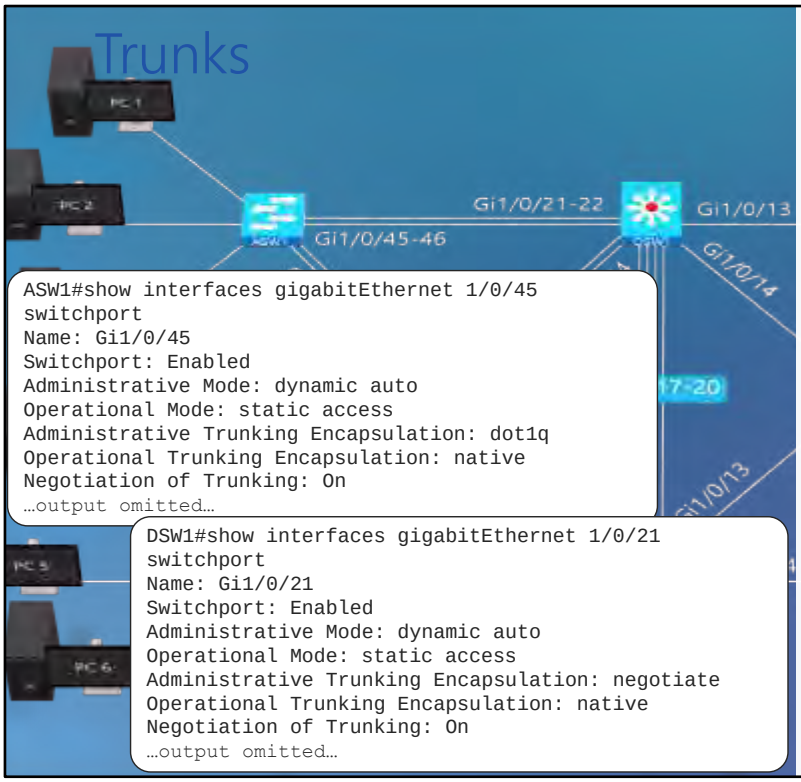
Dynamic Trunking Protocol



	Dynamic Auto	Dynamic Desirable	Trunk	Trunk Nonegotiate	Access
Dynamic Auto	Access	Trunk	Trunk	Limited Connectivity	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Limited Connectivity	Access
Trunk	Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Trunk Nonegotiate	Limited Connectivity	Limited Connectivity	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Limited Connectivity	Access

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trunks




```
ASW1#show interfaces gigabitEthernet 1/0/45
switchport
Name: Gi1/0/45
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
…output omitted…
```

```
DSW1#show interfaces gigabitEthernet 1/0/21
switchport
Name: Gi1/0/21
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trunks

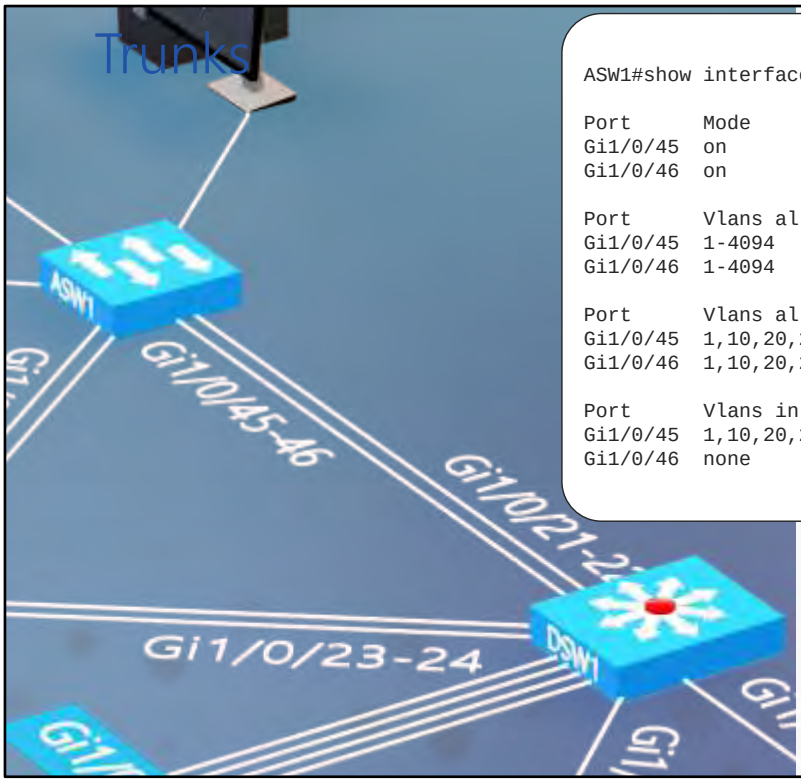
```
ASW1(config)#interface range gigabitEthernet 1/0/45-46
ASW1(config-if-range)#switchport mode trunk
ASW1(config-if-range)#switchport nonegotiate
ASW1(config-if-range)#end
```

```
DSW1#configure terminal
DSW1(config)#interface range gigabitEthernet 1/0/21-22
DSW1(config-if-range)#switchport trunk encapsulation dot1q*
DSW1(config-if-range)#switchport mode trunk
DSW1(config-if-range)#switchport nonegotiate
DSW1(config-if-range)#end
```

* - depends on switch platform and IOS version

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

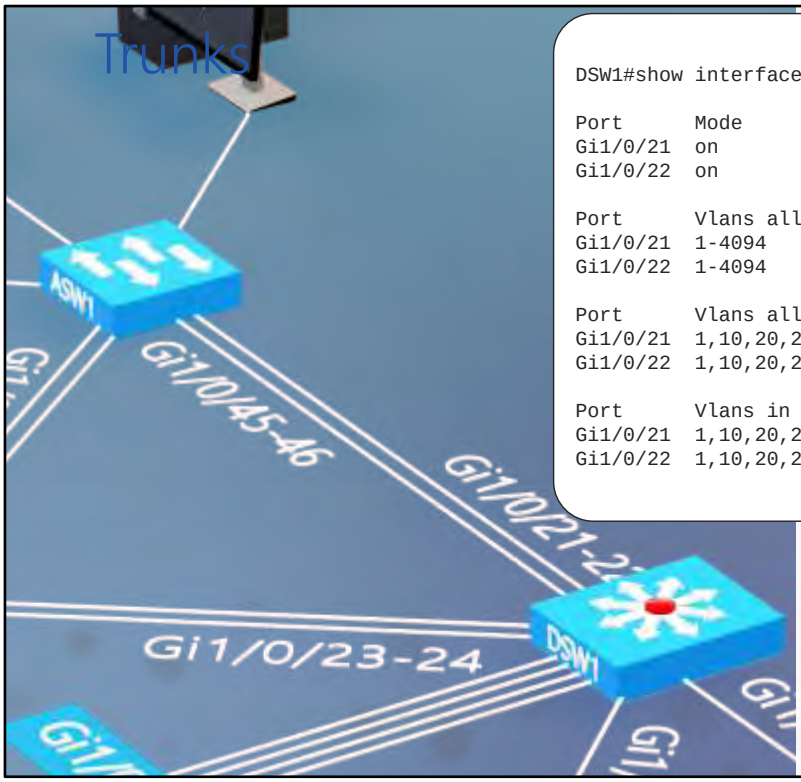
Trunks




```
ASW1#show interfaces trunk

Port      Mode             Encapsulation  Status     Native vlan
Gi1/0/45  on               802.1q         trunking   1
Gi1/0/46  on               802.1q         trunking   1

Port      Vlans allowed on trunk
Gi1/0/45  1-4094
Gi1/0/46  1-4094

Port      Vlans allowed and active in management domain
Gi1/0/45  1,10,20,25,50
Gi1/0/46  1,10,20,25,50

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/45  1,10,20,25,50
Gi1/0/46  none
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

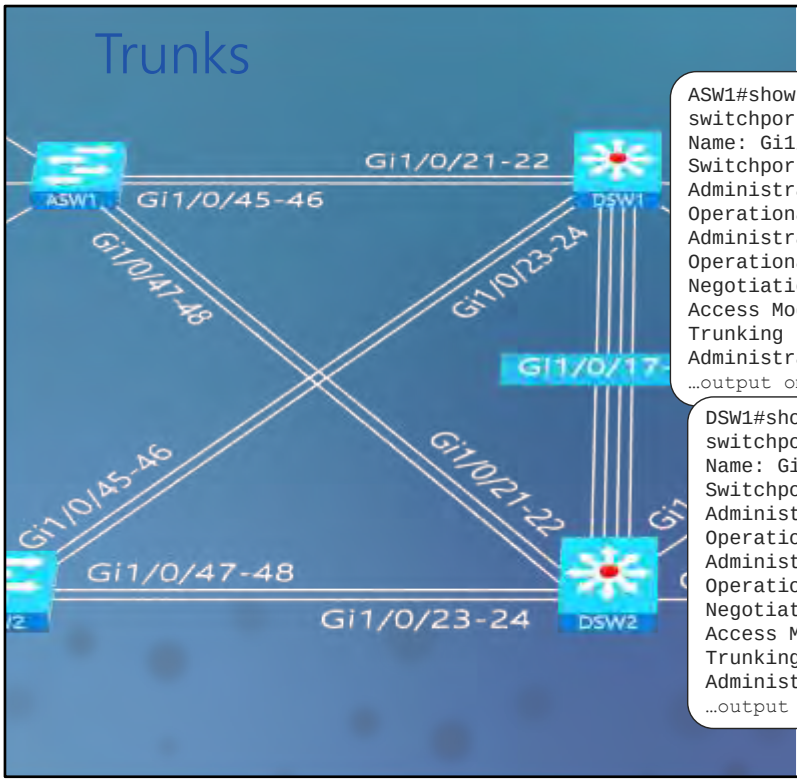
Trunks




```
DSW1#show interfaces trunk

Port      Mode             Encapsulation  Status    Native vlan
Gi1/0/21  on               802.1q         trunking  1
Gi1/0/22  on               802.1q         trunking  1

Port      Vlans allowed on trunk
Gi1/0/21  1-4094
Gi1/0/22  1-4094

Port      Vlans allowed and active in management domain
Gi1/0/21  1,10,20,25,50
Gi1/0/22  1,10,20,25,50

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/21  1,10,20,25,50
Gi1/0/22  1,10,20,25,50
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trunks

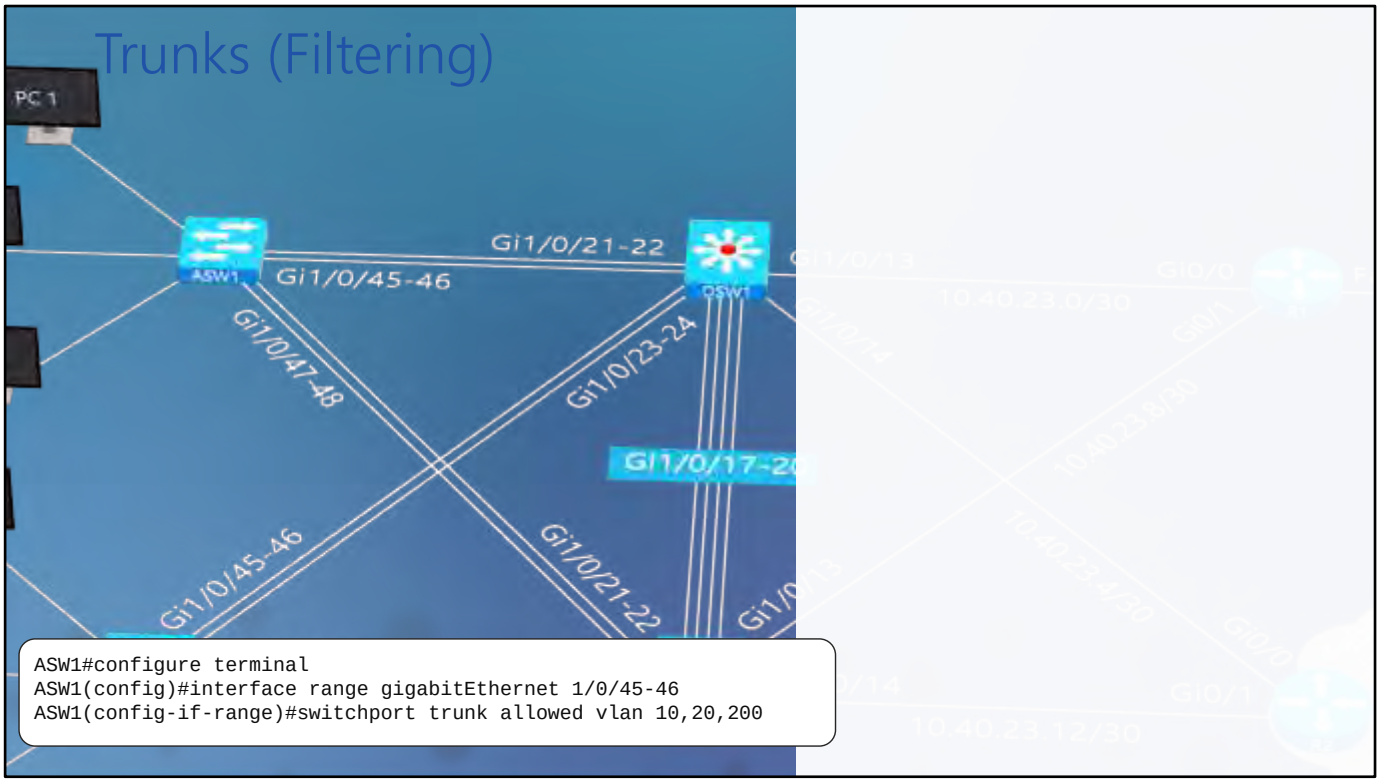



```
ASW1#show interfaces gigabitEthernet 1/0/45
switchport
Name: Gi1/0/45
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
…output omitted…
```

```
DSW1#show interfaces gigabitEthernet 1/0/21
switchport
Name: Gi1/0/21
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

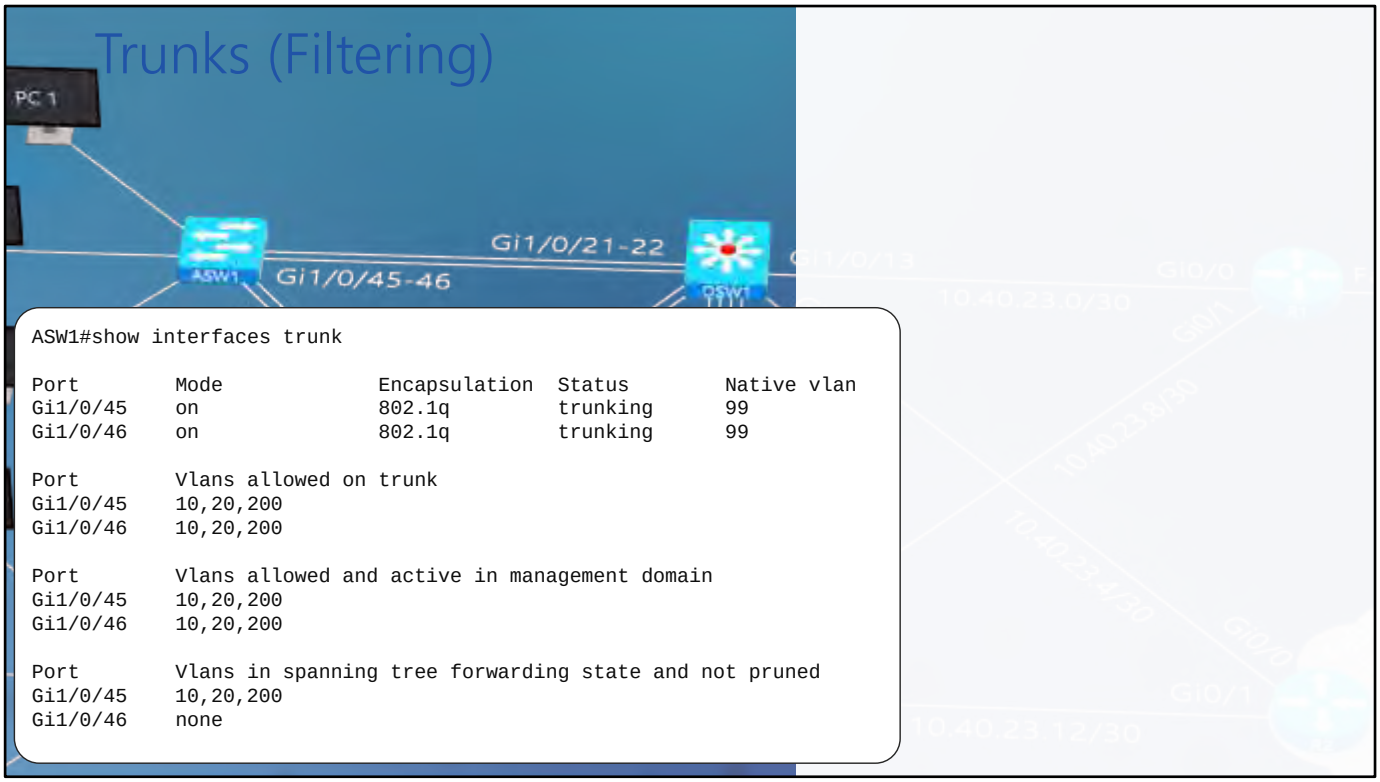
Trunks (Filtering)




```
ASW1#configure terminal
ASW1(config)#interface range gigabitEthernet 1/0/45-46
ASW1(config-if-range)#switchport trunk allowed vlan 10,20,200
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

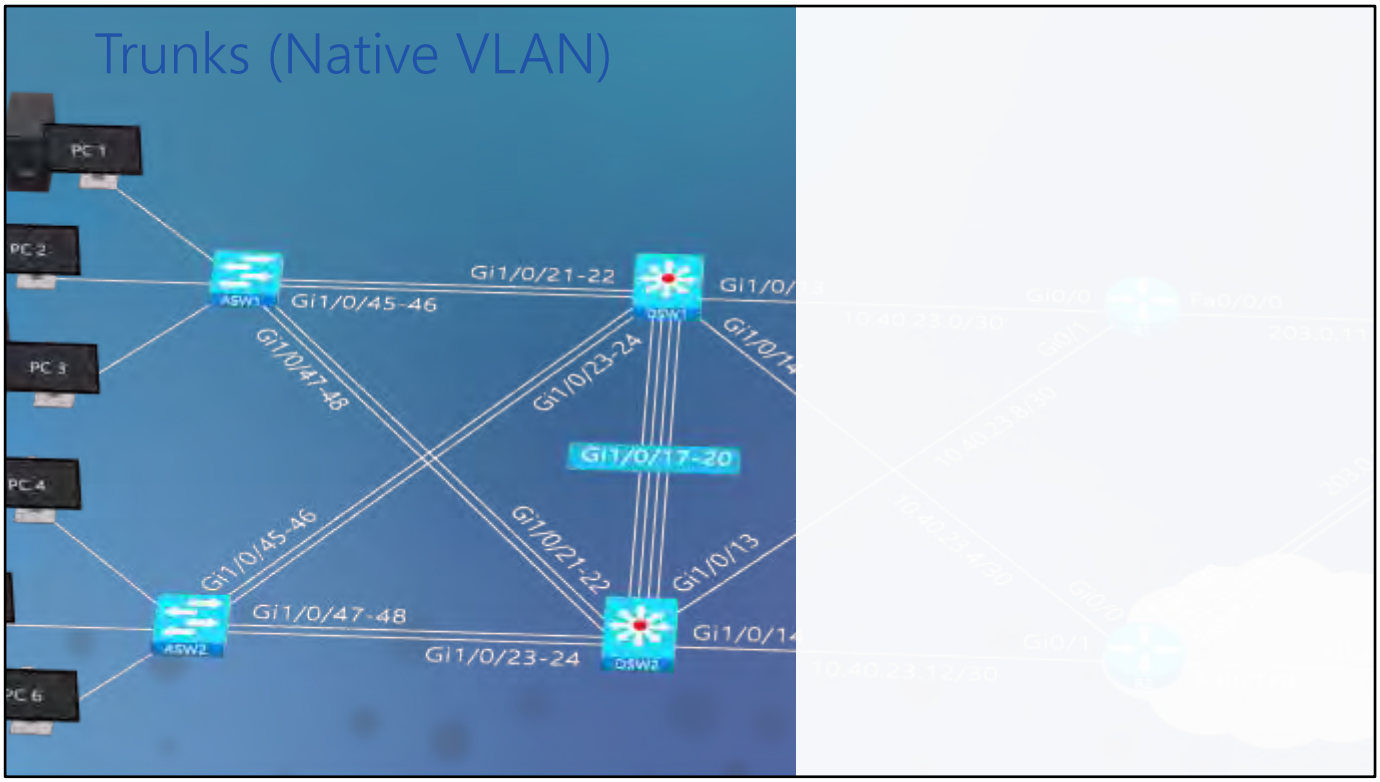
Trunks (Filtering)




```
ASW1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/45    on               802.1q         trunking      99
Gi1/0/46    on               802.1q         trunking      99

Port        Vlans allowed on trunk
Gi1/0/45    10,20,200
Gi1/0/46    10,20,200

Port        Vlans allowed and active in management domain
Gi1/0/45    10,20,200
Gi1/0/46    10,20,200

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/45    10,20,200
Gi1/0/46    none
```

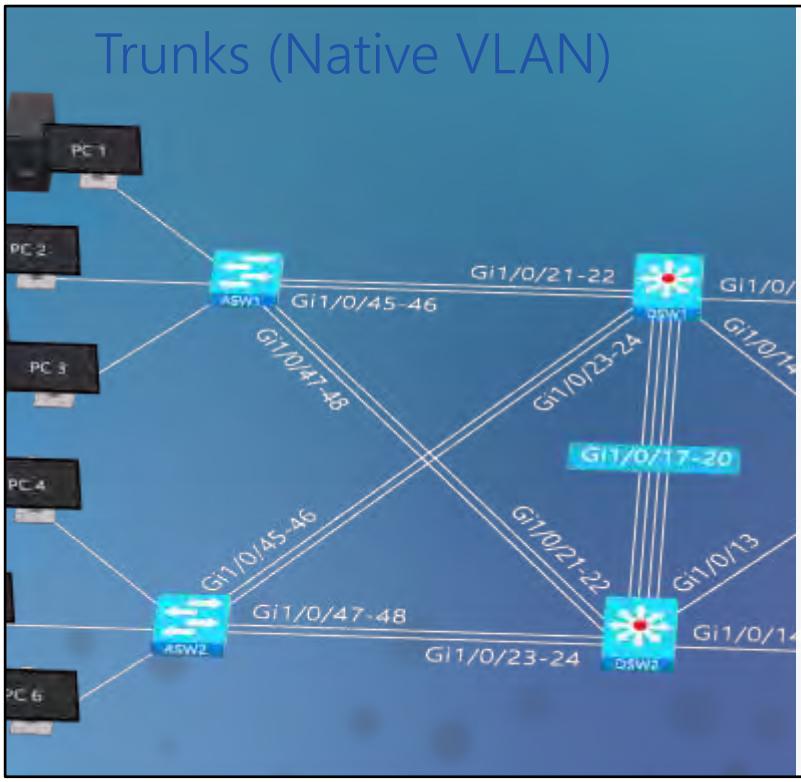
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trunks (Native VLAN)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

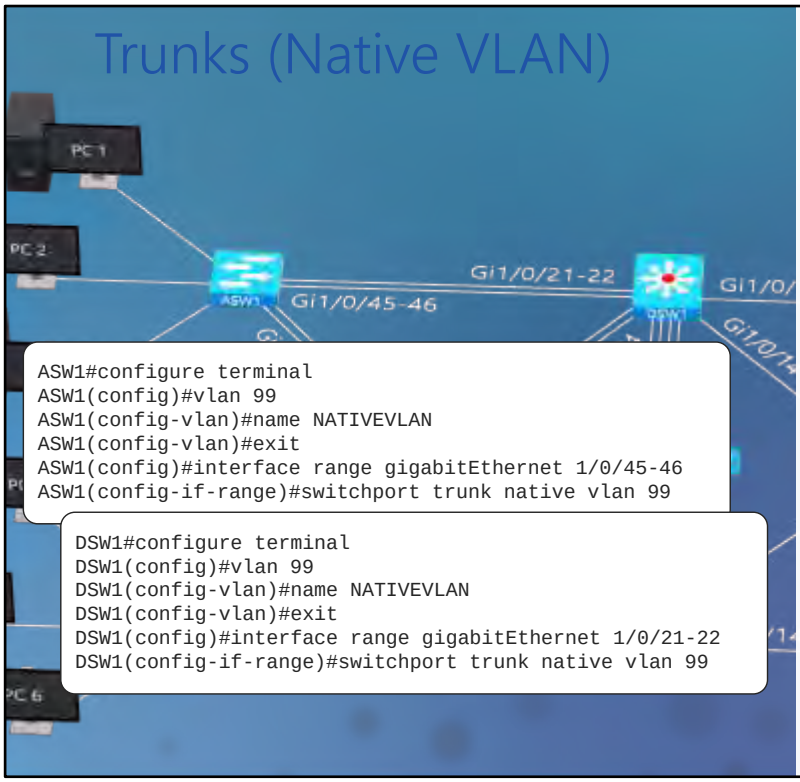
Trunks (Native VLAN)



- Native VLAN frames are carried over the trunk untagged
  - The default native VLAN is VLAN 1
- Native VLAN must match on both ends of the trunk
  - A native VLAN mismatch will merge traffic between VLANs
- Change the Native VLAN to a VLAN you are not using.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trunks (Native VLAN)

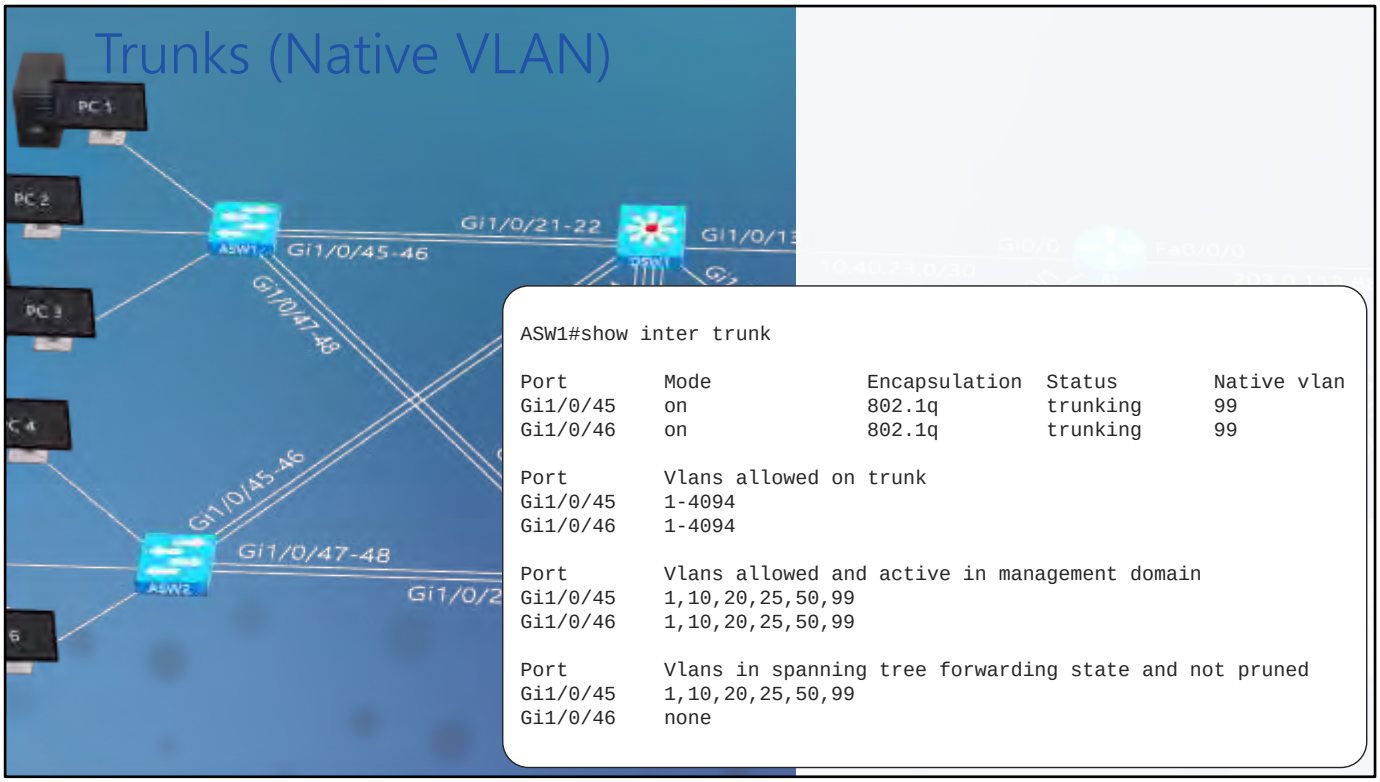



```
ASW1#configure terminal
ASW1(config)#vlan 99
ASW1(config-vlan)#name NATIVEVLAN
ASW1(config-vlan)#exit
ASW1(config)#interface range gigabitEthernet 1/0/45-46
ASW1(config-if-range)#switchport trunk native vlan 99
```

```
DSW1#configure terminal
DSW1(config)#vlan 99
DSW1(config-vlan)#name NATIVEVLAN
DSW1(config-vlan)#exit
DSW1(config)#interface range gigabitEthernet 1/0/21-22
DSW1(config-if-range)#switchport trunk native vlan 99
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

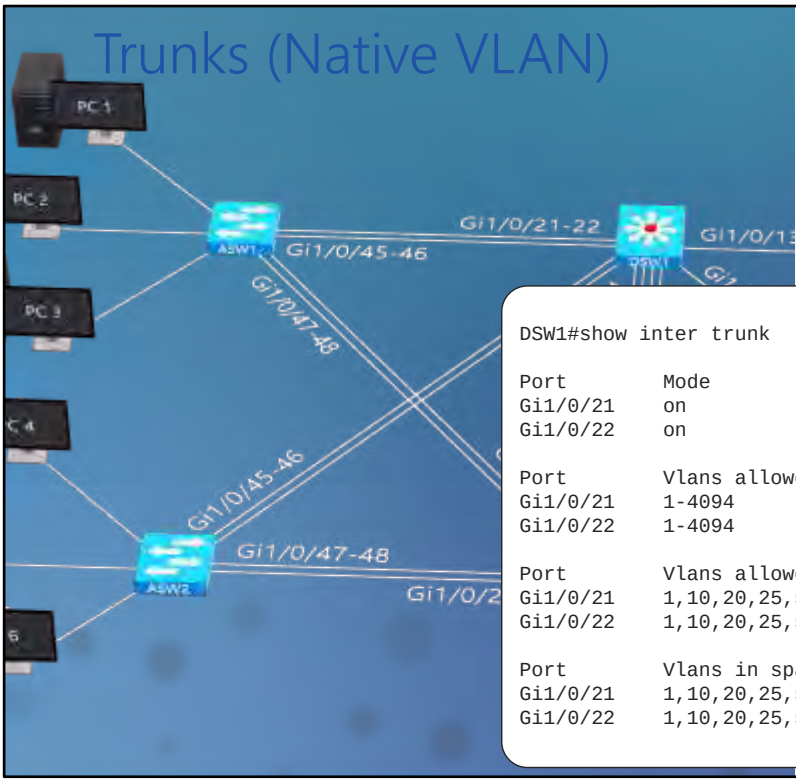
Trunks (Native VLAN)




```
ASW1#show inter trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/45    on               802.1q         trunking      99
Gi1/0/46    on               802.1q         trunking      99

Port        Vlans allowed on trunk
Gi1/0/45    1-4094
Gi1/0/46    1-4094

Port        Vlans allowed and active in management domain
Gi1/0/45    1,10,20,25,50,99
Gi1/0/46    1,10,20,25,50,99

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/45    1,10,20,25,50,99
Gi1/0/46    none
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trunks (Native VLAN)

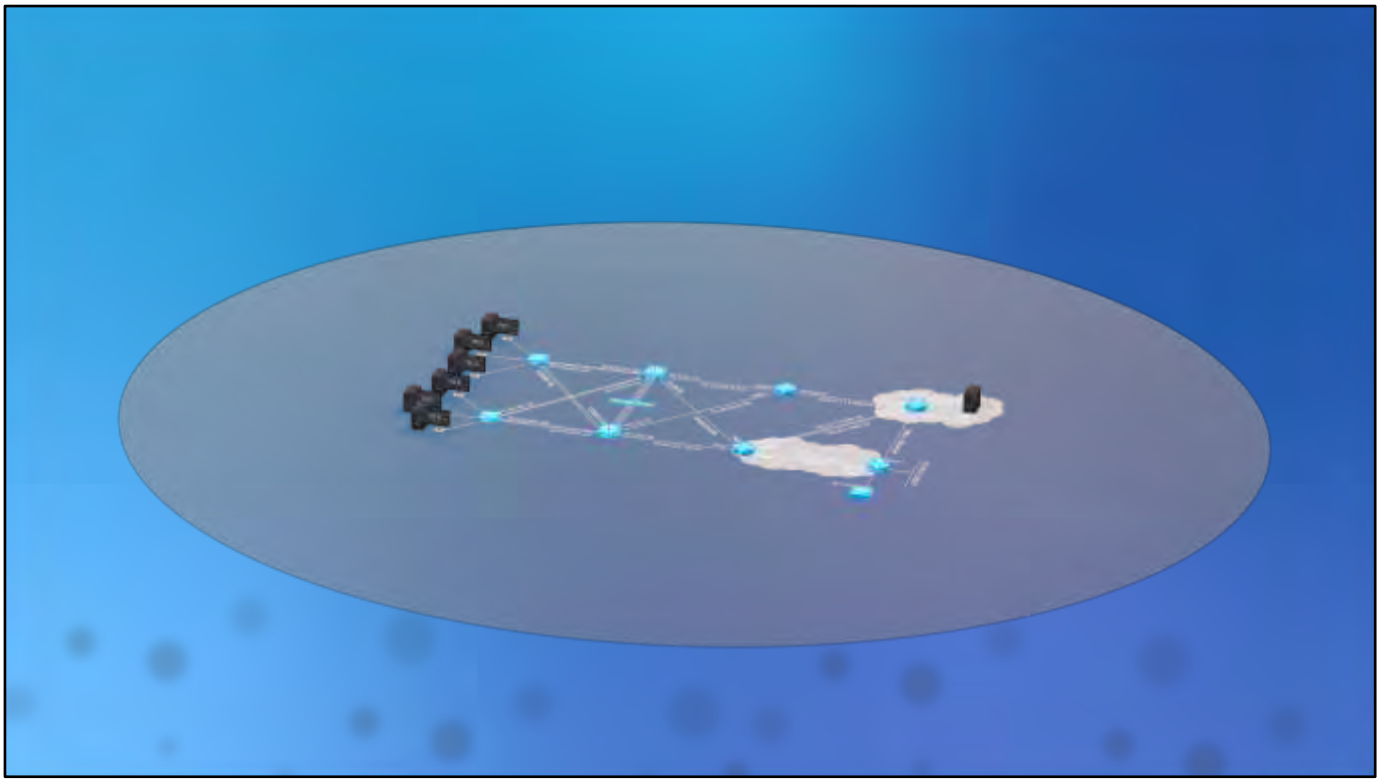



```
DSW1#show inter trunk

Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/21    on               802.1q         trunking      99
Gi1/0/22    on               802.1q         trunking      99

Port        Vlans allowed on trunk
Gi1/0/21    1-4094
Gi1/0/22    1-4094

Port        Vlans allowed and active in management domain
Gi1/0/21    1,10,20,25,50,99
Gi1/0/22    1,10,20,25,50,99

Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/21    1,10,20,25,50,99
Gi1/0/22    1,10,20,25,50,99
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

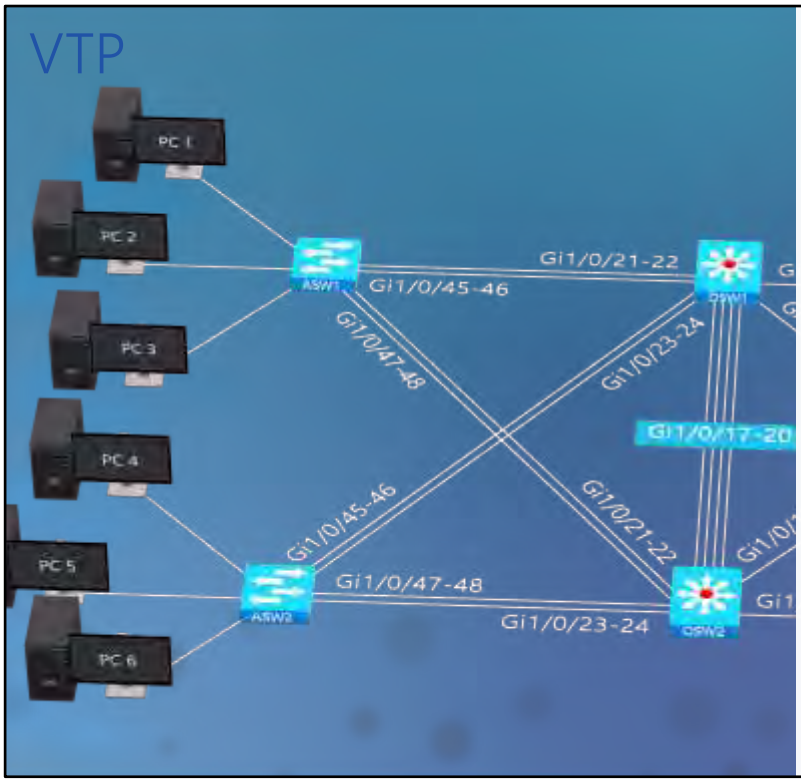
VLAN Trunking Protocol (VTP)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VTP



Supports auto propagation of VLANs across a domain

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VTP Overview

VTP – Supports auto propagation of VLANs across a domain

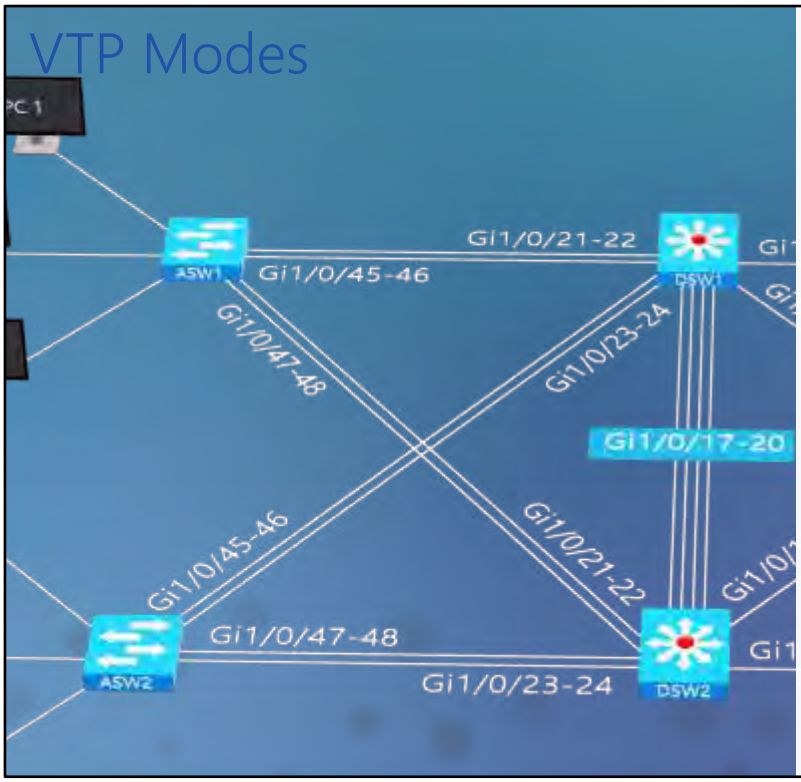
VLANs are written to VLAN database (stored in flash as vlan.dat)

VTP default config:

- Server mode
- Version 1
- Domain: null

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VTP Modes



Server:

Send and Receive VTP messages, Configure VLANs, synchronize database.

Client:

Send and Receive VTP messages, Can't configure VLANs, synchronize database.

Transparent:

Ignores VTP messages, Forwards received VTP messages, Configure VLANs

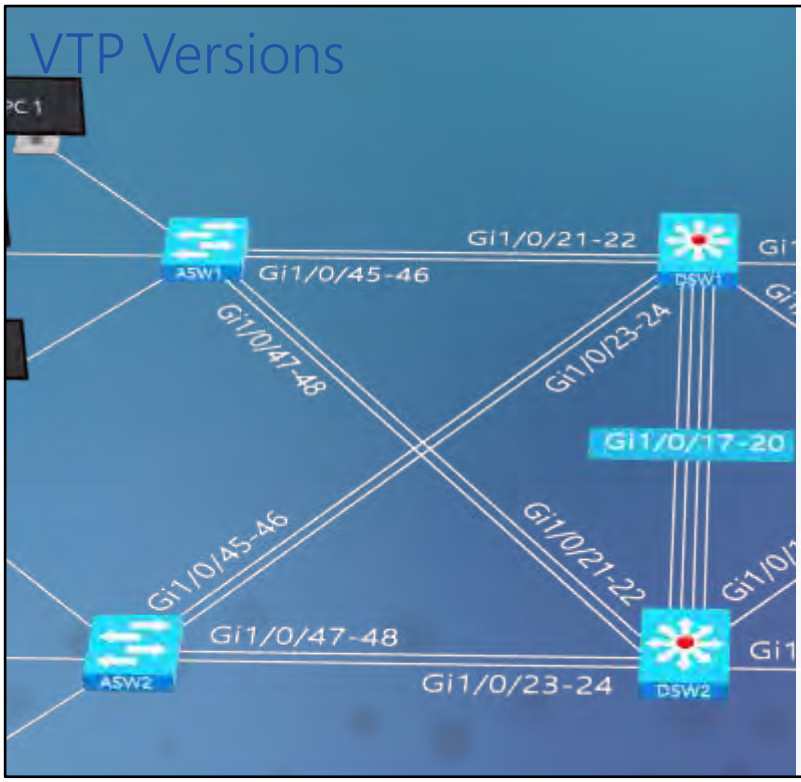
Off:

Shuts off VTP, Configure VLANs.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VTP Versions



Version 1:

support only normal-range VLANs (VLANs 1 to 1005)

Version 2:

support only normal-range VLANs (VLANs 1 to 1005)

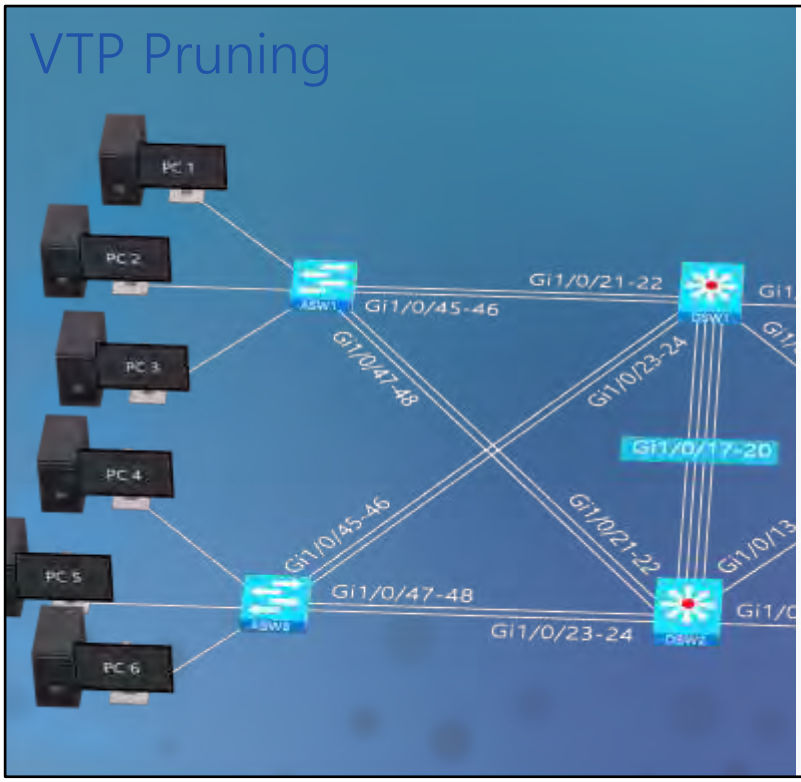
Version 3:

supports the entire VLAN range (VLANs 1 to 4094)

©2023 by StormWind LLC. All rights reserved.

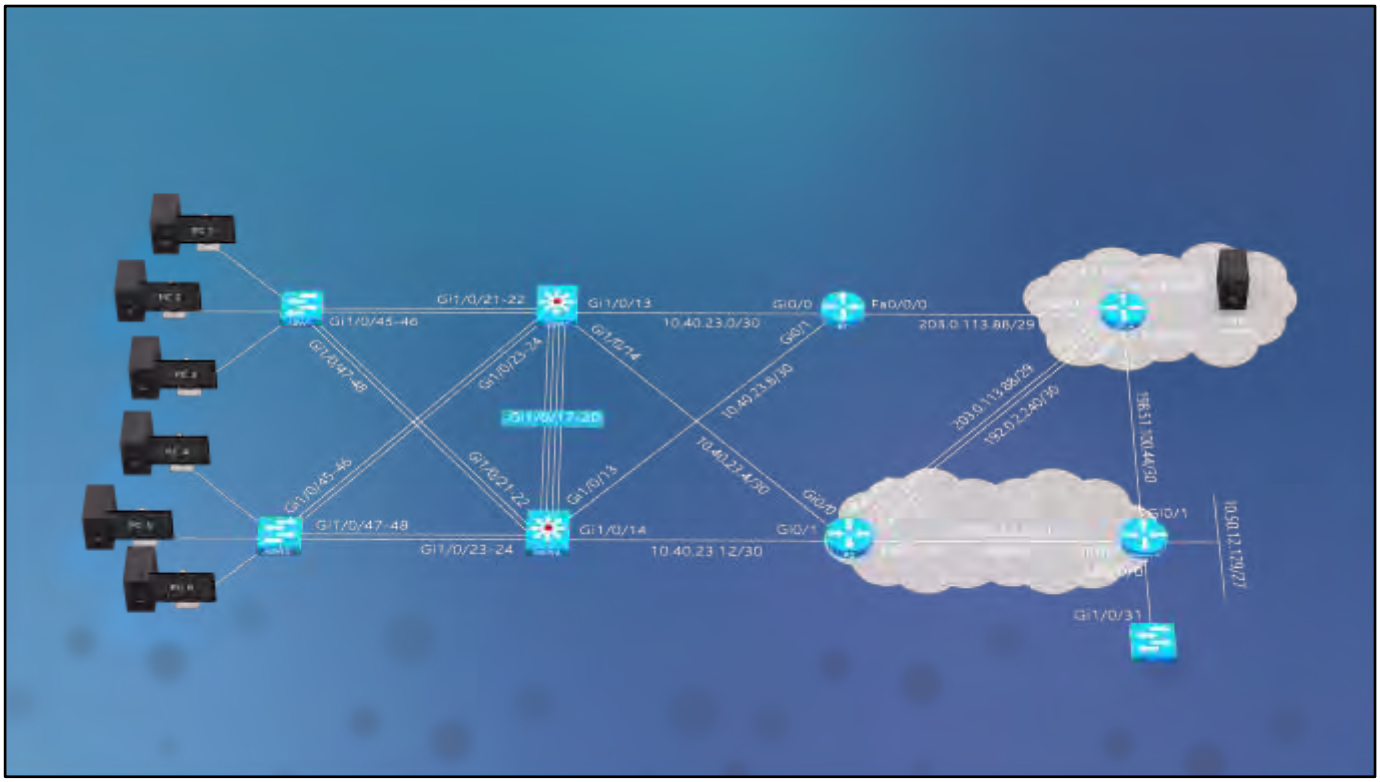
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VTP Pruning



Used to add/remove VLANs off a trunk dynamically

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

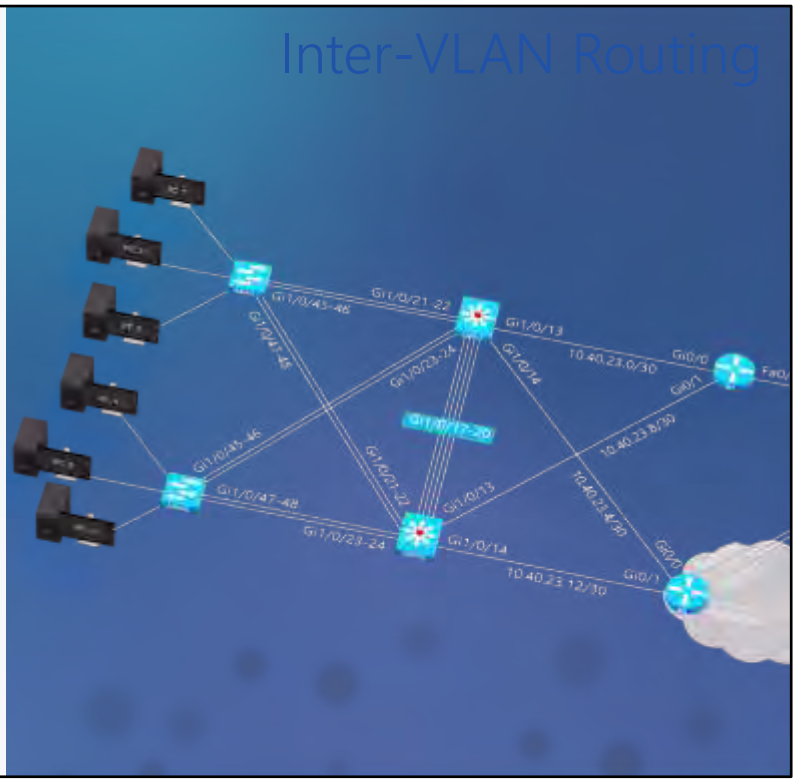


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Inter-VLAN Routing

VLANs have unique IP subnets.

Routing is required to forward traffic between VLANs and in and out of VLANs.



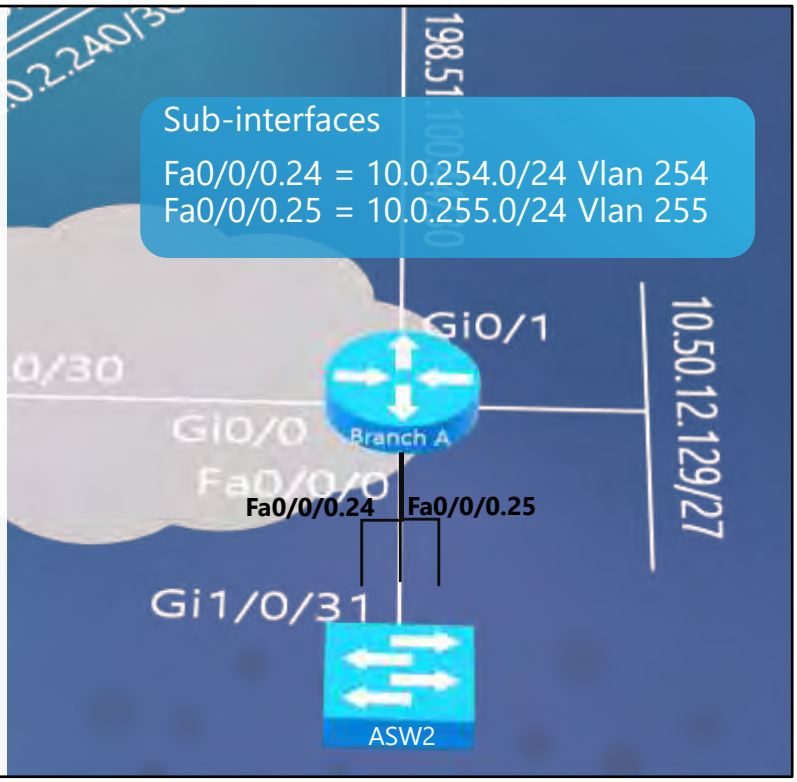
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

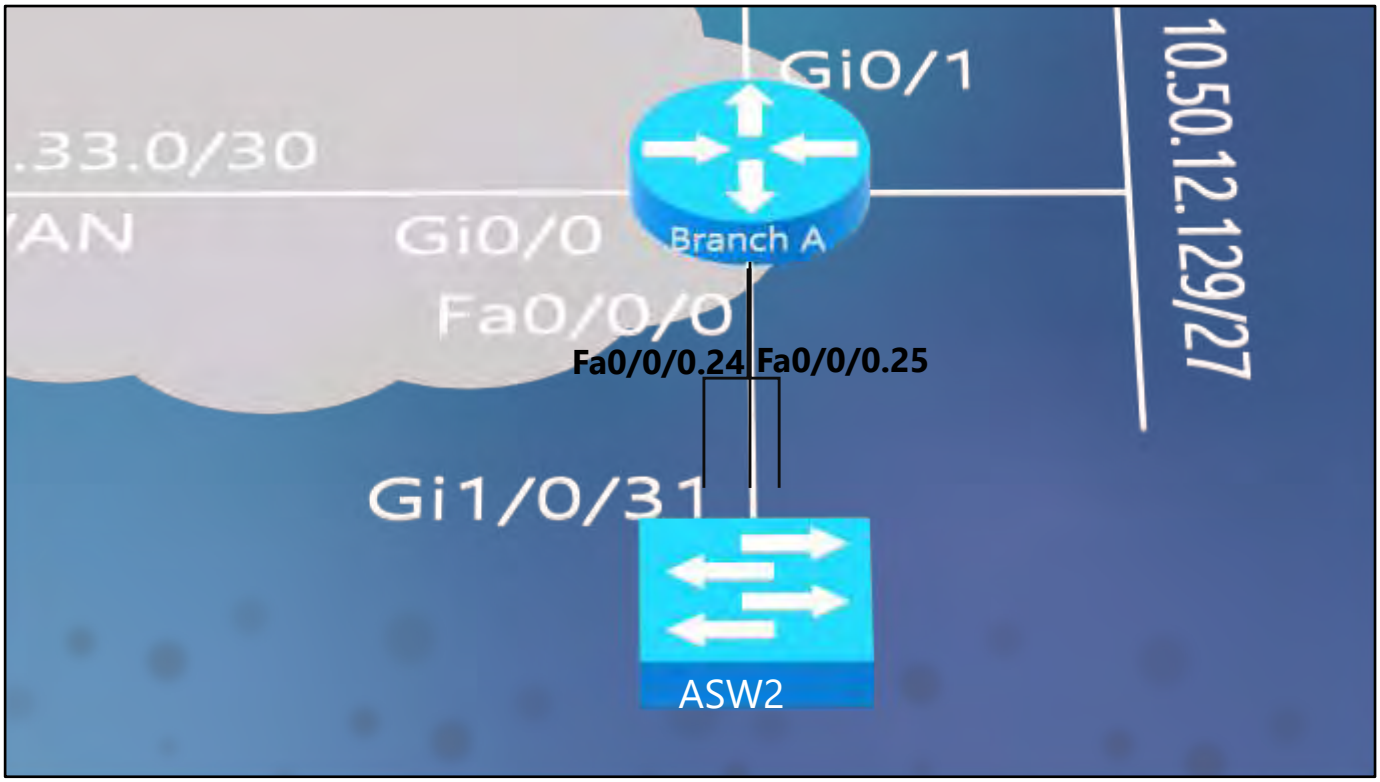
Inter-VLAN Routing

Option: Router on a Stick

One physical router interface broken into multiple sub-interfaces.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

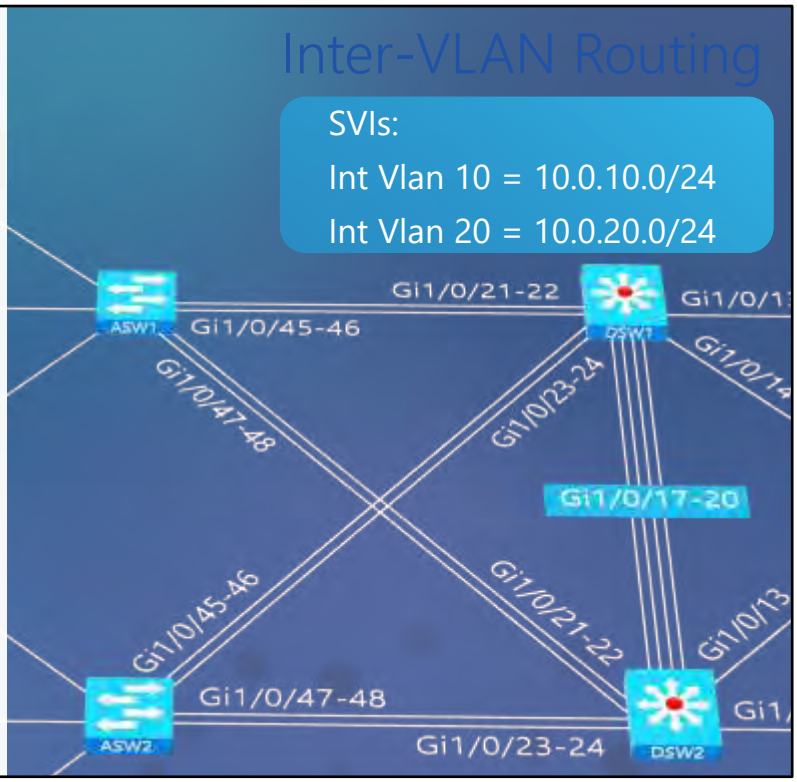


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

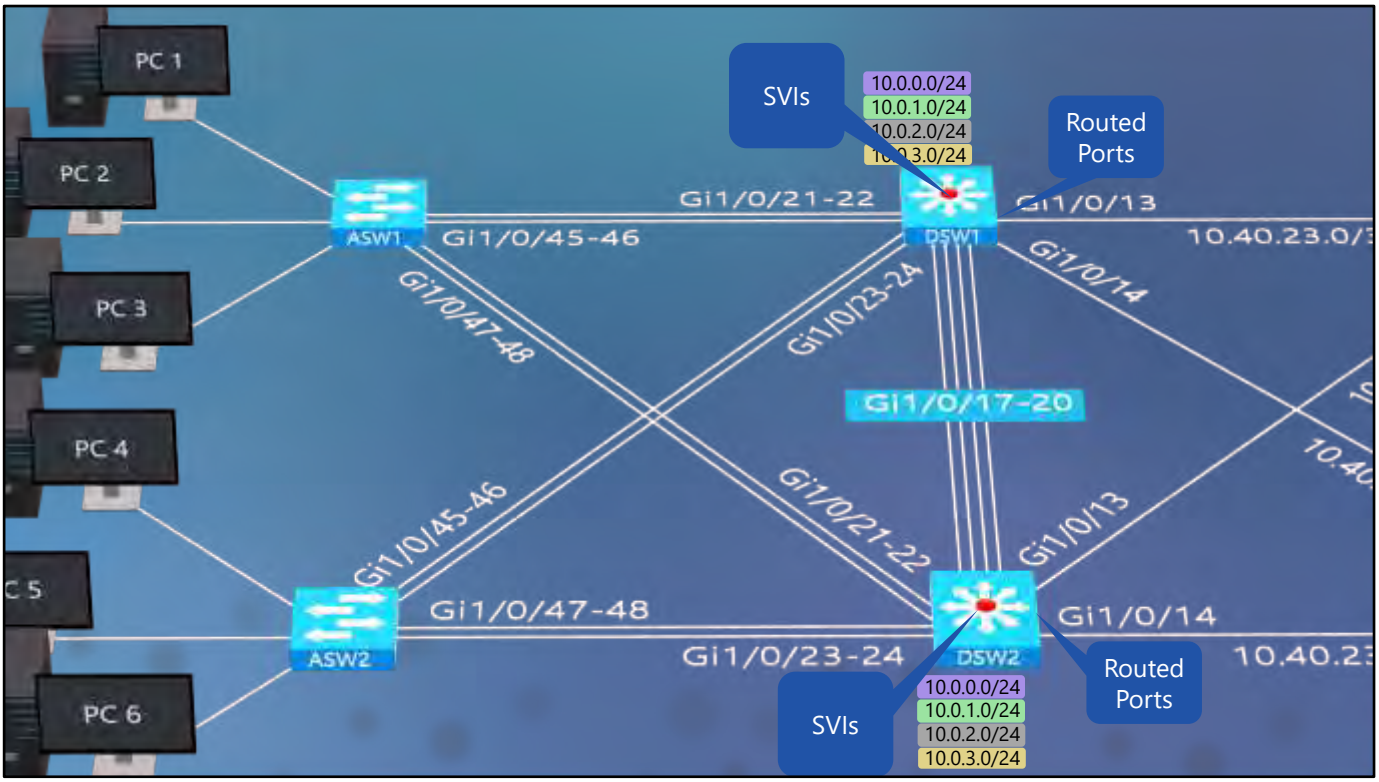
Inter-VLAN Routing

Option: Layer 3 Switch SVIs

Virtual Layer 3 interfaces that connect the VLANs on the device to the Layer 3 router engine on the device.



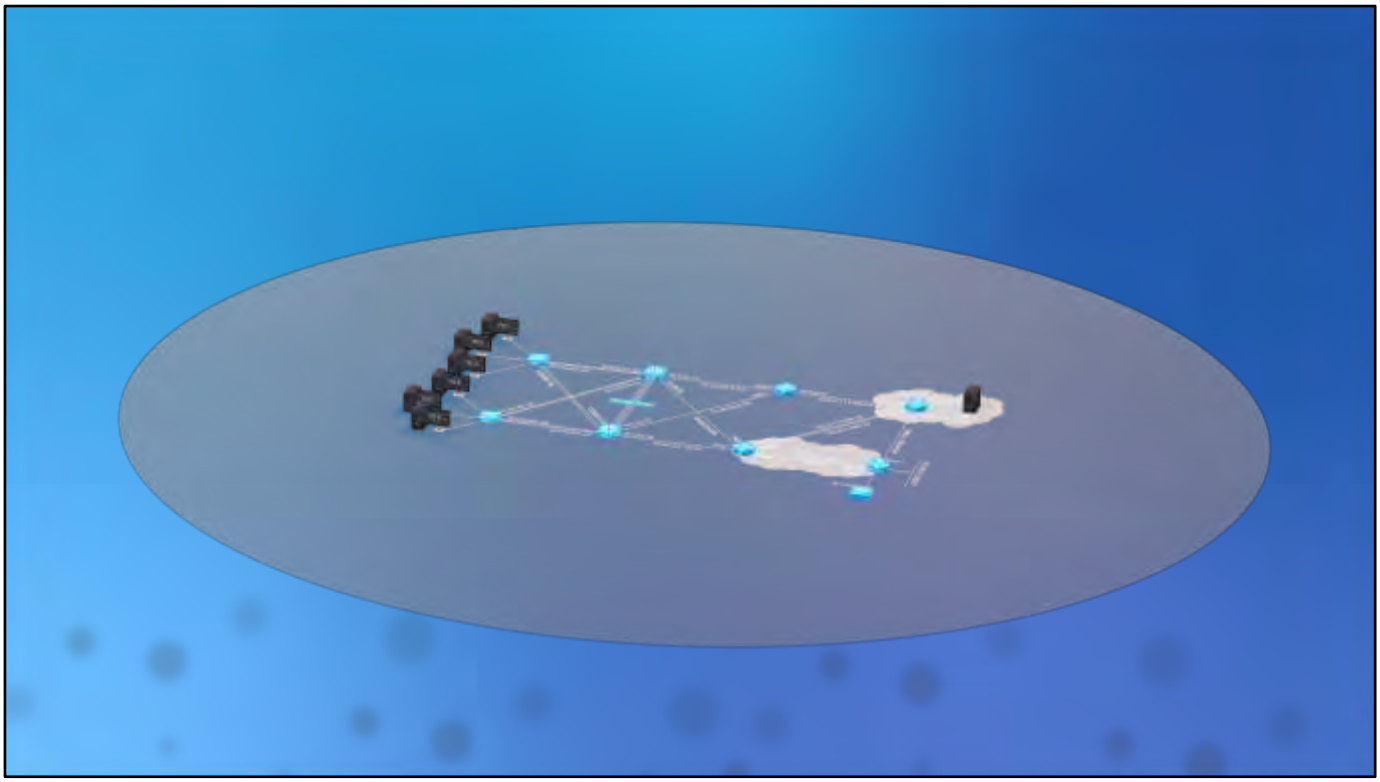
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

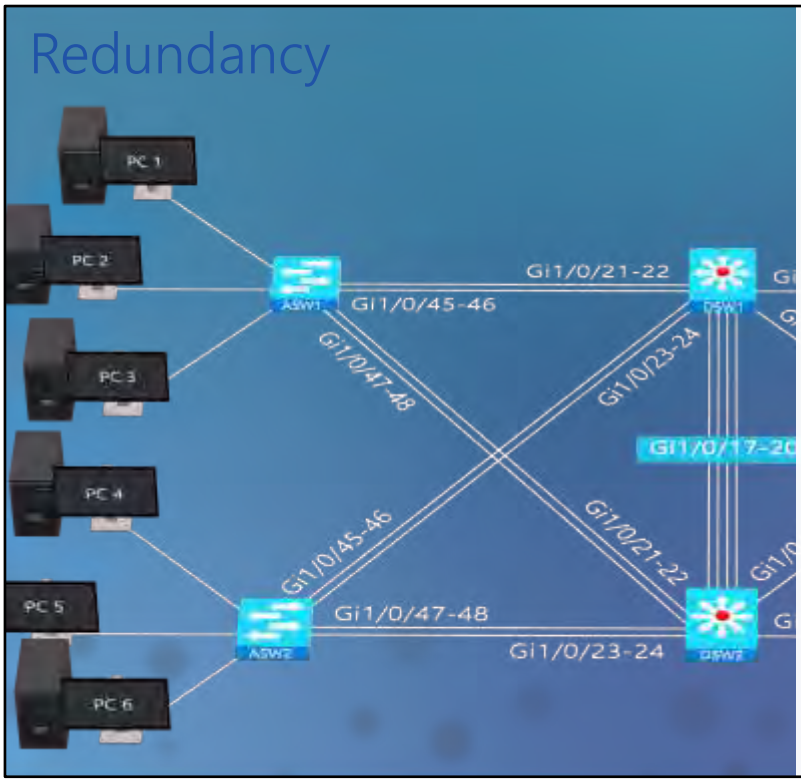
STP Overview and Algorithm Deep Dive

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Redundancy



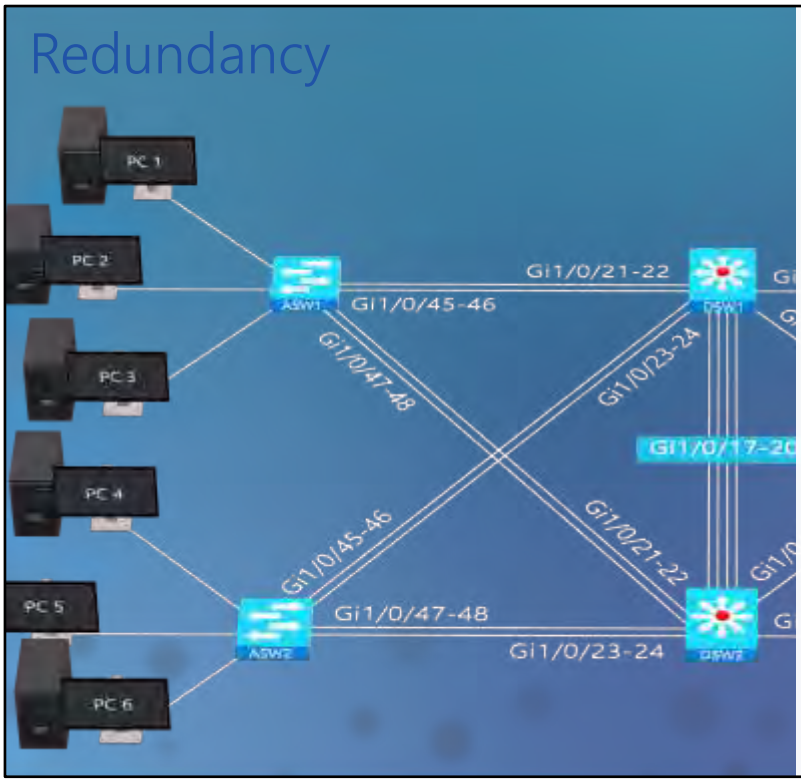
Required to **eliminate single points of failure** in L2 network

Ensures if a link or a switch goes down, there is a backup path

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Redundancy

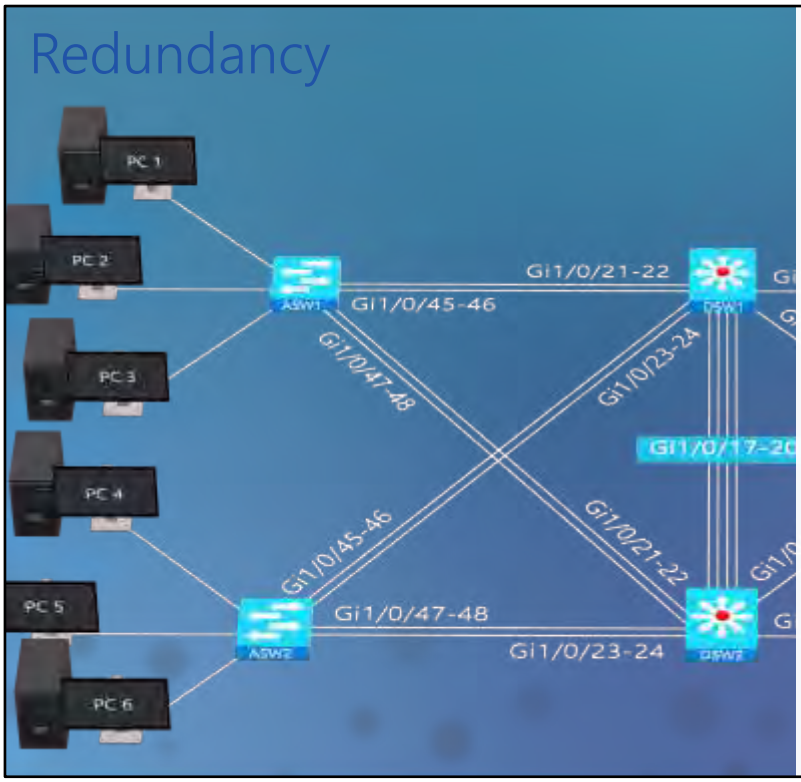


Switches default behavior:

- Flood unknown unicast
- Flood broadcasts

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Redundancy



Switches default behavior:

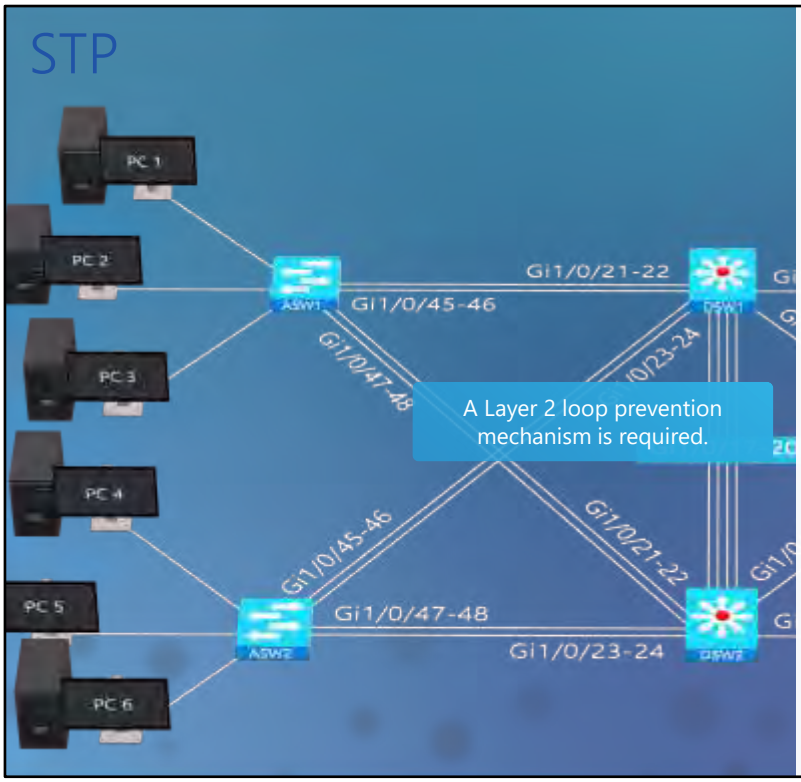
- Flood unknown unicast
- Flood broadcasts

This will cause broadcast storms, MAC table instability problems, and could lock up a network.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP



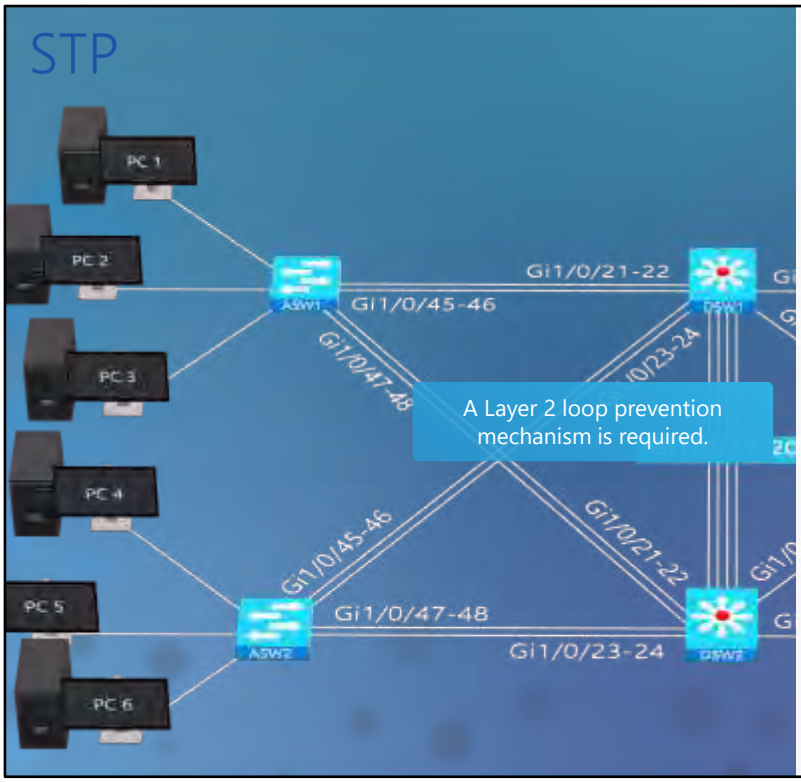
Switches default behavior:

- Flood unknown unicast
- Flood broadcasts

This will cause broadcast storms, MAC table instability problems, and could lock up a network.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP



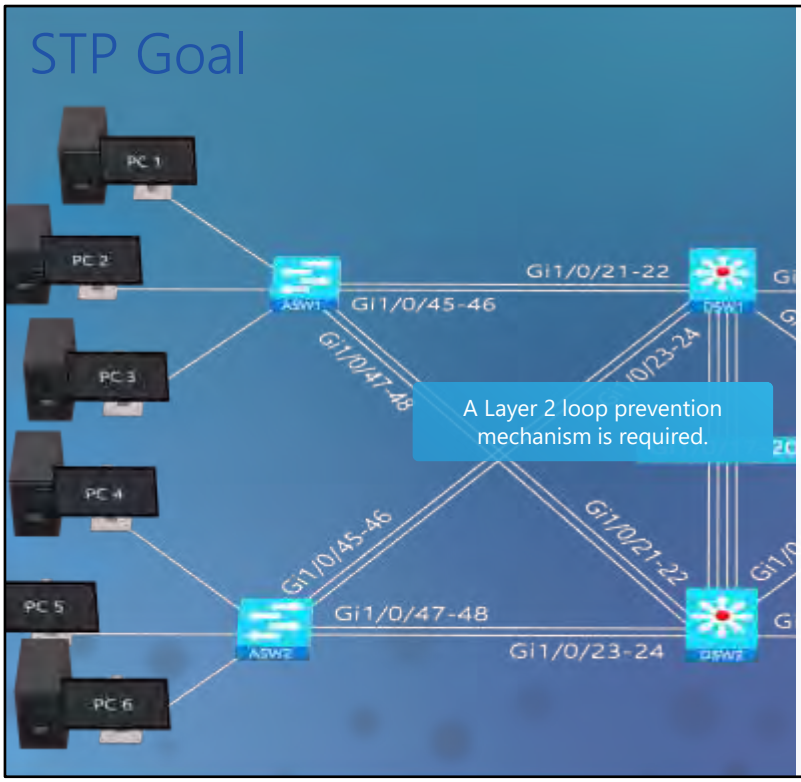
Originally designed by Radia Perlman

Standardized as IEEE 802.1D in 1990

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Goal



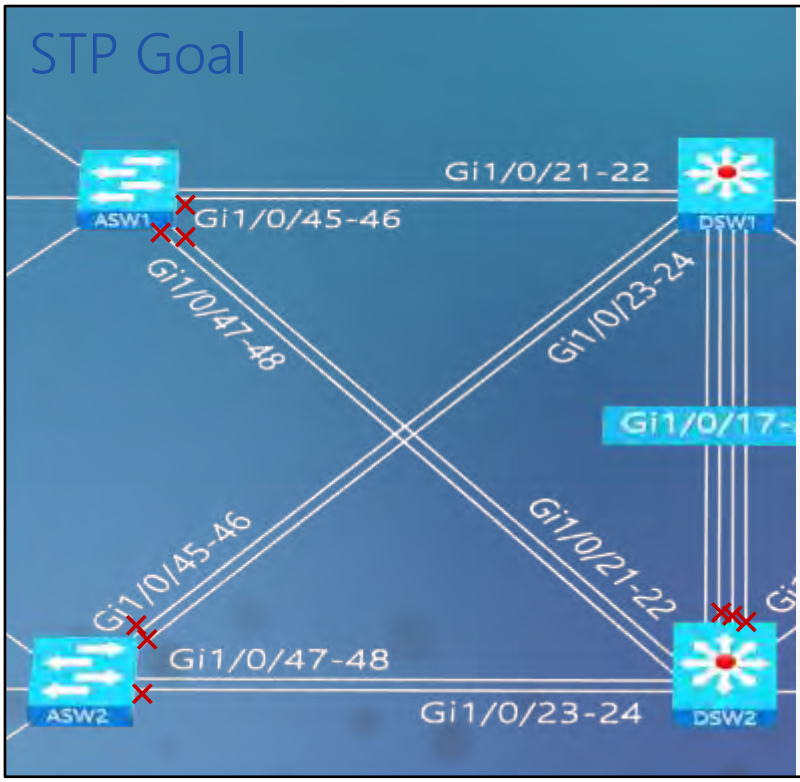
A Layer 2 loop prevention mechanism is required.

Identify ports to block so that loops will be eliminated.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Goal

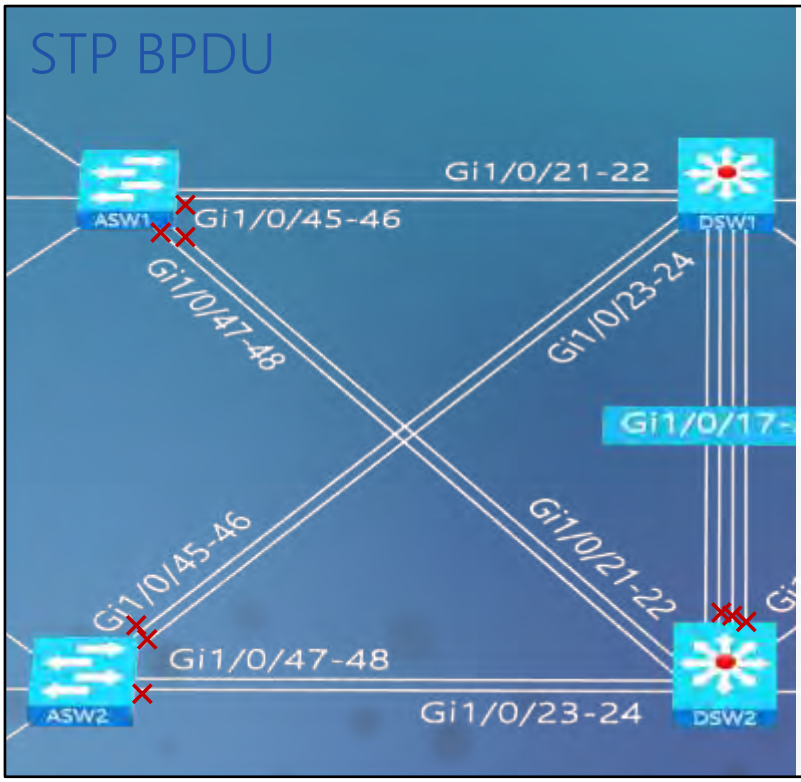


Identify ports to block so that loops will be eliminated.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP BPDU



Uses BPDU's sent every 2 seconds, to share data such as:

- Protocol Identifier
- Protocol Version
- BPDU Type
- Flags
- Root Bridge ID
- Root Path Cost
- Sending Bridge ID
- Sending Port ID
- Message Age
- Max Age
- Hello Time
- Forward Delay

This information will be used to build the spanning tree topology

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Types of Spanning Tree Protocol

IEEE 802.1D	The legacy implementation of STP aka: Common Spanning Tree (CST) Assumes one STP instance for the Layer 2 network, regardless of # of VLANs
PVST+	***PVST+ is default on Cisco Catalyst switches** Cisco's version of STP (802.1D) Provides a separate 802.1D instance/tree for every VLAN configured
IEEE 802.1W	Industry standard version of STP that converges faster than 802.1D Assumes one STP instance for the Layer 2 network, regardless of # of VLANs
RPVST+	Cisco's version of 802.1W Provides a separate 802.1W instance/tree for every VLAN configured
MSTP/802.1s	A version of STP that allows you to group VLANs together into various trees. Originally developed by Cisco as MSTP and is now an industry standard as 802.1s

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Overview

- For each STP loop, a blocked port is found
- Each blocked port breaks the loop
- Port roles such as root ports and designed ports can be left active (forwarding) and not cause a loop

Port Role	Port State	Operational Effect
Root Port (RP)	Forwarding	Include in broadcast domain
Designated Port (DP)	Forwarding	Include in broadcast domain
Nondesignated Port	Blocking	Exclude from broadcast domain

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Spanning-Tree Algorithm Steps

The spanning-tree algorithm follows these steps:

1. Elect a root bridge* in each instance of STP.
2. All non-root switches elect a single root port (RP).
3. All segments (i.e. collision domain) elect a single designated port (DP).
4. Transition Root and Designated ports to forwarding Transition all other ports to blocking state.

*** Note: Bridge and switch are used interchangeably in STP**

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 1. Elect Root Bridge

The spanning-tree algorithm follows these steps:

1. Elect a root bridge* in each instance of STP.
2. All non-root switches elect a single root port (RP).
3. All segments (i.e. collision domain) elect a single designated port (DP).
4. Transition Root and Designated ports to forwarding Transition all other ports to blocking state.

*** Note: Bridge and switch are used interchangeably in STP**

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 1. Elect Root Bridge

Root Bridge

The switch that all other switches use as the reference point when building the spanning tree topology.

Decision based on *lowest Bridge ID* (BID)

Priority first, then lowest MAC

Secondary Root Bridge

The switch that takes over as the root bridge if the Root Bridge is unavailable

Secondary Root is the next lowest Bridge ID

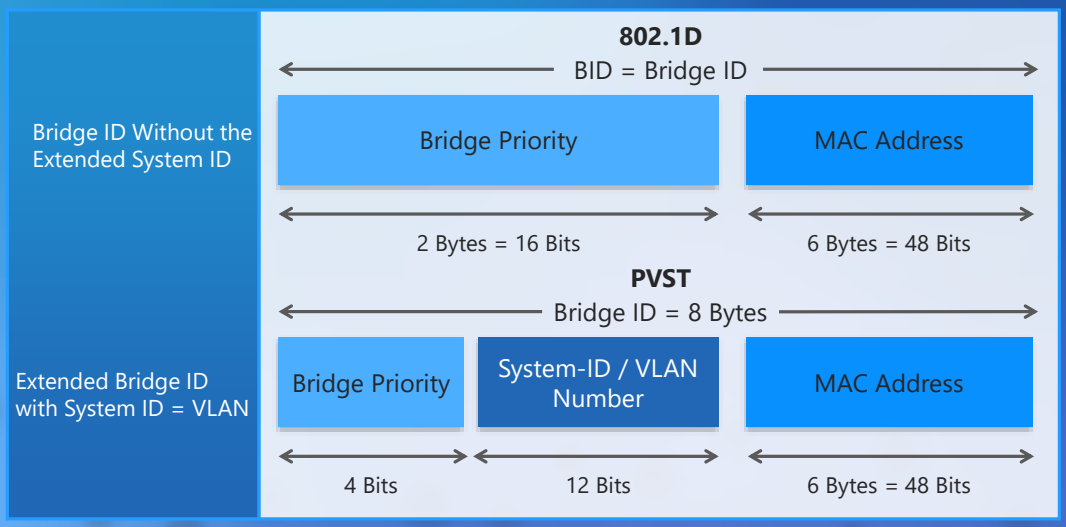
BID = Bridge ID

Bridge Priority	MAC Address
Range: 0-65535 Default: 32768	Unique for every device

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PVST + Bridge ID



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PVST + Bridge ID

Extended Bridge ID with System ID = VLAN

```
ASW2#show spanning-tree vlan 10

…output omitted…

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     d4a0.2a6e.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

…output omitted…
```

PVST

Bridge ID = 8 Bytes

Bridge Priority	System-ID / VLAN Number	MAC Address
4 Bits	12 Bits	6 Bytes = 48 Bits

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PVST + Bridge ID

Extended Bridge ID with System ID = VLAN

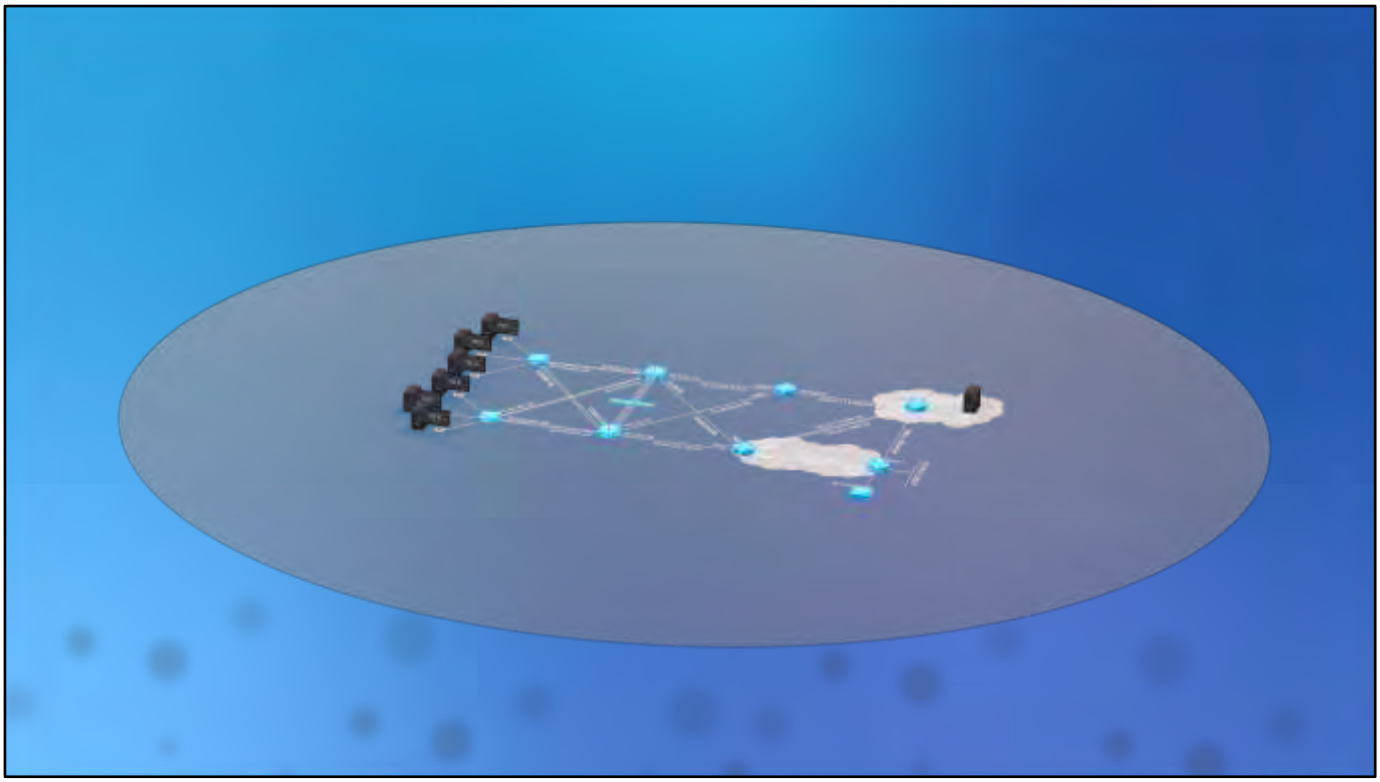
```
ASW2(config)#spanning-tree vlan 10 priority 5000
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440
```

PVST

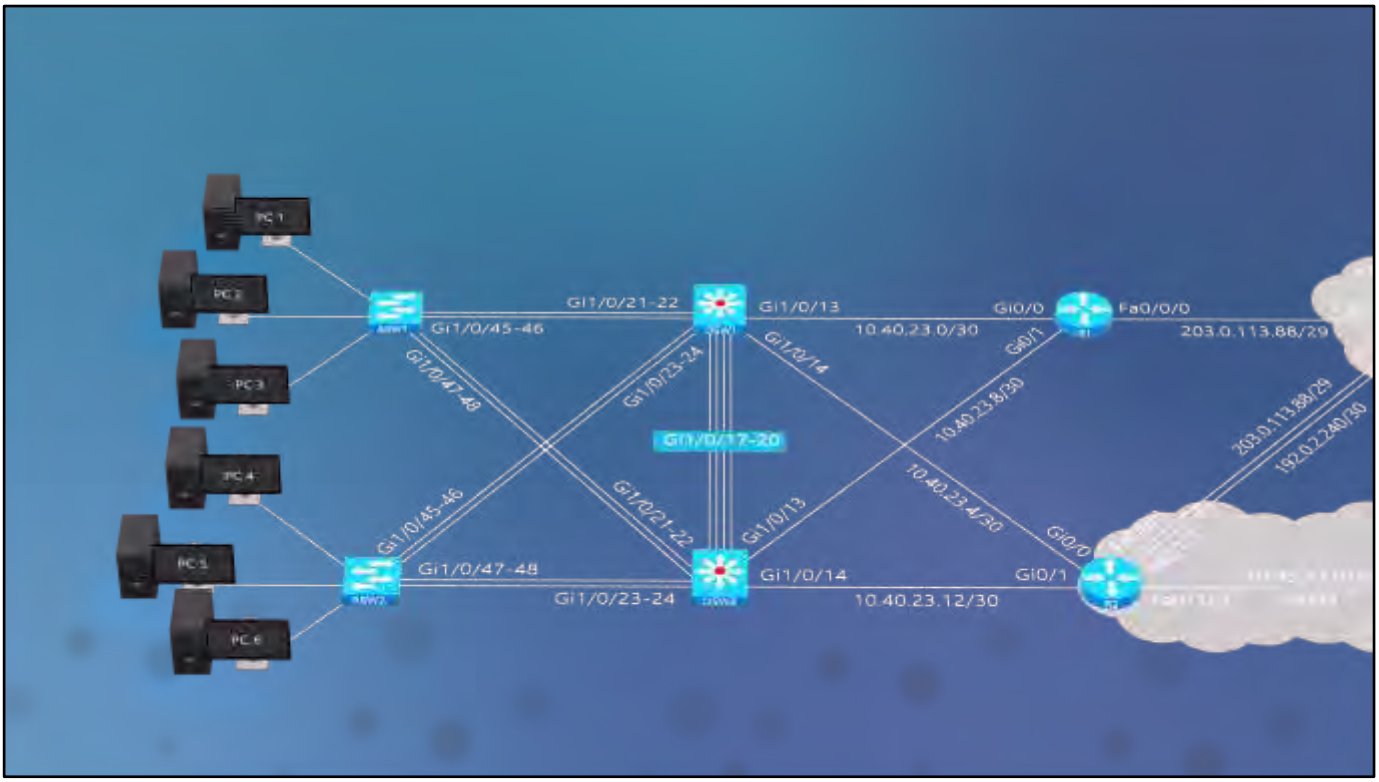
Bridge ID = 8 Bytes

Bridge Priority	System-ID / VLAN Number	MAC Address
4 Bits	12 Bits	6 Bytes = 48 Bits

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 1. Elect Root Bridge

```
ASW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
…output omitted…

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     d4a0.2a63.dd80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

…output omitted…
```

```
ASW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
…output omitted…

 Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
            Address     d4a0.2a6e.d780
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec

…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 1. Elect Root Bridge

```
ASW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
…output omitted…

 Bridge ID  Priority    32778  (priority 32768 sys-id-ext
            Address     d4a0.2a63.dd80
            Hello Time   2 sec  Max Age 20 sec  Forward
            Aging Time  300 sec
…output omitted…
```

```
ASW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
…output omitted…

 Bridge ID  Priority    32778  (priority 32768 sys-id-ext
            Address     d4a0.2a6e.d780
            Hello Time   2 sec  Max Age 20 sec  Forward
            Aging Time  300 sec
…output omitted…
```

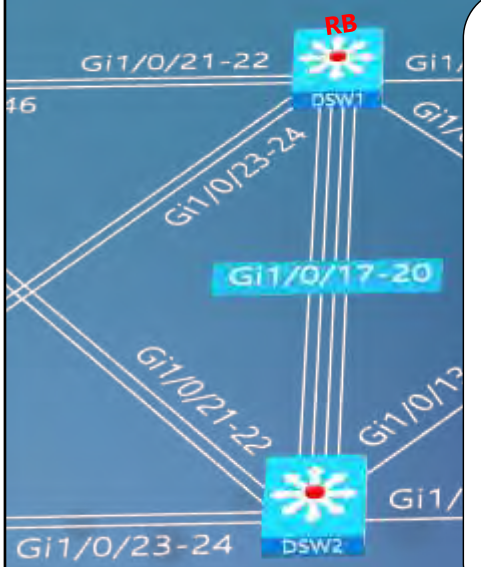
```
DSW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
…output omitted…

 Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
            Address     2c54.2d3f.e700
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec
…output omitted…
```

```
DSW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
…output omitted…

 Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
            Address     4c00.828c.4300
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time  300 sec
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

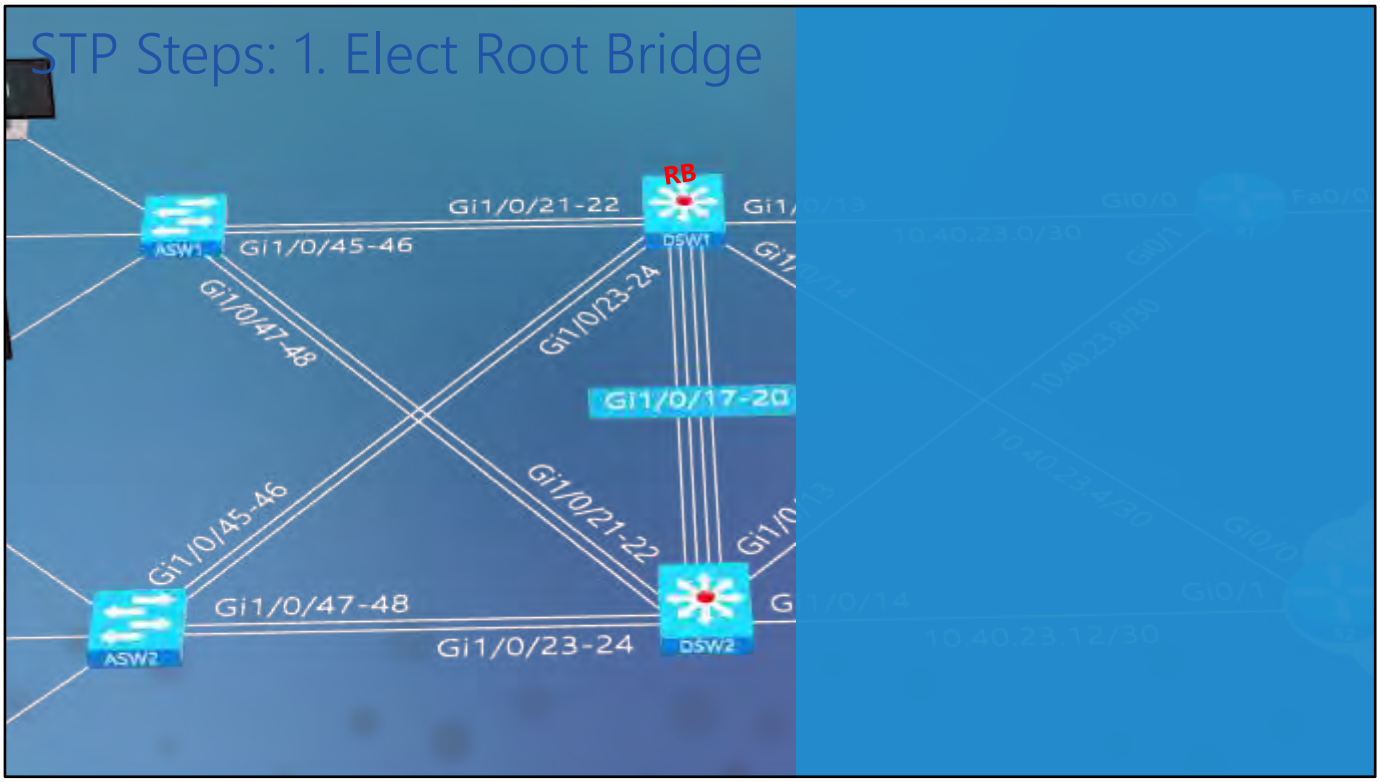
STP Steps: 1. Elect Root Bridge




```
DSW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    32778
             Address     2c54.2d3f.e700
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
             Address     2c54.2d3f.e700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  15  sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ---------------------
Gi1/0/17            Desg FWD 4         128.17   P2p
Gi1/0/18            Desg FWD 4         128.18   P2p
Gi1/0/19            Desg FWD 4         128.19   P2p
Gi1/0/20            Desg FWD 4         128.20   P2p
Gi1/0/21            Desg FWD 4         128.21   P2p
Gi1/0/22            Desg FWD 4         128.22   P2p
Gi1/0/23            Desg FWD 4         128.23   P2p
Gi1/0/24            Desg FWD 4         128.24   P2p
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 1. Elect Root Bridge



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 2. Elect Root Ports

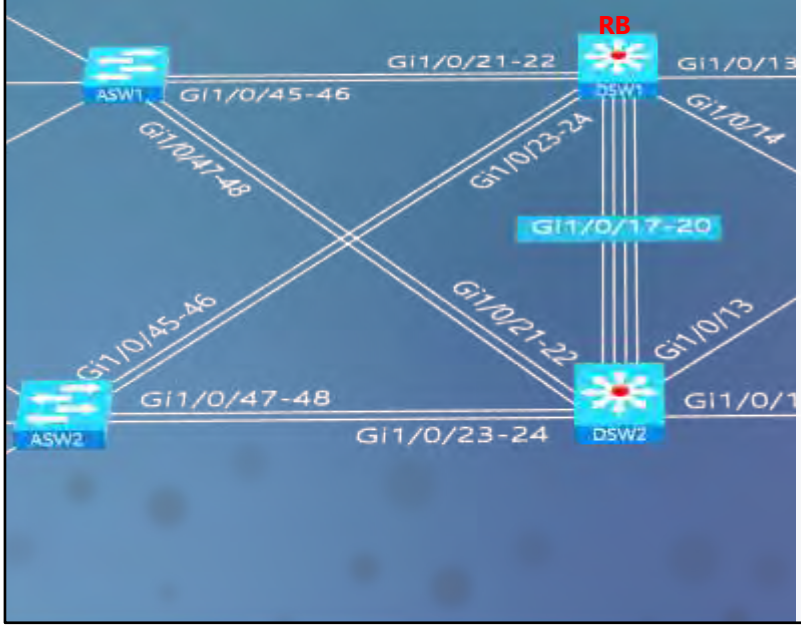
The spanning-tree algorithm follows these steps:

1. Elect a root bridge* in each instance of STP.
2. All non-root switches elect a single root port (RP).
3. All segments (i.e. collision domain) elect a single designated port (DP).
4. Transition Root and Designated ports to forwarding Transition all other ports to blocking state.

*** Note: Bridge and switch are used interchangeably in STP**

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 2. Elect Root Ports



Root port is selected based on cost

Port with the lowest cumulative cost back to the Root Bridge

Cost is based on bandwidth of link and has been pre-defined

Short Method:	Long Method:
100 Mbps - 19	100 Mbps - 200000
1 Gbps - 4	1 Gbps - 20000
10 Gbps - 2	10 Gbps - 2000

Equal cost paths are broken by upstream BID

If there is a tie for upstream BID, lowest port ID value wins

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 2. Elect Root Ports

Equal cost paths are broken by upstream BID

If there is a tie for upstream BID, lowest port ID value wins

Short Method:

100 Mbps - 19
1 Gbps - 4
10 Gbps - 2

BPDU:

- Protocol Identifier
- Protocol Version
- BPDU Type
- Flags
- Root Bridge ID
- Root Path Cost
- Sending Bridge ID
- Sending Port ID
- Message Age
- Max Age
- Hello Time
- Forward Delay

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 2. Elect Root Ports

Equal cost paths are broken by upstream BID

If there is a tie for upstream BID, lowest port ID value wins

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 3. Elect Designated Ports

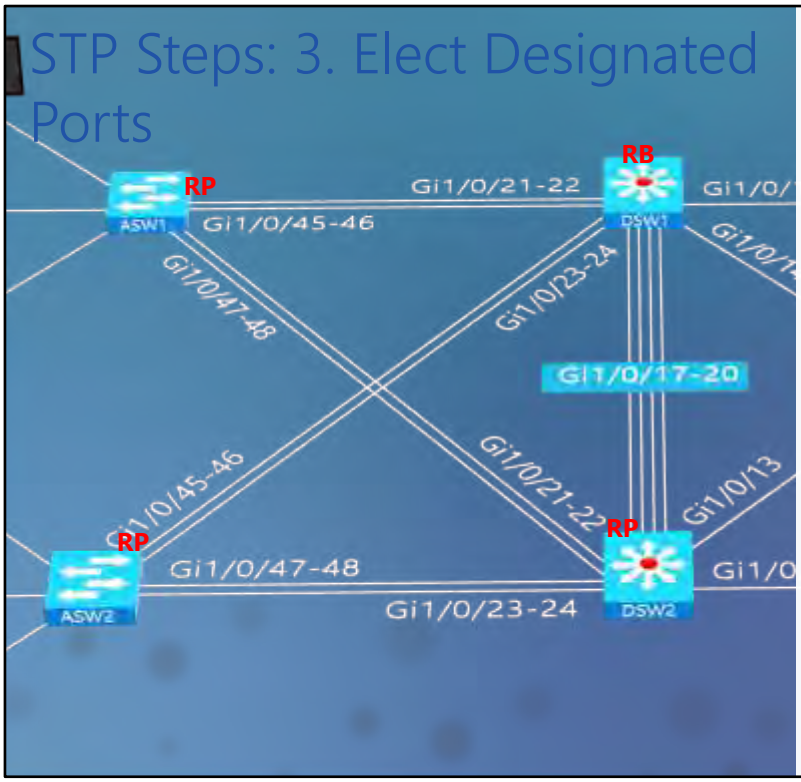
The spanning-tree algorithm follows these steps:

1. Elect a root bridge* in each instance of STP.
2. All non-root switches elect a single root port (RP).
3. All segments (i.e. collision domain) elect a single designated port (DP).
4. Transition Root and Designated ports to forwarding Transition all other ports to blocking state.

*** Note: Bridge and switch are used interchangeably in STP**

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 3. Elect Designated Ports



Port on segment with the lowest cumulative cost path to the Root Bridge

*Designated ports are ALWAYS on the opposite side of Root ports

*All ports on a Root Bridge are Designated

Short Method:	Long Method:
100 Mbps - 19	100 Mbps - 200000
1 Gbps - 4	1 Gbps - 20000
10 Gbps - 2	10 Gbps - 2000

Equal cost paths are broken by upstream BID

If there is a tie for upstream BID, lowest port ID value wins

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 3. Elect Designated Ports

Equal cost paths are broken by upstream BID

If there is a tie for upstream BID, lowest port ID value wins

Port on segment with the lowest cumulative cost path to the Root Bridge

***All ports on a Root Bridge are Designated**

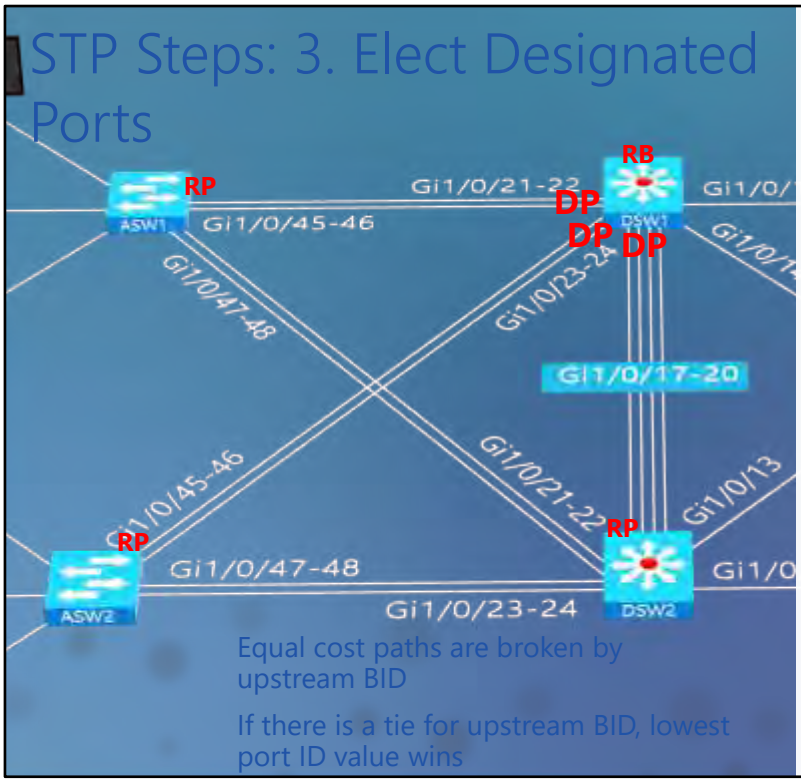
***Designated ports are ALWAYS on the opposite side of Root ports**

Short Method:

100 Mbps - 19
1 Gbps - 4
10 Gbps - 2

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 3. Elect Designated Ports



Equal cost paths are broken by upstream BID

If there is a tie for upstream BID, lowest port ID value wins

Short Method:

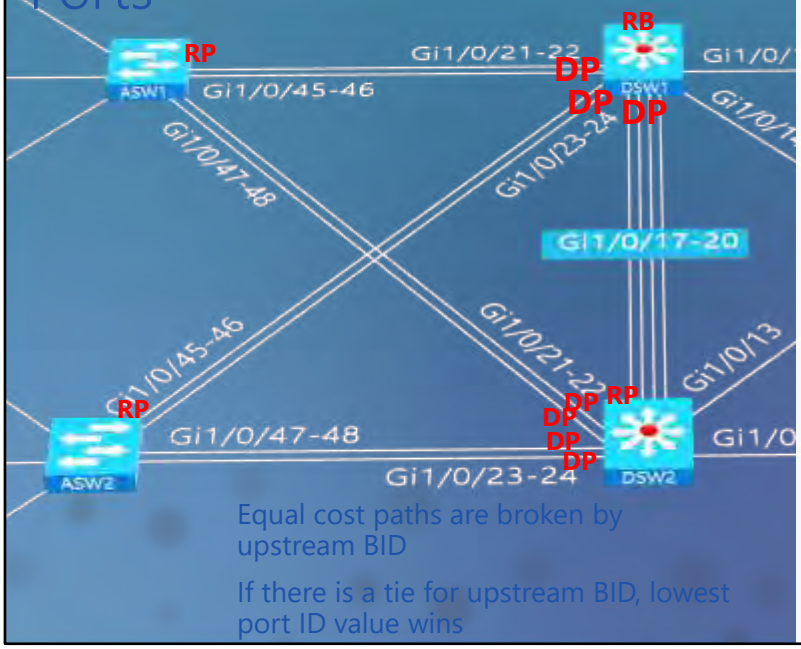
100 Mbps - 19
1 Gbps - 4
10 Gbps - 2

BPDU:

Protocol Identifier
Protocol Version
BPDU Type
Flags
Root Bridge ID
Root Path Cost
Sending Bridge ID
Sending Port ID
Message Age
Max Age
Hello Time
Forward Delay

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 3. Elect Designated Ports



Equal cost paths are broken by upstream BID

If there is a tie for upstream BID, lowest port ID value wins

Short Method:

100 Mbps - 19
1 Gbps - 4
10 Gbps - 2

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 3. Elect Designated Ports

Equal cost paths are broken by upstream BID

If there is a tie for upstream BID, lowest port ID value wins

Short Method:

100 Mbps - 19
1 Gbps - 4
10 Gbps - 2

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 4. Ports Transitions to Forwarding or Blocking

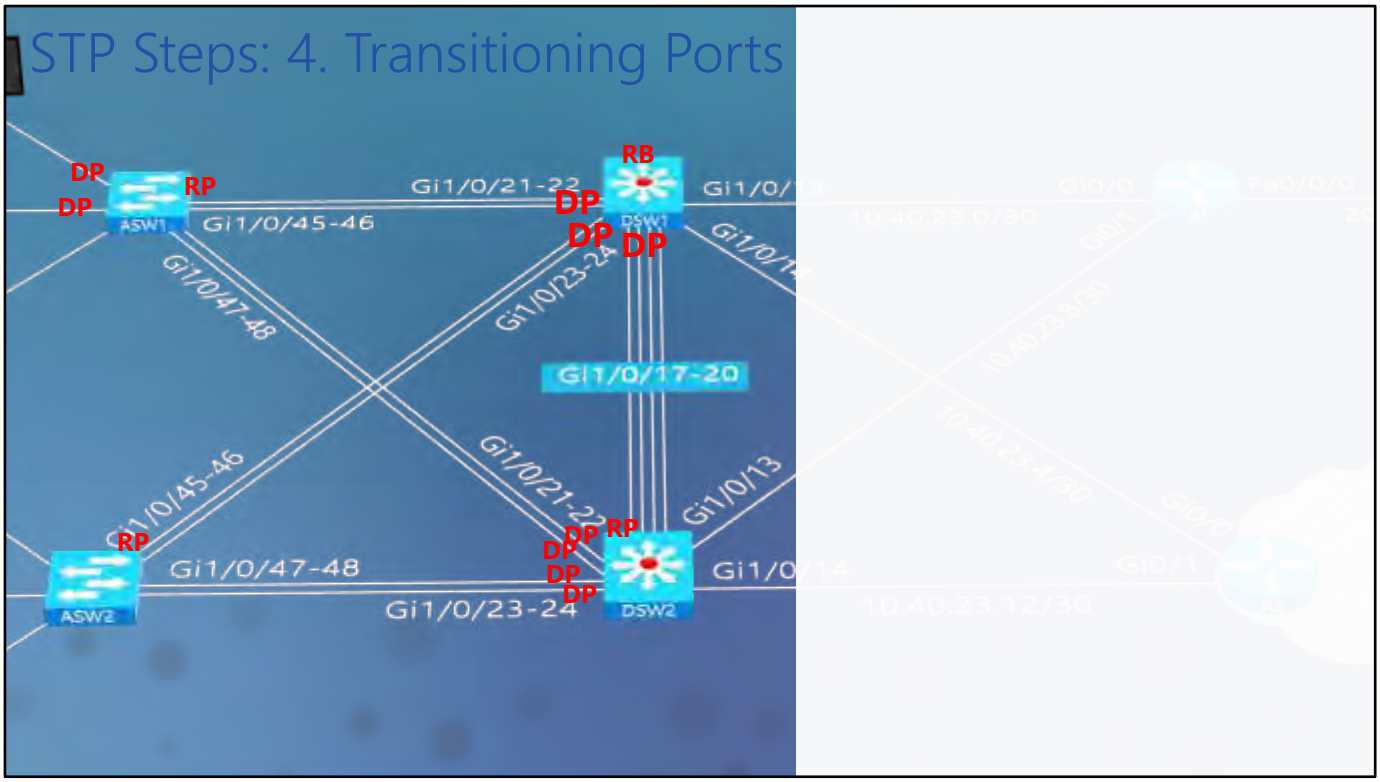
The spanning-tree algorithm follows these steps:

1. Elect a root bridge* in each instance of STP.
2. All non-root switches elect a single root port (RP).
3. All segments (i.e. collision domain) elect a single designated port (DP).
4. Transition Root and Designated ports to forwarding Transition all other ports to blocking state.

*** Note: Bridge and switch are used interchangeably in STP**

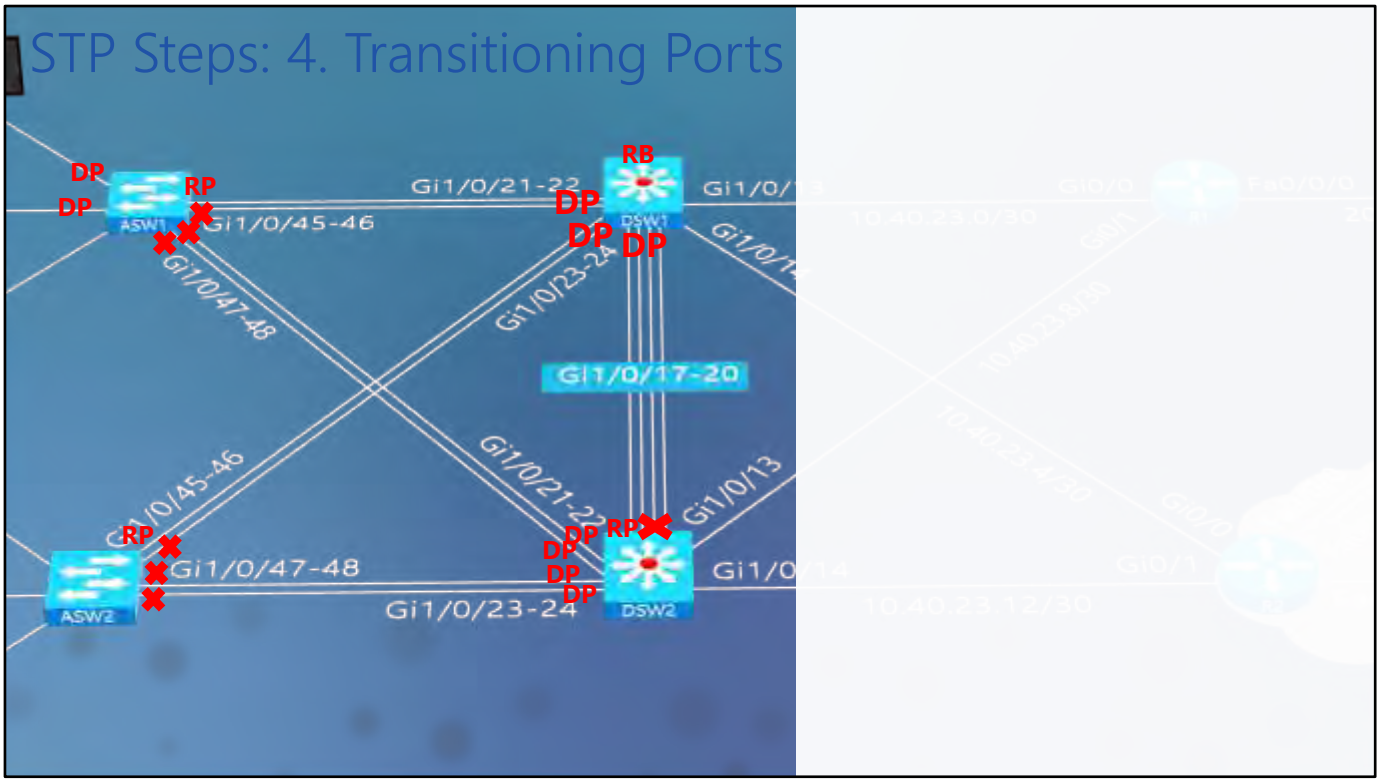
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 4. Transitioning Ports



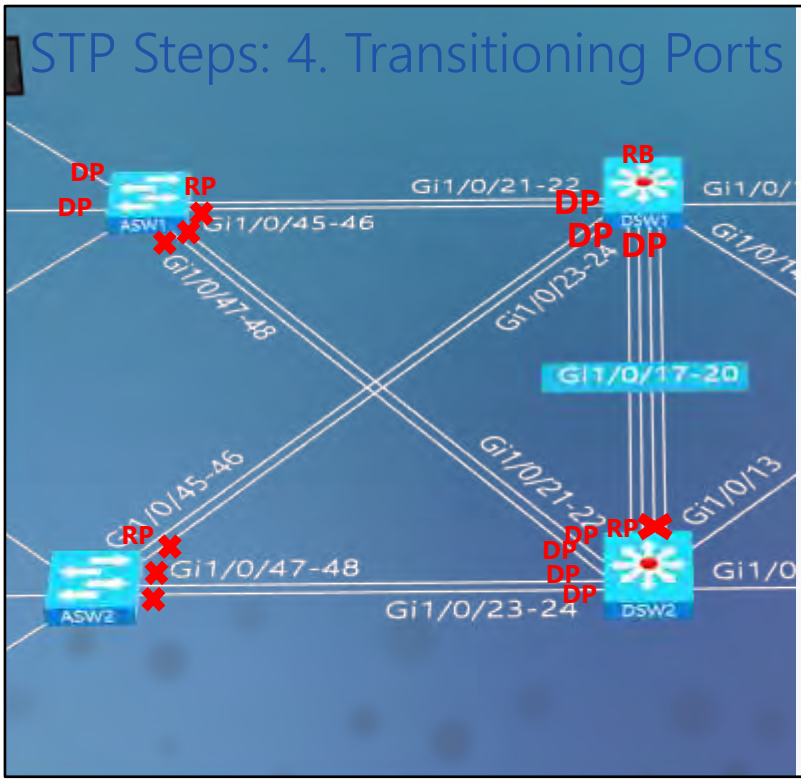
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 4. Transitioning Ports



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Steps: 4. Transitioning Ports



Root ports and designated ports transition to the forwarding state

- Are able to send and receive frames
- Wil populate the MAC address table based on SRC MAC of received frames

All other ports stay in the blocking state

- Does not send or receive frames
- Does not populate the MAC address table
- Will accept BPDUs and send them to the switch system module
- Will receive and respond to network management messages

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP Convergence, Configuration and Manipulation

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PVST+ Convergence Time

Each port on a switch using PVST+ is in one of the following states:

State		Time in State
Blocking	Used to block traffic and prevent a Layer 2 loop. When a port is enabled it will immediately enter the blocked state and will exit the blocked state in the absence of BPDUs or if a BPDU indicates it should.	Until a network change happens in a stable topology. 20 seconds when the network is converging.
Listening	Used to listen for and process BPDUs to determine if the port should be a DP or a RP or Blocked.	15 seconds when the network is converging.
Learning	Same as listening but is now also learning MAC addresses and populating the MAC address table.	15 seconds when the network is converging.
Forwarding	Used to forward frames.	Until a network change happens.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PVST+ Convergence Time

Each port on a switch using PVST+ is in one of the following states:

State		Time in State
Blocking	U[illegible]d prevent a L[illegible]rt is enabled it will immediate[illegible] state a[illegible] state in the a[illegible] BPDU indicates it should.	Until a network change happens in a stable topology. 20 seconds when the network is converging.
Listening	Used to listen for and process BPDUs to d[illegible]ould be a DP or a[illegible]	15 seconds when the network is converging.
Learning	Same as listening [illegible] and populating th[illegible]	15 seconds when the network is converging.
Forwarding	Used to forward frames.	Until a network change happens.

Blocking

20 sec = max age time

Listening

15 sec = forward delay

Learning

15 sec = forward delay

Forwarding

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Convergence Time

IEEE 802.1D	Up to 50 seconds
PVST+	Up to 50 seconds
IEEE 802.1W	2 seconds or less
RPVST+	2 seconds or less
MSTP/802.1s	2 seconds or less

Blocking

20 sec = max age time

Listening

15 sec = forward delay

Learning

15 sec = forward delay

Forwarding

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Comparison of RSTP and STP Port Mechanisms

STP Ports

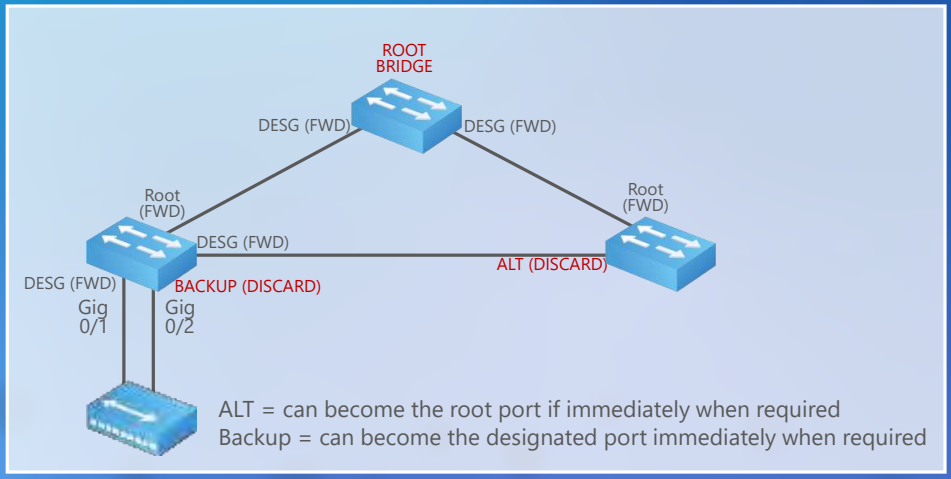
Port Role	Port State	Operational Effect
Root Port (RP)	Forwarding	Include in broadcast domain
Designated Port (DP)	Forwarding	Include in broadcast domain
Nondesignated Port	Blocking	Exclude from broadcast domain
While Transitioning	Listening and Learning	Exclude from broadcast domain

RSTP Ports

Port Role	Port State	Operational Effect
Root Port (RP)	Forwarding	Include in broadcast domain
Designated Port (DP)	Forwarding	Include in broadcast domain
Alternative	Discarding	Exclude from broadcast domain
Backup	Discarding	Exclude from broadcast domain
While Transitioning	Learning	Exclude from broadcast domain

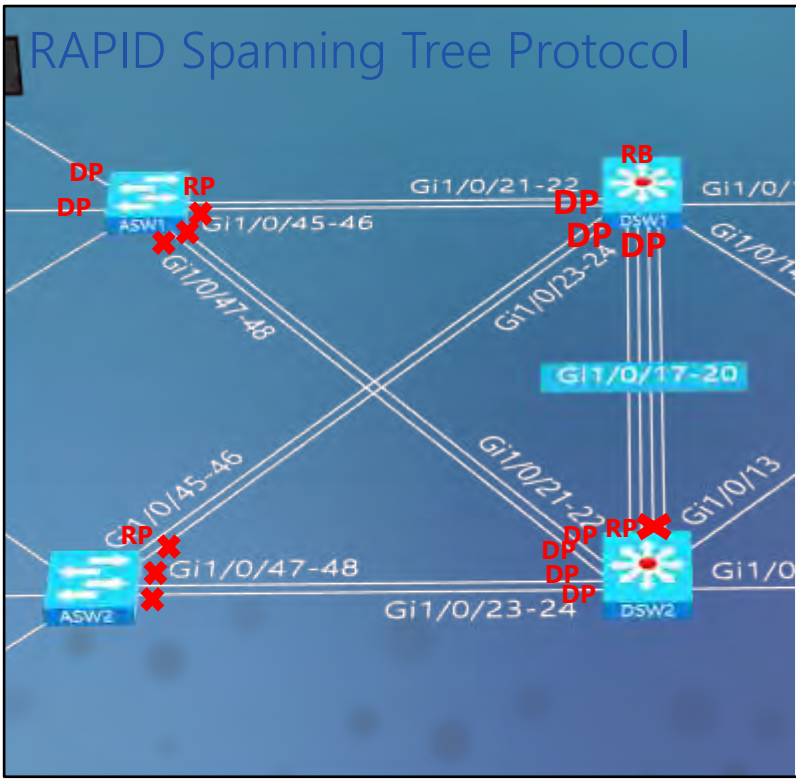
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Rapid PVST Port Roles



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RAPID Spanning Tree Protocol



Rapid PVST supports faster convergence

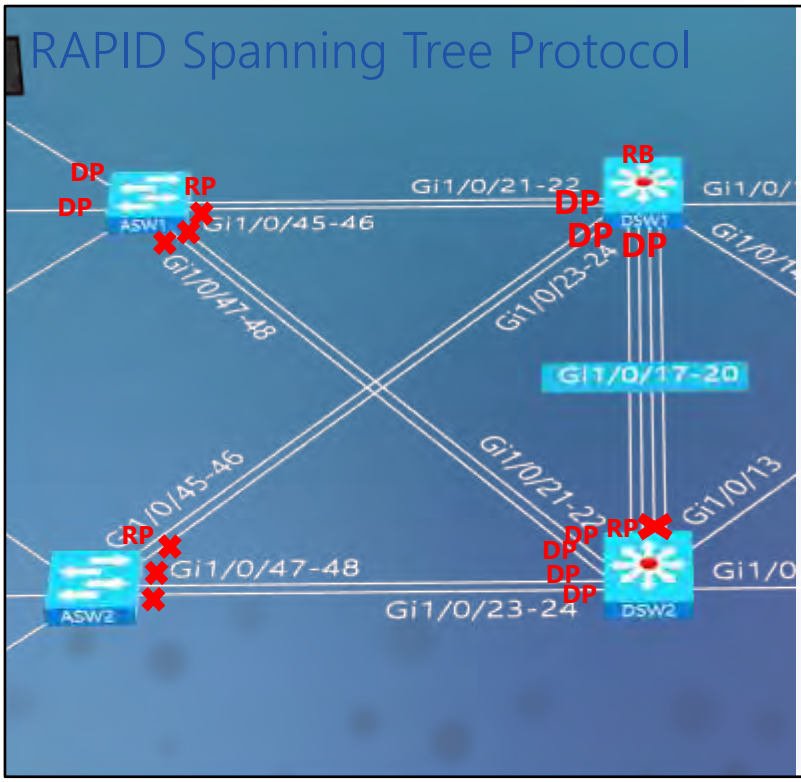
Enable on all switches

If a switch is not running Rapid, the RAPID switch defaults to STP with that switch.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RAPID Spanning Tree Protocol

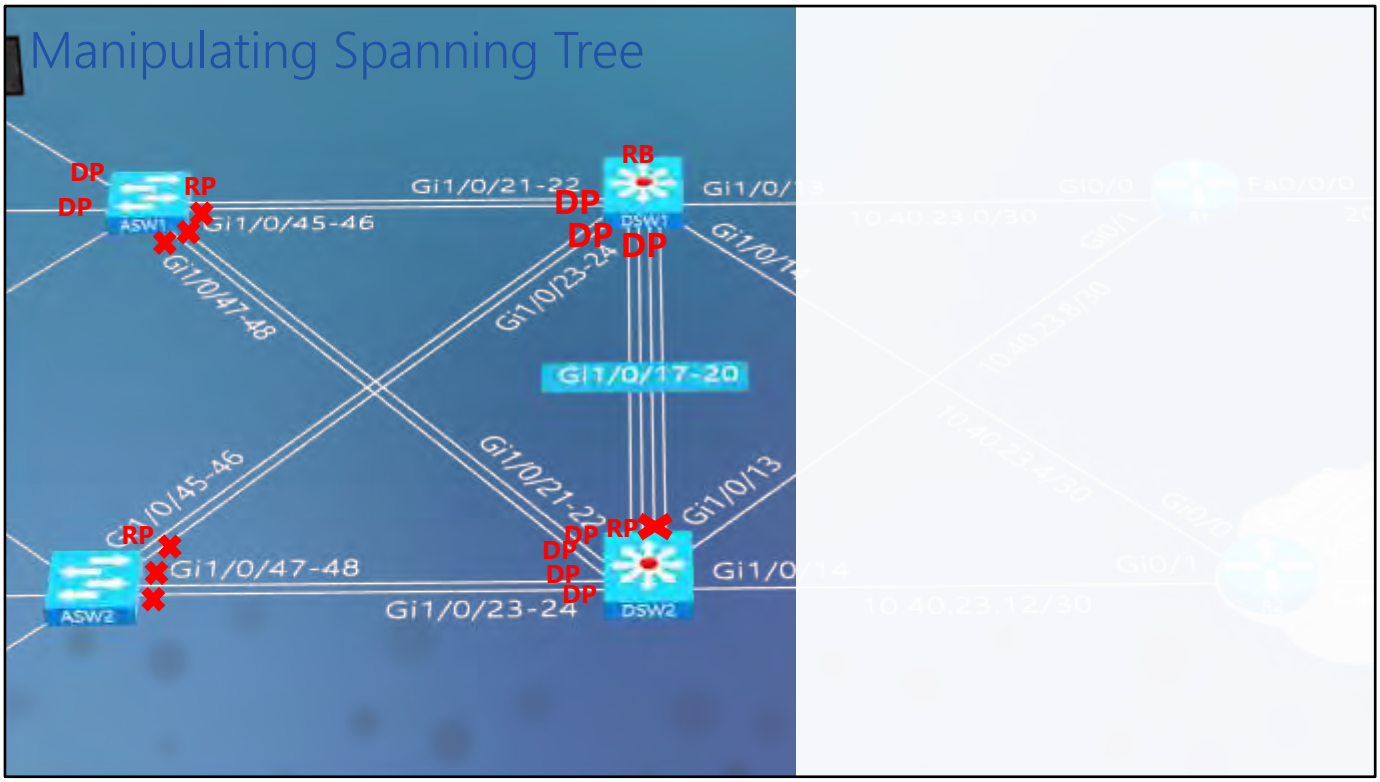



```
ASW1#configure terminal
ASW1(config)#spanning-tree mode rapid-pvst
ASW1(config)#

ASW2#configure terminal
ASW2(config)#spanning-tree mode rapid-pvst
ASW2(config)#

DSW1#configure terminal
DSW2(config)#spanning-tree mode rapid-pvst
DSW2(config)#

DSW2#configure terminal
DSW2(config)#spanning-tree mode rapid-pvst
DSW2(config)#
```

```
ASW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    32778
             Address     2c54.2d3f.e700
             Cost        4
             Port        45
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

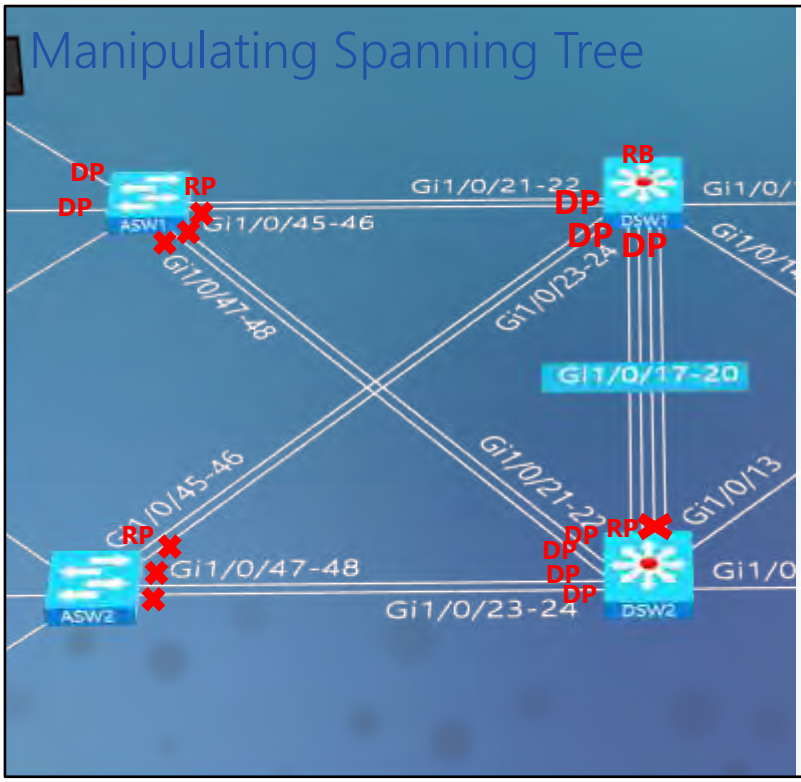
Manipulating Spanning Tree



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree



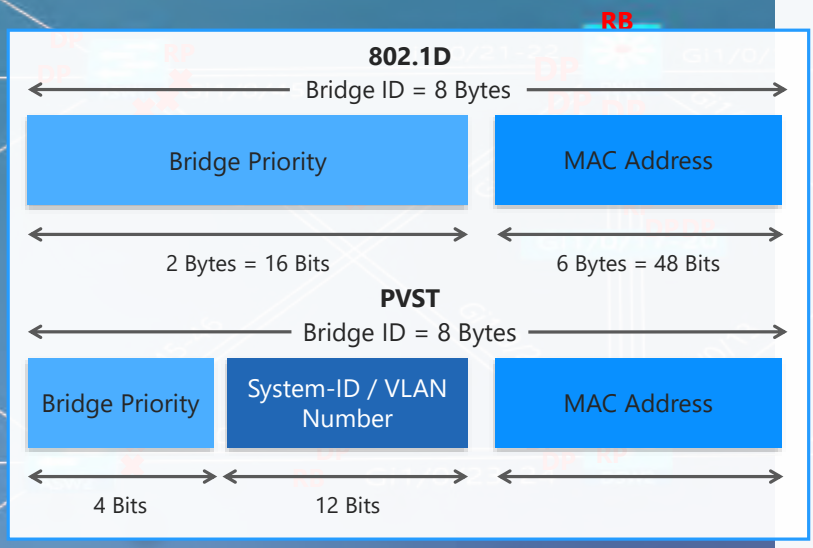
Change the Root Bridge

- Change the Bridge Priority
  - Default priority is 32768
  - Priority can be reduced in increments of 4096

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree

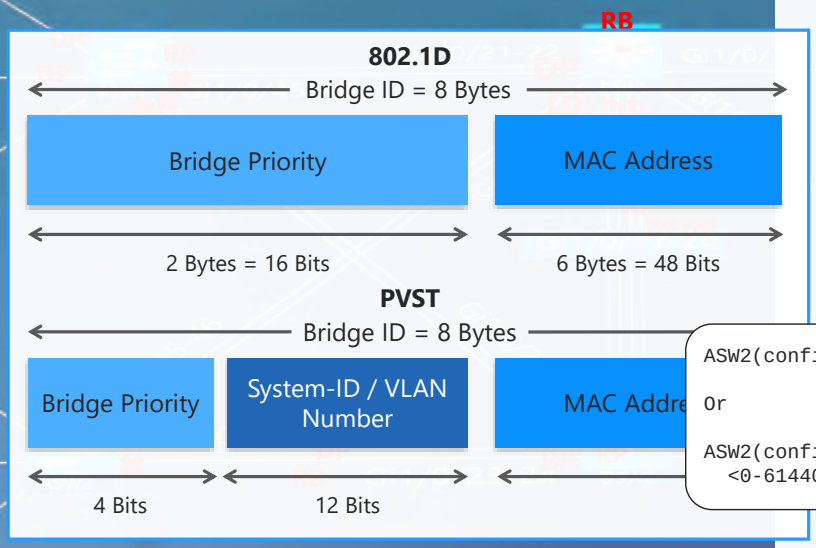


Change the Root Bridge

- Change the Bridge Priority
  - Default priority is 32768
  - **Priority can be reduced in increments of 4096**

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree



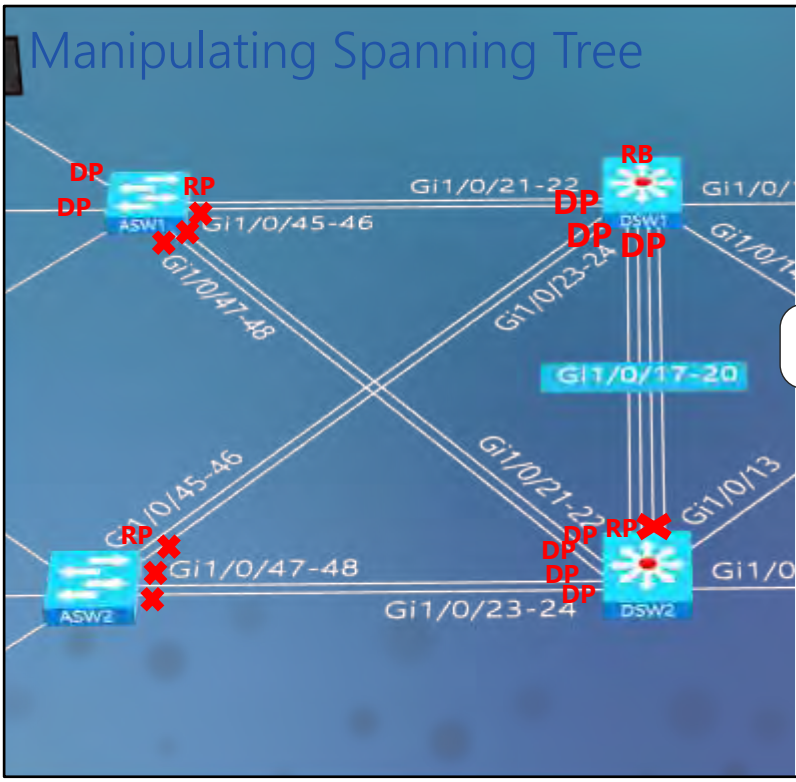
Change the Root Bridge

- Change the Bridge Priority
  - Default priority is 32768
  - Priority can be reduced in increments of 4096
- There are two ways to configure:

```
ASW2(config)#spanning-tree vlan 10 root primary

Or

ASW2(config)#spanning-tree vlan 10 priority ?
  <0-61440>  bridge priority in increments of 4096
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree

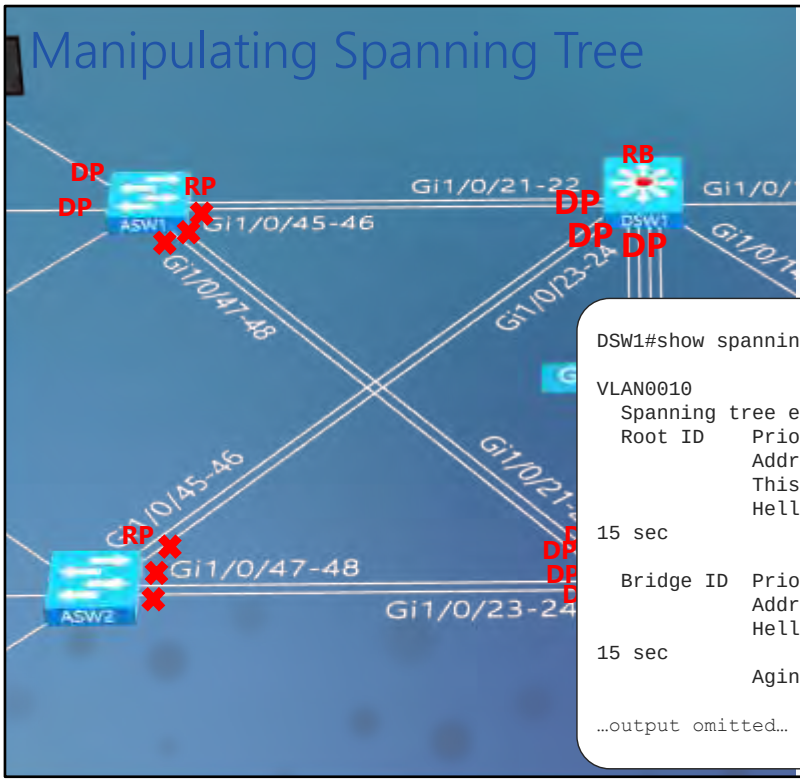


Change the Root Bridge Or Set the Root Bridge to Lowest Priority

```
DSW1#configure terminal
DSW1(config)#spanning-tree vlan 10 priority 0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree

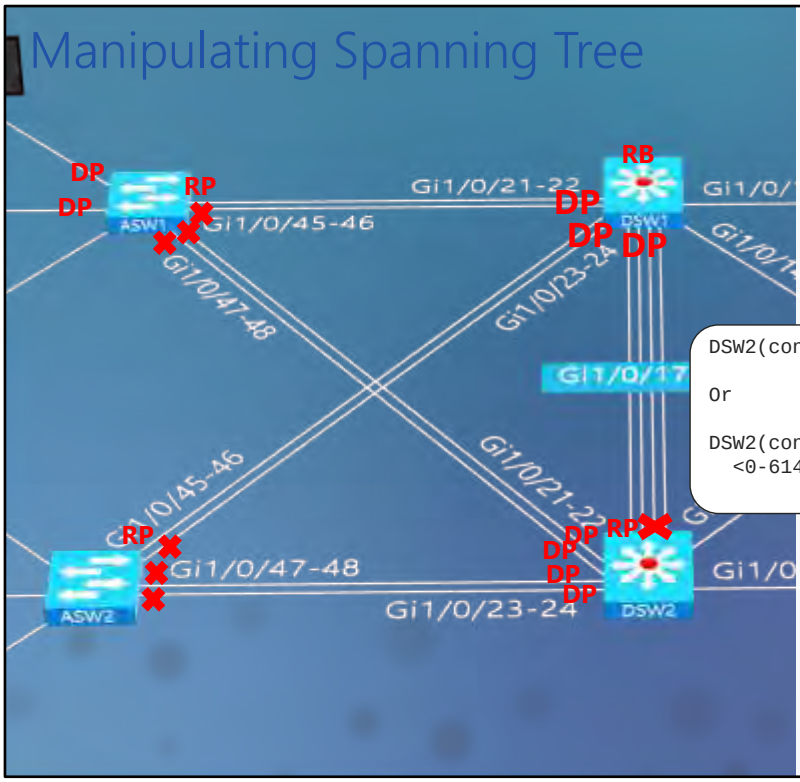


Change the Root Bridge Or Set the Root Bridge to Lowest Priority

```
DSW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol rstp
  Root ID    Priority    10
             Address     2c54.2d3f.e700
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay
15 sec

  Bridge ID  Priority    10     (priority 0 sys-id-ext 10)
             Address     2c54.2d3f.e700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay
15 sec
             Aging Time  300 sec

…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree



Secondary Root Bridge

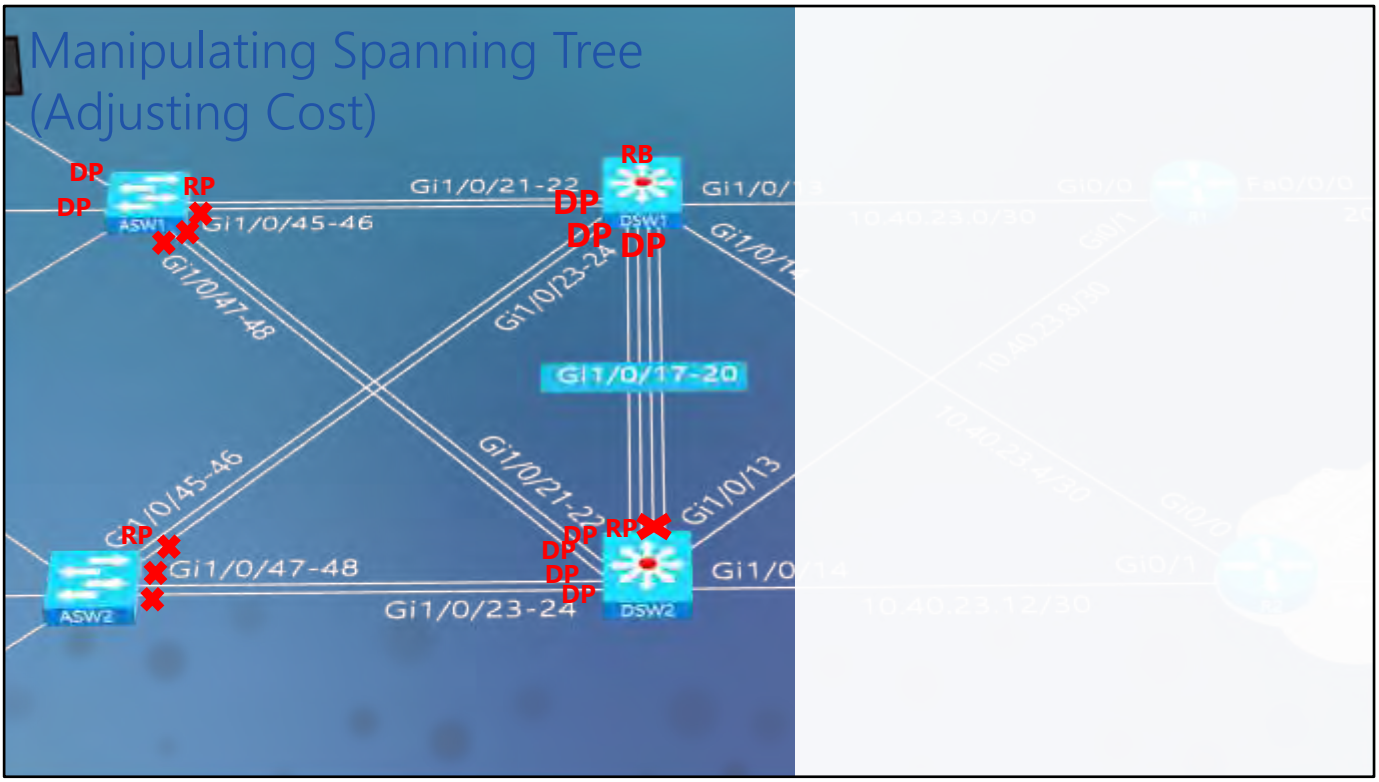
- Used as Root Bridge if primary fails
- Configure the switch with the next best priority when compared to the existing Root Bridge.

```
DSW2(config)#spanning-tree vlan 10 root secondary

Or

DSW2(config)#spanning-tree vlan 10 priority ?
  <0-61440>  bridge priority in increments of 4096
```

©2023 by StormWind LLC. All rights reserved.

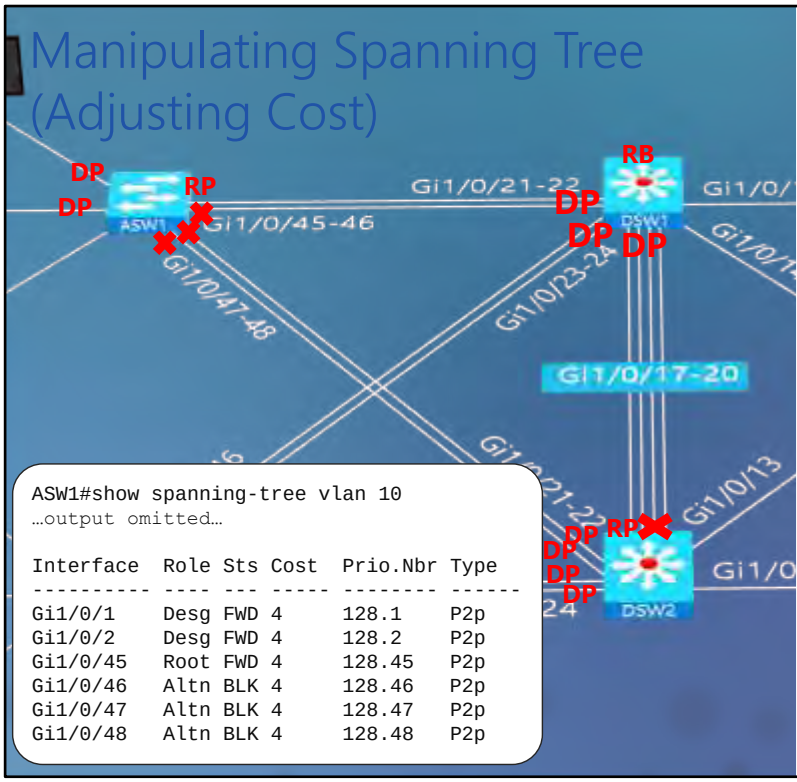
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree (Adjusting Cost)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

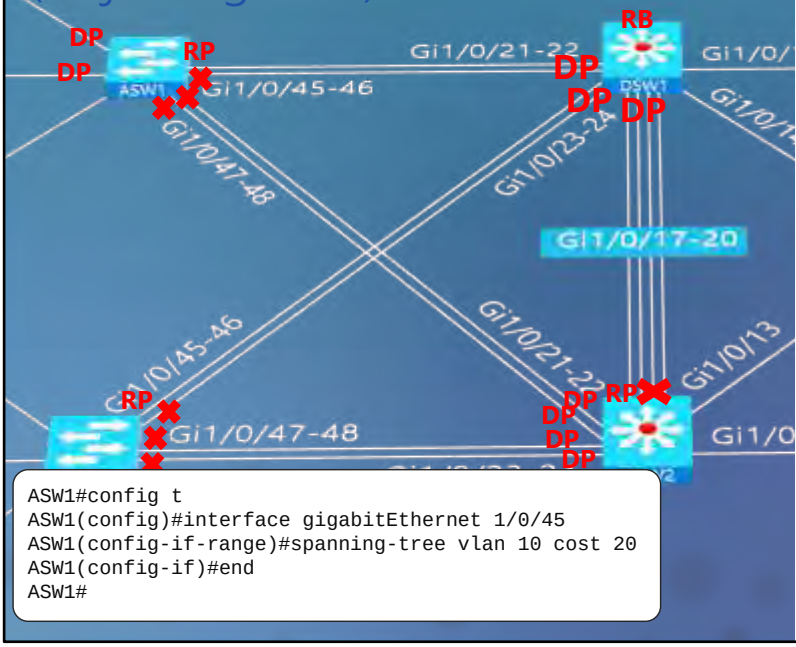
Manipulating Spanning Tree (Adjusting Cost)




```
ASW1#show spanning-tree vlan 10
…output omitted…

Interface   Role Sts Cost   Prio.Nbr Type
---------- ---- --- ----- -------- ------
Gi1/0/1     Desg FWD 4      128.1    P2p
Gi1/0/2     Desg FWD 4      128.2    P2p
Gi1/0/45    Root FWD 4      128.45   P2p
Gi1/0/46    Altn BLK 4      128.46   P2p
Gi1/0/47    Altn BLK 4      128.47   P2p
Gi1/0/48    Altn BLK 4      128.48   P2p
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

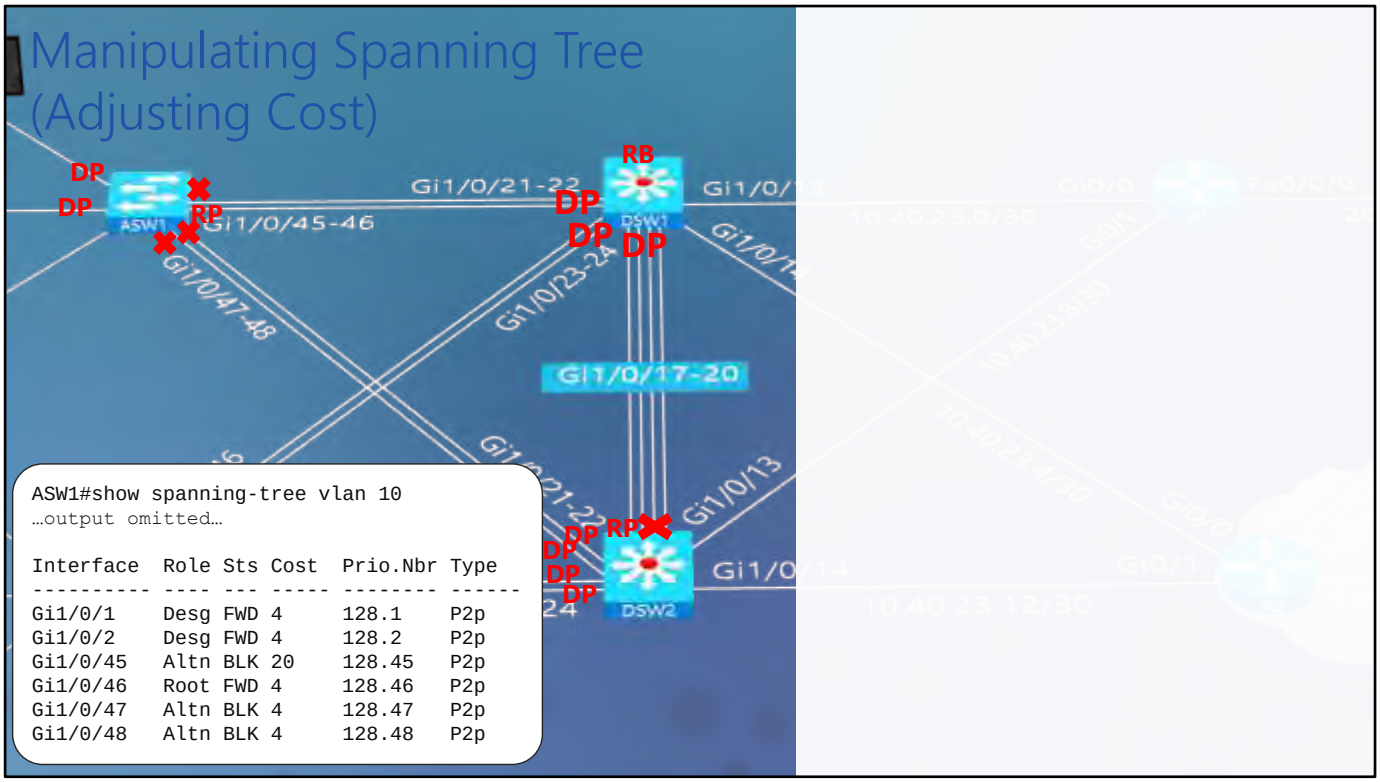
Manipulating Spanning Tree (Adjusting Cost)




```
ASW1#config t
ASW1(config)#interface gigabitEthernet 1/0/45
ASW1(config-if-range)#spanning-tree vlan 10 cost 20
ASW1(config-if)#end
ASW1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

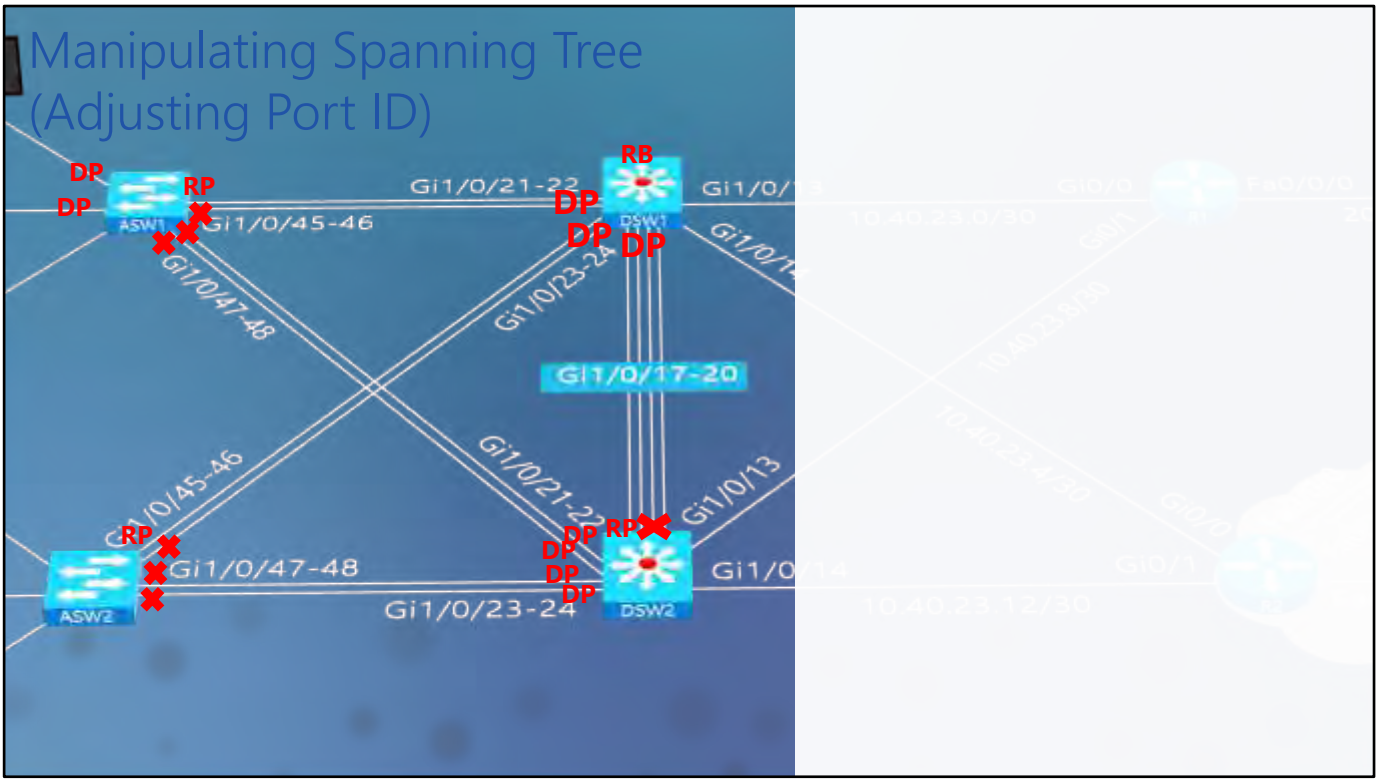
Manipulating Spanning Tree (Adjusting Cost)




```
ASW1#show spanning-tree vlan 10
…output omitted…

Interface   Role Sts Cost   Prio.Nbr Type
---------- ---- --- ----- -------- ------
Gi1/0/1     Desg FWD 4      128.1    P2p
Gi1/0/2     Desg FWD 4      128.2    P2p
Gi1/0/45    Altn BLK 20     128.45   P2p
Gi1/0/46    Root FWD 4      128.46   P2p
Gi1/0/47    Altn BLK 4      128.47   P2p
Gi1/0/48    Altn BLK 4      128.48   P2p
```

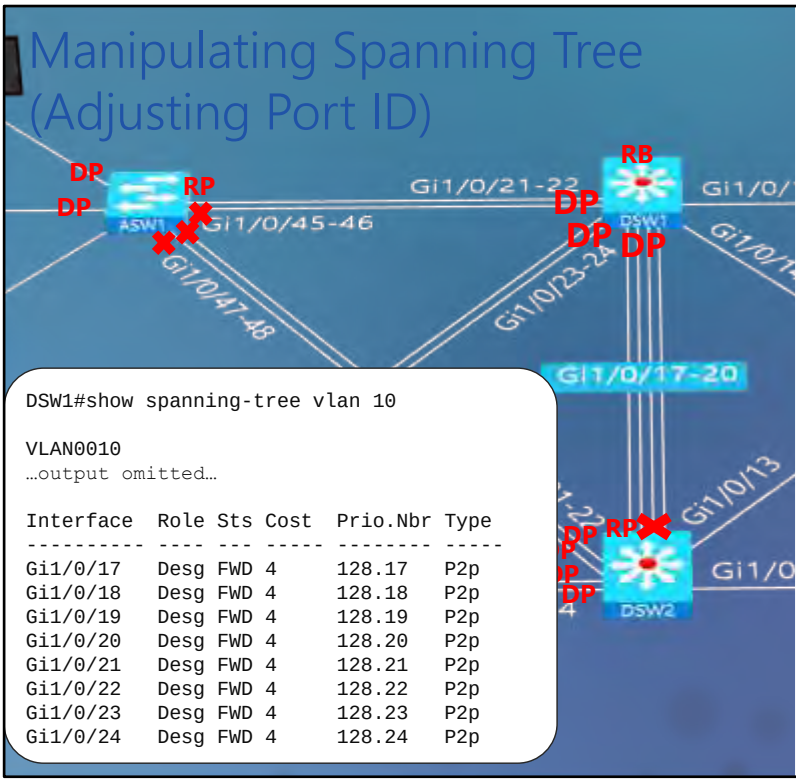
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree (Adjusting Port ID)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree (Adjusting Port ID)

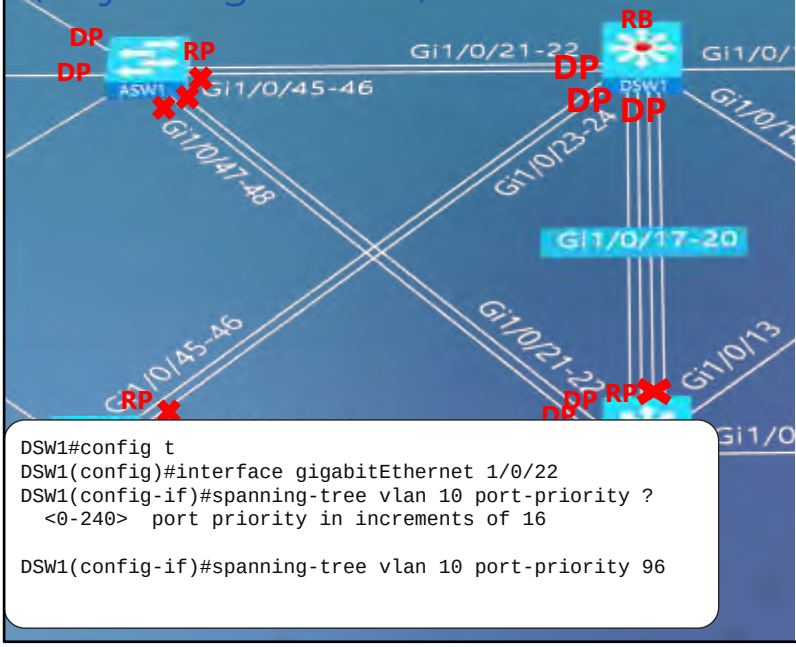



```
DSW1#show spanning-tree vlan 10

VLAN0010
…output omitted…

Interface   Role Sts Cost   Prio.Nbr Type
---------- ---- --- ----- -------- -----
Gi1/0/17    Desg FWD 4      128.17   P2p
Gi1/0/18    Desg FWD 4      128.18   P2p
Gi1/0/19    Desg FWD 4      128.19   P2p
Gi1/0/20    Desg FWD 4      128.20   P2p
Gi1/0/21    Desg FWD 4      128.21   P2p
Gi1/0/22    Desg FWD 4      128.22   P2p
Gi1/0/23    Desg FWD 4      128.23   P2p
Gi1/0/24    Desg FWD 4      128.24   P2p
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

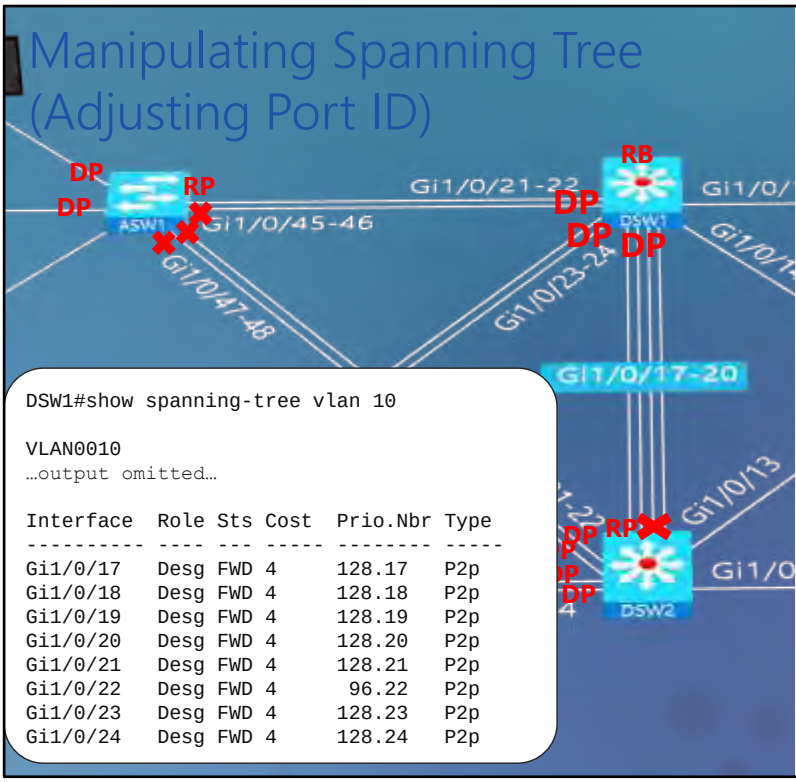
Manipulating Spanning Tree (Adjusting Port ID)




```
DSW1#config t
DSW1(config)#interface gigabitEthernet 1/0/22
DSW1(config-if)#spanning-tree vlan 10 port-priority ?
  <0-240>  port priority in increments of 16

DSW1(config-if)#spanning-tree vlan 10 port-priority 96
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating Spanning Tree (Adjusting Port ID)

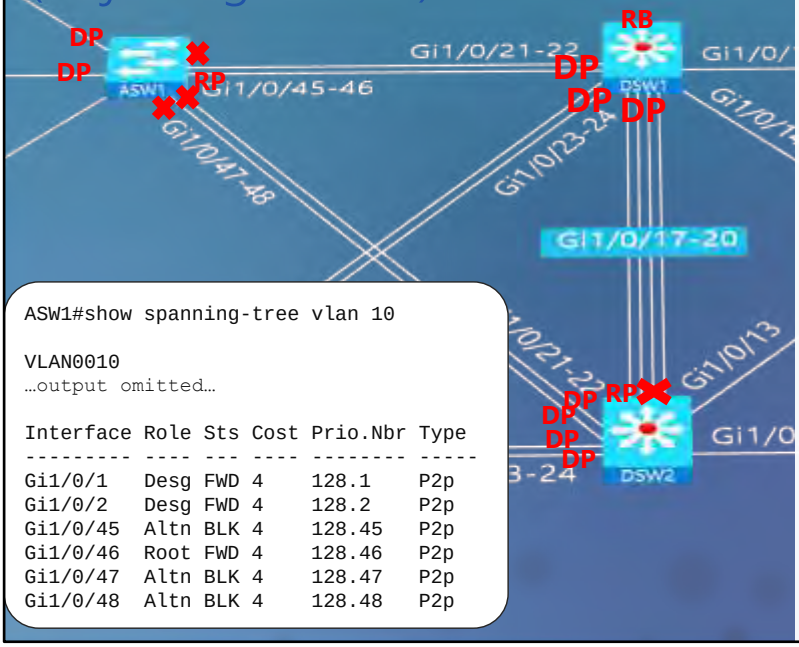



```
DSW1#show spanning-tree vlan 10

VLAN0010
…output omitted…

Interface   Role Sts Cost   Prio.Nbr Type
---------- ---- --- ----- -------- -----
Gi1/0/17    Desg FWD 4      128.17   P2p
Gi1/0/18    Desg FWD 4      128.18   P2p
Gi1/0/19    Desg FWD 4      128.19   P2p
Gi1/0/20    Desg FWD 4      128.20   P2p
Gi1/0/21    Desg FWD 4      128.21   P2p
Gi1/0/22    Desg FWD 4       96.22   P2p
Gi1/0/23    Desg FWD 4      128.23   P2p
Gi1/0/24    Desg FWD 4      128.24   P2p
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

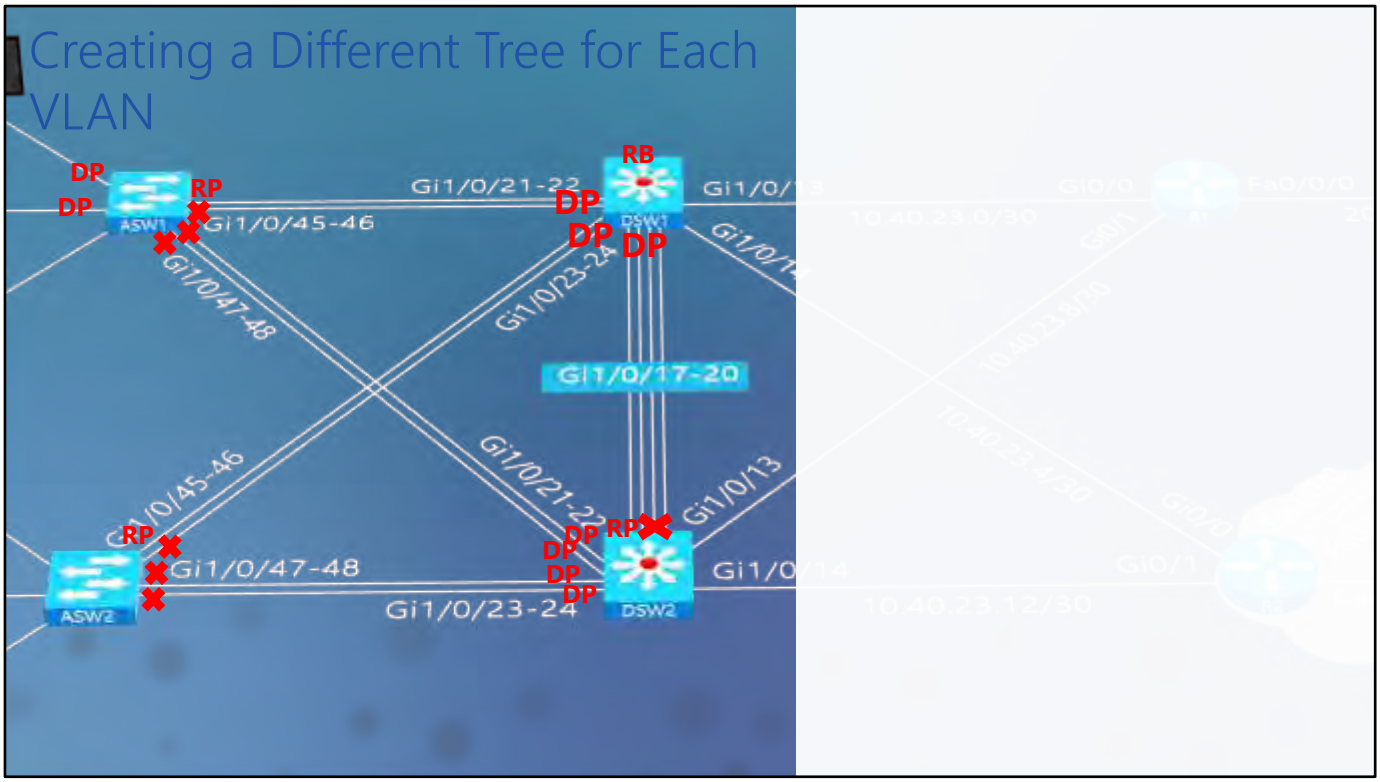
Manipulating Spanning Tree (Adjusting Port ID)




```
ASW1#show spanning-tree vlan 10

VLAN0010
…output omitted…

Interface Role Sts Cost Prio.Nbr Type
--------- ---- --- ---- -------- -----
Gi1/0/1   Desg FWD 4    128.1    P2p
Gi1/0/2   Desg FWD 4    128.2    P2p
Gi1/0/45  Altn BLK 4    128.45   P2p
Gi1/0/46  Root FWD 4    128.46   P2p
Gi1/0/47  Altn BLK 4    128.47   P2p
Gi1/0/48  Altn BLK 4    128.48   P2p
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

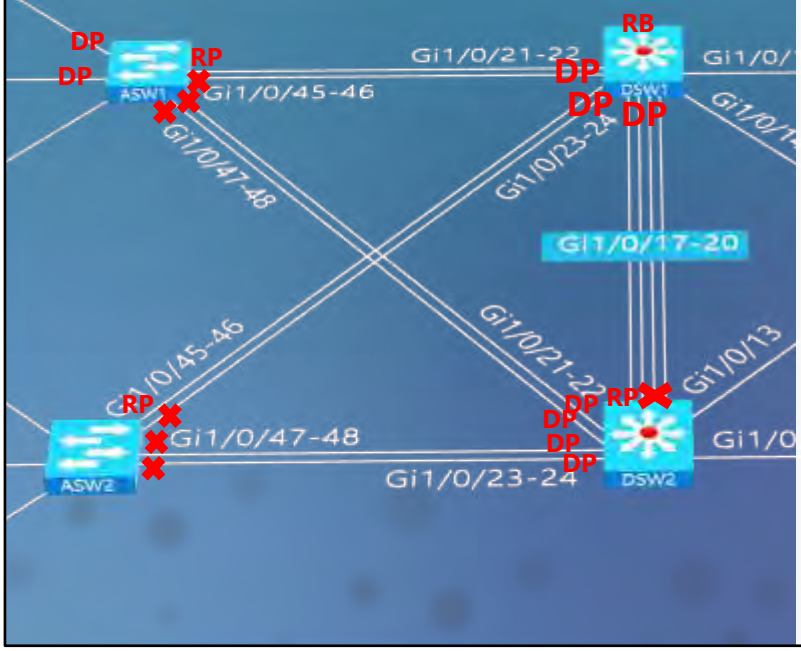
Creating a Different Tree for Each VLAN



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Creating a Different Tree for Each VLAN



Allows for "balancing" of traffic in the Layer 2 network

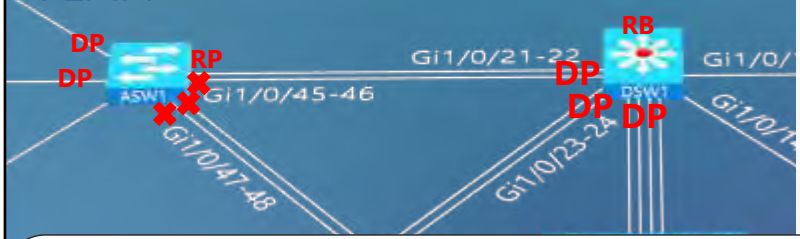
Consider VLAN 50:

- If DSW1 is configured as the Root Bridge, the exact same tree will be created as we see here.
- However, if DSW2 is configured as the Root Bridge for VLAN 50 then a different tree is built, and traffic would flow through DSW2 instead of DSW1.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Creating a Different Tree for Each VLAN




```
DSW1#show span vlan 50

VLAN0050
  Spanning tree enabled protocol rstp
  Root ID    Priority    32818
             Address     2c54.2d3f.e700
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32818  (priority 32768 sys-id-ext 50)
             Address     2c54.2d3f.e700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

…output omitted…
```

Allows for "balancing" of traffic in the Layer 2 network

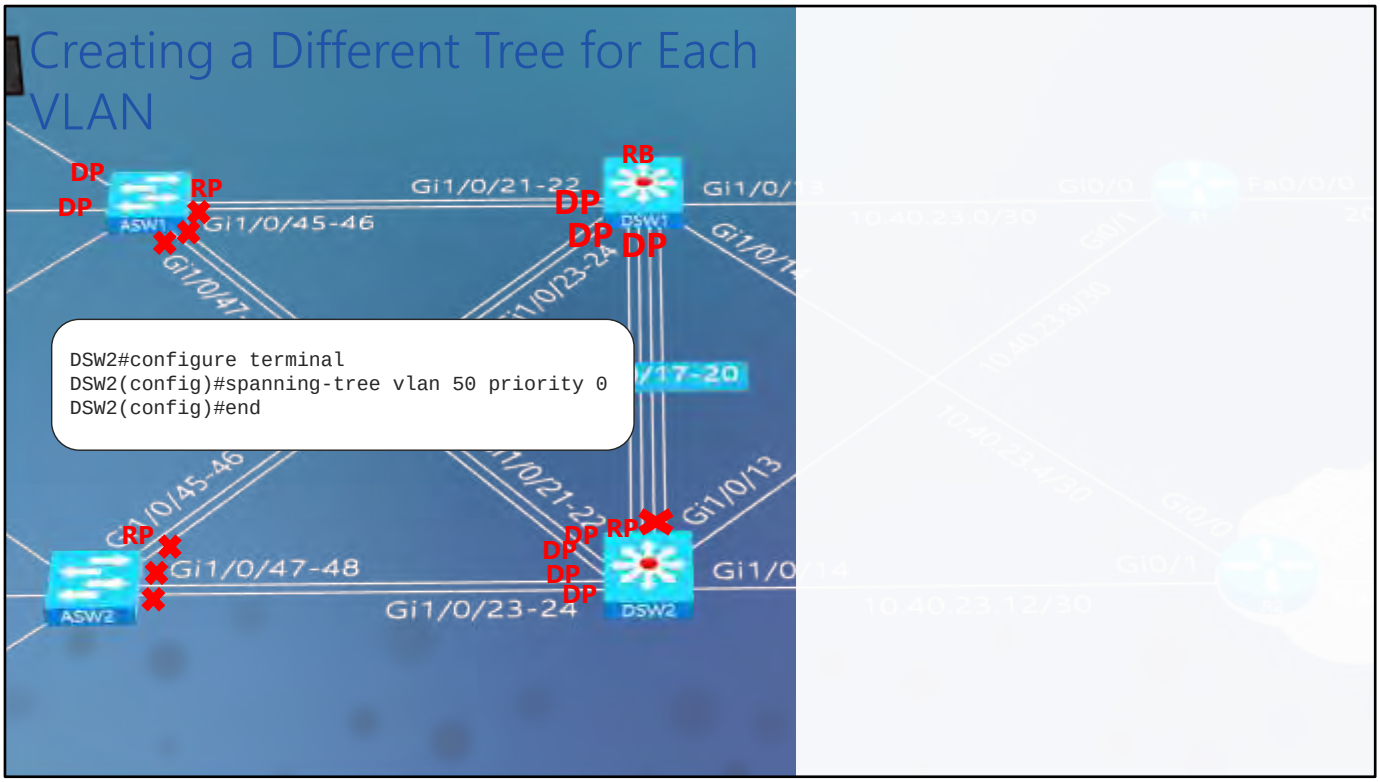
Consider VLAN 50:

- If DSW1 is configured as the Root Bridge, the exact same tree will be created as we see here.
- However, if DSW2 is configured as the Root Bridge for VLAN 50 then a different tree is built, and traffic would flow through DSW2 instead of DSW1.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

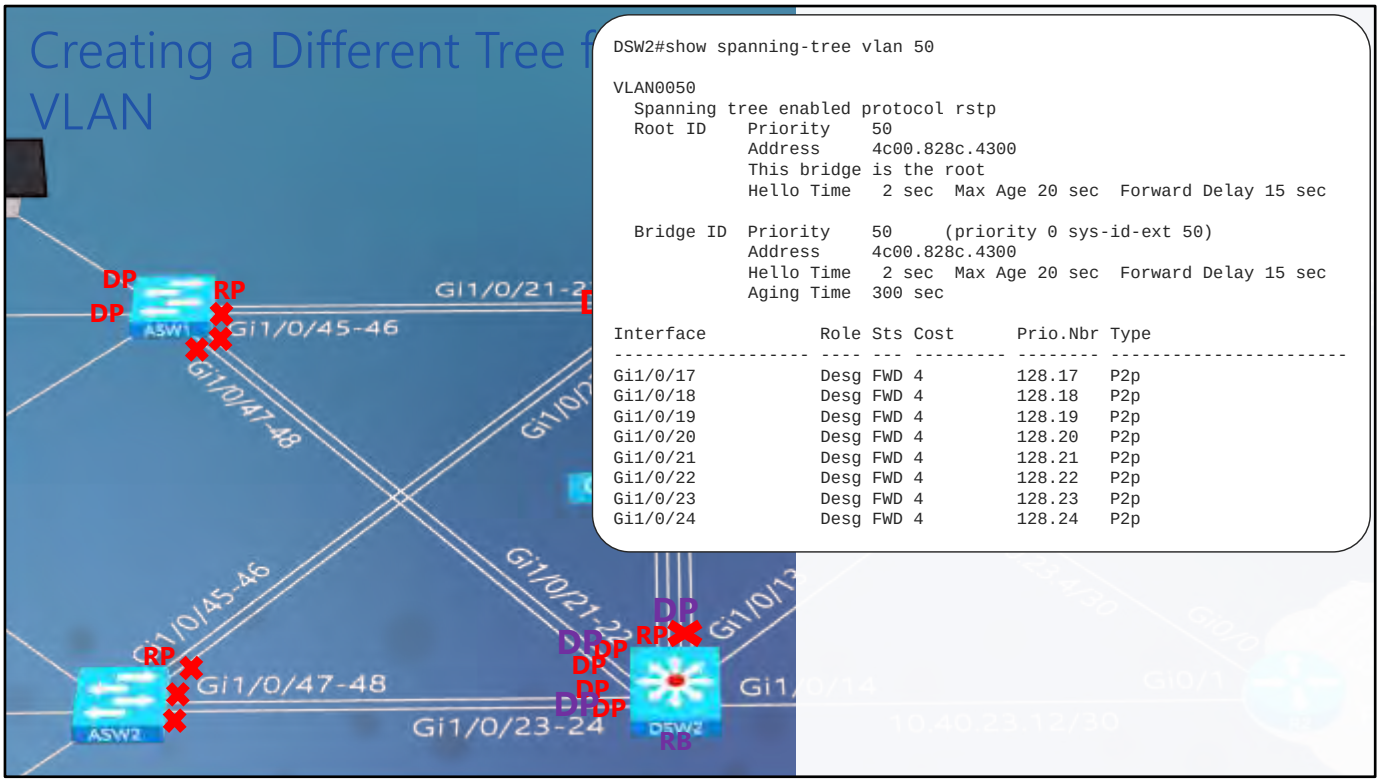
Creating a Different Tree for Each VLAN




```
DSW2#configure terminal
DSW2(config)#spanning-tree vlan 50 priority 0
DSW2(config)#end
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

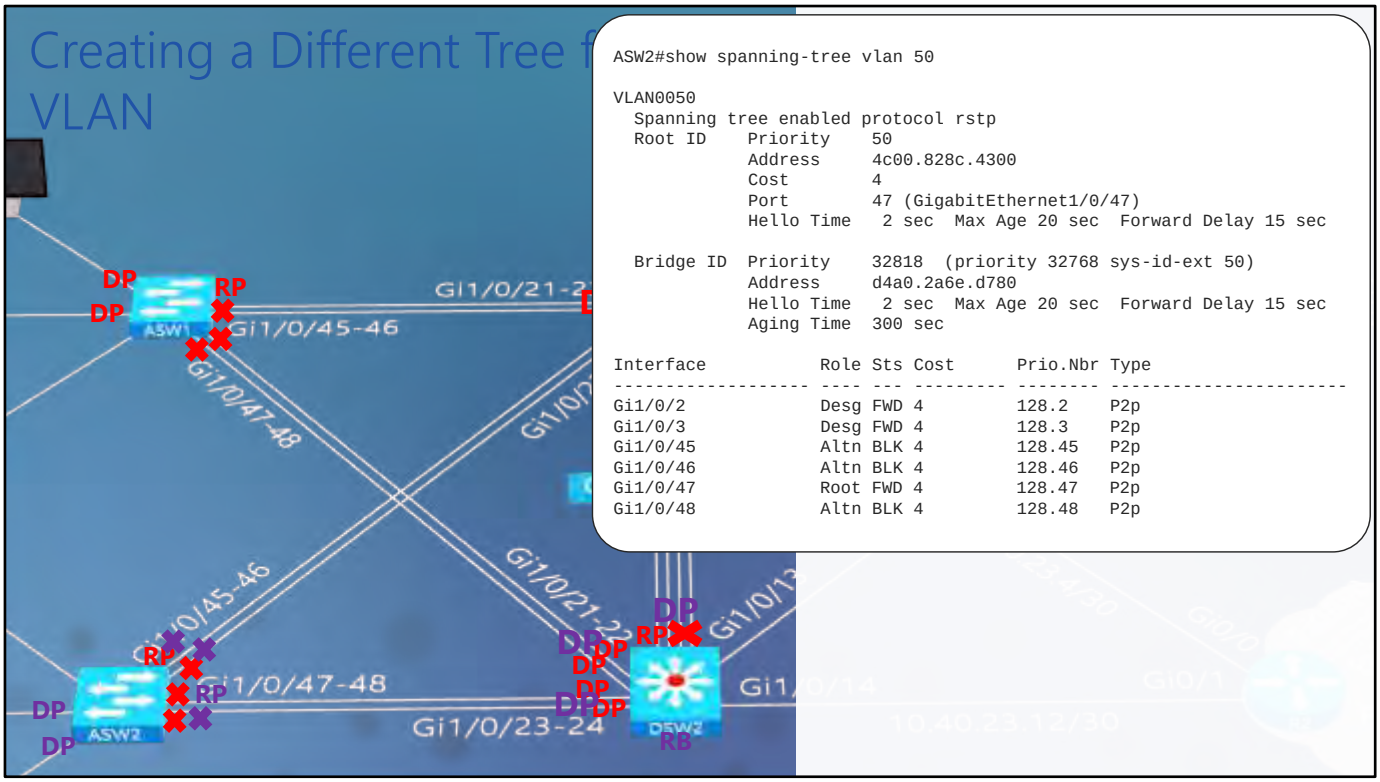
Creating a Different Tree f
VLAN




```
DSW2#show spanning-tree vlan 50

VLAN0050
  Spanning tree enabled protocol rstp
  Root ID    Priority    50
             Address     4c00.828c.4300
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    50     (priority 0 sys-id-ext 50)
             Address     4c00.828c.4300
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Gi1/0/17            Desg FWD 4         128.17   P2p
Gi1/0/18            Desg FWD 4         128.18   P2p
Gi1/0/19            Desg FWD 4         128.19   P2p
Gi1/0/20            Desg FWD 4         128.20   P2p
Gi1/0/21            Desg FWD 4         128.21   P2p
Gi1/0/22            Desg FWD 4         128.22   P2p
Gi1/0/23            Desg FWD 4         128.23   P2p
Gi1/0/24            Desg FWD 4         128.24   P2p
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

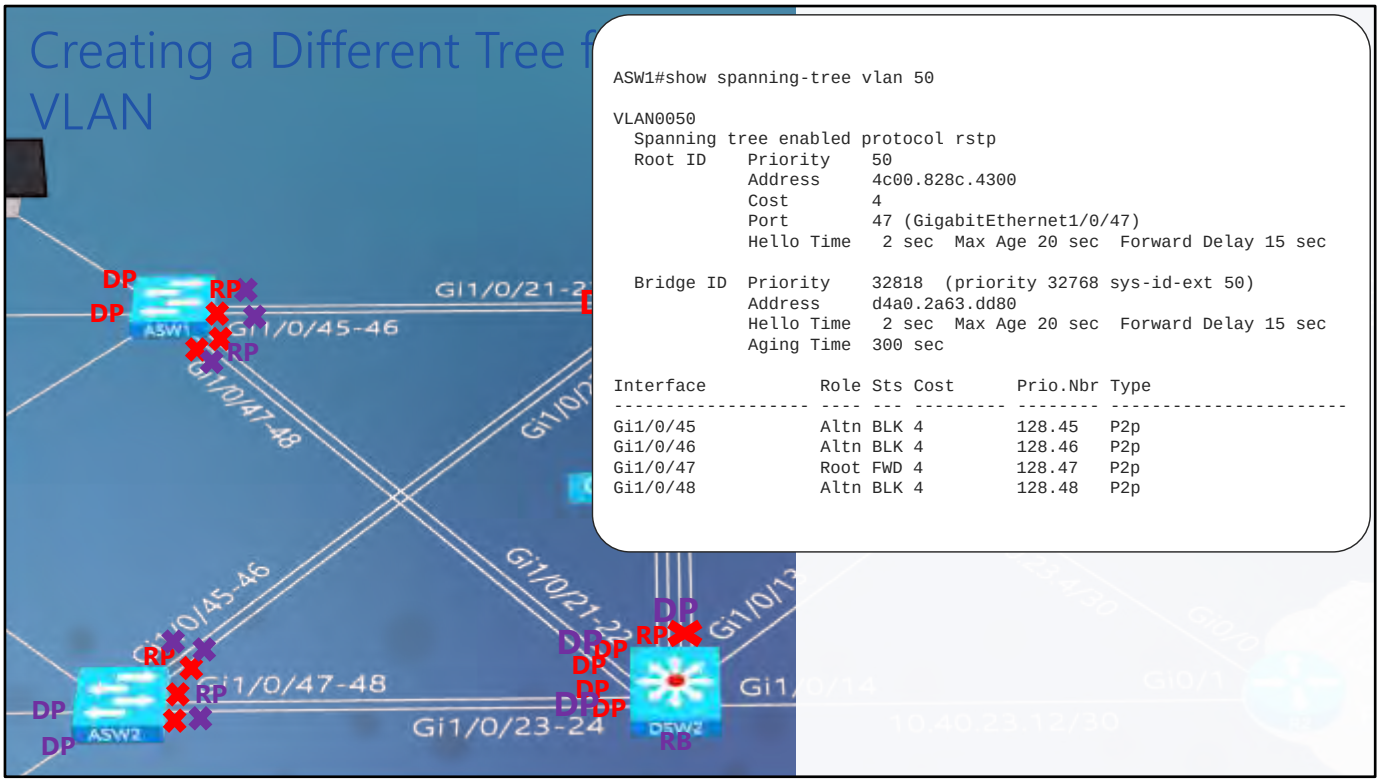
Creating a Different Tree f
VLAN




```
ASW2#show spanning-tree vlan 50

VLAN0050
  Spanning tree enabled protocol rstp
  Root ID    Priority    50
             Address     4c00.828c.4300
             Cost        4
             Port        47 (GigabitEthernet1/0/47)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32818  (priority 32768 sys-id-ext 50)
             Address     d4a0.2a6e.d780
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ------------------------
Gi1/0/2             Desg FWD 4         128.2    P2p
Gi1/0/3             Desg FWD 4         128.3    P2p
Gi1/0/45            Altn BLK 4         128.45   P2p
Gi1/0/46            Altn BLK 4         128.46   P2p
Gi1/0/47            Root FWD 4         128.47   P2p
Gi1/0/48            Altn BLK 4         128.48   P2p
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

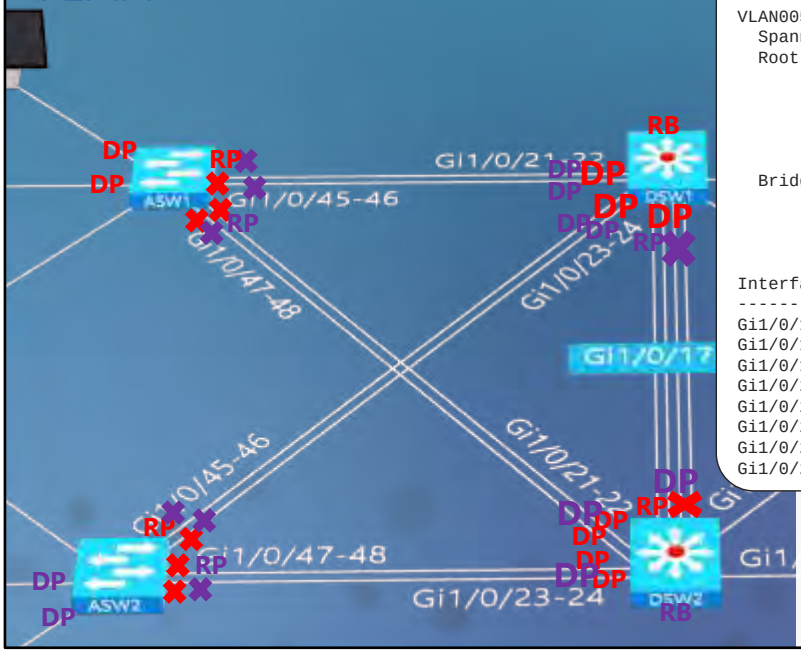
Creating a Different Tree f
VLAN




```
ASW1#show spanning-tree vlan 50

VLAN0050
  Spanning tree enabled protocol rstp
  Root ID    Priority    50
             Address     4c00.828c.4300
             Cost        4
             Port        47 (GigabitEthernet1/0/47)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32818  (priority 32768 sys-id-ext 50)
             Address     d4a0.2a63.dd80
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ----------------------
Gi1/0/45            Altn BLK 4         128.45   P2p
Gi1/0/46            Altn BLK 4         128.46   P2p
Gi1/0/47            Root FWD 4         128.47   P2p
Gi1/0/48            Altn BLK 4         128.48   P2p
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Creating a Different Tree for Each VLAN

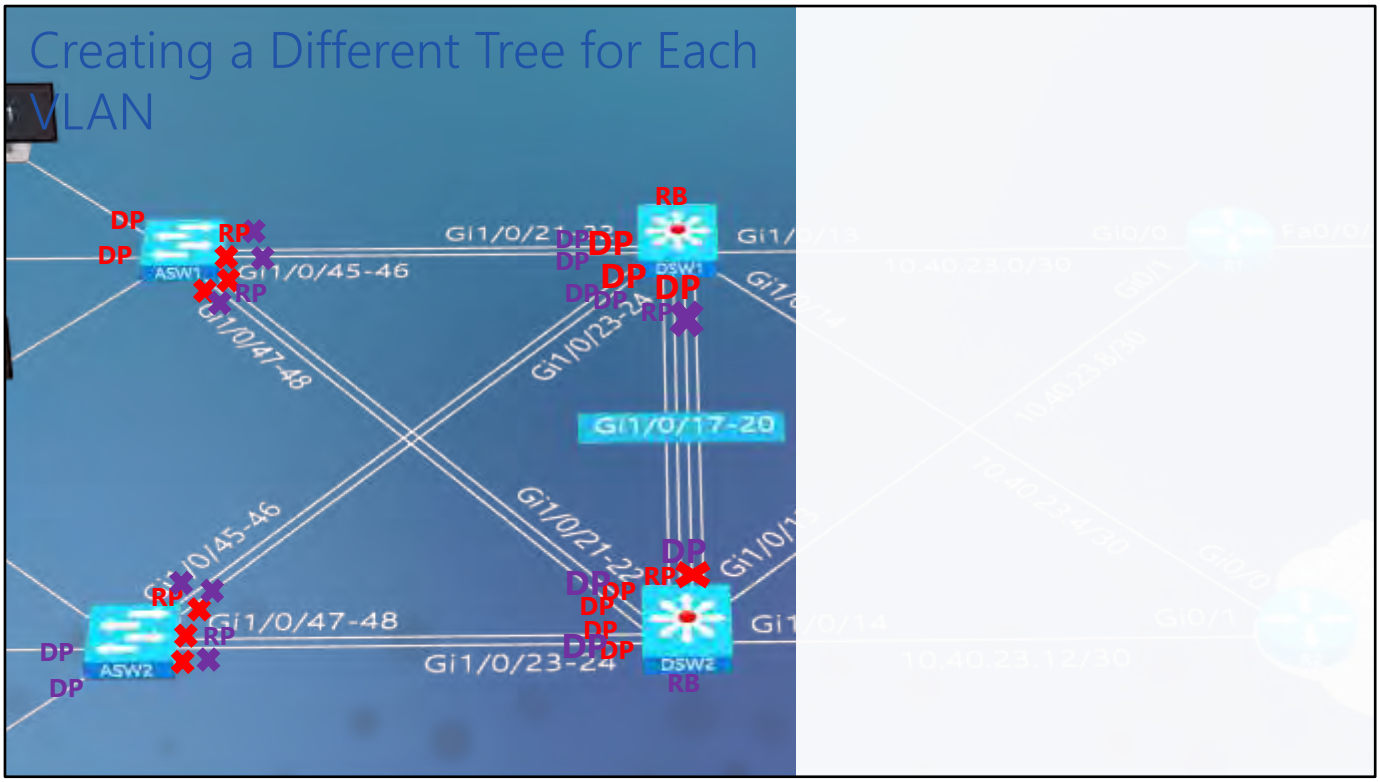



```
DSW1#show span vlan 50

VLAN0050
  Spanning tree enabled protocol rstp
  Root ID    Priority    50
             Address     4c00.828c.4300
             Cost        4
             Port        17 (GigabitEthernet1/0/17)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay

  Bridge ID  Priority    32818  (priority 32768 sys-id-ext 50)
             Address     2c54.2d3f.e700
             Hello Time   2 sec  Max Age 20 sec  Forward Delay
             Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- ----------
Gi1/0/17            Root FWD 4         128.17   P2p
Gi1/0/18            Altn BLK 4         128.18   P2p
Gi1/0/19            Altn BLK 4         128.19   P2p
Gi1/0/20            Altn BLK 4         128.20   P2p
Gi1/0/21            Desg FWD 4         128.21   P2p
Gi1/0/22            Desg FWD 4         128.22   P2p
Gi1/0/23            Desg FWD 4         128.23   P2p
Gi1/0/24            Desg FWD 4         128.24   P2p
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Creating a Different Tree for Each VLAN



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

STP PortFast, BPDU Guard, BPDU Filter, and Root Guard

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring PortFast and BPDUGuard

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PortFast and BPDUGuard

PortFast	Improves convergence time - Bypasses listening and learning states - Places port into a forwarding state Reduces STP messages when port enabled or disabled
BPDU Guard	Improves security - Shuts down the port, if BPDU is received Used in conjunction with PortFast

***Used on Access Ports

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring PortFast and BPDUGuard

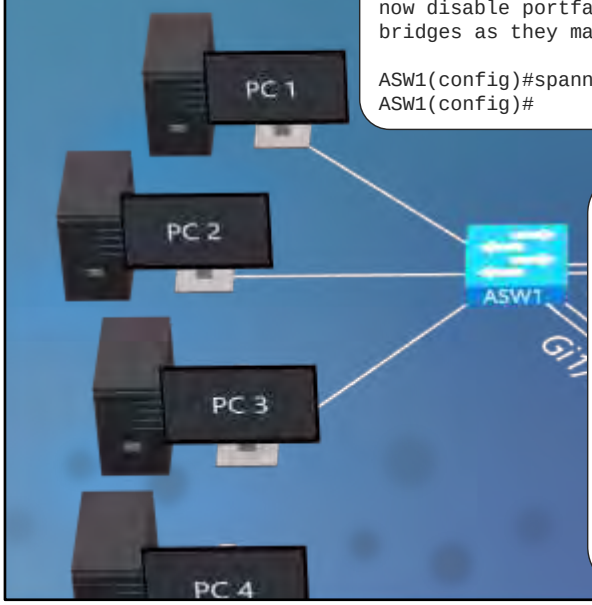
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring PortFast and BPDUGuard

```
ASW1#configure terminal
ASW1(config)#spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You should
now disable portfast explicitly on switched ports leading to hubs, switches and
bridges as they may create temporary bridging loops.

ASW1(config)#spanning-tree portfast bpduguard default
ASW1(config)#
```

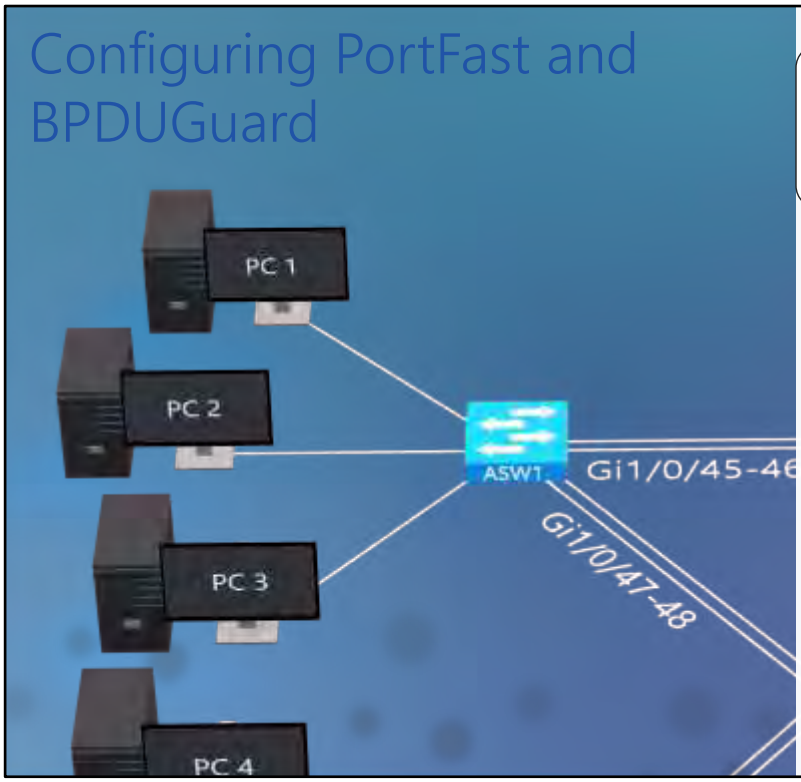
OR

```
ASW1#configure terminal
ASW1(config)#interface range gigabitEthernet 1/0/1-3
ASW1(config-if-range)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected
to a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface  when portfast is enabled,
can cause temporary bridging loops. Use with CAUTION

%Portfast will be configured in 3 interfaces due to the
range command
 but will only have effect when the interfaces are in a non-
trunking mode.

ASW1(config-if-range)#spanning-tree bpduguard enable
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

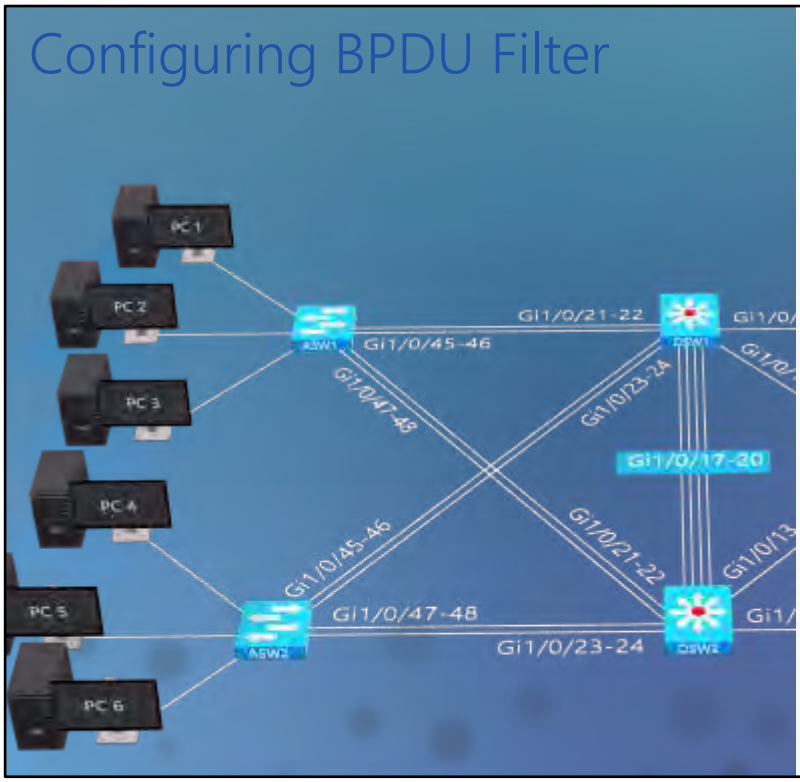
Configuring PortFast and BPDUGuard




```
ASW1#configure terminal
ASW1(config)#interface gigabitethernet 1/0/1
ASW1(config-if)#switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring BPDU Filter



BPDU Filter

Filters BPDUs in and out of an interface

Options:

Globally

spanning-tree portfast bpdufilter default

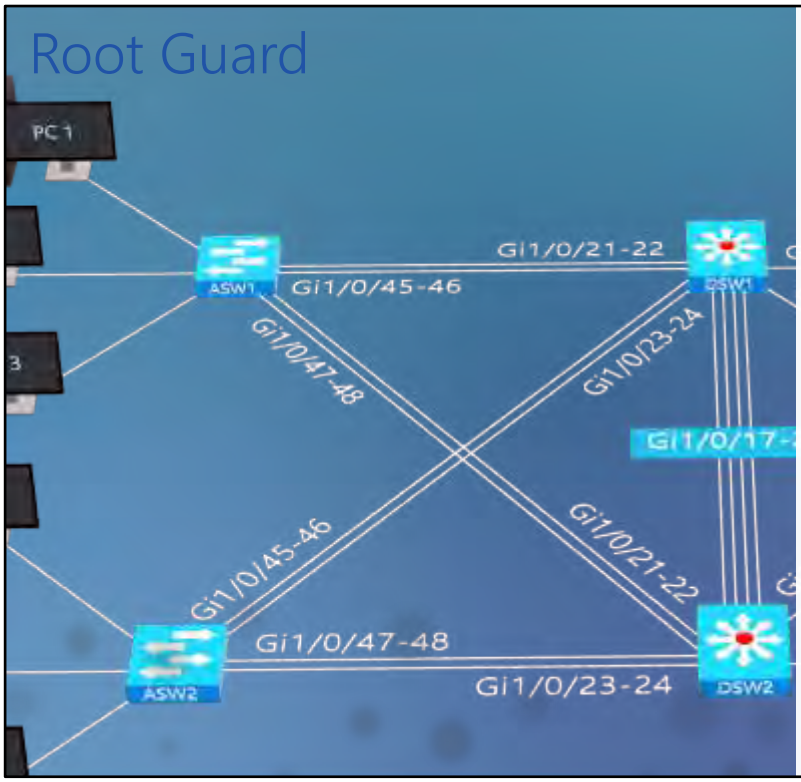
Interface

spanning-tree bpdufilter enable

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Root Guard



Protect who the root bridge is by making sure that if a superior BPDU arrives on a Root Guard enabled interface, that interface will be placed in the root inconsistent state.

This will ensure that the RB remains the root bridge as the superior BPDU does not affect the RB decision.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol (MSTP)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol

Consider a network with 1000 VLANS

802.1W = 1 STP tree total for all 1000 VLANs = 1 STP tree

RPVST+ = 1 STP tree per VLAN = 1000 STP trees

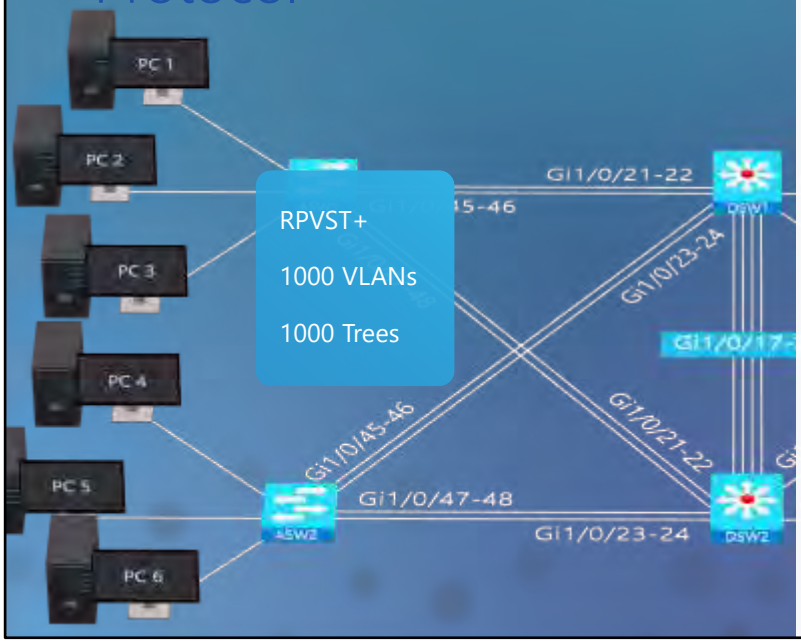
MSTP (802.1s) = X VLANs per STP tree

- Build trees and place whatever VLANs you want in them
- Reducing the total number of trees

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol



Consider a network with 1000 VLANS

802.1W = 1 STP tree total for all 1000 VLANs = 1 STP tree

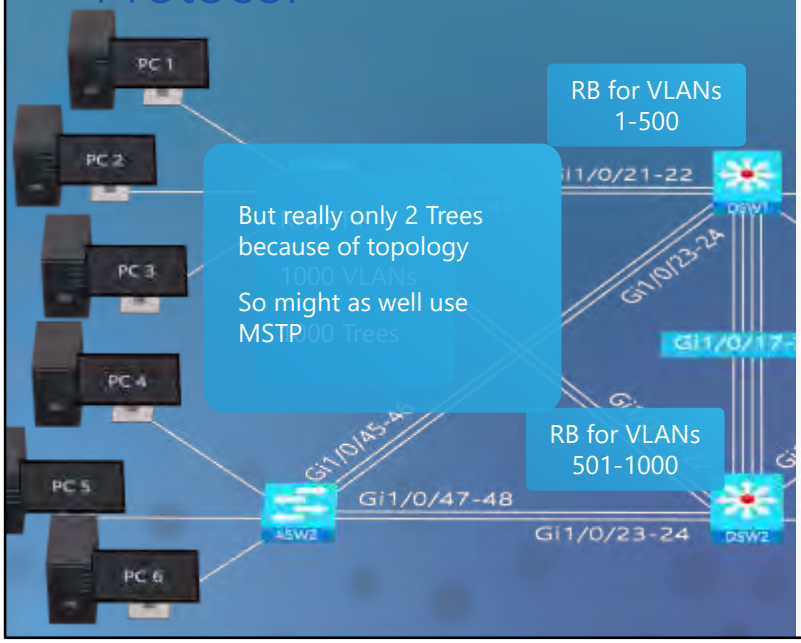
RPVST+ = 1 STP tree per VLAN = 1000 STP trees

MSTP (802.1s) = X VLANs per STP tree

- Build trees and place whatever VLANs you want in them
- Reducing the total number of trees

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol



Consider a network with 1000 VLANS

802.1W = 1 STP tree total for all 1000 VLANs = 1 STP tree

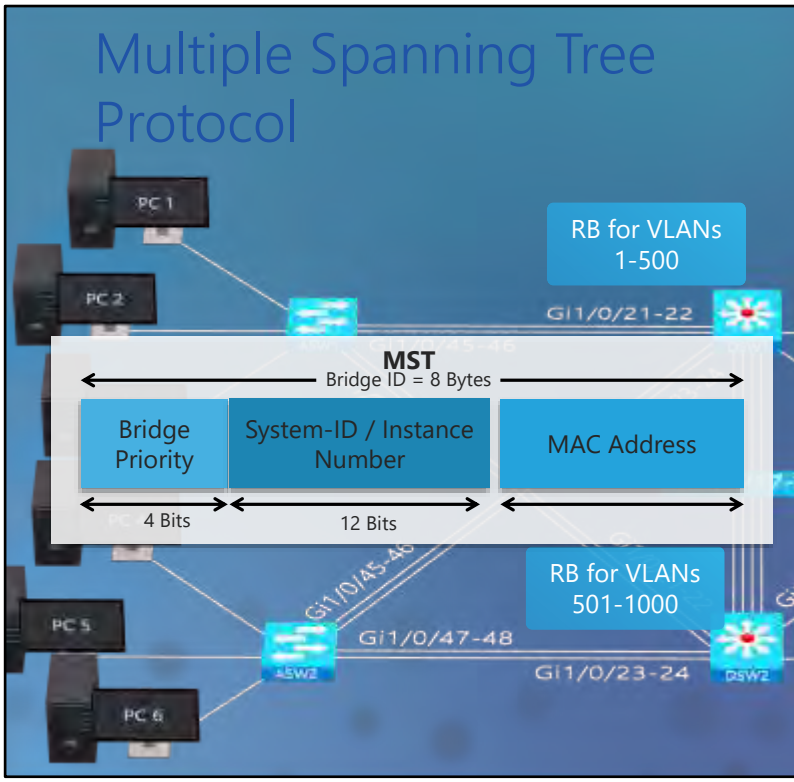
RPVST+ = 1 STP tree per VLAN = 1000 STP trees

MSTP (802.1s) = X VLANs per STP tree

- Build trees and place whatever VLANs you want in them
- Reducing the total number of trees

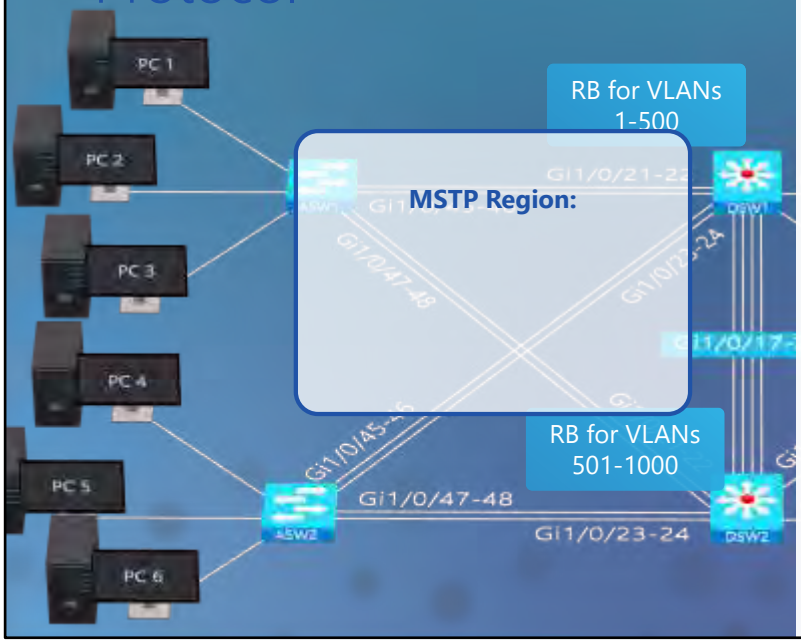
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol



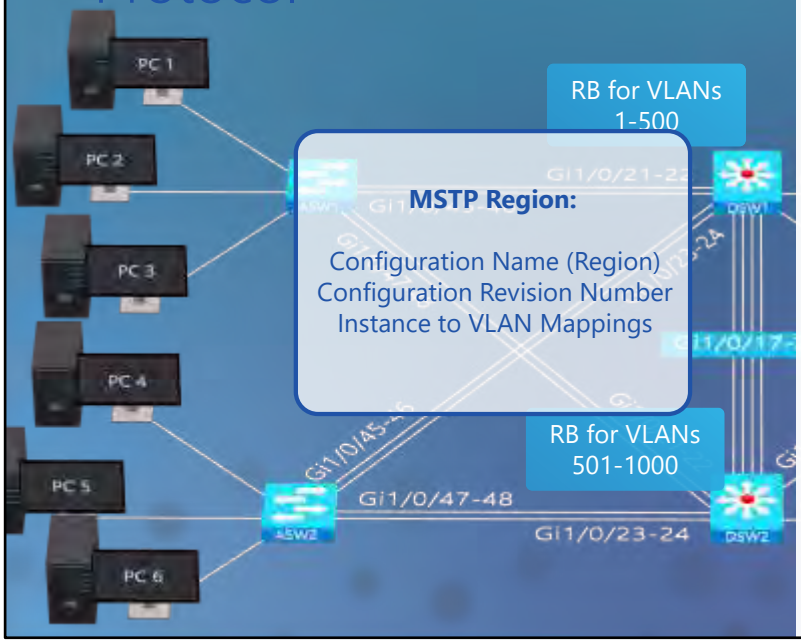
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol



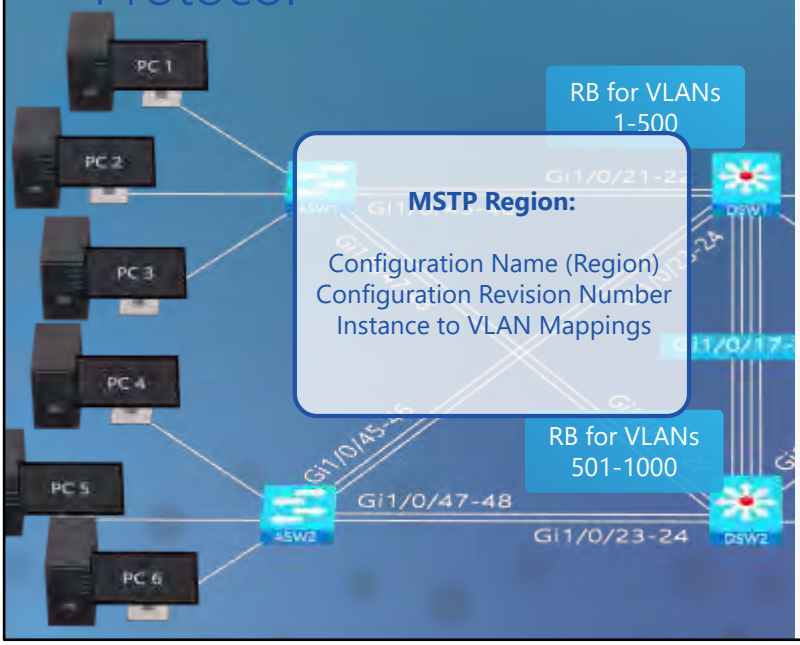
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol




```
DSW1#configure terminal
DSW1(config)#spanning-tree mst configuration
DSW1(config-mst)#revision 4
DSW1(config-mst)#name ENCORE
DSW1(config-mst)#instance 1 vlan 1-500
DSW1(config-mst)#instance 2 vlan 501-1000
```

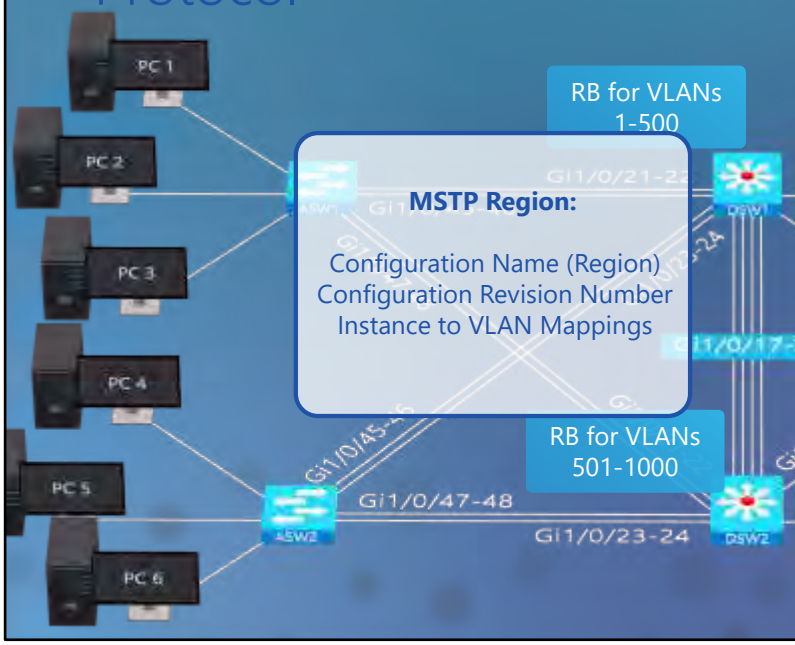
```
DSW2#configure terminal
DSW2(config)#spanning-tree mst configuration
DSW2(config-mst)#revision 4
DSW2(config-mst)#name ENCORE
DSW2(config-mst)#instance 1 vlan 1-500
DSW2(config-mst)#instance 2 vlan 501-1000
```

```
ASW1#configure terminal
ASW1(config)#spanning-tree mst configuration
ASW1(config-mst)#revision 4
ASW1(config-mst)#name ENCORE
ASW1(config-mst)#instance 1 vlan 1-500
ASW1(config-mst)#instance 2 vlan 501-1000
```

```
ASW2#configure terminal
ASW2(config)#spanning-tree mst configuration
ASW2(config-mst)#revision 4
ASW2(config-mst)#name ENCORE
ASW2(config-mst)#instance 1 vlan 1-500
ASW2(config-mst)#instance 2 vlan 501-1000
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

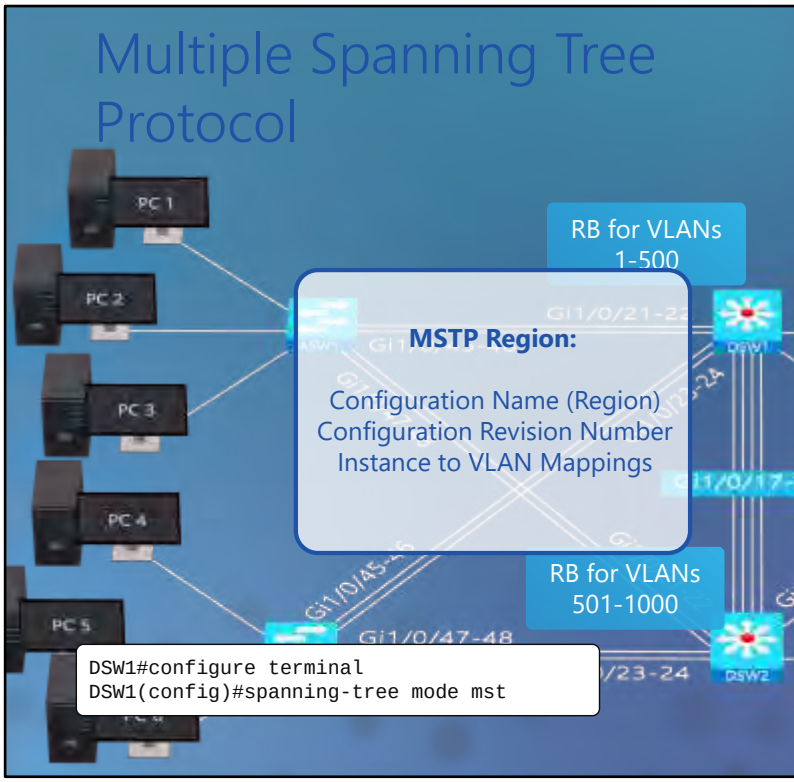
Multiple Spanning Tree Protocol




```
DSW1#show spanning-tree mst configuration
% Switch is not in mst mode
Name      [ENCORE]
Revision  4     Instances configured 3

Instance  Vlans mapped
--------  -------------------------------
0         1001-4094
1         1-500
2         501-1000
---------------------------------------
DSW1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

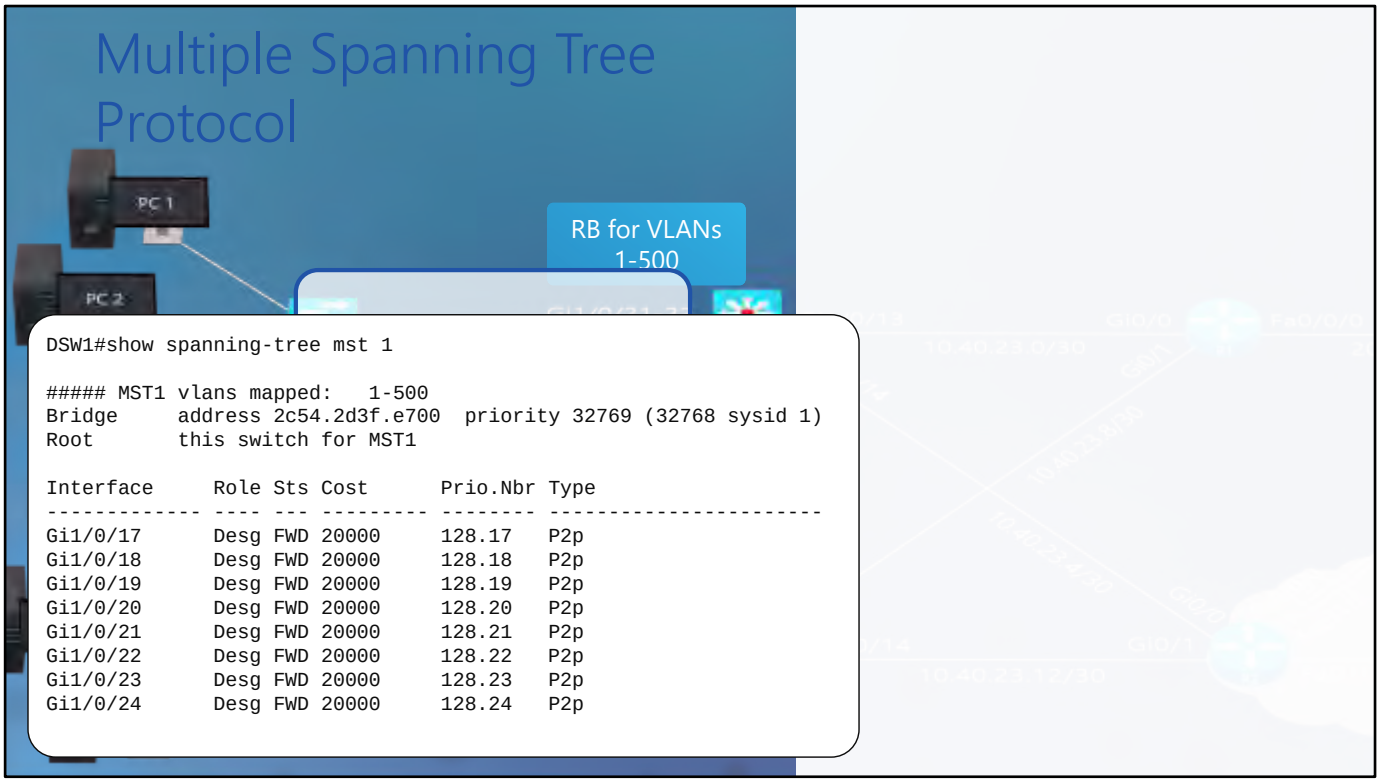
Multiple Spanning Tree Protocol




```
DSW1#configure terminal
DSW1(config)#spanning-tree mode mst
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

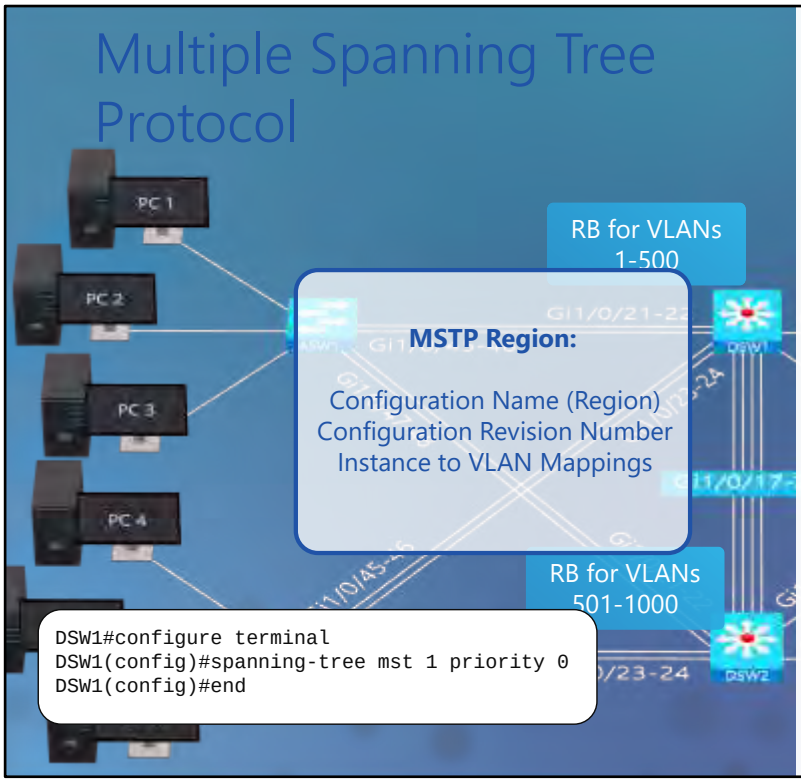
Multiple Spanning Tree Protocol




```
DSW1#show spanning-tree mst 1

##### MST1 vlans mapped:   1-500
Bridge     address 2c54.2d3f.e700  priority 32769 (32768 sysid 1)
Root       this switch for MST1

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ------------------------
Gi1/0/17      Desg FWD 20000     128.17   P2p
Gi1/0/18      Desg FWD 20000     128.18   P2p
Gi1/0/19      Desg FWD 20000     128.19   P2p
Gi1/0/20      Desg FWD 20000     128.20   P2p
Gi1/0/21      Desg FWD 20000     128.21   P2p
Gi1/0/22      Desg FWD 20000     128.22   P2p
Gi1/0/23      Desg FWD 20000     128.23   P2p
Gi1/0/24      Desg FWD 20000     128.24   P2p
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol




```
DSW1#configure terminal
DSW1(config)#spanning-tree mst 1 priority 0
DSW1(config)#end
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

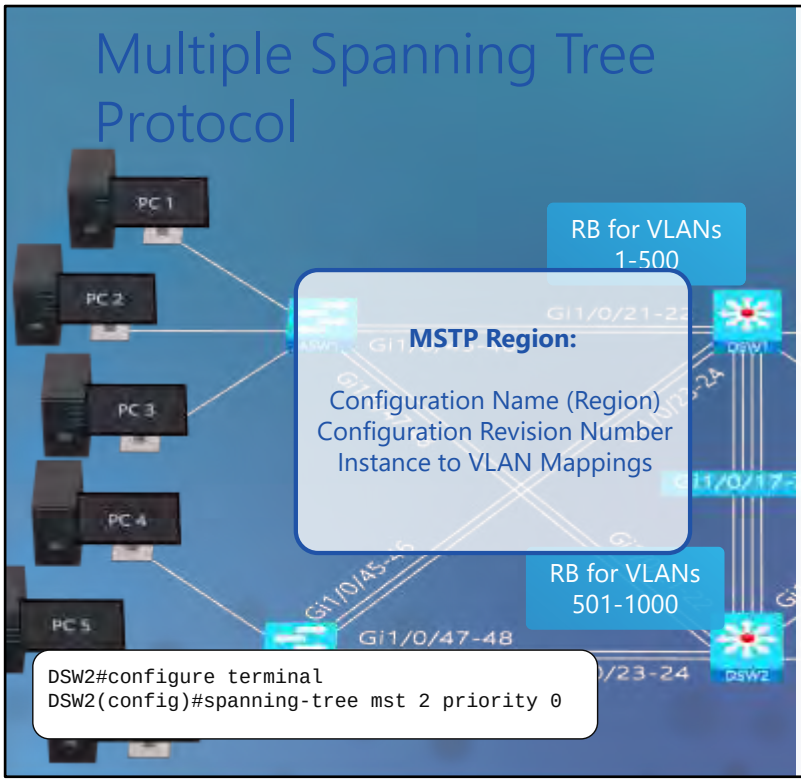
Multiple Spanning Tree Protocol

RB for VLANs 1-500

```
DSW1#show spanning-tree mst 1

##### MST1 vlans mapped:   1-500
Bridge     address 2c54.2d3f.e700  priority 1 (0 sysid 1)
Root       this switch for MST1

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ----------------
Gi1/0/17      Desg FWD 20000     128.17   P2p
Gi1/0/18      Desg FWD 20000     128.18   P2p
Gi1/0/19      Desg FWD 20000     128.19   P2p
Gi1/0/20      Desg FWD 20000     128.20   P2p
Gi1/0/21      Desg FWD 20000     128.21   P2p
Gi1/0/22      Desg FWD 20000     128.22   P2p
Gi1/0/23      Desg FWD 20000     128.23   P2p
Gi1/0/24      Desg FWD 20000     128.24   P2p
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol

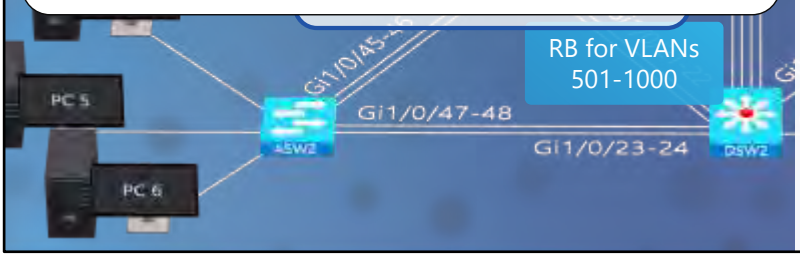



```
DSW2#configure terminal
DSW2(config)#spanning-tree mst 2 priority 0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree

```
DSW2#show spanning-tree mst 2

##### MST2 vlans mapped:   501-1000
Bridge     address 4c00.828c.4300  priority   2  (0 sysid 2)
Root       this switch for MST2

Interface     Role Sts Cost      Prio.Nbr Type
------------- ---- --- --------- -------- ------
Gi1/0/17      Desg FWD 20000     128.17   P2p
Gi1/0/18      Desg FWD 20000     128.18   P2p
Gi1/0/19      Desg FWD 20000     128.19   P2p
Gi1/0/20      Desg FWD 20000     128.20   P2p
Gi1/0/21      Desg FWD 20000     128.21   P2p
Gi1/0/22      Desg FWD 20000     128.22   P2p
Gi1/0/23      Desg FWD 20000     128.23   P2p
Gi1/0/24      Desg FWD 20000     128.24   P2p
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree

```
DSW1#show spanning-tree mst configuration digest
Name      [ENCORE]
Revision  4     Instances configured 3
Digest          0x038C259C3EC6C04CC0FCDAF006251107
Pre-std Digest  0xA38C06EF1F2F2249556A5CB2210C9C3E
```

MSTP Region:

Configuration Name (Region)
Configuration Revision Number
Instance to VLAN Mappings

```
DSW2#show spanning-tree mst configuration digest
Name      [ENCORE]
Revision  4     Instances configured 3
Digest          0x038C259C3EC6C04CC0FCDAF006251107
Pre-std Digest  0xA38C06EF1F2F2249556A5CB2210C9C3E
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol

- Does not send a BPDU for every instance
- Does not encapsulate VLAN list in messages
- By default all VLANs are mapped to Instance Number 0 (IST or MSTI0)
  - BPDU only sent for IST

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol

- Does not send a BPDU for every instance
- Does not encapsulate VLAN list in messages
- By default all VLANs are mapped to Instance Number 0 (IST or MSTI0)
  - BPDU only sent for IST
- The IST carries all STP related information
  - for itself as standard RSTP information
  - additional information in special fields
    - configuration name
    - revision number
    - hash value (calculated based on VLAN to Instance mappings)

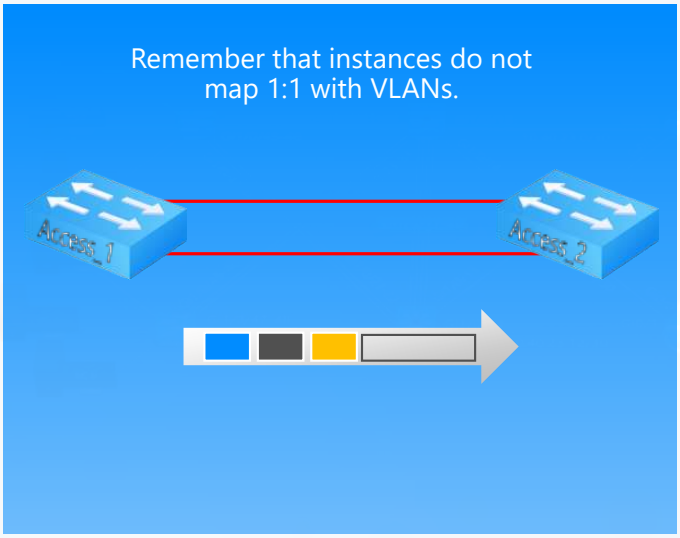
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multiple Spanning Tree Protocol

- Does not send a BPDU for every instance
- Does not encapsulate VLAN list in messages
- By default all VLANs are mapped to Instance Number 0 (IST or MSTI0)
  - BPDU only sent for IST
- The IST carries all STP related information
  - for itself as standard RSTP information
  - additional information in special fields
    - configuration name
    - revision number
    - hash value (calculated based on VLAN to Instance mappings)
- Other instances are known as:
  - Multiple Spanning Tree Instances (MSTIs)
    - M-Records used to carry MSTI information in IST BPDUs
      - 1 M-Record for each MSTI

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

More Things to Consider: MSTP

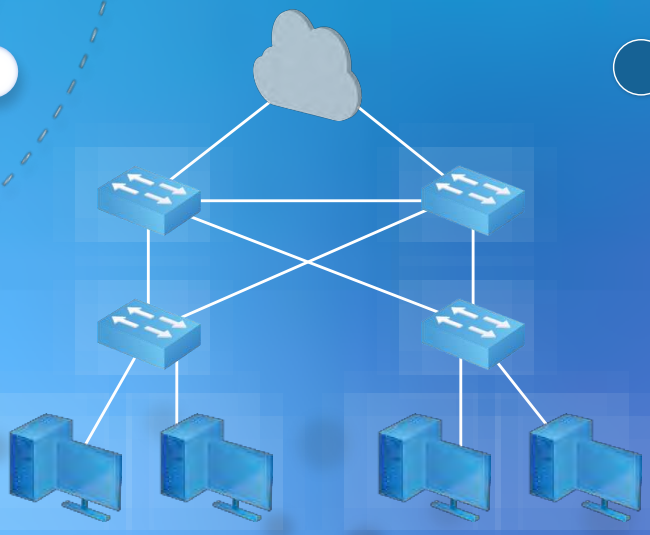


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EtherChannels

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

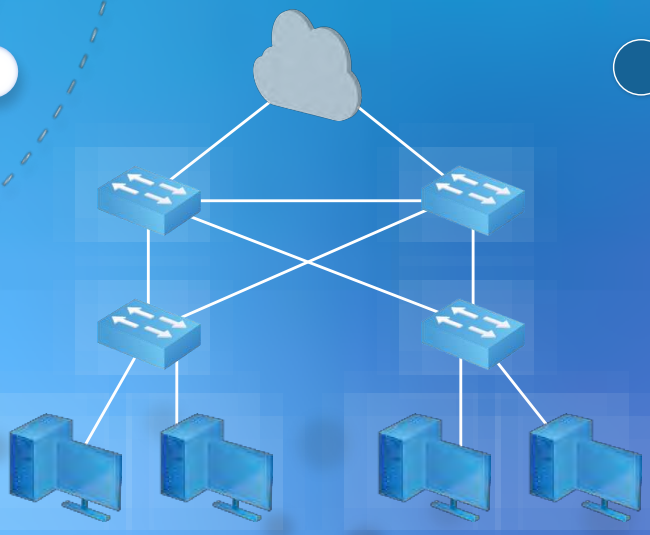
Overview of EtherChannel



- How do we increase the bandwidth between the switches?

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

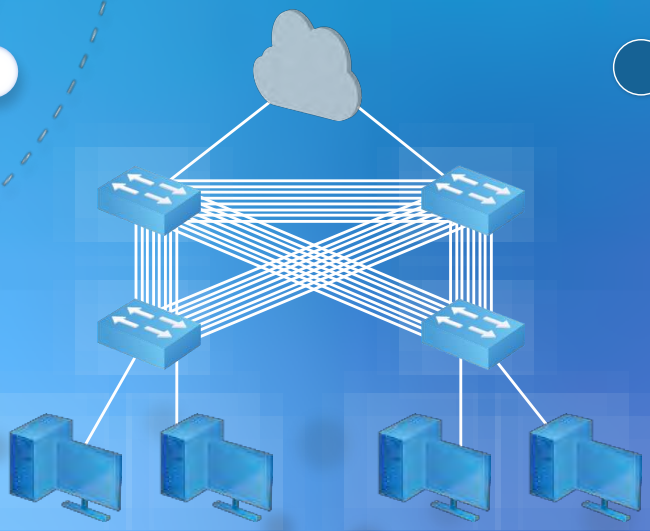
Overview of EtherChannel



- How do we increase the bandwidth between the switches?
  - Upgrade to better switches with higher port speeds
  - Upgrade just the ports on the switch if it is a modular switch
  - Add more links between the switches

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

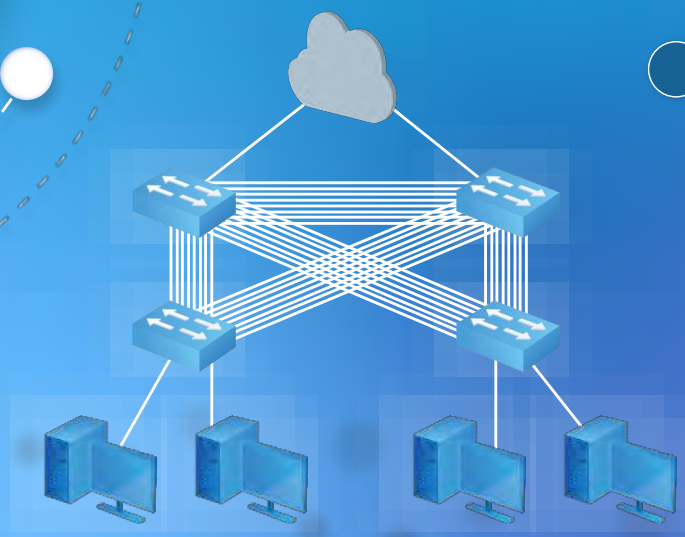
Overview of EtherChannel



- How do we increase the bandwidth between the switches?
  - Add more links between the switches

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

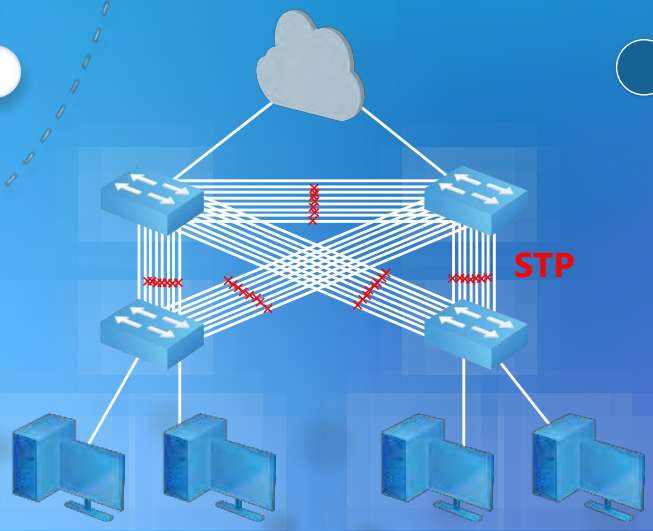
Overview of EtherChannel



- How do we increase the bandwidth between the switches?
  - Add more links between the switches
  - What is the problem?

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

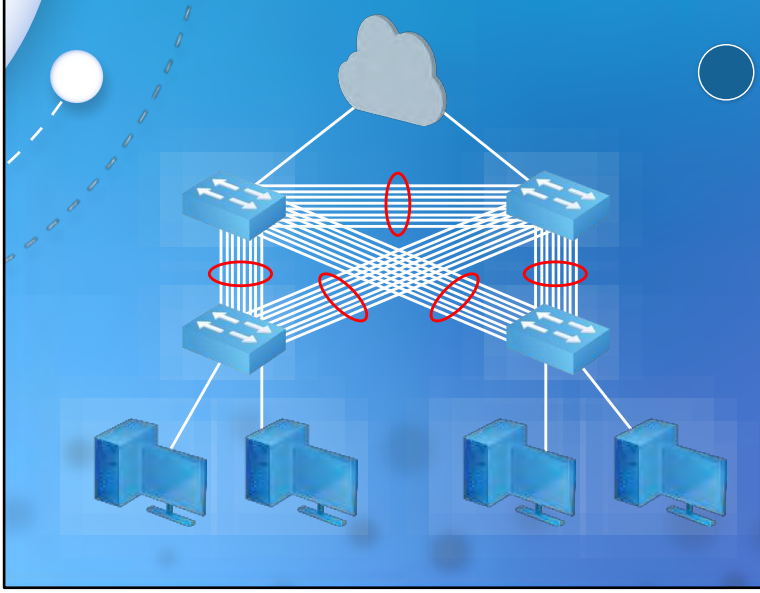
Overview of EtherChannel



- How do we increase the bandwidth between the switches?
  - Add more links between the switches
  - What is the problem?

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Overview of EtherChannel



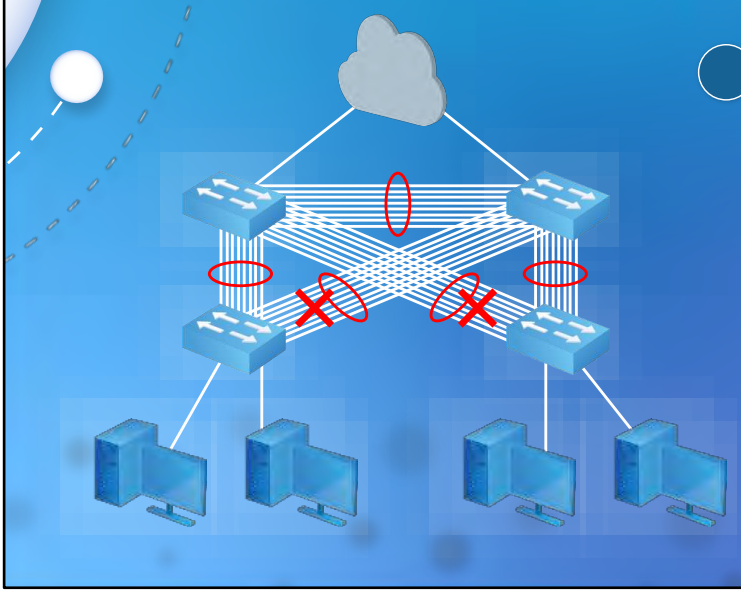
- Solution:

  EtherChannel - Link Aggregation, Port Channel, Channel Group

  - Cost Effective
  - Scalable

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Overview of EtherChannel



- Solution:

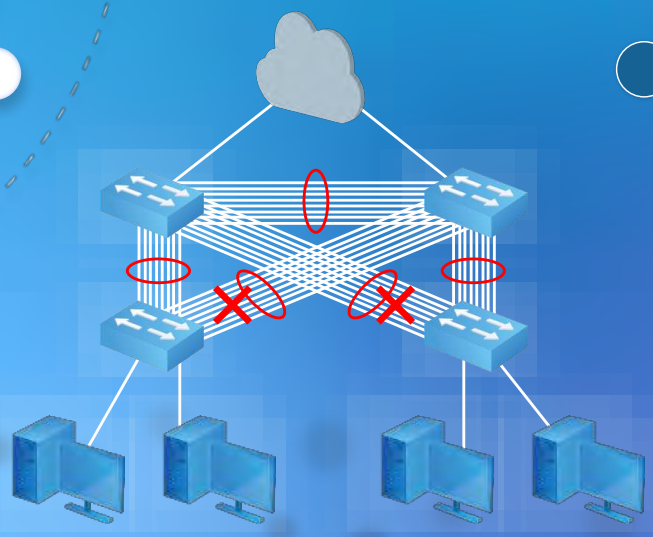
  EtherChannel - Link Aggregation, Port Channel, Channel Group

  - Cost Effective
  - Scalable

  STP will still block entire bundles as necessary to prevent a loop

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Overview of EtherChannel



- Two or more physical links logically treated as one
- Increases available bandwidth
- Appears as one logical port to STP
- Can support L2/L3 EtherChannels
- Variety of ways to Load Share

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

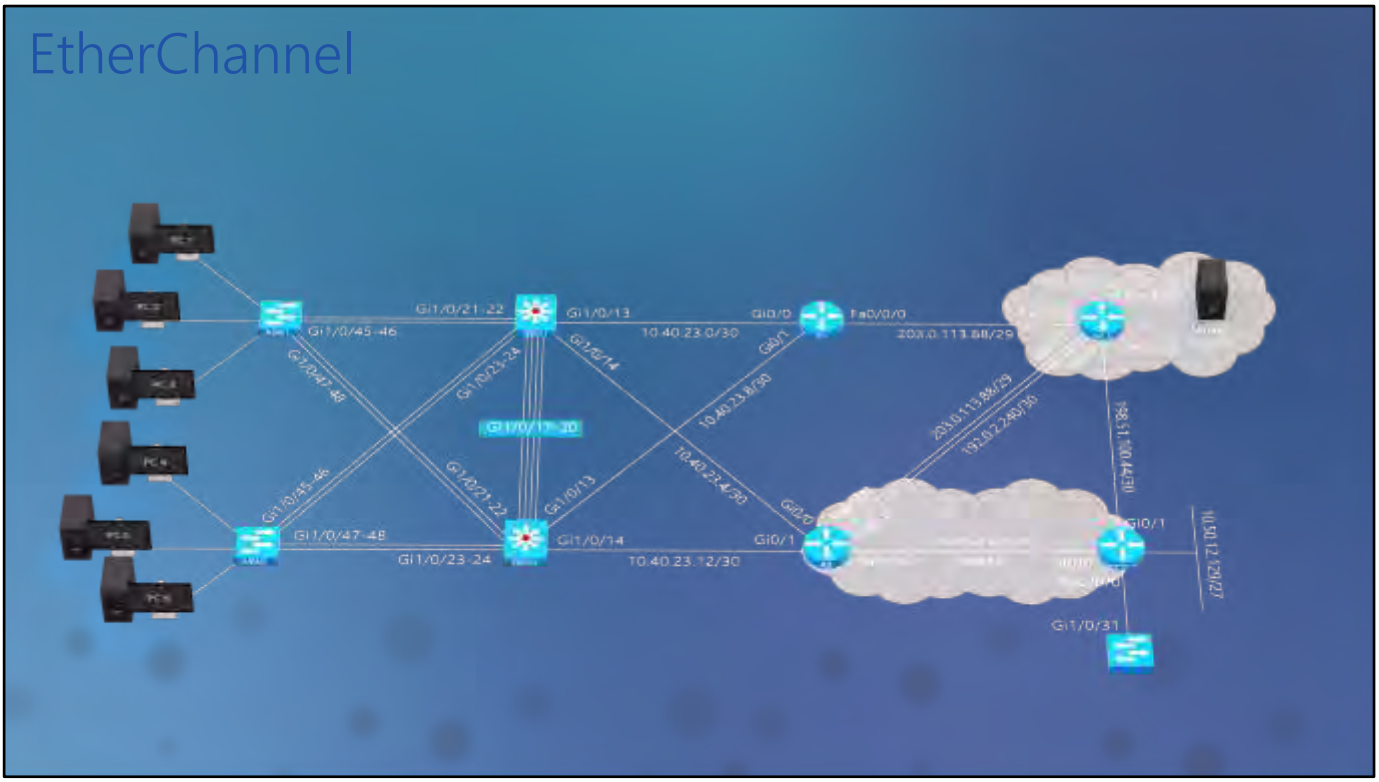
EtherChannel Protocols

Two main protocols exist to negotiate EtherChannel:

PAgP	**Port Aggregation Protocol** is Cisco proprietary protocol
LACP	**Link Aggregation Control Protocol** is IEEE 802.3ad standard
None	A Port Channel can be configured **without a protocol**

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

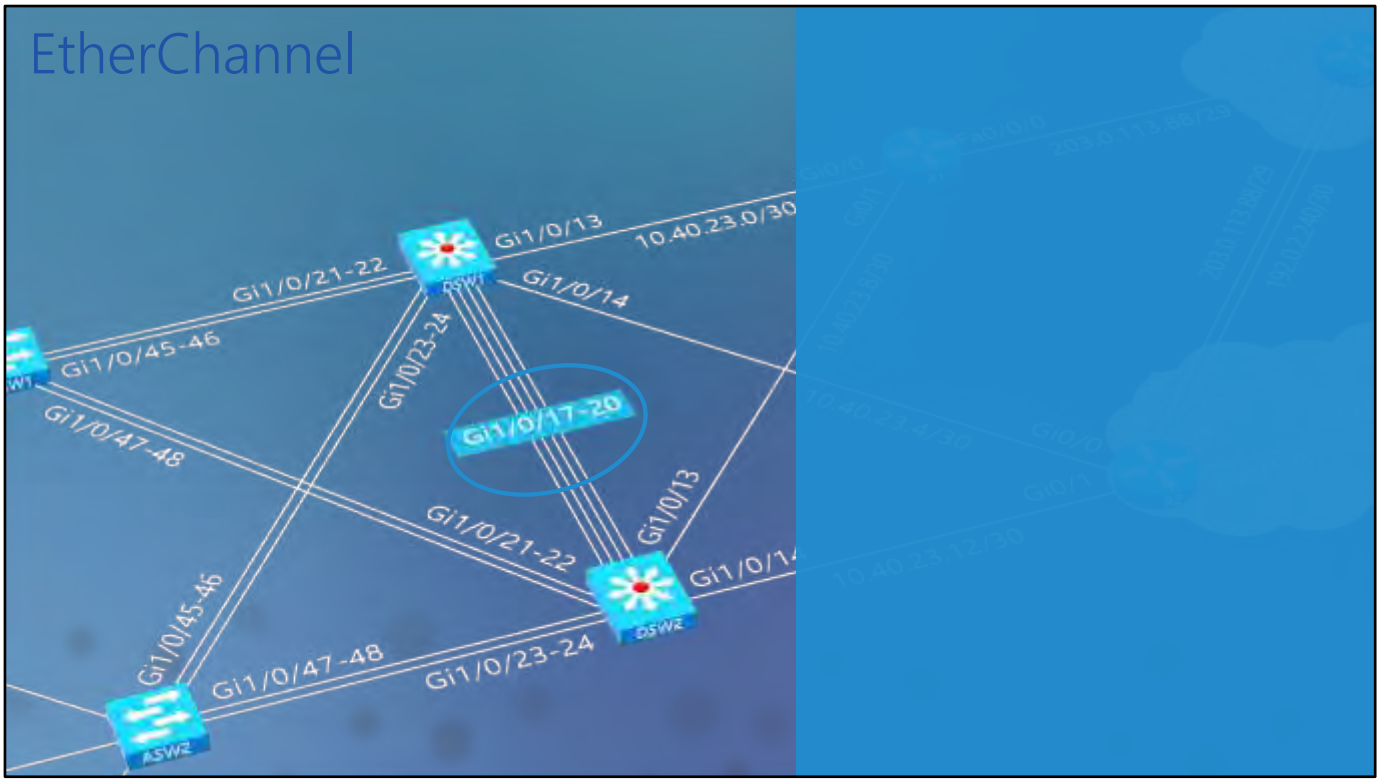
EtherChannel



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

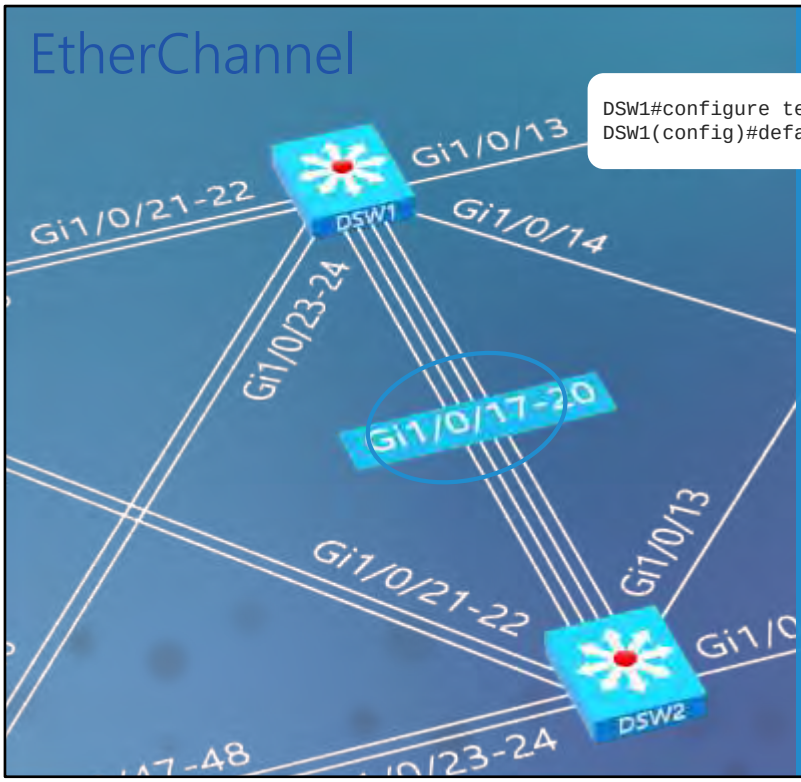
EtherChannel



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EtherChannel




```
DSW1#configure terminal
DSW1(config)#default interface range gigabitEthernet 1/0/17-20
```

Notes:

All physical ports must have the same configuration:

- Speed and duplex
- Trunks: Native and allowed VLANs
- Access: VLAN provisioned on ports

Only 2 switches per bundle

- Ports must be in same bundle

Misconfiguration Errors

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring PAgP

PAgP

Desirable: Initiate the EtherChannel session with neighboring switch
Auto: Wait for the neighboring switch to initiate the EtherChannel session

```
DSW1(config)#interface range gigabitEthernet 1/47-48
DSW1(config-if-range)#channel-group number mode [desirable|auto]
```

Channel Establishment	Desirable	Auto
Desirable	Yes	Yes
Auto	Yes	No

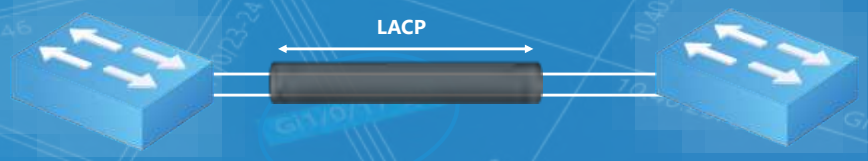
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring LACP

LACP

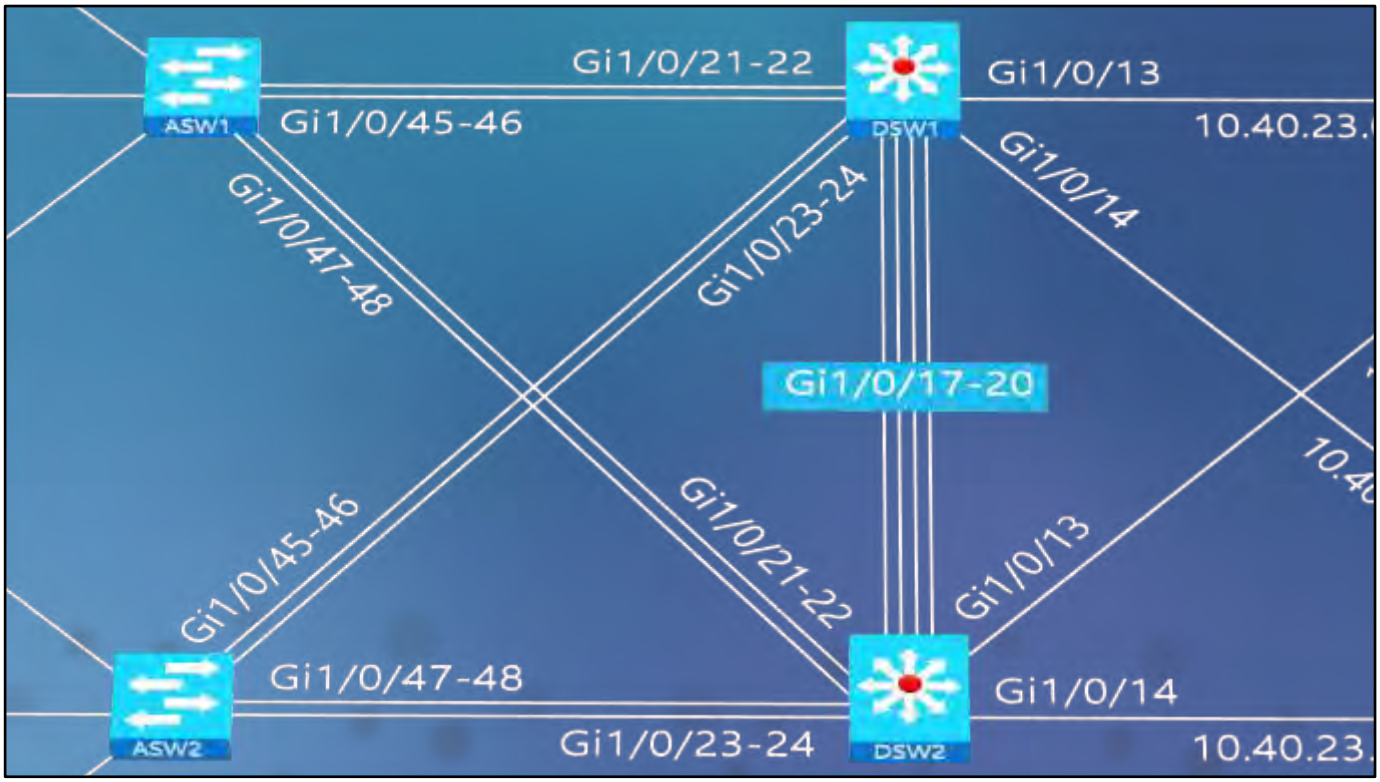
Active: Initiate the EtherChannel session with neighboring switch
Passive: Wait for the neighboring switch to initiate the EtherChannel session

```
DSW1(config)#interface range gigabitEthernet 1/47-48
DSW1(config-if-range)#channel-group number mode [active|passive]
```



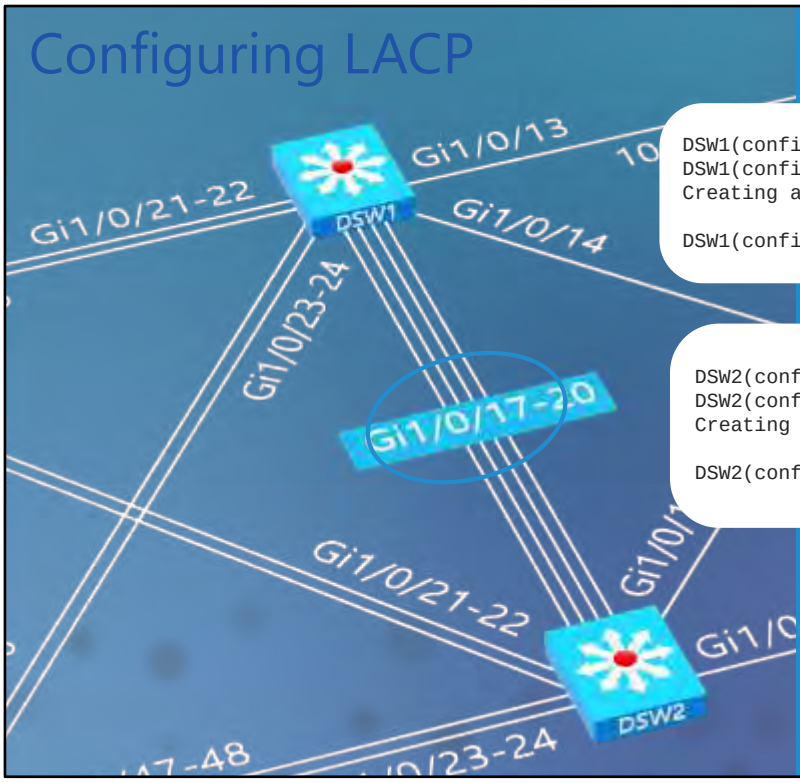
Channel Establishment	Active	Passive
Active	Yes	Yes
Passive	Yes	No

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring LACP




```
DSW1(config)#interface range gigabitEthernet 1/0/17-20
DSW1(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

DSW1(config-if-range)#
```

```
DSW2(config)#interface range gigabitEthernet 1/0/17-20
DSW2(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

DSW2(config-if-range)#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

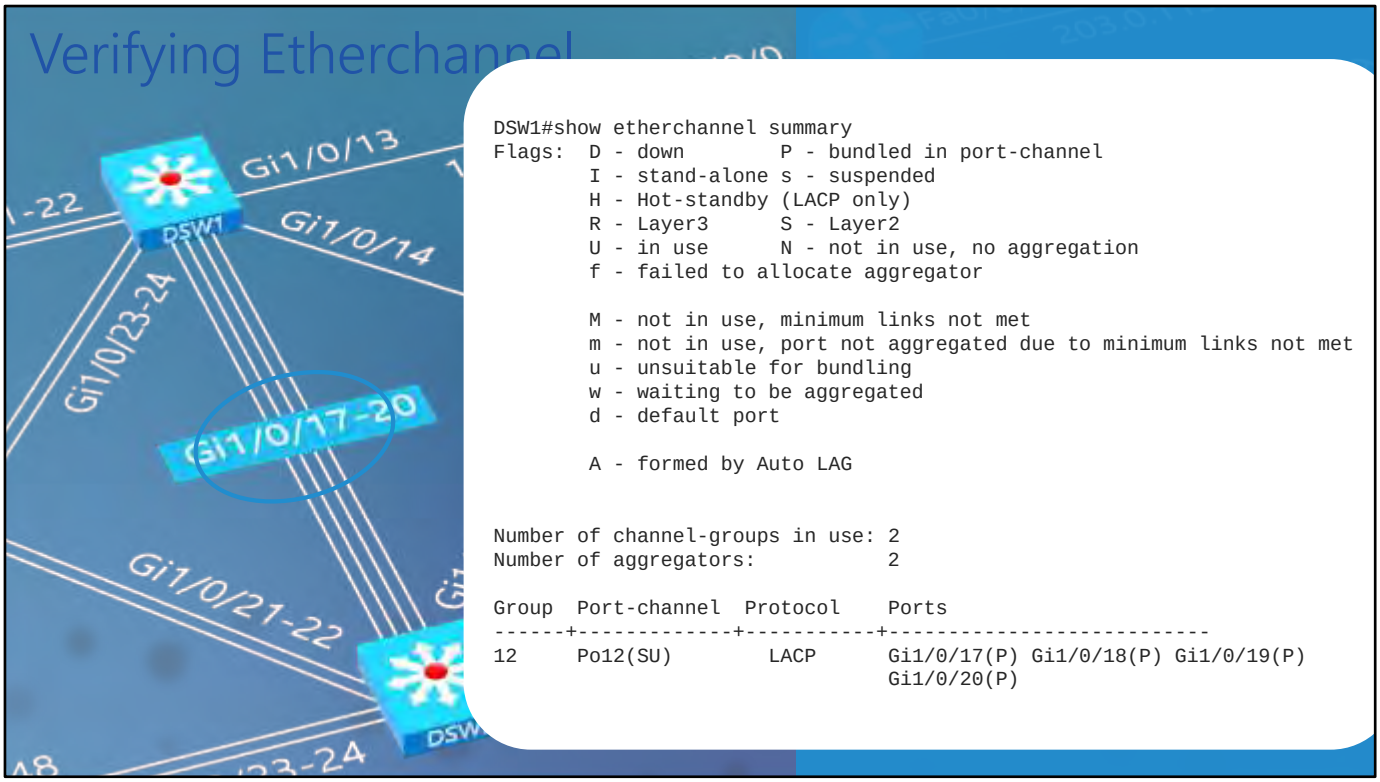
Configuring LACP

```
DSW1(config)#interface port-channel 12
DSW1(config-if)#switchport trunk encapsulation dot1q
DSW1(config-if)#switchport mode trunk
DSW1(config-if)#switchport nonegotiate
DSW1(config-if)#switchport trunk allowed vlan 10,20,25,50
DSW1(config-if)#
```

```
DSW2(config)#interface port-channel 12
DSW2(config-if)#switchport trunk encapsulation dot1q
DSW2(config-if)#switchport mode trunk
DSW2(config-if)#switchport nonegotiate
DSW2(config-if)#switchport trunk allowed vlan 10,20,25,50
DSW2(config-if)#
```


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

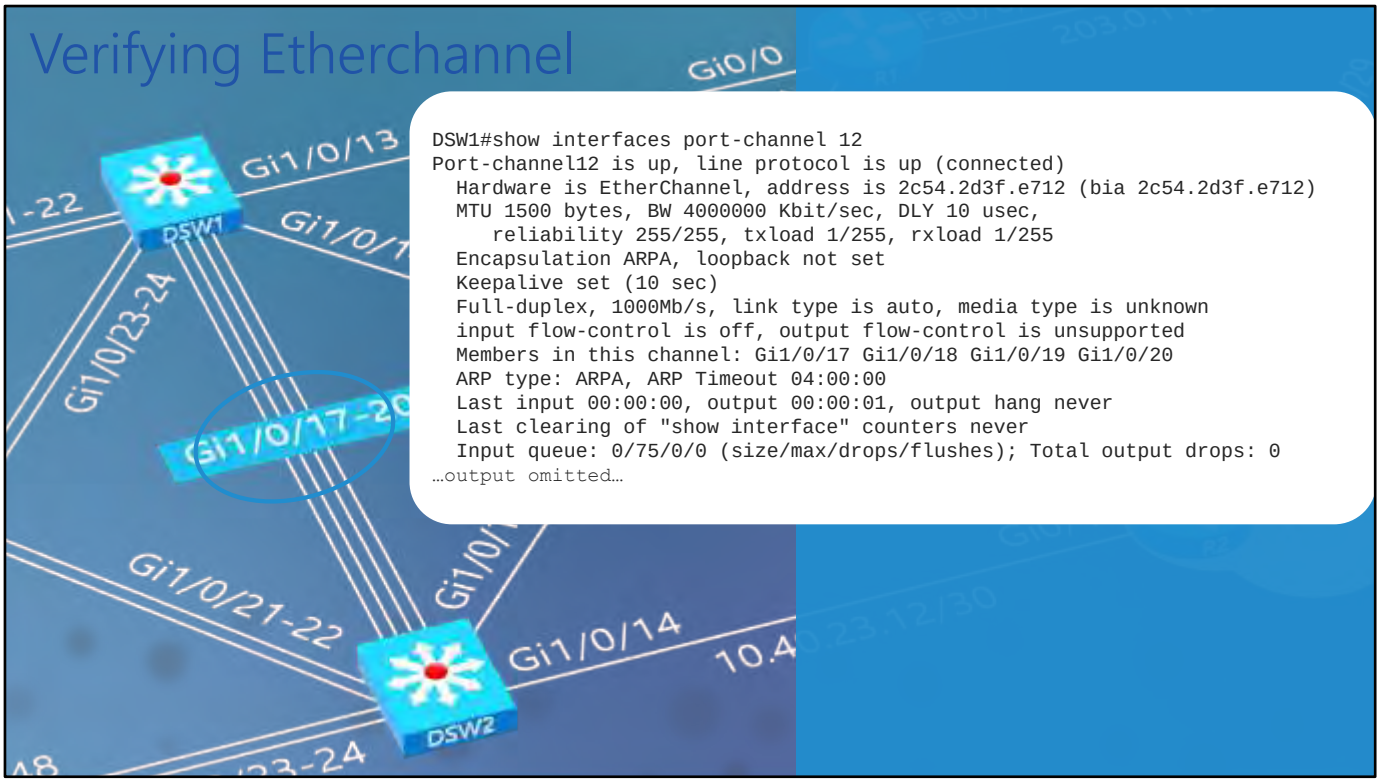
Verifying Etherchannel




```
DSW1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------
12     Po12(SU)        LACP      Gi1/0/17(P) Gi1/0/18(P) Gi1/0/19(P)
                                 Gi1/0/20(P)
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying Etherchannel

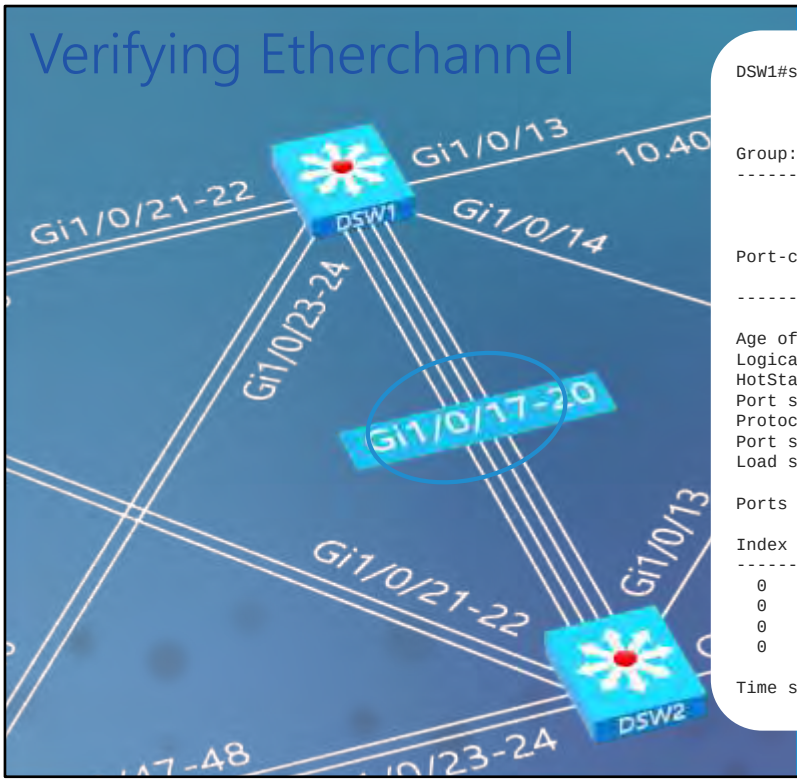



```
DSW1#show interfaces port-channel 12
Port-channel12 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 2c54.2d3f.e712 (bia 2c54.2d3f.e712)
  MTU 1500 bytes, BW 4000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, link type is auto, media type is unknown
  input flow-control is off, output flow-control is unsupported
  Members in this channel: Gi1/0/17 Gi1/0/18 Gi1/0/19 Gi1/0/20
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

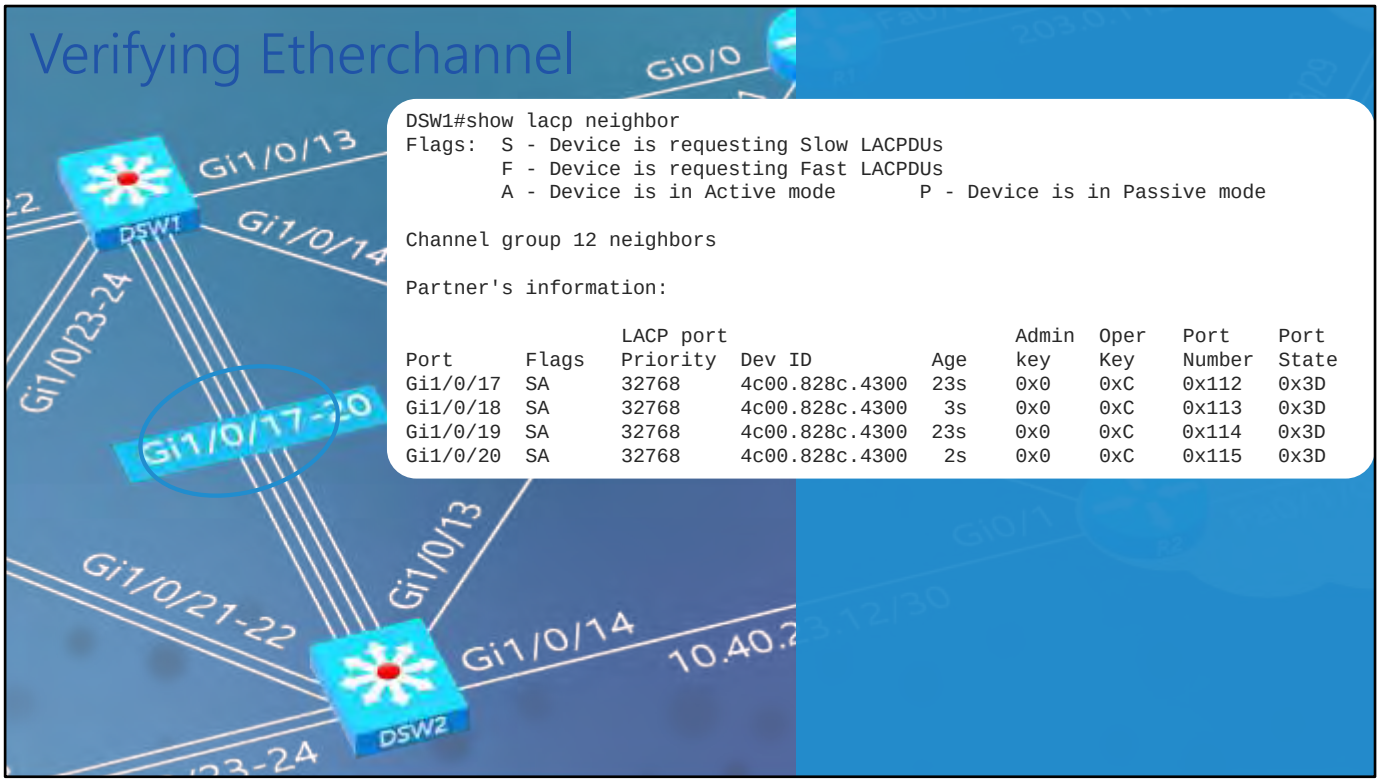
Verifying Etherchannel




```
DSW1#show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 12
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po12    (Primary Aggregator)

------------

Age of the Port-channel   = 0d:00h:07m:56s
Logical slot/port   = 10/12          Number of ports = 4
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled
Load share deferral = Disabled

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi1/0/17 Active             0
  0     00     Gi1/0/18 Active             0
  0     00     Gi1/0/19 Active             0
  0     00     Gi1/0/20 Active             0

Time since last port bundled:    0d:00h:04m:37s    Gi1/0/20
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying Etherchannel

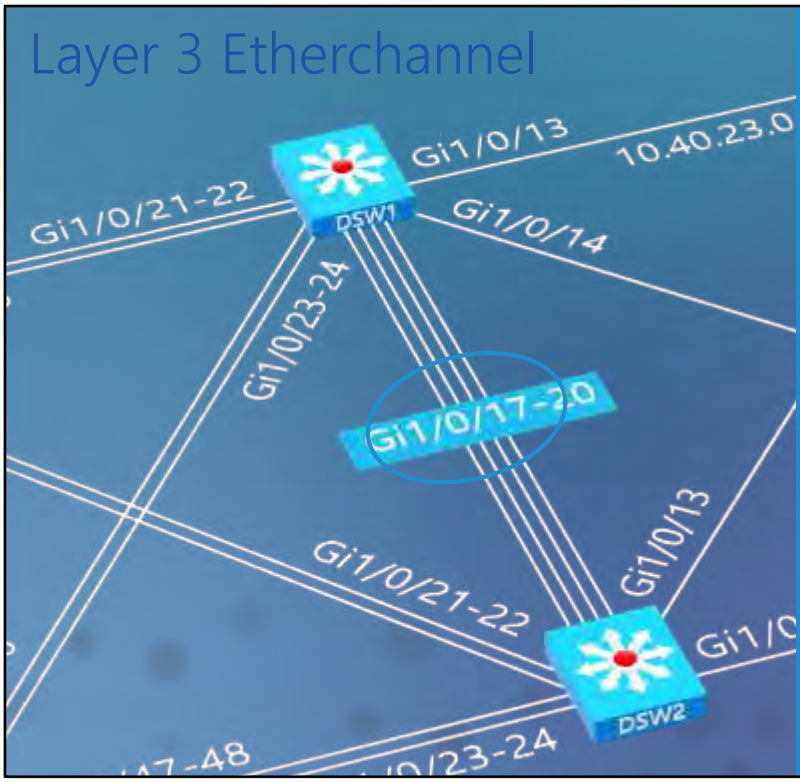



```
DSW1#show lacp neighbor
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 12 neighbors

Partner's information:

                  LACP port                          Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID          Age     key    Key    Number  State
Gi1/0/17  SA      32768     4c00.828c.4300  23s     0x0    0xC    0x112   0x3D
Gi1/0/18  SA      32768     4c00.828c.4300   3s     0x0    0xC    0x113   0x3D
Gi1/0/19  SA      32768     4c00.828c.4300  23s     0x0    0xC    0x114   0x3D
Gi1/0/20  SA      32768     4c00.828c.4300   2s     0x0    0xC    0x115   0x3D
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

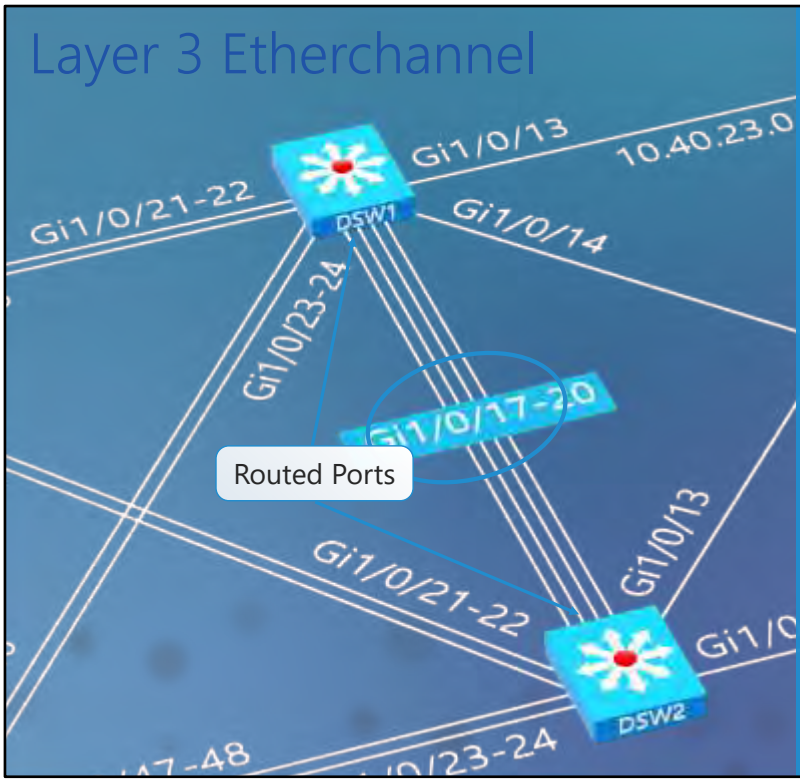
Layer 3 Etherchannel



Etherchannel bundle using Layer 3

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

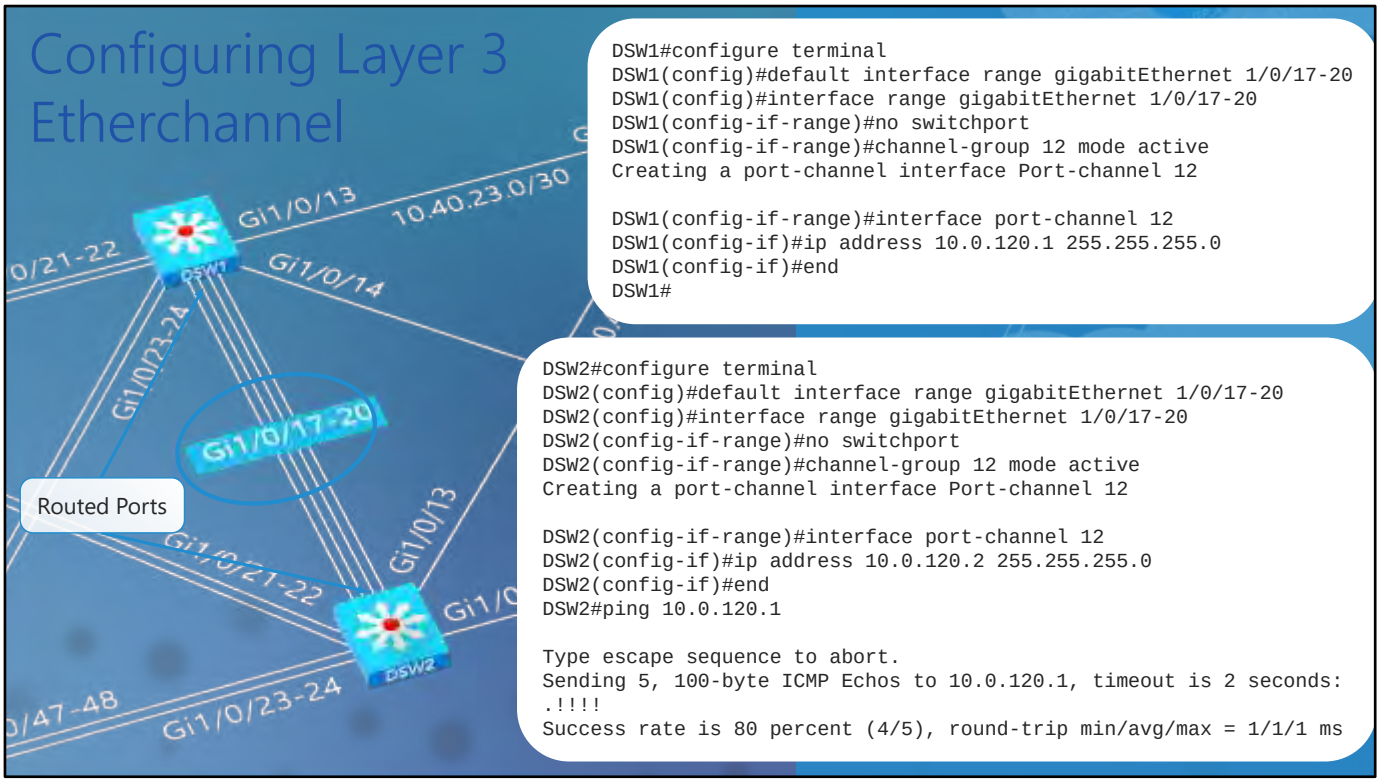
Layer 3 Etherchannel



Etherchannel bundle using Layer 3

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configuring Layer 3 Etherchannel

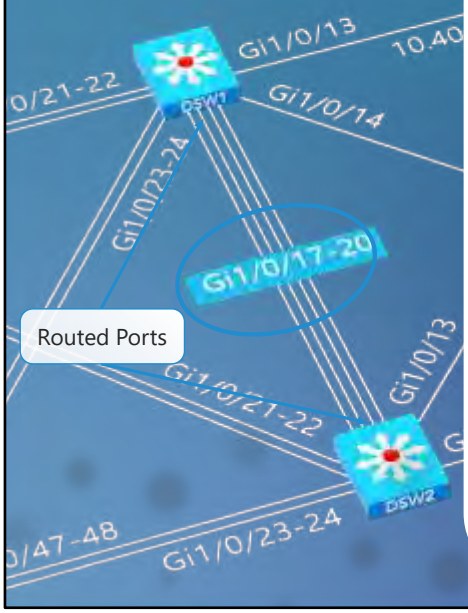



```
DSW1#configure terminal
DSW1(config)#default interface range gigabitEthernet 1/0/17-20
DSW1(config)#interface range gigabitEthernet 1/0/17-20
DSW1(config-if-range)#no switchport
DSW1(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

DSW1(config-if-range)#interface port-channel 12
DSW1(config-if)#ip address 10.0.120.1 255.255.255.0
DSW1(config-if)#end
DSW1#
```

```
DSW2#configure terminal
DSW2(config)#default interface range gigabitEthernet 1/0/17-20
DSW2(config)#interface range gigabitEthernet 1/0/17-20
DSW2(config-if-range)#no switchport
DSW2(config-if-range)#channel-group 12 mode active
Creating a port-channel interface Port-channel 12

DSW2(config-if-range)#interface port-channel 12
DSW2(config-if)#ip address 10.0.120.2 255.255.255.0
DSW2(config-if)#end
DSW2#ping 10.0.120.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.120.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying Layer 3 Etherchannel

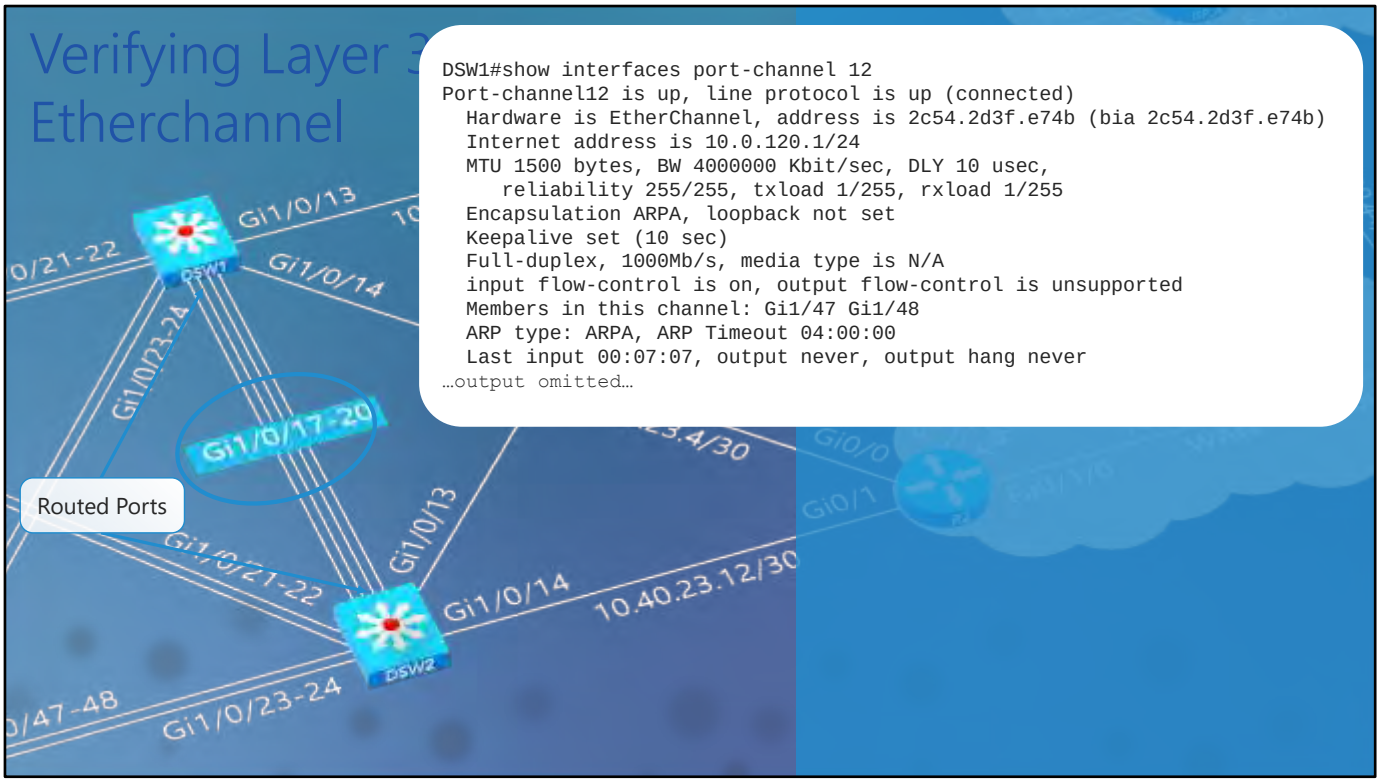



```
DSW1#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+---------------------------
12     Po12(RU)        LACP      Gi1/0/17(P) Gi1/0/18(P) Gi1/0/19(P)
                                 Gi1/0/20(P)
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying Layer 3 Etherchannel

```
DSW1#show interfaces port-channel 12
Port-channel12 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 2c54.2d3f.e74b (bia 2c54.2d3f.e74b)
  Internet address is 10.0.120.1/24
  MTU 1500 bytes, BW 4000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s, media type is N/A
  input flow-control is on, output flow-control is unsupported
  Members in this channel: Gi1/47 Gi1/48
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:07:07, output never, output hang never
…output omitted…
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Load-Balancing

Depending on the switch model, the default method may vary. You can change the algorithm globally on a switch, therefore all Port Channels will use the same method.

Examples include:

- SRC-DST MAC
- SRC-DST IP

To change the default:

```
port-channel load-balance <method>
```

To verify:

```
show etherchannel load-balance
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

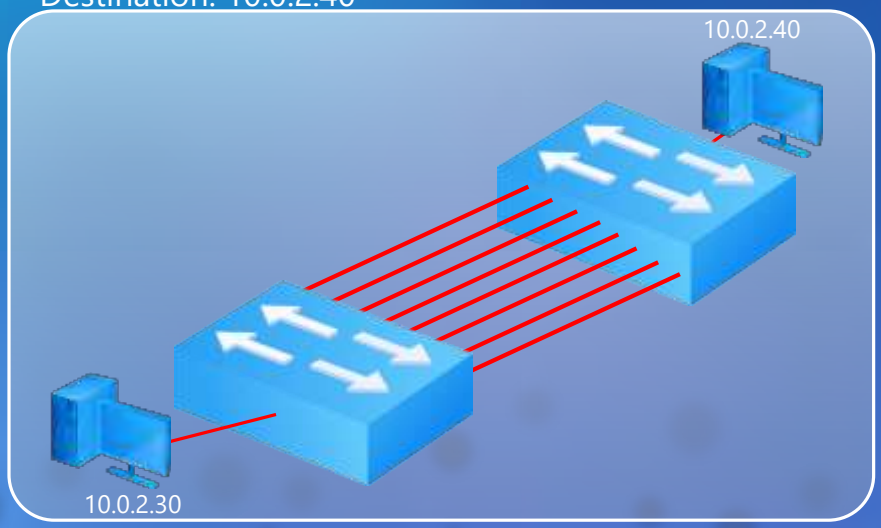
Load-Balancing Options

Hash Input Code	Hash Input Description	Switch Model
dst-ip	Destination IP address	All models
dst-mac	Destination MAC address	All models
src-dst-ip	Source and destination IP address	All models
src-dst-mac	Source and destination MAC address	All models
src-ip	Source IP address	All models
src-mac	Source MAC address	All models
src-port	Source port number	4500,6500
dst-port	Destination port number	4500,6500
src-dst-port	Source and destination port number	4500,6500

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Example of Load-Balancing

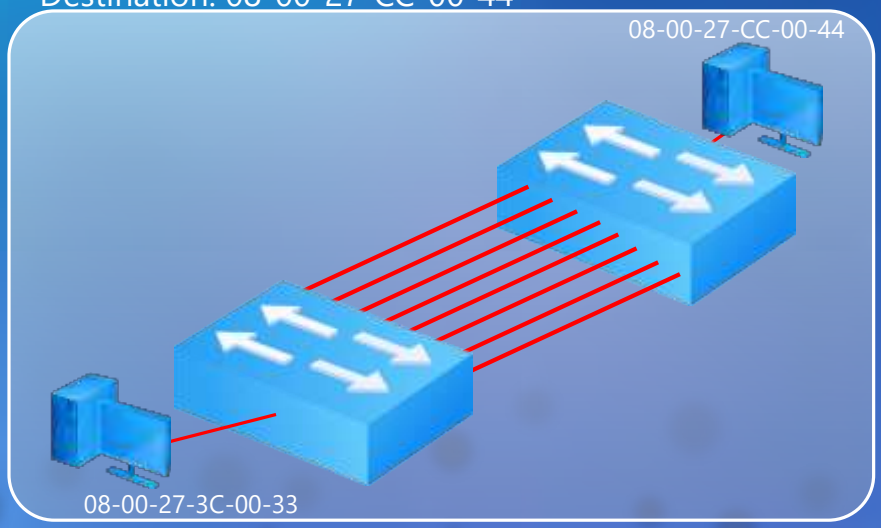
Source: 10.0.2.30
Destination: 10.0.2.40



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Example of Load-Balancing

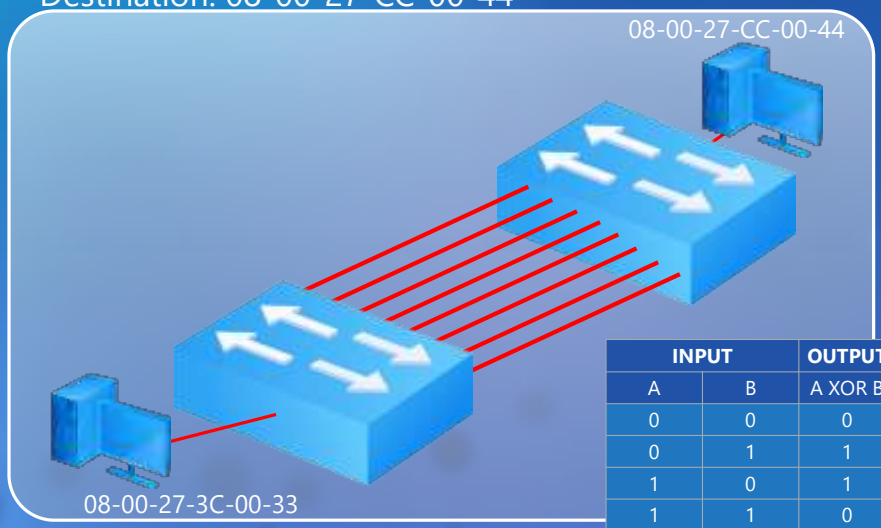
Source: 08-00-27-3C-00-33
Destination: 08-00-27-CC-00-44



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Example of Load-Balancing

Source: 08-00-27-3C-00-33
Destination: 08-00-27-CC-00-44



INPUT		OUTPUT
A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Reviewing Load-Balancing

After reviewing the values you can reset the counters

```
clear counters
```

*Then you can always reissue an extended ping

To verify:

```
show interface fa 1/0/23 | incl packets output
```

To verify:

```
show interface fa 1/0/24 | incl packets output
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EtherChannel Guard

Tells you if EtherChannel is misconfigured.

```
%PM-SP-4-ERR_DISABLE: channel-misconfig error detected on Po3, putting Fa1/1 in
err-disable state
```

EtherChannel Guard is enabled by default.

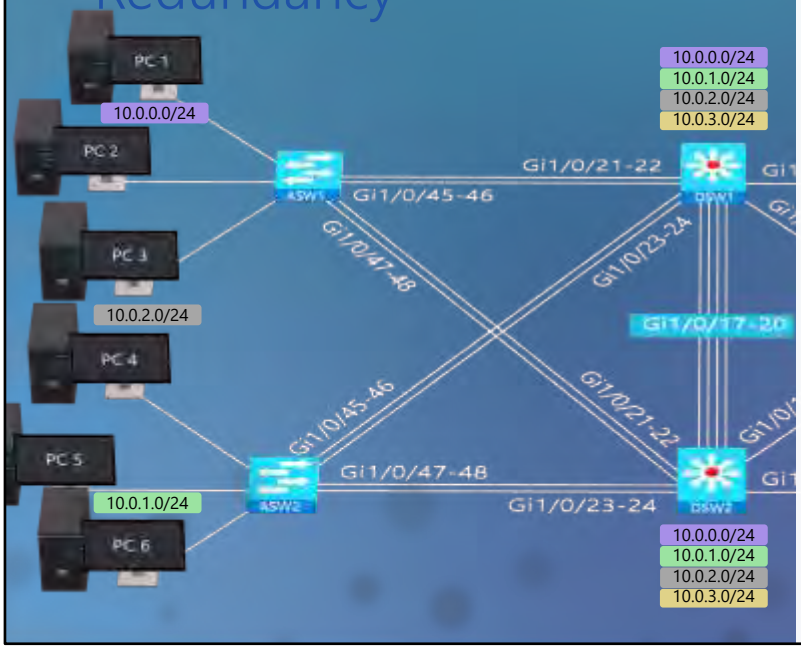
```
Switch1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
<... output omitted ...>
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

First-Hop Redundancy Protocol (FHRP) Overview

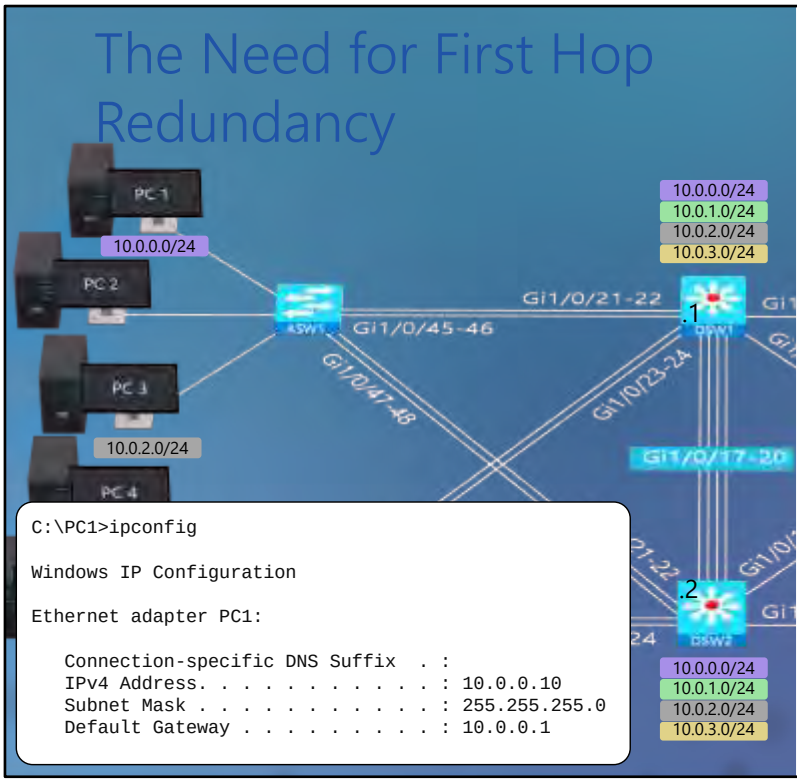
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

The Need for First Hop Redundancy



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

The Need for First Hop Redundancy

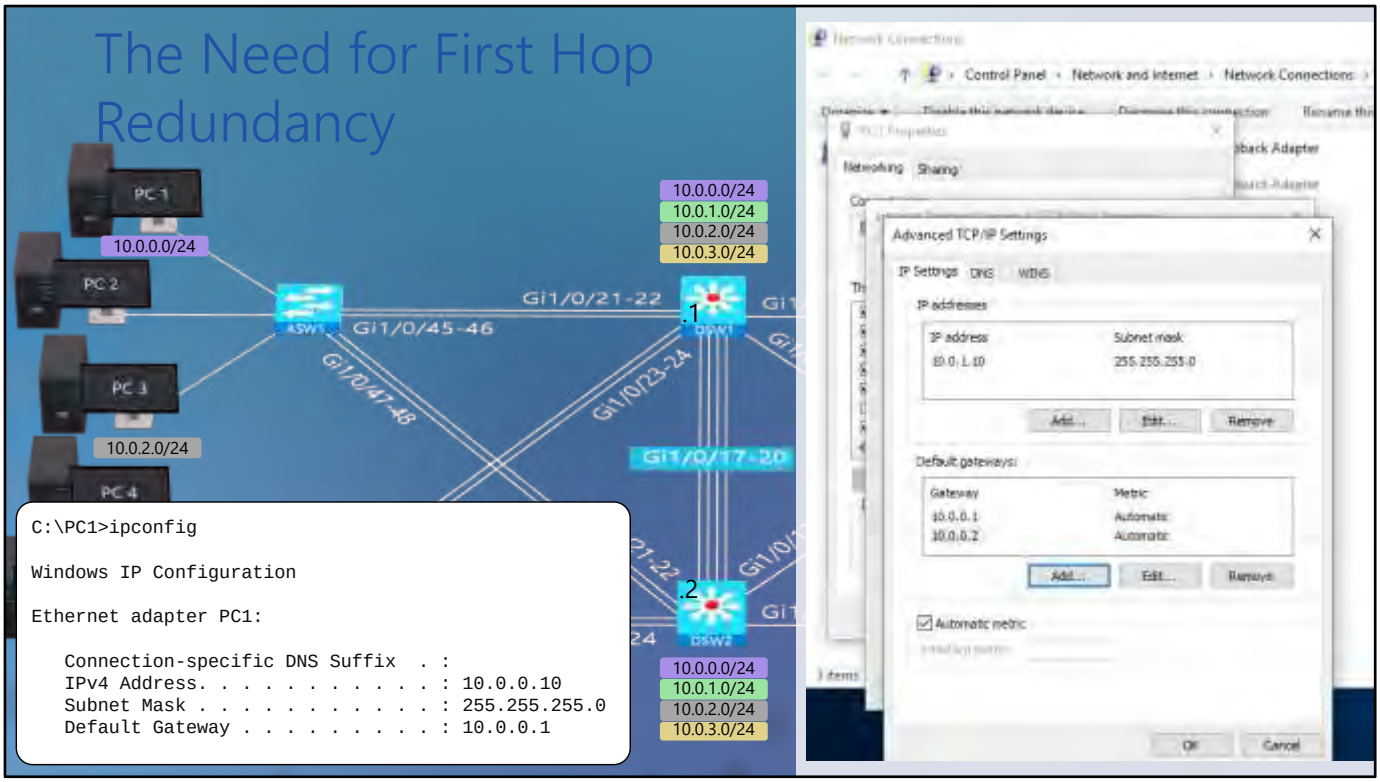



```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

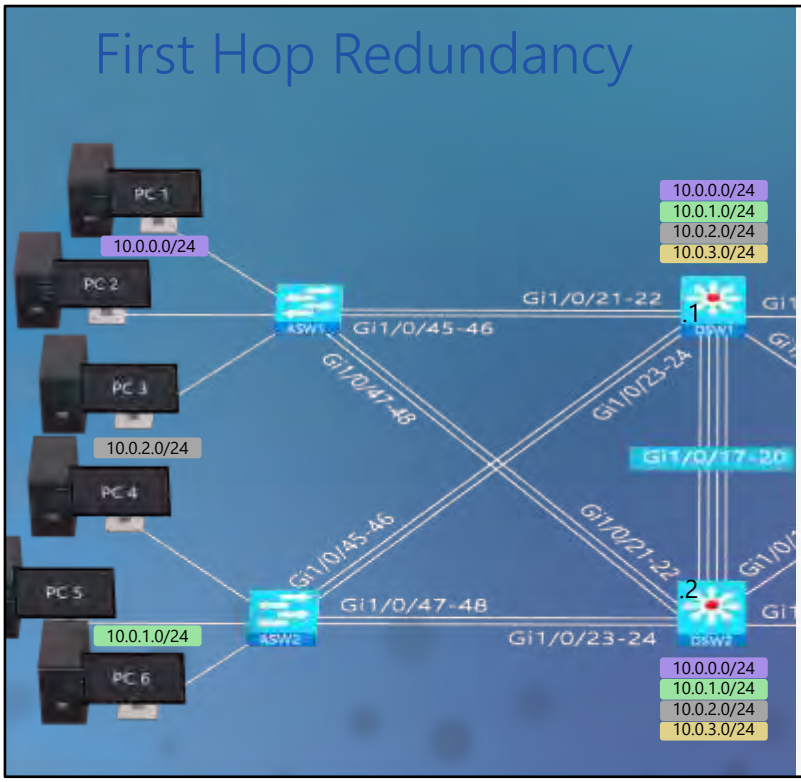
The Need for First Hop Redundancy



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

First Hop Redundancy



Routers / Layer 3 switches work together (GROUP) to create the illusion of a single virtual router

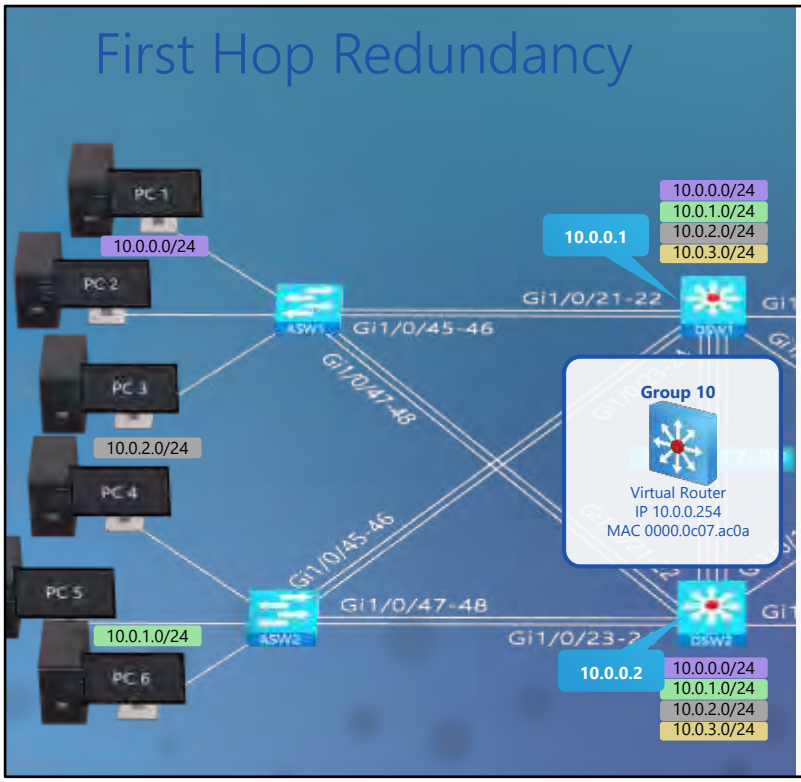
The virtual router will be the default gateway for the subnet/vlan

- An IP address that will be shared between the physical devices
- A MAC address that will be shared between the physical devices

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

First Hop Redundancy



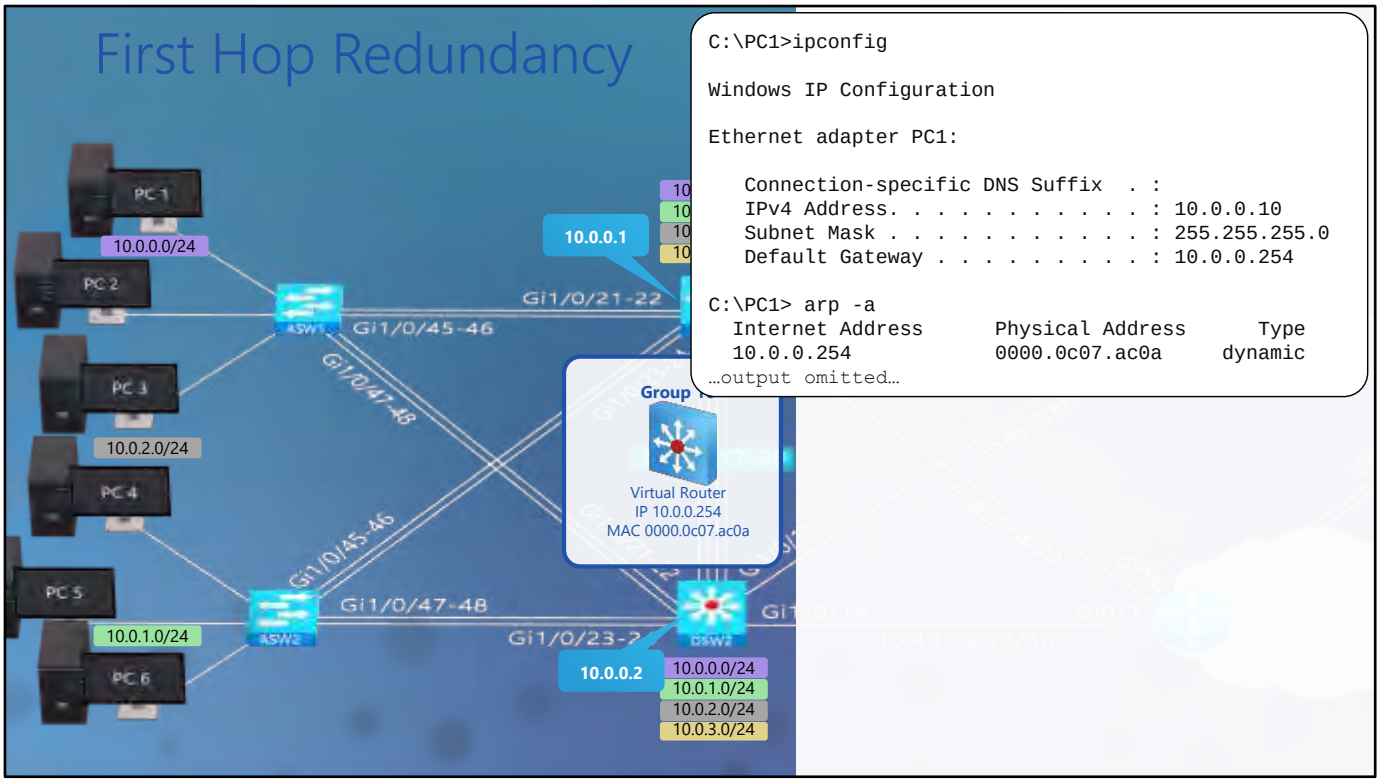
Routers / Layer 3 switches work together (GROUP) to create the illusion of a single virtual router

The virtual router will be the default gateway for the subnet/vlan

- An IP address that will be shared between the physical devices
- A MAC address that will be shared between the physical devices

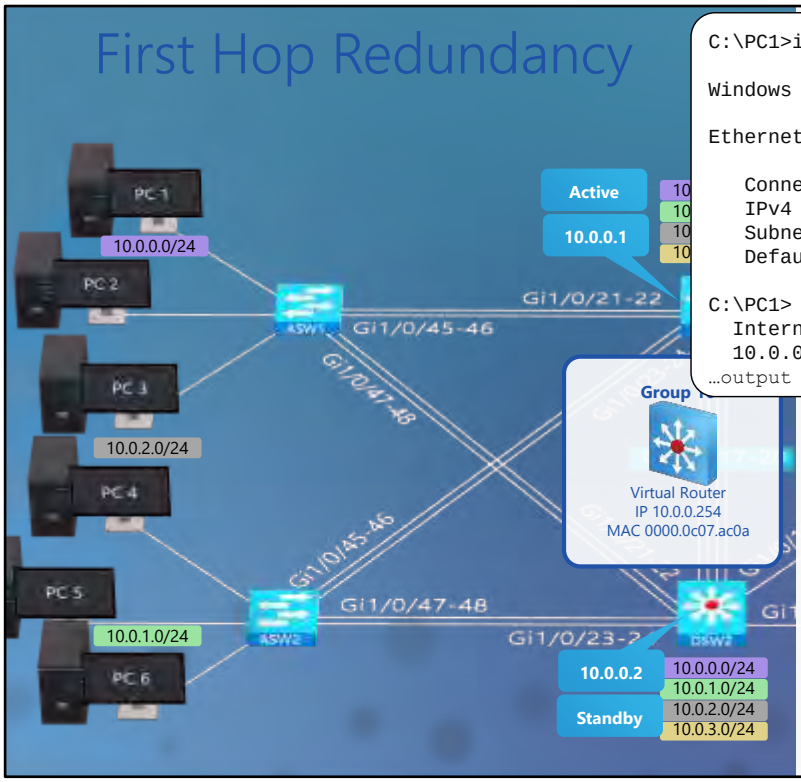
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



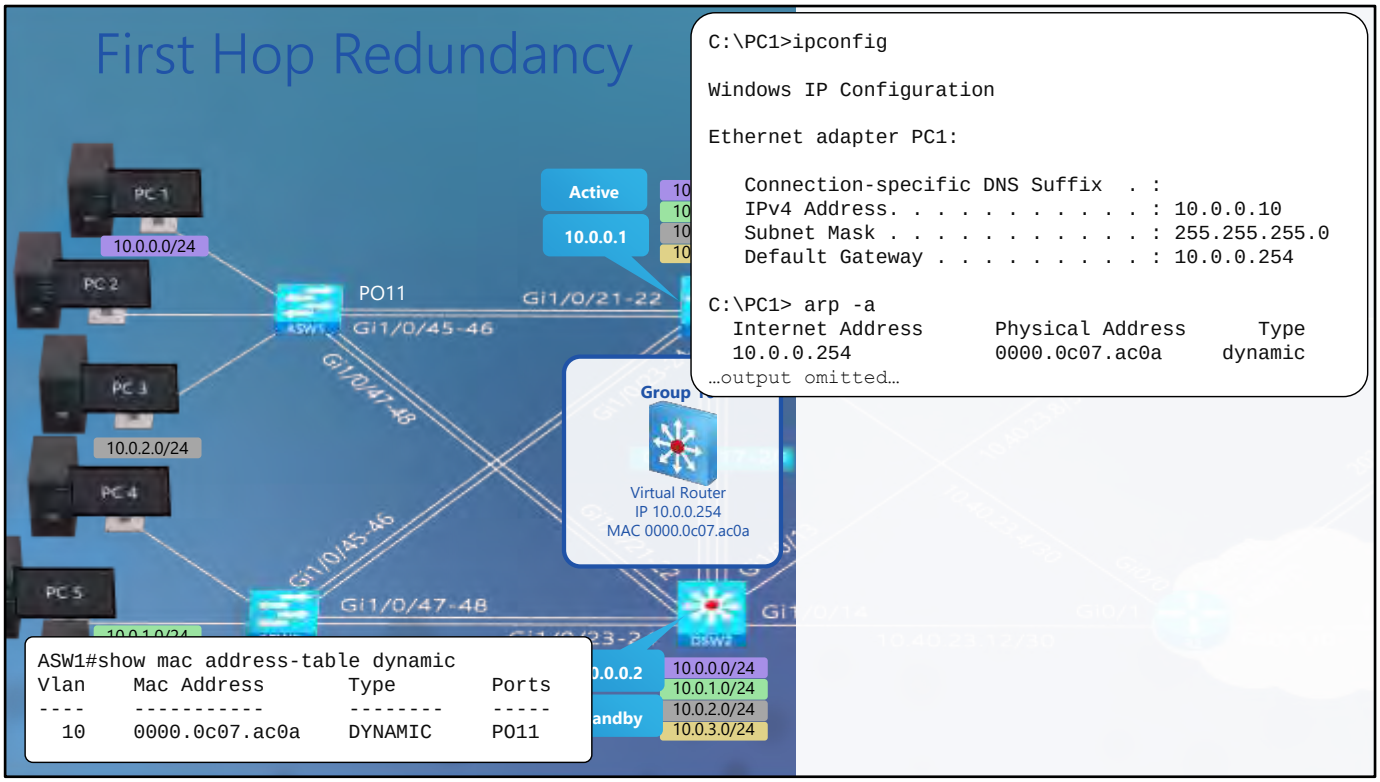
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

First Hop Redundancy

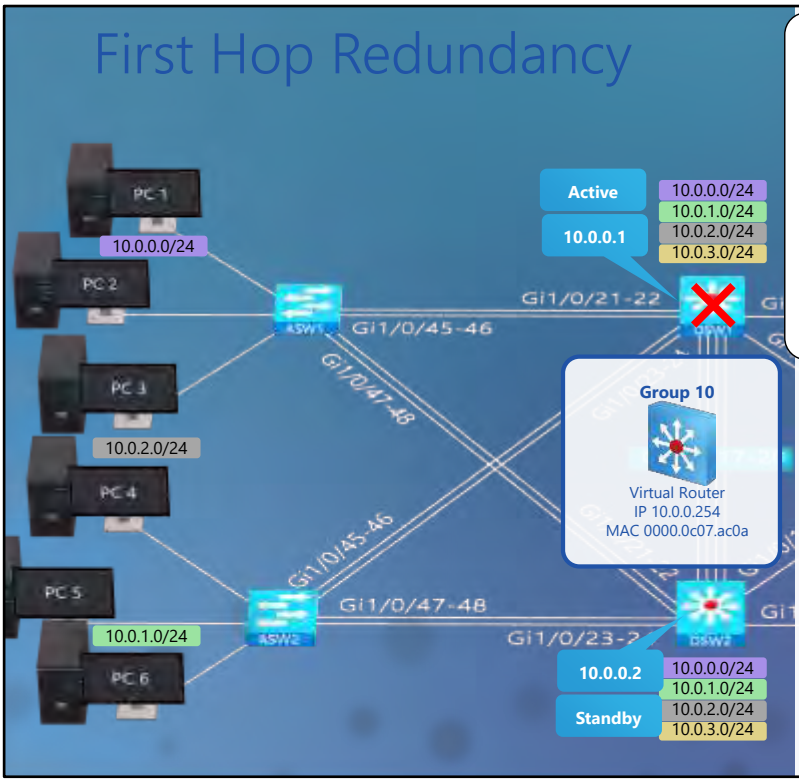



```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

C:\PC1> arp -a
  Internet Address      Physical Address      Type
  10.0.0.254            0000.0c07.ac0a     dynamic
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

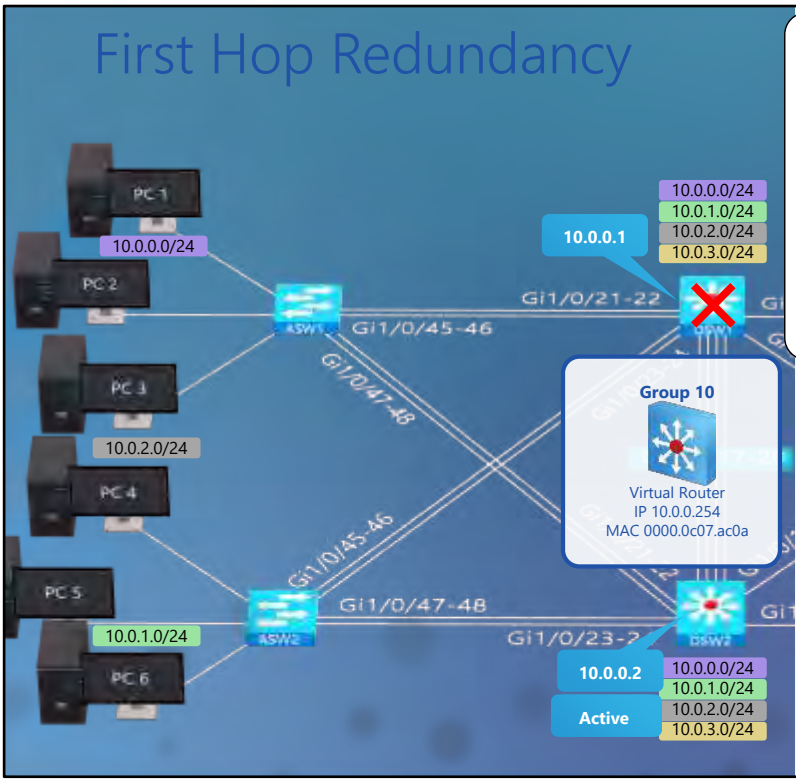


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

C:\PC1> arp -a
  Internet Address      Physical Address      Type
  10.0.0.254            0000.0c07.ac0a     dynamic
…output omitted…
```

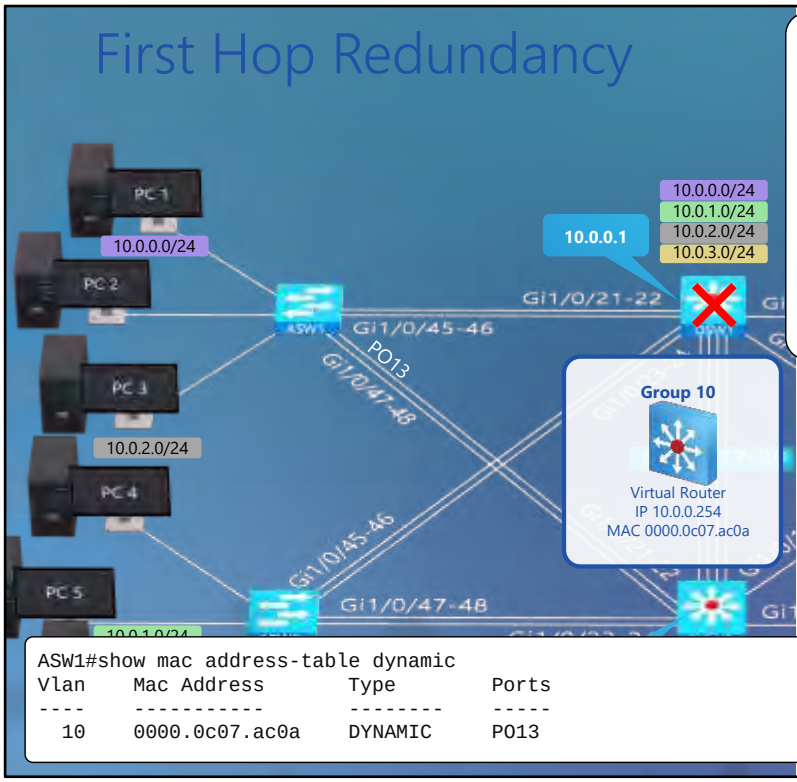
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

C:\PC1> arp -a
  Internet Address      Physical Address      Type
  10.0.0.254            0000.0c07.ac0a     dynamic
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

First Hop Redundancy

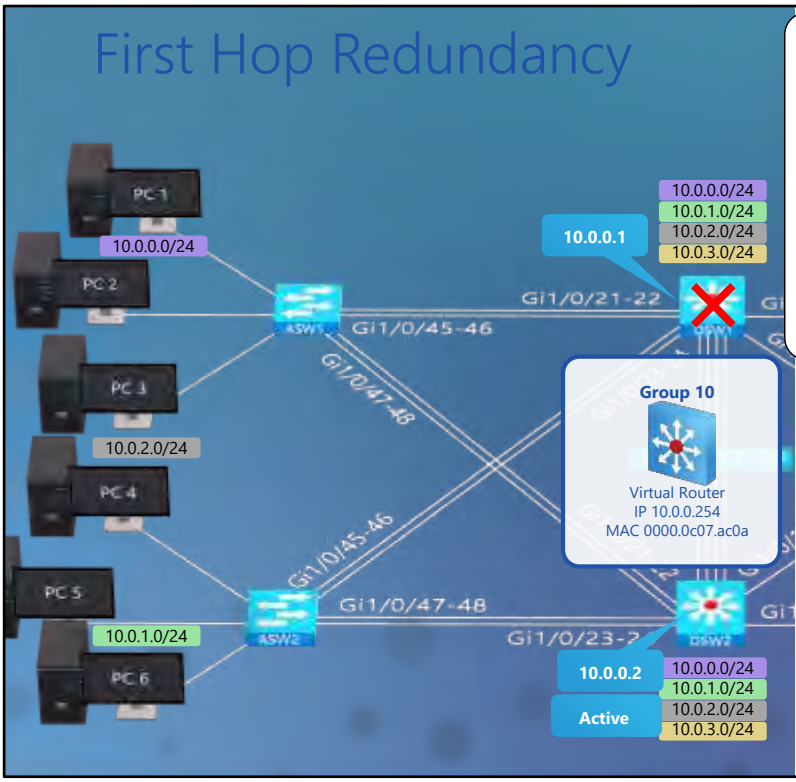



```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

C:\PC1> arp -a
  Internet Address      Physical Address      Type
  10.0.0.254            0000.0c07.ac0a     dynamic
…output omitted…
```

```
ASW1#show mac address-table dynamic
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0000.0c07.ac0a    DYNAMIC     PO13
```

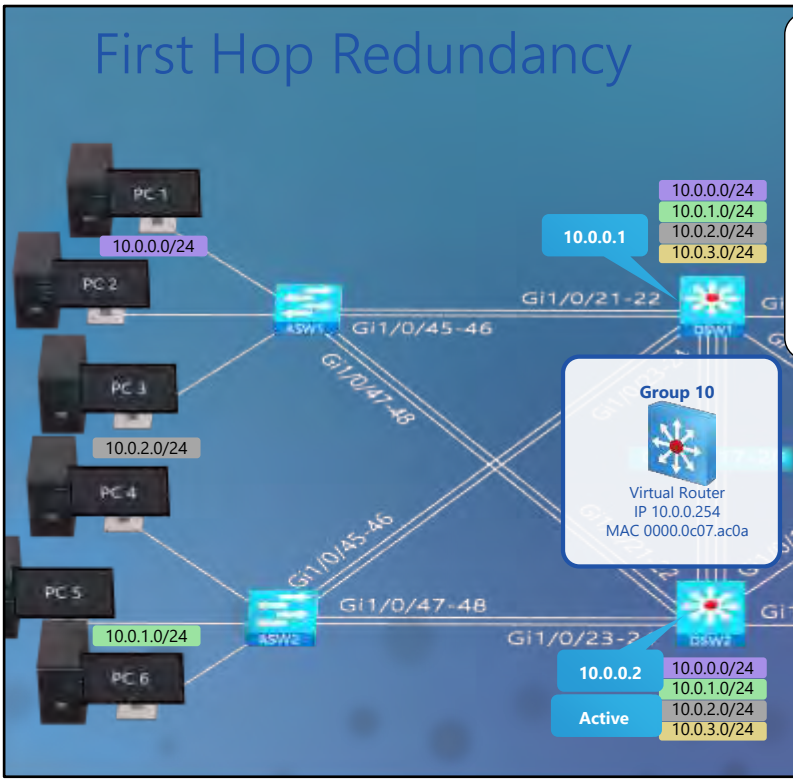
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



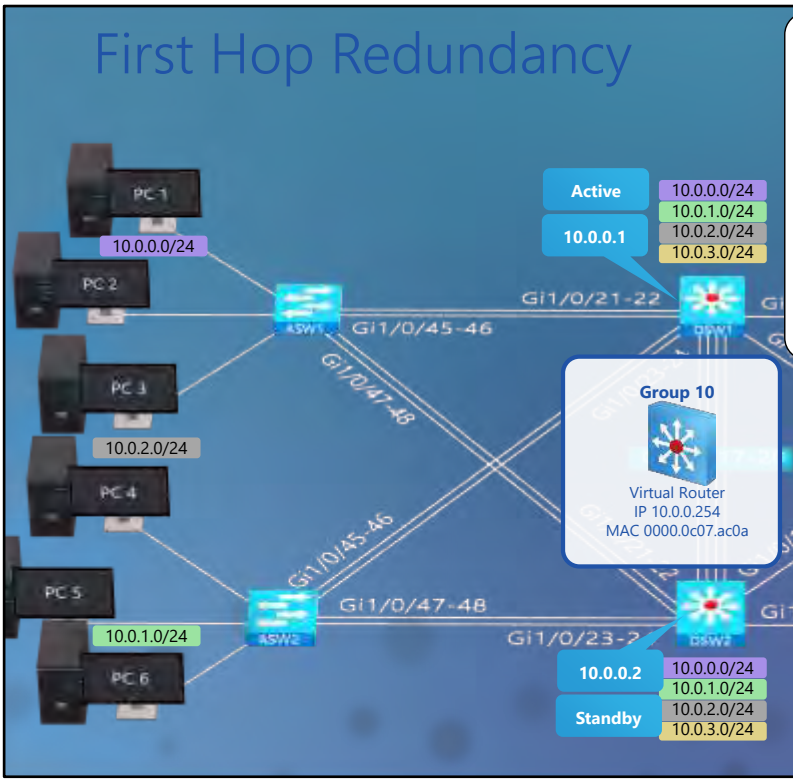

```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

C:\PC1> arp -a
  Internet Address      Physical Address      Type
  10.0.0.254            0000.0c07.ac0a     dynamic
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

C:\PC1> arp -a
  Internet Address      Physical Address      Type
  10.0.0.254            0000.0c07.ac0a     dynamic
…output omitted…
```

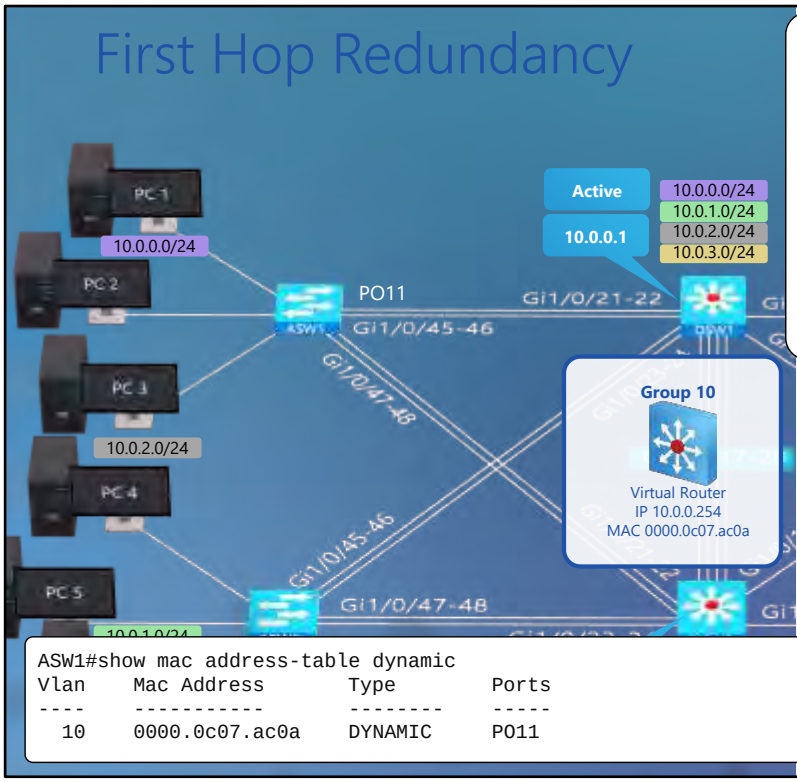
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.




```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

C:\PC1> arp -a
  Internet Address      Physical Address      Type
  10.0.0.254            0000.0c07.ac0a     dynamic
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

First Hop Redundancy




```
C:\PC1>ipconfig

Windows IP Configuration

Ethernet adapter PC1:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.0.0.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.254

C:\PC1> arp -a
  Internet Address      Physical Address      Type
  10.0.0.254            0000.0c07.ac0a     dynamic
…output omitted…
```

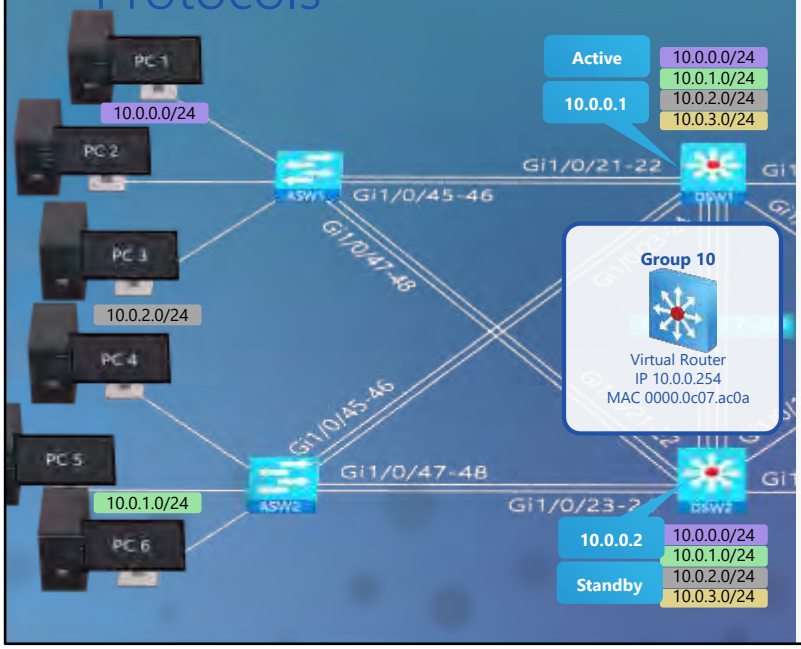
```
ASW1#show mac address-table dynamic
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0000.0c07.ac0a    DYNAMIC     PO11
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

First Hop Redundancy Protocols



HSRP – Hot Standby Router Protocol

- Cisco Proprietary
- Provides redundant gateways

VRRP – Virtual Router Redundancy Protocol

- Industry Standard
- Provides redundant gateways

GLBP – Gateway Load Balancing Protocol

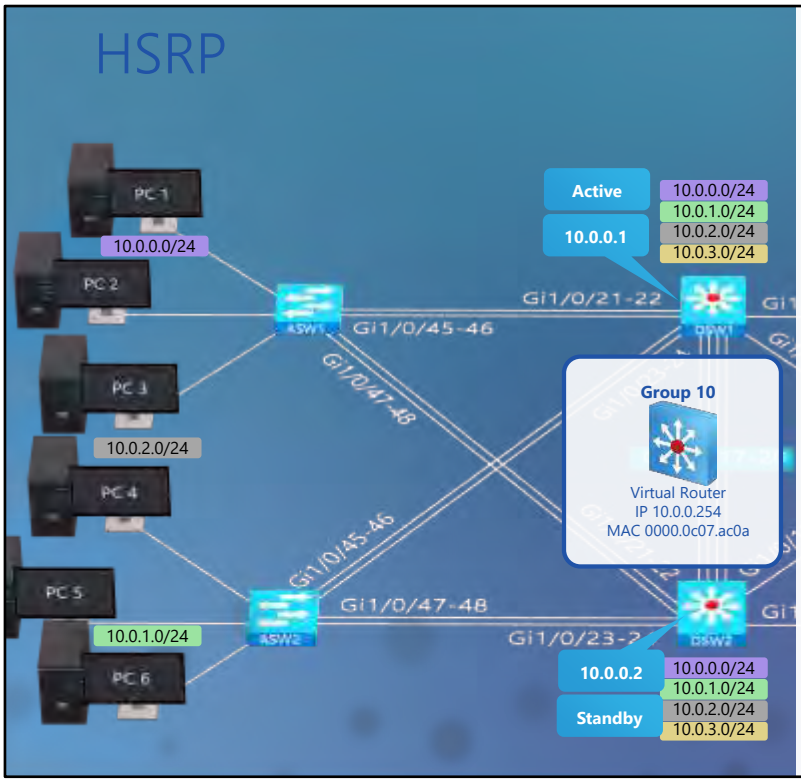
- Cisco Proprietary
- Provides redundant gateways and gateway load balancing

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Hot Standby Router Protocol (HSRP)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

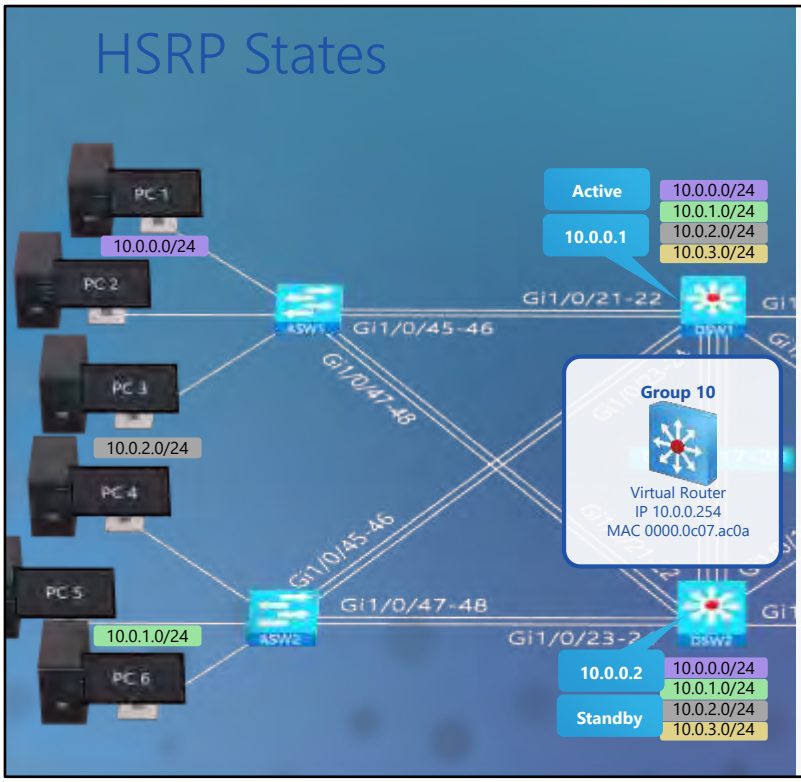
HSRP



- 1 Active Router per Group
  - Router with highest priority
  - Forwards packets
  - Responds to ARP requests
  - Sends and Receives Hello Packets
- 1 Standby Router per Group
  - Router with second highest priority
  - Sends and Receives Hello Packets
  - Waits for Active to fail so it can become Active
- 1 or more Listeners
  - Listens for Hello Packets
  - Waits for Active or Standby to fail to become Active or Standby

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

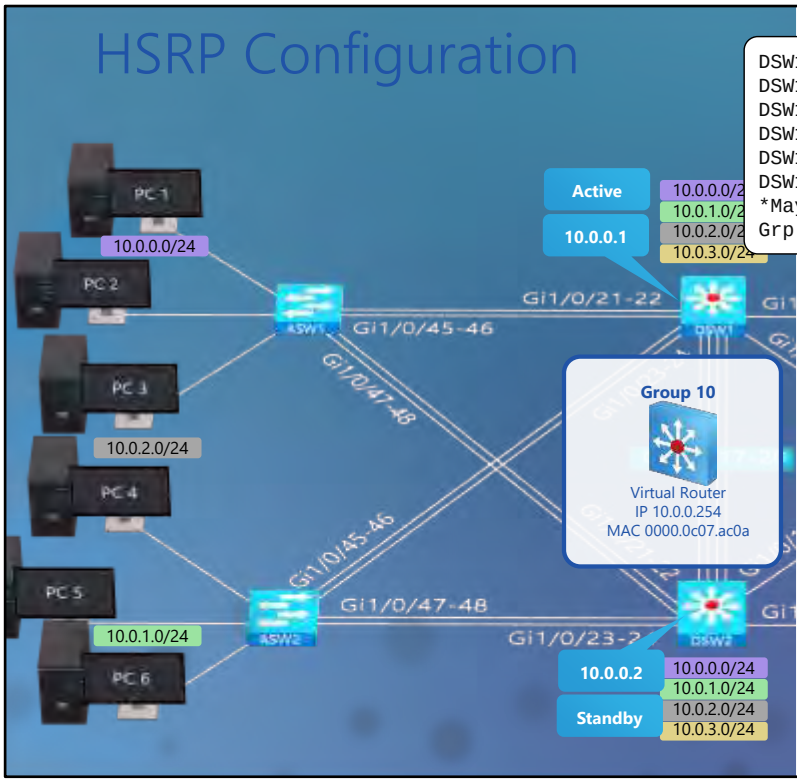
HSRP States



State	Definition
Initial	The state at the start. Also, it is the state after a configuration change or when an interface first comes up.
Listen	The router knows the virtual IP address. It listens for hello messages from other routers.
Speak	The router sends periodic hello messages and actively participates in the election of the active or standby router.
Standby	The router is a candidate to become the next active router and sends periodic hello messages.
Active	The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

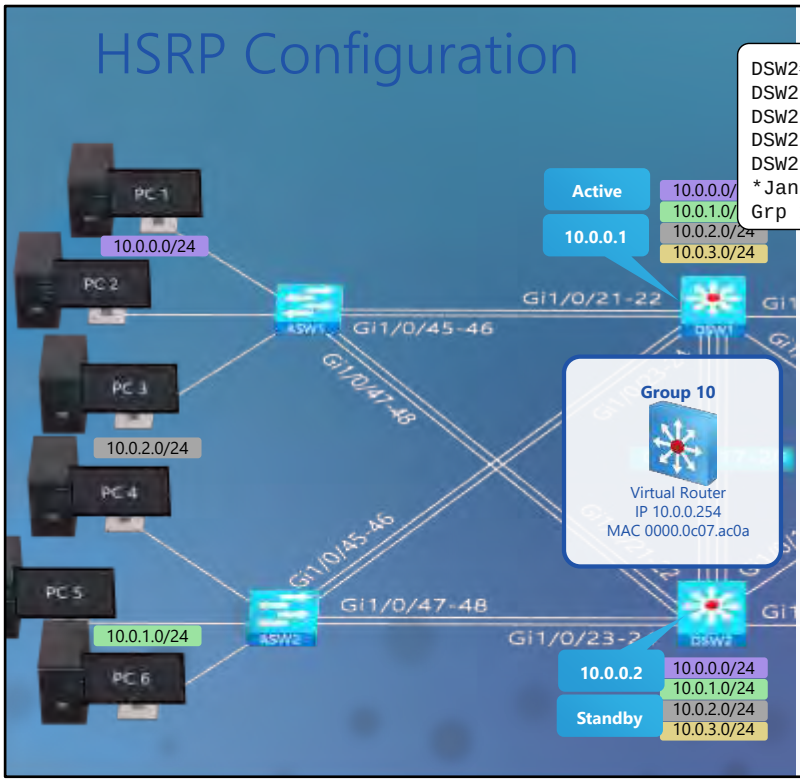
HSRP Configuration




```
DSW1#configure terminal
DSW1(config)#interface vlan 10
DSW1(config-if)#standby 10 ip 10.0.0.254
DSW1(config-if)#standby 10 priority 250
DSW1(config-if)#standby 10 preempt
DSW1(config-if)#
*May 15 11:40:58.308: %HSRP-5-STATECHANGE: Vlan10
Grp 10 state Standby -> Active
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

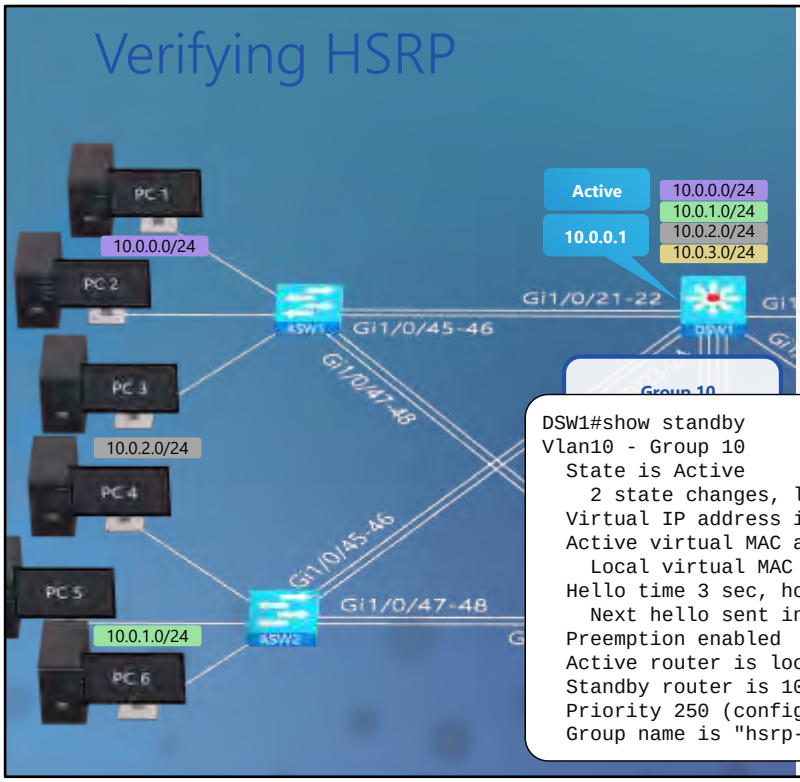
HSRP Configuration




```
DSW2#configure terminal
DSW2(config)#interface vlan 10
DSW2(config-if)#standby 10 ip 10.0.0.254
DSW2(config-if)#standby 10 preempt
DSW2(config-if)#
*Jan 17 06:22:53.792: %HSRP-5-STATECHANGE: Vlan10
Grp 10 state Speak -> Standby
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

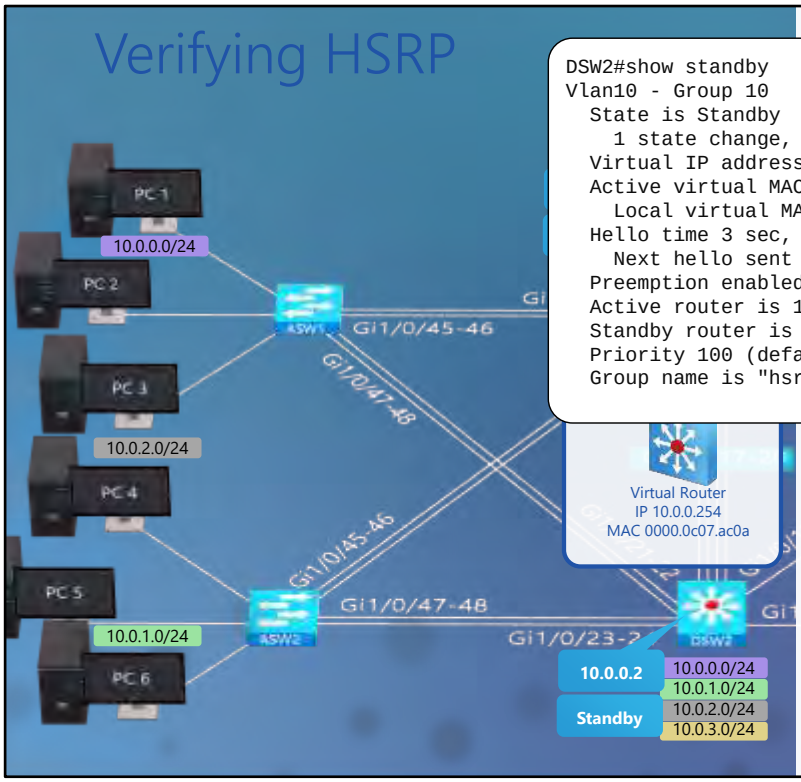
Verifying HSRP




```
DSW1#show standby
Vlan10 - Group 10
  State is Active
    2 state changes, last state change 00:10:11
  Virtual IP address is 10.0.0.254
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.240 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.0.2, priority 100 (expires in 10.096 sec)
  Priority 250 (configured 250)
  Group name is "hsrp-Vl10-10" (default)
```

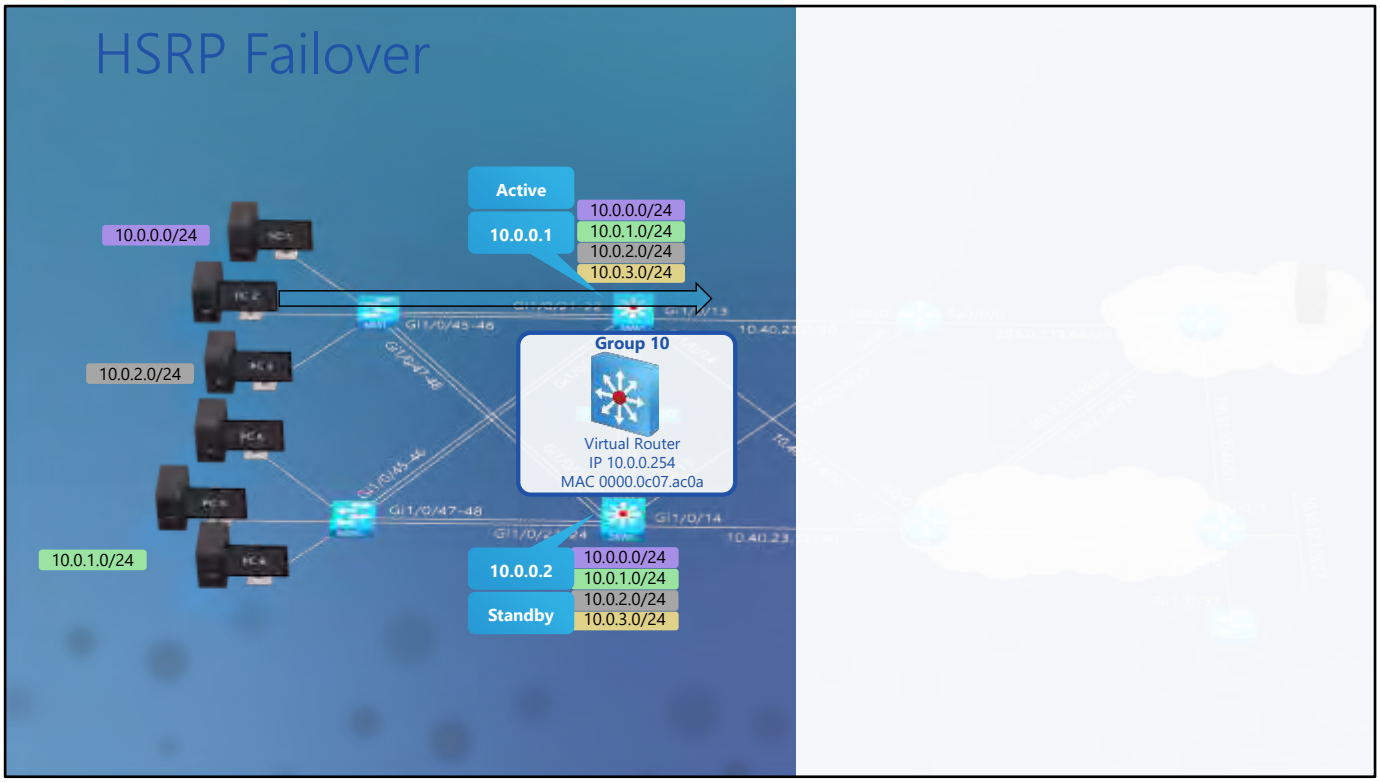
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying HSRP

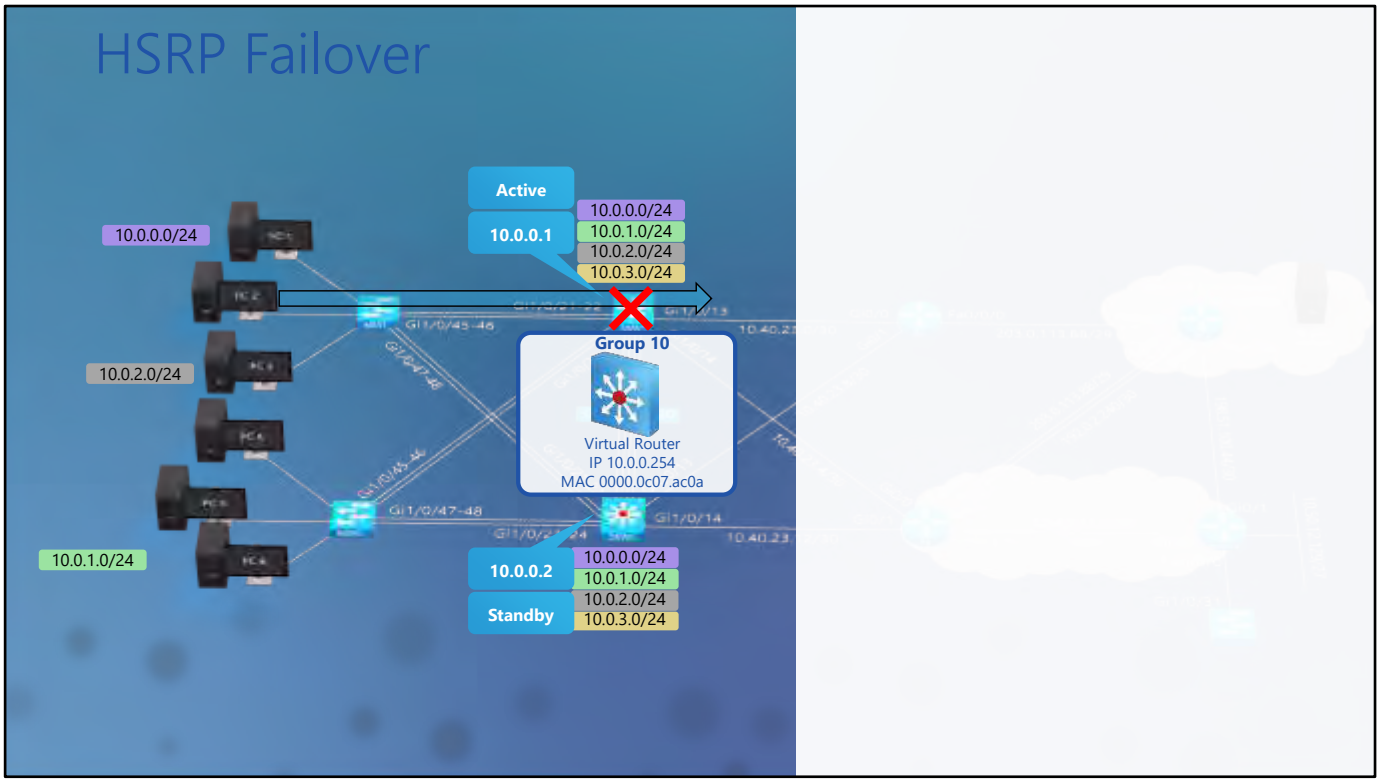



```
DSW2#show standby
Vlan10 - Group 10
  State is Standby
    1 state change, last state change 00:03:33
  Virtual IP address is 10.0.0.254
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.192 secs
  Preemption enabled
  Active router is 10.0.0.1, priority 250 (expires in 9.040 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Vl10-10" (default)
```

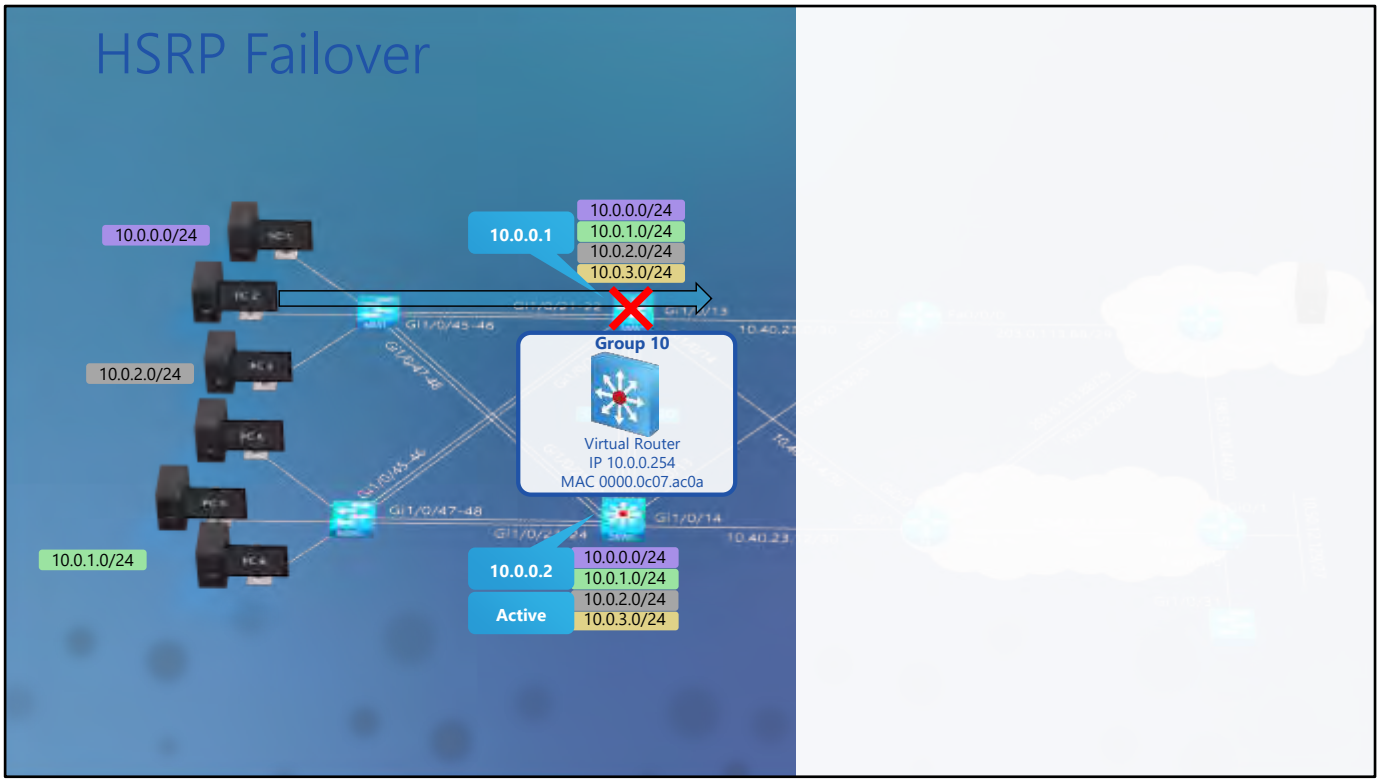
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



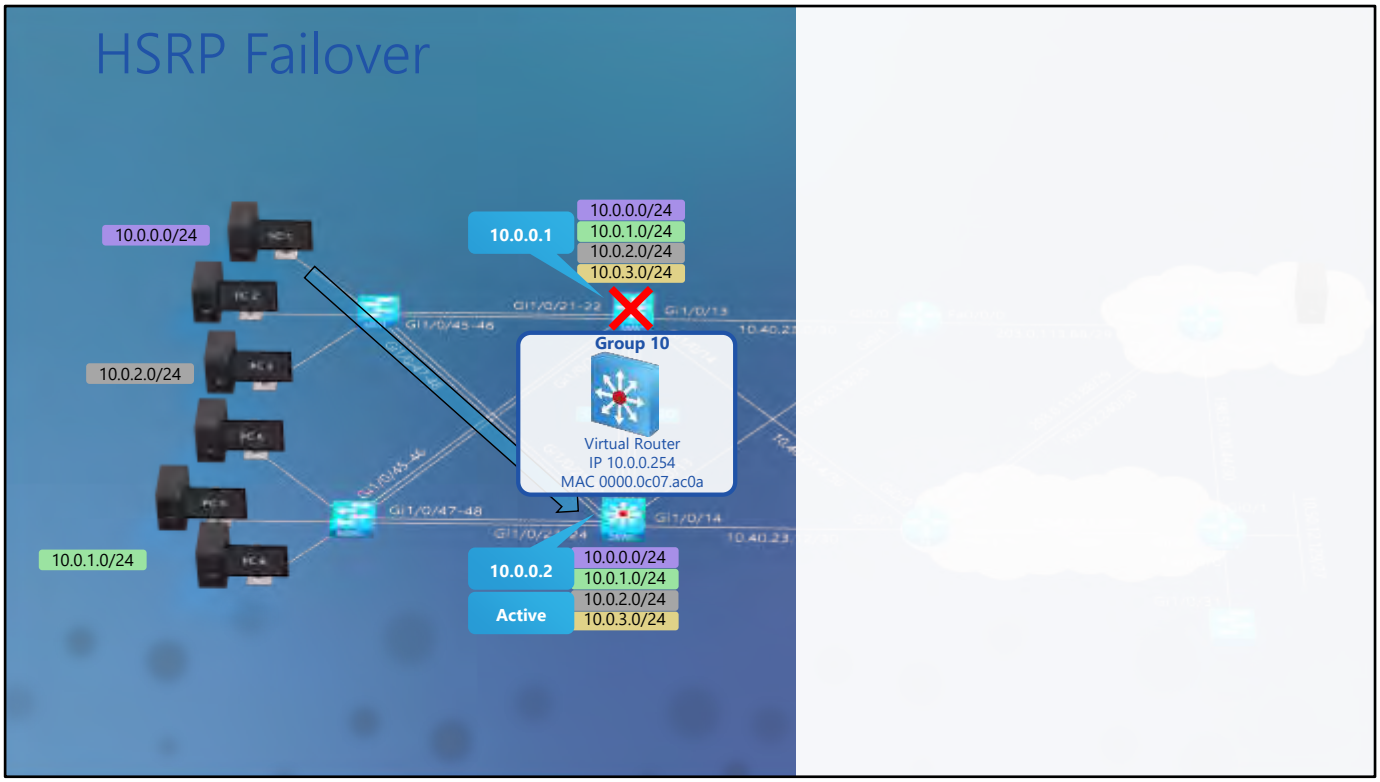
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



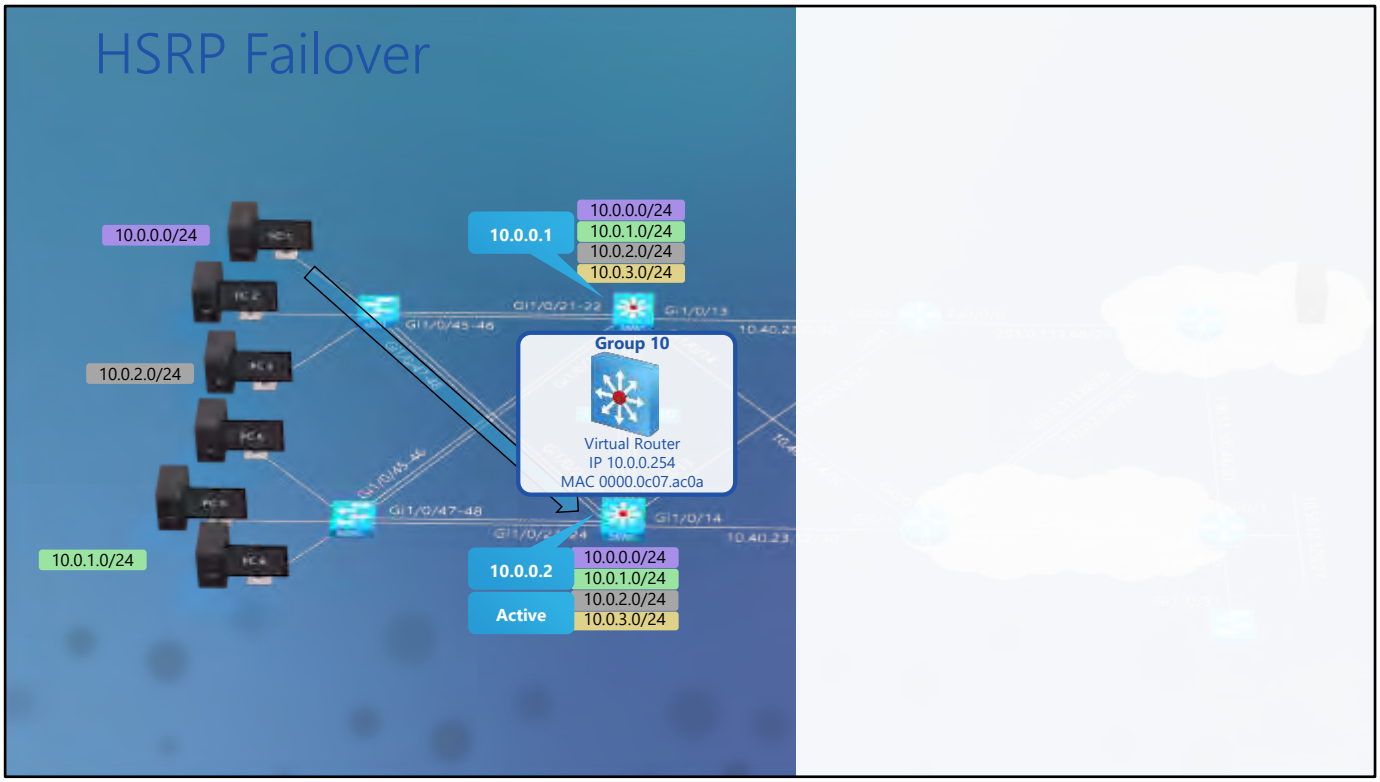
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



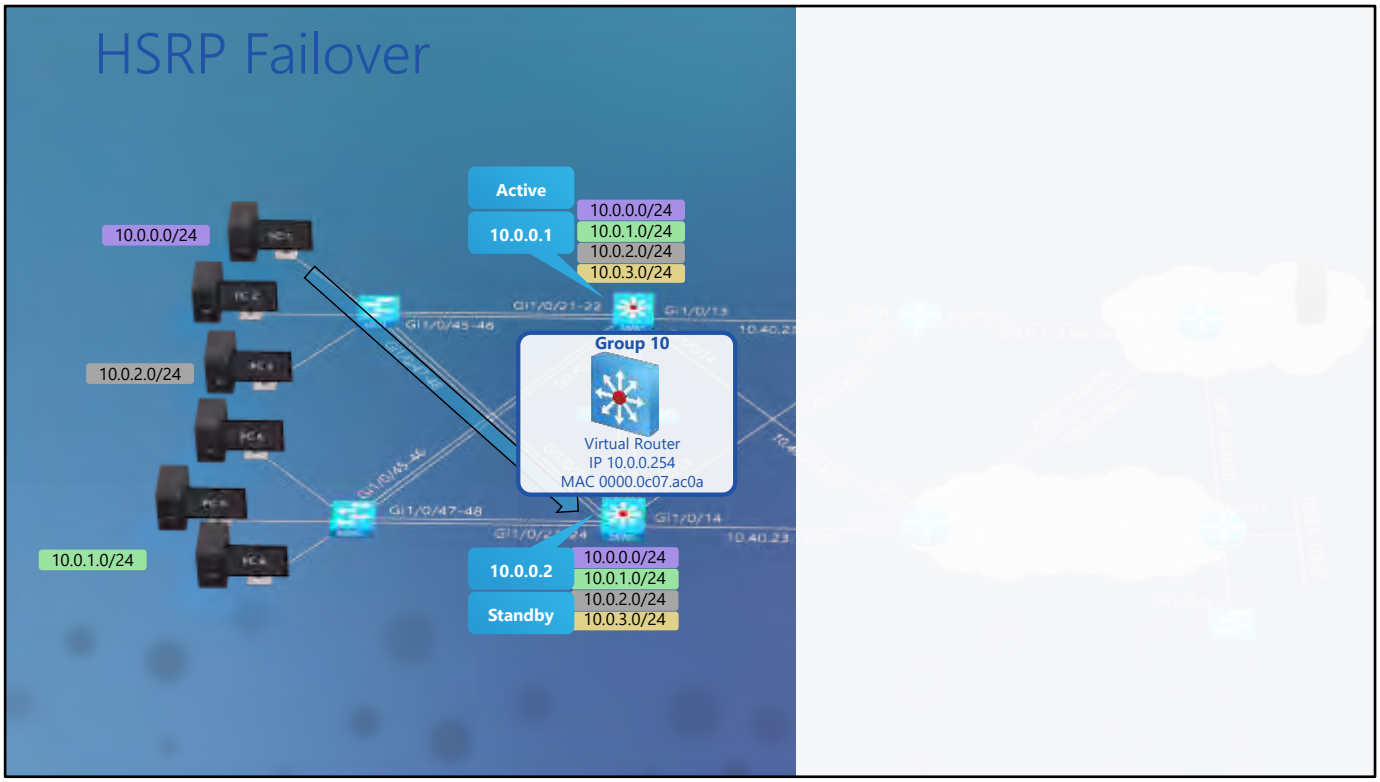
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



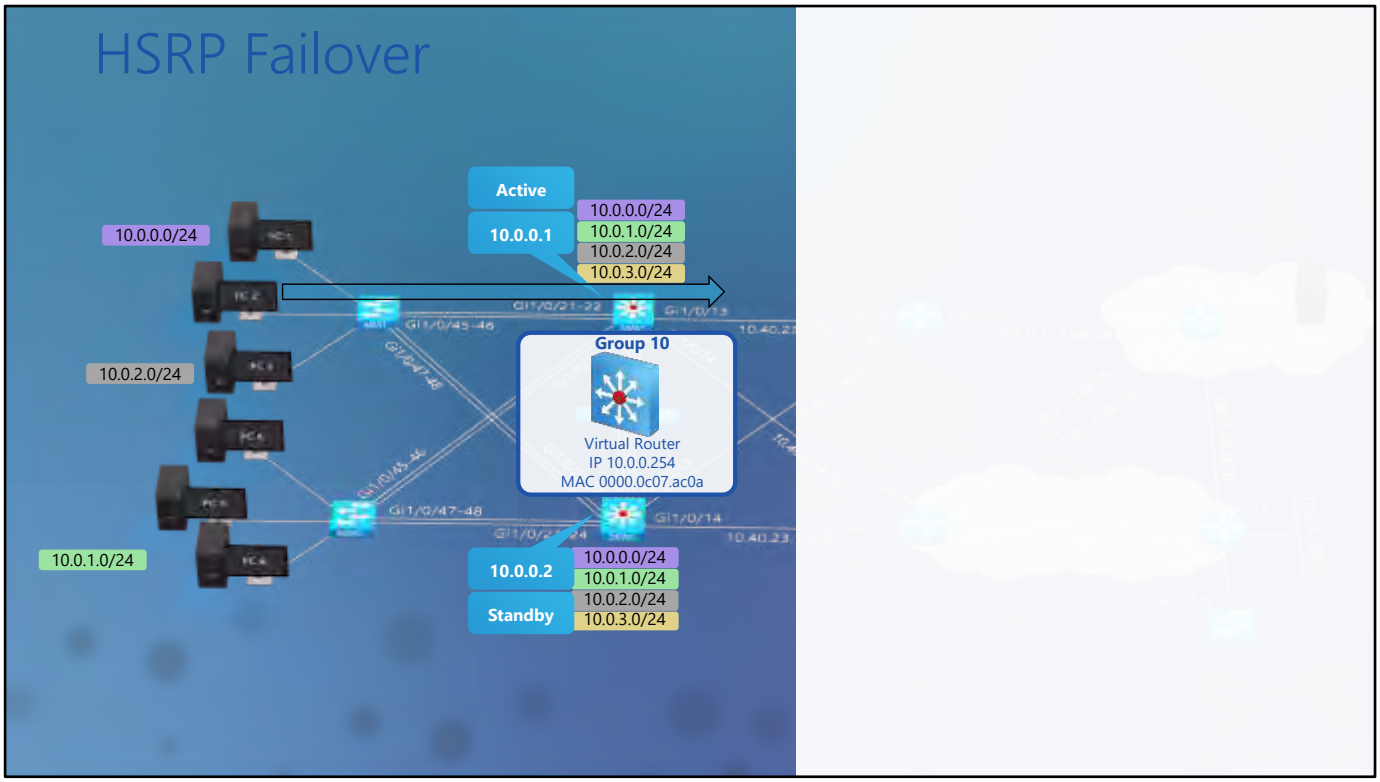
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



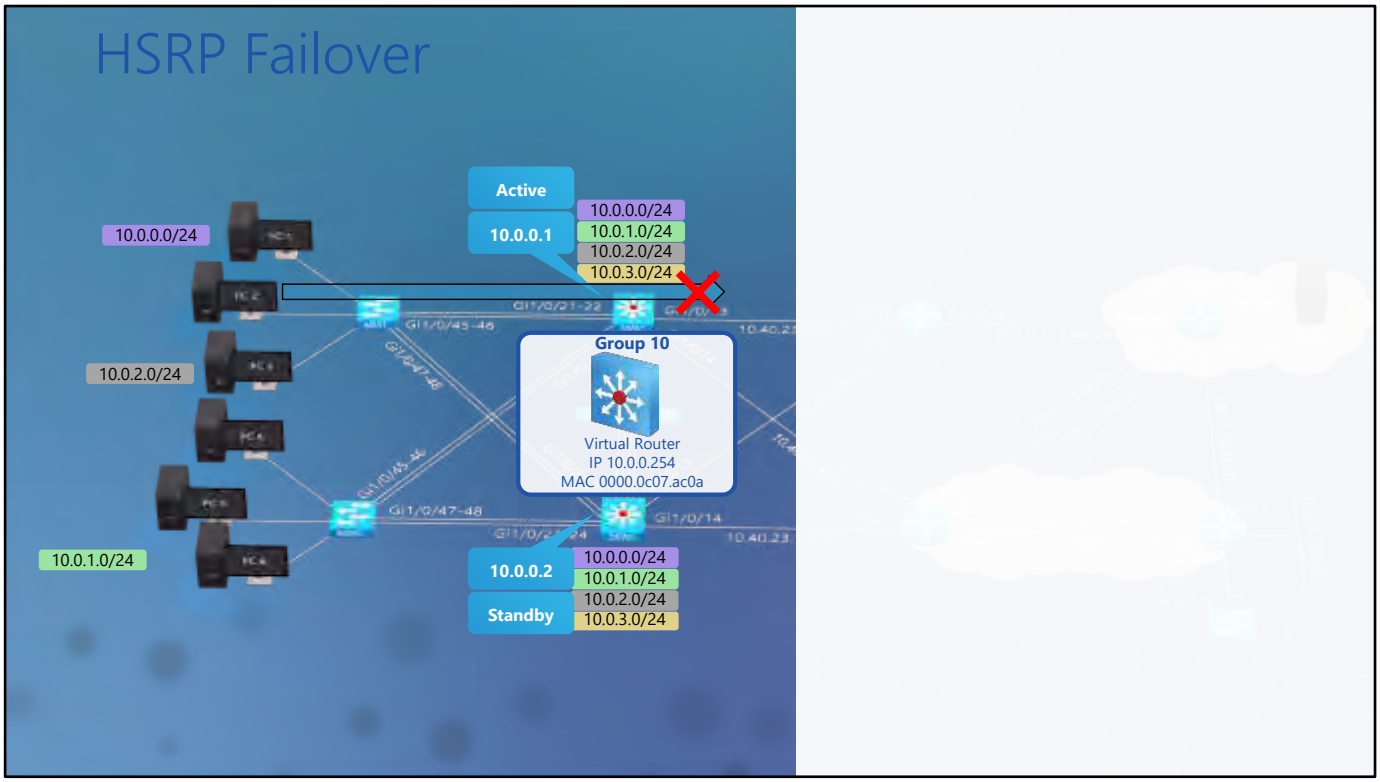
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

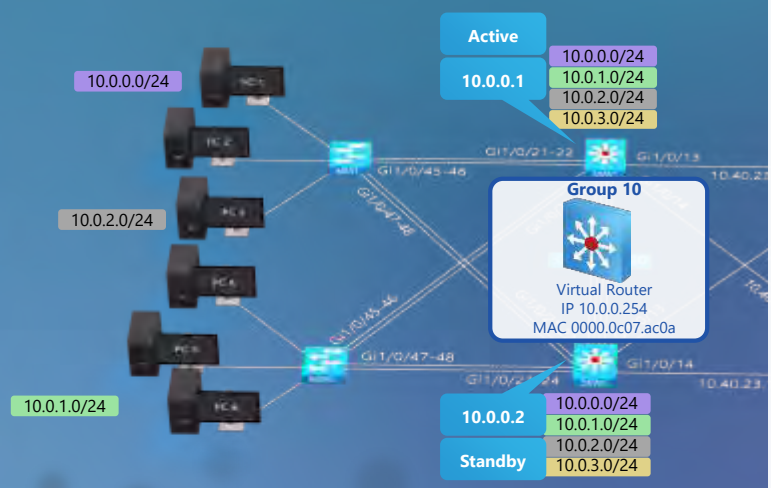


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

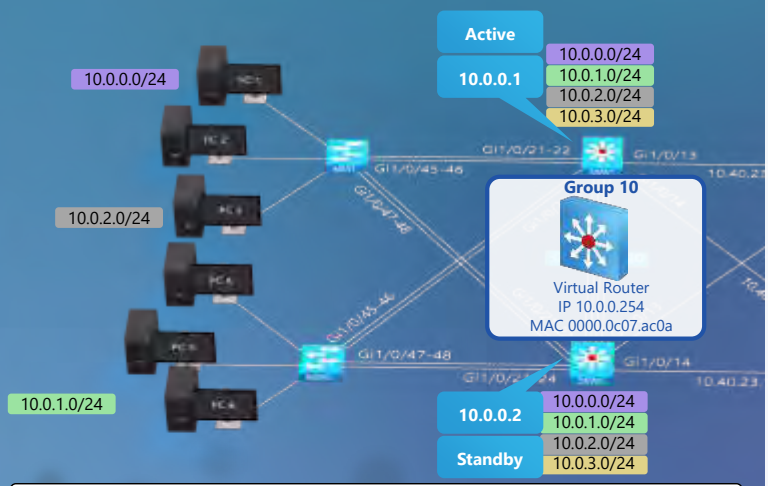
HSRP Tracking



Keep track of the status of an interface and if it goes down decrement the priority of the Active device to a value that is lower than the standby, so the standby becomes active.

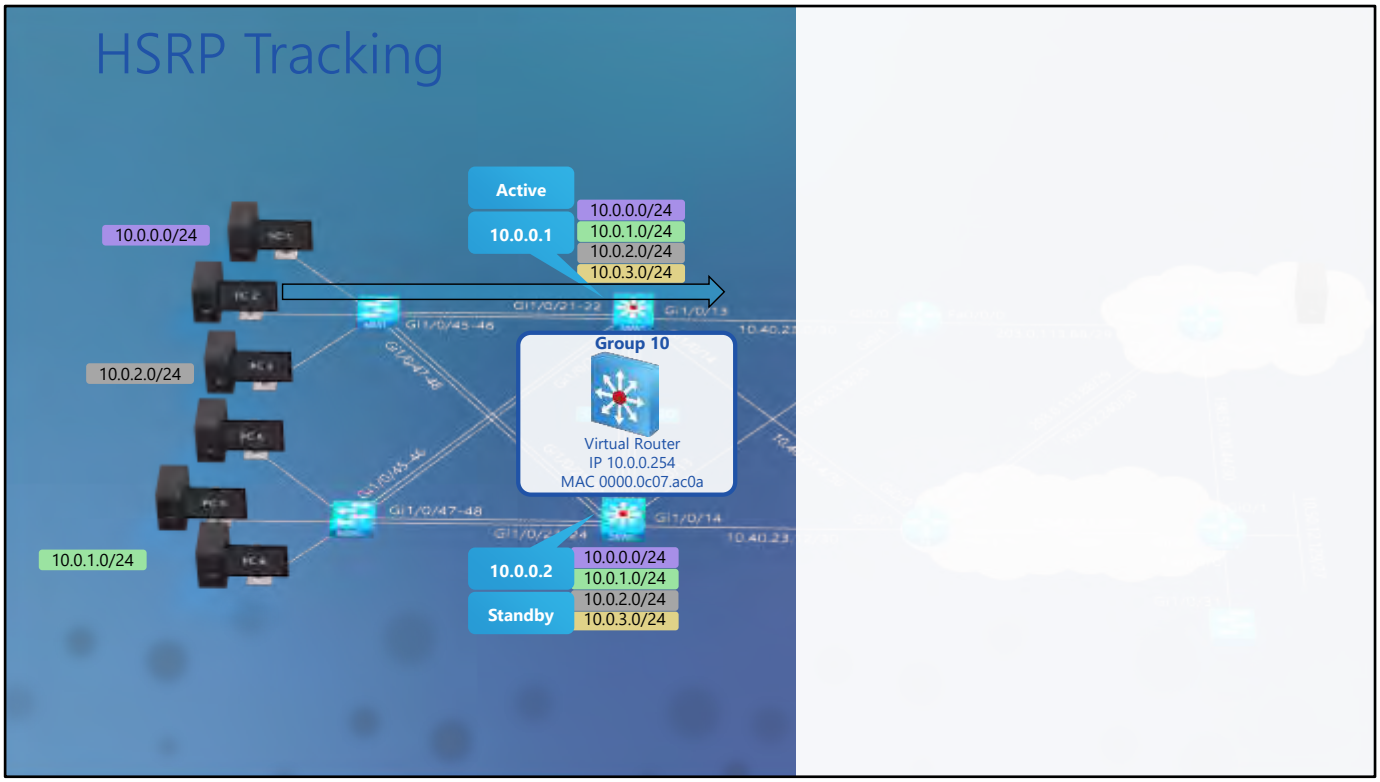
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Tracking



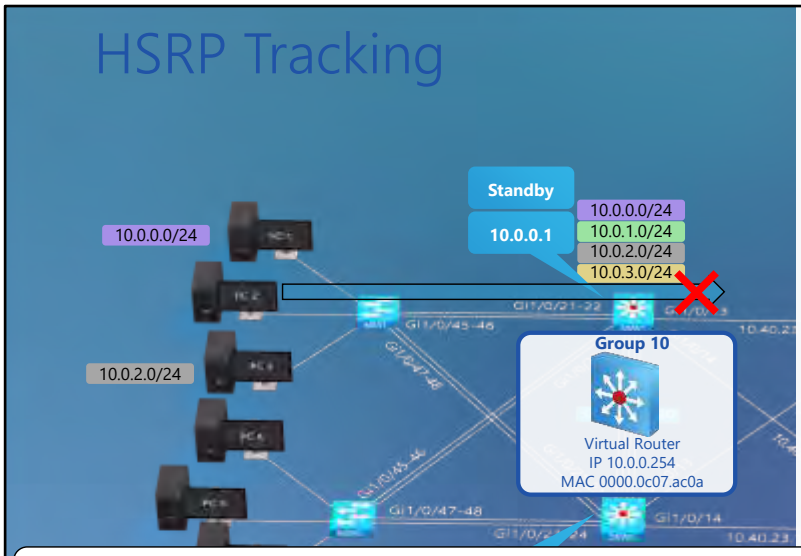

```
DSW1#configure terminal
DSW1(config)#interface vlan 10
DSW1(config-if)#standby 10 track gigabitEthernet 1/0/13 250
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

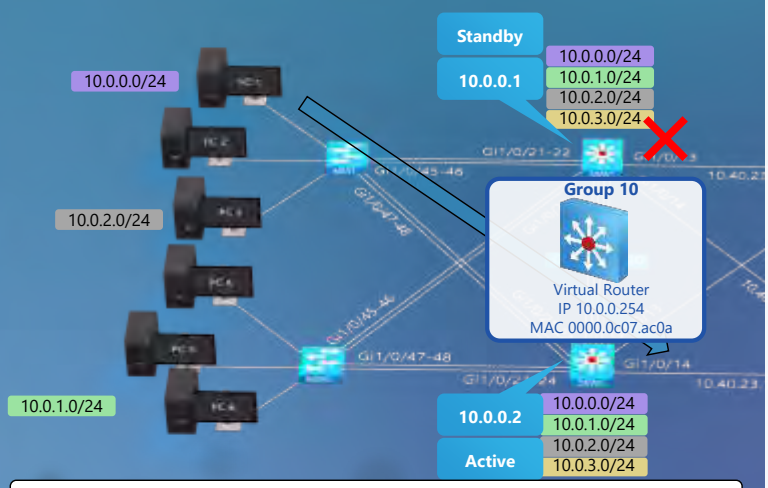
HSRP Tracking




```
DSW1#configure terminal
DSW1(config)#int gigabitEthernet 1/0/13
DSW1(config-if)#shut
DSW1(config-if)#
%TRACKING-5-STATE: 1 interface Gi1/0/13 line-protocol Up->Down
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active -> Speak
DSW1(config-if)#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

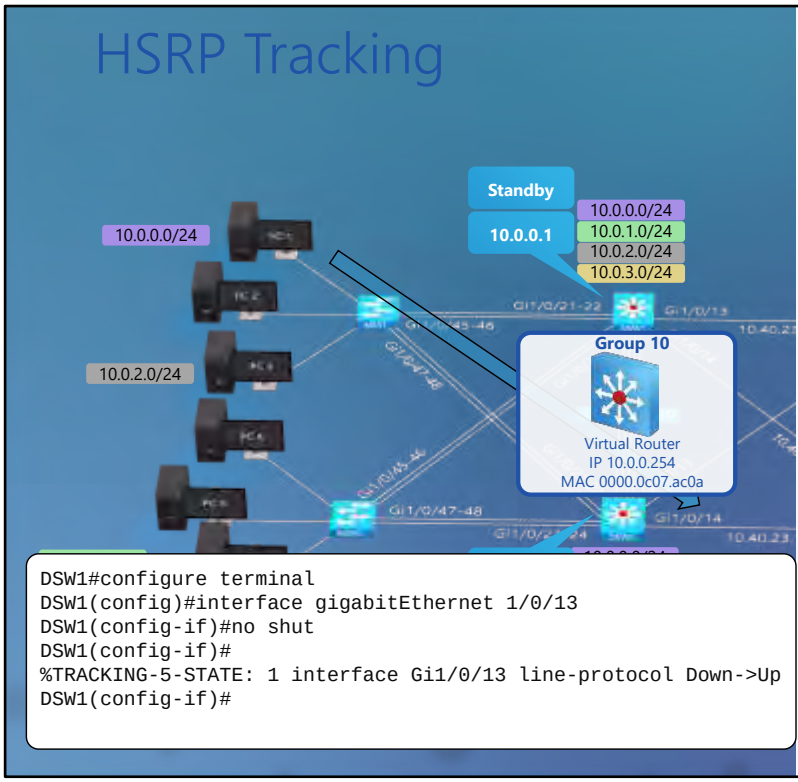
HSRP Tracking




```
DSW2#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
DSW2#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

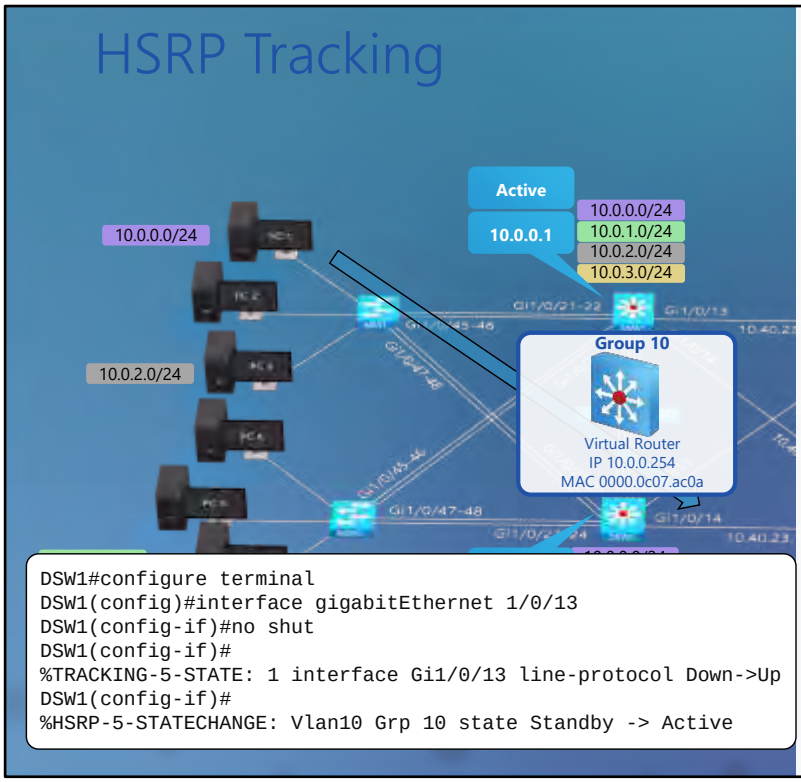
HSRP Tracking




```
DSW1#configure terminal
DSW1(config)#interface gigabitEthernet 1/0/13
DSW1(config-if)#no shut
DSW1(config-if)#
%TRACKING-5-STATE: 1 interface Gi1/0/13 line-protocol Down->Up
DSW1(config-if)#
```

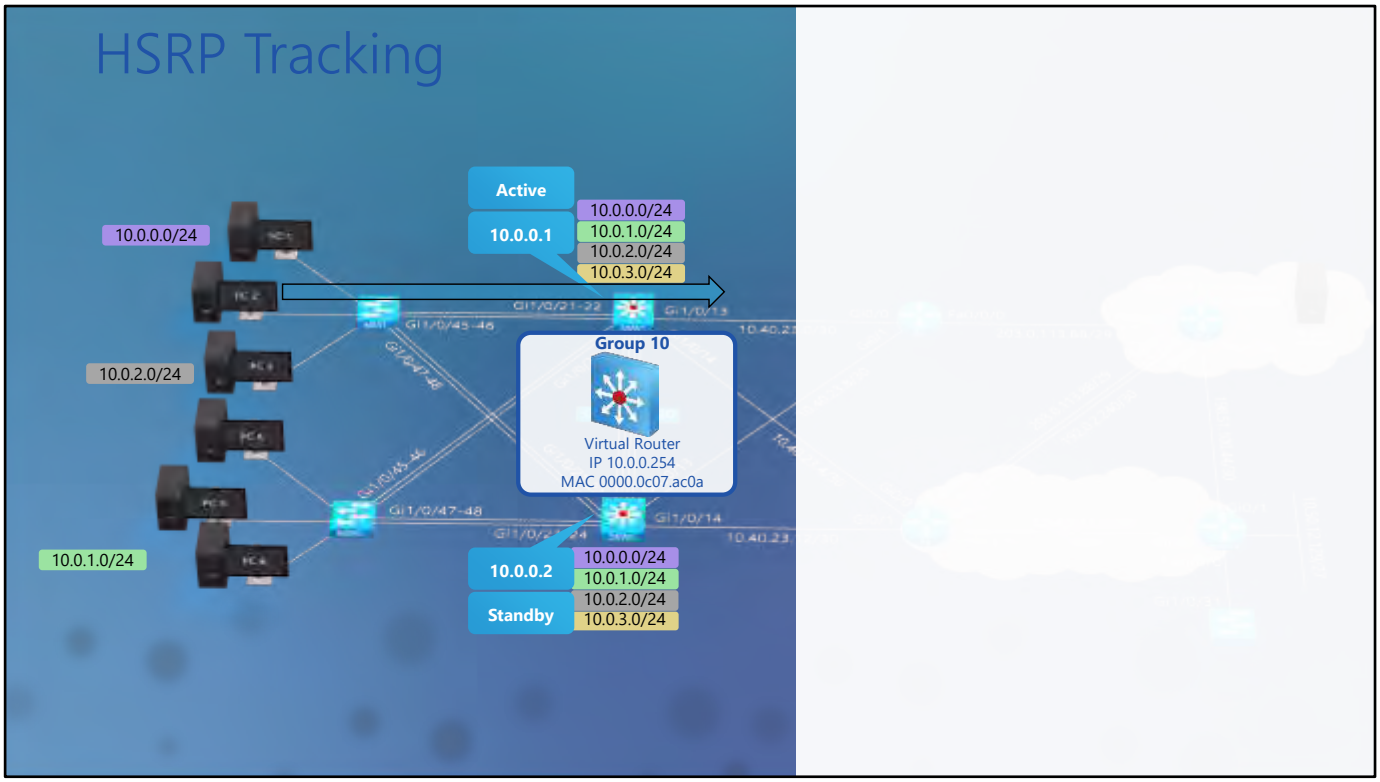
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Tracking



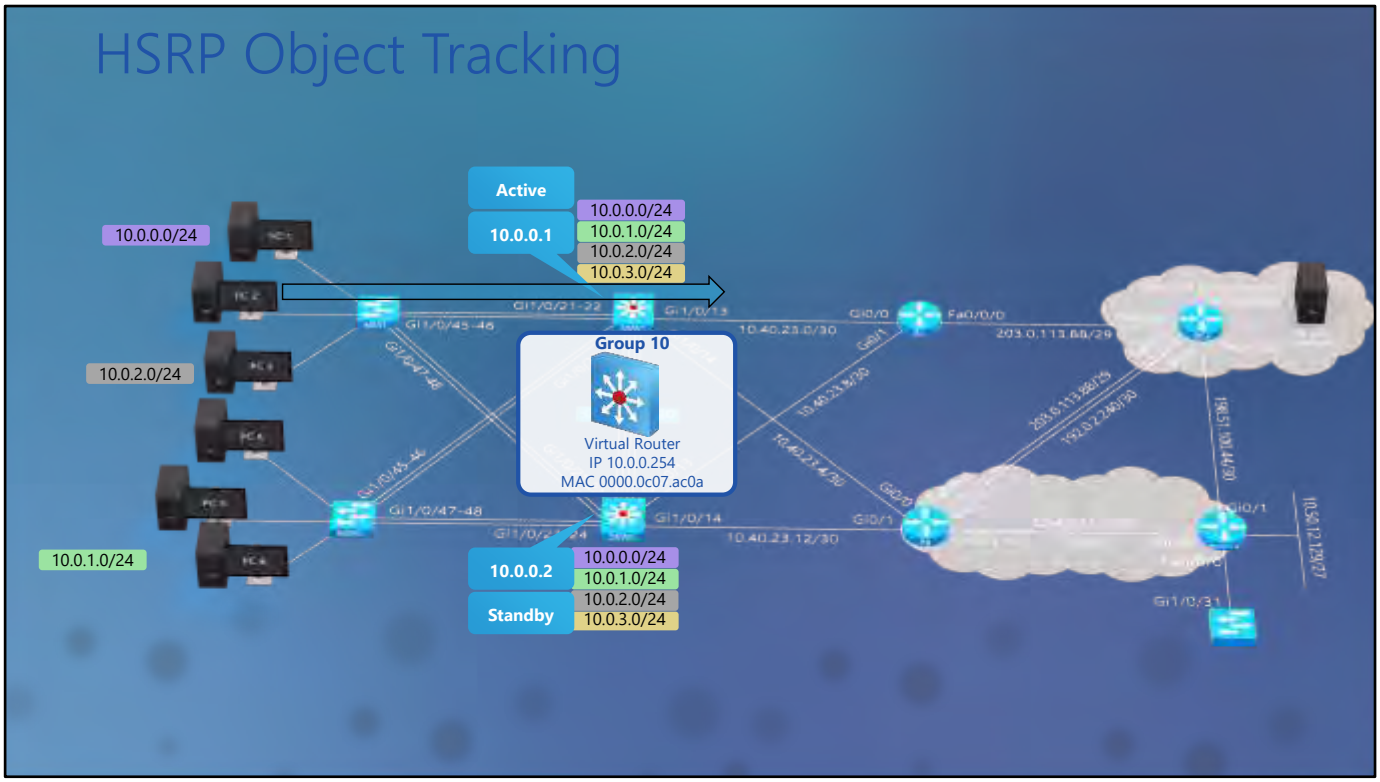

```
DSW1#configure terminal
DSW1(config)#interface gigabitEthernet 1/0/13
DSW1(config-if)#no shut
DSW1(config-if)#
%TRACKING-5-STATE: 1 interface Gi1/0/13 line-protocol Down->Up
DSW1(config-if)#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



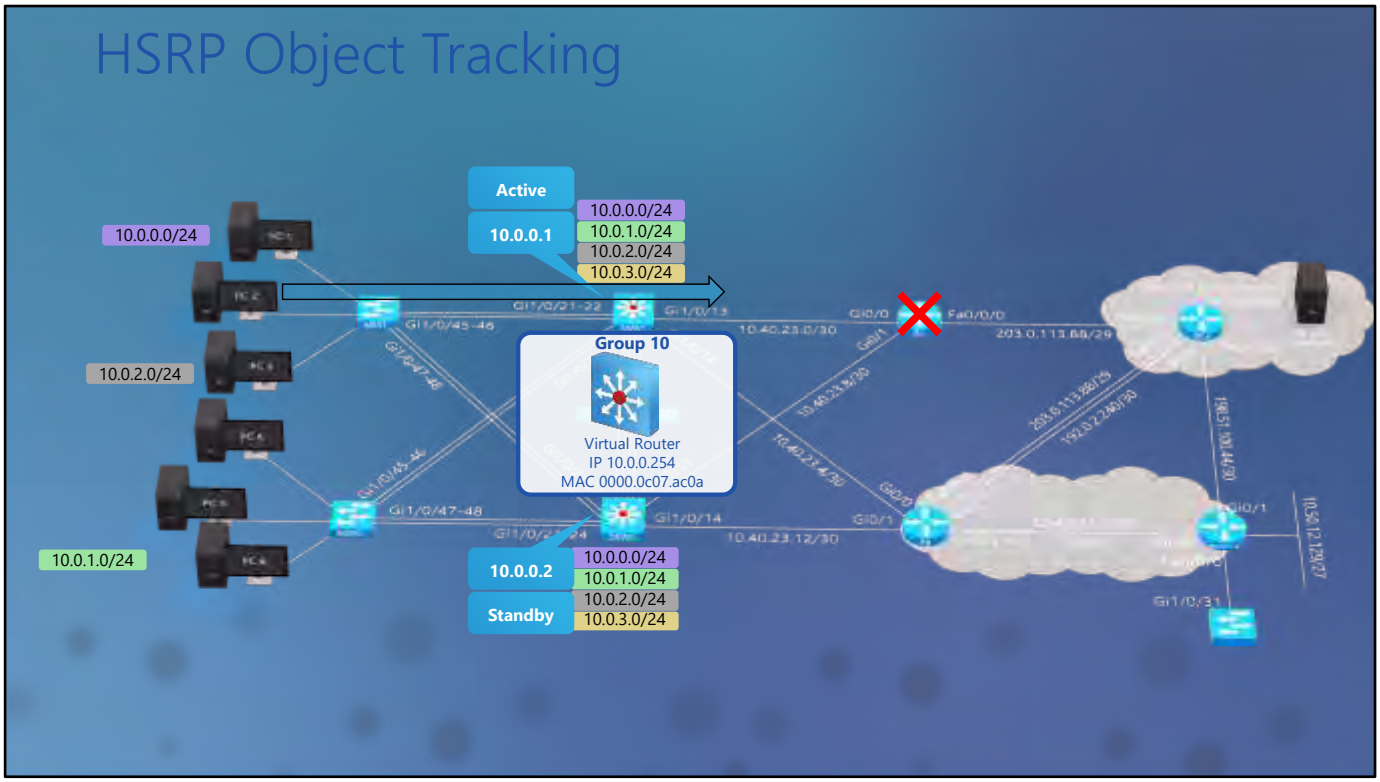
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Object Tracking



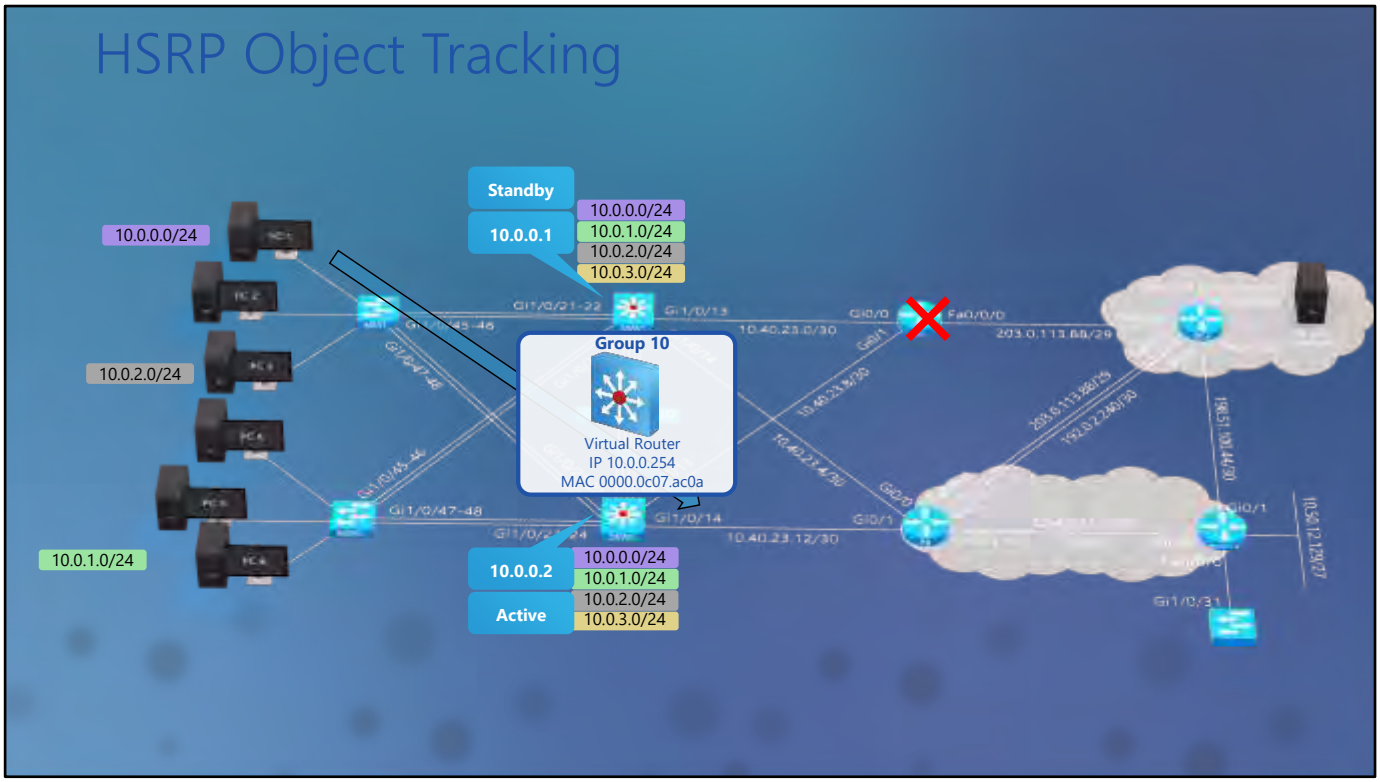
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Object Tracking



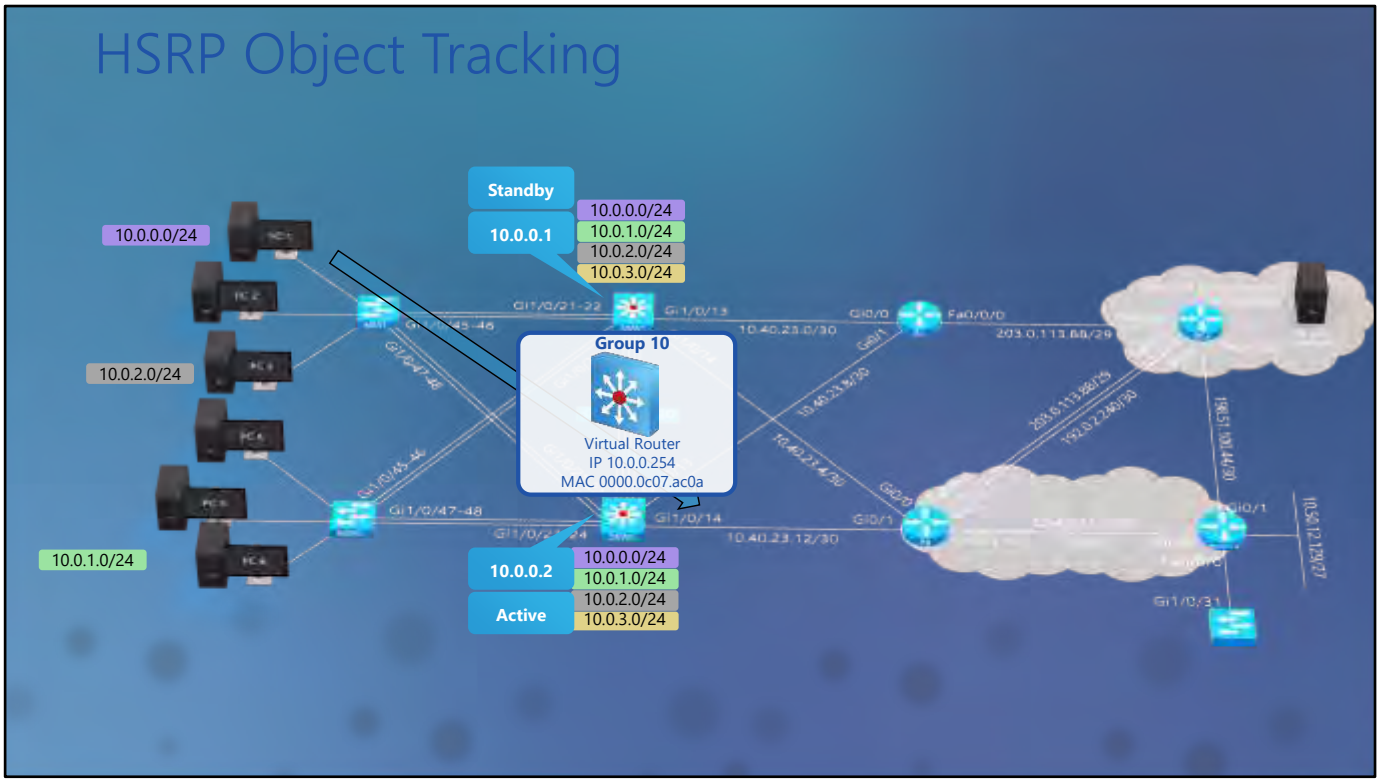
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Object Tracking



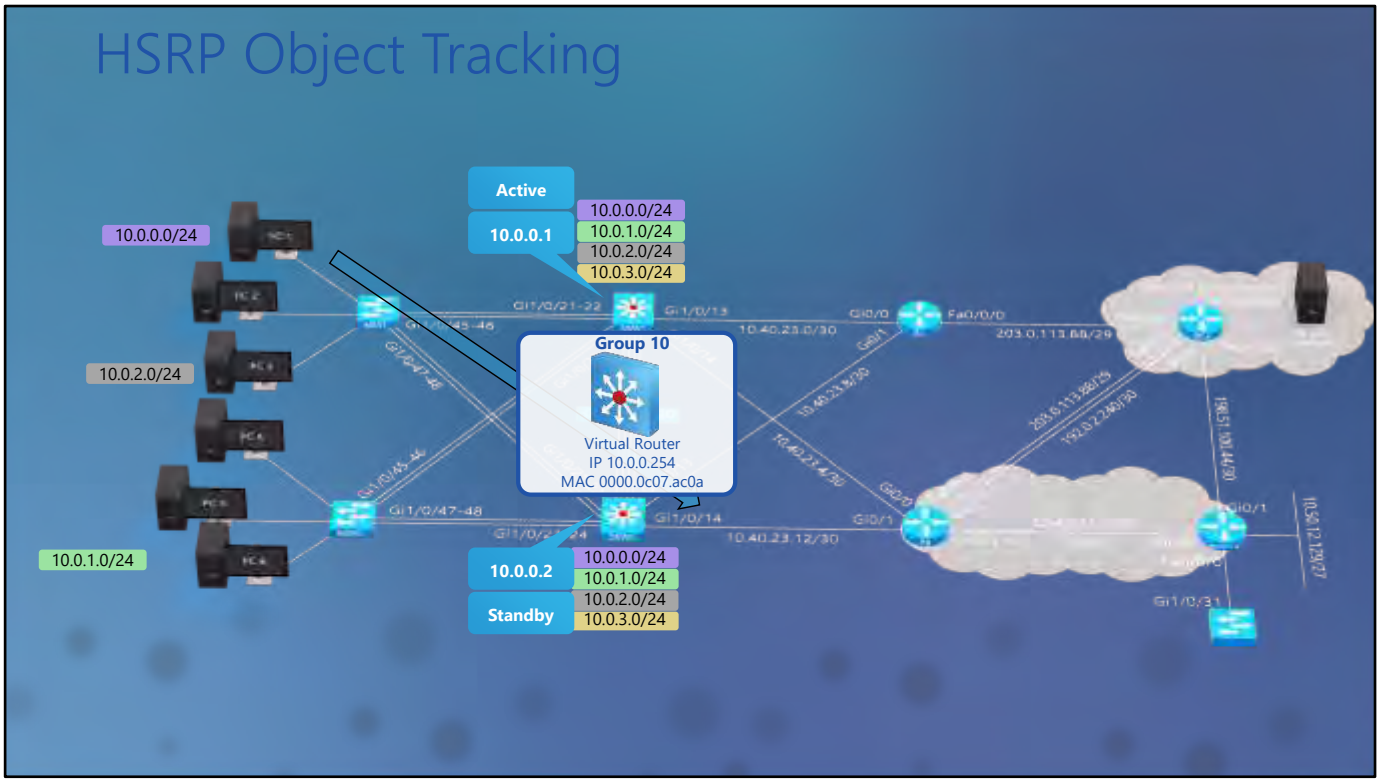
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Object Tracking



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

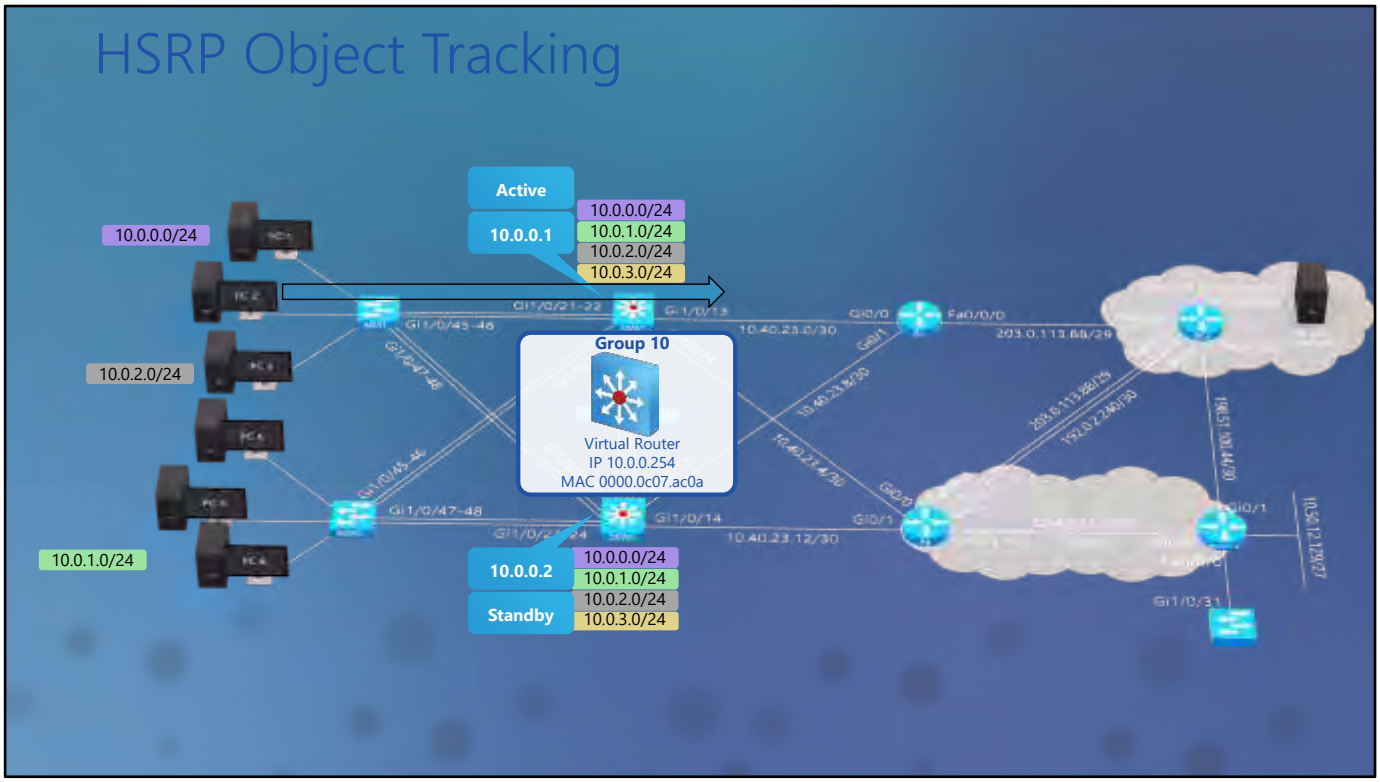
HSRP Object Tracking



©2023 by StormWind LLC. All rights reserved.

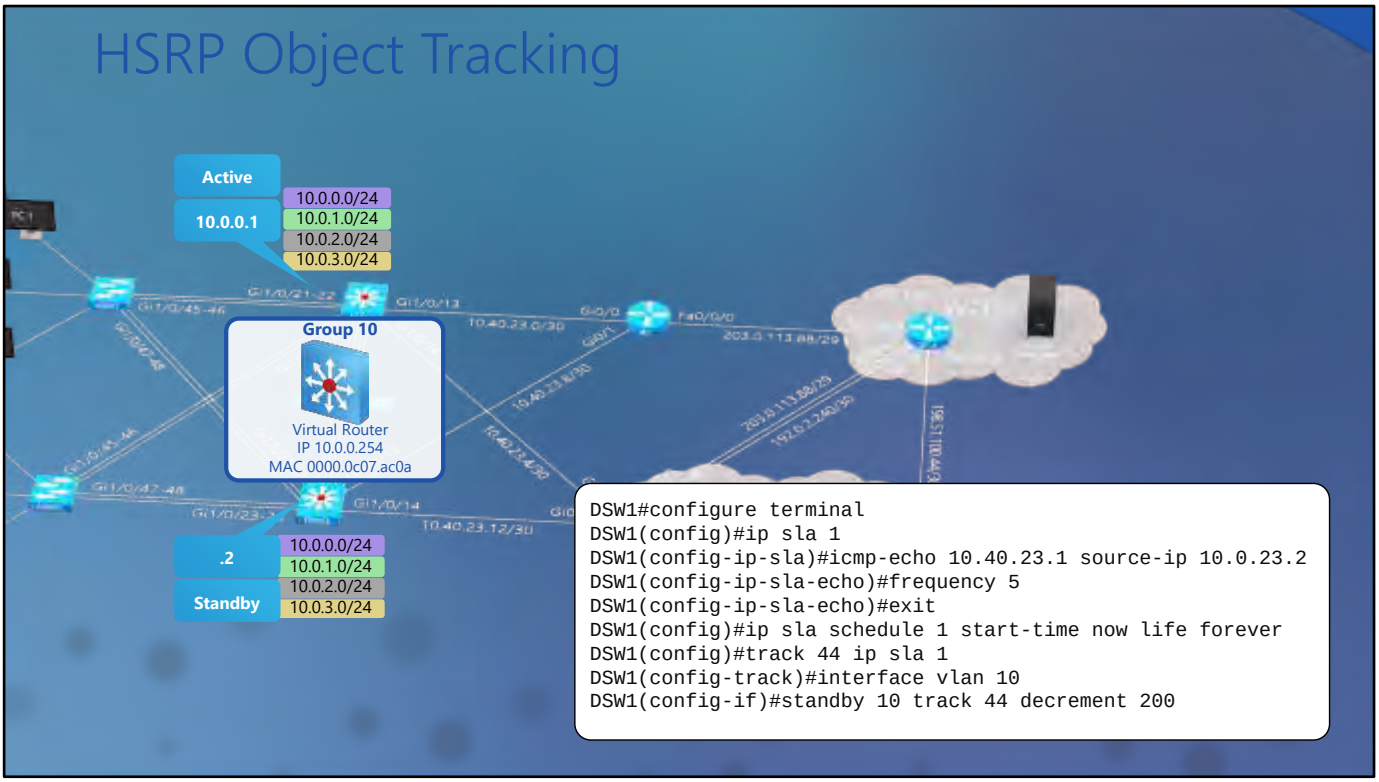
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Object Tracking



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

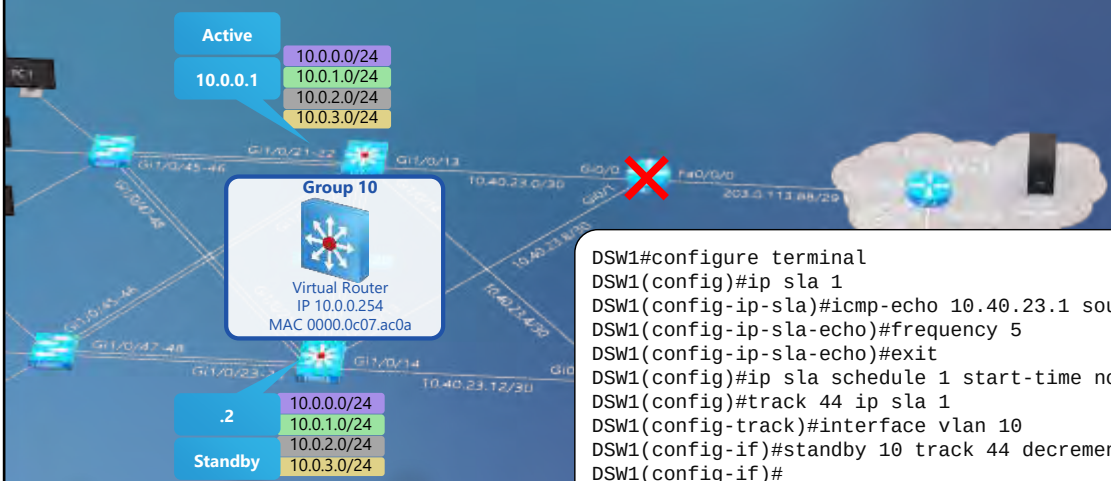
HSRP Object Tracking




```
DSW1#configure terminal
DSW1(config)#ip sla 1
DSW1(config-ip-sla)#icmp-echo 10.40.23.1 source-ip 10.0.23.2
DSW1(config-ip-sla-echo)#frequency 5
DSW1(config-ip-sla-echo)#exit
DSW1(config)#ip sla schedule 1 start-time now life forever
DSW1(config)#track 44 ip sla 1
DSW1(config-track)#interface vlan 10
DSW1(config-if)#standby 10 track 44 decrement 200
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

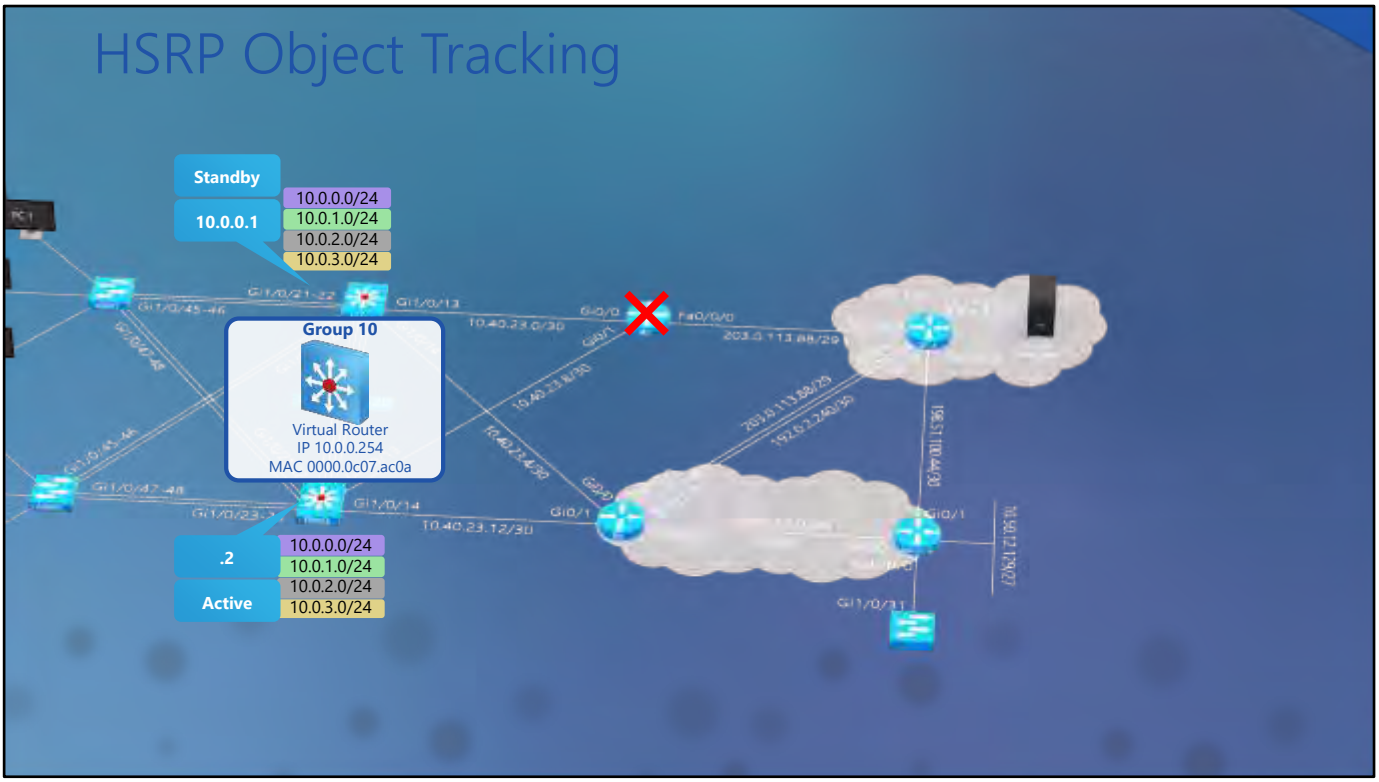
HSRP Object Tracking




```
DSW1#configure terminal
DSW1(config)#ip sla 1
DSW1(config-ip-sla)#icmp-echo 10.40.23.1 source-ip 10.0.23.2
DSW1(config-ip-sla-echo)#frequency 5
DSW1(config-ip-sla-echo)#exit
DSW1(config)#ip sla schedule 1 start-time now life forever
DSW1(config)#track 44 ip sla 1
DSW1(config-track)#interface vlan 10
DSW1(config-if)#standby 10 track 44 decrement 200
DSW1(config-if)#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Active -> Speak
DSW1(config-if)#end
DSW1#
%HSRP-5-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

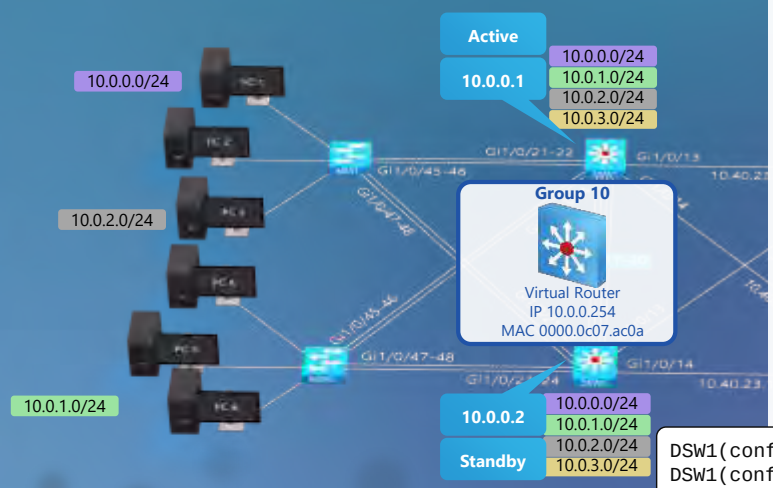
HSRP Object Tracking



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Timers



Timers can support millisecond values

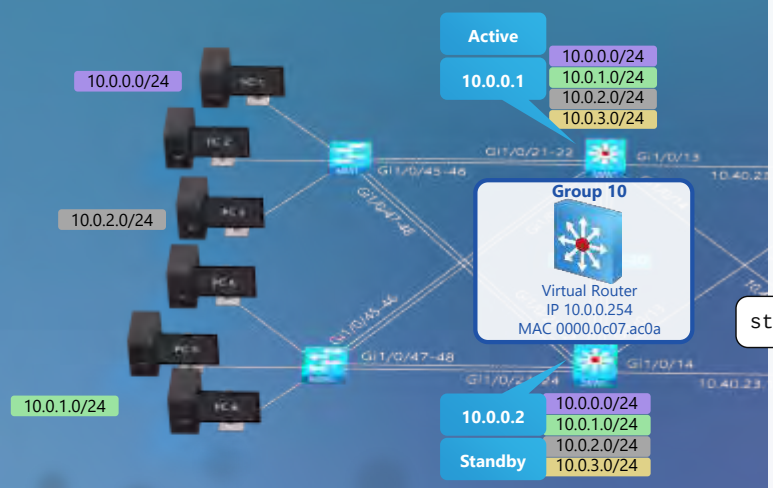
It's recommended to delay pre-emption to allow Active Router to come back online and allow for Routing Protocol convergence.

To change the timers & preemption timer:

```
DSW1(config-if)#standby 10 timers 1 3
DSW1(config-if)#standby 10 timers msec 500 msec 2750
DSW1(config-if)#standby 10 preempt delay ?
  minimum  Delay at least this long
  reload   Delay after reload
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Authentication



HSRP supports cleartext and MD5 authentication as well as key chains

Keys are associated to SVI's or interfaces

Matching configuration is required on HSRP peers

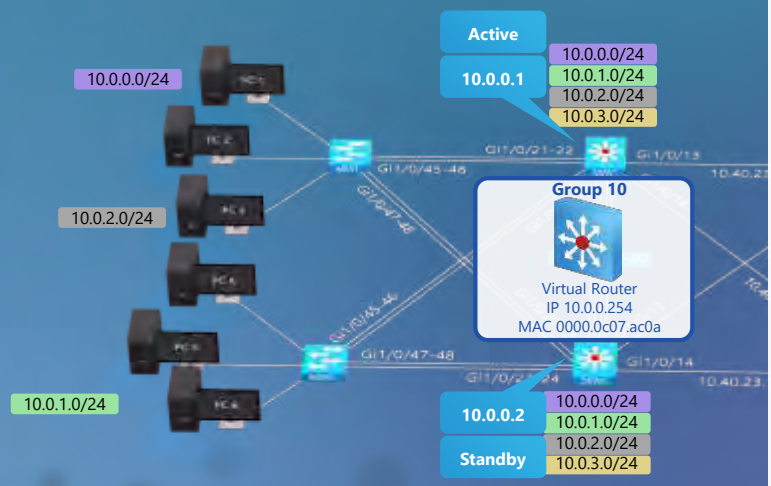
To configure MD5:

```
standby X authentication md5 key-string P@ssw0rd
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HSRP Versions



HSRP **version 1** is default

Version 1 supports **0-255** groups

Version 2 supports **0-4095** groups & **IPv6 addressing**

The virtual MAC address changes from 0000.0C07.ACYY to **0000.0C9F.FXXX**

The multicast address changes from **224.0.0.2 to 224.0.0.102**.

Use the **standby version 2** interface command

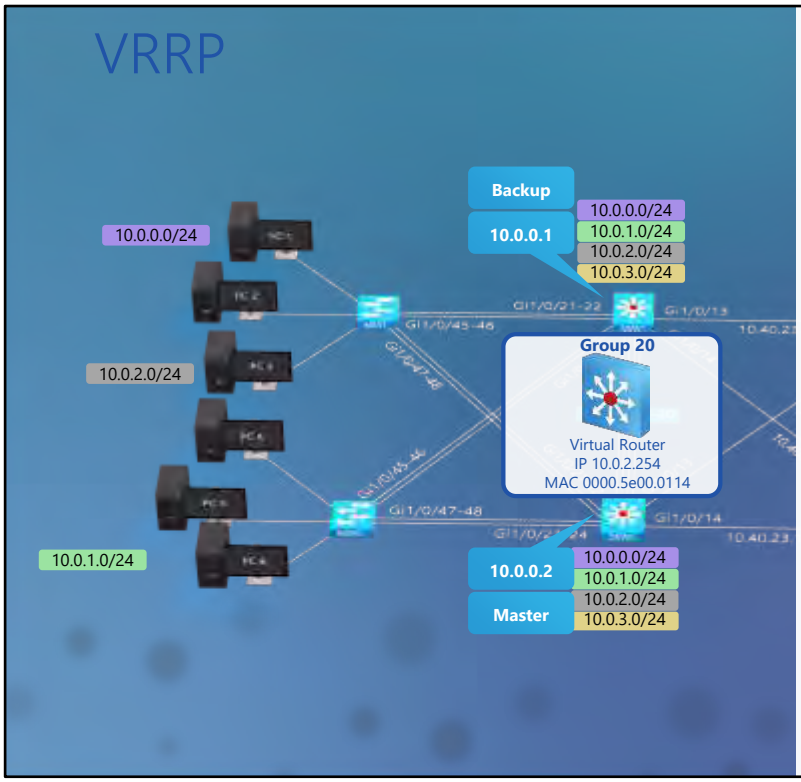
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Virtual Router Redundancy Protocol (VRRP)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP



1 Master Router per Group

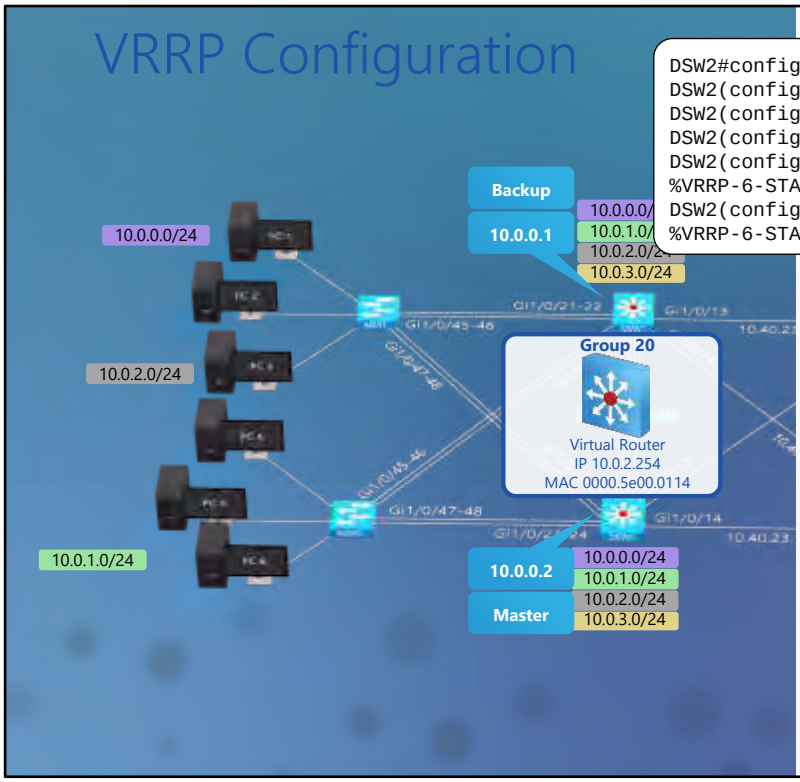
- Router with highest priority
- Forwards packets
- Responds to ARP requests
- Sends and Receives Hello Packets

1 or more Backup Routers per Group

- Router with second highest priority
- Sends and Receives Hello Packets
- Waits for Master to fail so it can become Master

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

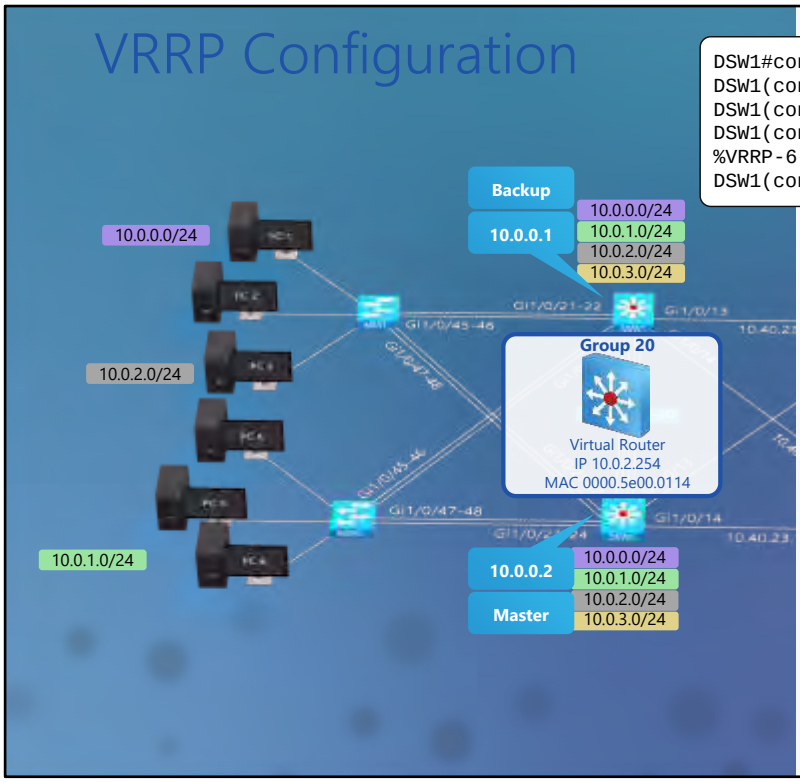
VRRP Configuration




```
DSW2#configure terminal
DSW2(config)#interface vlan 20
DSW2(config-if)#vrrp 20 ip 10.0.2.254
DSW2(config-if)#vrrp 20 priority 200
DSW2(config-if)#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Init -> Backup
DSW2(config-if)#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Backup -> Master
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

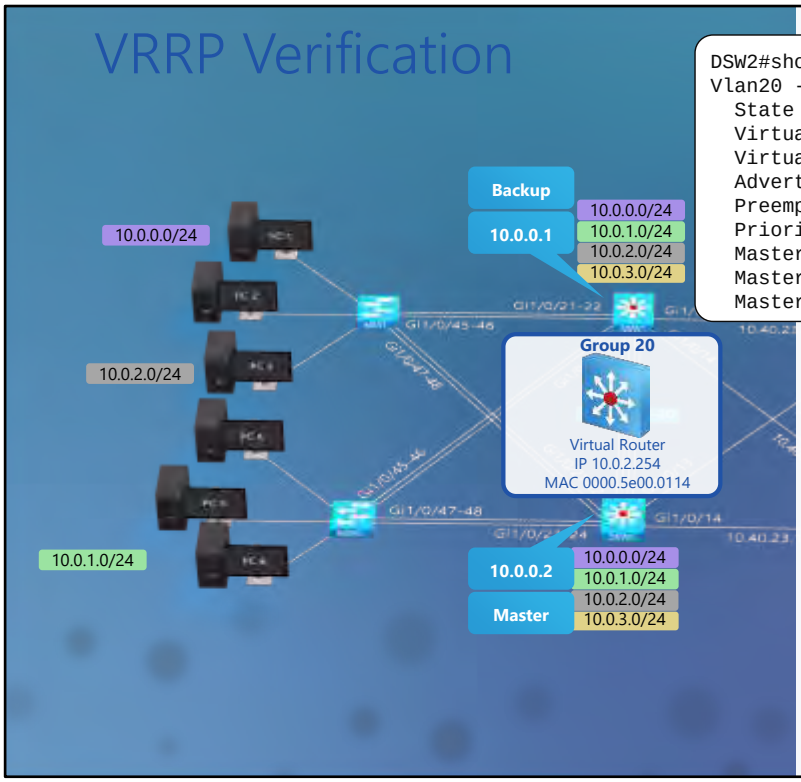
VRRP Configuration




```
DSW1#configure terminal
DSW1(config)#interface vlan 20
DSW1(config-if)#vrrp 20 ip 10.0.2.254
DSW1(config-if)#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Init -> Backup
DSW1(config-if)#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

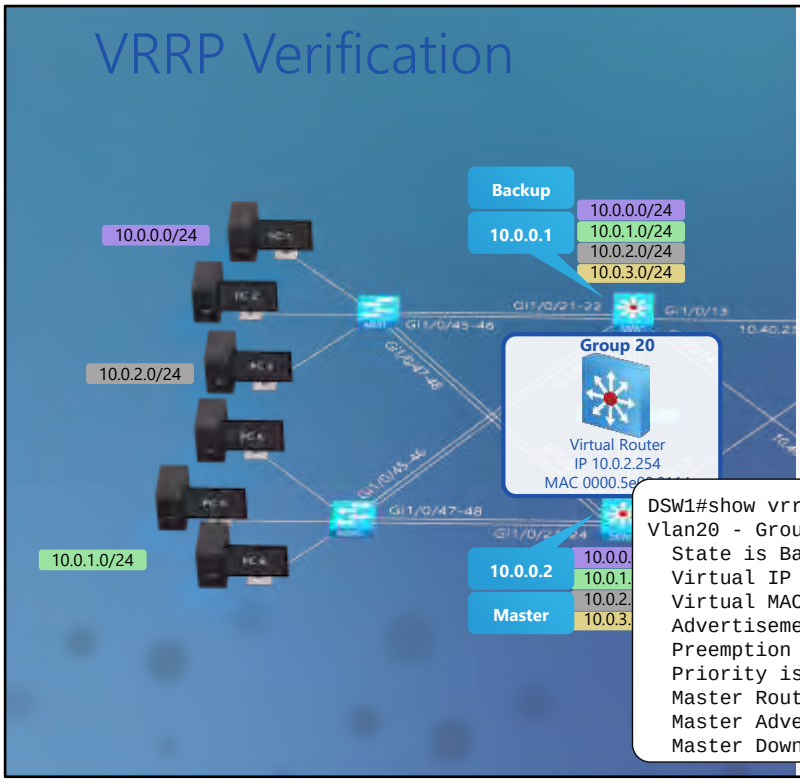
VRRP Verification




```
DSW2#show vrrp
Vlan20 - Group 20
  State is Master
  Virtual IP address is 10.0.2.254
  Virtual MAC address is 0000.5e00.0114
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 200
  Master Router is 10.0.2.2 (local), priority is 200
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.218 sec
```

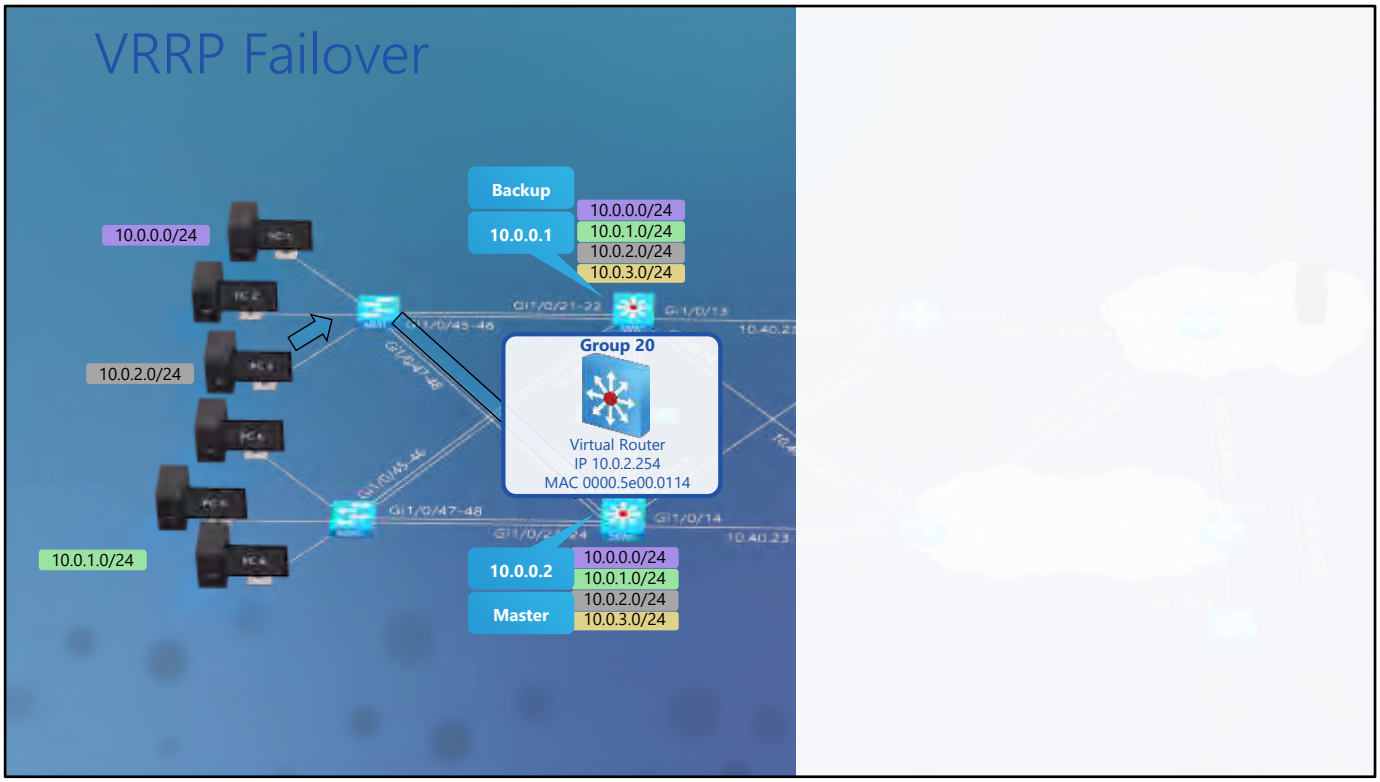
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Verification



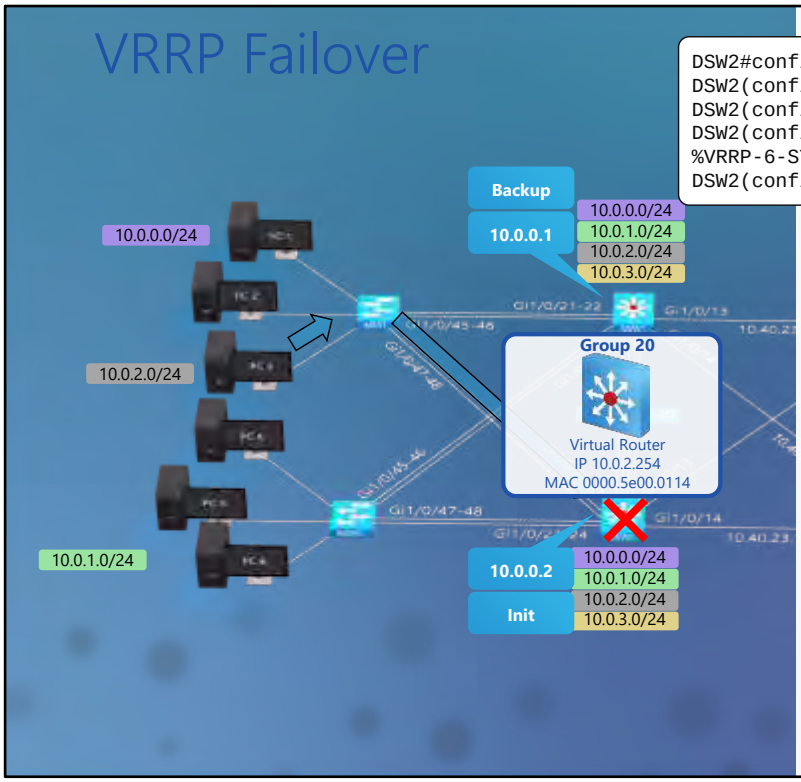

```
DSW1#show vrrp
Vlan20 - Group 20
  State is Backup
  Virtual IP address is 10.0.2.254
  Virtual MAC address is 0000.5e00.0114
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 100
  Master Router is 10.0.2.2, priority is 200
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.609 sec (expires in 2.813 sec)
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



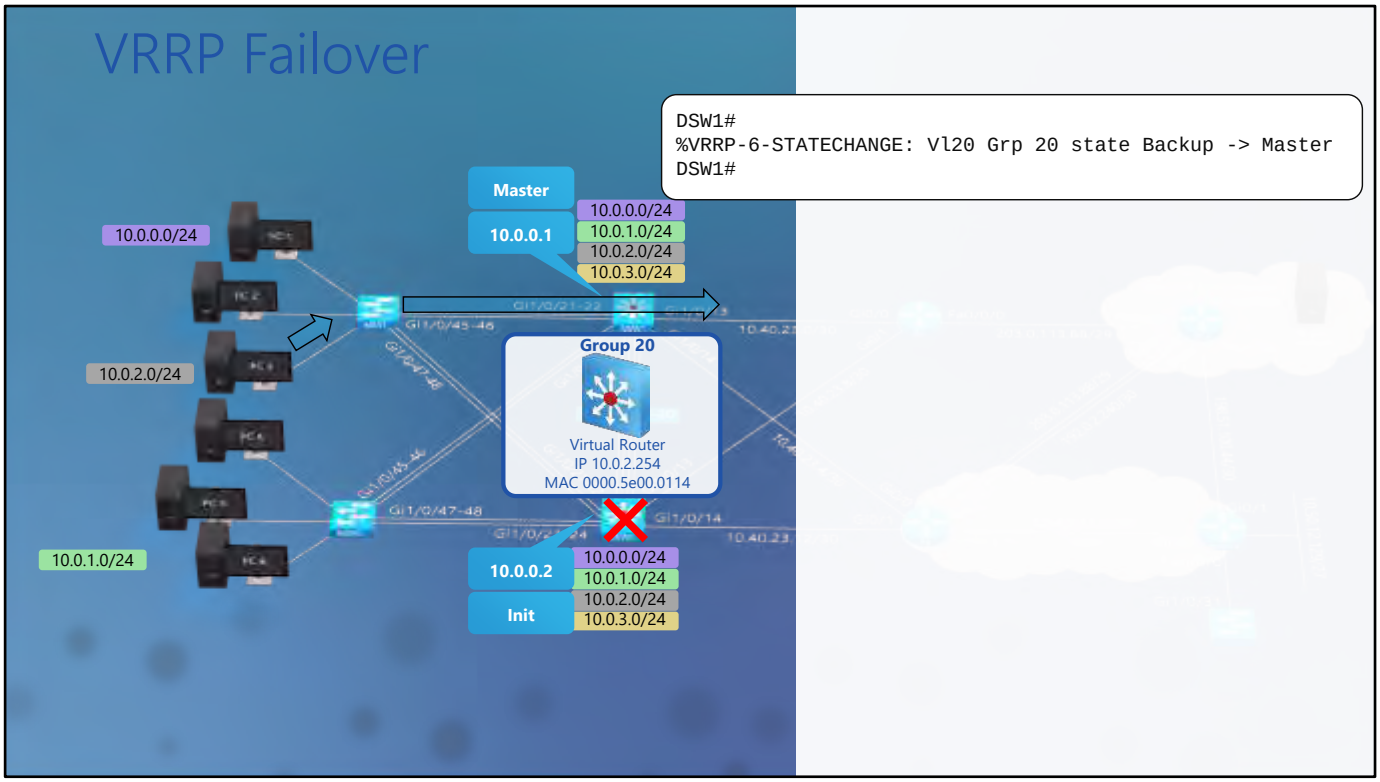
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Failover



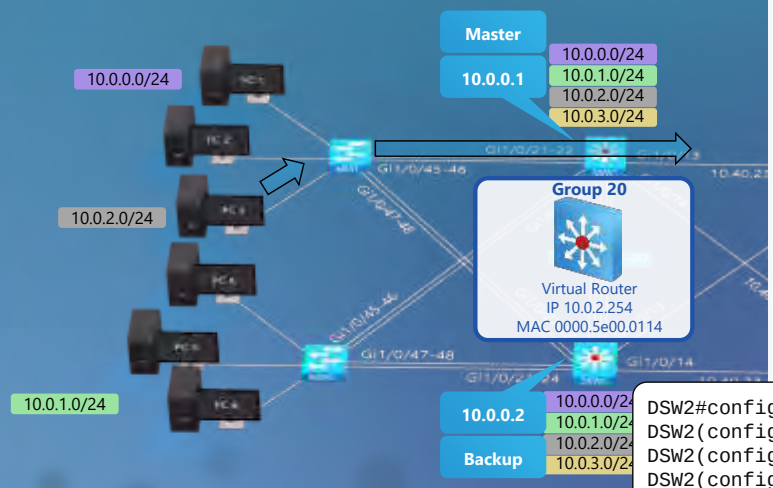

```
DSW2#configure terminal
DSW2(config)#interface range gigabitEthernet 1/0/13-24
DSW2(config-if-range)#shut
DSW2(config-if-range)#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Master -> Init
DSW2(config-if-range)#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

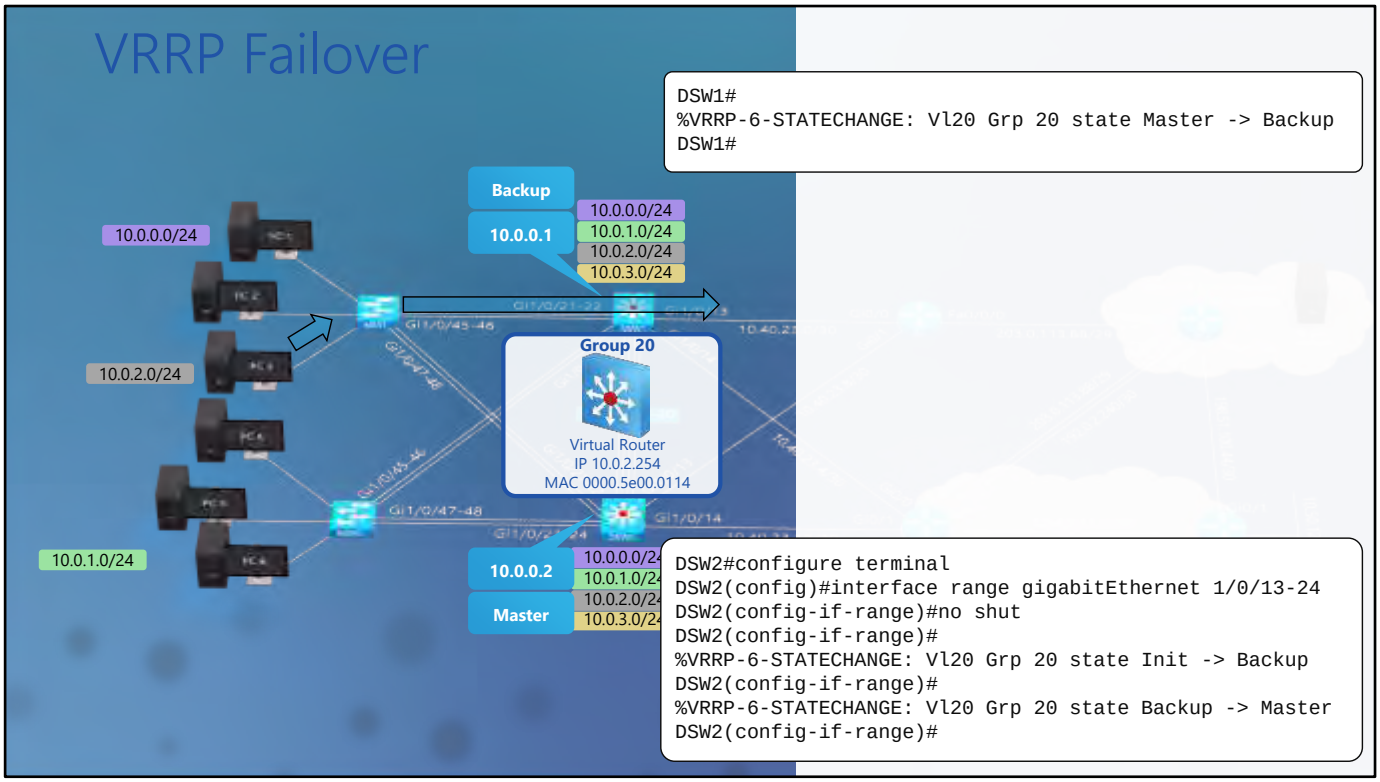
VRRP Failover




```
DSW2#configure terminal
DSW2(config)#interface range gigabitEthernet 1/0/13-24
DSW2(config-if-range)#no shut
DSW2(config-if-range)#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Init -> Backup
DSW2(config-if-range)#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

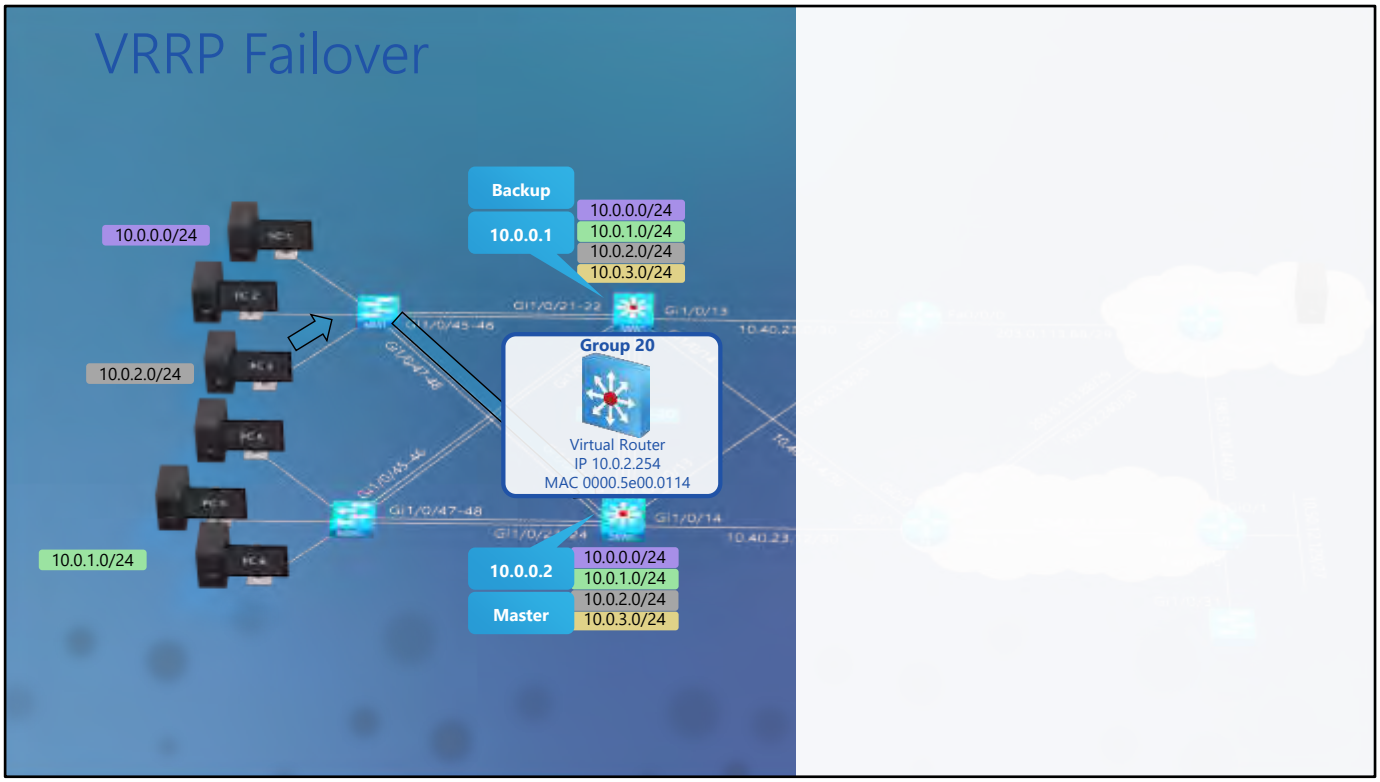
VRRP Failover




```
DSW1#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Master -> Backup
DSW1#
```

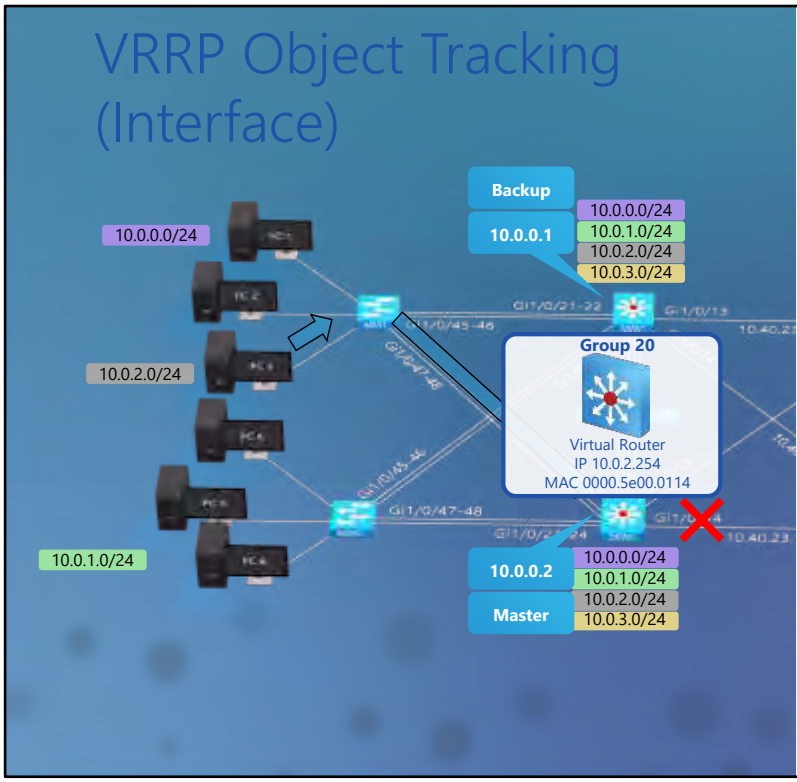
```
DSW2#configure terminal
DSW2(config)#interface range gigabitEthernet 1/0/13-24
DSW2(config-if-range)#no shut
DSW2(config-if-range)#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Init -> Backup
DSW2(config-if-range)#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Backup -> Master
DSW2(config-if-range)#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



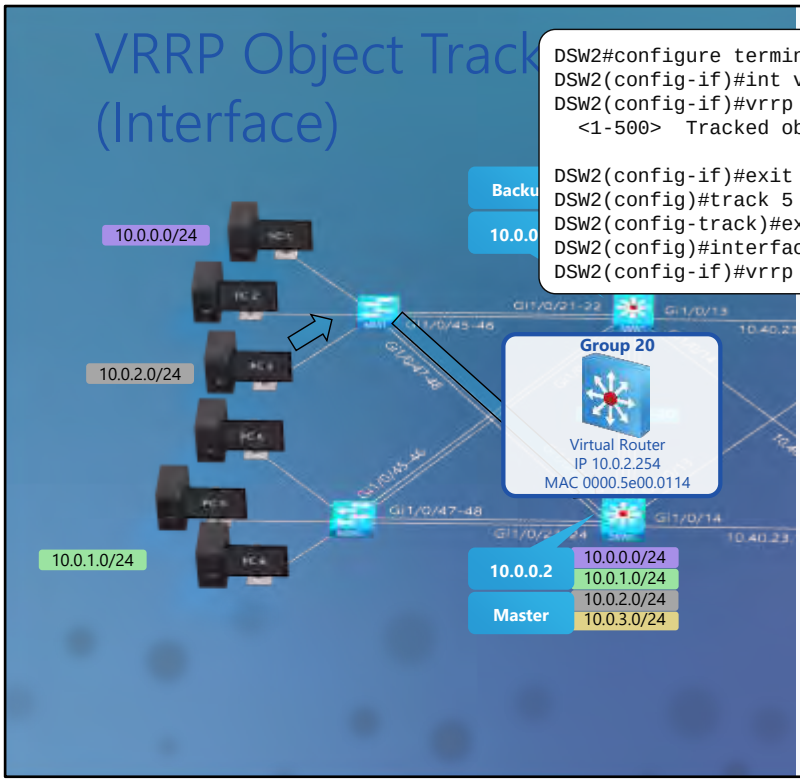
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Object Tracking (Interface)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

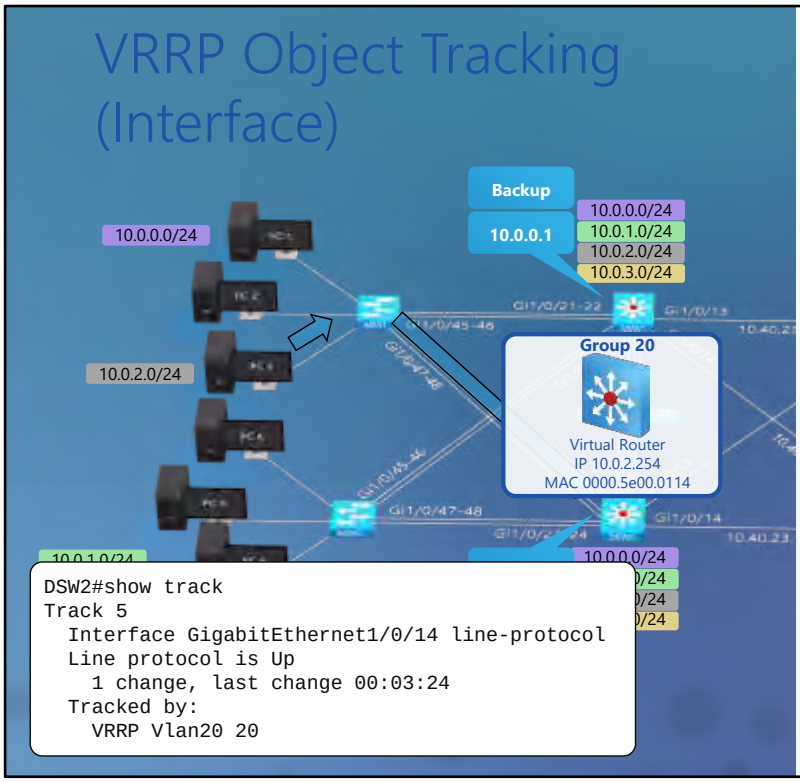
VRRP Object Track (Interface)




```
DSW2#configure terminal
DSW2(config-if)#int vlan 20
DSW2(config-if)#vrrp 20 track ?
  <1-500>  Tracked object

DSW2(config-if)#exit
DSW2(config)#track 5 interface gigabitEthernet 1/0/14 line-protocol
DSW2(config-track)#exit
DSW2(config)#interface vlan 20
DSW2(config-if)#vrrp 20 track 5 decrement 200
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

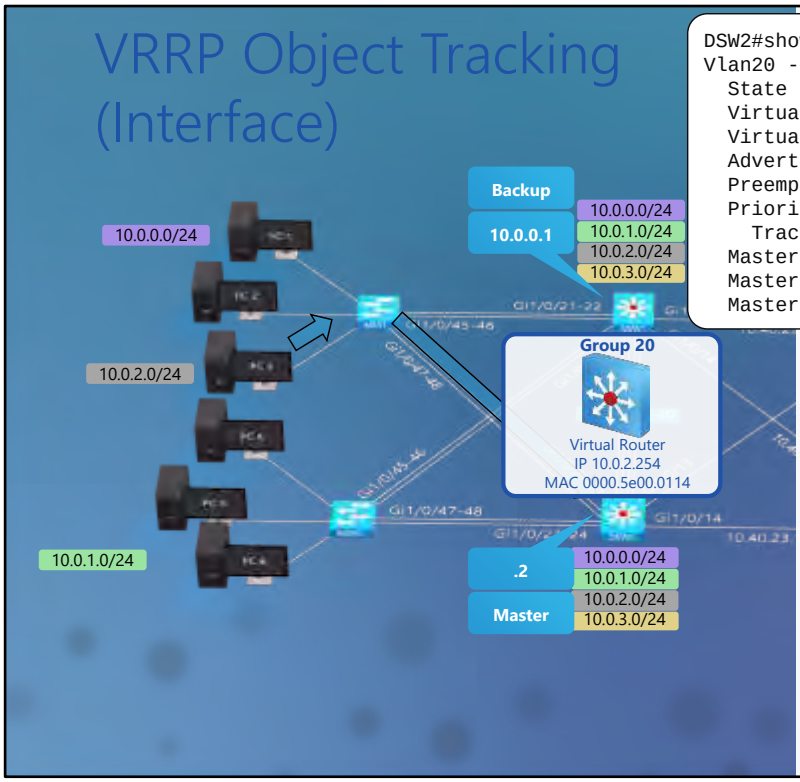
VRRP Object Tracking (Interface)




```
DSW2#show track
Track 5
  Interface GigabitEthernet1/0/14 line-protocol
  Line protocol is Up
    1 change, last change 00:03:24
  Tracked by:
    VRRP Vlan20 20
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Object Tracking (Interface)

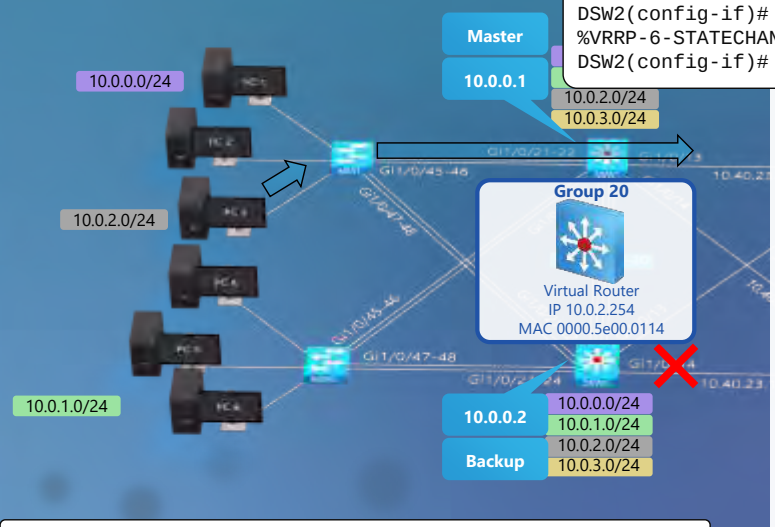



```
DSW2#show vrrp
Vlan20 - Group 20
  State is Master
  Virtual IP address is 10.0.2.254
  Virtual MAC address is 0000.5e00.0114
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 200
    Track object 5 state Up decrement 200
  Master Router is 10.0.2.2 (local), priority is 200
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.218 sec
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Object Tracking (Interface)

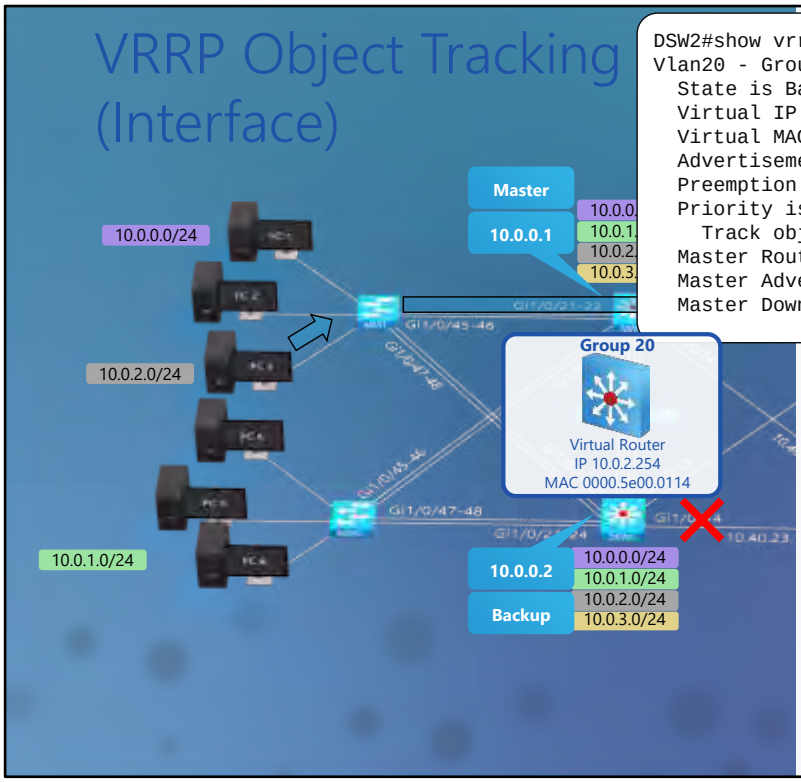
```
DSW2#configure terminal
DSW2(config)#interface gigabitEthernet 1/0/14
DSW2(config-if)#shut
DSW2(config-if)#
%TRACKING-5-STATE: 5 interface Gi1/0/14 line-protocol Up->Down
DSW2(config-if)#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Master -> Backup
DSW2(config-if)#
```




```
DSW1#
%VRRP-6-STATECHANGE: Vl20 Grp 20 state Backup -> Master
DSW1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

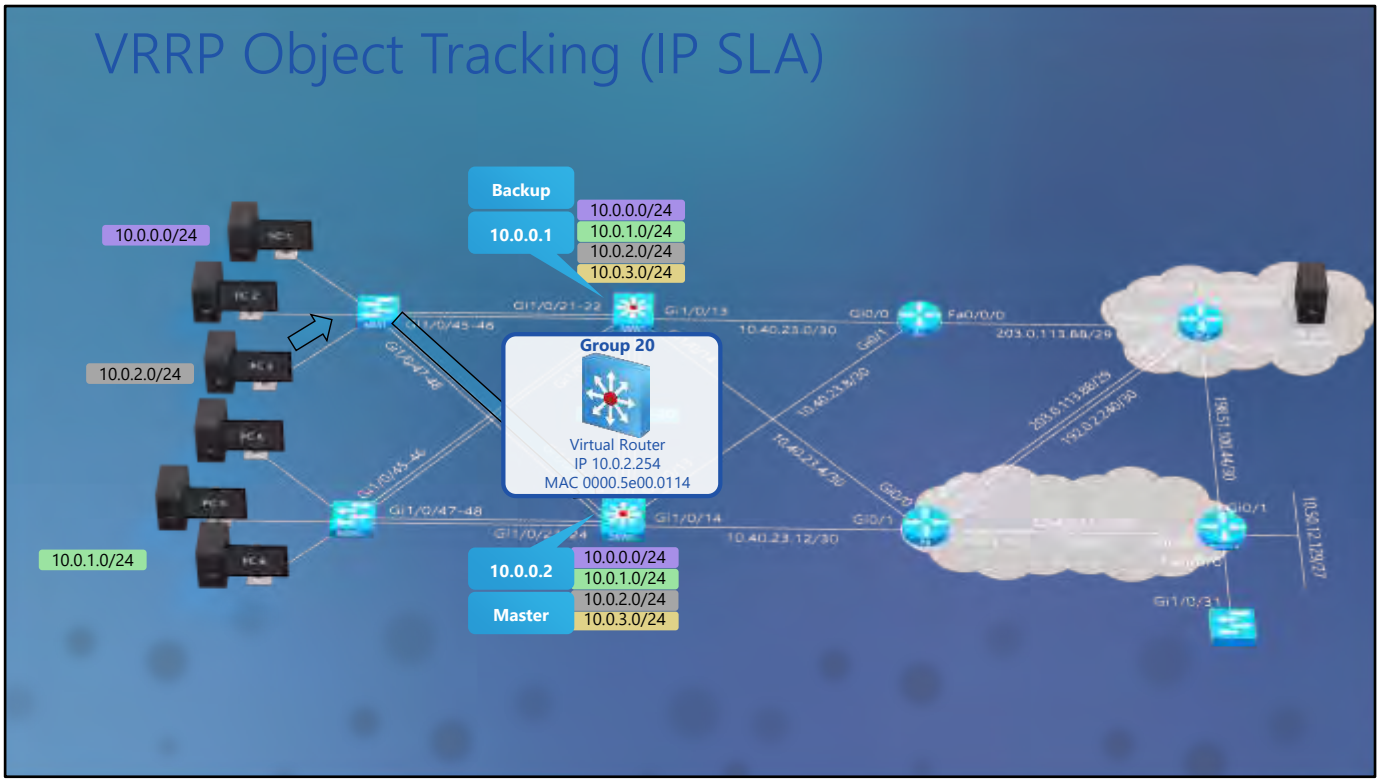
VRRP Object Tracking (Interface)




```
DSW2#show vrrp
Vlan20 - Group 20
  State is Backup
  Virtual IP address is 10.0.2.254
  Virtual MAC address is 0000.5e00.0114
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 0   (cfgd 200)
    Track object 5 state Down decrement 200
  Master Router is 10.0.2.1, priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.218 sec (expires in 2.522 sec)
```

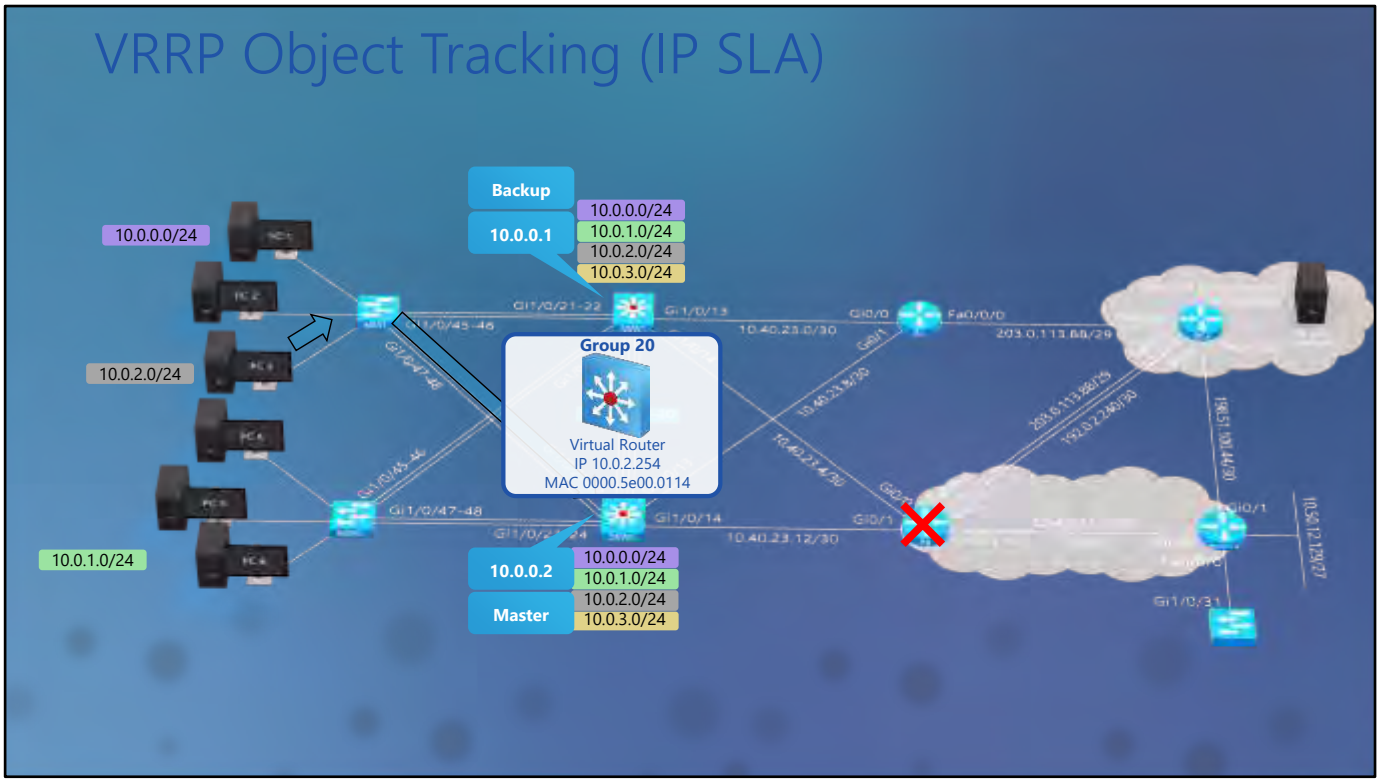
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Object Tracking (IP SLA)



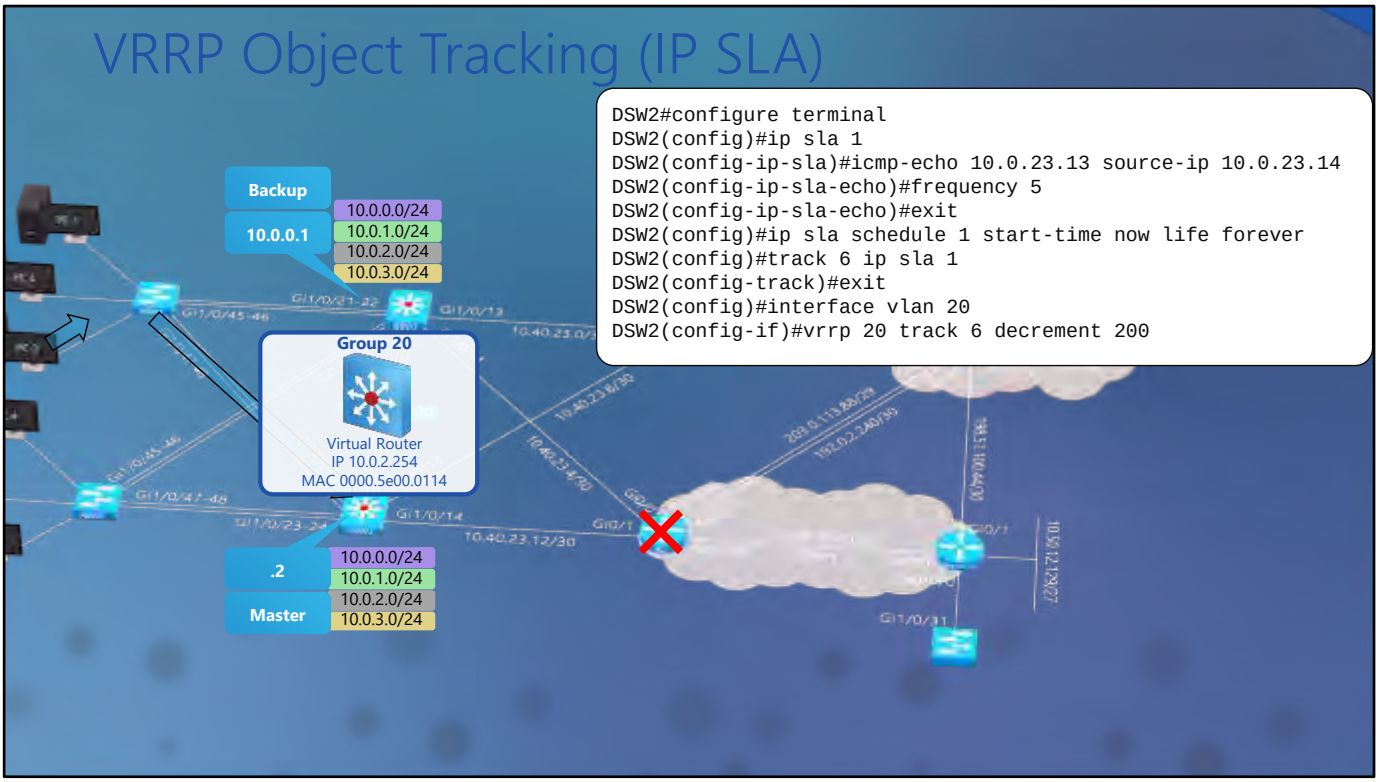
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Object Tracking (IP SLA)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Object Tracking (IP SLA)

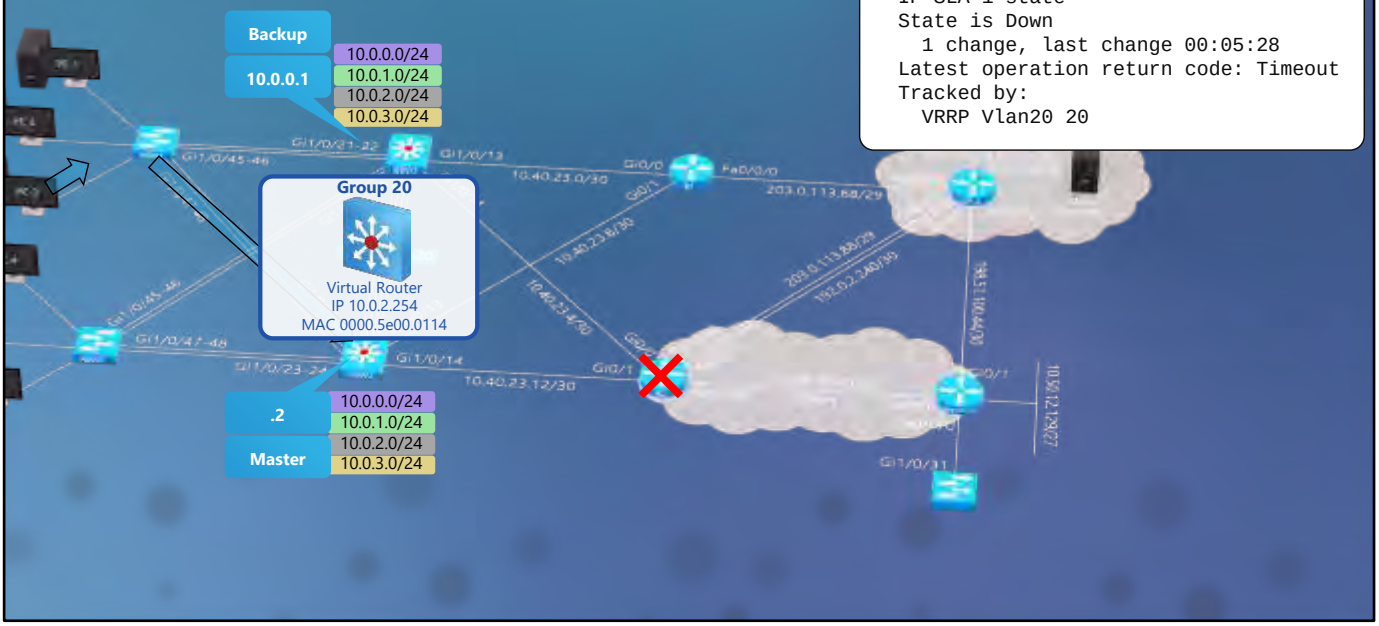



```
DSW2#configure terminal
DSW2(config)#ip sla 1
DSW2(config-ip-sla)#icmp-echo 10.0.23.13 source-ip 10.0.23.14
DSW2(config-ip-sla-echo)#frequency 5
DSW2(config-ip-sla-echo)#exit
DSW2(config)#ip sla schedule 1 start-time now life forever
DSW2(config)#track 6 ip sla 1
DSW2(config-track)#exit
DSW2(config)#interface vlan 20
DSW2(config-if)#vrrp 20 track 6 decrement 200
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

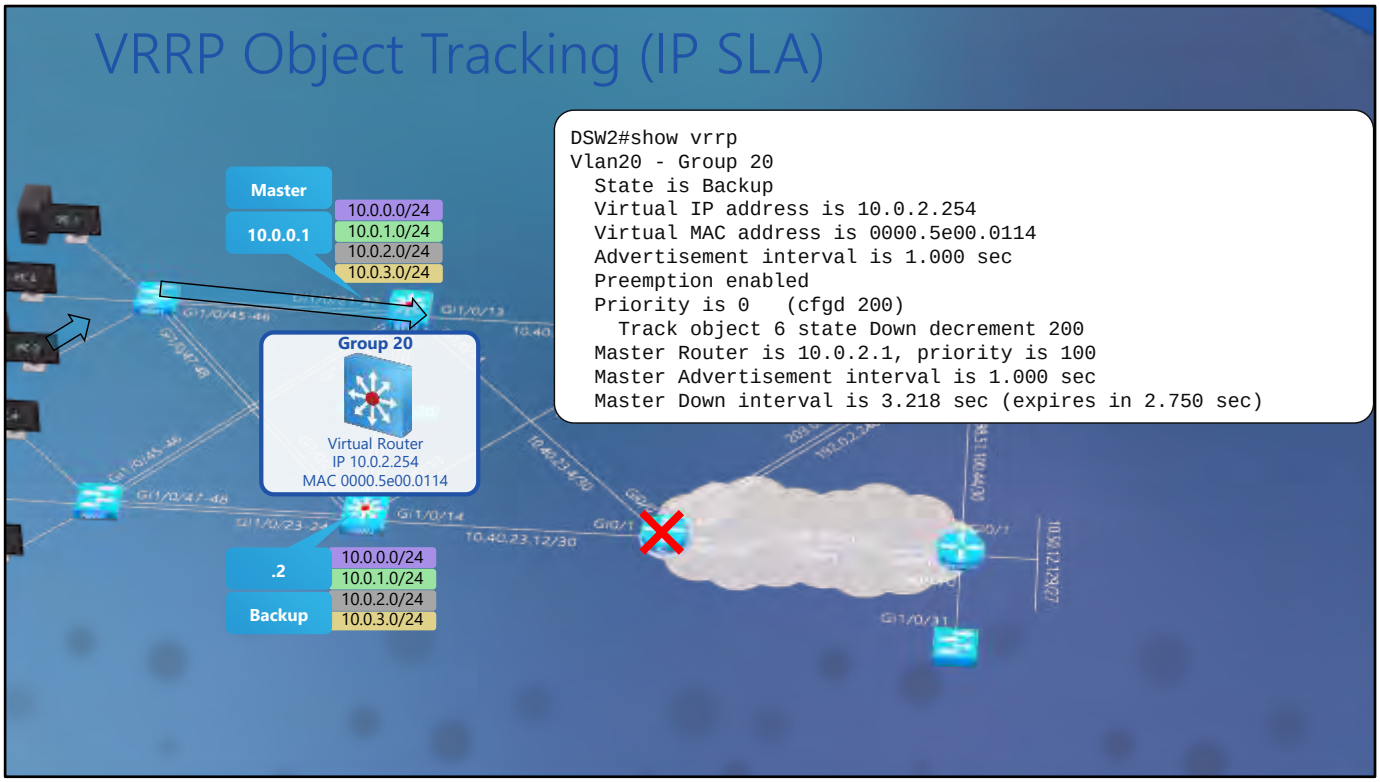
VRRP Object Tracking (IP SLA)

```
DSW2#show track
Track 6
  IP SLA 1 state
  State is Down
    1 change, last change 00:05:28
  Latest operation return code: Timeout
  Tracked by:
    VRRP Vlan20 20
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

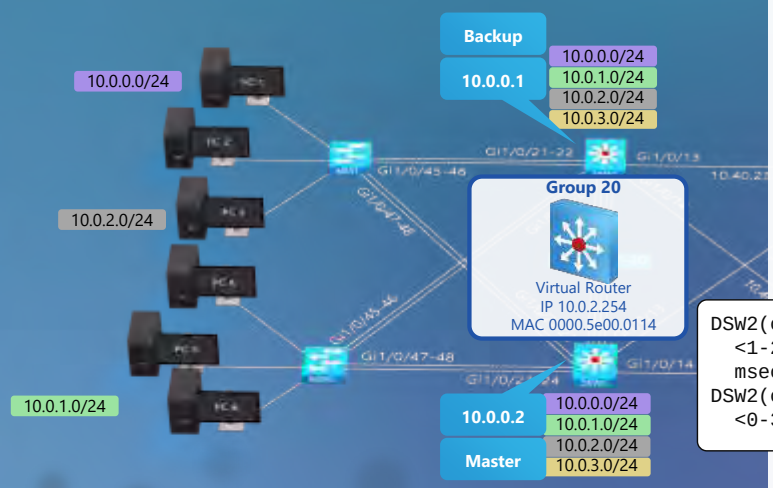
VRRP Object Tracking (IP SLA)




```
DSW2#show vrrp
Vlan20 - Group 20
  State is Backup
  Virtual IP address is 10.0.2.254
  Virtual MAC address is 0000.5e00.0114
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 0   (cfgd 200)
    Track object 6 state Down decrement 200
  Master Router is 10.0.2.1, priority is 100
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.218 sec (expires in 2.750 sec)
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Timers



Timers can support millisecond values

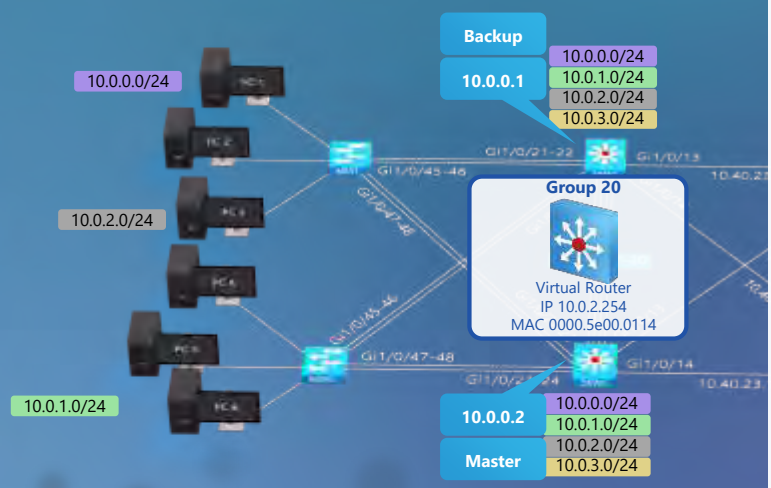
It's recommended to delay pre-emption to allow Master Router to come back online and allow for Routing Protocol convergence.

To change the timers & preemption timer:

```
DSW2(config-if)#vrrp 20 timers advertise ?
  <1-255>  Advertisement interval in seconds
  msec     Specify time in milliseconds
DSW2(config-if)#vrrp 20 preempt delay minimum ?
  <0-3600>  Seconds to delay
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRRP Authentication



VRRP supports cleartext authentication

Matching configuration is required on peers

```
vrrp 20 authentication text SHAREDPASSWORD
```

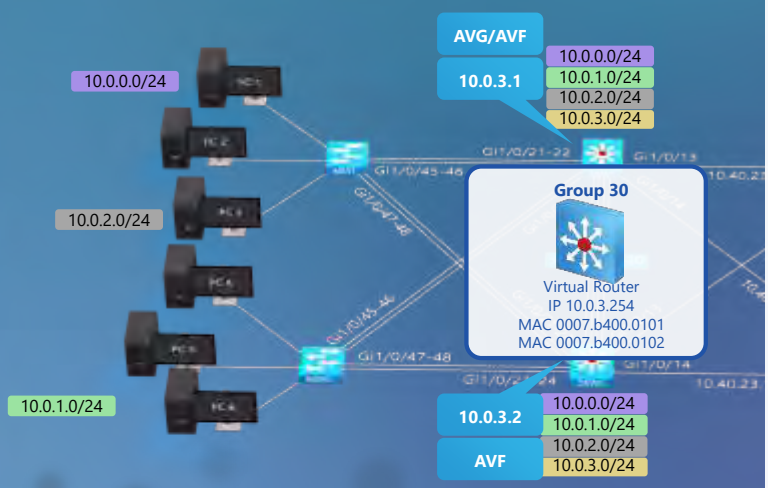
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Gateway Load Balancing Protocol (GLBP)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

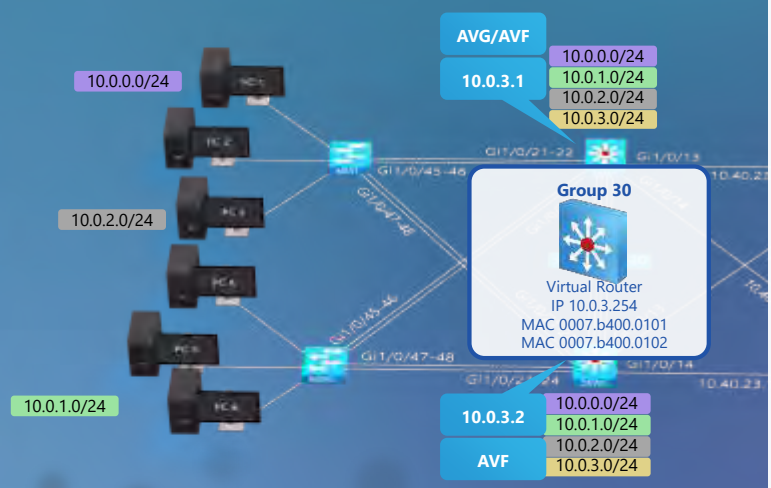
GLBP



Both gateways can be used at the same time for a single VLAN/Subnet

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GLBP AVG and AVF



AVG – Active Virtual Gateway

1 Active

1 Standby

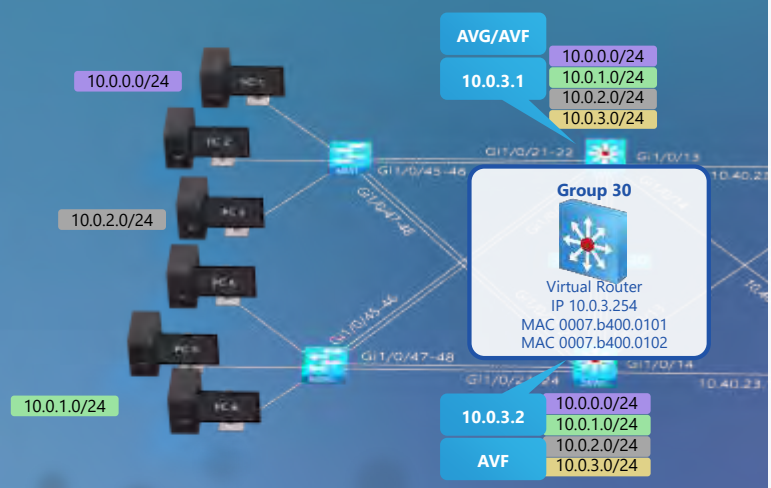
AVF – Active Virtual Forwarder

Max 4

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GLBP Configuration

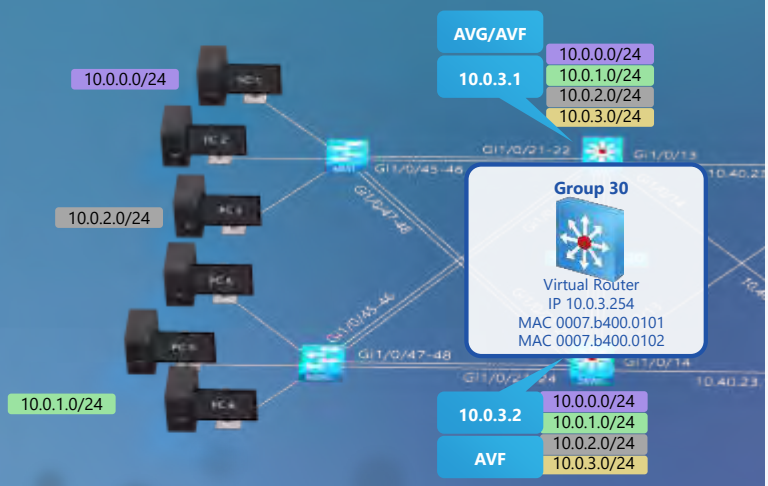



```
DSW1#configure terminal
DSW1(config)#interface vlan 30
DSW1(config-if)#glbp 30 10.0.3.254
DSW1(config-if)#glbp 30 priority 110
DSW1(config-if)#glbp 30 timers 5 15
DSW1(config-if)#glbp 30 preempt
DSW1(config-if)#glbp 30 load-balancing
[host-dependent | round-robin | weighted]
```

```
DSW2#configure terminal
DSW2(config)#interface vlan 30
DSW2(config-if)#glbp 30 10.0.3.254
DSW2(config-if)#glbp 30 priority 100
DSW2(config-if)#glbp 30 timers 5 15
DSW2(config-if)#glbp 30 preempt
DSW2(config-if)#glbp 30 load-balancing
[host-dependent | round-robin | weighted]
```

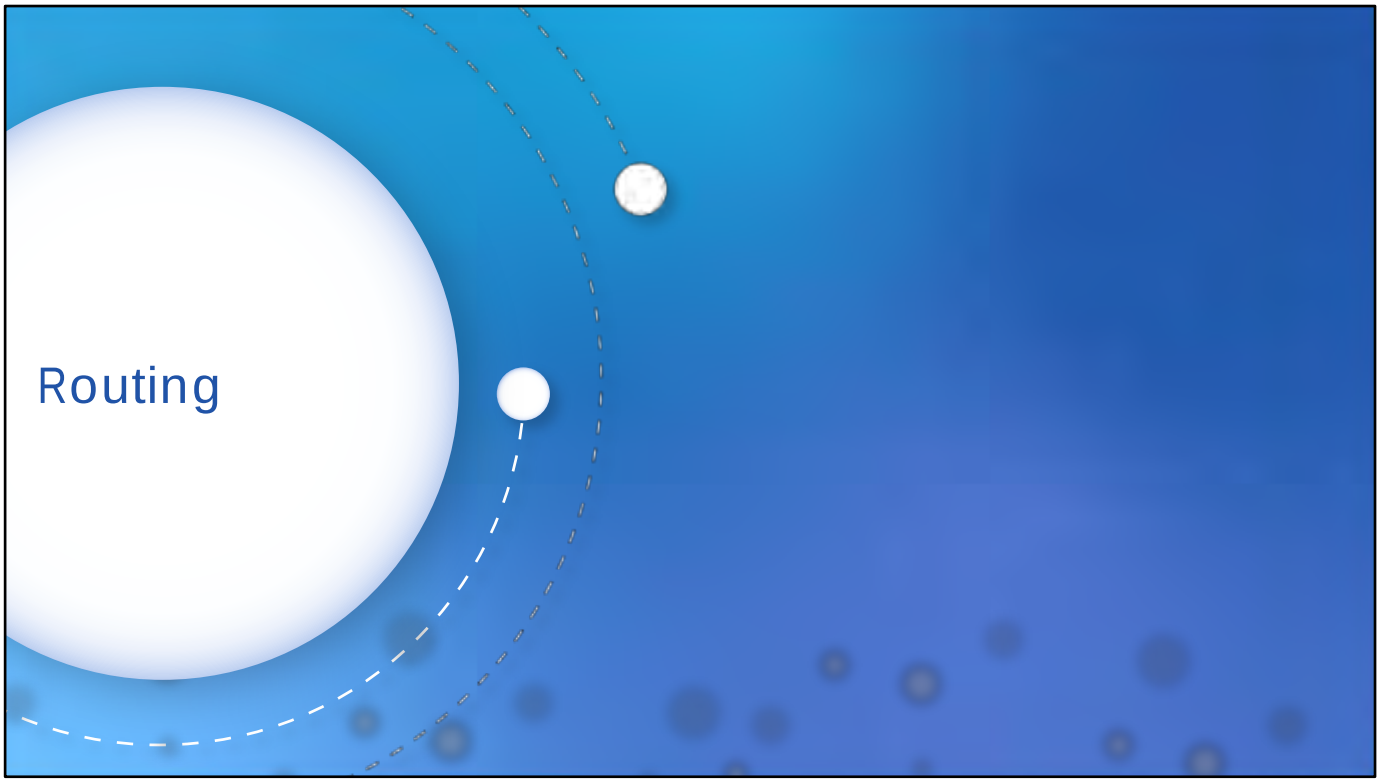
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GLBP LOAD BALANCING OPTIONS



- None
- Weighted
- Host dependent
- Round robin

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

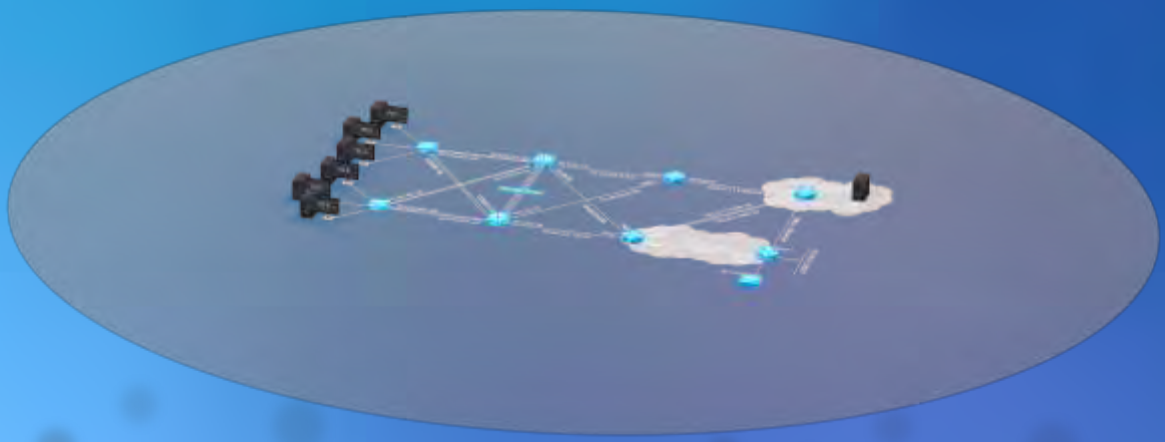


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Routing Introduction

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Routing



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Routing

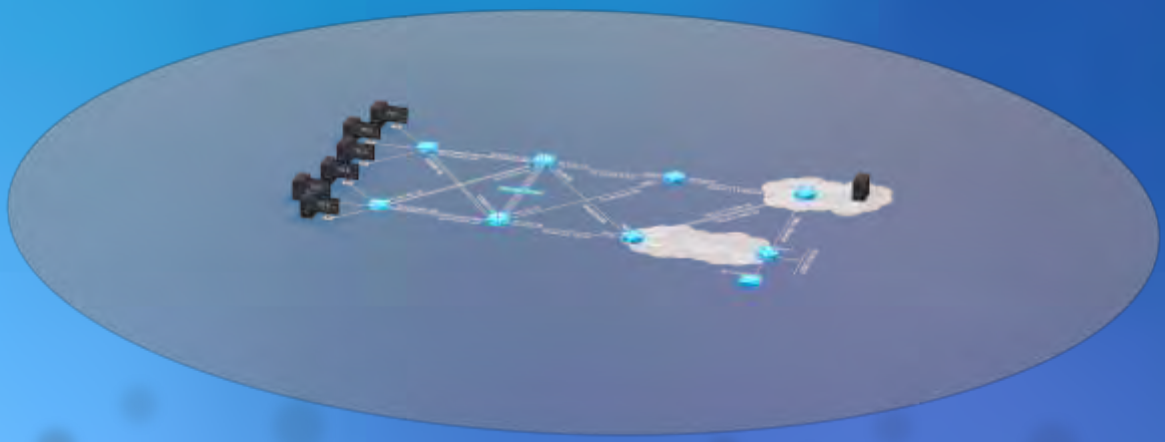
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Routing

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.34.0 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
      172.17.0.0/24 is subnetted, 1 subnets
O        172.17.34.0 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Routing



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Routers will install the best route from the best source

Step 1 Identify the best source

Administrative Distance

Step 2 Identify best route from best source

Metric

Step 3 Install result in routing table

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.34.0 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
      172.17.0.0/24 is subnetted, 1 subnets
O        172.17.34.0 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Routers will install the best route from the best source

Step 1 Identify the best source

Administrative Distance

Step 2 Identify best route from best source

Metric

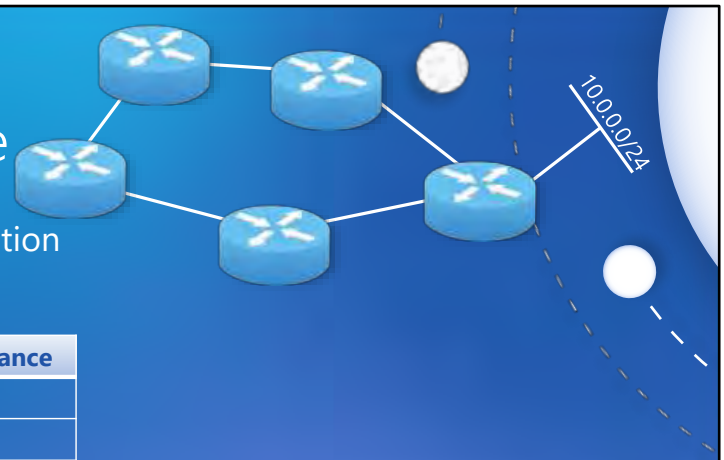
Step 3 Install result in routing table

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.34.0 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
      172.17.0.0/24 is subnetted, 1 subnets
O        172.17.34.0 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Administrative Distance



Ranks the sources of routing information

- Lower is better

Source	Administrative Distance
Connected	0
Static	1
eBGP	20
EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
iBGP	200

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Routers will install the best route from the best source

Step 1 Identify the best source

Administrative Distance

Step 2 Identify best route from best source

Metric

Step 3 Install result in routing table

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.34.0 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
      172.17.0.0/24 is subnetted, 1 subnets
O        172.17.34.0 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Routers will install the best route from the best source

Step 1 Identify the best source

Administrative Distance

Step 2 Identify best route from best source

Metric

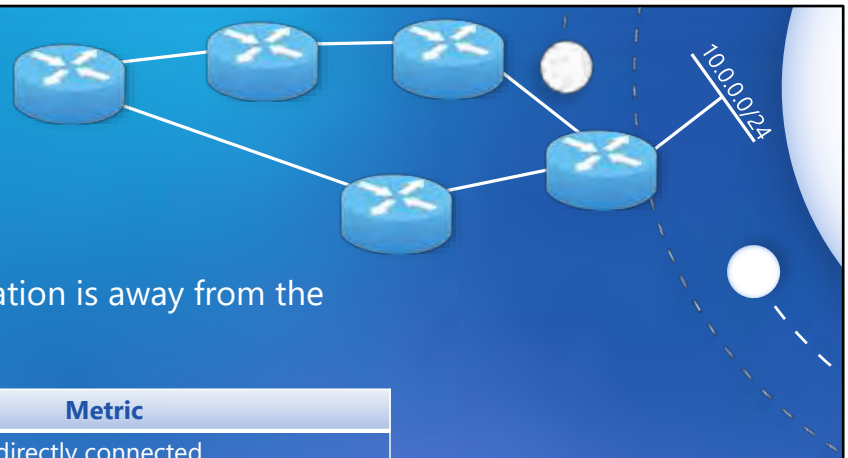
Step 3 Install result in routing table

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.34.0 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
      172.17.0.0/24 is subnetted, 1 subnets
O        172.17.34.0 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Metric



Identifies how far the destination is away from the local routers perspective.

Source	Metric
Connected	0 because it is directly connected
Static	0 because the metric is not known
RIP	Hop Count – Max 15 hops (16 unreachable)
EIGRP	Lowest Bandwidth + Cumulative Delay of path
OSPF	Cost = sum of all the costs along the path
BGP	Attributes used to influence routing policy

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Routers will install the best route from the best source

Step 1 Identify the best source

Administrative Distance

Step 2 Identify best route from best source

Metric

Step 3 Install result in routing table

```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.34.0 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
      172.17.0.0/24 is subnetted, 1 subnets
O        172.17.34.0 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Routers will install the best route from the best source

Step 1 Identify the best source

Administrative Distance

Step 2 Identify best route from best source

Metric

Step 3 Install result in routing table

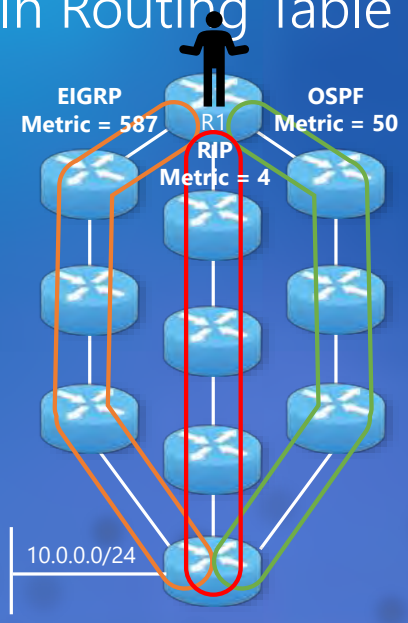
```
R2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.34.0 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
      172.17.0.0/24 is subnetted, 1 subnets
O        172.17.34.0 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
      203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Which route to 10.0.0.0/24 will be placed in R1s routing table?

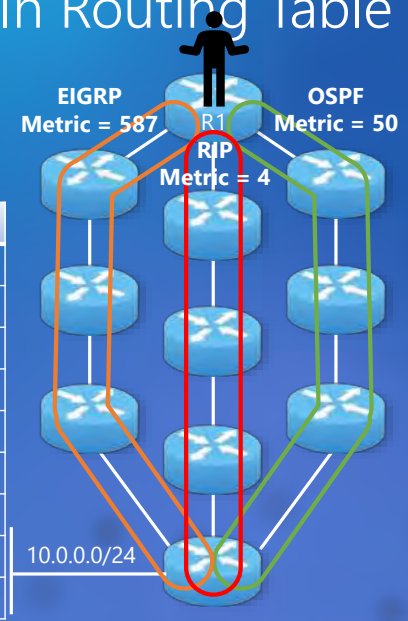


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Which route to 10.0.0.0/24 will be placed in R1s routing table?

Source	Administrative Distance
Connected	0
Static	1
eBGP	20
EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
iBGP	200

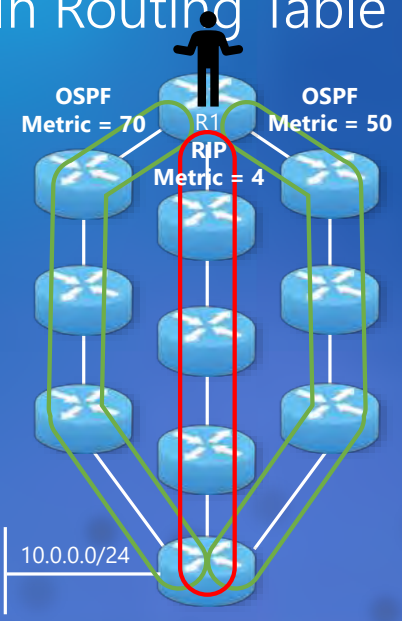


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Which route to 10.0.0.0/24 will be placed in R1s routing table?

Source	Administrative Distance
Connected	0
Static	1
eBGP	20
EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
iBGP	200

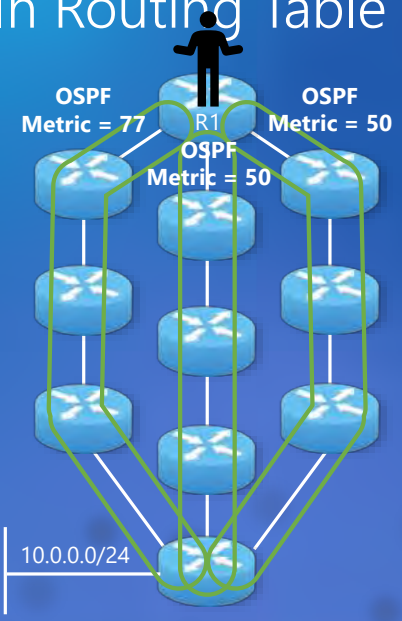


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What To Put In Routing Table

Which route to 10.0.0.0/24 will be placed in R1s routing table?

Source	Administrative Distance
Connected	0
Static	1
eBGP	20
EIGRP	90
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
iBGP	200



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What Entry In the Routing Table to Use

Routers will route based on the longest match rule

1) Find the network entry (or entries) the destination IP address lives in…

2) Use the one with the subnet mask closer to /32 when multiple match.

```
R2#show ip route
…output omitted…

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
O        10.0.10.16/28 [110/4] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
O        10.0.10.64/26 [110/7] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
O        10.0.10.128/25 [110/3] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
O     172.16.34.0/24 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
O     172.17.34.0/24 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Determining What Entry In the Routing Table to Use

Routers will route based on the longest match rule

1) Find the network entry (or entries) the destination IP address lives in…

2) Use the one with the subnet mask closer to /32 when multiple match.

A packet arrives destined to:

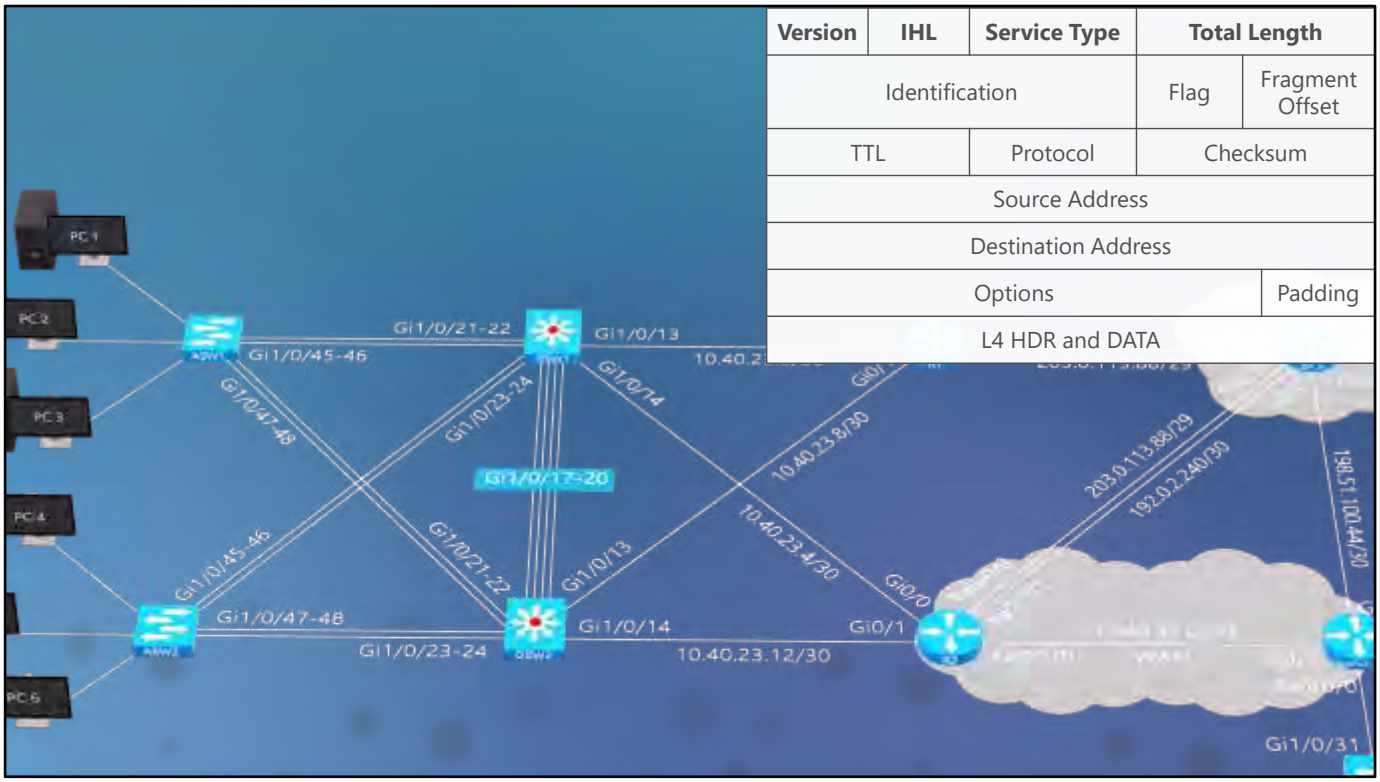
10.0.10.25

Which entry will be used to forward it?

```
R2#show ip route
…output omitted…

Gateway of last resort is 203.0.113.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 203.0.113.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.10.0/24 is directly connected, GigabitEthernet0/0
L        10.0.10.2/32 is directly connected, GigabitEthernet0/0
O        10.0.10.16/28 [110/4] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
O        10.0.10.64/26 [110/7] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
O        10.0.10.128/25 [110/3] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.2/32 is directly connected, GigabitEthernet1/0
C        10.0.123.0/24 is directly connected, GigabitEthernet2/0
L        10.0.123.2/32 is directly connected, GigabitEthernet2/0
O     172.16.34.0/24 [110/2] via 10.0.123.3, 00:05:37, GigabitEthernet2/0
O     172.17.34.0/24 [110/65] via 10.0.123.3, 00:05:27, GigabitEthernet2/0
O     192.168.4.0/24 [110/3] via 10.0.123.3, 00:03:37, GigabitEthernet2/0
C        203.0.113.0/24 is directly connected, GigabitEthernet3/0
L        203.0.113.2/32 is directly connected, GigabitEthernet3/0
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



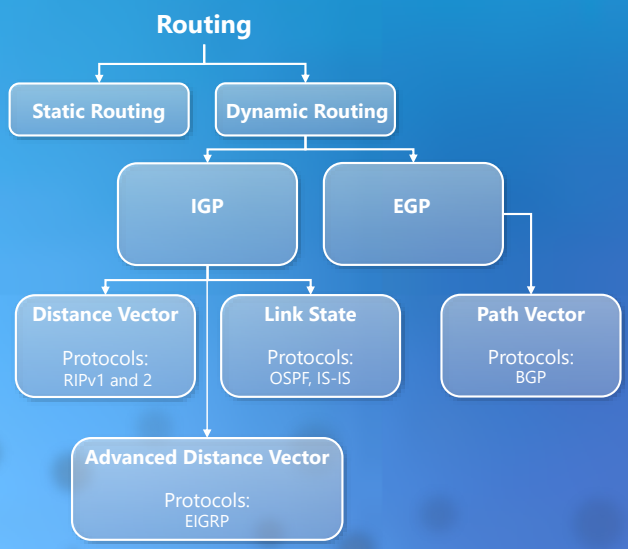
Version	IHL	Service Type	Total Length	
Identification			Flag	Fragment Offset
TTL		Protocol	Checksum	
Source Address				
Destination Address				
Options				Padding
L4 HDR and DATA				

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Routing Overview

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Routing Options



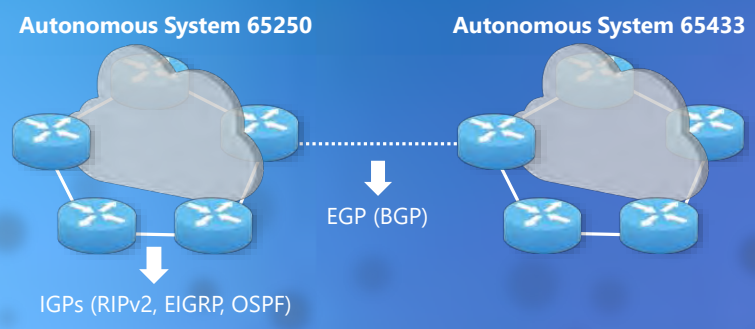
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Routing Protocols: Interior and Exterior

Interior Gateway Protocols (IGP) run within the local autonomous system

Exterior Gateway Protocols (EGP) run between different autonomous systems

Autonomous System (AS) is a collection of networks overseen by one organization

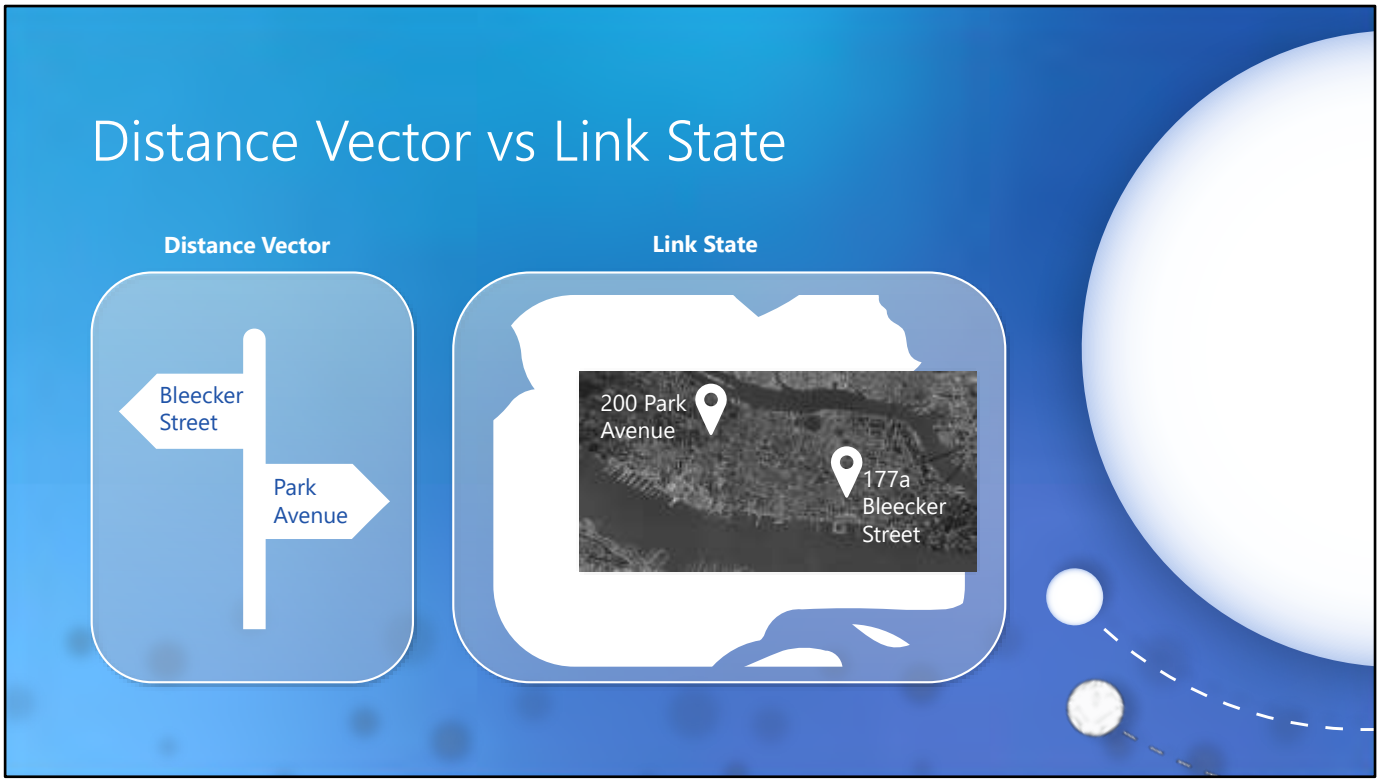


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

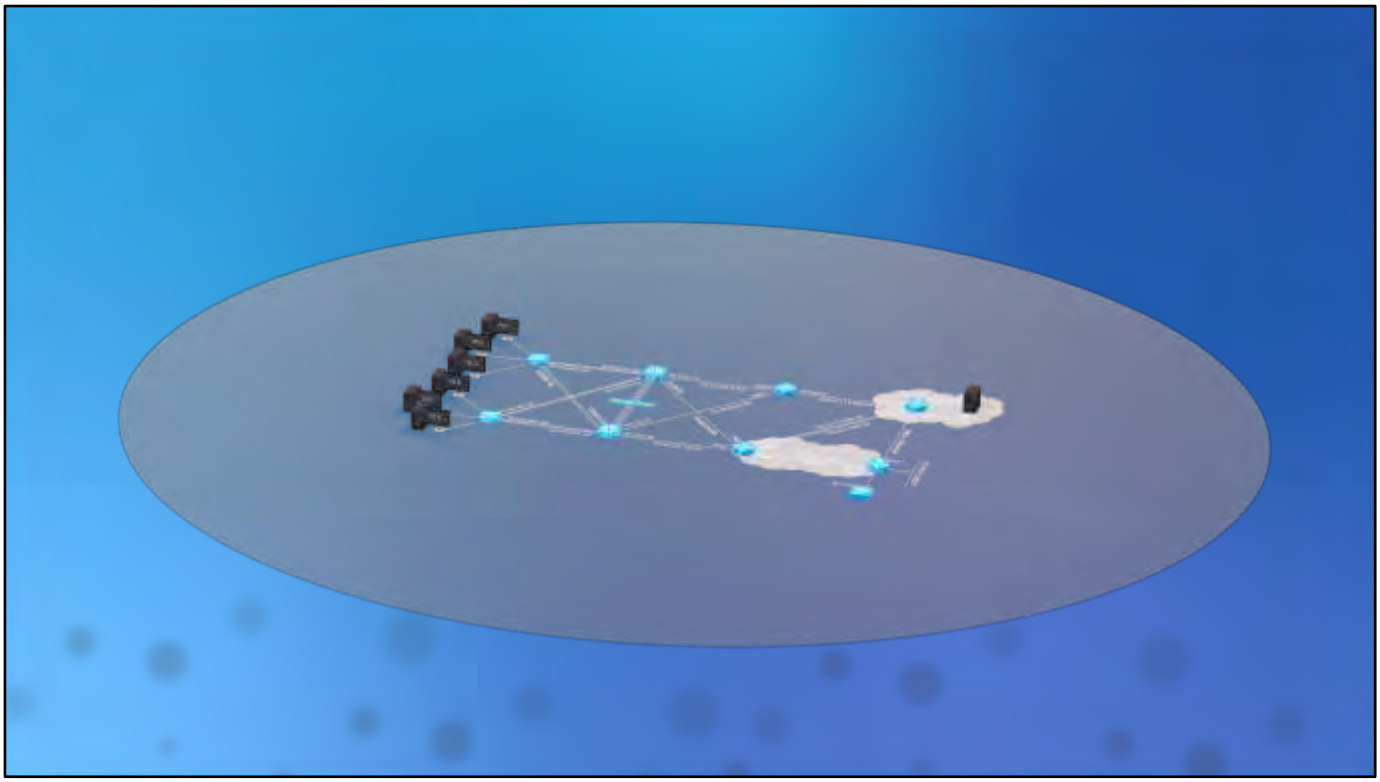
Dynamic Routing Protocols

Protocol	Type	Cisco Proprietary	Metric	EGP/IGP	AD
RIPv2	Distance Vector	No	Hop Count	IGP	120
EIGRP	Advanced Distance Vector	Yes	Bandwidth and Delay	IGP	90/170
OSPF	Link State	No	Cost	IGP	110
IS-IS	Link State	No	Cost	IGP	115
BGP	Path Vector	No	Attribute (AS Path)	EGP	20/200

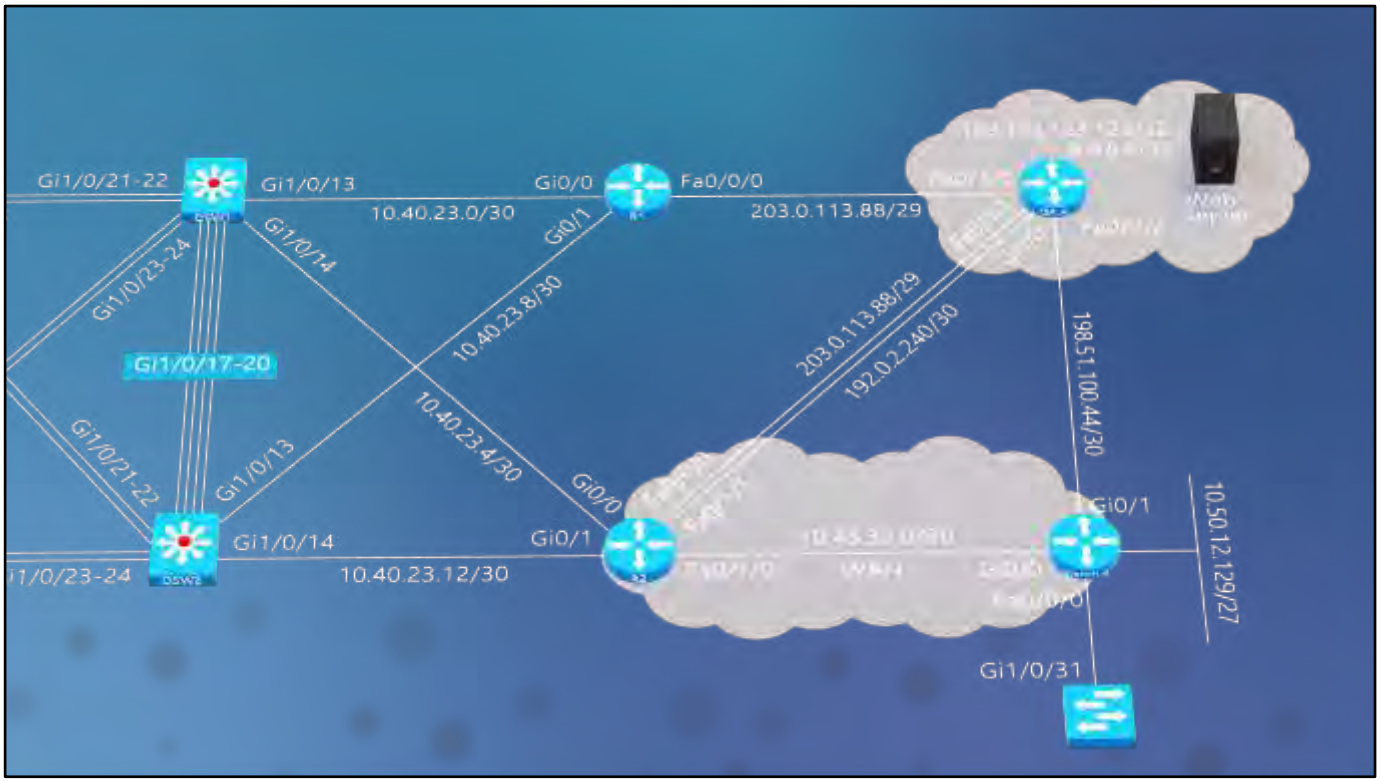
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



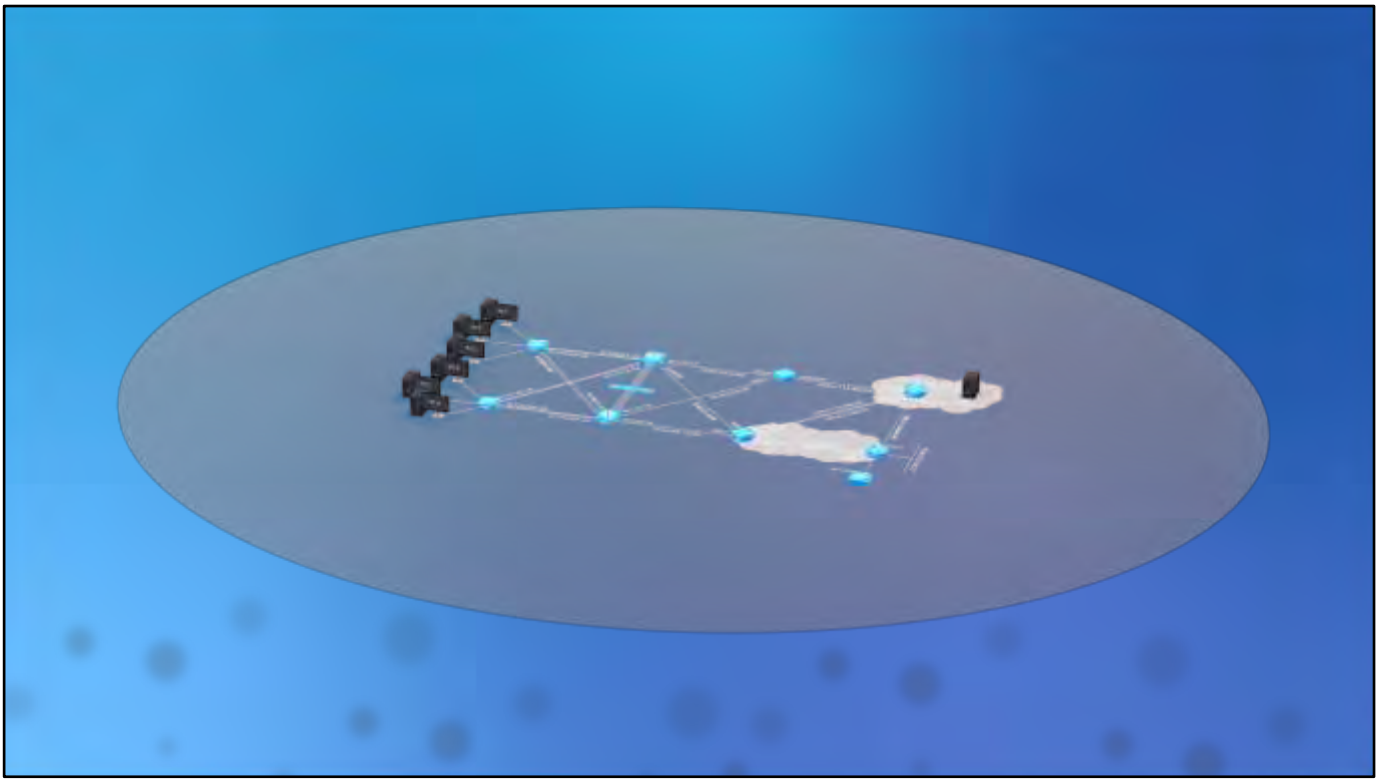
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Routing Protocols

Protocol	Type	Cisco Proprietary	Metric	EGP/IGP	AD
RIPv2	Distance Vector	No	Hop Count	IGP	120
EIGRP	Advanced Distance Vector	Yes	Bandwidth and Delay	IGP	90/170
OSPF	Link State	No	Cost	IGP	110
IS-IS	Link State	No	Cost	IGP	115
BGP	Path Vector	No	Attribute (AS Path)	EGP	20/200

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Comparing OSPF and EIGRP

EIGRP	OSPF
Cisco Proprietary	IETF Standard
Maintains pre-calculated, alternate, loop free paths that are used immediately when a link fails	Must calculate alternate paths to use upon link failure
Uses the DUAL algorithm	Uses the Dijkstra SPF algorithm
Requires an AS number that must match on all routers	Uses a Process ID that does not have to match on all routers
Advanced Distance Vector Routing Protocol	Link State Routing Protocol
Administrative Distance 90 for Internal route types and 170 for External route types	Administrative Distance 110 for all OSPF route types
Build large flexible networks	Build large scalable segmented networks using Areas
Metric is based on lowest bandwidth and cumulative delay along the path (FD)	Metric is based on interface bandwidths (cost) along the path
Summarization can happen on any EIGRP enabled interface	Summarization can happen on ABRs and ASBRs
Supports Auto-Summarization	Does not support Auto-Summarization
Supports a max of 255 router hops but defaults to 100	Supports an unlimited number of router hops
Supports equal and unequal metric load balancing	Supports equal metric load balancing
Hello = 5 Dead = 15	Hello = 10 Dead = 4x Hello (40)
Neighbor Table, Topology Table, Routing Table	Neighbor Table, Link State Database, Routing Table
	Virtual Links can be used to connect not directly connected areas to the backbone area

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPFv2 Overview, Packets, States, and Design

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF

- Open Shortest Path First
- Interior Gateway Routing Protocol
  - Link State Routing Protocol
- Developed by IETF
  - Open Standard
- Current version for IPv4 is OSPFv2
  - RFC 2328
- Current version for IPv6 is OSPFv3
  - RFC 5340

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF

Key Features:

- Scalable
- Converges quickly
- Supports
  - VLSM
  - ECMP
- Independent transport
- Efficient use of updates
- Simple Metric
- Manual route summarization
- Authentication

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF

- Discovers neighboring routers
  - Forms neighbor adjacencies
- Uses LSAs to exchange information
  - When neighborship forms
  - When a change occurs
  - Every 30 mins
    - LSAs are dead after 60 mins
- Maintains a complete view of the network
- Uses the SPF Algorithm to make decisions
- Uses COST as the metric

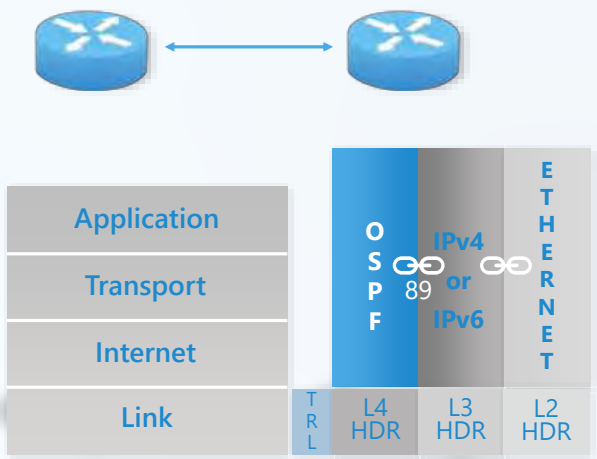
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Packets

Type	Packet Name
1	Hello
2	DBD
3	LSR
4	LSU
5	LSAck

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

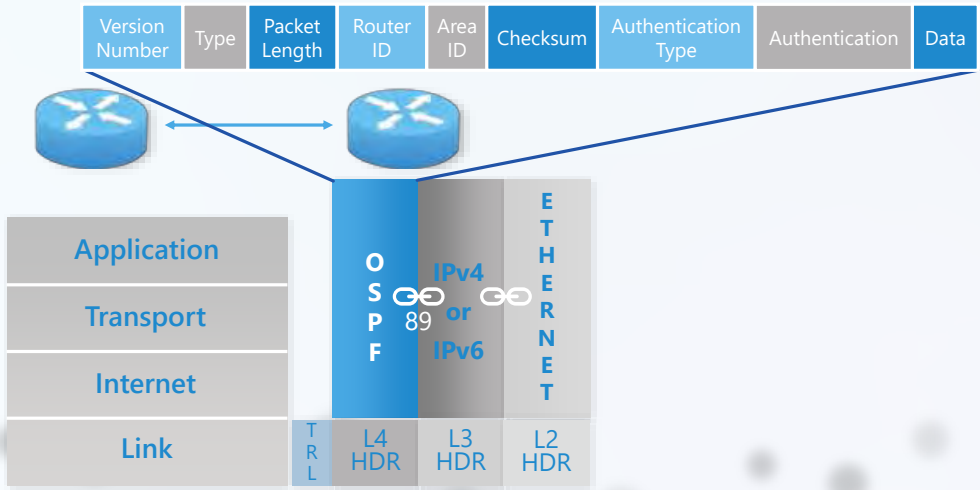
OSPF Packets



*HDR = Header

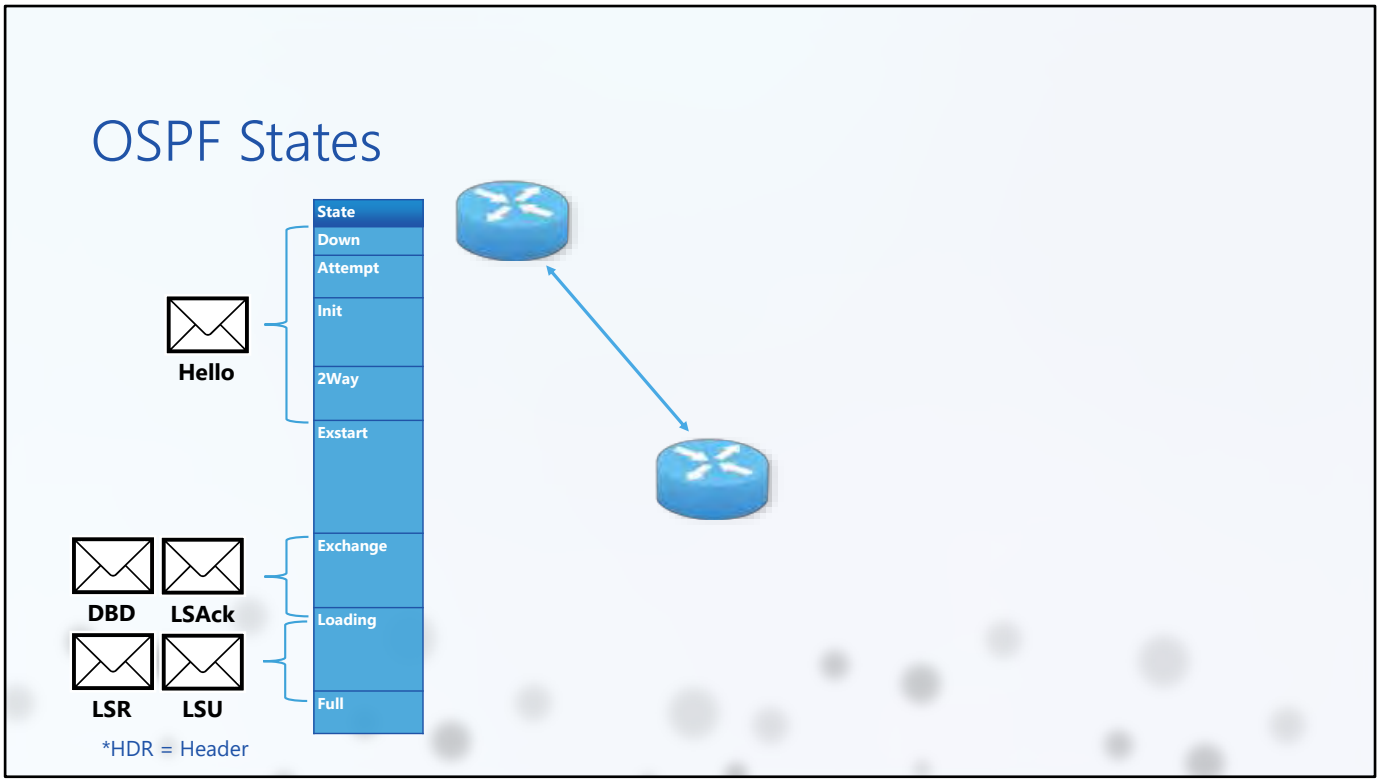
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Packets



*HDR = Header

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

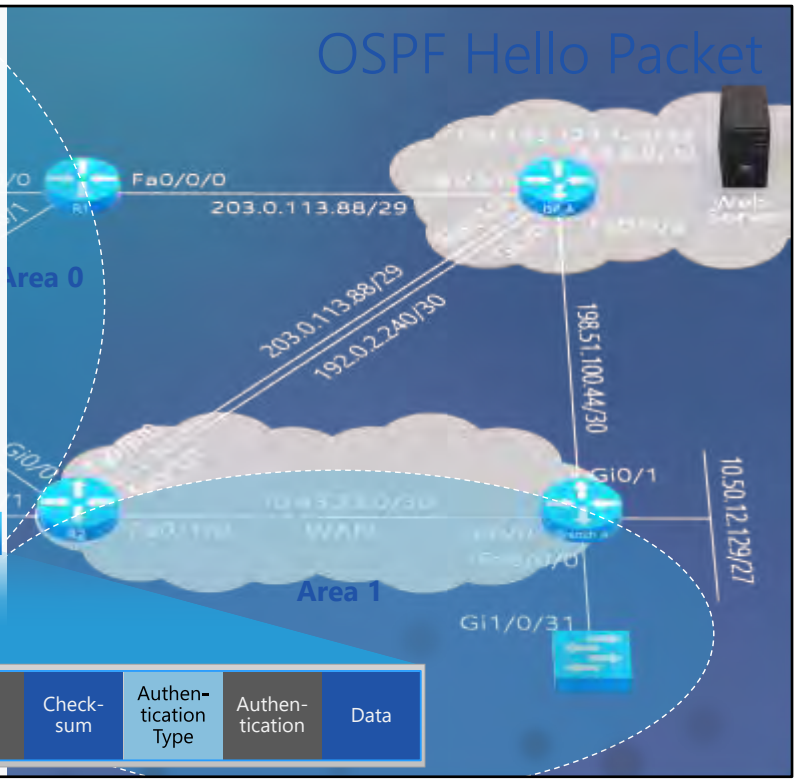


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Hello Packet

- Router ID
- Area ID
- Authentication
- Data
  - hello/dead interval
  - Neighbors
  - Router priority
  - DR IP address
  - BDR IP address
  - Stub area flag

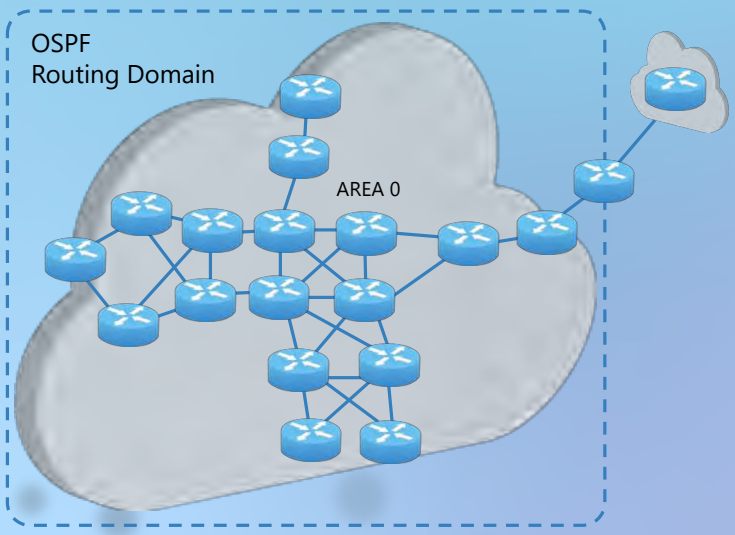
Hello are sent to multicast address 224.0.0.5



Version Number	Type	Packet Length	Router ID	Area ID	Check-sum	Authen-tication Type	Authen-tication	Data

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Areas

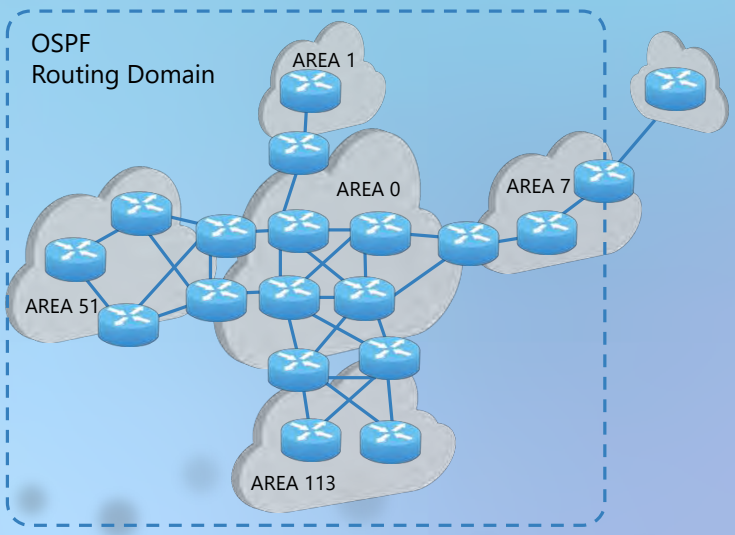


Scalability

- Single Area – limited
- Multi-Area – virtually unlimited

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Areas

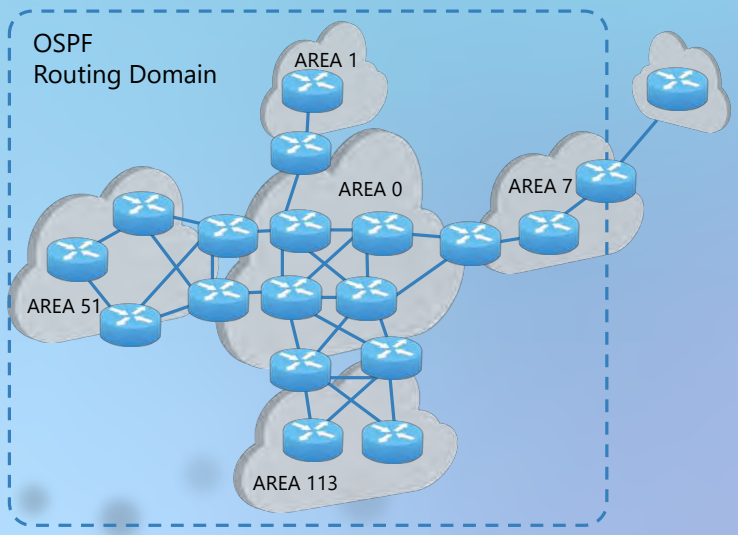


Scalability

- Single Area – limited
- Multi-Area – virtually unlimited

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Areas



Router Types:

Backbone router - a router with at least 1 interface in area 0

Internal router - all interfaces are in a single area

ABR – has at least one interface in area 0 and another interface in any other area

ASBR – has at least one interface in any area and another interface connected to a different routing domain

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPFv2 Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

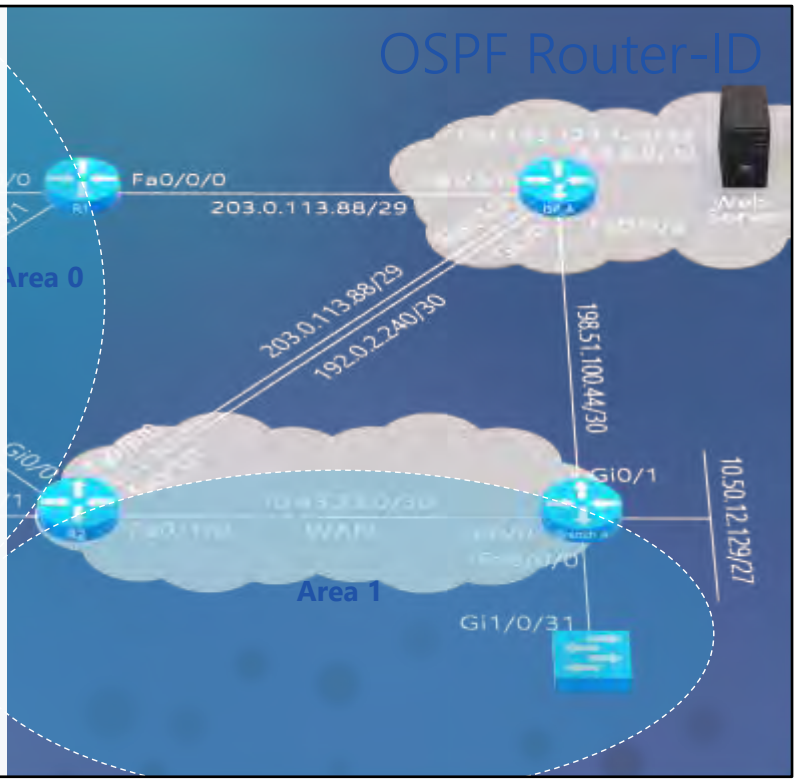
OSPF Router-ID

How a router uniquely identifies itself in OSPF

It can be manually configured with the `router-id`.

If `router-id` is not configured, the highest IP address on a loopback interface when OSPF starts is the router ID

If there is no loopback interface, then the router selects the highest IP address on any interface when OSPF process begins



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

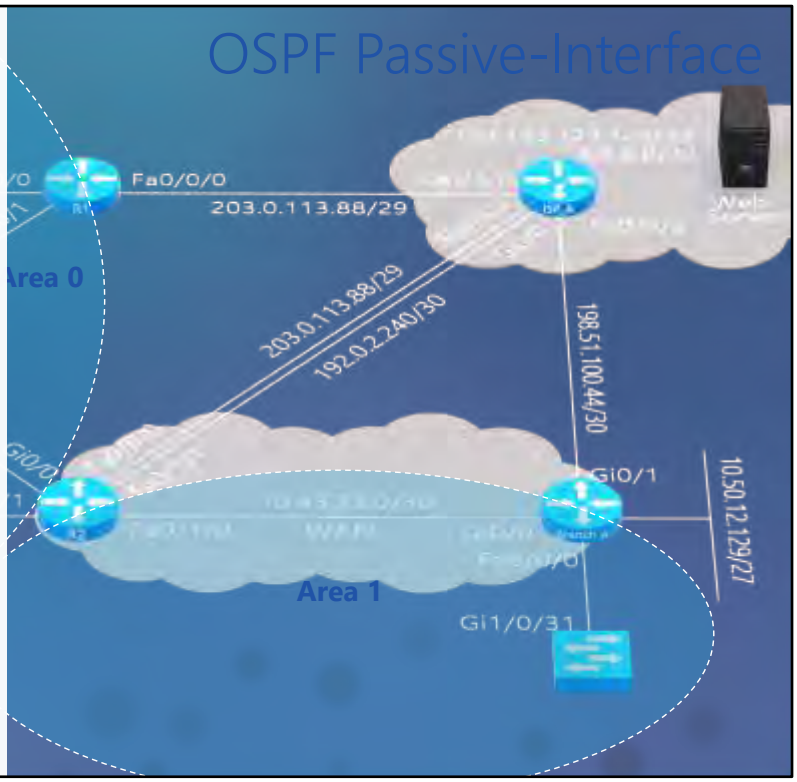
OSPF Passive-Interface

Suppress the send and receiving of OSPF messages on an interface.

Interface is still participating in the OSPF process.

Reduce the amount of OSPF traffic in the Layer 2 network.

Ensures rogue OSPF devices in L2 network can't form neighbor adjacencies with routers and infect or LSDB with false information.



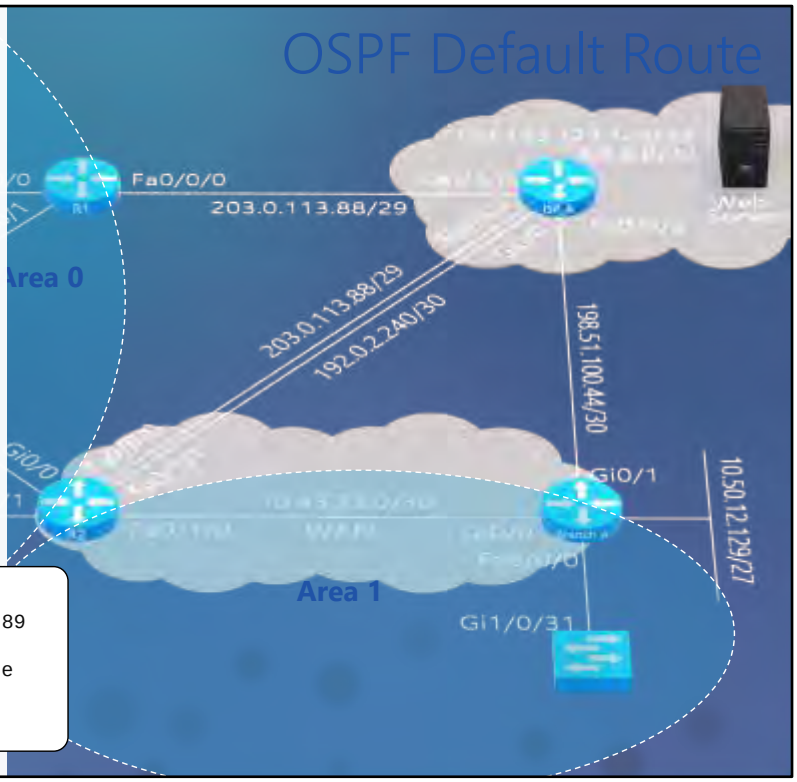
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Default Route

Inject a default route listed in the routing table into the OSPF database so it can be shared with other OSPF enabled routers.




```
R2#configure terminal
R2(config)#ip route 0.0.0.0 0.0.0.0 203.0.113.89
R2(config)#router ospf 1
R2(config-router)#default-information originate
R2(config-router)#end
R2#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

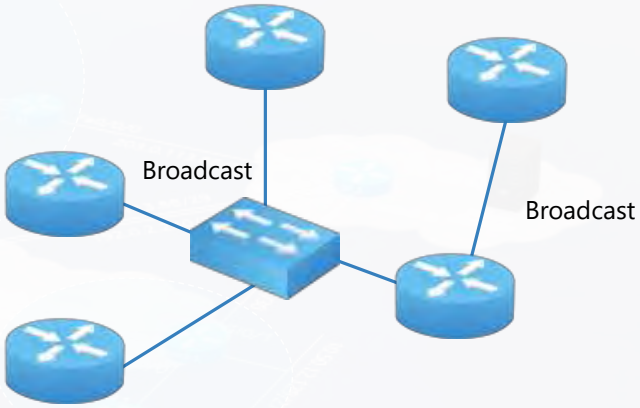
OSPFv2 DR/BDR Election and Network Types

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

Optimizes OSPF Adjacency Behavior in a Multi-Access Network.

- Reduces routing update traffic
- Manages link state synchronization



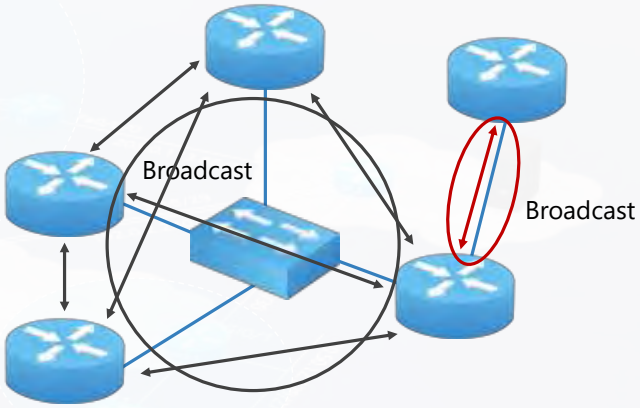
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

Without

Everyone establishes a Full adjacency with each other and performs a Full database synchronization

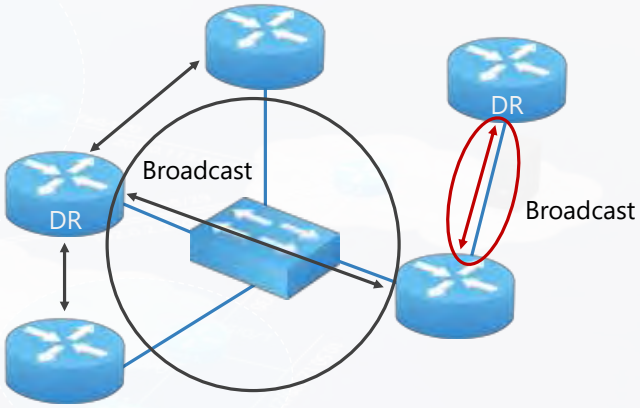


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

With

Everyone establishes a Full adjacency with the DR and only Fully synchronize LSDB with the DR using 224.0.0.6.



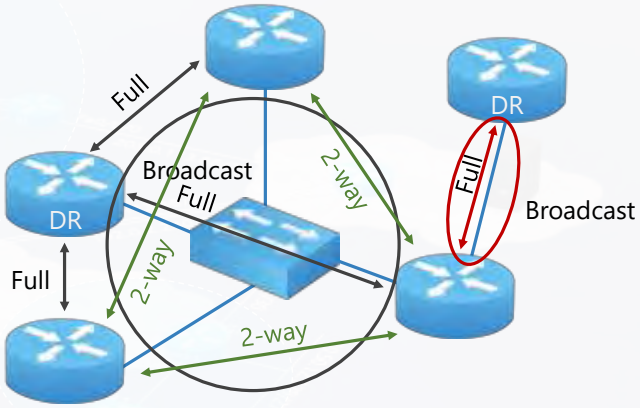
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

With

Everyone establishes a Full adjacency with the DR and only Fully synchronize LSDB with the DR using 224.0.0.6.

DR uses 224.0.0.5 to propagate LSAs to routers

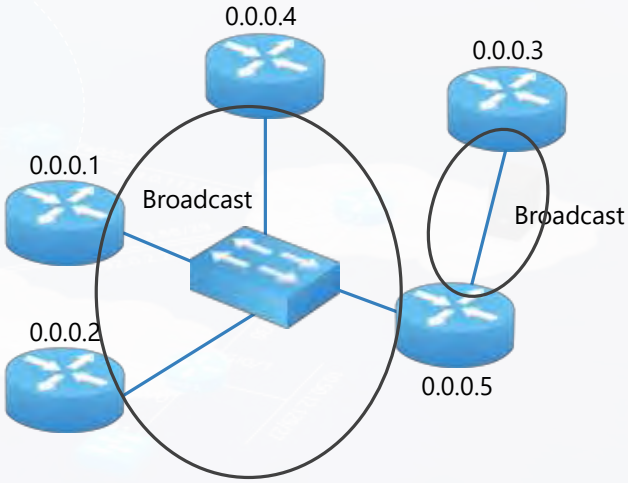


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

A **Designated Router** (DR) is elected in Multi-access Networks

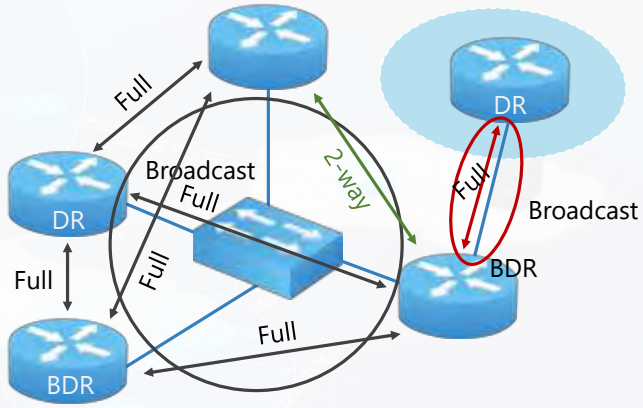
- Highest Priority / Highest Router ID
  - Default Priority = 1



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

DR and BDR Synchronization



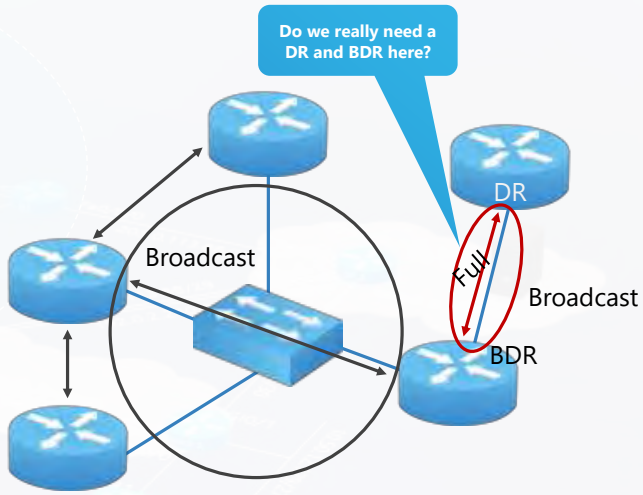
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF DR/BDR

A **Designated Router** (DR) is elected in Multi-access Networks

Highest Priority / Highest Router ID

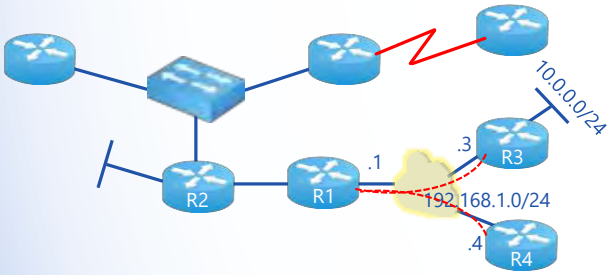
Default Priority = 1



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Network Types

- Point-To-Point
- Broadcast
- Nonbroadcast
- Point-To-Multipoint
- Point-To-Multipoint Nonbroadcast
- Loopback



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

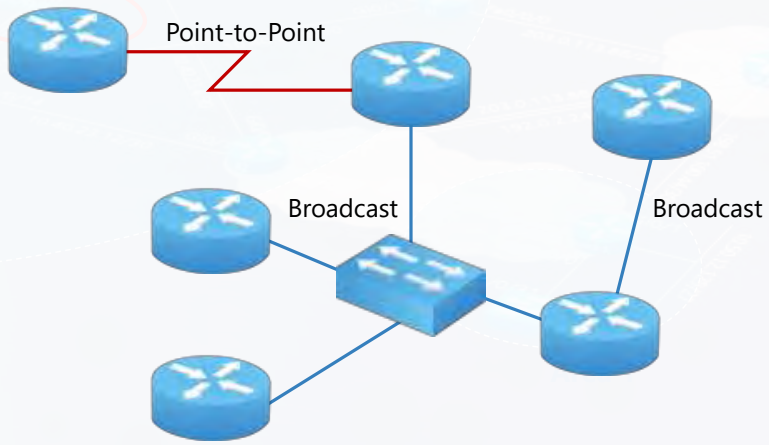
OSPF Network Types

	Timers	Neighbors	DR Election
Point-To-Point	10/40	Dynamic	No
Broadcast	10/40	Dynamic	Yes
Nonbroadcast	30/120	Static	Yes
Point-To-Multipoint	30/120	Dynamic	No
Point-To-Multipoint Nonbroadcast	30/120	Static	No
Loopback	N/A	N/A	N/A

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Network Types

OSPF Network Type	Uses DR/BDR	Default Hello Interval (sec)	Dynamic Neighbor Discovery	More Than 2 Routers Allowed in Subnet?
Point-to-point	No	10	Yes	No
Broadcast	Yes	10	Yes	Yes



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPFv2 LSAs and Metric

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Route Types

O – OSPF destination in the same area
OI – OSPF destination in a different area
OE1/2 – Destination outside OSPF domain

```
DSW1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.120.2 to network 0.0.0.0

     172.17.0.0/24 is subnetted, 1 subnets
O IA    172.17.34.0 [110/658] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
     172.16.0.0/24 is subnetted, 1 subnets
O IA    172.16.34.0 [110/21] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
O IA 192.168.4.0/24 [110/22] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
     10.0.0.0/24 is subnetted, 9 subnets
C       10.0.10.0 is directly connected, GigabitEthernet1/44
O       10.0.12.0 [110/11] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
...output omitted...
O       10.0.20.0 [110/11] via 10.0.120.2, 00:05:35, Port-channel12
O       10.0.123.0 [110/11] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
C       10.0.120.0 is directly connected, Port-channel12
O*E2 0.0.0.0/0 [110/1] via 10.0.120.2, 00:05:35, Port-channel12
               [110/1] via 10.0.10.1, 00:05:35, GigabitEthernet1/44
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF LSAs

Used to exchange link-state information between routers

Uses LSAs to exchange information

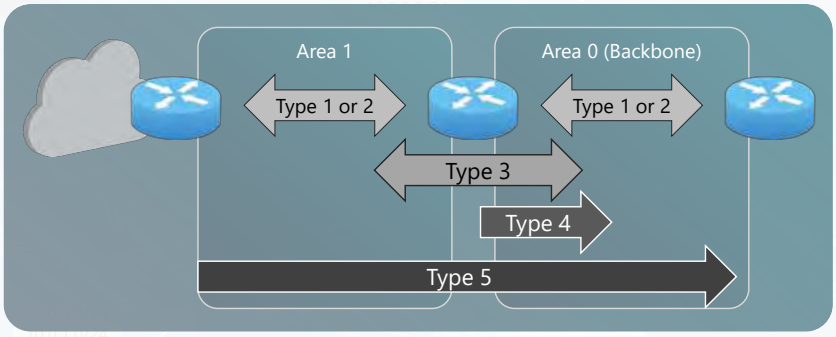
- As soon as a neighborship is formed
- When a change occurs
- Every 30 mins

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LSA Types

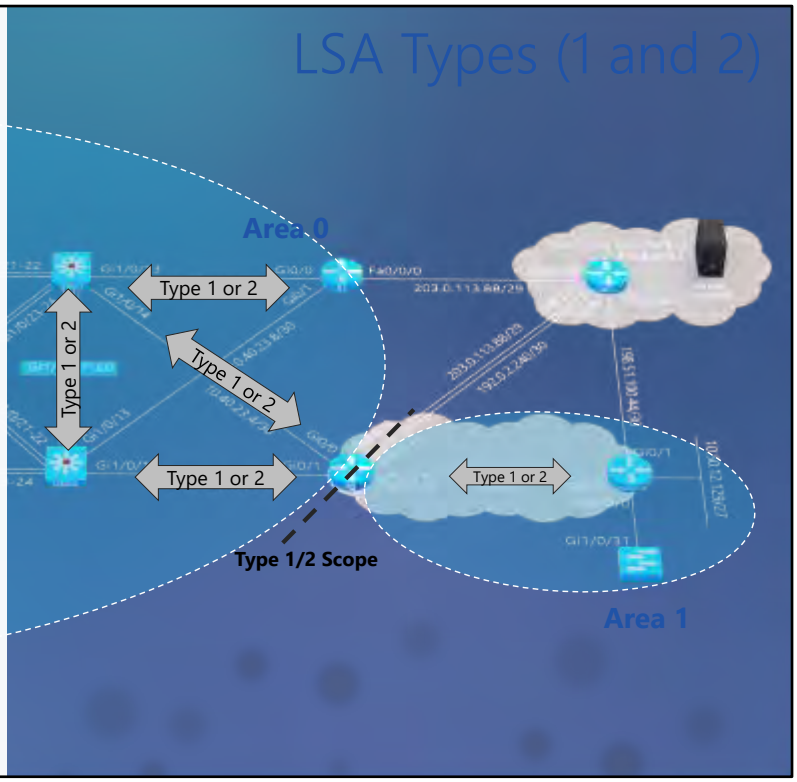


LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LSA Types (1 and 2)

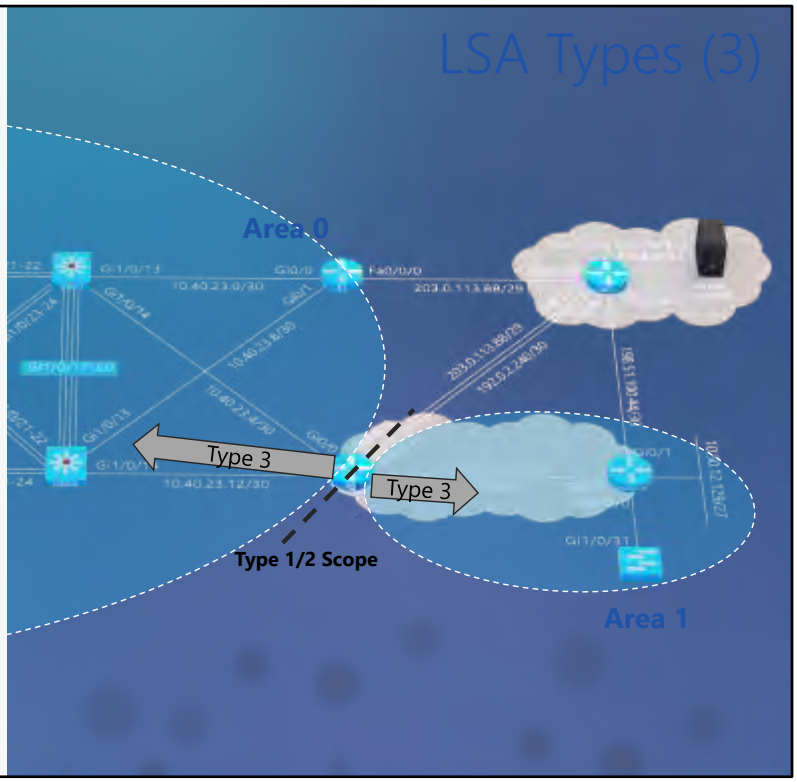
LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

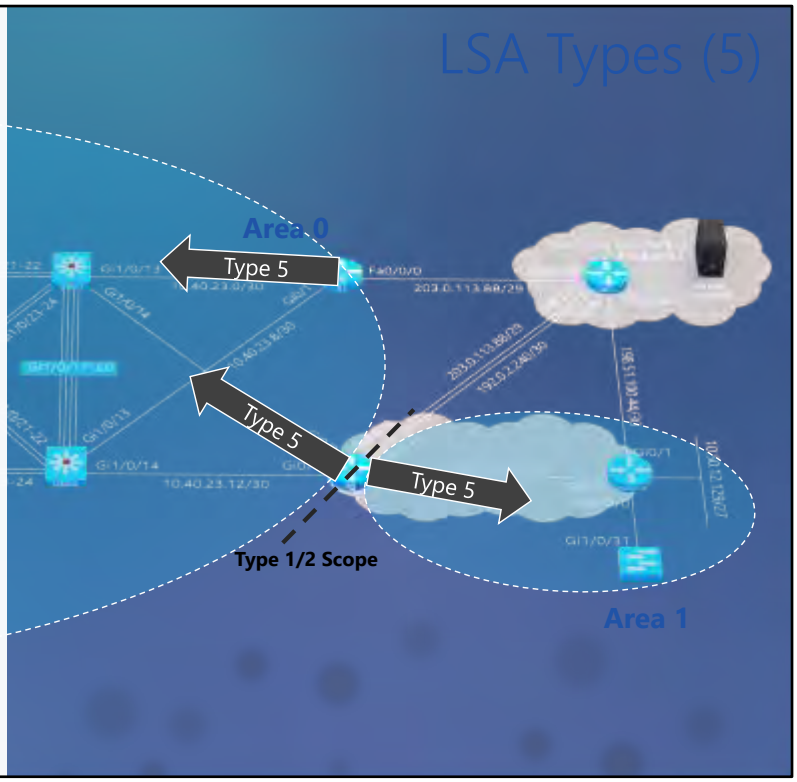
LSA Types (3)

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LSA Types (5)

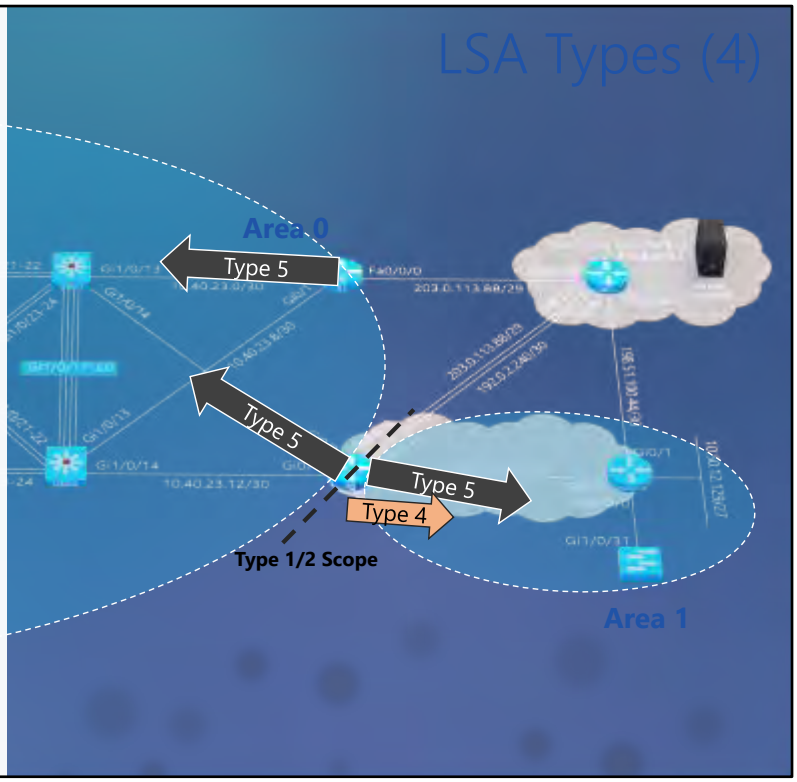


LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LSA Types (4)

LSA Type	Description
1	Router LSA = O routes
2	Network LSA
3	Summary LSA = O IA routes
4	ASBR summary LSA
5	Autonomous system LSA = E routes



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF COST

OSPF's metric is "cost"

The **cost** is based on the interface bandwidth

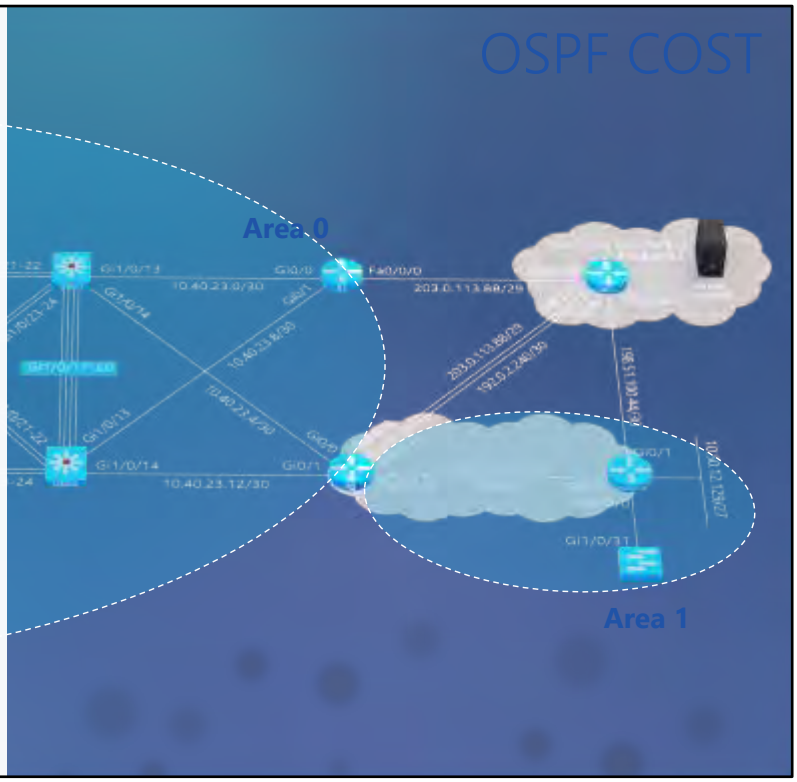
Cost = Reference Bandwidth / Interface Bandwidth

Reference bandwidth by default is **100 Mbs**

Change the reference bandwidth:

auto-cost reference-bandwidth

Total path cost is cumulated for every link/hop to the destination



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

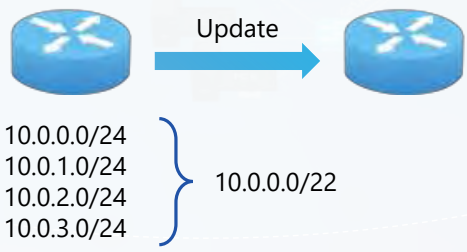
OSPFv2 Summarization

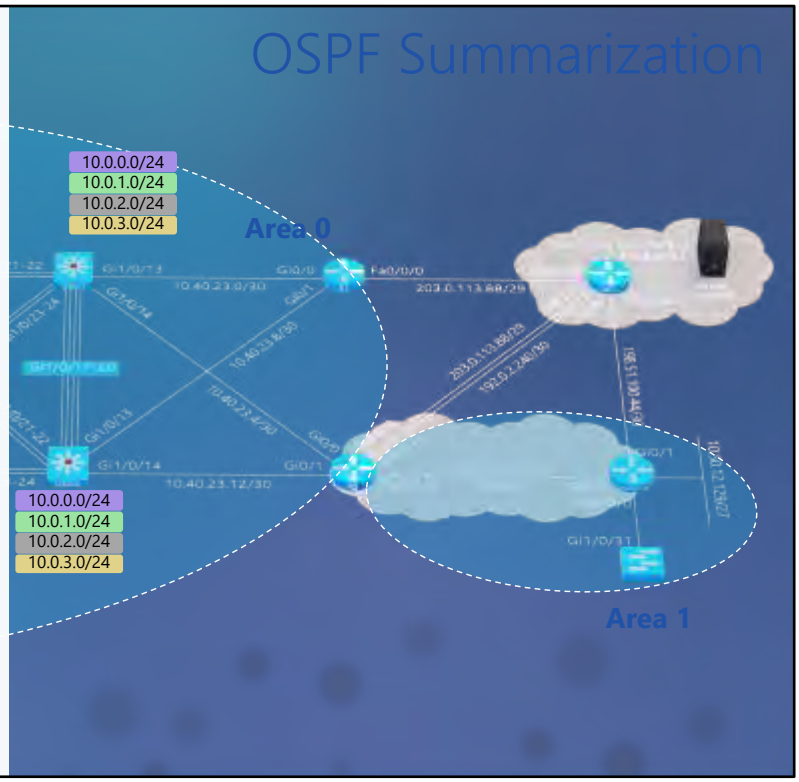
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Summarization

Consolidation of advertised addresses

- reduces size and number of updates
- localizes topology change
- reduces size of LSDB
- reduces size of routing table





©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Summarization

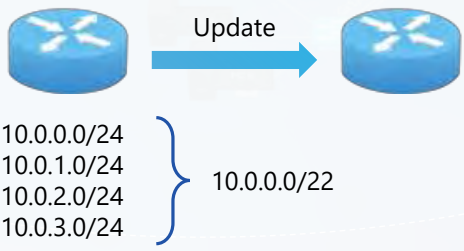
Can be done on:

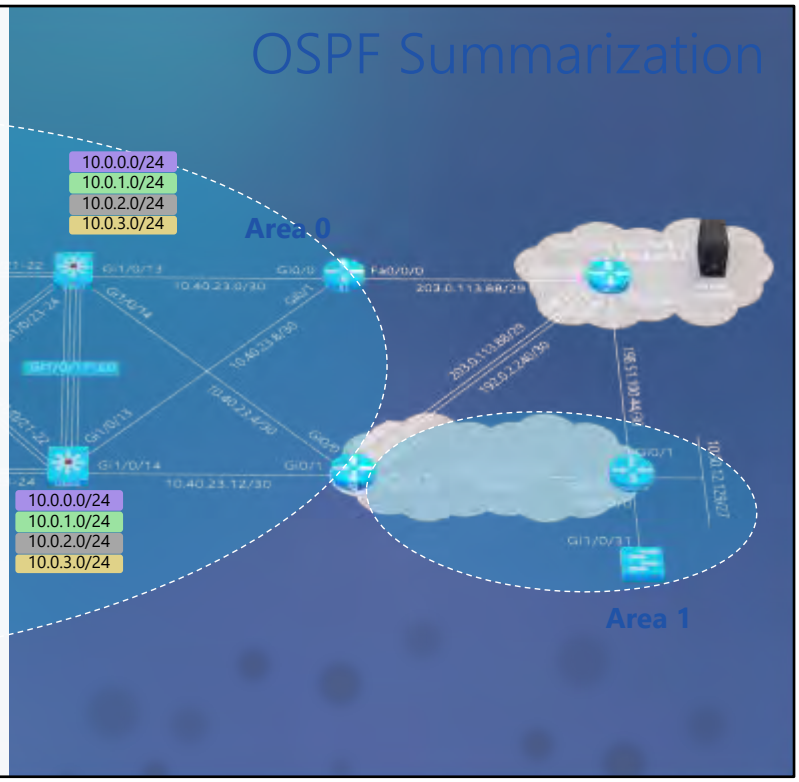
ABR – summarize Type 3 LSAs

```
area area_number range address mask
```

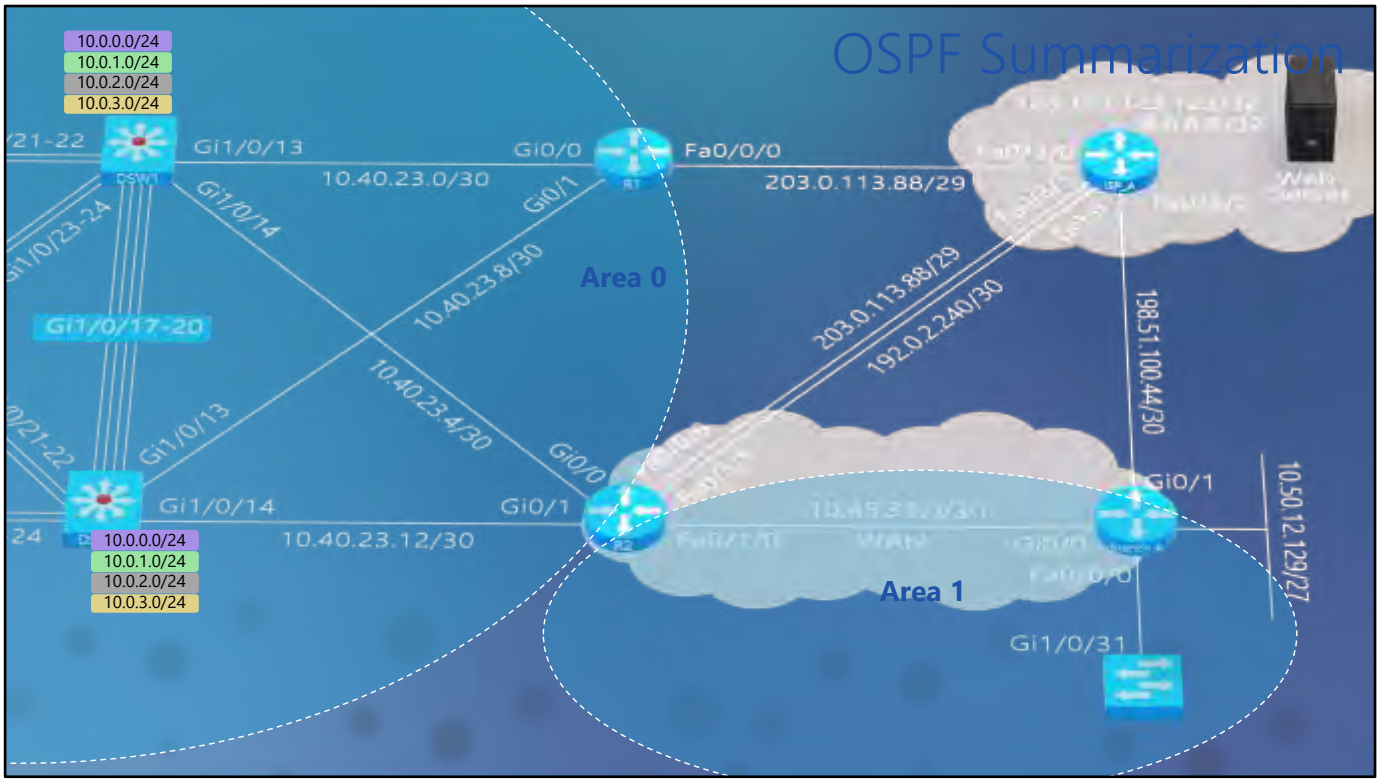
ASBR – summarize Type 5 LSAs

```
summary-address address mask
```





©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

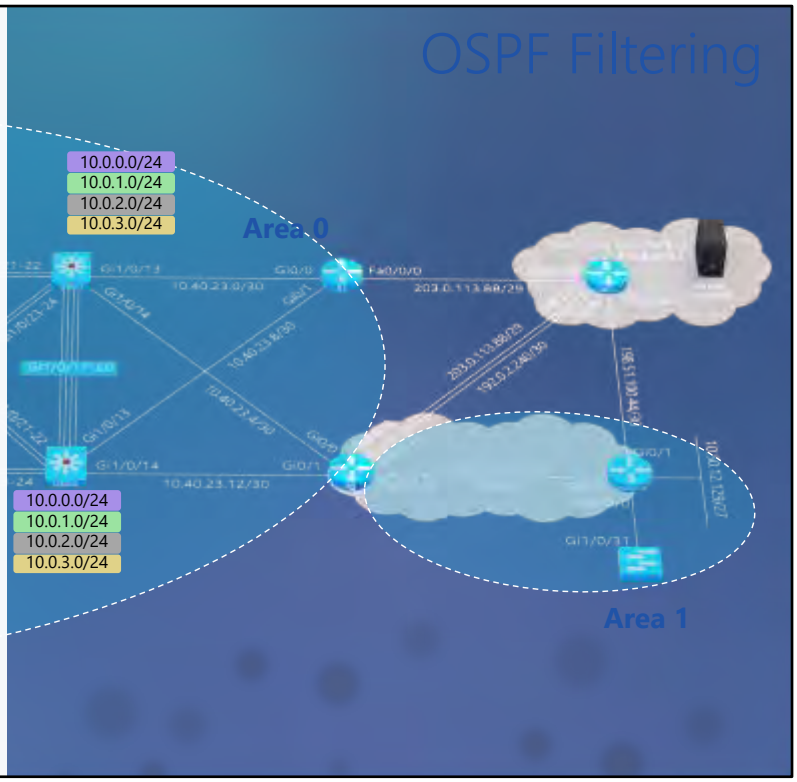
OSPFv2 Filtering, Prefix Suppression and Bidirectional Forwarding Detection

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Filtering

Used to control:

- What can be placed in the routing table
- What will be shared with other routers



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

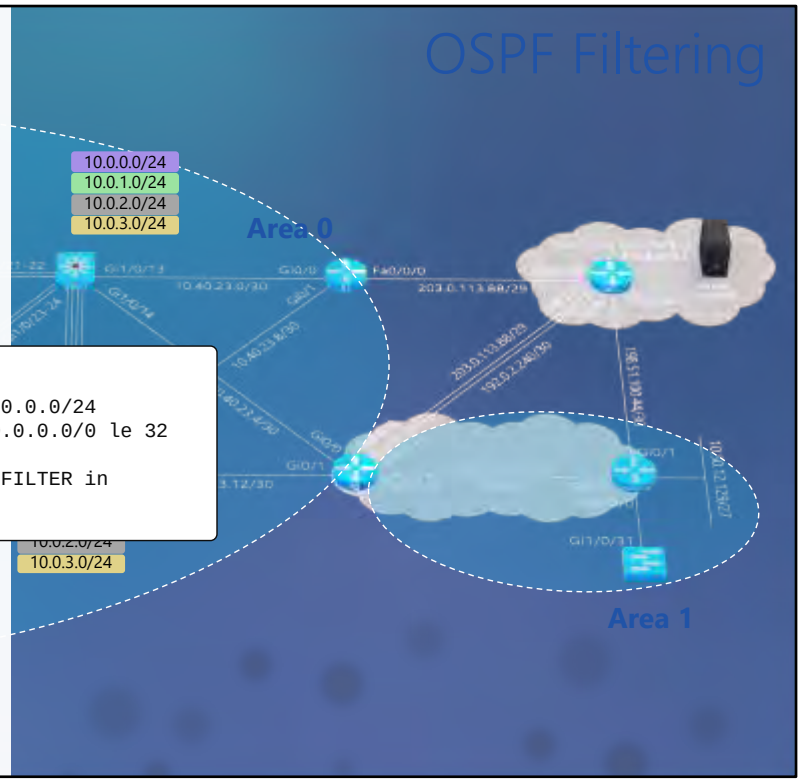
OSPF Filtering

Used to control:

What can be placed in the routing table

Distribute-List

```
BRANCHA#configure terminal
BRANCHA(config)#ip prefix-list FILTER deny 10.0.0.0/24
BRANCHA(config)#ip prefix-list FILTER permit 0.0.0.0/0 le 32
BRANCHA(config)#router ospf 1
BRANCHA(config-router)#distribute-list prefix FILTER in
BRANCHA(config-router)#end
```



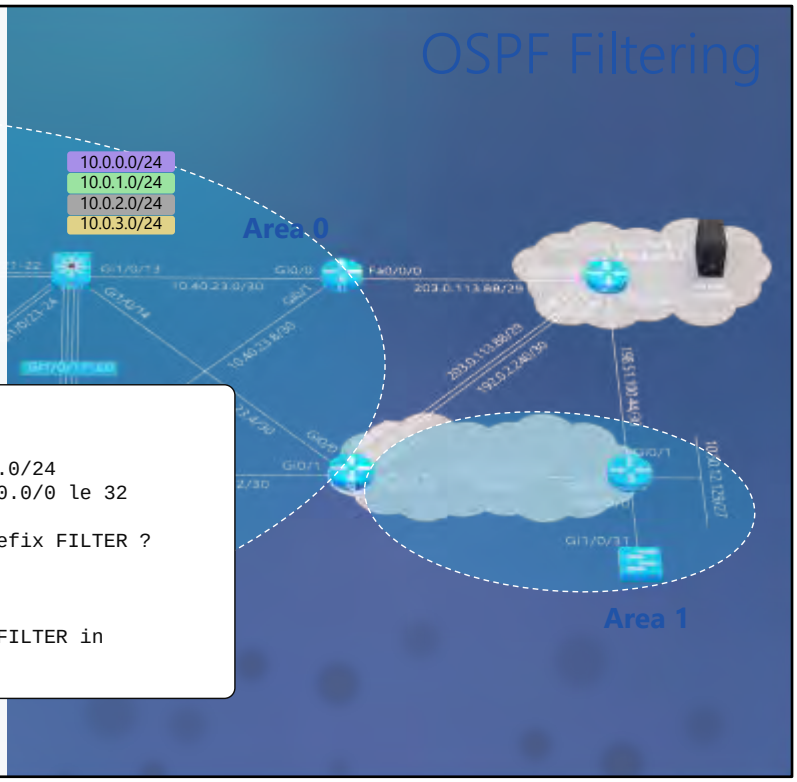
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

OSPF Filtering

Used to control:

- What will be shared with other routers
  - Type 3 Filter List




```
R2#configure terminal
R2(config)#ip prefix-list FILTER deny 10.0.0.0/24
R2(config)#ip prefix-list FILTER permit 0.0.0.0/0 le 32
R2(config)#router ospf 1
BranchA(config-router)#area 1 filter-list prefix FILTER ?
  in   Filter networks sent to this area
  out  Filter networks sent from this area

R2(config-router)#area 1 filter-list prefix FILTER in
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

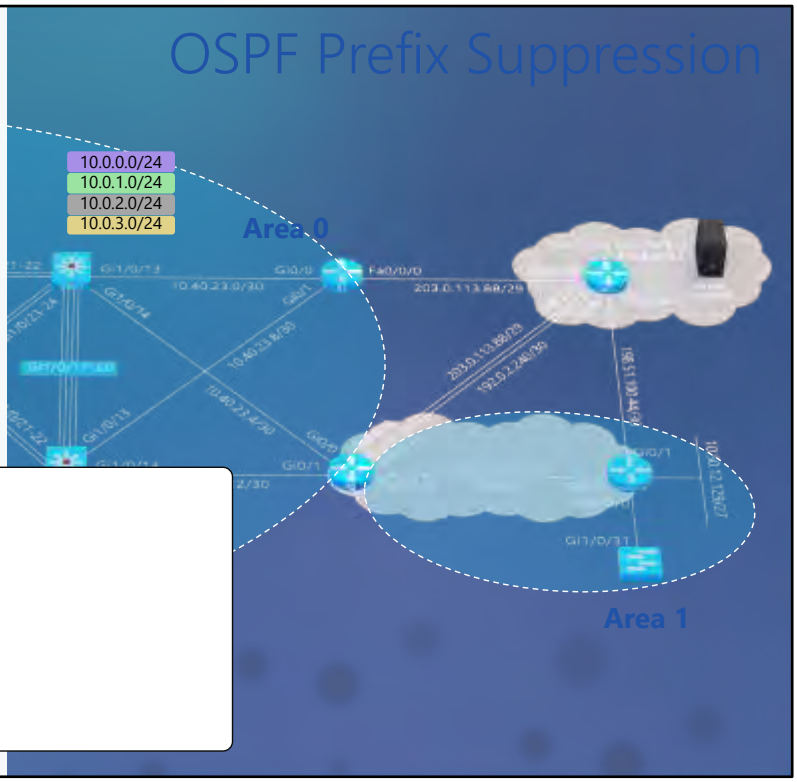
OSPF Prefix Suppression

Used to control:

The sharing of local network IDs associated with interfaces participating in the routing process.

Example: Suppress the sharing of transit links as they should never be the destination of traffic.

```
R2#configure terminal
R2(config)#router ospf 1
R2(config-router)#prefix-suppression

… or …

R2#configure terminal
R2(config)#interface gig 0/0
R2(config-router)#ip ospf prefix-suppression
R2(config-router)#int gig 0/1
R2(config-router)#ip ospf prefix-suppression
```



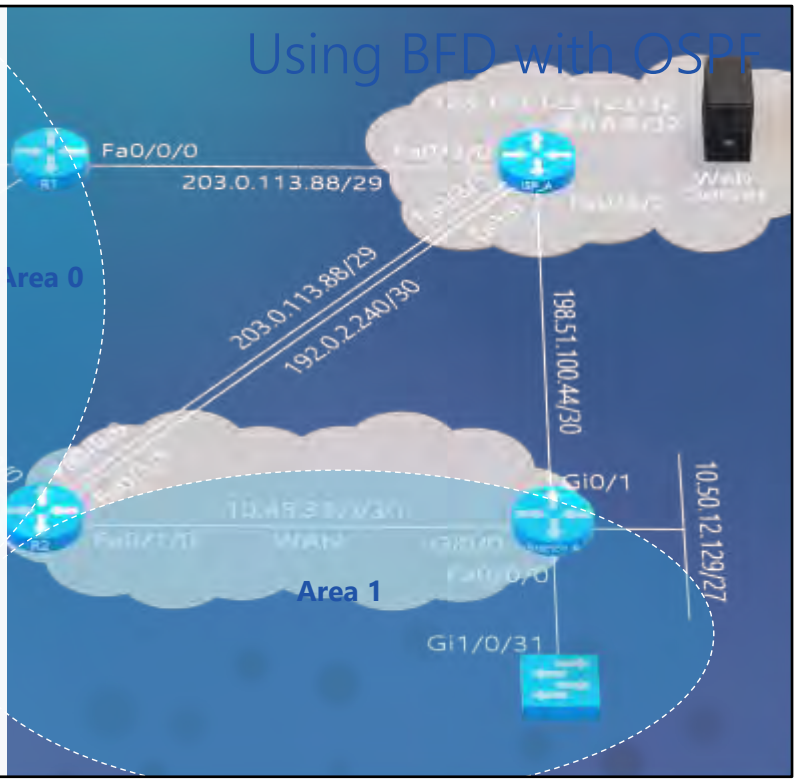
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Using BFD with OSPF

BFD:

A detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols.

Provides sub second convergence with our dynamic routing protocols



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EBGP Overview, Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Border Gateway Protocol

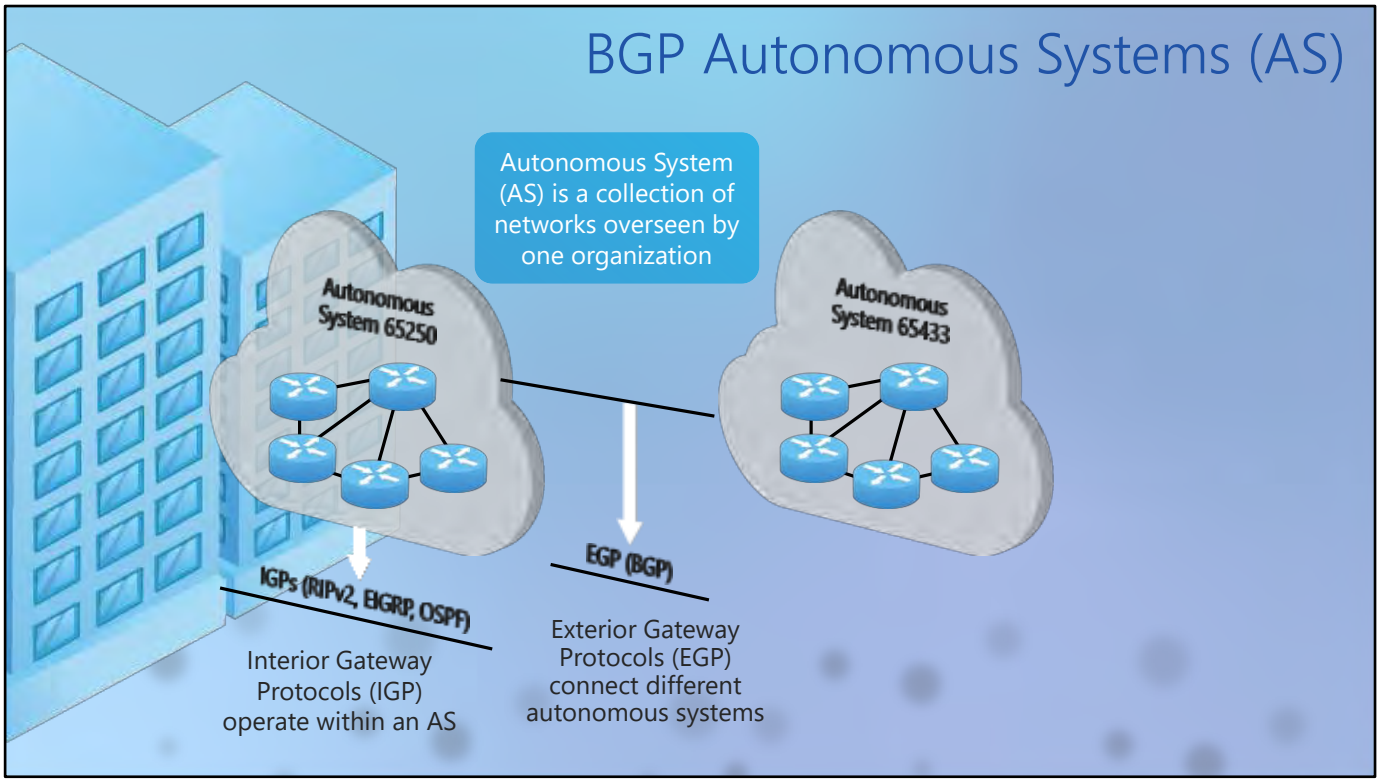
Routing Protocol For the Internet

Very Scalable

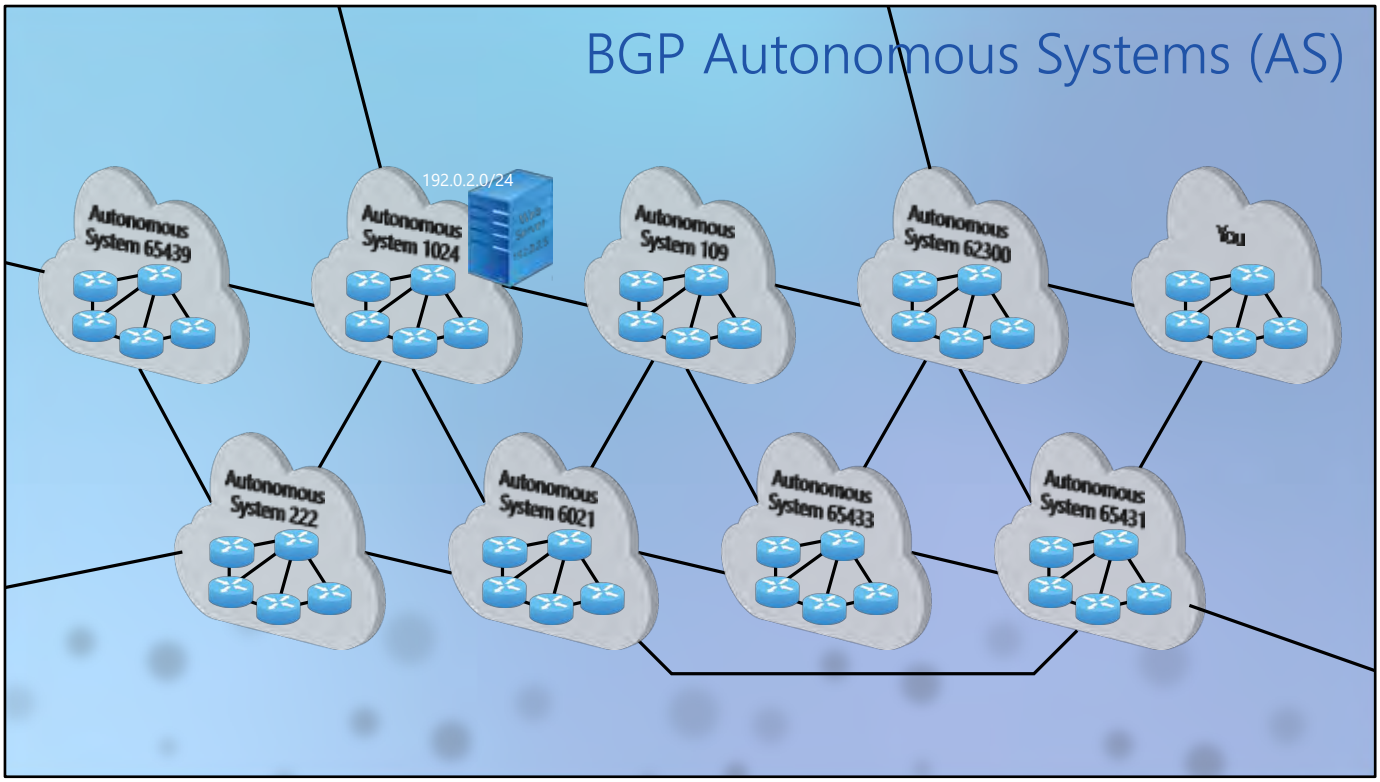
Used heavily by ISPs

Used lightly by non-ISPs

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Autonomous System Numbers

Public – Assigned By IANA through RIRs and ISPs

- 2 byte original range 1 to 64511
- 4 byte new range 65536 to 4199999999

Private – Assigned By You

- 64512 to 65534
- 4200000000 to 4294967294

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

BGP Basics

- Uses TCP port 179
  - client/server
- Classified as:
  - Path Vector (similar to D.V.)
- Forms neighborships
- Advertises NLRI
  - Prefix
  - Advertises Path Attributes (PA)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

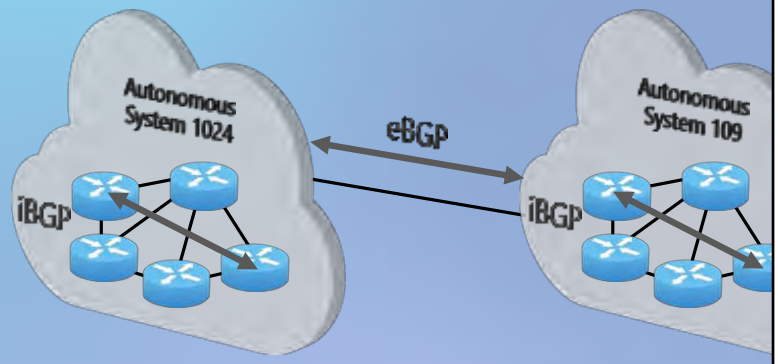
eBGP vs iBGP

eBGP

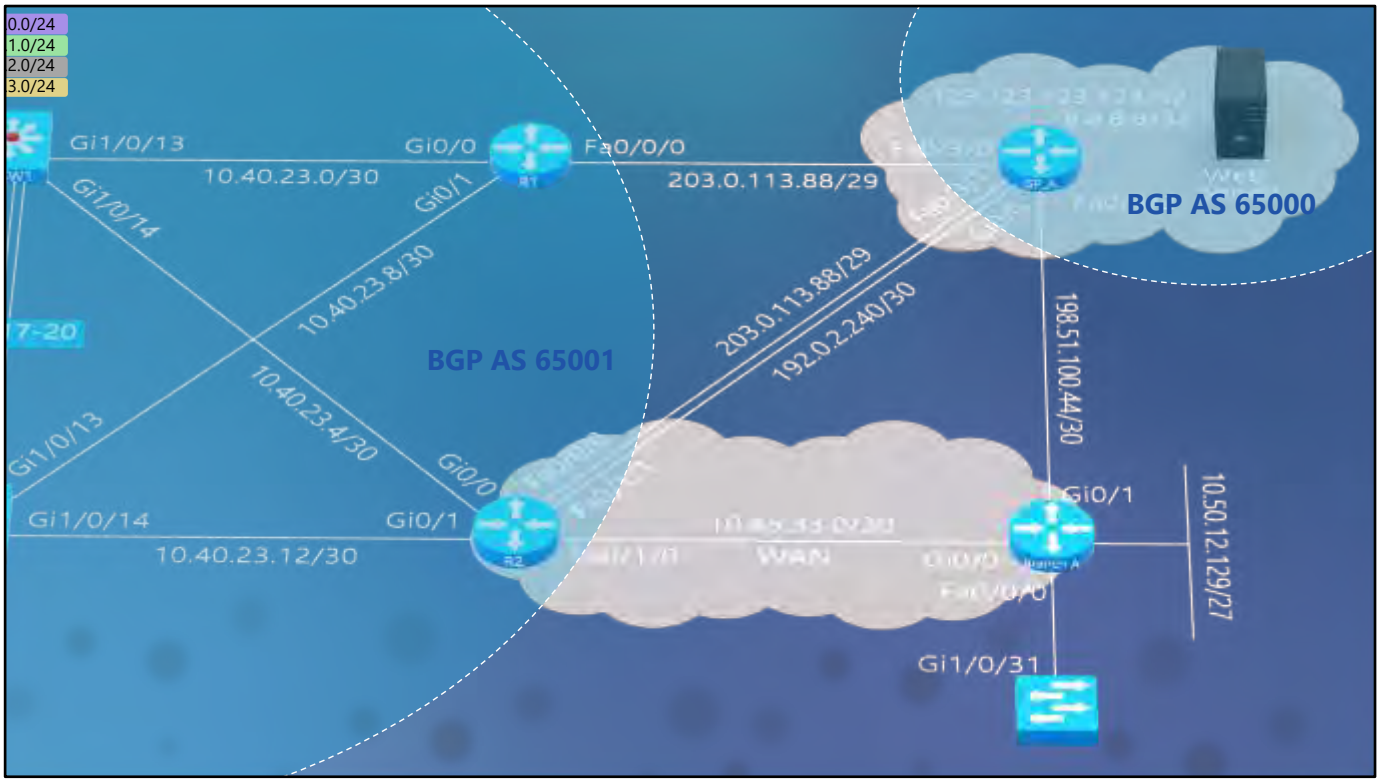
Peering between directly connected routers in different AS, AD of 20

iBGP

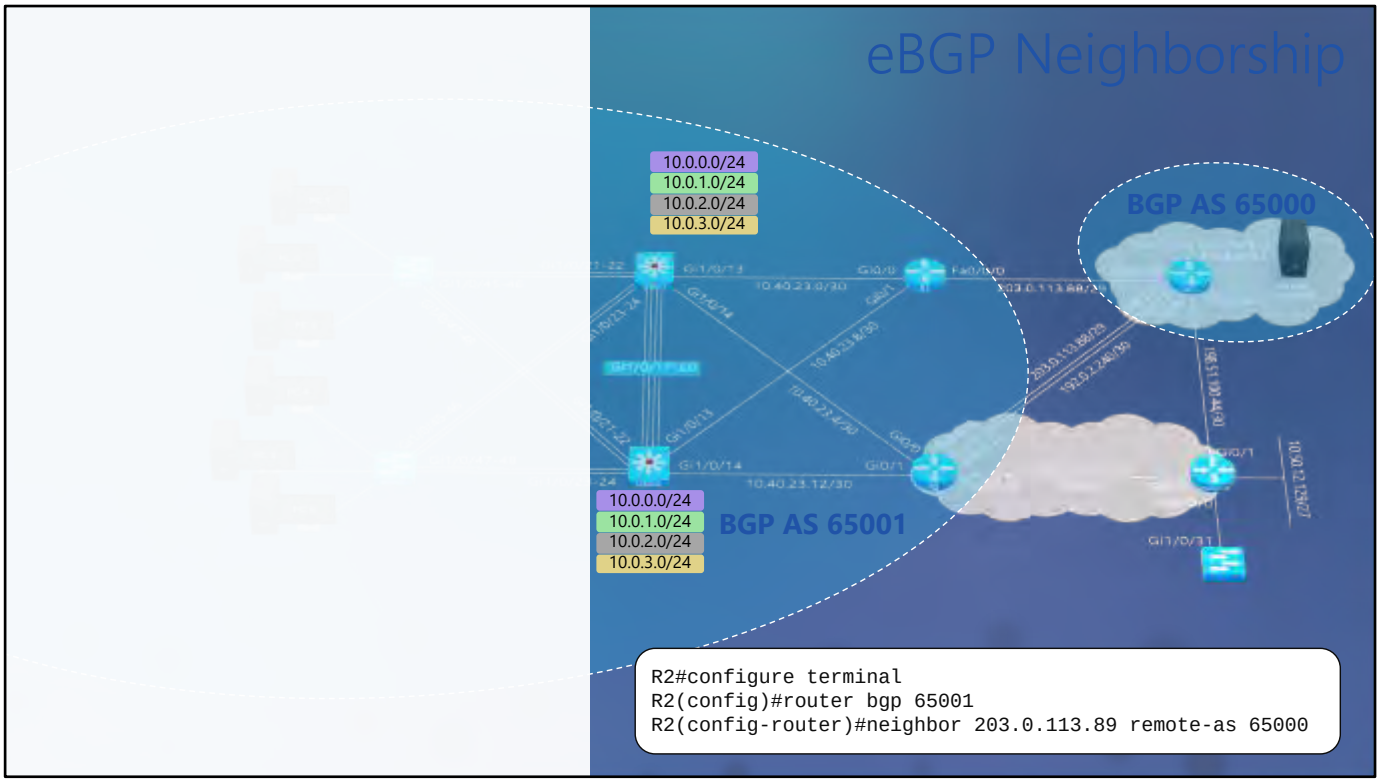
Peering between any routers in same AS, AD of 200



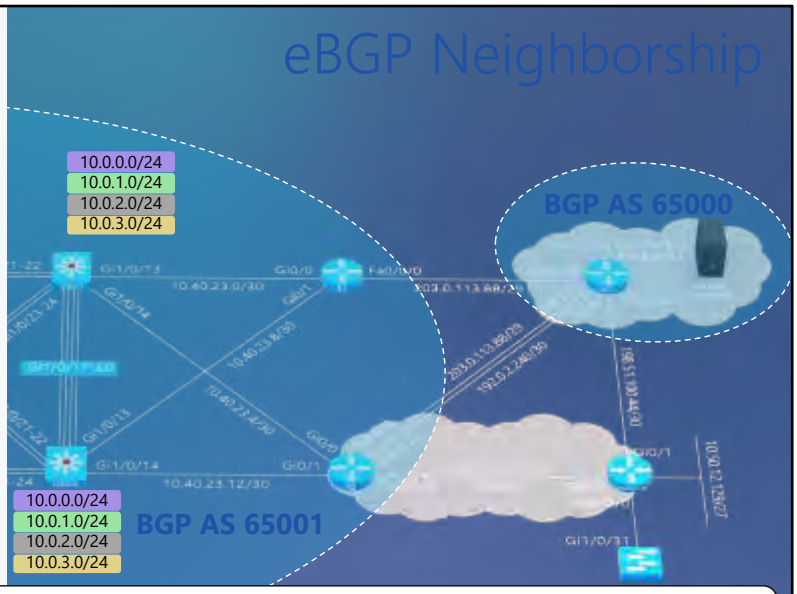
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

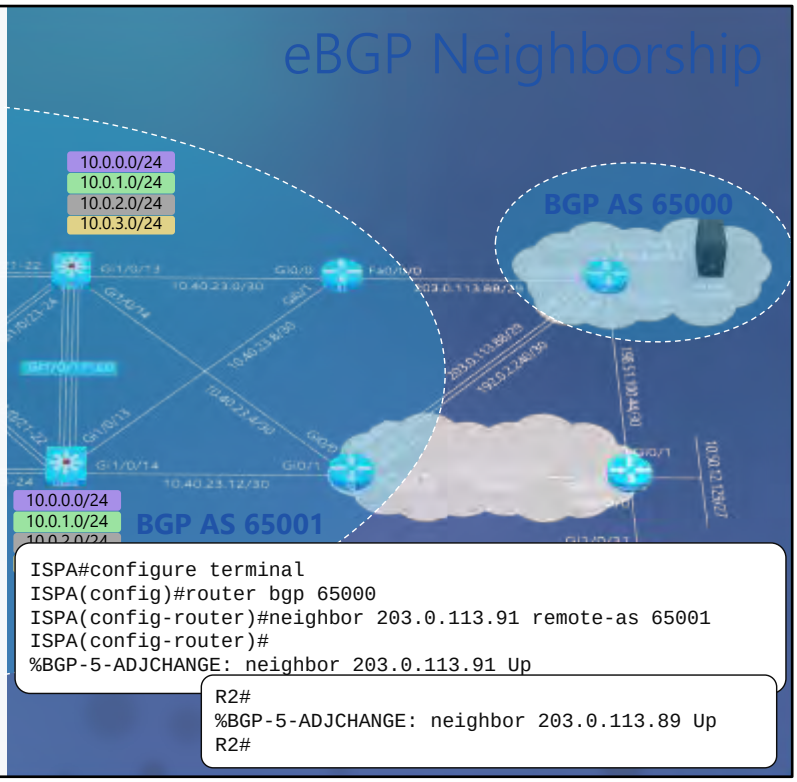


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

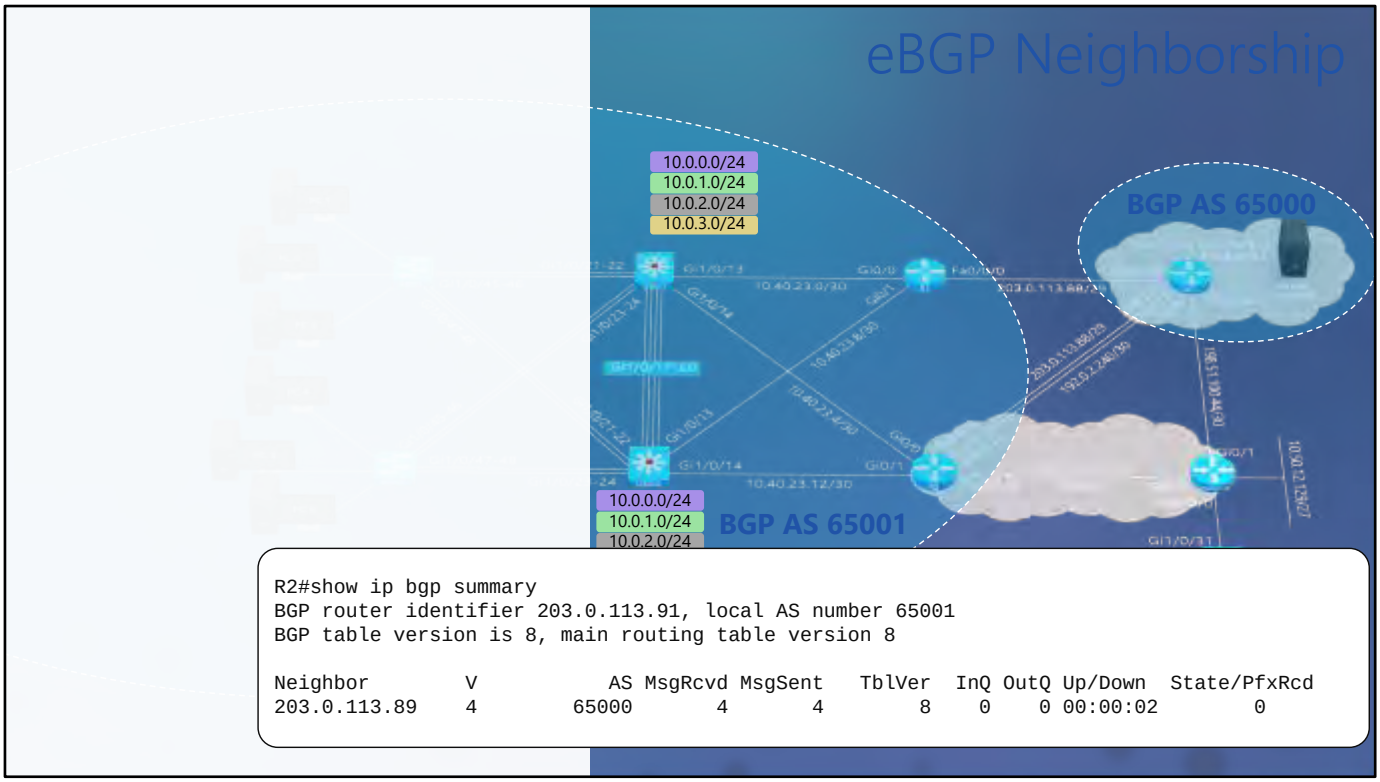



```
R2#show ip bgp summary
BGP router identifier 203.0.113.90, local AS number 65001
BGP table version is 8, main routing table version 8

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
203.0.113.89    4        65000       0       0        1    0    0 00:00:04 Idle
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

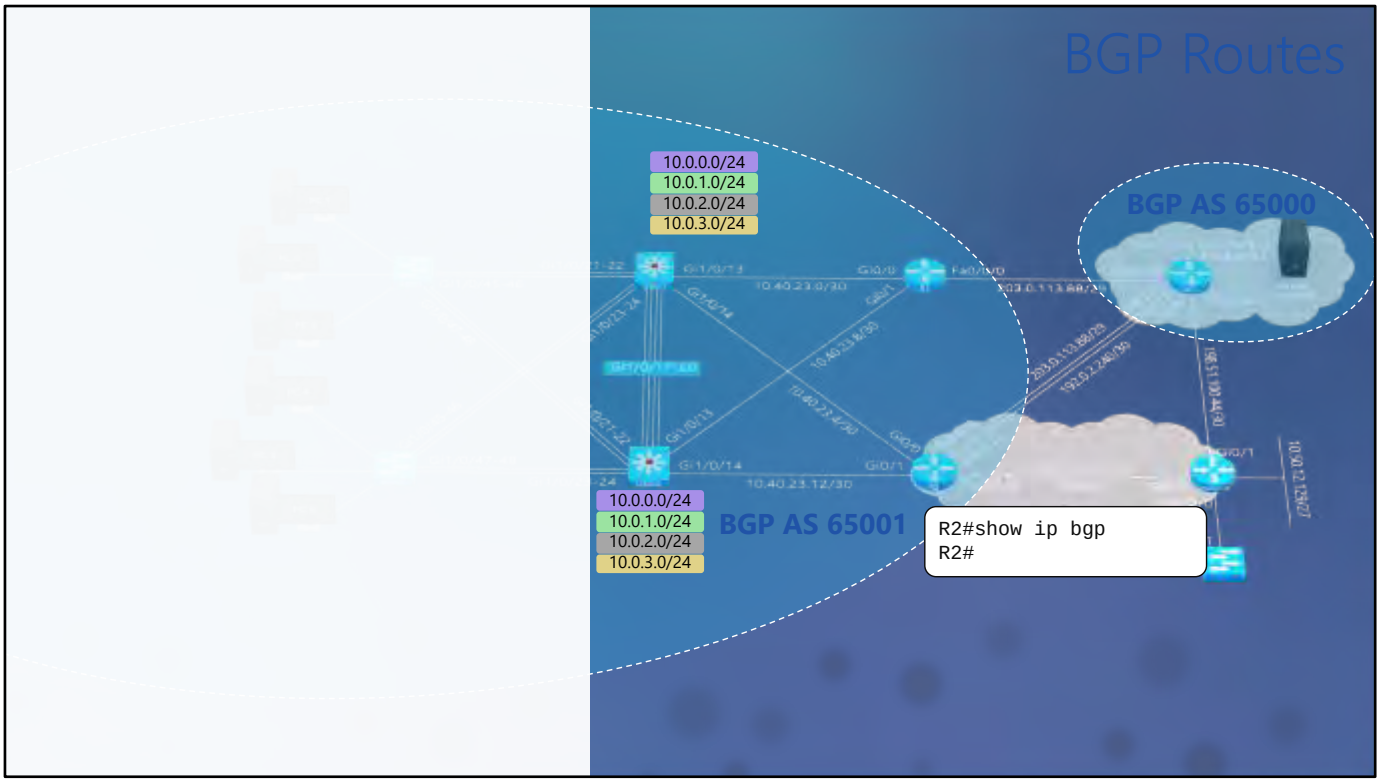


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



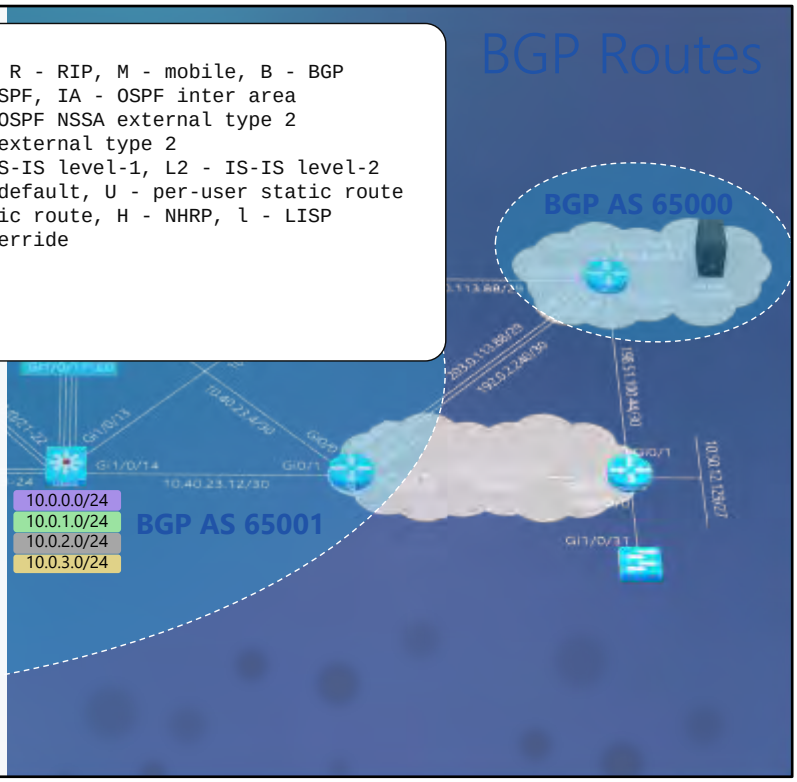

```
R2#show ip bgp summary
BGP router identifier 203.0.113.91, local AS number 65001
BGP table version is 8, main routing table version 8

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
203.0.113.89    4        65000       4       4        8    0    0 00:00:02        0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
R2#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

R2#
```



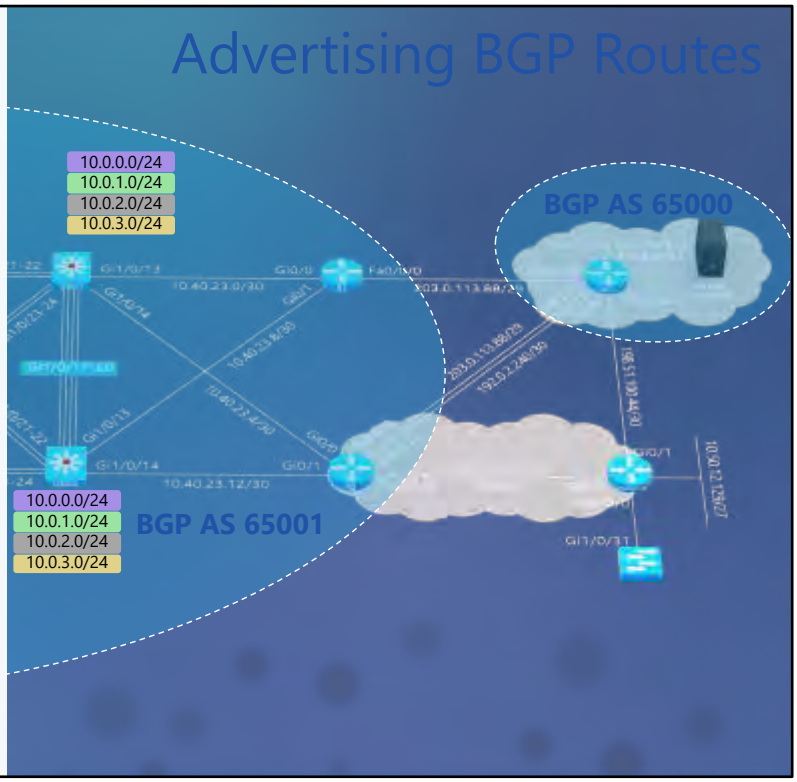
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

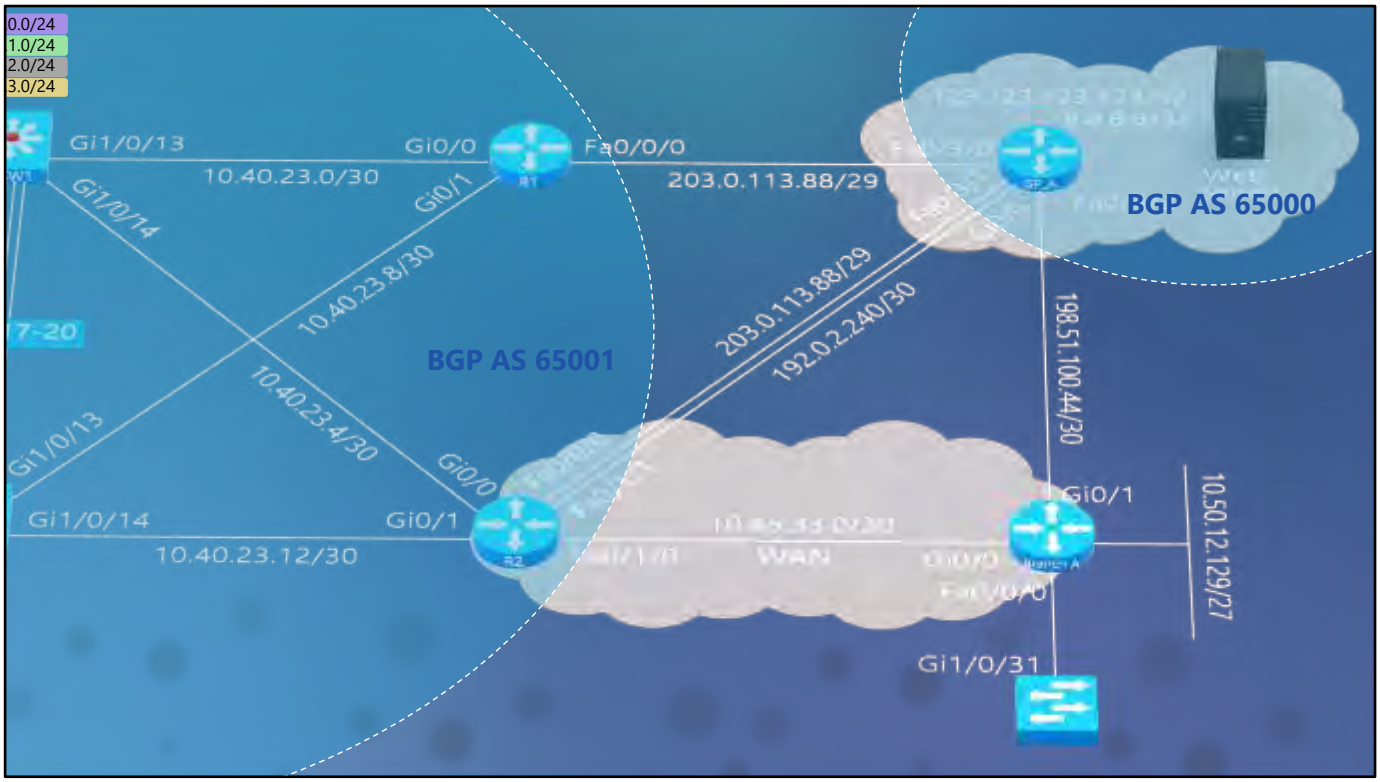
Advertising BGP Routes

Up until this point the "**network**" command had a completely different use

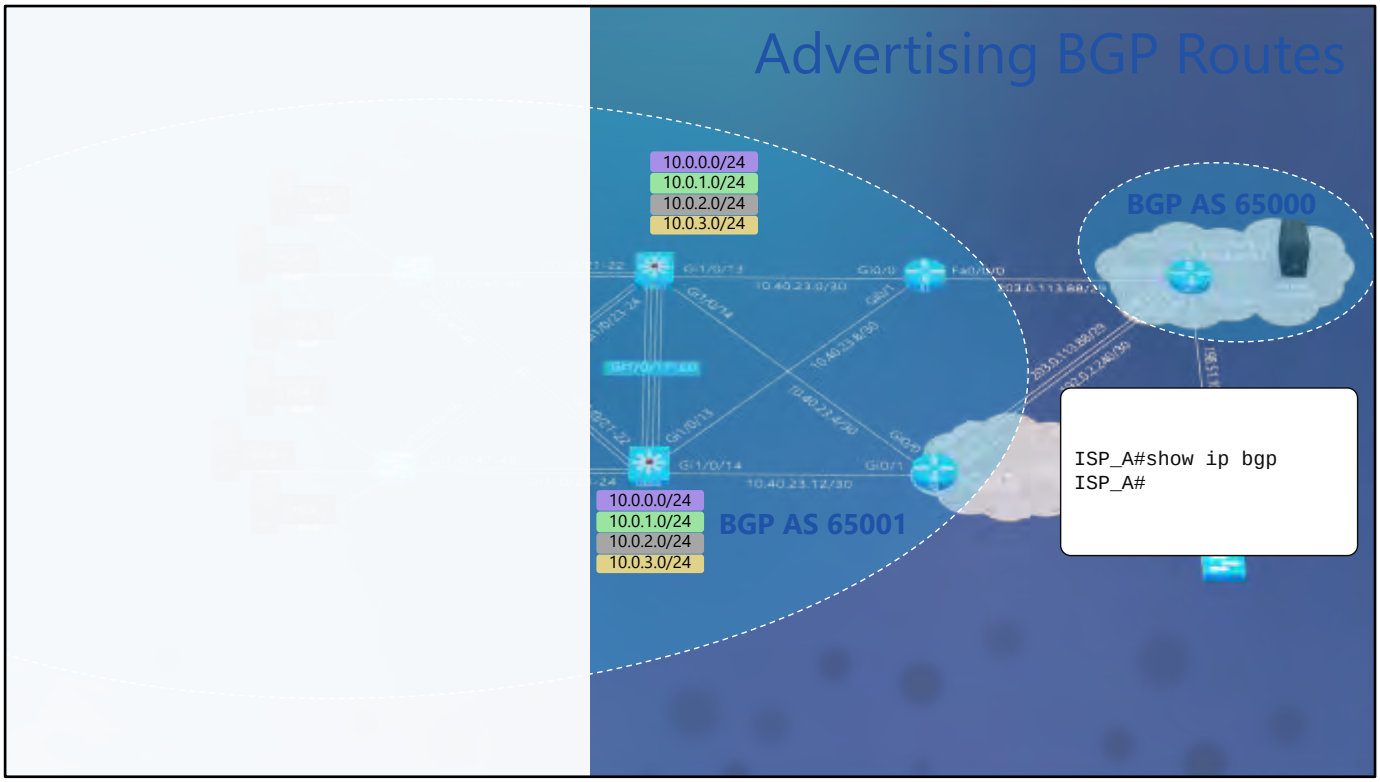
- The **network** command allows you to advertise a prefix to your neighbor
- You must be **exact** with matching on prefix
- If not found in the **routing table**, it will not be advertised



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

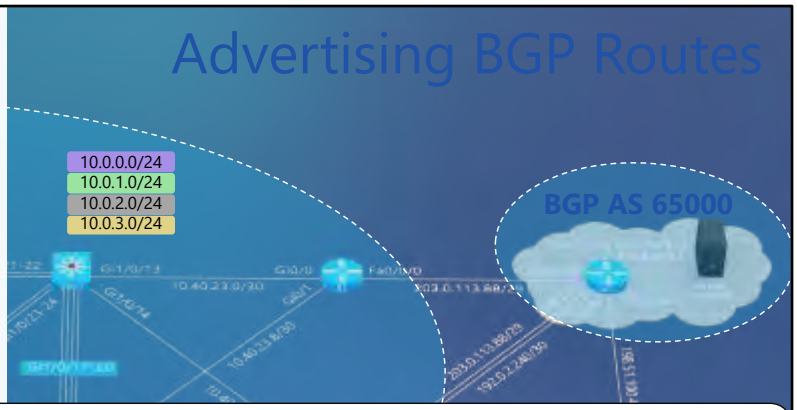


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

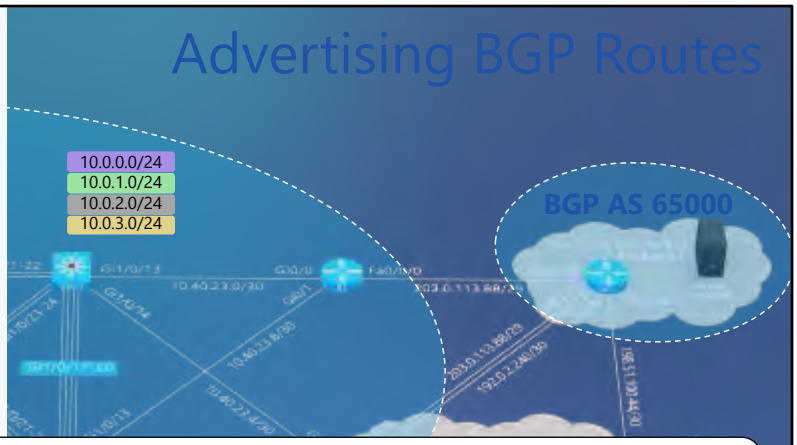
Advertising BGP Routes




```
ISP_A#show ip route
…output omitted…

      8.0.0.0/32 is subnetted, 1 subnets
C        8.8.8.8 is directly connected, Loopback8
      123.0.0.0/32 is subnetted, 1 subnets
C        123.123.123.123 is directly connected, Loopback123
      192.0.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.0.2.240/30 is directly connected, GigabitEthernet0/0
…output omitted…
ISP_A#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ISP_A(config)#router bgp 65000
ISP_A(config-router)#network 8.8.8.8 mask 255.255.255.255
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Advertising BGP Routes

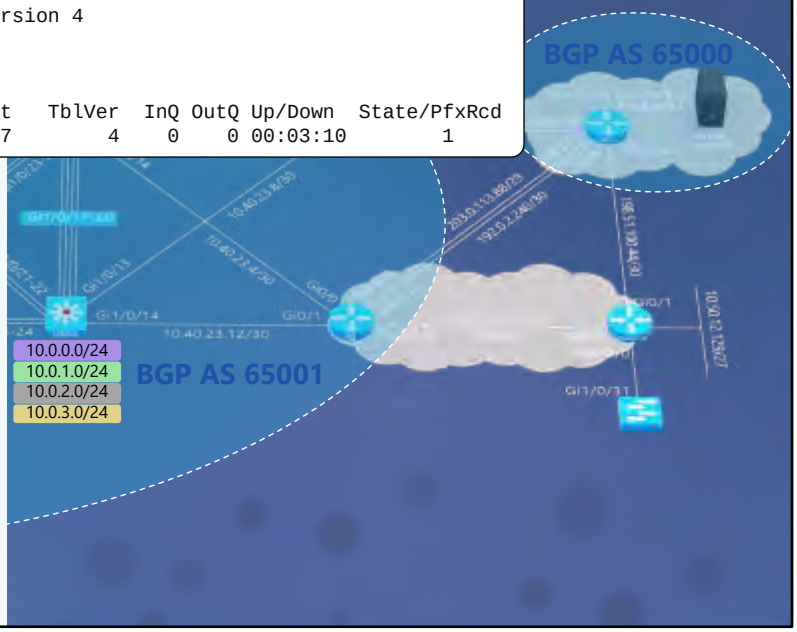



```
ISP_A#show ip bgp
BGP table version is 2, local router ID is 123.123.123.123
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   8.8.8.8/32       0.0.0.0                  0         32768 i
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Advertising BGP Routes

```
R2#show ip bgp summary
BGP router identifier 10.2.2.2, local AS number 65001
BGP table version is 4, main routing table version 4
1 network entries using 144 bytes of memory
…output omitted…

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
203.0.113.89    4        65000       9       7        4    0    0 00:03:10        1
```

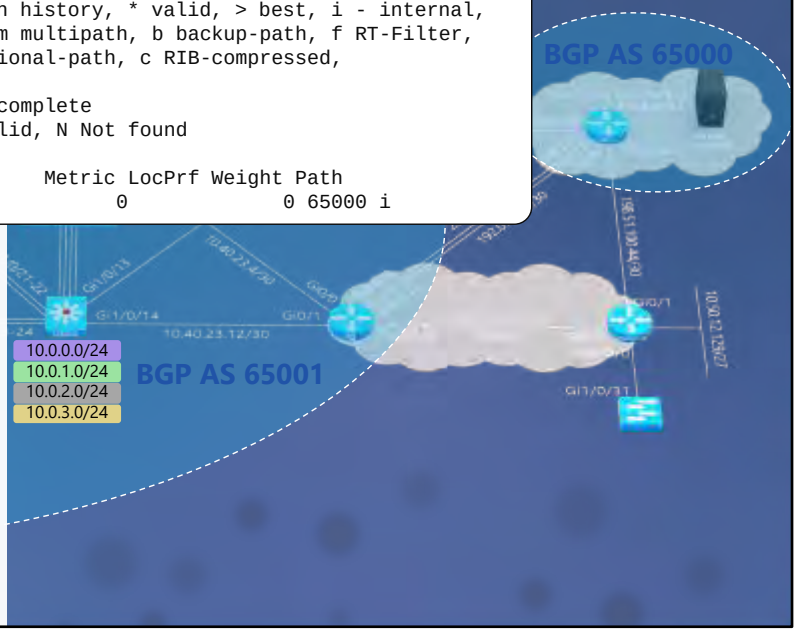


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Advertising BGP Routes

```
R2#show ip bgp
BGP table version is 4, local router ID is 10.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 *>   8.8.8.8/32       203.0.113.89             0             0 65000 i
```

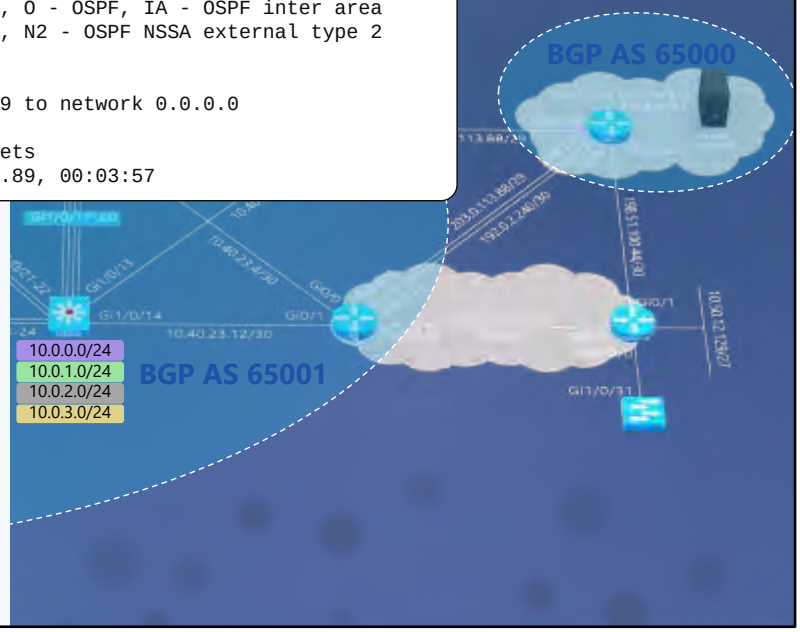


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Advertising BGP Routes

```
R2#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
…output omitted…

Gateway of last resort is 203.0.113.89 to network 0.0.0.0

      8.0.0.0/32 is subnetted, 1 subnets
B        8.8.8.8 [20/0] via 203.0.113.89, 00:03:57
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

BGP Messages

Open

Used to establish peering by exchanging basic parameters such as AS number and authentication values

Keepalive

Sent periodically to maintain peering

Update

Used to exchange path attributes and prefixes when adding and withdrawing routes

Notification

Signals BGP issues and errors, typically causes BGP peering to reset

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

BGP States

Idle

BGP process is waiting for next attempt to establish a peering

Connect

TCP Connection being established

Active

TCP Connection was not successful, a second attempt is made, if successful Open msg is sent, if not return to Idle state

Open Sent

BGP Open messages are being sent

Open confirm

BGP Open messages have been successfully sent and received

Established

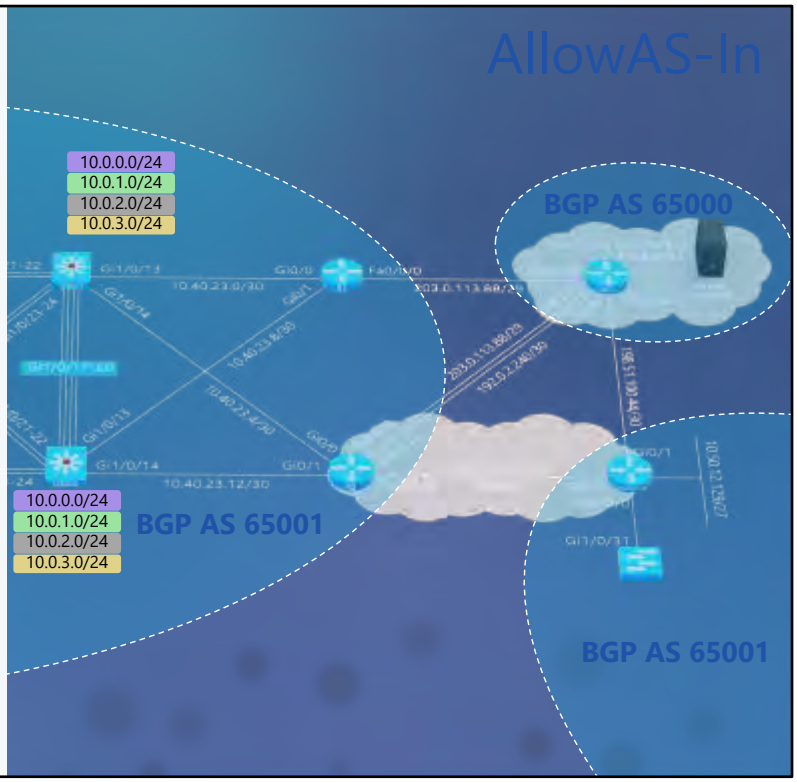
Neighbor details match, peering is successful, Update messages can be exchanged

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AllowAS-In

Allows you to receive and keep routes even if your AS number is already in the AS path.

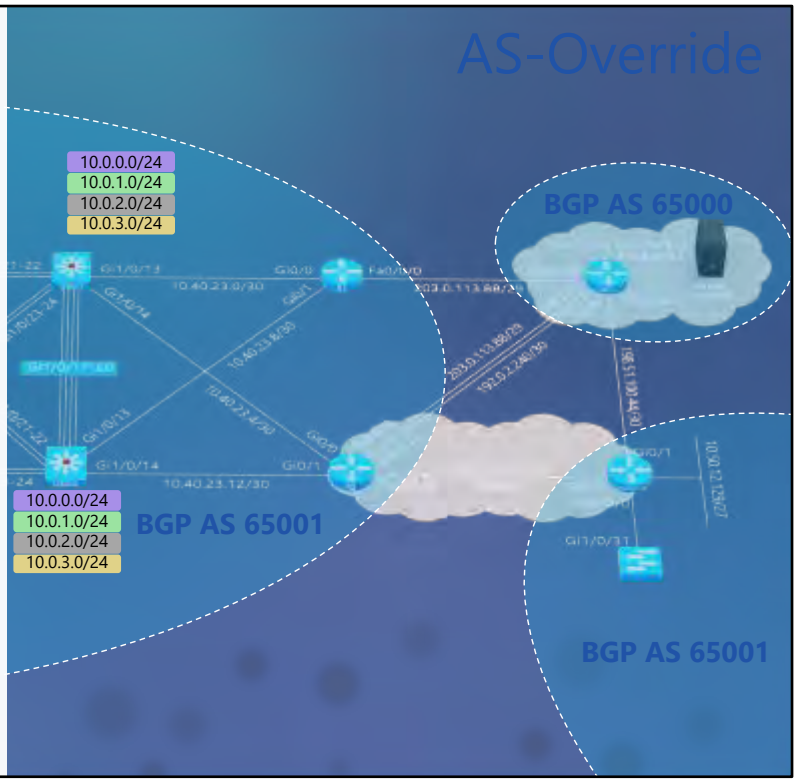


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AS-Override

Allows you to remove an AS number and replace it with your own AS number.

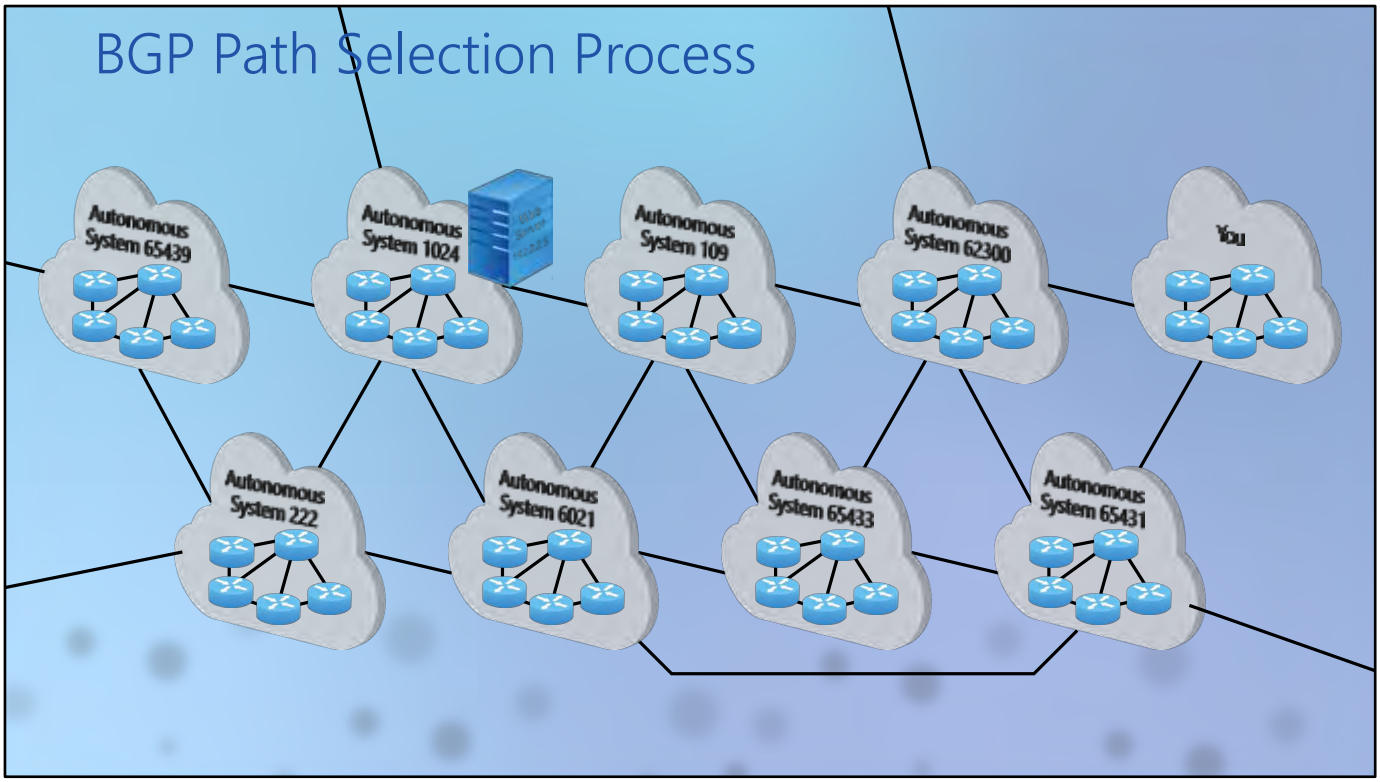


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

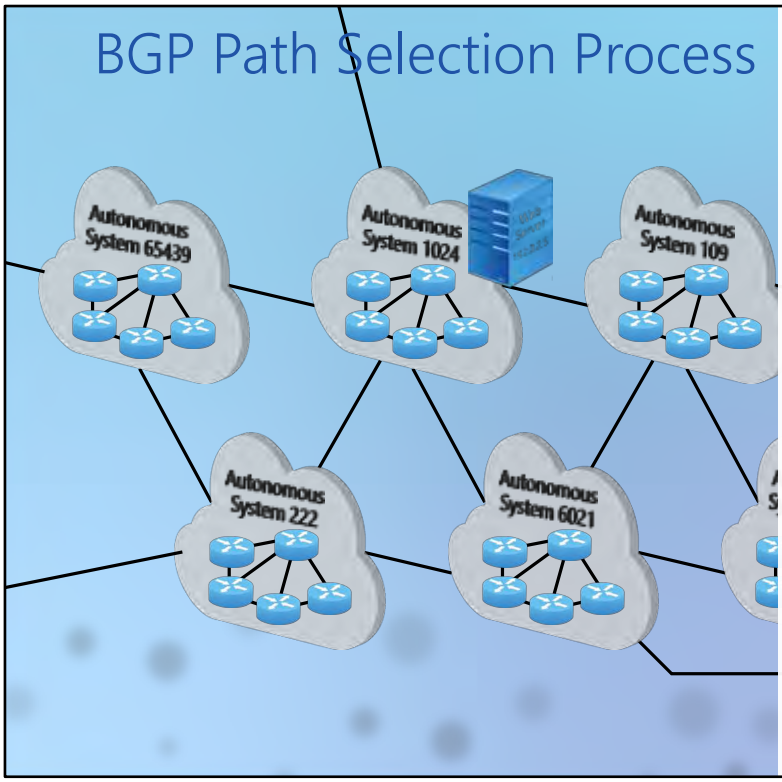
BGP Best Path Selection Process

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

BGP Path Selection Process

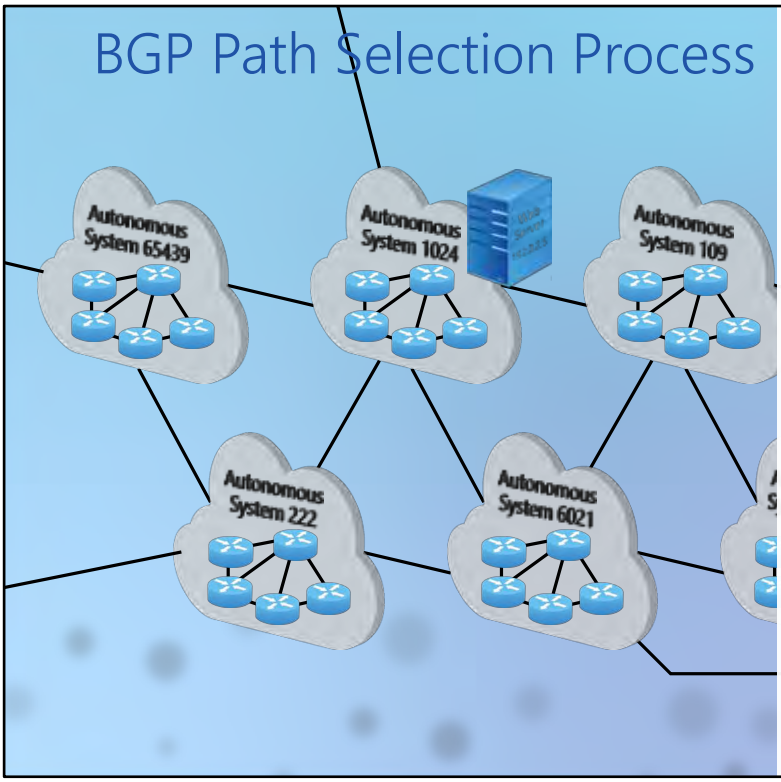


Since BGP routers receive information about each prefix from multiple peers, this leads to multiple paths being available for the same destination.

The BGP best path algorithm is used to determine the single best path to use.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

BGP Path Selection Process



Ignore paths that

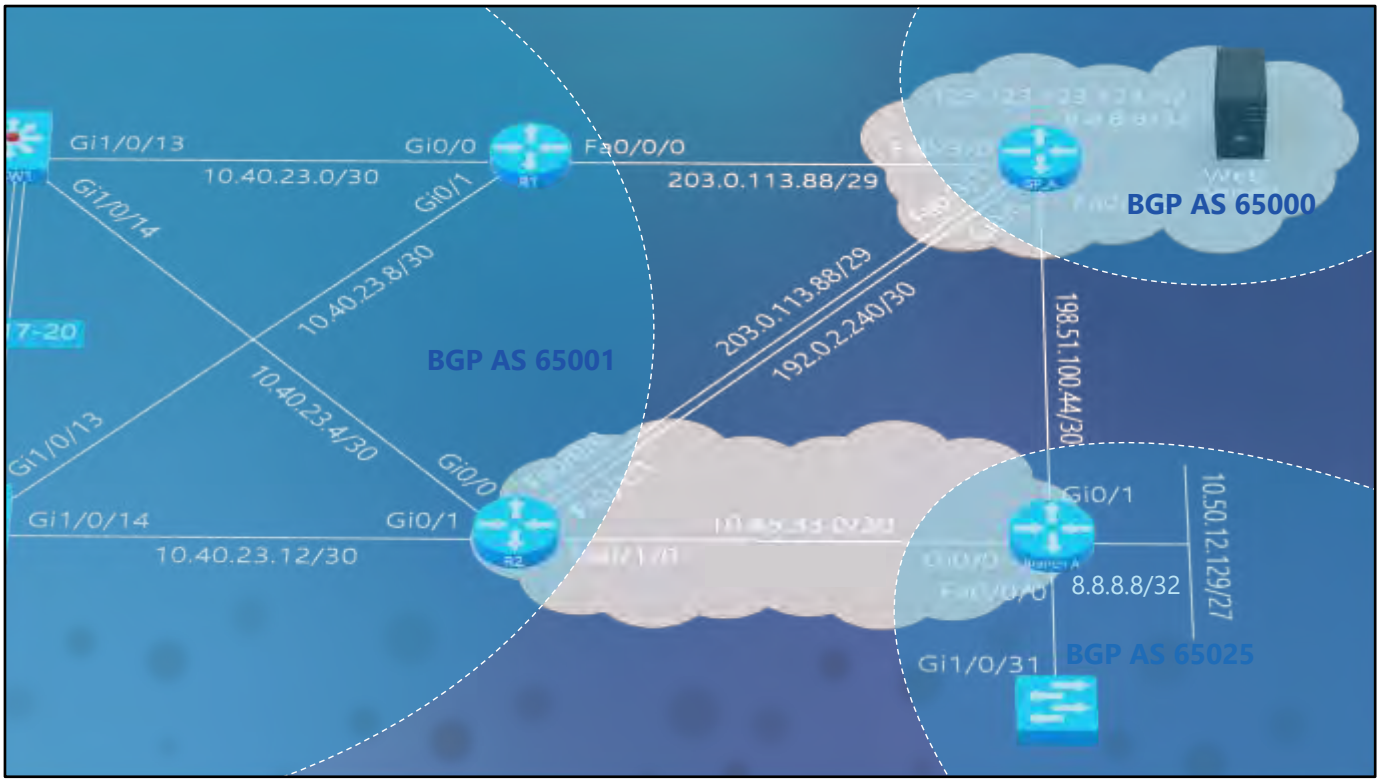
- Have a next hop IP address that is not reachable
- Have a path that contains your own local AS number

1. Prefer the path with the highest **WEIGHT**.
2. Prefer the path with the highest **LOCAL_PREF**.
3. Prefer the path what was locally **ORIGINATED**.
4. Prefer the path with the shortest **AS_PATH**.
5. Prefer the path with the lowest **ORIGIN type**.
6. Prefer the path with the lowest **Multi-exit discriminator (MED)**
7. Prefer eBGP over iBGP paths.
8. Prefer the path with the lowest IGP metric to the BGP next hop.
9. Prefer the older path.
10. Prefer the path with the peering router that has the lower router ID.
11. Prefer the path with the peer who has the lower neighbor address.

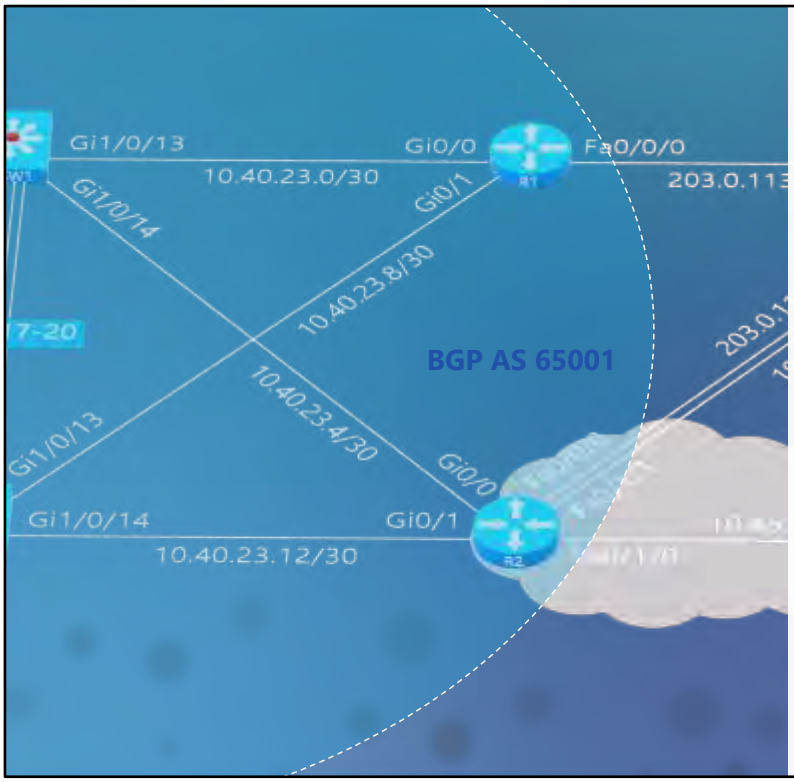
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manipulating BGP Best Path Selection Process

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Ignore paths that

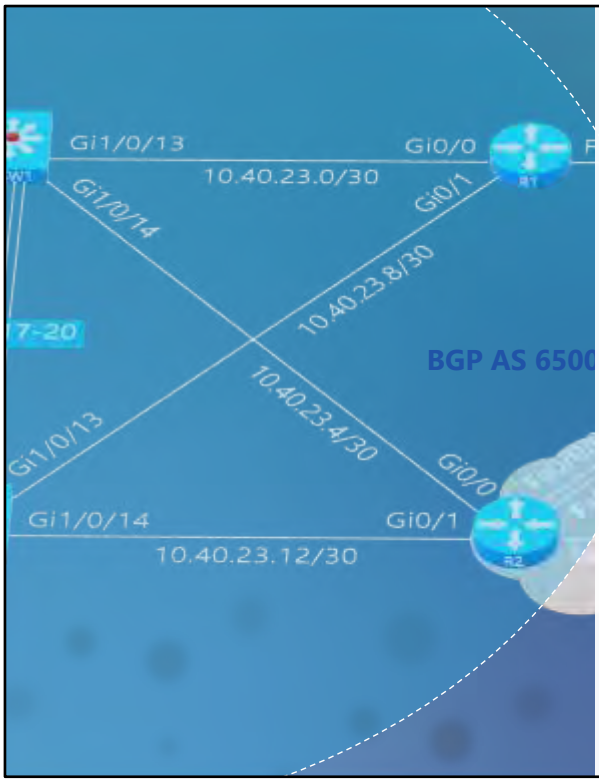
Have a next hop IP address that is not reachable

Have a path that contains your own local AS number

1. Prefer the path with the highest **WEIGHT**.
2. Prefer the path with the highest **LOCAL_PREF**.
3. Prefer the path what was locally **ORIGINATED**.
4. Prefer the path with the shortest **AS_PATH**.
5. Prefer the path with the lowest **ORIGIN type**.
6. Prefer the path with the lowest **Multi-exit discriminator (MED)**
7. Prefer eBGP over iBGP paths.
8. Prefer the path with the lowest IGP metric to the BGP next hop.
9. Prefer the older path.
10. Prefer the path with the peering router that has the lower router ID.
11. Prefer the path with the peer who has the lower neighbor address.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Ways to Influence Routes

- Weight
- Local preference
- AS Path Prepending
- MED

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Weight

Weight – Cisco Proprietary / Locally significant to the router

- Use it to influence path leaving AS when a router has dual connections
- Higher is better (default for learned is 0, for locally generated 32768)
- Can't be passed to a neighboring BGP router

Example configured without a Route Map:

```
router bgp 65124
 neighbor 203.0.113.1 weight 40
```

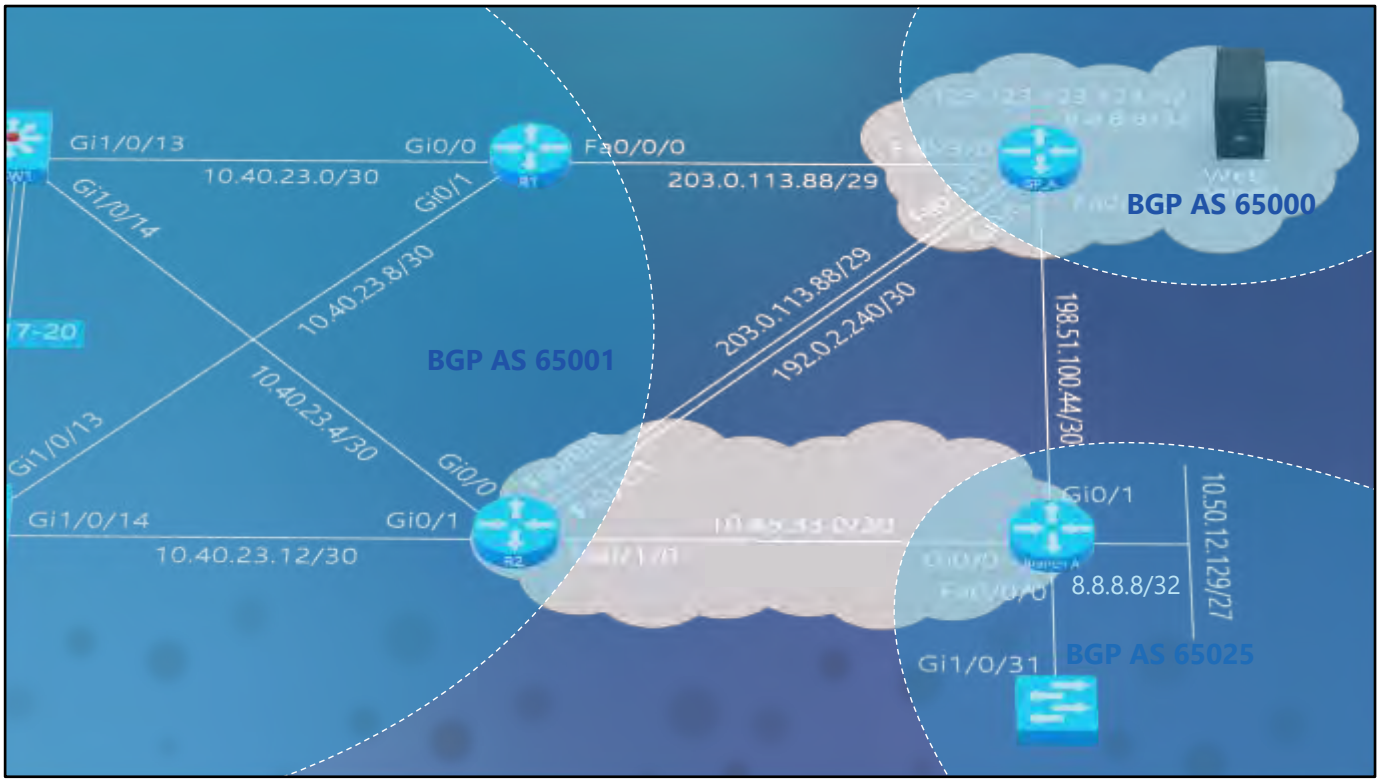
Example configured with Route Map:

```
ip prefix-list PL_WEIGHT seq 5 permit 192.0.2.0/24
route-map WEIGHT permit 10
 match ip address prefix-list PL_WEIGHT
 set weight 70
route-map WEIGHT permit 20
router bgp 65124
 neighbor 22.22.22.1 route-map WEIGHT in
```

Clearing a route to refresh new attributes:

```
clear ip bgp * in
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Local Preference

Local Preference – Passed to other routers in an AS

- Use it to influence path leaving AS when dual-homed.
- Force routers inside an AS to prefer one ISP over another.
- Default value is 100 and higher is better.
- Can be set as eBGP routes are learned.

Set local pref of all routes advertised to iBGP peers:

```
router bgp 65124
 bgp default local-preference 150
```

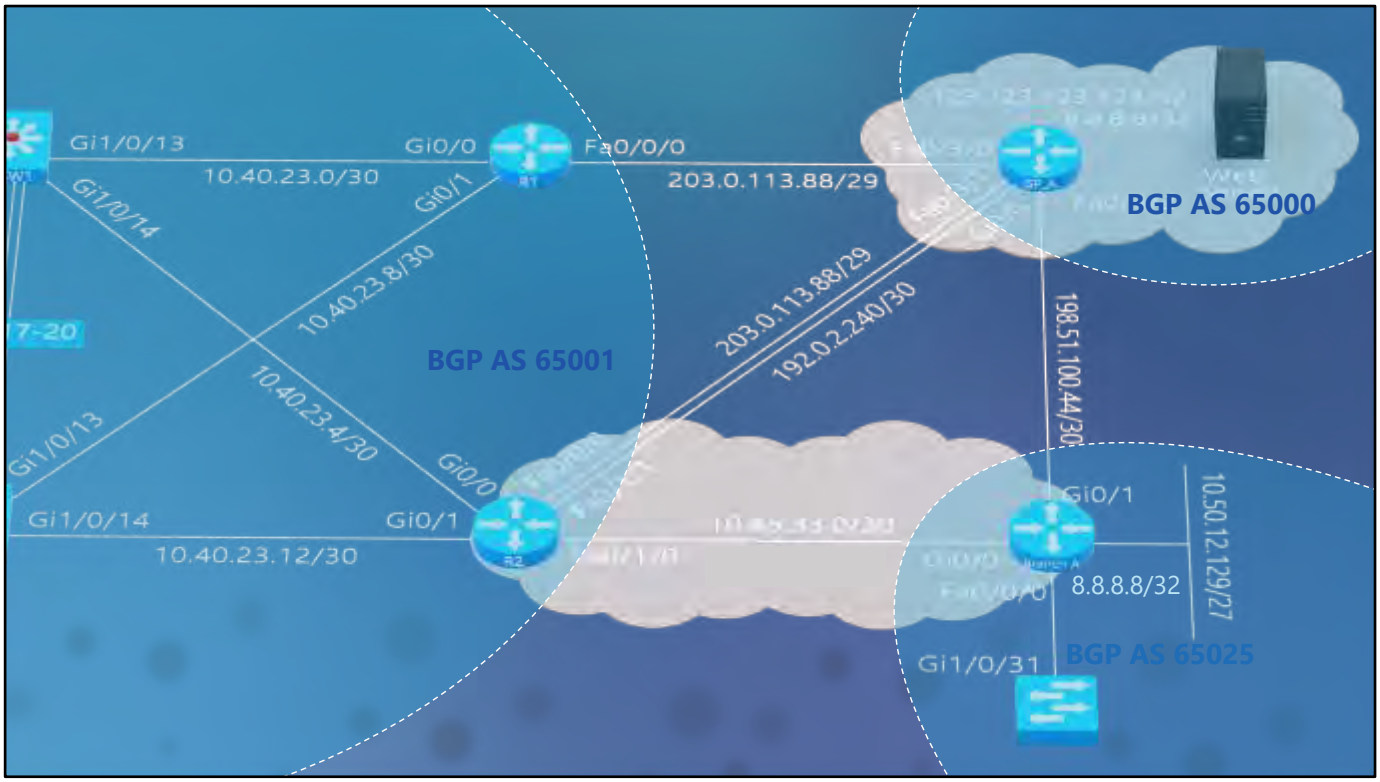
Example configured with a Route Map:

```
ip prefix-list PL_LP seq 5 permit 192.0.2.0/24
route-map LOCAL_PREF permit 10
 match ip address prefix-list PL_LP
 set local-preference 171
route-map LOCAL_PREF permit 20
router bgp 65124
 neighbor 22.22.22.1 route-map LOCAL_PREF in
```

Clearing a route to refresh new attributes:

```
clear ip bgp * in
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AS Path Prepend

AS Path Prepend – Passed to other routers in other AS

Use it to influence path to your AS when multiple AS peering's exist.

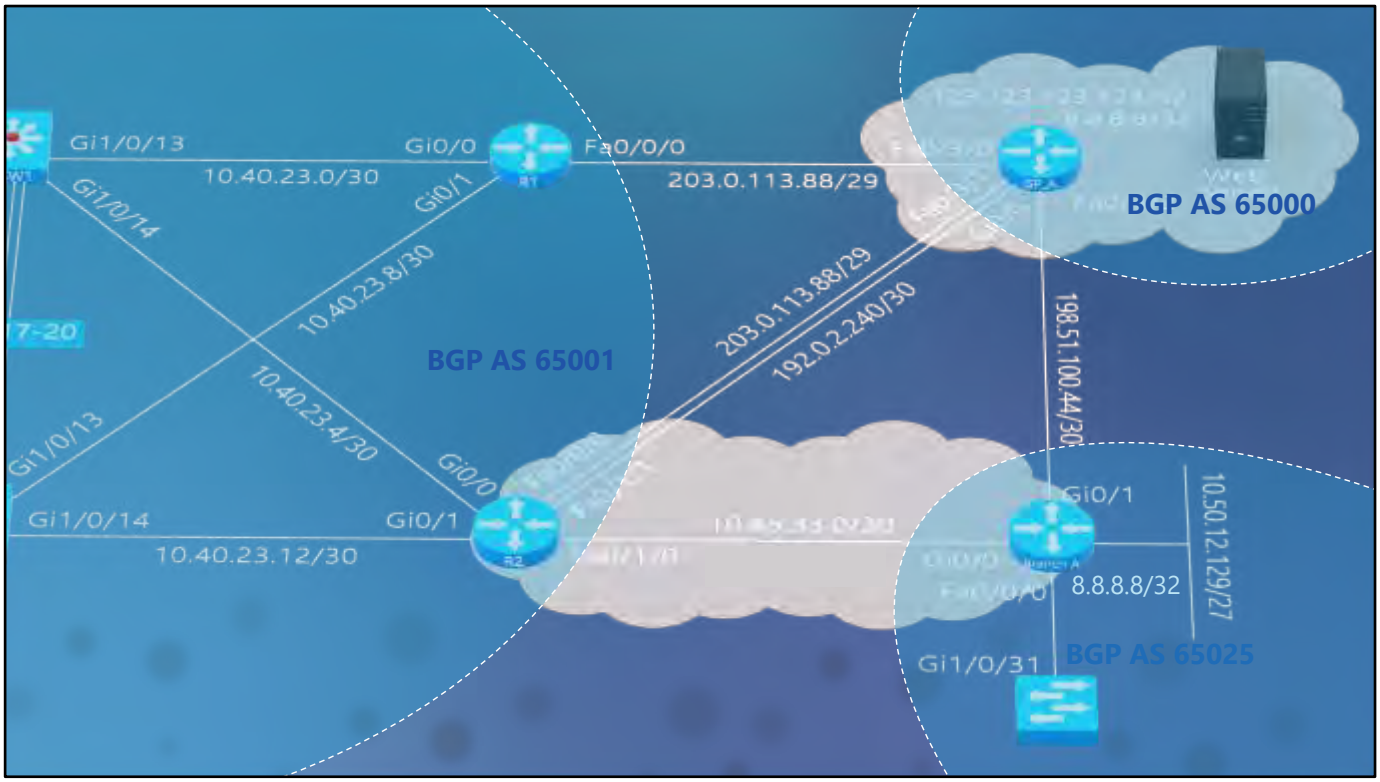
Manually configured to make return path less preferred by adding "additional hops"

Example configured with a Route Map:

```
ip prefix-list PL_ASPATH seq 5 permit 124.124.124.0/24
route-map ASPATH permit 10
 match ip address prefix-list PL_ASPATH
 set as-path prepend 65124 65124 65124 65124 65124
route-map ASPATH permit 20
router bgp
 neighbor 198.51.100.1 route-map AS_PATH out
 neighbor 203.0.113.1 route-map AS_PATH out
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multi-Exit Discriminator (MED)

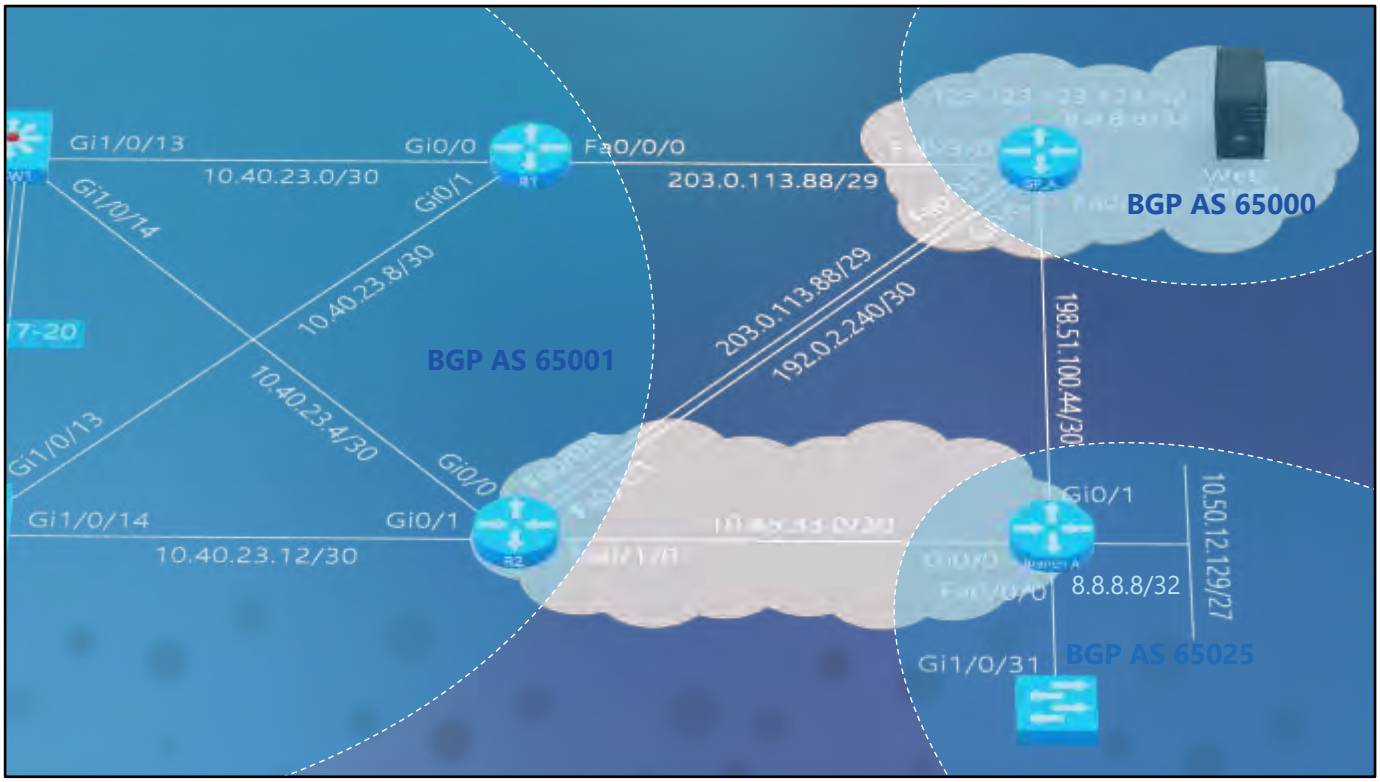
MED – Passed to other AS when you have dual homed connections.

- Tells the ISP a value to help determine which path should be preferred
- Lower is better or more preferred

Example configured with a Route Map:

```
route-map MED permit 10
 set metric 5
router bgp
  neighbor 203.0.113.1 route-map MED out
```

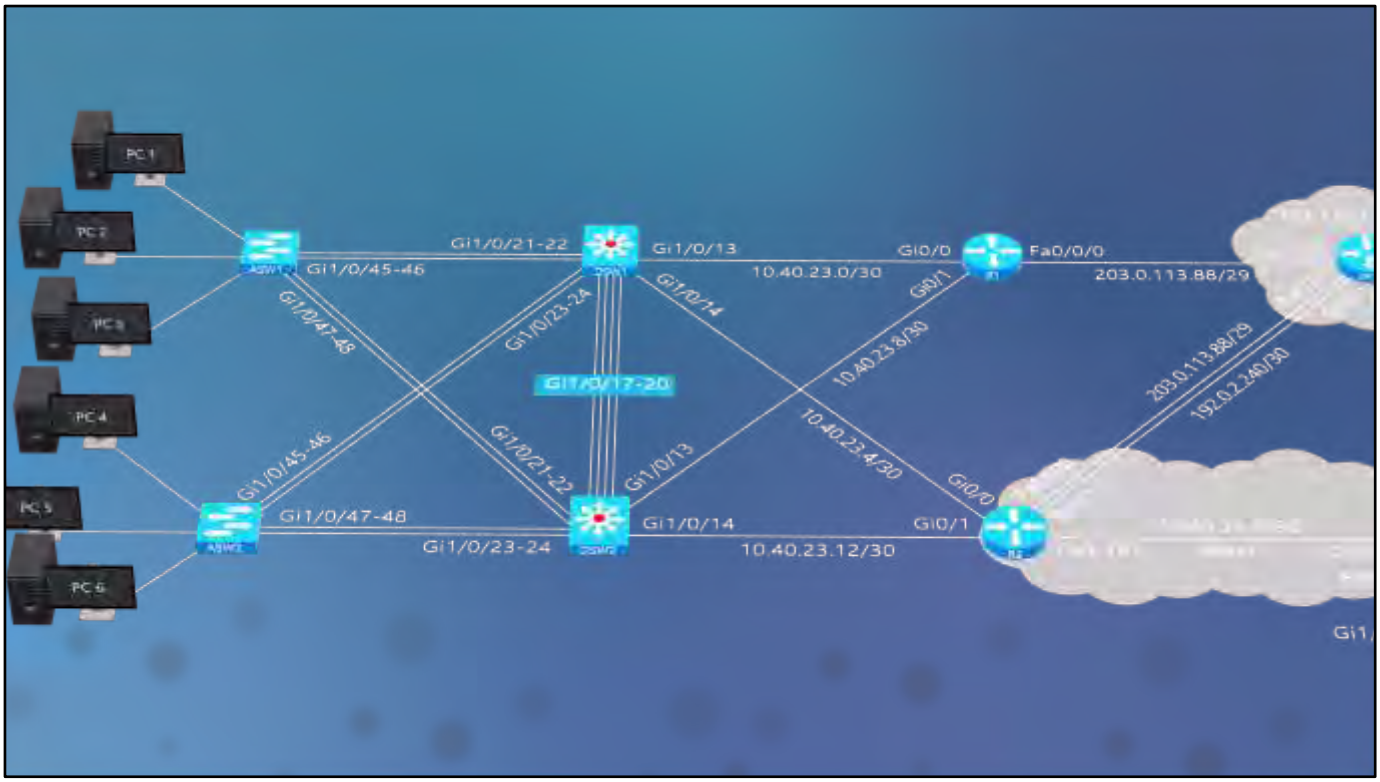
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Policy Based Routing (PBR)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Policy Based Routing (PBR)

A feature used to override the default forwarding decision:

- Default – forward based on destination IP address
- PBR – forward based on anything you want
  - source IP
  - port numbers
  - protocols
  - … and more
  - – mark packets for QoS purposes

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Policy Based Routing (PBR)

PBR creation:

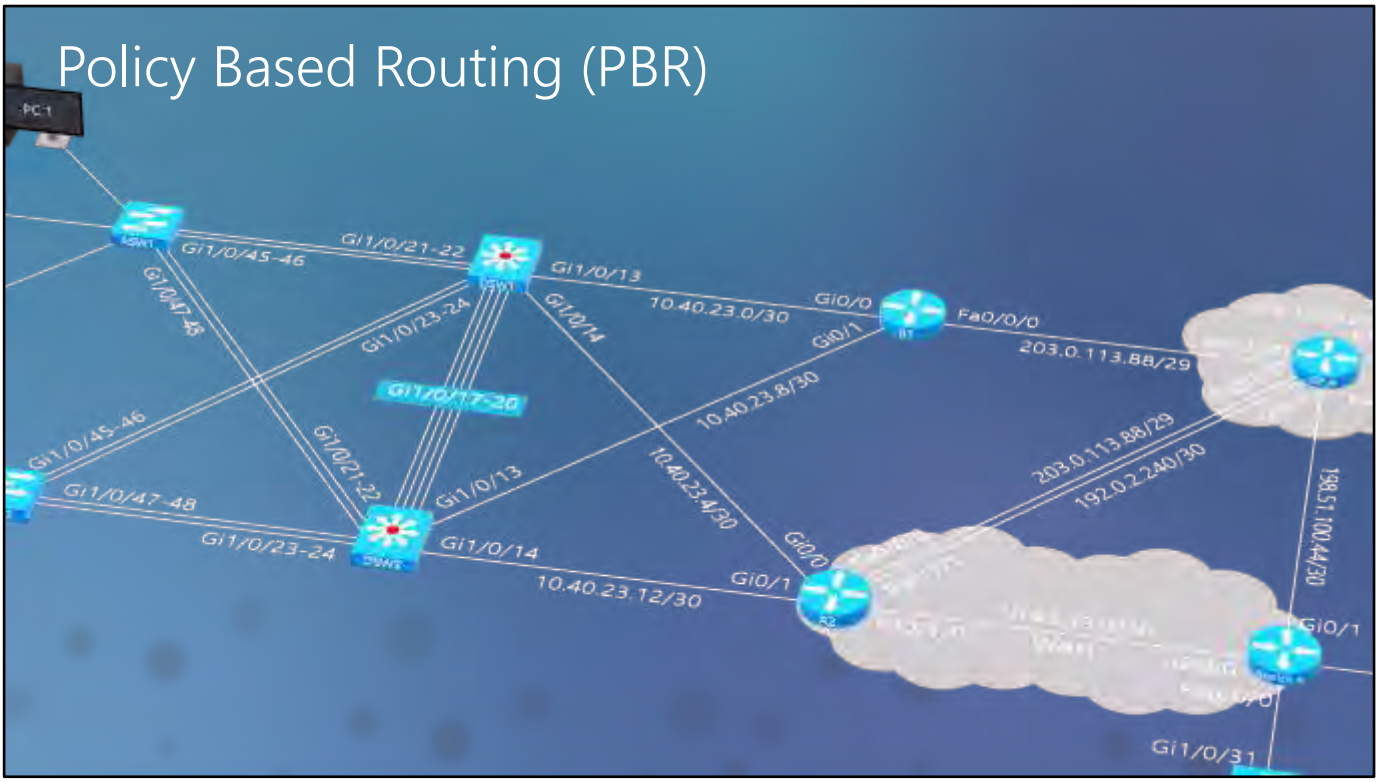
- ACLs – for identification purposes
- Route Maps – to define what happens
  - match
  - set

PBR applied:

- inbound interface – for arriving packets
  - R1(config-if)#ip policy route-map *route-map_name*
- control plane – for packets generated by router
  - R1(config-if)#ip local policy route-map *route-map_name*

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Policy Based Routing (PBR)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Policy Based Routing (PBR)

Default Keyword:

set ip next-hop *next_hop_ip*

vs

set ip default next-hop *next_hop_ip*

set interface *exit_interface*

vs

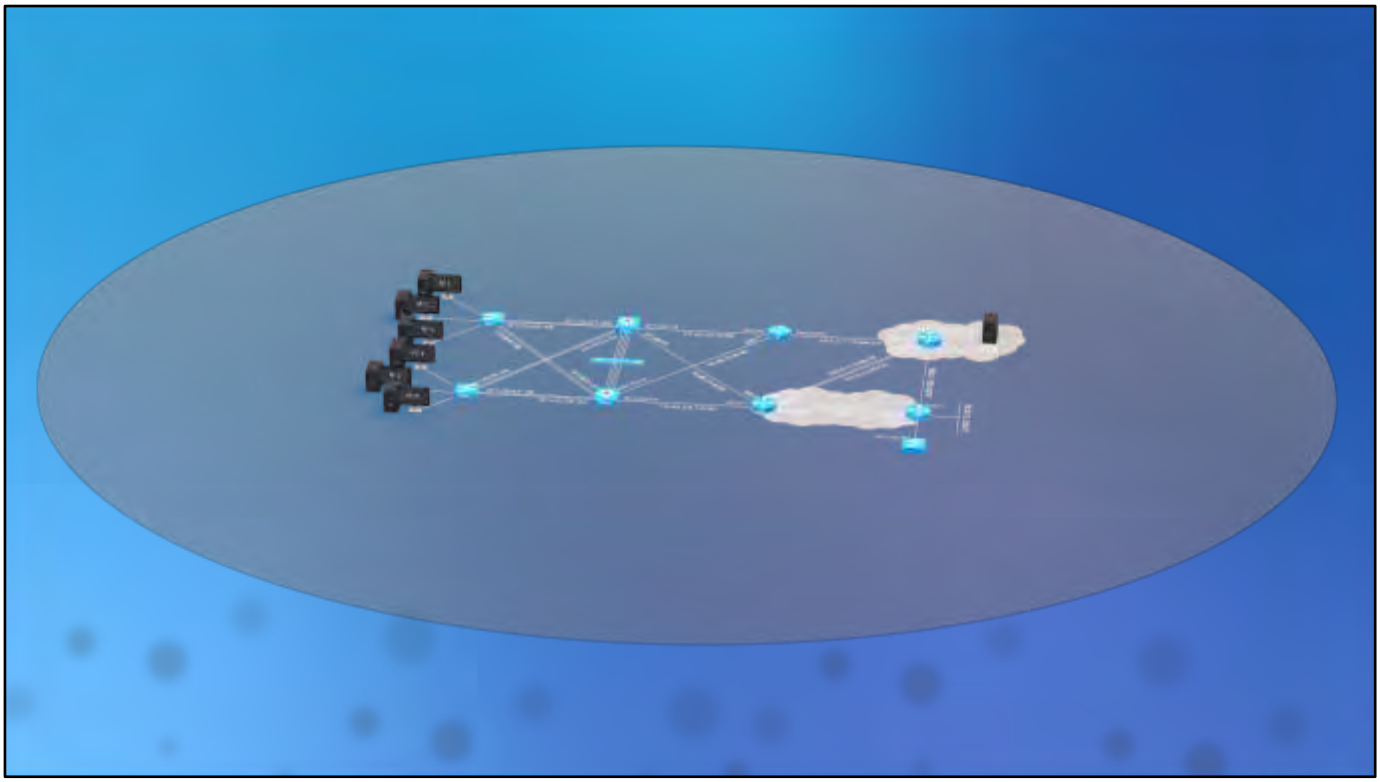
set default interface *exit_interface*

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

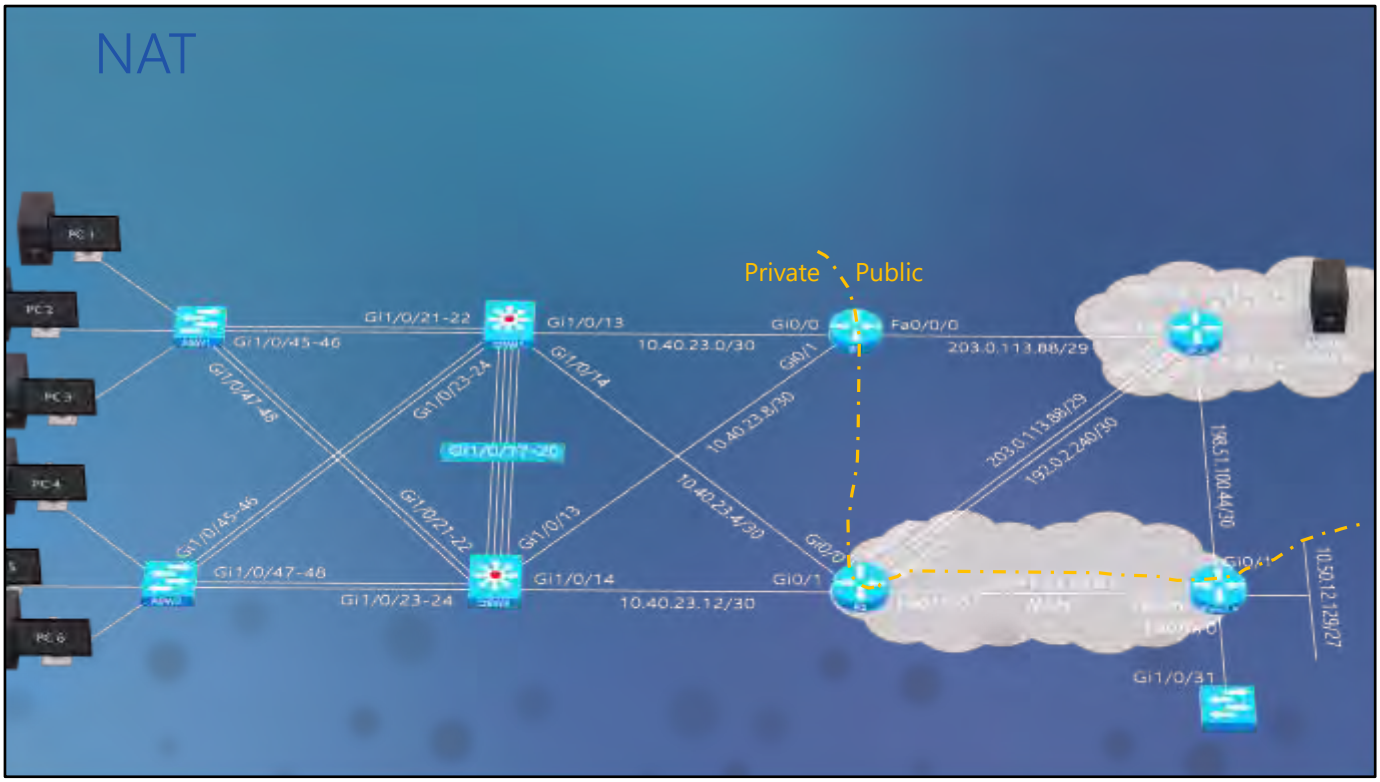
Network Address Translation (NAT)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

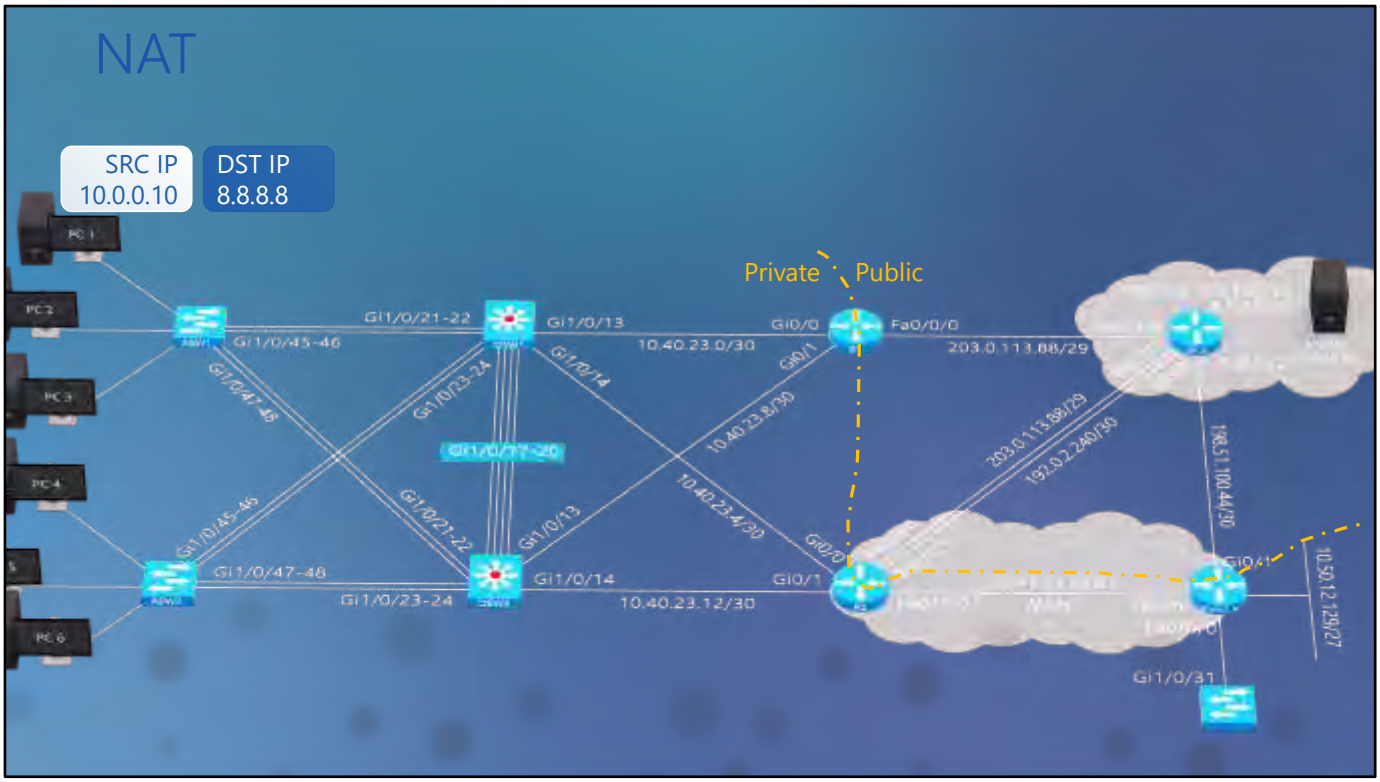


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

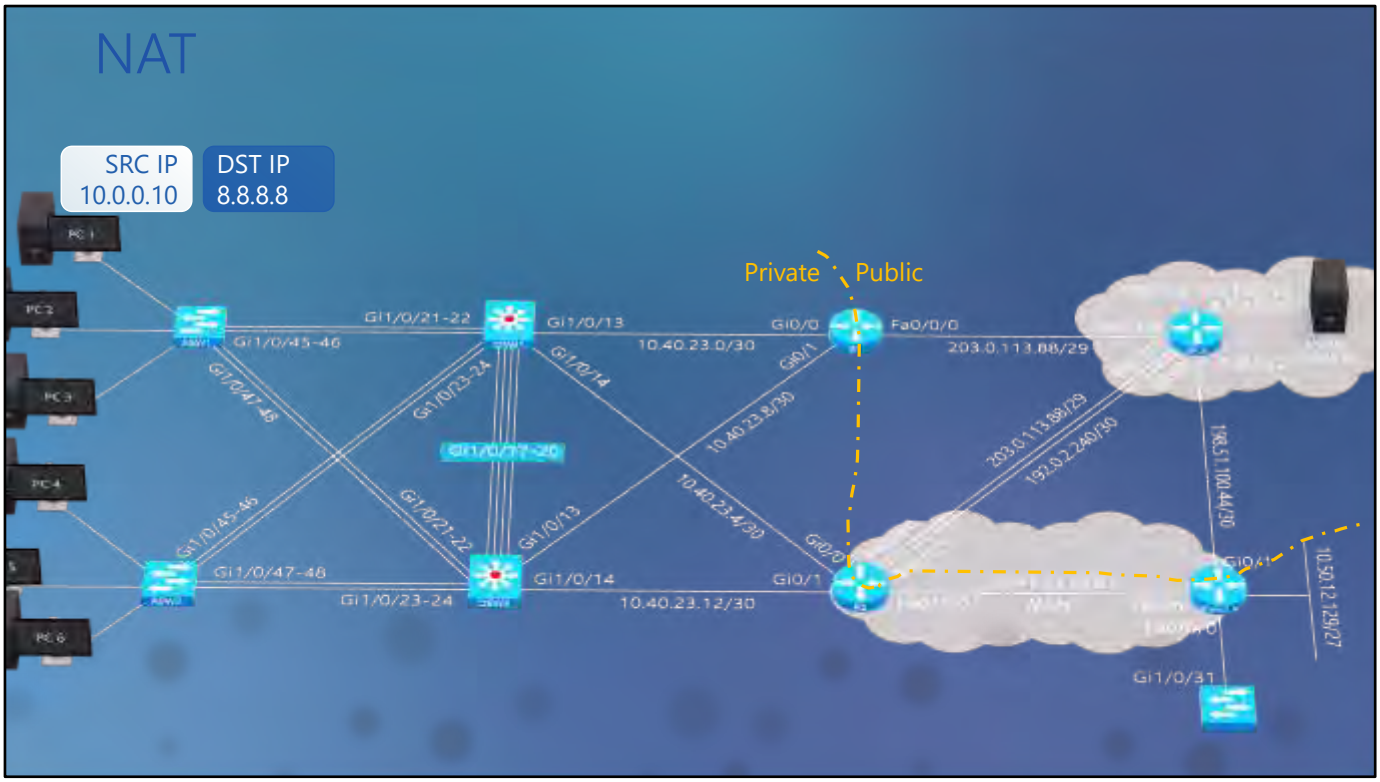
NAT



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



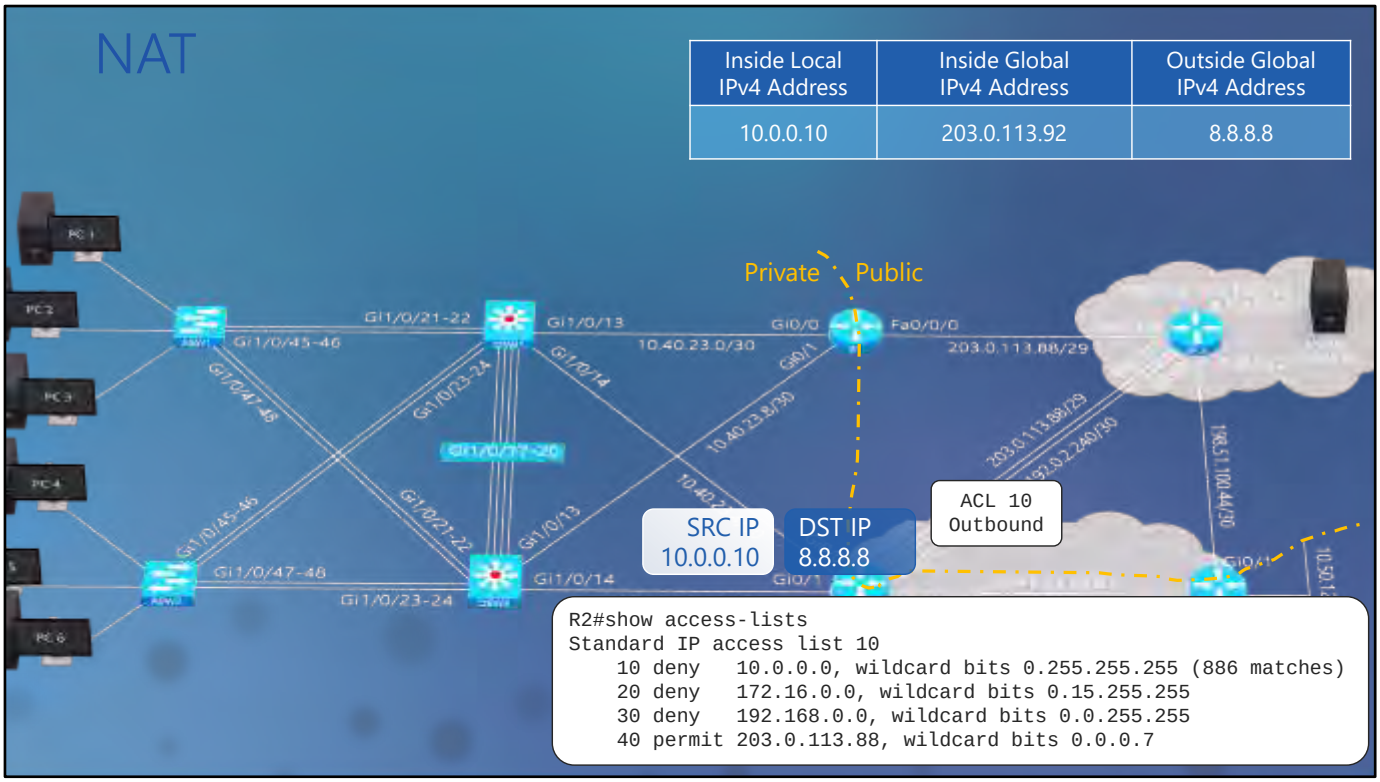
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NAT

Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
10.0.0.10	203.0.113.92	8.8.8.8

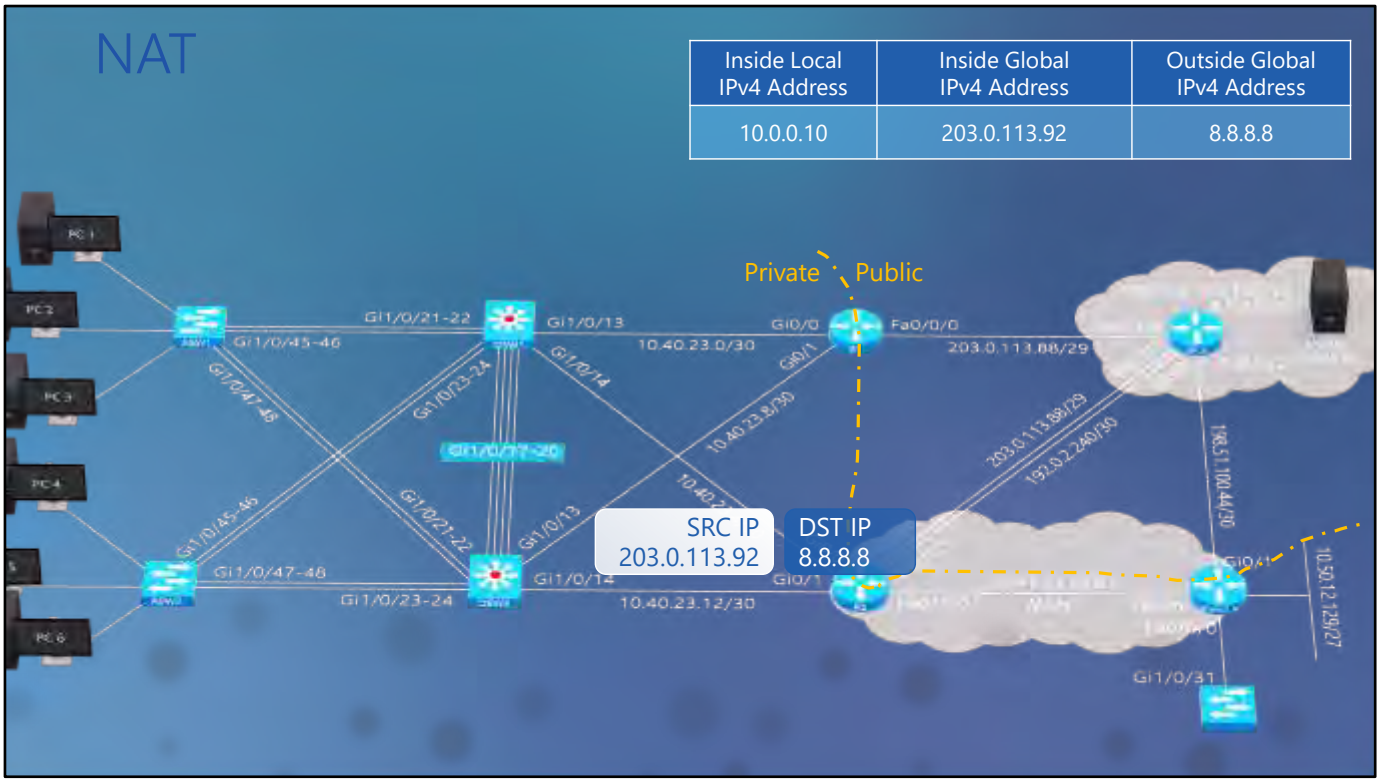



```
R2#show access-lists
Standard IP access list 10
    10 deny   10.0.0.0, wildcard bits 0.255.255.255 (886 matches)
    20 deny   172.16.0.0, wildcard bits 0.15.255.255
    30 deny   192.168.0.0, wildcard bits 0.0.255.255
    40 permit 203.0.113.88, wildcard bits 0.0.0.7
```

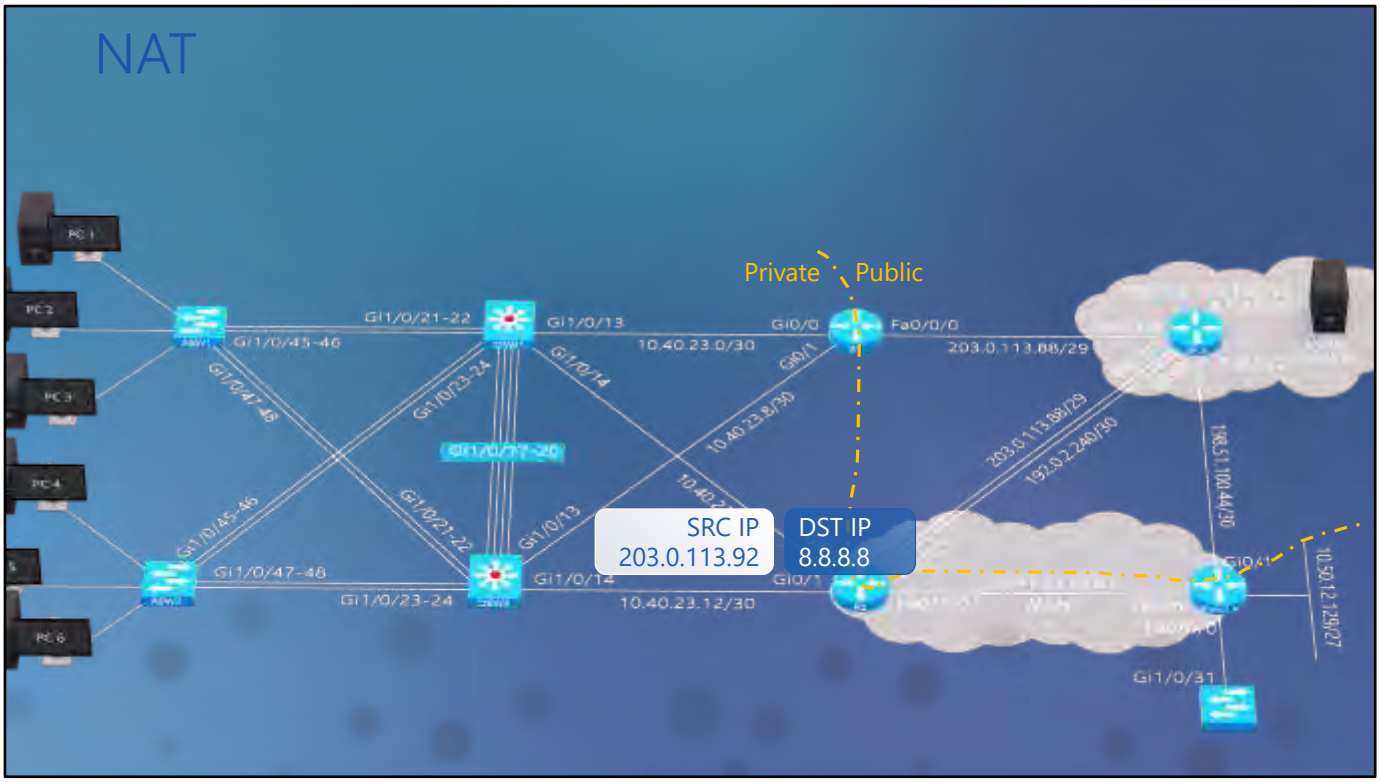
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NAT

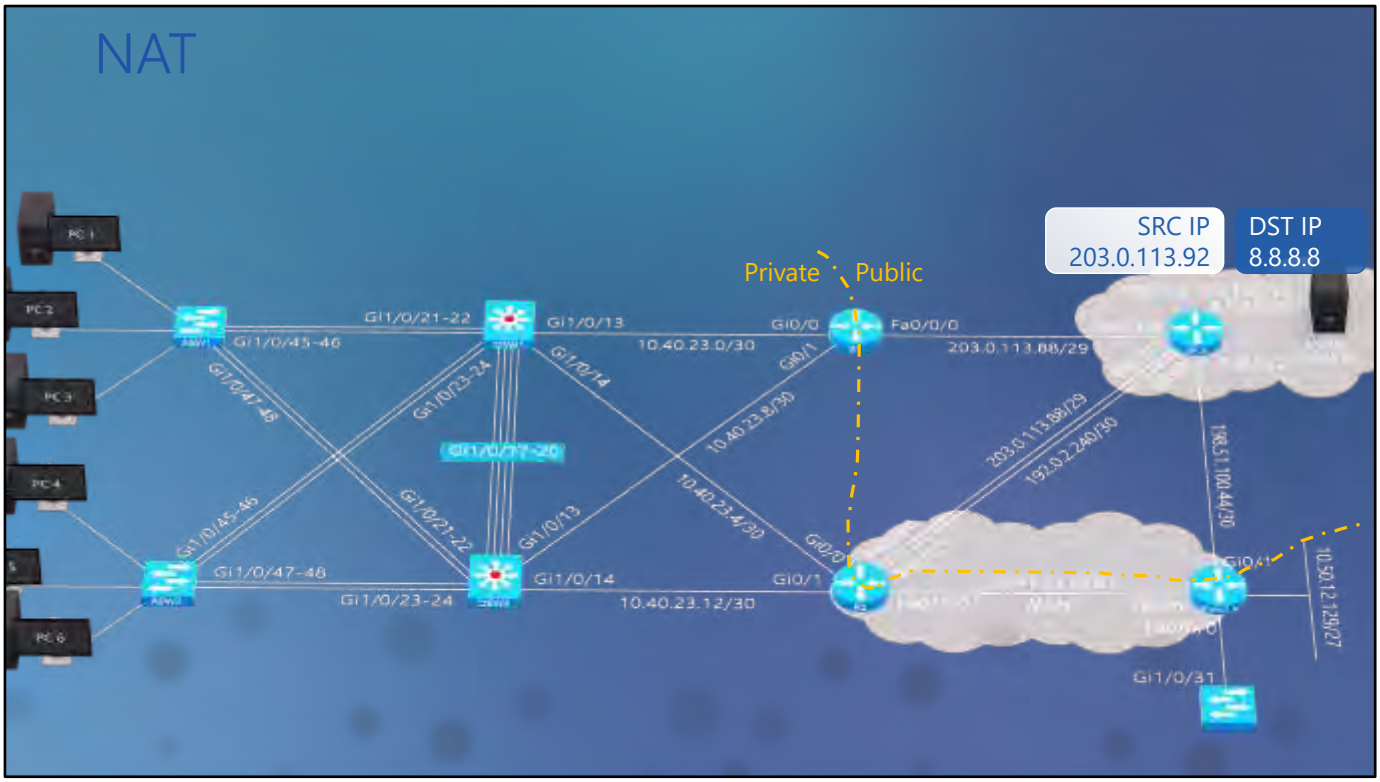
Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
10.0.0.10	203.0.113.92	8.8.8.8



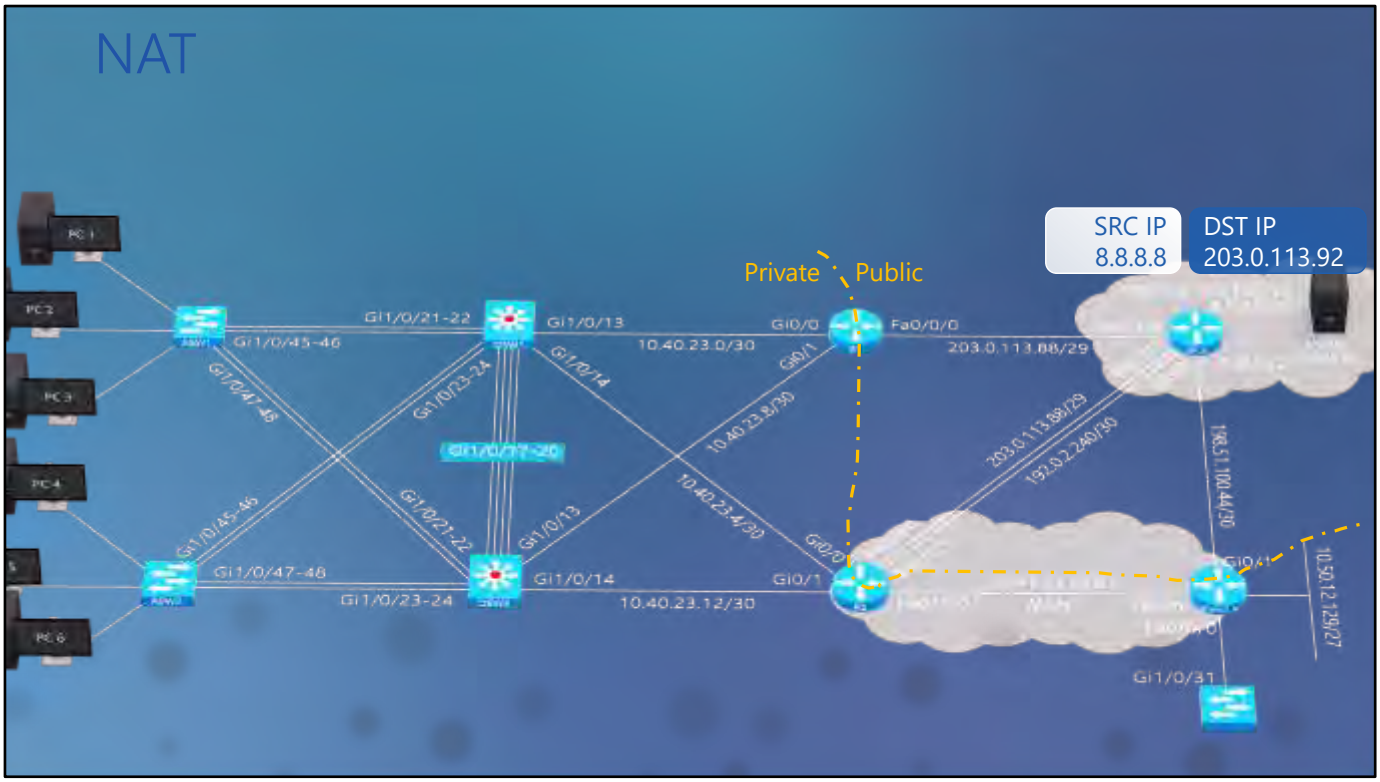
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



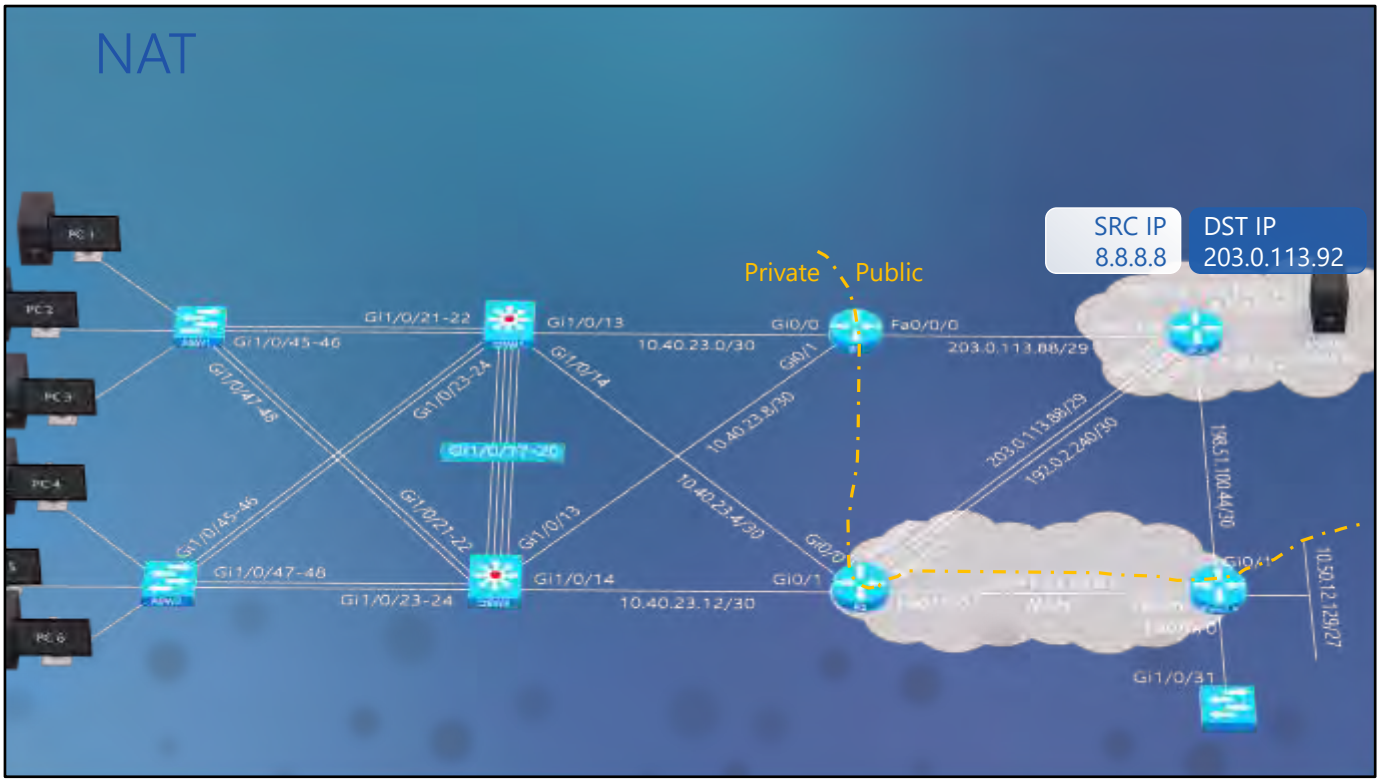
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



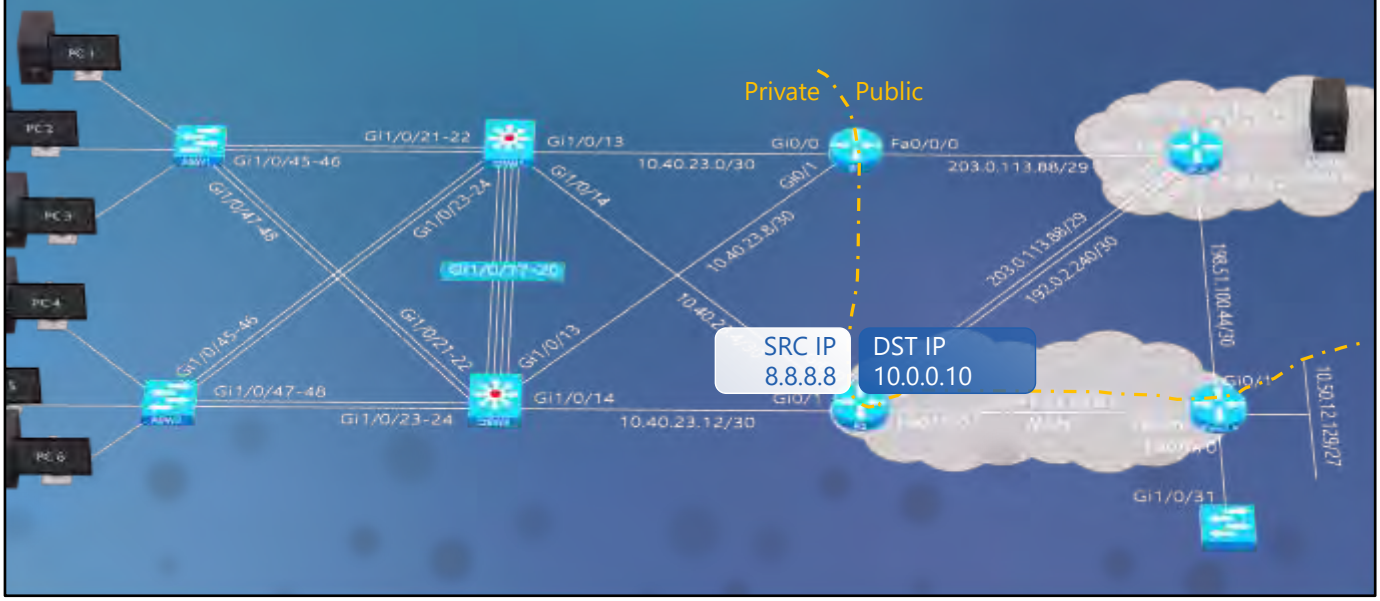
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



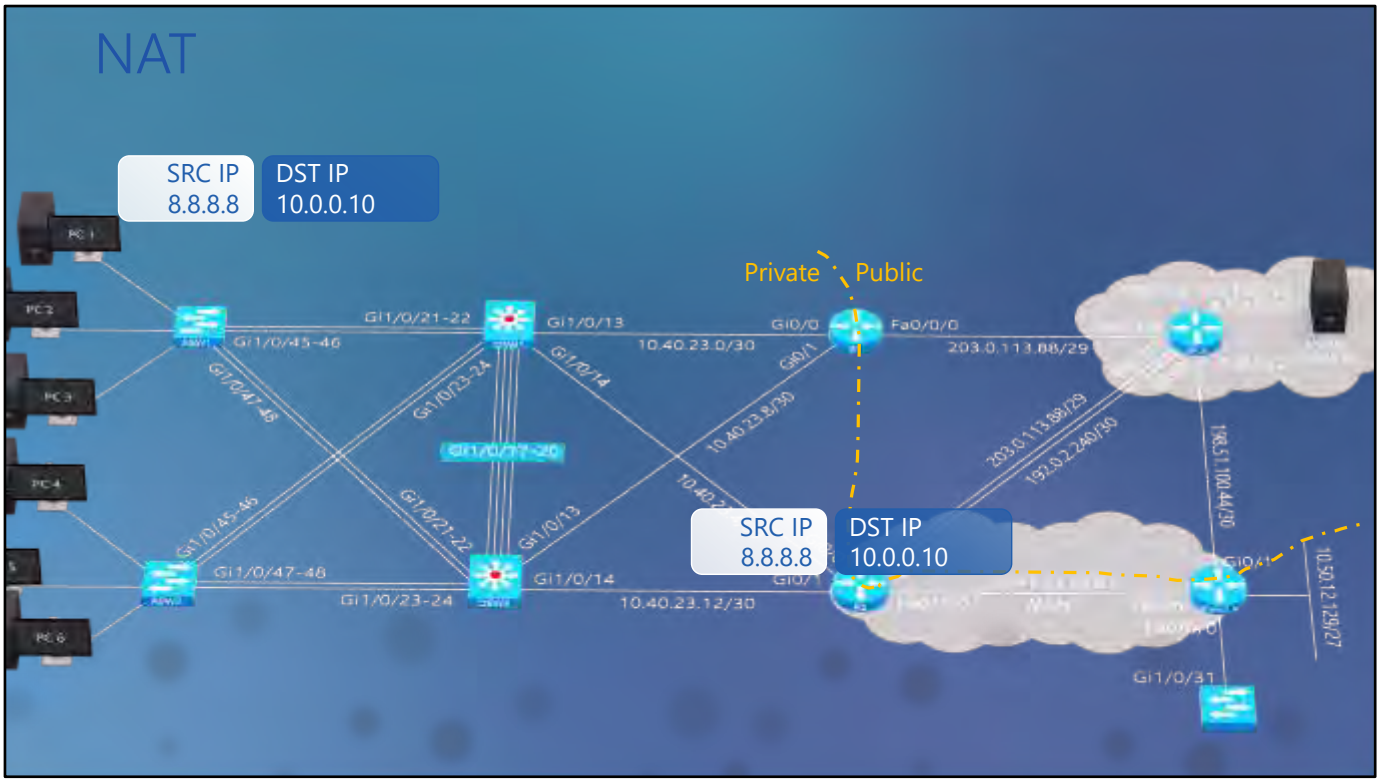
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NAT

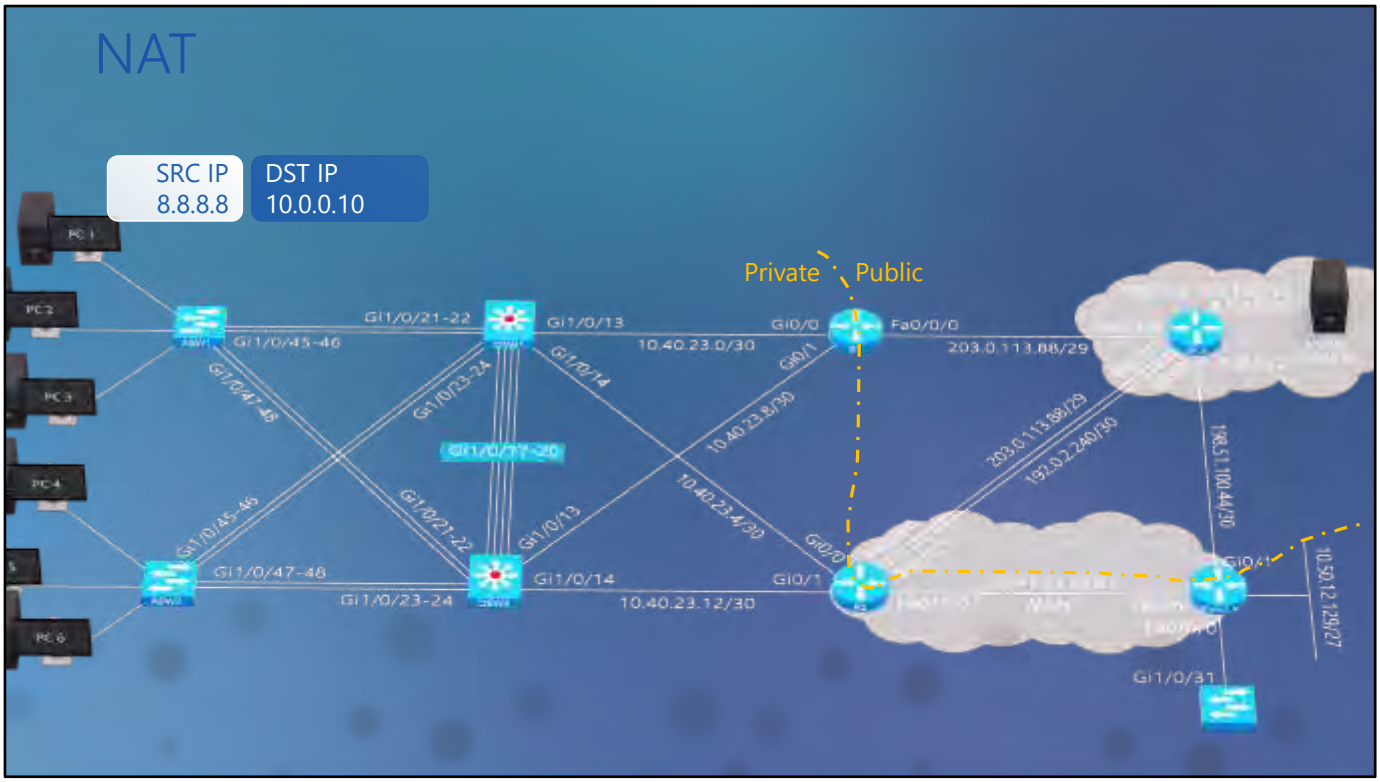
Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
10.0.0.10	203.0.113.92	8.8.8.8



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

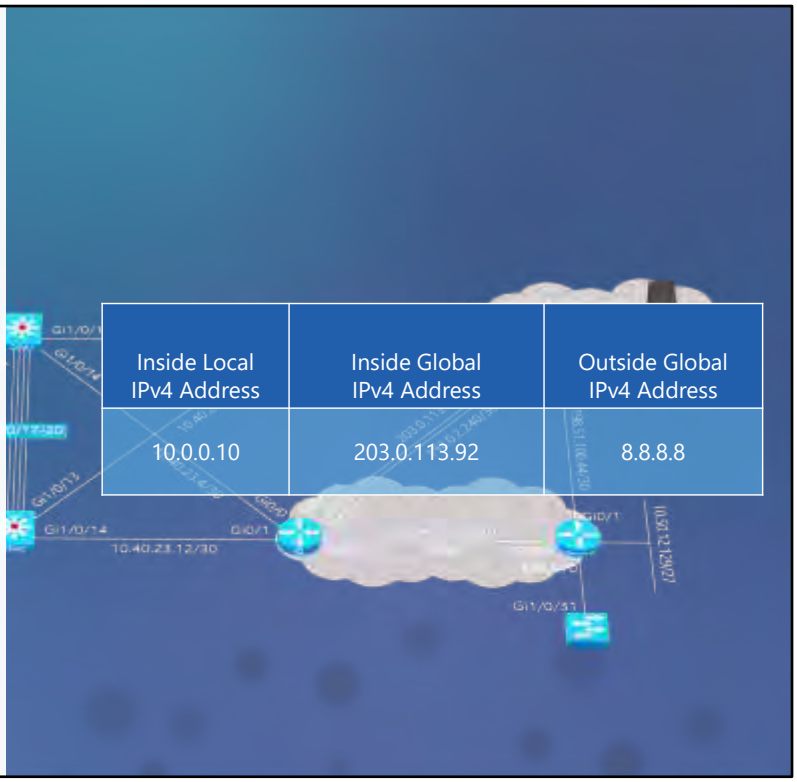


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NAT

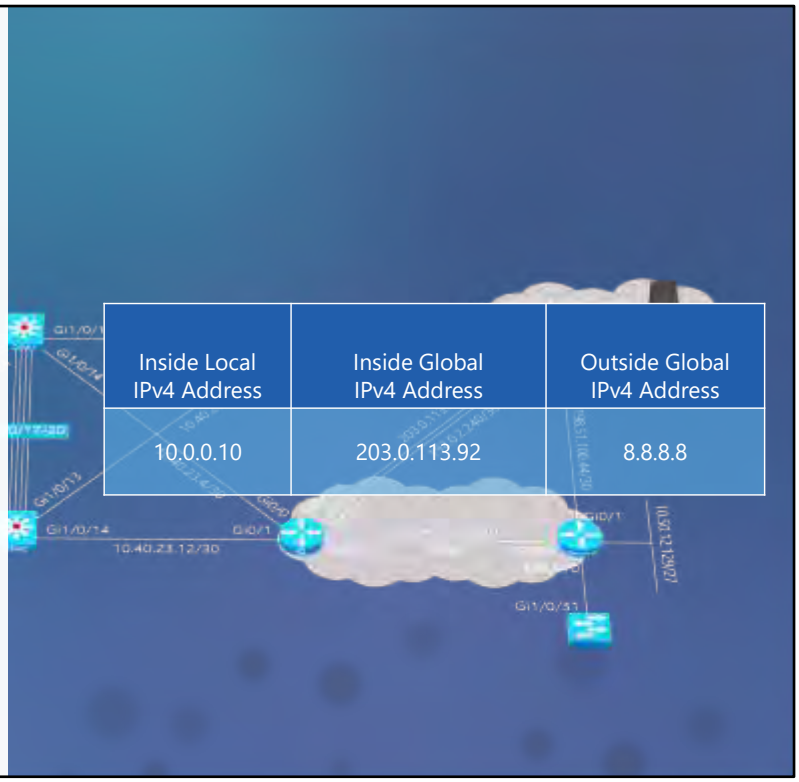


Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
10.0.0.10	203.0.113.92	8.8.8.8

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NAT

Inside Local Addresses	Specifies a private IP inside the network
Inside Global Addresses	Specifies the public IP that private IP is translated to
Outside Global Addresses	Specifies a destination host outside the private network



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NAT

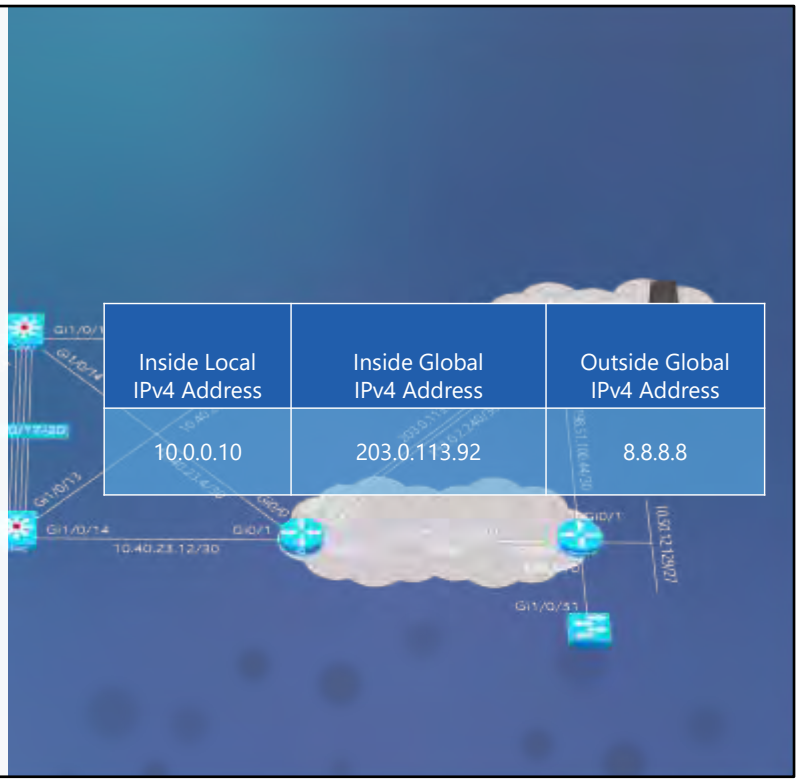
Types of NAT

Static NAT uses one-to-one address mapping.

Dynamic NAT uses many-to-many address mapping.

PAT uses many-to-one address mapping.

Dynamic with PAT uses many-to-many address mapping.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Static NAT

Types of NAT

Static NAT uses one-to-one address mapping.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Static NAT

```
R2#config terminal
R2(config)#interface range gig0/0, gig0/1, fastE0/1/0
R2(config-if-range)#ip nat inside
R2(config-if-range)#interface fastethernet 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#ip nat inside source static 10.0.0.10 203.0.113.92
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Static NAT

```
R2#show ip nat translations
Pro Inside global       Inside local       Outside local   Outside global
www  203.0.113.92:65000 10.0.0.10:65000    8.8.8.8:80      8.8.8.8:80
---  203.0.113.92       10.0.0.10          ---             ---
```

```
R2#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 3, occurred 4d19h ago
Outside interfaces:
  FastEthernet0/0/0
Inside interfaces:
  GigabitEthernet0/0, GigabitEthernet0/1, FastEthernet0/1/0
Hits: 27  Misses: 0
CEF Translated packets: 27, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic NAT

Types of NAT

Dynamic NAT uses many-to-many address mapping.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic NAT

```
R2#config terminal
R2(config)#interface range gig0/0, gig0/1, fastE0/1/0
R2(config-if-range)#ip nat inside
R2(config-if-range)#interface fastethernet 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#ip nat pool STORMWIND_DEMO 203.0.113.92 203.0.113.94 prefix-length 29
R2(config)#access-list 50 permit 10.0.0.10 0.0.0.0
R2(config)#access-list 50 permit 10.0.1.50 0.0.0.0
R2(config)#access-list 50 permit 10.0.2.20 0.0.0.0
R2(config)#ip nat inside source list 50 pool STORMWIND_DEMO
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic NAT

```
R2#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 3, occurred 4d19h ago
Outside interfaces:
  FastEthernet0/0/0
Inside interfaces:
  GigabitEthernet0/0, GigabitEthernet0/1, FastEthernet0/1/0
Hits: 37  Misses: 0
CEF Translated packets: 37, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 7] access-list 50 pool STORMWINDDEMO refcount 0
 pool STORMWINDDEMO: netmask 255.255.255.248
        start 203.0.113.92 end 203.0.113.94
        type generic, total addresses 3, allocated 0 (0%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic NAT

```
R2#show ip nat translations
Pro Inside global       Inside local     Outside local    Outside global
www  203.0.113.92:56789 10.0.0.10:56789  8.8.8.8:80       8.8.8.8:80
---  203.0.113.92       10.0.0.10        ---              ---
www  203.0.113.94:59867 10.0.1.50:59867  8.8.8.8:80       8.8.8.8:80
---  203.0.113.94       10.0.1.50        ---              ---
www  203.0.113.93:62345 10.0.2.20:62345  8.8.8.8:80       8.8.8.8:80
---  203.0.113.93       10.0.2.20        ---              ---
R2#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PAT

Types of NAT

PAT uses many-to-one address mapping.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PAT With a Single IP

```
R2#config terminal
R2(config)#interface range gig0/0, gig0/1, fastE0/1/0
R2(config-if-range)#ip nat inside
R2(config-if-range)#interface range fastethernet 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#access-list 50 permit 10.0.0.0 0.0.0.255
R2(config)#access-list 50 permit 10.0.1.0 0.0.0.255
R2(config)#access-list 50 permit 10.0.2.0 0.0.0.255
R2(config)#access-list 50 permit 10.0.3.0 0.0.0.255
R2(config)#ip nat inside source list 50 interface fastEthernet 0/0/0 overload
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PAT With a Single IP

```
R2#show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 6, occurred 00:02:57 ago
Outside interfaces:
  FastEthernet0/0/0
Inside interfaces:
  GigabitEthernet0/0, GigabitEthernet0/1, FastEthernet0/1/0
Hits: 65  Misses: 0
CEF Translated packets: 65, CEF Punted packets: 0
Expired translations: 7
Dynamic mappings:
-- Inside Source
[Id: 8] access-list 50 interface FastEthernet0/0/0 refcount 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PAT With a Single IP

```
R2#show ip nat translations
Pro Inside global        Inside local       Outside local      Outside global
www  203.0.113.91:62345  10.0.0.10:62345    8.8.8.8:80         8.8.8.8:80
www  203.0.113.91:49876  10.0.1.50:49876    8.8.8.8:80         8.8.8.8:80
www  203.0.113.91:64544  10.0.2.20:62345    8.8.8.8:80         8.8.8.8:80
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PAT With Multiple IPs

Types of NAT

Dynamic with PAT uses many-to-many address mapping.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PAT With Multiple IPs

```
R2#config terminal
R2(config)#interface range gig0/0, gig0/1, fastE0/1/0
R2(config-if-range)#ip nat inside
R2(config-if-range)#interface fastethernet 0/0/0
R2(config-if)#ip nat outside
R2(config-if)#exit
R2(config)#ip nat pool STORMWIND_DEMO 203.0.113.92 203.0.113.94 prefix-length 29
R2(config)#access-list 50 permit 10.0.0.0 0.0.0.255
R2(config)#access-list 50 permit 10.0.1.0 0.0.0.255
R2(config)#access-list 50 permit 10.0.2.0 0.0.0.255
R2(config)#access-list 50 permit 10.0.3.0 0.0.0.255
R2(config)#ip nat inside source list 50 pool STORMWIND_DEMO overload
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

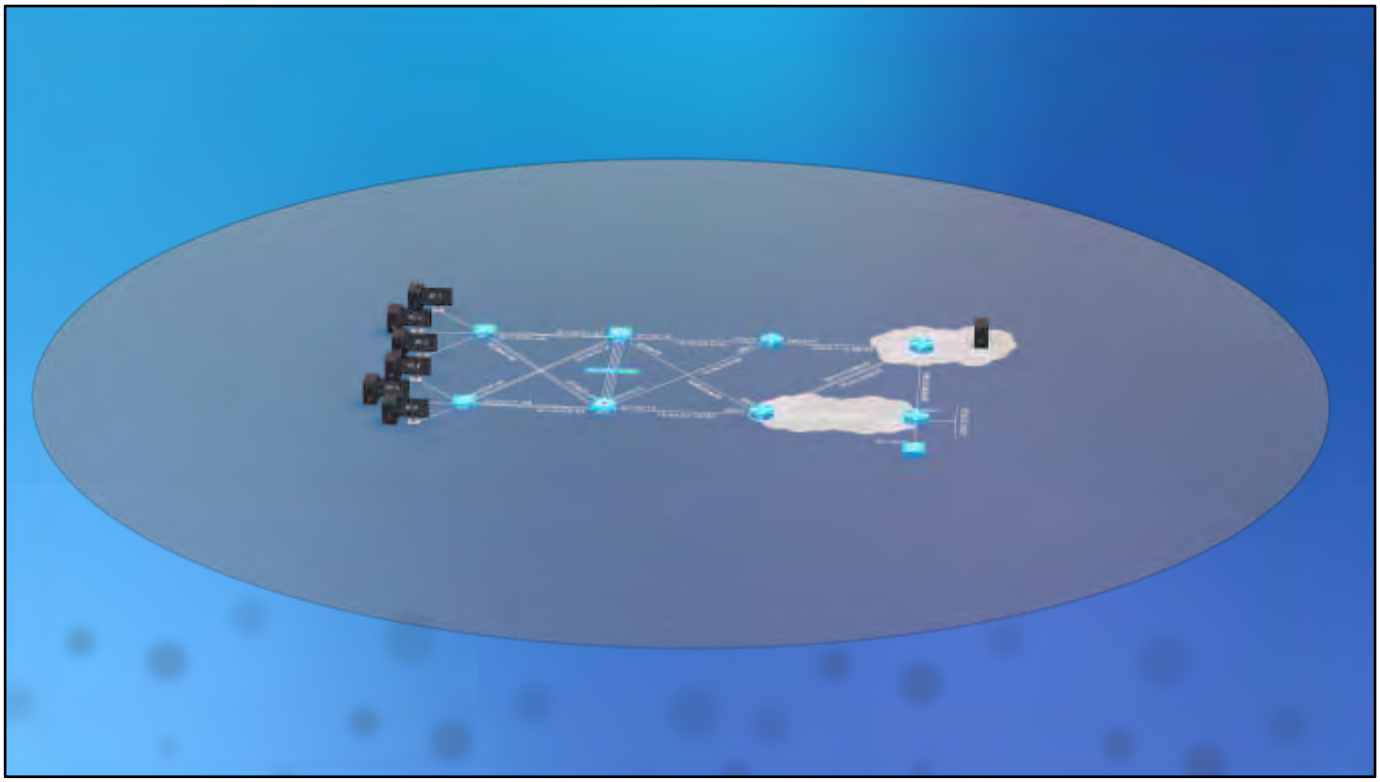
PAT With Multiple IPs

```
R2#show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
www  203.0.113.94:43987 10.0.0.10:43987    123.123.123.123:80 123.123.123.123:80
www  203.0.113.95:57896 10.0.0.10:57896    123.123.123.123:80 123.123.123.123:80
www  203.0.113.94:49999 10.0.0.10:49999    8.8.8.8:80         8.8.8.8:80
www  203.0.113.96:59123 10.0.1.50:59123    123.123.123.123:80 123.123.123.123:80
www  203.0.113.95:65321 10.0.1.50:65321    123.123.123.123:80 123.123.123.123:80
www  203.0.113.94:43988 10.0.1.50:43987    8.8.8.8:80         8.8.8.8:80
www  203.0.113.95:54321 10.0.2.20:54321    123.123.123.123:80 123.123.123.123:80
www  203.0.113.94:65142 10.0.2.20:65142    123.123.123.123:80 123.123.123.123:80
www  203.0.113.96:61111 10.0.2.20:61111    8.8.8.8:80         8.8.8.8:80
```

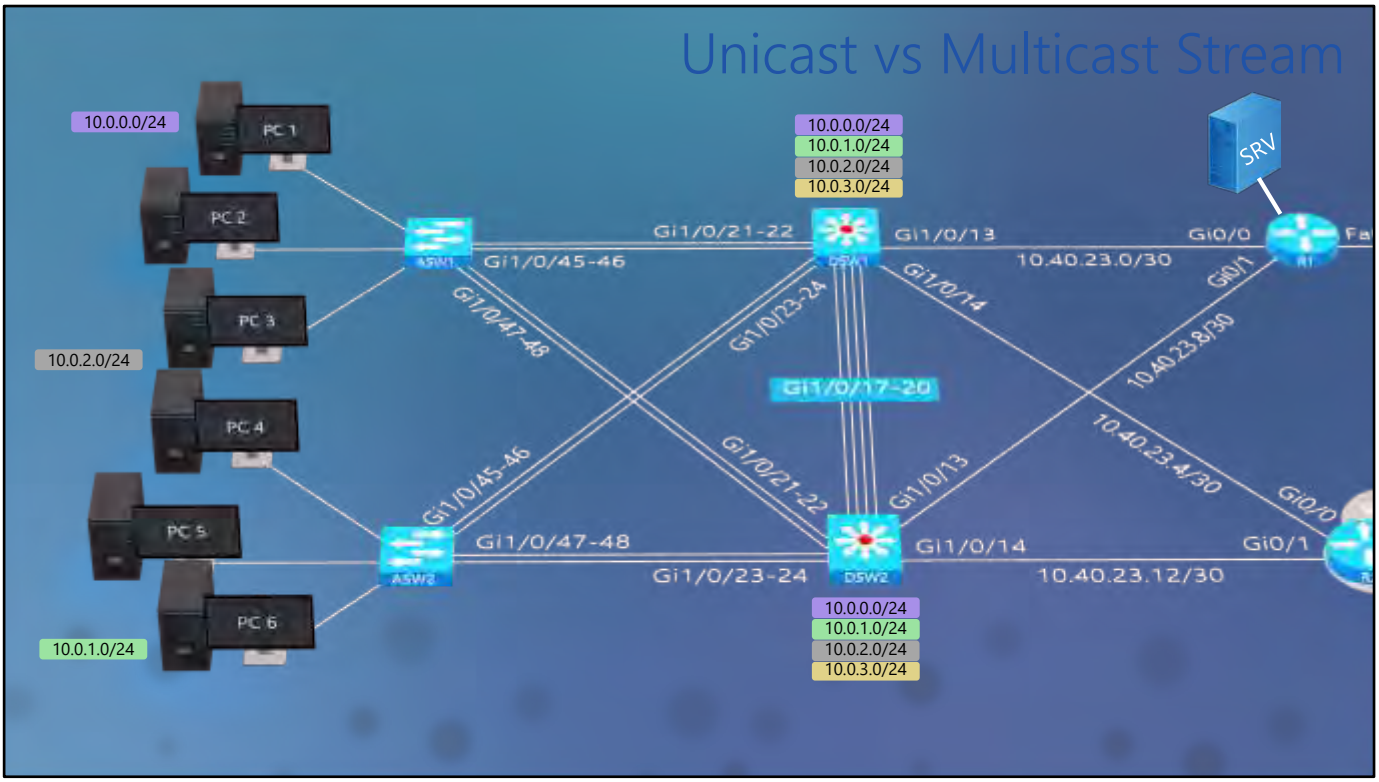
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multicast Protocol Overview

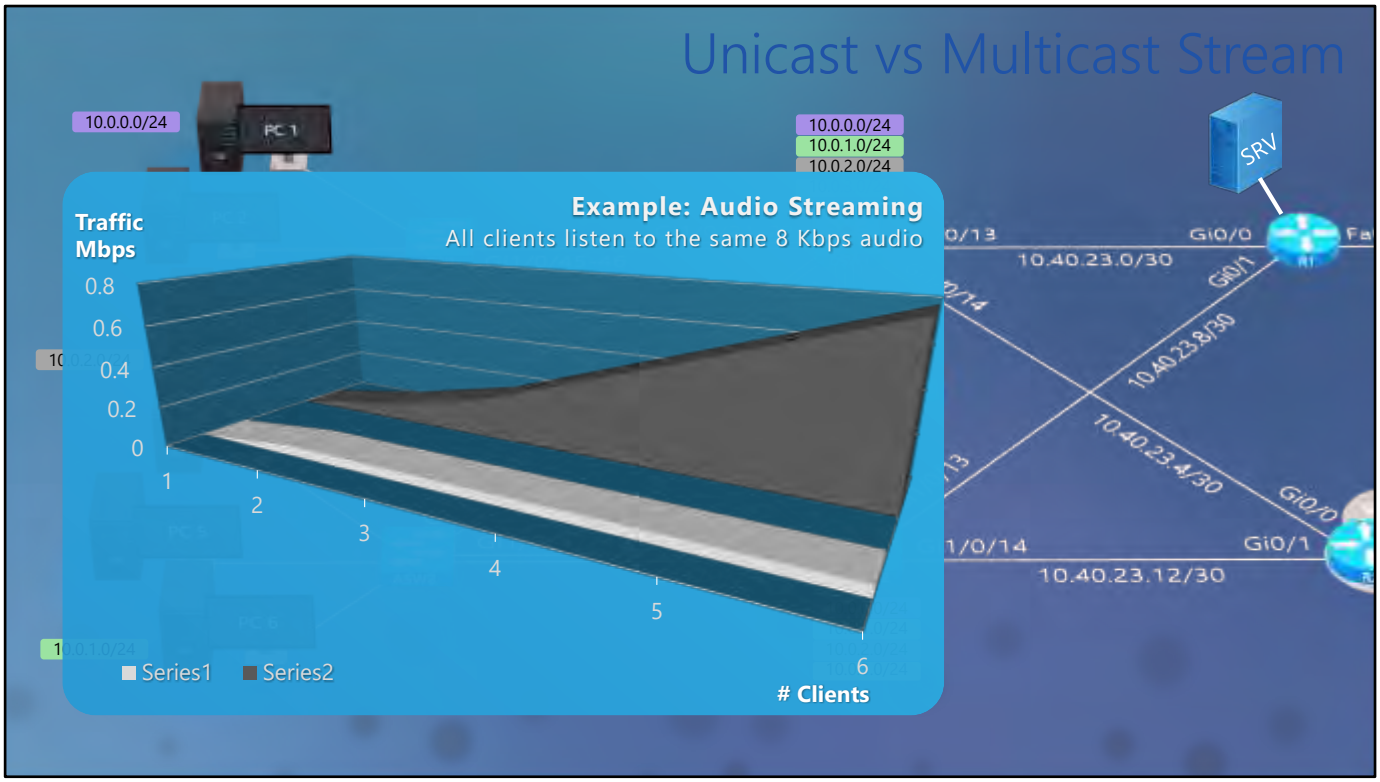
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



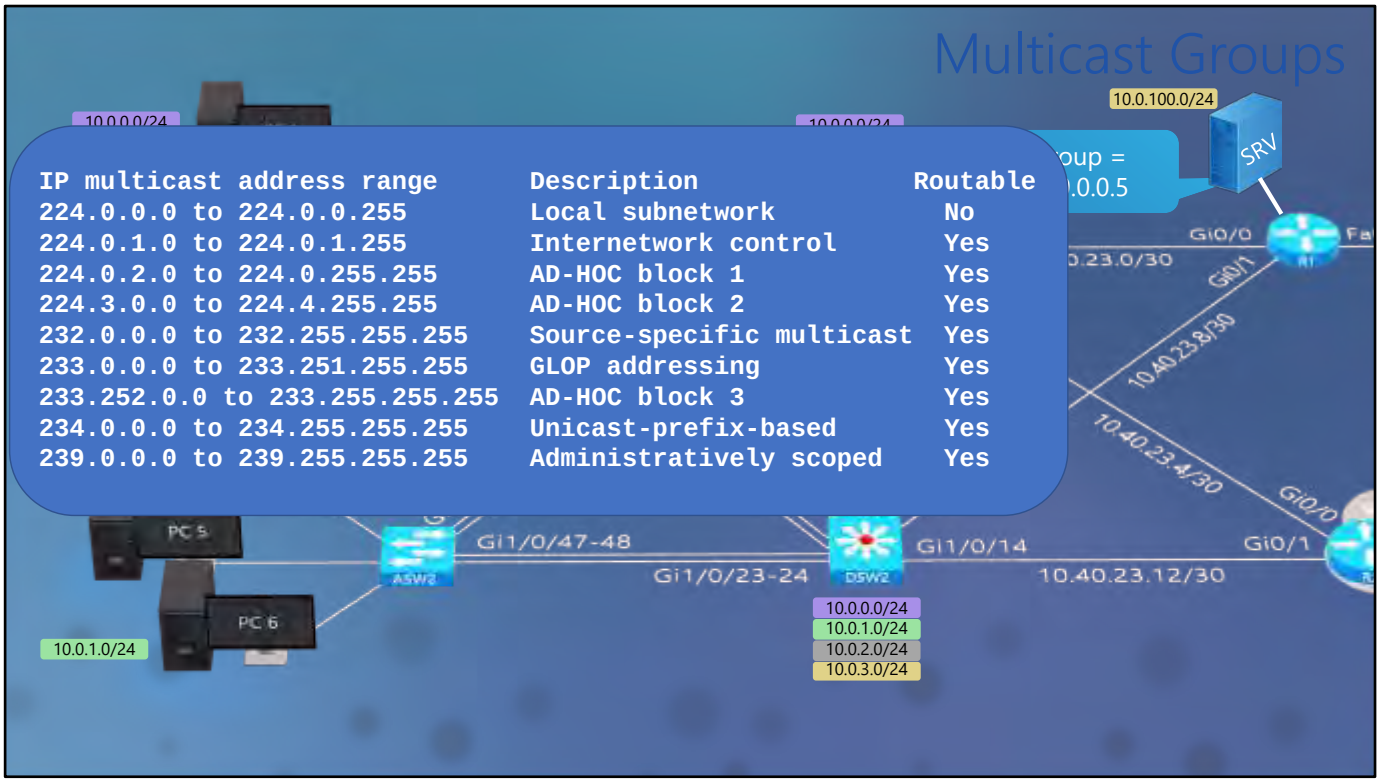
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Multicast Groups

IP multicast address range	Description	Routable
224.0.0.0 to 224.0.0.255	Local subnetwork	No
224.0.1.0 to 224.0.1.255	Internetwork control	Yes
224.0.2.0 to 224.0.255.255	AD-HOC block 1	Yes
224.3.0.0 to 224.4.255.255	AD-HOC block 2	Yes
232.0.0.0 to 232.255.255.255	Source-specific multicast	Yes
233.0.0.0 to 233.251.255.255	GLOP addressing	Yes
233.252.0.0 to 233.255.255.255	AD-HOC block 3	Yes
234.0.0.0 to 234.255.255.255	Unicast-prefix-based	Yes
239.0.0.0 to 239.255.255.255	Administratively scoped	Yes



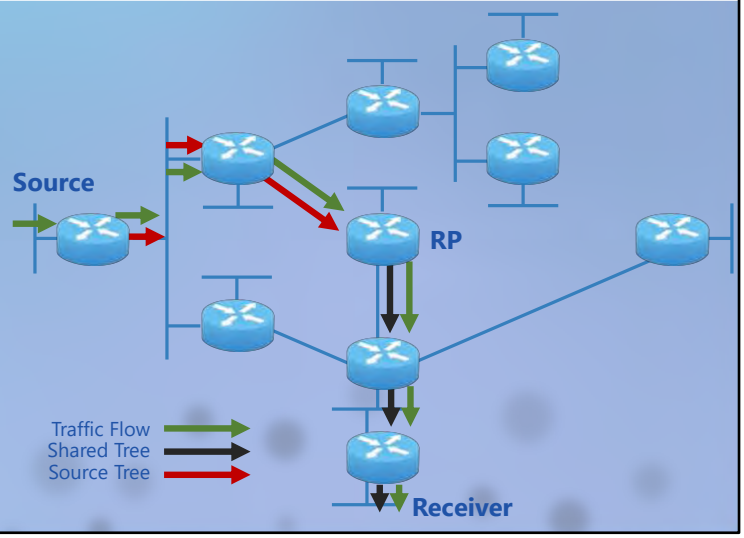
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IGMP and PIM

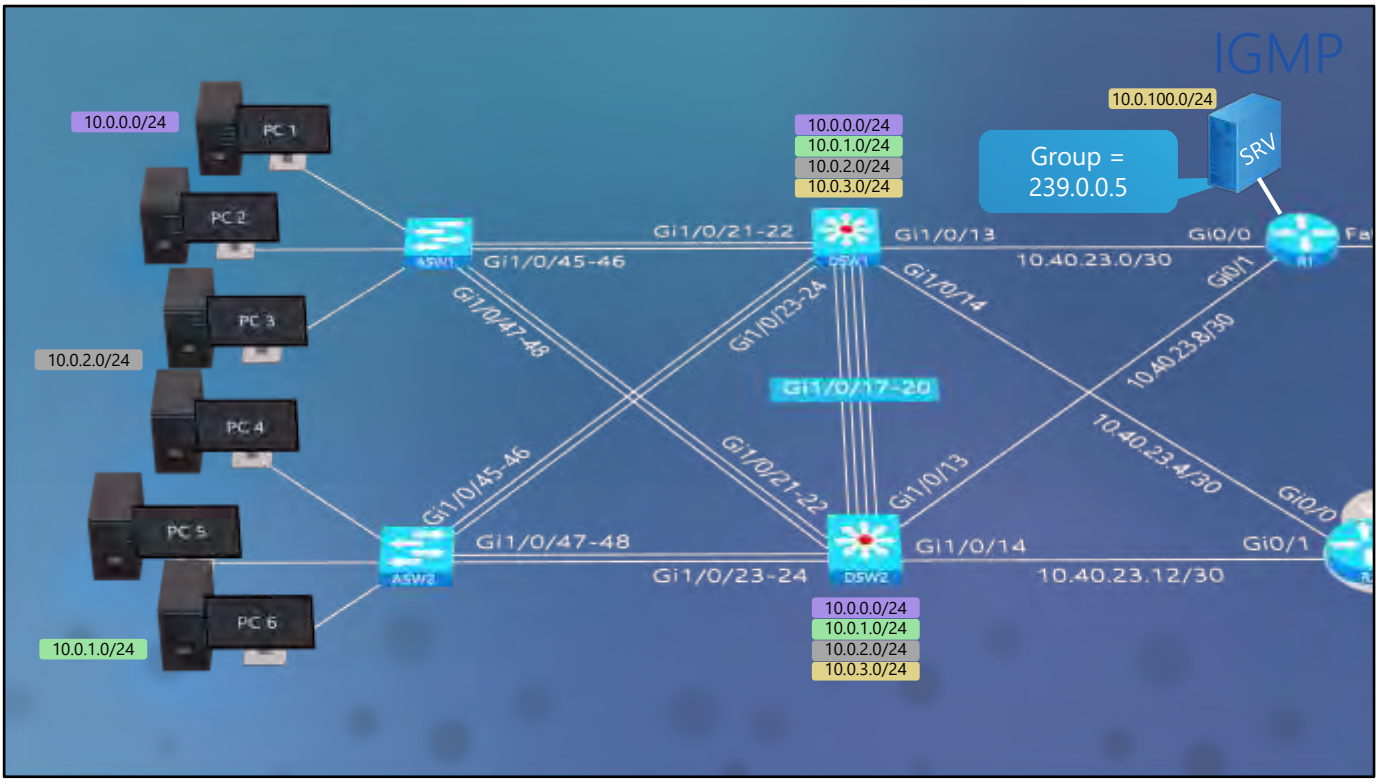
Protocols used by Multicast

IGMP – used between hosts and routers for hosts to communicate their desire to join/leave/remain in a group

PIM – used by the routers to build the multicast tree that will be used to forward multicast streams through the network



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

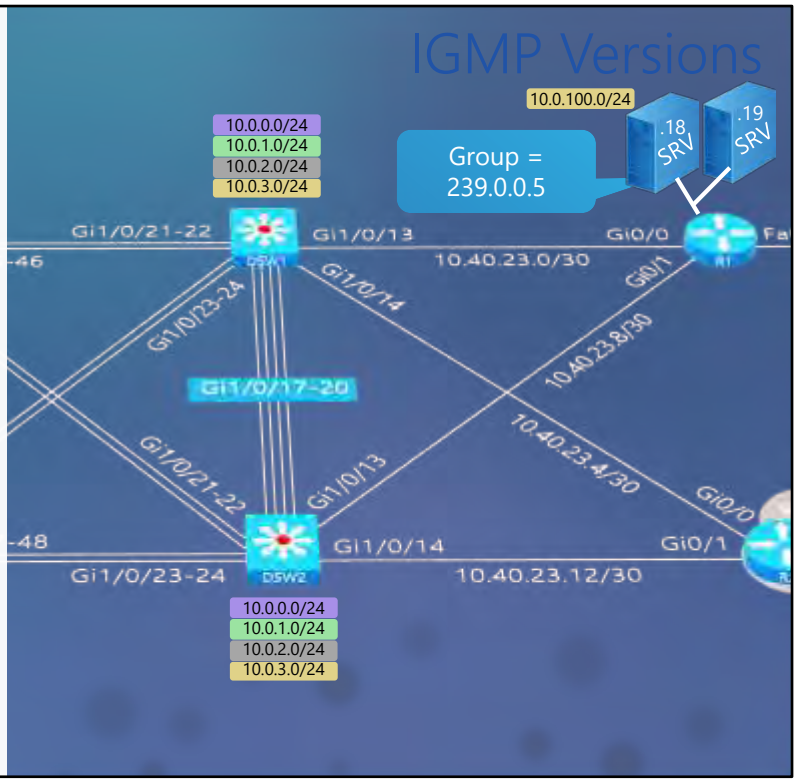
IGMP Versions

IGMPv2

- Join message
  - Sent to group address (*,G)
- Membership queries can be
  - General – sent to 224.0.0.1
  - Group specific – sent to group address
- Leave group message
  - Sent to 224.0.0.2

IGMPv3

- Join message
  - Sent to group address (*,G)
  - Servers source address and group – for source specific multicast (S,G)
- Leave group message
  - Sent to 224.0.0.22



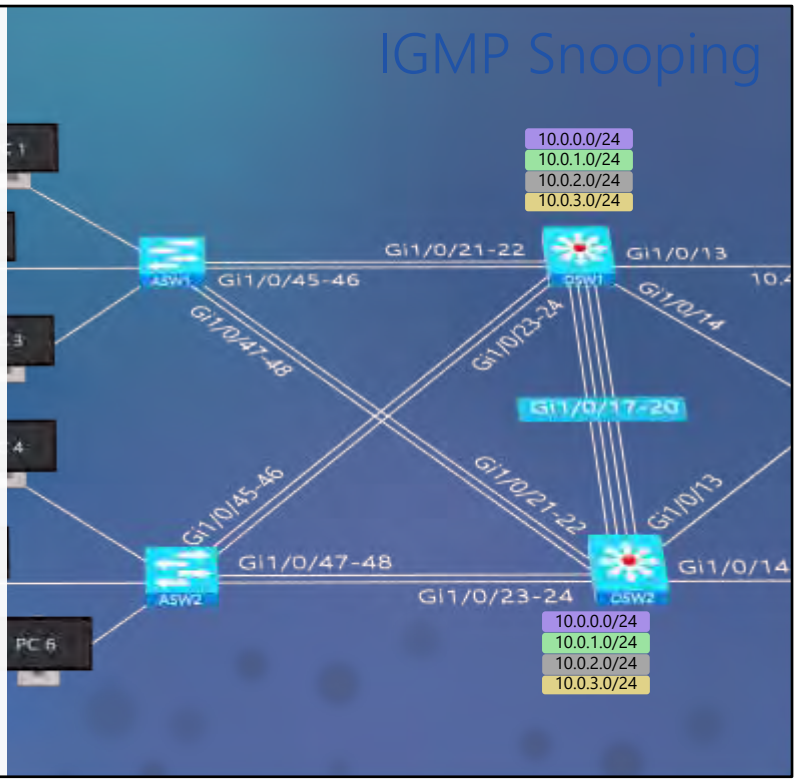
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IGMP Snooping

A switch feature for examining IGMP messages

Permits the switch to forward multicast frames instead of flooding them

Reduces bandwidth consumption of the multicast stream



©2023 by StormWind LLC. All rights reserved.

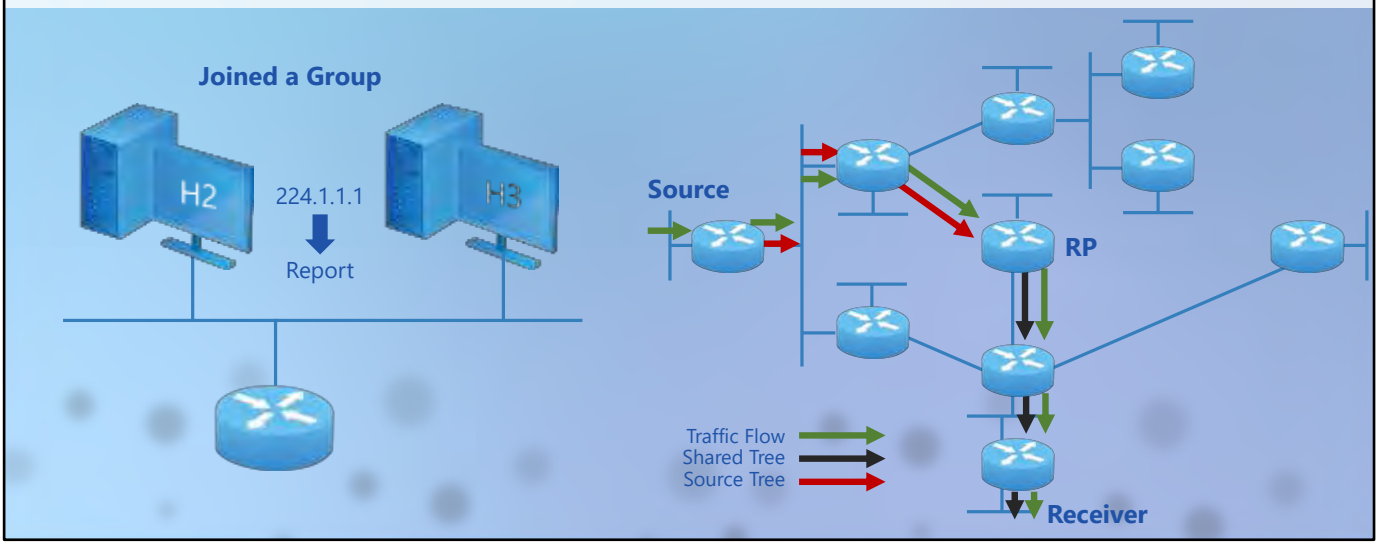
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IGMP and PIM

Protocols used by Multicast

IGMP – used between hosts and routers for hosts to communicate their desire to join/leave/remain in a group

PIM – used by the routers to build the multicast tree that will be used to forward multicast streams through the network



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

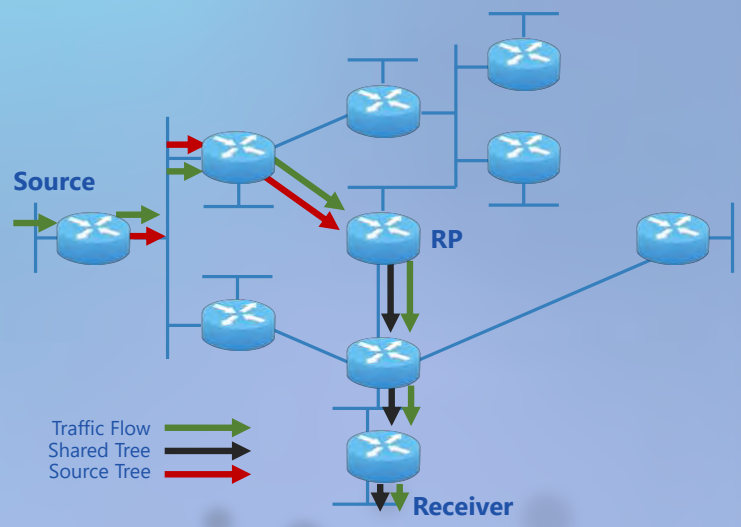
PIM

Dense Mode (1-many)

Sparse Mode (1-many)

Sparse-Dense (1-many)

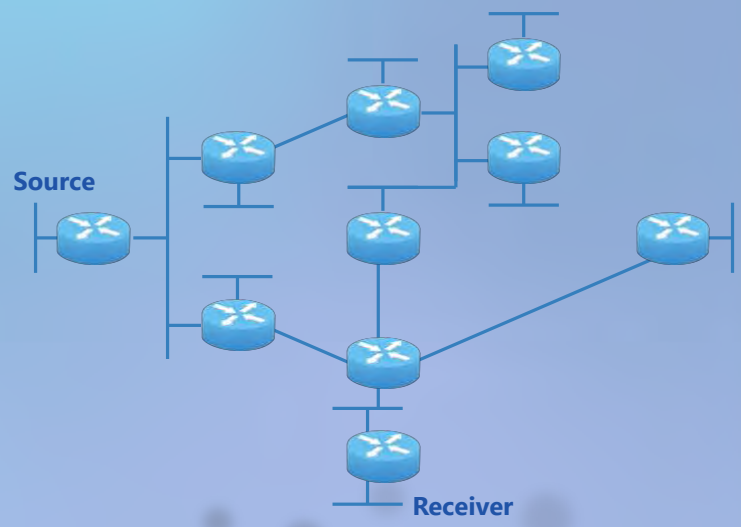
Bidirectional (many-many)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PIM

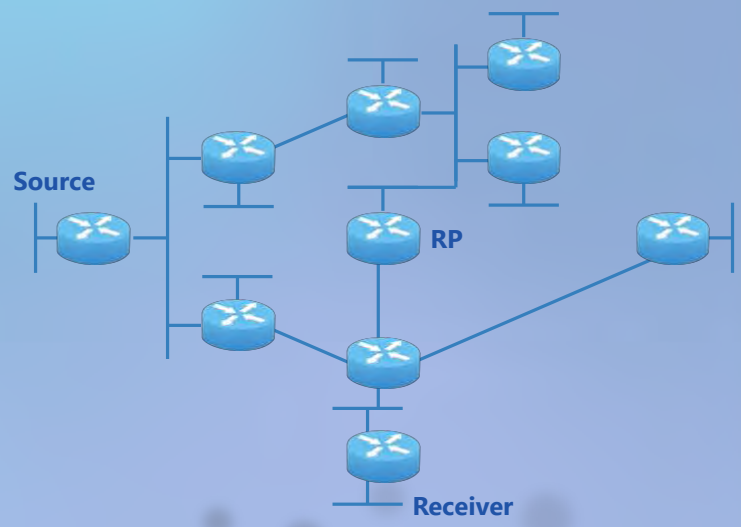
- Dense Mode (1-many)
  - Push model that floods multicast streams to every corner of the network regardless of users requesting the stream or not.
  - The tree is then build backwards based on if the clients are using it or not.
  - Known as flood and prune.
- Sparse Mode (1-many)
- Sparse-Dense (1-many)
- Bidirectional (many-many)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PIM

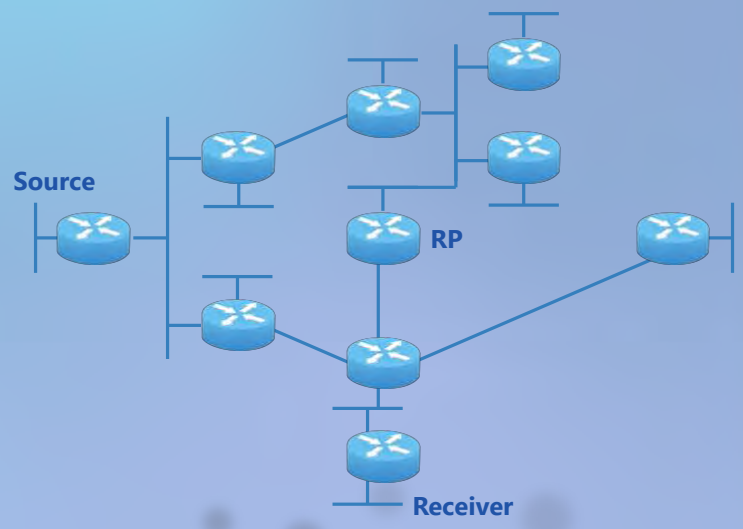
- Dense Mode (1-many)
- Sparse Mode (1-many)
  - Pull model that delivers multicast streams to only those networks with end users that have requested the stream.
  - Build tree based on the requests.
- Sparse-Dense (1-many)
- Bidirectional (many-many)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PIM

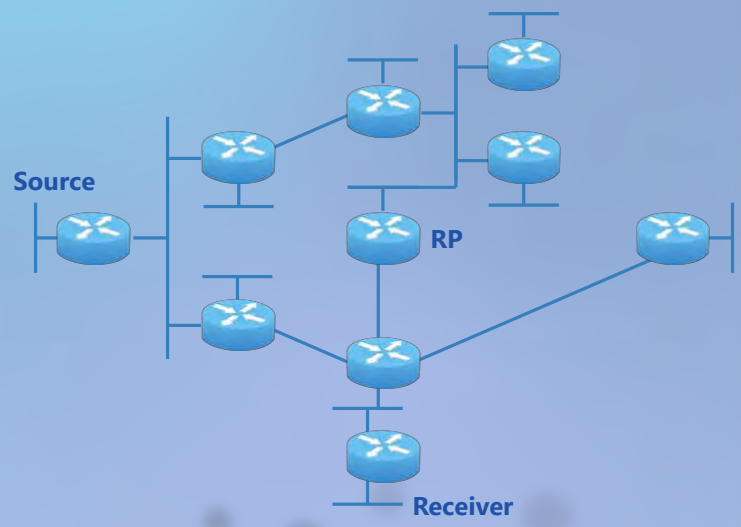
- Dense Mode (1-many)
- Sparse Mode (1-many)
- Sparse-Dense (1-many)
  - Pull and/or Push model based on the group requirements.
- Bidirectional (many-many)



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PIM

- Dense Mode (1-many)
- Sparse Mode (1-many)
- Sparse-Dense (1-many)
- Bidirectional (many-many)
  - Pull model designed for many-many applications where there is more than one source and they are not centralized.



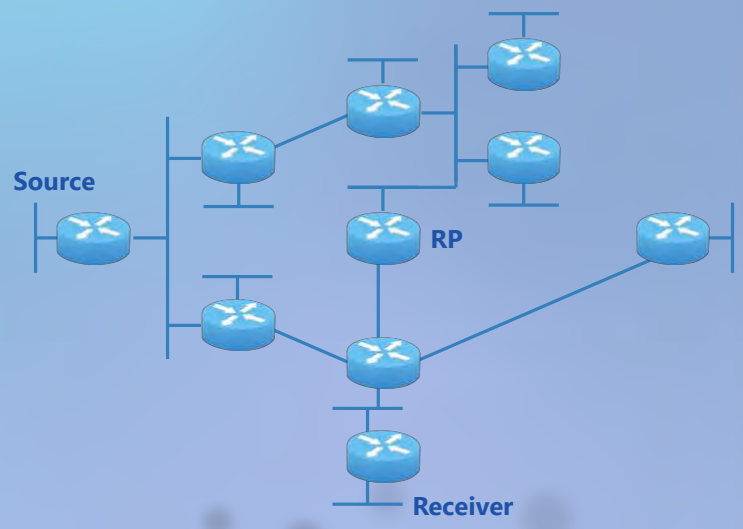
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PIM MSDP

A mechanism to connect multiple PIM-SM domains.

The purpose of MSDP is to discover multicast sources in other PIM domains.

Requires all addresses of all MSDP peers to be known in Border Gateway Protocol (BGP).



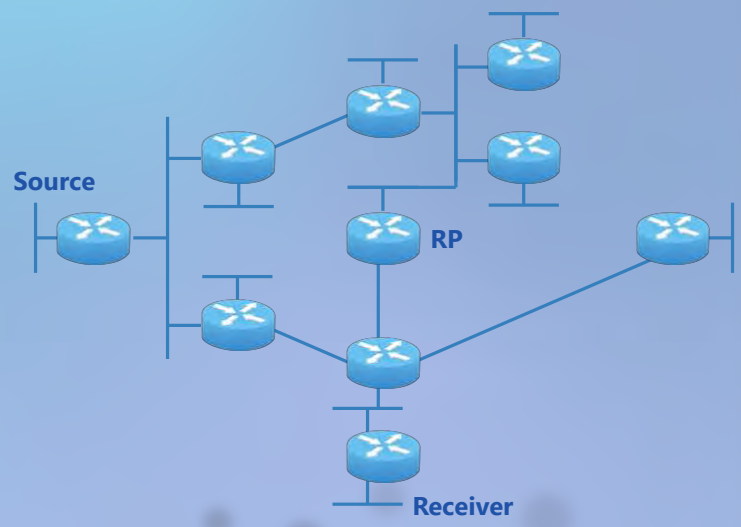
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PIM RPF

Multicast Reverse Path Forwarding

RPC Check

- Used to prevent multicast loops
- Source address of incoming multicast packet is checked against the unicast routing table



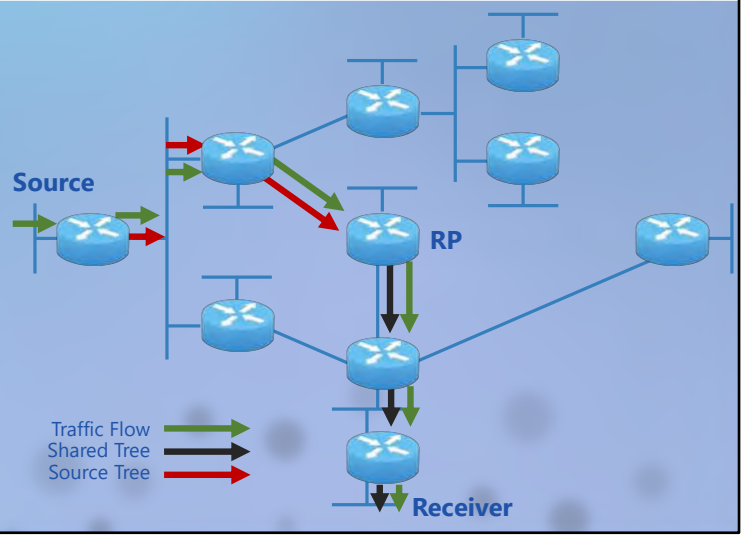
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IGMP and PIM

Protocols used by Multicast

IGMP – used between hosts and routers for hosts to communicate their desire to join/leave/remain in a group

PIM – used by the routers to build the multicast tree that will be used to forward multicast streams through the network



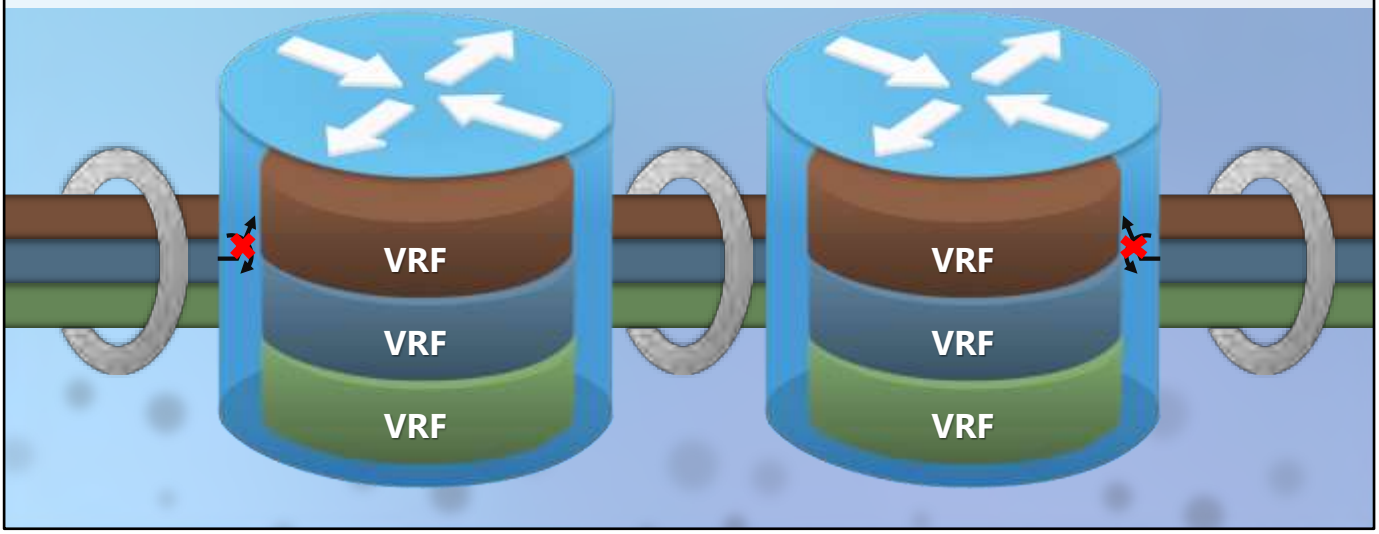
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Virtual Routing and Forwarding (VRF)

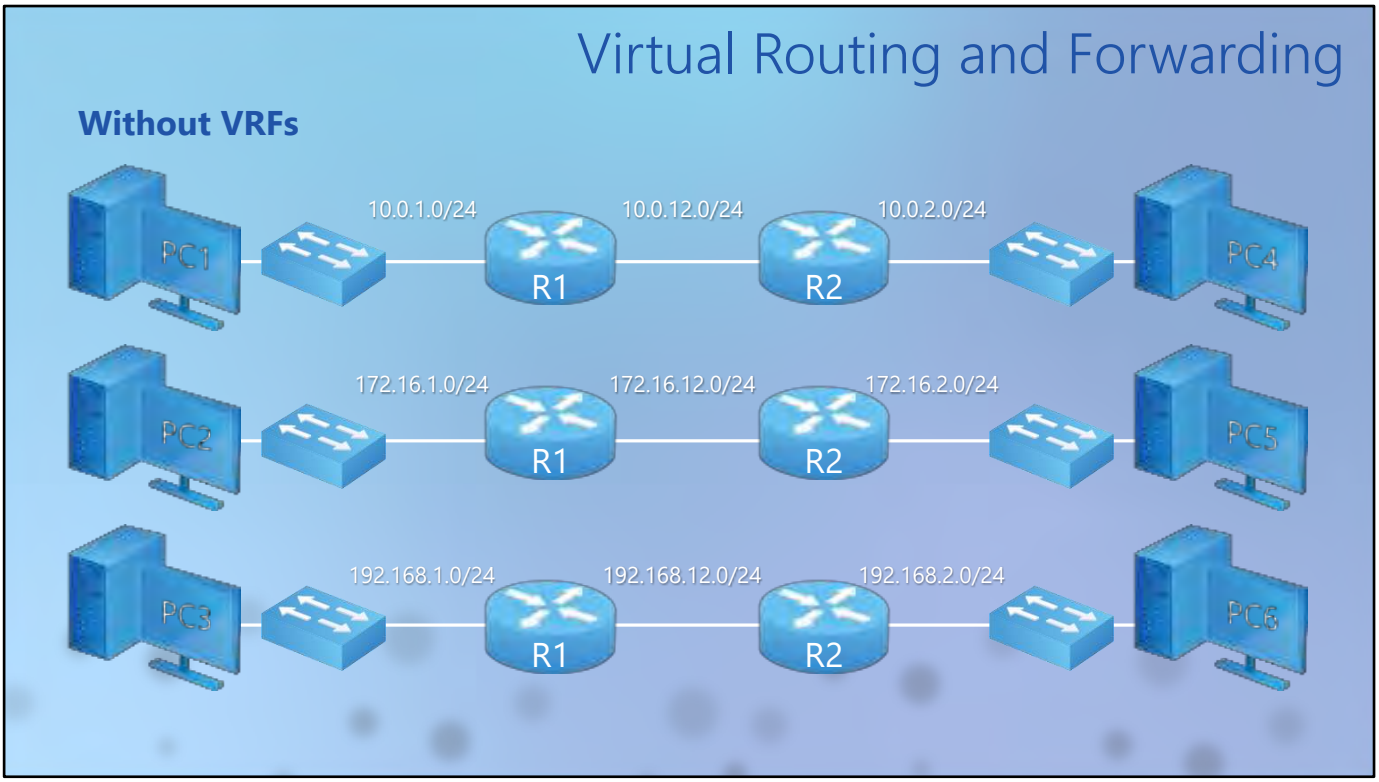
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Virtual Routing and Forwarding

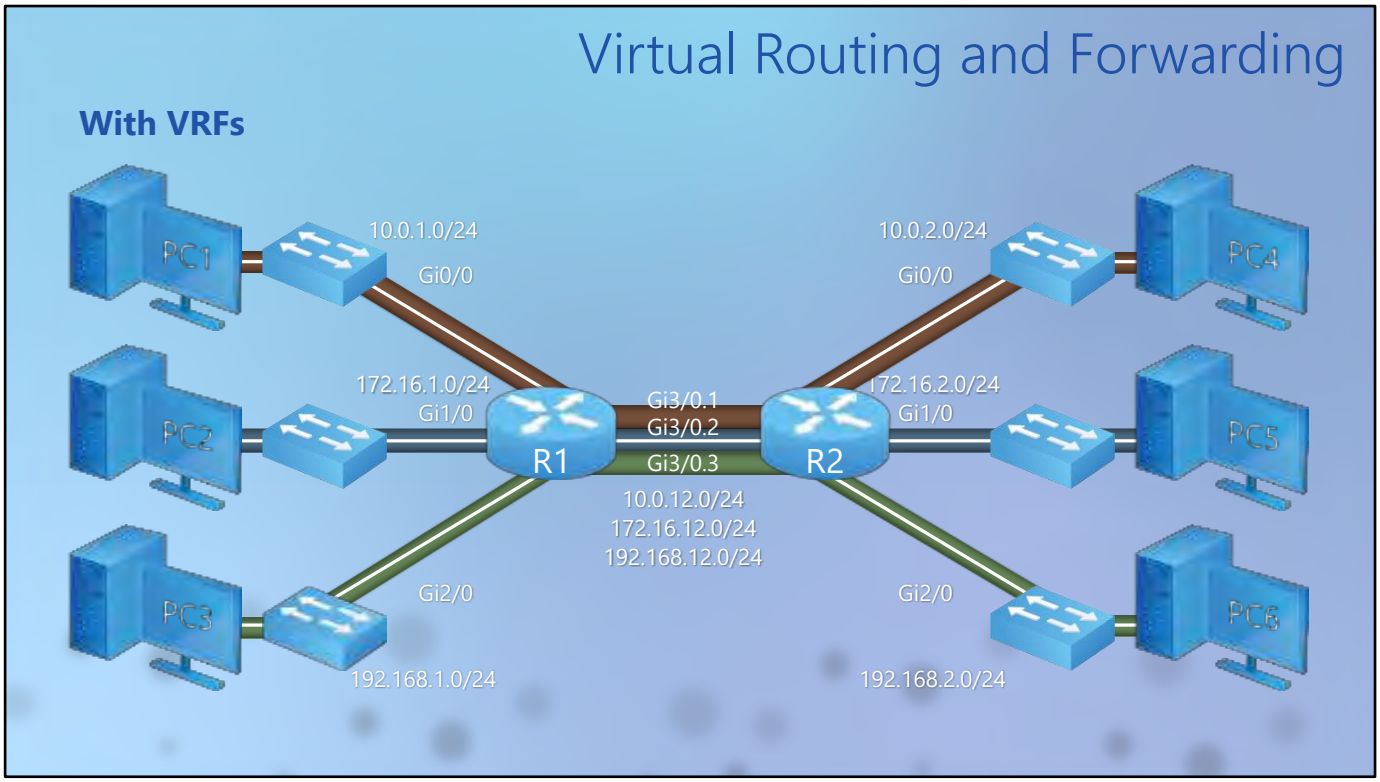
- Technique which creates multiple virtual networks within a single network entity
- Creates separate virtual routers on a single physical router
  - Router interfaces, routing tables, and forwarding tables are isolated on a VRF by VRF basis
    - Prevent traffic from one VRF interfering or interfacing with another VRF



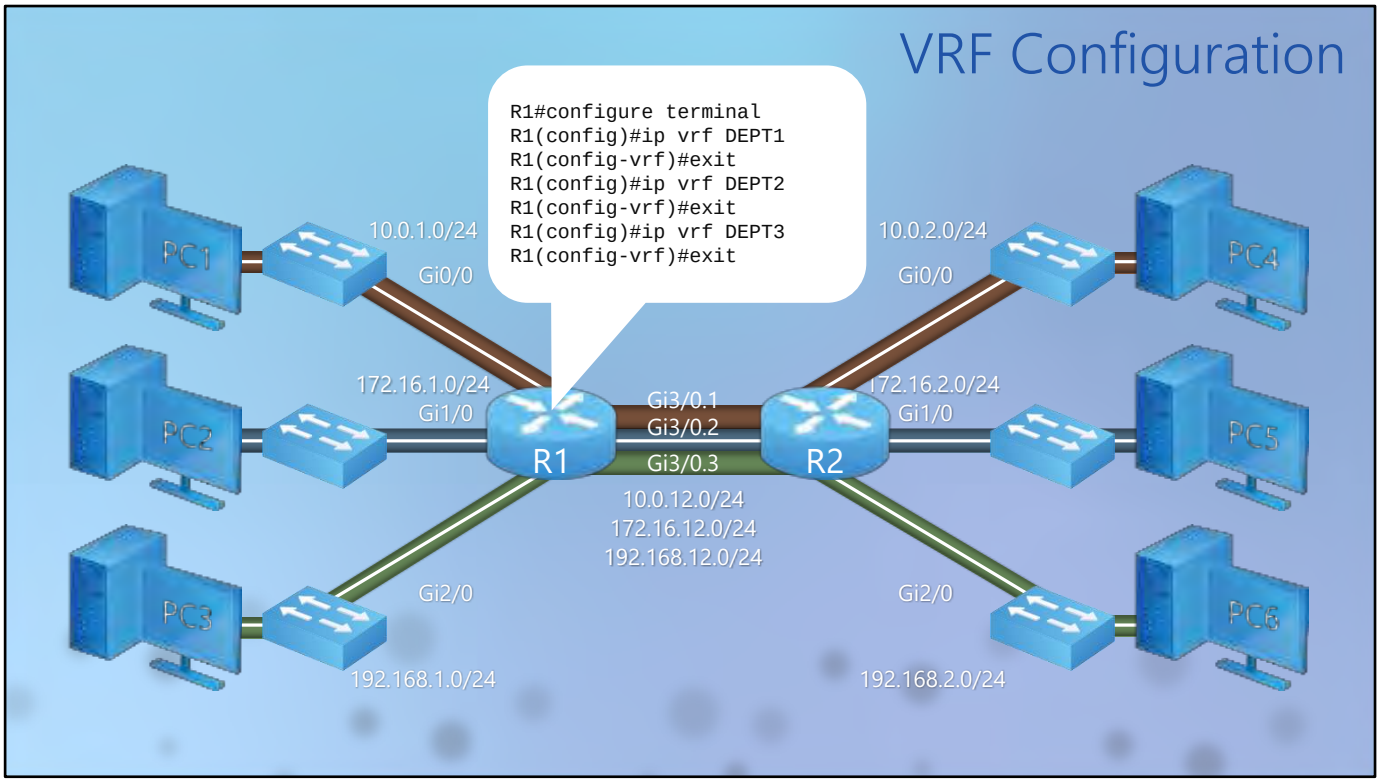
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



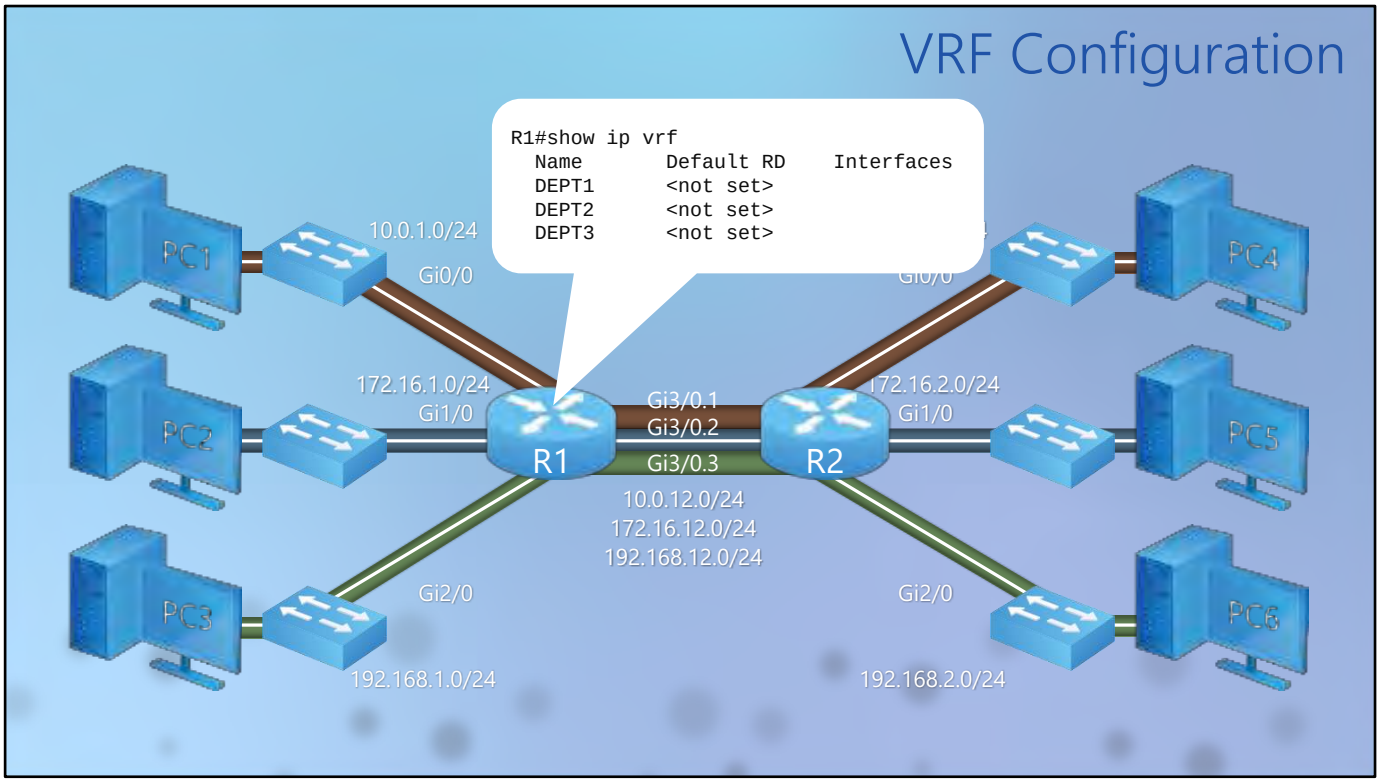
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



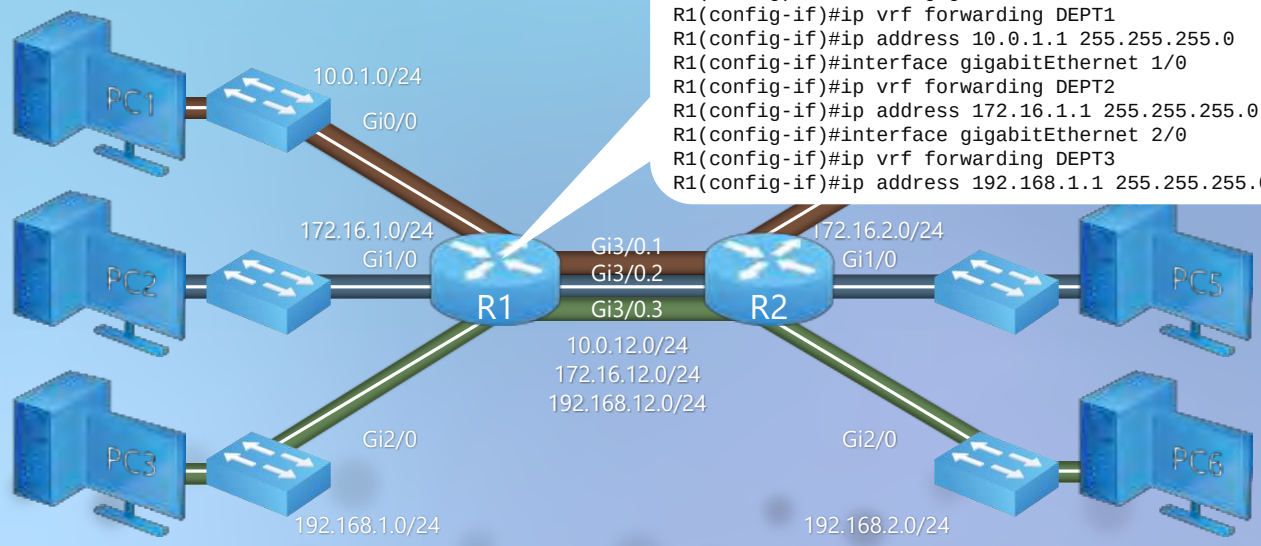
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



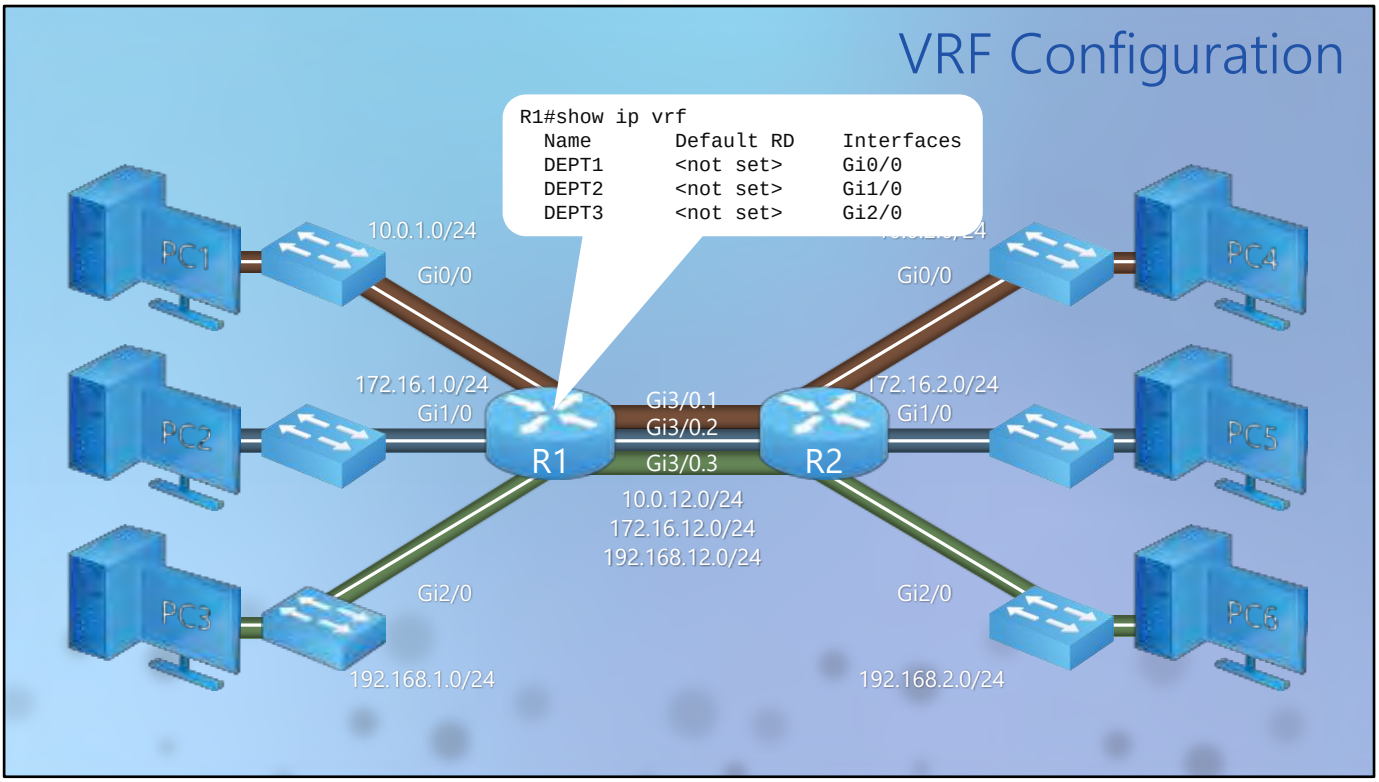
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRF Configuration

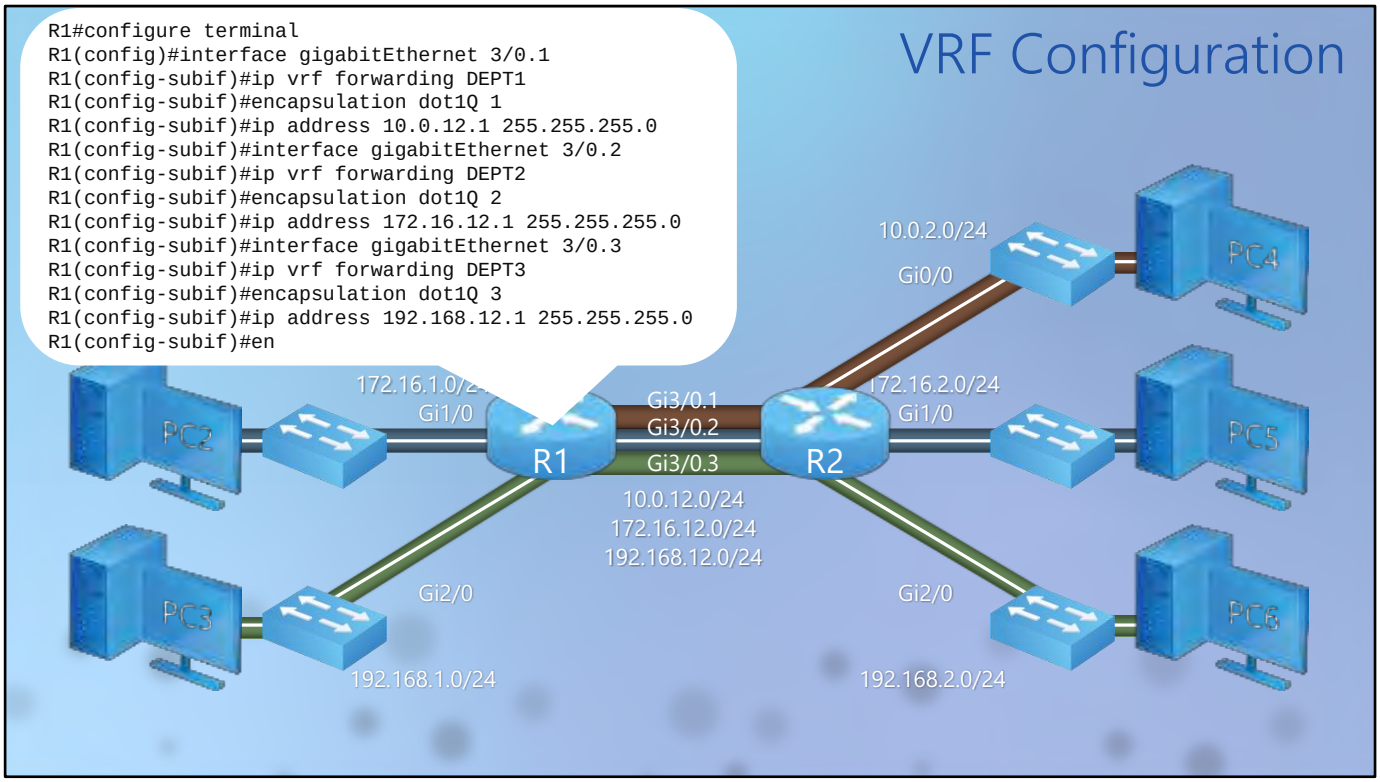
```
R1#configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#ip vrf forwarding DEPT1
R1(config-if)#ip address 10.0.1.1 255.255.255.0
R1(config-if)#interface gigabitEthernet 1/0
R1(config-if)#ip vrf forwarding DEPT2
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#interface gigabitEthernet 2/0
R1(config-if)#ip vrf forwarding DEPT3
R1(config-if)#ip address 192.168.1.1 255.255.255.0
```



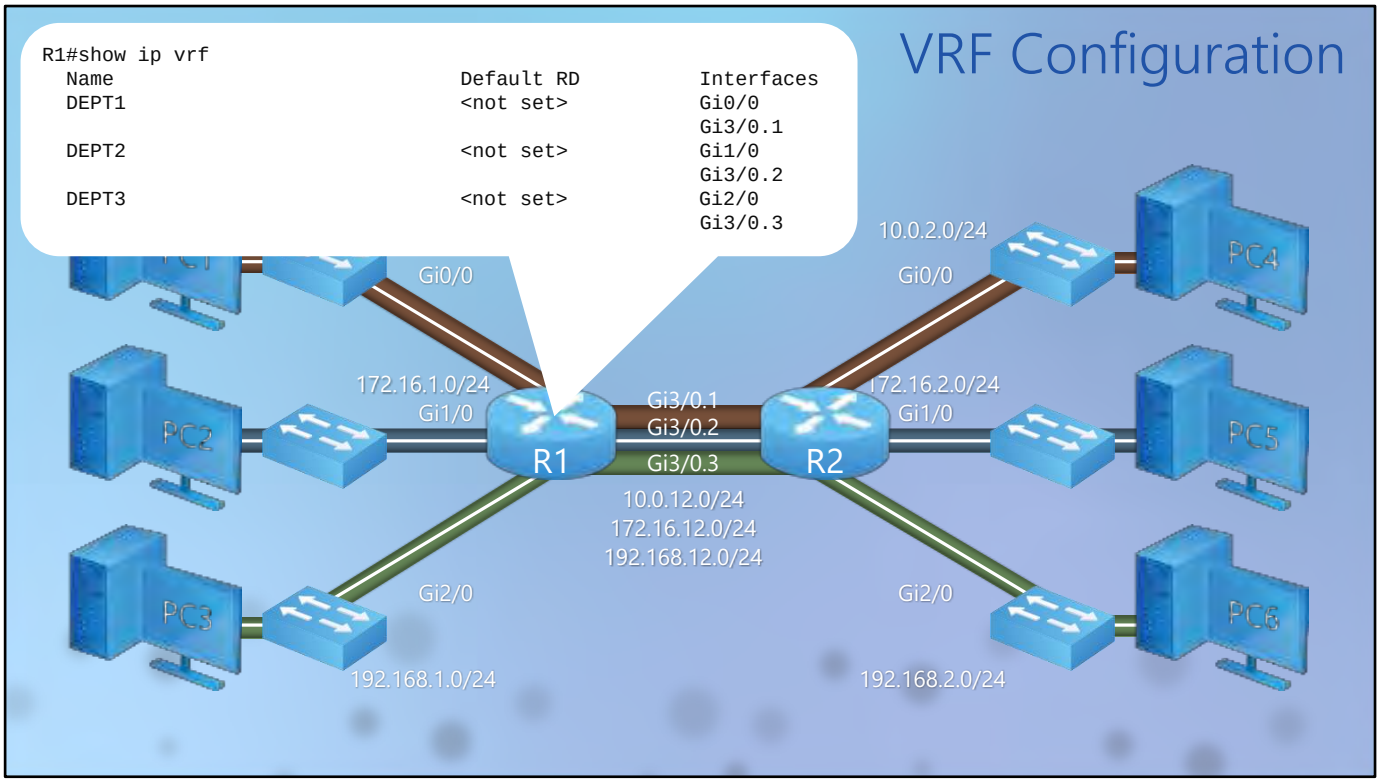
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



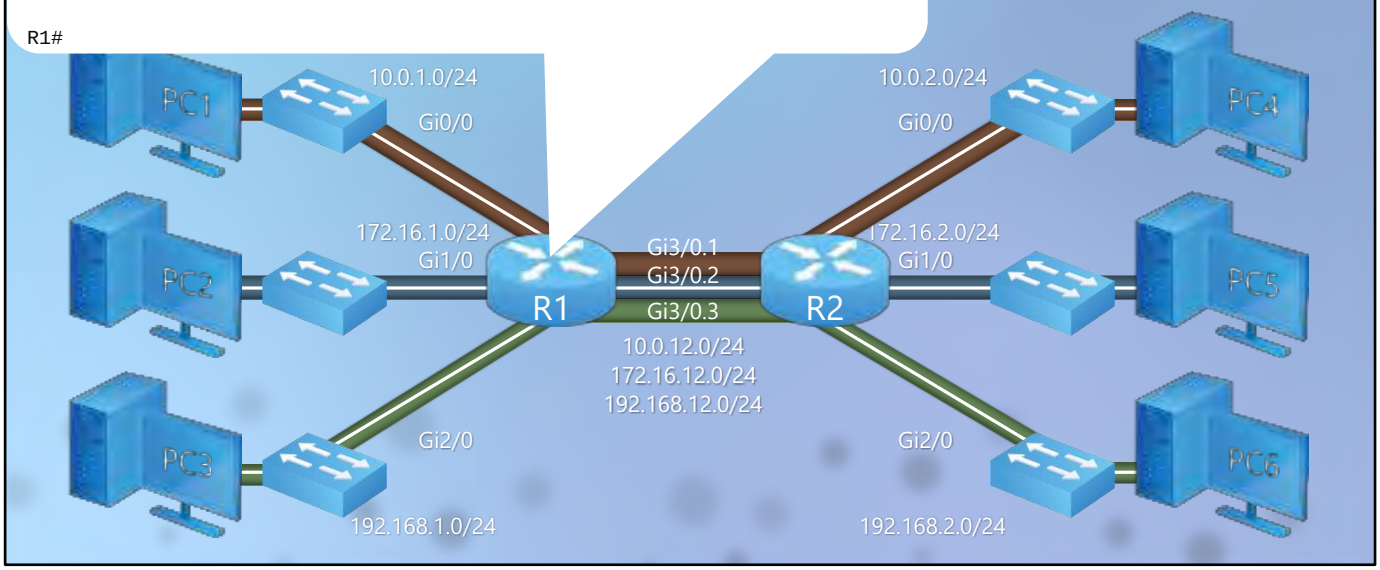
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRF Configuration

```
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
…output omitted…

Gateway of last resort is not set

R1#
```

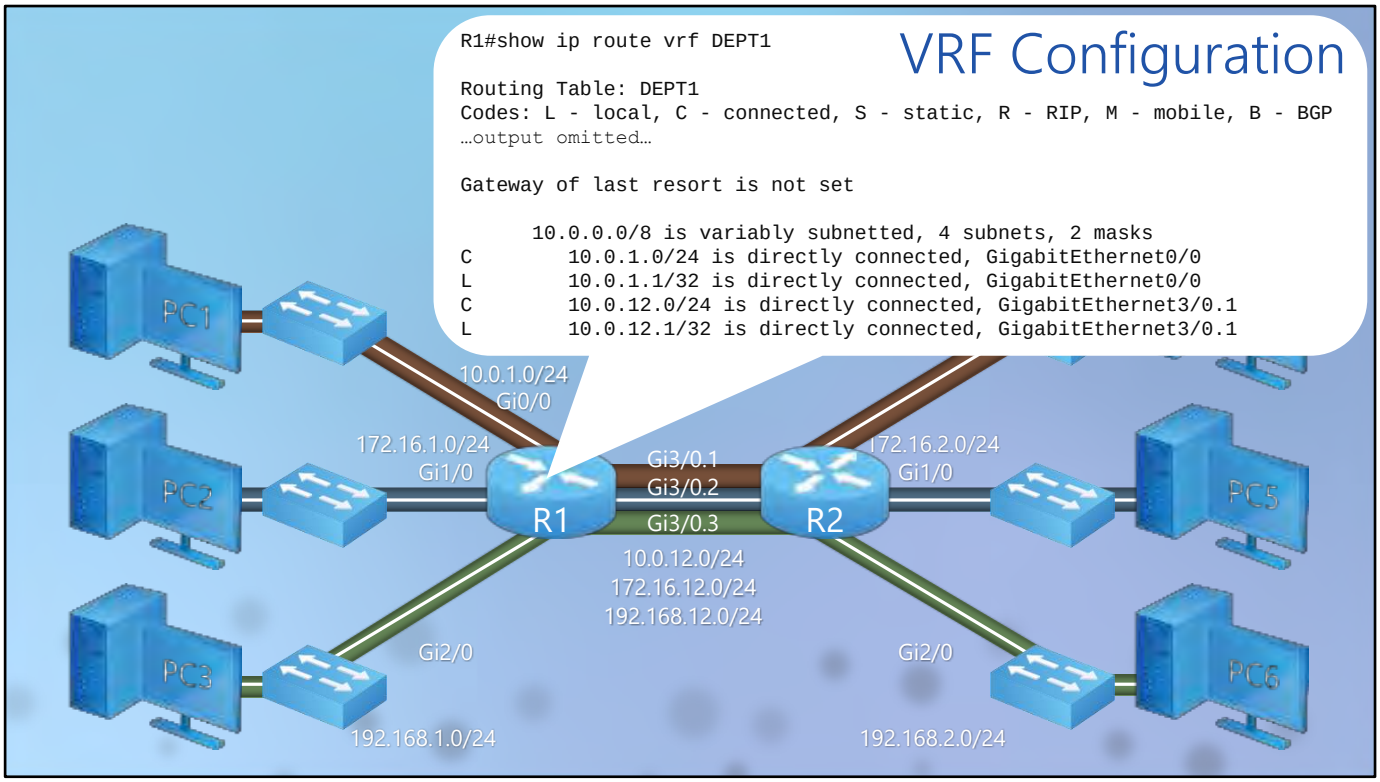


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRF Configuration

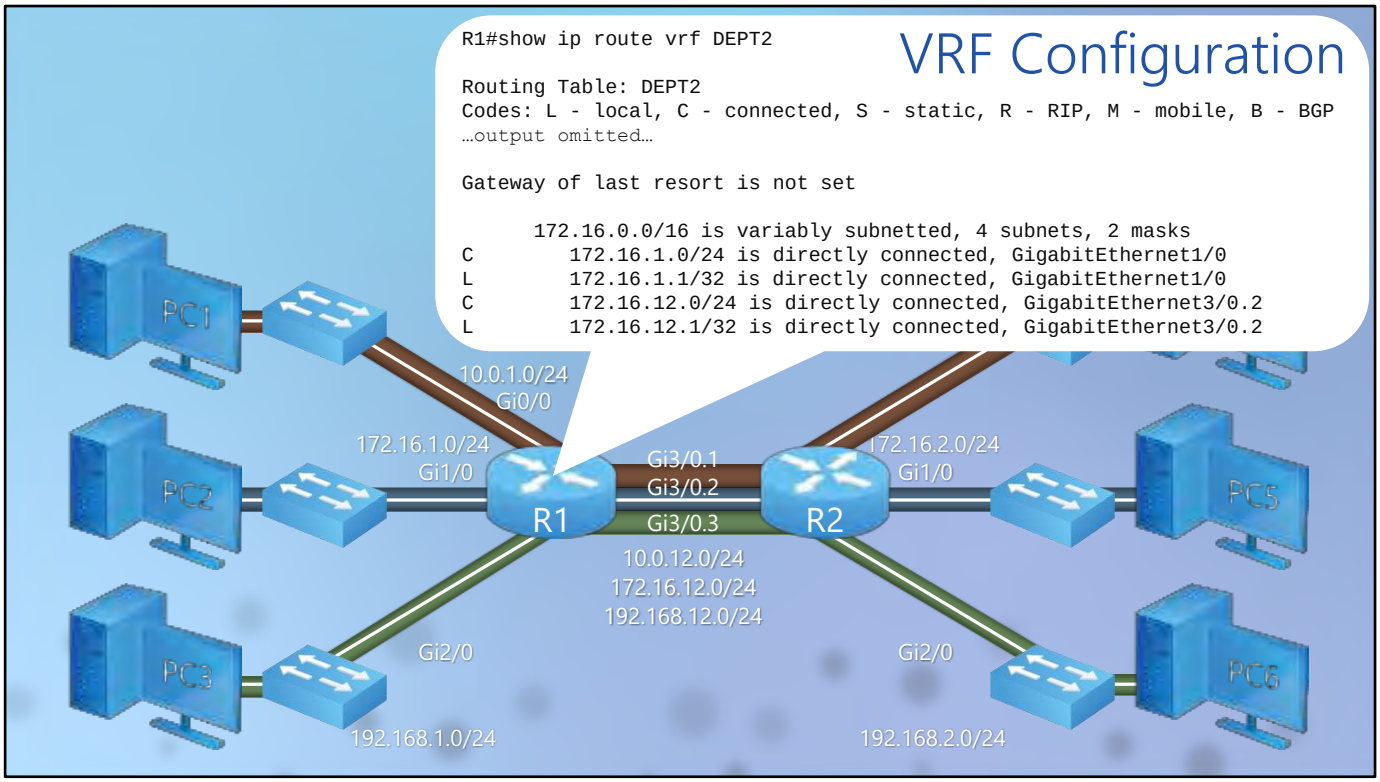
```
R1#show ip route vrf DEPT1

Routing Table: DEPT1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
…output omitted…

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.1.0/24 is directly connected, GigabitEthernet0/0
L        10.0.1.1/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet3/0.1
L        10.0.12.1/32 is directly connected, GigabitEthernet3/0.1
```



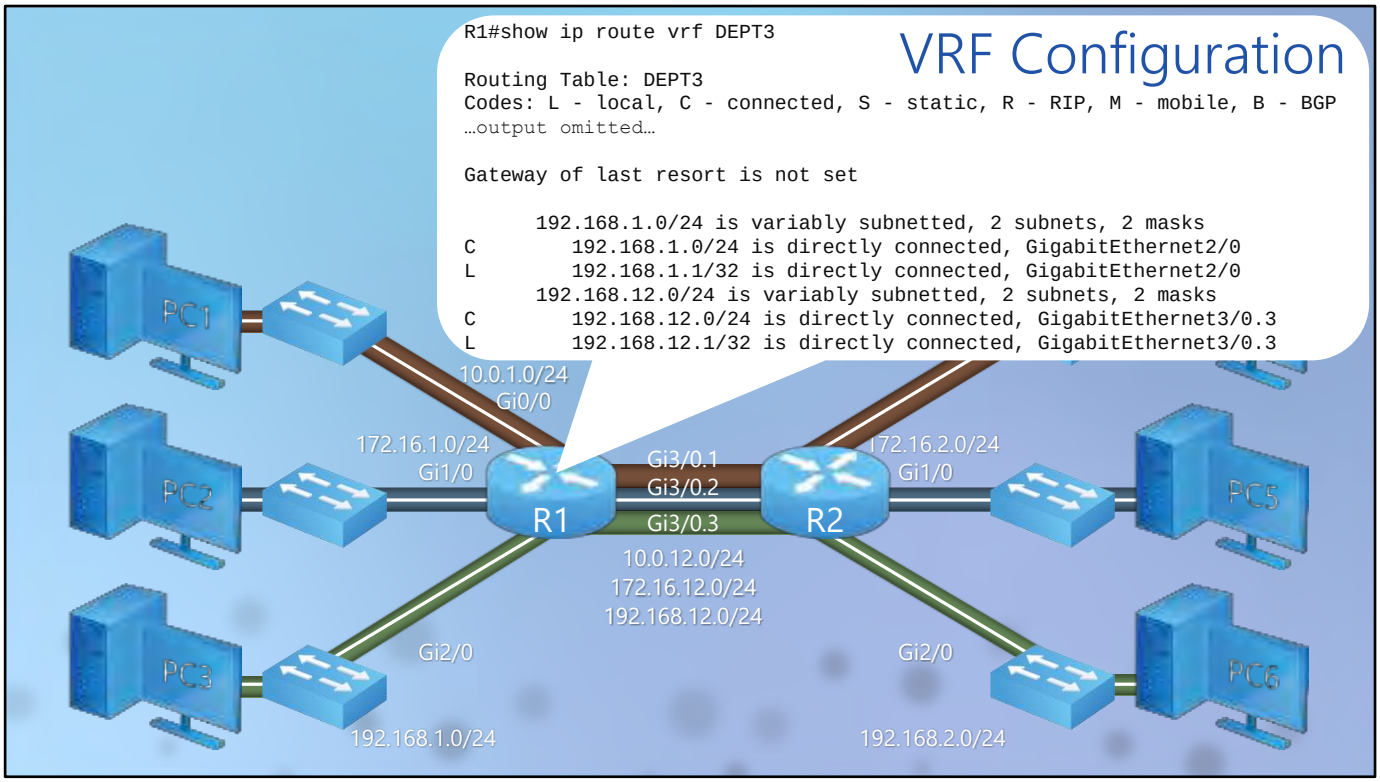
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRF Configuration

```
R1#show ip route vrf DEPT2

Routing Table: DEPT2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
…output omitted…

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet1/0
L        172.16.1.1/32 is directly connected, GigabitEthernet1/0
C        172.16.12.0/24 is directly connected, GigabitEthernet3/0.2
L        172.16.12.1/32 is directly connected, GigabitEthernet3/0.2
```



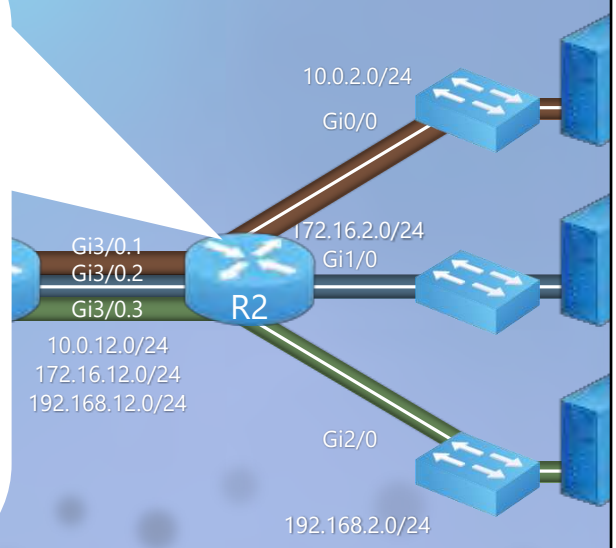
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



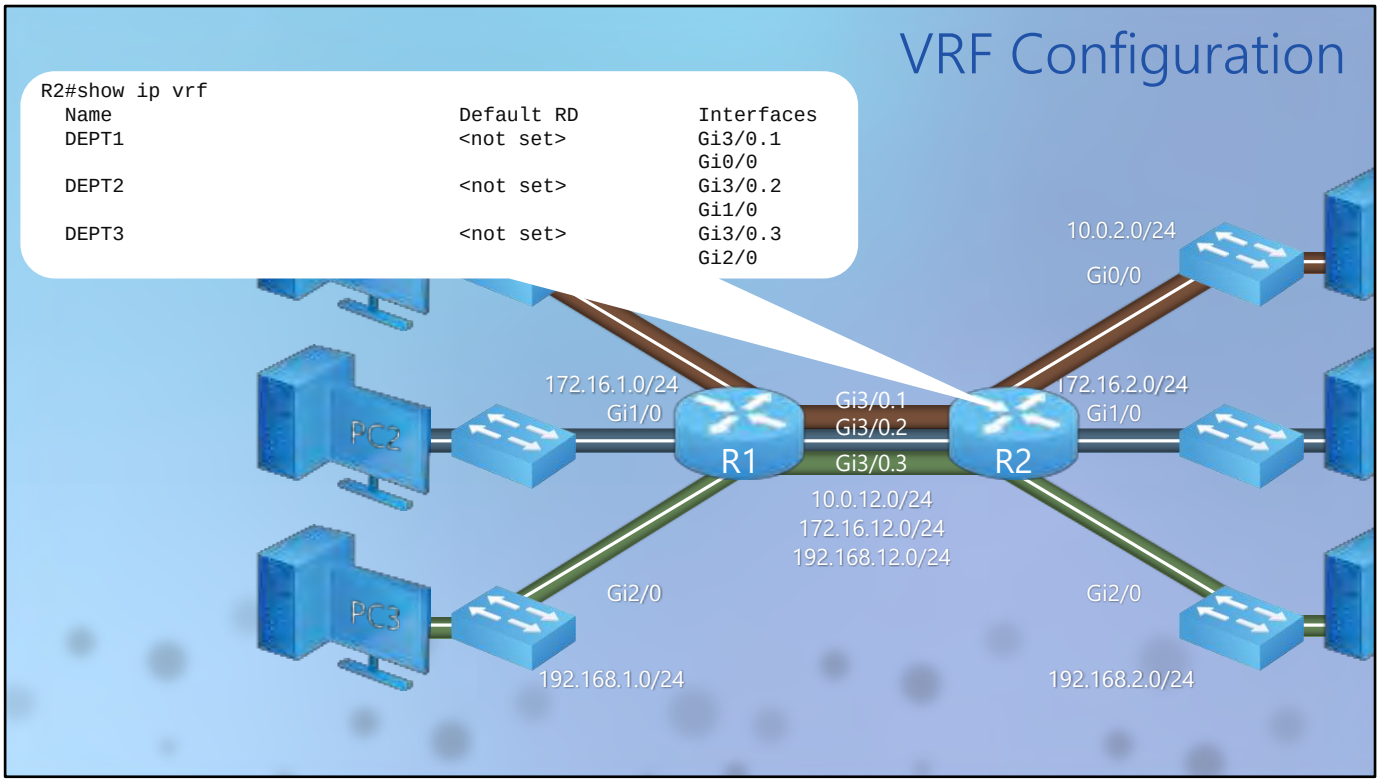
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRF Configuration

```
R2#configure terminal
R2(config)#ip vrf DEPT1
R2(config-vrf)#ip vrf DEPT2
R2(config-vrf)#ip vrf DEPT3
R2(config-vrf)#interface GigabitEthernet0/0
R2(config-if)# ip vrf forwarding DEPT1
R2(config-if)# ip address 10.0.2.2 255.255.255.0
R2(config-if)#interface GigabitEthernet1/0
R2(config-if)# ip vrf forwarding DEPT2
R2(config-if)# ip address 172.16.2.2 255.255.255.0
R2(config-if)#interface GigabitEthernet2/0
R2(config-if)# ip vrf forwarding DEPT3
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)#interface GigabitEthernet3/0.1
R2(config-subif)# encapsulation dot1Q 1
R2(config-subif)# ip vrf forwarding DEPT1
R2(config-subif)# ip address 10.0.12.2 255.255.255.0
R2(config-subif)#interface GigabitEthernet3/0.2
R2(config-subif)# encapsulation dot1Q 2
R2(config-subif)# ip vrf forwarding DEPT2
R2(config-subif)# ip address 172.16.12.2 255.255.255.0
R2(config-subif)#interface GigabitEthernet3/0.3
R2(config-subif)# encapsulation dot1Q 3
R2(config-subif)# ip vrf forwarding DEPT3
R2(config-subif)# ip address 192.168.12.2 255.255.255.0
```



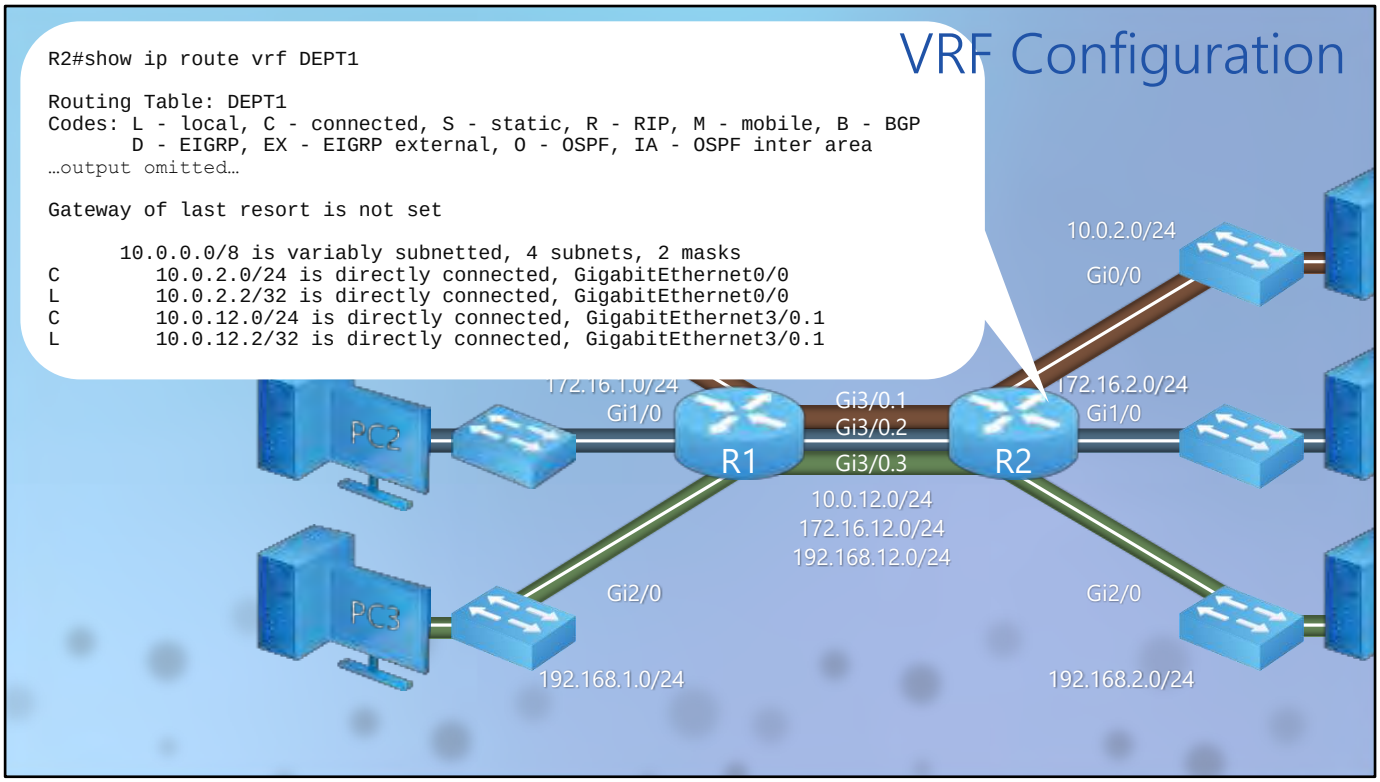
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRF Configuration

```
R2#show ip route vrf DEPT1

Routing Table: DEPT1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
…output omitted…

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.0.2.0/24 is directly connected, GigabitEthernet0/0
L        10.0.2.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet3/0.1
L        10.0.12.2/32 is directly connected, GigabitEthernet3/0.1
```

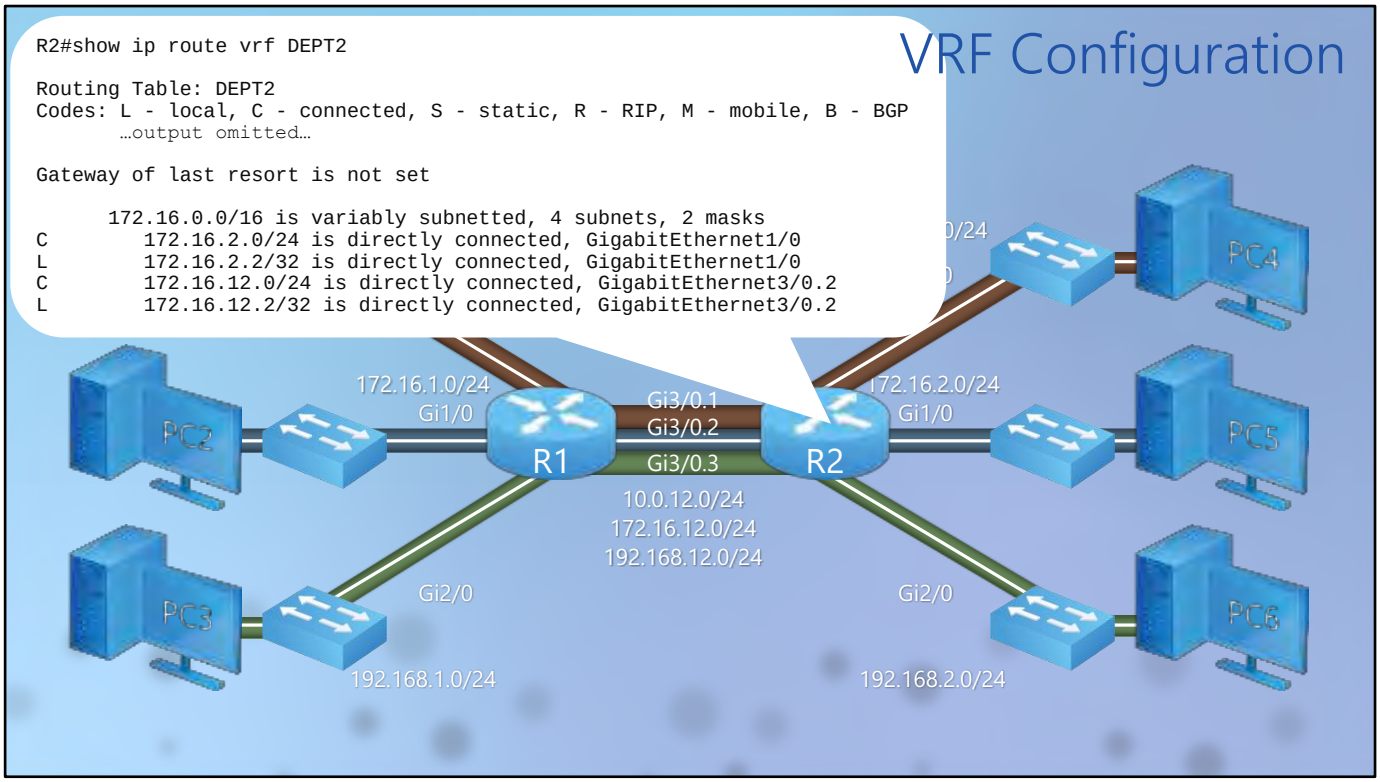


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VRF Configuration

```
R2#show ip route vrf DEPT2

Routing Table: DEPT2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       …output omitted…

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.2.0/24 is directly connected, GigabitEthernet1/0
L        172.16.2.2/32 is directly connected, GigabitEthernet1/0
C        172.16.12.0/24 is directly connected, GigabitEthernet3/0.2
L        172.16.12.2/32 is directly connected, GigabitEthernet3/0.2
```

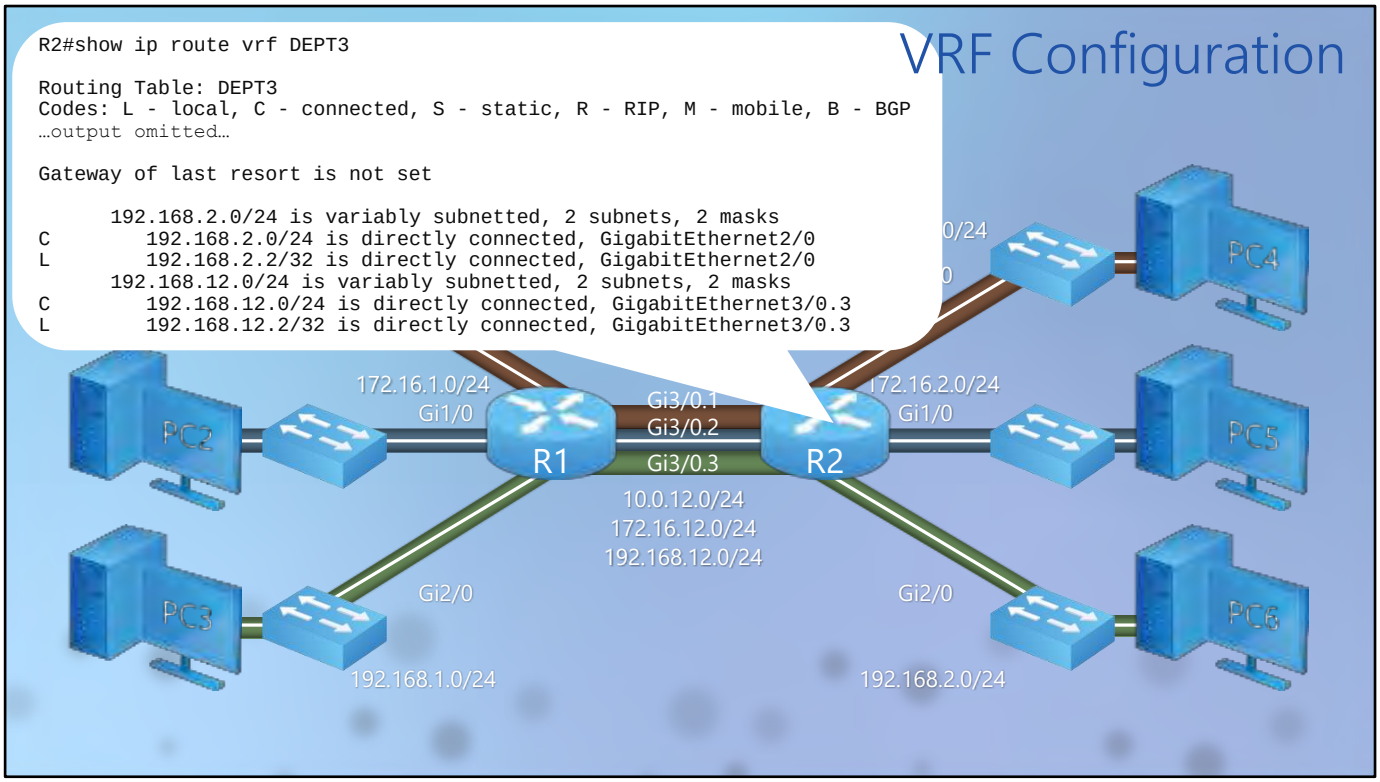


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

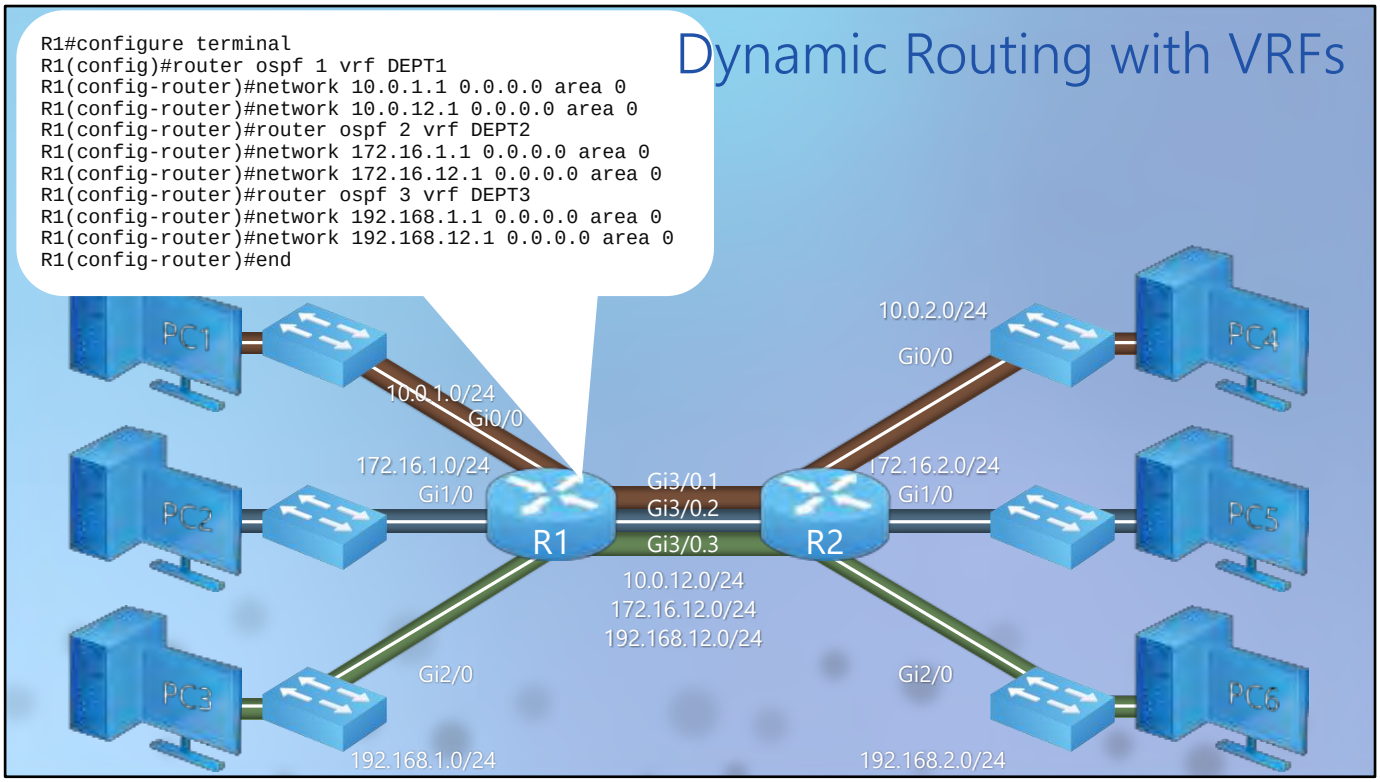
VRF Configuration

```
R2#show ip route vrf DEPT3

Routing Table: DEPT3
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
…output omitted…

Gateway of last resort is not set

      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet2/0
L        192.168.2.2/32 is directly connected, GigabitEthernet2/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet3/0.3
L        192.168.12.2/32 is directly connected, GigabitEthernet3/0.3
```

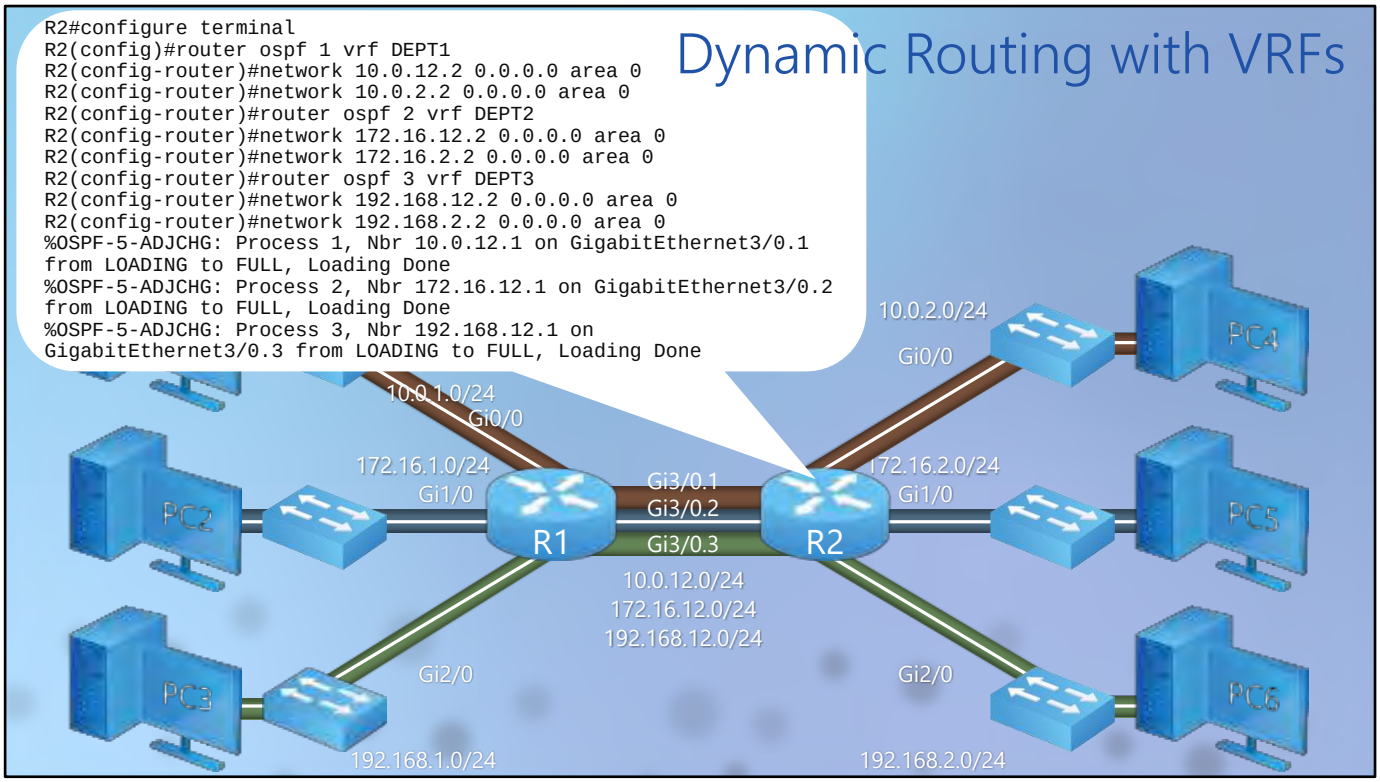


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

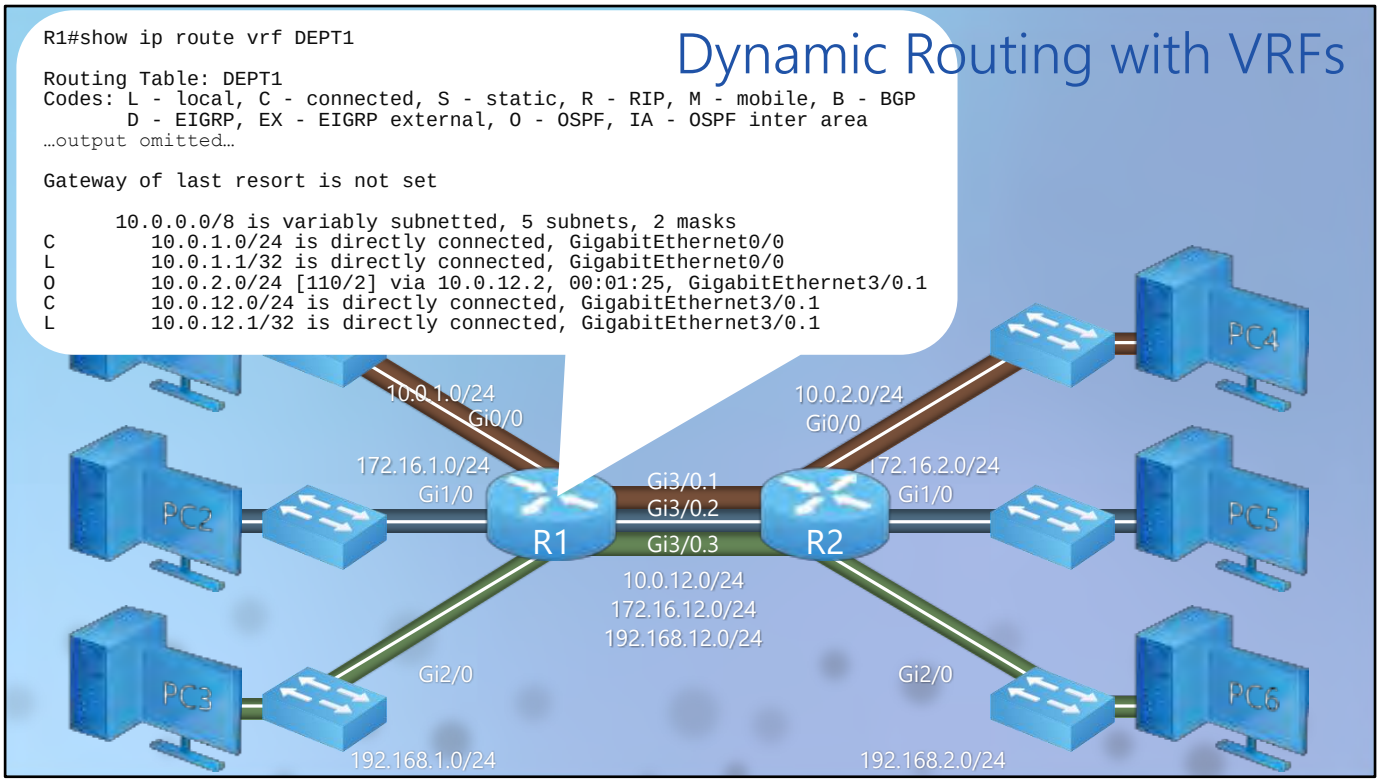


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Routing with VRFs

```
R1#show ip route vrf DEPT1

Routing Table: DEPT1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
…output omitted…

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.0.1.0/24 is directly connected, GigabitEthernet0/0
L        10.0.1.1/32 is directly connected, GigabitEthernet0/0
O        10.0.2.0/24 [110/2] via 10.0.12.2, 00:01:25, GigabitEthernet3/0.1
C        10.0.12.0/24 is directly connected, GigabitEthernet3/0.1
L        10.0.12.1/32 is directly connected, GigabitEthernet3/0.1
```

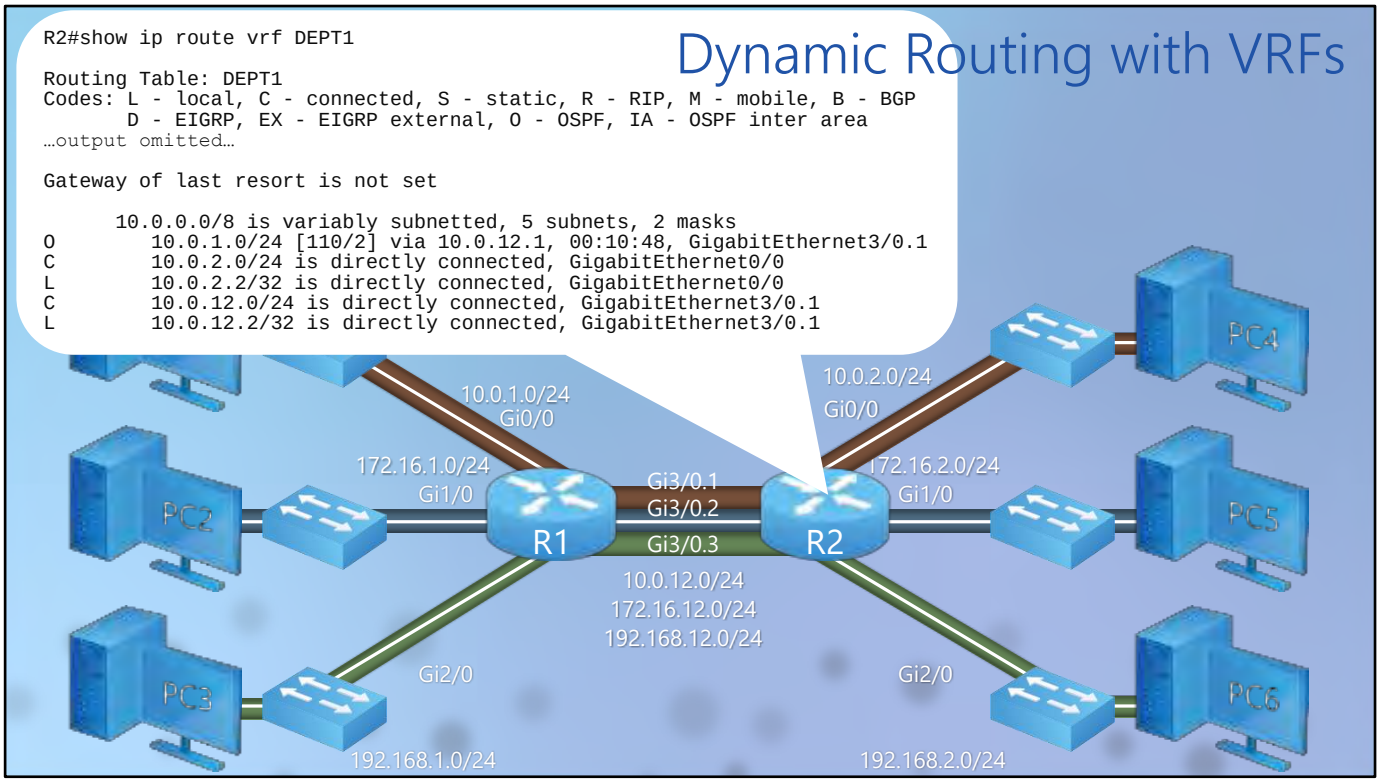


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Routing with VRFs

```
R2#show ip route vrf DEPT1

Routing Table: DEPT1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
…output omitted…

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O        10.0.1.0/24 [110/2] via 10.0.12.1, 00:10:48, GigabitEthernet3/0.1
C        10.0.2.0/24 is directly connected, GigabitEthernet0/0
L        10.0.2.2/32 is directly connected, GigabitEthernet0/0
C        10.0.12.0/24 is directly connected, GigabitEthernet3/0.1
L        10.0.12.2/32 is directly connected, GigabitEthernet3/0.1
```

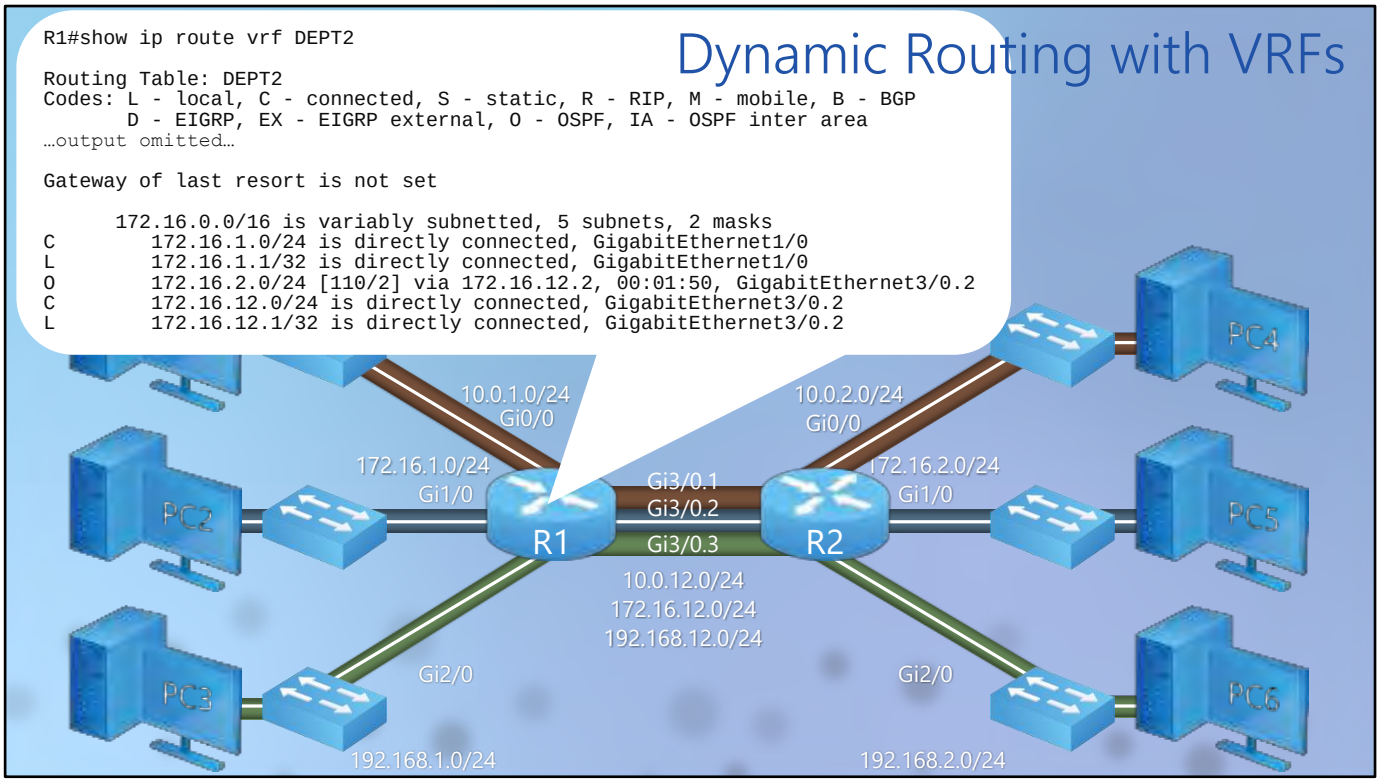


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Routing with VRFs

```
R1#show ip route vrf DEPT2

Routing Table: DEPT2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
…output omitted…

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet1/0
L        172.16.1.1/32 is directly connected, GigabitEthernet1/0
O        172.16.2.0/24 [110/2] via 172.16.12.2, 00:01:50, GigabitEthernet3/0.2
C        172.16.12.0/24 is directly connected, GigabitEthernet3/0.2
L        172.16.12.1/32 is directly connected, GigabitEthernet3/0.2
```

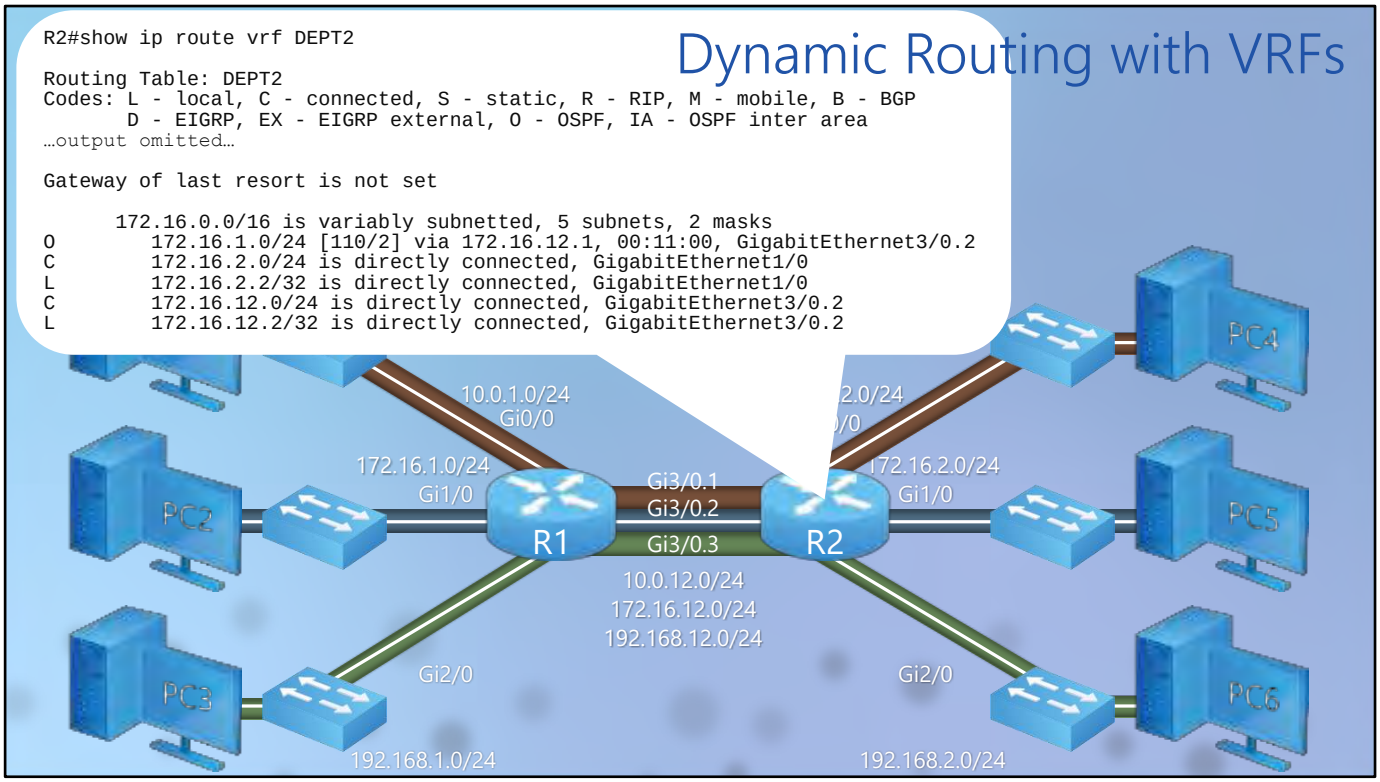


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Routing with VRFs

```
R2#show ip route vrf DEPT2

Routing Table: DEPT2
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
…output omitted…

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
O        172.16.1.0/24 [110/2] via 172.16.12.1, 00:11:00, GigabitEthernet3/0.2
C        172.16.2.0/24 is directly connected, GigabitEthernet1/0
L        172.16.2.2/32 is directly connected, GigabitEthernet1/0
C        172.16.12.0/24 is directly connected, GigabitEthernet3/0.2
L        172.16.12.2/32 is directly connected, GigabitEthernet3/0.2
```

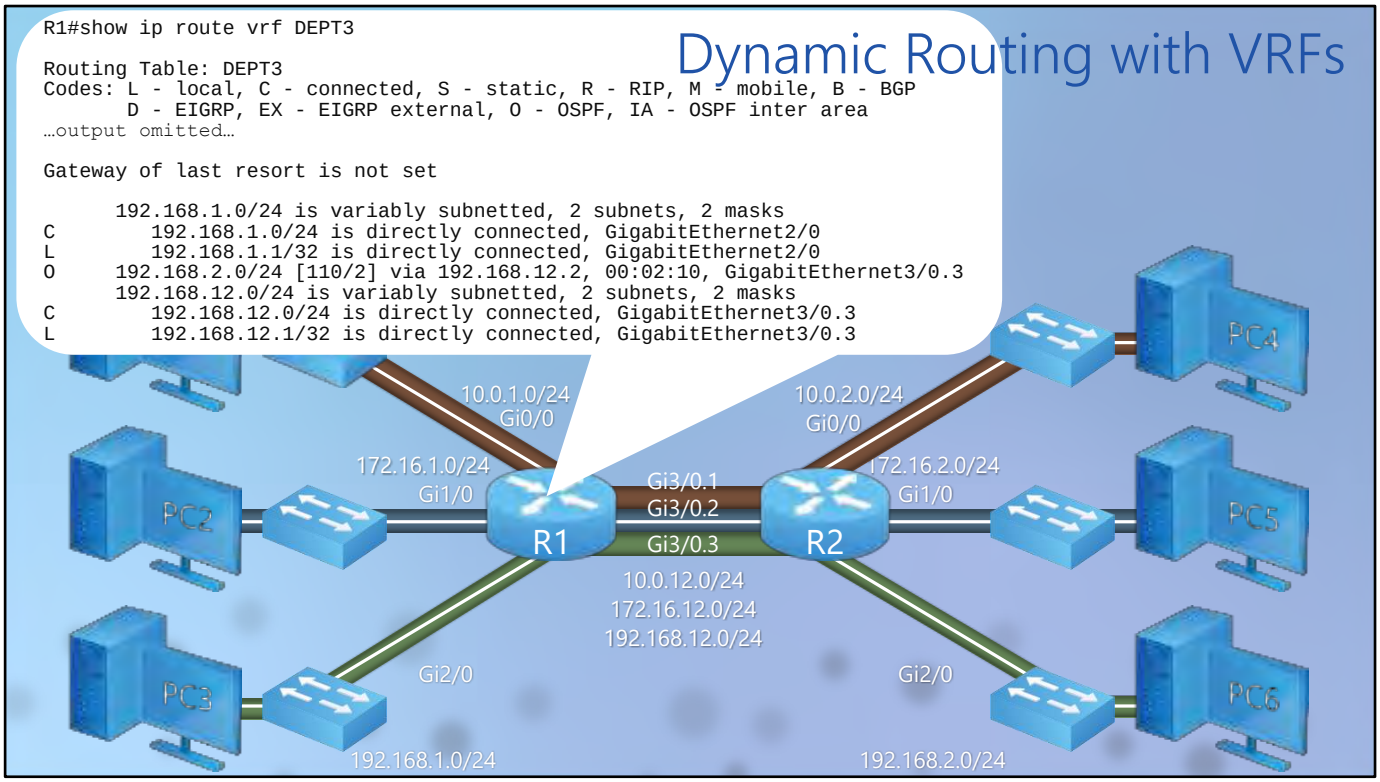


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Routing with VRFs

```
R1#show ip route vrf DEPT3

Routing Table: DEPT3
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
…output omitted…

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet2/0
L        192.168.1.1/32 is directly connected, GigabitEthernet2/0
O     192.168.2.0/24 [110/2] via 192.168.12.2, 00:02:10, GigabitEthernet3/0.3
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet3/0.3
L        192.168.12.1/32 is directly connected, GigabitEthernet3/0.3
```

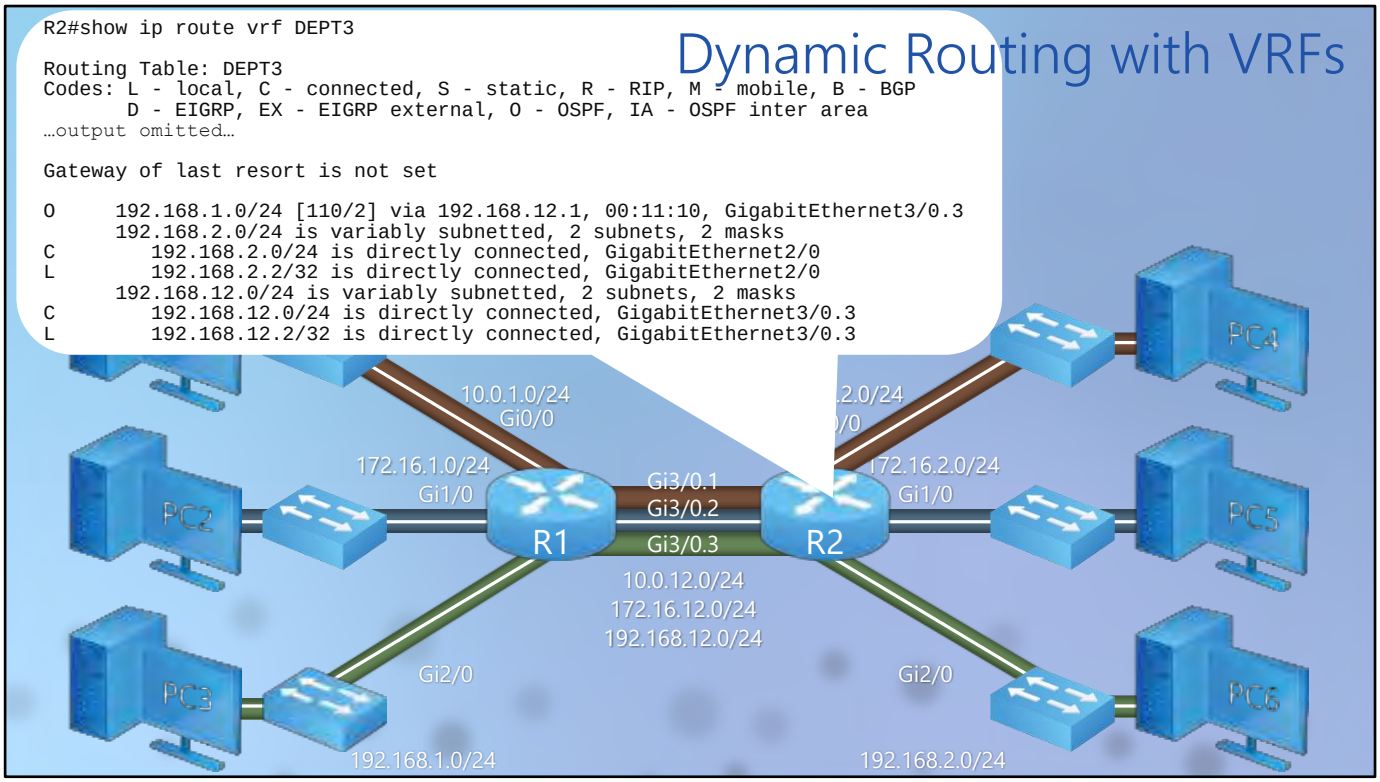


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

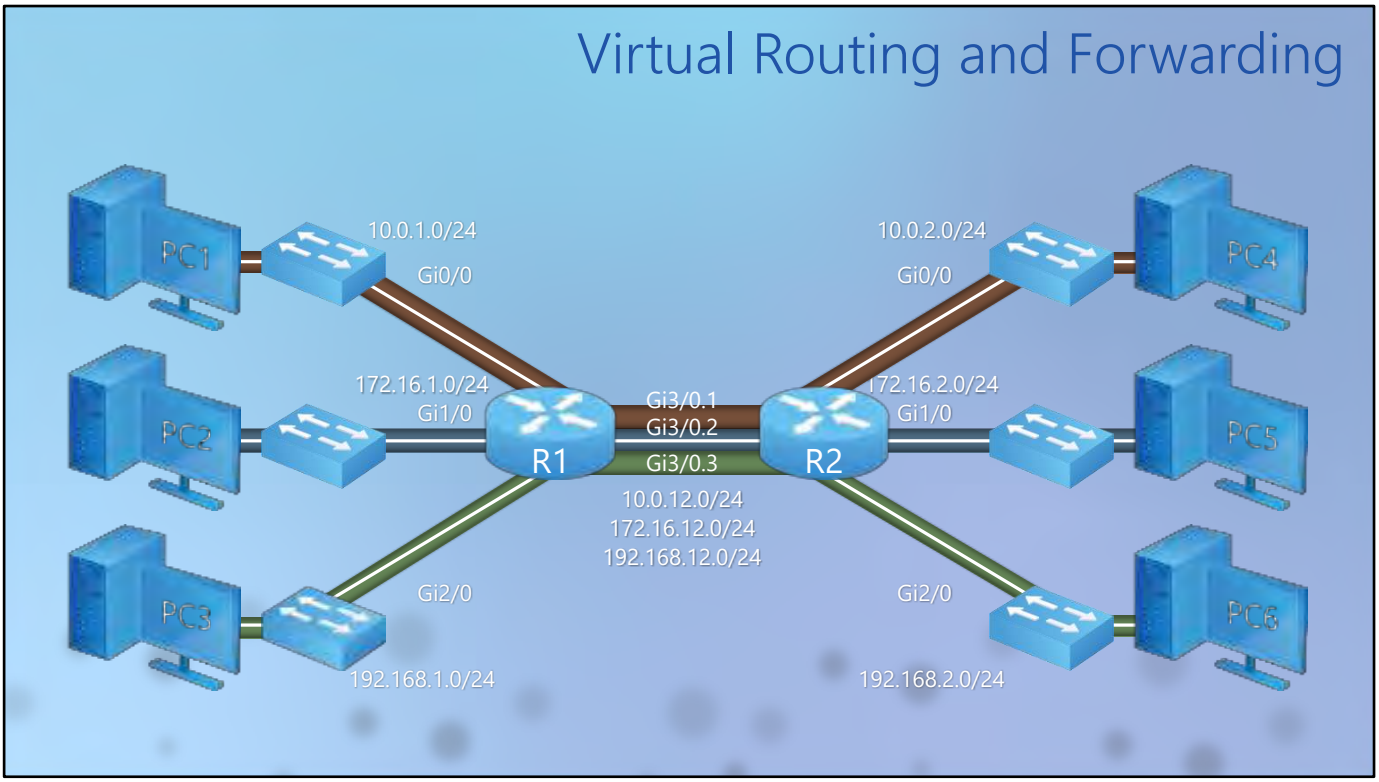
Dynamic Routing with VRFs

```
R2#show ip route vrf DEPT3

Routing Table: DEPT3
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
…output omitted…

Gateway of last resort is not set

O     192.168.1.0/24 [110/2] via 192.168.12.1, 00:11:10, GigabitEthernet3/0.3
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, GigabitEthernet2/0
L        192.168.2.2/32 is directly connected, GigabitEthernet2/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, GigabitEthernet3/0.3
L        192.168.12.2/32 is directly connected, GigabitEthernet3/0.3
```

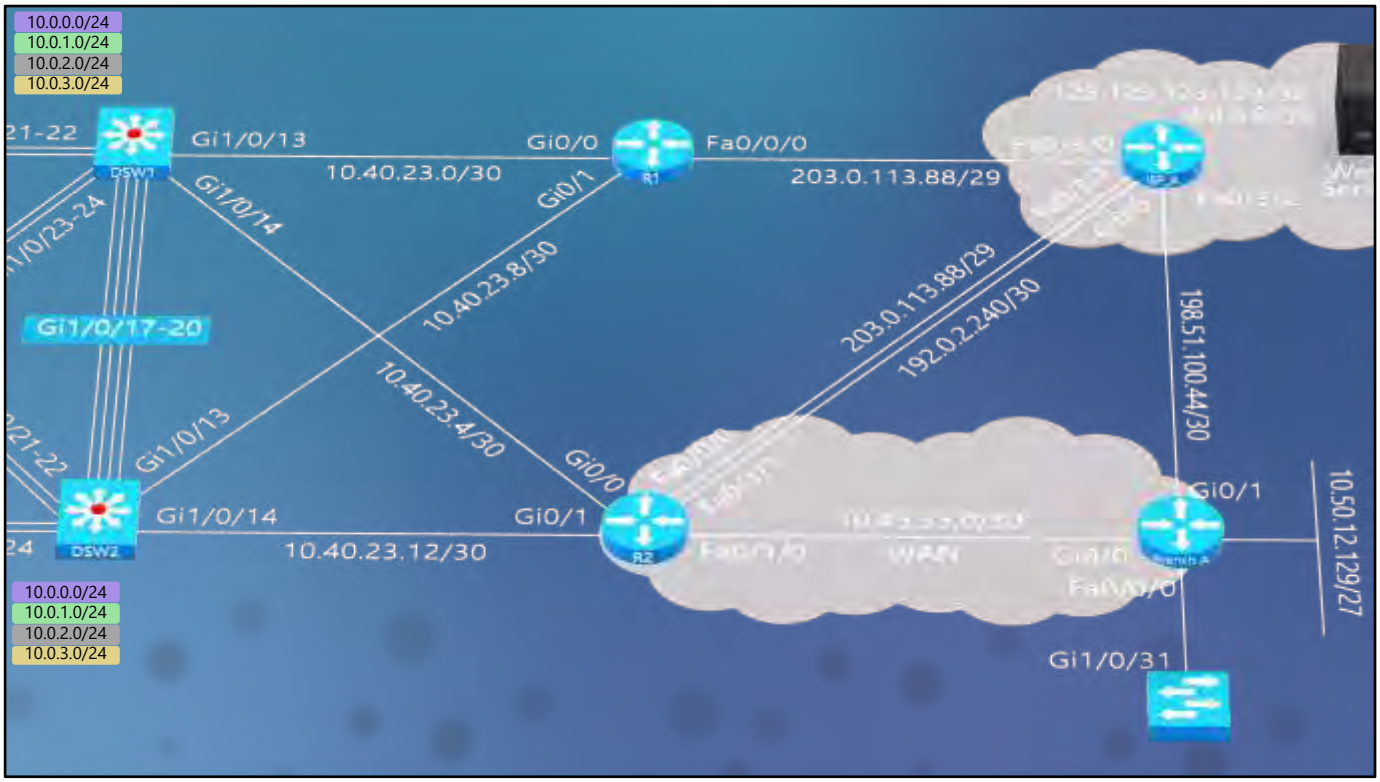


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

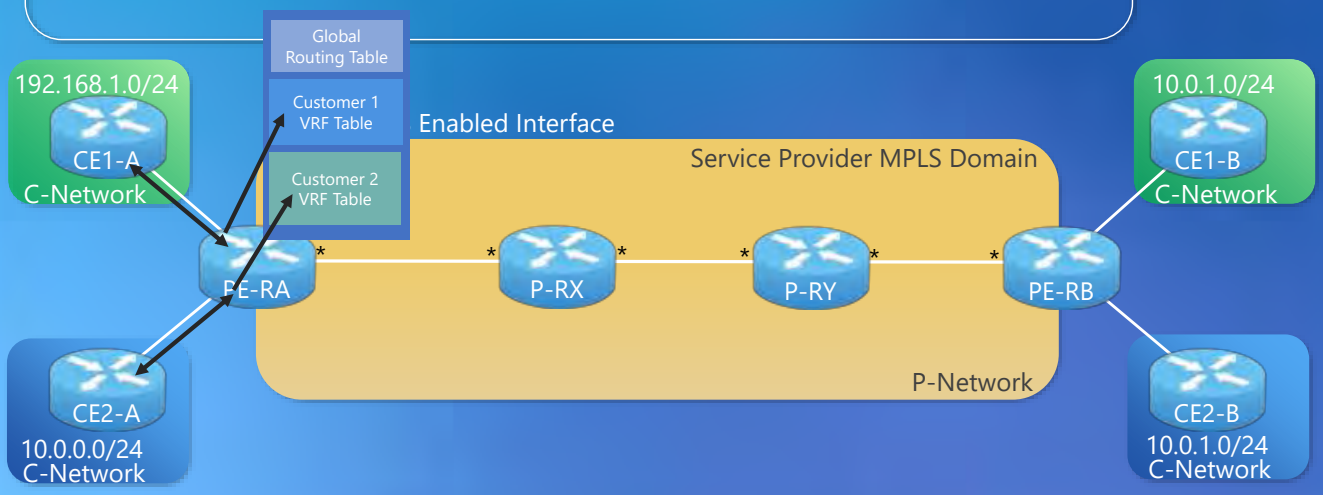


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

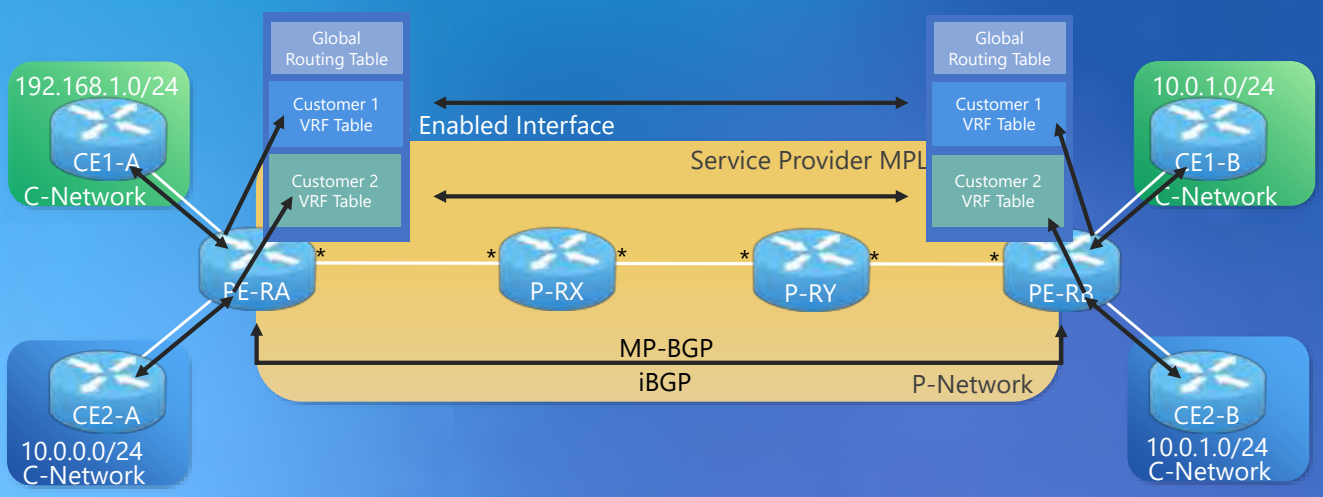
MPLS L3 VPN PE Routers

Use VRFs to isolate routes learned from CE routers



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

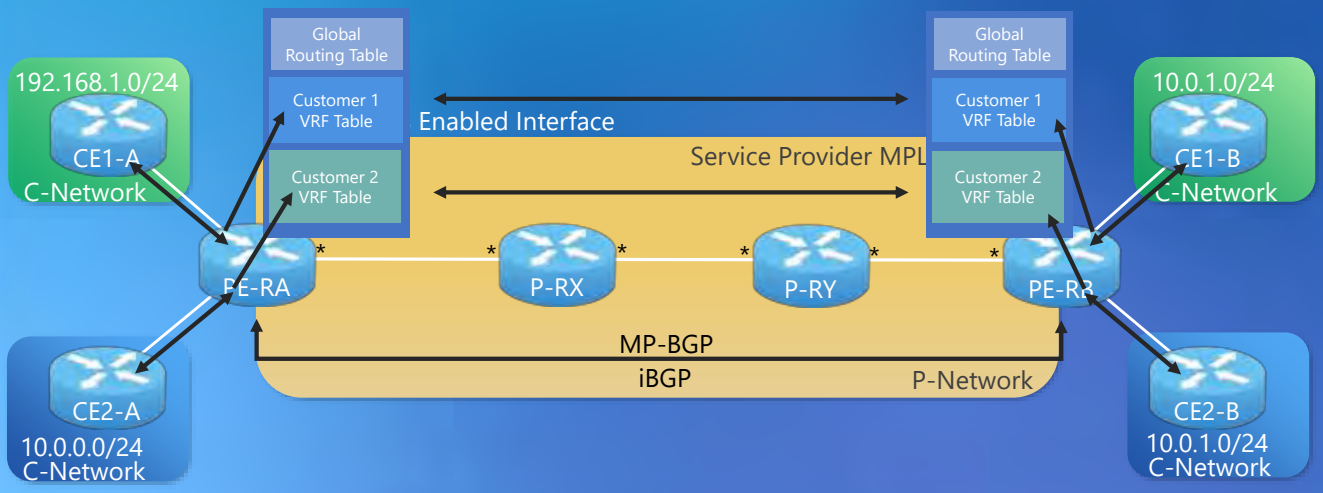
MPLS L3 VPN Route Distinguisher



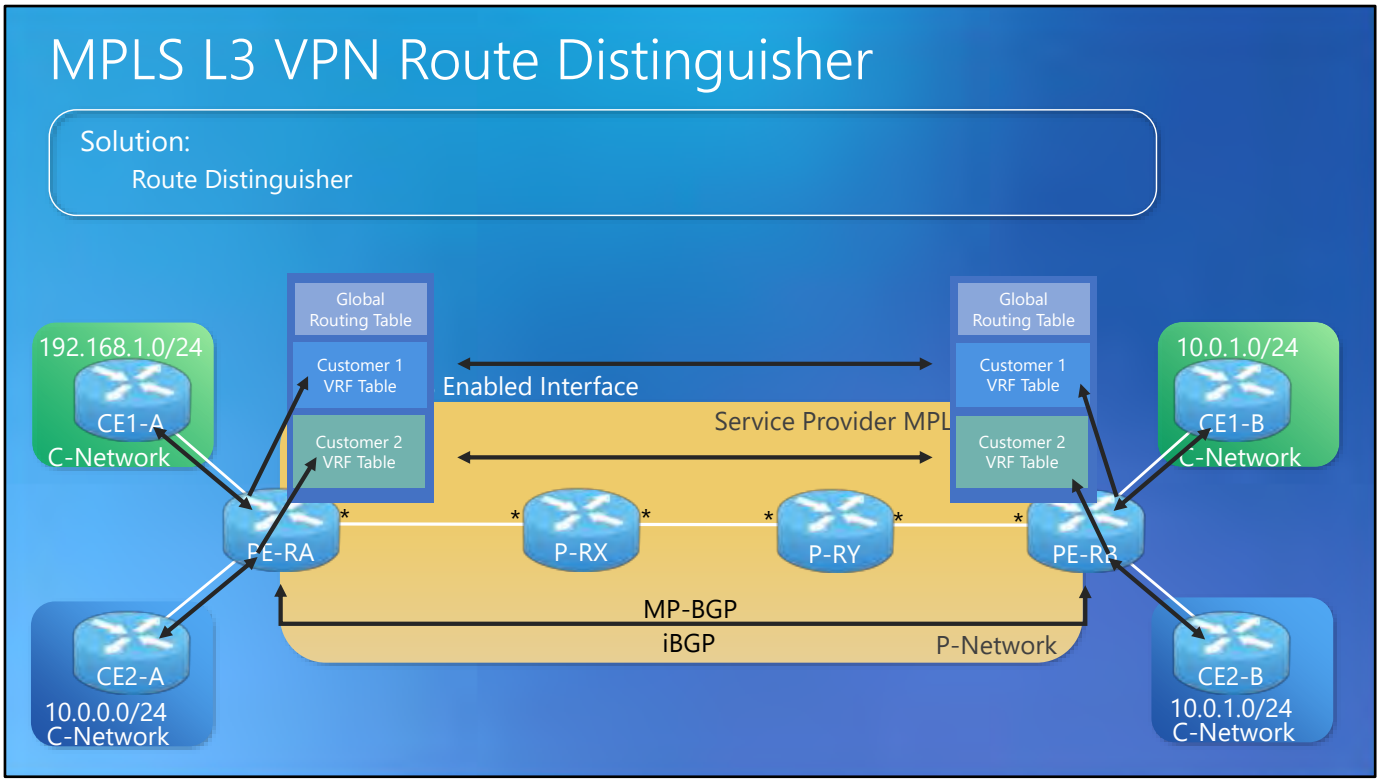
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Distinguisher

Problem:
Overlapping address spaces



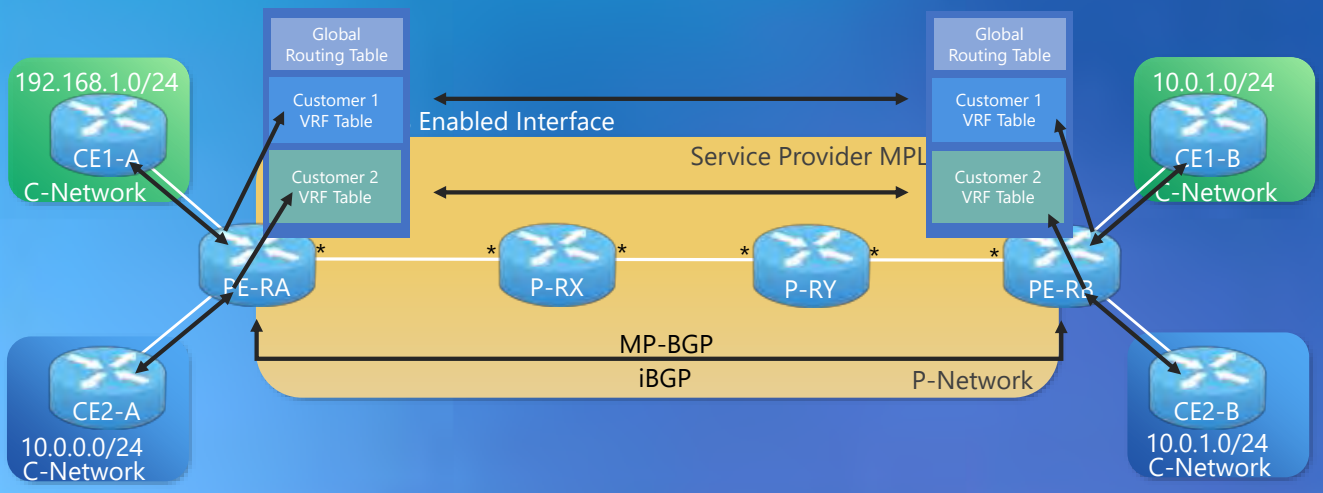
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Distinguisher

A 64-bit ID added to the IPv4/6 address to make it unique
Also known as the VPN identifier



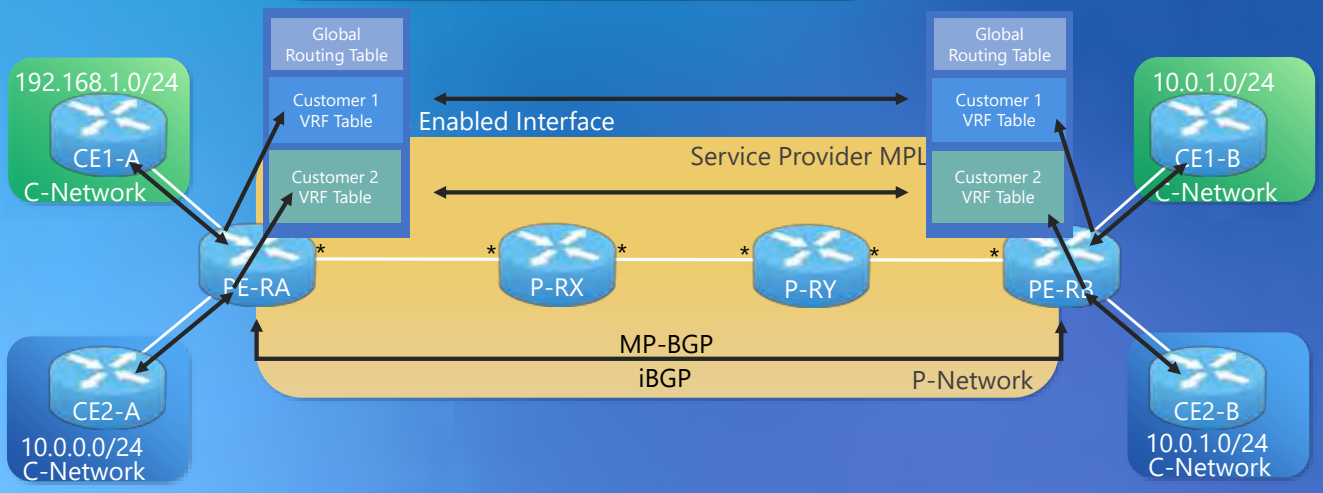
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Distinguisher

A 64-bit ID added to the IPv4/6 address to make it unique

Also known as t

Route Distinguisher (8bytes)	IPv4 Address (4 Bytes)	= VPNv4 Address
Route Distinguisher (8bytes)	IPv4 Address (16 Bytes)	= VPNv6 Address

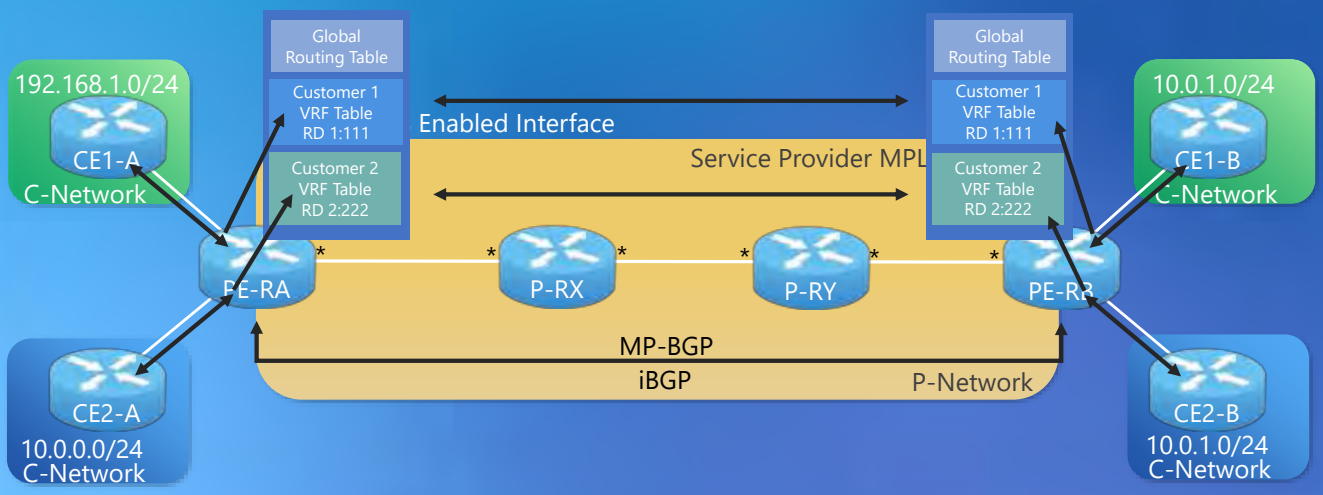


©2023 by StormWind LLC. All rights reserved.

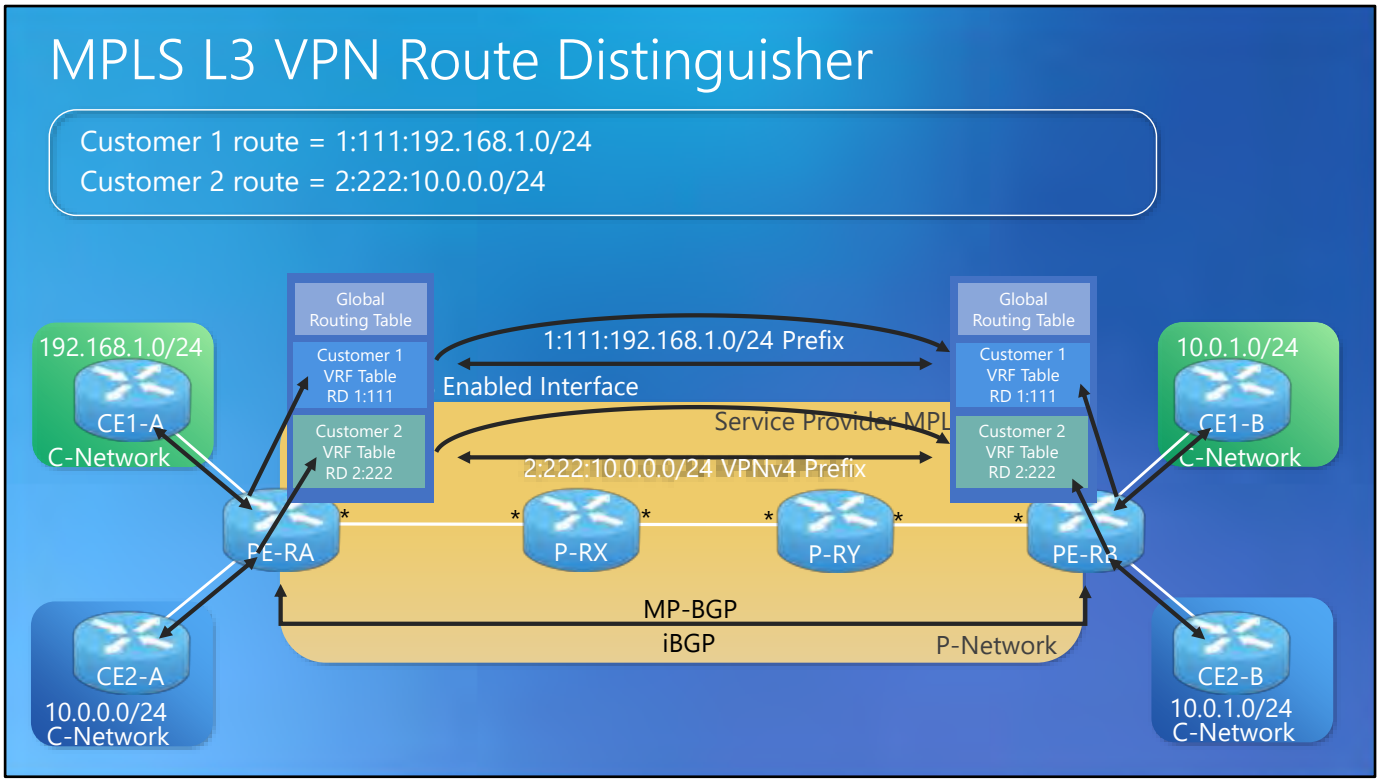
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Distinguisher

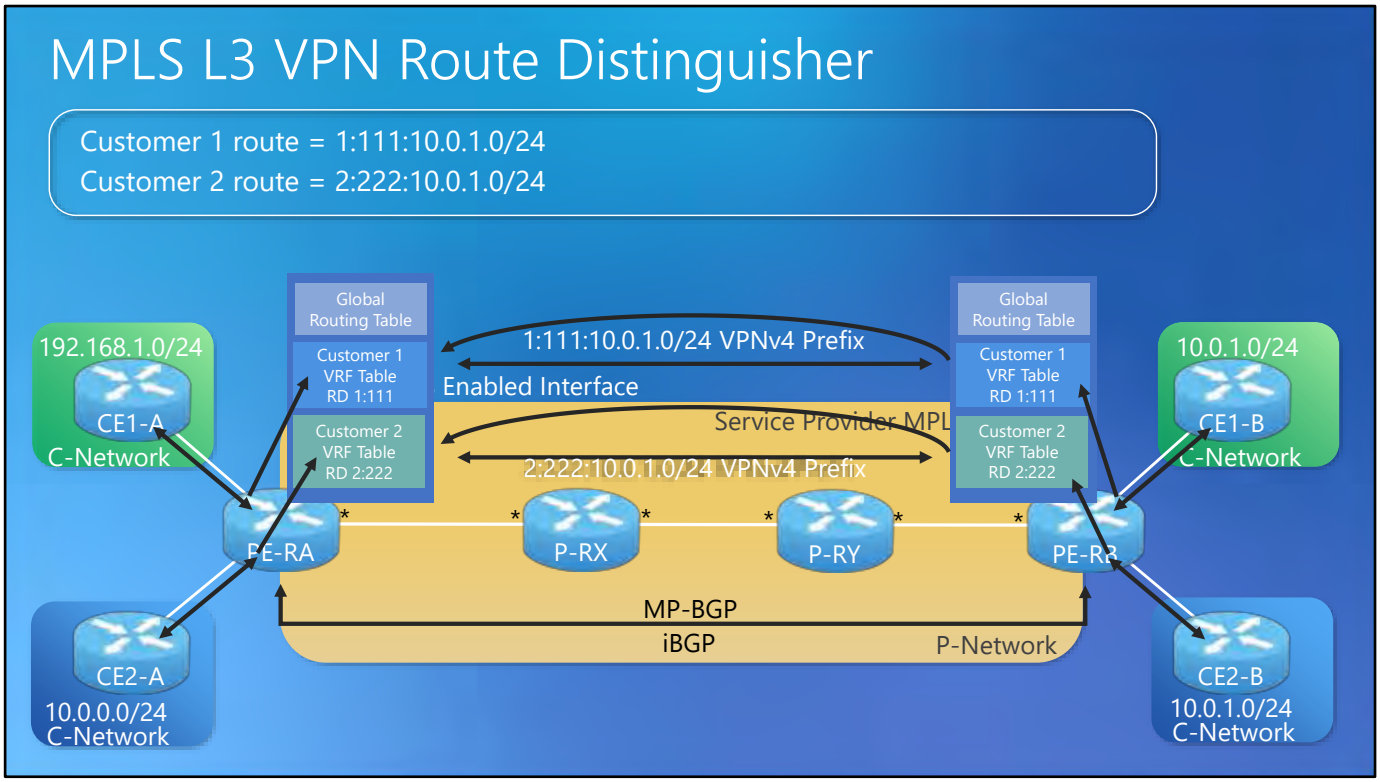
RD 1:111 is assigned to Customer 1 VRF
RD 2:222 is assigned to Customer 2 VRF



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



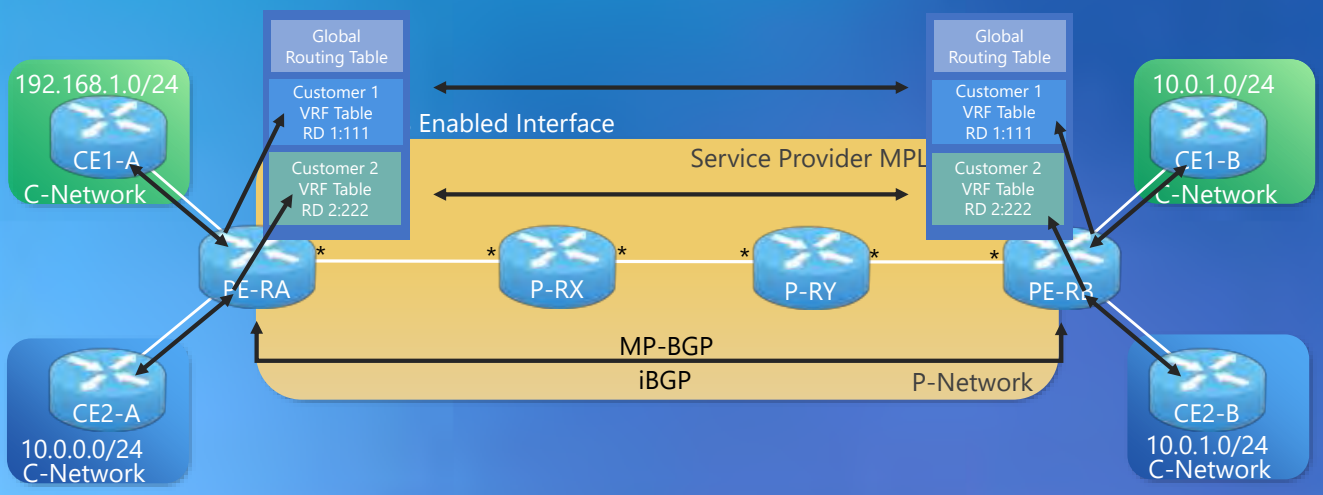
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Target

How do we ensure isolation when sharing routes?

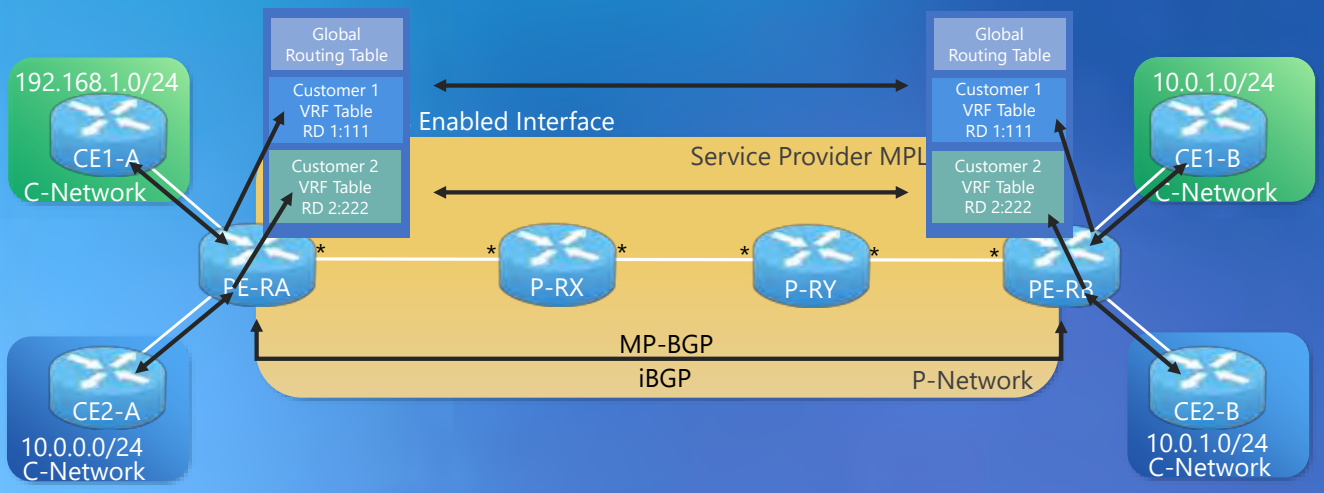


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Target

How do we ensure isolation when sharing routes?

Route Targets

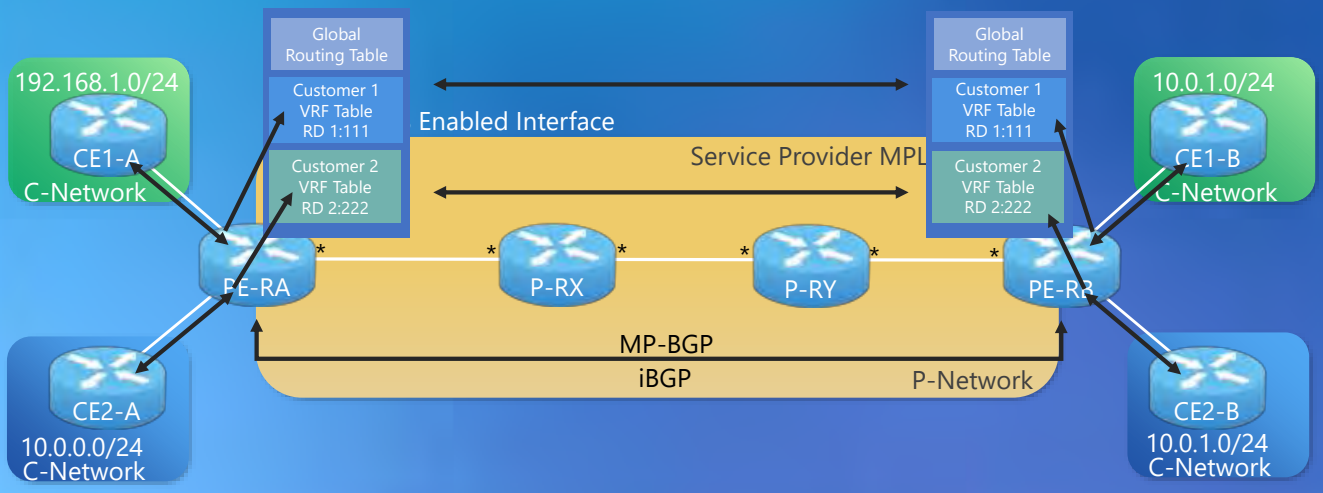


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Target

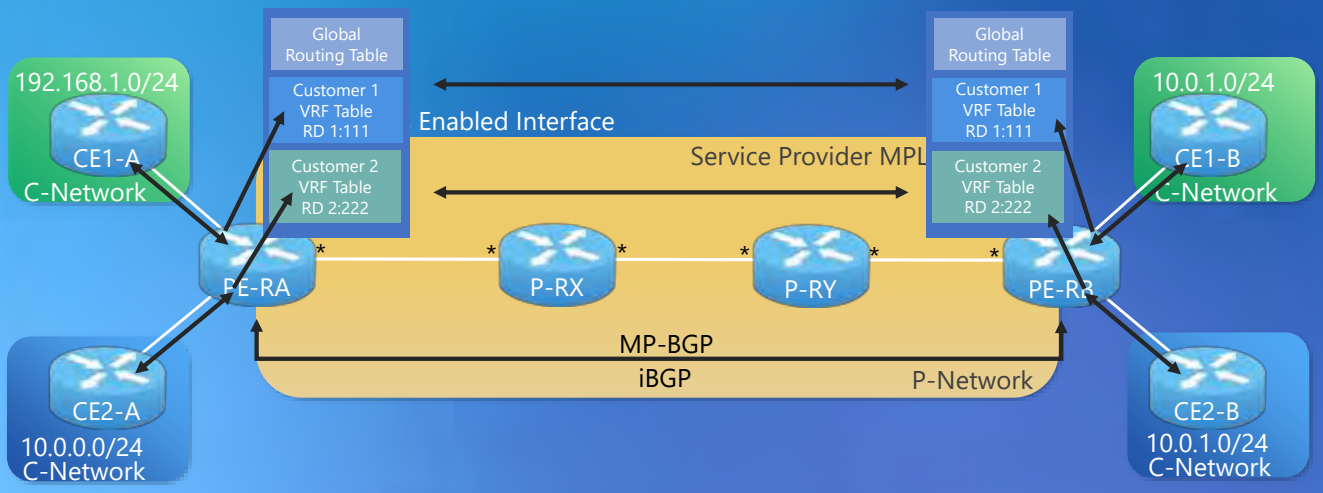
They identify the VPN membership of the route to control import and export functions.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Target

Route targets have:
- Import and Export values

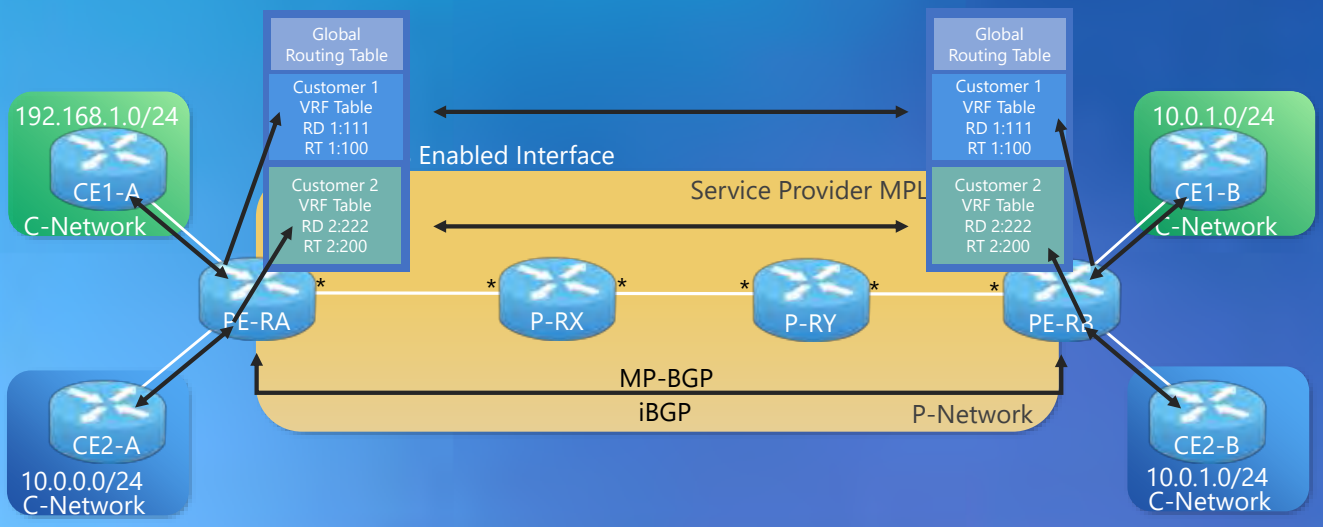


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MPLS L3 VPN Route Target

Import value

Associated with each VRF and identifies the routes to import



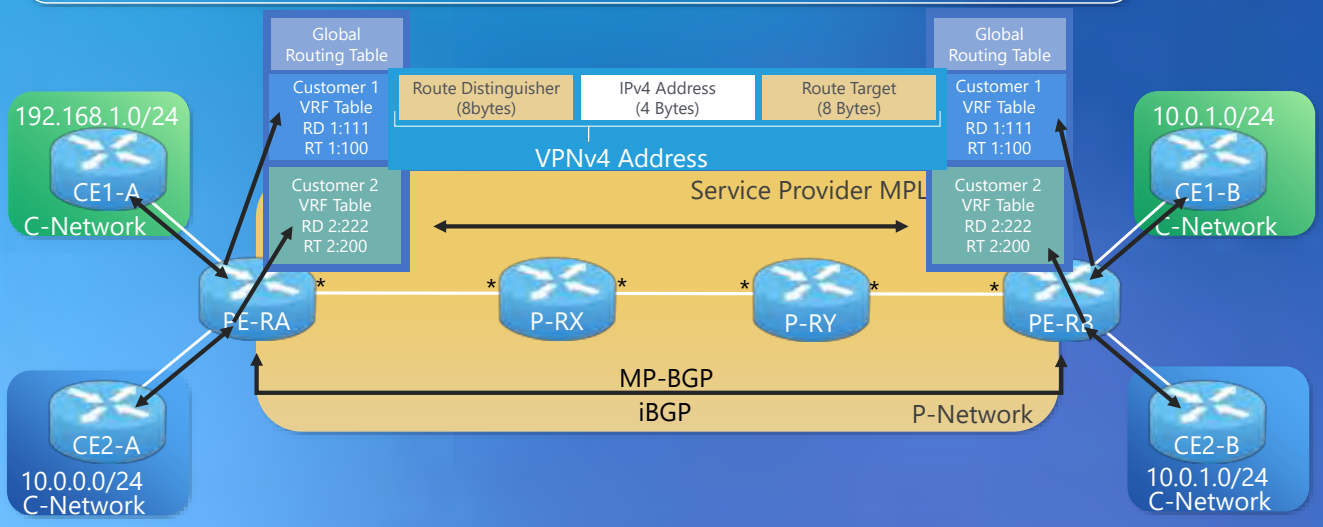
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

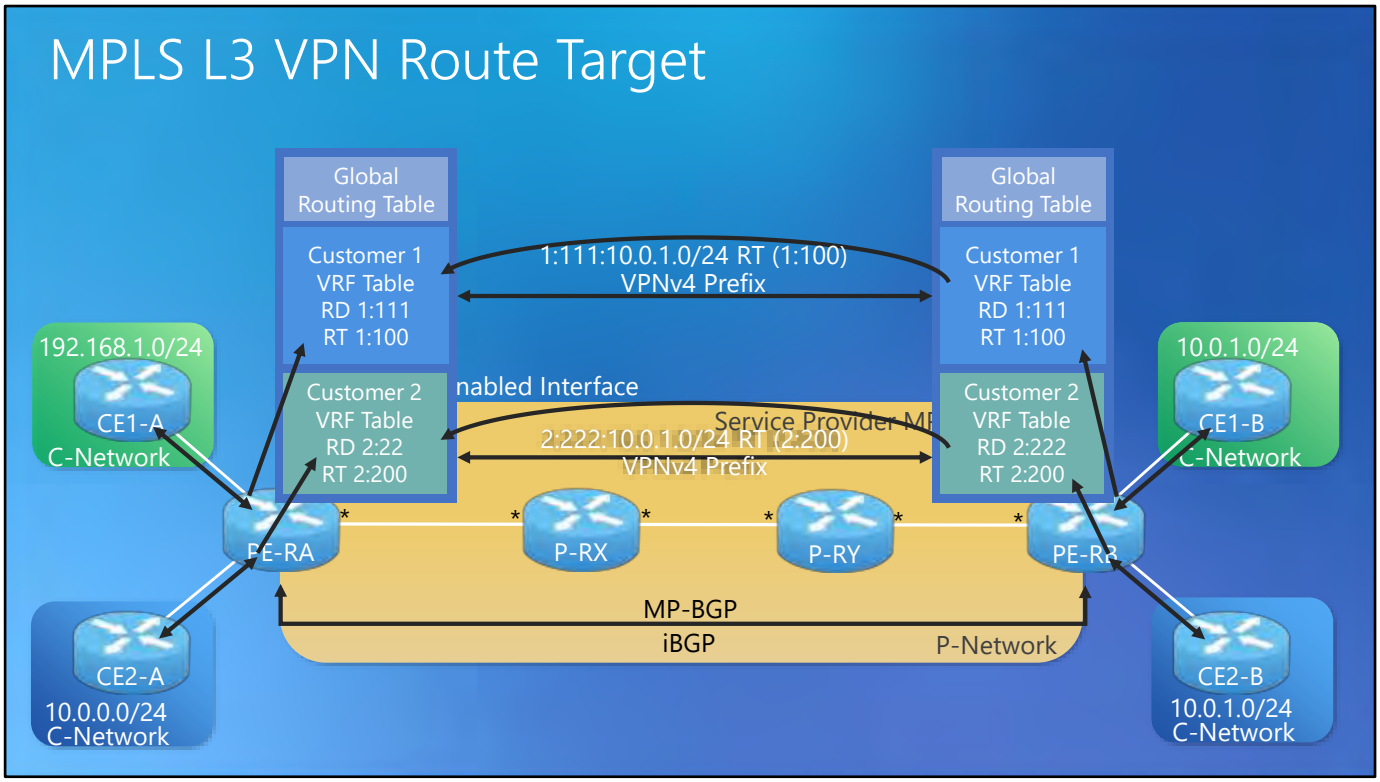
MPLS L3 VPN Route Target

Export value

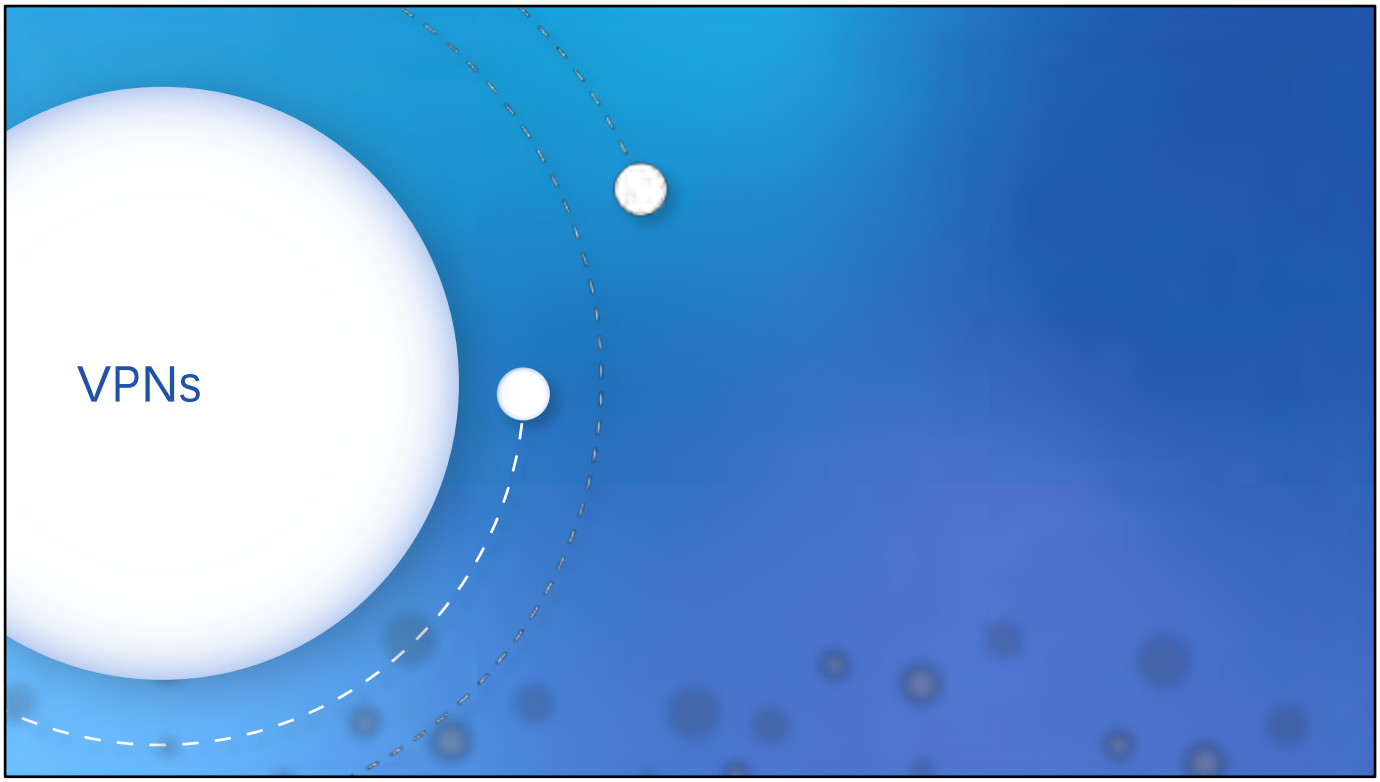
- Attached to route when converted to a VPNv4/6 address
- Identifies the target where it is going



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

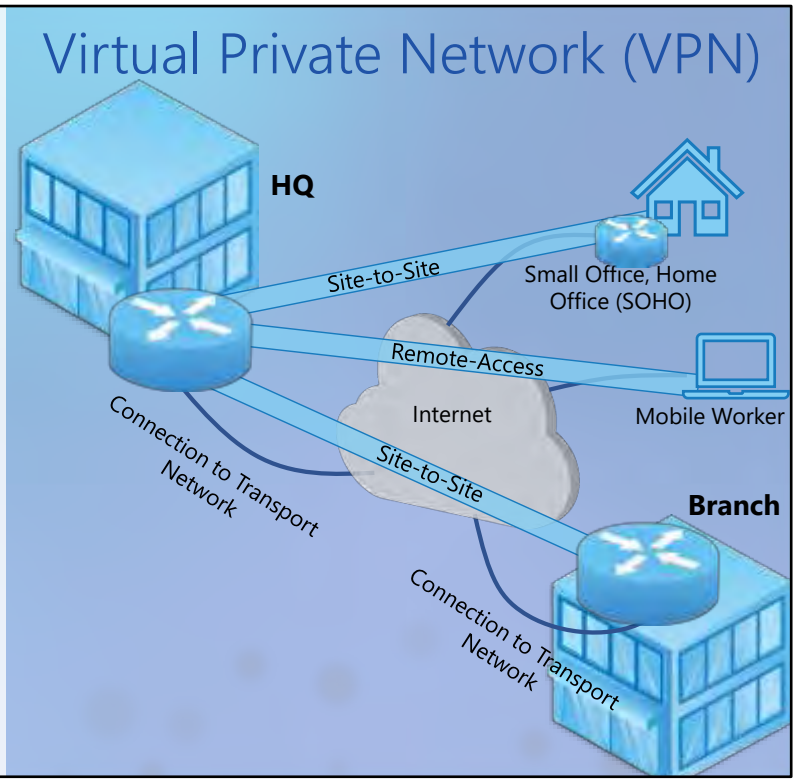


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE Tunnel Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Tunnel that virtually connects two non-directly connected points, directly to each other.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

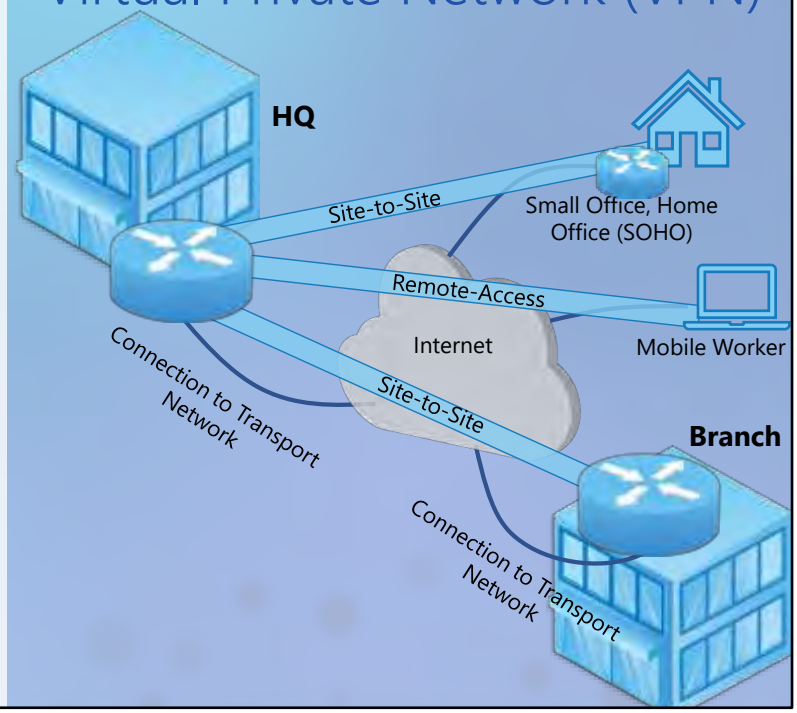
Virtual Private Network (VPN)

Layer 2 examples:

VLANs, QinQ, Frame Relay PVCs, ATM PVCs, VPLS, VPWS

Layer 3 examples:

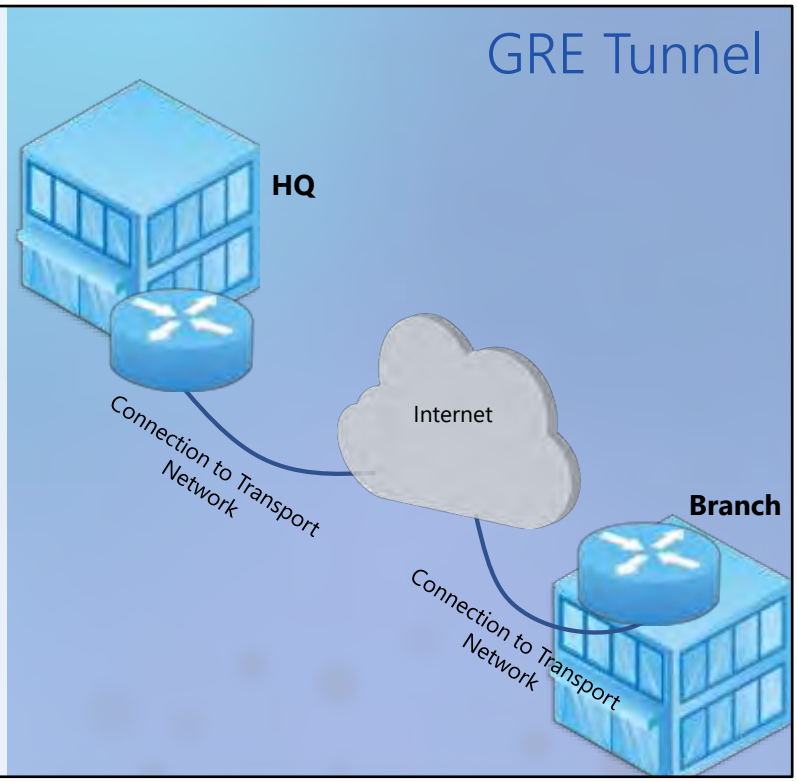
GRE, MPLS Layer 3 VPNS, IPSec



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE

Used to create **Point to Point** links over IP networks



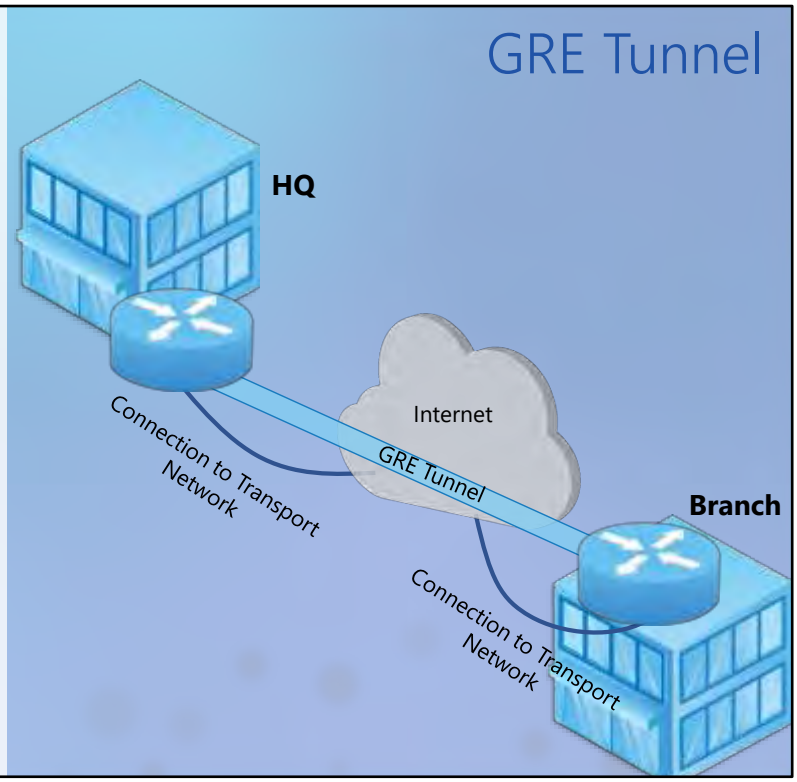
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE

Used to create **Point to Point** links over IP networks

Utilizes IP **protocol 47**

Originally designed by Cisco, but now defined by **RFC 2784**



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

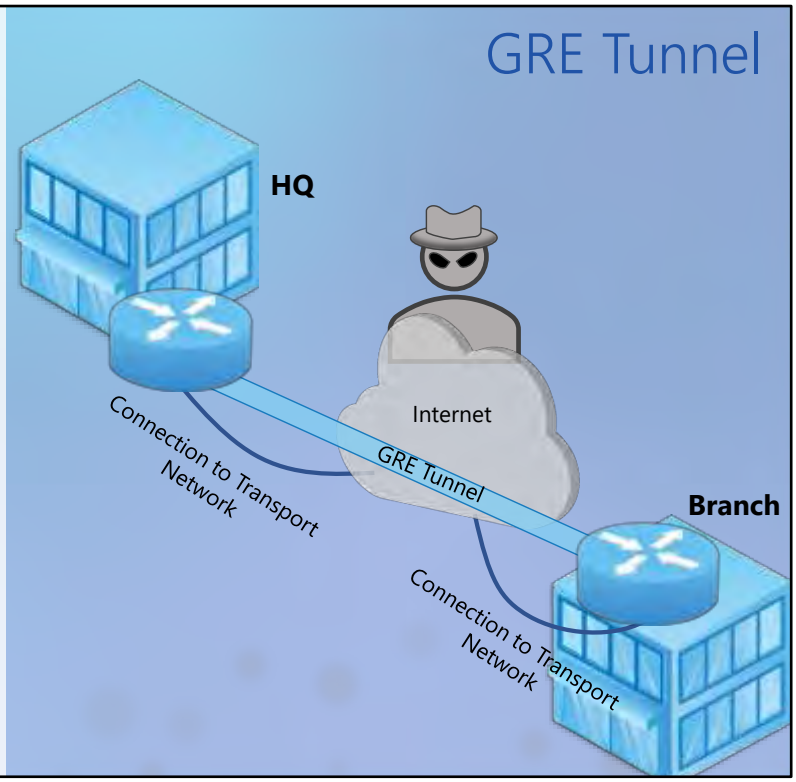
GRE

Used to create **Point to Point** links over IP networks

Utilizes IP **protocol 47**

Originally designed by Cisco, but now defined by **RFC 2784**

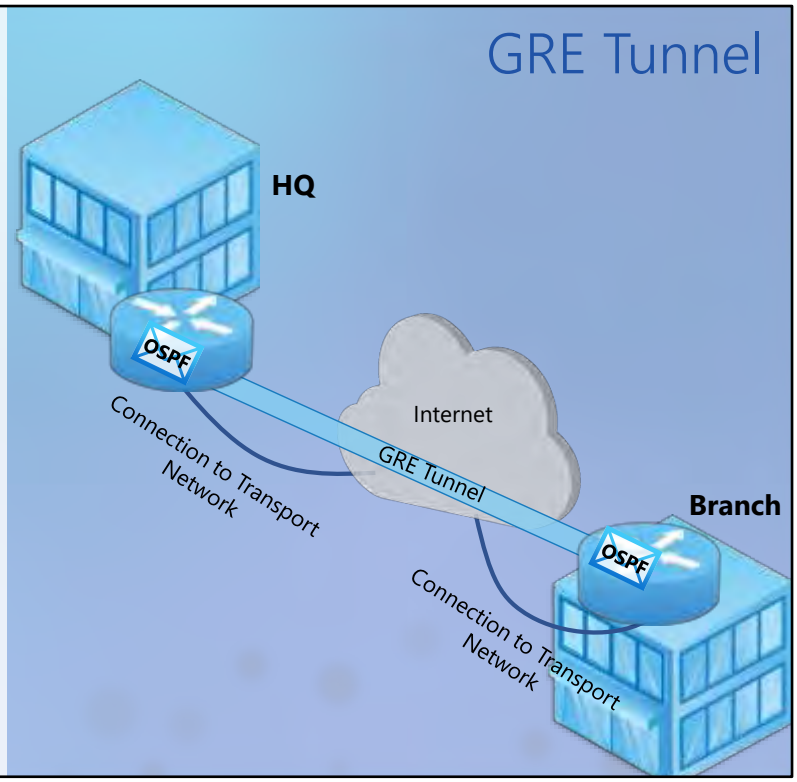
No encryption!!!



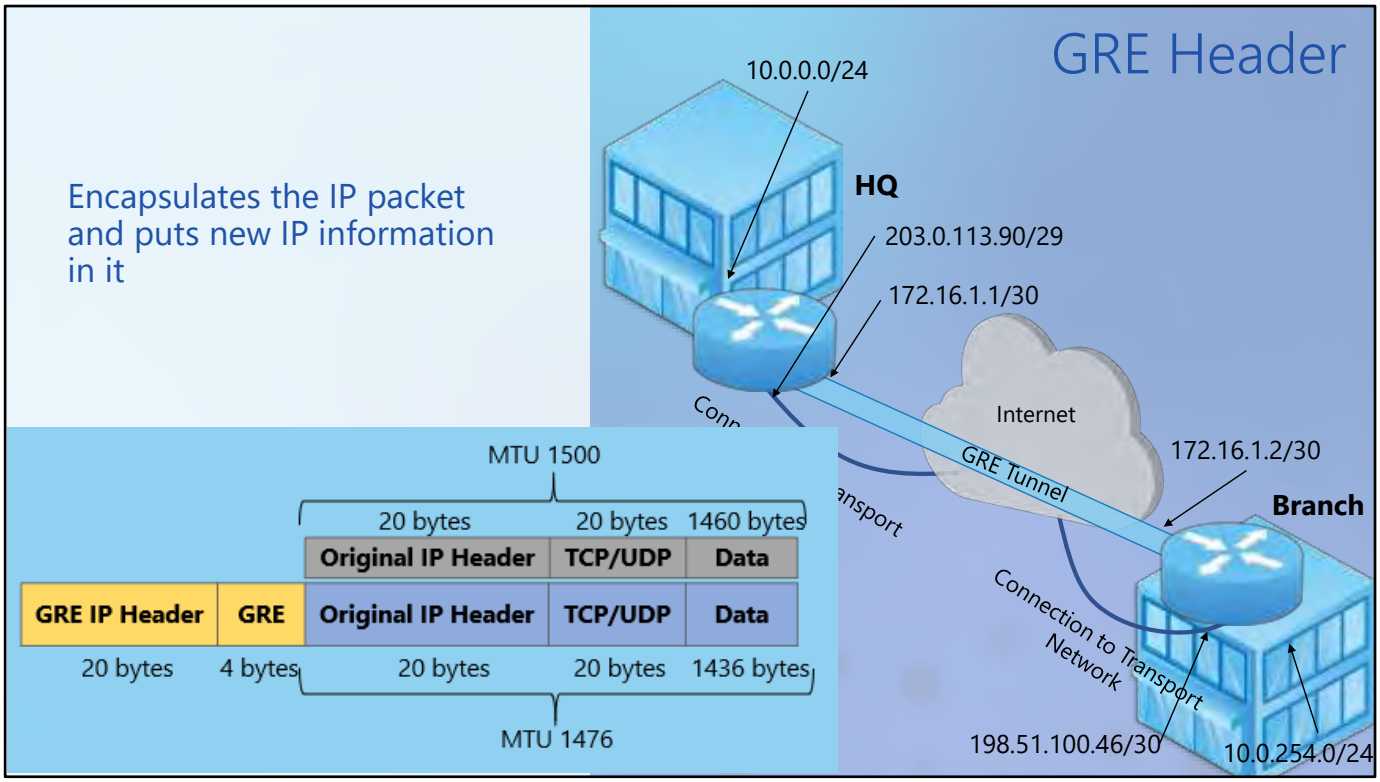
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE

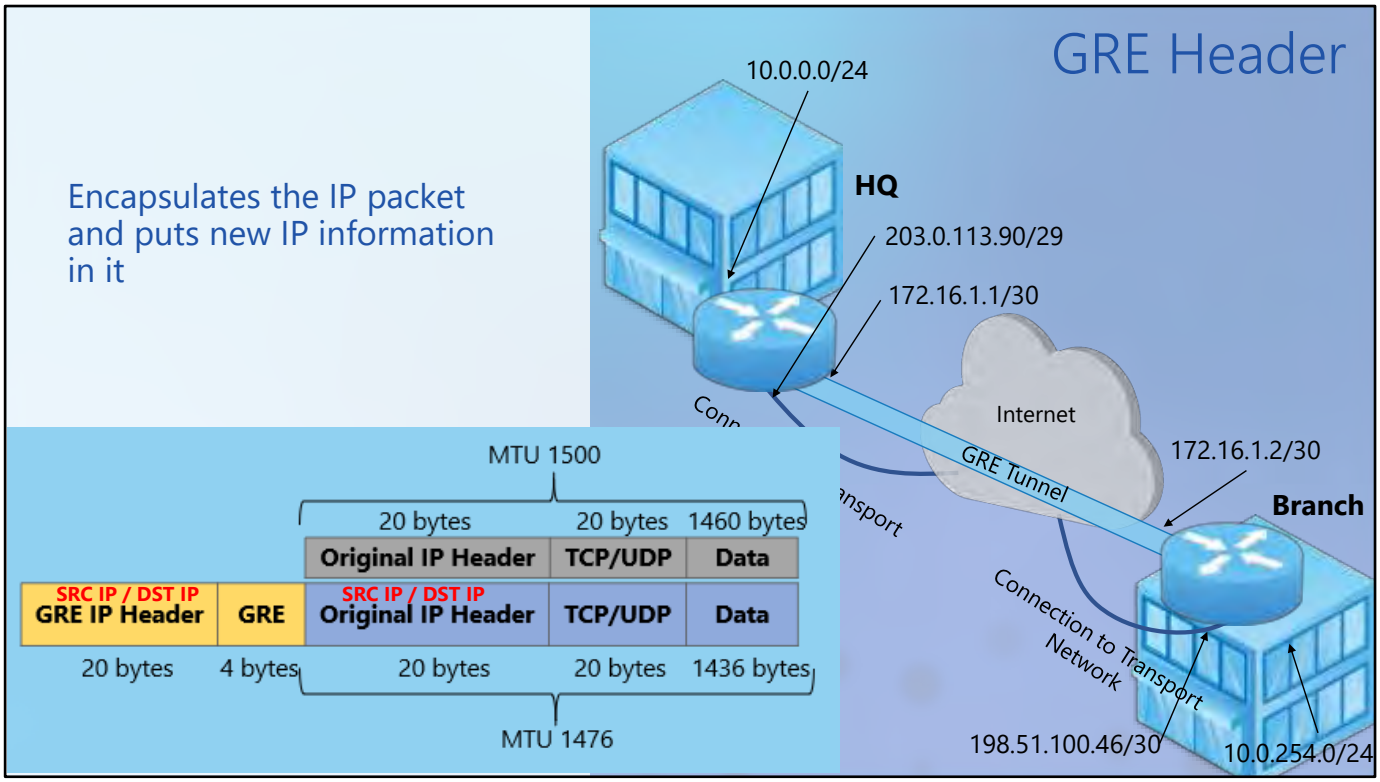
- Used to create **Point to Point** links over IP networks
- Utilizes IP **protocol 47**
- Originally designed by Cisco, but now defined by **RFC 2784**
- No encryption!!!
- Multiprotocol Support



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



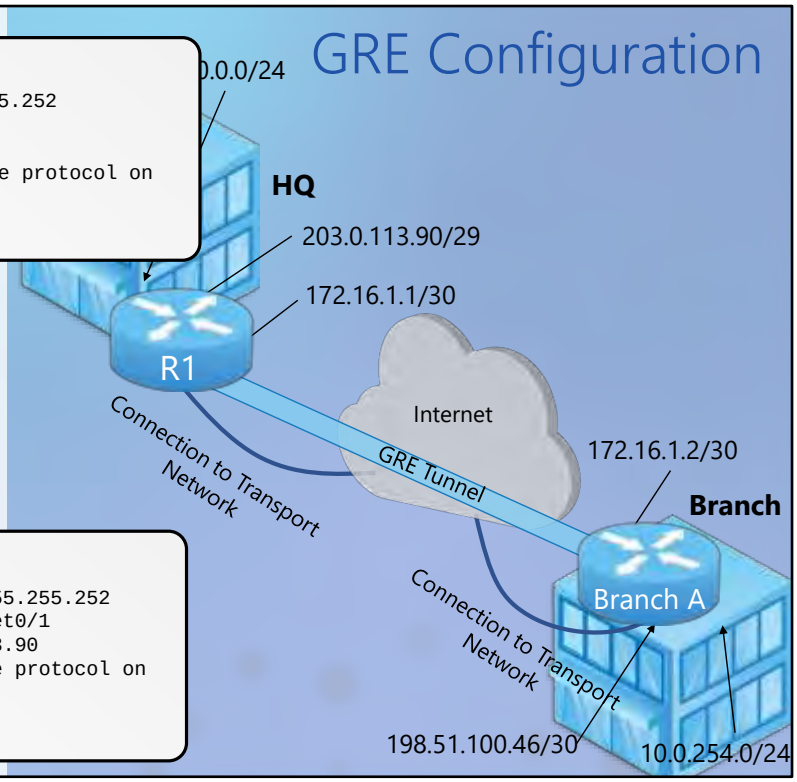
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE Configuration

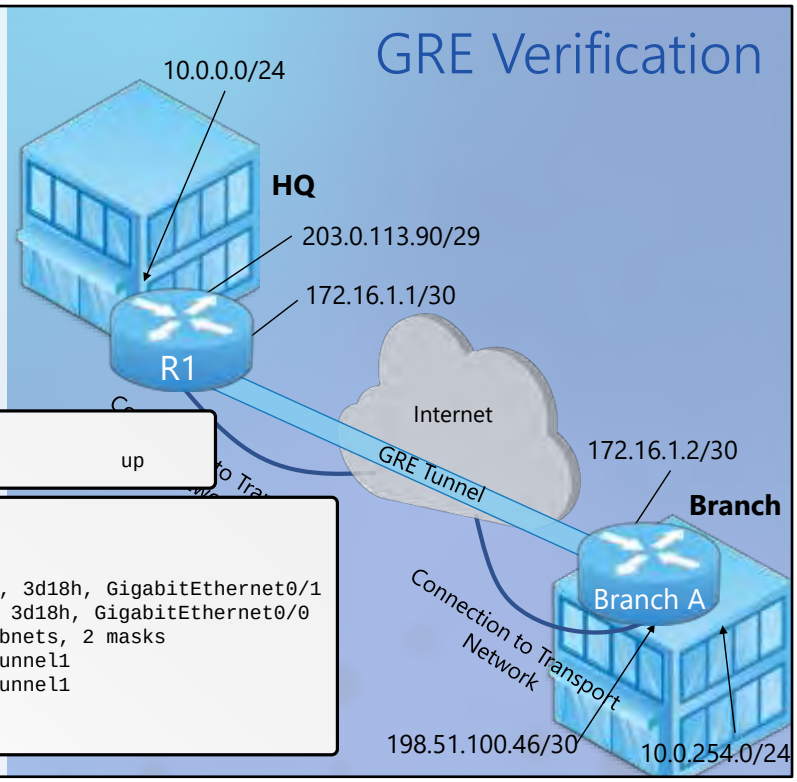
```
R1#configure terminal
R1(config)#int tunnel 1
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#tunnel source fastEthernet 0/0/0
R1(config-if)#tunnel destination 198.51.100.46
.Jul  6 11:35:04.960: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel1, changed state to up
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip ospf 1 area 0
```




```
BranchA#configure terminal
BranchA(config)#interface tunnel 1
BranchA(config-if)#ip address 172.16.1.2 255.255.255.252
BranchA(config-if)#tunnel source GigabitEthernet0/1
BranchA(config-if)#tunnel destination 203.0.113.90
*Jul  6 12:08:13.646: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Tunnel1, changed state to up
BranchA(config-if)#tunnel mode gre ip
BranchA(config-if)#ip ospf 1 area 0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

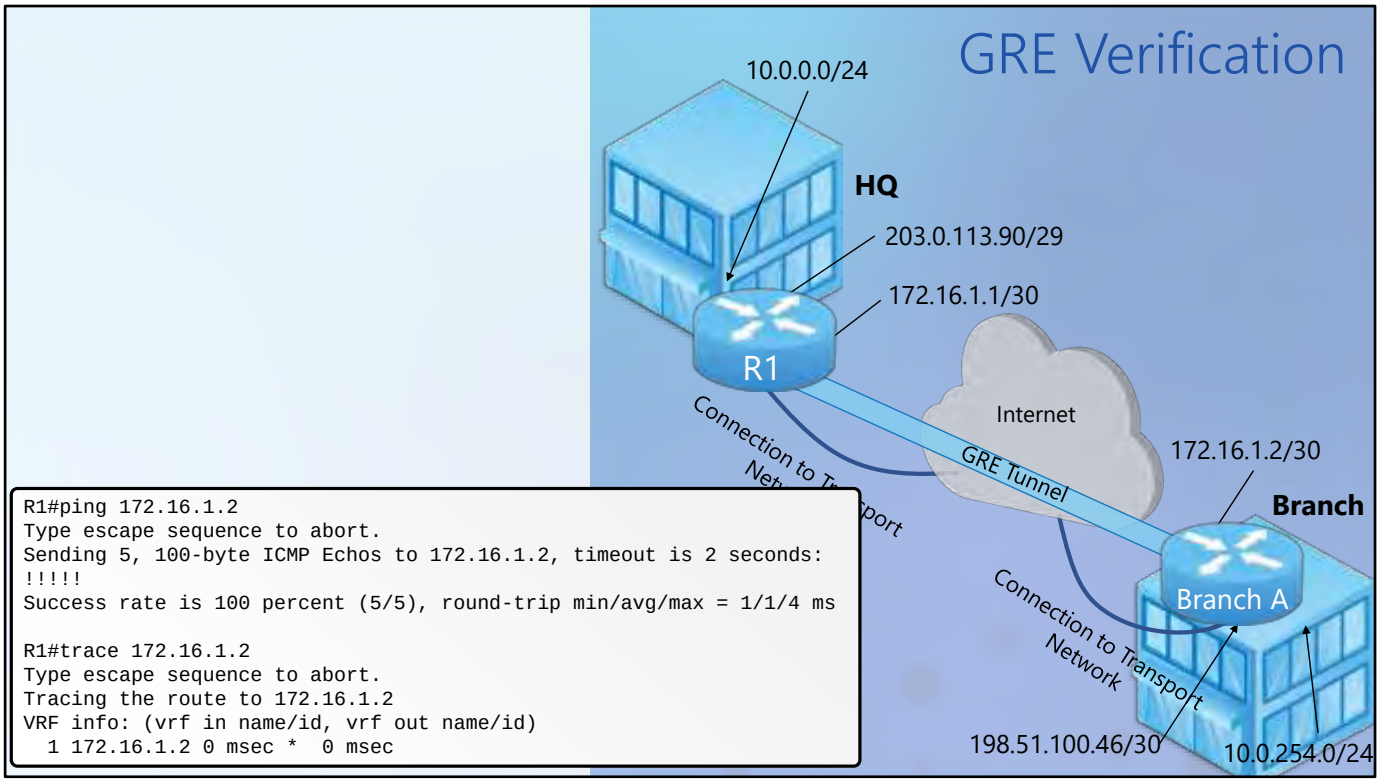
GRE Verification




```
R1#show ip interface brief | include Tunnel
Tunnel1             172.16.1.1   YES manual up           up
```

```
R1#show ip route
…output omitted…

O IA     10.45.33.0/30 [110/12] via 10.40.23.10, 3d18h, GigabitEthernet0/1
                       [110/12] via 10.40.23.2, 3d18h, GigabitEthernet0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/30 is directly connected, Tunnel1
L        172.16.1.1/32 is directly connected, Tunnel1
      198.51.100.0/32 is subnetted, 1 subnets
…output omitted…
```

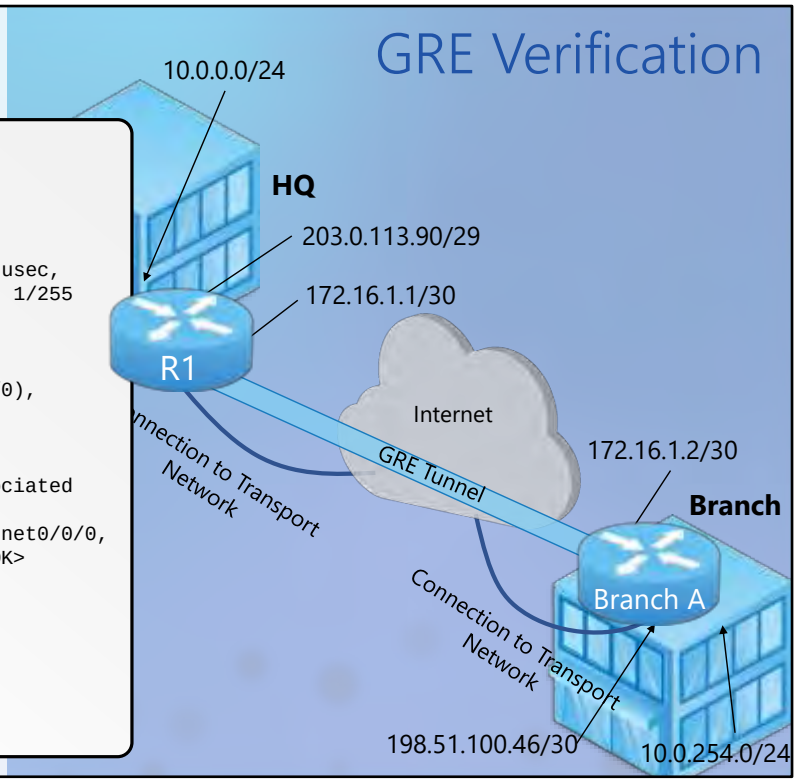
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE Verification

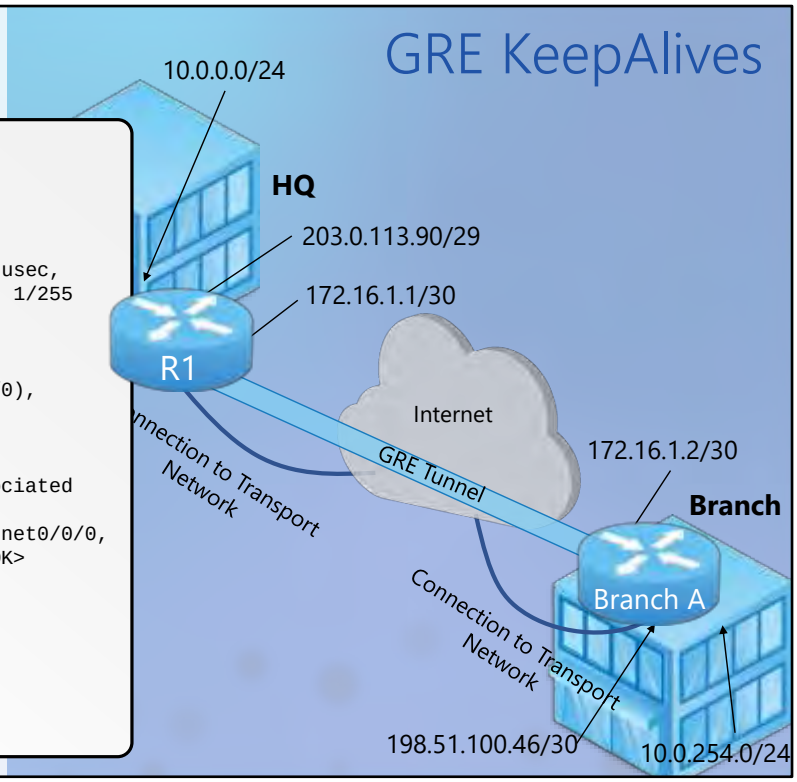
```
R1# show interfaces tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.1.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 203.0.113.90 (FastEthernet0/0/0),
destination 198.51.100.46
   Tunnel Subblocks:
      src-track:
         Tunnel1 source tracking subblock associated
with FastEthernet0/0/0
          Set of tunnels with source FastEthernet0/0/0,
1 member (includes iterators), on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
…output omitted…
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE KeepAlives

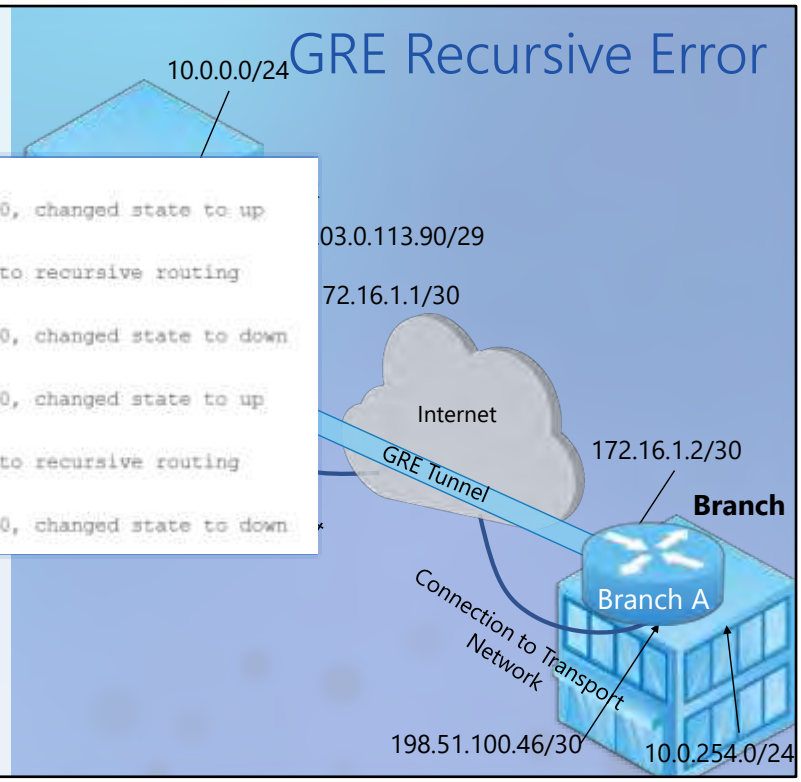
```
R1# show interfaces tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.1.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel linestate evaluation up
  Tunnel source 203.0.113.90 (FastEthernet0/0/0),
destination 198.51.100.46
   Tunnel Subblocks:
      src-track:
         Tunnel1 source tracking subblock associated
with FastEthernet0/0/0
          Set of tunnels with source FastEthernet0/0/0,
1 member (includes iterators), on interface <OK>
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
…output omitted…
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE Recursive Error

```
01:11:39: %LINEPROTO-5-UPDOWN:
          Line protocol on Interface Tunnel0, changed state to up
01:11:48: %TUN-5-RECURDOWN:
          Tunnel0 temporarily disabled due to recursive routing
01:11:49: %LINEPROTO-5-UPDOWN:
          Line protocol on Interface Tunnel0, changed state to down
01:12:49: %LINEPROTO-5-UPDOWN:
          Line protocol on Interface Tunnel0, changed state to up
01:12:58: %TUN-5-RECURDOWN:
          Tunnel0 temporarily disabled due to recursive routing
01:12:59: %LINEPROTO-5-UPDOWN:
          Line protocol on Interface Tunnel0, changed state to down
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

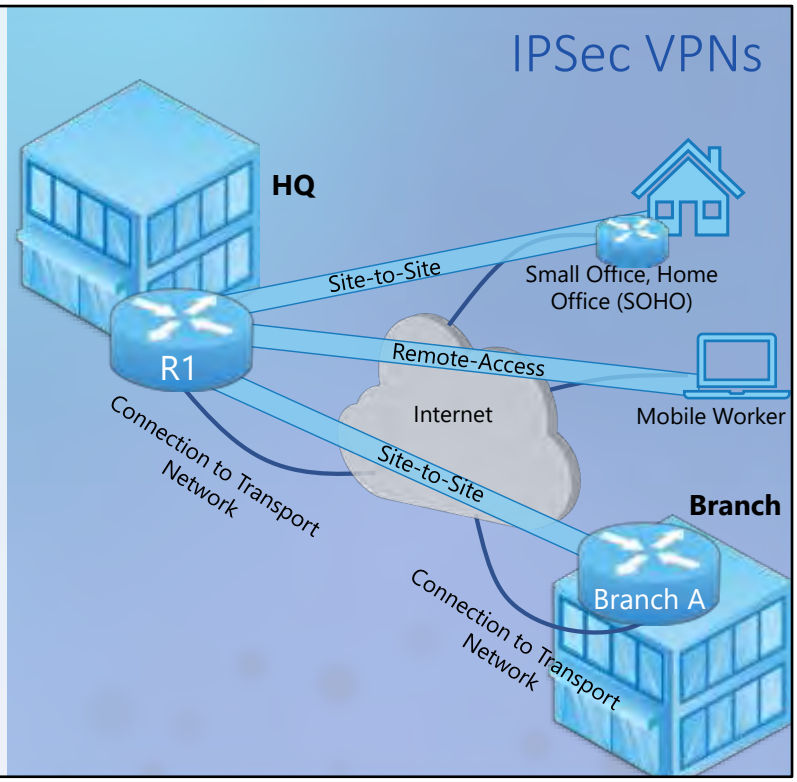
IPSec Introduction

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec VPNs

Provides secure tunnels over an untrusted network

- Encrypt IPv4 and IPv6 unicast traffic as it crosses the Internet (untrusted network)

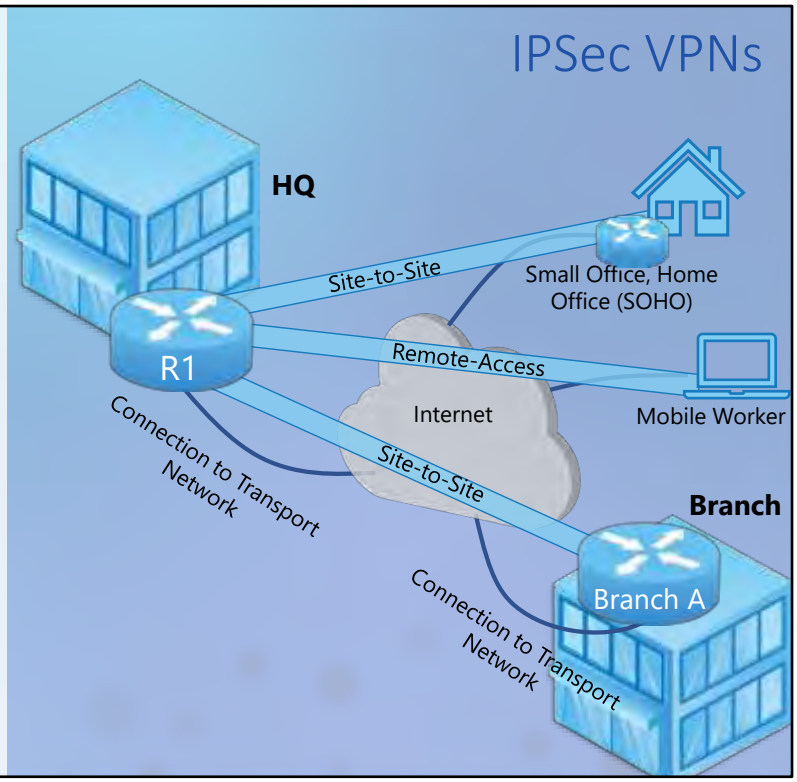


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec VPNs

Provides secure tunnels over an untrusted network

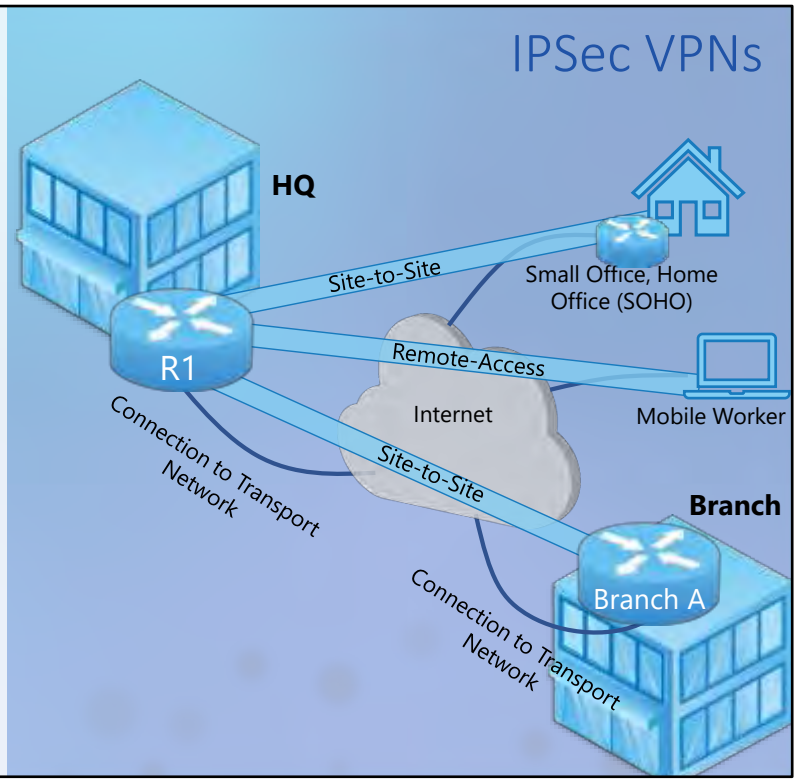
- Encrypt IPv4 and IPv6 unicast traffic as it crosses the Internet (untrusted network)
- *Does not support other protocols



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec VPNs

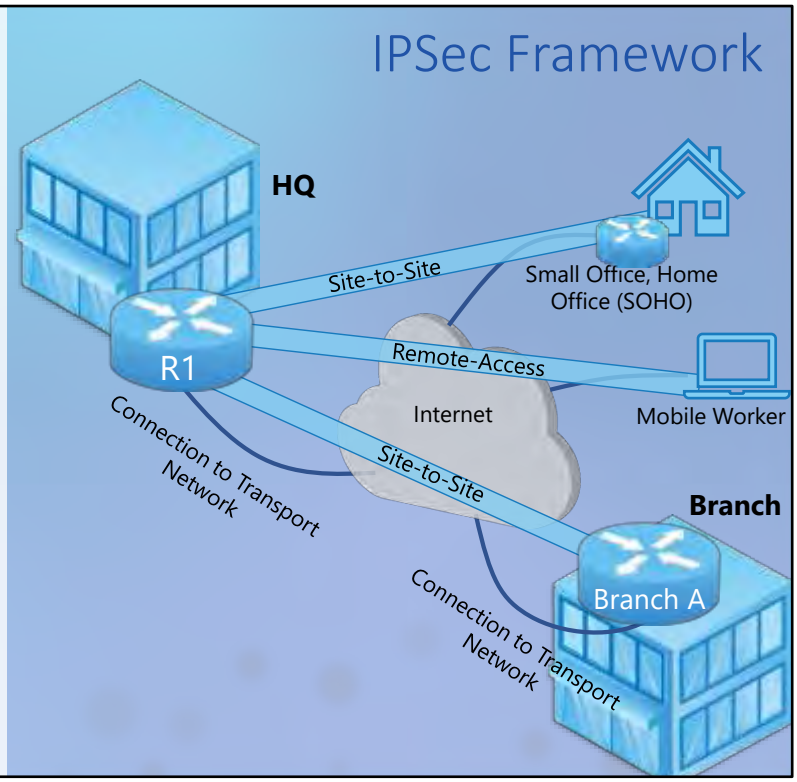
- Site-to-Site
  - Secure Point-to-Point connection between sites
- Remote Access
  - Secure Point-to-Point connection between a device and a site



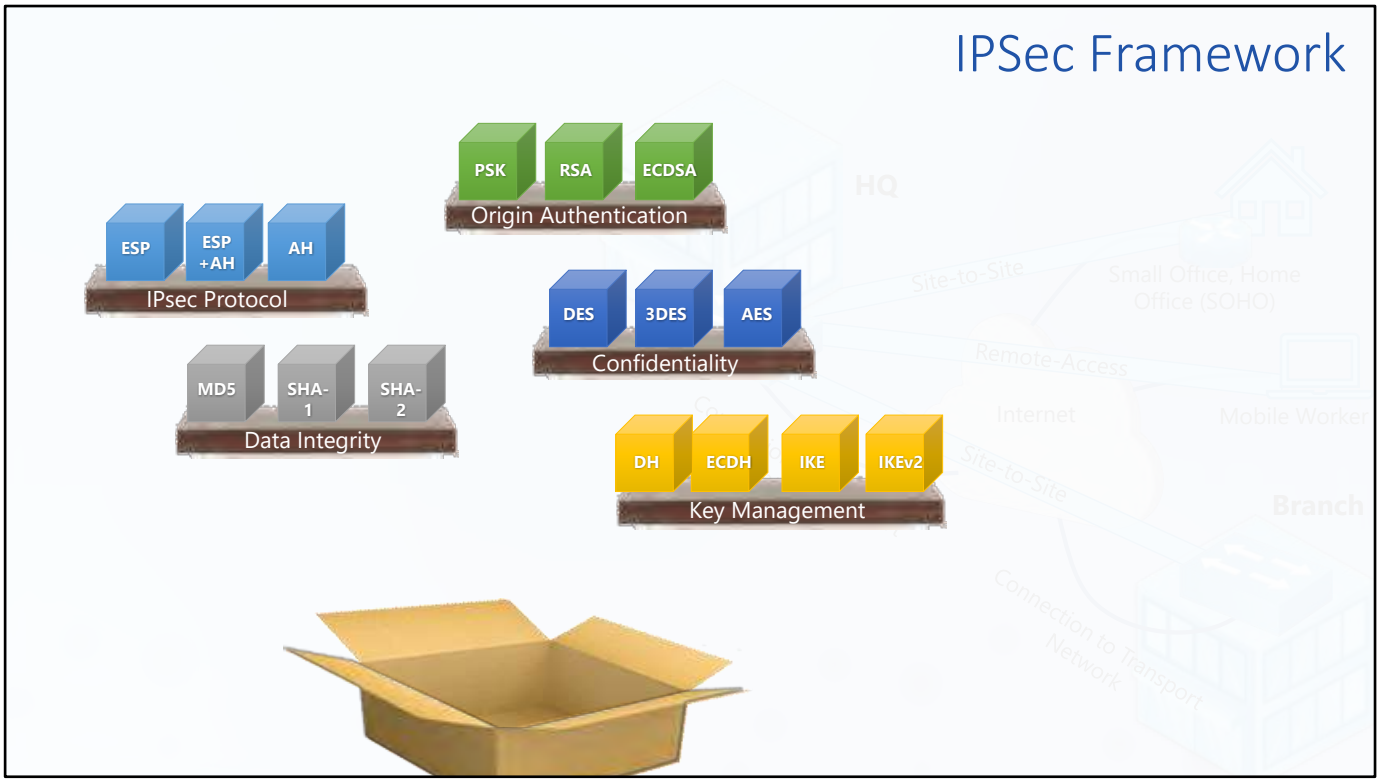
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Framework

- A framework that provides security at Layer 3 for IPv4 and IPv6 traffic
  - Requires IPv4 or IPv6 as the underlying transport network
- Provides the following security services:
  - Authentication
  - Integrity
  - Confidentiality
  - Anti-replay



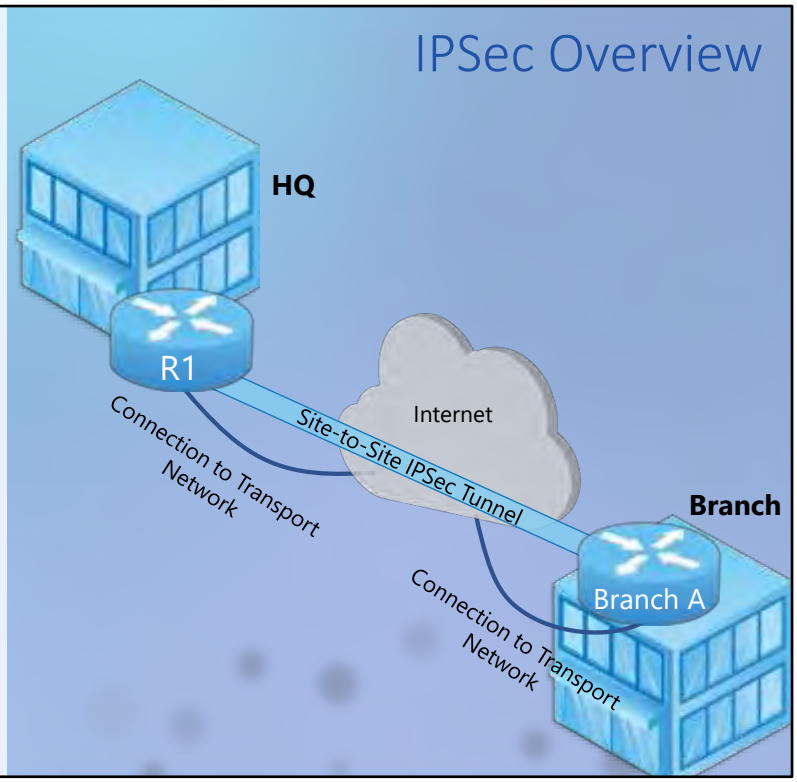
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



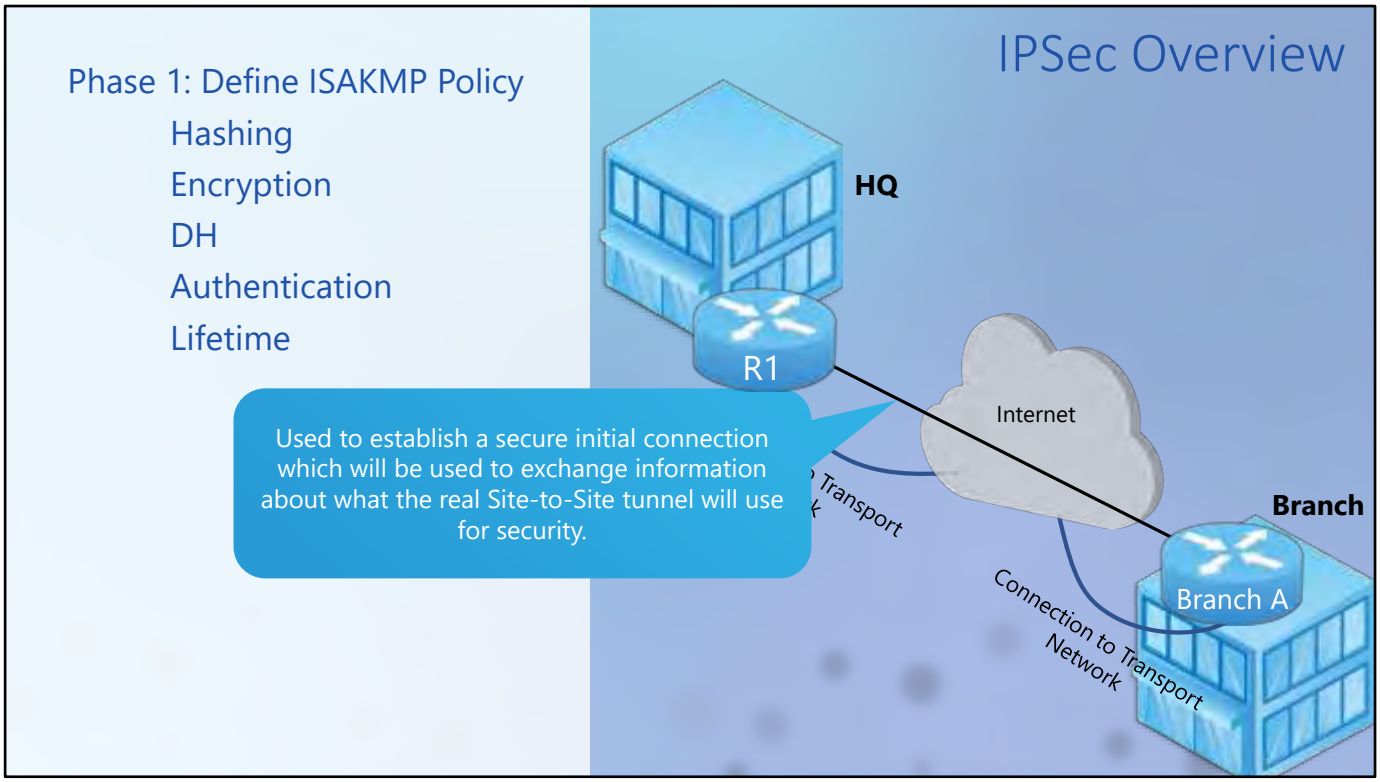
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Overview

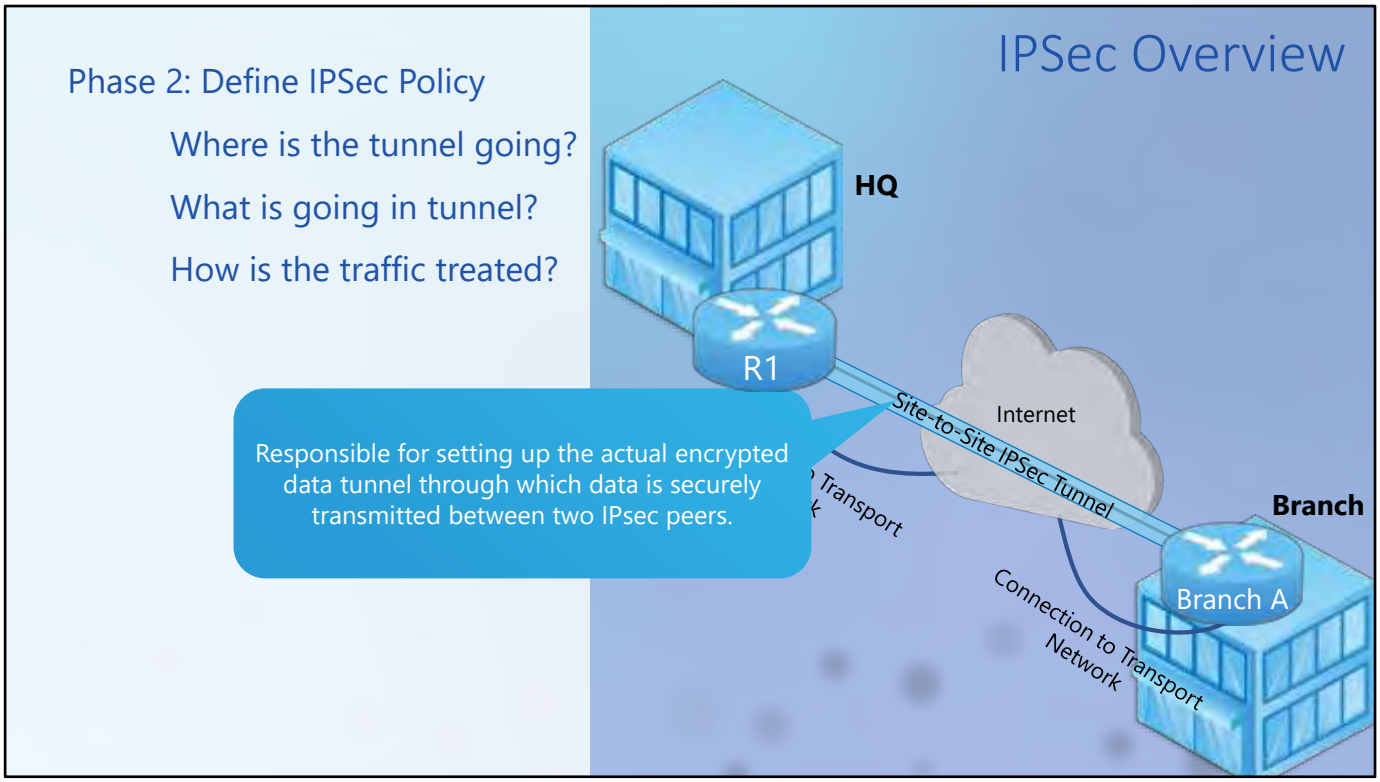
- Dynamic negotiation of tunnels to establish security association (SA)
  - ISAKMP
  - IKE
- Multiple Phases
  - Phase 1 (Creates ISAKMP SA)
  - Phase 2 (Creates IPSec SA)



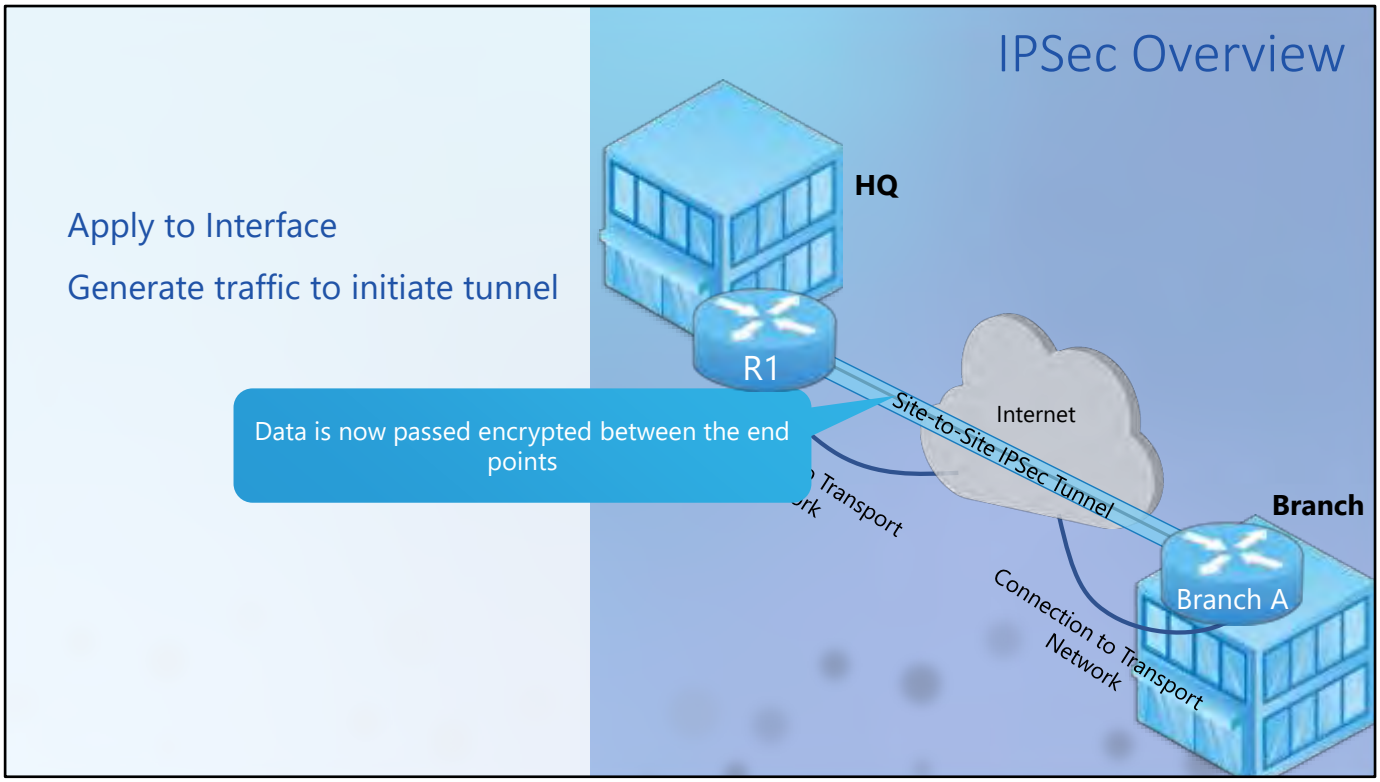
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

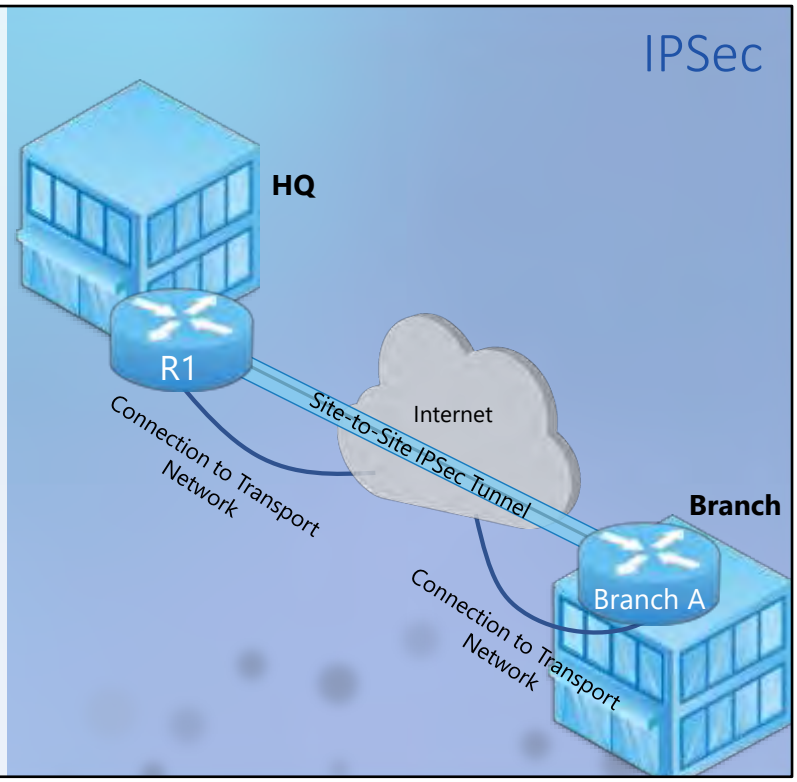


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

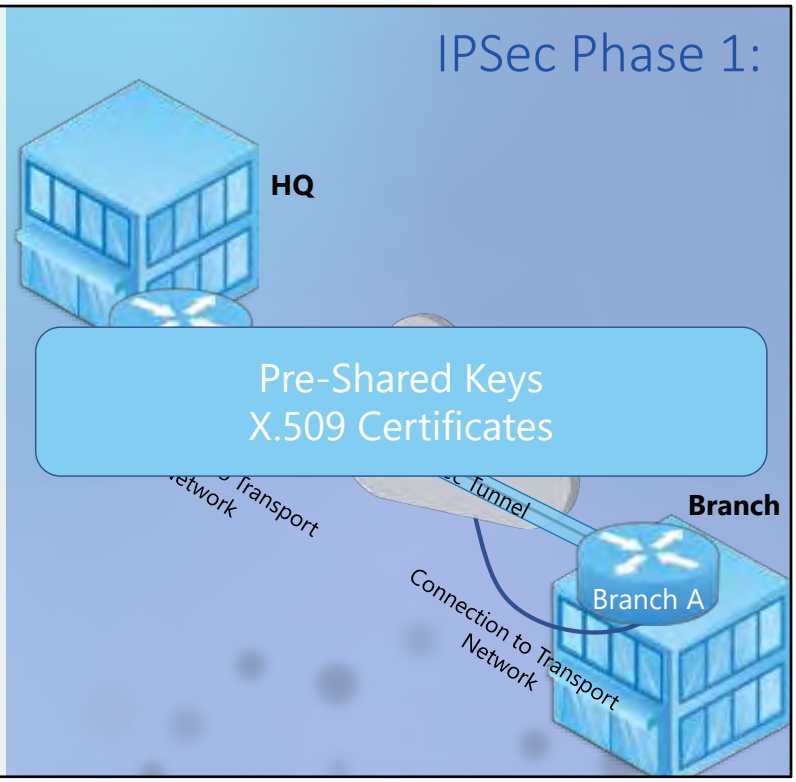
- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Phase 1:

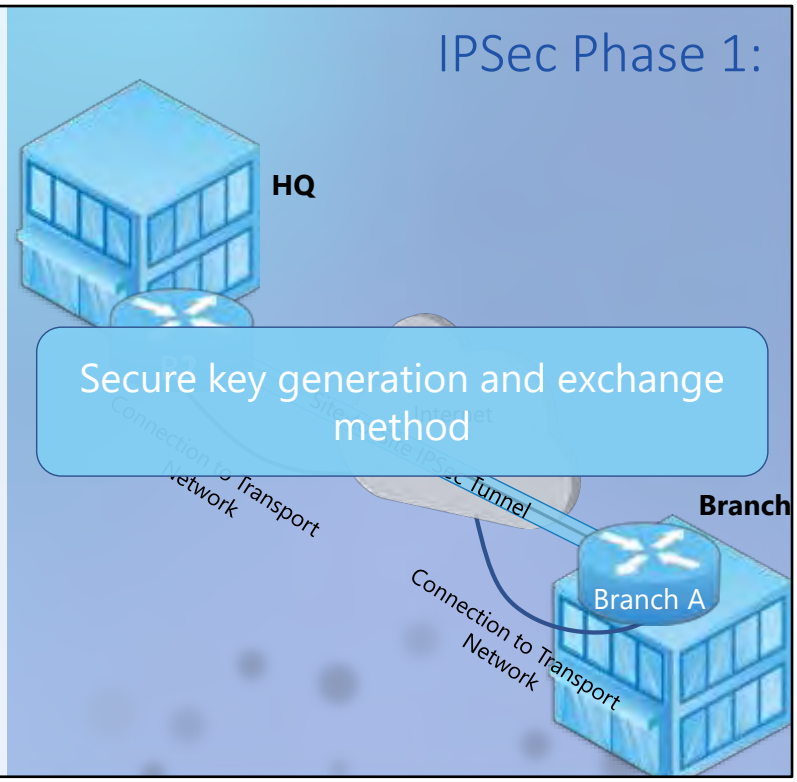
- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Phase 1:

- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel

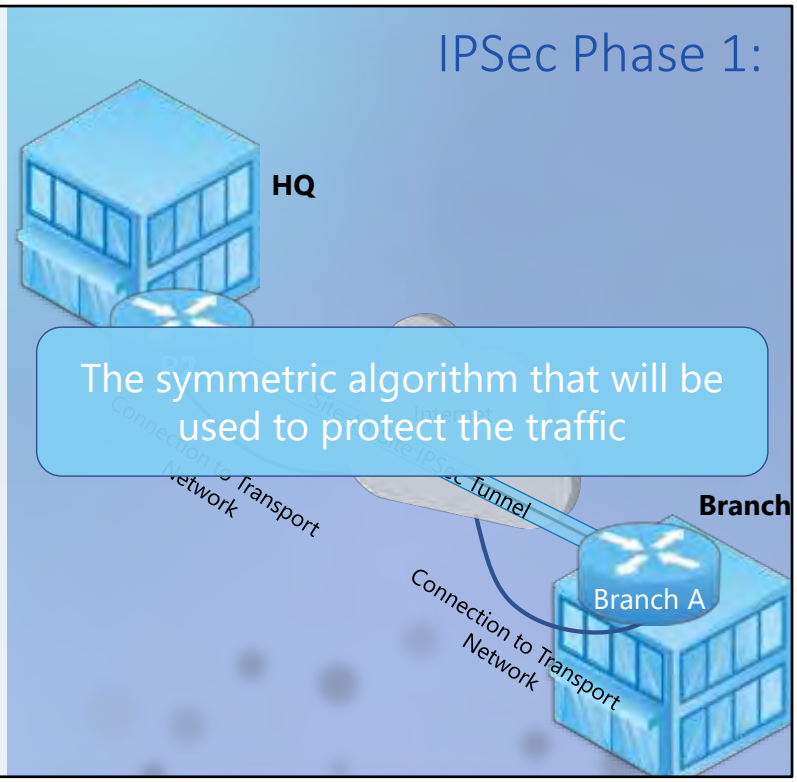


Secure key generation and exchange method

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Phase 1:

- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel

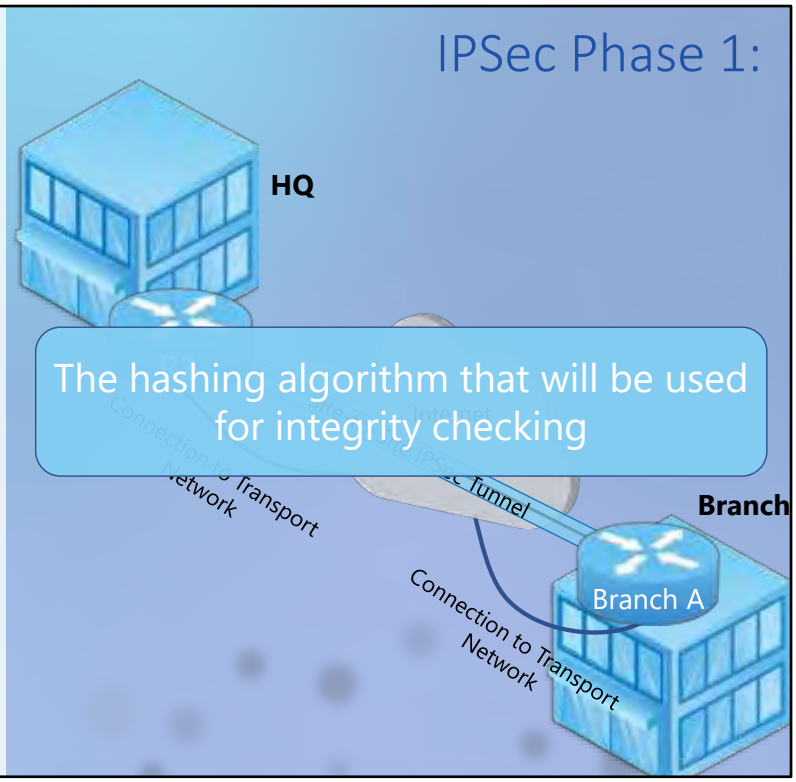


The symmetric algorithm that will be used to protect the traffic

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Phase 1:

- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel

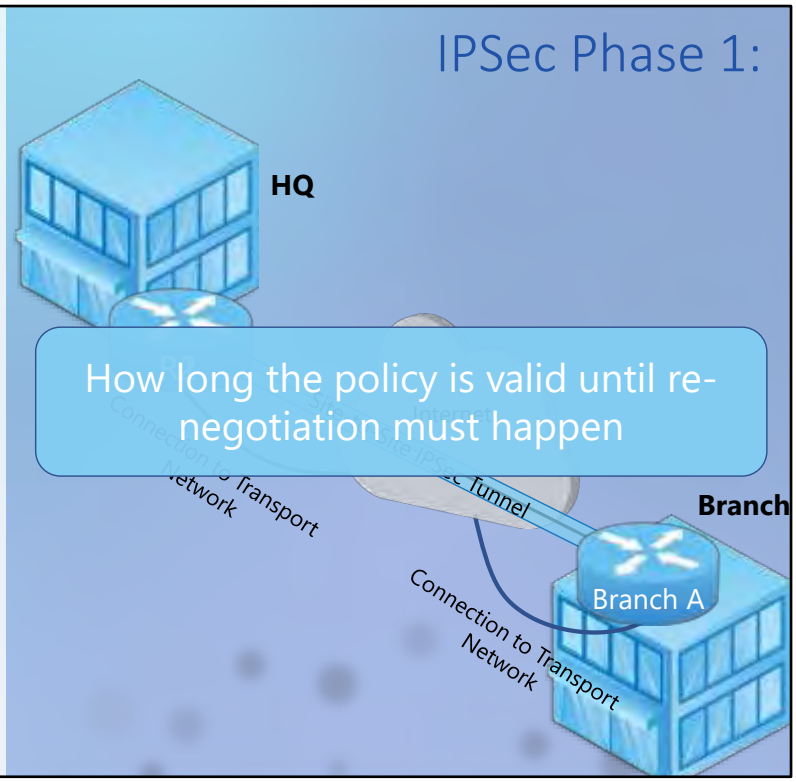


The hashing algorithm that will be used for integrity checking

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Phase 1:

- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel

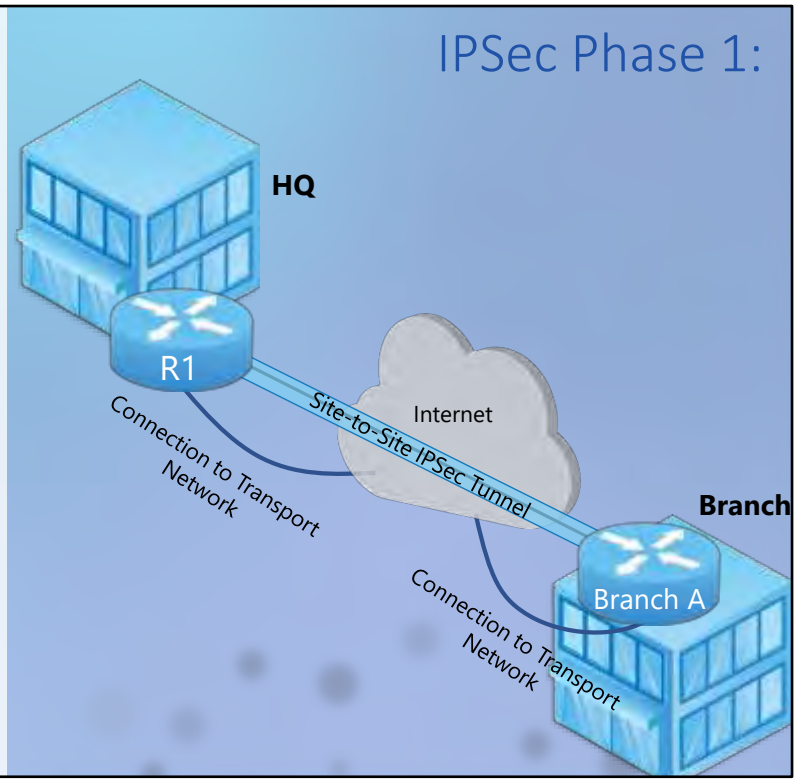


How long the policy is valid until re-negotiation must happen

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Phase 1:

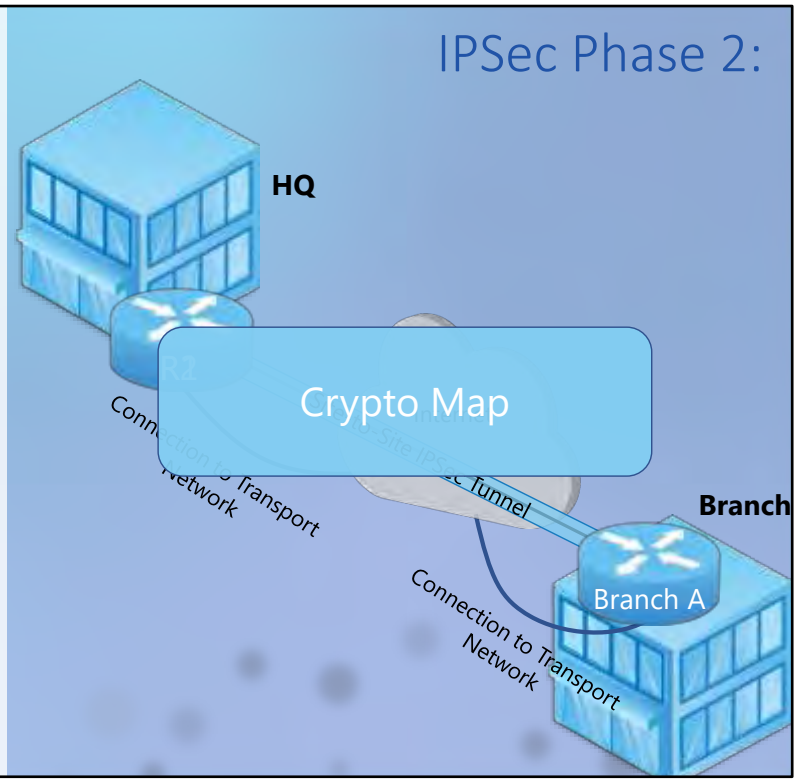
- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Phase 2:

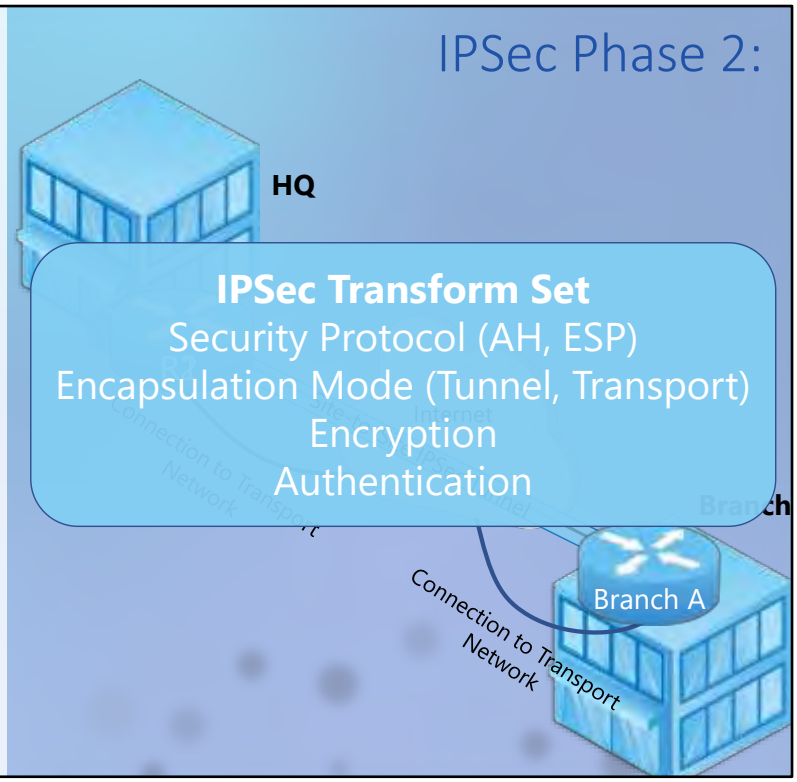
- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

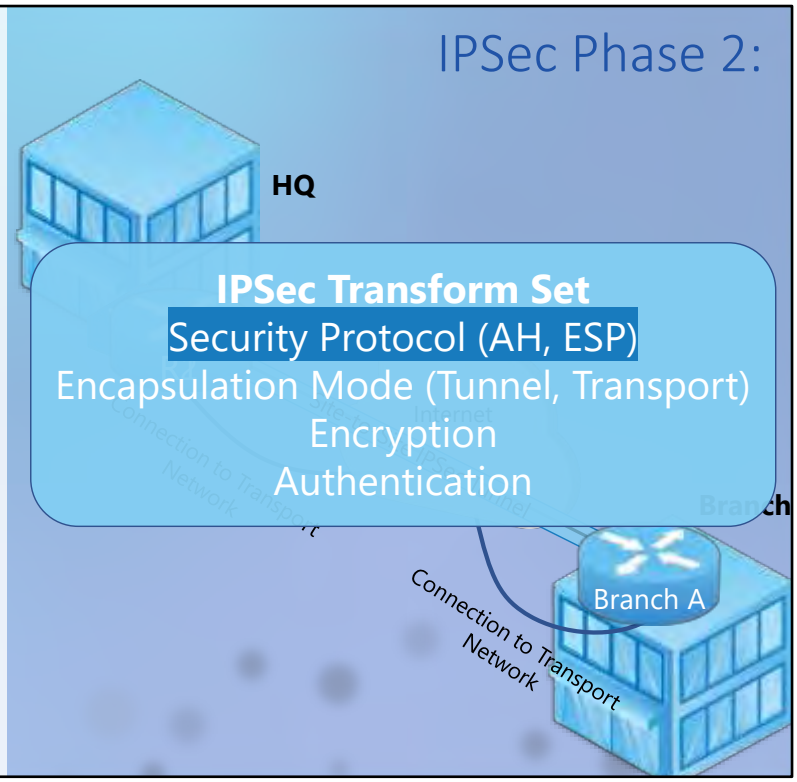
IPSec Phase 2:

- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel

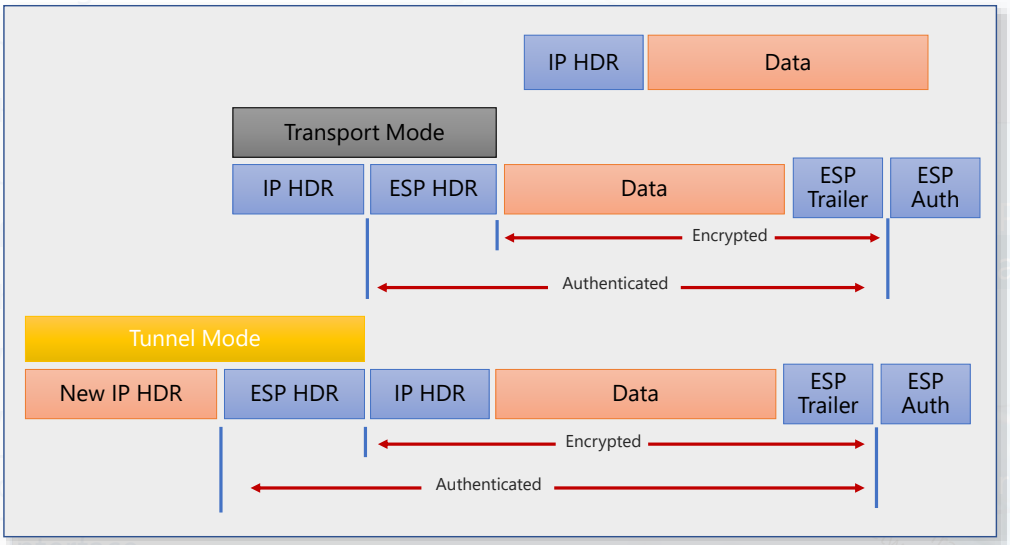


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Define Phase 1 ISAKMP Policy

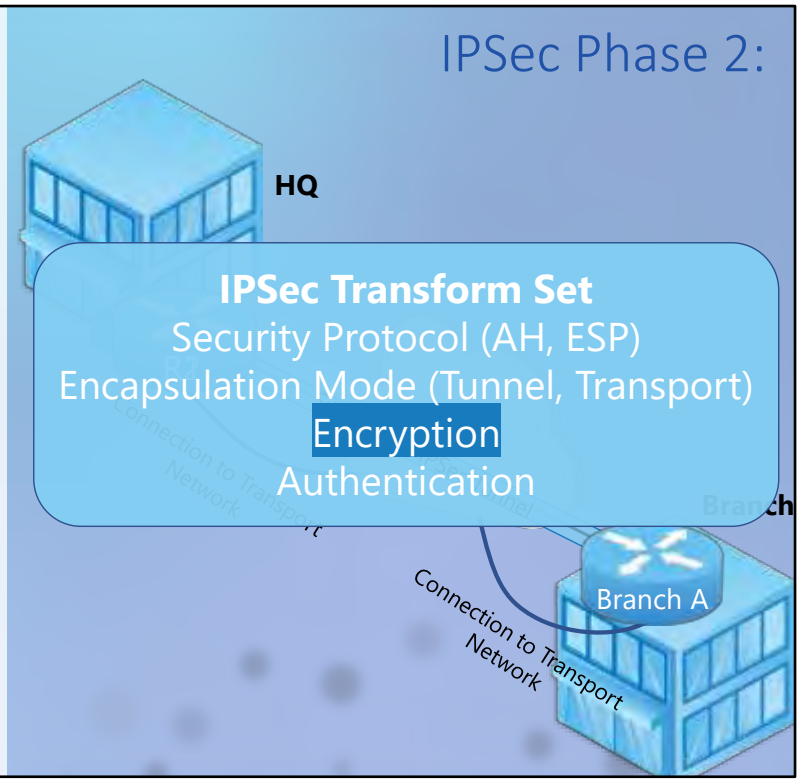
- Hashing
- Encryption
- DH
- Authentication
- Lifetime

Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?

Apply to Interface

Generate traffic to initiate tunnel



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Define Phase 1 ISAKMP Policy

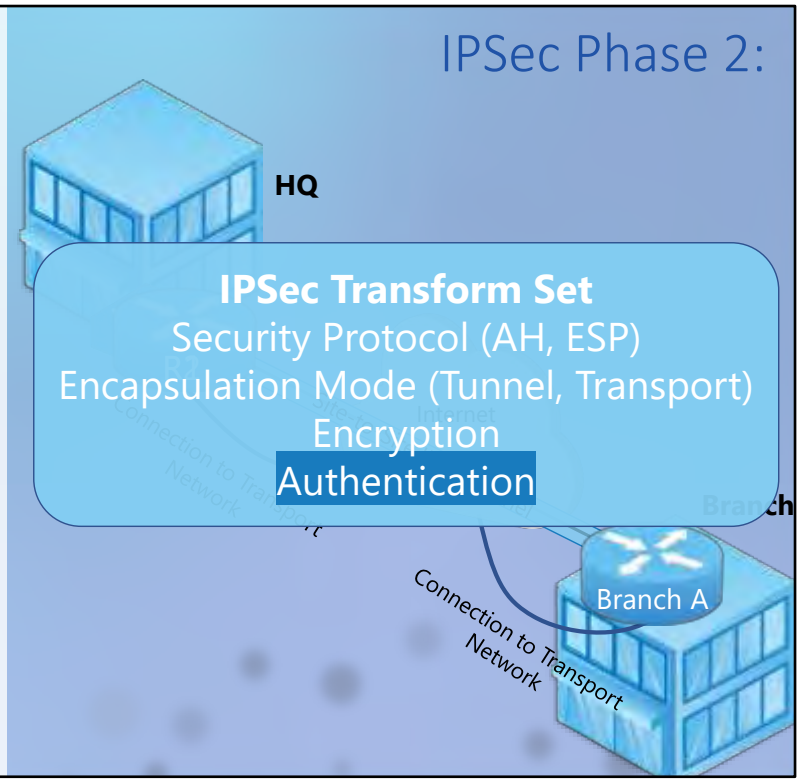
- Hashing
- Encryption
- DH
- Authentication
- Lifetime

Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?

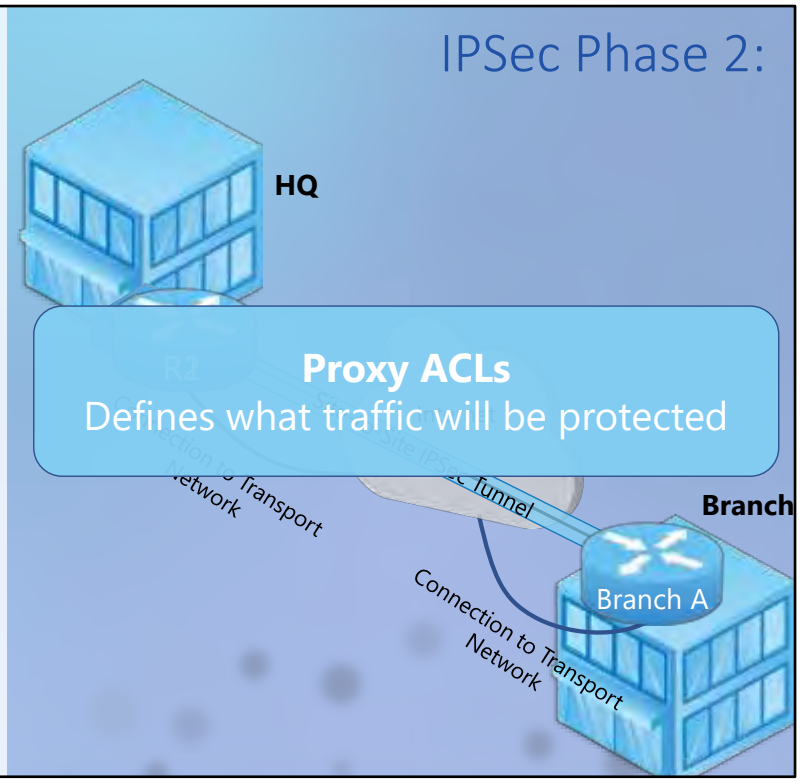
Apply to Interface

Generate traffic to initiate tunnel



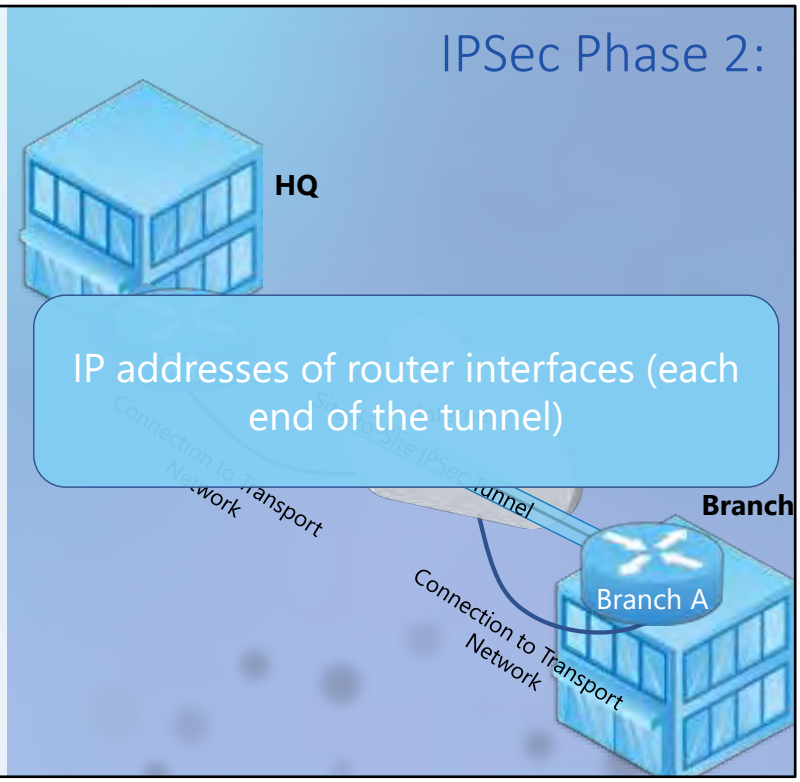
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

- Define Phase 1 ISAKMP Policy
  - Hashing
  - Encryption
  - DH
  - Authentication
  - Lifetime
- Define Phase 2 IPSec Policy
  - Where is the tunnel going?
  - What is going in tunnel?
  - How is the traffic treated?
- Apply to Interface
- Generate traffic to initiate tunnel



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Site-to-Site VPN Tunnel Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Define Phase 1 ISAKMP Policy

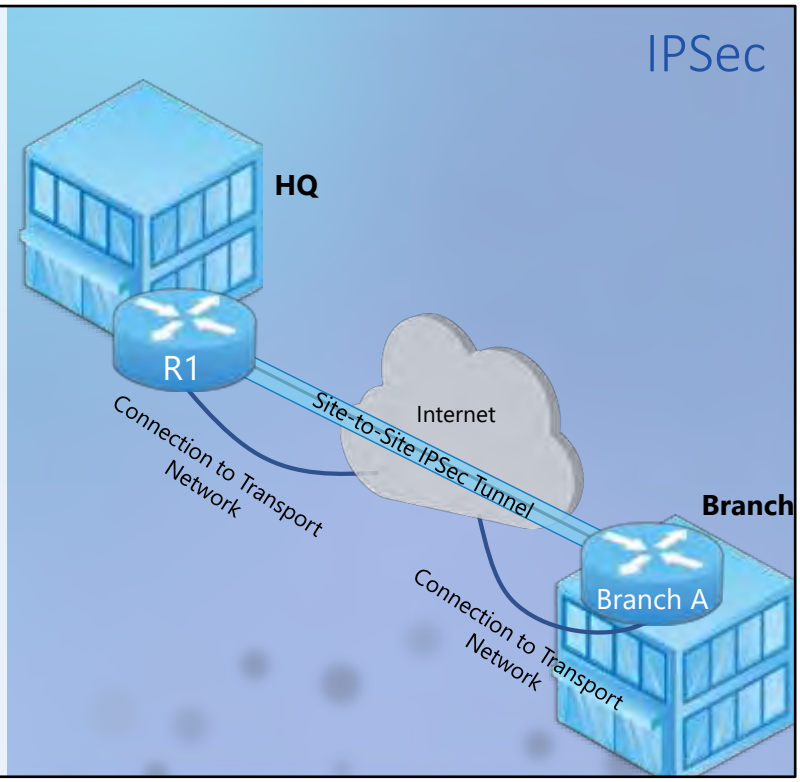
- Hashing
- Encryption
- DH
- Authentication
- Lifetime

Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?

Apply to Interface

Generate traffic to initiate tunnel

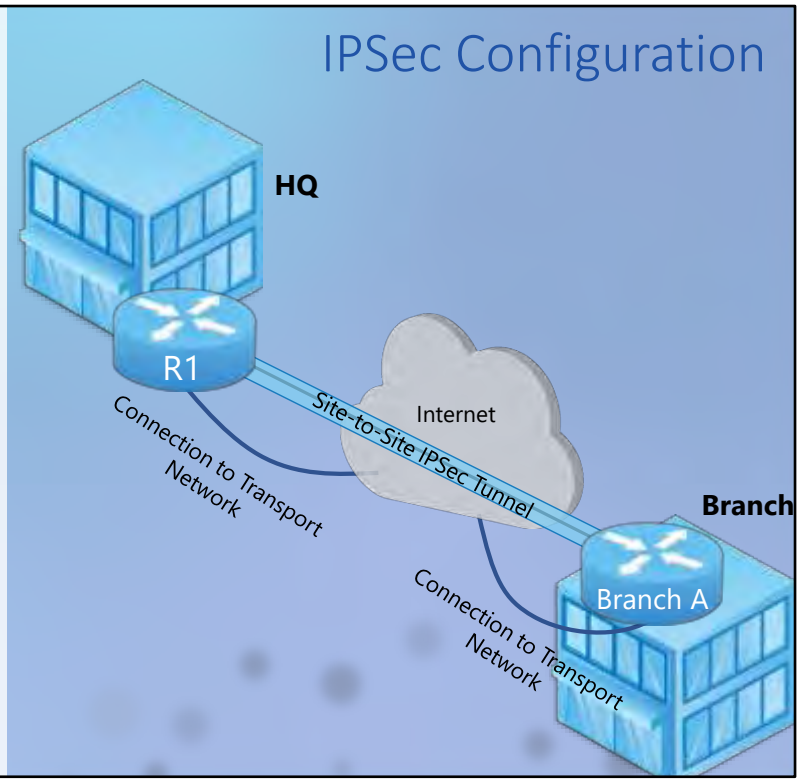


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

Define Phase 1 ISAKMP Policy

- Hashing
- Encryption
- DH
- Authentication
- Lifetime

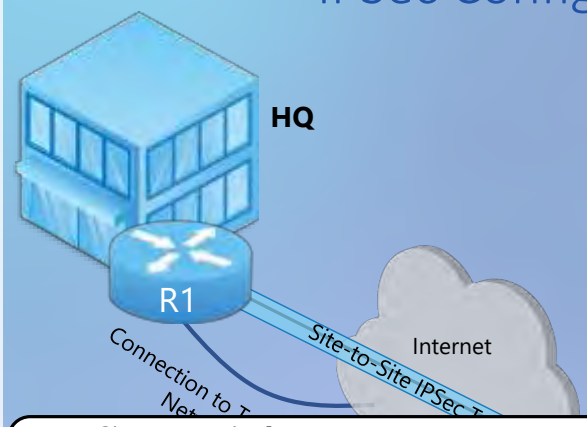


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

Define Phase 1 ISAKMP Policy

- Hashing
- Encryption
- DH
- Authentication
- Lifetime




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#group 16
R1(config-isakmp)#hash sha256
R1(config-isakmp)#exit
R1(config)#crypto isakmp key PASSWORD address 198.51.100.46
R1(config)#end
R1#
```

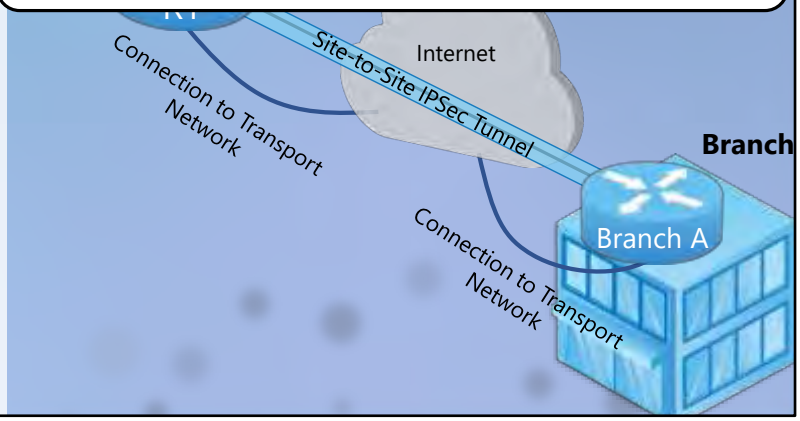
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

Define Phase 1 ISAKMP Policy

- Hashing
- Encryption
- DH
- Authentication
- Lifetime

```
BranchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BranchA(config)#crypto isakmp policy 10
BranchA(config-isakmp)# encryption aes 256
BranchA(config-isakmp)# hash sha256
BranchA(config-isakmp)# authentication pre-share
BranchA(config-isakmp)# group 16
BranchA(config-isakmp)#exit
BranchA(config)#crypto isakmp key PASSWORD address 203.0.113.90
BranchA(config)#end
BranchA#
```

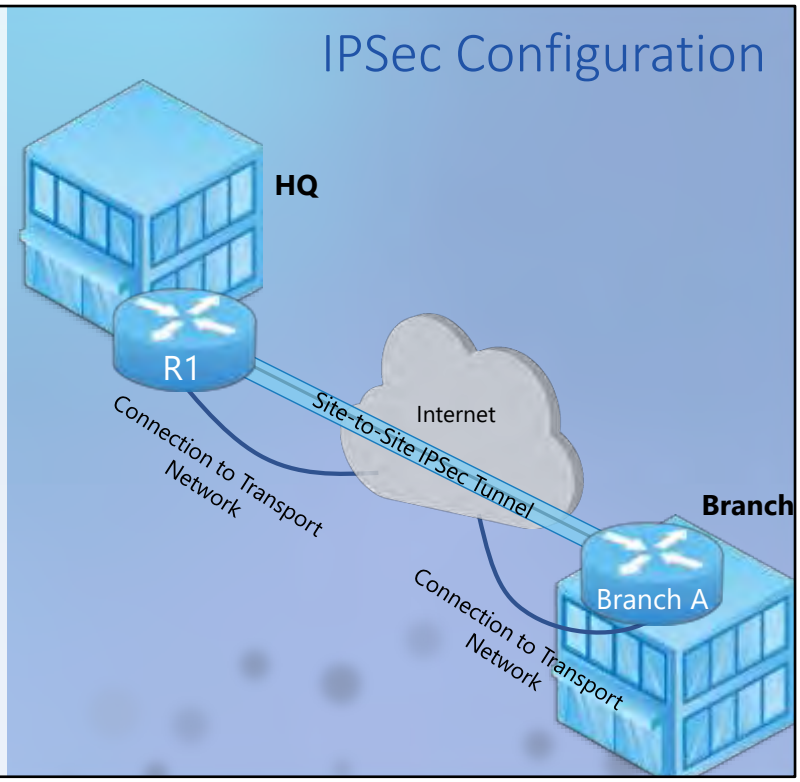


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?



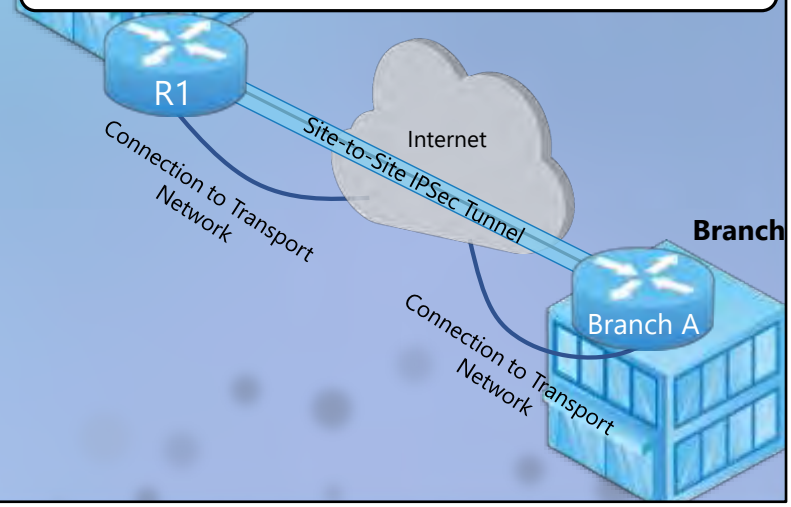
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?

```
R1(config)#crypto map IPSEC_VPN_CM 10 ipsec-isakmp
R1(config-crypto-map)#match address IPSEC_VPN_ACL
R1(config-crypto-map)#set peer 198.51.100.46
R1(config-crypto-map)#set transform-set IPSEC_VPN_TRANSFORM
R1(config-crypto-map)#exit
R1(config)#
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

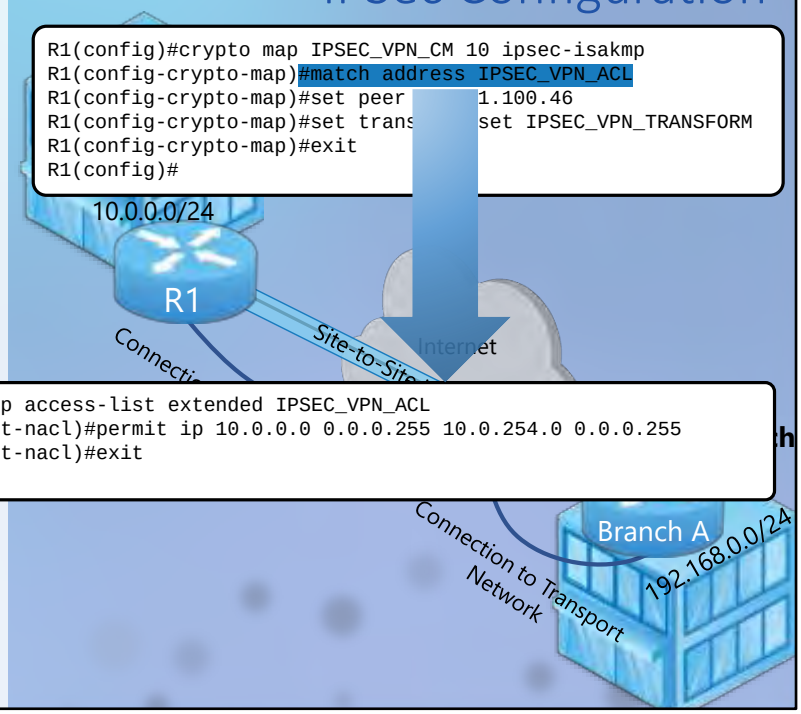
IPSec Configuration

Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic tr

```
R1(config)#crypto map IPSEC_VPN_CM 10 ipsec-isakmp
R1(config-crypto-map)#match address IPSEC_VPN_ACL
R1(config-crypto-map)#set peer 1.100.46
R1(config-crypto-map)#set trans set IPSEC_VPN_TRANSFORM
R1(config-crypto-map)#exit
R1(config)#
```

```
R1(config)#ip access-list extended IPSEC_VPN_ACL
R1(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 10.0.254.0 0.0.0.255
R1(config-ext-nacl)#exit
R1(config)#
```



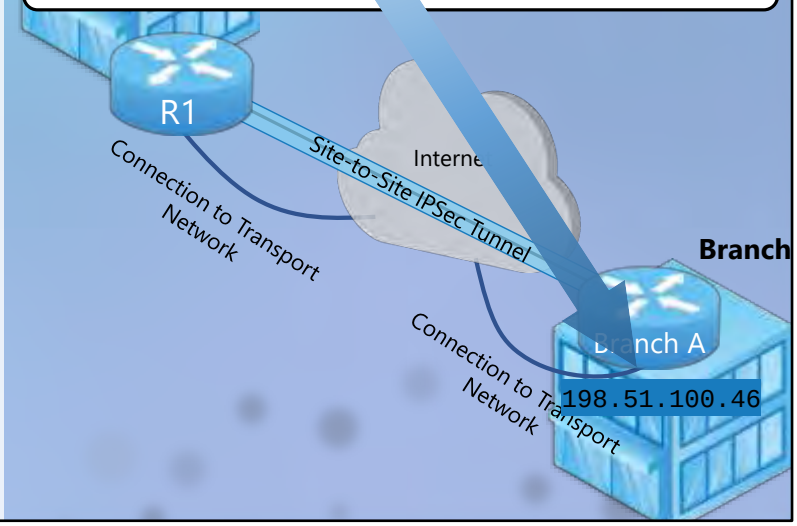
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?

```
R1(config)#crypto map IPSEC_VPN_CM 10 ipsec-isakmp
R1(config-crypto-map)#match address IPSEC_VPN_ACL
R1(config-crypto-map)#set peer 198.51.100.46
R1(config-crypto-map)#set transform-set IPSEC_VPN_TRANSFORM
R1(config-crypto-map)#exit
R1(config)#
```



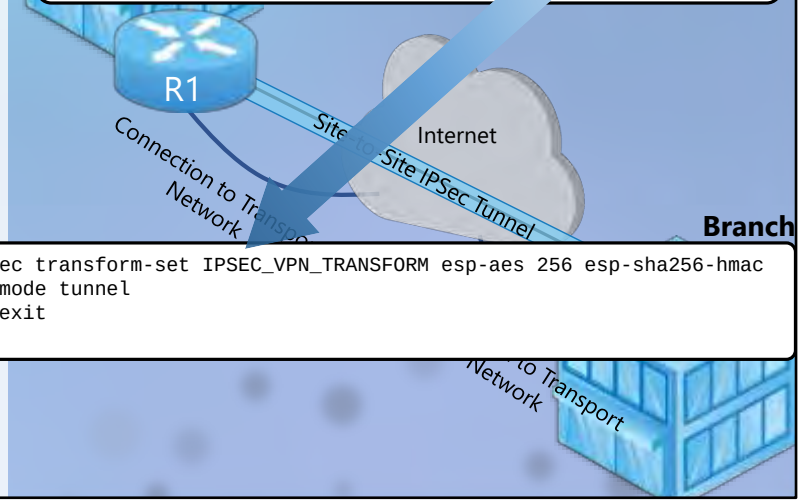
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?

```
R1(config)#crypto map IPSEC_VPN_CM 10 ipsec-isakmp
R1(config-crypto-map)#match address IPSEC_VPN_ACL
R1(config-crypto-map)#set peer 198.51.100.46
R1(config-crypto-map)#set transform-set IPSEC_VPN_TRANSFORM
R1(config-crypto-map)#exit
R1(config)#
```




```
R1(config)#crypto ipsec transform-set IPSEC_VPN_TRANSFORM esp-aes 256 esp-sha256-hmac
R1(cfg-crypto-trans)#mode tunnel
R1(cfg-crypto-trans)#exit
R1(config)#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

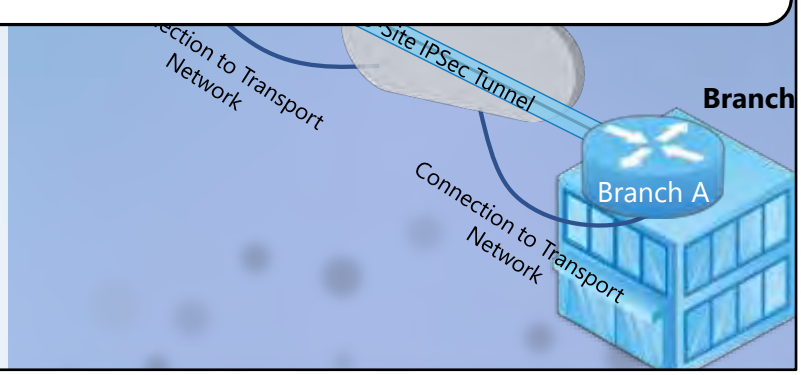
```
BranchA(config)# crypto ipsec transform-set IPSEC_VPN_TRANSFORM esp-aes 256 esp-sha256-hmac
BranchA(cfg-crypto-trans)# mode tunnel
BranchA(cfg-crypto-trans)# exit
BranchA(config)# ip access-list extended IPSEC_VPN_ACL
BranchA(config-ext-nacl)# permit ip 10.0.254.0 0.0.0.255 10.0.0.0 0.0.0.255
BranchA(config-ext-nacl)# exit
BranchA(config)# crypto map IPSEC_VPN_CM 10 ipsec-isakmp
BranchA(config-crypto-map)# set peer 203.0.113.90
BranchA(config-crypto-map)# set transform-set IPSEC_VPN_TRANSFORM
BranchA(config-crypto-map)# match address IPSEC_VPN_ACL
BranchA(config-crypto-map)#end
BranchA #
```

Define Phase

Where

What is

How is the traffic treated?

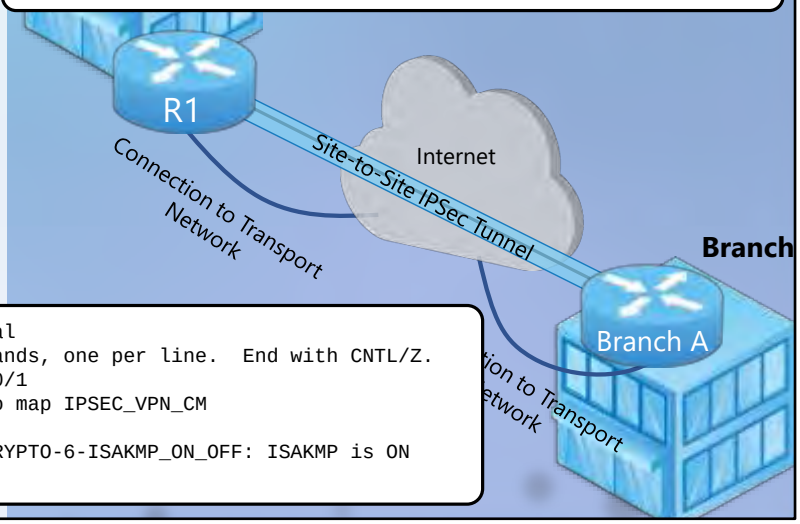


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSec Configuration

Apply to Outgoing Interface

```
R1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fa 0/0/0
R1(config-if)#crypto map IPSEC_VPN_CM
*Nov  7 16:03:18.963: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```



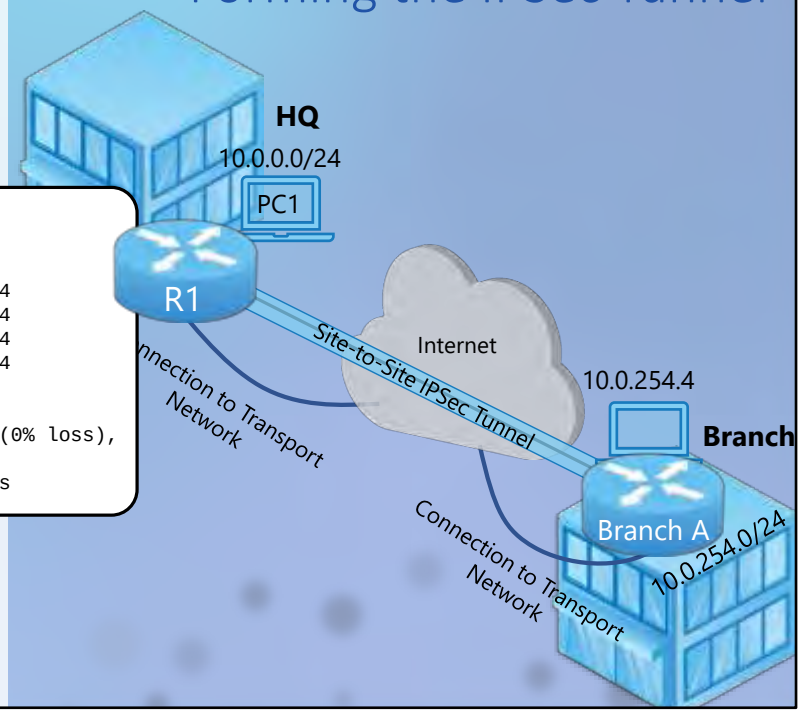

```
BranchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BranchA(config)#int gig 0/1
BranchA(config-if)#crypto map IPSEC_VPN_CM
BranchA(config-if)#
*Nov  7 16:05:50.575: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
BranchA(config-if)#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Forming the IPSec Tunnel

Generate Interesting Traffic

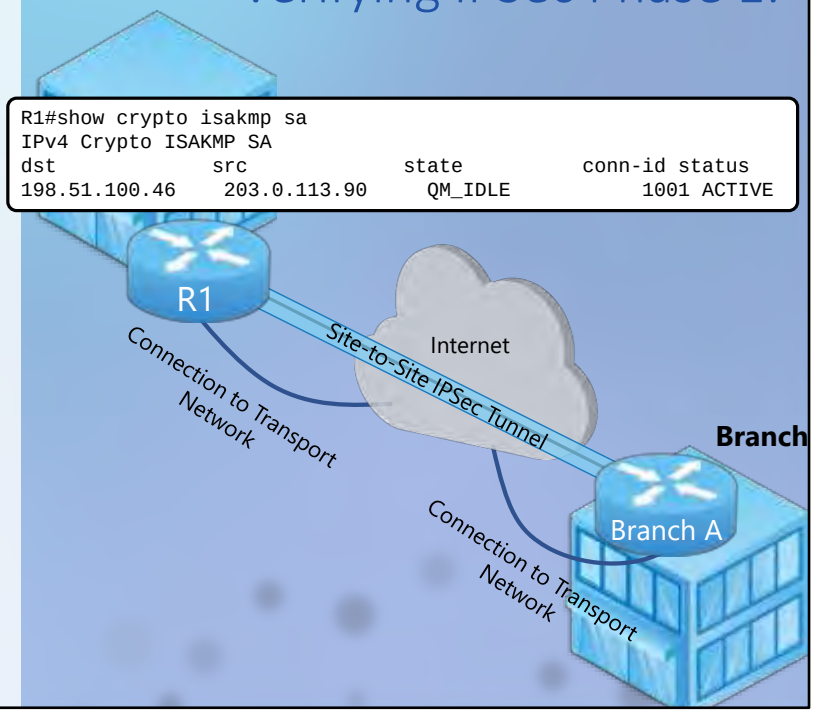
```
PC1>ping 10.0.254.4

Pinging 10.0.254.4 with 32 bytes of data:
Reply from 10.0.254.4: bytes=32 time=2ms TTL=64
Reply from 10.0.254.4: bytes=32 time=3ms TTL=64
Reply from 10.0.254.4: bytes=32 time=2ms TTL=64
Reply from 10.0.254.4: bytes=32 time=2ms TTL=64

Ping statistics for 10.0.254.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying IPSec Phase 1:

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
198.51.100.46    203.0.113.90     QM_IDLE           1001 ACTIVE
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying IPSec Phase 2:

```
R1#show crypto ipsec sa
interface: FastEthernet0/0/0
    Crypto map tag: IPSEC_VPN_CM, local addr 203.0.113.90

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.254.0/255.255.255.0/0/0)
   current_peer 198.51.100.46 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 1004, #pkts encrypt: 1004, #pkts digest: 1004
    #pkts decaps: 1004, #pkts decrypt: 1004, #pkts verify: 1004
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 203.0.113.90, remote crypto endpt.: 198.51.100.46
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0/0
     current outbound spi: 0x6C59604B(1817796683)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF693ABB1(4136872881)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: IPSEC_VPN_CM
        sa timing: remaining key lifetime (k/sec): (4264455/3103)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)
```

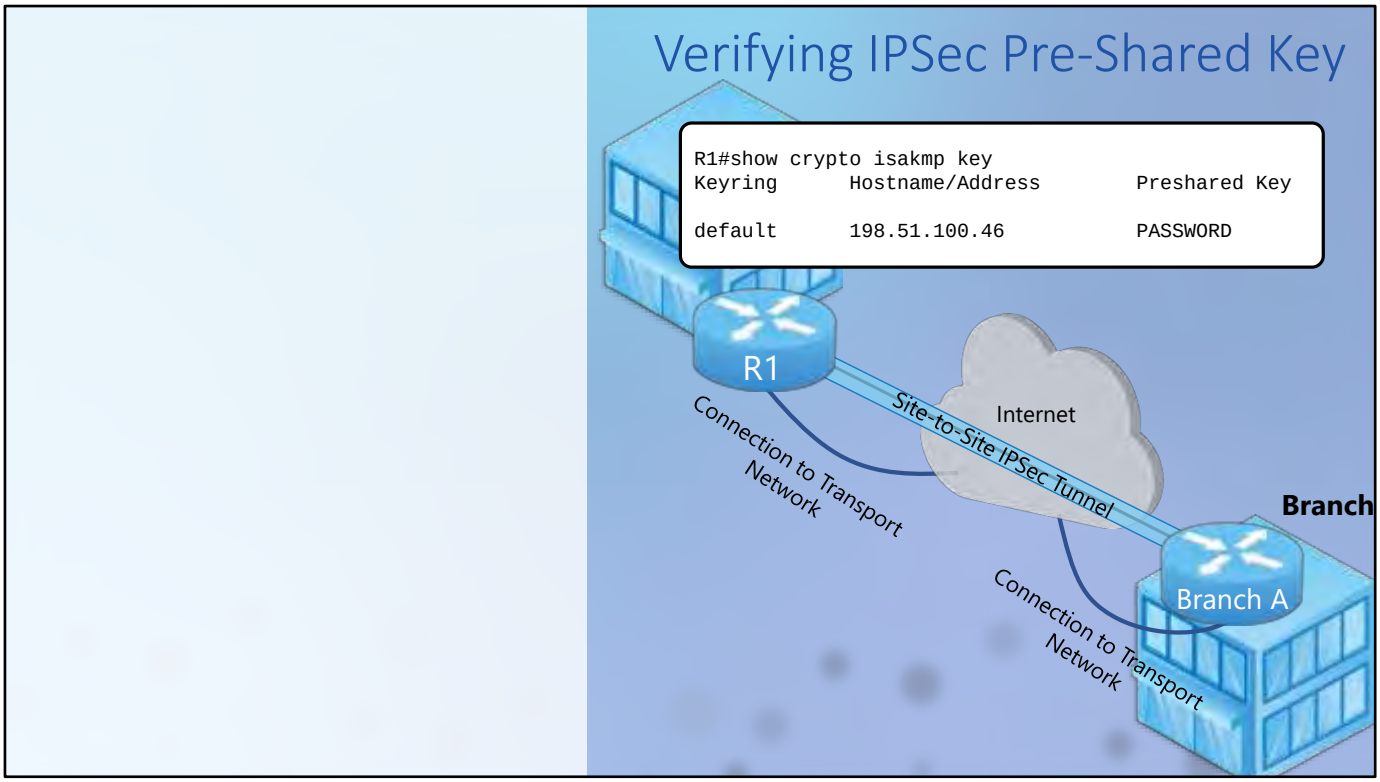
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 203.0.113.90, remote crypto endpt.: 198.51.100.46
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0/0
     current outbound spi: 0x6C59604B(1817796683)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xF693ABB1(4136872881)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: IPSEC_VPN_CM
        sa timing: remaining key lifetime (k/sec): (4264455/3103)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x6C59604B(1817796683)
        transform: esp-256-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: IPSEC_VPN_CM
        sa timing: remaining key lifetime (k/sec): (4264455/3103)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:
     outbound pcp sas:
R1#
```

©2023 by StormWind LLC. All rights reserved.

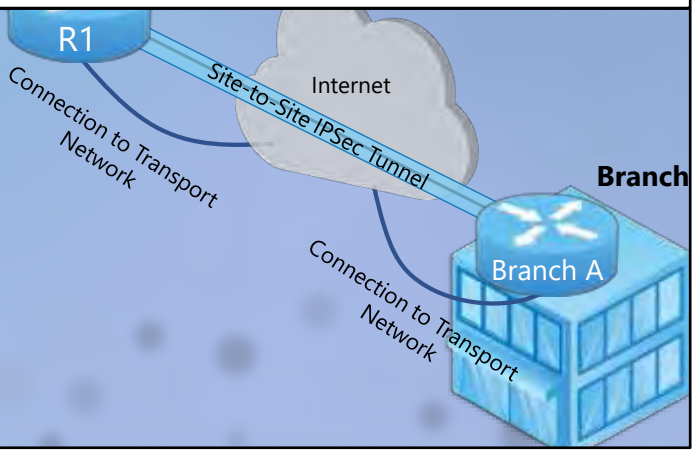
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying IPSec Policy

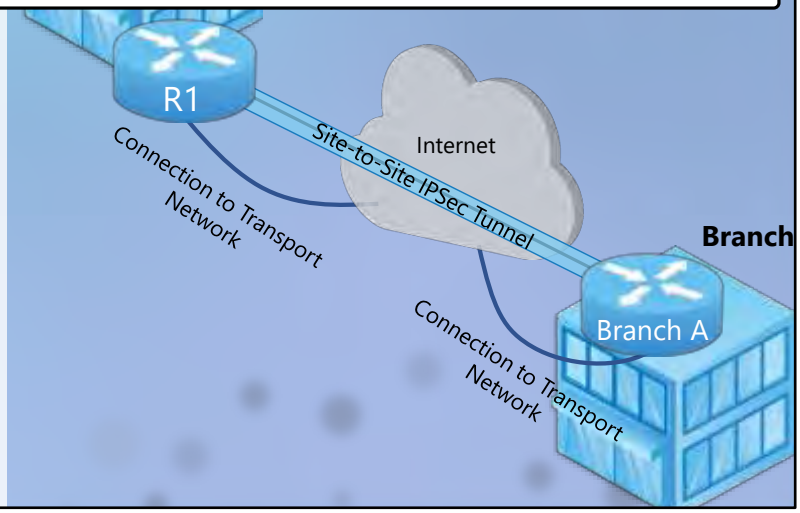
```
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   AES - Advanced Encryption Standard (256 bit keys).
        hash algorithm:         Secure Hash Standard 2 (256 bit)
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #16 (4096 bit)
        lifetime:               86400 seconds, no volume limit
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

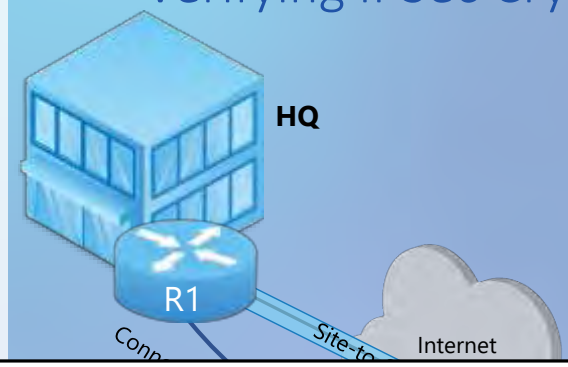
Verifying IPSec Transform-Set

```
R1#show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set IPSEC_VPN_TRANSFORM: { esp-256-aes esp-sha256-hmac  }
   will negotiate = { Tunnel,  },
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying IPSec Crypto-Map

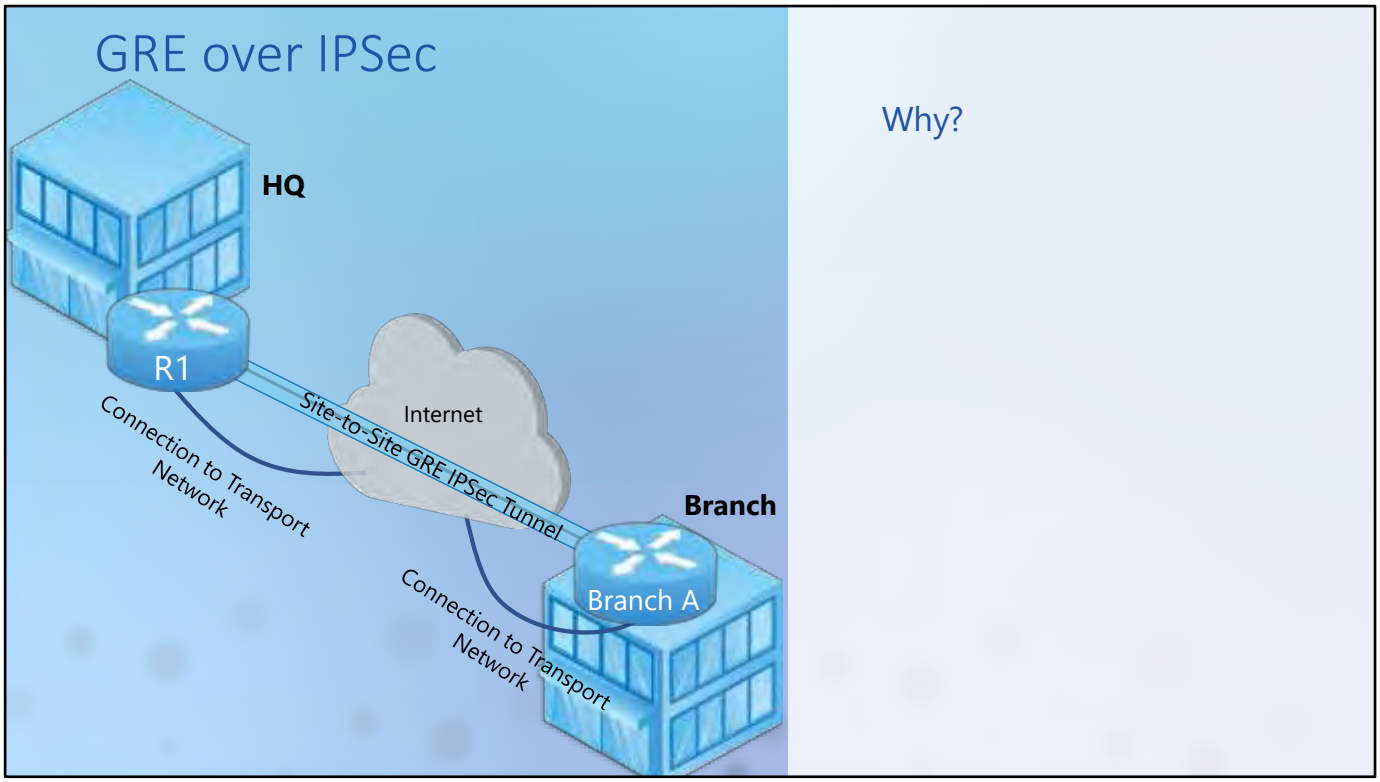



```
R1#show crypto map
Crypto Map IPv4 "IPSEC_VPN_CM" 10 ipsec-isakmp
        Peer = 198.51.100.46
        Extended IP access list IPSEC_VPN_ACL
            access-list IPSEC_VPN_ACL permit ip 10.0.0.0 0.255.255.255 10.0.254.0 0.255.255.255
        Current peer: 198.51.100.46
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                IPSEC_VPN_TRANSFORM:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map IPSEC_VPN_CM:
                FastEthernet0/0/0
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

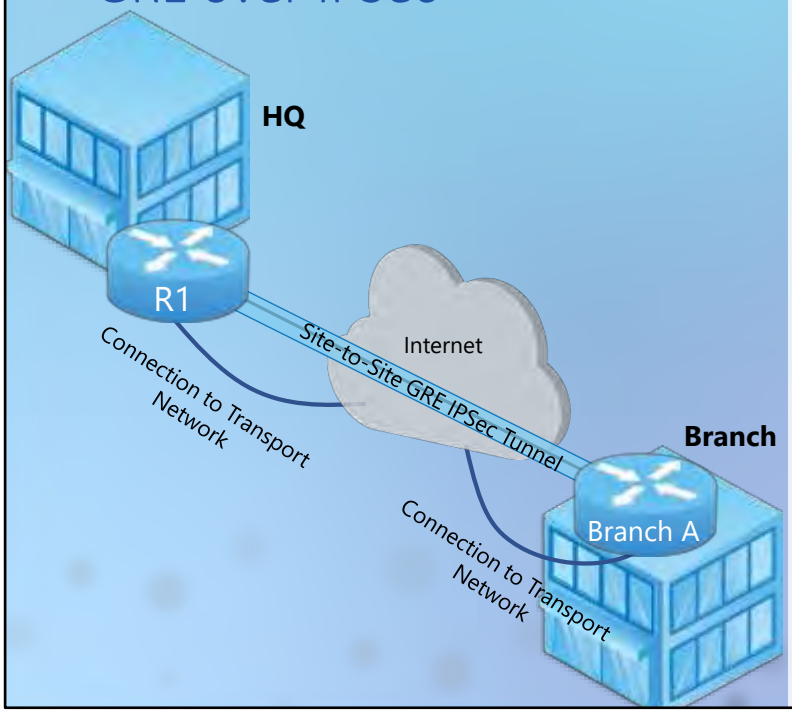
GRE over IPSec Tunnel Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec



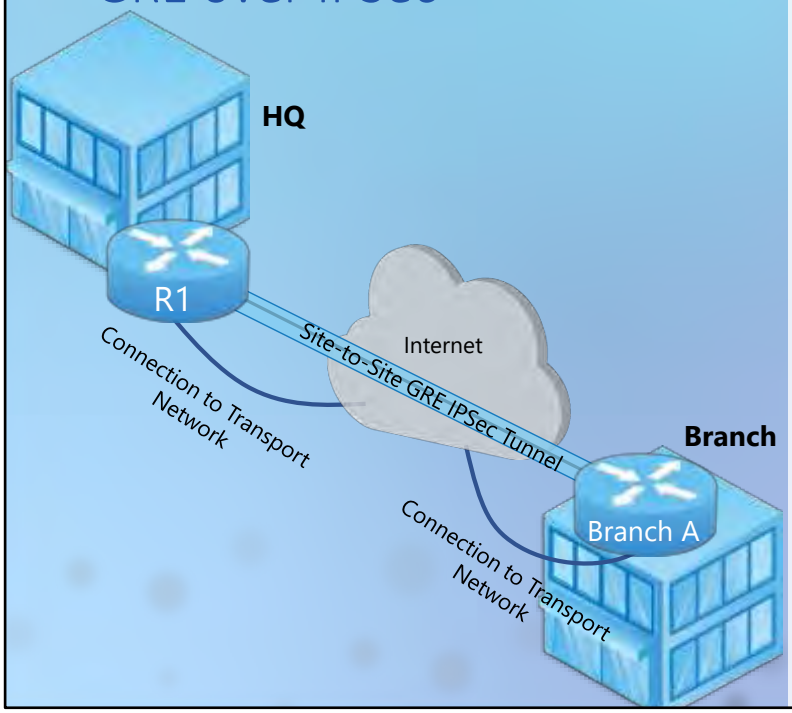
Why?

IPSec VPNs don't natively support routing protocols but they are really great at protecting traffic

GRE Tunnels natively support routing protocols, but they are horrible at protecting traffic

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec



Why?

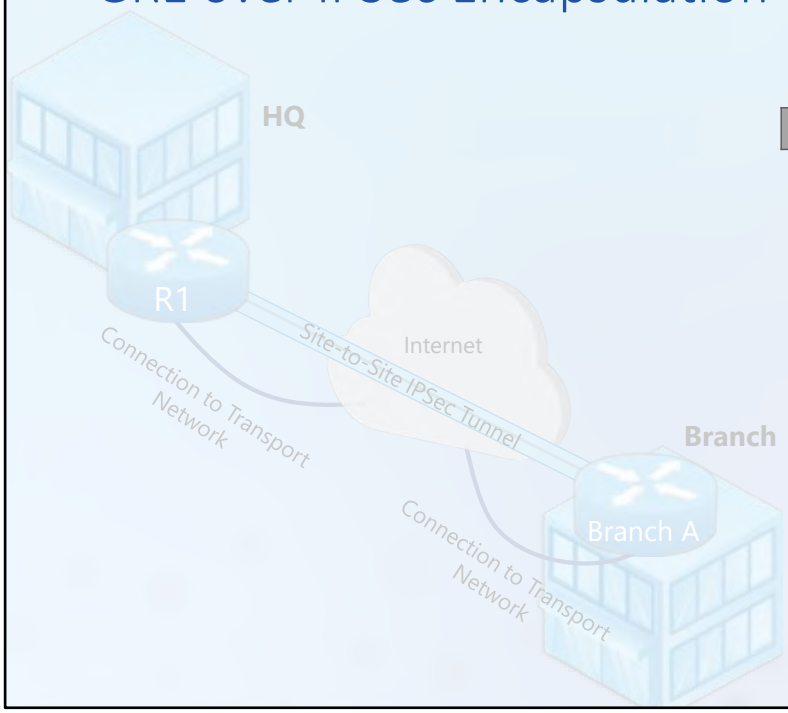
IPSec VPNs don't natively support routing protocols but they are really great at protecting traffic

GRE Tunnels natively support routing protocols, but they are horrible at protecting traffic

GRE tunnel is used for routing / IPSec is used to encrypt the GRE tunnel

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

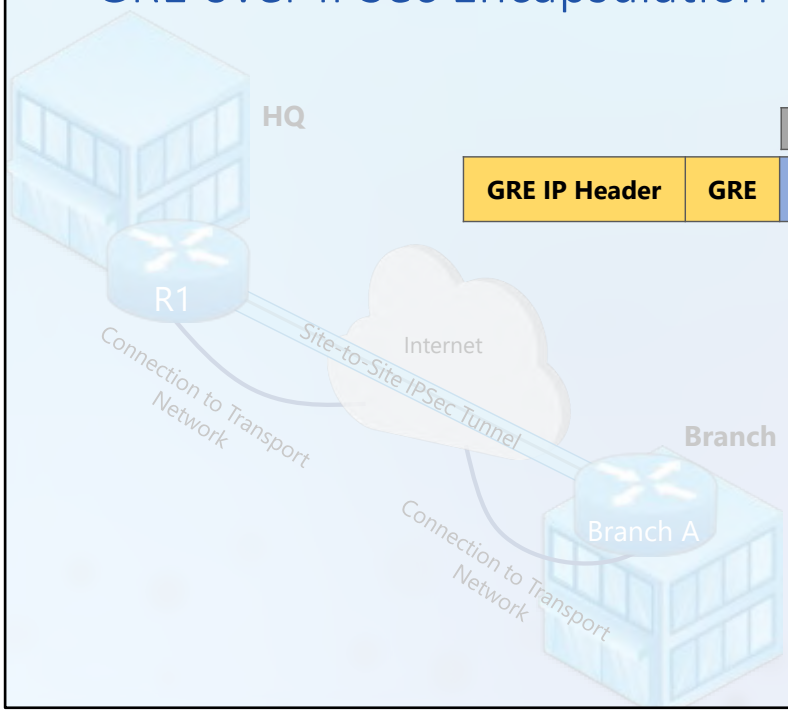
GRE over IPSec Encapsulation



Original IP Header	TCP/UDP	Data

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

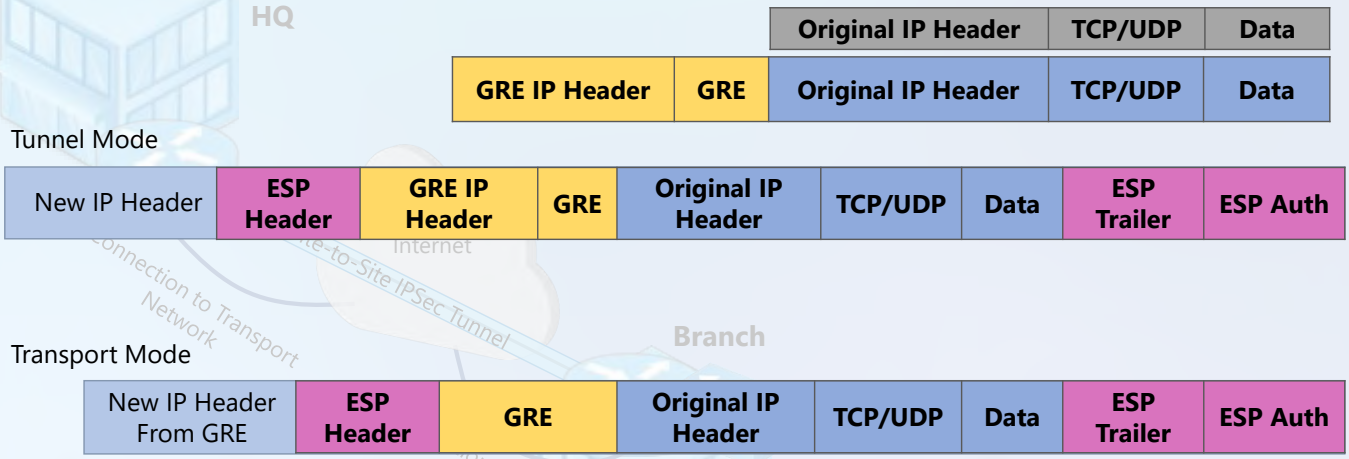
GRE over IPSec Encapsulation



		Original IP Header	TCP/UDP	Data
GRE IP Header	GRE	Original IP Header	TCP/UDP	Data

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Encapsulation



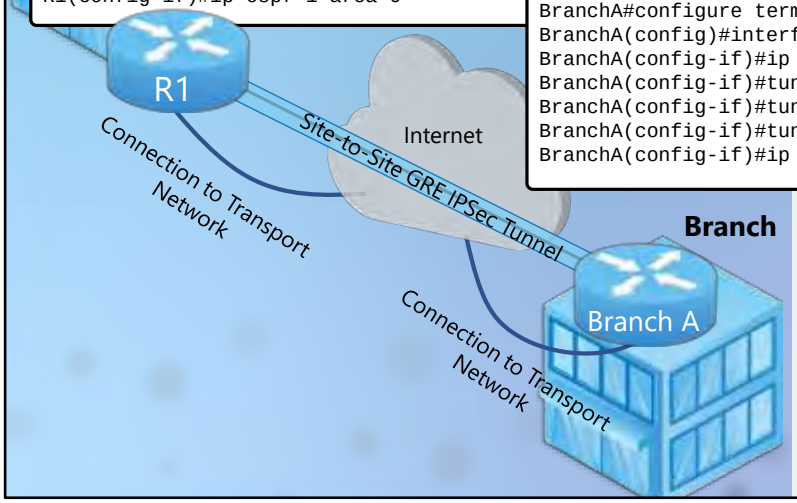
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Configuration

```
R1#configure terminal
R1(config)#int tunnel 1
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#tunnel source fastEthernet 0/0/0
R1(config-if)#tunnel destination 198.51.100.46
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip ospf 1 area 0
```

Define GRE Tunnels

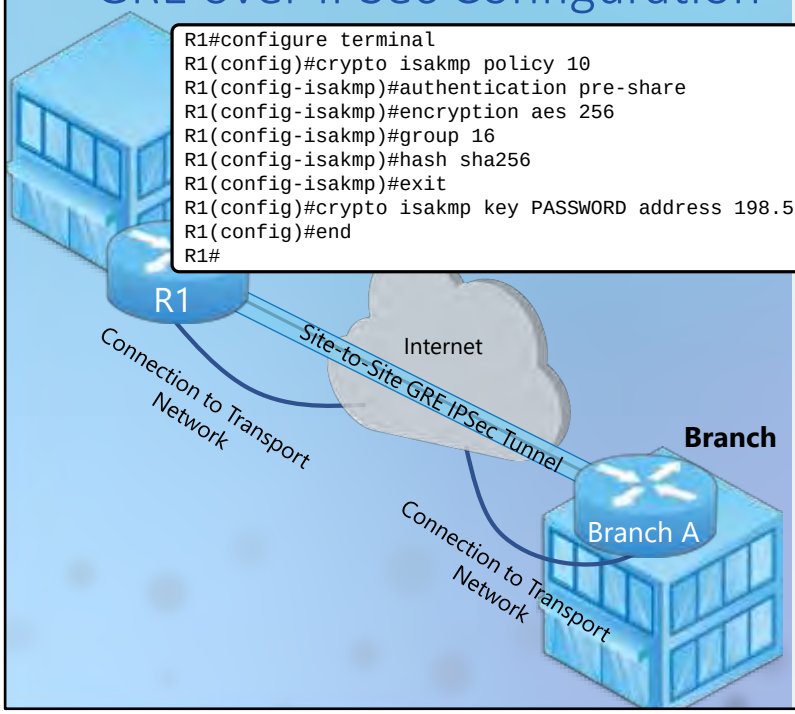
```
BranchA#configure terminal
BranchA(config)#interface tunnel 1
BranchA(config-if)#ip address 172.16.1.2 255.255.255.252
BranchA(config-if)#tunnel source GigabitEthernet0/1
BranchA(config-if)#tunnel destination 203.0.113.90
BranchA(config-if)#tunnel mode gre ip
BranchA(config-if)#ip ospf 1 area 0
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Configuration

```
R1#configure terminal
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#group 16
R1(config-isakmp)#hash sha256
R1(config-isakmp)#exit
R1(config)#crypto isakmp key PASSWORD address 198.51.100.46
R1(config)#end
R1#
```



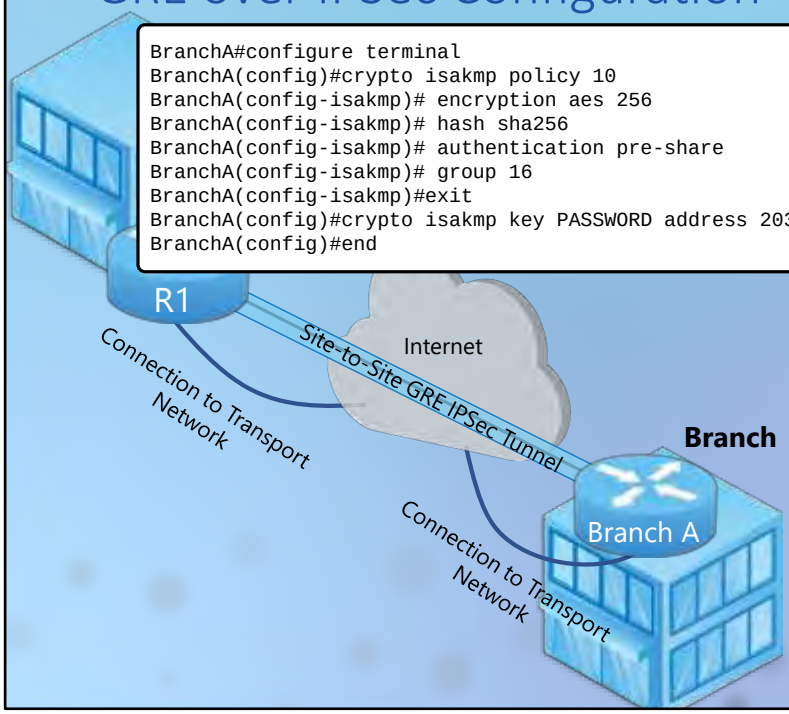
Define Phase 1 ISAKMP Policy

- Hashing
- Encryption
- DH
- Authentication
- Lifetime

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Configuration

```
BranchA#configure terminal
BranchA(config)#crypto isakmp policy 10
BranchA(config-isakmp)# encryption aes 256
BranchA(config-isakmp)# hash sha256
BranchA(config-isakmp)# authentication pre-share
BranchA(config-isakmp)# group 16
BranchA(config-isakmp)#exit
BranchA(config)#crypto isakmp key PASSWORD address 203.0.113.90
BranchA(config)#end
```

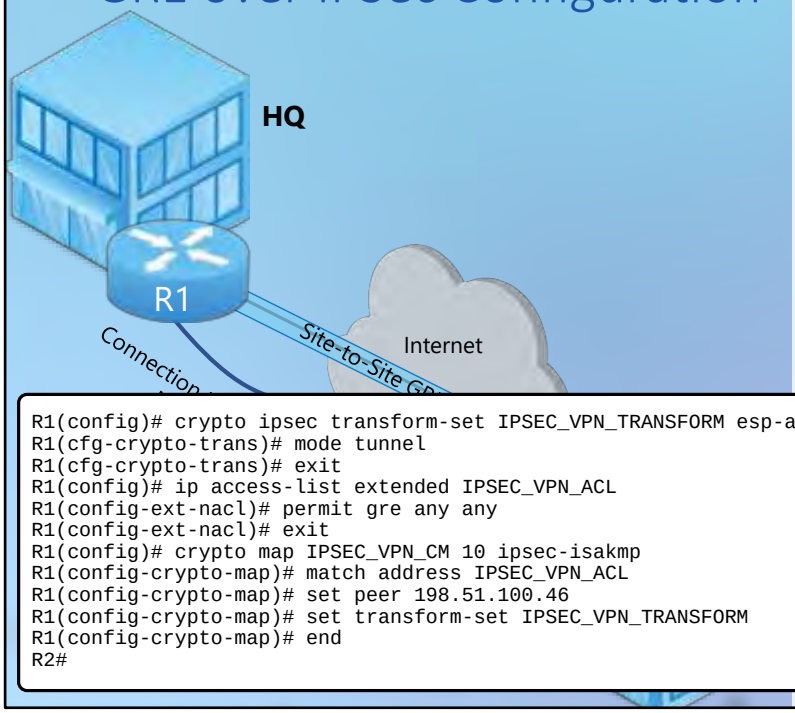


Define Phase 1 ISAKMP Policy

- Hashing
- Encryption
- DH
- Authentication
- Lifetime

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Configuration



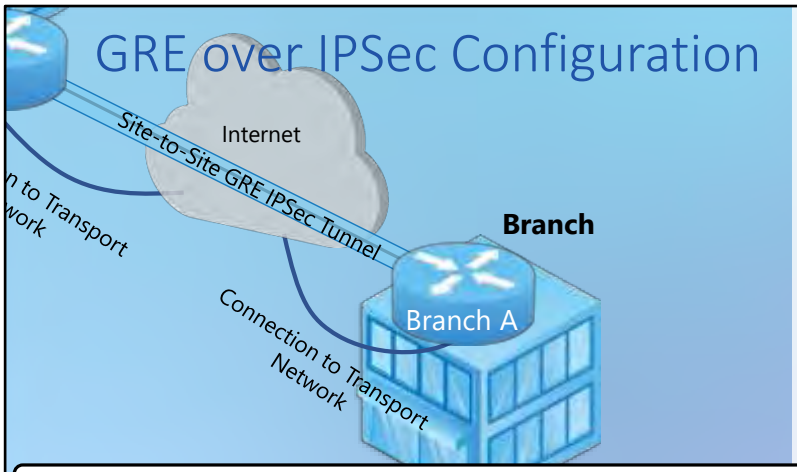
Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?

```
R1(config)# crypto ipsec transform-set IPSEC_VPN_TRANSFORM esp-aes 256 esp-sha256-hmac
R1(cfg-crypto-trans)# mode tunnel
R1(cfg-crypto-trans)# exit
R1(config)# ip access-list extended IPSEC_VPN_ACL
R1(config-ext-nacl)# permit gre any any
R1(config-ext-nacl)# exit
R1(config)# crypto map IPSEC_VPN_CM 10 ipsec-isakmp
R1(config-crypto-map)# match address IPSEC_VPN_ACL
R1(config-crypto-map)# set peer 198.51.100.46
R1(config-crypto-map)# set transform-set IPSEC_VPN_TRANSFORM
R1(config-crypto-map)# end
R2#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Configuration



Define Phase 2 IPSec Policy

- Where is the tunnel going?
- What is going in tunnel?
- How is the traffic treated?

```
BranchA(config)# crypto ipsec transform-set IPSEC_VPN_TRANSFORM esp-aes 256 esp-sha256-hmac
BranchA(cfg-crypto-trans)# mode tunnel
BranchA(cfg-crypto-trans)# exit
BranchA(config)# ip access-list extended IPSEC_VPN_ACL
BranchA(config-ext-nacl)# permit gre any any
BranchA(config-ext-nacl)# exit
BranchA(config)# crypto map IPSEC_VPN_CM 10 ipsec-isakmp
BranchA(config-crypto-map)# set peer 203.0.113.90
BranchA(config-crypto-map)# set transform-set IPSEC_VPN_TRANSFORM
BranchA(config-crypto-map)# match address IPSEC_VPN_ACL
BranchA(config-crypto-map)#end
```

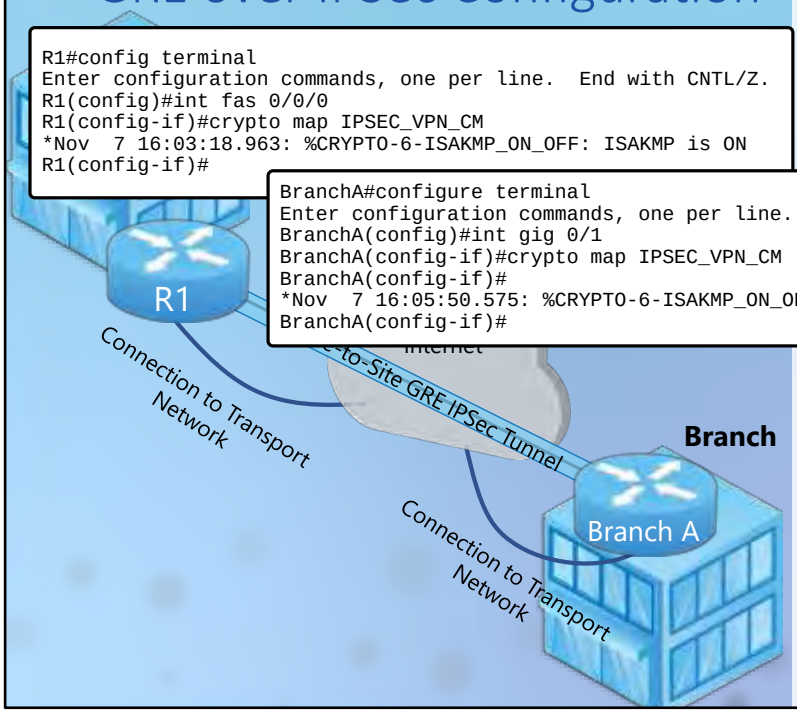
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Configuration

```
R1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int fas 0/0/0
R1(config-if)#crypto map IPSEC_VPN_CM
*Nov  7 16:03:18.963: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#
```

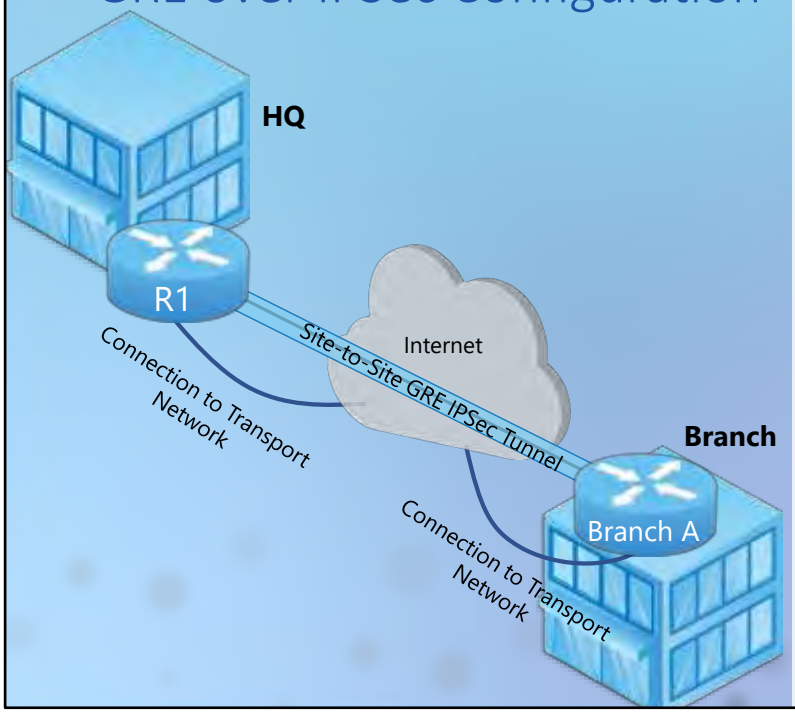
Apply to Outgoing Interface

```
BranchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
BranchA(config)#int gig 0/1
BranchA(config-if)#crypto map IPSEC_VPN_CM
BranchA(config-if)#
*Nov  7 16:05:50.575: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
BranchA(config-if)#
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Configuration



Verification is the same as covered before:

Verify GRE with:

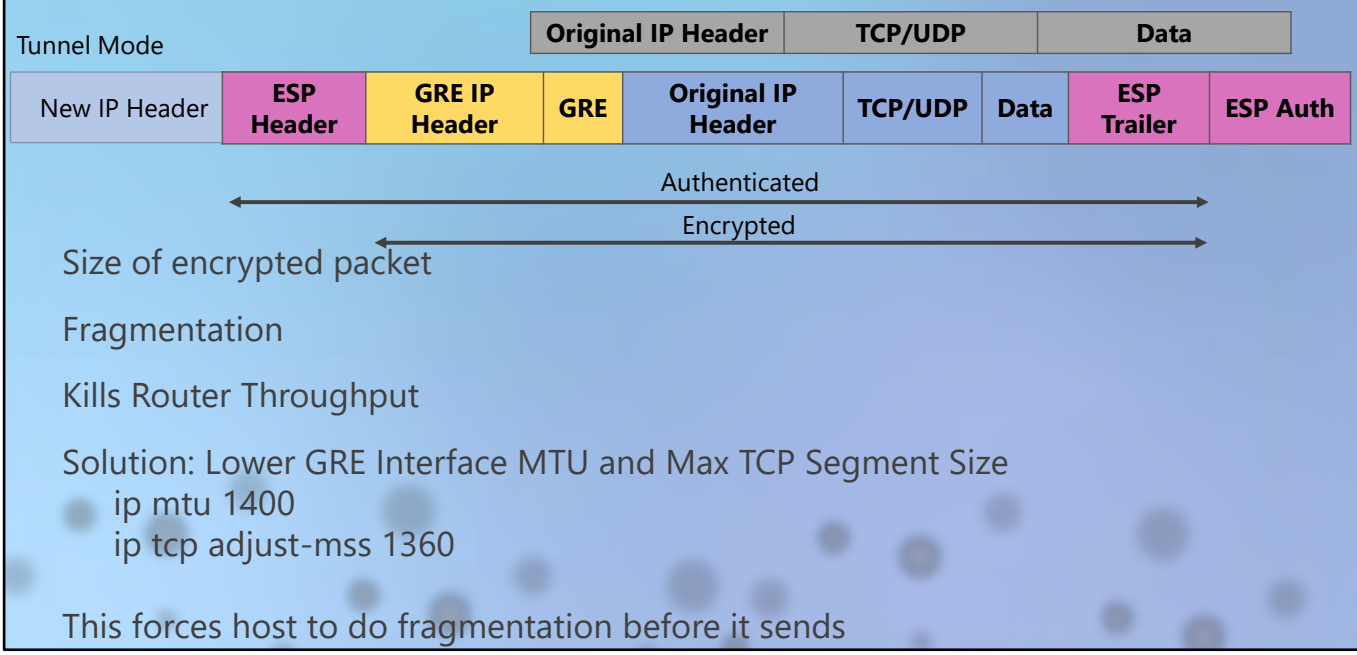
```
show interface tunnel tun_num
```

Verify IPSec with:

```
show crypto isakmp sa
show crypto ipsec sa
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

GRE over IPSec Issues



Size of encrypted packet

Fragmentation

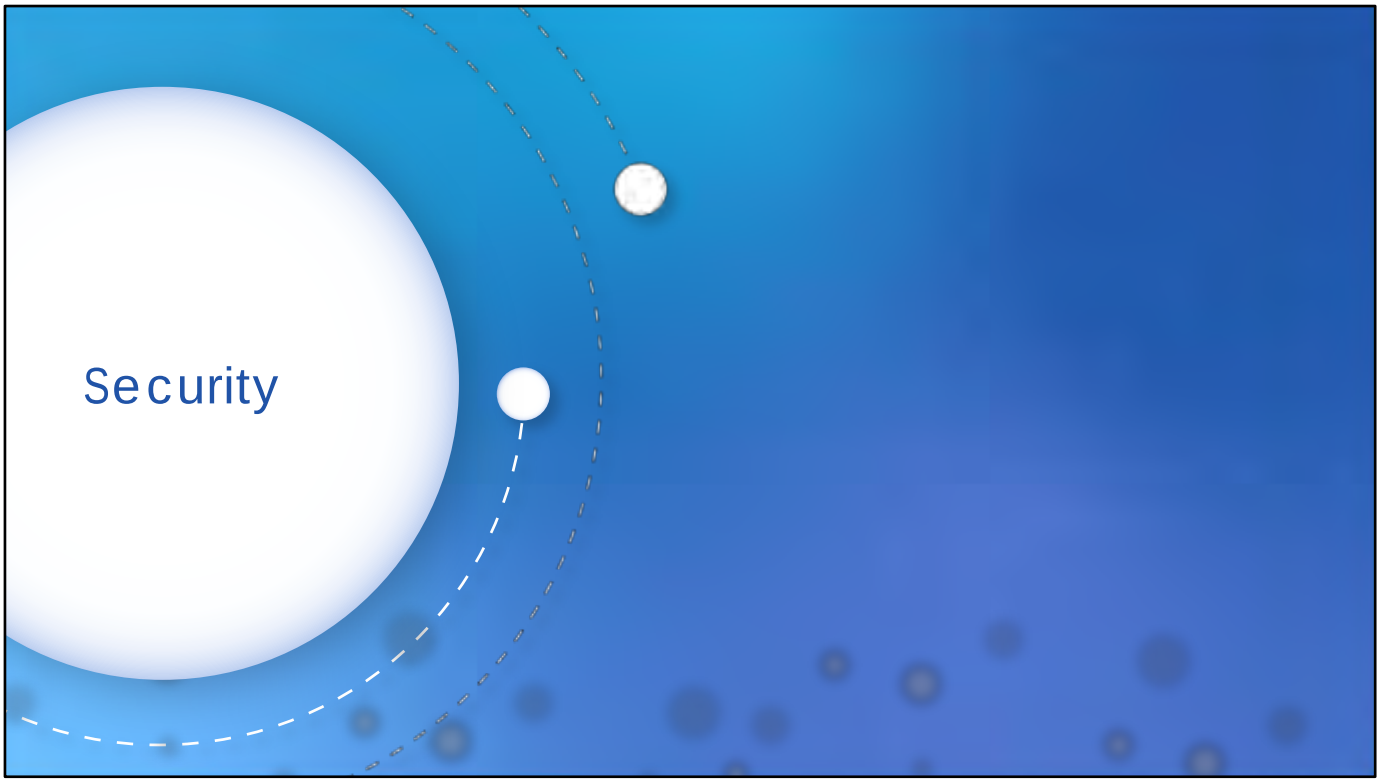
Kills Router Throughput

Solution: Lower GRE Interface MTU and Max TCP Segment Size

```
ip mtu 1400
ip tcp adjust-mss 1360
```

This forces host to do fragmentation before it sends

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Device Access, Authentication Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Privileged EXEC Mode

By default authentication is not required to access privileged EXEC mode:

Enable password prevents unauthorized access to privilege mode

```
ASW1(config)# enable password cisco
```

Enable secret stores the password as a hash

```
ASW1(config)# enable secret cisco
```

Enable secret vs **Enable password**

```
ASW1#show run | include enable
enable secret 5 $1$b0RL$rJiwafa.QEWOB992KQzCS0
enable password cisco
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Privileged EXEC Mode

Enable secret options

```
R1(config)#enable secret ?
  0       Specifies an UNENCRYPTED password will follow
  5       Specifies a MD5 HASHED secret will follow
  8       Specifies a PBKDF2 HASHED secret will follow
  9       Specifies a SCRYPT HASHED secret will follow
  LINE    The UNENCRYPTED (cleartext) 'enable' secret
  level   Set exec level password
```

Enable algorithm-type

```
R1(config)#enable algorithm-type ?
  md5     Encode the password using the MD5 algorithm
  scrypt  Encode the password using the SCRYPT hashing algorithm
  sha256  Encode the password using the PBKDF2 hashing algorithm
```

Enable algorithm-type stores the password as a hash

```
R1(config)#enable algorithm-type sha256 secret cisco
R1(config)#do sho run | i enable
enable secret 8 $8$9F9awpzr9kDJXm$VIWU3nfsY7Ee/u.rJUwdLQtUW5sg2qo0kCo99FRvZdk
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Console and VTY Lines

Line Passwords

```
ASW1#show run | b line
line con 0
 exec-timeout 0 0
 password cisco
 login
 logging synchronous
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
end
```

logging synchronous: prevents logs from interrupting command input
password: sets password on the line
login: enables the use of the password on the line
exec-timeout: controls idle timer for auto logout

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Console and VTY Lines

Usernames and Passwords

```
ASW1 #configure terminal
ASW1(config)#username RAYMOND password AWESOME
…or…
ASW1(config)#username RAYMOND secret AWESOME
ASW1(config)#line vty 0 4
ASW1(config-line)#login local
ASW1(config-line)#end
ASW1#show run | b line
line vty 0 4
 exec-timeout 0 0
 password cisco
 login local
!
End
ASW1#show run | include username
username RAYMOND password 0 AWESOME
username RAYMOND secret 5 $1$TP/I$47x2WjpeZYFbPdw7fKqQh1
```

login local: enables the password on the line using the local username and password database / ignores the line password

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Securing Console and VTY Lines

Usernames and Passwords

```
ASW1 #configure terminal
ASW1(config)#username RAYMOND password AWESOME
…or…
ASW1(config)#username RAYMOND secret AWESOME
```

```
R1(config)#username RAYMOND algorithm-type ?
  md5     Encode the password using the MD5 algorithm
  scrypt  Encode the password using the SCRYPT hashing algorithm
  sha256  Encode the password using the PBKDF2 hashing algorithm

R1(config)#username RAYMOND algorithm-type sha256 secret cisco

R1(config)#do sho run | i username
username RAYMOND secret 8 $8$yqKZVyUNhfu2UF$dS1EXlZxv.tSqvO3XmzPn73euFLBZwA4.rKW8ypaJQM
```

```
username RAYMOND password 0 AWESOME
username RAYMOND secret 5 $1$TP/I$47x2WjpeZYFbPdw7fKqQh1
```

login local: enables the password on the line using the local username and password database / ignores the line password

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying Console and VTY Connections

Verifying connections with **show users:**

```
ASW1#show users
    Line    User       Host(s)     Idle       Location
   0 con 0             idle        00:00:00
*  1 vty 0             idle        00:00:00   192.168.2.103
   2 vty 1  admin      idle        00:00:08   172.16.34.3


! To clear a session type:
clear line line_number

line_number = the number on the left of the output
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Encrypting Plain-Text Passwords

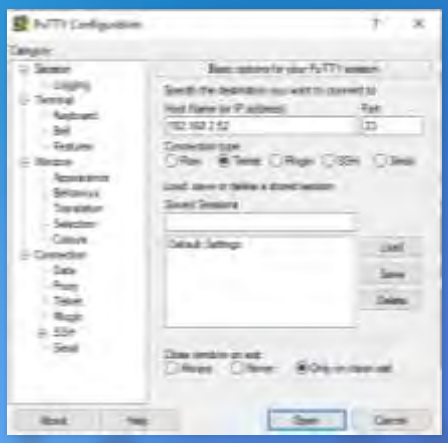
To encrypt plain text passwords, use this command:

```
ASW1#show run | include enable
enable secret 5 $1$b0RL$rJiwafa.QEWOB992KQzCS0
enable password cisco

ASW1(config)#service password-encryption

ASW1#show run | include enable
enable secret 5 $1$b0RL$rJiwafa.QEWOB992KQzCS0
enable password 7 110A1016141D
ASW1#show run | b line
line con 0
 exec-timeout 0 0
 password 7 0822455D0A16091610
 logging synchronous
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password 7 0822455D0A16091610
 login
```

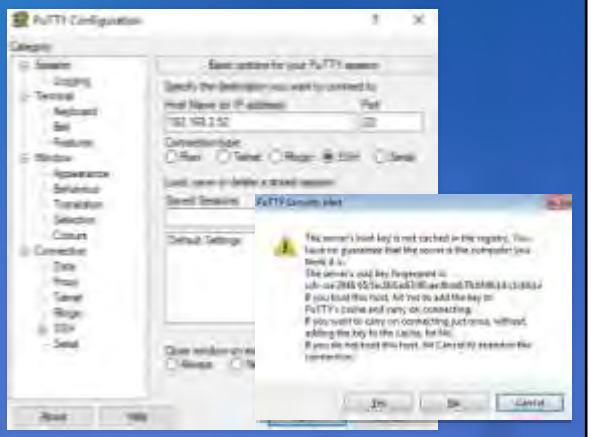
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Telnet vs SSH

Telnet:
Non-Encrypted communication



SSH:
Encrypted communication



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Configure Secure Shell (SSH)

```
ASW1#config t
ASW1(config)#hostname ASW1
ASW1(config)#ip domain-name stormwindciscodemos.com
ASW1(config)#username raymond secret awesome

ASW1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: ASW1.stormwindciscodemos.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-
exportable...[OK]

ASW1(config)#line vty 0 4
ASW1(config-line)#login local
ASW1(config-line)#transport input ssh
ASW1(config-line)#exit
ASW1(config)#ip ssh version 2
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Telnet vs SSH

To verify that SSH is enabled: **show ip ssh**

```
ASW1#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

To view any active SSH sessions: **show ssh**

```
ASW1#show ssh
%No SSHv1 server connections running.
%No SSHv2 server connections running.
```

```
ASW1#show ssh
%No SSHv1 server connections running.
Connection Version Mode Encryption  Hmac         State             Username
1          2.0     IN   aes256-cbc  hmac-sha1    Session started    raymond
1          2.0     OUT  aes256-cbc  hmac-sha1    Session started    raymond
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Authentication

Authentication – proving you are who you say you are

Authorization – identifying what are you allowed to access

Accounting – keeping track of what you do

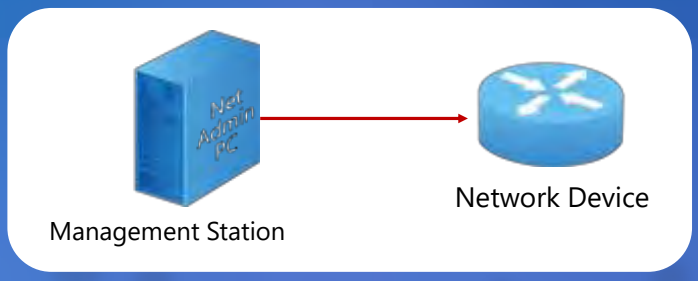
Local Database – database on individual network devices

AAA Server – database on centralized external server

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Configuration – Local Database

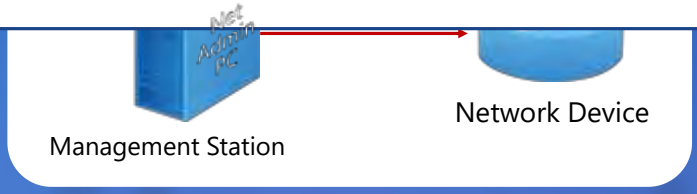
```
R1#configure terminal
R1(config)#username raymond privilege 15 secret awesome
R1(config)#aaa new-model
R1(config)#aaa authentication login AAA_AUTH_VTY local
R1(config)#aaa authorization exec default local
R1(config)#line vty 0 4
R1(config-line)#login authentication AAA_AUTH_VTY
R1(config-line)#
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Common Criteria – Local Database

```
R1#configure terminal
R1(config)#username raymond privilege 15 secret awesome
R1(config)#aaa new-model
R1(config)#aaa common-criteria policy ENCOR
R1(config-cc-policy)#char-changes 4
R1(config-cc-policy)#max-length 24
R1(config-cc-policy)#min-length 8
R1(config-cc-policy)#lifetime month 3
R1(config-cc-policy)#exit
R1(config)#username raymond priv 15 common-criteria-policy ENCOR secret awesome
R1(config)#aaa authentication login default local
R1(config)#aaa authorization exec default local
R1(config)#line vty 0 4
R1(config-line)#login authentication default
R1(config-line)#
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Authentication

Authentication – proving you are who you say you are

Authorization – identifying what are you allowed to access

Accounting – keeping track of what you do

Cisco switches support two main protocols to communicate with AAA Server:

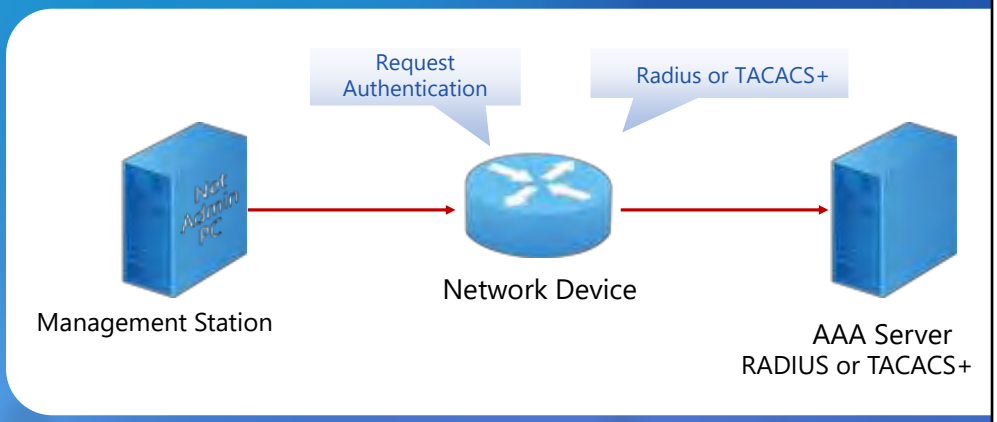
Radius – open standard using UDP

TACACS+ - Cisco proprietary using TCP

©2023 by StormWind LLC. All rights reserved.

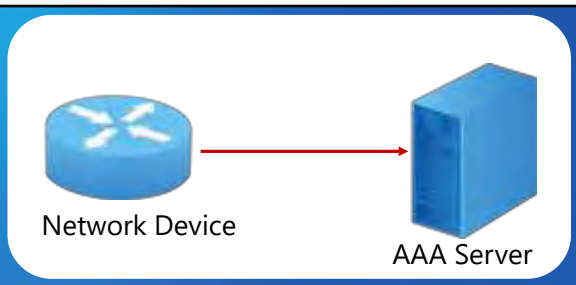
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Authentication - Server



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Radius vs Tacacs+



Radius

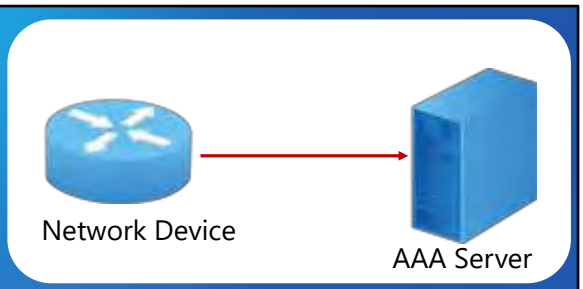
- UDP ports 1812 and 1813
- Combines authentication and authorization and separates accounting
- One-way, unidirectional, with a single challenge response
- Encrypts only password in packet

TACACS+

- TCP port 49
- Uses AAA model and separates three services
- Two-way, bidirectional, with multiple challenge responses
- Encrypts entire packet body

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

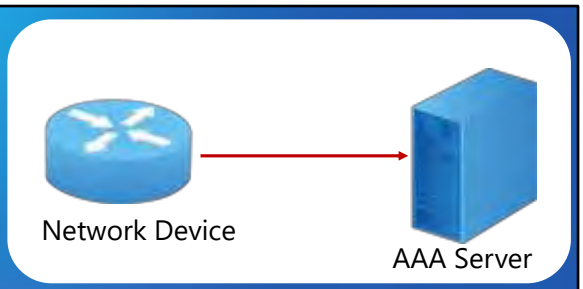
AAA Authentication Tacacs+




```
R1#configure terminal
R1(config)#username Raymond secret awesome
R1(config)#aaa new-model
R1(config)#tacacs server TACSRV1
R1(config-server-tacacs)#address ipv4 10.0.3.8
R1(config-server-tacacs)#port 49
R1(config-server-tacacs)#key PASSWORD
R1(config-server-tacacs)#exit
R1(config)#aaa group server tacacs+ TACGROUP
R1(config-sg-tacacs+)#server name TACSRV1
R1(config-sg-tacacs+)#exit
R1(config)#aaa authentication login default group TACGROUP local
R1(config)#aaa authorization exec default group TACGROUP local
R1(config)#line vty 0 4
R1(config-line)#login authentication default
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AAA Authentication Radius




```
R1#configure terminal
R1(config)#username raymond secret awesome
R1(config)#aaa new-model
R1(config)#radius server RADSRV1
R1(config-radius-server)#address ipv4 10.0.3.8 auth-port 1812 acct-port 1813
R1(config-radius-server)#key PASSWORD
R1(config-radius-server)#exit
R1(config)#aaa group server radius RADGROUP
R1(config-sg-radius)#server name RADSRV1
R1(config-sg-radius)#exit
R1(config)#aaa authentication login default group RADGROUP local
R1(config)#aaa authorization exec default group RADGROUP local
R1(config)#line vty 0 4
R1(config-line)#login authentication default
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Intro to Access-Control Lists (ACLs) and Wildcard Masks

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Access Control List

ACL

An ACL provides traffic identification

When traffic is identified, a variety of actions can be applied based on purpose:

- Permit, Deny, Change traffic direction, and more
  - NAT, Traffic Filter, QoS, PBR, Route Filter, etc…

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Access Control List

ACL
An ACL is made of Access Control Entries (ACEs) ACEs can be permit and deny statements Access Lists can be used on routers and switches

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Operation of ACLs

Avengers HQ ACL

1	Tony Stark	Permit
2	Steve Rogers	Permit
3	Bruce Banner	Permit
4	Thor Odinson	Deny
5	Natasha Romanoff	Permit
6	All Original Avengers	Permit
7	Pepper Potts	Deny
8	Carol Danvers	Permit
9	Peter Parker	Deny
10	Scott Lang	Deny
11	Hope Van Dyne	Deny
12	James Rhodes	Permit
13	Wanda Maximoff	Permit
14	Vision	Permit

1) Top Down Processing

2) Immediate Execution Upon A Match

3) Implicit Deny All At the Very End

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Operation of ACLs

Avengers HQ ACL

1	Tony Stark	Permit
2	Steve Rogers	Permit
3	Bruce Banner	Permit
4	All Original Avengers	Permit
5	Thor Odinson	Deny
6	Natasha Romanoff	Permit
7	Pepper Potts	Deny
8	Carol Danvers	Permit
9	Peter Parker	Deny
10	Scott Lang	Deny
11	Hope Van Dyne	Deny
12	James Rhodes	Permit
13	Wanda Maximoff	Permit
14	Vision	Permit

1) Top Down Processing

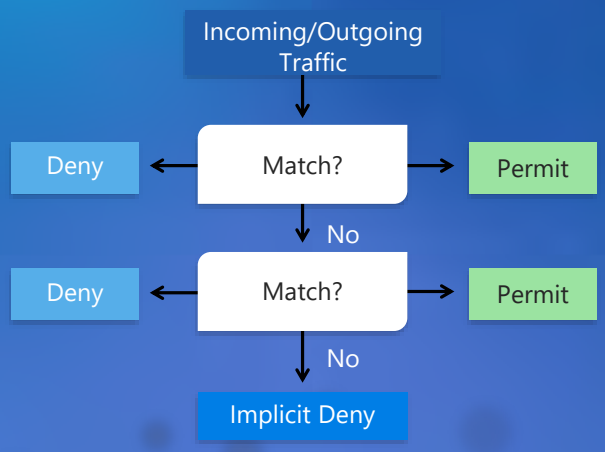
2) Immediate Execution Upon A Match

3) Implicit Deny All At the Very End

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Operation of ACLs



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Example ACL

```
Router(config)# ip access-list standard PRIVATE_IPS
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
Router(config-std-nacl)# permit 172.16.0.0 0.15.255.255
Router(config-std-nacl)# permit 192.168.0.0 0.0.255.255
Router(config-std-nacl)# exit
Router(config)# interface gig0/0
Router(config-if)# ip access-group PRIVATE_IPS in
```

Access List Entries (ACE)

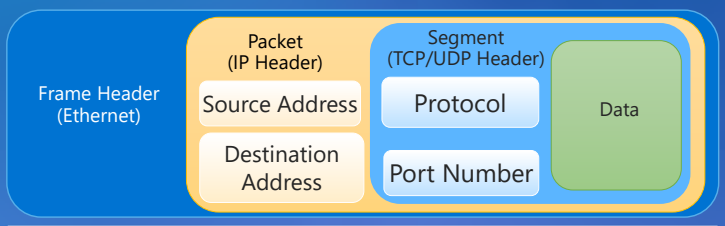
Application of an ACL

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ACL Types

Standard ACL

Only filters based on source IP address of packet



Extended ACL

Can filter based on source and destination IP address
Can filter based on different types of Layer 4 Protocols
Can filter based on different port numbers

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ACL Types

There are two ways to ID your ACLs		
ID	**IPv4 ACL Type**	**Number Range or Identifier**
Number	Standard	1-99, 1300-1999
Number	Extended	100-199, 2000-2699
Name	Standard	*Name*
Name	Extended	*Name*

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Numbered Standard ACLs

To configure a Numbered ACL, you will use “access-list”

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

*If no mask specified, default is 0.0.0.0 (Standard ACLs only)

```
Router#show access-lists
Standard IP access list 5
     10 permit 10.1.1.0, wildcard bits 0.0.0.255
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Named Standard ACLs

To configure Named Standard ACLs, you must use “ip access-list”

```
Router(config)#ip access-list standard TEST
Router(config-std-nacl)#permit 10.1.1.1
Router(config-std-nacl)#permit 10.2.0.0 0.0.255.255
```

```
Router #show access-lists
Standard IP access list TEST
    10 permit 10.1.1.1
    20 permit 10.2.0.0, wildcard bits 0.0.255.255
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

ACLs require **wildcard masks** to indicate the size of network address space to match

A wildcard mask looks like a “backward” or “inverted” subnet mask but it has a completely different purpose.

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

Examples:

0.0.0.255
0.0.0.240
0.0.240.255
0.0.252.255

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.XXXXXXXX – X = 0 or 1 since we "do not care"

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.XXXXXXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 0 – If X's are all 0's

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.XXXXXXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 0 – If X's are all 0's

10. 1. 1. 255 – If X's are all 1's

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.11111111 – Wildcard Mask in Binary

00001010.00000001.00000001.XXXXXXXX – X = 0 or 1 since we "do not care"

Range
- 10. 1. 1. 0 – If X's are all 0's
- 10. 1. 1. 255 – If X's are all 1's

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000XXXX – X = 0 or 1 since we "do not care"

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000XXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 0 – If X's are all 0's

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000XXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 0 – If X's are all 0's

10. 1. 1. 15 – If X's are all 1's

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

00001010.00000001.00000001.00000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0000XXXX – X = 0 or 1 since we "do not care"

Range

10.	1.	1.	0 – If X's are all 0's
10.	1.	1.	15 – If X's are all 1's

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100XXXX – X = 0 or 1 since we "do not care"

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100XXXX – X = 0 or 1 since we "do not care"

10. 1. 1. 64 – If X's are all 0's

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100XXXX – X = 0 or 1 since we "do not care"

10.	1.	1.	64 – If X's are all 0's
10.	1.	1.	79 – If X's are all 1's

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

00001010.00000001.00000001.01000000 – IP address in binary

00000000.00000000.00000000.00001111 – Wildcard Mask in Binary

00001010.00000001.00000001.0100XXXX – X = 0 or 1 since we "do not care"

Range
- 10. 1. 1. 64 – If X's are all 0's
- 10. 1. 1. 79 – If X's are all 1's

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 192.168.0.0 0.0.0.254
```

11000000.10101000.00000000.00000000 – IP address in binary

00000000.00000000.00000000.11111110 – Wildcard Mask in Binary

11000000.10101000.00000000.XXXXXXX0 – X = 0 or 1 since we "do not care"

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

What binary bits mean in a wildcard mask:

A 0 bit means **match**

"I care about this bit", "use this bit", "preserve this bit", "carry this bit down"

A 1 bit means **ignore**

"I DON'T care about this bit", "DON'T use this bit", "DON'T preserve this bit", "DON'T carry this bit down"

```
Router(config)#access-list 5 permit 192.168.0.1 0.0.0.254
```

11000000.10101000.00000000.00000001 – IP address in binary

00000000.00000000.00000000.11111110 – Wildcard Mask in Binary

11000000.10101000.00000000.XXXXXXX1 – X = 0 or 1 since we "do not care"

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

```
  255.255.255.255 - All 255s
- 255.255.255.    0 - Subnet mask
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

```
  255.255.255.255 - All 255s
- 255.255.255.   0 - Subnet mask
      0.   0.   0.255 – Wildcard Mask
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/24 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

```
  255.255.255.255 - All 255s
- 255.255.255.   0 - Subnet mask
      0.   0.   0.255 – Wildcard Mask
```

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.255
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

```
  255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask
      0.   0.   0.  15 – Wildcard Mask
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.0/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask
0. 0. 0. 15 – Wildcard Mask

```
Router(config)#access-list 5 permit 10.1.1.0 0.0.0.15
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.64/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.64/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.64/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

```
  255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask
      0.   0.   0.  15 – Wildcard Mask
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You want an ACL that will permit all traffic for the 10.1.1.64/28 network. What address and wildcard mask combination will accomplish this for you?

A quick way to determine a wildcard mask is subtracting the subnet mask from 255.255.255.255

255.255.255.255 - All 255s
- 255.255.255.240 - Subnet mask
0. 0. 0. 15 – Wildcard Mask

```
Router(config)#access-list 5 permit 10.1.1.64 0.0.0.15
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

First of all we could create 32 different entries using the technique we just covered.

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.2.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.3.0 0.0.0.255
…….etc…….
Router(config)#access-list 10 permit 172.16.29.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.30.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.31.0 0.0.0.255
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.31.255
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.1.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.2.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.3.0 0.0.0.255
……….etc…….
Router(config)#access-list 10 permit 172.16.29.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.30.0 0.0.0.255
Router(config)#access-list 10 permit 172.16.31.0 0.0.0.255
```

them together.

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.31.255
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.0.0 -	10101100.00010000.00000000.00000000
172.16.31.0 -	10101100.00010000.00011111.00000000

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.0.0 - 10101100.00010000.00000000.00000000
172.16.31.0 - 10101100.00010000.00011111.00000000

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.0.0 - 10101100.00010000.00000000.00000000
172.16.31.0 - 10101100.00010000.00011111.00000000

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.0.0 - 10101100.00010000.00000000.00000000
172.16.31.0 - 10101100.00010000.00011111.00000000

← Zeros | Ones →

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.0.0 - 10101100.00010000.00000000.00000000
172.16.31.0 - 10101100.00010000.00011111.00000000

← Zeros | Ones →

00000000.00000000.00011111.11111111 – Wildcard Mask

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

```
172.16.0.0 -   10101100.00010000.00000000.00000000
172.16.31.0 -  10101100.00010000.00011111.00000000
               ←———— Zeros | Ones ————→
               00000000.00000000.00011111.11111111 – Wildcard Mask
                     0.       0.      31.     255
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

You need an ACL that will permit all traffic for the 172.16.0.0/24 network to the 172.16.31.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

```
172.16.0.0 -  10101100.00010000.00000000.00000000
172.16.31.0 -  10101100.00010000.00011111.00000000
                ←——— Zeros | Ones ———→
              00000000.00000000.00011111.11111111 – Wildcard Mask
                    0.        0.       31.      255
```

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.31.255
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.10.0 - 10101100.00010000.00001010.00000000
172.16.26.0 - 10101100.00010000.00011010.00000000

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.10.0 - 10101100.00010000.00001010.00000000
172.16.26.0 - 10101100.00010000.00011010.00000000

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.10.0 - 10101100.00010000.00001010.00000000
172.16.26.0 - 10101100.00010000.00011010.00000000

← Zeros | Ones →

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

172.16.10.0 - 10101100.00010000.00001010.00000000
172.16.26.0 - 10101100.00010000.00011010.00000000

← Zeros | Ones →

00000000.00000000.00011111.11111111 – Wildcard Mask

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario: Be Careful

You need an ACL that will permit all traffic for the 172.16.10.0/24 network to the 172.16.26.0/24 network inclusive. What address and wildcard mask combination will accomplish this for you?

Or we could create an ACL that groups them together.

```
172.16.10.0 -   10101100.00010000.00001010.00000000
172.16.26.0 -   10101100.00010000.00011010.00000000
                ←——————— Zeros | Ones ———→
                00000000.00000000.00011111.11111111 – Wildcard Mask
                      0.        0.       31.      255
```

```
Router(config)#access-list 10 permit 172.16.0.0 0.0.31.255
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

10.10.10.248 to 10.10.10.255

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wildcard Masks

Scenario:

10.10.32.0/24 to 10.10.39.0/24

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Extended Access-Control Lists (ACLs)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Extended ACLs - Numbered

Extra Values:

- Protocol
- Source and Destination
- Operator / Port

```
Router(config)#access-list 101 deny ip host 172.16.1.25 host 8.8.8.8
Router(config)#access-list 101 permit tcp 172.16.1.0 0.0.0.255 any eq 23
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Extended ACLs - Named

```
Router(config)#ip access-list extended TEST
Router(config-ext-nacl)# deny ip host 172.16.1.25 host 8.8.8.8
Router(config-ext-nacl)# deny ip host 172.16.1.50 any
Router(config-ext-nacl)# deny tcp 172.16.1.0 0.0.0.255 any eq 23
Router(config-ext-nacl)# permit ip any any


Router # show access-list
Extended IP access list TEST
    10 deny ip host 172.16.1.25 host 8.8.8.8
    20 deny ip host 172.16.1.50 any
    30 deny tcp 172.16.1.0 0.0.0.255 any eq telnet
    40 permit ip any any
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Editing Named ACLs

To remove a single line item from a named ACL, you can use the “no <seq #>” command

```
Router # show access-list
Extended IP access list TEST
    10 deny ip host 172.16.1.25 host 8.8.8.8
    20 deny ip host 172.16.1.50 any
    30 deny tcp 172.16.1.0 0.0.0.255 any eq telnet
    40 permit ip any any

Router(config)#ip access-list extended TEST
Router(config-ext-nacl)#no 20
Router(config-ext-nacl)#end

Router #show ip access-list
Extended IP access list TEST
    10 deny ip host 172.16.1.25 host 8.8.8.8
    30 deny tcp 172.16.1.0 0.0.0.255 any eq telnet
    40 permit ip any any
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

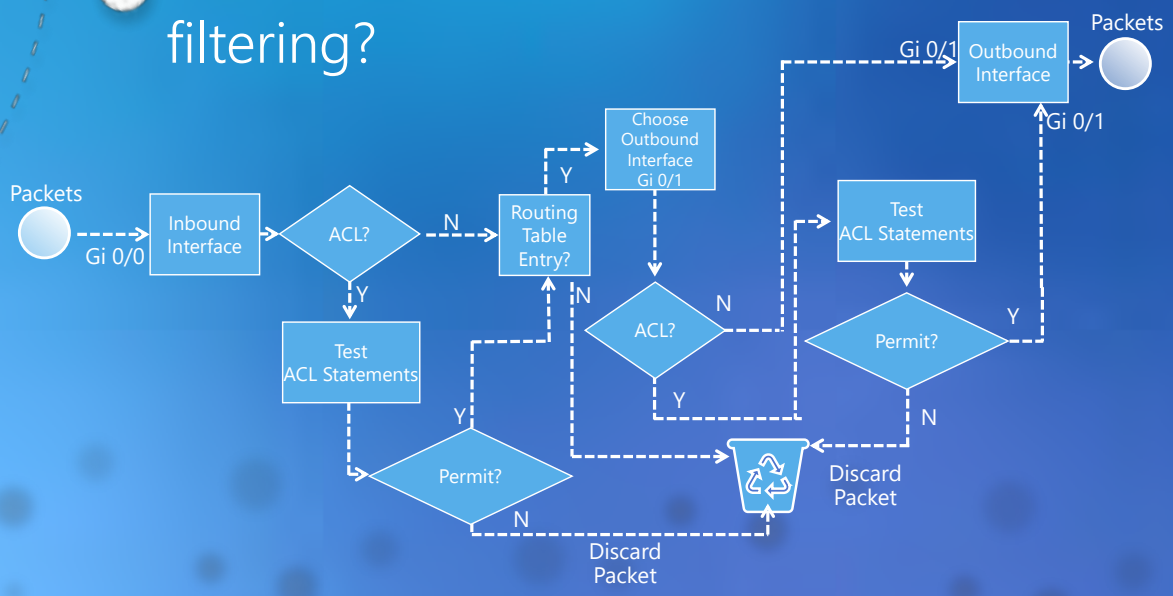
Editing Named ACLs

To add a single line item to a named ACL, you can use the “seq #” in the command to specify the location.

```
Router #show ip access-list
Extended IP access list TEST
    10 deny ip host 172.16.1.25 host 8.8.8.8
    30 deny tcp 172.16.1.0 0.0.0.255 any eq telnet
    40 permit ip any any

Router(config)#ip access-list extended TEST
Router(config-ext-nacl)#5 deny ip host 172.16.1.50 any
Router(config-ext-nacl)#end

Router # show access-list
Extended IP access list TEST
    5 deny ip host 172.16.1.50 any
   10 deny ip host 172.16.1.25 host 8.8.8.8
   30 deny tcp 172.16.1.0 0.0.0.255 any eq telnet
   40 permit ip any any
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

When is an ACL checked for traffic filtering?



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Applying ACLs for traffic filtering

```
Router(config)#int gigabitethernet 0/0
Router(config-if)#ip access-group TEST {in | out}
```

Important: Only one ACL is allowed per protocol, direction, and interface.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Verifying ACLs

```
Router#show access-lists
Standard IP access list SALES
    10 deny 10.1.1.0, wildcard bits 0.0.0.255
    20 permit 10.3.3.1
    30 permit 10.4.4.1
    40 permit 10.5.5.1
Extended IP access list HR
    10 permit tcp host 10.22.22.1 any eq telnet (25 matches)
    20 permit tcp host 10.33.33.1 any eq ftp
    30 permit tcp host 10.44.44.1 any eq ftp-data
```

```
Router#show ip interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
    Internet address is 10.1.1.1/24
    Broadcast address is 255.255.255.255
    Address determined by setup command
    MTU is 1500 bytes
    Helper address is not set
    Directed broadcast forwarding is disabled
    Outgoing access list is not set
    Inbound access list is SALES
    Proxy ARP is enabled
    Local Proxy ARP is disabled
    <text omitted>
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Removing ACLs

To remove the command off the interface:

```
R1(config-if)#no ip access-group [number|name] [in|out]
```

To delete the entire ACL

```
R1(config)#no ip access-list number
R1(config)#no ip access-list [standard|extended] name
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ACL Troubleshooting Checklist

Is the ACL logic correct?

Is the ACL applied inline with the packet flow?

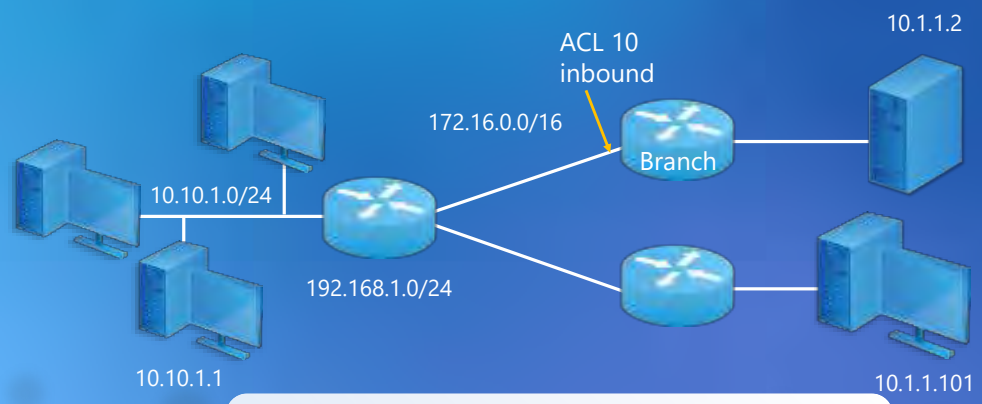
Is the ACL applied in the correct direction?

- Top down processing
- Immediate execution upon a match
- Implicit deny any

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ACL Troubleshooting 1

Host 10.10.1.1 has no connectivity with 10.1.1.2.

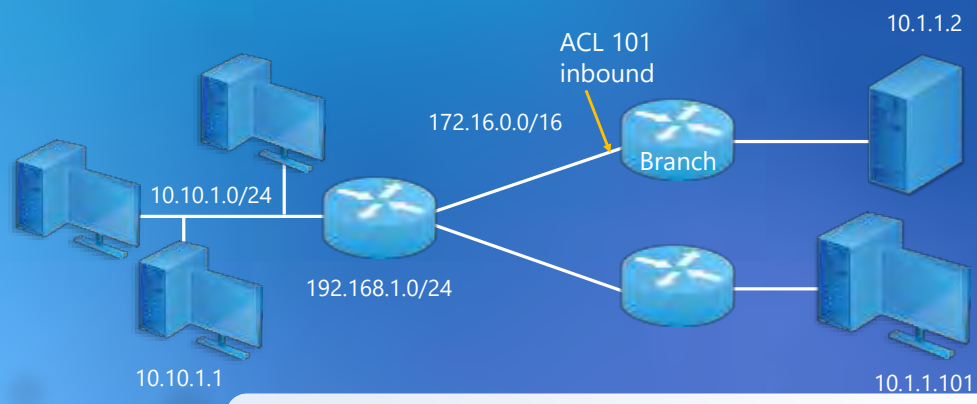



```
Branch#show access-lists 10
Standard IP access list 10
    10 deny 10.10.1.0, wildcard bits 0.0.0.255
    20 permit 10.10.1.1
    30 permit any
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ACL Troubleshooting 2

Host 10.10.1.1 has no http connectivity to 10.1.1.2.

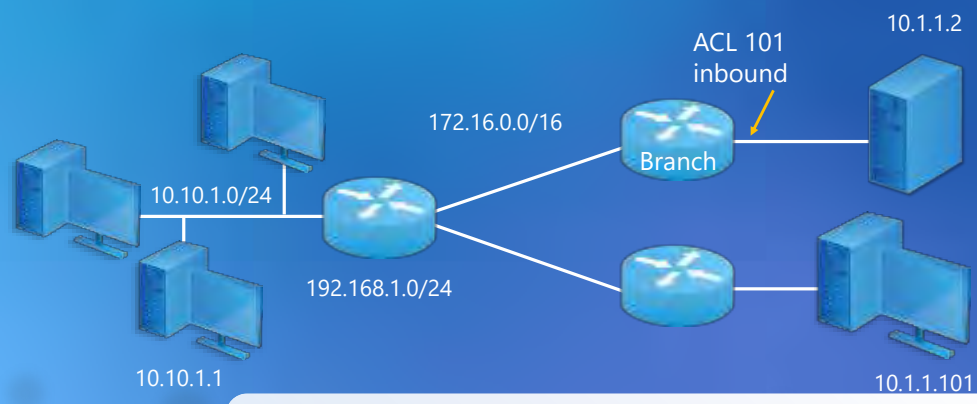



```
Branch#show access-lists 101
Extended IP access list 101
    10 permit tcp 10.10.1.0 0.0.0.255 eq www host 10.1.1.2
    30 deny ip any any
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ACL Troubleshooting 3

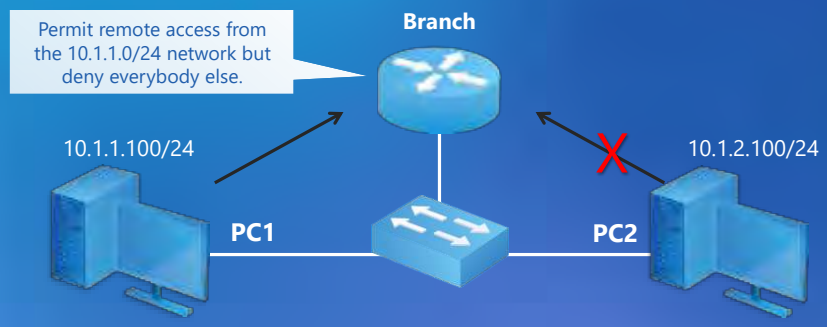
Host 10.10.1.1 has no http connectivity to 10.1.1.2.




```
Branch#show access-lists 101
Extended IP access list 101
    10 permit tcp host 10.1.1.2 10.10.1.0 0.0.0.255 eq www
    30 deny ip any any
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Using ACLs on VTY Lines



Use an ACL to permit Telnet access from 10.1.1.0 /24, but deny everybody else:

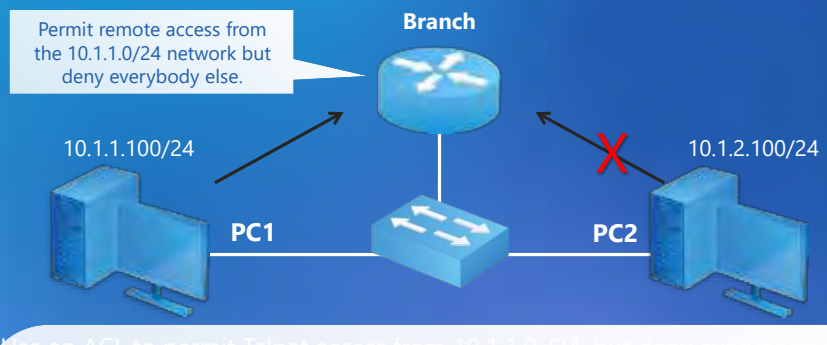
```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#access-list 1 deny any log
```

Apply the ACL on vty lines: with these commands.

```
Router(config)#line vty 0 4
Router(config-line)#access-class 1 in
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Using ACLs on VTY Lines



Use an ACL to permit Telnet access from 10.1.1.0 /24, but deny everybody else.

```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#access-list 1 deny any log
```

Apply the ACL on vty lines: with these commands.

```
Router(config)#line vty 0 4
Router(config-line)#access-class 1 in
```

```
PC2#telnet 172.16.34.4
Trying 172.16.34.4 ...
% Connection refused by remote host
```

```
Branch#
*Jan 16 06:08:23.029: %SEC-6-IPACCESSLOGNP: list 1 denied 0 10.1.2.100 ->
0.0.0.0, 1 packet
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACLs

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based Access Control List

Turn on and off an ACL entry based on time

By default an ACL entry is always “on” when the ACL has been applied.

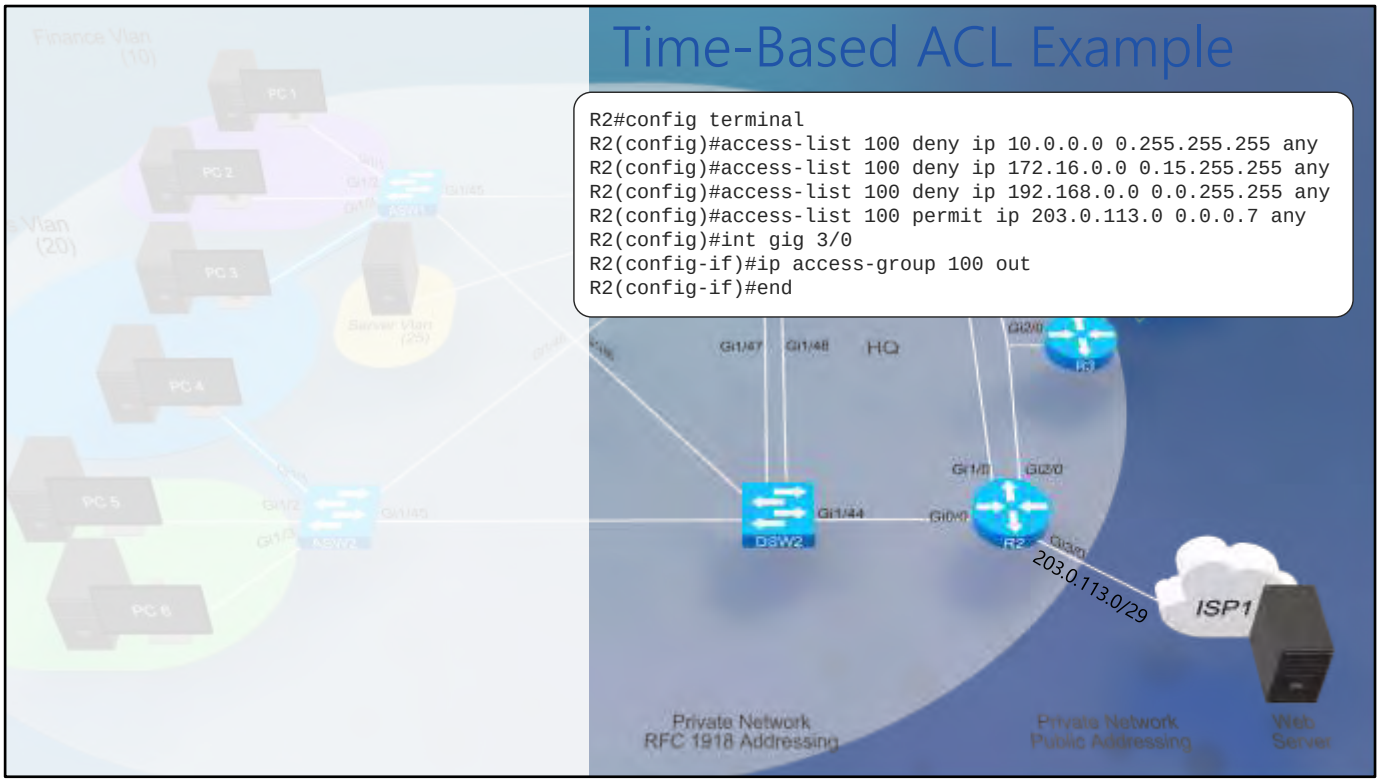
Time-Based ACLS control when the ACL entry is “on” and “off” for an ACL that has been applied.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACL Example

```
R2#config terminal
R2(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R2(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R2(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R2(config)#access-list 100 permit ip 203.0.113.0 0.0.0.7 any
R2(config)#int gig 3/0
R2(config-if)#ip access-group 100 out
R2(config-if)#end
```

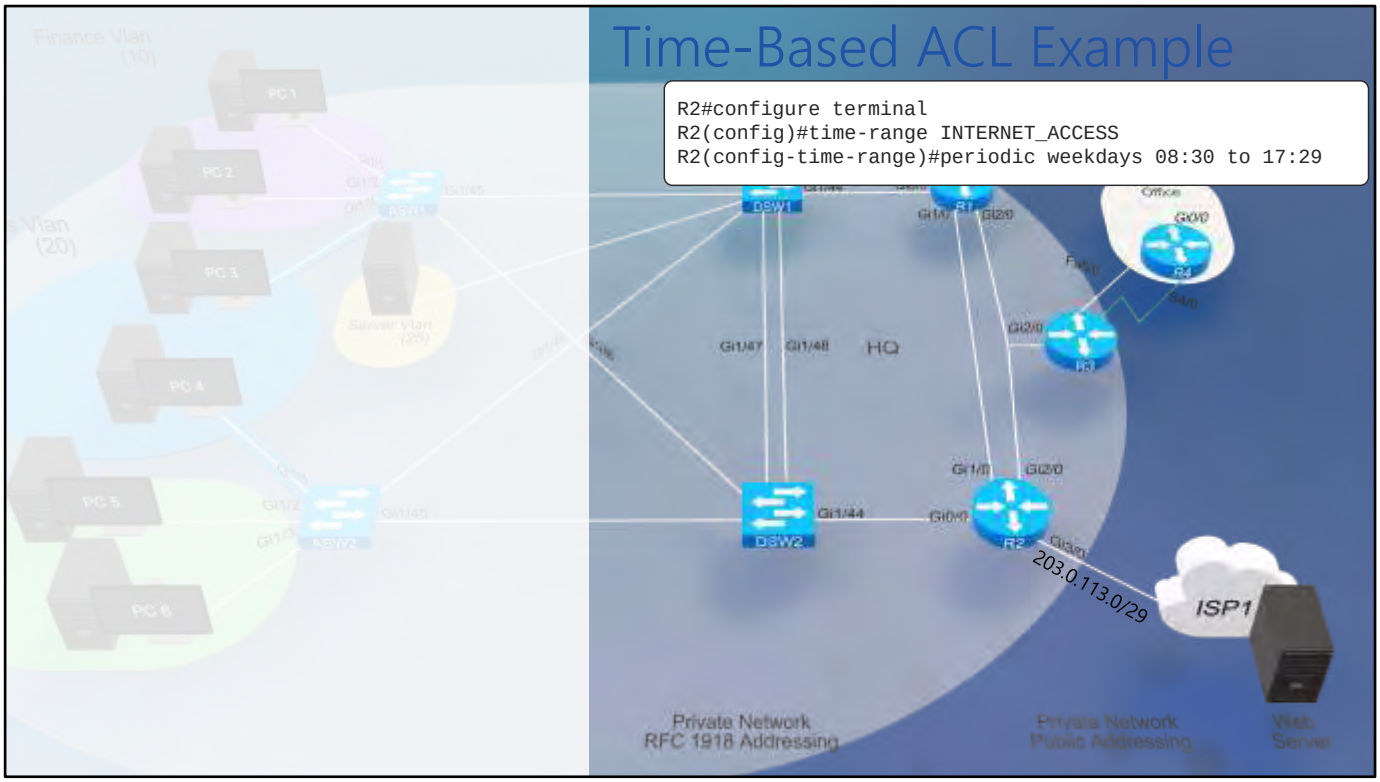


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACL Example

```
R2#configure terminal
R2(config)#time-range INTERNET_ACCESS
R2(config-time-range)#periodic weekdays 08:30 to 17:29
```

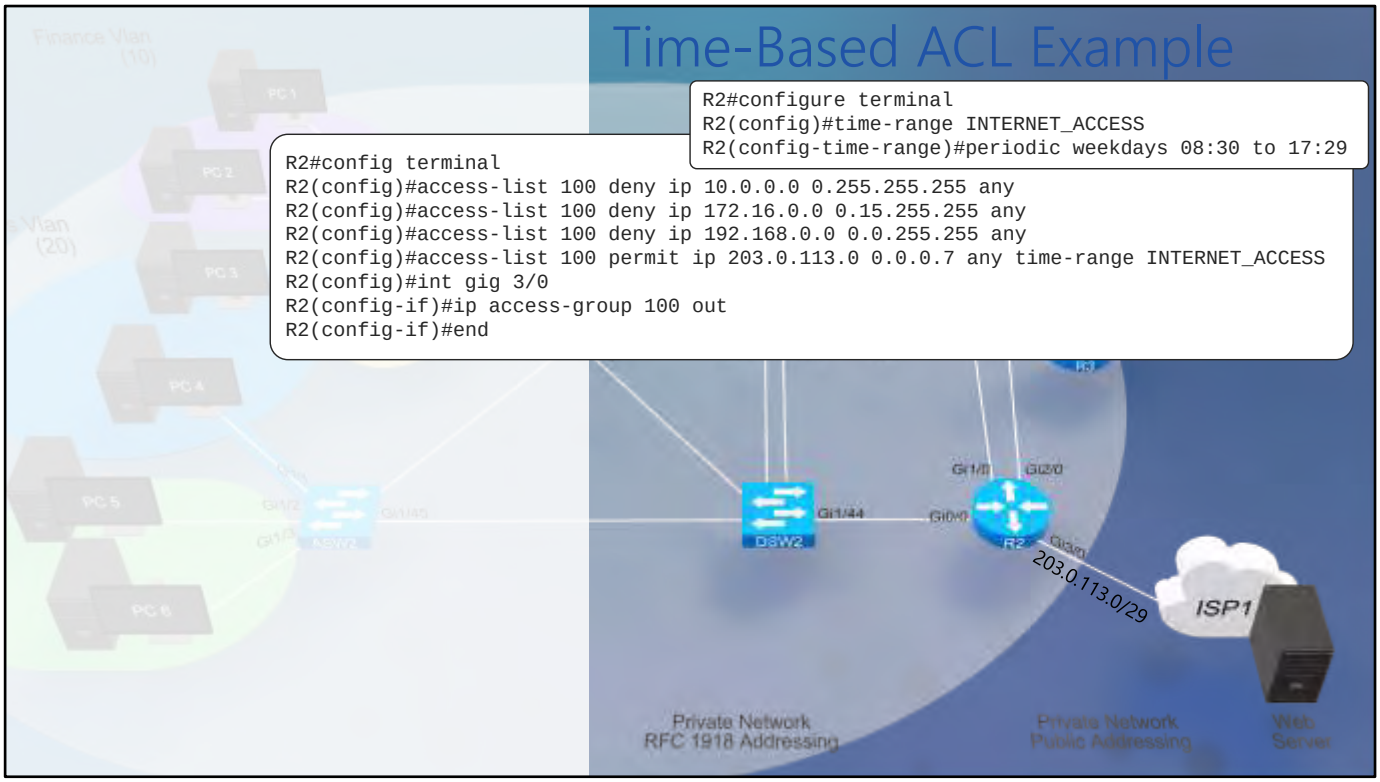


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACL Example

```
R2#configure terminal
R2(config)#time-range INTERNET_ACCESS
R2(config-time-range)#periodic weekdays 08:30 to 17:29
```

```
R2#config terminal
R2(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R2(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R2(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R2(config)#access-list 100 permit ip 203.0.113.0 0.0.0.7 any time-range INTERNET_ACCESS
R2(config)#int gig 3/0
R2(config-if)#ip access-group 100 out
R2(config-if)#end
```



©2023 by StormWind LLC. All rights reserved.

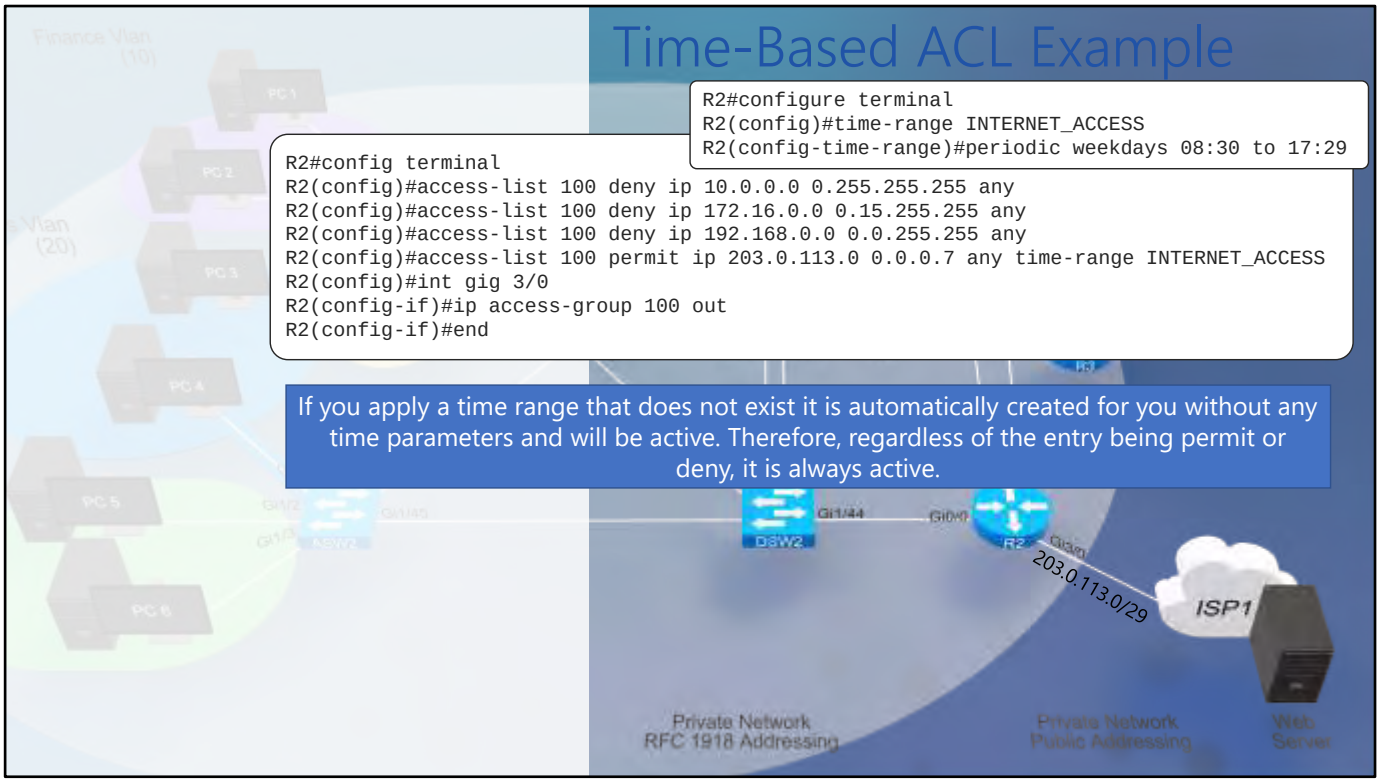
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACL Example

```
R2#configure terminal
R2(config)#time-range INTERNET_ACCESS
R2(config-time-range)#periodic weekdays 08:30 to 17:29
```

```
R2#config terminal
R2(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R2(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R2(config)#access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R2(config)#access-list 100 permit ip 203.0.113.0 0.0.0.7 any time-range INTERNET_ACCESS
R2(config)#int gig 3/0
R2(config-if)#ip access-group 100 out
R2(config-if)#end
```

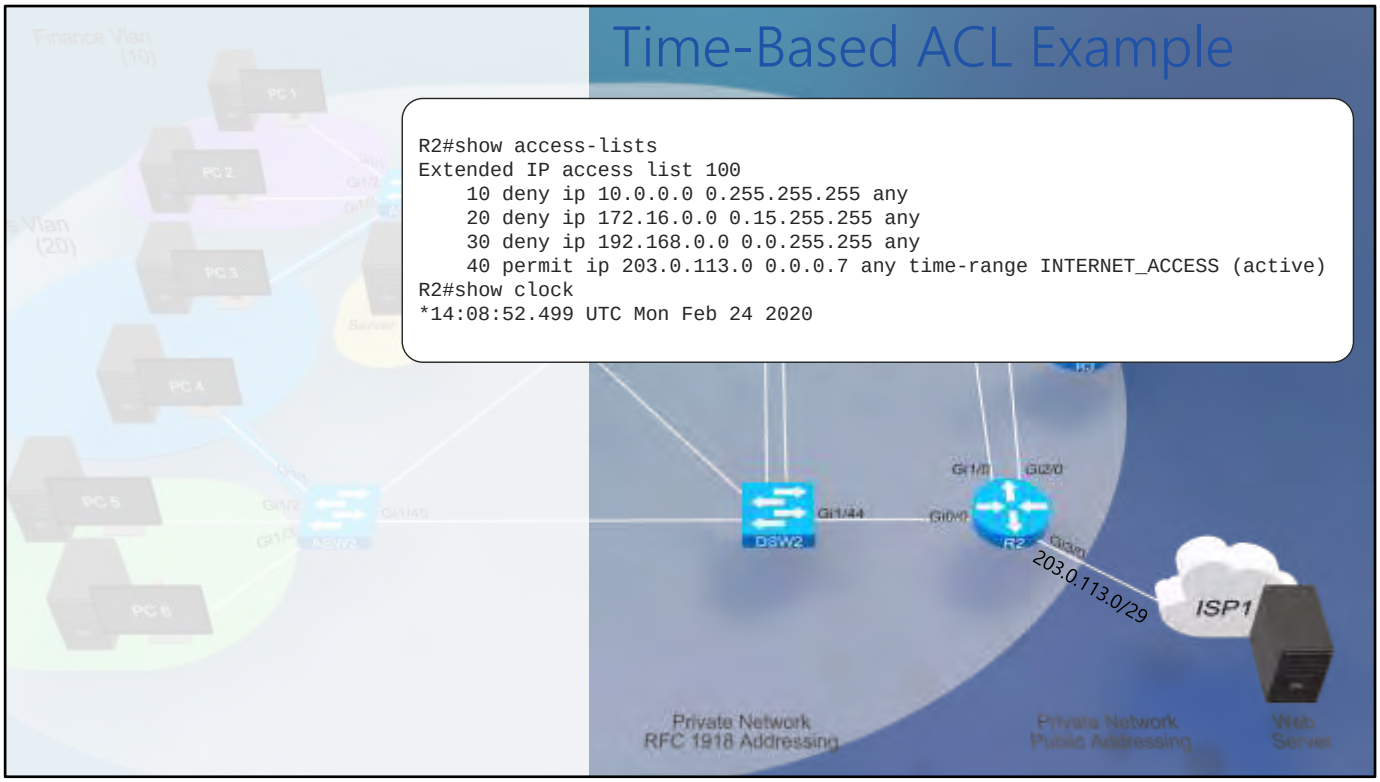
If you apply a time range that does not exist it is automatically created for you without any time parameters and will be active. Therefore, regardless of the entry being permit or deny, it is always active.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACL Example

```
R2#show access-lists
Extended IP access list 100
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 permit ip 203.0.113.0 0.0.0.7 any time-range INTERNET_ACCESS (active)
R2#show clock
*14:08:52.499 UTC Mon Feb 24 2020
```

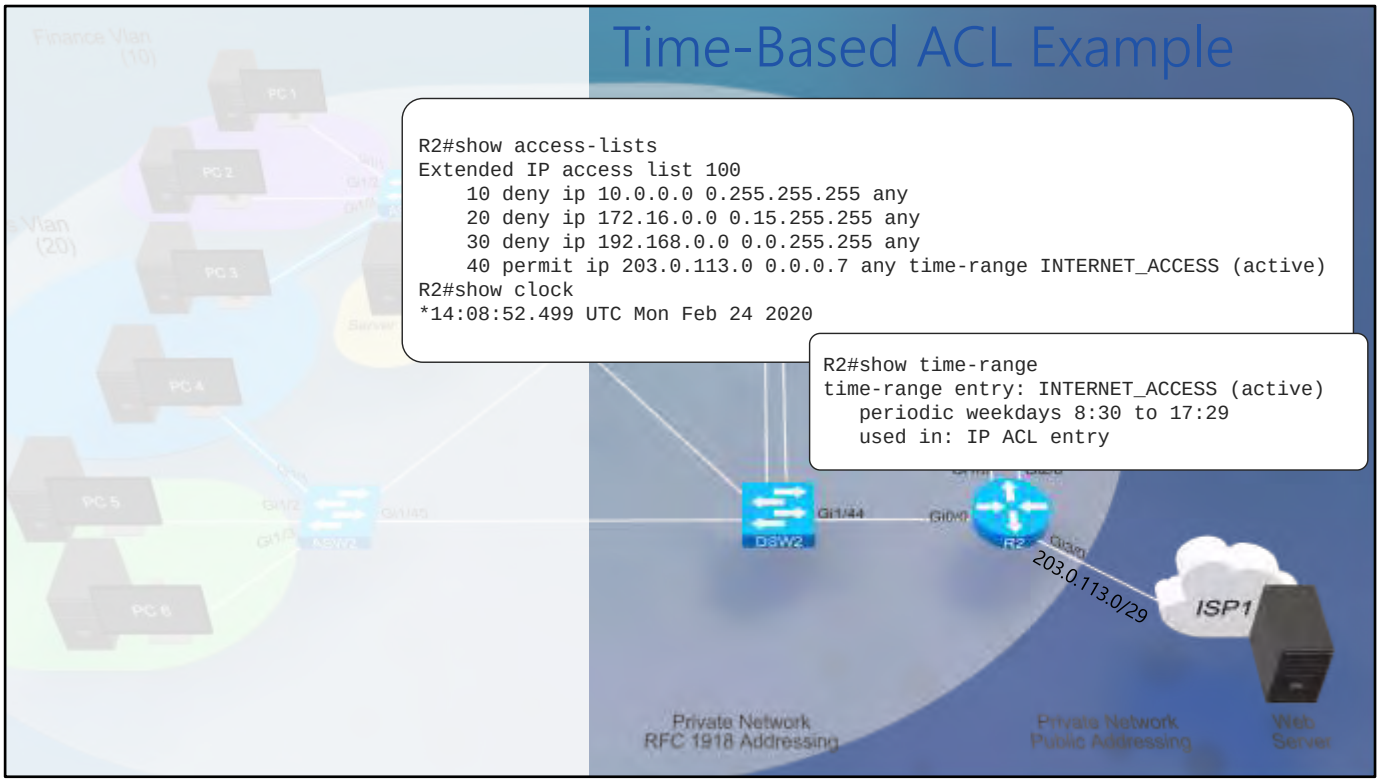


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACL Example

```
R2#show access-lists
Extended IP access list 100
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 permit ip 203.0.113.0 0.0.0.7 any time-range INTERNET_ACCESS (active)
R2#show clock
*14:08:52.499 UTC Mon Feb 24 2020
```

```
R2#show time-range
time-range entry: INTERNET_ACCESS (active)
   periodic weekdays 8:30 to 17:29
   used in: IP ACL entry
```

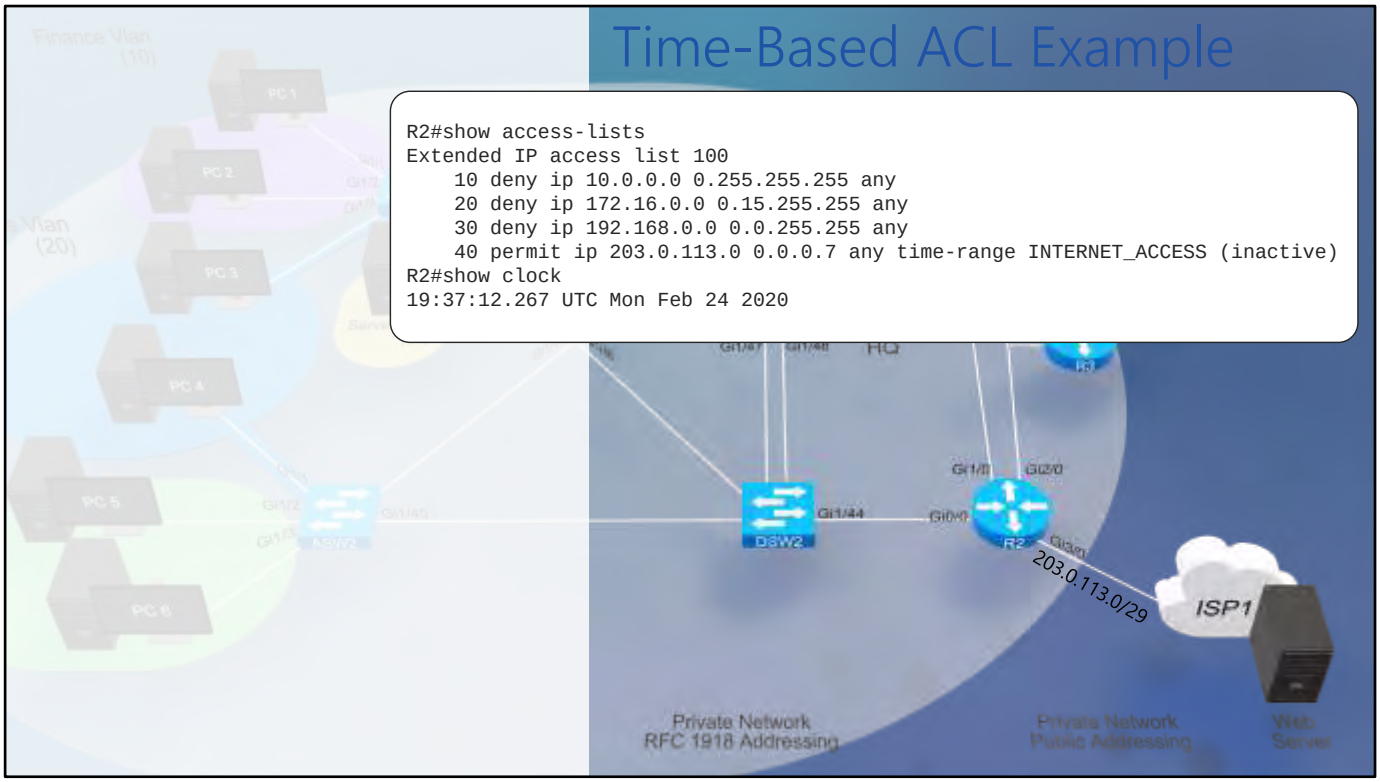


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACL Example

```
R2#show access-lists
Extended IP access list 100
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 permit ip 203.0.113.0 0.0.0.7 any time-range INTERNET_ACCESS (inactive)
R2#show clock
19:37:12.267 UTC Mon Feb 24 2020
```

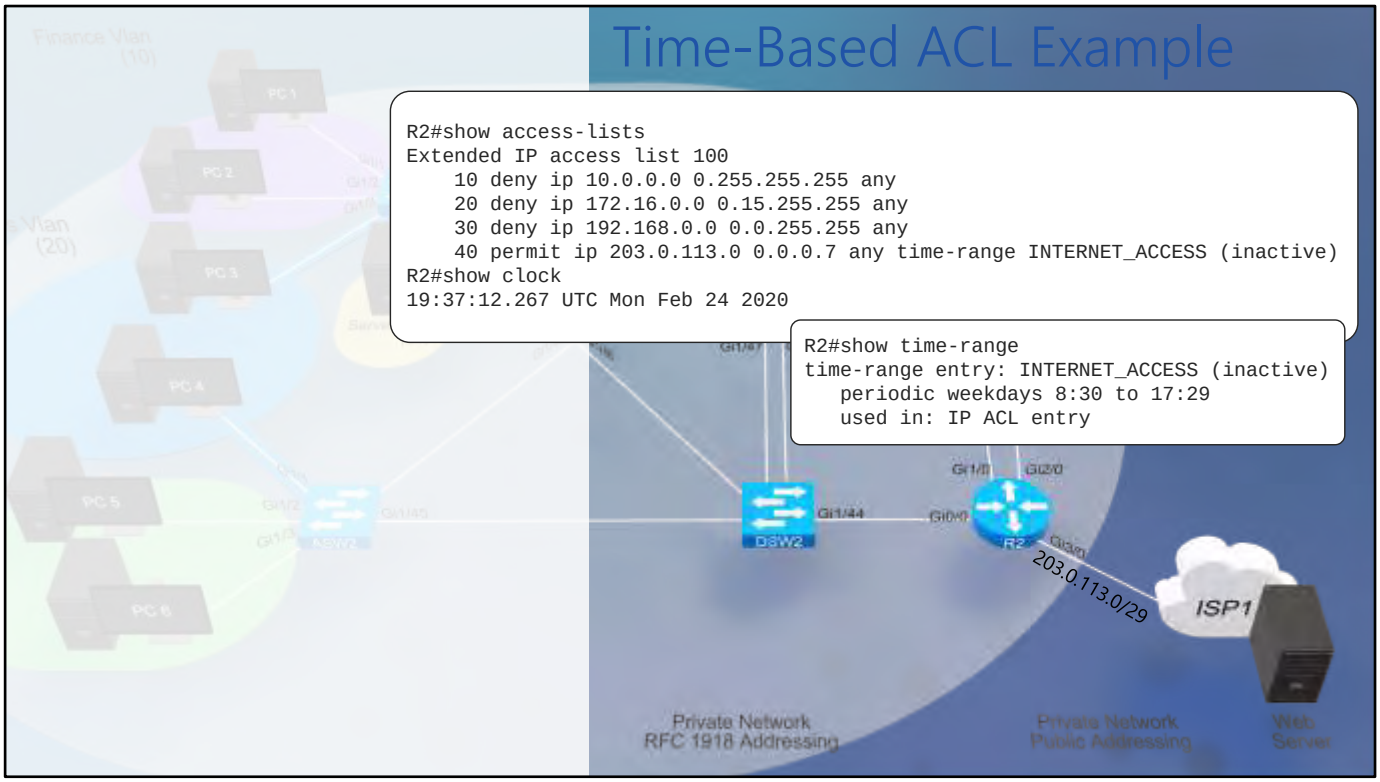


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Time-Based ACL Example

```
R2#show access-lists
Extended IP access list 100
    10 deny ip 10.0.0.0 0.255.255.255 any
    20 deny ip 172.16.0.0 0.15.255.255 any
    30 deny ip 192.168.0.0 0.0.255.255 any
    40 permit ip 203.0.113.0 0.0.0.7 any time-range INTERNET_ACCESS (inactive)
R2#show clock
19:37:12.267 UTC Mon Feb 24 2020
```

```
R2#show time-range
time-range entry: INTERNET_ACCESS (inactive)
   periodic weekdays 8:30 to 17:29
   used in: IP ACL entry
```

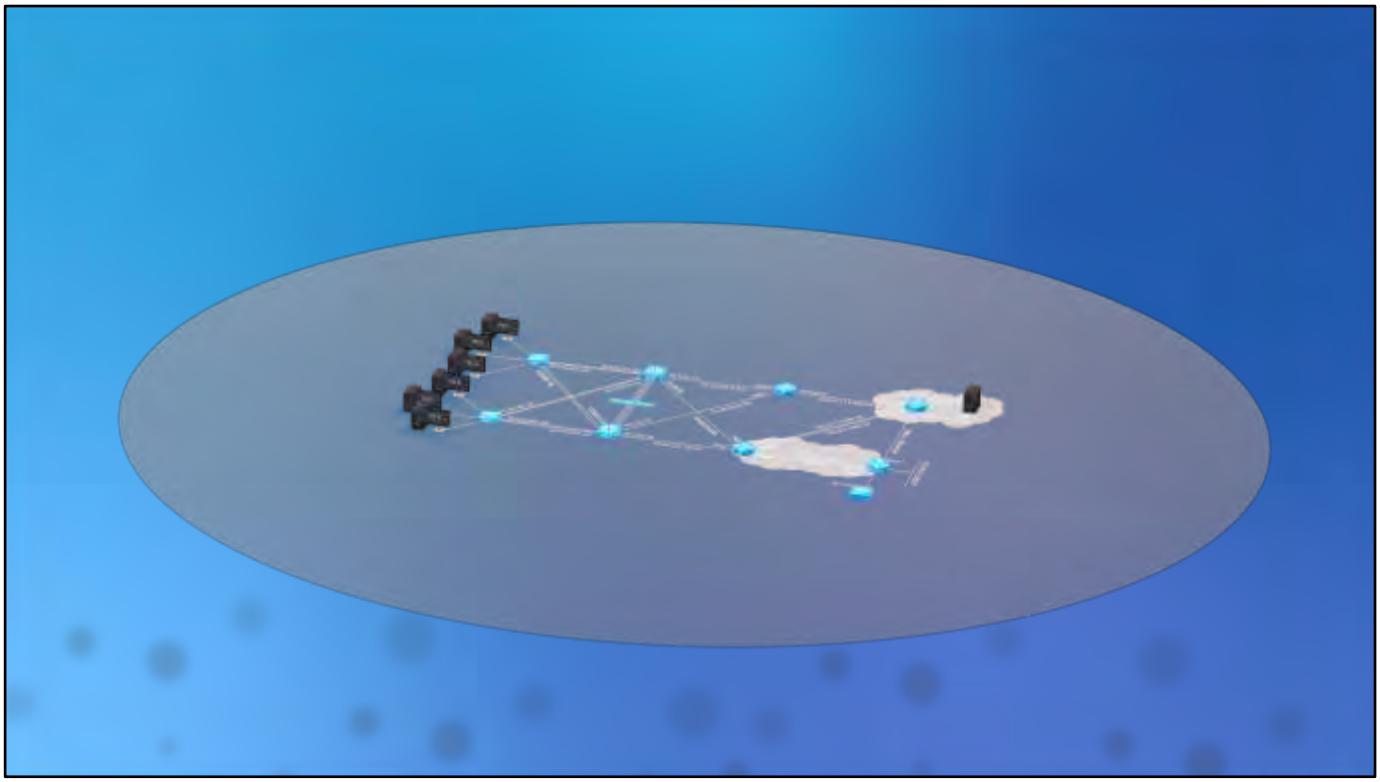


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

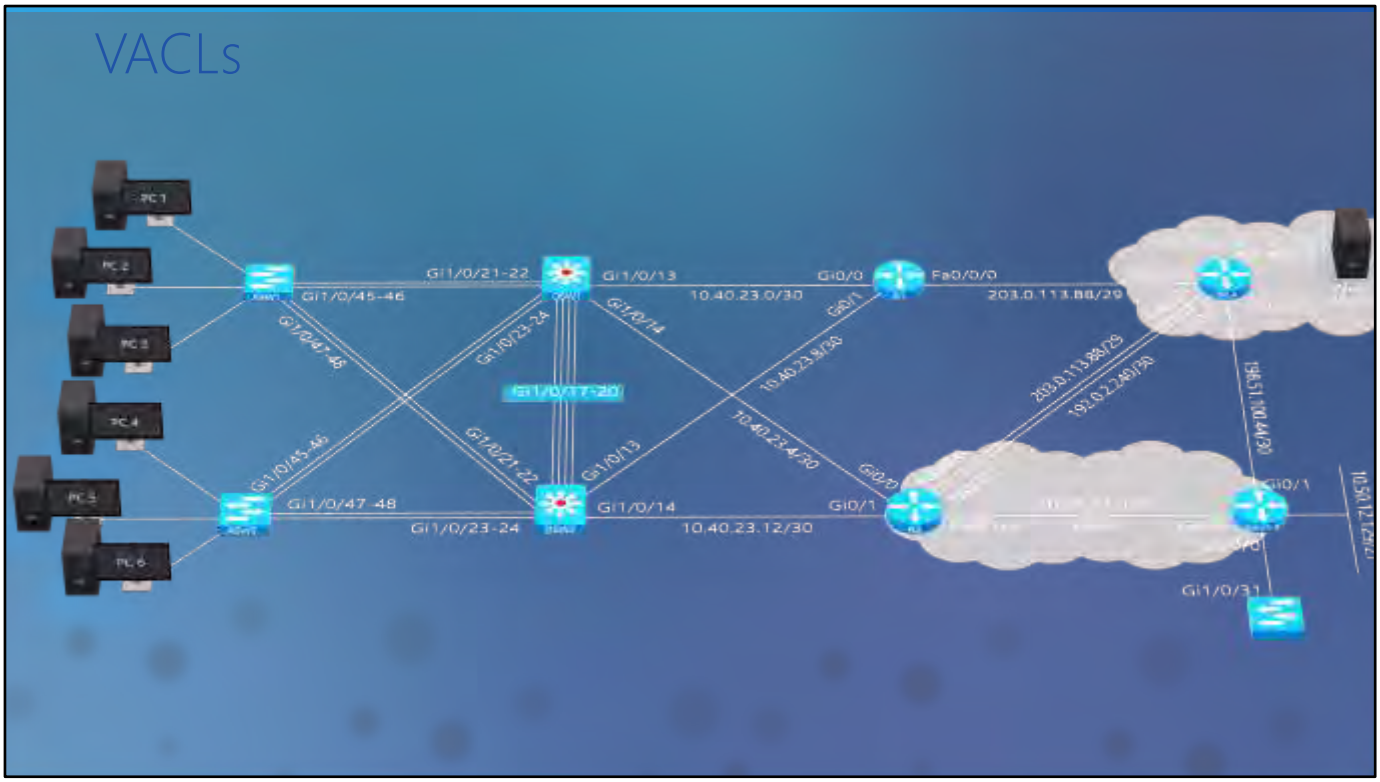
VLAN Access-Control Lists (VACLs)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



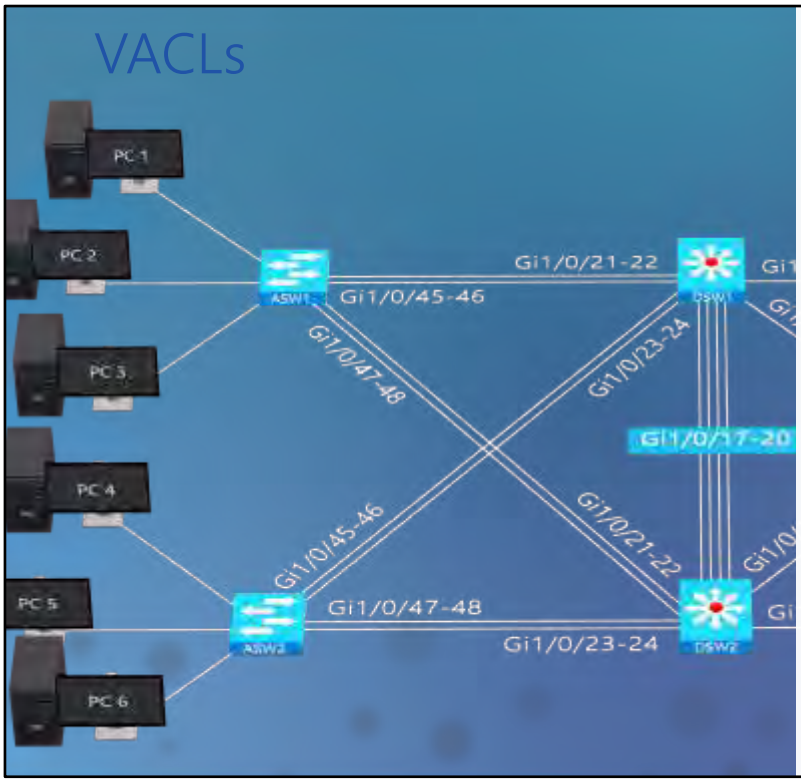
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VACLs



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VACLs



Used to control traffic:

Flowing within a subnet/vlan/broadcast domain

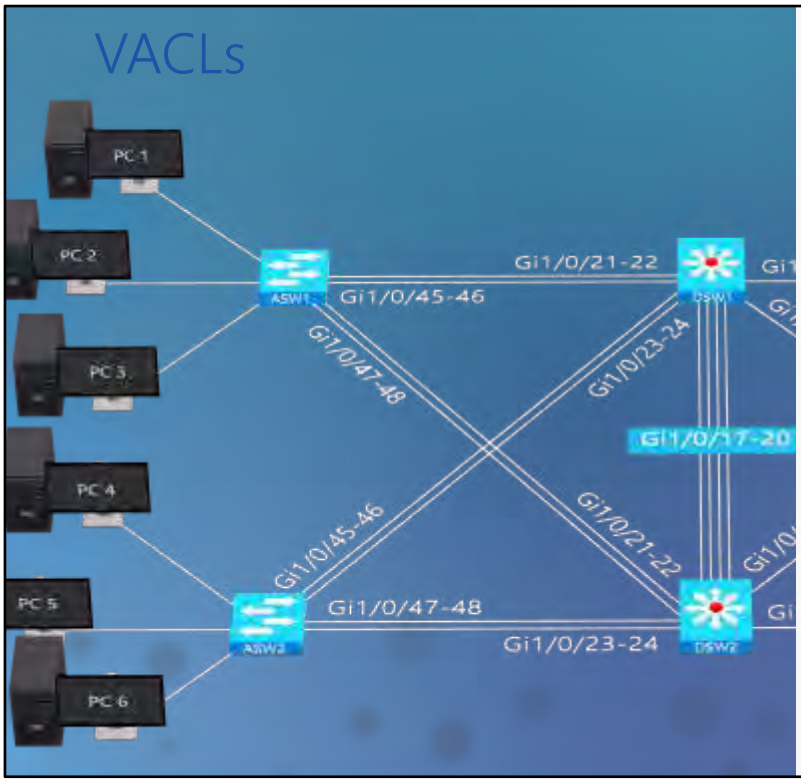
Or

Entering or leaving a subnet/vlan/broadcast domain.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VACLs



Guidelines:

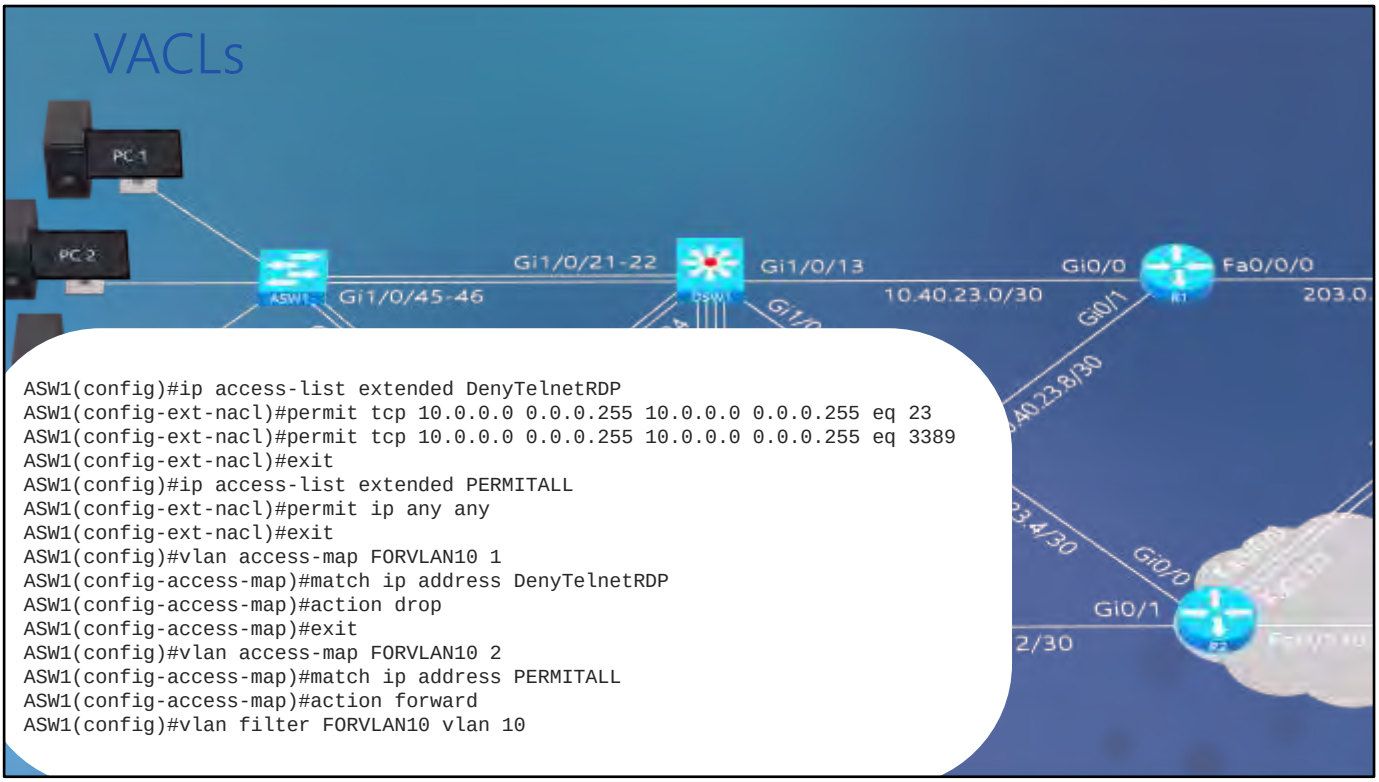
Create permit ACLs matching traffic

Create a VLAN Access Map and specify the ACLs to match and the action you want to take

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

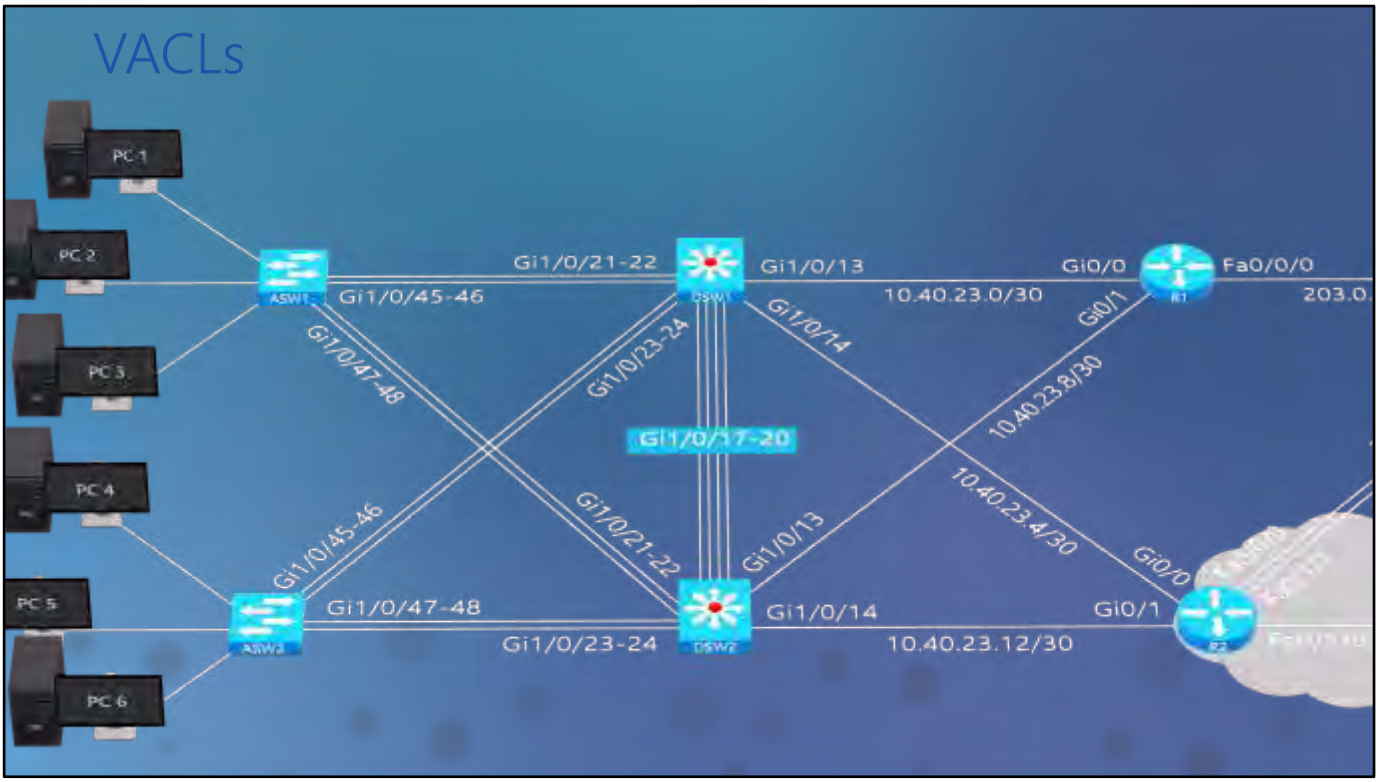
VACLs




```
ASW1(config)#ip access-list extended DenyTelnetRDP
ASW1(config-ext-nacl)#permit tcp 10.0.0.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 23
ASW1(config-ext-nacl)#permit tcp 10.0.0.0 0.0.0.255 10.0.0.0 0.0.0.255 eq 3389
ASW1(config-ext-nacl)#exit
ASW1(config)#ip access-list extended PERMITALL
ASW1(config-ext-nacl)#permit ip any any
ASW1(config-ext-nacl)#exit
ASW1(config)#vlan access-map FORVLAN10 1
ASW1(config-access-map)#match ip address DenyTelnetRDP
ASW1(config-access-map)#action drop
ASW1(config-access-map)#exit
ASW1(config)#vlan access-map FORVLAN10 2
ASW1(config-access-map)#match ip address PERMITALL
ASW1(config-access-map)#action forward
ASW1(config)#vlan filter FORVLAN10 vlan 10
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VACLs



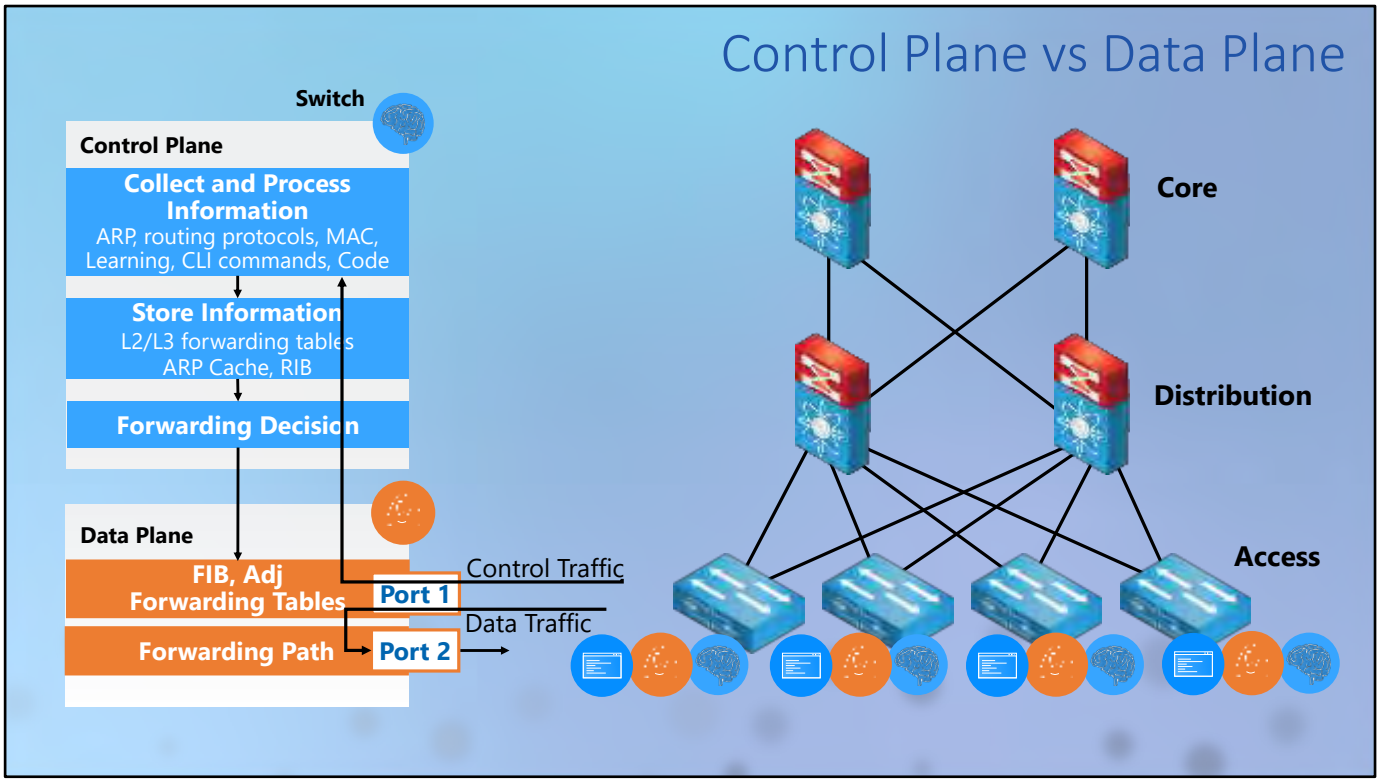
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VLANs

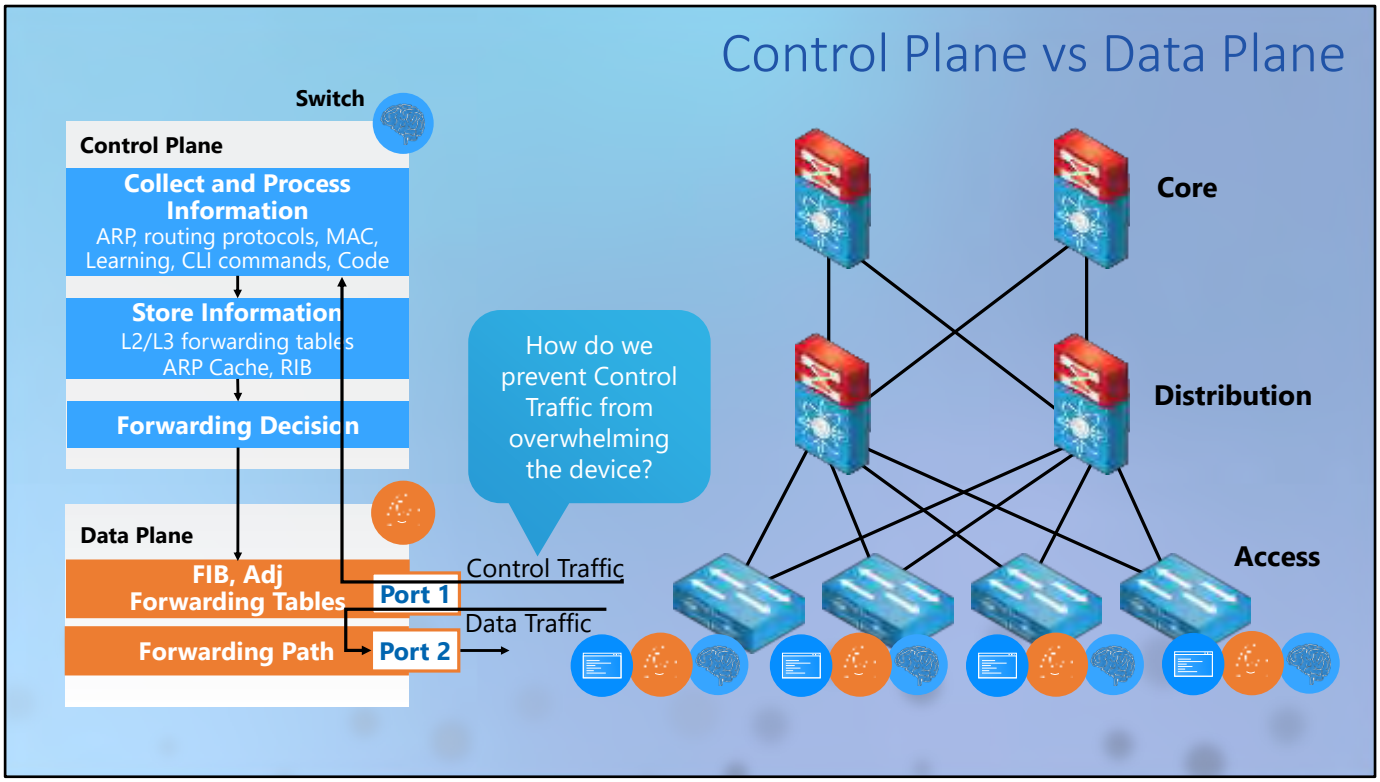
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Control Plane Policing (CoPP)

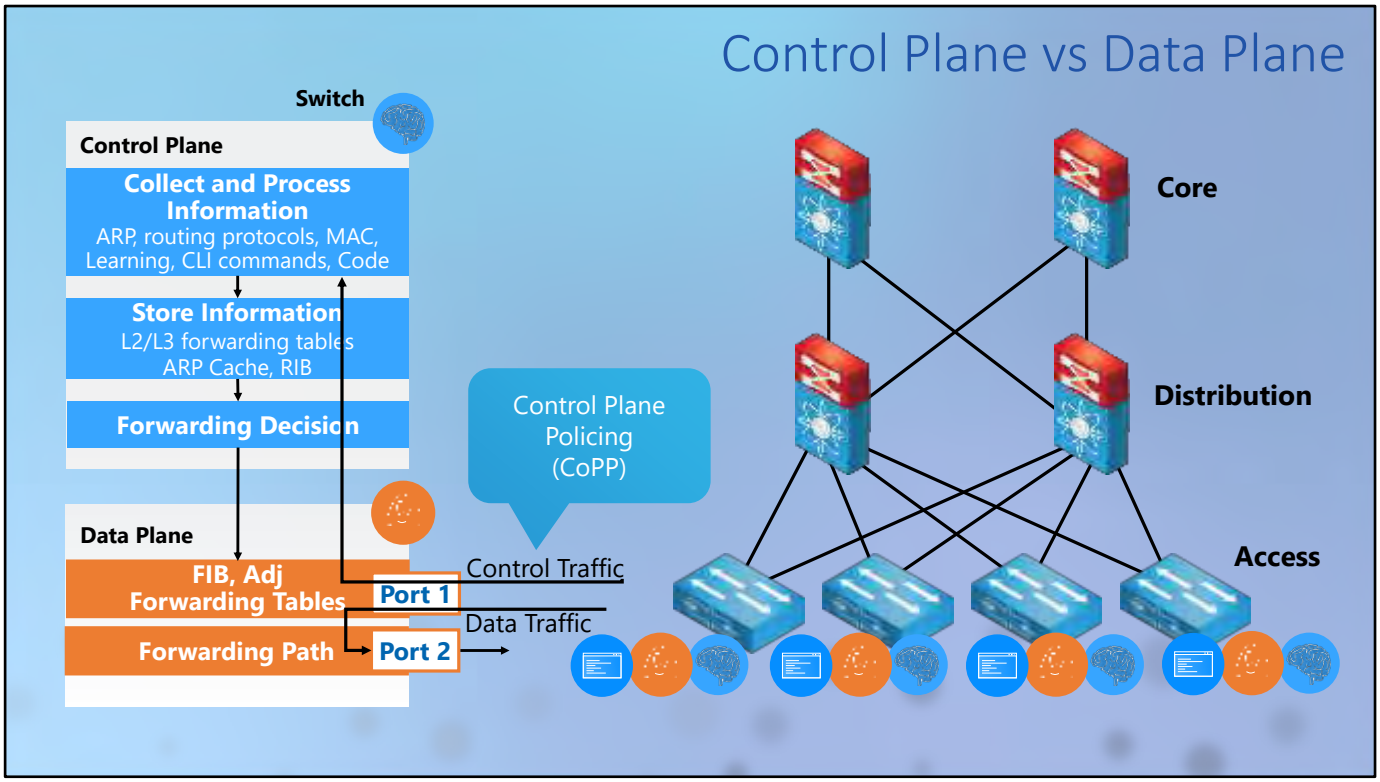
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



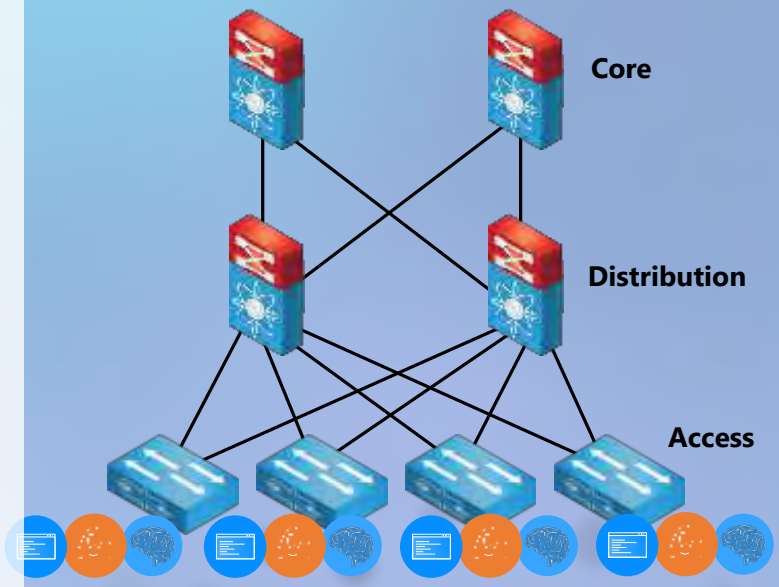
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

CoPP

- Prohibit the control plane and thus the CPU from becoming overwhelmed
  - through rate limiting
    - Either transmit to CPU or drop traffic
- Focus is on traffic TO the device
  - Not through the device



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

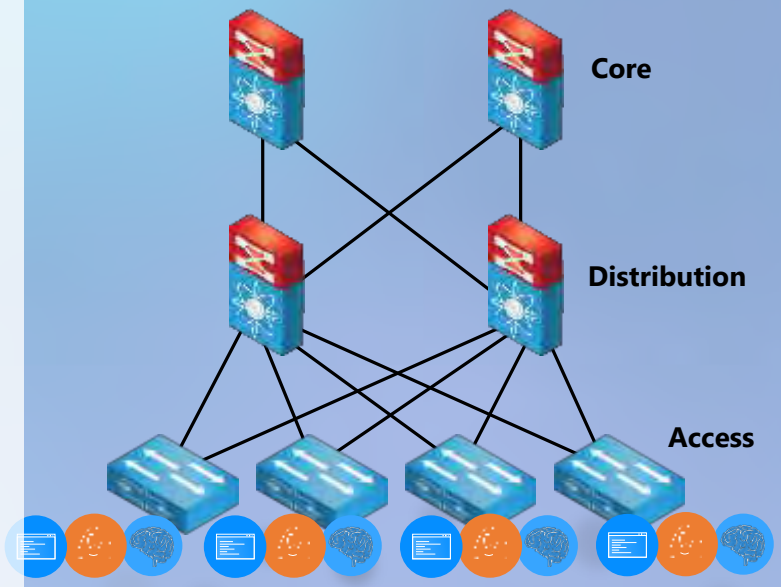
CoPP

MQC uses three main configuration elements:

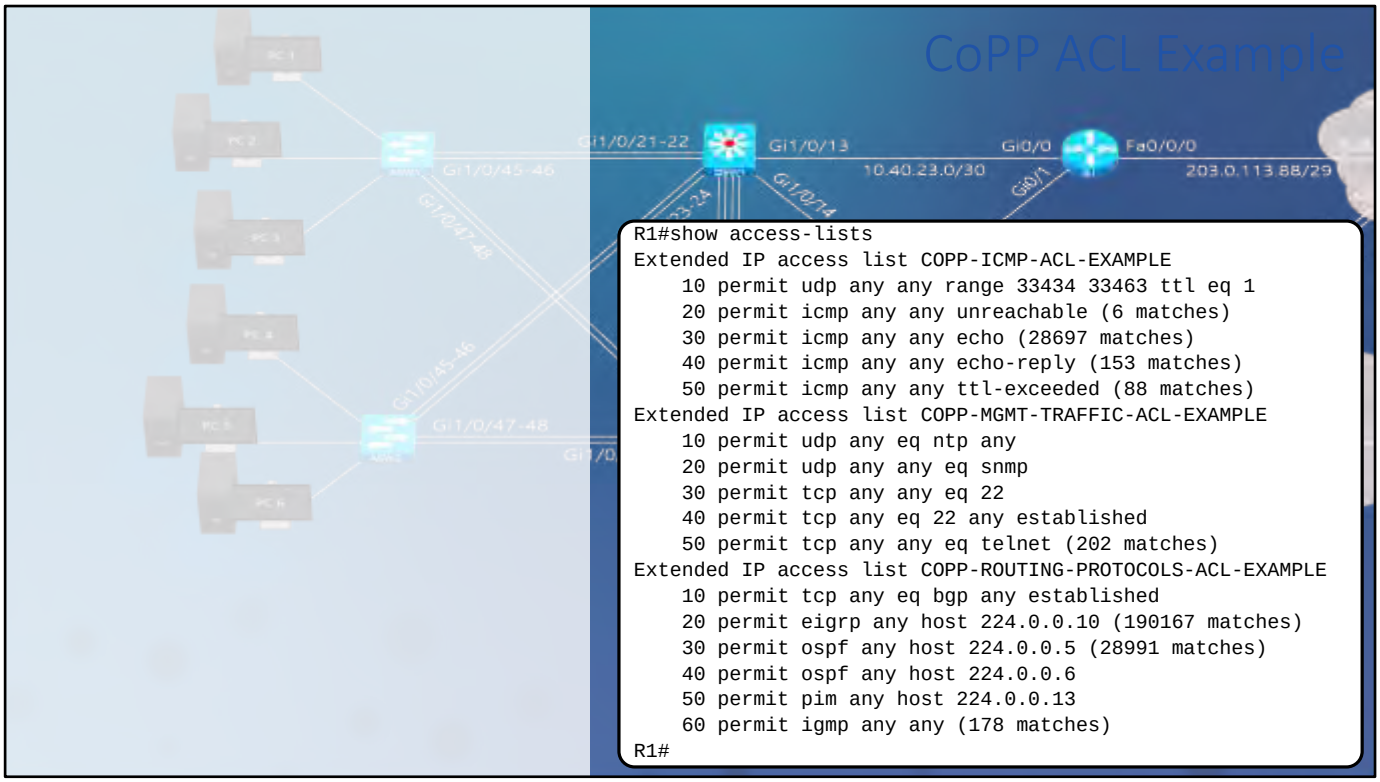
class-map = Identify traffic to match

policy-map = Define what happens to the traffic that matches

service-policy = Applies policy to interface

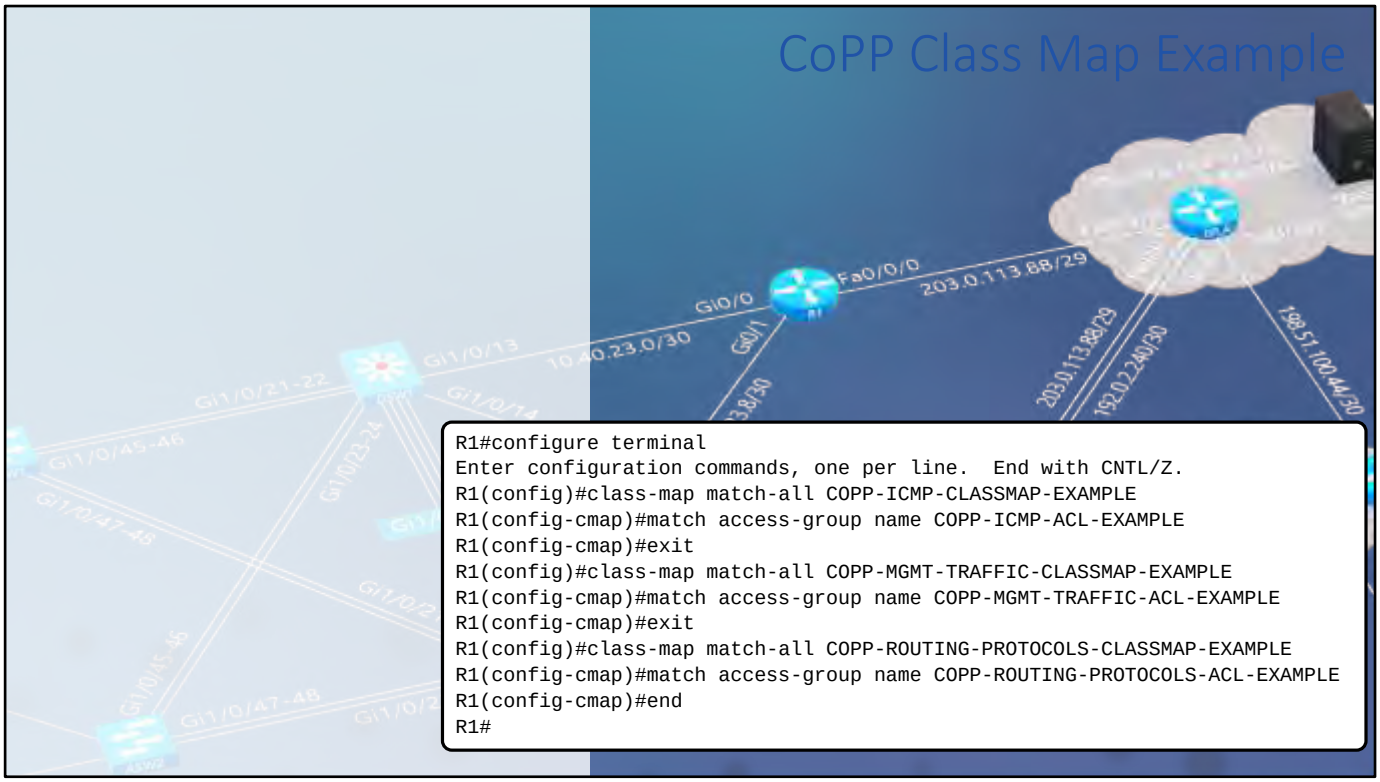


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

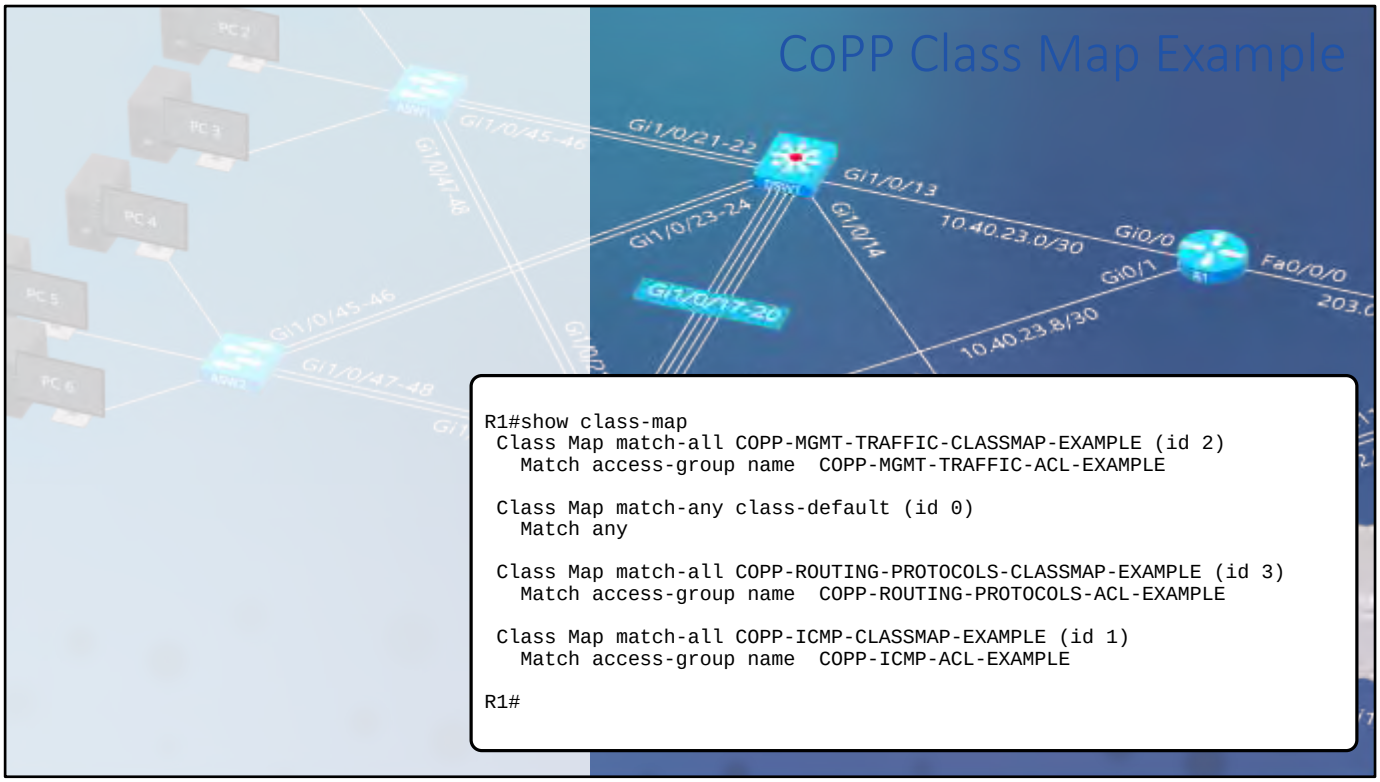
CoPP Class Map Example




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#class-map match-all COPP-ICMP-CLASSMAP-EXAMPLE
R1(config-cmap)#match access-group name COPP-ICMP-ACL-EXAMPLE
R1(config-cmap)#exit
R1(config)#class-map match-all COPP-MGMT-TRAFFIC-CLASSMAP-EXAMPLE
R1(config-cmap)#match access-group name COPP-MGMT-TRAFFIC-ACL-EXAMPLE
R1(config-cmap)#exit
R1(config)#class-map match-all COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE
R1(config-cmap)#match access-group name COPP-ROUTING-PROTOCOLS-ACL-EXAMPLE
R1(config-cmap)#end
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

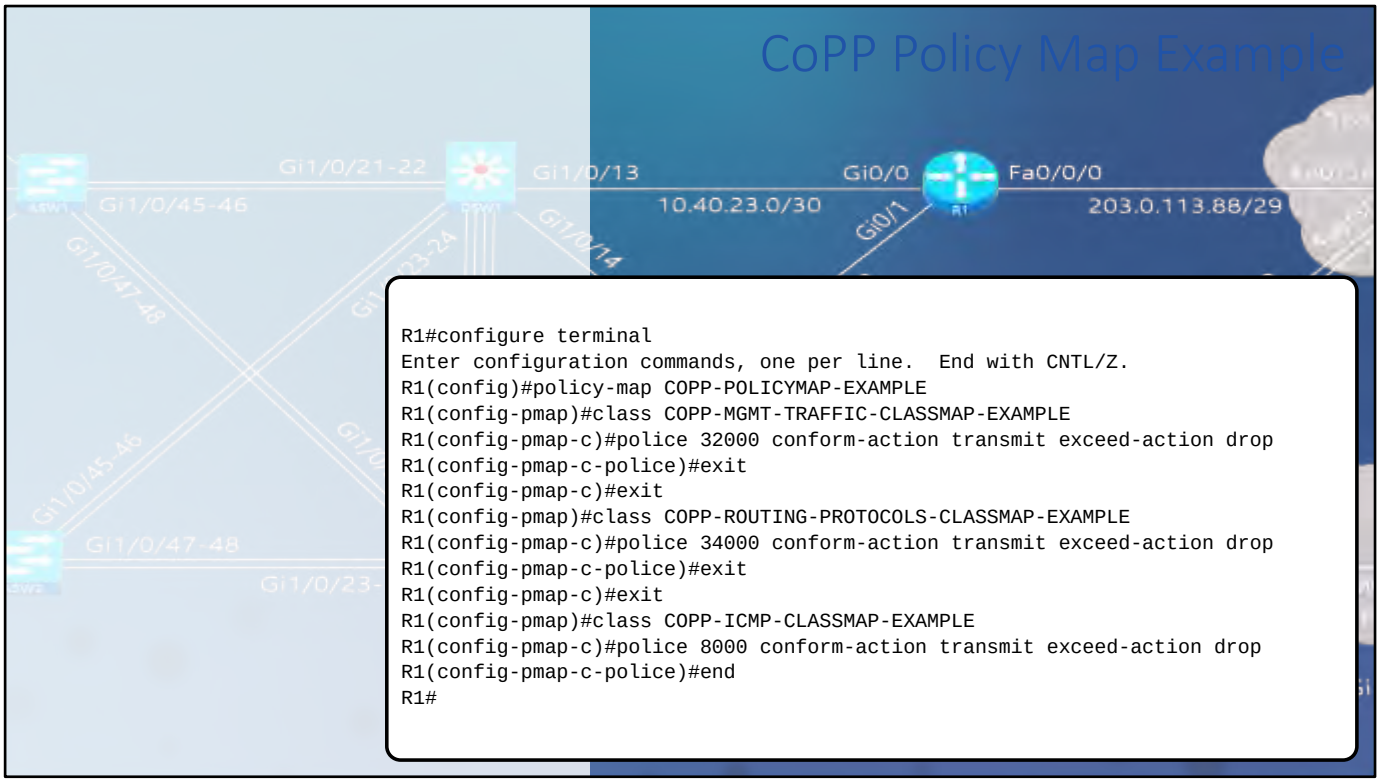
CoPP Class Map Example




```
R1#show class-map
 Class Map match-all COPP-MGMT-TRAFFIC-CLASSMAP-EXAMPLE (id 2)
   Match access-group name  COPP-MGMT-TRAFFIC-ACL-EXAMPLE

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-all COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE (id 3)
   Match access-group name  COPP-ROUTING-PROTOCOLS-ACL-EXAMPLE

 Class Map match-all COPP-ICMP-CLASSMAP-EXAMPLE (id 1)
   Match access-group name  COPP-ICMP-ACL-EXAMPLE

R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

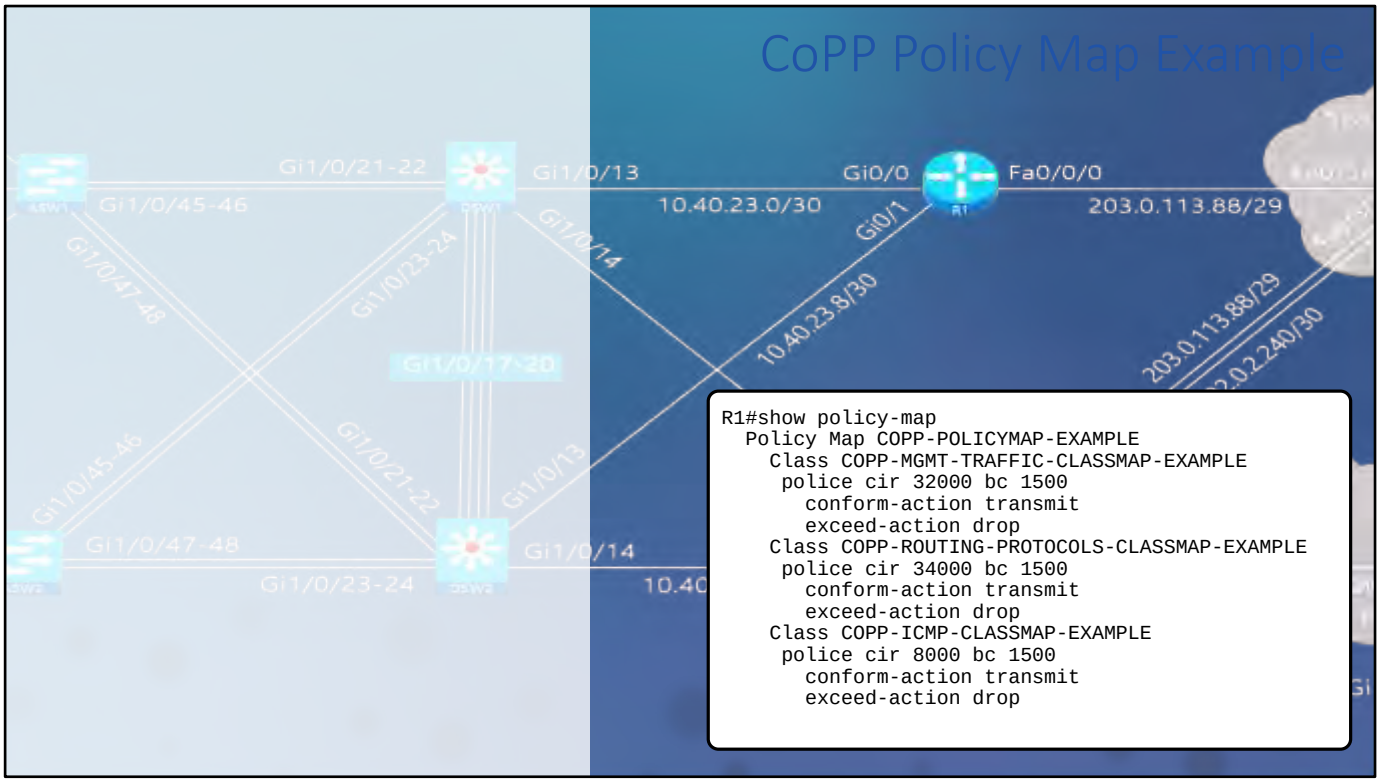
CoPP Policy Map Example




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#policy-map COPP-POLICYMAP-EXAMPLE
R1(config-pmap)#class COPP-MGMT-TRAFFIC-CLASSMAP-EXAMPLE
R1(config-pmap-c)#police 32000 conform-action transmit exceed-action drop
R1(config-pmap-c-police)#exit
R1(config-pmap-c)#exit
R1(config-pmap)#class COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE
R1(config-pmap-c)#police 34000 conform-action transmit exceed-action drop
R1(config-pmap-c-police)#exit
R1(config-pmap-c)#exit
R1(config-pmap)#class COPP-ICMP-CLASSMAP-EXAMPLE
R1(config-pmap-c)#police 8000 conform-action transmit exceed-action drop
R1(config-pmap-c-police)#end
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

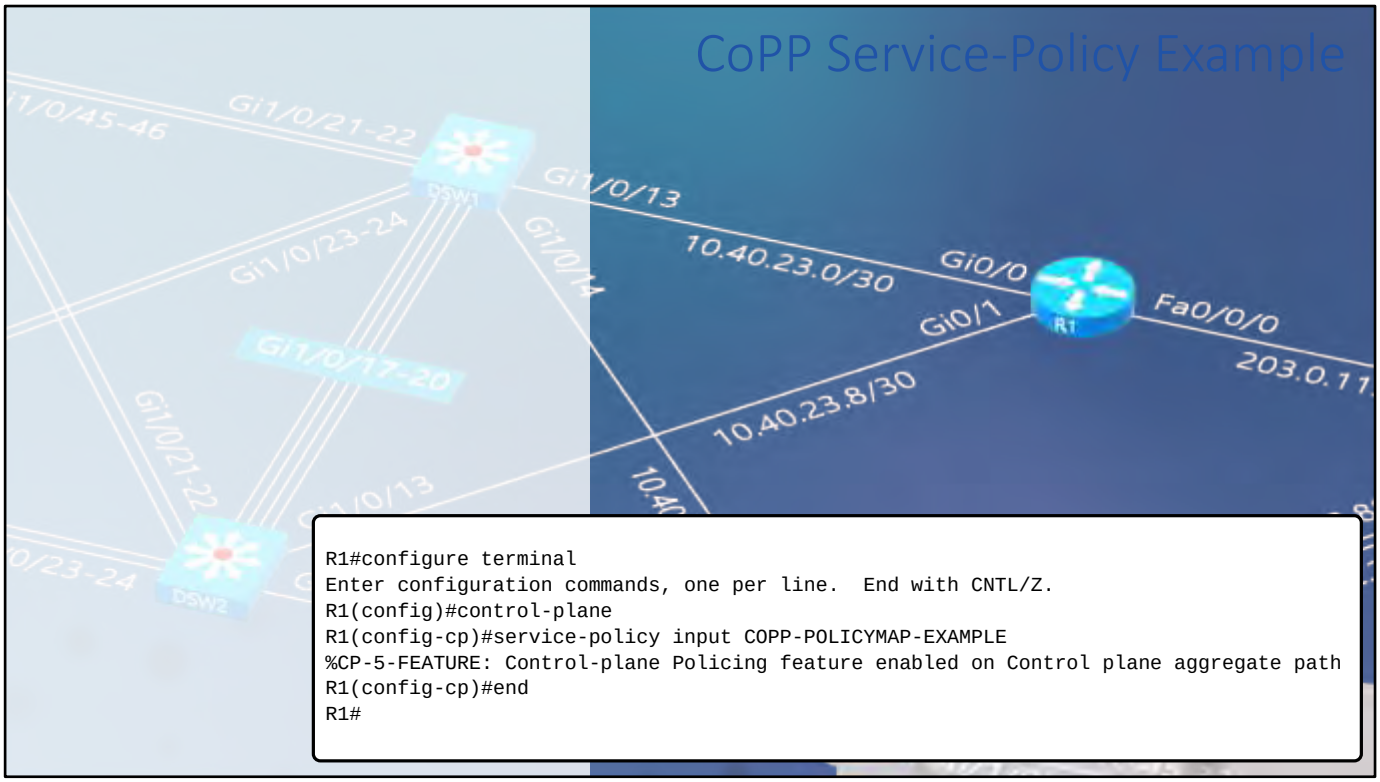
CoPP Policy Map Example




```
R1#show policy-map
  Policy Map COPP-POLICYMAP-EXAMPLE
    Class COPP-MGMT-TRAFFIC-CLASSMAP-EXAMPLE
     police cir 32000 bc 1500
       conform-action transmit
       exceed-action drop
    Class COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE
     police cir 34000 bc 1500
       conform-action transmit
       exceed-action drop
    Class COPP-ICMP-CLASSMAP-EXAMPLE
     police cir 8000 bc 1500
       conform-action transmit
       exceed-action drop
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

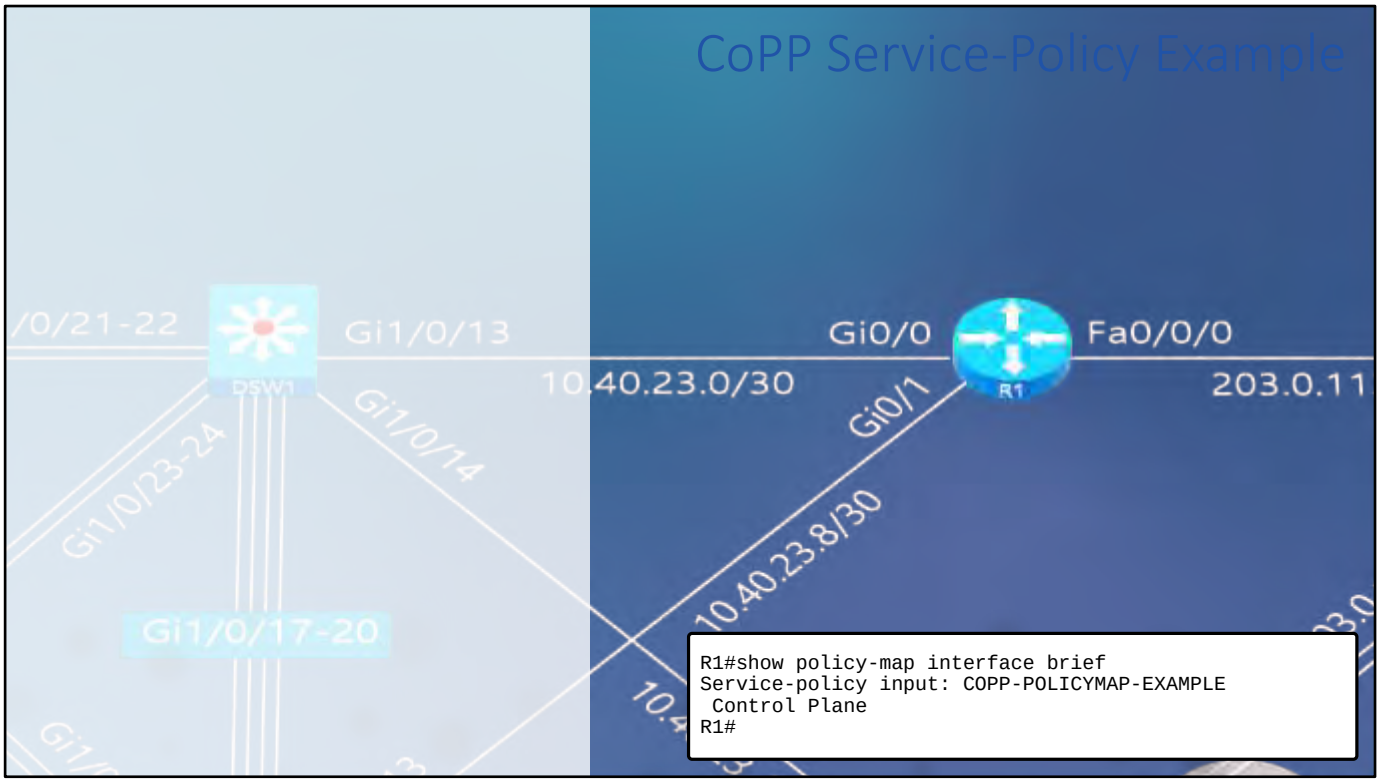
CoPP Service-Policy Example




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#control-plane
R1(config-cp)#service-policy input COPP-POLICYMAP-EXAMPLE
%CP-5-FEATURE: Control-plane Policing feature enabled on Control plane aggregate path
R1(config-cp)#end
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

CoPP Service-Policy Example




```
R1#show policy-map interface brief
Service-policy input: COPP-POLICYMAP-EXAMPLE
 Control Plane
R1#
```

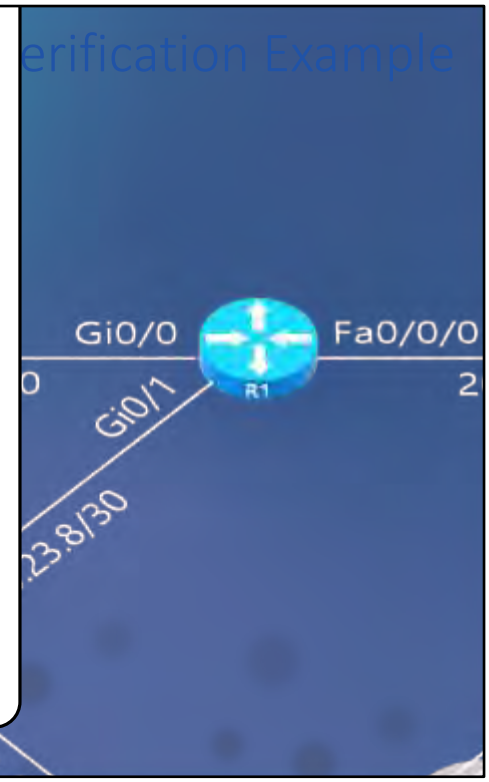
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

CoPP Verification Example

```
R1#show policy-map control-plane
 Control Plane

  Service-policy input: COPP-POLICYMAP-EXAMPLE

    Class-map: COPP-MGMT-TRAFFIC-CLASSMAP-EXAMPLE (match-all)
      120 packets, 6662 bytes
      5 minute offered rate 1000 bps, drop rate 0000 bps
      Match: access-group name COPP-MGMT-TRAFFIC-ACL-EXAMPLE
      police:
          cir 32000 bps, bc 1500 bytes
        conformed 120 packets, 6662 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 1000 bps, exceeded 0000 bps

    Class-map: COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE (match-all)
      94 packets, 9104 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name COPP-ROUTING-PROTOCOLS-ACL-EXAMPLE
      police:
          cir 34000 bps, bc 1500 bytes
        conformed 94 packets, 9104 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceeded 0000 bps

    Class-map: COPP-ICMP-CLASSMAP-EXAMPLE (match-all)
      200 packets, 196412 bytes
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

```
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 1000 bps, exceeded 0000 bps

  Class-map: COPP-ROUTING-PROTOCOLS-CLASSMAP-EXAMPLE (match-all)
    94 packets, 9104 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: access-group name COPP-ROUTING-PROTOCOLS-ACL-EXAMPLE
    police:
        cir 34000 bps, bc 1500 bytes
      conformed 94 packets, 9104 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 0000 bps, exceeded 0000 bps

  Class-map: COPP-ICMP-CLASSMAP-EXAMPLE (match-all)
    200 packets, 196412 bytes
    5 minute offered rate 7000 bps, drop rate 4000 bps
    Match: access-group name COPP-ICMP-ACL-EXAMPLE
    police:
        cir 8000 bps, bc 1500 bytes
      conformed 103 packets, 98054 bytes; actions:
        transmit
      exceeded 97 packets, 98358 bytes; actions:
        drop
      conformed 4000 bps, exceeded 4000 bps

  Class-map: class-default (match-any)
    42 packets, 6900 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
```



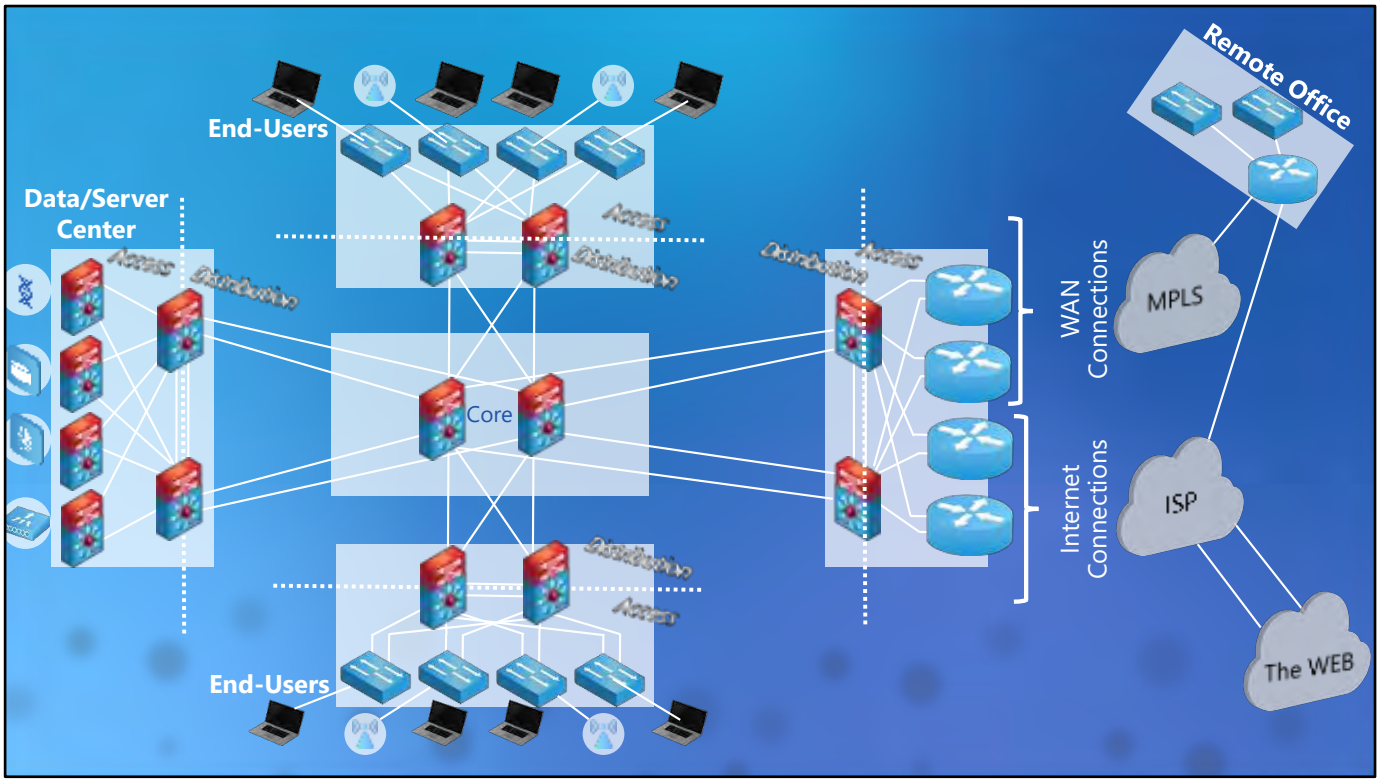
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Next Generation Campus Networks

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

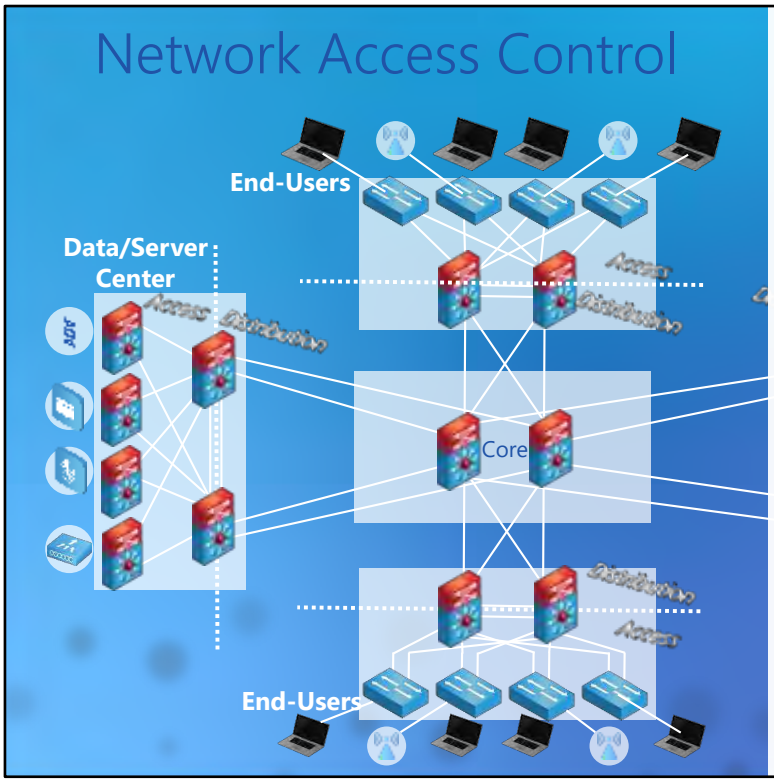
Network Access Control, TrustSec, and MACSec

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Network Access Control



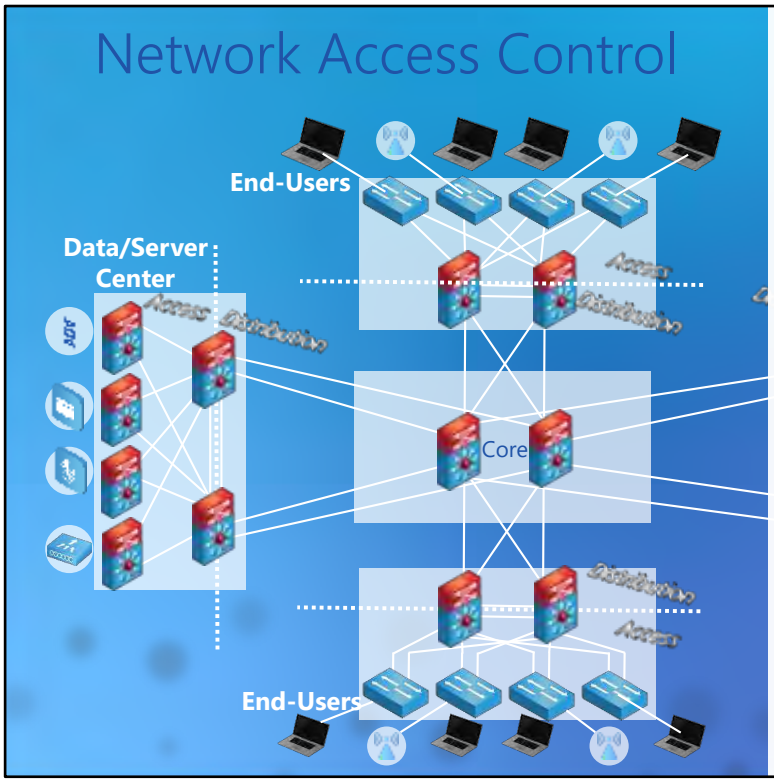
How can we authenticate who or what is connecting to the wired or wireless network?

- 802.1x
- MAC Authentication Bypass (MAB)
- Web Authentication (WebAuth)

Purpose: Deny access until the user/device successfully authenticates

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Network Access Control

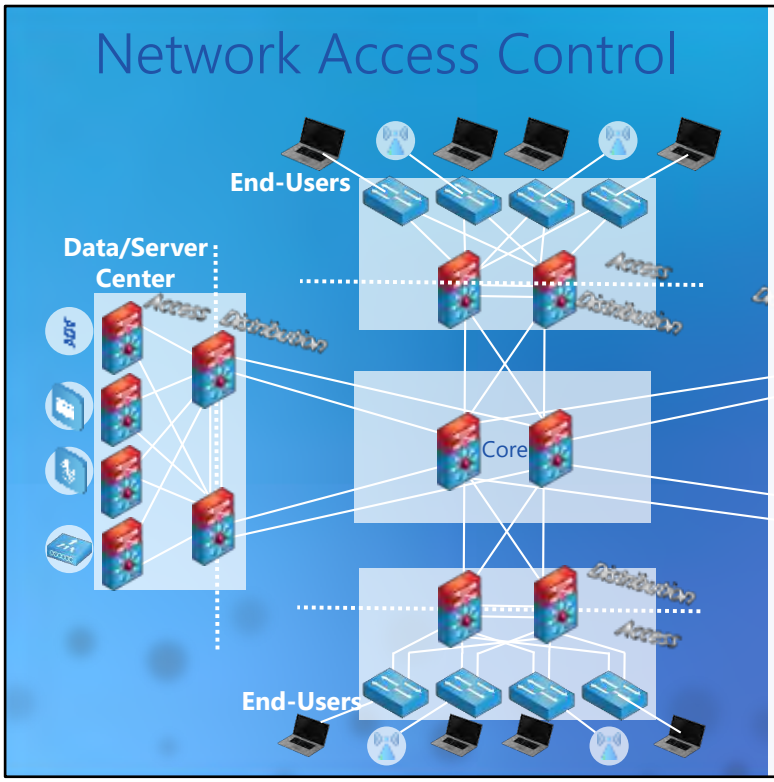


How can we authenticate who or what is connecting to the wired or wireless network?

- 802.1x
  - Usernames and Passwords with a Supplicant
- MAC Authentication Bypass (MAB)
- Web Authentication (WebAuth)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Network Access Control

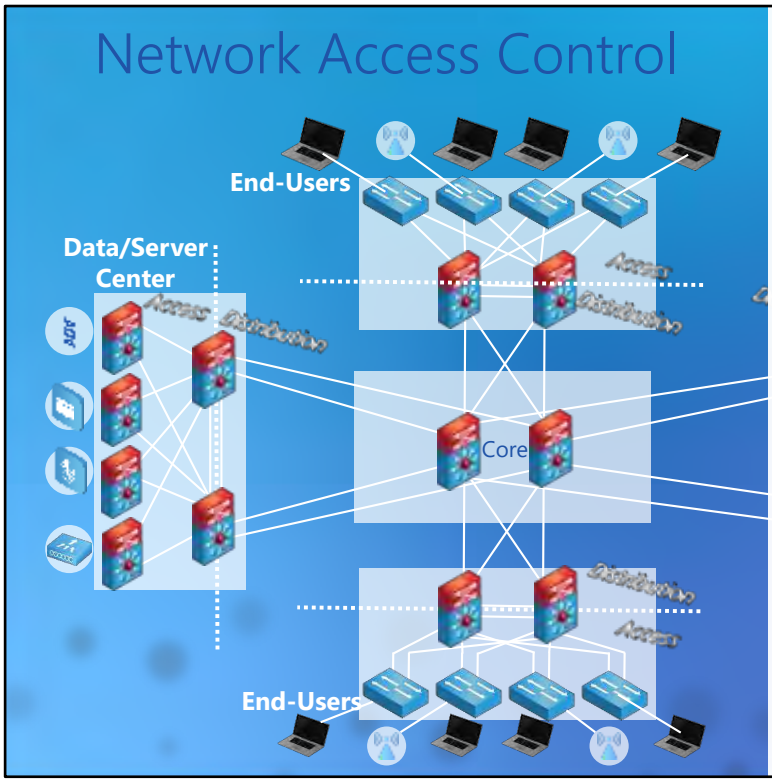


How can we authenticate who or what is connecting to the wired or wireless network?

- 802.1x
  - Usernames and Passwords with a Supplicant
- MAC Authentication Bypass (MAB)
  - MAC addresses
- Web Authentication (WebAuth)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

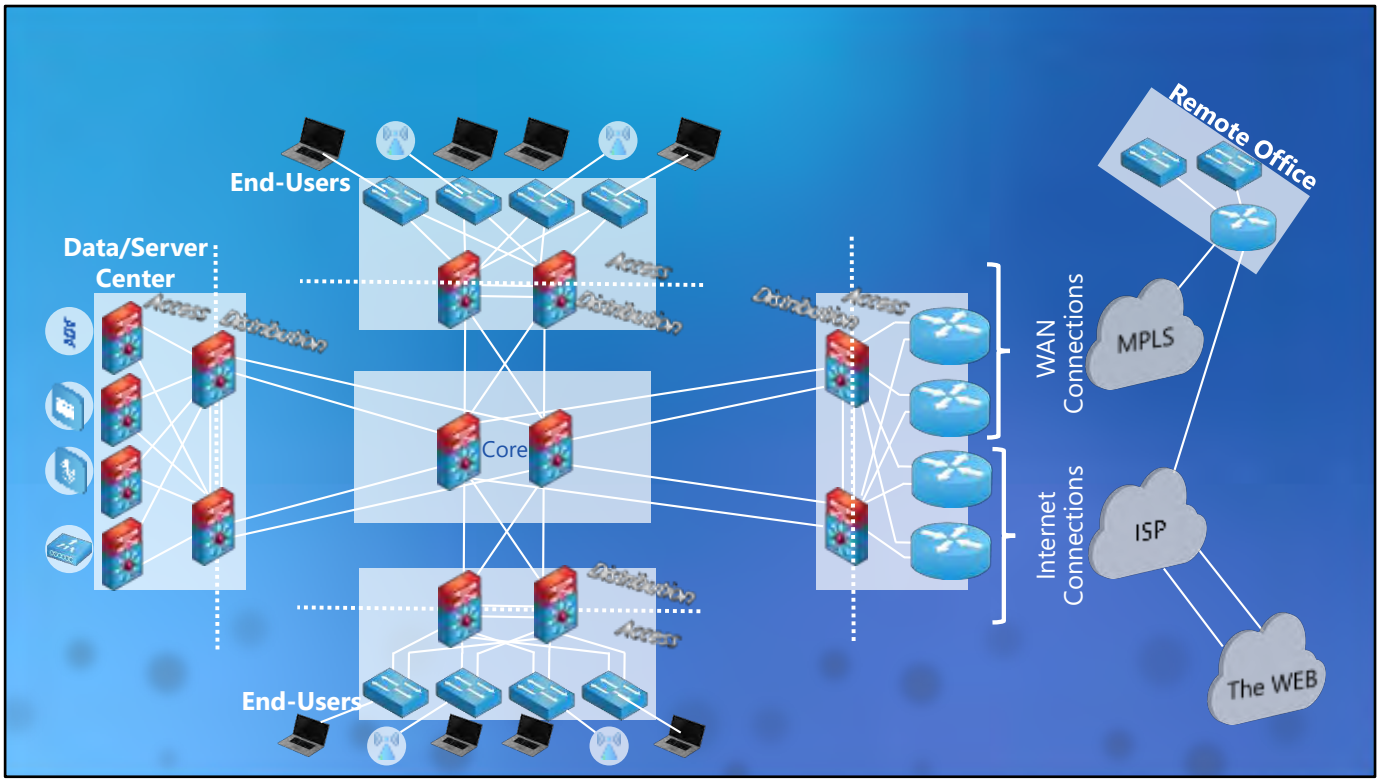
Network Access Control



How can we authenticate who or what is connecting to the wired or wireless network?

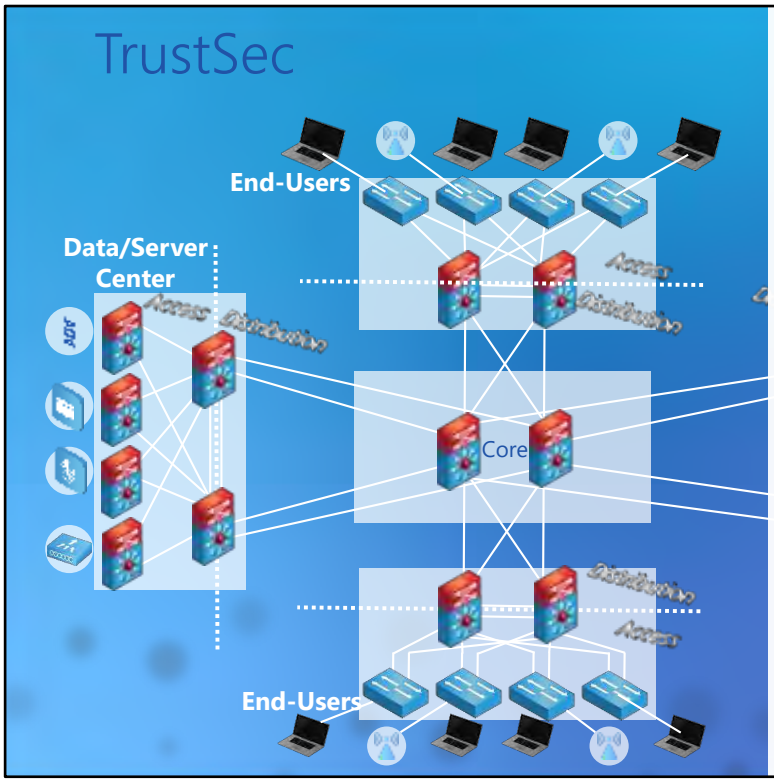
- 802.1x
  - Usernames and Passwords with a Supplicant
- MAC Authentication Bypass (MAB)
  - MAC addresses
- Web Authentication (WebAuth)
  - Usernames and Passwords with a Web portal

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

TrustSec

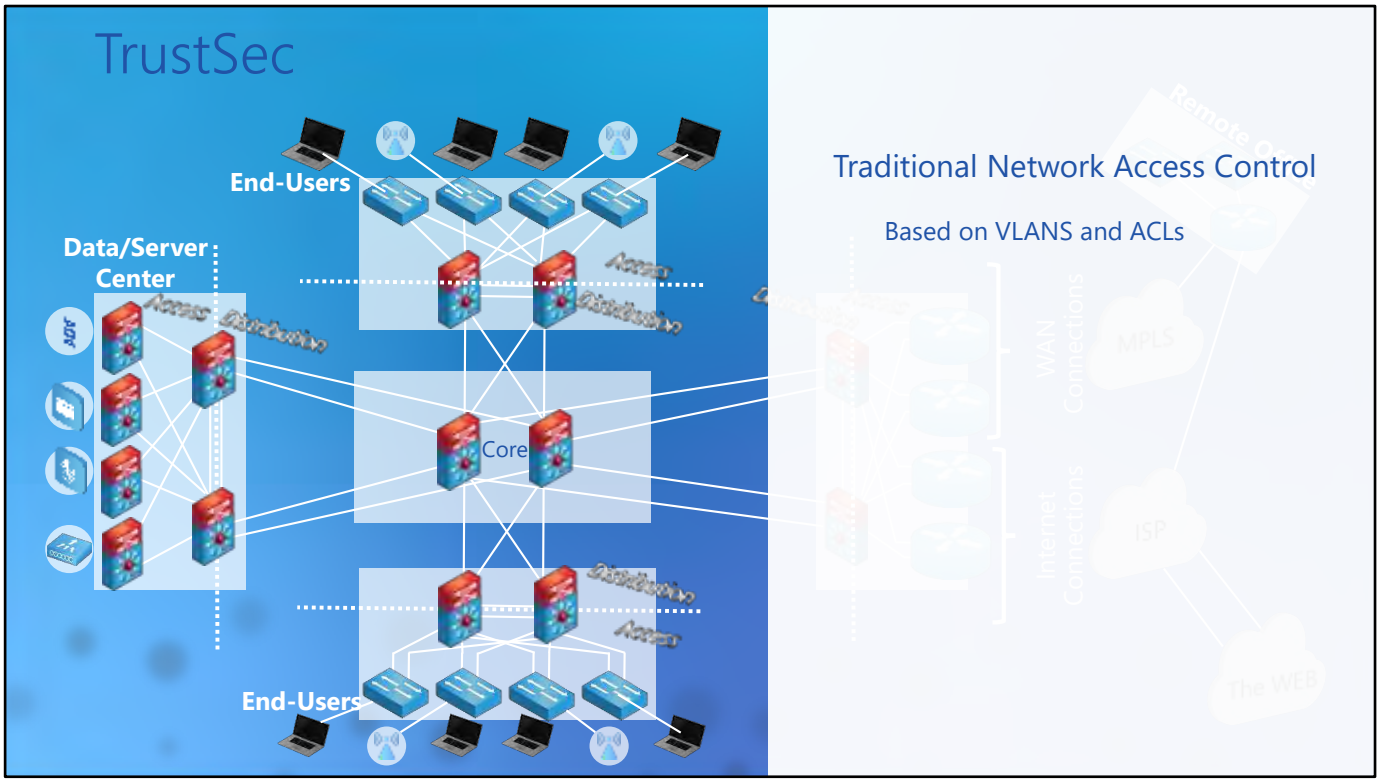


A centralized classification and policy enforcement function

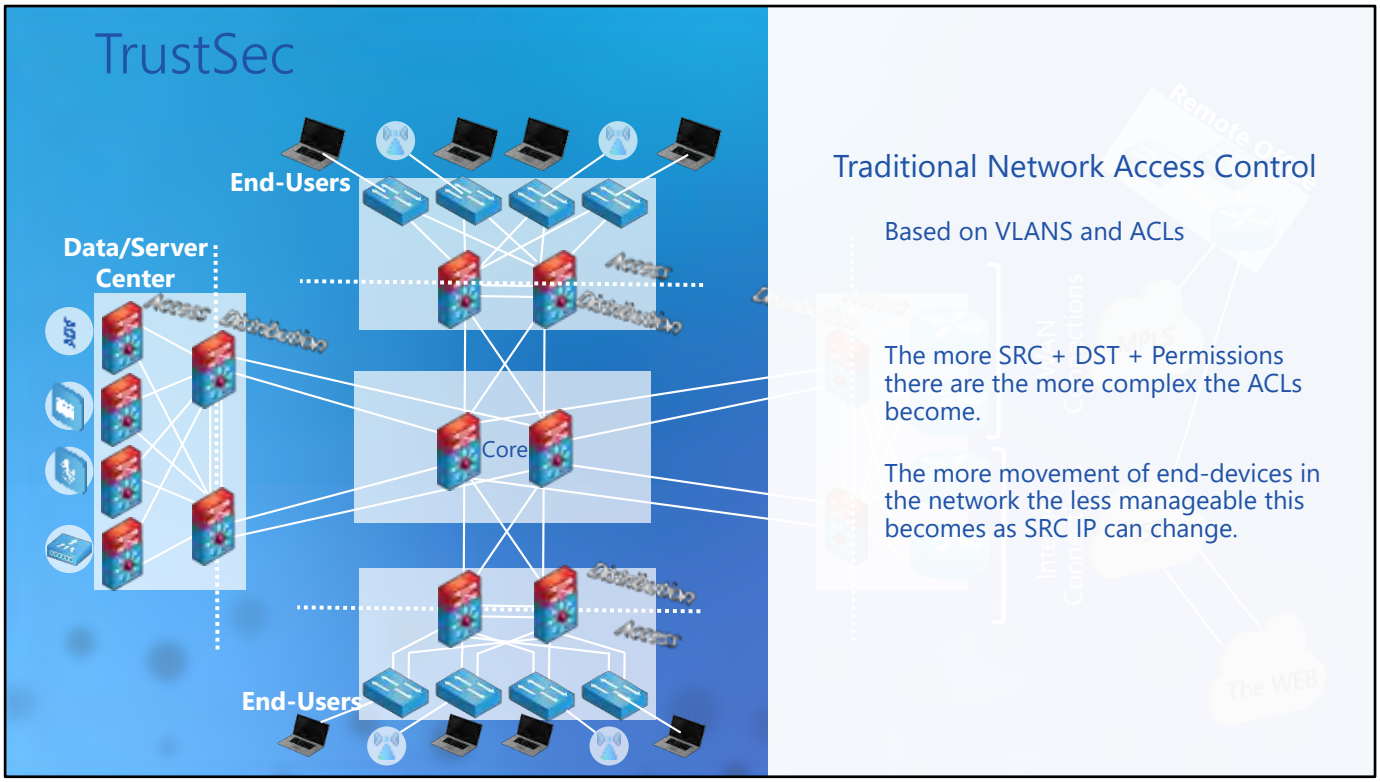
- Available for
  - Switches
  - Routers
  - Wireless
  - Firewall

Centrally managed using ISE

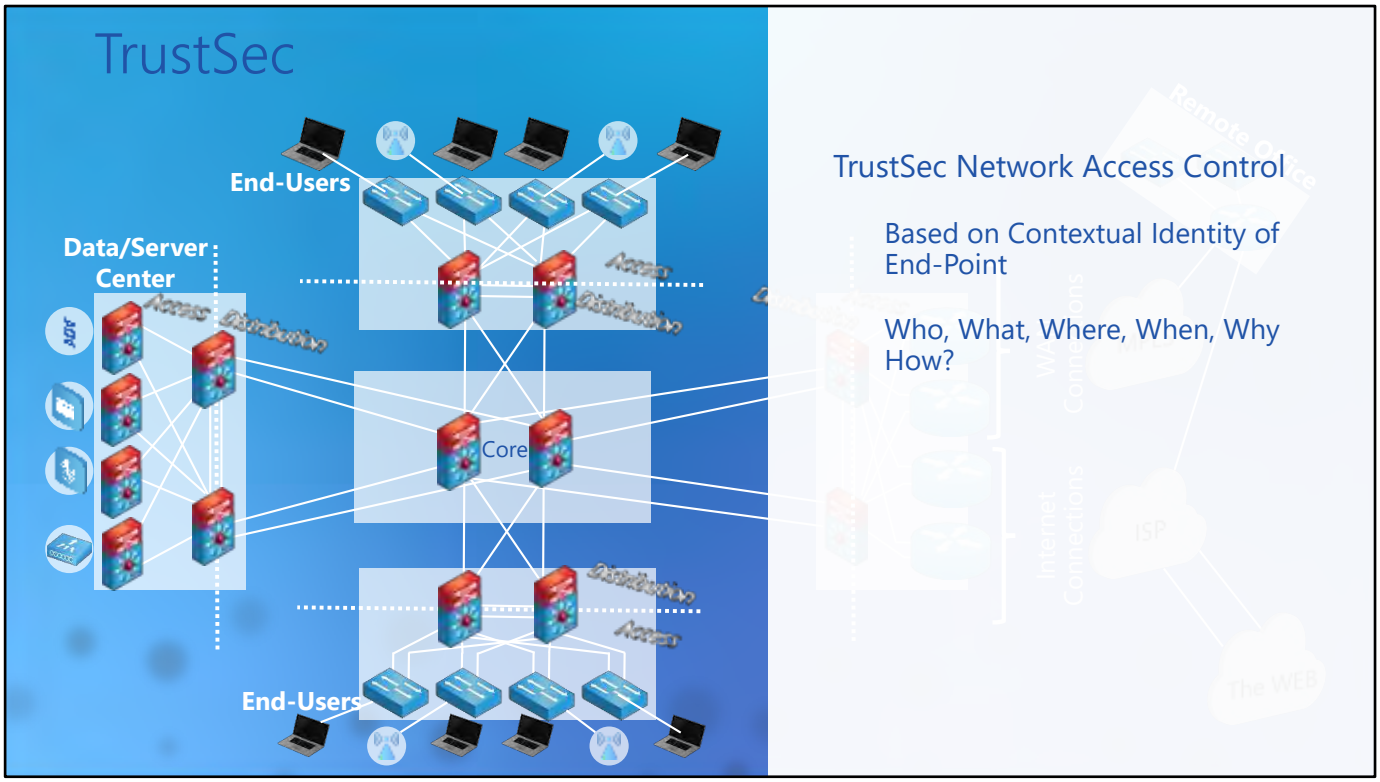
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



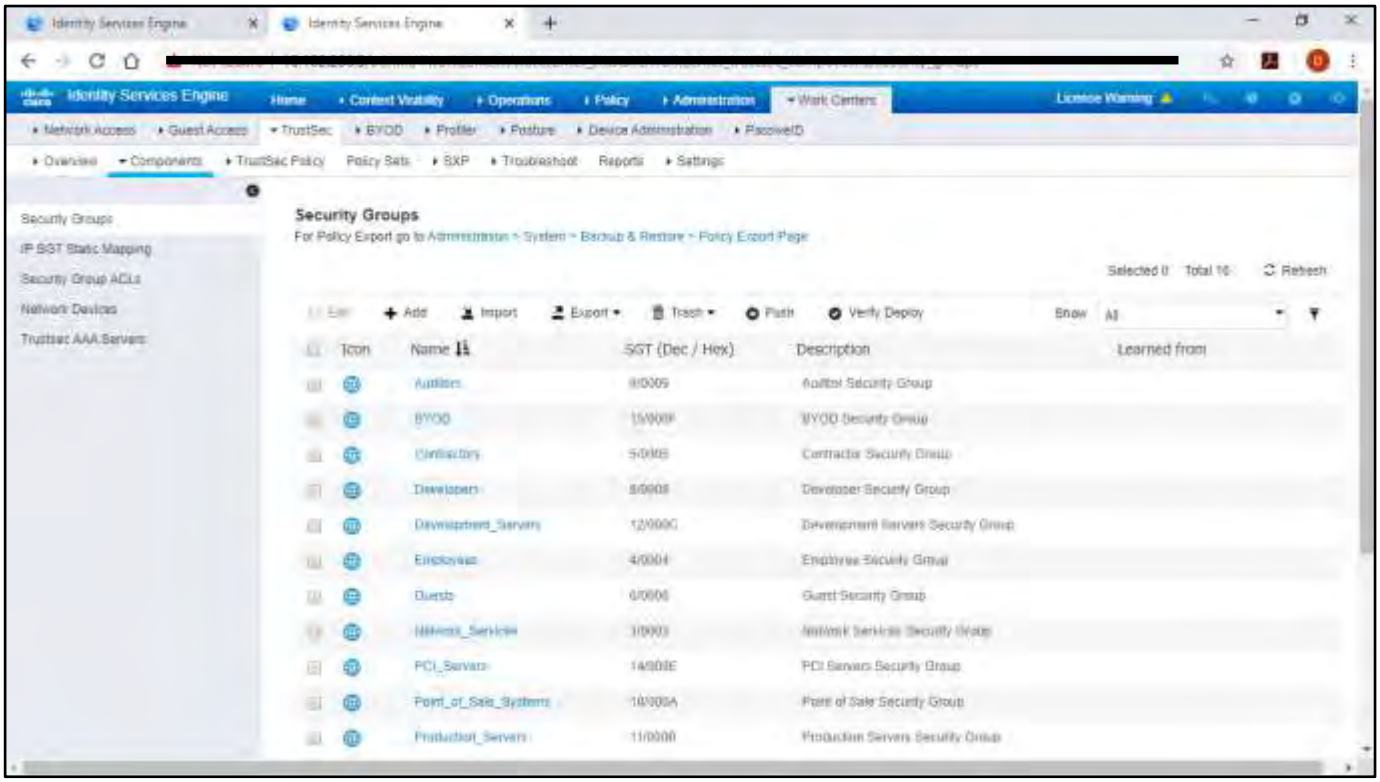
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



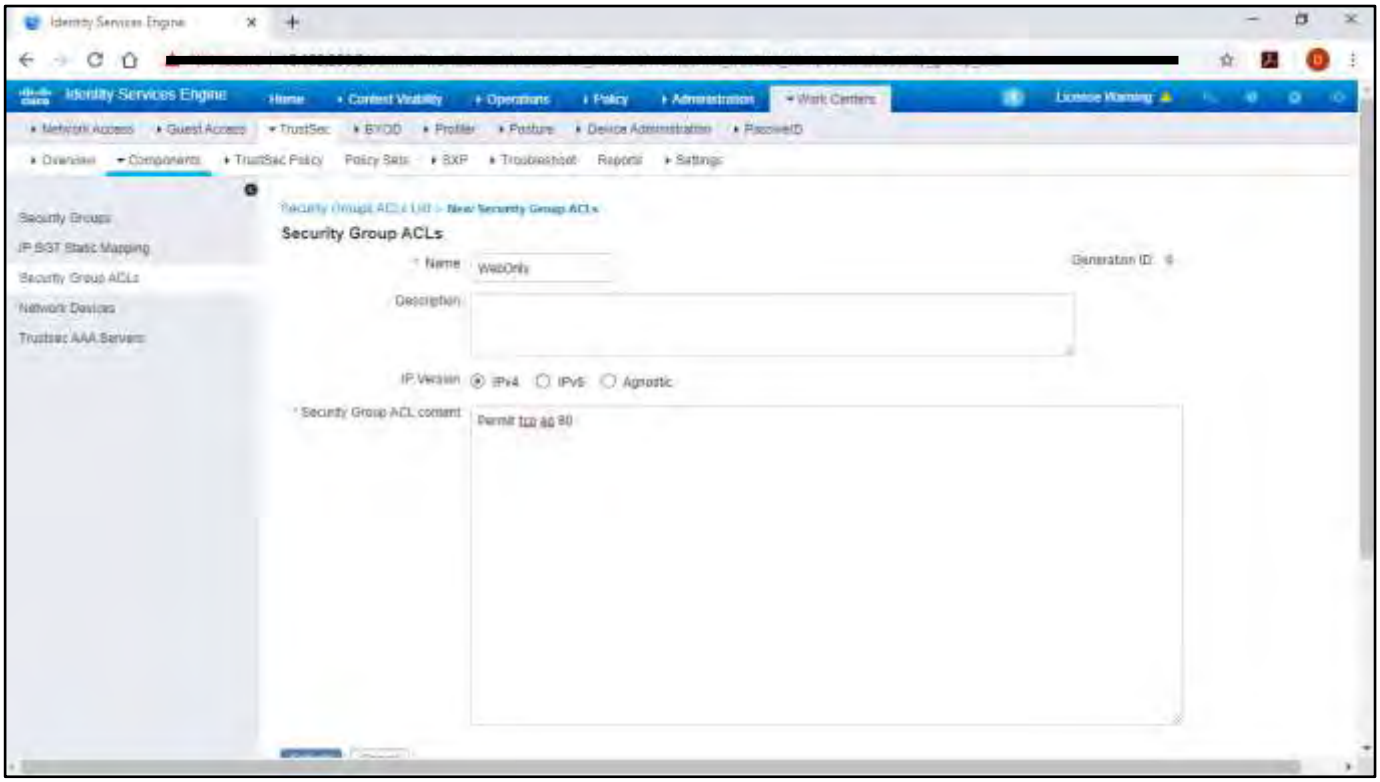
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

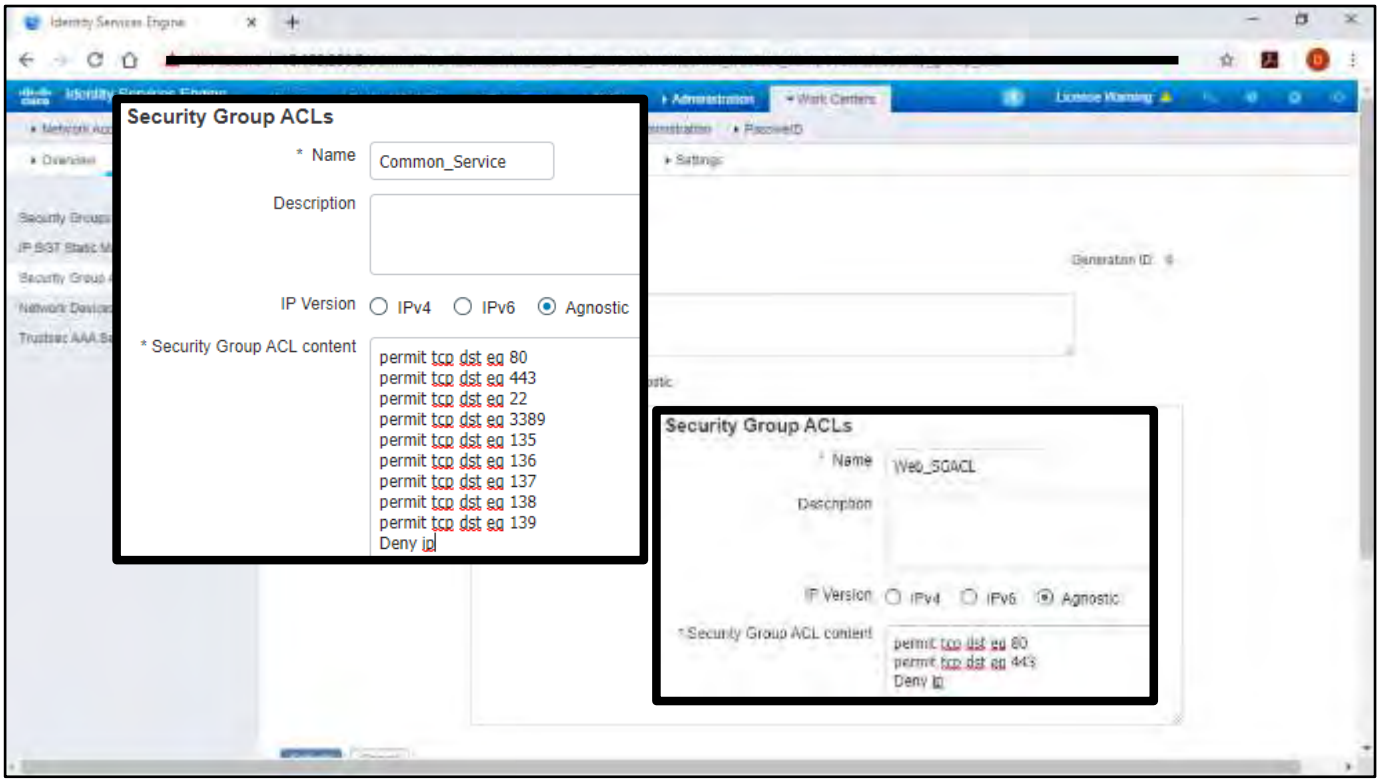


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

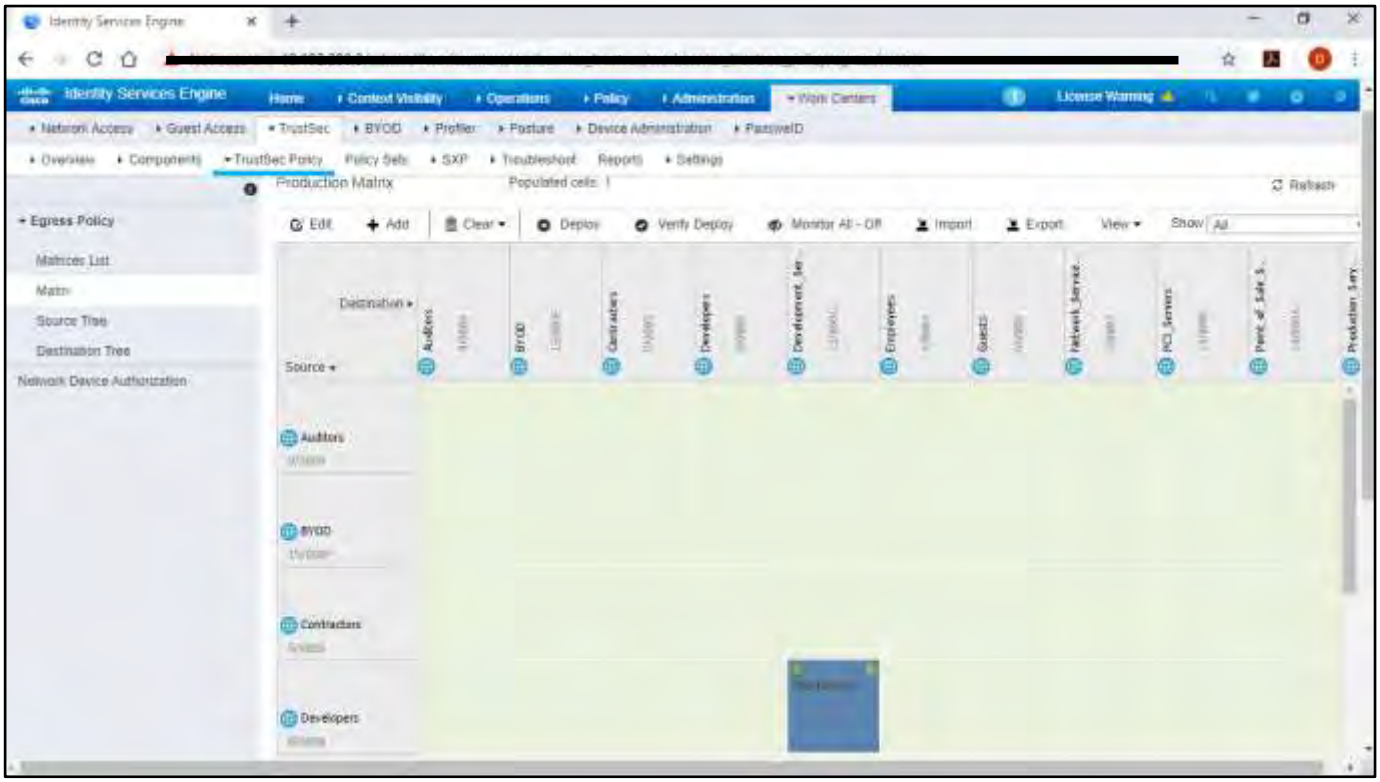


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

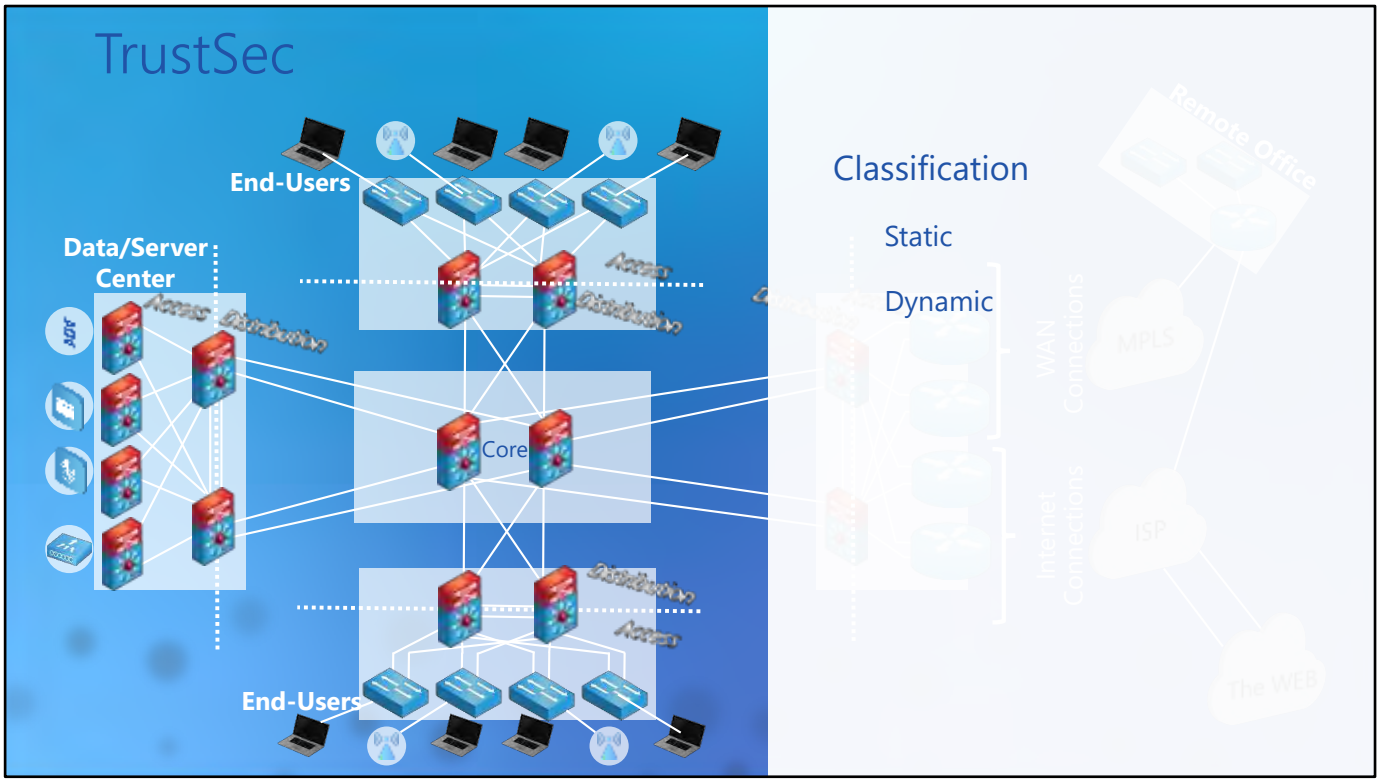


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



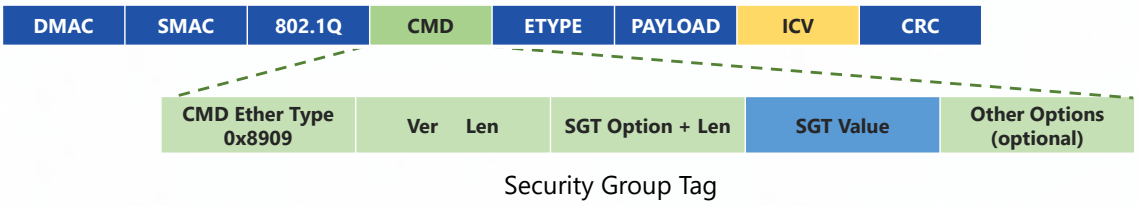
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



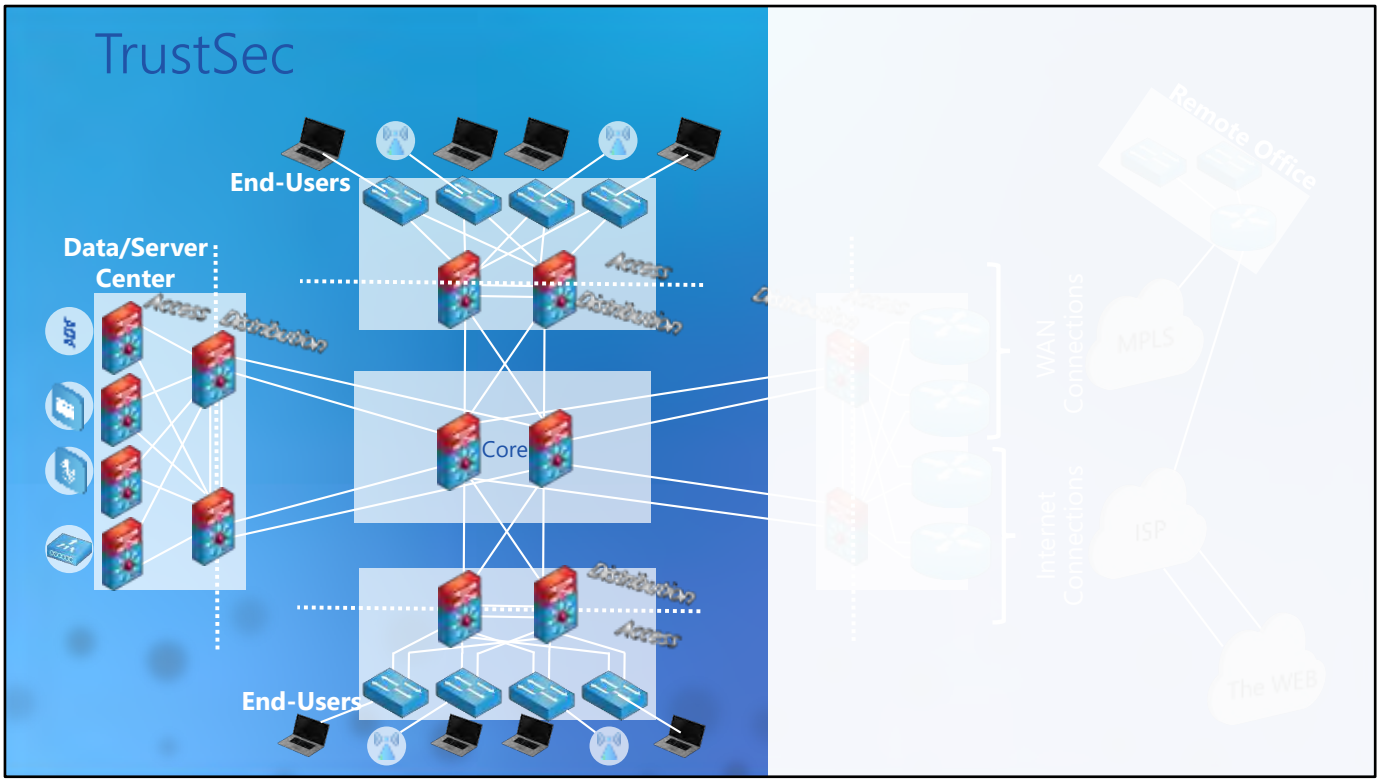
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

TrustSec

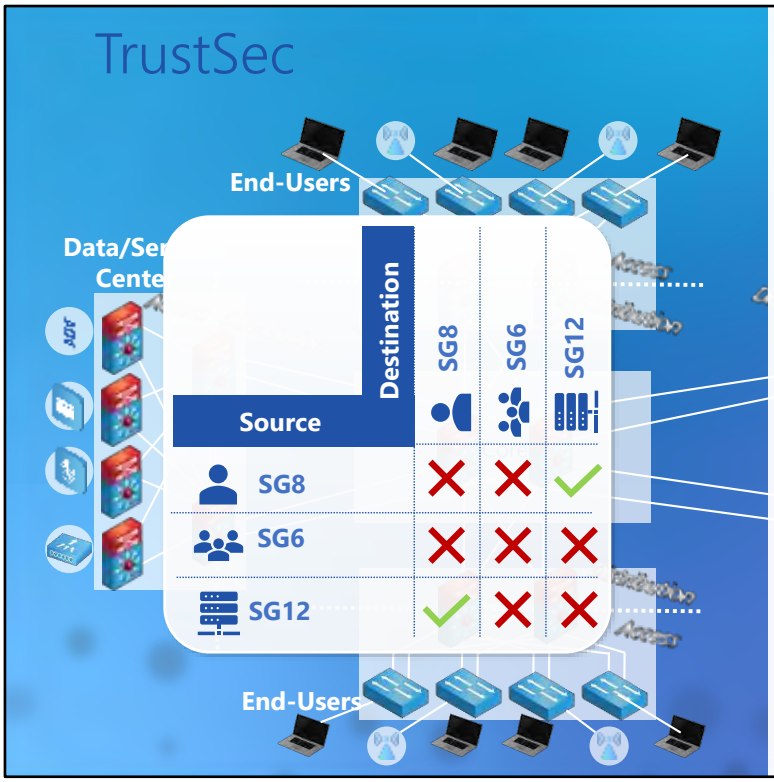


Security Group Tag

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

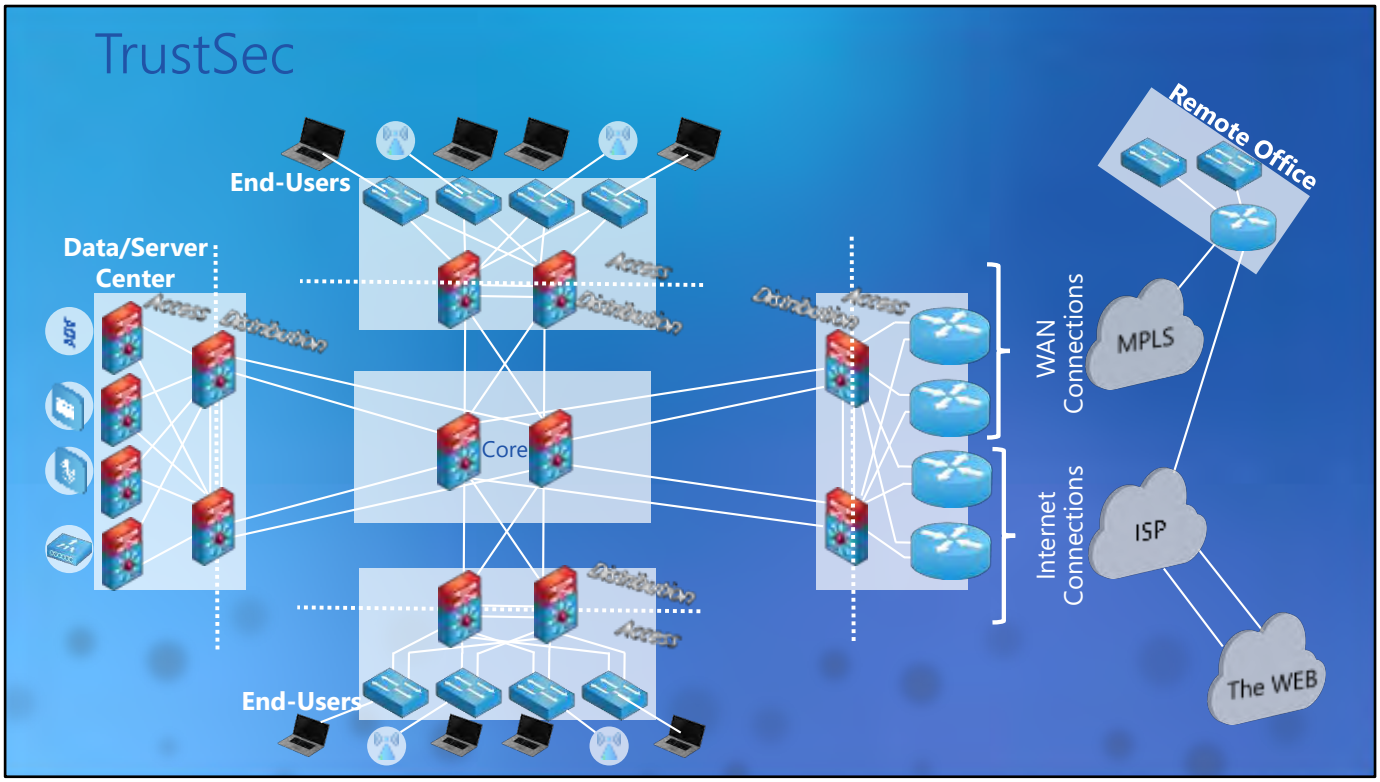


Enforcement

- Typically on the Egress network device
  - Destination based
  - Using "The Matrix"

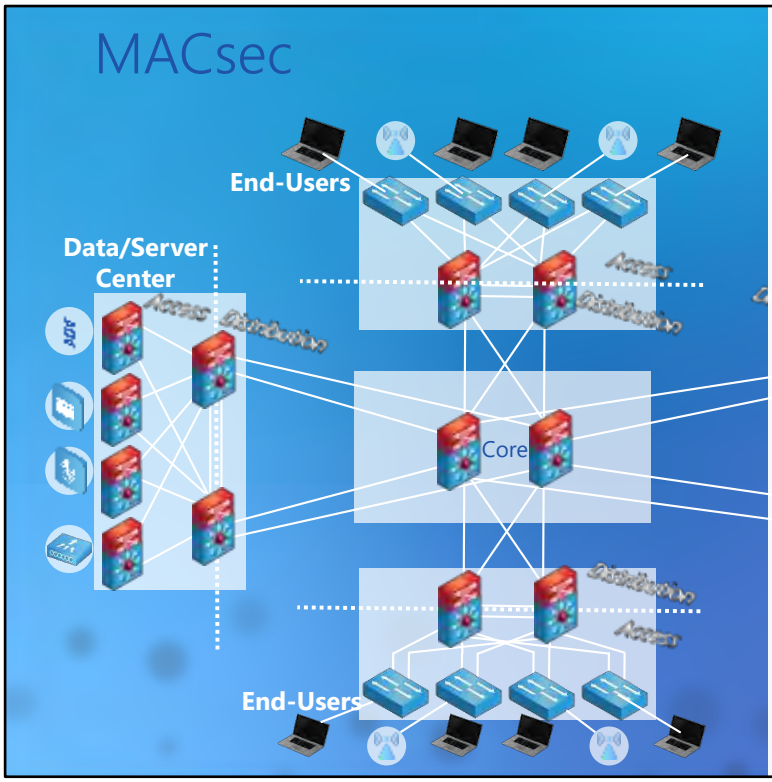
Every network device needs a copy of "the matrix" from ISE so they can make decisions without having to bug ISE every time.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MACsec



IEEE 802.1AE standard

A Layer 2 hop-by-hop encryption method for secure L2 communication

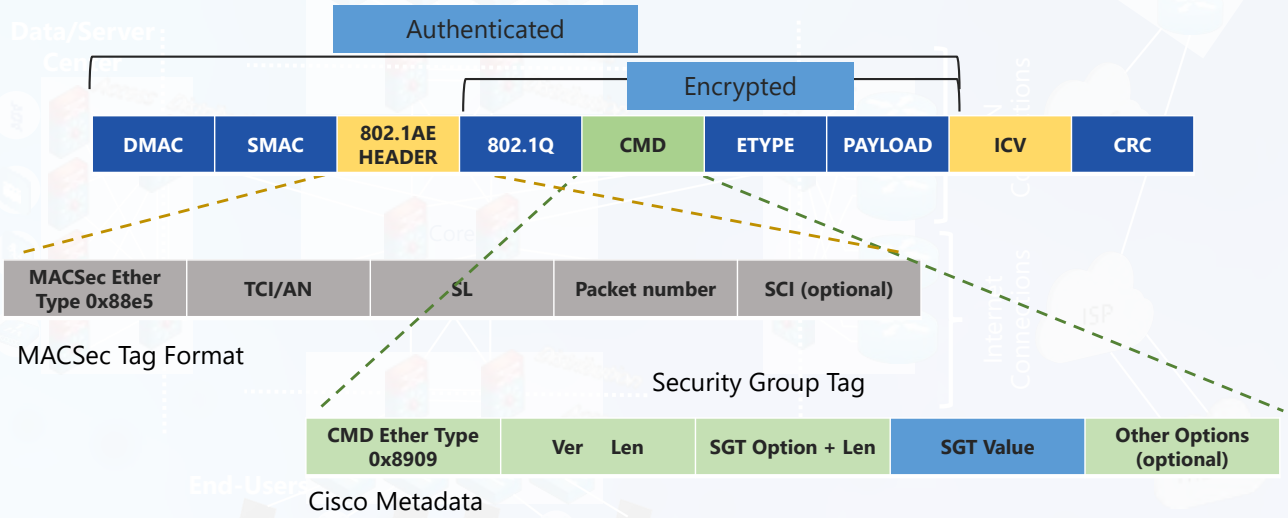
- Provides data confidentiality and integrity
- Encrypts traffic between two MACsec peers

Note: traffic will be unencrypted in the switch for processing:

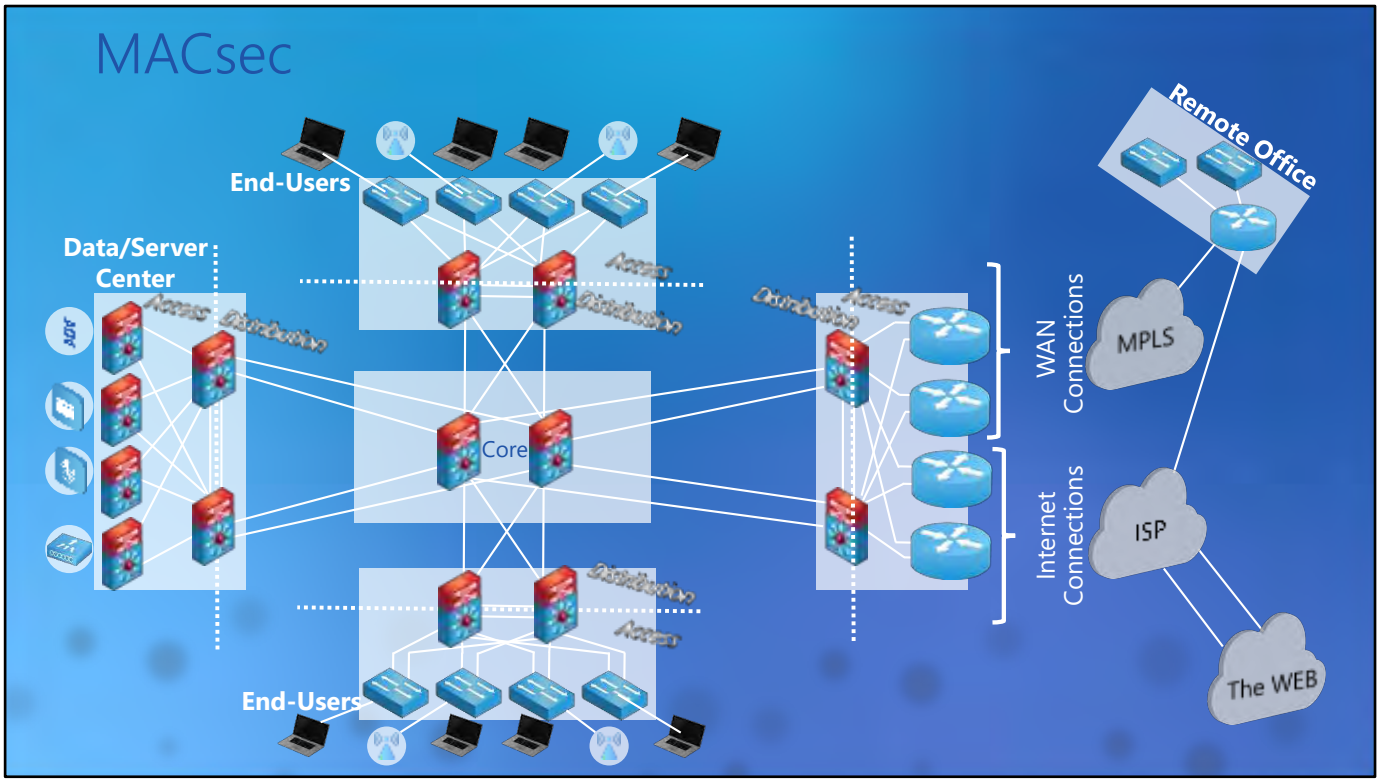
- SGT tags
- QoS markings/classification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MACsec



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP and VXLAN

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Location/ID Separation Protocol (LISP)

Created to address routing scalability problems on the Internet

It is a:

- Routing architecture
- Data and Control Plane protocol

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Location/ID Separation Protocol (LISP)

- World Problems
  - Aggregation
  - Traffic Engineering
  - Multihoming
  - Instability
  - Mobility
- Solution
  - LISP

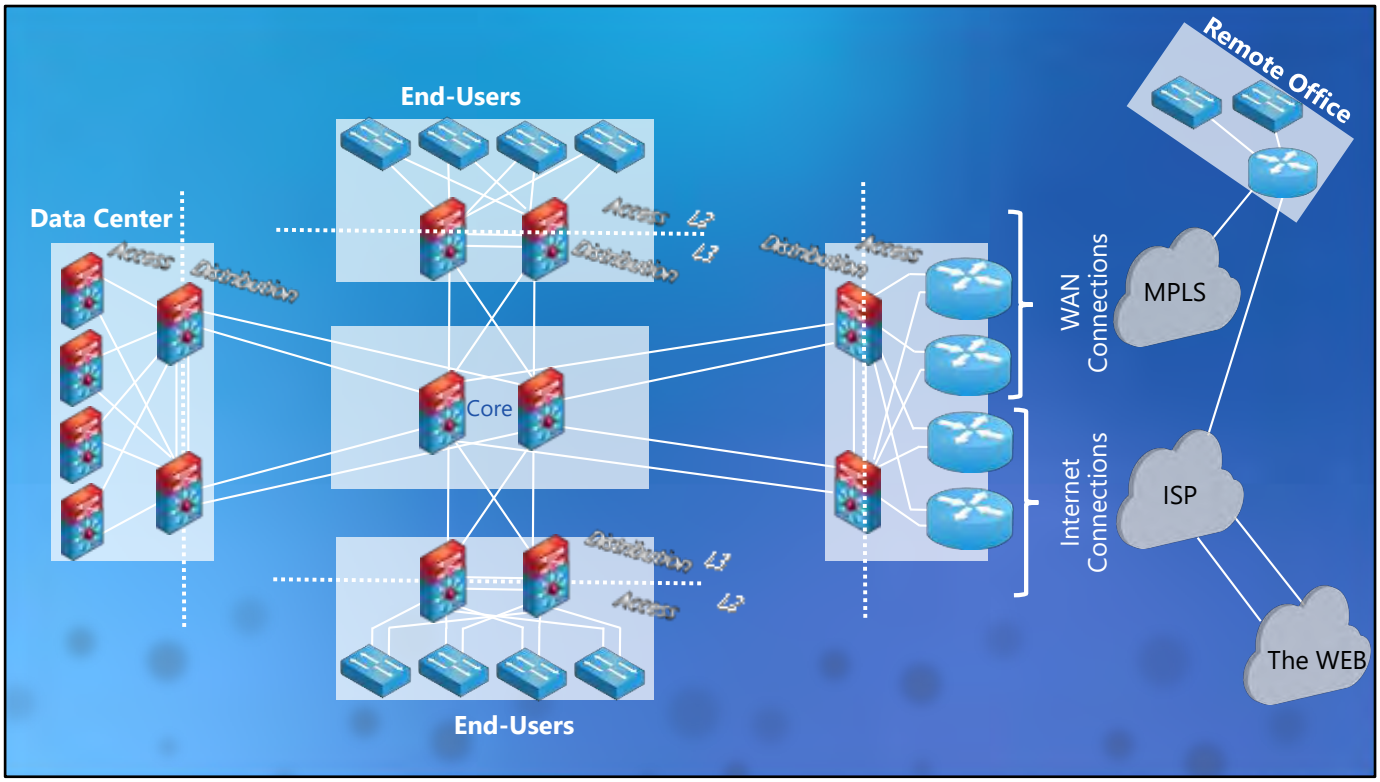
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Location/ID Separation Protocol (LISP)

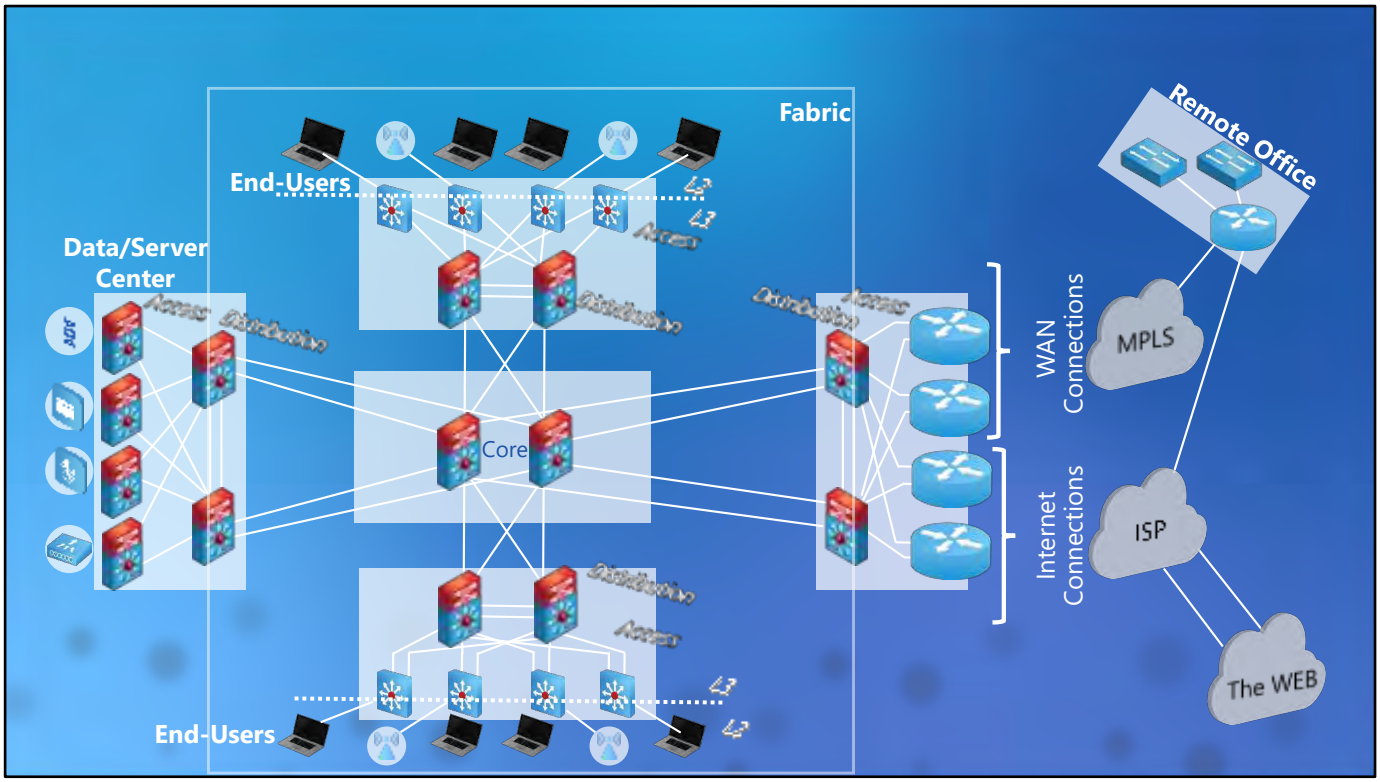
Now being implemented in

- Data centers
- Campus networks
- Branch offices
- Next-gen WANs
- Service Provider Cores

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

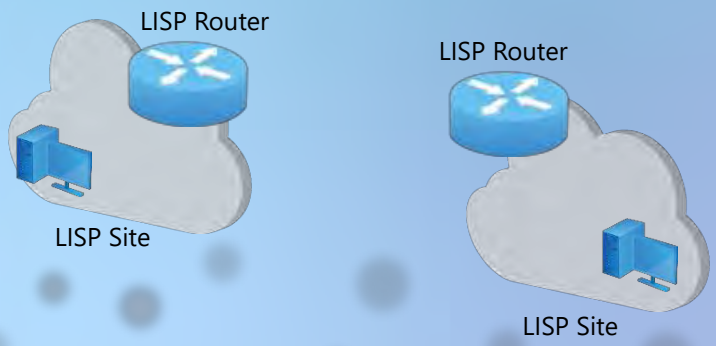


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



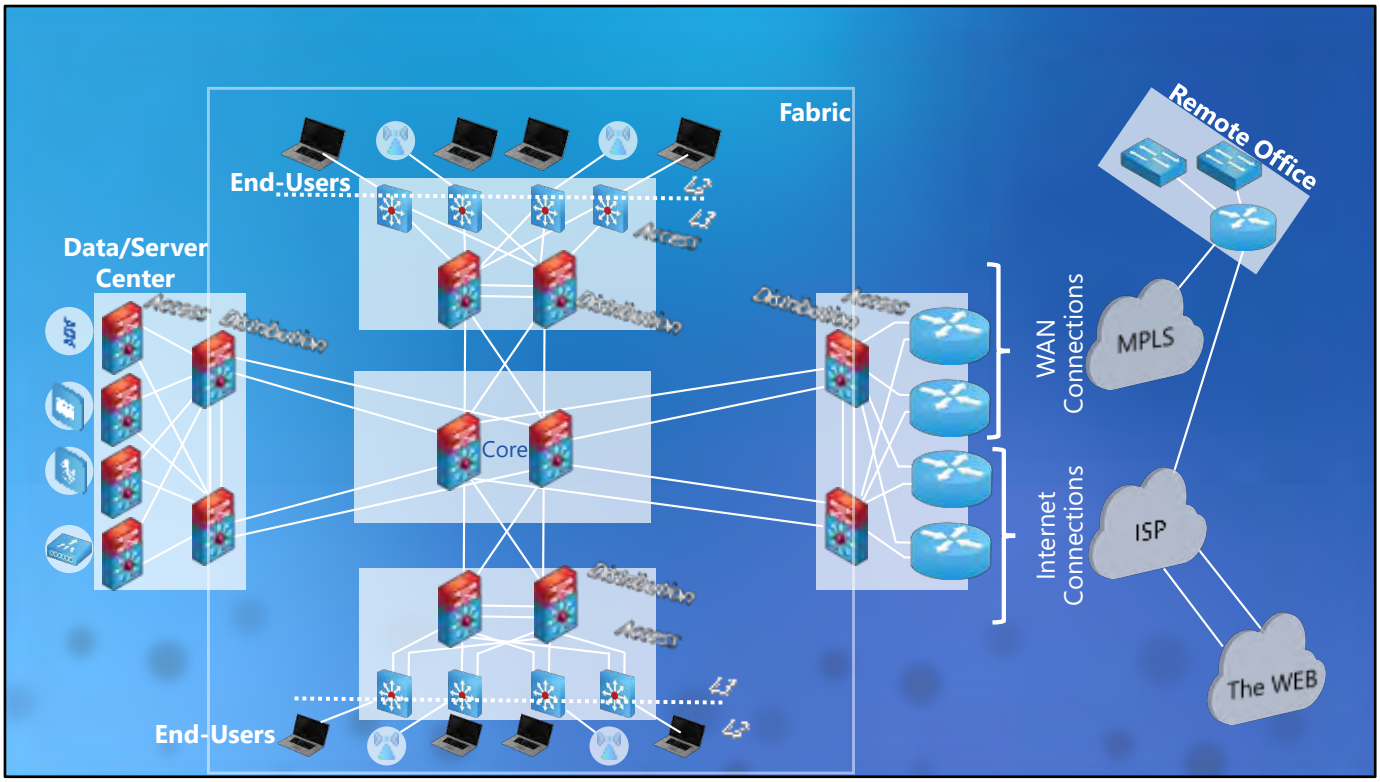
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Sites



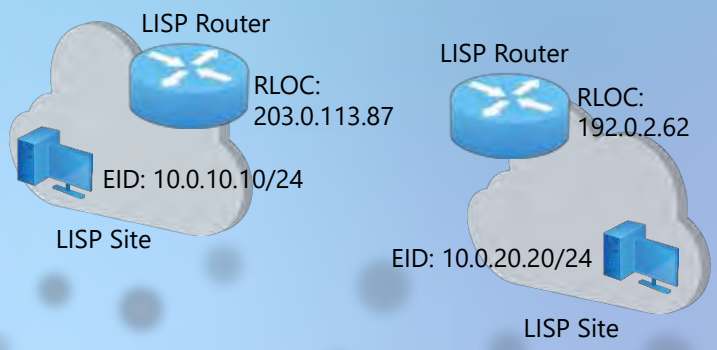
Where LISP routers and Endpoints reside

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Namespaces



Endpoint Identifiers (EIDs)

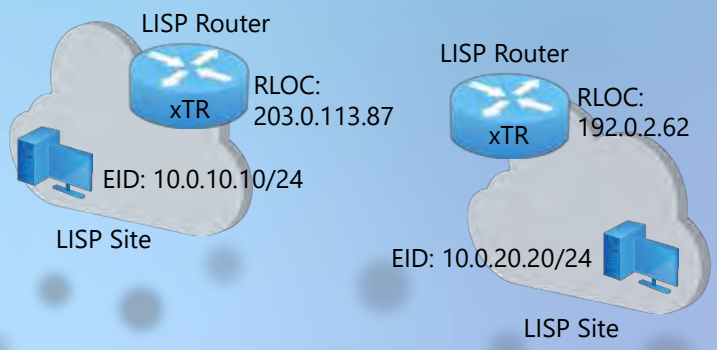
- IP assigned to end hosts

Routing Locators (RLOCs)

- IP assigned to devices that make up the routing system

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Routers



xTR

A tunnel router that performs ITR and ETR functions

ITR (Ingress Tunnel Router)

A LISP router that encapsulates IP packets from EIDs in a site that are destined to another site.

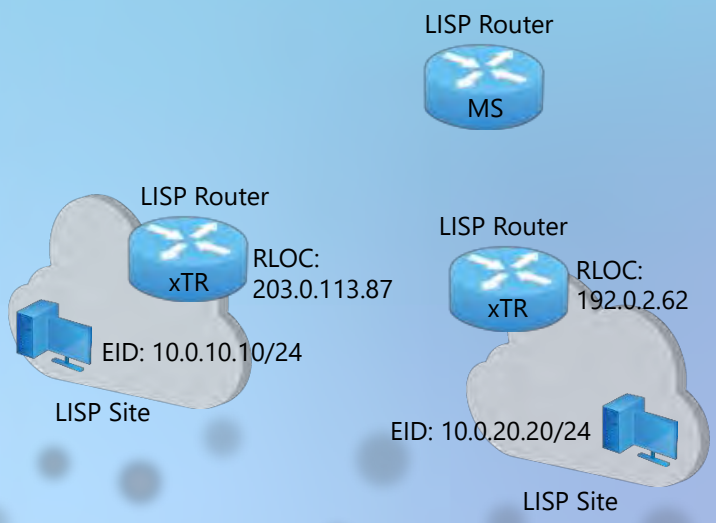
ETR (Egress Tunnel Router)

A LISP router that de-encapsulates LISP packets from a site that are destined to an EID in its site.

Publishes EID-to-RLOC mappings for a site

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

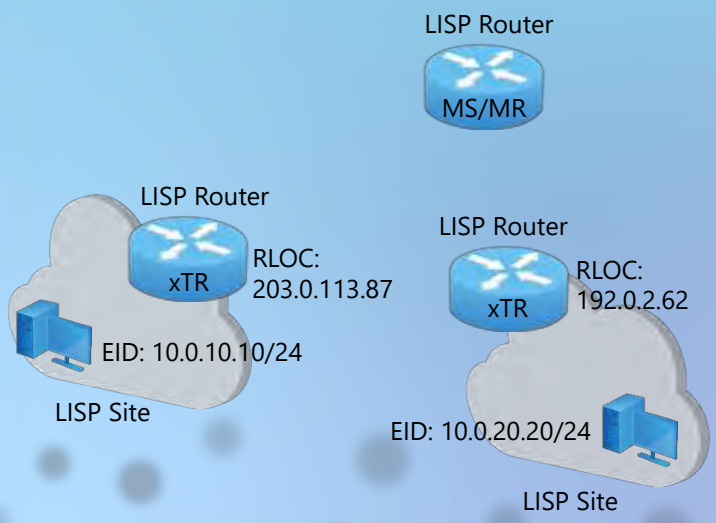
LISP Map Server (MS)



- Learns EID-to-Prefix mapping entries
  - From the ETRs
- Stores mappings
  - Local EID-to-RLOC database

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Map Resolver (MR)

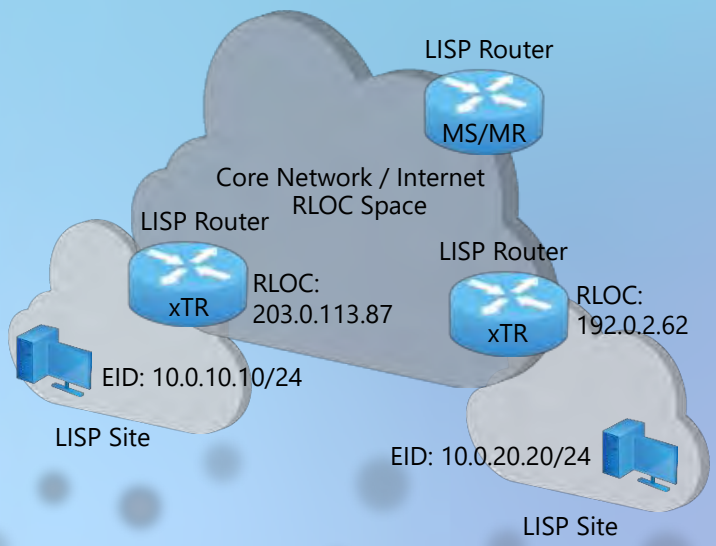


Resolves mapping requests that are received from ITRs.

Consults MS for answer

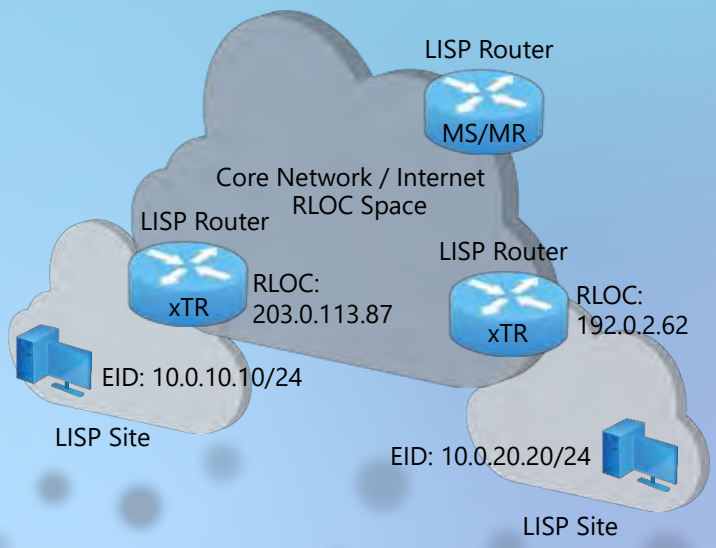
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Registration



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Registration

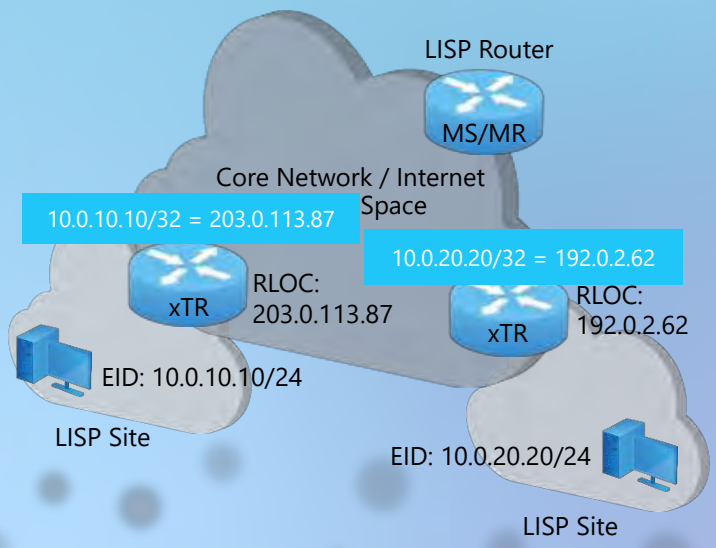


ETRs send mappings to MS

- Based on networks and devices connected to the LISP site.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Registration

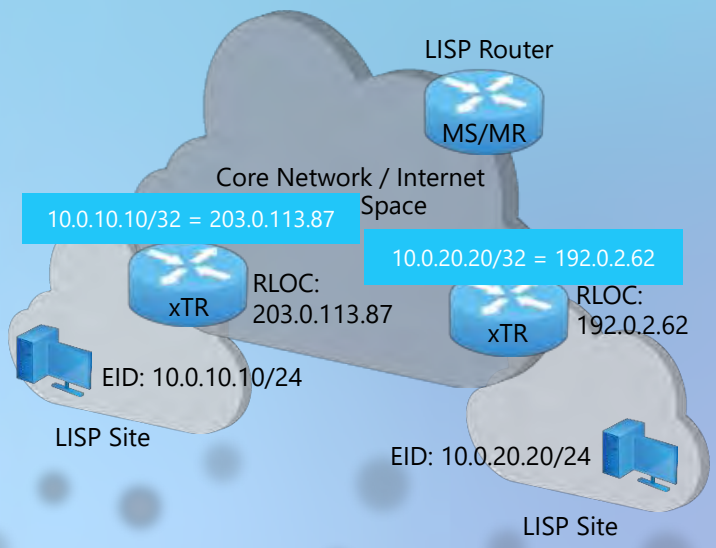


ETRs send mappings to MS

- Based on networks and devices connected to the LISP site.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Registration

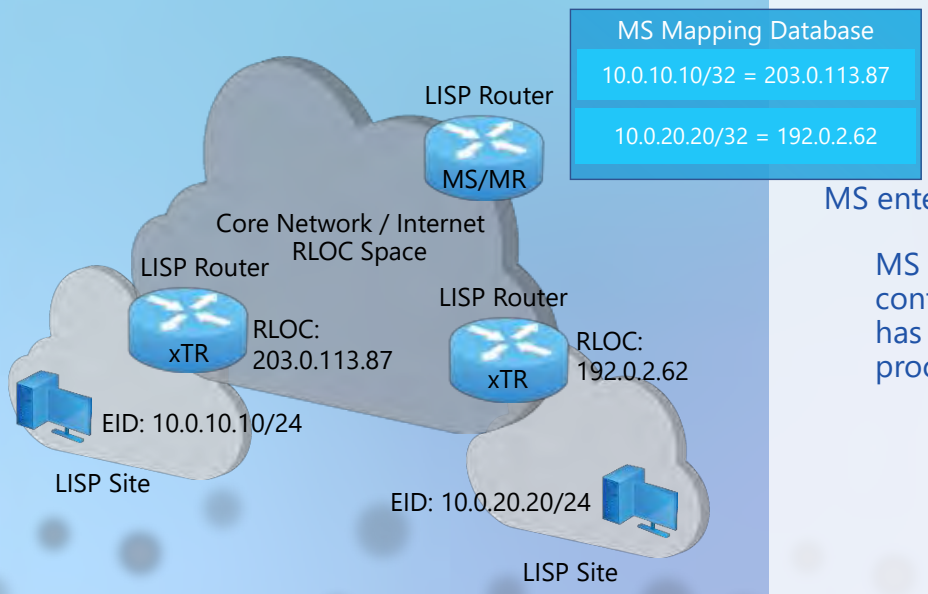


ETRs send mappings to MS

- Based on networks and devices connected to the LISP site.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Registration

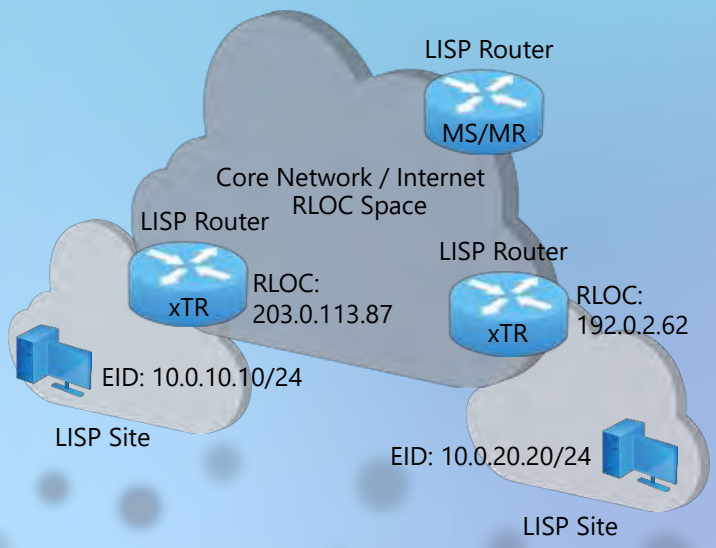


MS enters info in database

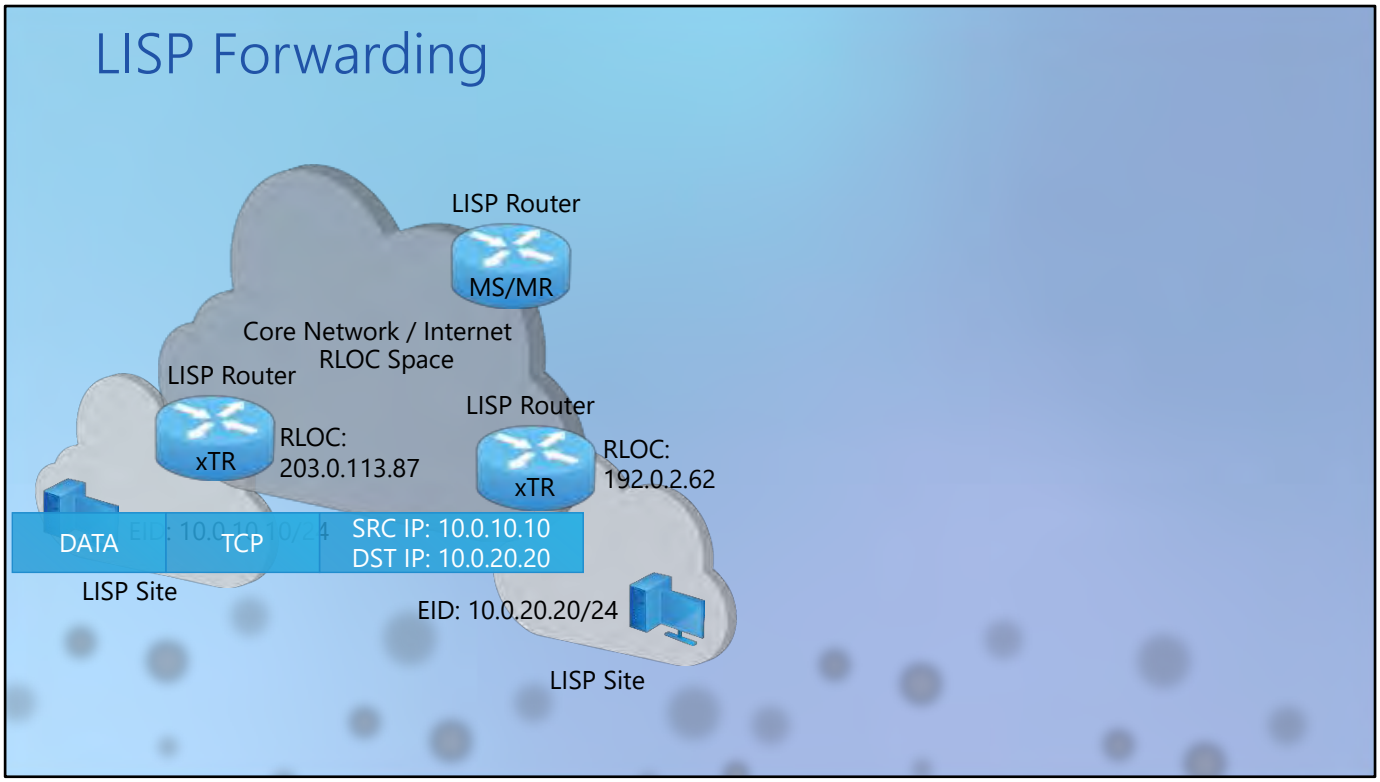
MS sends map notify to ETR to confirm that the map register has been received and processed.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

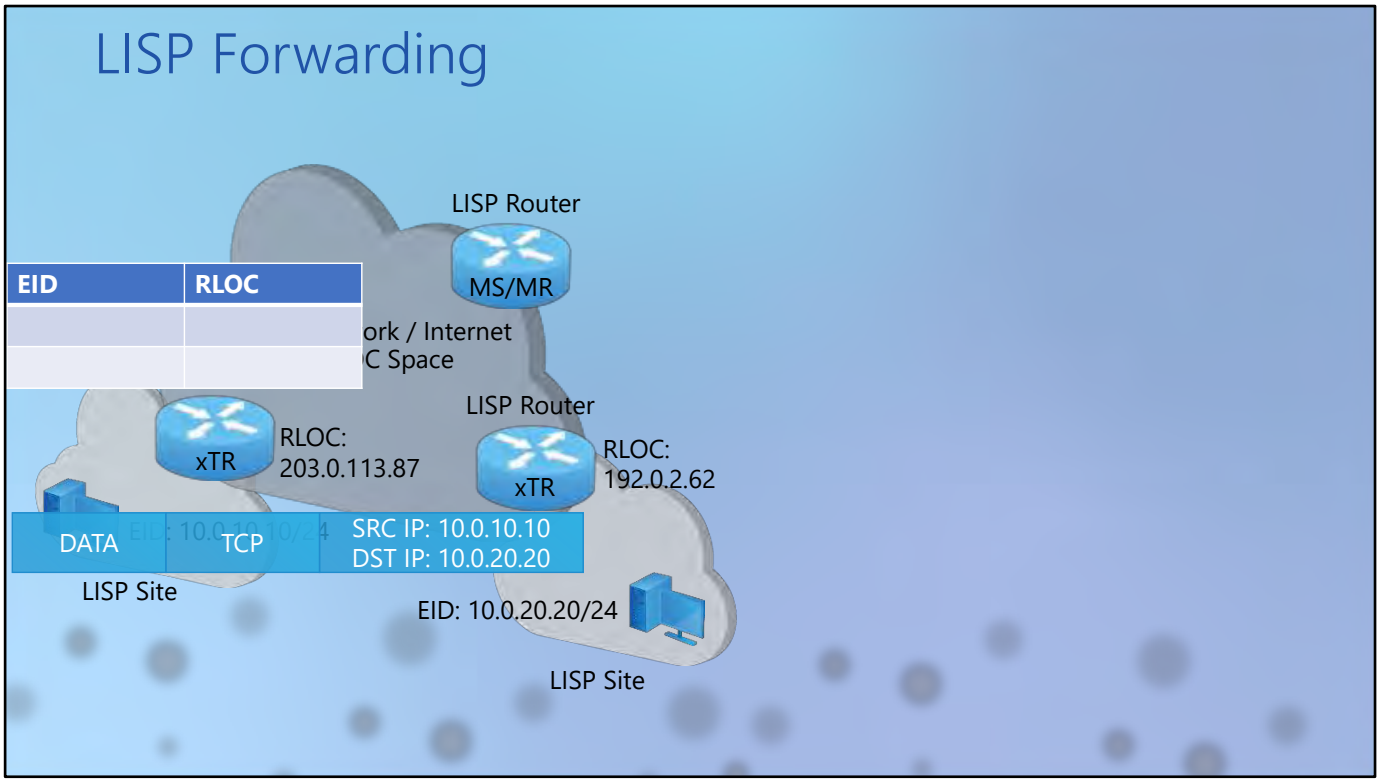
LISP Forwarding



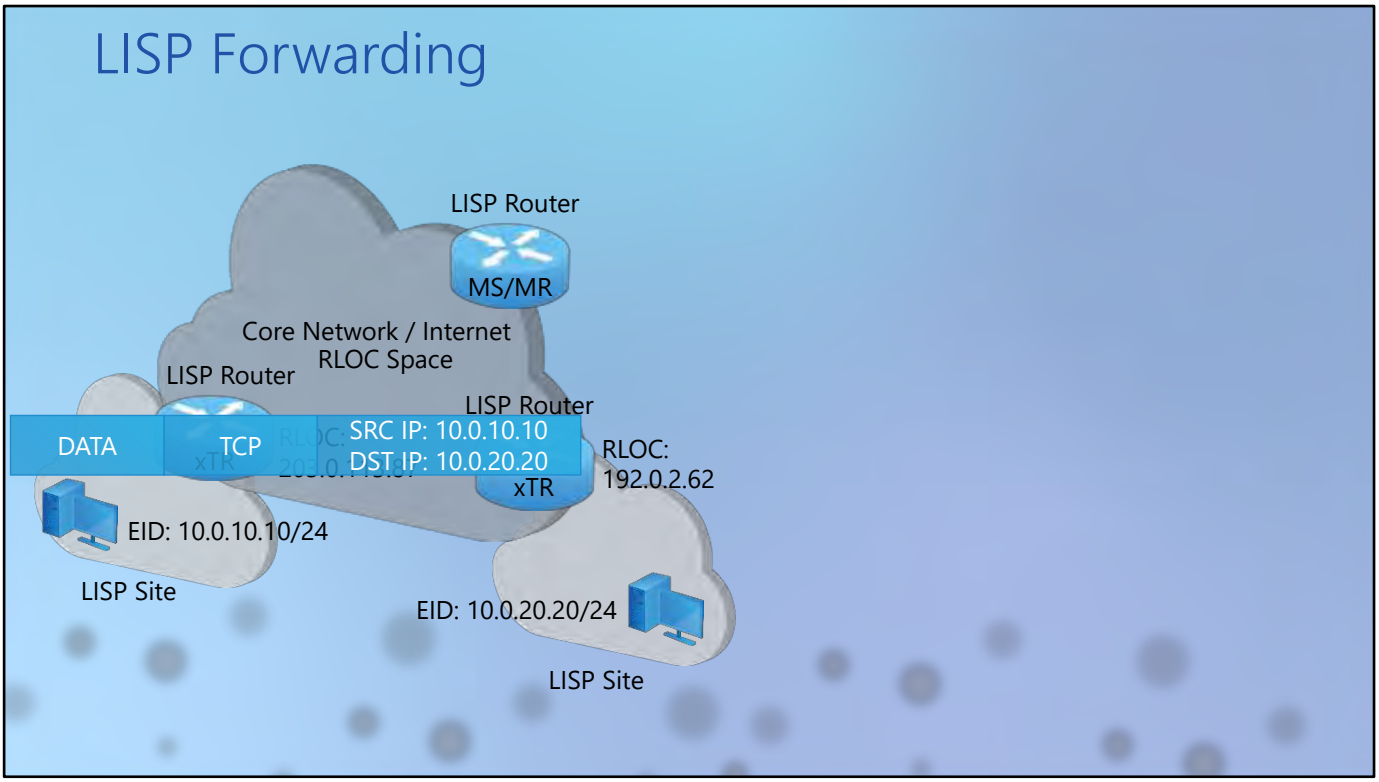
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



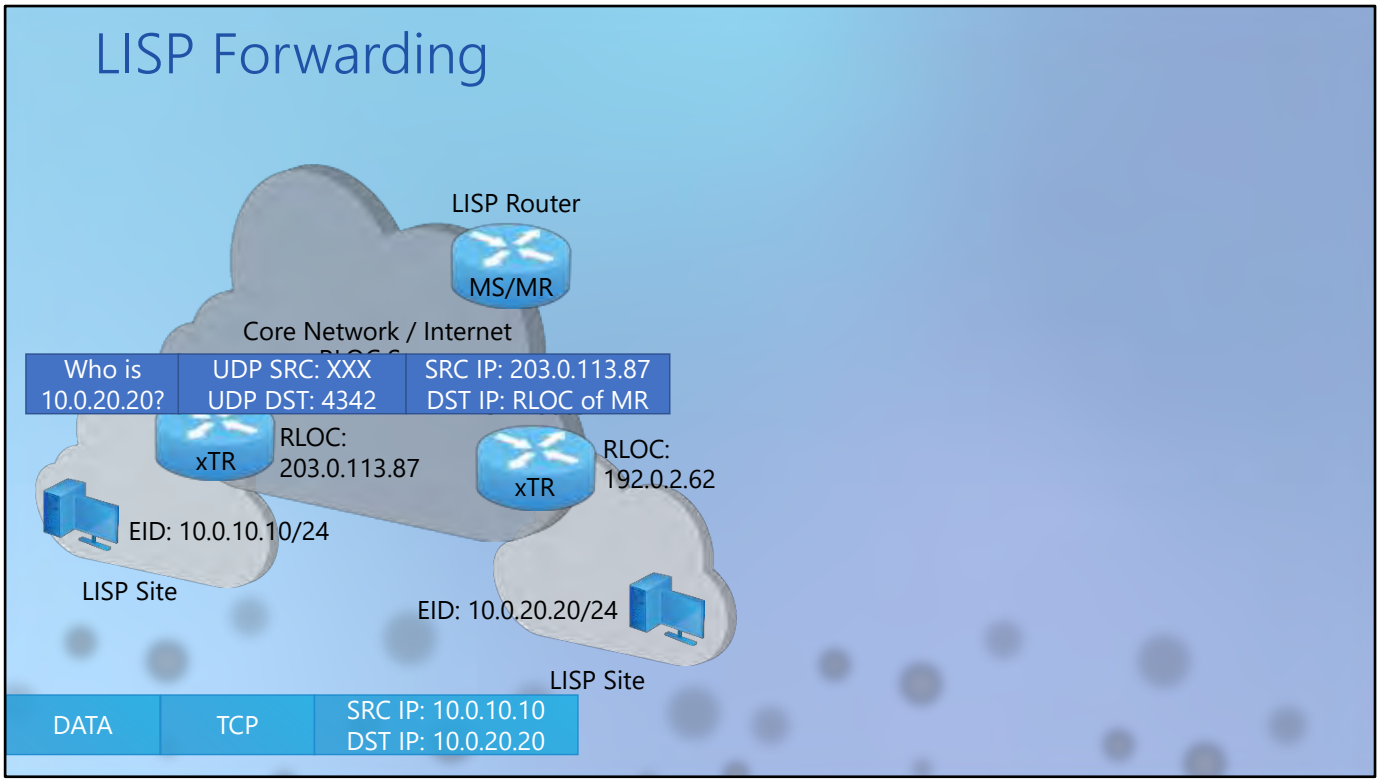
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



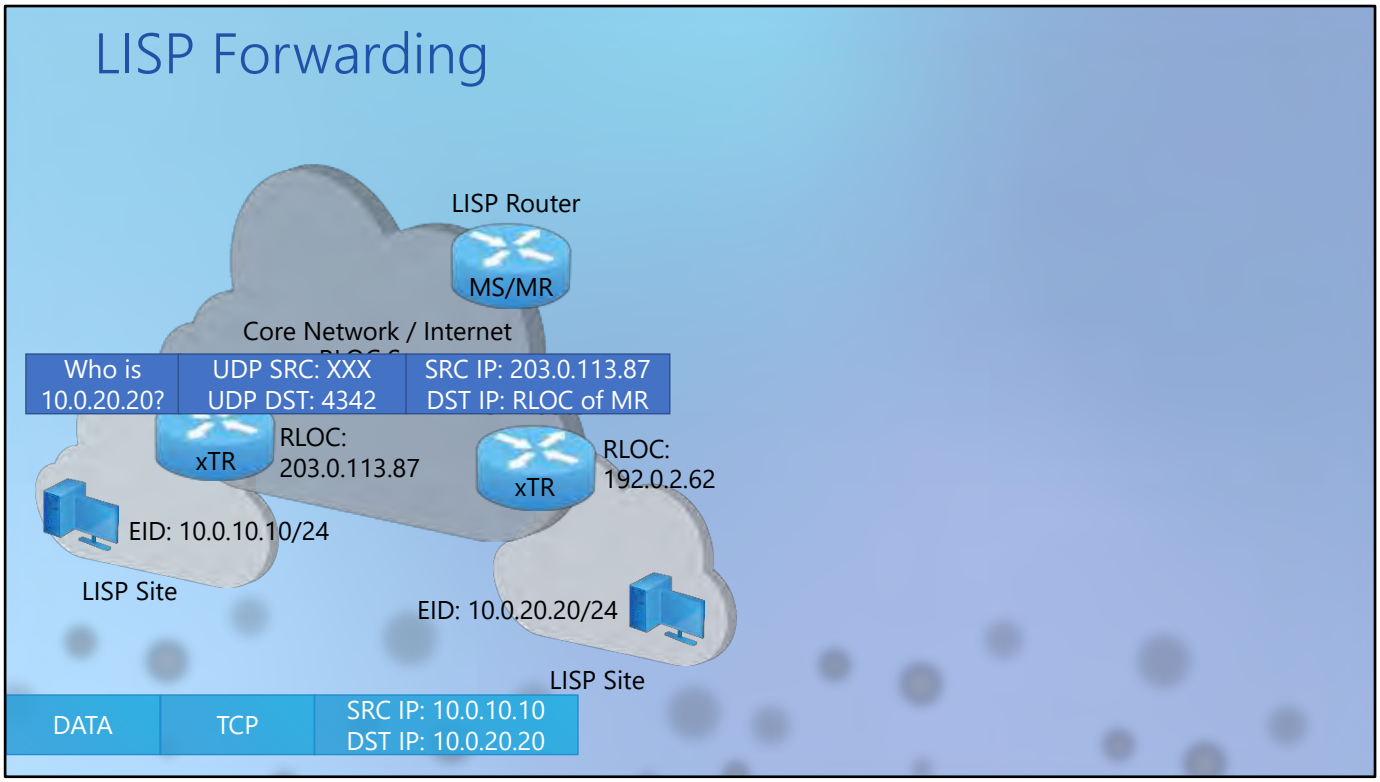
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



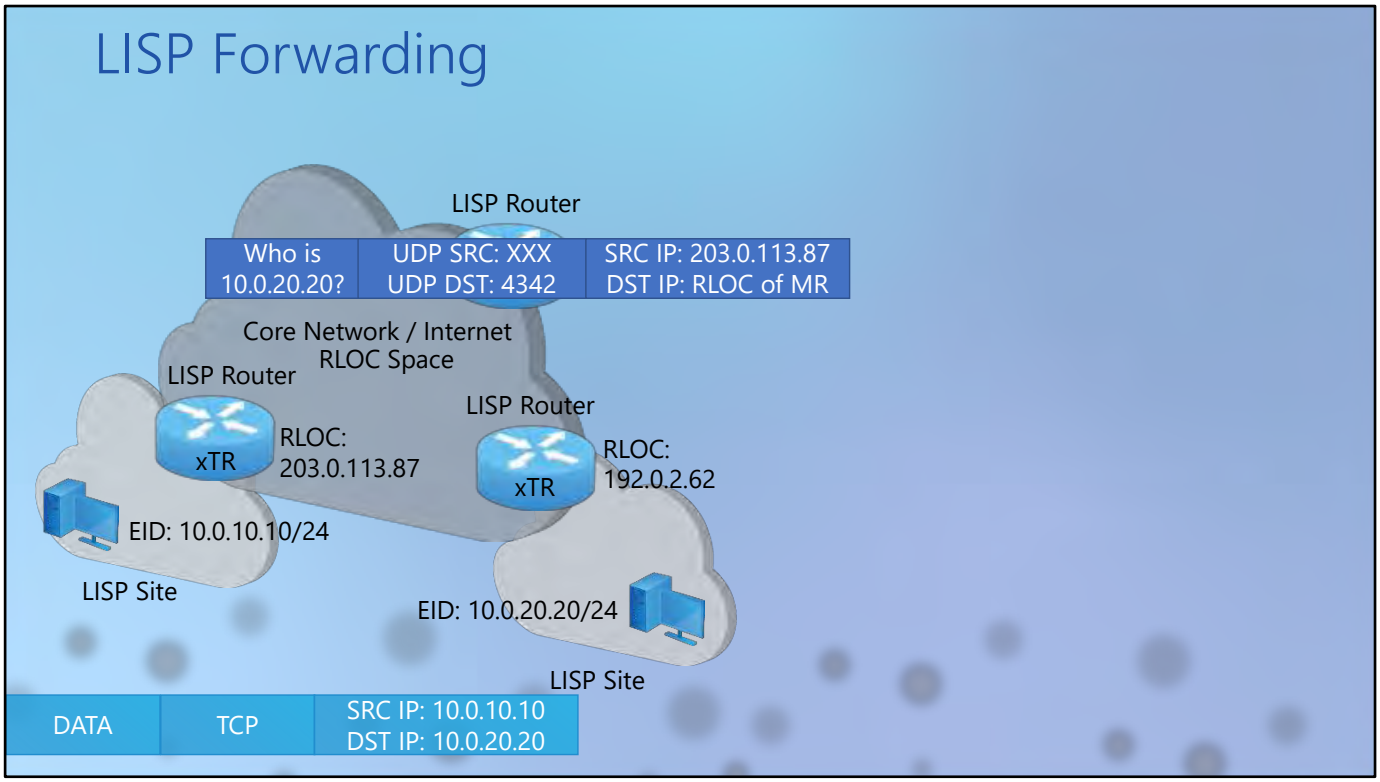
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



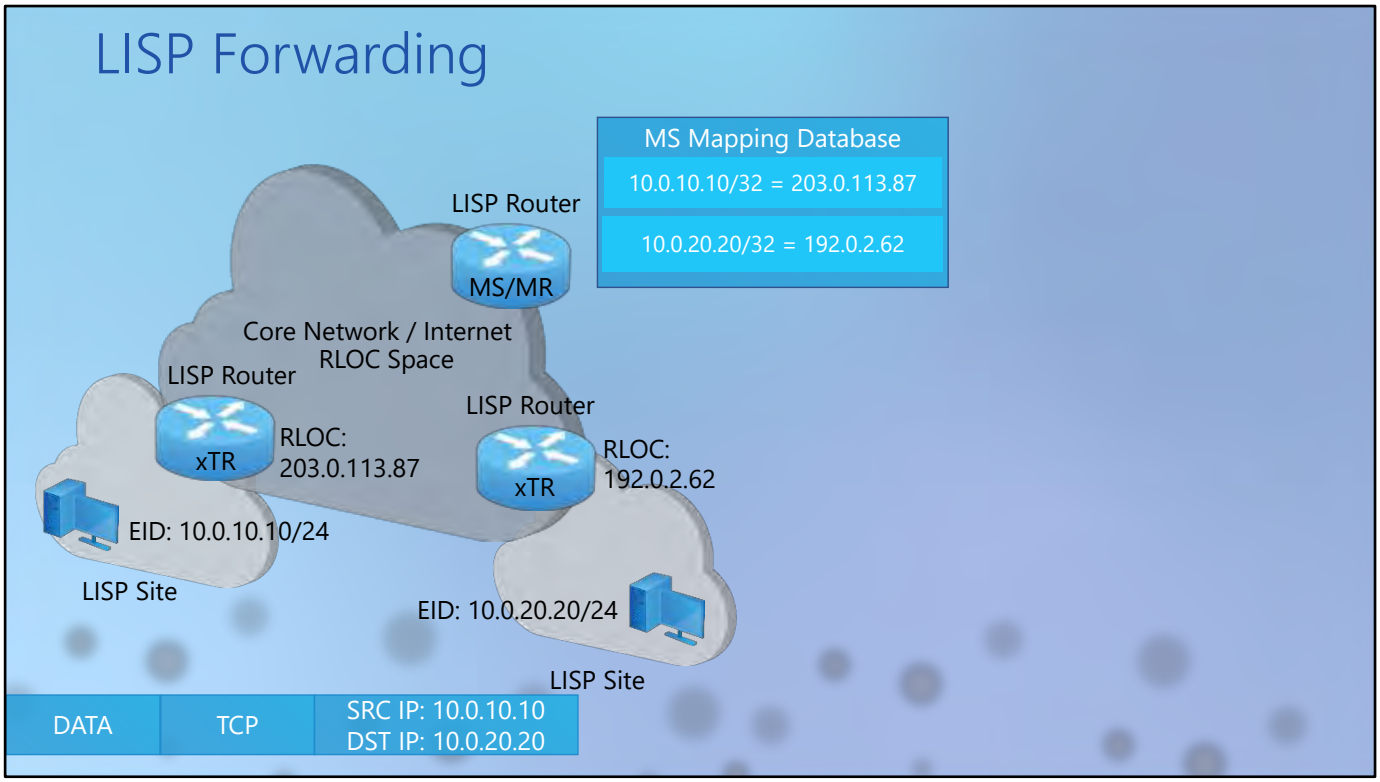
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



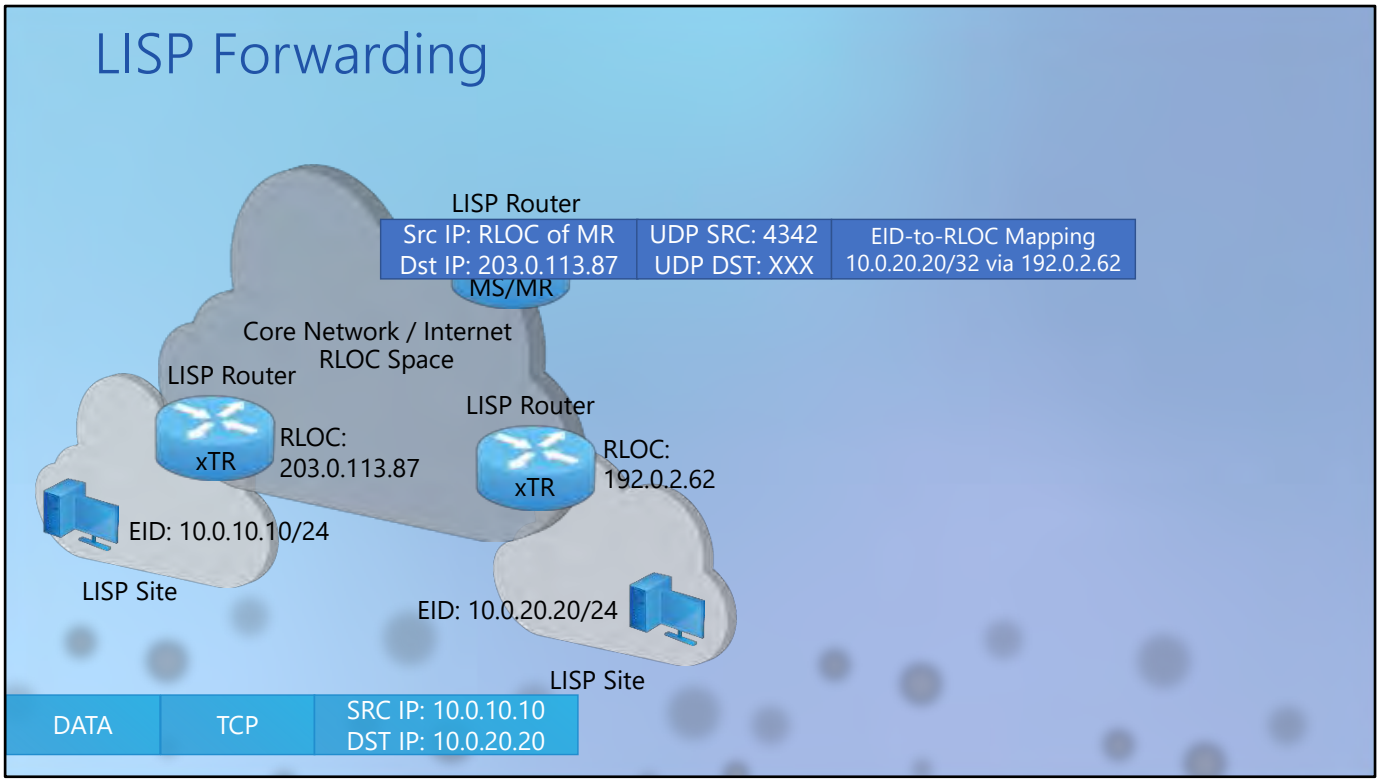
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



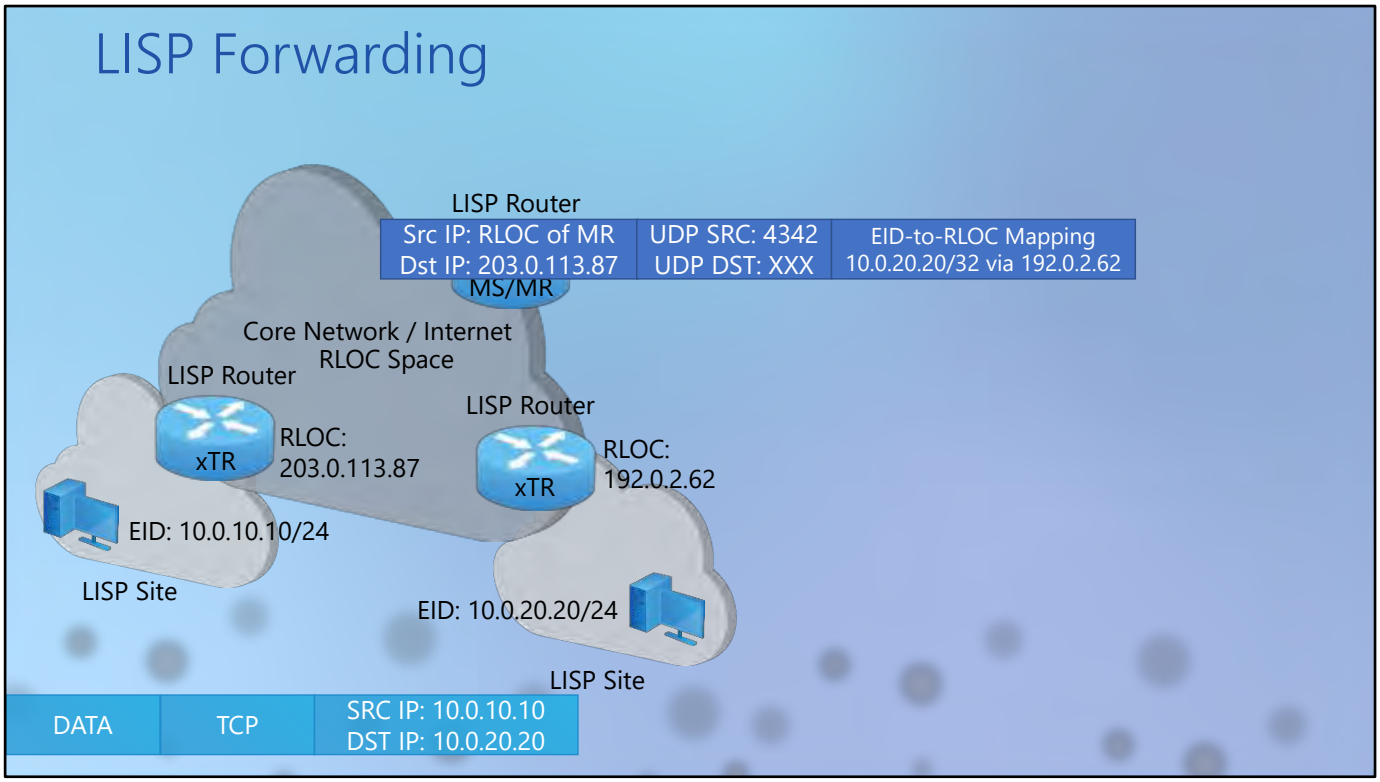
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



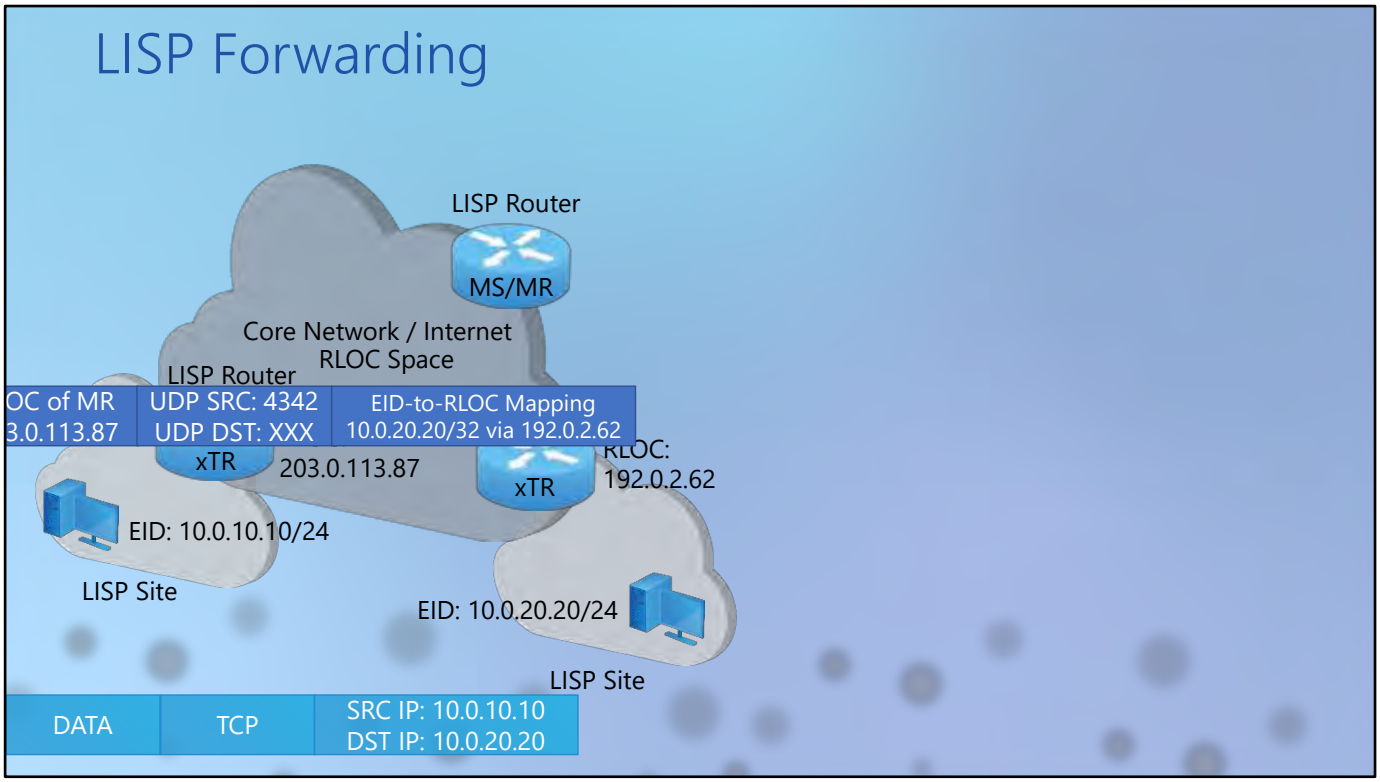
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



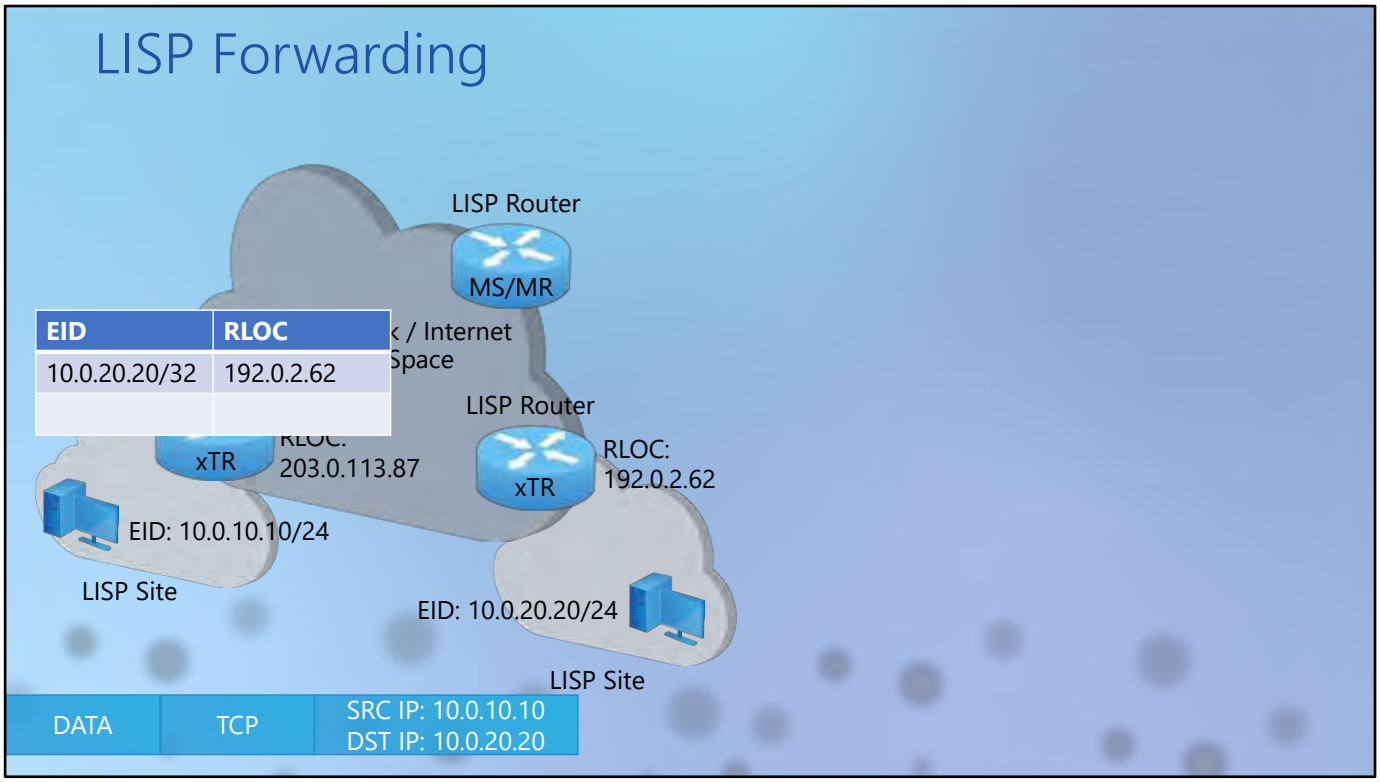
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



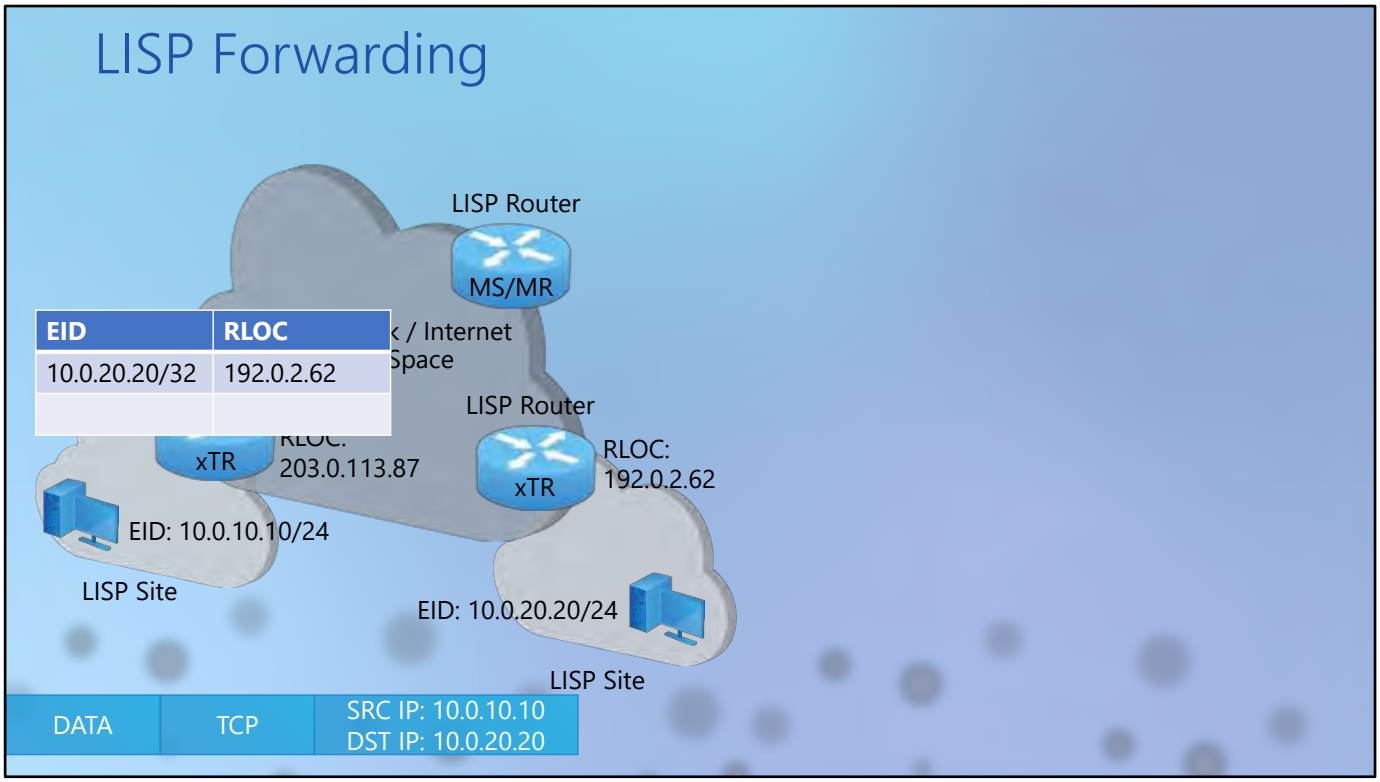
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



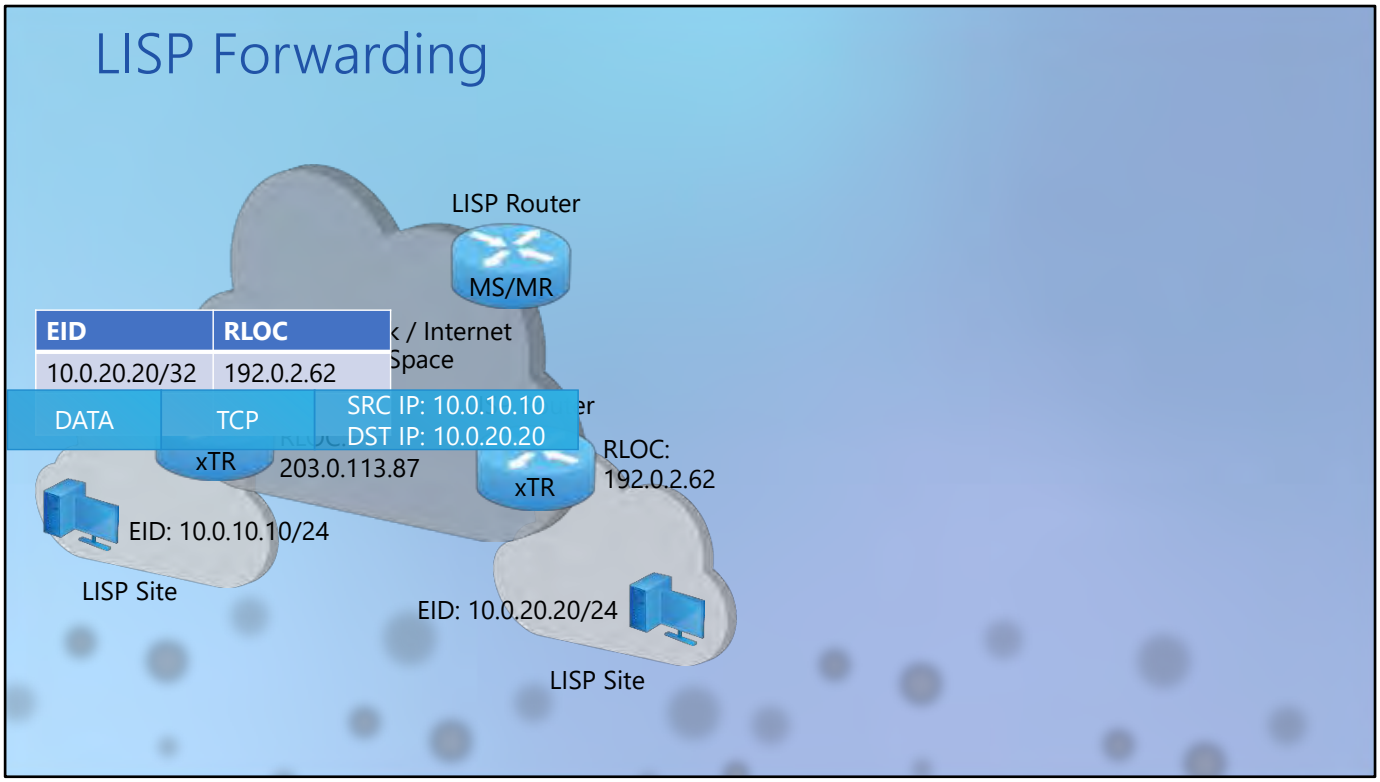
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



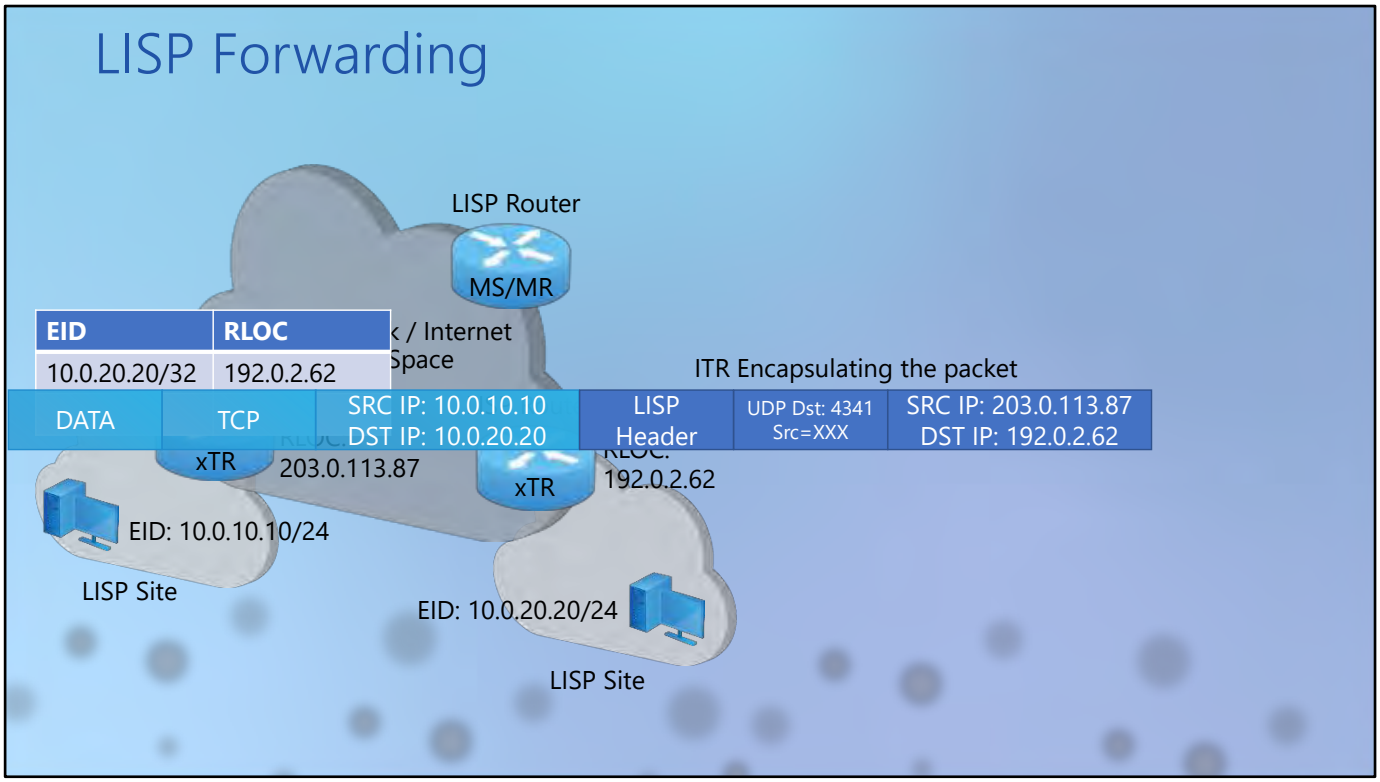
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



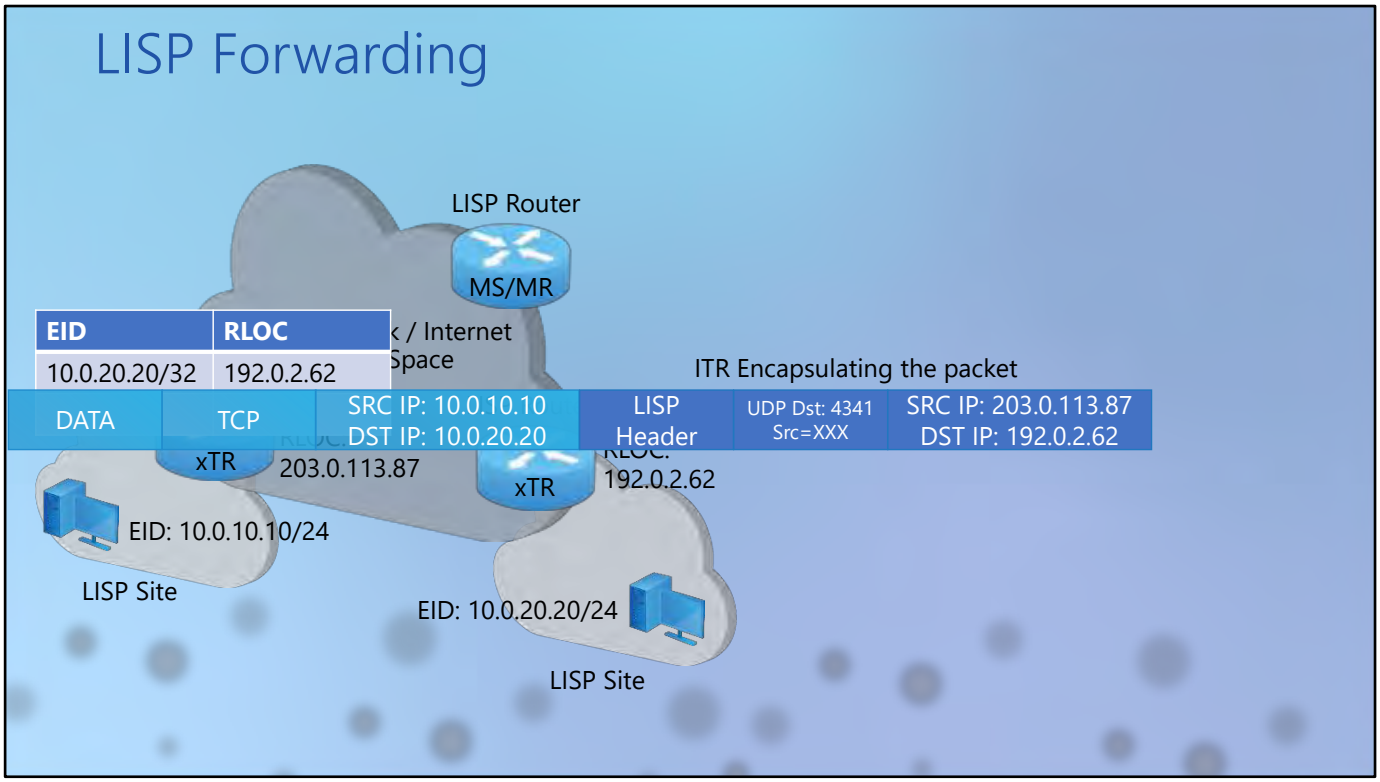
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

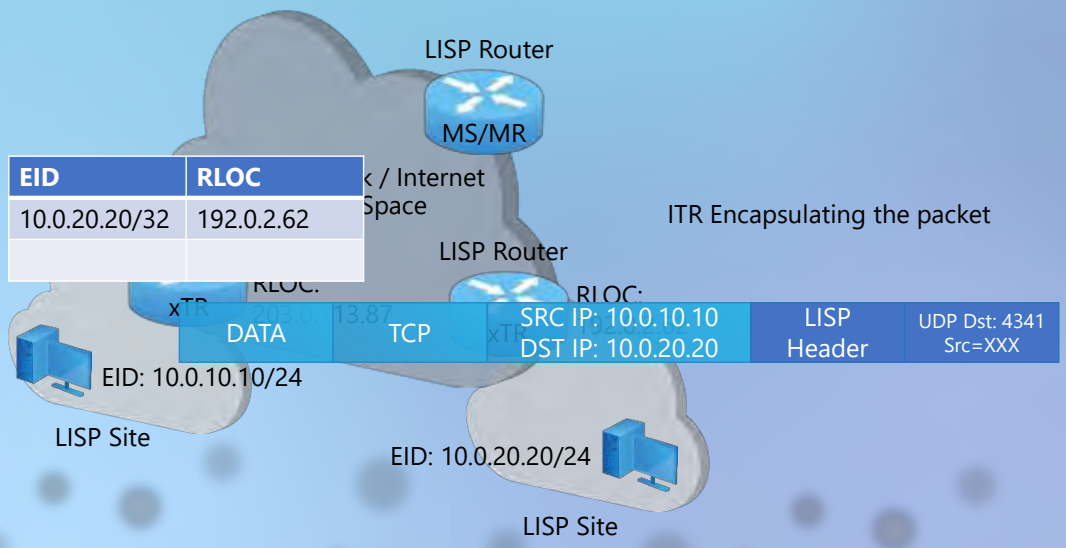


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

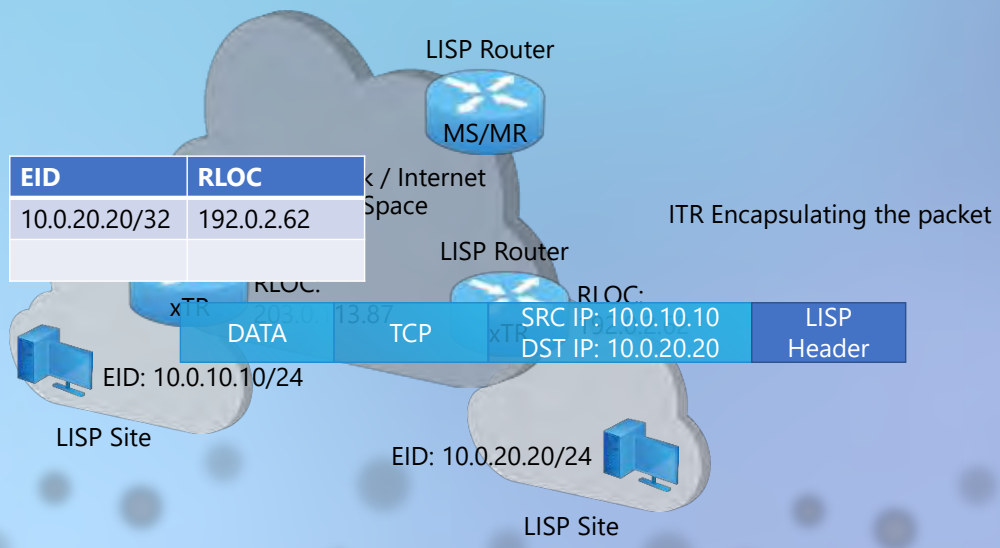
LISP Forwarding



EID	RLOC
10.0.20.20/32	192.0.2.62

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

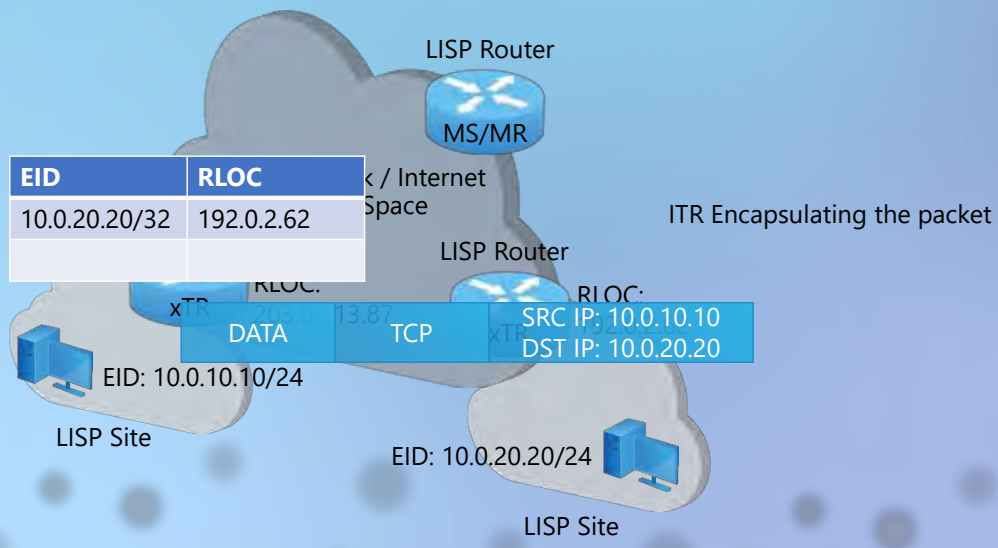
LISP Forwarding



EID	RLOC
10.0.20.20/32	192.0.2.62

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

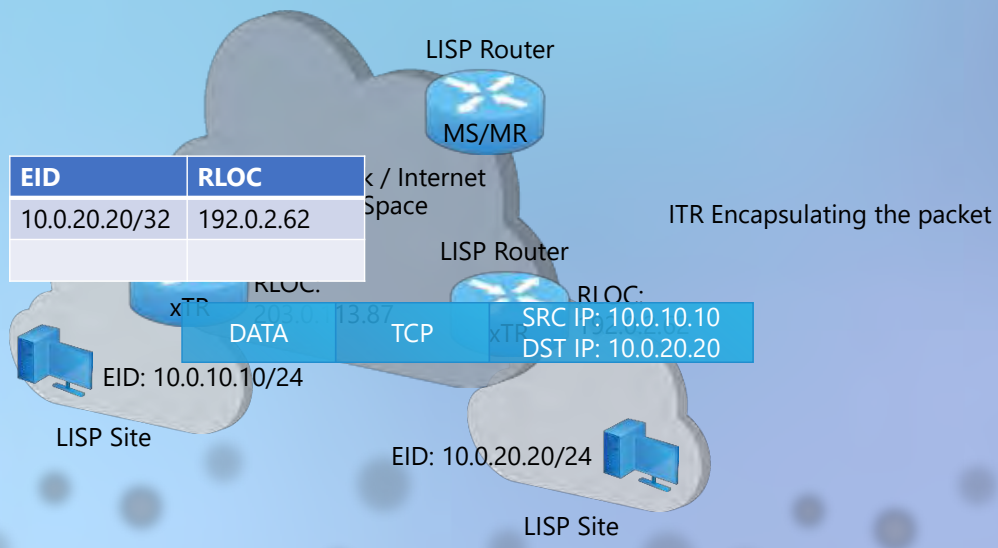
LISP Forwarding



EID	RLOC
10.0.20.20/32	192.0.2.62

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

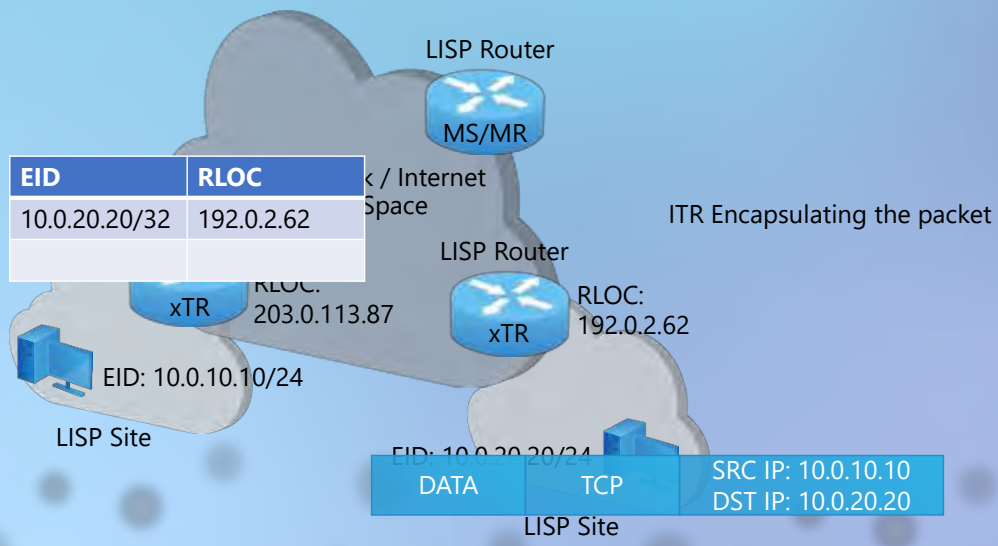
LISP Forwarding



EID	RLOC
10.0.20.20/32	192.0.2.62

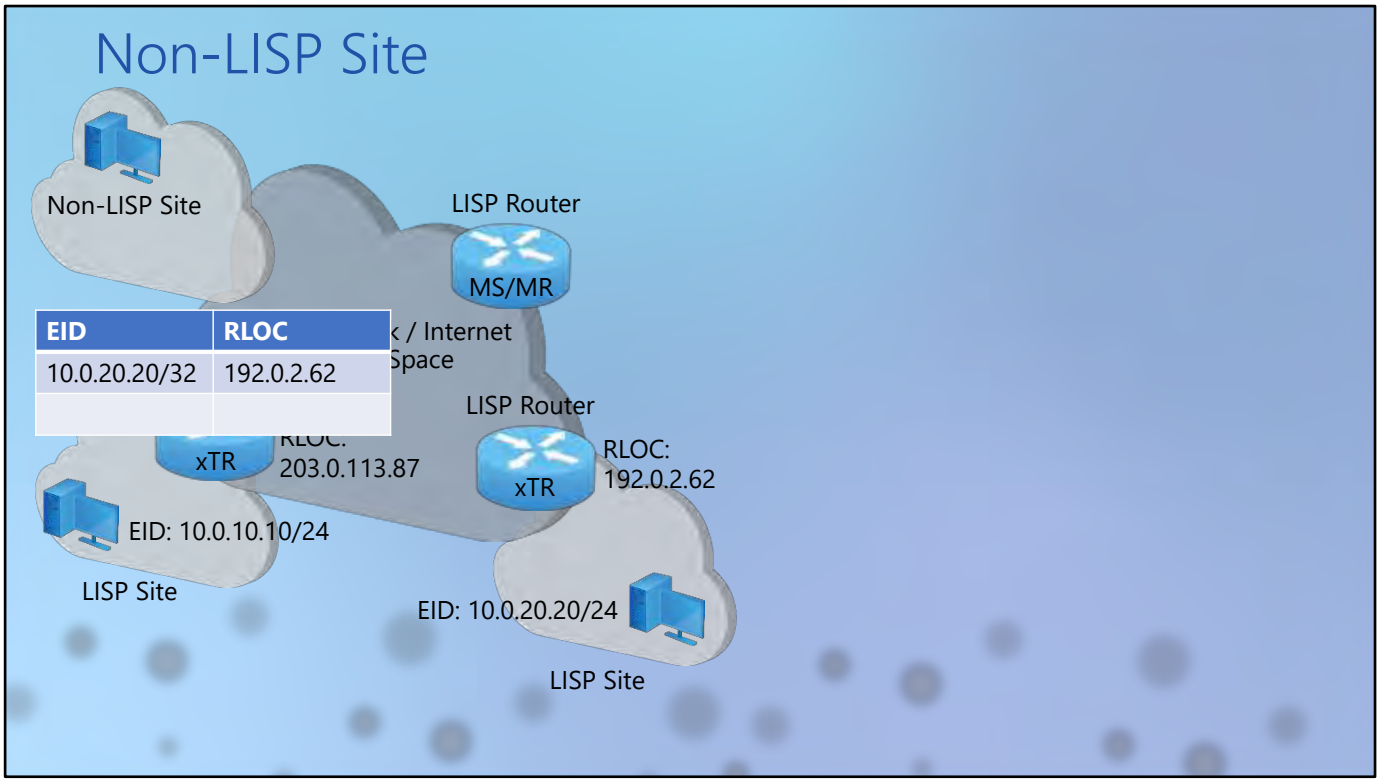
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

LISP Forwarding

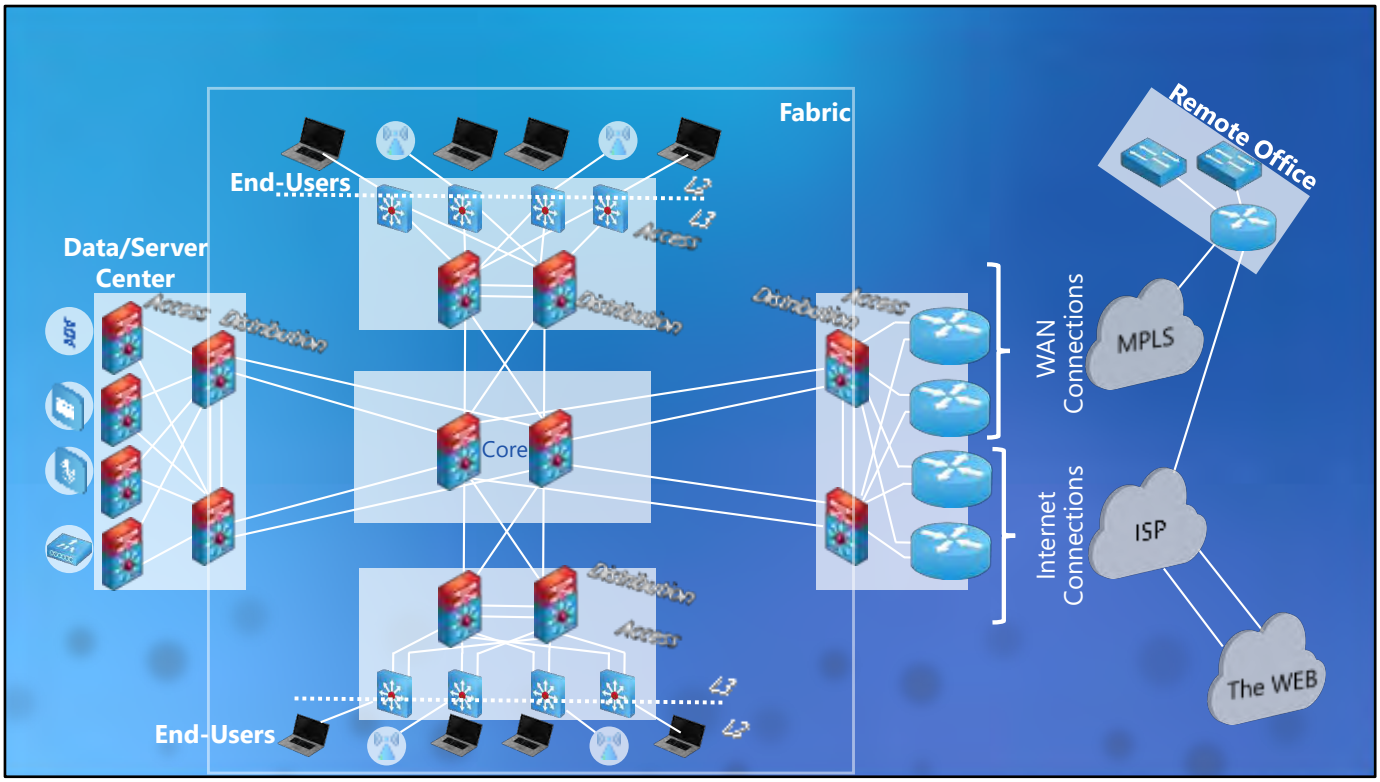


EID	RLOC
10.0.20.20/32	192.0.2.62

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

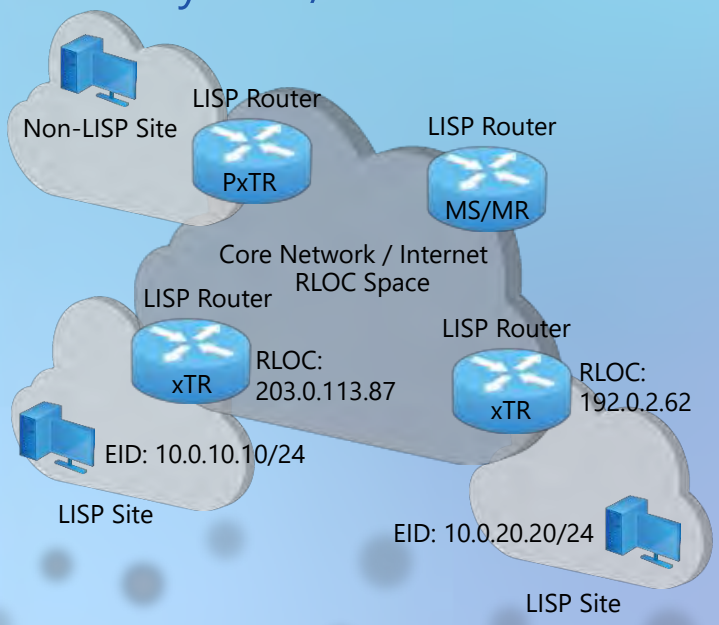


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

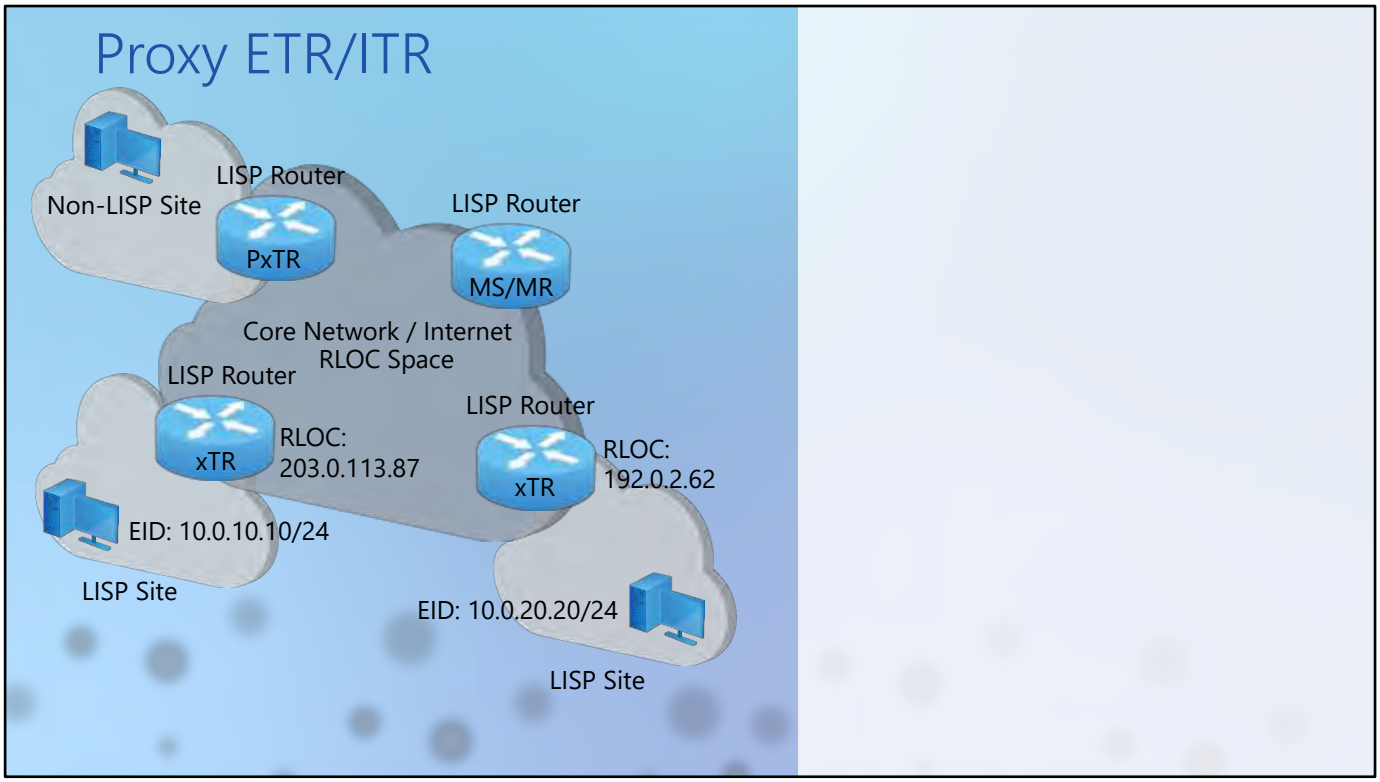
Proxy ETR/ITR



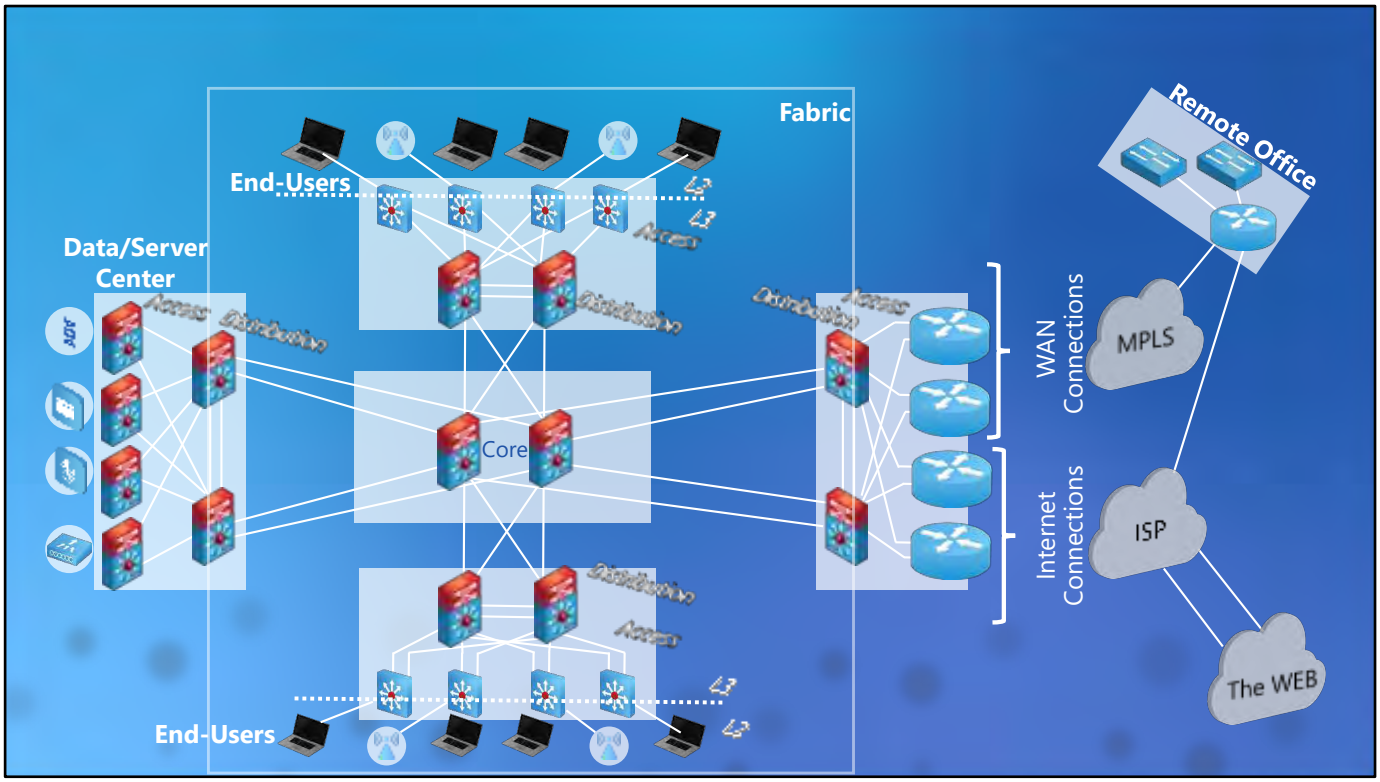
PxTR - Router connected to non-LISP sites

- PETR
  - Receives traffic from LISP sites
- PITR
  - Sends traffic to LISP sites

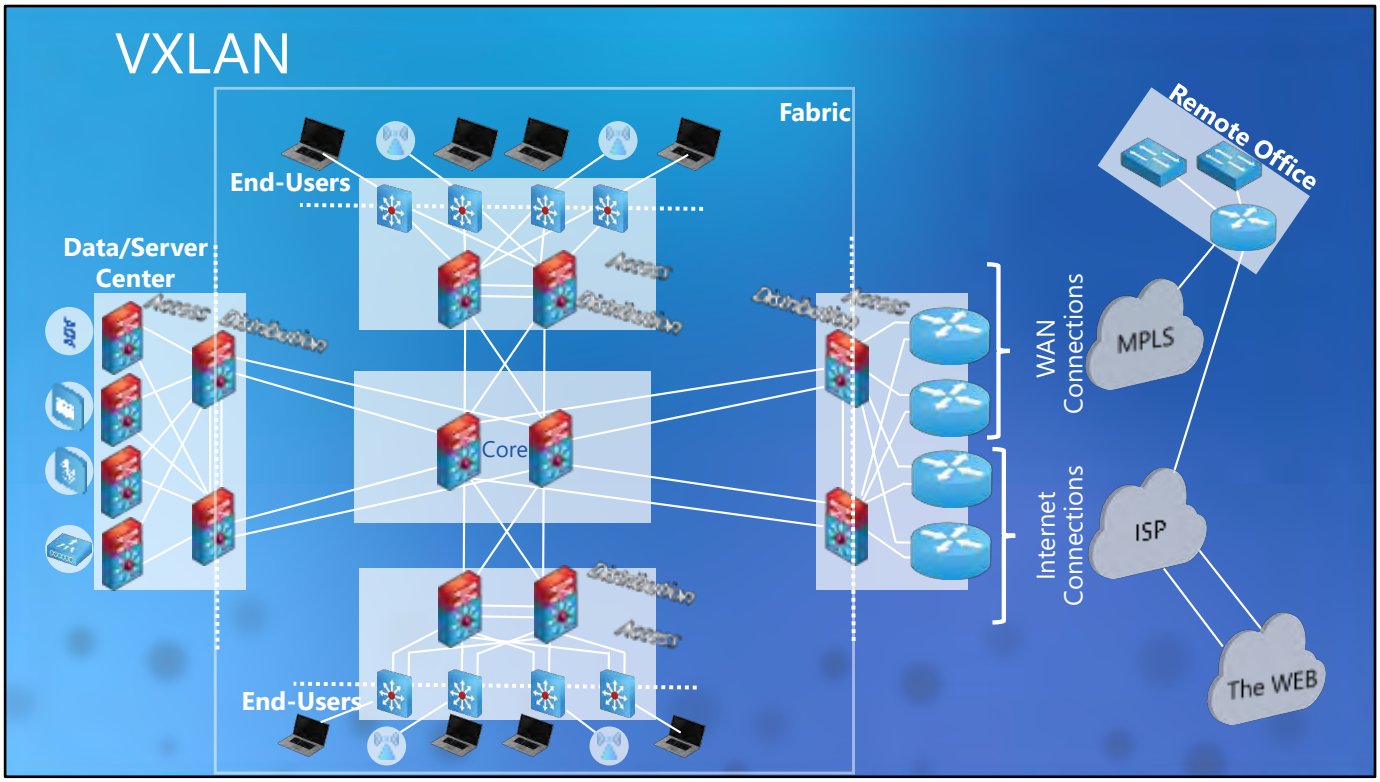
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

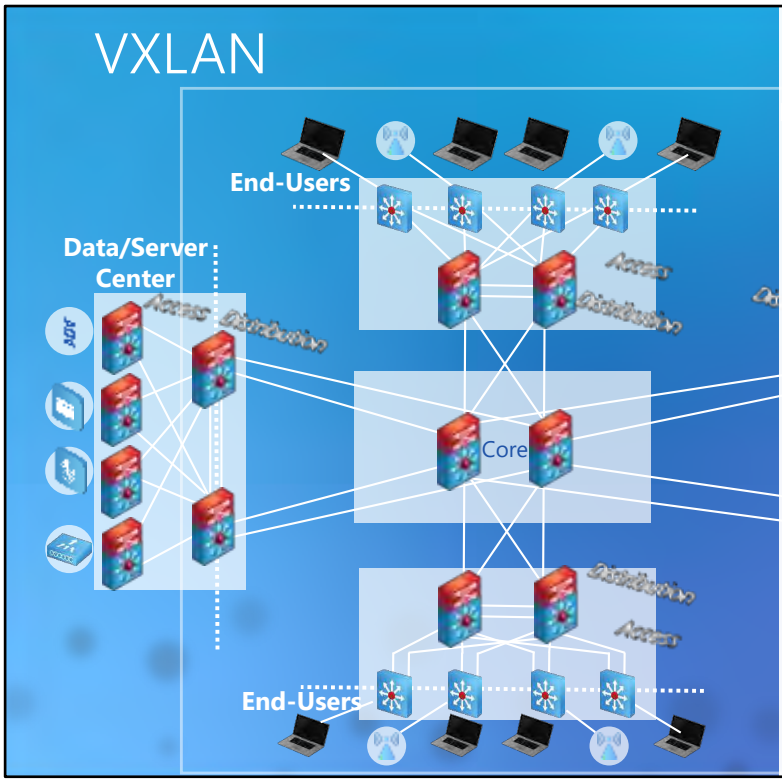


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VXLAN



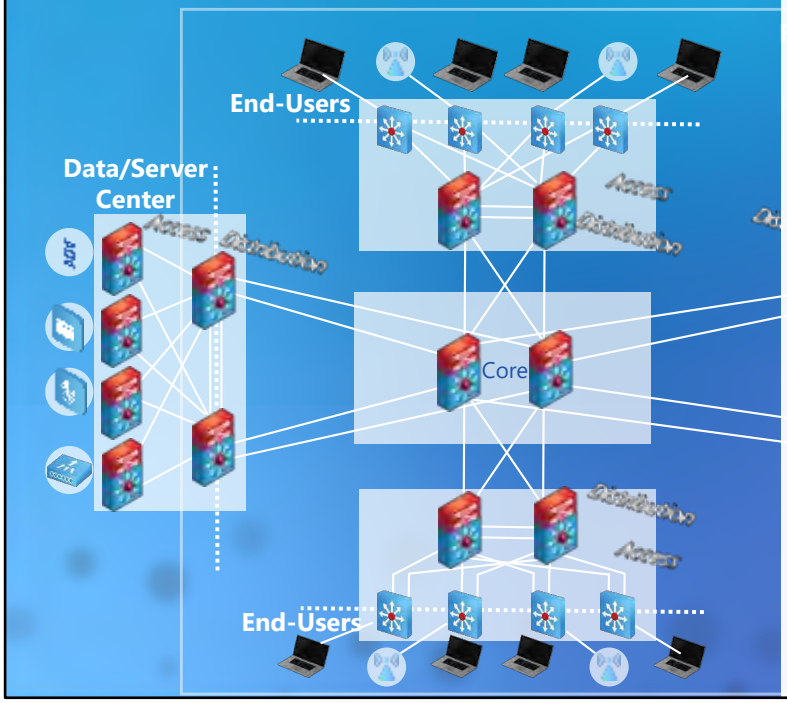
Build/Extend a Layer 2 network over a Layer 3 network.

While preserving the L2 header information.

It is an Overlay.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VXLAN vs VLAN



Scalability

16million VLANs vs 4000ish VLANs

VNI = VXLAN network identifier

Elasticity

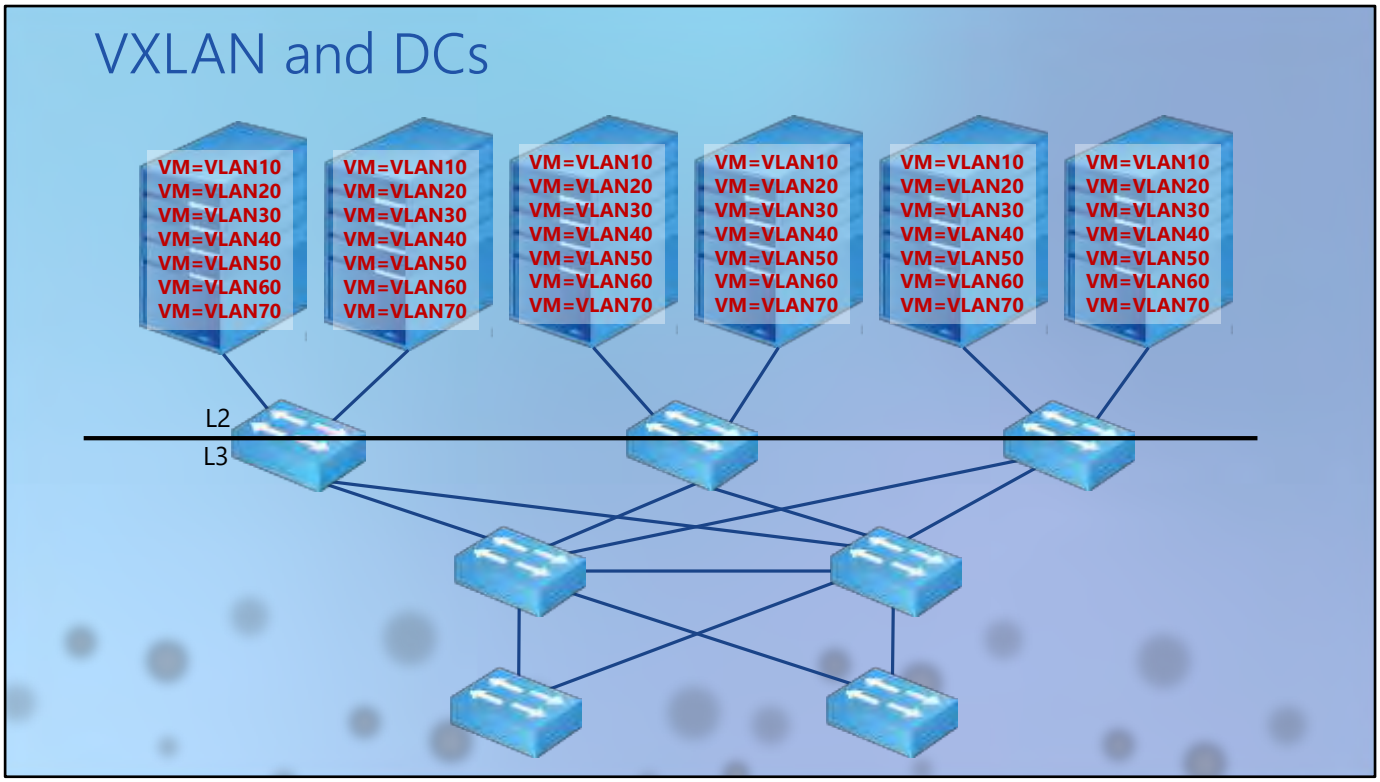
Provides L2 adjacencies across router boundaries

ECMP

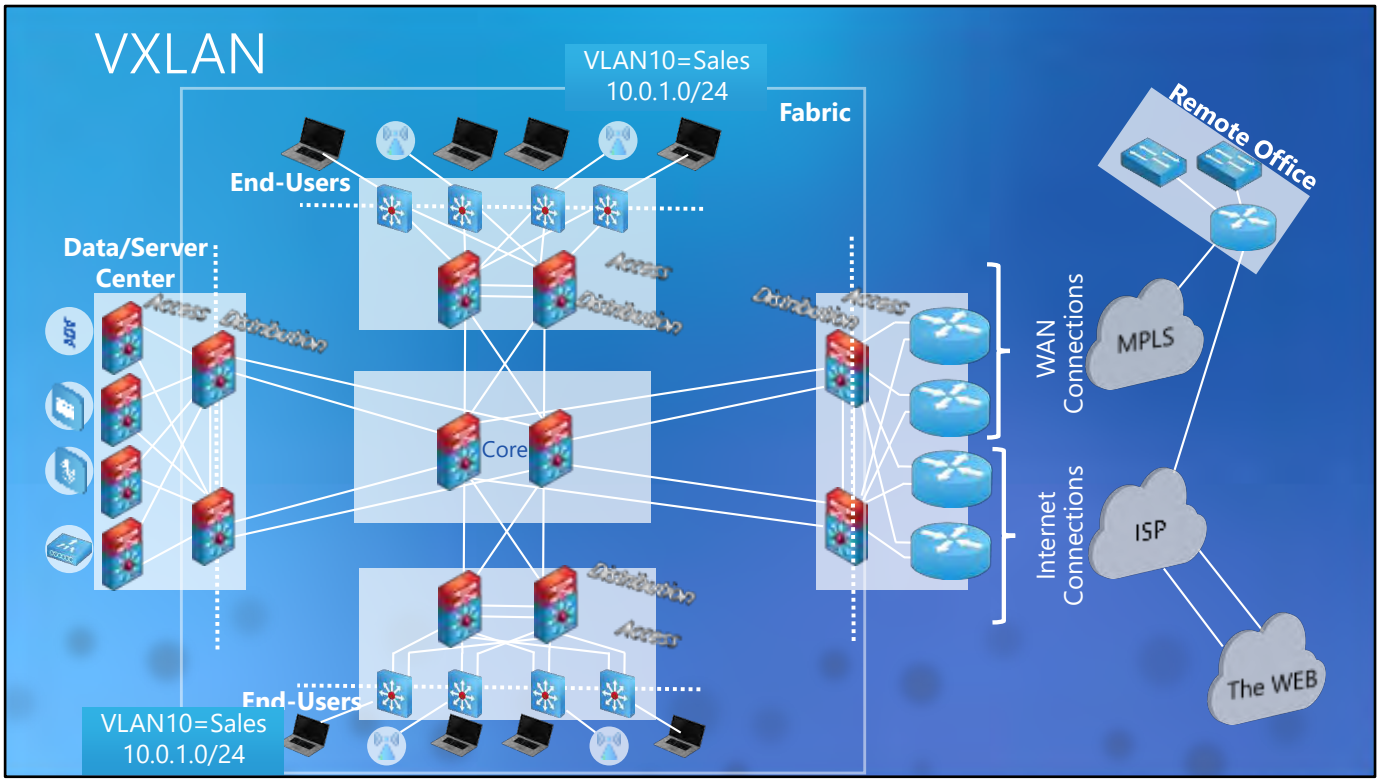
Provides load balancing on the transport network

©2023 by StormWind LLC. All rights reserved.

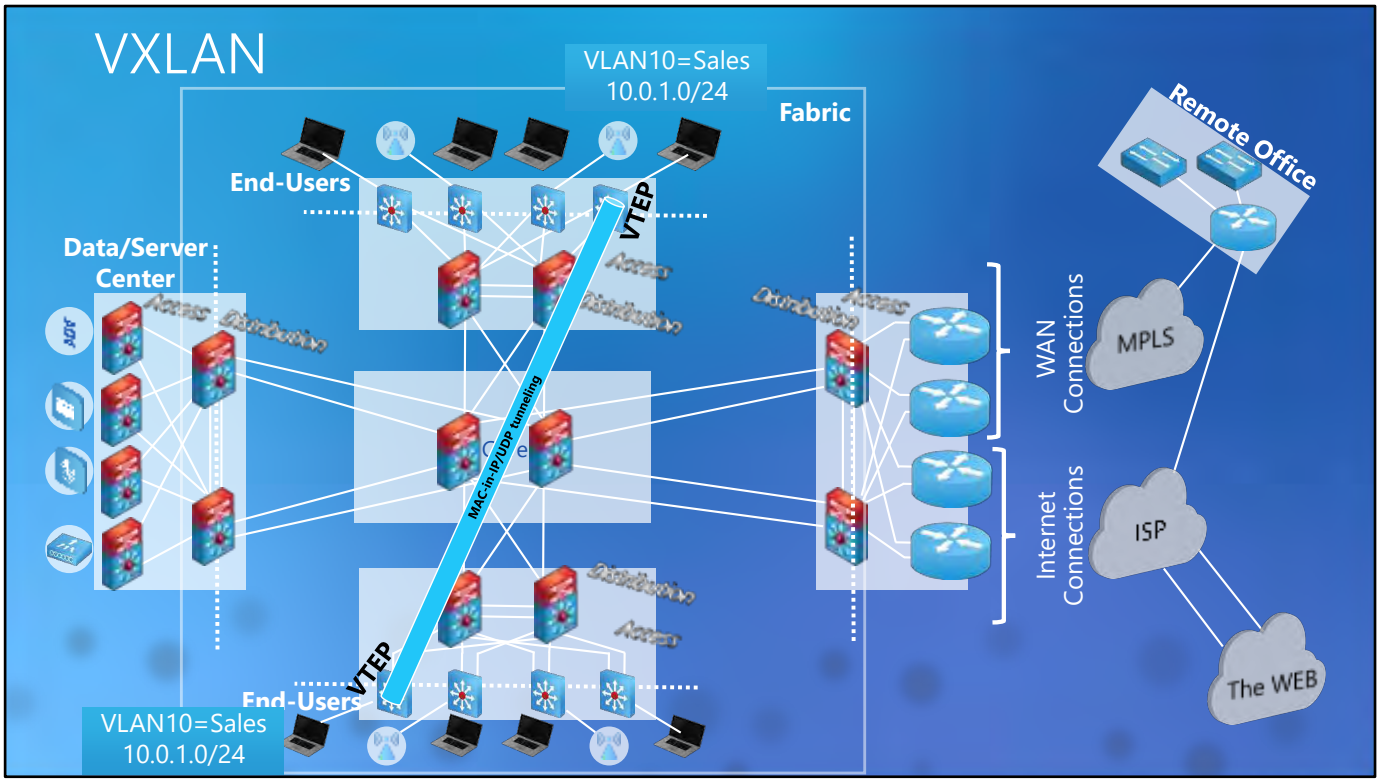
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

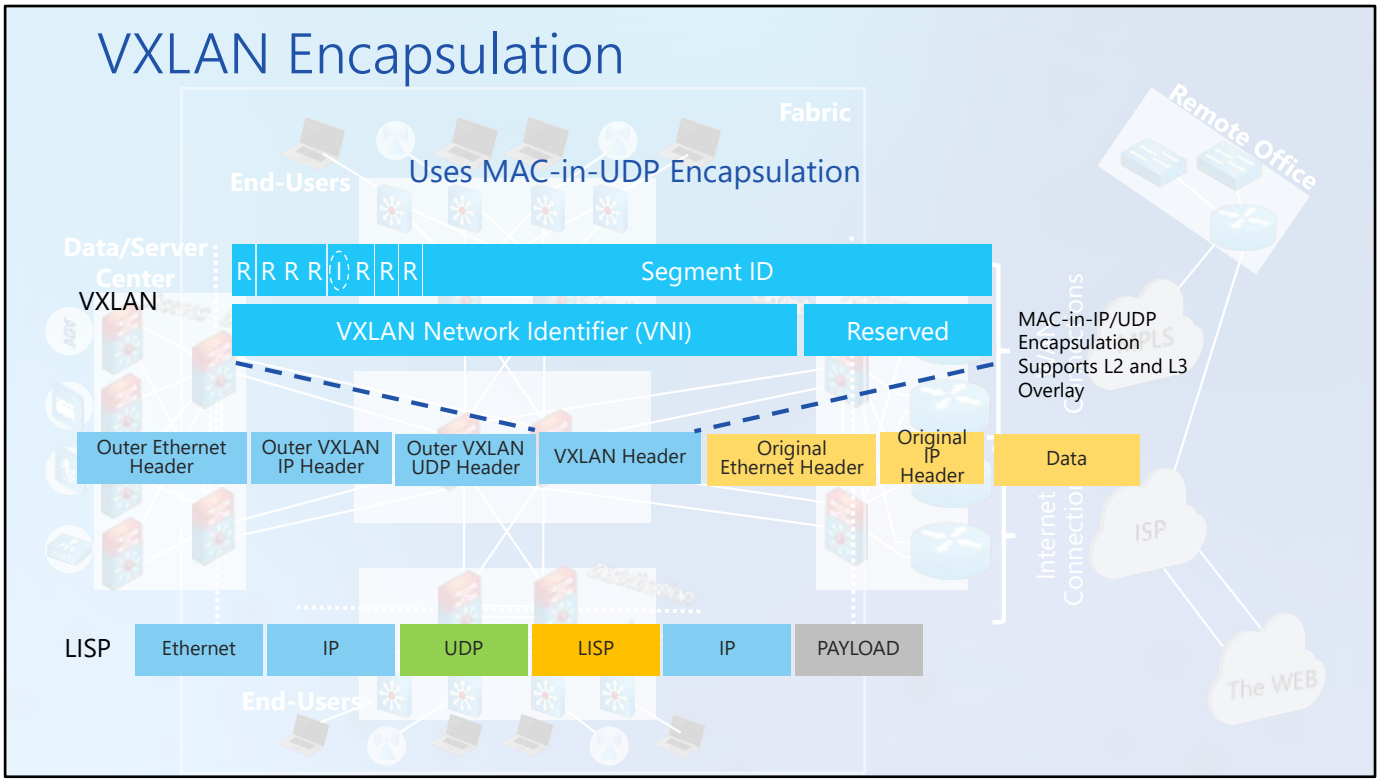


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

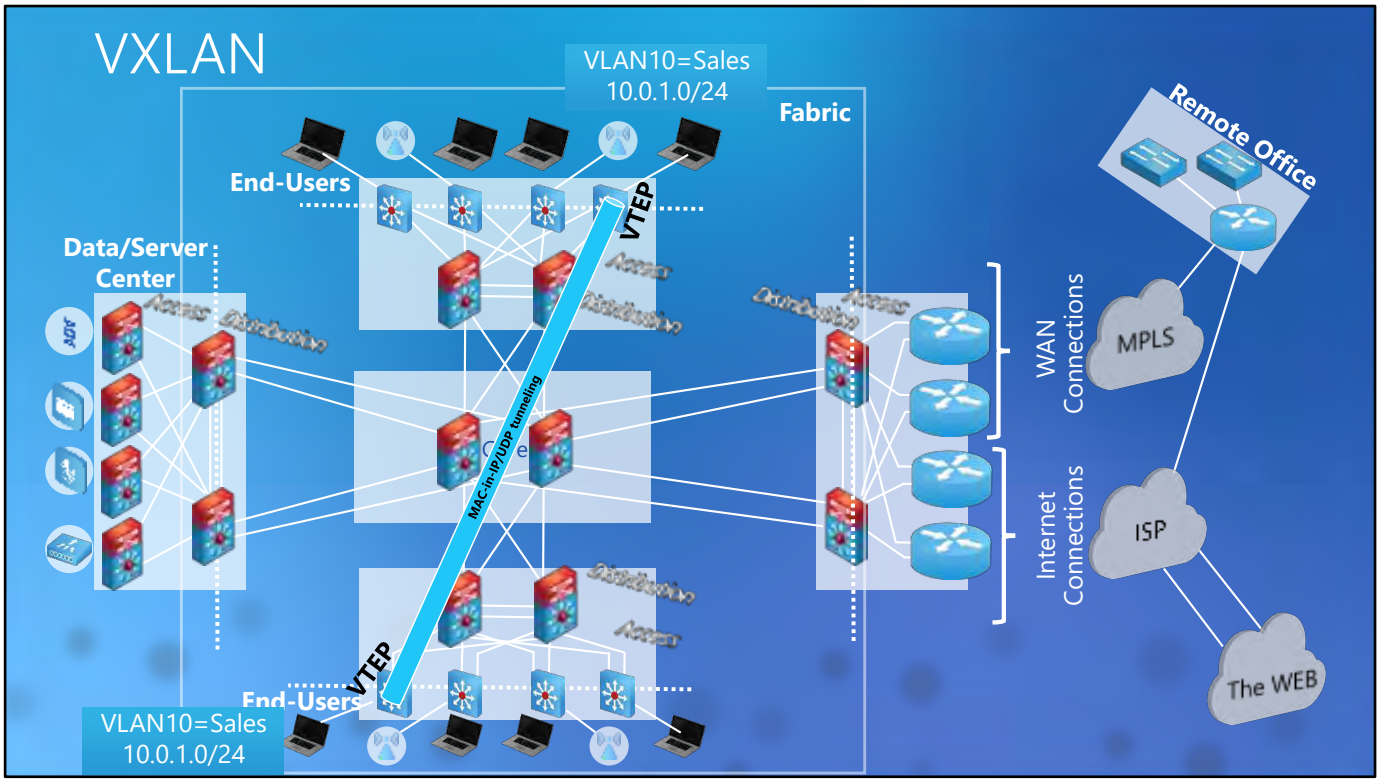


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VXLAN Encapsulation

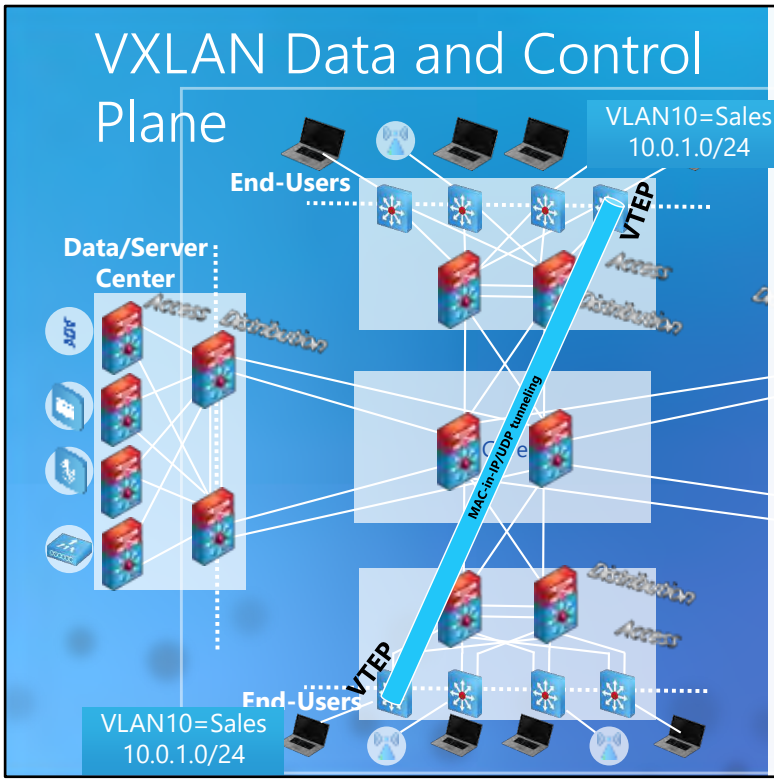


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VXLAN Data and Control Plane



VXLAN only defines the Data Plane

- The actual forwarding of the frames from tunnel source to destination

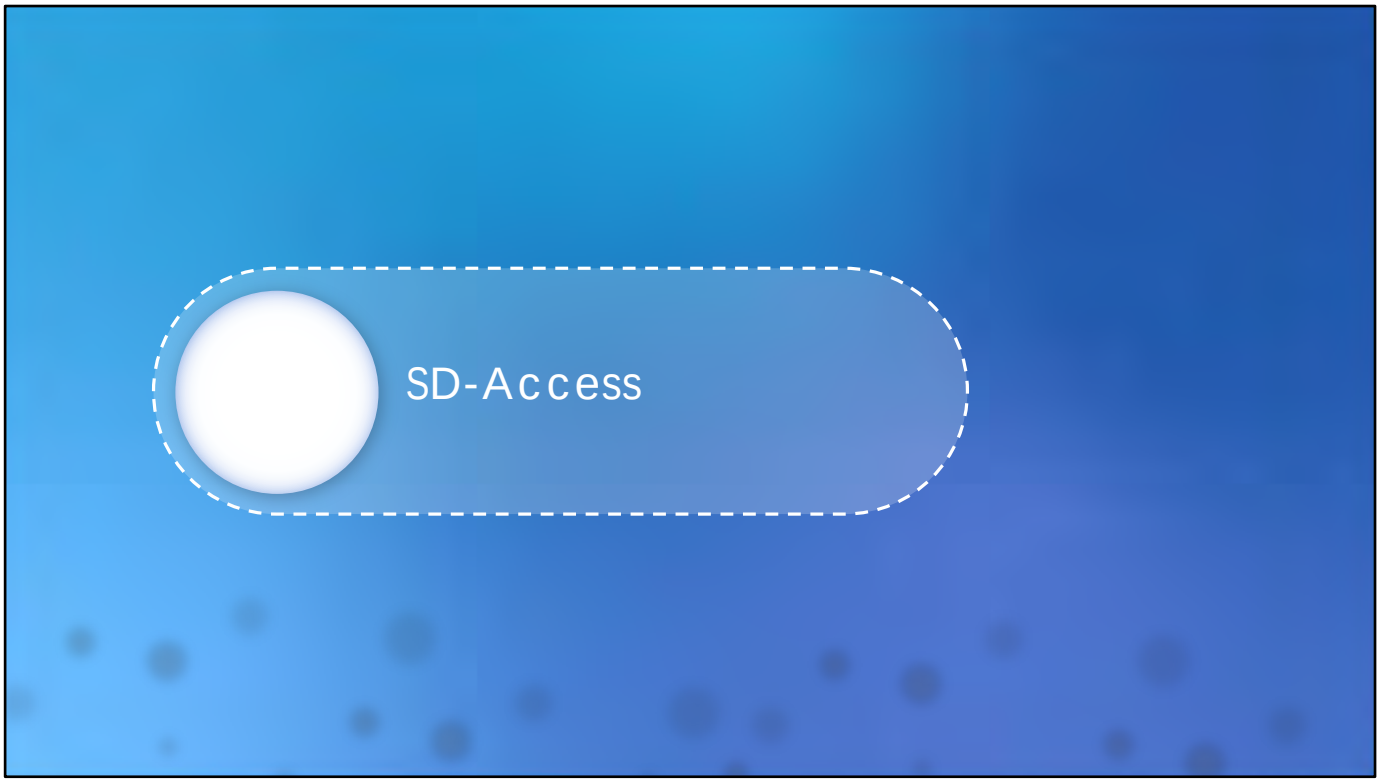
Various Control Plane options exist

- Multicast underlay*
- static unicast
- MP-BGP EVPN*
- LISP**

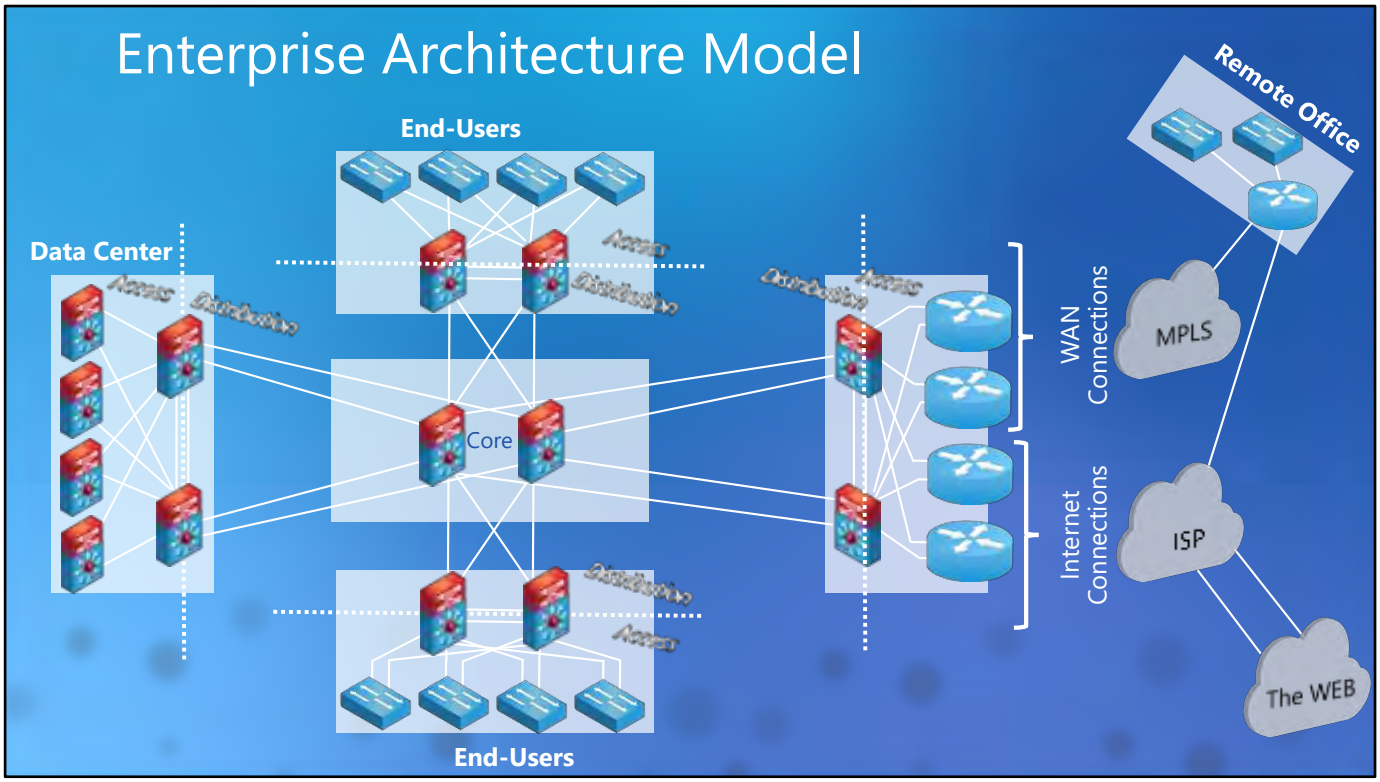
* Popular options for data center and cloud

** Popular with campus environments

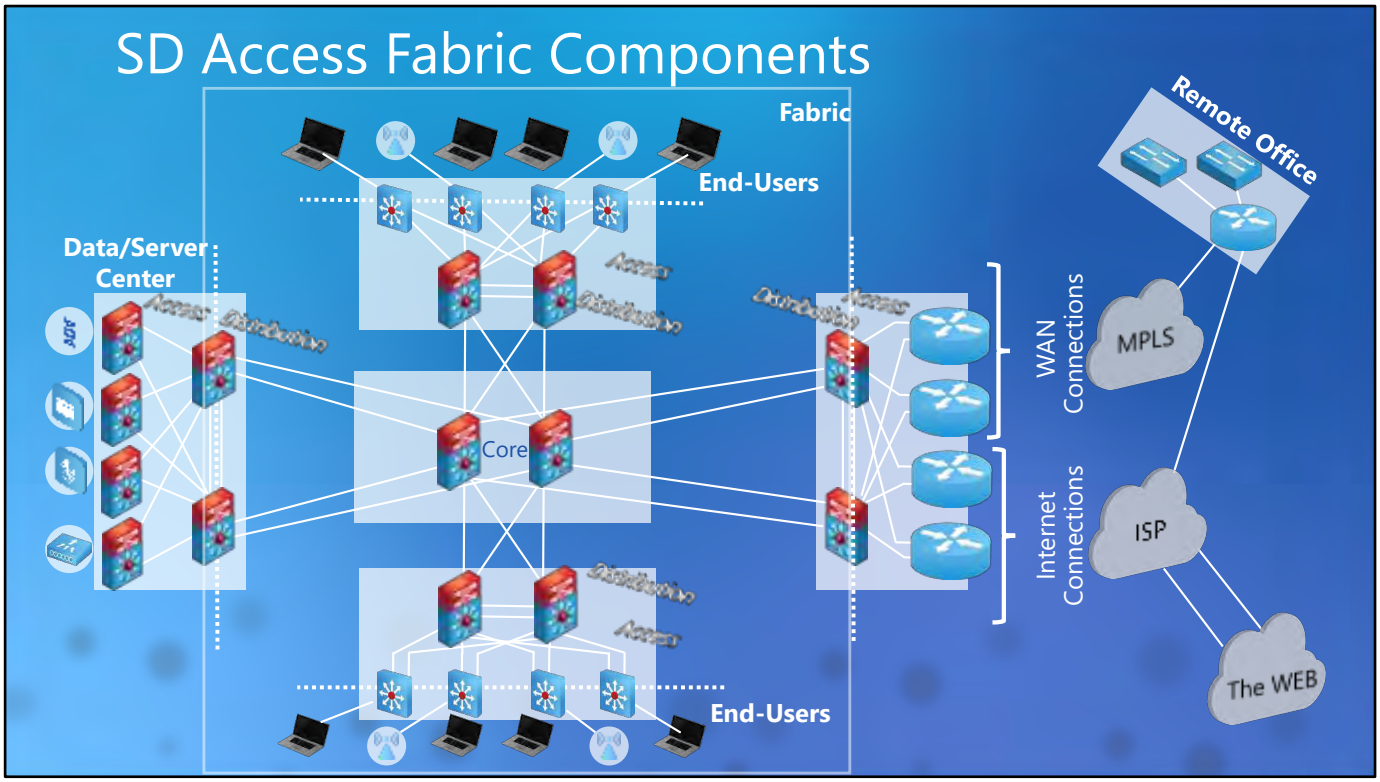
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SD Access Layers

Underlay

Overlay

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

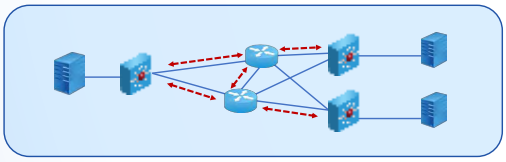
SD Access Layers

Underlay | **Overlay**

Dedicated to the physical devices and forwarding of traffic

Routers, Switches, WLC, Layer 3 routing protocols, etc

Simple, scalable and resilient foundation for communication between all devices



Underlay Network

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

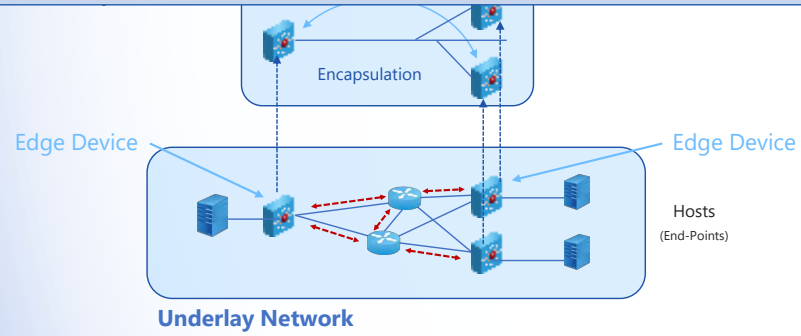
SD Access Layers

Underlay | **Overlay**

Logical, virtualized topology built on top of the physical underlay

Where wired and wireless users and devices are logically connected, and services and policies are applied

Known as the "**Fabric**"

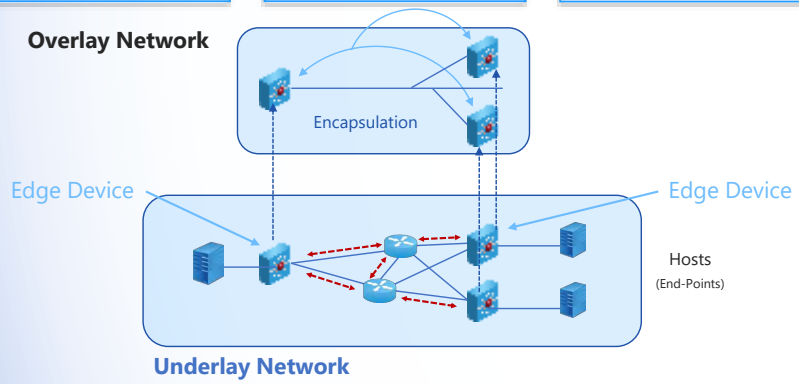


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SD Access Fabric

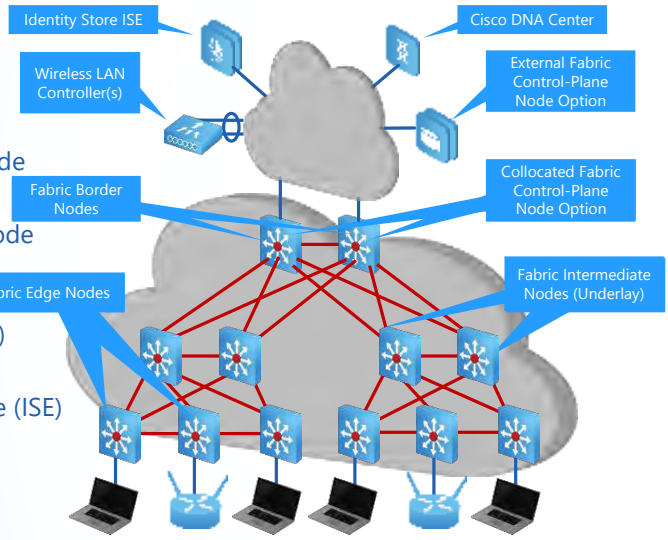
Fabric Data Plane	Fabric Control Plane	Fabric Policy Plane
Used for forwarding Created using **VXLAN with GPO** for encapsulating packets	Used for building the tables needed by the data plane mapping and resolving users and devices Created using **LISP**	SGT and group-based policies are used to translate the business intent into the network policy **TrustSec**



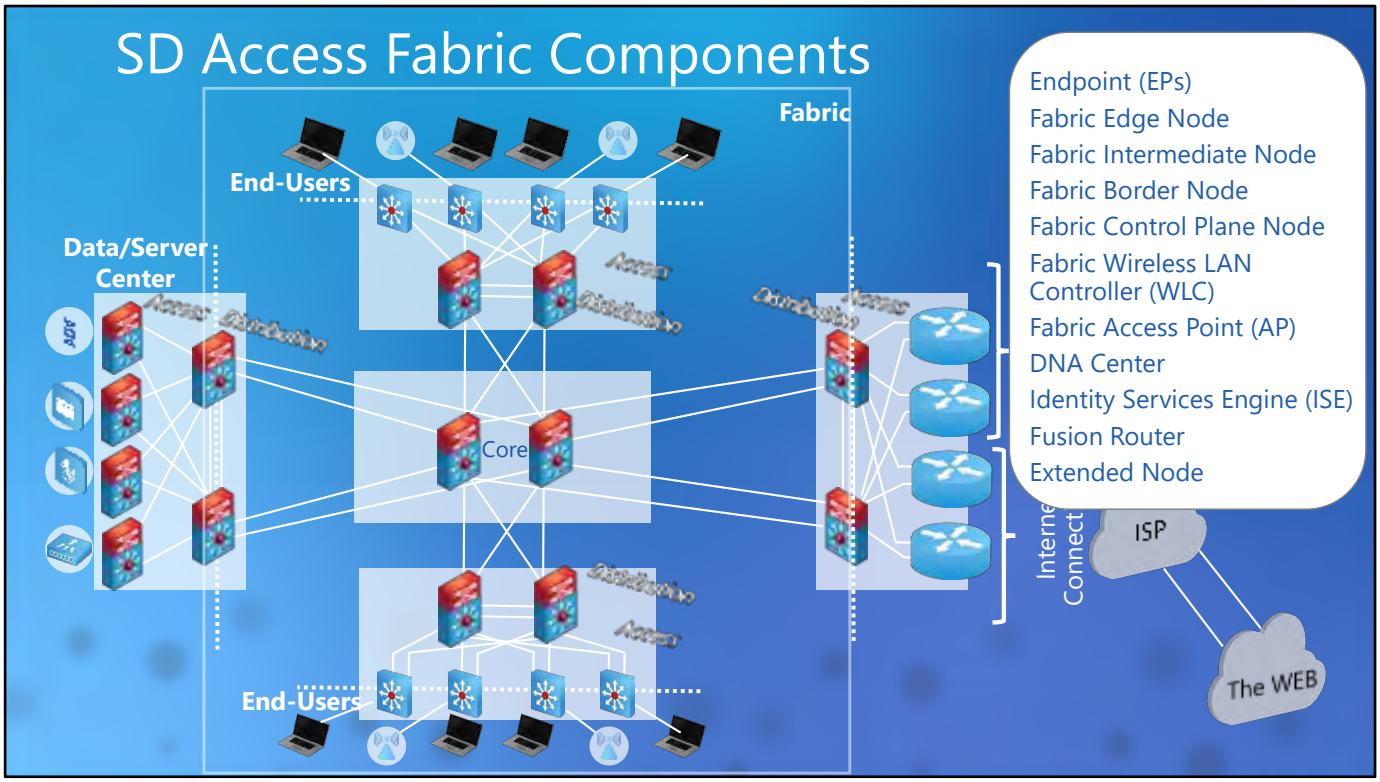
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SD Access Fabric Components

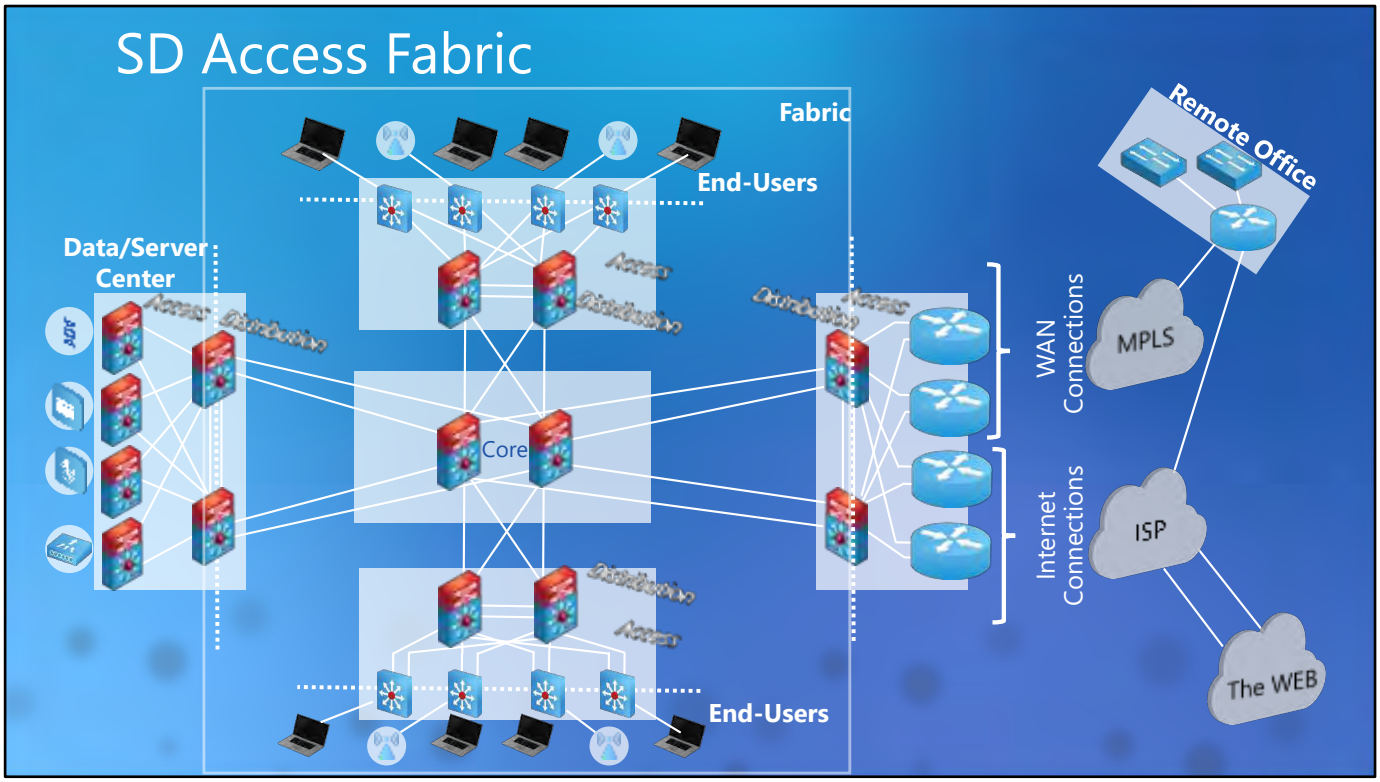
- Endpoint (EPs)
- Fabric Edge Node
- Fabric Intermediate Node
- Fabric Border Node
- Fabric Control Plane Node
- Fabric Wireless LAN Controller (WLC)
- Fabric Access Point (AP)
- DNA Center
- Identity Services Engine (ISE)
- Fusion Router
- Extended Node



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

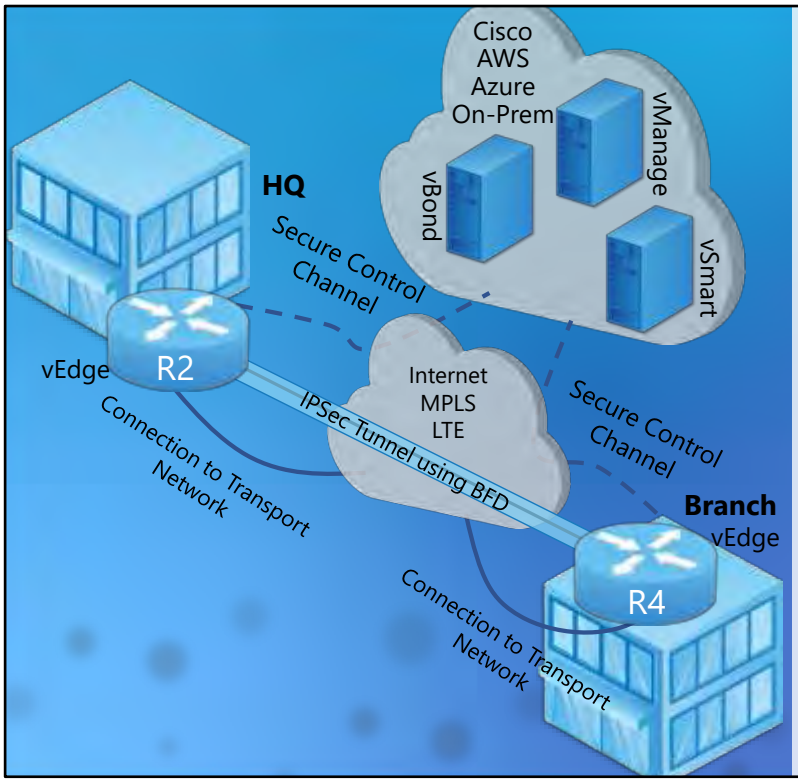


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



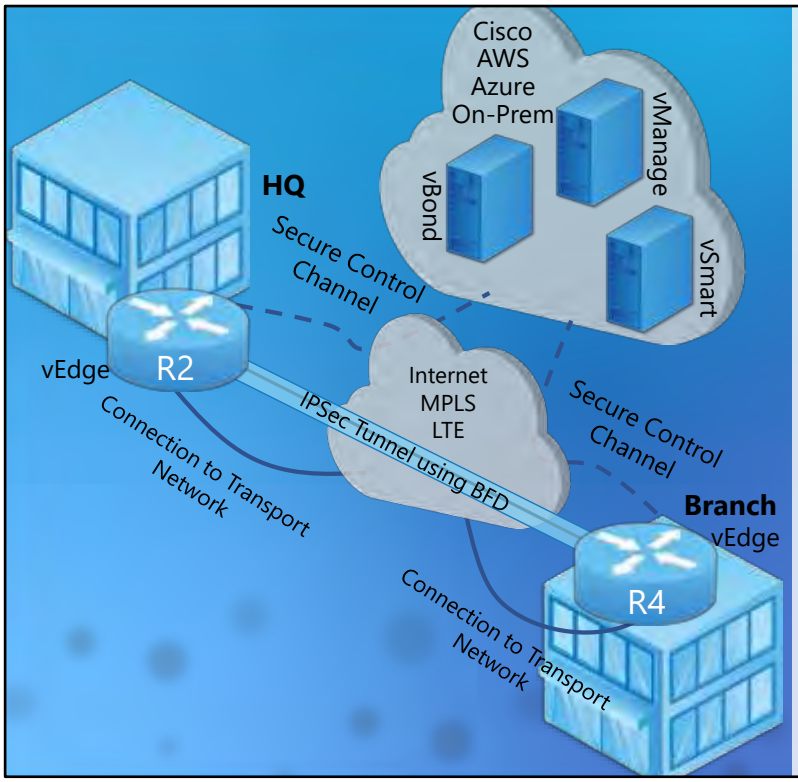
SD-WAN

Software-Defined Wide Area Network

A technology that utilizes software-defined networking principles to manage and optimize the distribution of network traffic across a wide area network (WAN).

It offers the ability to dynamically route and prioritize network traffic based on factors such as application type, network conditions, and business policies.

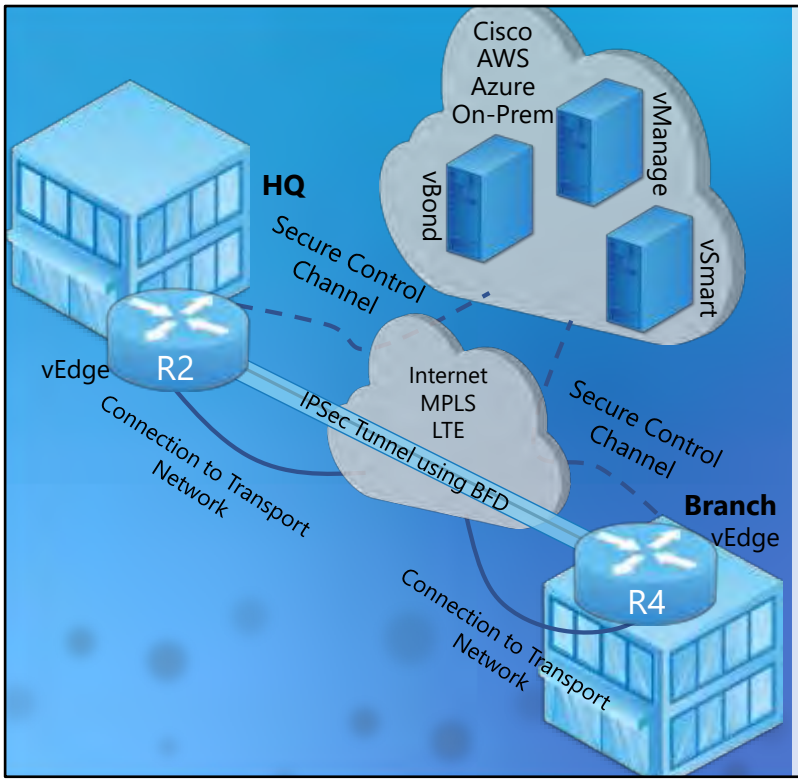
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Benefits of SD-WAN

- Improved Network Performance
- Shorter installation times
- Cost Savings
- Centralized Management
- Application-Aware Routing
- Flexibility and Agility
- Security Enhancement
- Redundancy and Failover
- Cloud Readiness

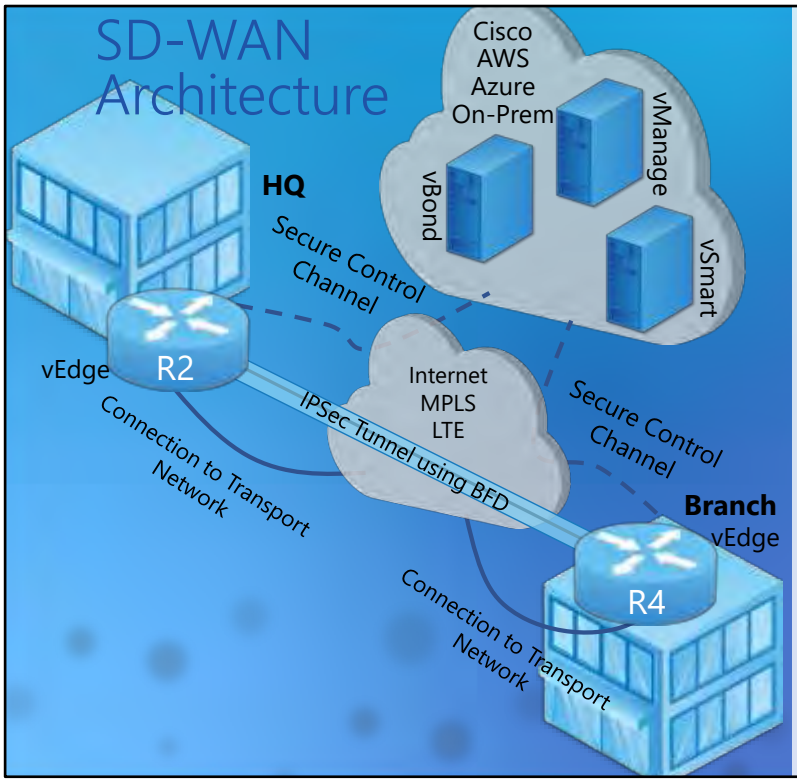
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Limitations of SD-WAN

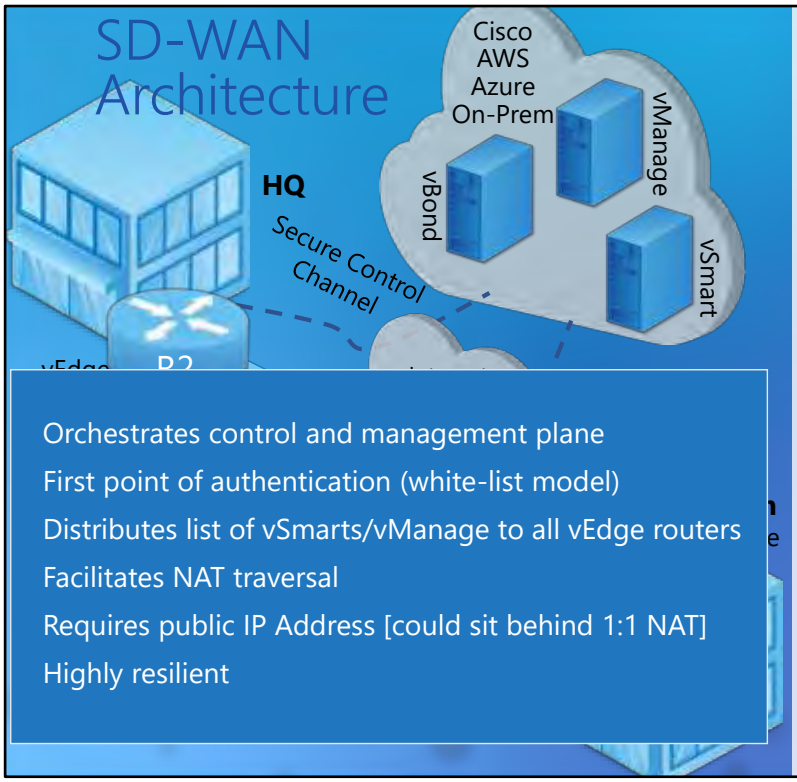
- Initial Investment
- Complexity
- Dependence on Internet Connectivity
- Security Concerns
- Vendor Lock-in
- Quality of Service (QoS) Issues
- Integration Challenges
- Learning Curve

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



- Orchestration Plane
  - vBond
    - Onboarding of SD-WAN
- Management Plane
  - vManage
    - Dashbord for Management
- Control Plane
  - vSmart
    - Learns information from vEDGEs and vManage
    - Distributes Routes / Polices / Security Info to vEdges
- Data Plane
  - Edge / vEdge
    - Traffic forwarding, security, encryption, QoS

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Orchestration Plane

- vBond
  - Onboarding of SD-WAN

Management Plane

- vManage
  - Dashbord for Management

Control Plane

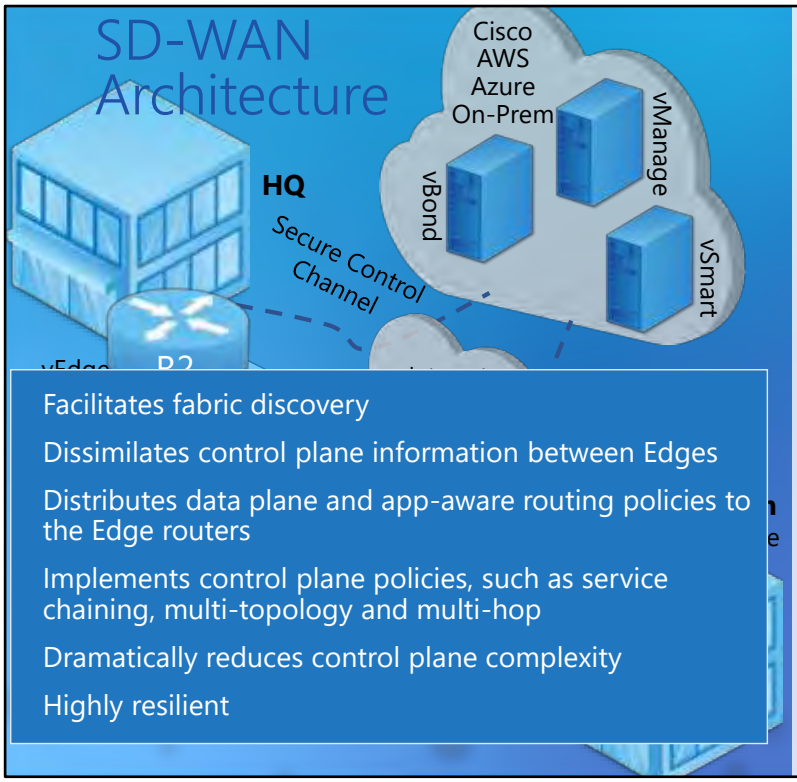
- vSmart
  - Learns information from vEDGEs and vManage
  - Distributes Routes / Polices / Security Info to vEdges

Data Plane

- Edge / vEdge
  - Traffic forwarding, security, encryption, QoS

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SD-WAN Architecture



- Facilitates fabric discovery
- Dissimilates control plane information between Edges
- Distributes data plane and app-aware routing policies to the Edge routers
- Implements control plane policies, such as service chaining, multi-topology and multi-hop
- Dramatically reduces control plane complexity
- Highly resilient

Orchestration Plane
- vBond
  - Onboarding of SD-WAN

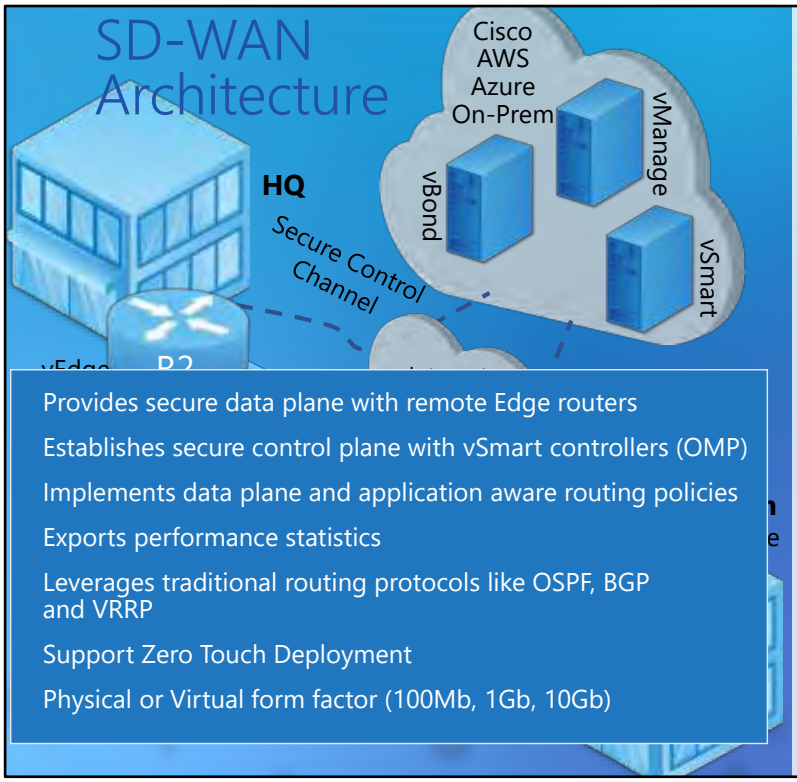
Management Plane
- vManage
  - Dashbord for Management

Control Plane
- vSmart
  - Learns information from vEDGEs and vManage
  - Distributes Routes / Polices / Security Info to vEdges

Data Plane
- Edge / vEdge
  - Traffic forwarding, security, encryption, QoS

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SD-WAN Architecture



- Provides secure data plane with remote Edge routers
- Establishes secure control plane with vSmart controllers (OMP)
- Implements data plane and application aware routing policies
- Exports performance statistics
- Leverages traditional routing protocols like OSPF, BGP and VRRP
- Support Zero Touch Deployment
- Physical or Virtual form factor (100Mb, 1Gb, 10Gb)

Orchestration Plane
- vBond
  - Onboarding of SD-WAN

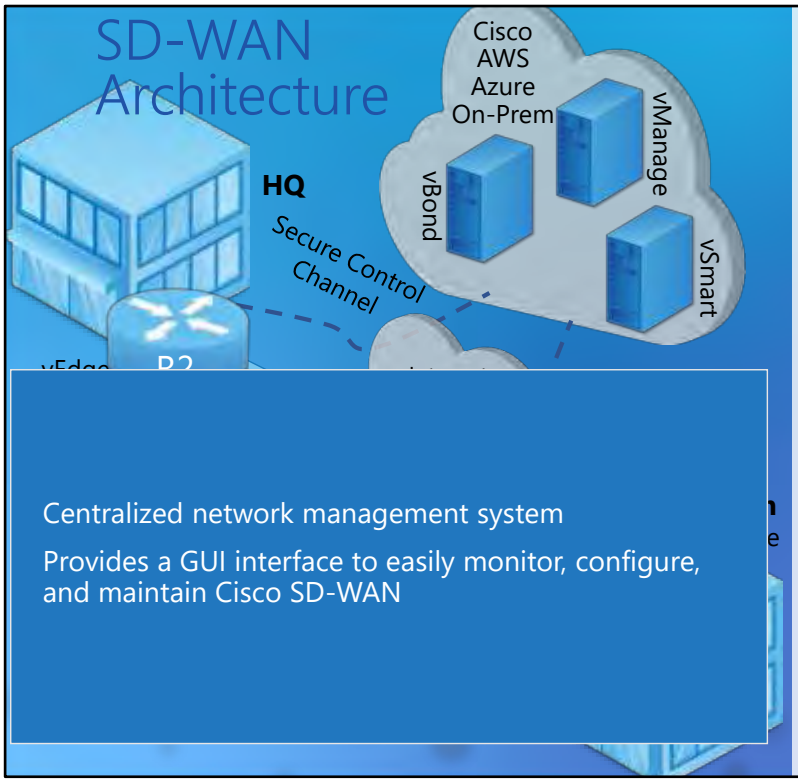
Management Plane
- vManage
  - Dashbord for Management

Control Plane
- vSmart
  - Learns information from vEDGEs and vManage
  - Distributes Routes / Polices / Security Info to vEdges

Data Plane
- Edge / vEdge
  - Traffic forwarding, security, encryption, QoS

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SD-WAN Architecture



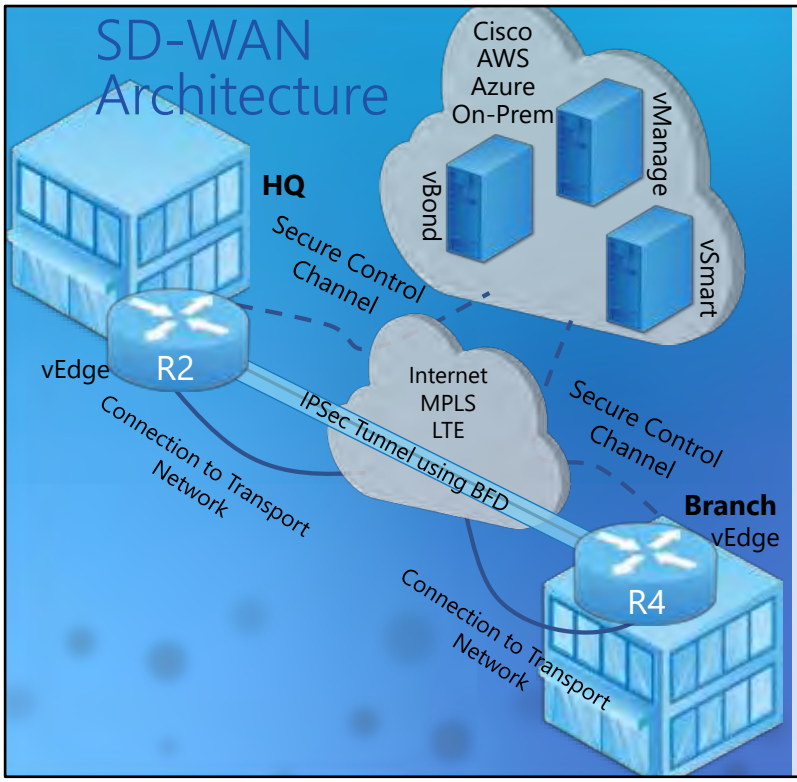
Centralized network management system

Provides a GUI interface to easily monitor, configure, and maintain Cisco SD-WAN

- Orchestration Plane
  - vBond
    - Onboarding of SD-WAN
- **Management Plane**
  - vManage
    - Dashbord for Management
- Control Plane
  - vSmart
    - Learns information from vEDGEs and vManage
    - Distributes Routes / Polices / Security Info to vEdges
- Data Plane
  - Edge / vEdge
    - Traffic forwarding, security, encryption, QoS

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



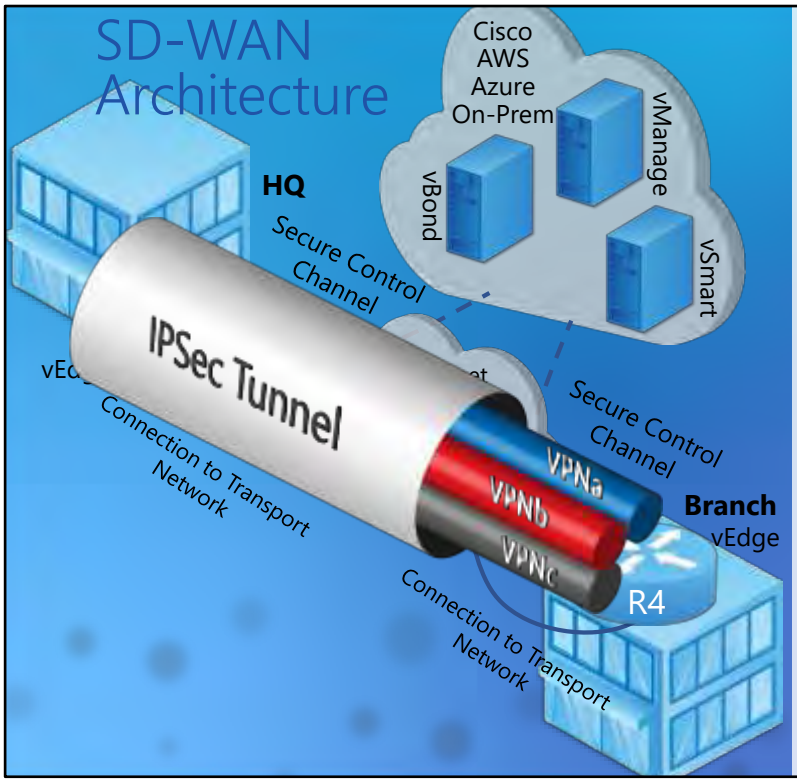
Dynamic Transport Layer Security (DTLS)

- Used to create secure control channels
  - Edge / vEdge to vSmart
  - Edge / vEdge to vManage
  - Edge / vEdge to vBond
  - vSmart to vSmart

Overlay Management Protocol (OMP)

- TCP based control plane protocol
  - Runs inside DTLS connections
- Edge / vEdge to vSmart info sharing
  - Reachability – Subnets, Routes, TLOCs
  - Security – Encryption Keys
  - Policy – Data/App-route Policies

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



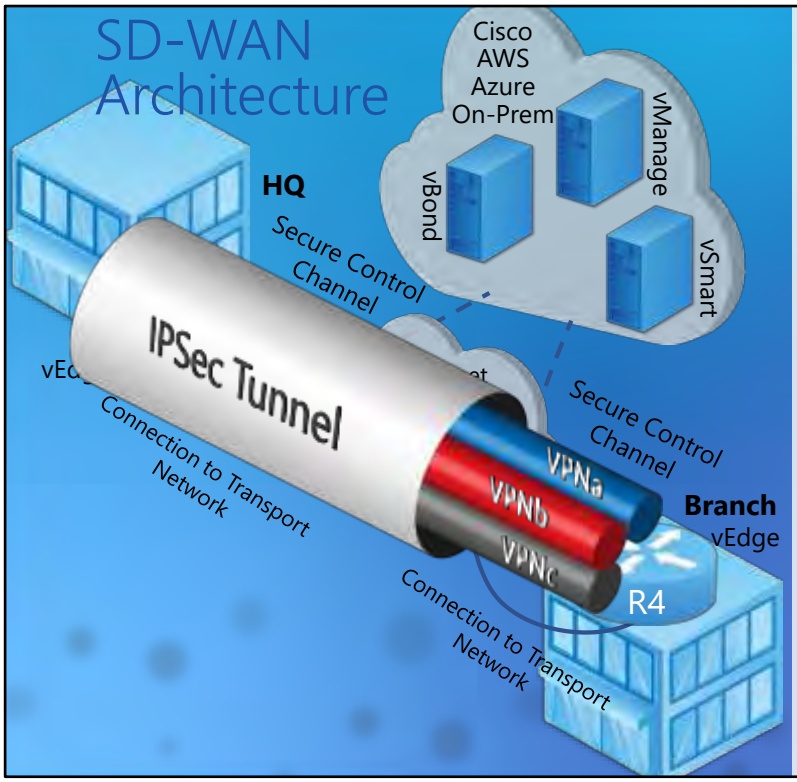
IPSec Tunnel

- Secure connection between Edge / vEdge devices
  - Provides secure transport of user data from one site to another
  - Uses BFD to detect
    - Loss, latency, jitter, failures

VPNs

- Provides isolation and segmentation of data traffic within the IPSec tunnel (like VRFs)
  - Multiple VPNs may exist in one tunnel
  - Each VPN has its own forwarding table

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



IPSec Tunnel

- Secure connection between Edge / vEdge devices
  - Provides secure transport of user data from one site to another
  - Uses BFD to detect
    - Loss, latency, jitter, failures

VPNs

- Provides isolation and segmentation of data traffic within the IPSec tunnel (like VRFs)
  - Multiple VPNs may exist in one tunnel
  - Each VPN has its own forwarding table

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

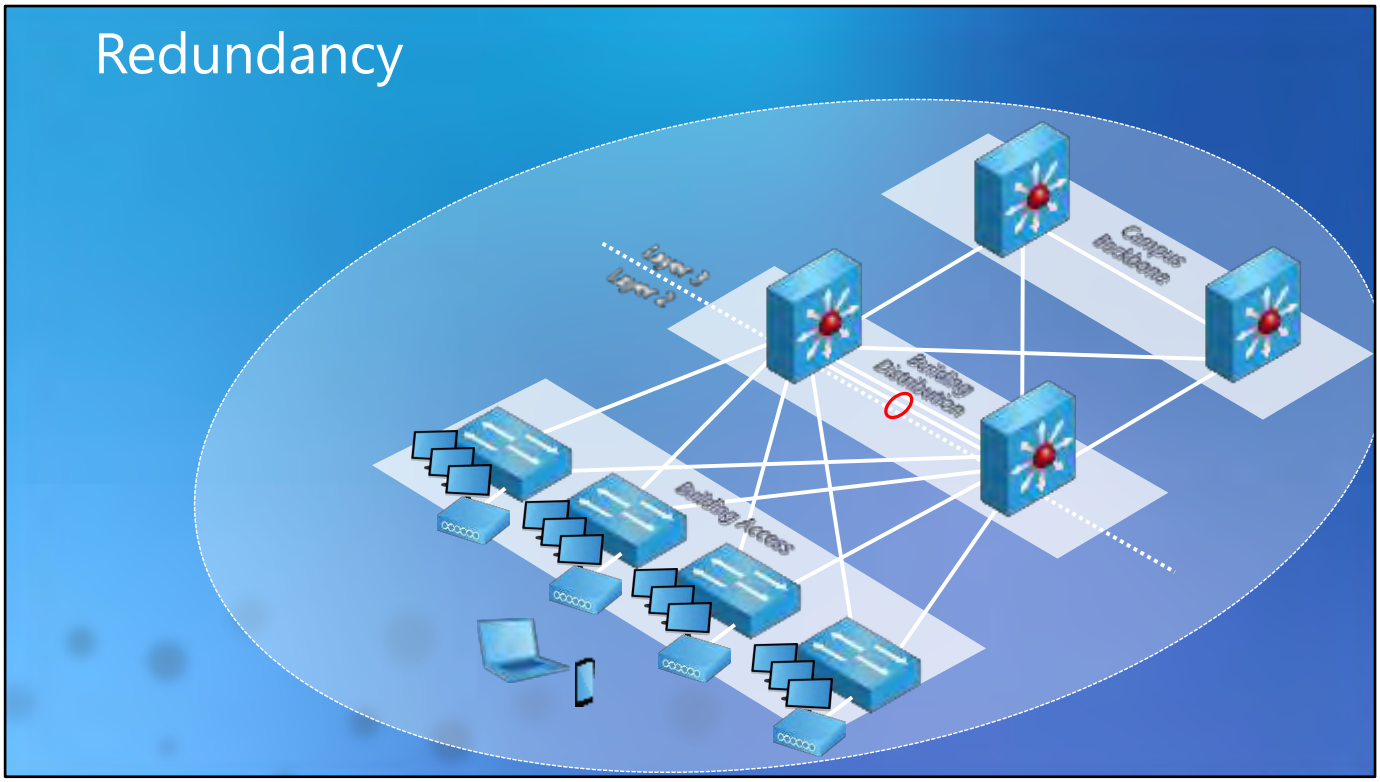
What Next For Exam Prep?

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

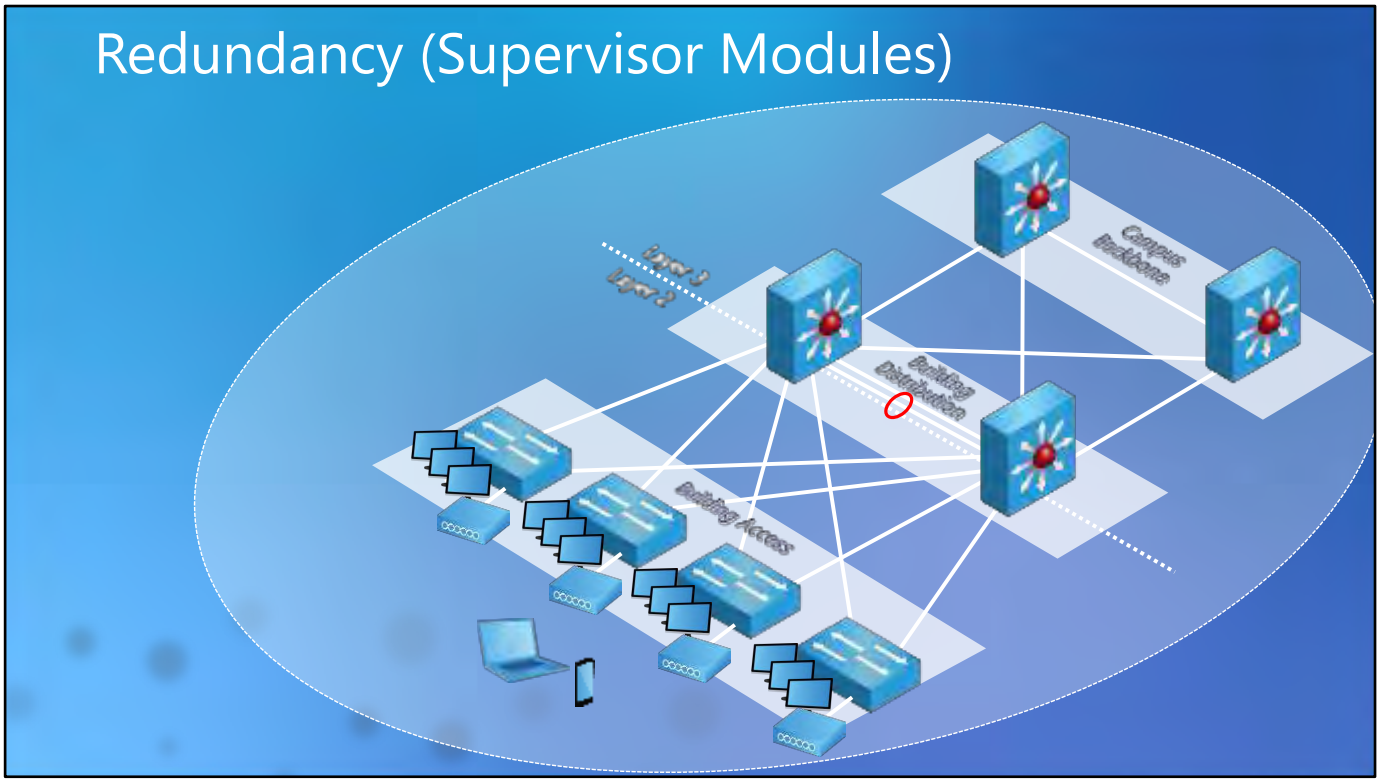
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Stateful Switchover and Non-Stop Forwarding

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

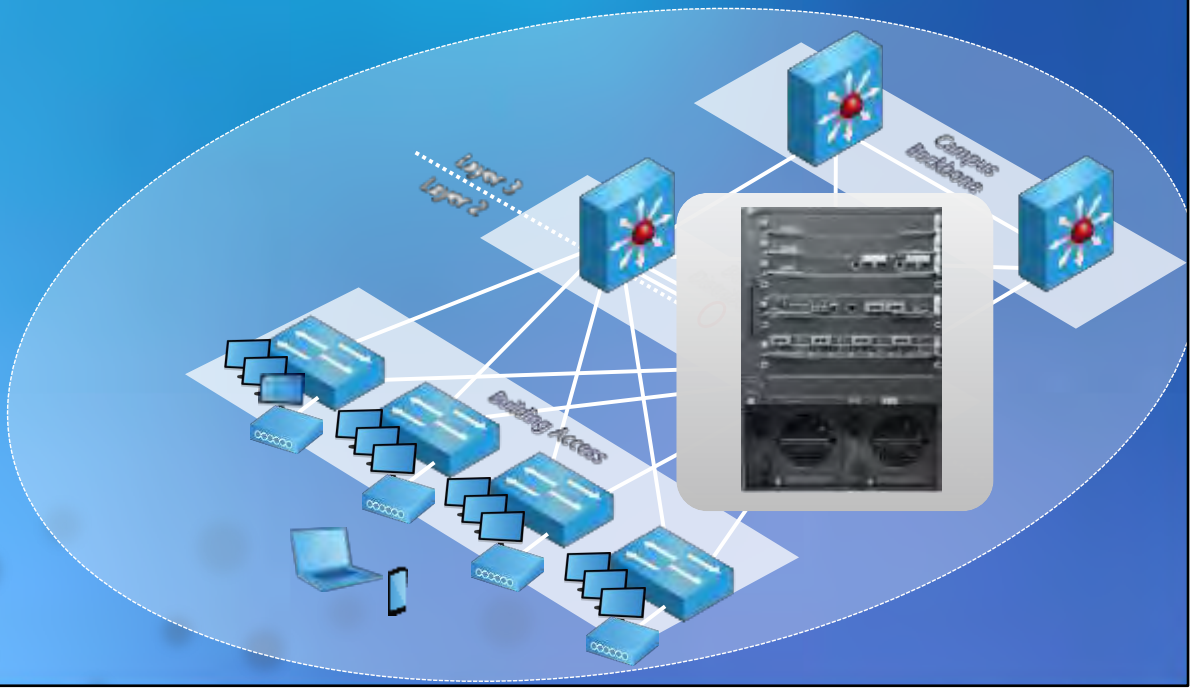


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

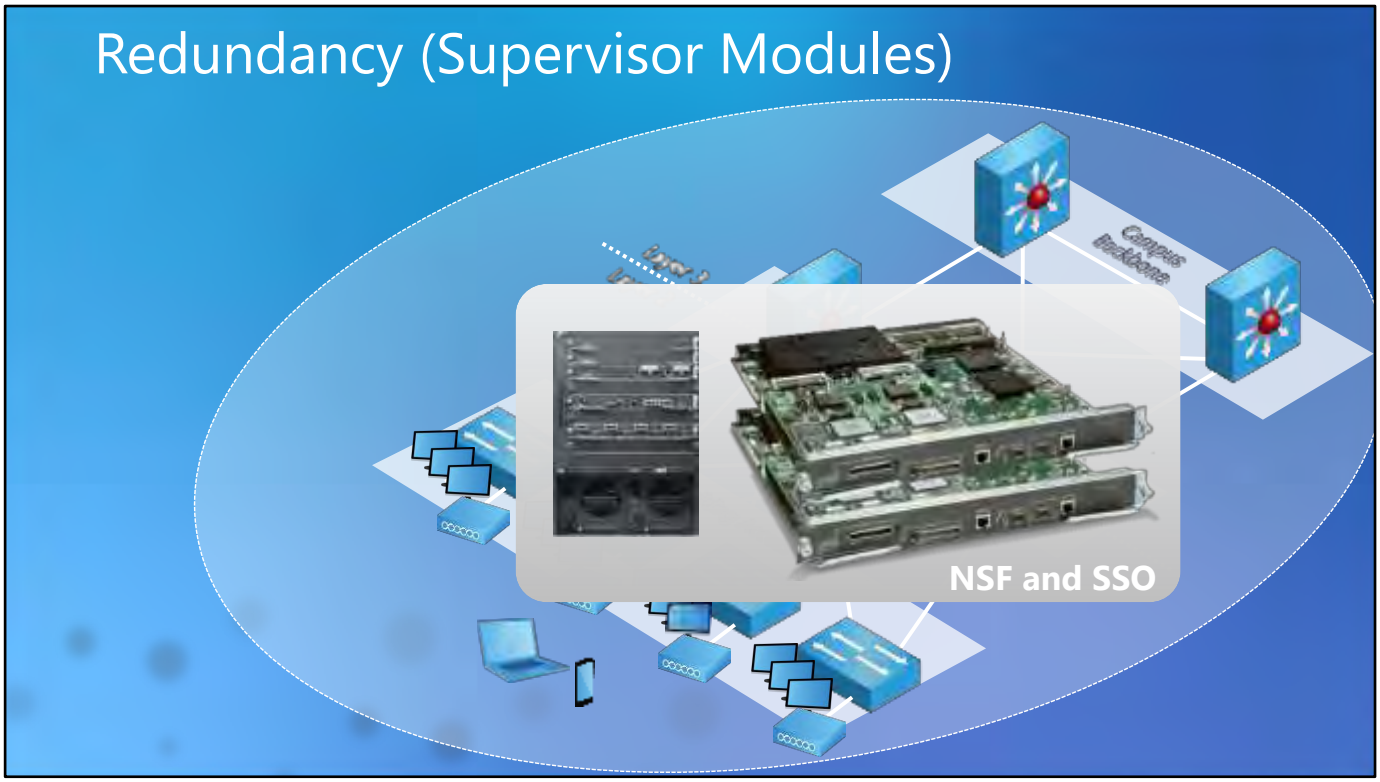


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Redundancy (Supervisor Modules)



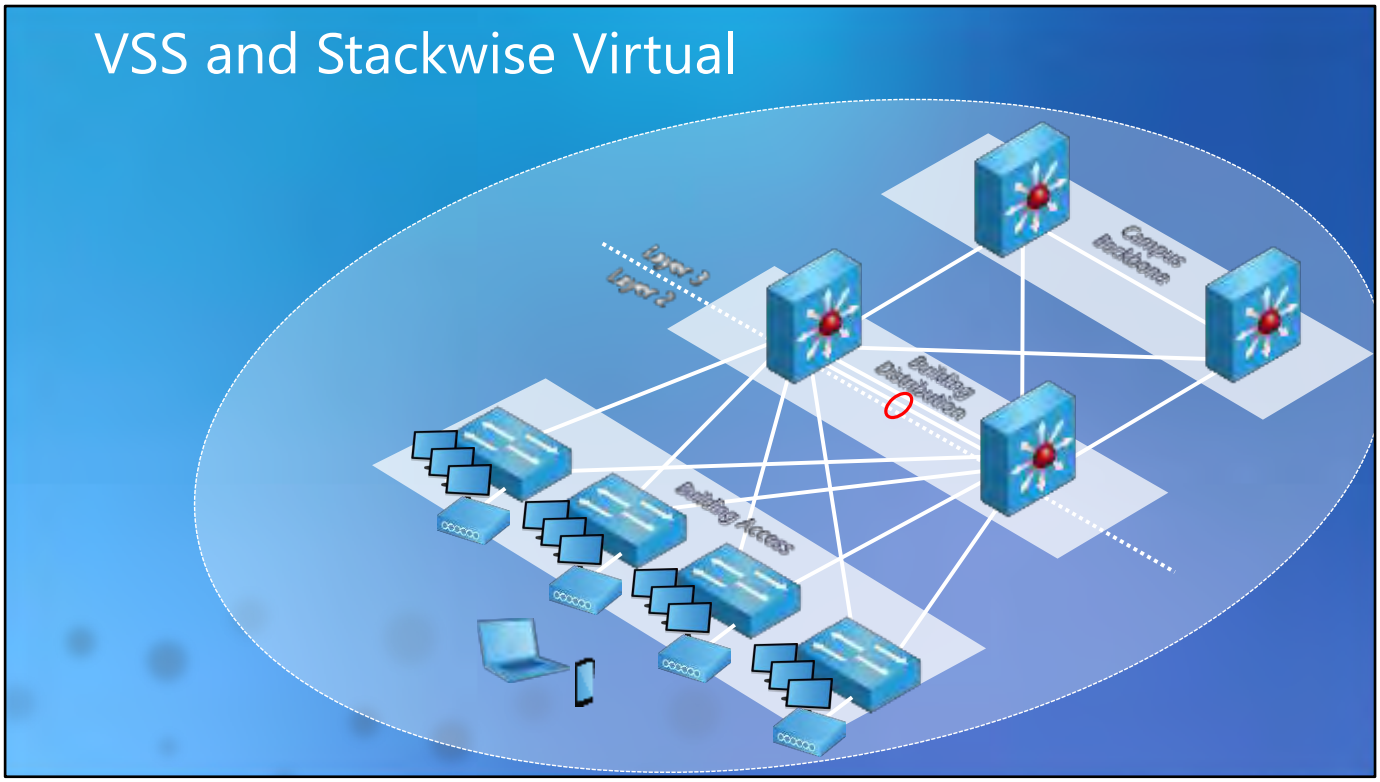
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



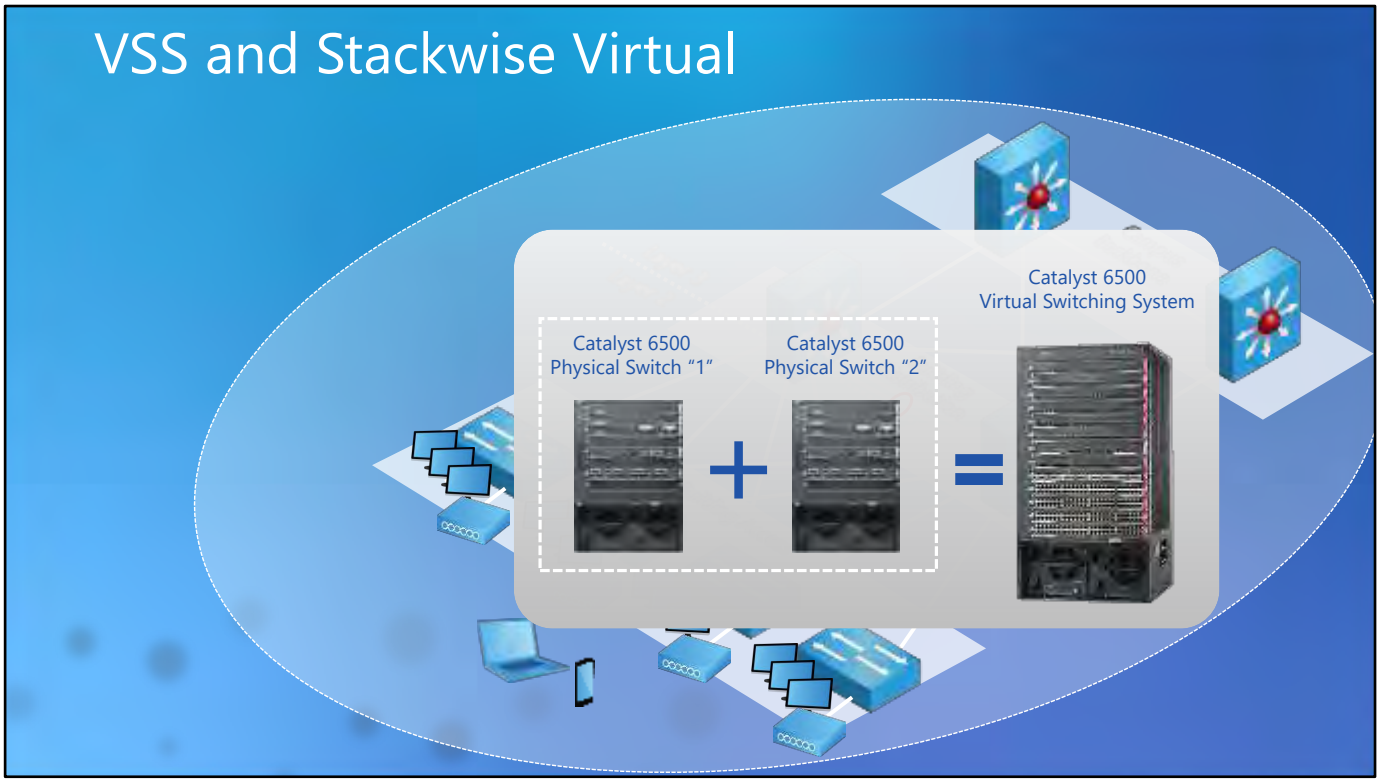
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

VSS and Stackwise

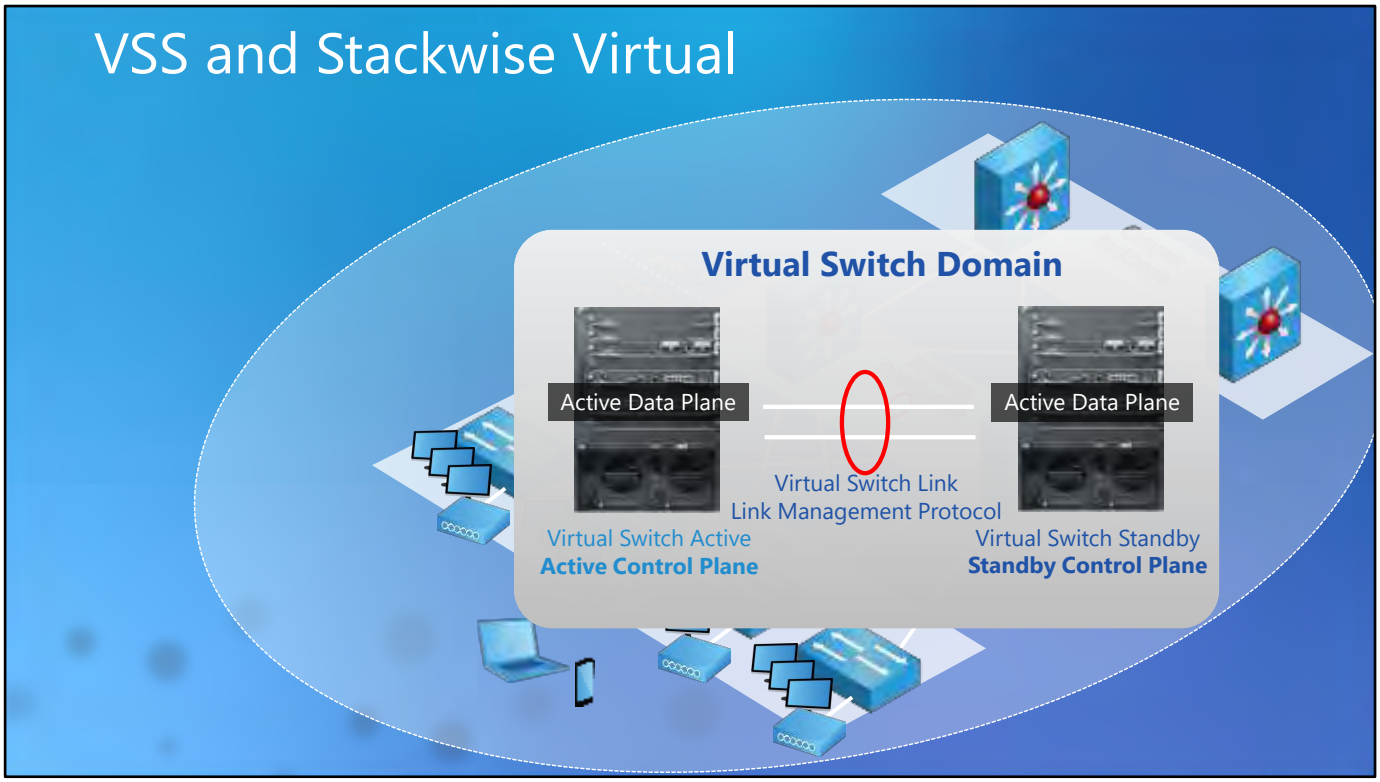
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



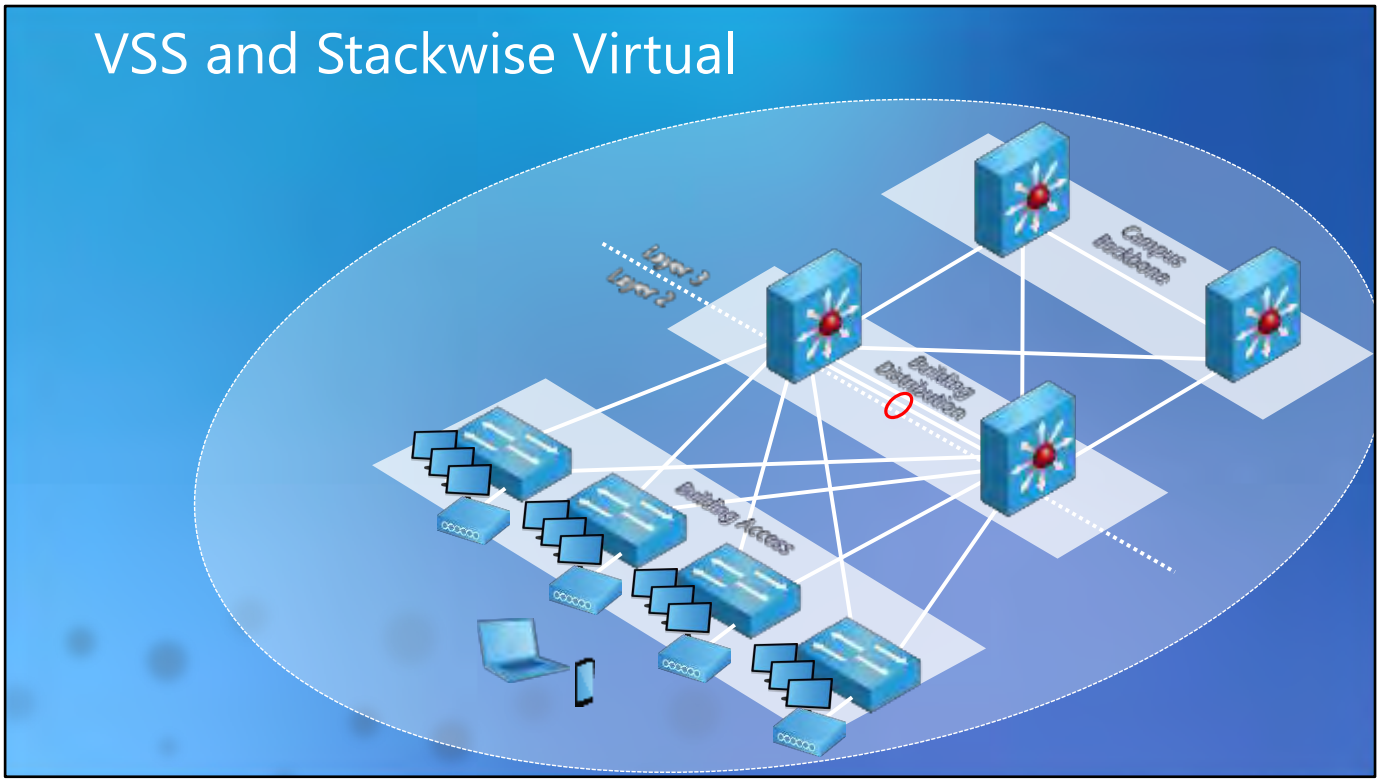
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



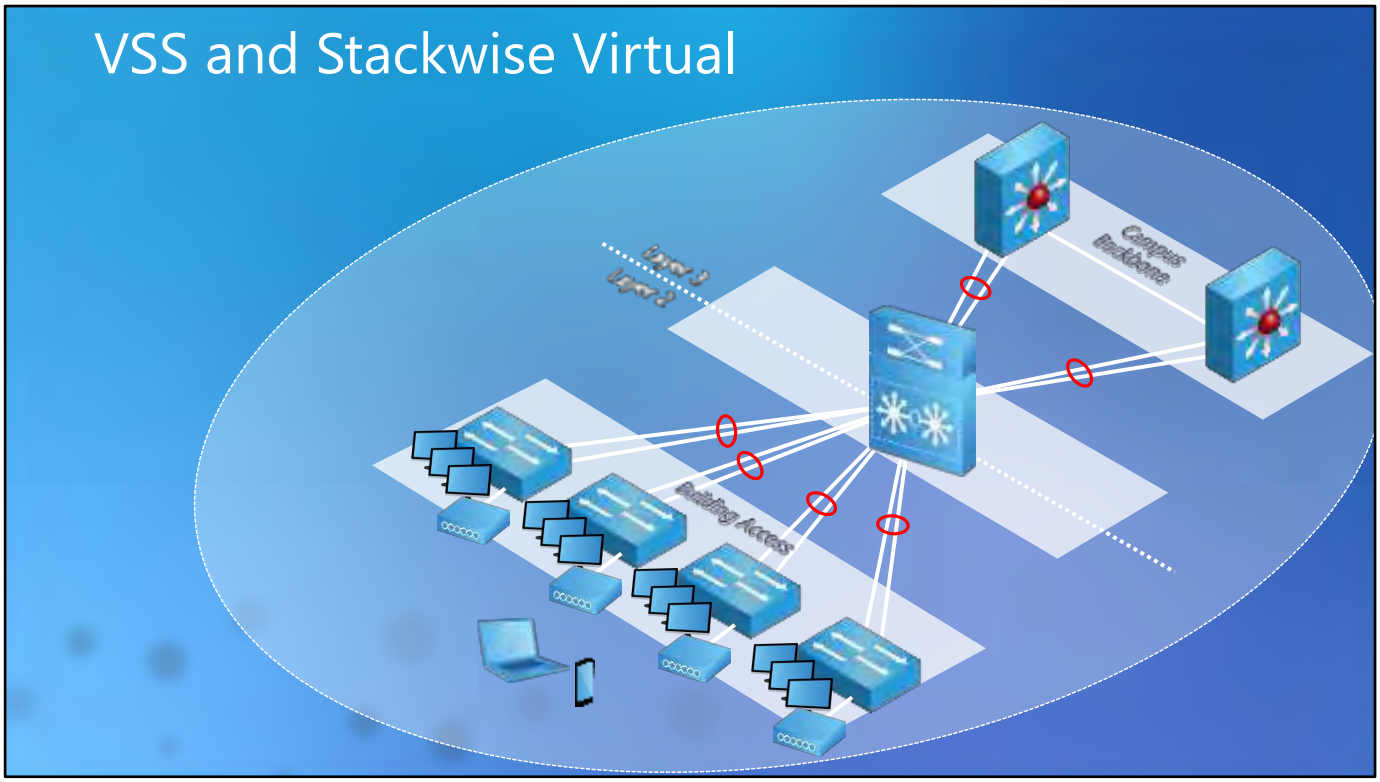
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



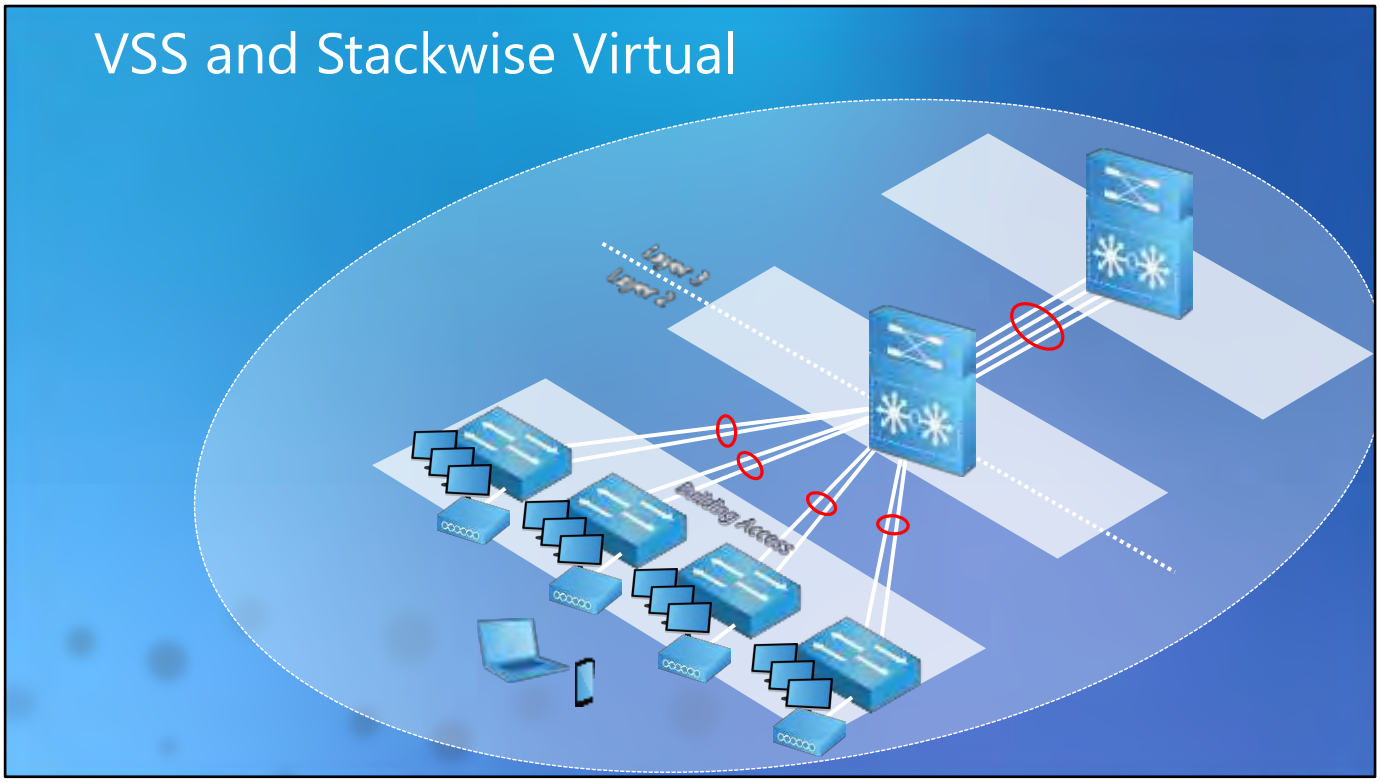
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



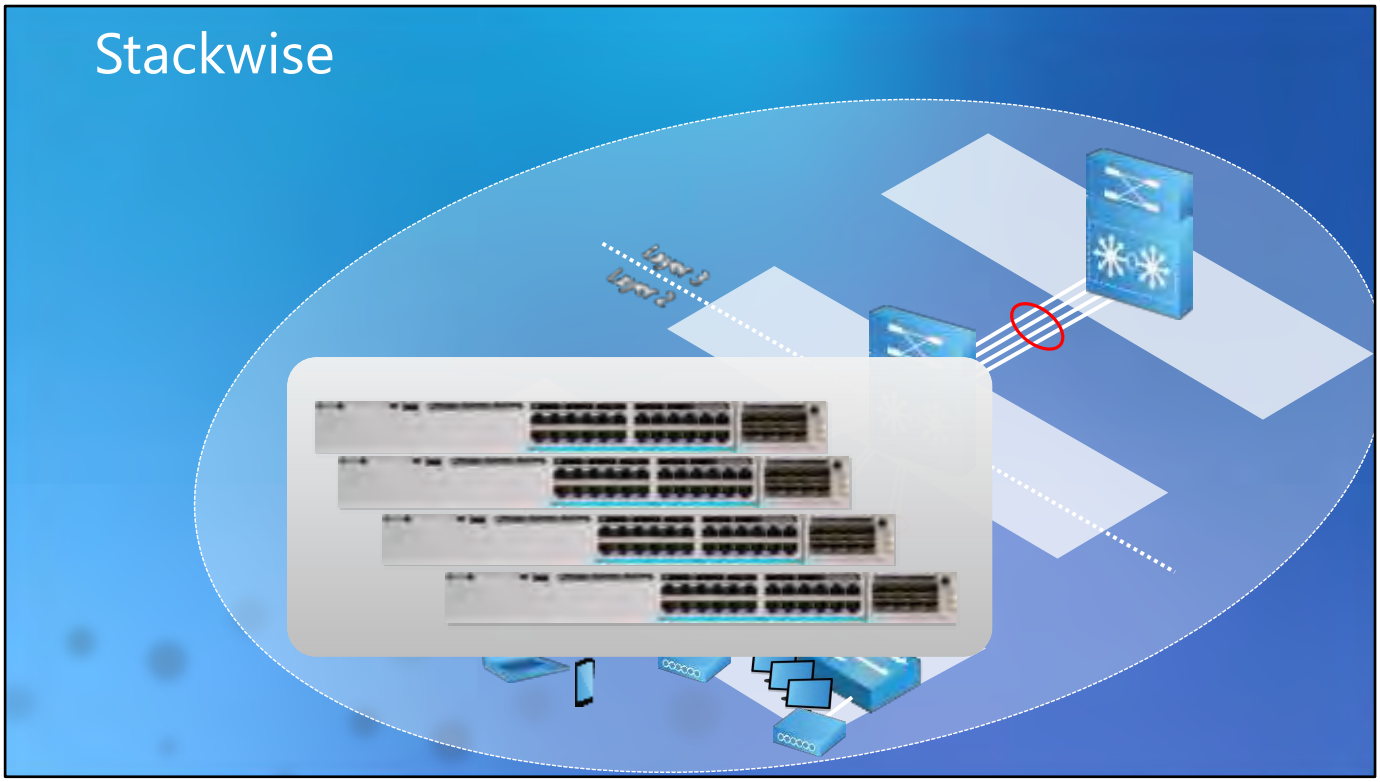
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



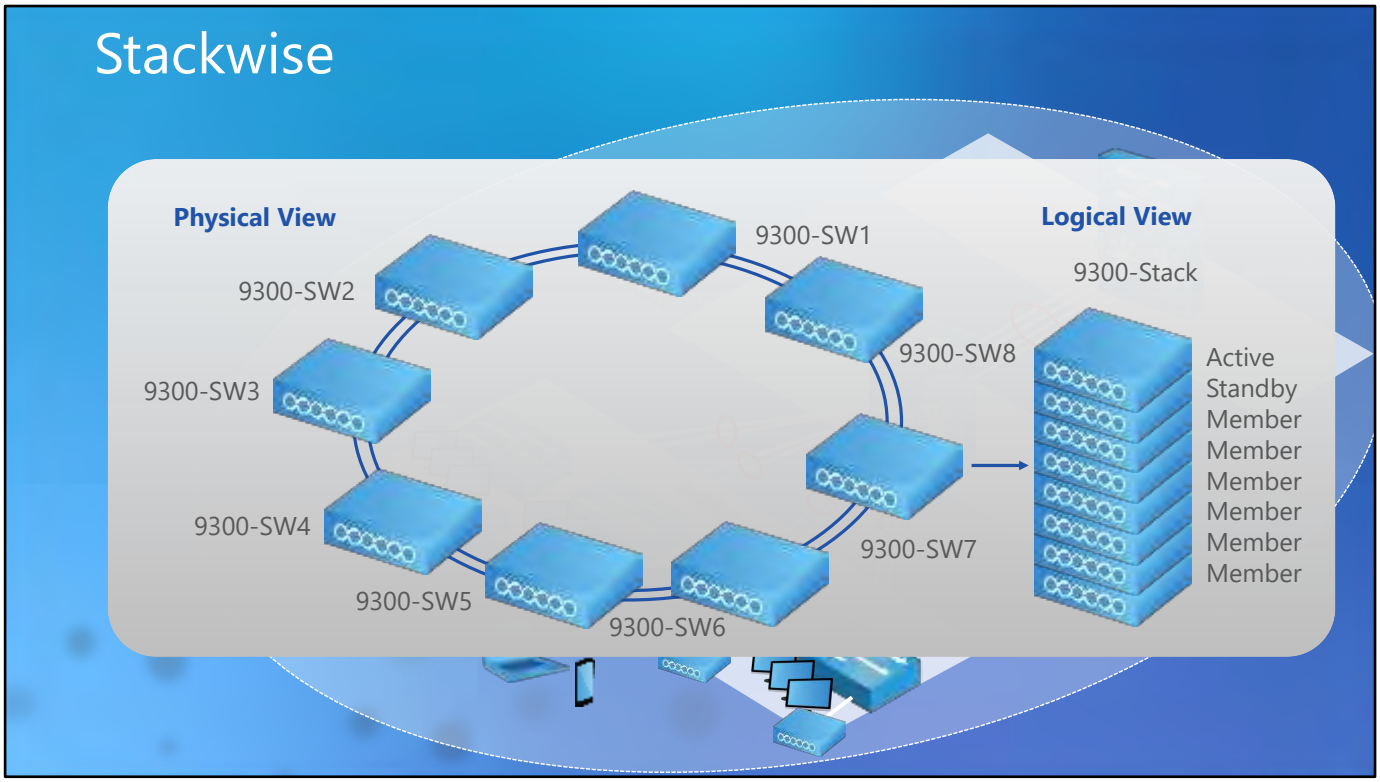
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



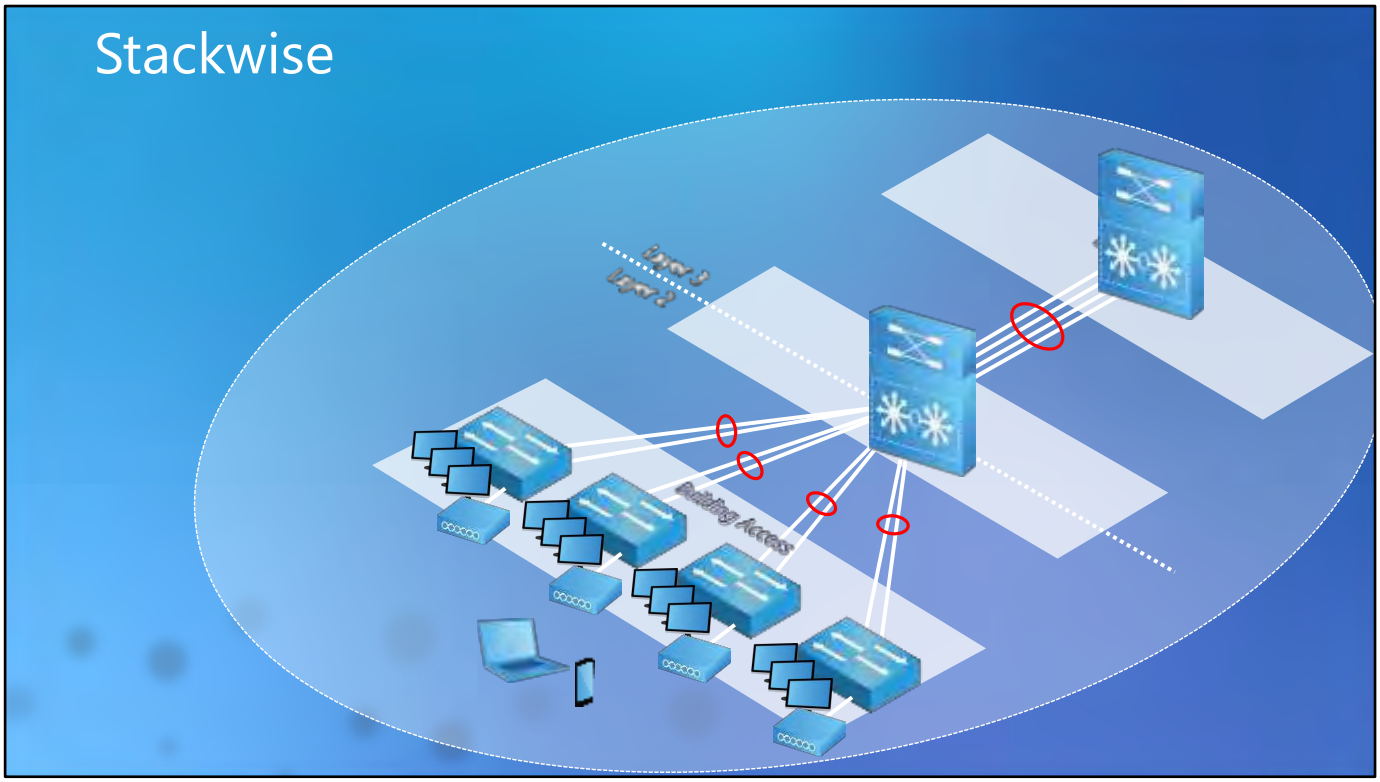
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

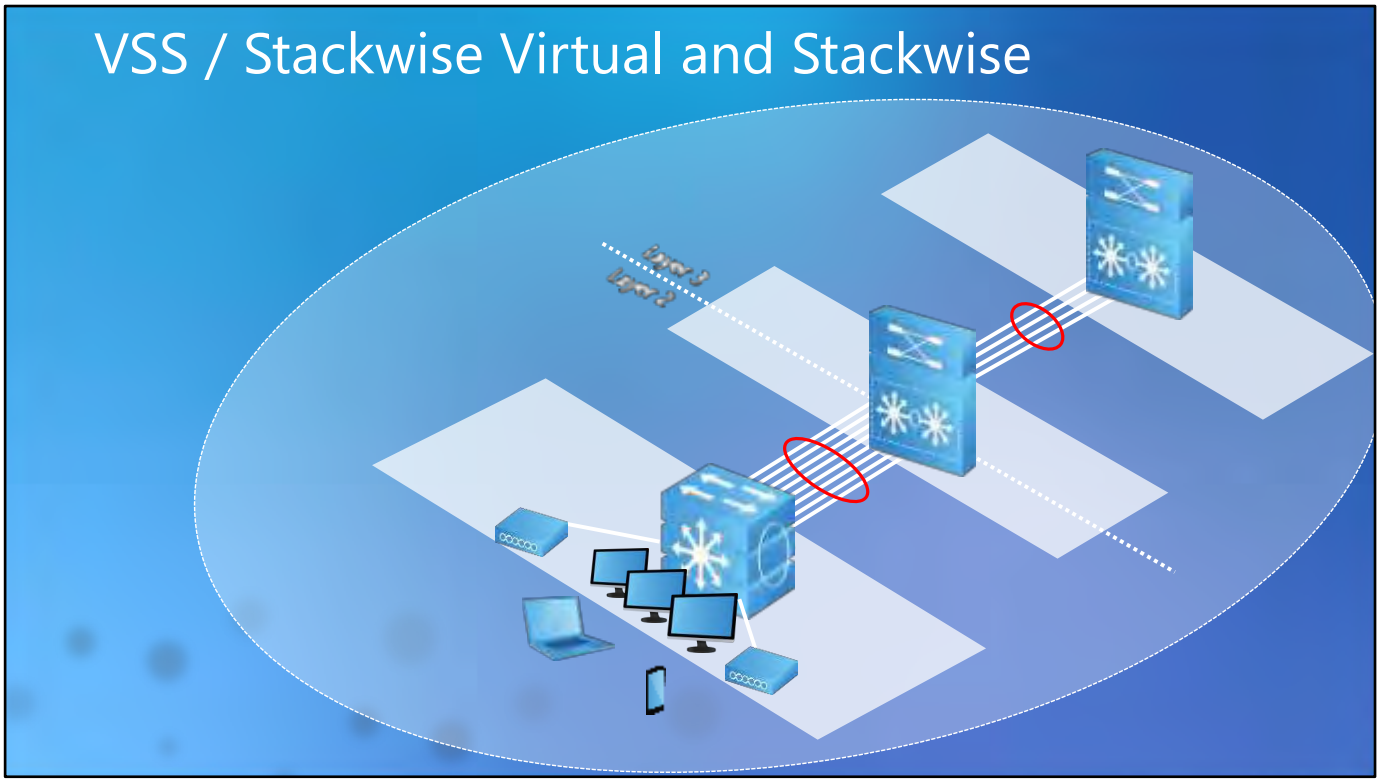
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



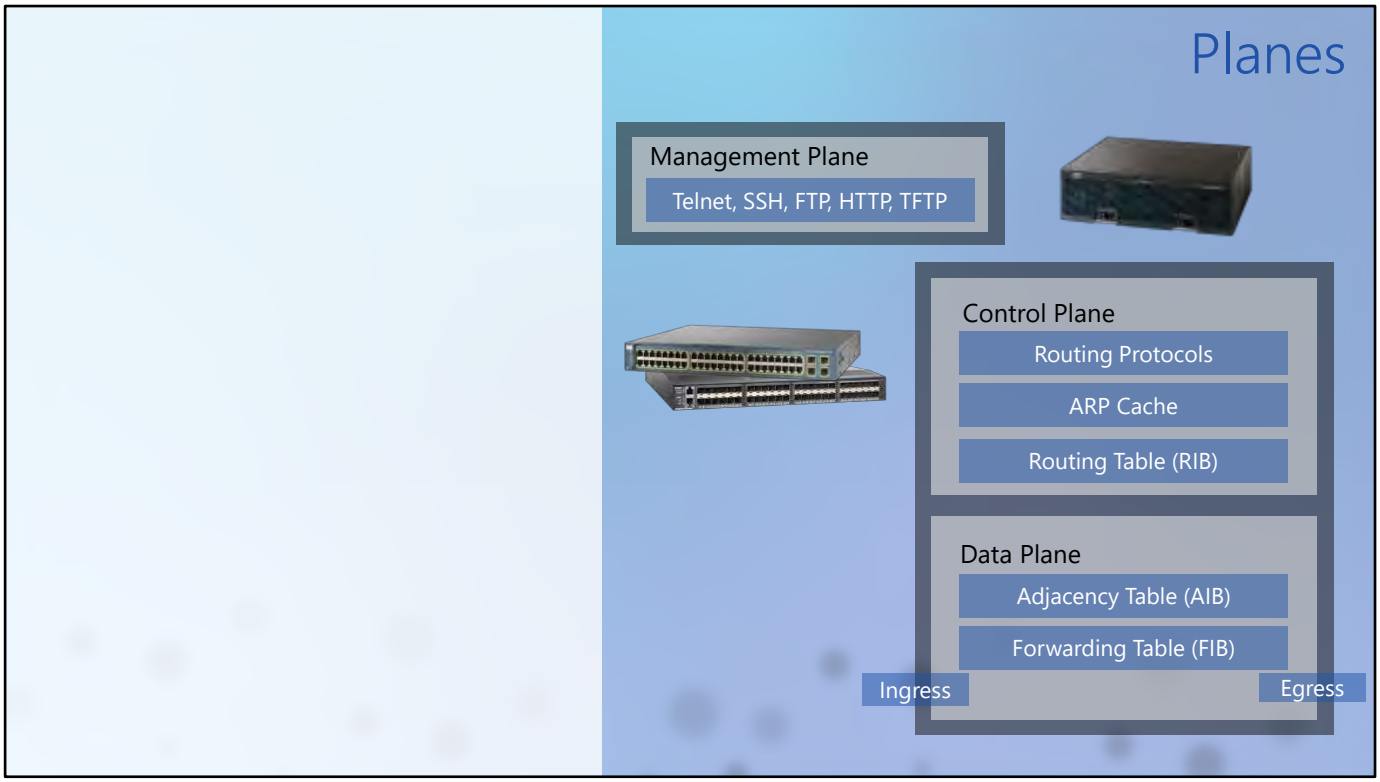
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Device Architecture

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RIB, FIB, and More

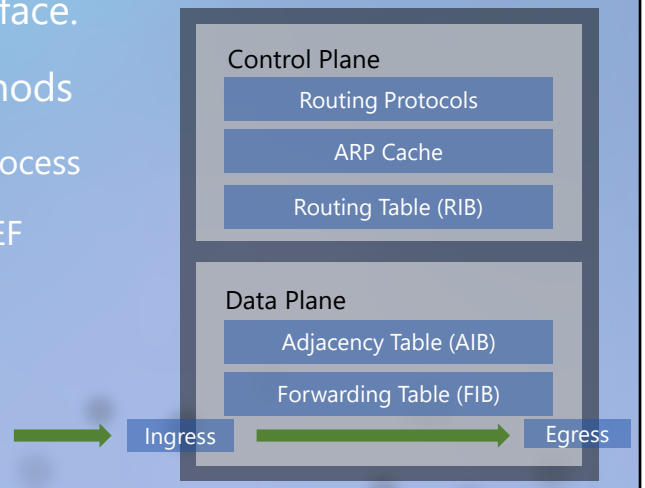
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Switching

The method which our routers and switches use to move ingress packets to the egress interface.

Methods

- Process
- CEF

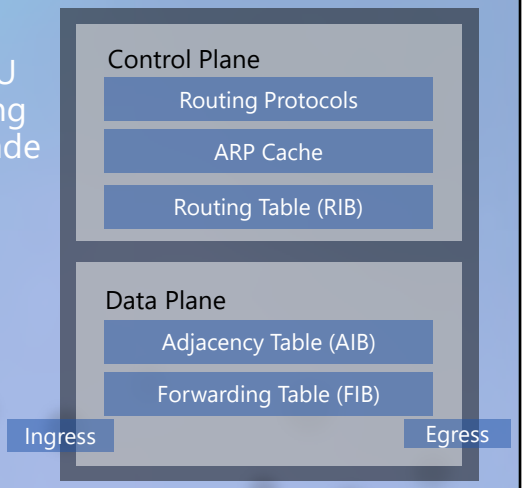


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Process vs CEF Switching

Process

- Slowest method
- Every packet examined by CPU and all forwarding decisions are made in software



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Process vs CEF Switching

CEF (Cisco Express Forwarding)

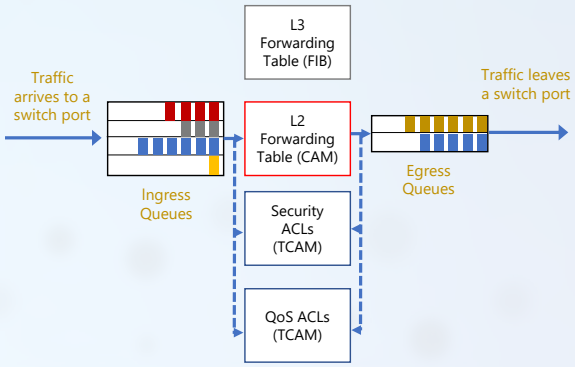
- Fastest method
- Packets are forwarded based on pre-populated tables in hardware

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

CAM vs TCAM

Content Addressable Memory

Ternary Content Addressable Memory



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

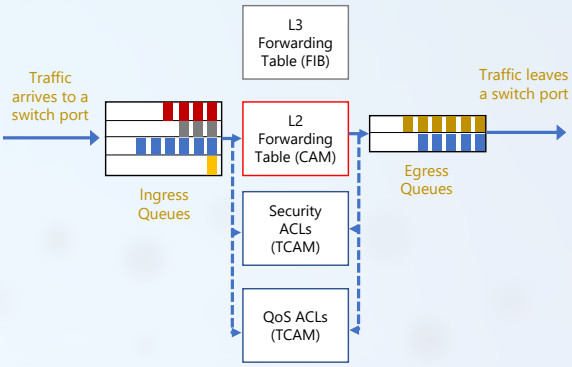
CAM vs TCAM

Tables stored in fast memory so that forwarding decisions are made extremely fast

- Used by L2 and L3 switches, and modern routers

L2 switching uses CAM

L3 switching uses TCAM and FIB



©2023 by StormWind LLC. All rights reserved.

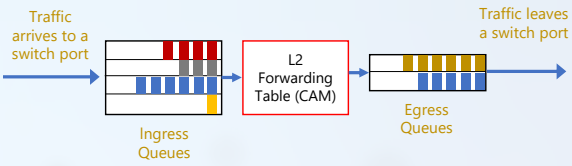
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

CAM vs TCAM

CAM

- Content-Addressable Memory
- Used to make L2 forwarding decisions
- Contains MAC address to port mappings

```
ASW1#show mac address-table dynamic
Unicast Entries
 vlan   mac address     type        protocols        port
-------+---------------+--------+--------------+--------------------
  10    00e0.4c69.85d2   dynamic ip,ipx         GigabitEthernet1/1
  10    00e0.4c69.8725   dynamic ip,ipx         GigabitEthernet1/2
  10    0800.2738.0011   dynamic ip             GigabitEthernet1/1
  10    e8b7.48a6.767f   dynamic ipx            GigabitEthernet1/45
  20    00e0.4c69.834a   dynamic ip,ipx         GigabitEthernet1/3
  20    00e0.4c69.86fe   dynamic ip,ipx         GigabitEthernet1/45
  50    00e0.4c69.84ab   dynamic ip,ipx         GigabitEthernet1/46
  50    00e0.4c69.85c6   dynamic ip,ipx         GigabitEthernet1/46
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

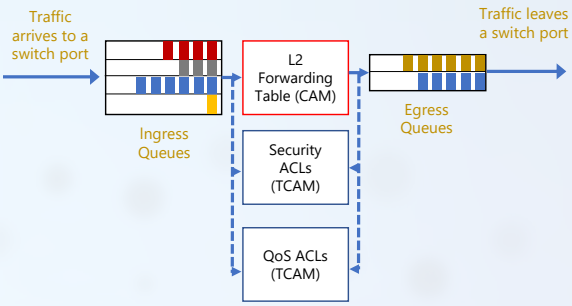
CAM vs TCAM

TCAM

Ternary Content-Addressable Memory

Stores

- ACL info
- QoS info
- CEF IP destination prefixes
- Other information associated with upper layer processing




```
DSW2#sho ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           no route
0.0.0.0/8           drop
0.0.0.0/32          receive
10.40.12.0/26       attached            Vlan421
10.40.12.0/32       receive             Vlan421
10.40.12.2/32       receive             Vlan421
10.40.12.63/32      receive             Vlan421
10.40.12.64/26      attached            Vlan422
10.40.12.64/32      receive             Vlan422
10.40.12.66/32      receive             Vlan422
10.40.12.127/32     receive             Vlan422
10.40.12.128/26     attached            Vlan423
10.40.12.128/32     receive             Vlan423
10.40.12.130/32     receive             Vlan423
10.40.12.191/32     receive             Vlan423
10.40.12.192/26     attached            Vlan424
10.40.12.192/32     receive             Vlan424
10.40.12.194/32     receive             Vlan424
10.40.12.255/32     receive             Vlan424
10.40.23.0/30       attached            GigabitEthernet1/0/13
10.40.23.0/32       receive             GigabitEthernet1/0/13
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

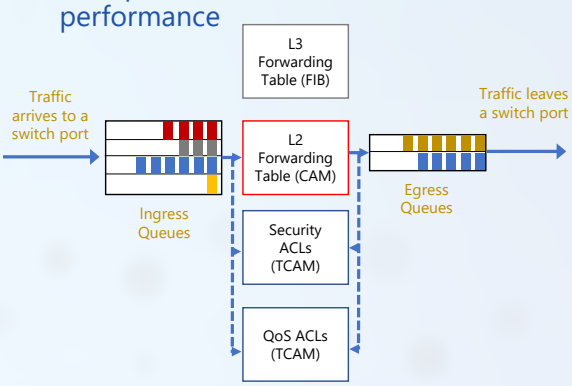
CAM vs TCAM

CAM tables

- Found on switches
- Mac to Port to VLAN mapping
- L2 forwarding decisions

TCAM tables

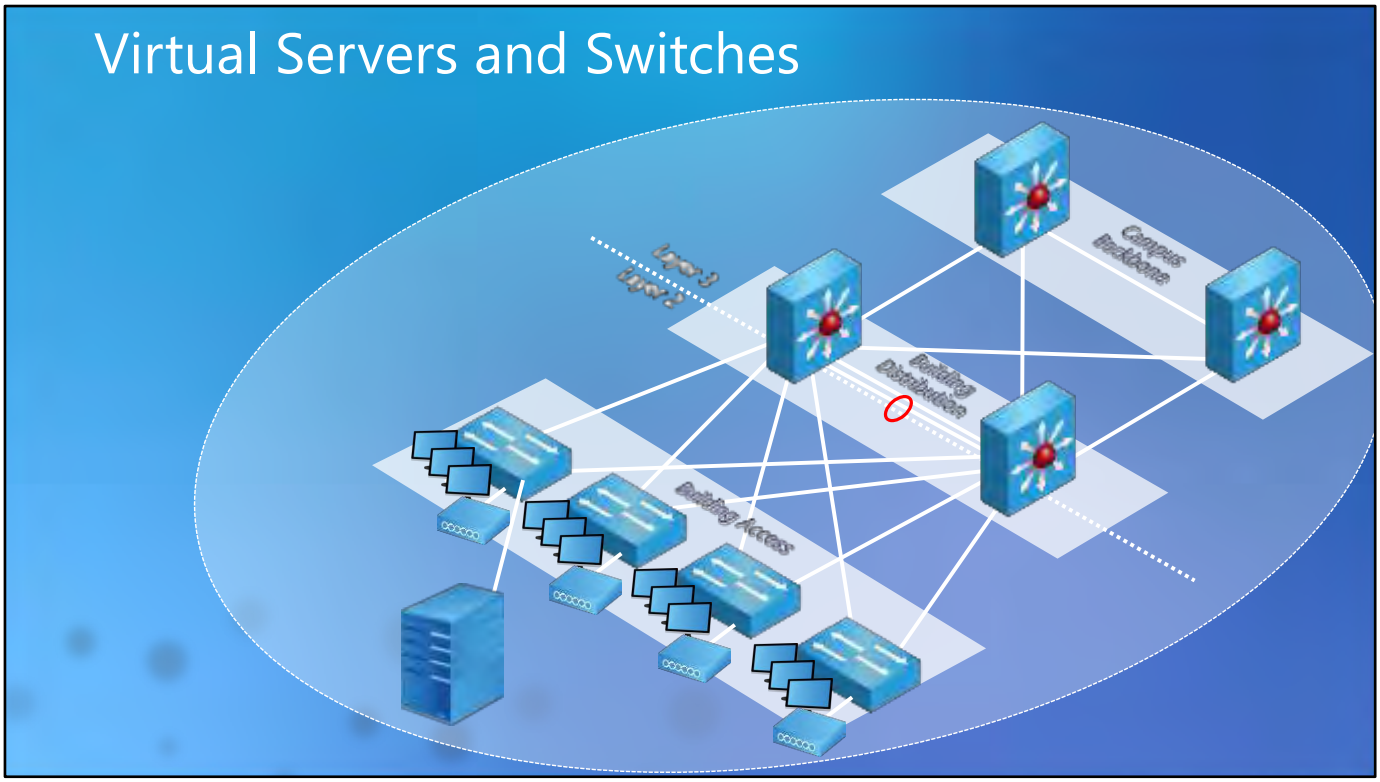
- On multilayer switches and routers
- ACLs, QoS, layer 3 processing
- Multiple TCAMs exist for better performance



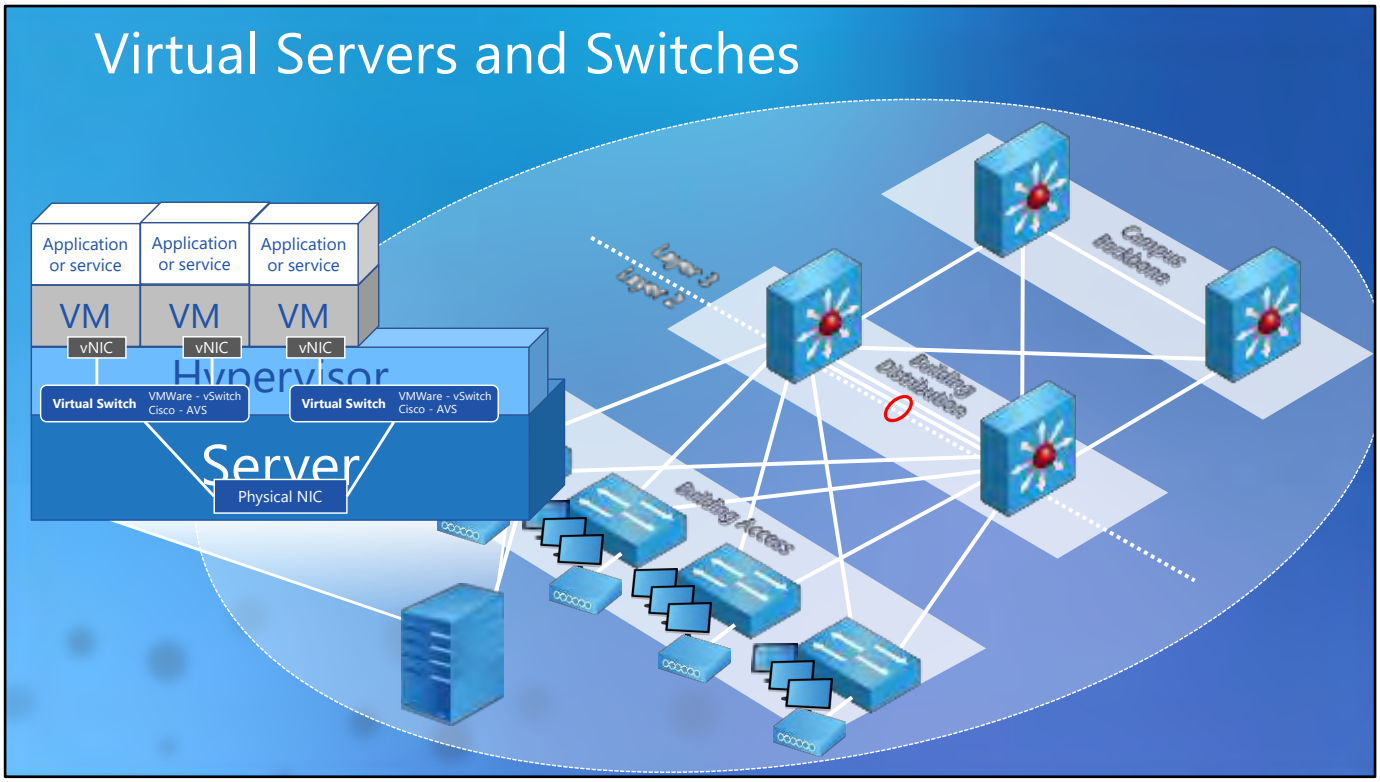
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Virtual Servers and Switches

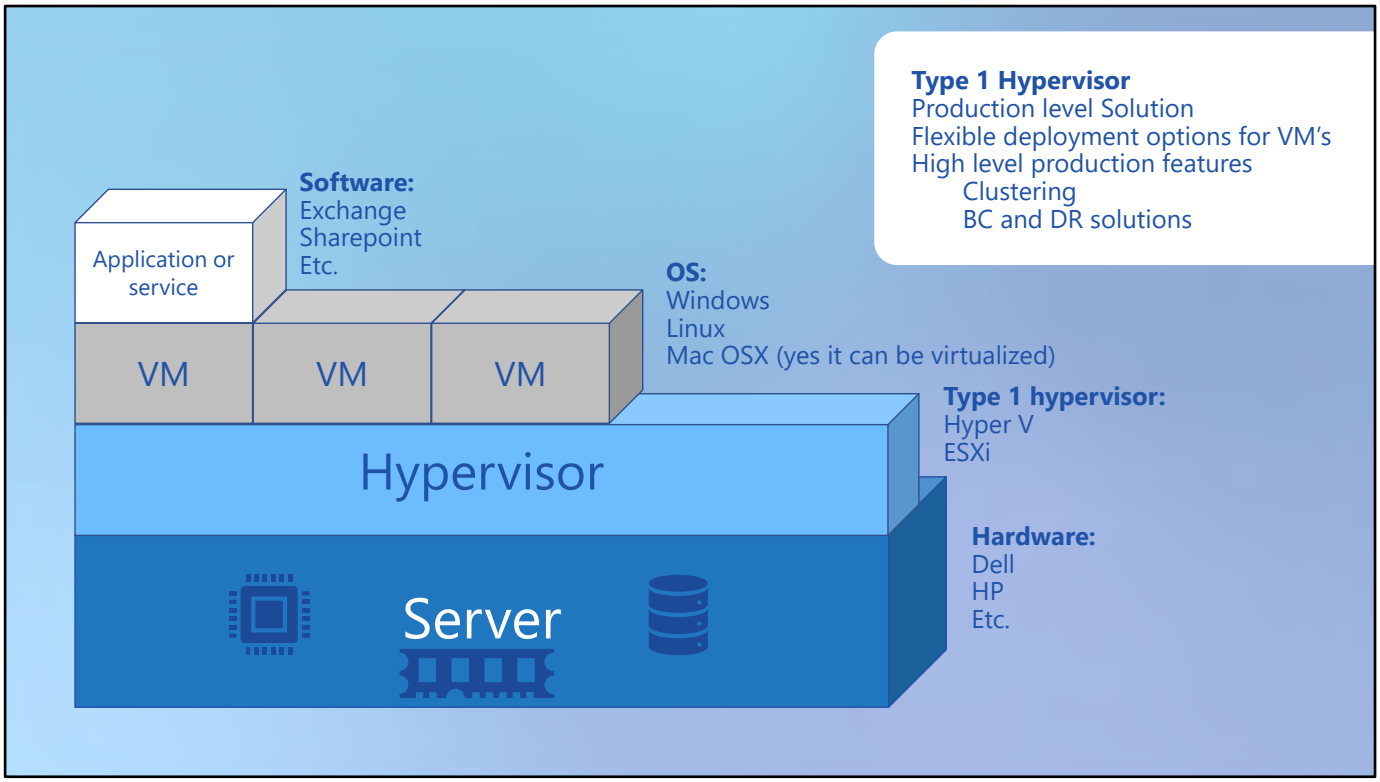
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



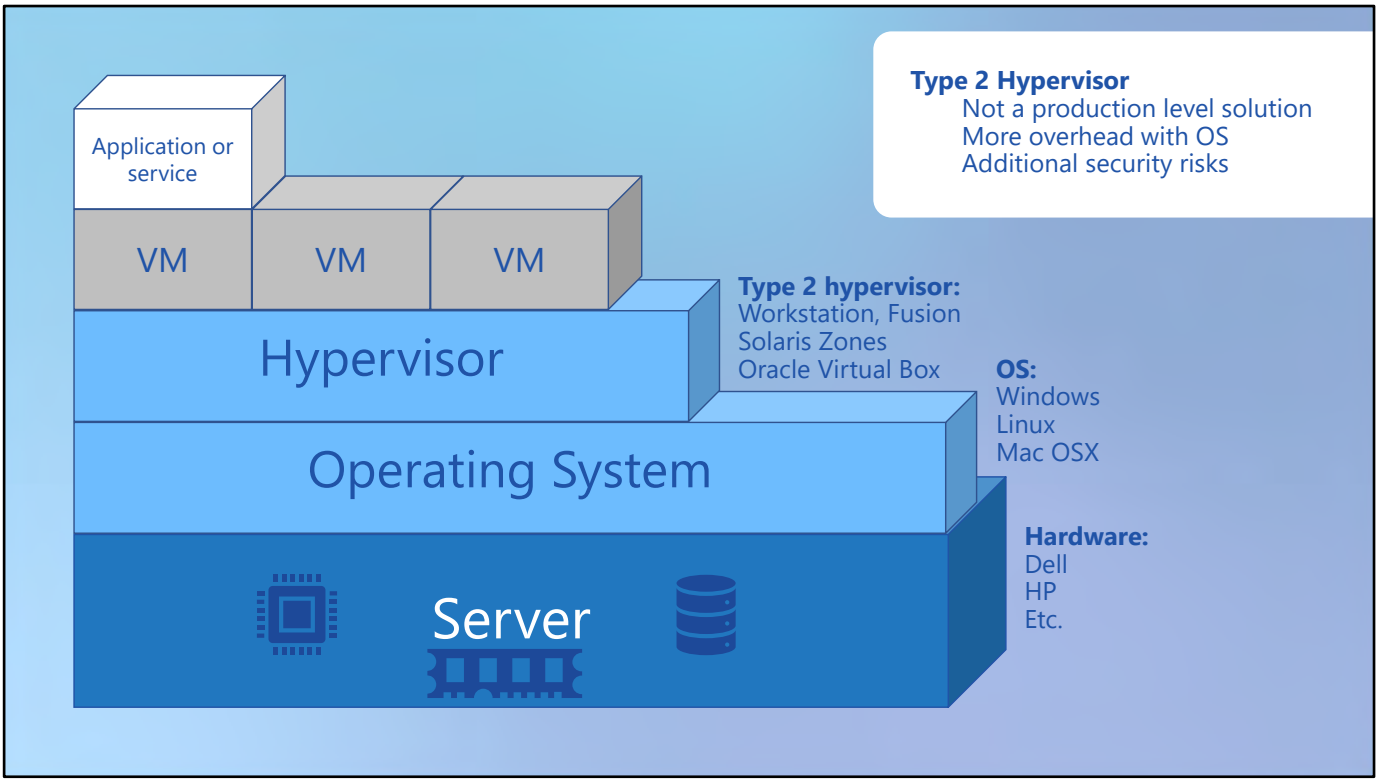
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



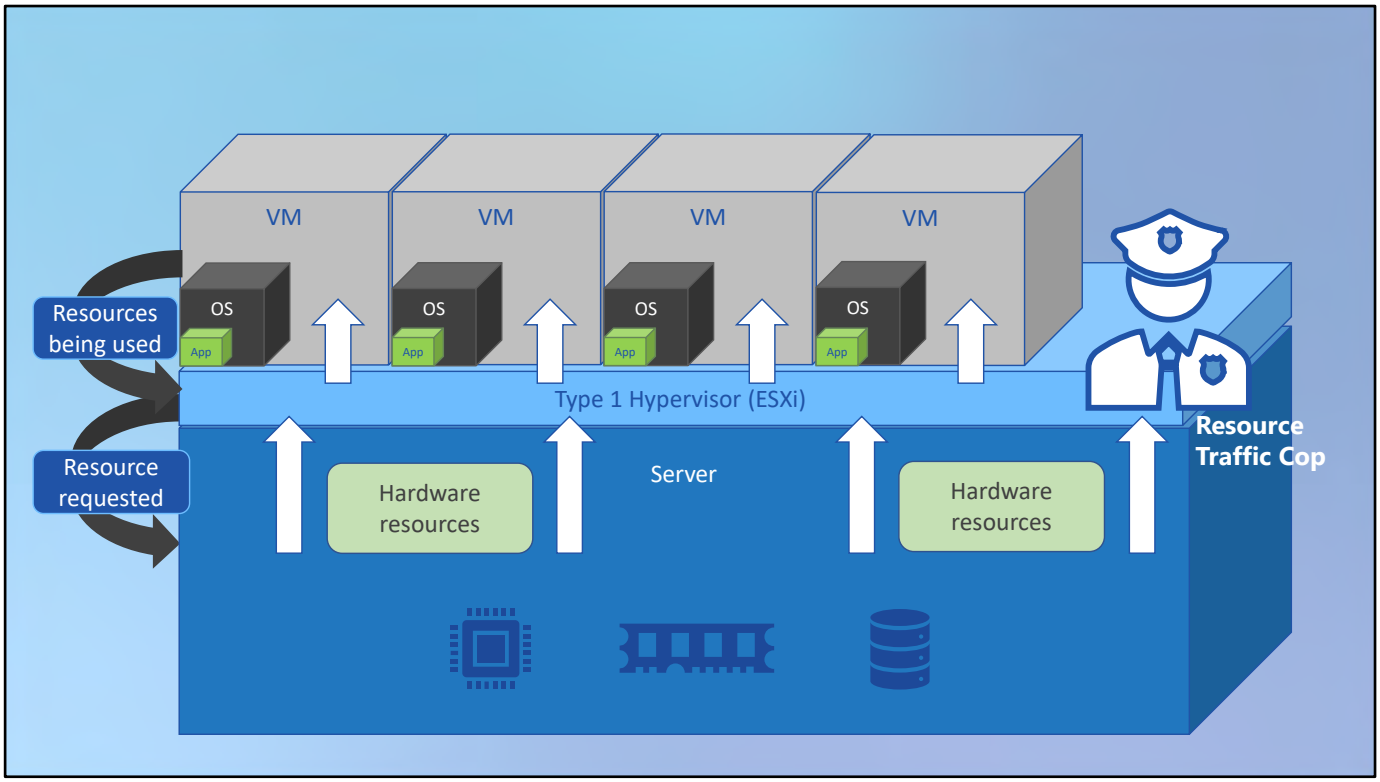
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



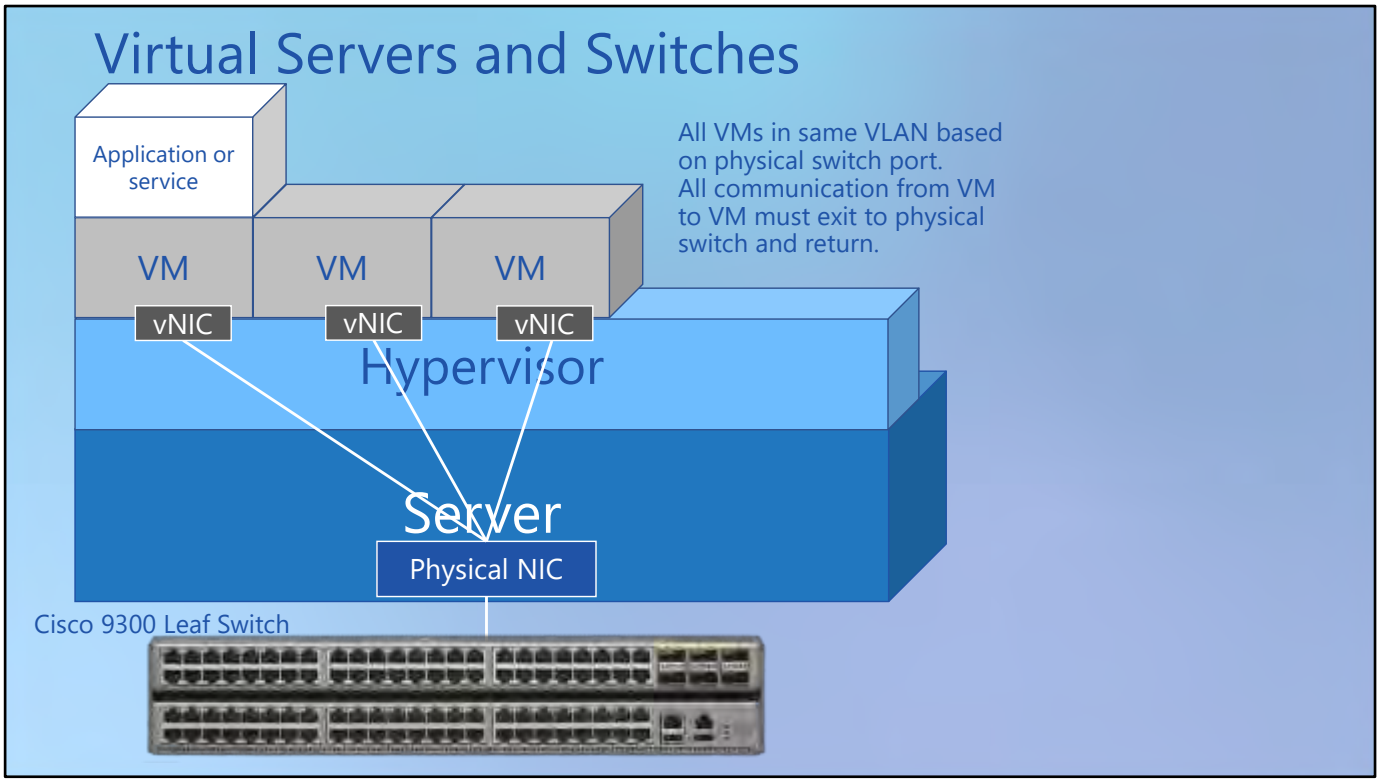
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



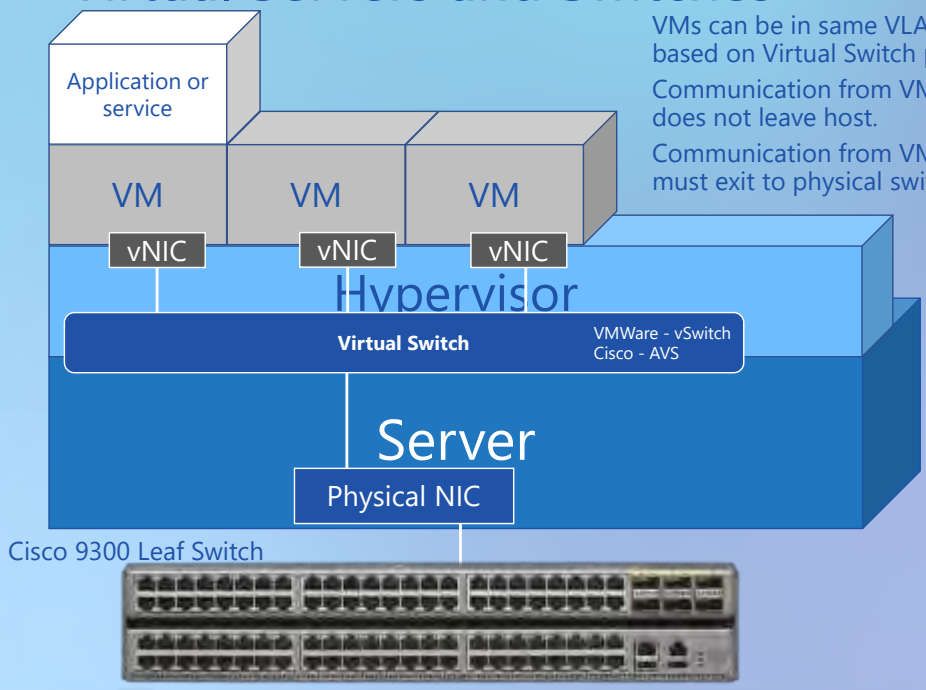
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Virtual Servers and Switches

VMs can be in same VLAN or different VLAN based on Virtual Switch port configuration

Communication from VM to VM in same VLAN does not leave host.

Communication from VM to VM in different VLAN must exit to physical switch and return.



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ENCOR Management Protocols and Services Preparation

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Network Time Protocol and Precision Time Protocol

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Synchronized Time

Why is synchronized time important?

Clock synchronization is critical for digital certificates

Event correlation & tracking

...and more!

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Manually Configuring Time

To set the time: By default it is set to UTC time.

```
R1#clock set 12:39:00 April 19 2019
R1#
*Apr 19 12:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:30:11 UTC Thu Apr
18 2019 to 12:39:00 UTC Fri Apr 19 2019, configured from console by console.
```

To set the timezone so clock is not displayed in UTC time:
Based on standard time.

```
R1(config)#clock timezone AST -4 0
R1(config)#
Apr 19 12:43:08.403: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:43:00 UTC Fri Apr
19 2019 to 08:43:08 AST Fri Apr 19 2019, configured from console by console.
```

To set the clock to auto adjust on daylight savings time:

```
R1(config)#clock summer-time ADT recurring 2 Sunday March 02:00 1 Sunday November 02:00
R1(config)#
Apr 19 12:45:08.239: %SYS-6-CLOCKUPDATE: System clock has been updated from 08:45:08 AST Fri Apr
19 2019 to 09:45:08 ADT Fri Apr 19 2019, configured from console by console.
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Network Time Protocol

- NTP is a protocol that Network Devices use to synchronize their time
- Uses UDP port 123
- NTP uses a Client / Server model
  - Stratum Levels 0-16
- NTP can use internal or external authoritative time sources such as:
  - Global NTP Server
  - GPS or Atomic Clock
  - Master clock (ie: Domain Controller)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

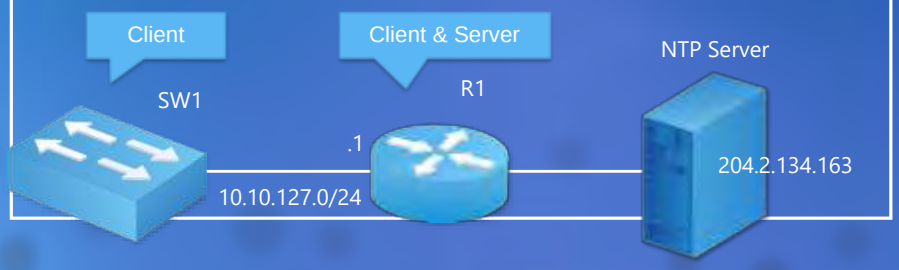
NTP Configuration

To make the router a client

```
R1(config)#ntp server 204.2.134.163
```

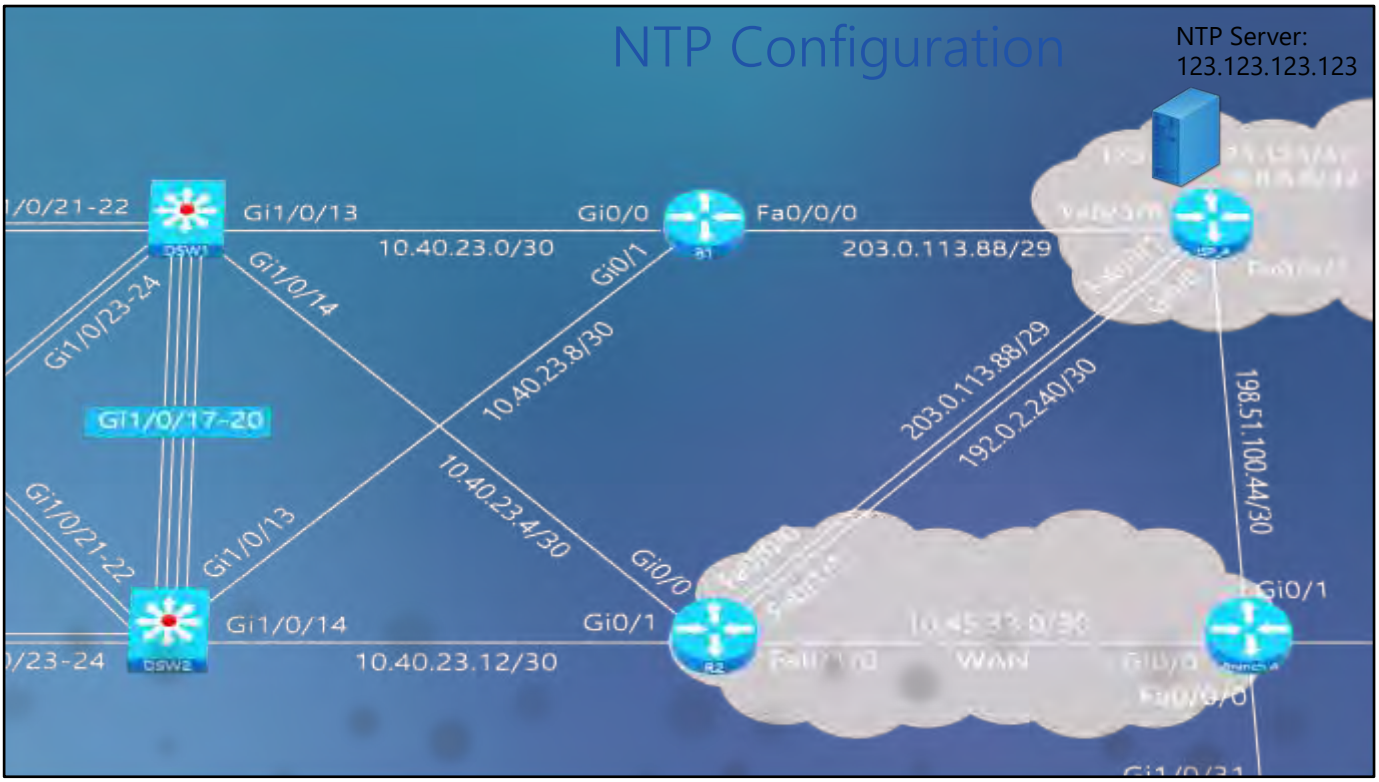
To make the router the authoritative source

```
R1(config)#ntp master
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NTP Configuration



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Precision Time Protocol (PTP)

Defined in IEEE 1588 as:

Precision Clock Synchronization

Designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead.

- Developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Precision Time Protocol (PTP)

Why?

PTP provides more accurate time synchronization vs NTP

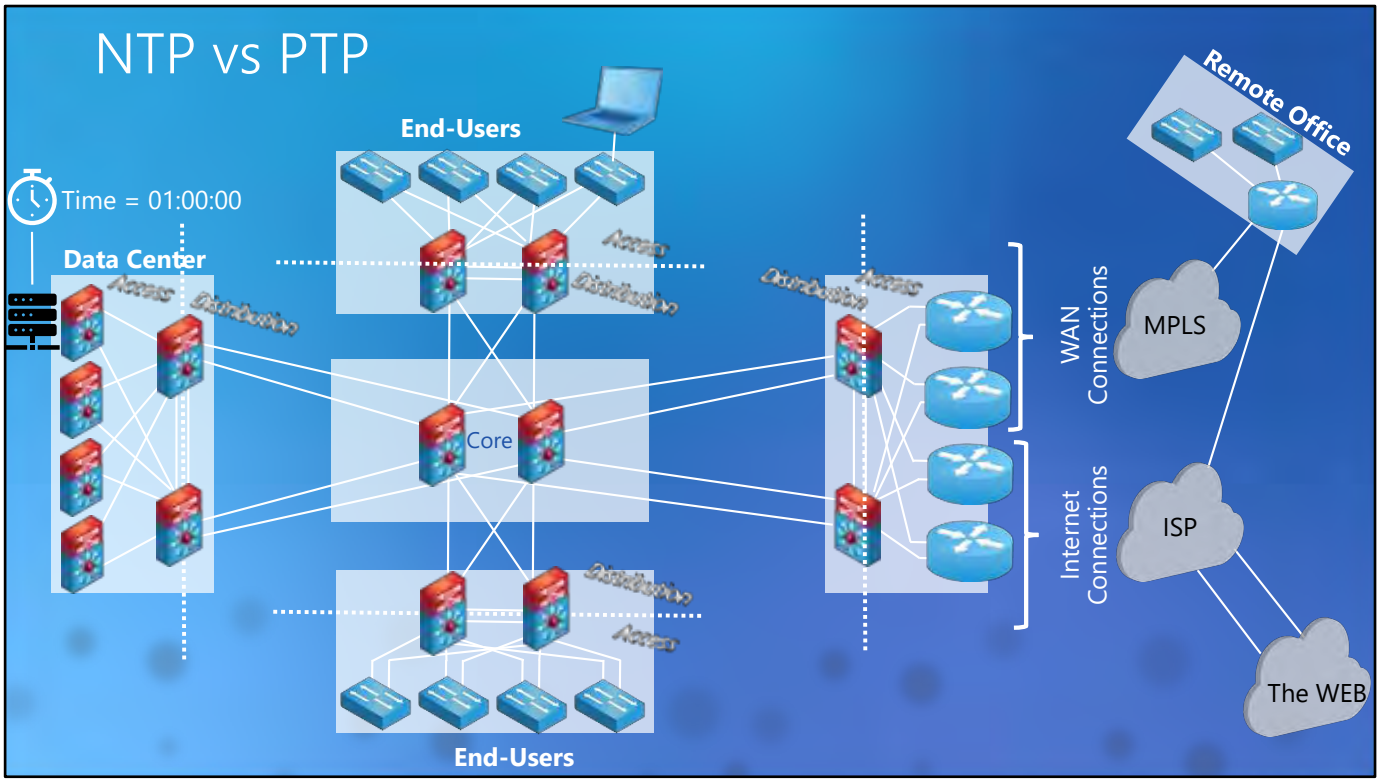
How?

By keeping track of the delay from the device providing time and the devices getting time

The devices getting time can then use this delay to modify the time so it is more accurate.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

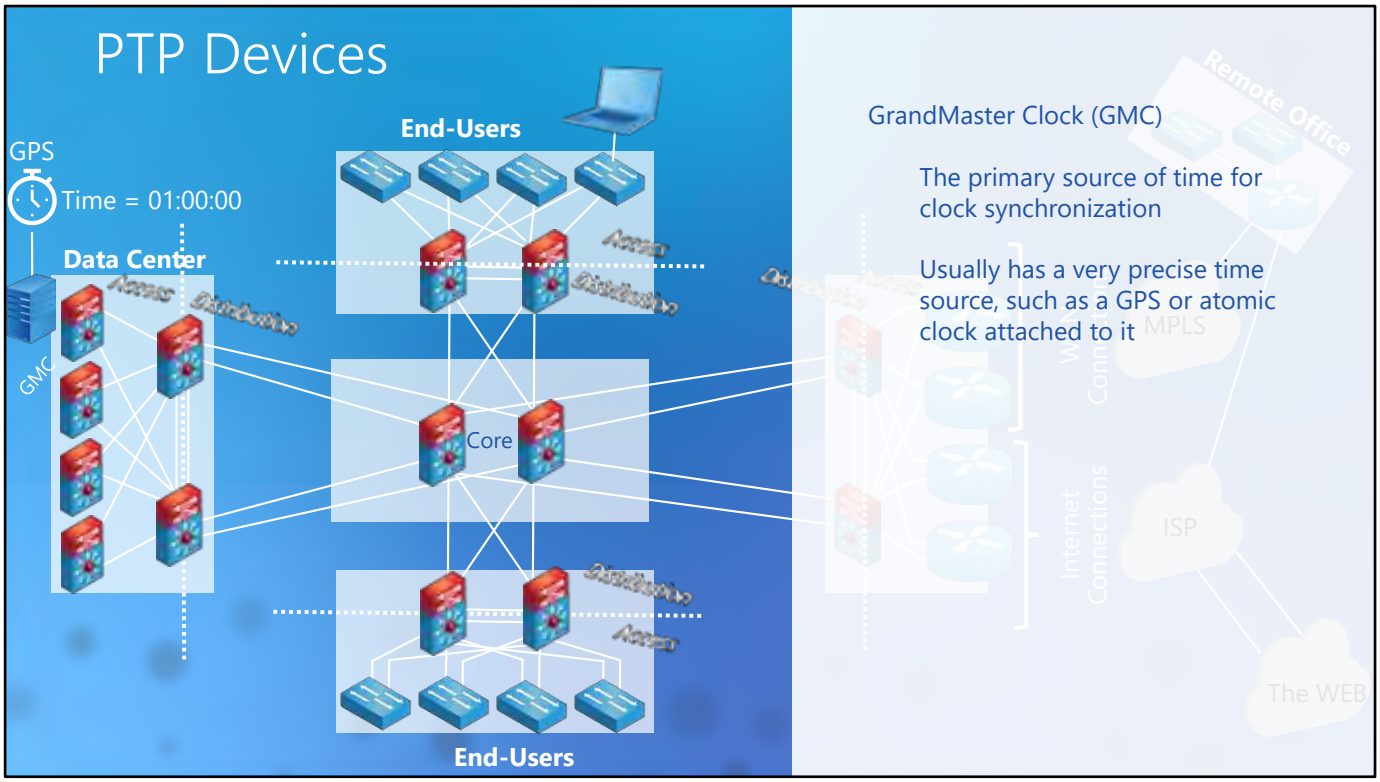


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

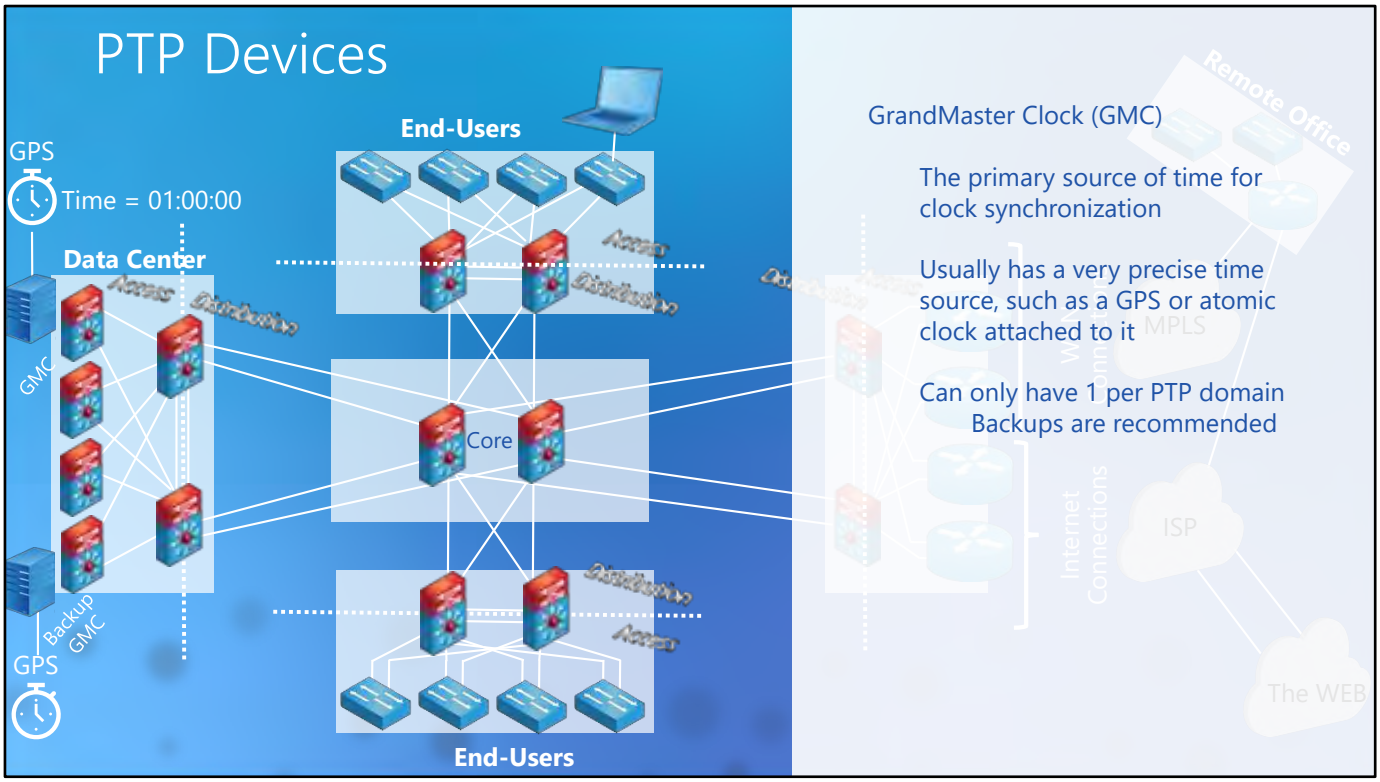
NTP vs PTP

Feature	PTP (Precision Time Protocol)	NTP (Network Time Protocol)
Accuracy	Sub-microsecond to nanosecond	Millisecond to sub-millisecond
Clock Synchronization	Highly precise synchronization	Moderate to good synchronization
Protocol Version	IEEE 1588-2008 (latest) (IEEE 1588 standard)	NTPv4 (latest) (IETF RFC 5905 standard)
Reference Clocks	Uses hardware timestamping	Uses software-based timestamping
Packet Timing	Timestamps Ethernet packets	Timestamps UDP packets
Topology	Master-slave architecture	Hierarchical client-server model
Clock Hierarchy	Support for clock hierarchy	Limited hierarchy support
Communication	Unicast and multicast modes	Primarily uses multicast and unicast
Convergence Time	Fast convergence for accurate time	Slower convergence, suitable for general timekeeping
Security	Limited security features	Provides some security mechanisms
Applications	Critical applications requiring ultra-precise timing (e.g., financial trading, industrial automation)	General network timekeeping, non-critical applications
Use Cases	Industrial automation, telecommunications, power grid management, audio/video production, financial markets	Network timekeeping, system clock synchronization
Hardware Requirements	Often requires hardware support for precision timestamping	Relatively less hardware-dependent
Complexity	More complex to implement	Simpler to implement and configure

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

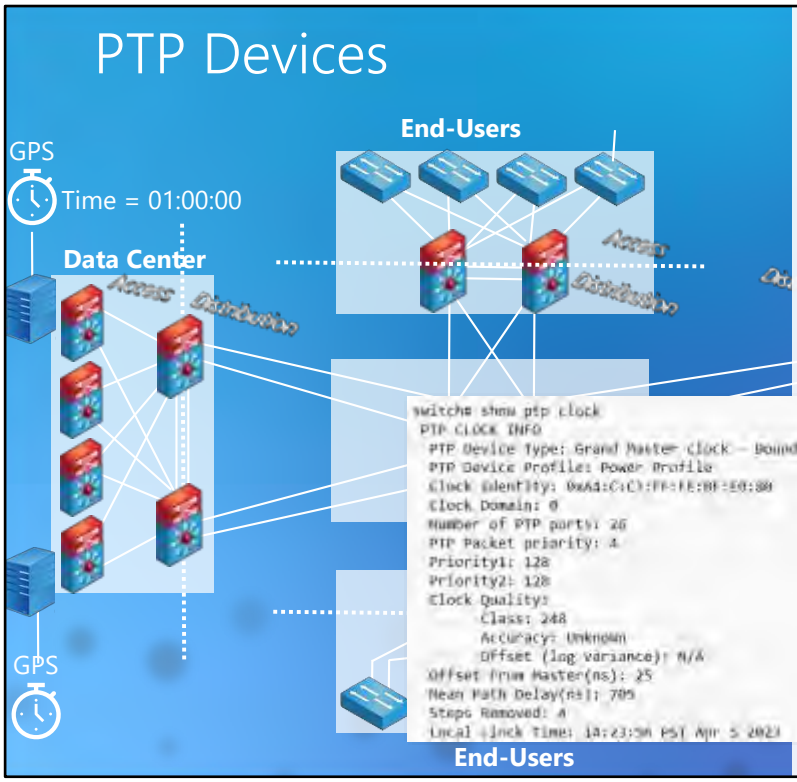


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

PTP Devices




```
switch# show ptp clock
 PTP CLOCK INFO
  PTP Device Type: Grand Master clock - Boundary clock
  PTP Device Profile: Power Profile
  Clock Identity: 0xA4:C1:C1:FF:FE:0F:E0:80
  Clock Domain: 0
  Number of PTP ports: 26
  PTP Packet priority: 4
  Priority1: 128
  Priority2: 128
  Clock Quality:
        Class: 248
        Accuracy: Unknown
        Offset (log variance): N/A
  Offset from Master(ns): 25
  Mean Path Delay(ns): 705
  Steps Removed: 4
  Local clock Time: 10:23:50 PST Apr 5 2023
```

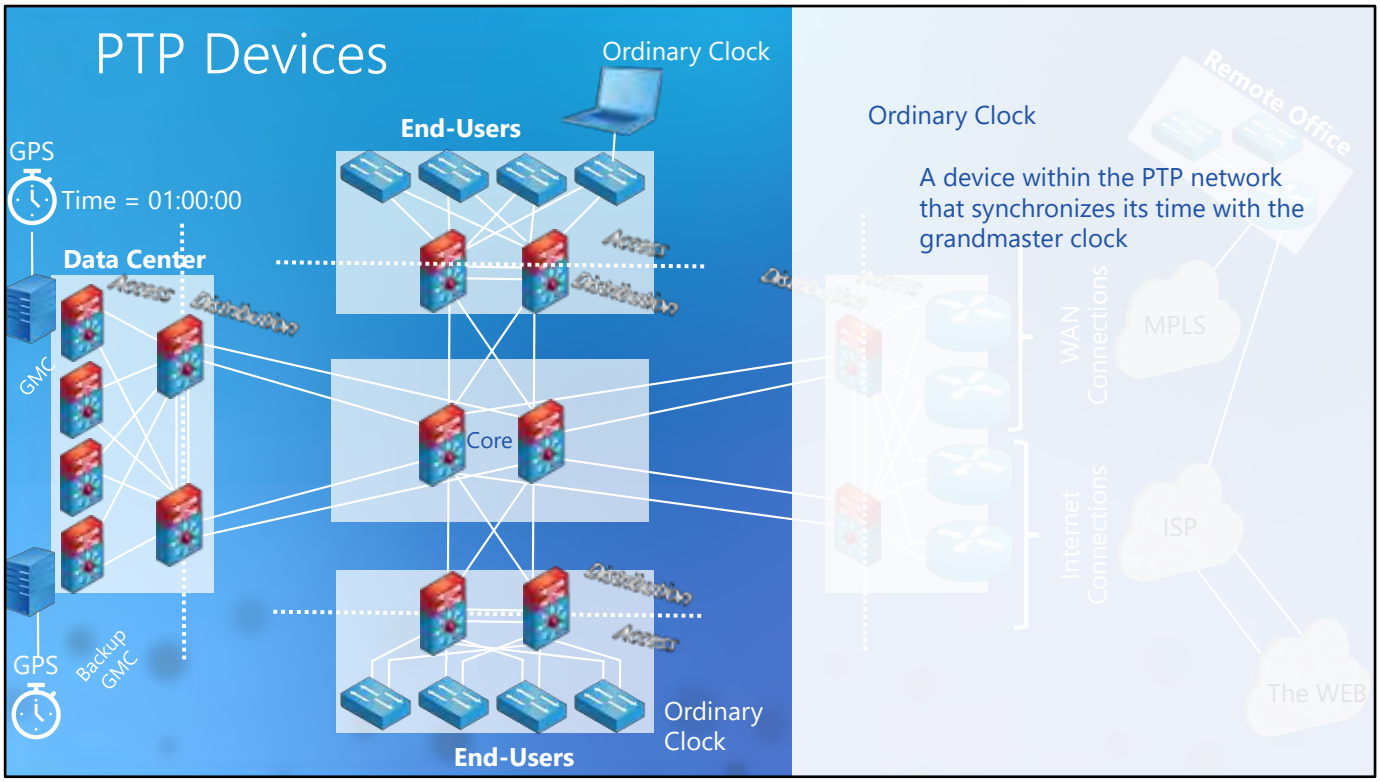
Best Master Clock Algorithm (BMCA)

Specifies how each clock on the network determines the best master clock in its subdomain of all the clocks it can see

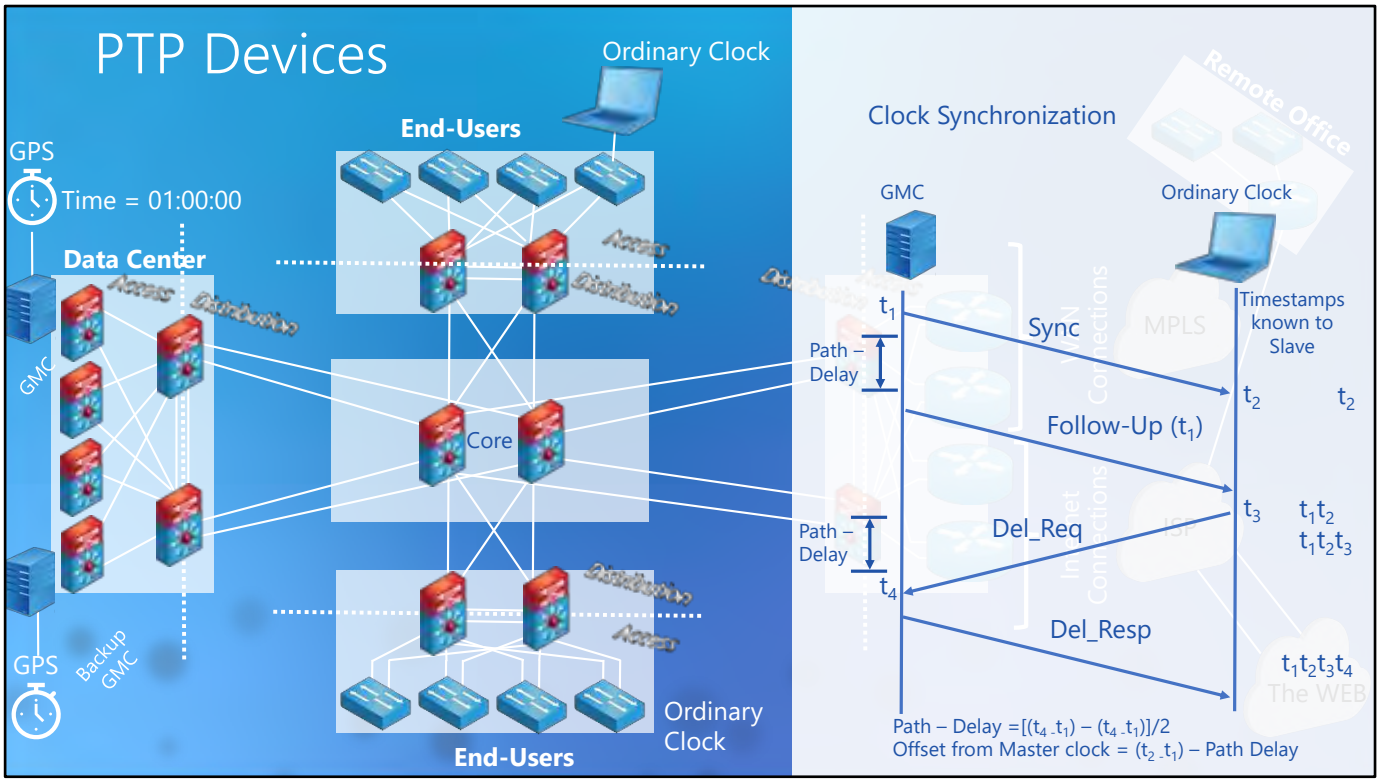
Decision Order

- Priority1
- Class
- Accuracy
- Variance
- Priority2
- Identity

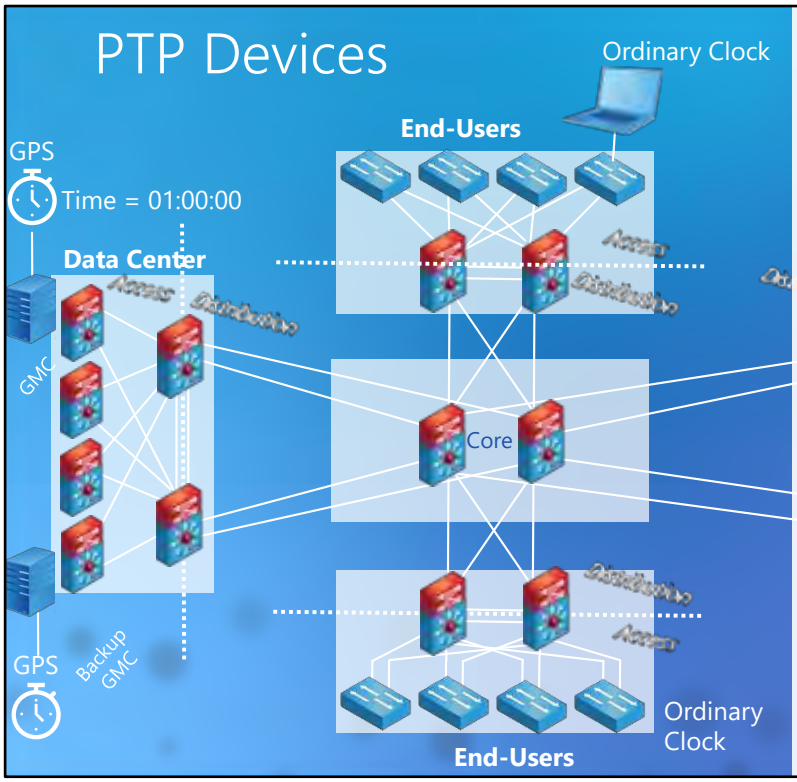
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



RECALL

PTP provides more accurate time synchronization vs NTP

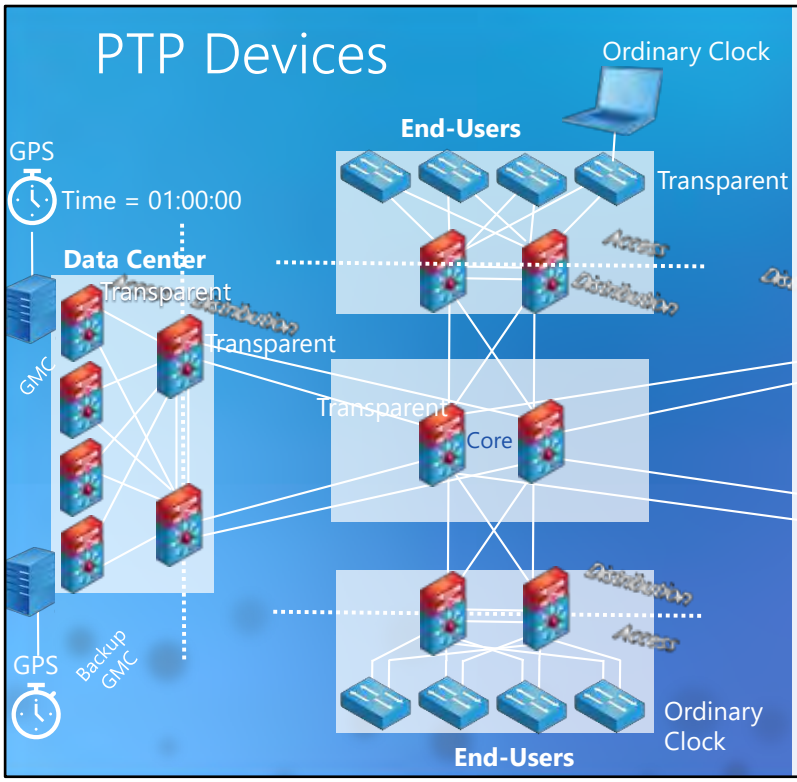
How?

By keeping track of the delay from the device providing time and the devices getting time

The devices getting time can then use this delay to modify the time so it is more accurate.

But how do the network devices in between affect time???

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Transparent Clock

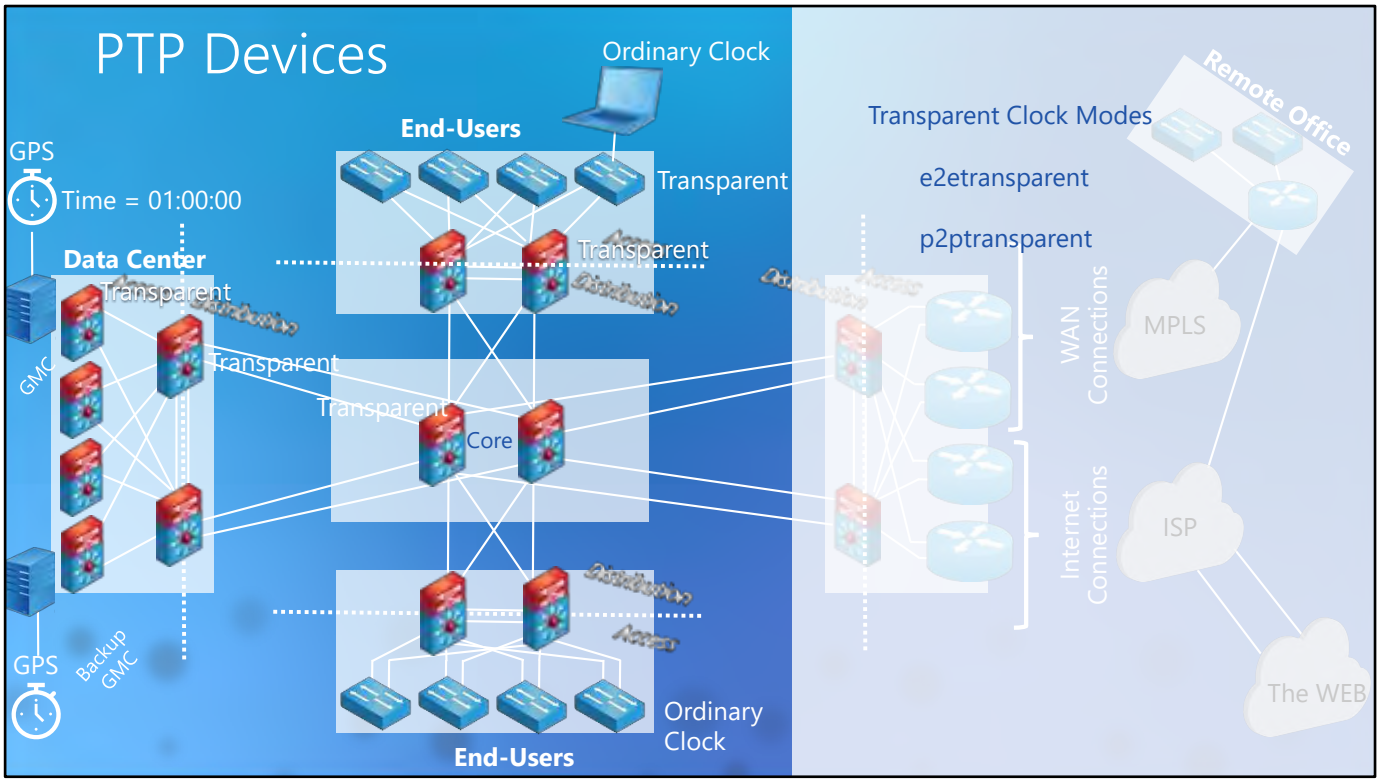
Your network devices

Typically operate in a two-step process:

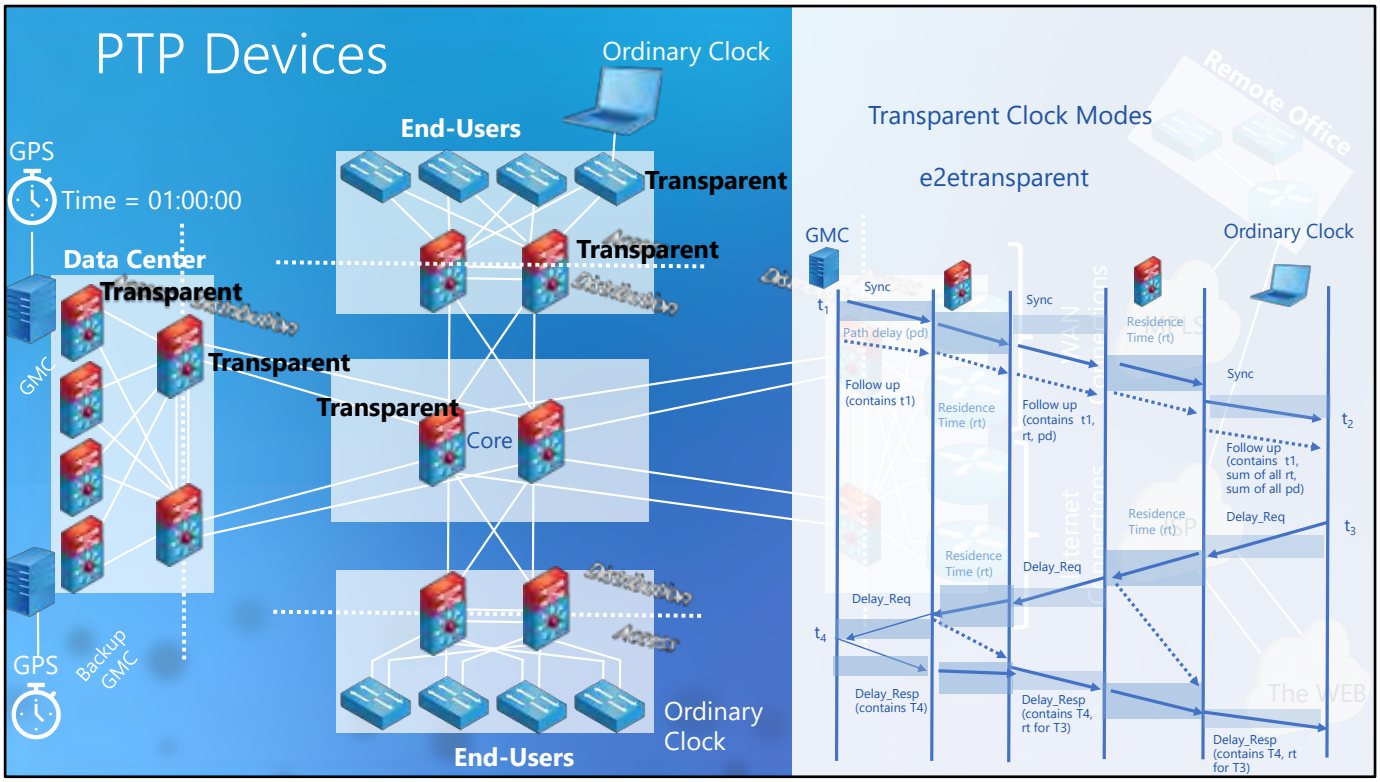
First, they measure the delay of incoming PTP packets and update the PTP packet with the additional measurements.

Second, they forward the packets with the updated measurements to the next hop in the network. This update compensates for switch delay and has an accuracy of within one picosecond

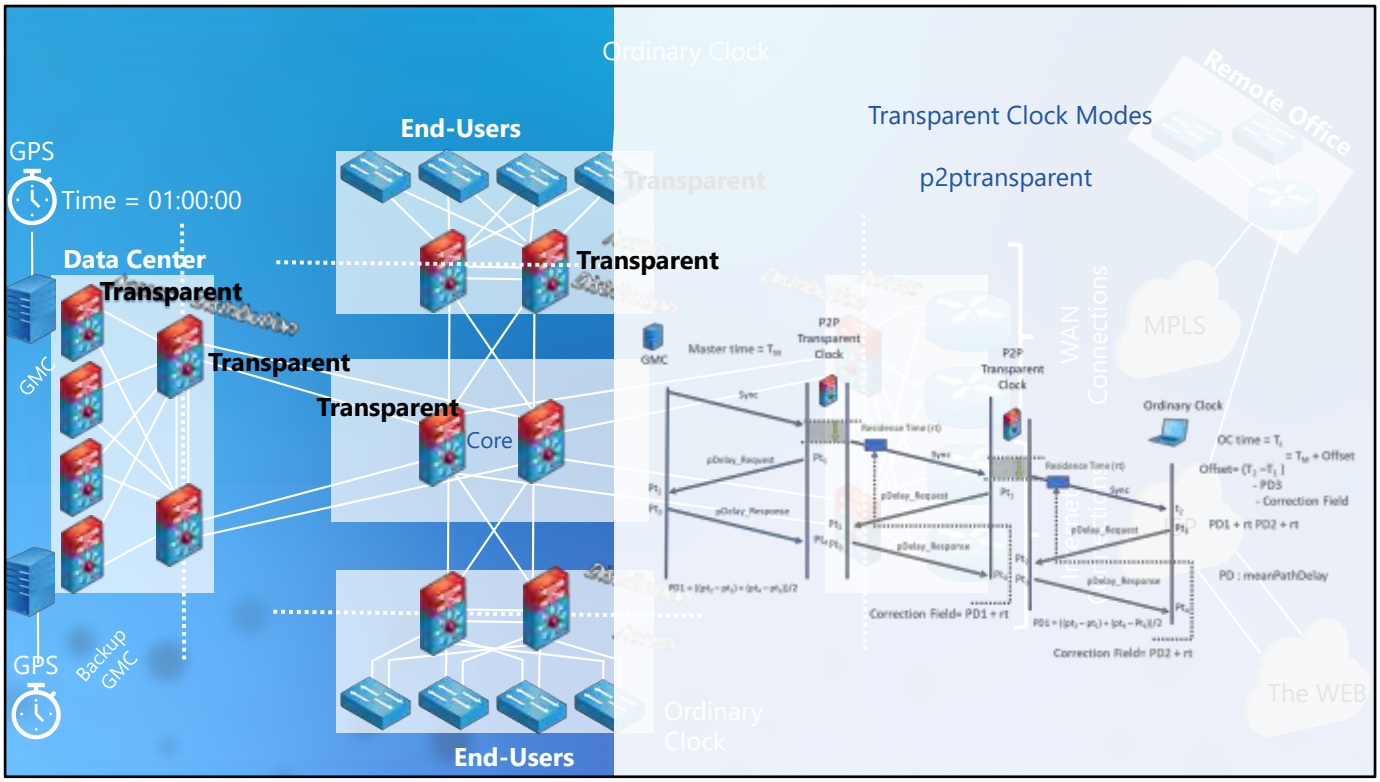
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



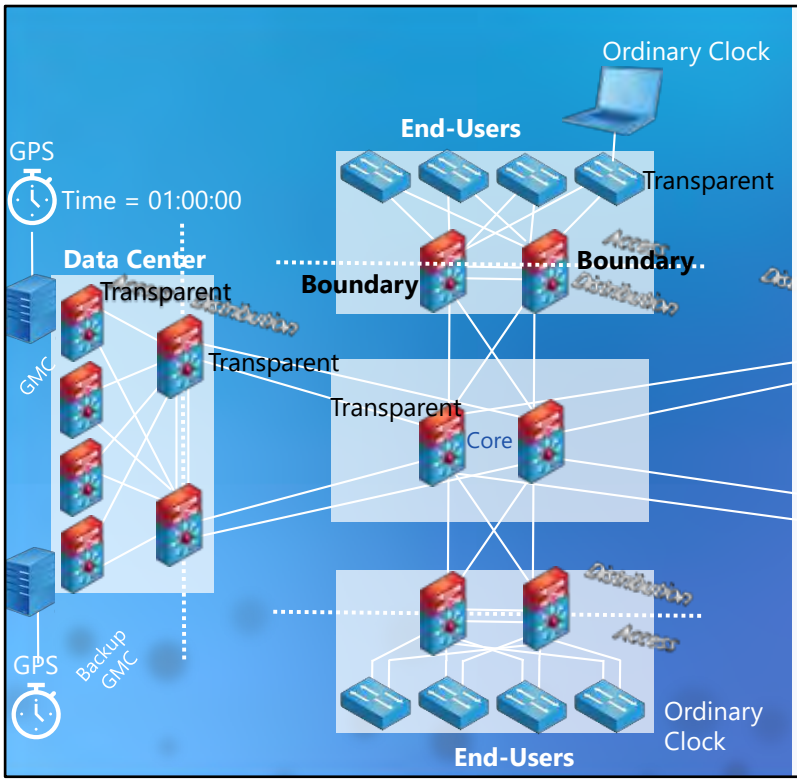
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Boundary Clock Mode

Your network devices

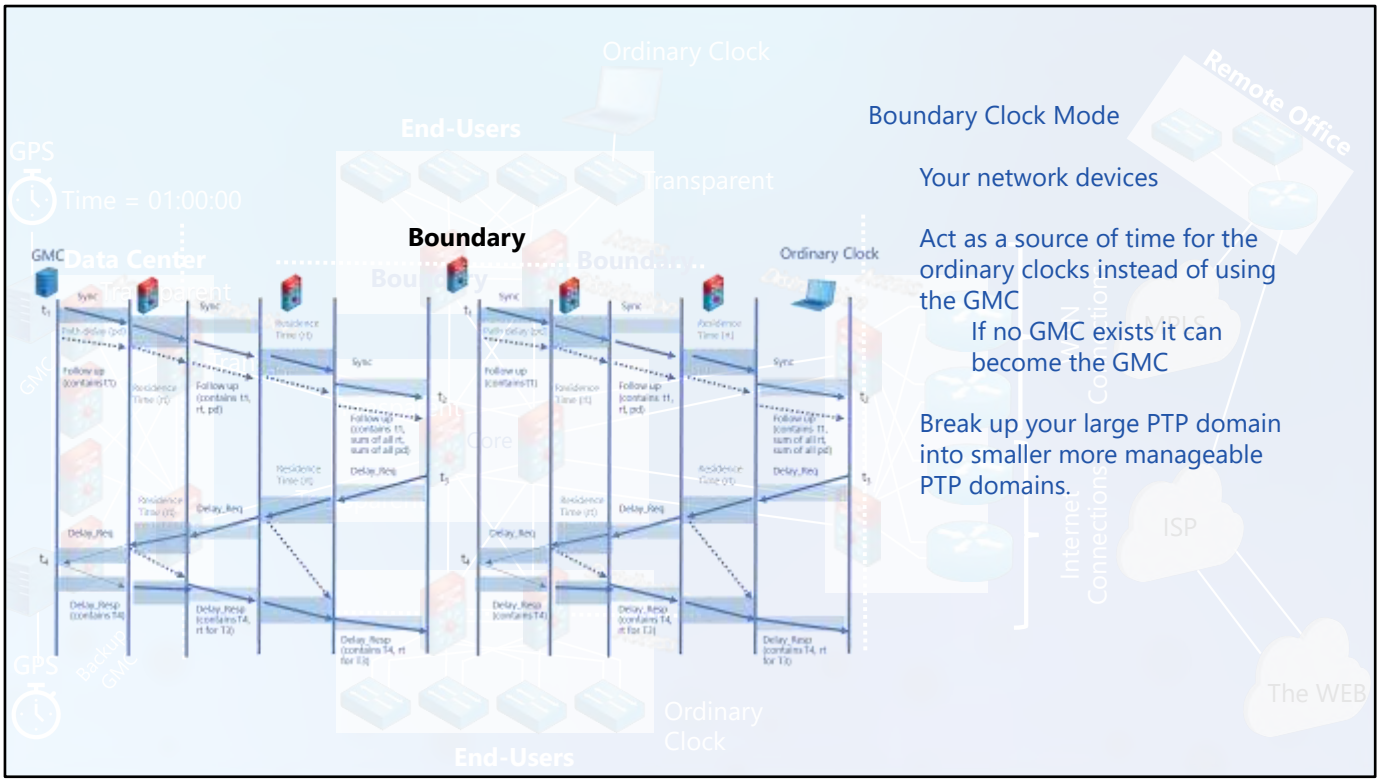
Act as a source of time for the ordinary clocks instead of using the GMC

If no GMC exists it can become the GMC

Break up your large PTP domain into smaller more manageable PTP domains.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



Boundary Clock Mode

Your network devices

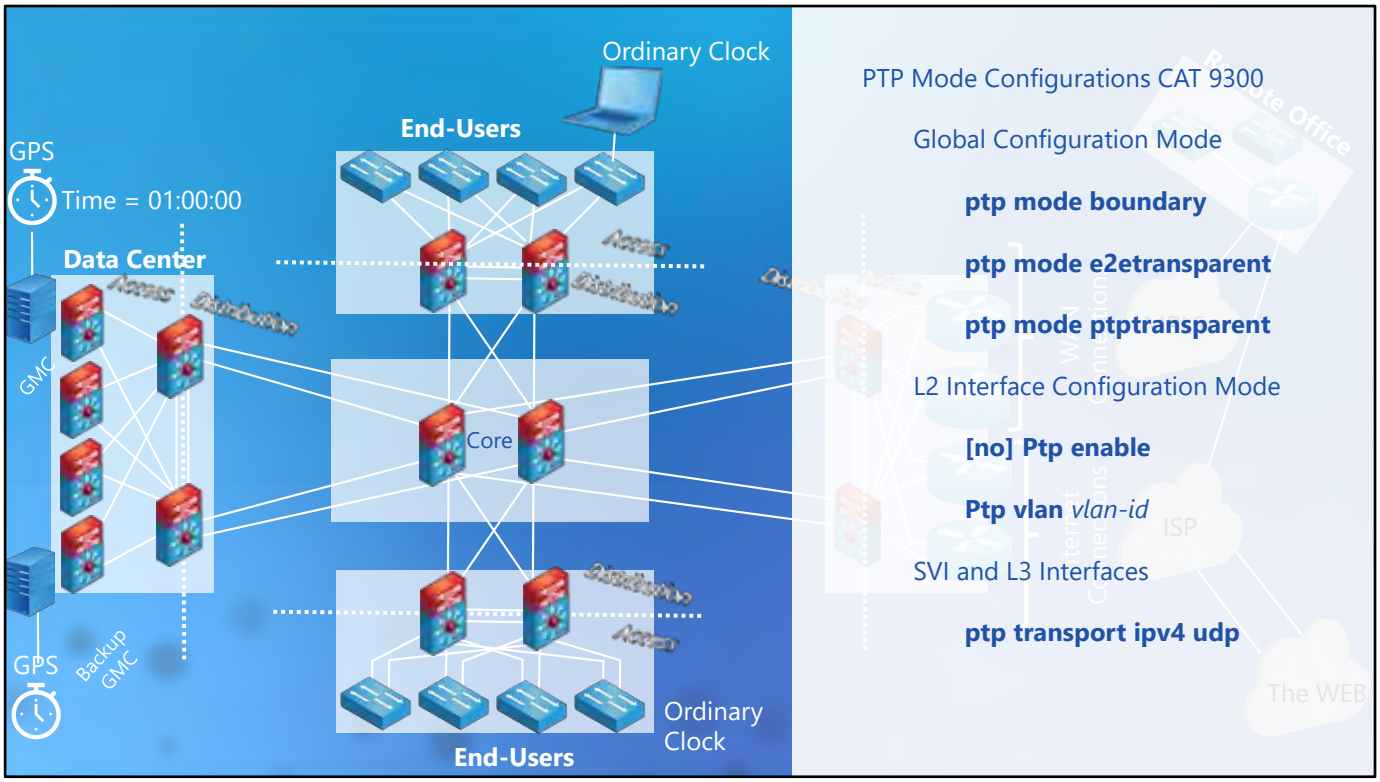
Act as a source of time for the ordinary clocks instead of using the GMC

If no GMC exists it can become the GMC

Break up your large PTP domain into smaller more manageable PTP domains.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SPAN, RSPAN, ERSPAN Configuration and Verification

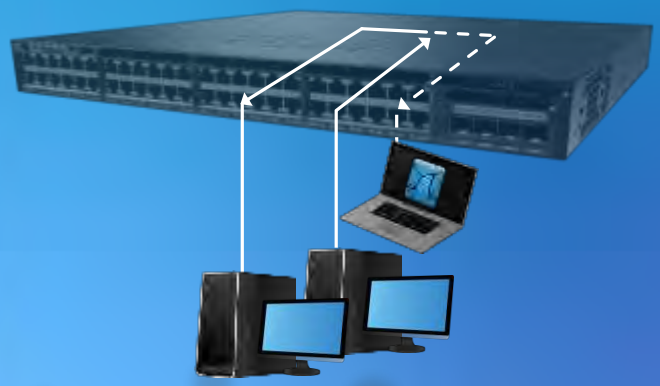
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SPAN/RSPAN/ERSPAN

- Tools that capture traffic entering or exiting a switchport
- Captured traffic is copied
- Copied traffic is sent to a destination
  - Where a packet capture device is connected
- Original traffic is forwarded normally

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SPAN

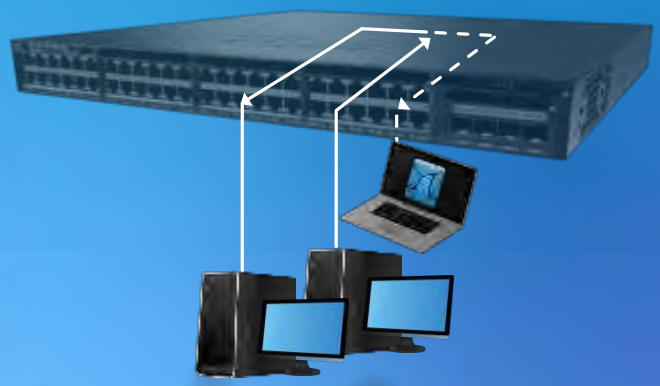


A tool for capturing traffic and sending a copy of it to another port on the same device

- All sources and destinations are on the same switch

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SPAN



Source

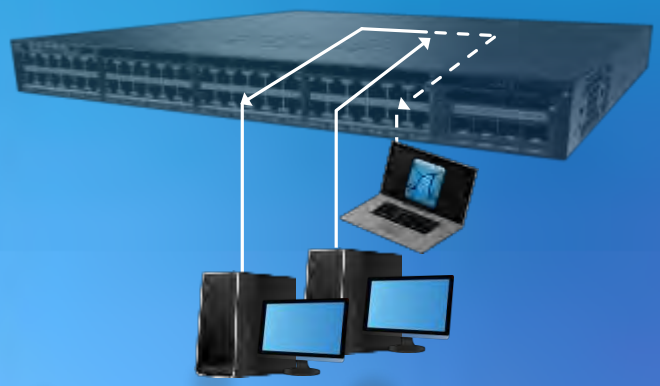
Traffic captured can be:

ingress and/or egress on multiple ports

access or trunk for an entire vlan

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SPAN

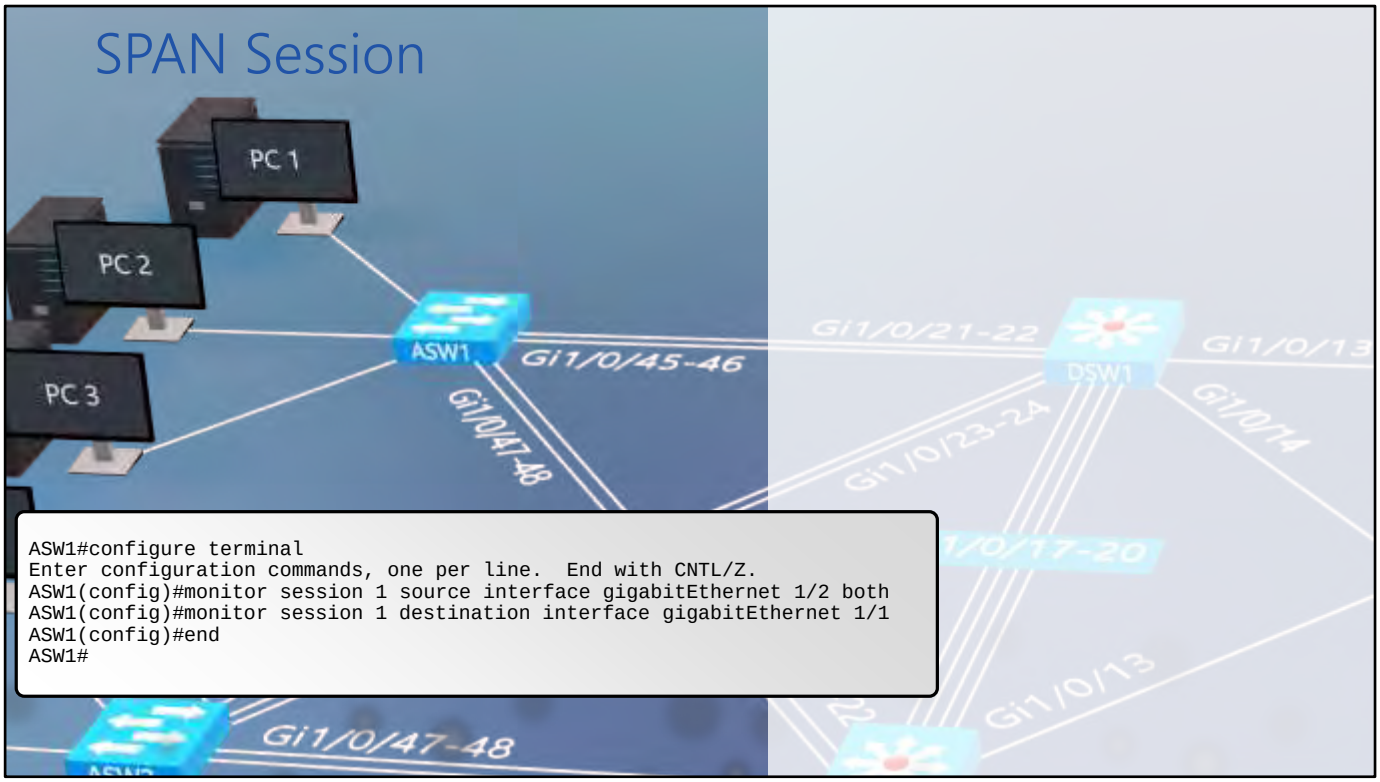


Destination

- A port connected to a device with software that can capture packets (WireShark)
  - Interface is Up/Down
  - Status is listed as monitored

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SPAN Session

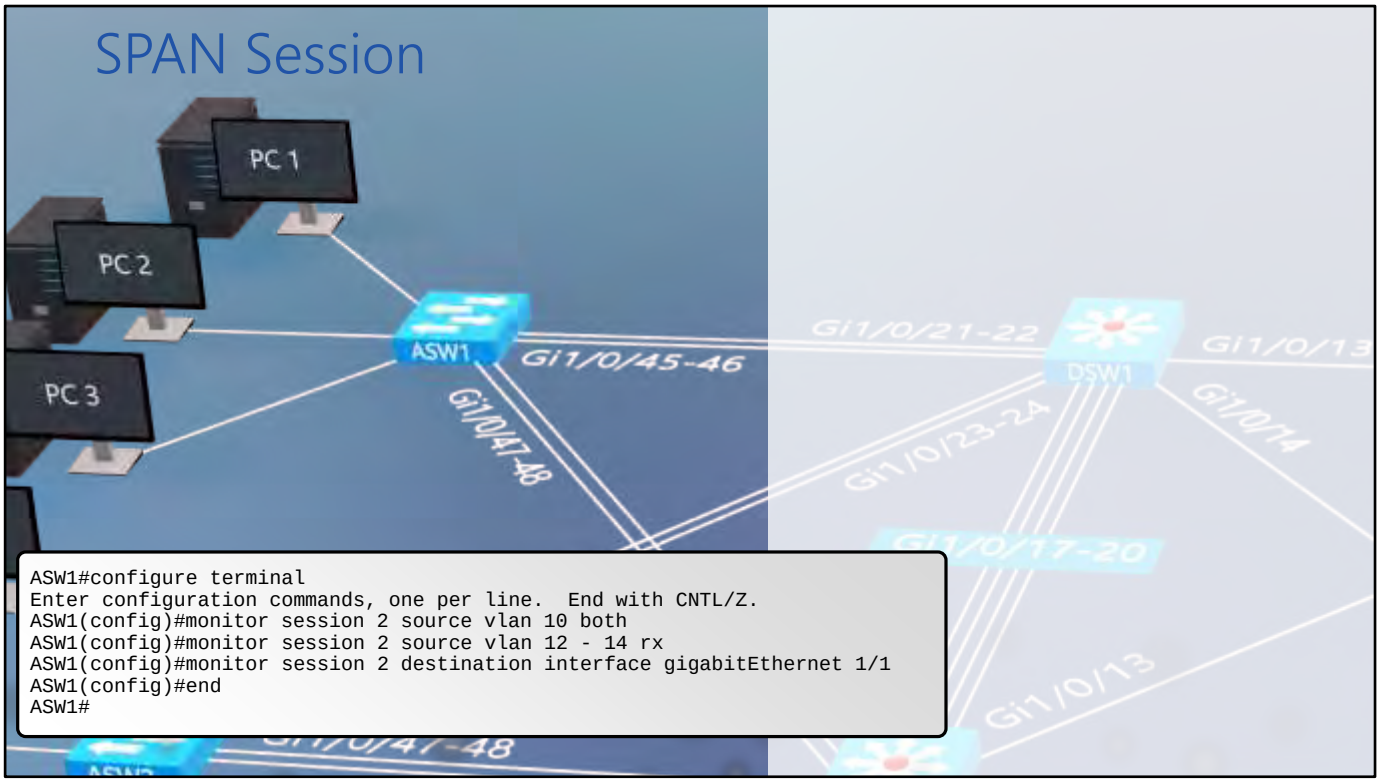



```
ASW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ASW1(config)#monitor session 1 source interface gigabitEthernet 1/2 both
ASW1(config)#monitor session 1 destination interface gigabitEthernet 1/1
ASW1(config)#end
ASW1#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

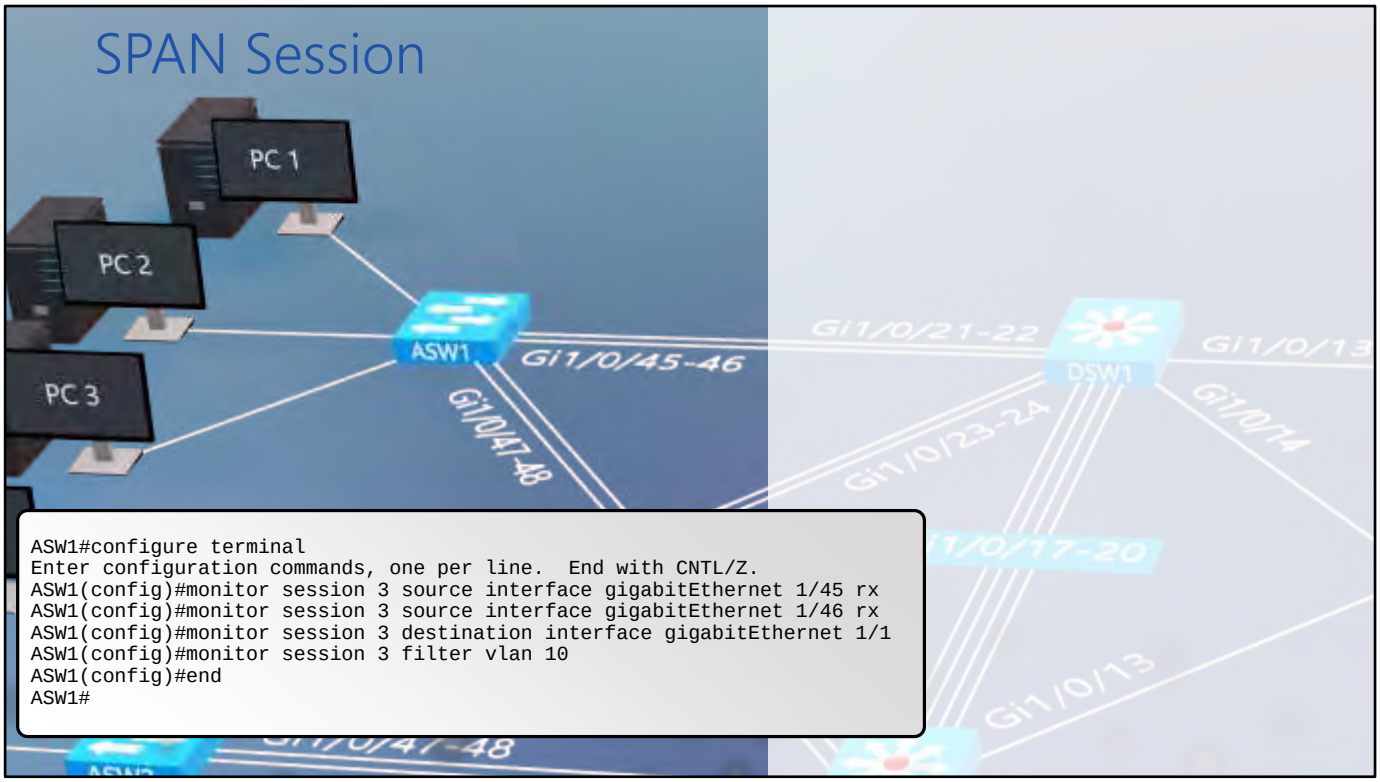
SPAN Session




```
ASW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ASW1(config)#monitor session 2 source vlan 10 both
ASW1(config)#monitor session 2 source vlan 12 - 14 rx
ASW1(config)#monitor session 2 destination interface gigabitEthernet 1/1
ASW1(config)#end
ASW1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

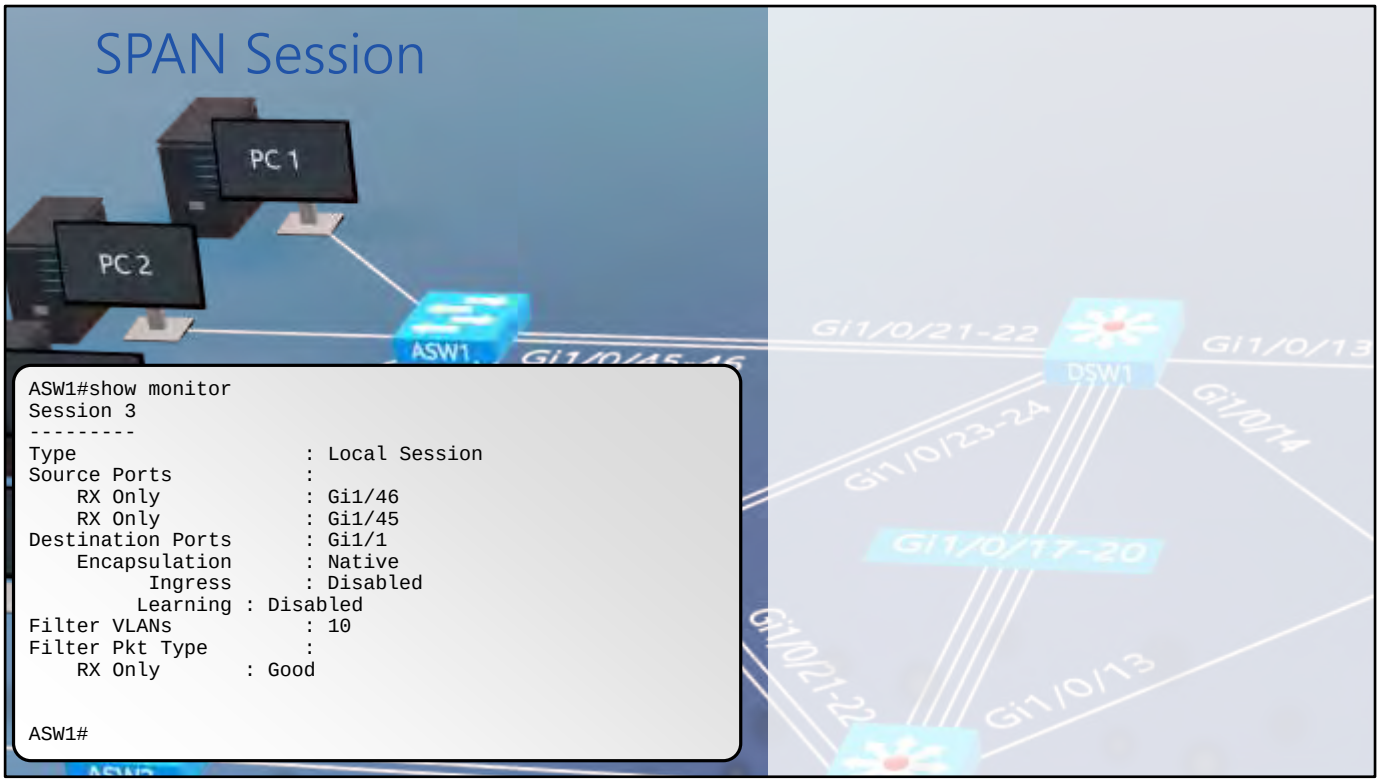
SPAN Session




```
ASW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ASW1(config)#monitor session 3 source interface gigabitEthernet 1/45 rx
ASW1(config)#monitor session 3 source interface gigabitEthernet 1/46 rx
ASW1(config)#monitor session 3 destination interface gigabitEthernet 1/1
ASW1(config)#monitor session 3 filter vlan 10
ASW1(config)#end
ASW1#
```

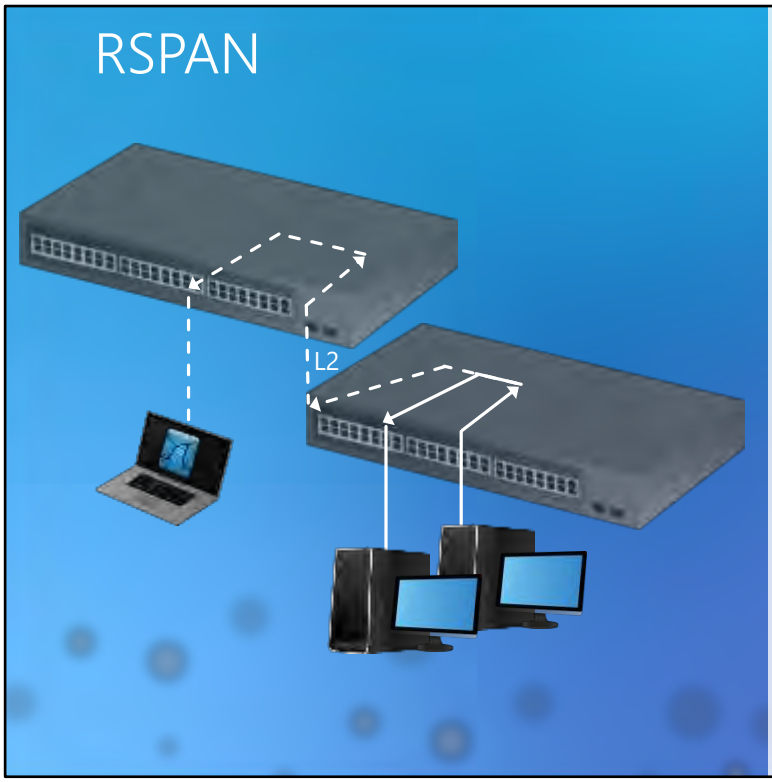
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SPAN Session




```
ASW1#show monitor
Session 3
---------
Type                    : Local Session
Source Ports            :
    RX Only             : Gi1/46
    RX Only             : Gi1/45
Destination Ports       : Gi1/1
    Encapsulation       : Native
          Ingress       : Disabled
         Learning : Disabled
Filter VLANs            : 10
Filter Pkt Type         :
    RX Only       : Good


ASW1#
```

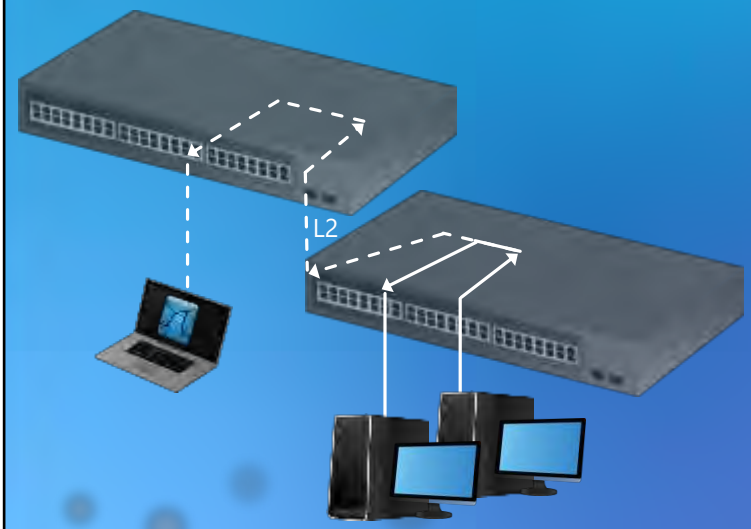
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



A tool for capturing traffic and sending a copy of it to another port on a different device across a L2 link

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RSPAN



Source

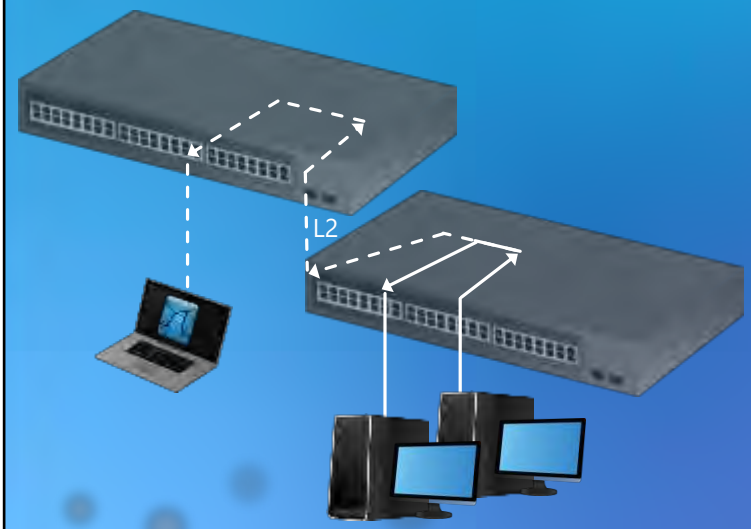
Traffic captured can be:

Ingress and/or egress on multiple ports

Access or trunk for an entire vlan

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RSPAN



Destination

- A port connected to a device with software that can capture packets (WireShark)
  - Interface is Up/Down
  - Status is listed as monitored

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RSPAN Session

RSPAN Session

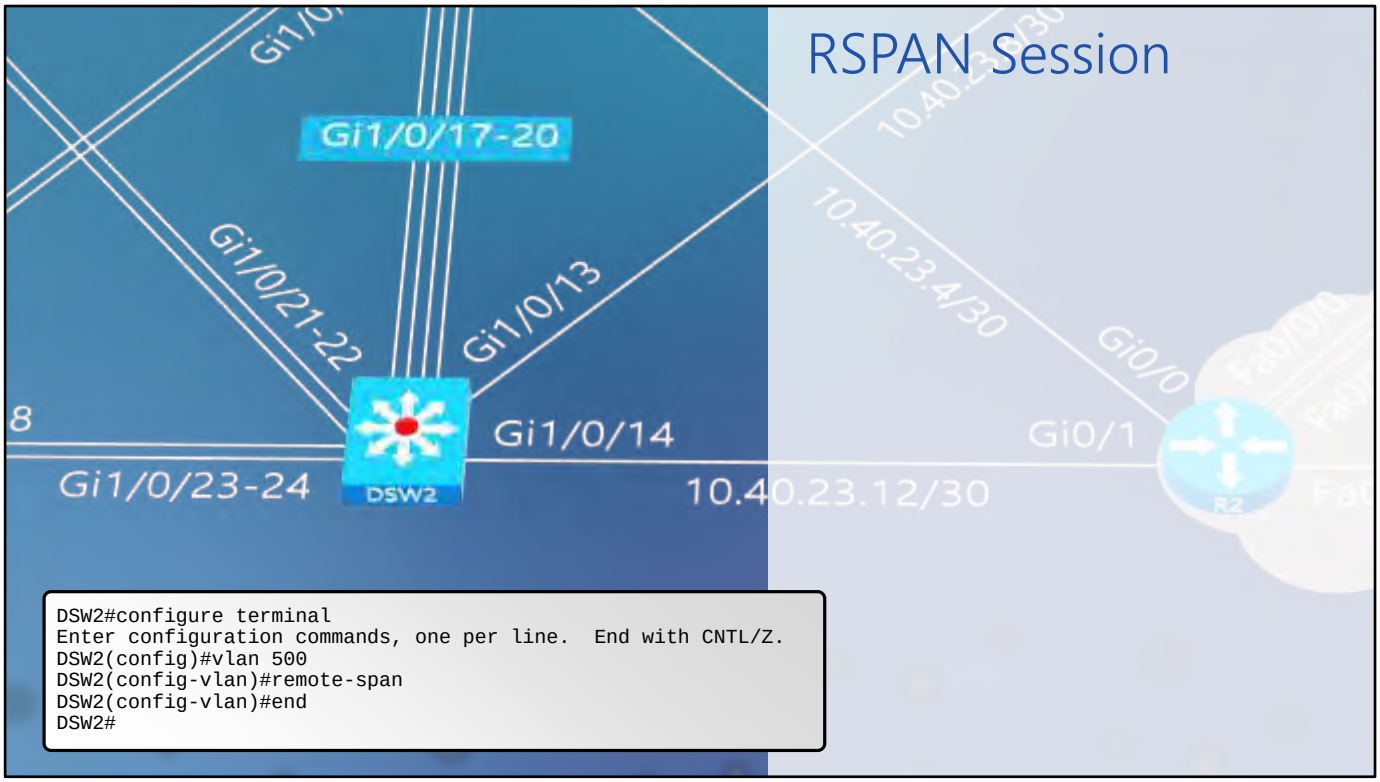
```
ASW1(config)#vlan 421
ASW1(config-vlan)#remote-span
ASW1(config-vlan)#do sho int status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      connected    421        a-full a-1000 10/100/1000BaseTX
Gi1/0/2                      connected    421        a-full a-1000 10/100/1000BaseTX
Gi1/0/3                      connected    1          a-full a-1000 10/100/1000BaseTX
Gi1/0/4                      notconnect   1            auto   auto 10/100/1000BaseTX
...output omitted...

*Jan 16 06:16:38.401: %PM-4-INACTIVE: putting Gi1/0/1 in inactive state because access VLAN is remote SPAN VLAN
*Jan 16 06:16:38.401: %PM-4-INACTIVE: putting Gi1/0/2 in inactive state because access VLAN is remote SPAN VLAN

ASW1(config)#do sho int status

Port      Name               Status       Vlan       Duplex  Speed Type
Gi1/0/1                      inactive     421        a-full a-1000 10/100/1000BaseTX
Gi1/0/2                      inactive     421        a-full a-1000 10/100/1000BaseTX
Gi1/0/3                      connected    1          a-full a-1000 10/100/1000BaseTX
Gi1/0/4                      notconnect   1            auto   auto 10/100/1000BaseTX
...output omitted...
```

```
ASW2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ASW2(config)#vlan 500
ASW2(config-vlan)#remote-span
ASW2(config-vlan)#exit
ASW2(config)#monitor session 1 source interface gig 1/1
ASW2(config)#monitor session 1 destination remote vlan 500
ASW2(config)#end
ASW2#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

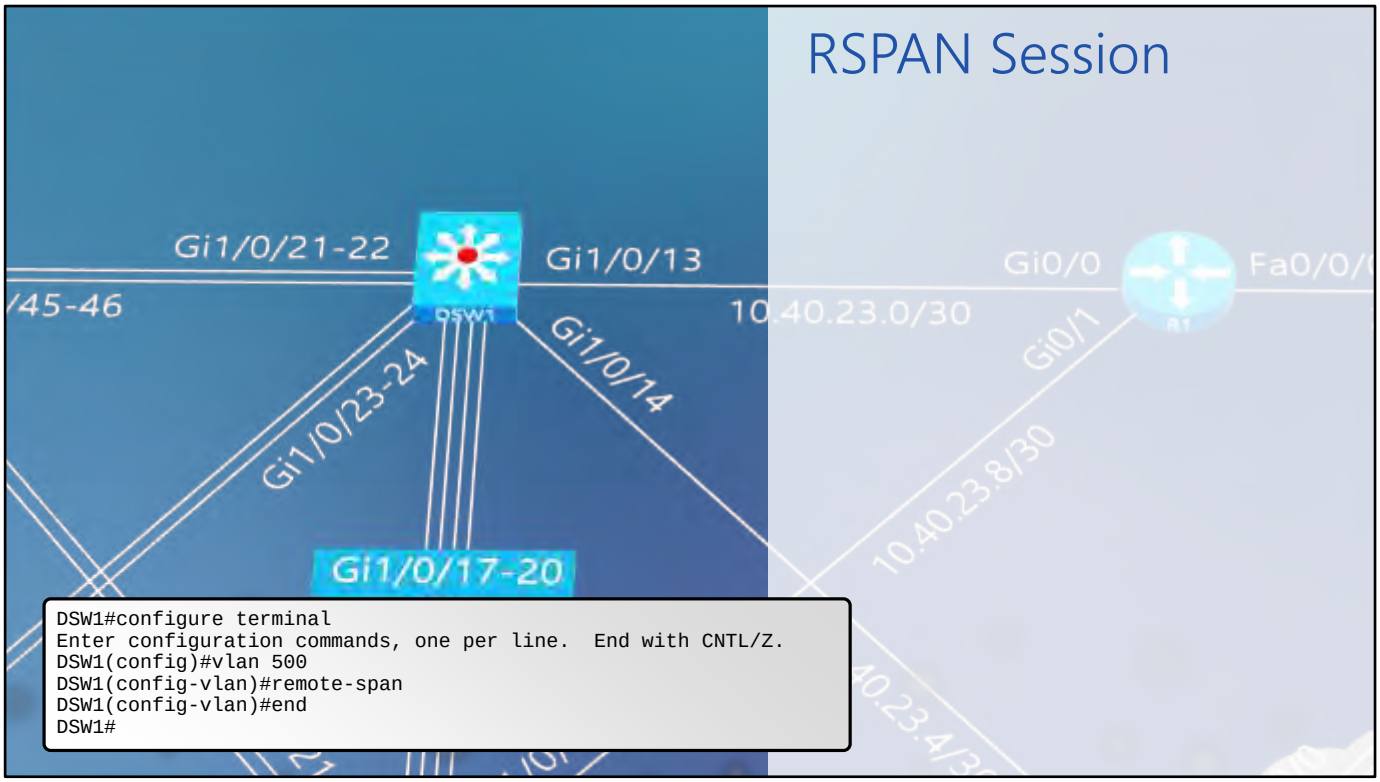
RSPAN Session




```
DSW2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DSW2(config)#vlan 500
DSW2(config-vlan)#remote-span
DSW2(config-vlan)#end
DSW2#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

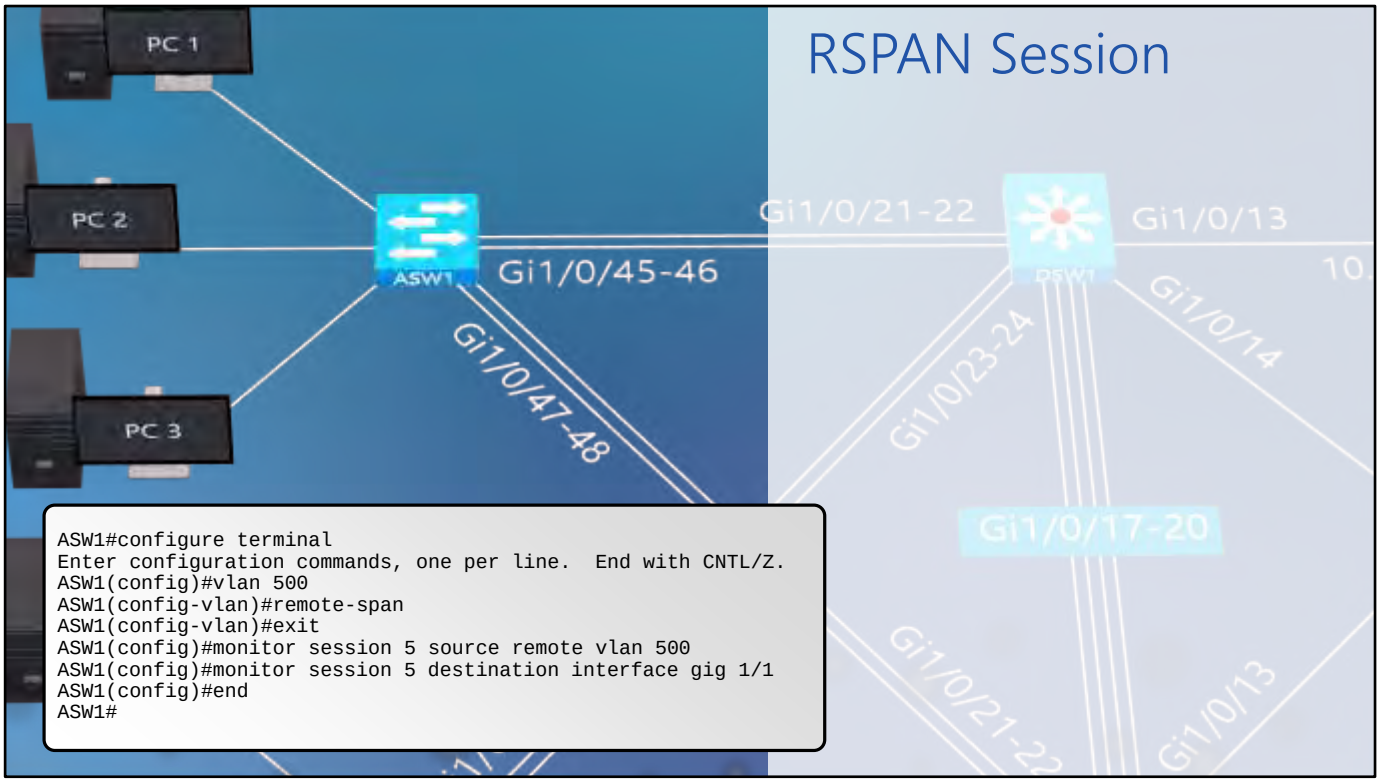
RSPAN Session




```
DSW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DSW1(config)#vlan 500
DSW1(config-vlan)#remote-span
DSW1(config-vlan)#end
DSW1#
```

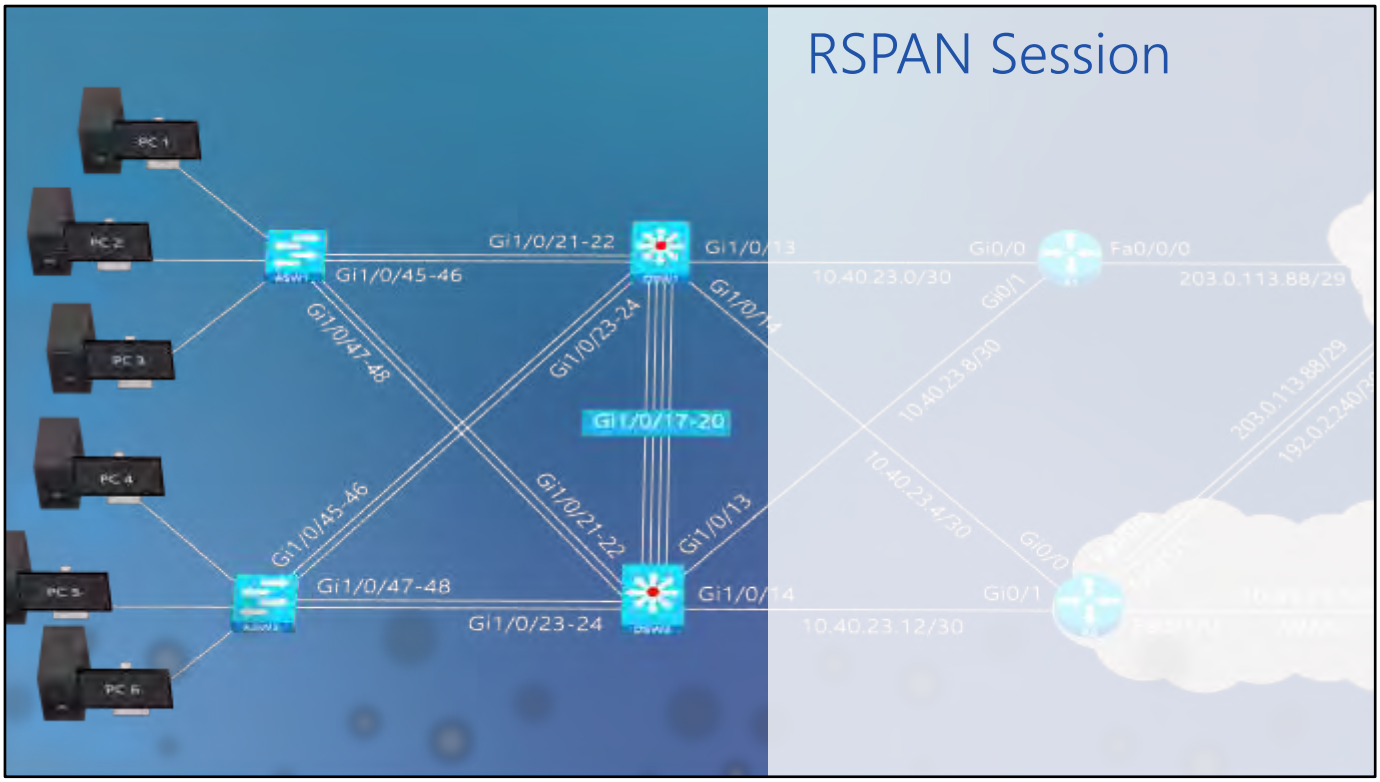
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RSPAN Session



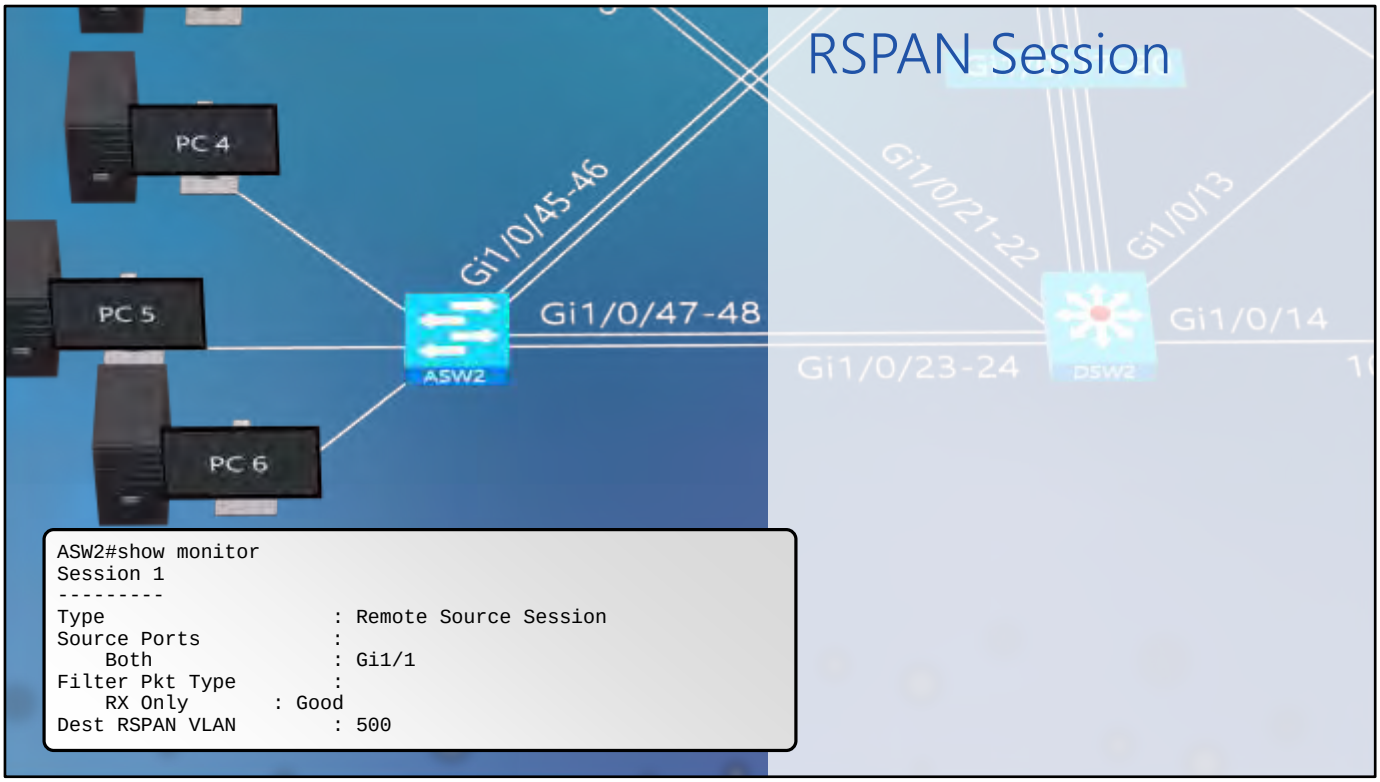

```
ASW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ASW1(config)#vlan 500
ASW1(config-vlan)#remote-span
ASW1(config-vlan)#exit
ASW1(config)#monitor session 5 source remote vlan 500
ASW1(config)#monitor session 5 destination interface gig 1/1
ASW1(config)#end
ASW1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

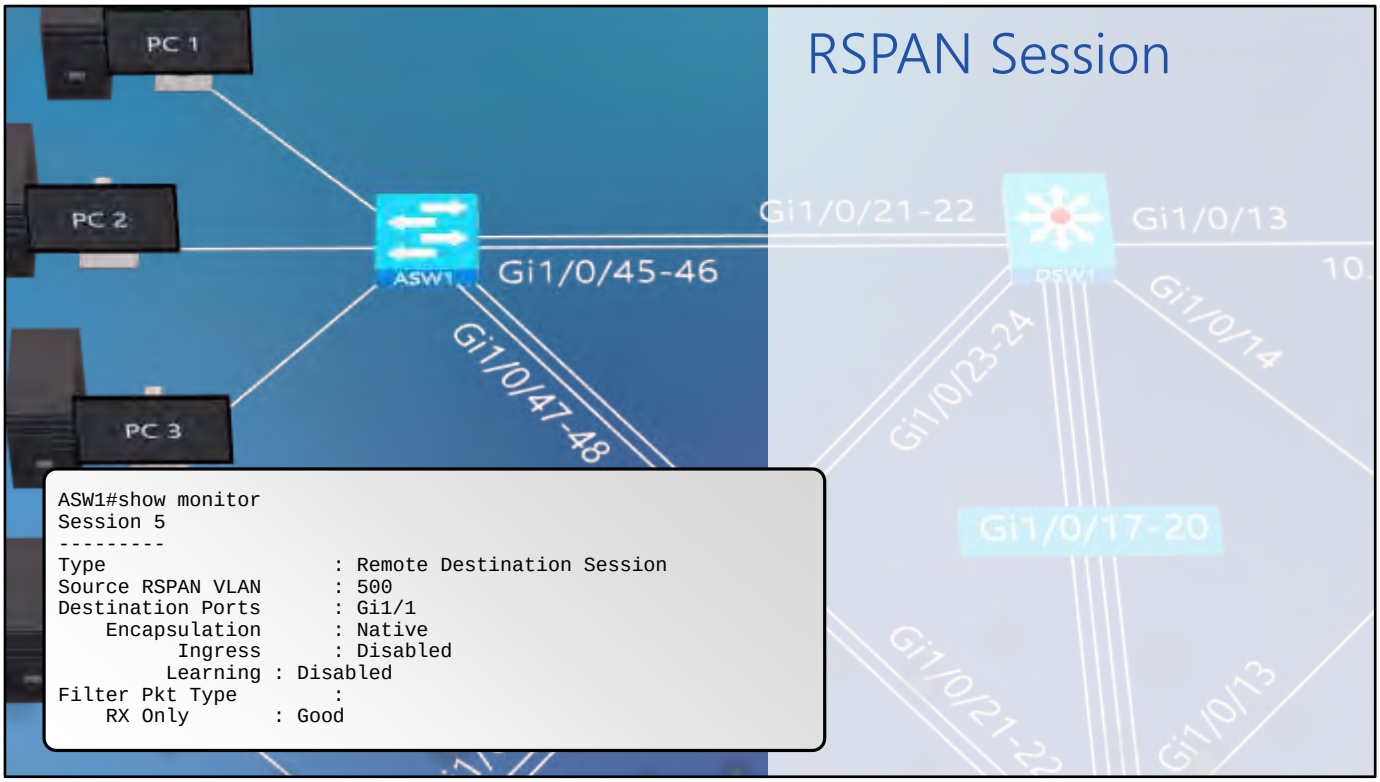
RSPAN Session




```
ASW2#show monitor
Session 1
---------
Type                    : Remote Source Session
Source Ports            :
    Both                : Gi1/1
Filter Pkt Type         :
    RX Only        : Good
Dest RSPAN VLAN         : 500
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

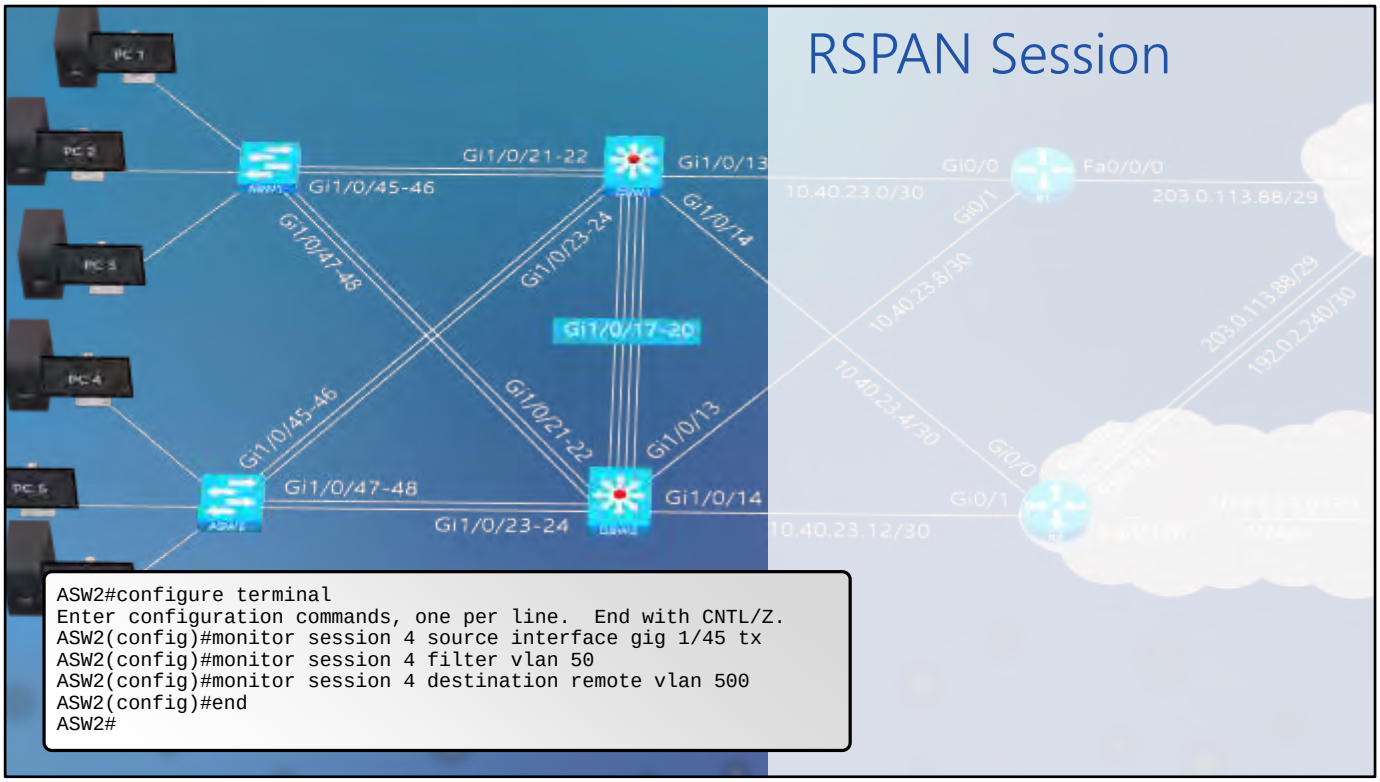
RSPAN Session




```
ASW1#show monitor
Session 5
---------
Type                    : Remote Destination Session
Source RSPAN VLAN       : 500
Destination Ports       : Gi1/1
    Encapsulation       : Native
          Ingress       : Disabled
         Learning : Disabled
Filter Pkt Type         :
    RX Only        : Good
```

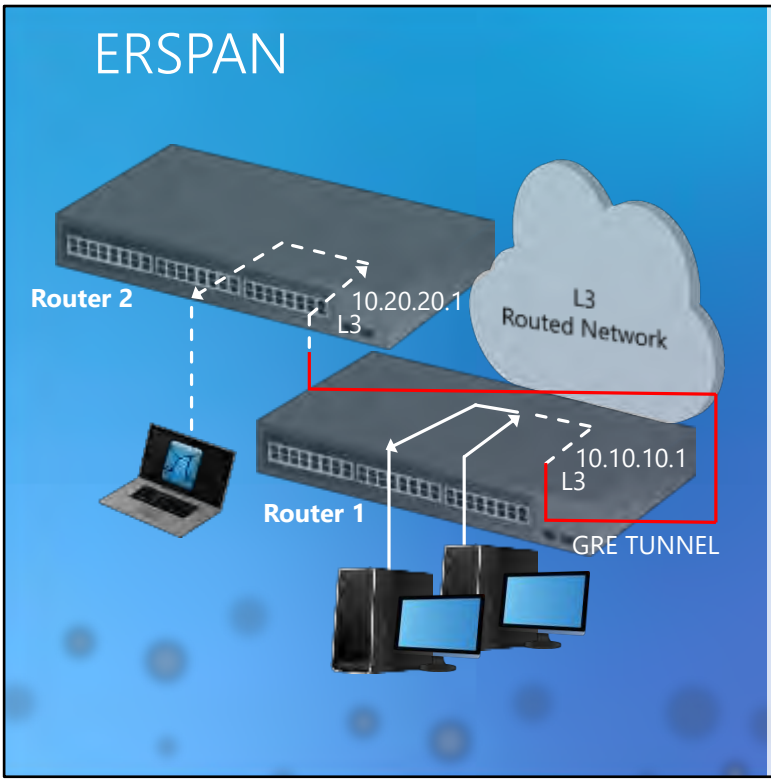
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RSPAN Session




```
ASW2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ASW2(config)#monitor session 4 source interface gig 1/45 tx
ASW2(config)#monitor session 4 filter vlan 50
ASW2(config)#monitor session 4 destination remote vlan 500
ASW2(config)#end
ASW2#
```

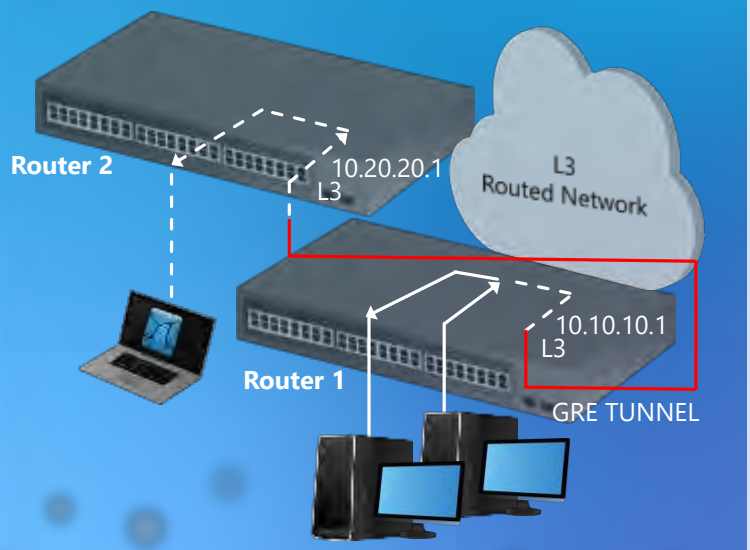
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



A tool for capturing traffic and sending a copy of it to another port on the same or different device across a L3 boundary.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ERSPAN

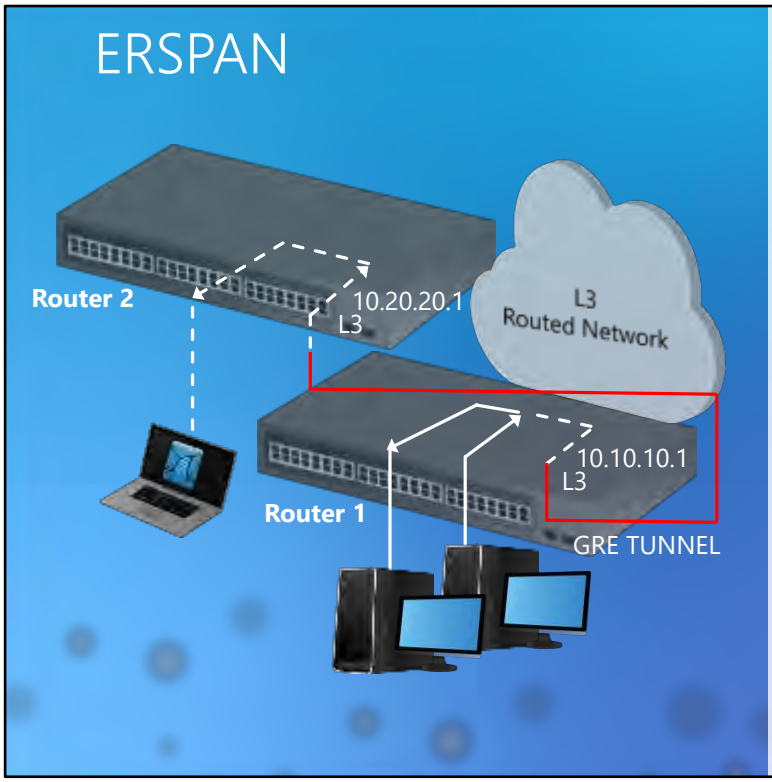


ERSPAN consists of:

- an ERSPAN source session
- routable ERSPAN GRE encapsulated traffic
- an ERSPAN destination session.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ERSPAN



Traffic can be captured ingress or egress on ports or vlans (same as span and rspan)

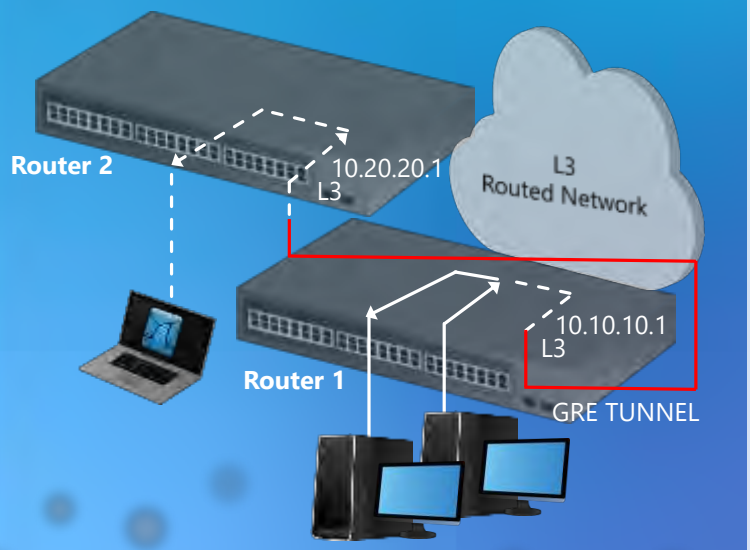
Captured traffic is sent out a layer 3 GRE tunnel interface to the other device

The receiving device collects the captured traffic and sends it out the port connected to the packet capture device.

***The ERSPAN feature is not supported on Layer 2 switching interfaces.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ERSPAN



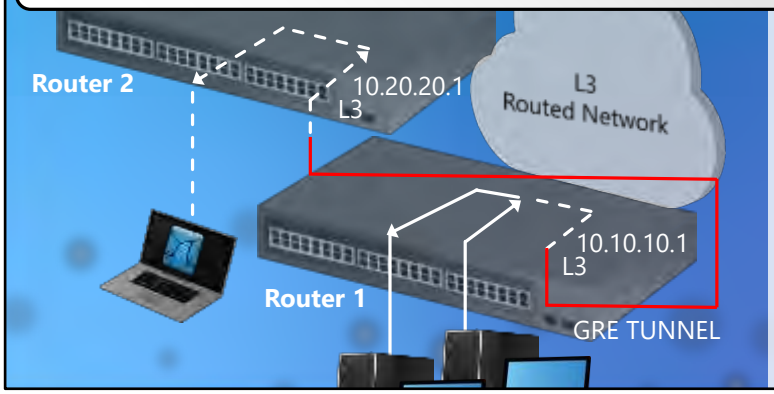
Supported Products:

- Nexus 55xx, 56xx, 60xx, 70xx, 77xx, 93xx, 95xx
- ASR 100x
- ISR 42xx, 43xx, 44xx
- CAT 4500, 6500, 7600, 9500, 9600

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ERSPAN

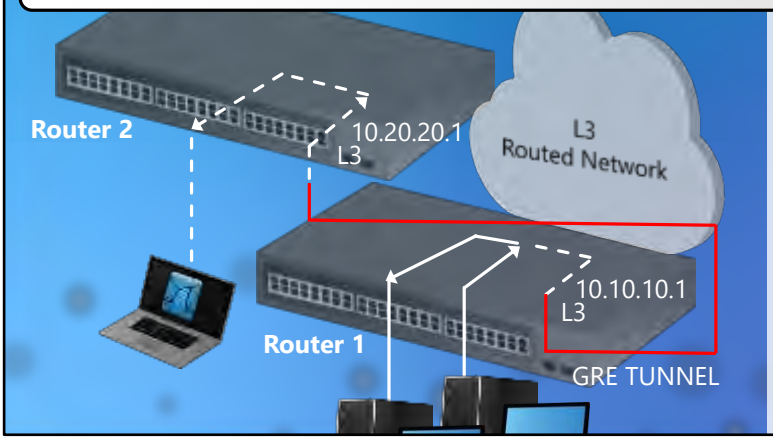
```
Router1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router1(config)#monitor session 1 type erspan-source
Router1(config-mon-erspan-src)#source interface gig 1/1 - 3 rx
…or…
Router1(config-mon-erspan-src)#source vlan 10
Router1(config-mon-erspan-src)#destination
Router1(config-mon-erspan-src-dst)#erspan-id 101
Router1(config-mon-erspan-src-dst)#ip address 10.20.20.1
Router1(config-mon-erspan-src-dst)#origin ip address 10.10.10.1
Router1(config-mon-erspan-src-dst)#no shut
Router1(config-mon-erspan-src-dst)#end
Router1#
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ERSPAN

```
Router2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router2(config)#monitor session 1 type erspan-destination
Router2(config-mon-erspan-dst)# destination interface GigabitEthernet1/0/1
Router2(config-mon-erspan-dst)# source
Router2(config-mon-erspan-dst-src)# erspan-id 101
Router2(config-mon-erspan-dst-src)# ip address 10.20.20.1
Router2(config-mon-erspan-dst-src)# no shutdown
Router2(config-mon-erspan-dst-src)# end
Router2#
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Configuration and Verification

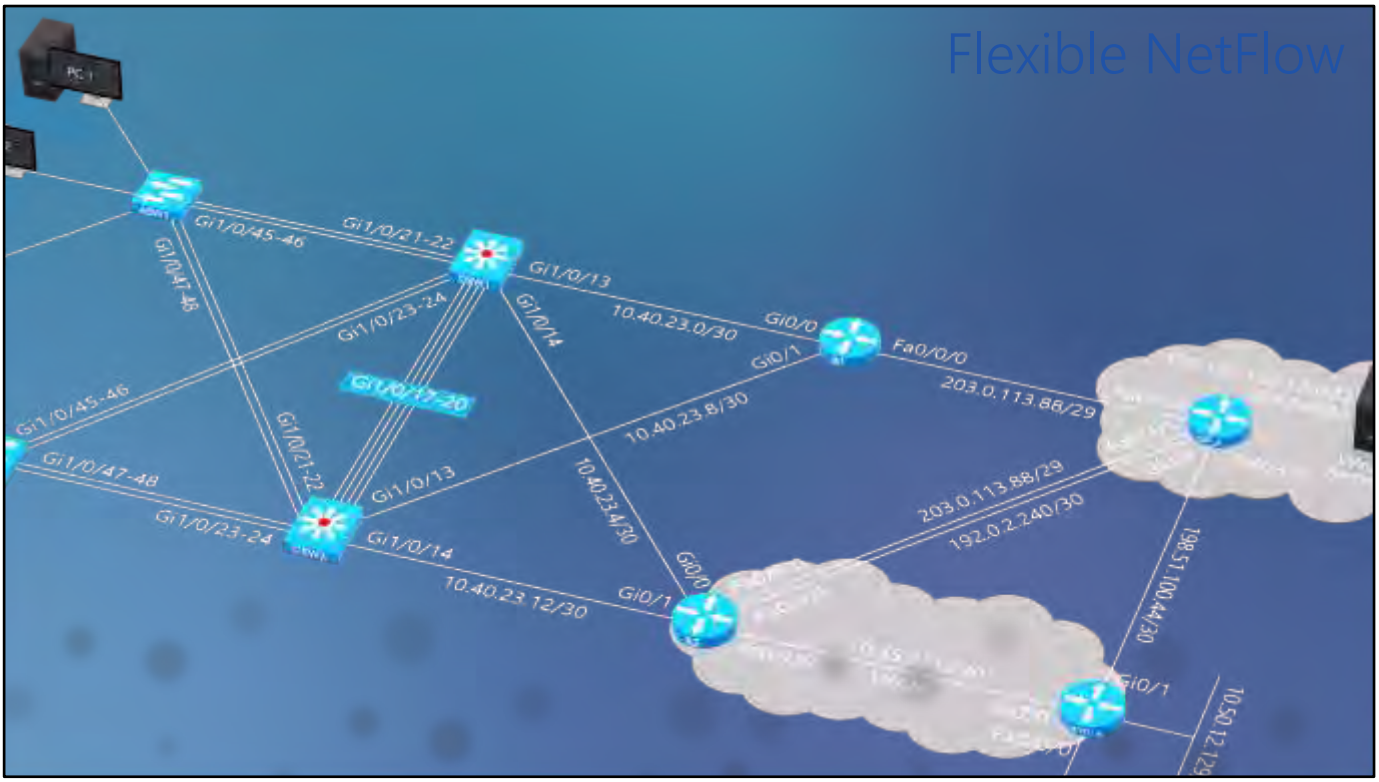
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

A tool that can gather traffic as it flows through the network

- For billing
- For security
- For performance
- For tracking

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

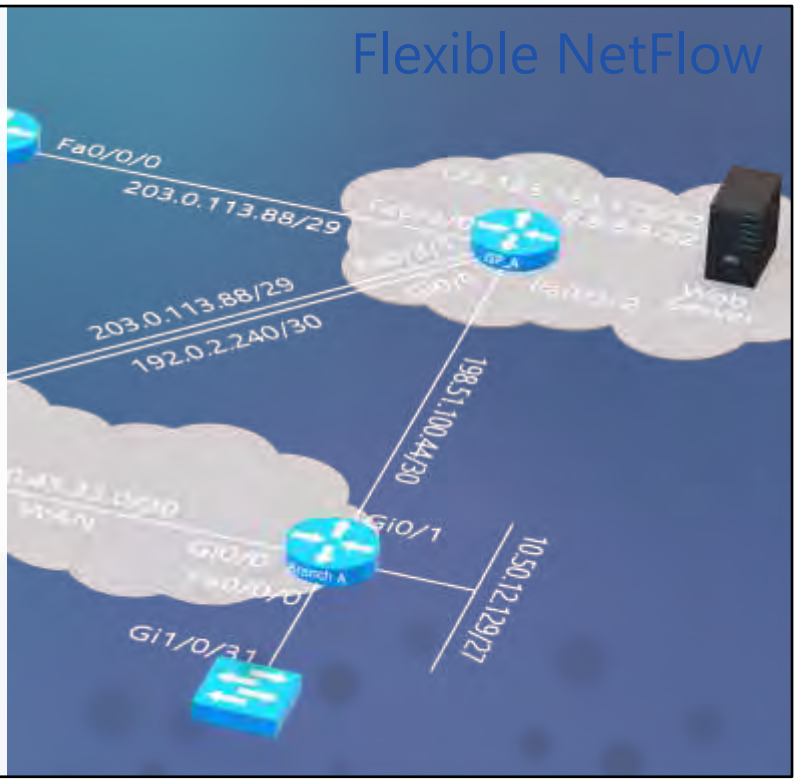
- Unidirectional
- Captures Flows (traffic from same)
  - Source IP address
  - Destination IP address
  - Source port number
  - Destination port number
  - Layer 3 protocol type
  - Type of service (ToS)
  - Input logical interface

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

Allows you to control what is considered part of a flow and what information you collect about that flow.

Provides reusable configuration components.



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

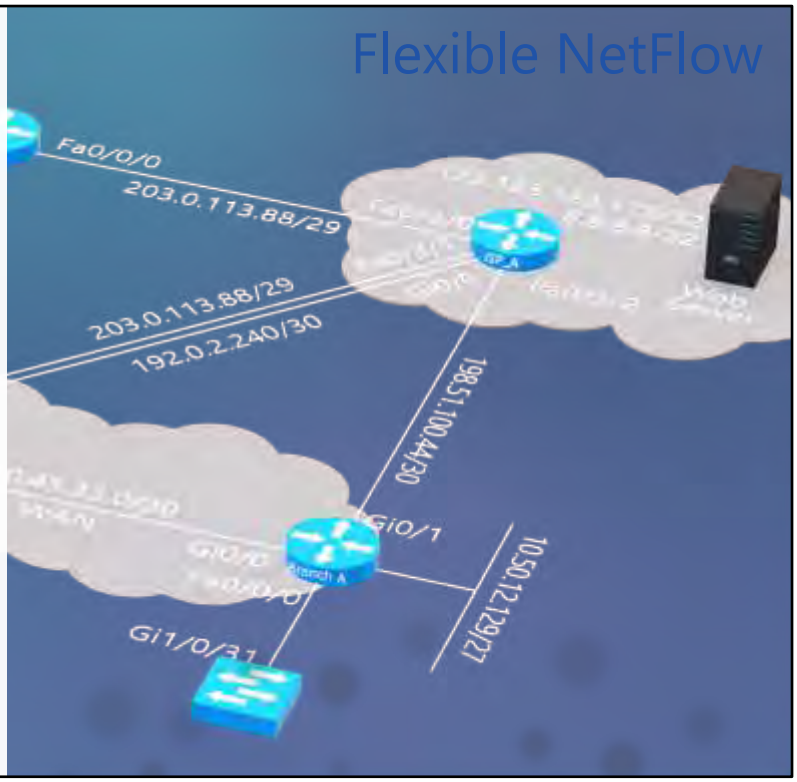
Flexible NetFlow

Flow Records

Flow Monitor

Flow Exporters

Flow Samplers

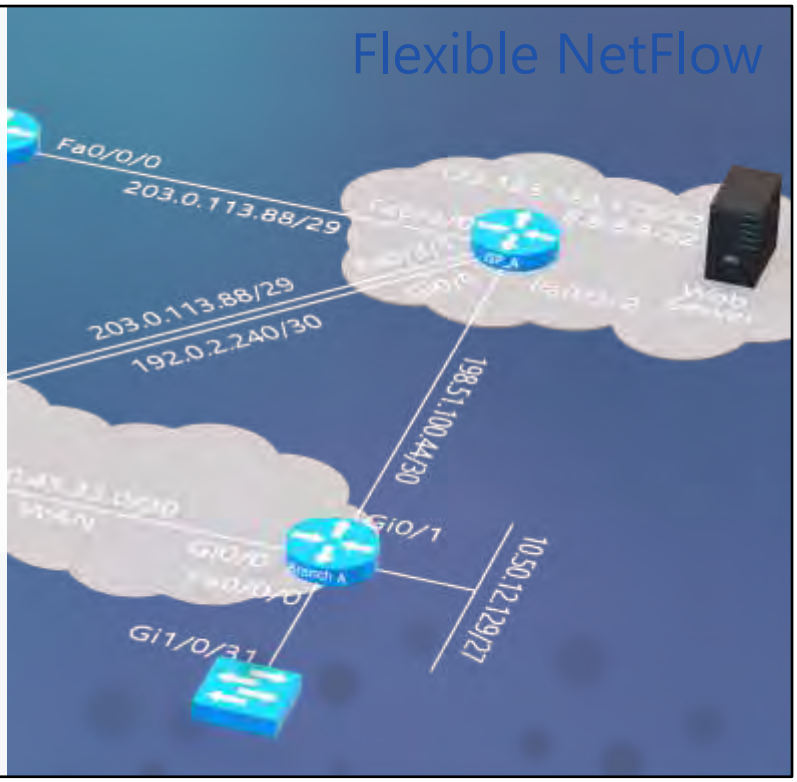


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

- Flow Records
  - Define what will be captured
    - Pre-defined
    - User-defined
- Flow Monitor
- Flow Exporters
- Flow Samplers



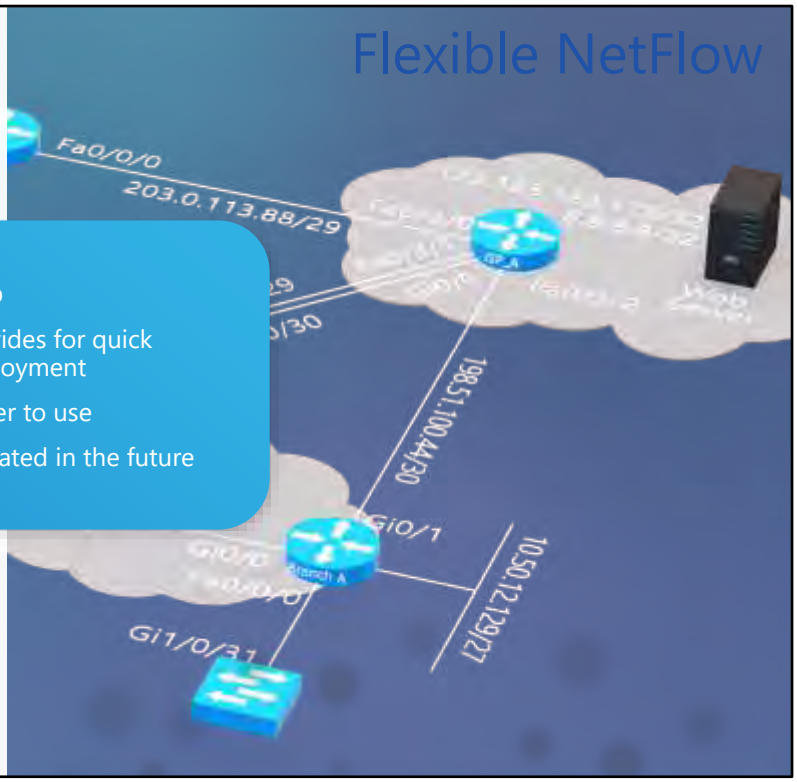
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

- Flow Records
  - Define what will be captured
    - Pre-defined
    - User-defined
- Flow Monitor
- Flow Exporters
- Flow Samplers

By Cisco

- Provides for quick deployment
- Easier to use
- Updated in the future



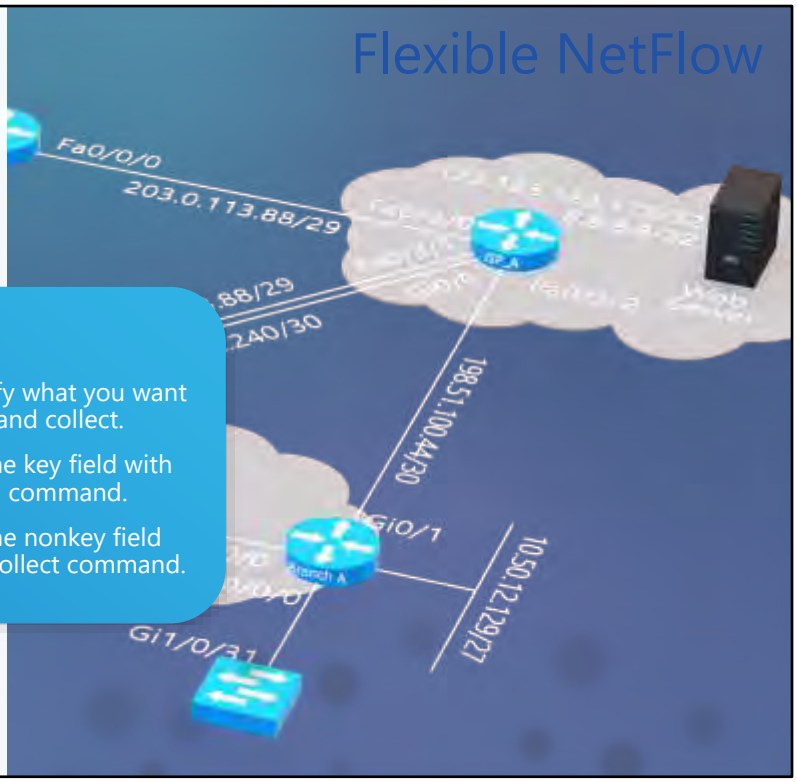
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

- Flow Records
  - Define what will be captured
    - Pre-defined
    - User-defined
- Flow Monitor
- Flow Exporters
- Flow Samplers

By YOU!

- You specify what you want to match and collect.
- Provide the key field with the match command.
- Provide the nonkey field with the collect command.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

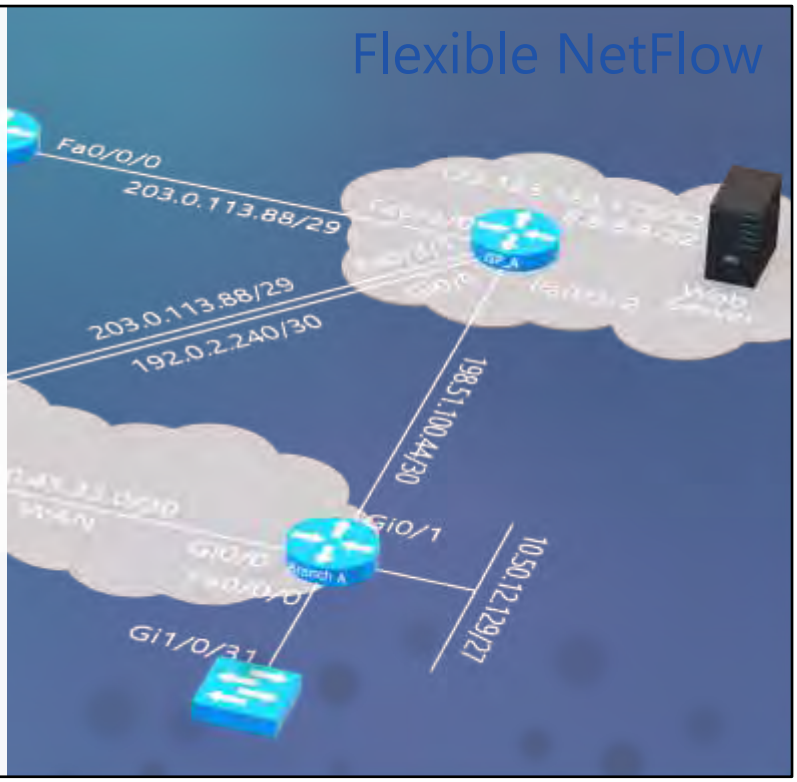
Flexible NetFlow

Flow Records

Flow Monitor

Flow Exporters

Flow Samplers

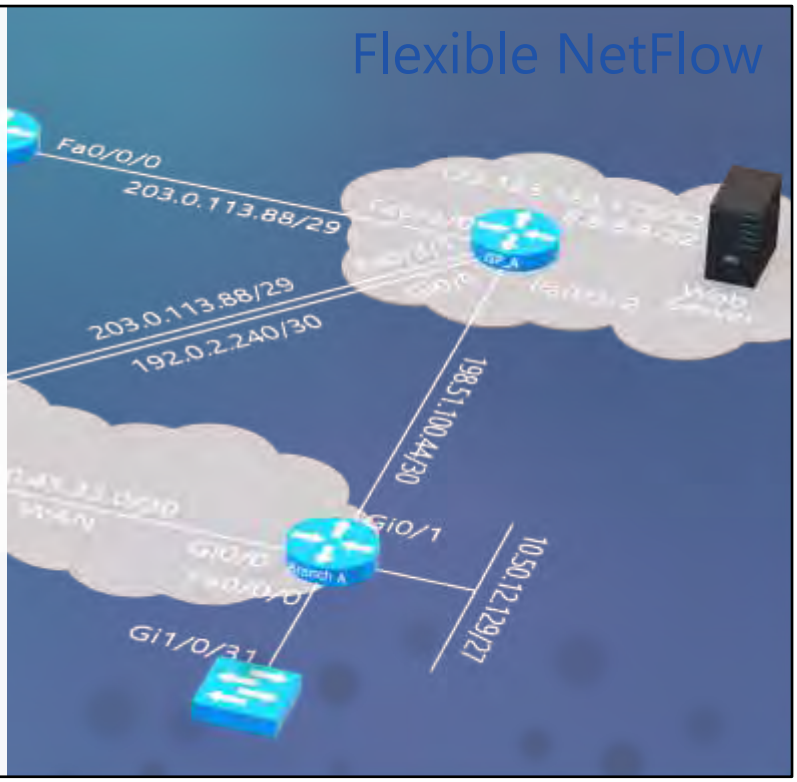


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

- Flow Records
- Flow Monitor
  - Performs the monitoring
    - Applied to interface
    - Defines flow record
    - Defines flow exporter
  - Stores results in the flow monitor cache
- Flow Exporters
- Flow Samplers



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

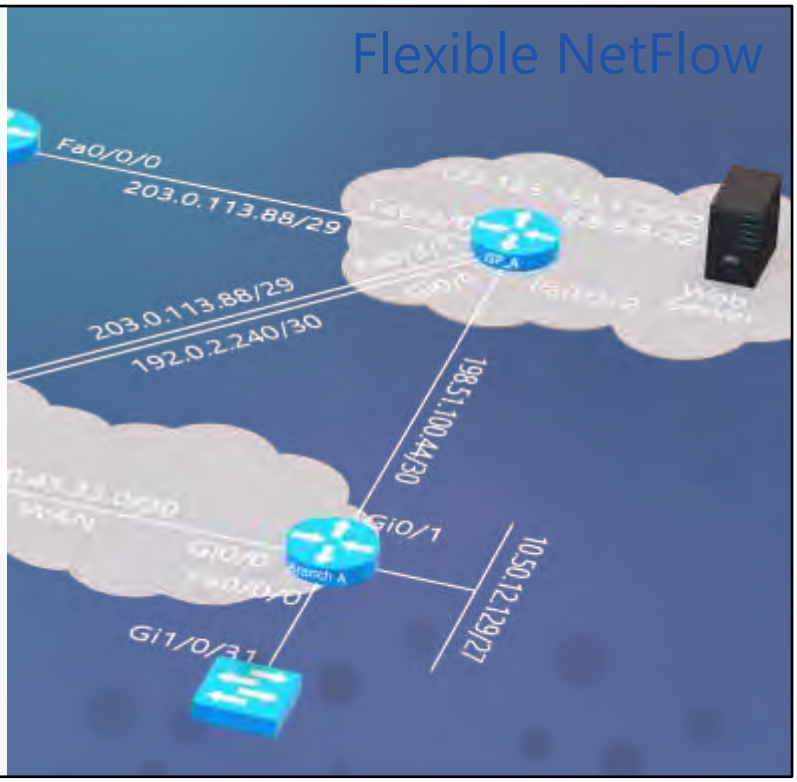
Flexible NetFlow

Flow Records

Flow Monitor

Flow Exporters

Flow Samplers

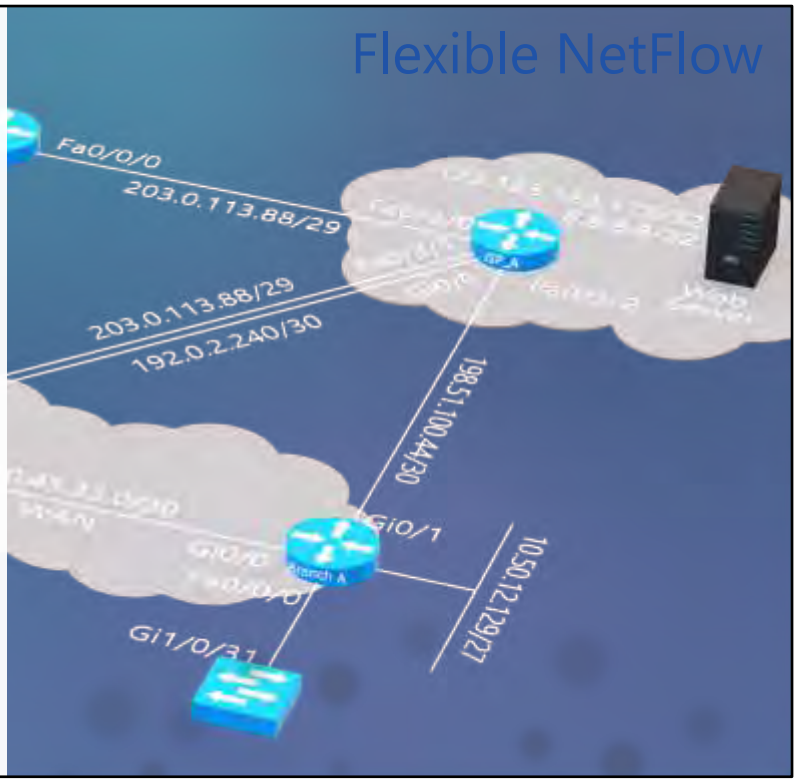


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

- Flow Records
- Flow Monitor
- Flow Exporters
  - Defines exporter parameters
    - Export Format (v5 or v9)
    - Src/Dst IP address
    - Transport Protocol
    - Src/Dst Port
- Flow Samplers



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

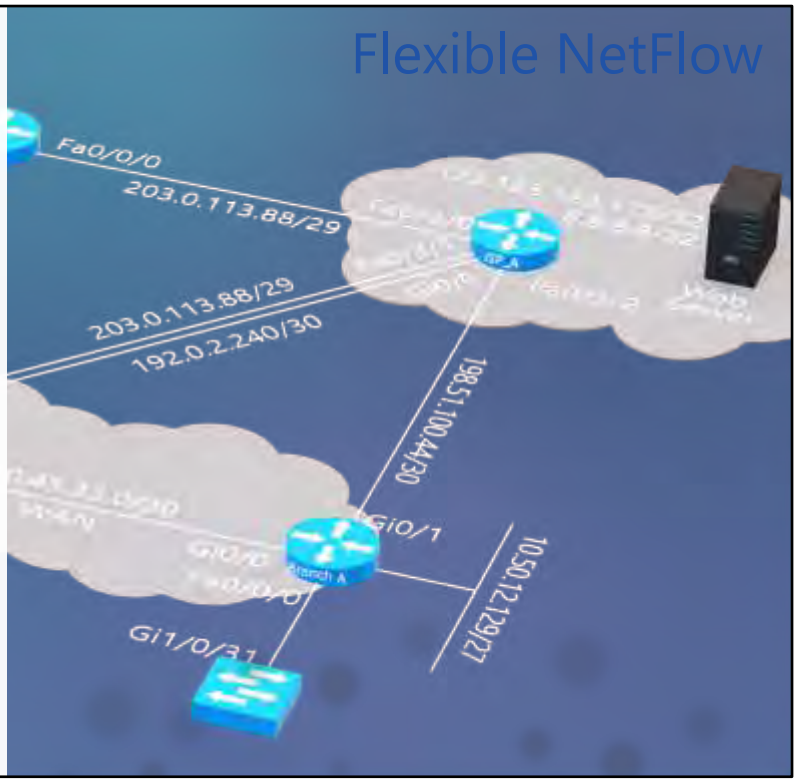
Flexible NetFlow

Flow Records

Flow Monitor

Flow Exporters

Flow Samplers

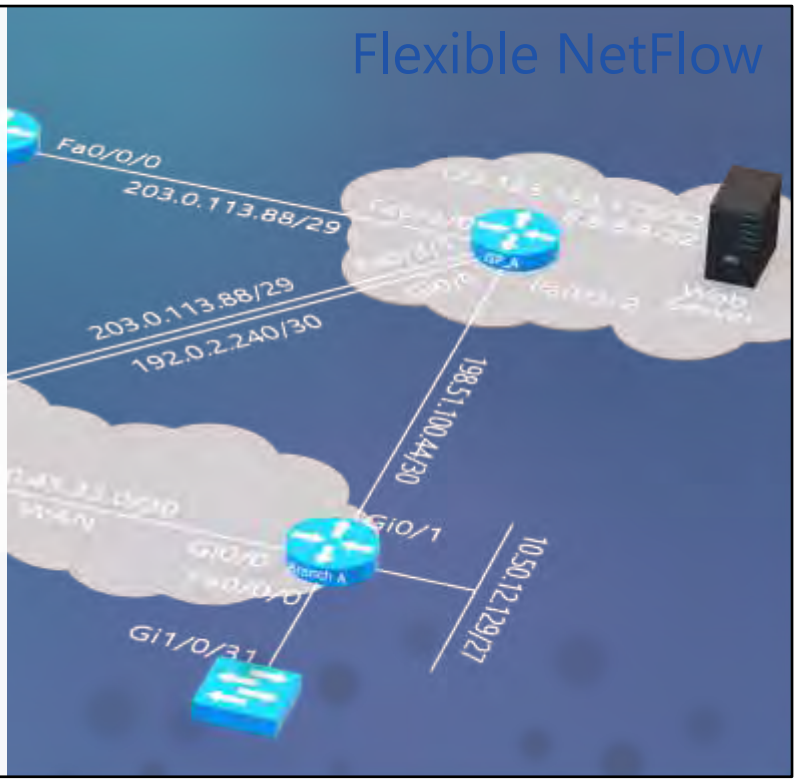


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow

- Flow Records
- Flow Monitor
- Flow Exporters
- Flow Samplers
  - Reduce the load on the device
  - Limits the number of packets that are analyzed



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

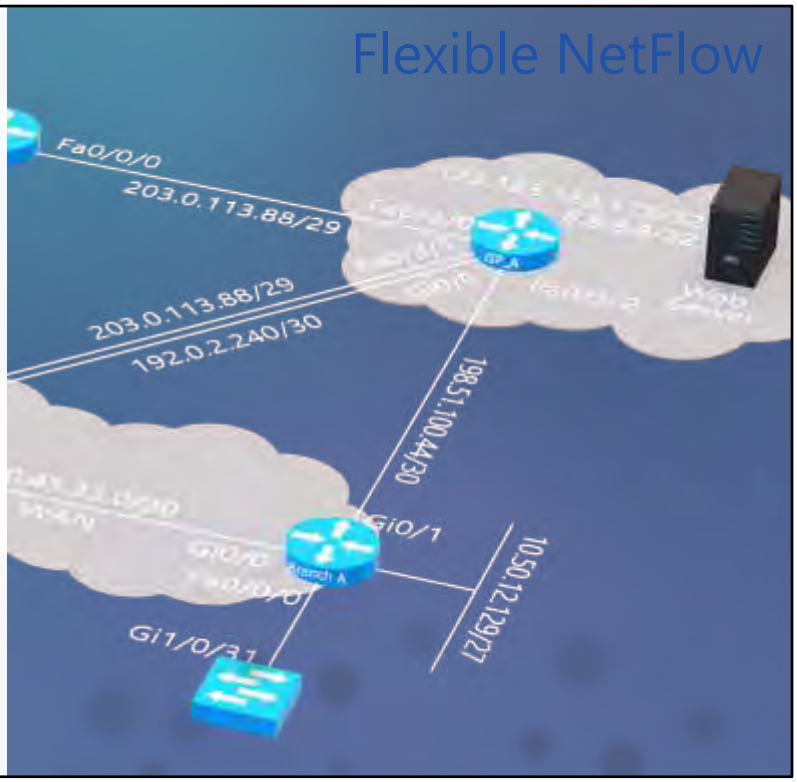
Flexible NetFlow

Flow Records

Flow Monitor

Flow Exporters

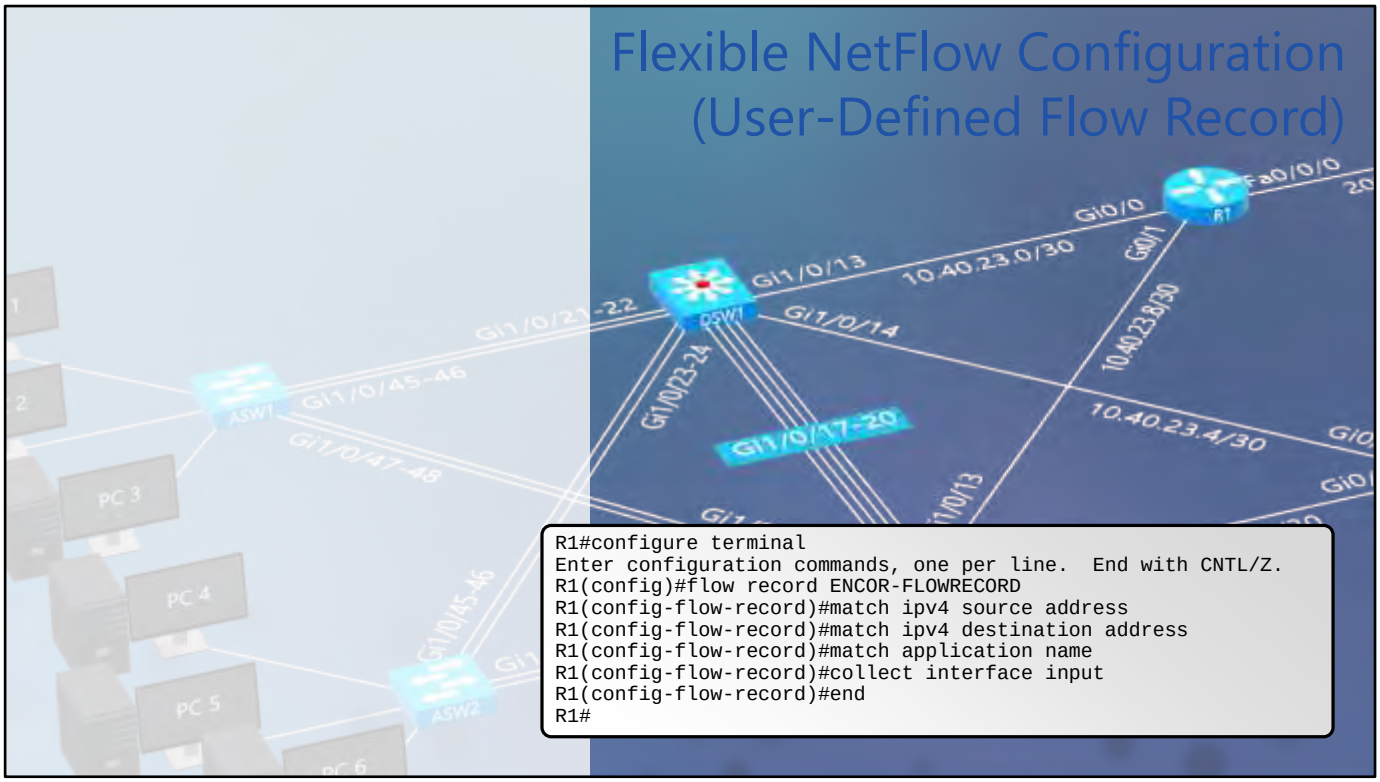
Flow Samplers



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

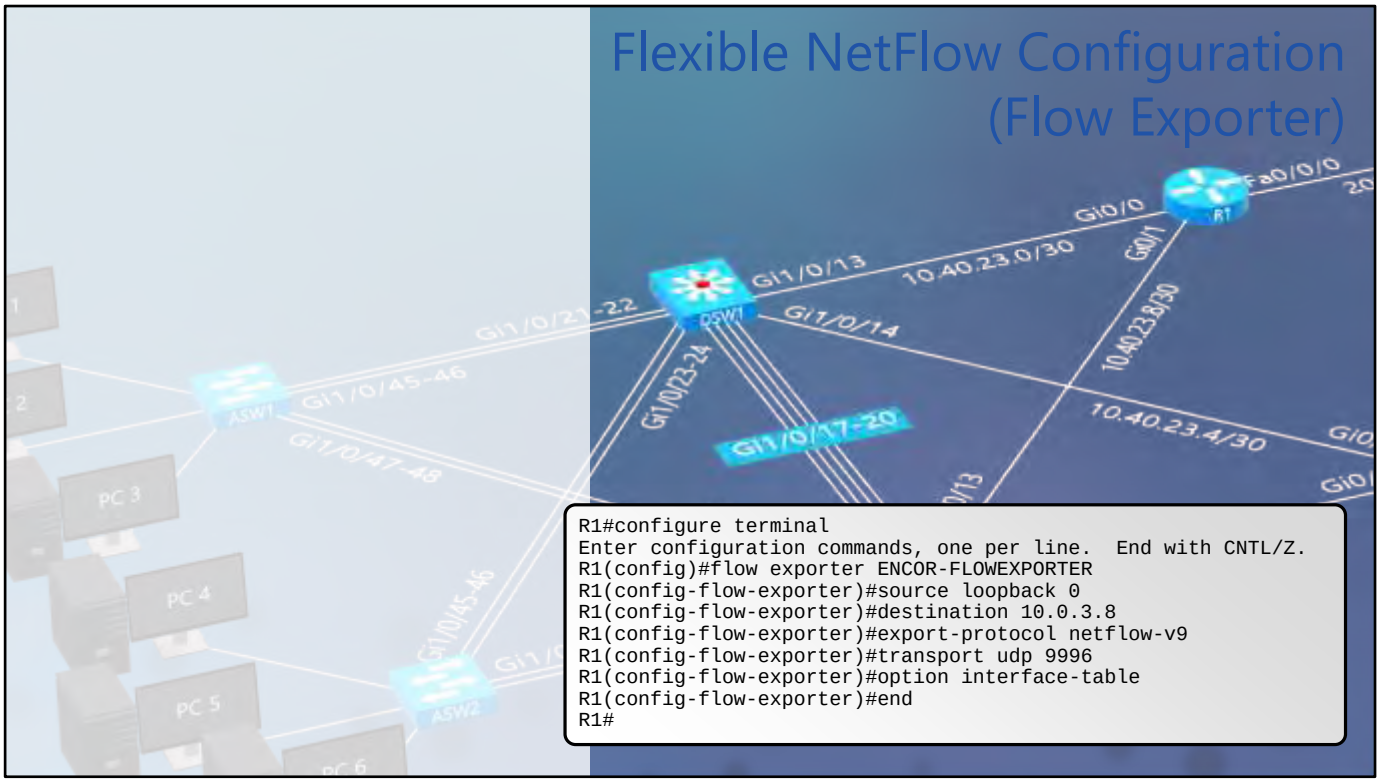
Flexible NetFlow Configuration (User-Defined Flow Record)




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#flow record ENCOR-FLOWRECORD
R1(config-flow-record)#match ipv4 source address
R1(config-flow-record)#match ipv4 destination address
R1(config-flow-record)#match application name
R1(config-flow-record)#collect interface input
R1(config-flow-record)#end
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

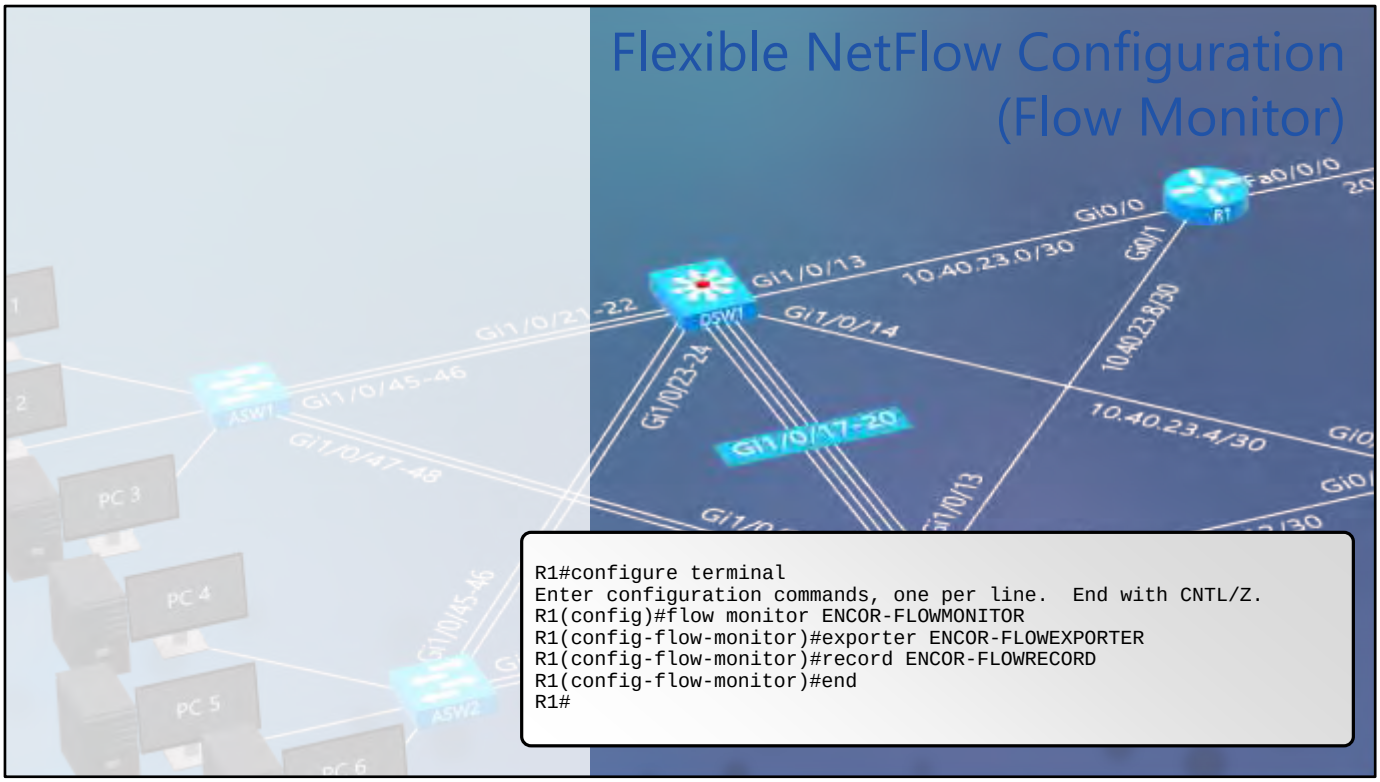
Flexible NetFlow Configuration (Flow Exporter)




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#flow exporter ENCOR-FLOWEXPORTER
R1(config-flow-exporter)#source loopback 0
R1(config-flow-exporter)#destination 10.0.3.8
R1(config-flow-exporter)#export-protocol netflow-v9
R1(config-flow-exporter)#transport udp 9996
R1(config-flow-exporter)#option interface-table
R1(config-flow-exporter)#end
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

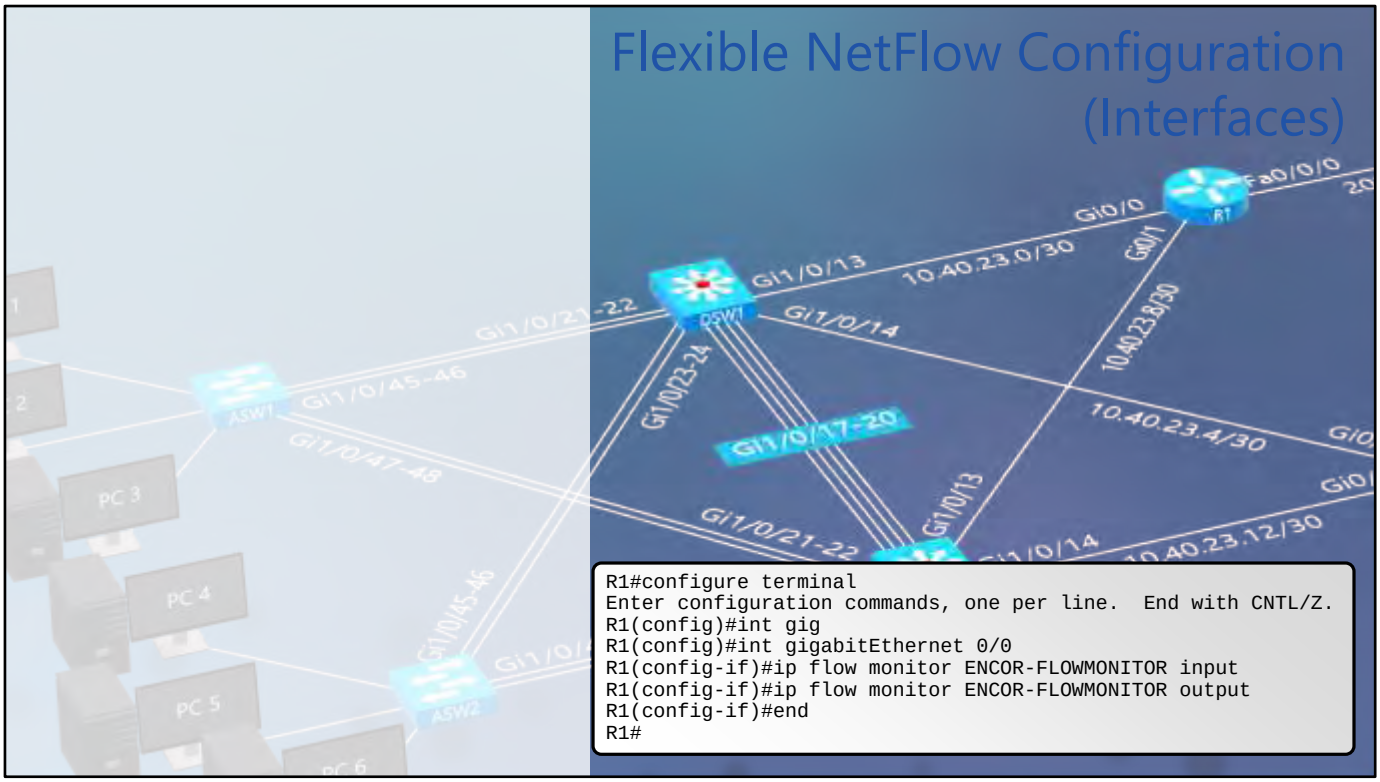
Flexible NetFlow Configuration (Flow Monitor)




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#flow monitor ENCOR-FLOWMONITOR
R1(config-flow-monitor)#exporter ENCOR-FLOWEXPORTER
R1(config-flow-monitor)#record ENCOR-FLOWRECORD
R1(config-flow-monitor)#end
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Configuration (Interfaces)




```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int gig
R1(config)#int gigabitEthernet 0/0
R1(config-if)#ip flow monitor ENCOR-FLOWMONITOR input
R1(config-if)#ip flow monitor ENCOR-FLOWMONITOR output
R1(config-if)#end
R1#
```

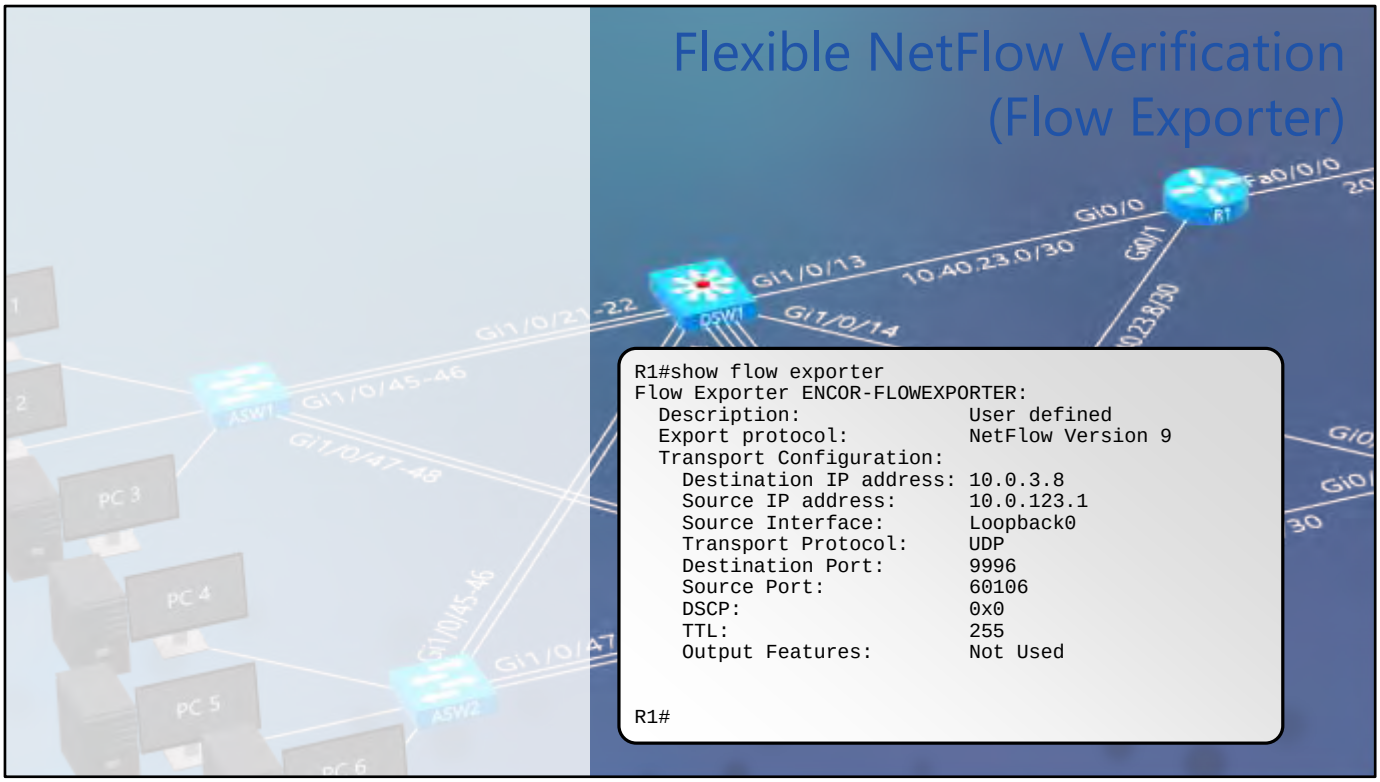
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Record)

```
R1#show flow record
flow record ENCOR-FLOWRECORD:
  Description:        User defined
  No. of users:       1
  Total field space:  16 bytes
  Fields:
    match ipv4 source address
    match ipv4 destination address
    match application name
    collect interface input

R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Exporter)

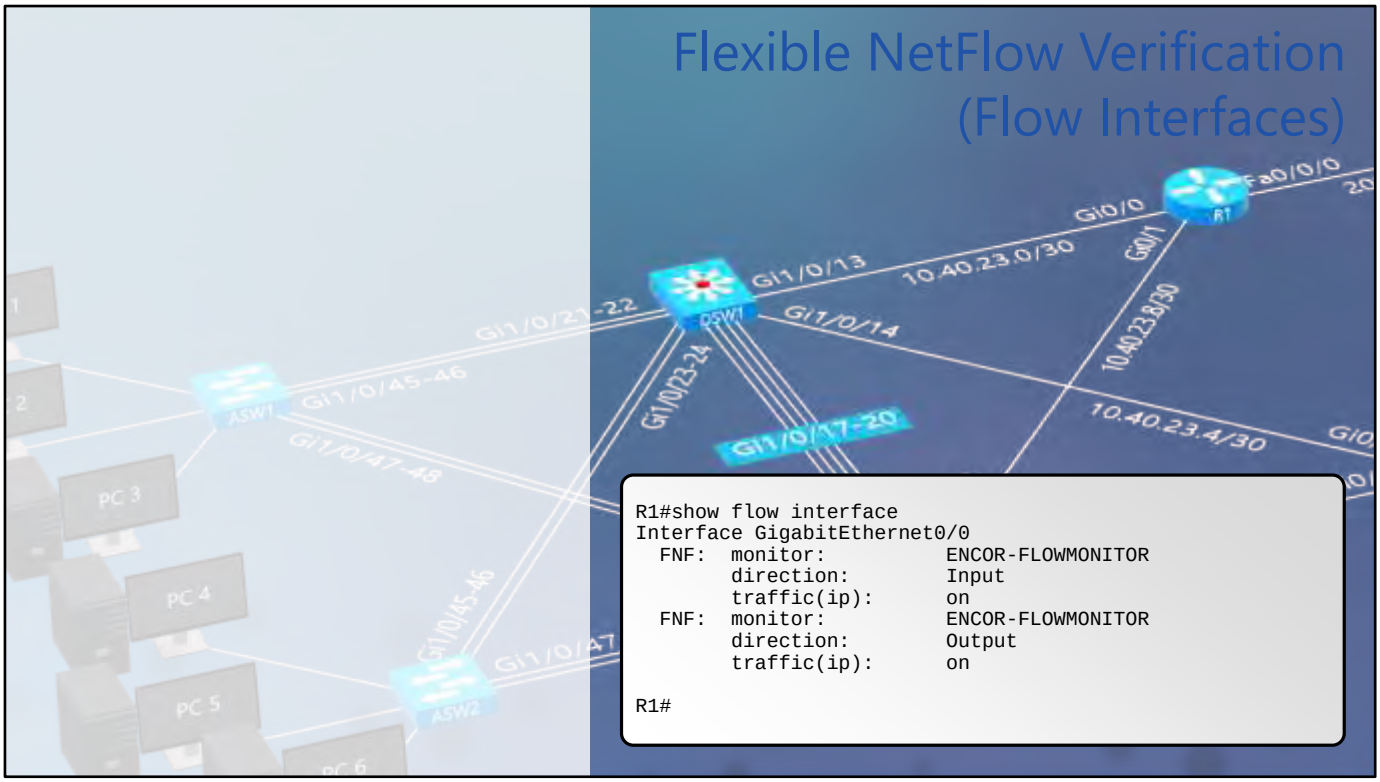



```
R1#show flow exporter
Flow Exporter ENCOR-FLOWEXPORTER:
  Description:               User defined
  Export protocol:           NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.0.3.8
    Source IP address:      10.0.123.1
    Source Interface:       Loopback0
    Transport Protocol:     UDP
    Destination Port:       9996
    Source Port:            60106
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Not Used


R1#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Interfaces)




```
R1#show flow interface
Interface GigabitEthernet0/0
  FNF:  monitor:          ENCOR-FLOWMONITOR
        direction:        Input
        traffic(ip):      on
  FNF:  monitor:          ENCOR-FLOWMONITOR
        direction:        Output
        traffic(ip):      on

R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Monitor)

```
R1#show flow monitor
Flow Monitor ENCOR-FLOWMONITOR:
  Description:       User defined
  Flow Record:       ENCOR-FLOWRECORD
  Flow Exporter:     ENCOR-FLOWEXPORTER
  Cache:
    Type:               normal
    Status:             allocated
    Size:               4096 entries / 213008 bytes
    Inactive Timeout:   15 secs
    Active Timeout:     1800 secs
    Update Timeout:     1800 secs


R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

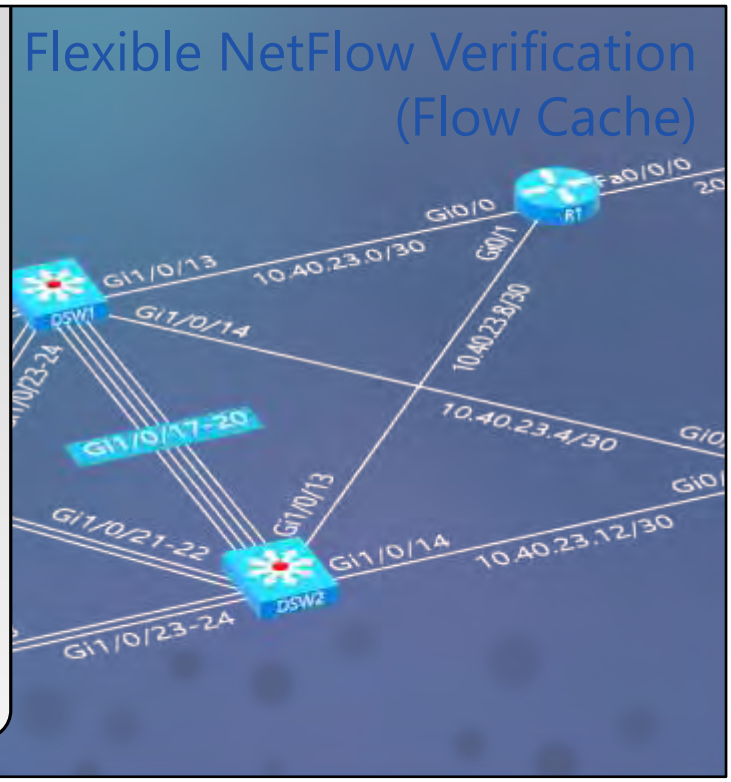
Flexible NetFlow Verification (Flow Cache)

```
R1#show flow monitor name ENCOR-FLOWMONITOR cache
  Cache type:                                Normal
  Cache size:                                  4096
  Current entries:                                4
  High Watermark:                                 5

  Flows added:                                    5
  Flows aged:                                     1
    - Active timeout      (  1800 secs)           0
    - Inactive timeout    (    15 secs)           1
    - Event aged                                  0
    - Watermark aged                              0
    - Emergency aged                              0

IPV4 SOURCE ADDRESS:       10.0.10.2
IPV4 DESTINATION ADDRESS:  224.0.0.10
APPLICATION NAME:          prot eigrp
interface input:           Gi0/0

IPV4 SOURCE ADDRESS:       10.0.10.2
IPV4 DESTINATION ADDRESS:  10.0.12.1
APPLICATION NAME:          prot icmp
interface input:           Gi0/0

IPV4 SOURCE ADDRESS:       10.0.10.2
IPV4 DESTINATION ADDRESS:  192.168.4.4
APPLICATION NAME:          prot icmp
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Verification (Flow Cache)

```
  Current entries:                                  4
  High Watermark:                                   5

  Flows added:                                      5
  Flows aged:                                       1
    - Active timeout      (  1800 secs)             0
    - Inactive timeout    (    15 secs)             1
    - Event aged                                    0
    - Watermark aged                                0
    - Emergency aged                                0

IPV4 SOURCE ADDRESS:        10.0.10.2
IPV4 DESTINATION ADDRESS:   224.0.0.10
APPLICATION NAME:           prot eigrp
interface input:            Gi0/0

IPV4 SOURCE ADDRESS:        10.0.10.2
IPV4 DESTINATION ADDRESS:   10.0.12.1
APPLICATION NAME:           prot icmp
interface input:            Gi0/0

IPV4 SOURCE ADDRESS:        10.0.10.2
IPV4 DESTINATION ADDRESS:   192.168.4.4
APPLICATION NAME:           prot icmp
interface input:            Gi0/0

IPV4 SOURCE ADDRESS:        192.168.4.4
IPV4 DESTINATION ADDRESS:   10.0.10.2
APPLICATION NAME:           prot icmp
interface input:            Gi2/0
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flexible NetFlow Configuration (Flow Sampler)

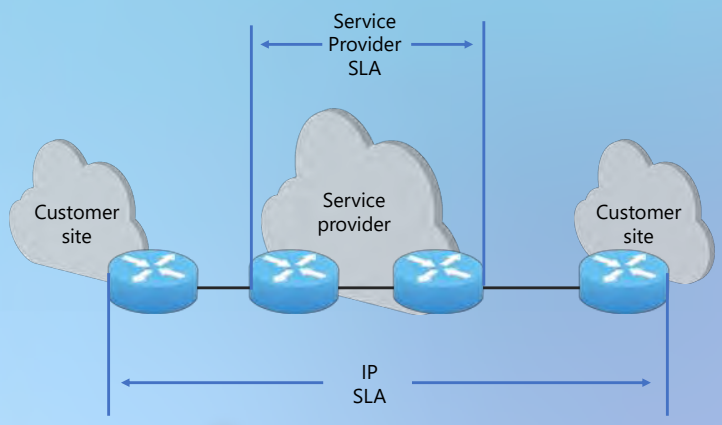
```
R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#sampler ENCOR-FLOWSAMPLER
R1(config-sampler)#mode random 1 out-of 50
R1(config-sampler)#exit
R1(config)#flow monitor ENCOR-FLOWMONITOR
R1(config-flow-monitor)#exporter ENCOR-FLOWEXPORTER
R1(config-flow-monitor)#record ENCOR-FLOWRECORD
R1(config-flow-monitor)#exit
R1(config)#int gigabitEthernet 0/0
R1(config-if)#ip flow monitor ENCOR-FLOWMONITOR sampler ENCOR-FLOWSAMPLER input
R1(config-if)#end
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IPSLA Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

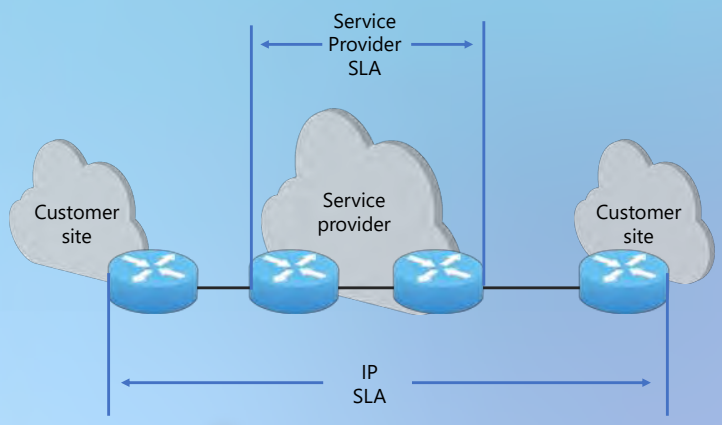
IP SLA Overview



- Tool built into Cisco IOS
  - Continuous monitoring and measuring of various aspects of the network
    - Delay (both round-trip and one-way)
    - Jitter (directional)
    - Packet loss (directional)
    - Packet sequencing (packet ordering)
    - Path (per hop)
    - Connectivity (directional)
    - Server or website download time
    - Voice quality scores

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA Overview

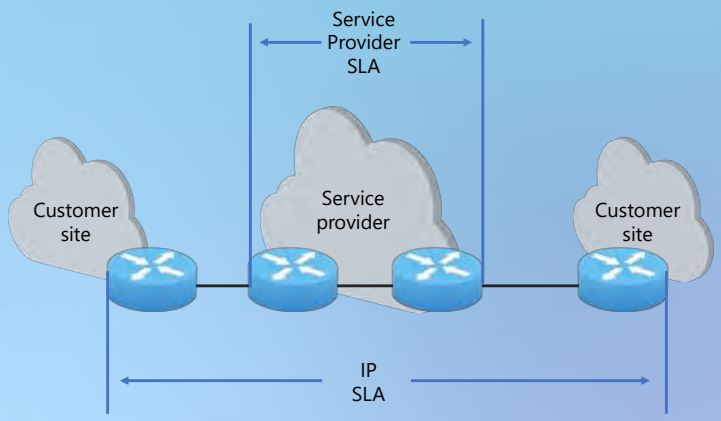


Purpose

- increase productivity
- lower operational costs
- reduce the frequency of network outages
- Troubleshooting
- Problem analysis
- Designing networks

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

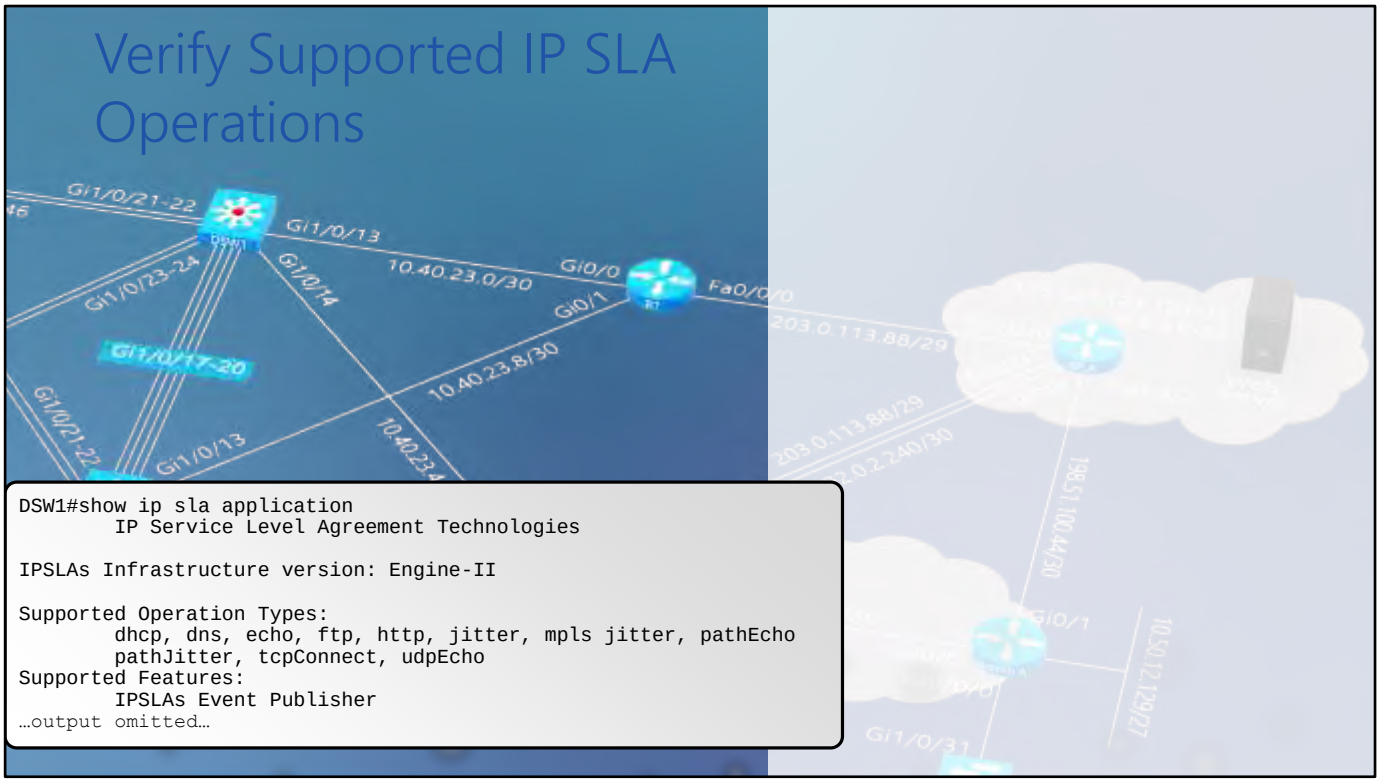
IP SLA Overview



- Uses Active traffic monitoring
  - Send a probe in a continuous, reliable, and predictable manner
  - Collect results of the probe
    - Store in memory (CLI)
    - Store in SNMP MIB

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

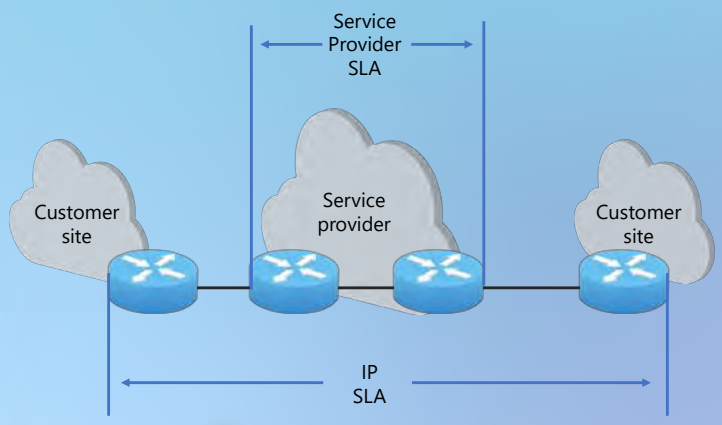
Verify Supported IP SLA Operations




```
DSW1#show ip sla application
        IP Service Level Agreement Technologies

IPSLAs Infrastructure version: Engine-II

Supported Operation Types:
        dhcp, dns, echo, ftp, http, jitter, mpls jitter, pathEcho
        pathJitter, tcpConnect, udpEcho
Supported Features:
        IPSLAs Event Publisher
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA

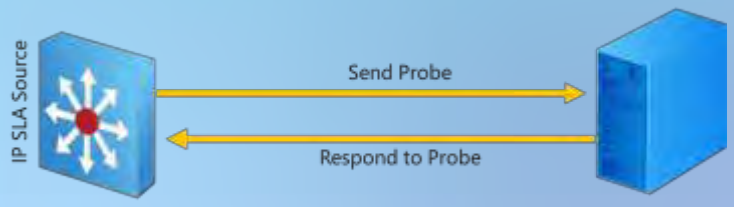


What do we need to know for the exam?

- Testing a servers response time with ICMP-Echo
- Testing network performance with UDP-Echo
- Failover for floating static routes
- Monitoring network for VOICE with UDP-Jitter

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

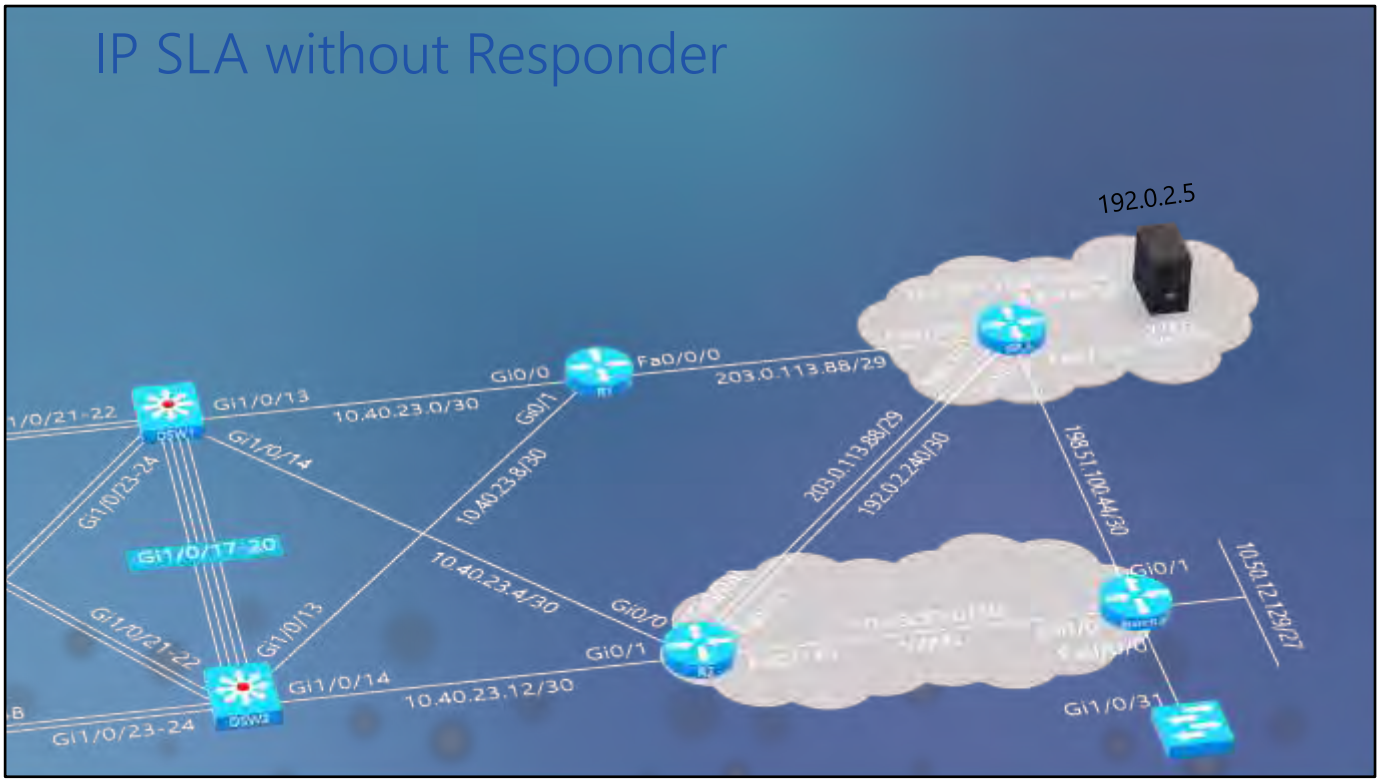
IP SLA without Responder



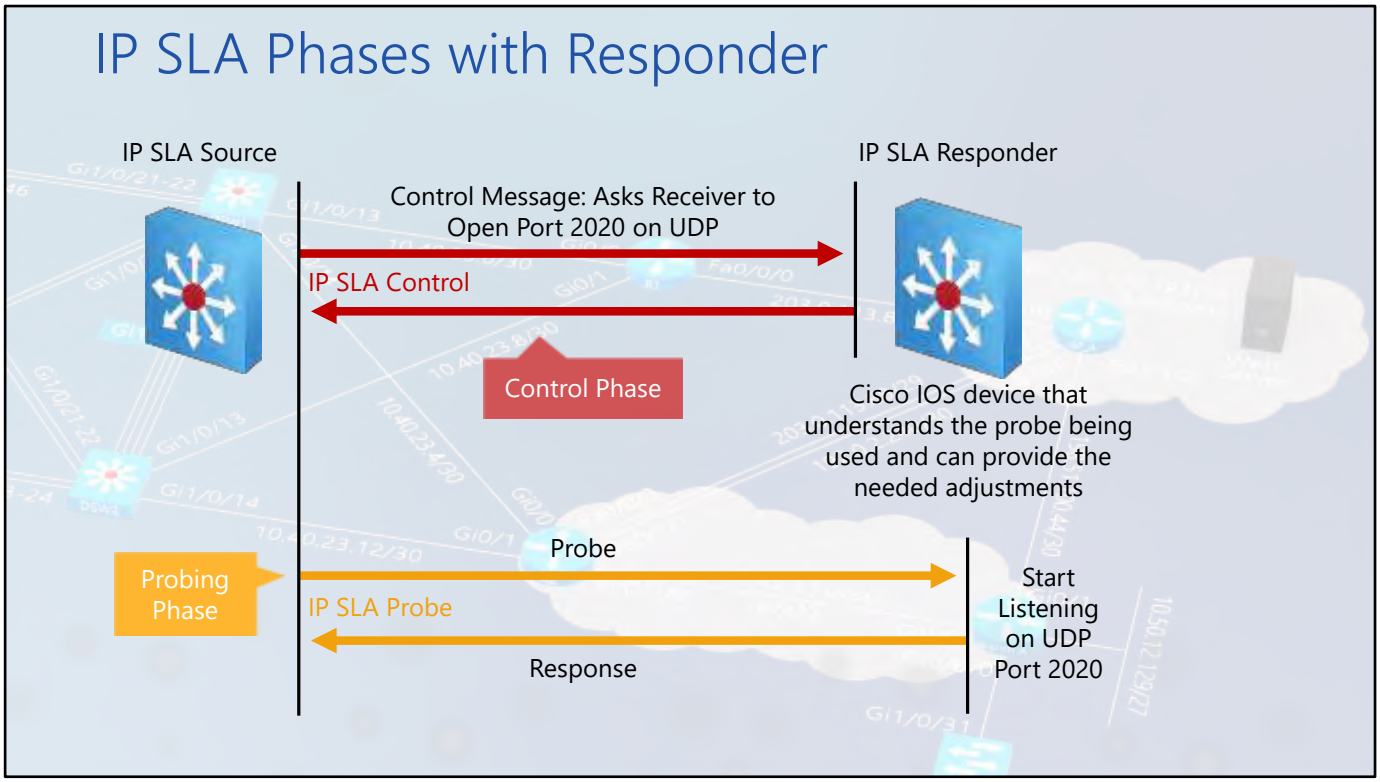
Any device that understands the probe being used!!

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA without Responder



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Responder Time Stamps

The SLA responder utilizes two time stamps (T2 and T3).

The SLA responder factors out processing time, making results very accurate.

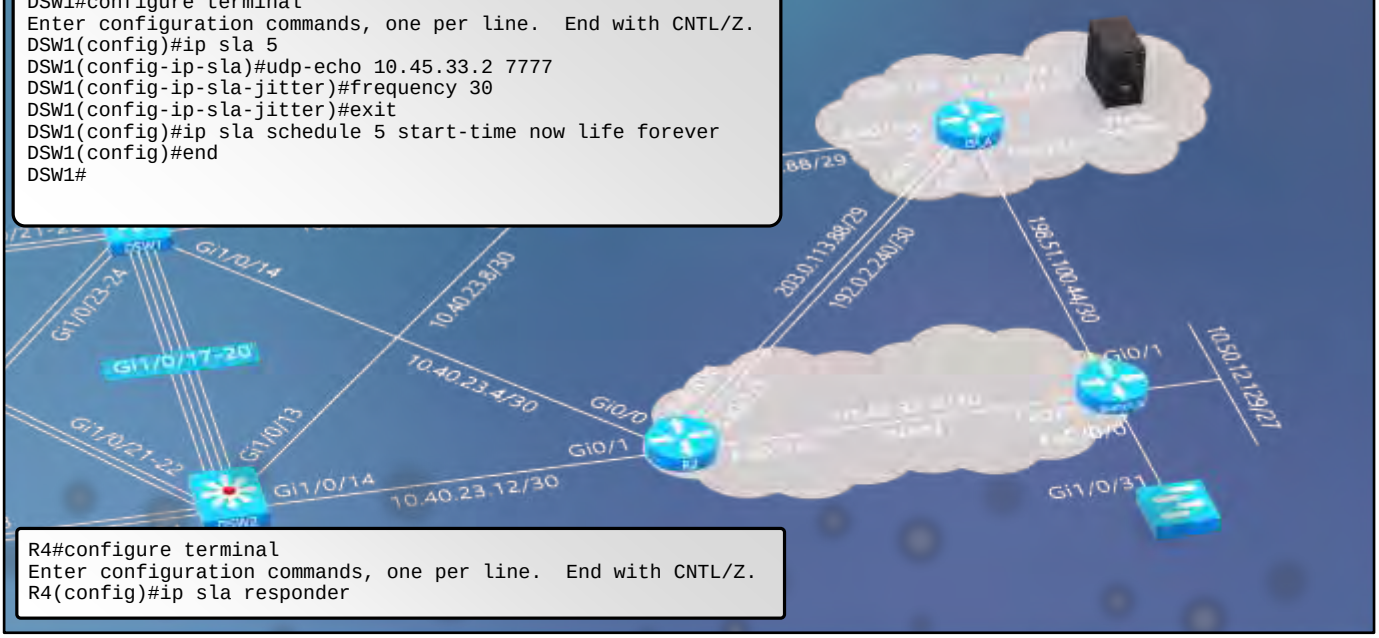
The SLA responder allows one-way measurements for latency, jitter, and packet loss.

Delta Value = T3 - T2

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA with Responder

```
DSW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DSW1(config)#ip sla 5
DSW1(config-ip-sla)#udp-echo 10.45.33.2 7777
DSW1(config-ip-sla-jitter)#frequency 30
DSW1(config-ip-sla-jitter)#exit
DSW1(config)#ip sla schedule 5 start-time now life forever
DSW1(config)#end
DSW1#
```



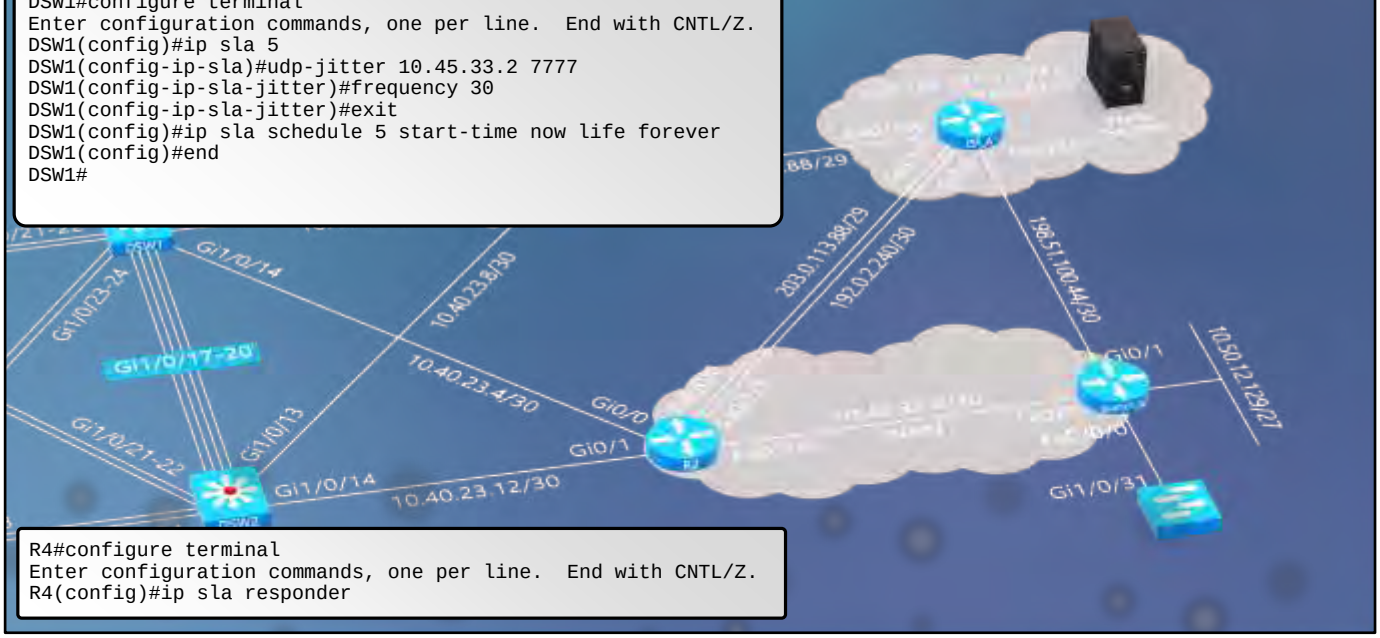

```
R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip sla responder
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA with Responder

```
DSW1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DSW1(config)#ip sla 5
DSW1(config-ip-sla)#udp-jitter 10.45.33.2 7777
DSW1(config-ip-sla-jitter)#frequency 30
DSW1(config-ip-sla-jitter)#exit
DSW1(config)#ip sla schedule 5 start-time now life forever
DSW1(config)#end
DSW1#
```




```
R4#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip sla responder
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA with Responder

```
DSW1#show ip sla configuration 5
IP SLAs, Infrastructure Engine-II.

Entry number: 5
Owner:
Tag:
Type of operation to perform: udp-jitter
Target address/Source address: 10.45.33.2/0.0.0.0
Target port/Source port: 7777/0
Type Of Service parameter: 0x0
Request size (ARR data portion): 32
Operation timeout (milliseconds): 5000
Packet Interval (milliseconds)/Number of packets: 20/10
Verify data: No
Vrf Name:
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 30
    Next Scheduled Start Time: Start Time already passed
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): Forever
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
Enhanced History:
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IP SLA with Res

```
DSW1#show ip sla statistics 5

Round Trip Time (RTT) for       Index 5
Type of operation: jitter
        Latest RTT: 41 ms
Latest operation start time: 07:34:23.392 UTC Tue Sep 24 2019
Latest operation return code: OK
RTT Values
        Number Of RTT: 10
        RTT Min/Avg/Max: 30/41/58 ms
Latency one-way time milliseconds
        Number of Latency one-way Samples: 7
        Source to Destination Latency one way Min/Avg/Max: 28/36/43 ms
        Destination to Source Latency one way Min/Avg/Max: 1/6/23 ms
Jitter time milliseconds
        Number of SD Jitter Samples: 9
        Number of DS Jitter Samples: 9
        Source to Destination Jitter Min/Avg/Max: 0/6/15 ms
        Destination to Source Jitter Min/Avg/Max: 1/9/25 ms
Packet Loss Values
        Loss Source to Destination: 0           Loss Destination to
Source: 0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 7
Number of failures: 0
Operation time to live: Forever
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMP Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Simple Network Management Protocol (SNMP)

- Management protocol used to poll devices such as:
  - Routers, Switches, Servers, etc.
- Used to collect and organize information about the device's wellbeing.
- Information is stored as variables in a database on the device called the MIB (management information base).

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

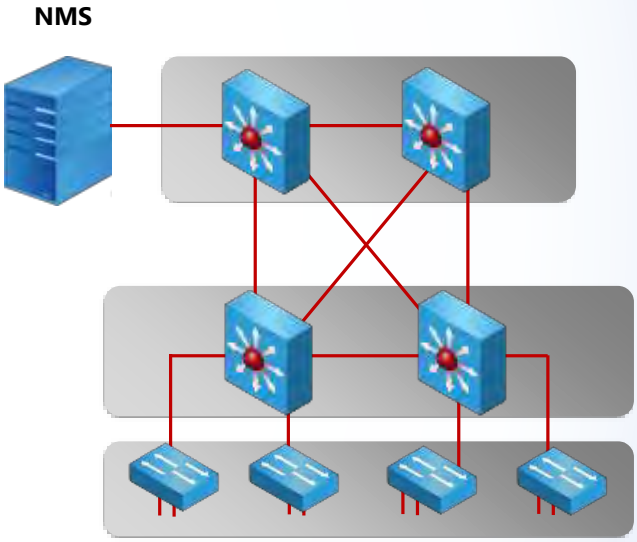
SNMP Overview

The NMS runs the SNMP manager software

The **SNMP agent** runs on the managed devices (i.e IOS routers and switches)

SNMP NMS will poll agent

SNMP **traps** and **informs** are event driven messages sent from the agent to the manager



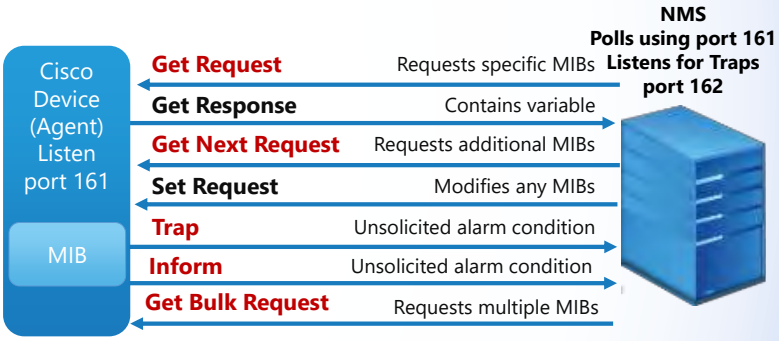
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMP Versions

SNMPv1 - 5 message types

SNMPv2 - Adds 2 types: Get Bulk Request and Inform Request.

SNMPv3 – More secure as it supports: authentication, integrity, encryption, authorization



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv2c Example

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv2c Example

```
R1(config)# access-list 20 permit host 10.0.3.8
R1(config)# snmp-server community NMS_RO_PWS ro 20
R1(config)# snmp-server community NMS_RW_PWS rw 20
R1(config)# snmp-server host 10.0.3.8 traps version 2c NMS_RO_PWS
R1(config)# snmp-server enable traps
R1(config)# snmp-server ifindex persist
```

```
R1#show snmp mib ifmib ifindex
GigabitEthernet0/1: Ifindex = 3
Loopback192: Ifindex = 12
Tunnel0: Ifindex = 9
Backplane-GigabitEthernet0/3: Ifindex = 4
FastEthernet0/0/1: Ifindex = 6
Embedded-Service-Engine0/0: Ifindex = 1
Null0: Ifindex = 7
GigabitEthernet0/0: Ifindex = 2
Tunnel1: Ifindex = 11
Virtual-Template1: Ifindex = 10
NVI0: Ifindex = 8
FastEthernet0/0/0: Ifindex = 5
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Example

```
R1(config)# access-list 20 permit host 10.0.3.8
R1(config)# snmp-server view MGMT ifAdminStatus include
R1(config)# snmp-server view MGMT ifOperStatus include
R1(config)# snmp-server group TEST v3 priv read MGMT access 20
R1(config)# snmp-server user USER1 TEST v3 auth sha p@ssw0rd priv aes 256 pa55word
R1(config)# snmp-server enable traps
R1(config)# snmp-server host 10.0.3.8 traps version 3 priv USER1 cpu ospf
R1(config)# snmp-server ifindex persist
```

```
R1#show snmp mib ifmib ifindex
GigabitEthernet0/1: Ifindex = 3
Loopback192: Ifindex = 12
Tunnel0: Ifindex = 9
Backplane-GigabitEthernet0/3: Ifindex = 4
FastEthernet0/0/1: Ifindex = 6
Embedded-Service-Engine0/0: Ifindex = 1
Null0: Ifindex = 7
GigabitEthernet0/0: Ifindex = 2
Tunnel1: Ifindex = 11
Virtual-Template1: Ifindex = 10
NVI0: Ifindex = 8
FastEthernet0/0/0: Ifindex = 5
R1#
```

©2023 by StormWind LLC. All rights reserved.

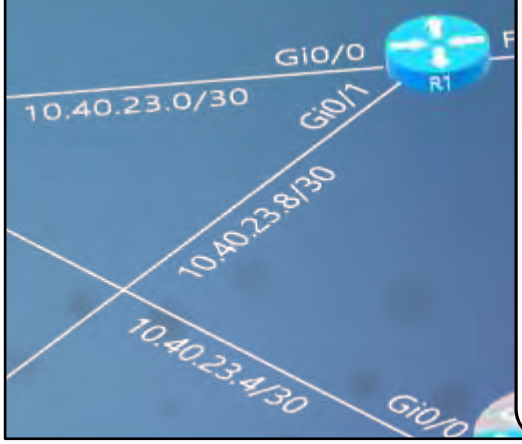
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification

```
R1#show snmp
Chassis: 4279256517
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
SNMP Dispatcher:
   queue 0/75 (current/max), 0 dropped
SNMP Engine:
   queue 0/1000 (current/max), 0 dropped

SNMP logging: enabled
    Logging to 10.0.3.8.162, 0/10, 0 sent, 0 dropped.
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification




```
R1#show snmp view
MGMT ifAdminStatus - included nonvolatile active
MGMT ifOperStatus - included nonvolatile active
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
cac_view interfaces - included read-only active
cac_view ip - included read-only active
cac_view ospf - included read-only active
cac_view bgp - included read-only active
cac_view dot1dBridge - included read-only active
cac_view ifMIB - included read-only active
cac_view nhrpMIB - included read-only active
cac_view ipMRouteStdMIB - included read-only active
cac_view igmpStdMIB - included read-only active
cac_view ospfv3MIB - included read-only active
cac_view ipForward - included read-only active
cac_view ipTrafficStats - included read-only active
cac_view ospfTrap - included read-only active
cac_view sysUpTime.0 - included read-only active
cac_view mplsLsrStdMIB - included read-only active
cac_view mplsLdpStdMIB - included read-only active
cac_view ciscoPingMIB - included read-only active
cac_view ciscoIpSecFlowMonitorMIB - included read-only active
cac_view ciscoIpSecPolMapMIB - included read-only active
cac_view ciscoPimMIB - included read-only active
cac_view ciscoBgp4MIB - included read-only active
cac_view ciscoIfExtensionMIB - included read-only active
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification

```
R1#show snmp user

User name: USER1
Engine ID: 800000090300CA0122F40006
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES256
Group-name: TEST

R1#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification

```
R1#show snmp user

User name: USER1
Engine ID: 800000090300CA0122F40006
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES256
Group-name: TEST

R1#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

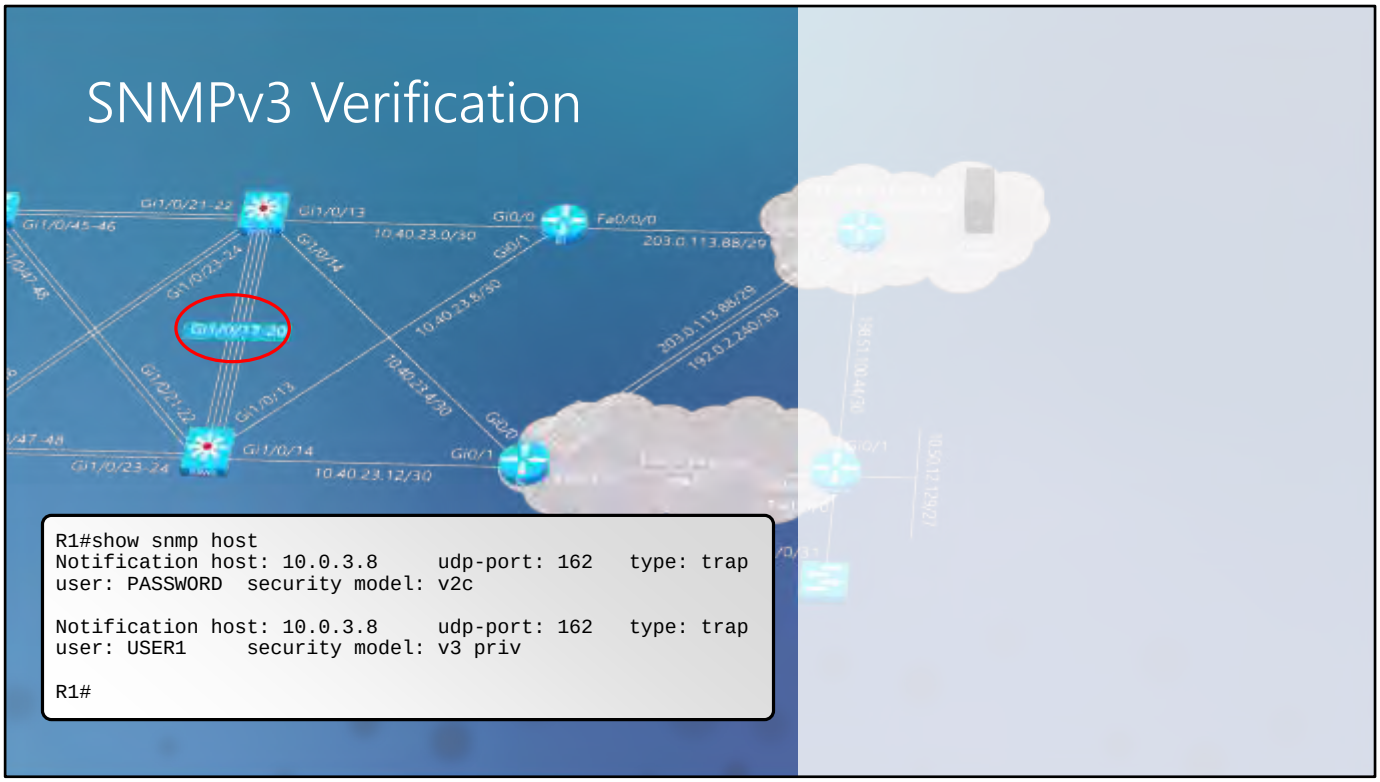
SNMPv3 Verification

```
R1#show snmp group
groupname: ILMI                                security model:v1
contextname: <no context specified>            storage-type: permanent
readview : *ilmi                               writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                                security model:v2c
contextname: <no context specified>            storage-type: permanent
readview : *ilmi                               writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: TEST                                security model:v3 priv
contextname: <no context specified>            storage-type: nonvolatile
readview : MGMT                                writeview: <no writeview
specified>
notifyview: *tv.00000000.00000000.00000800.0
row status: active

R1#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNMPv3 Verification

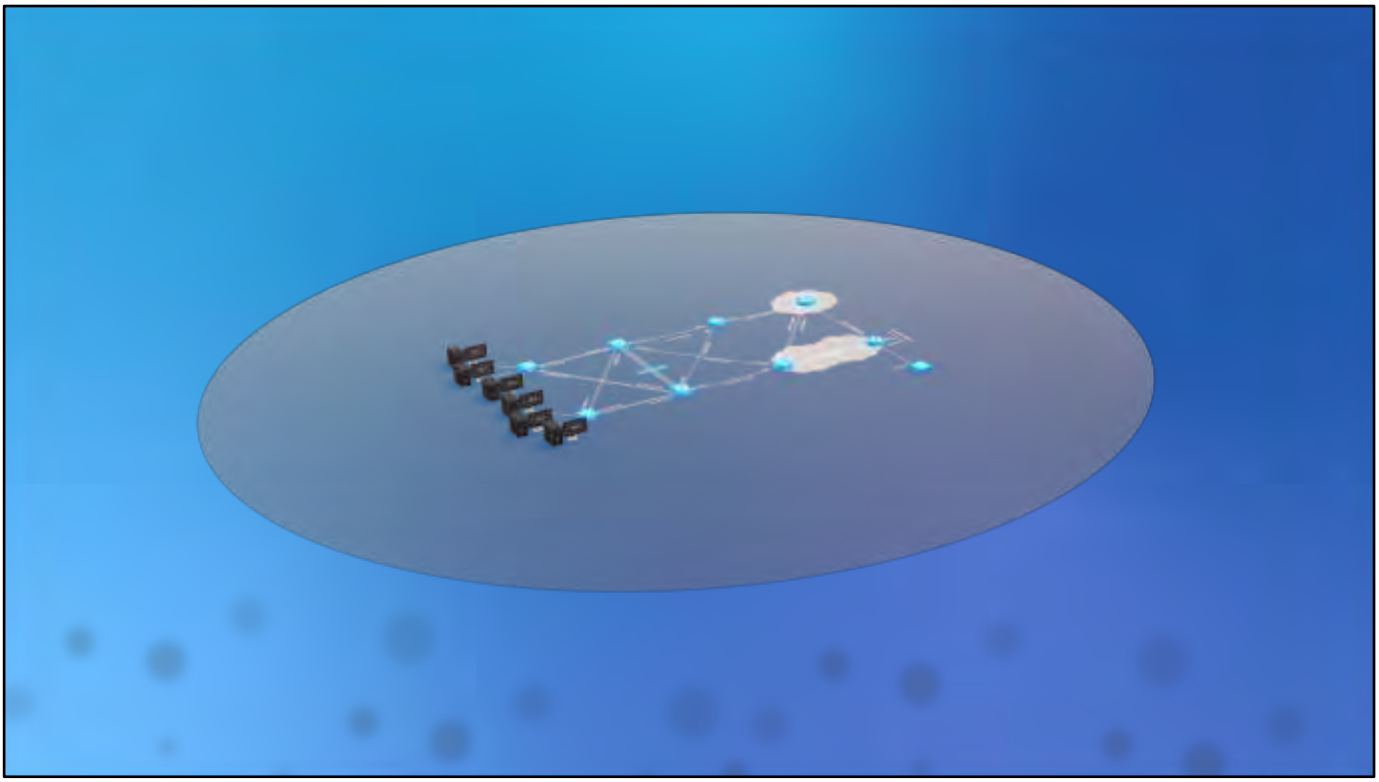



```
R1#show snmp host
Notification host: 10.0.3.8     udp-port: 162   type: trap
user: PASSWORD  security model: v2c

Notification host: 10.0.3.8     udp-port: 162   type: trap
user: USER1     security model: v3 priv

R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog Configuration and Verification

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog Overview

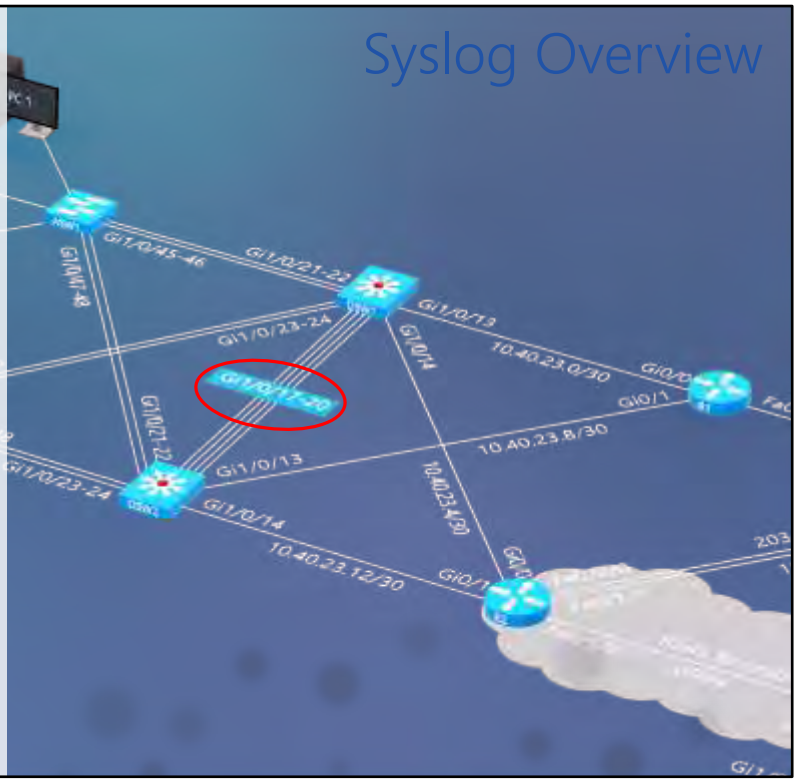
Syslog is used for monitoring and auditing.

Generally, when an event that is deemed important by a service occurs, the service generates a Syslog message to document the event.

On Cisco IOS devices, Syslog messages are sent to the console, vty lines, and ram by default.

Optimally, Syslog messages should be sent to a centralized repository such as a syslog server.

Syslog defines severity levels 0-7. The lower the number, the more severe the issue.



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog

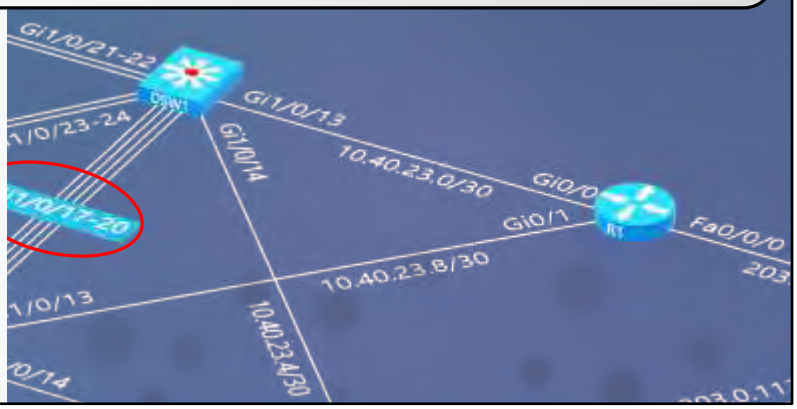
```
R1(config)#int gigabitEthernet 1/0
R1(config-if)#shut
R1(config-if)#
*Sep 22 13:05:08.981: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.12.2 (GigabitEthernet1/0) is down:
interface down
R1(config-if)#
*Sep 22 13:05:10.933: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively
down
*Sep 22 13:05:11.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state
to down
R1(config-if)#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog

```
R1(config)#int gigabitEthernet 1/0
R1(config-if)#shut
R1(config-if)#
*Sep 22 13:05:08.981: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.12.2 (GigabitEthernet1/0) is down:
interface down
R1(config-if)#
*Sep 22 13:05:10.933: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively
down
*Sep 22 13:05:11.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state
to down
R1(config-if)#
```

emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7

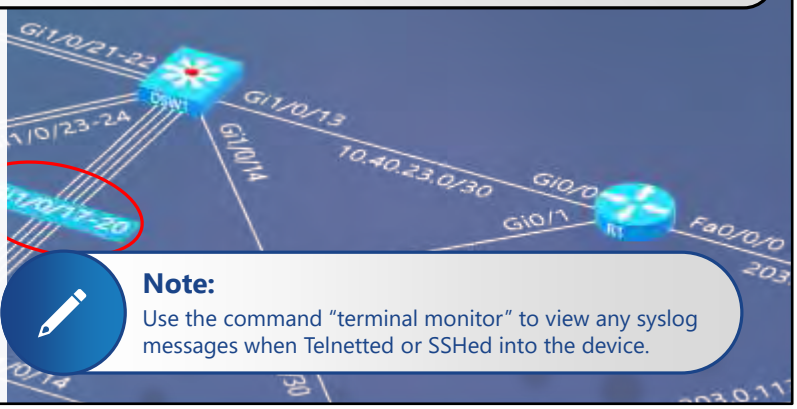


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog

```
R1(config)#int gigabitEthernet 1/0
R1(config-if)#shut
R1(config-if)#
*Sep 22 13:05:08.981: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.12.2 (GigabitEthernet1/0) is down:
interface down
R1(config-if)#
*Sep 22 13:05:10.933: %LINK-5-CHANGED: Interface GigabitEthernet1/0, changed state to administratively
down
*Sep 22 13:05:11.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state
to down
R1(config-if)#
```

emergencies	0
alerts	1
critical	2
errors	3
warnings	4
notifications	5
informational	6
debugging	7



Note:
Use the command "terminal monitor" to view any syslog messages when Telnetted or SSHed into the device.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

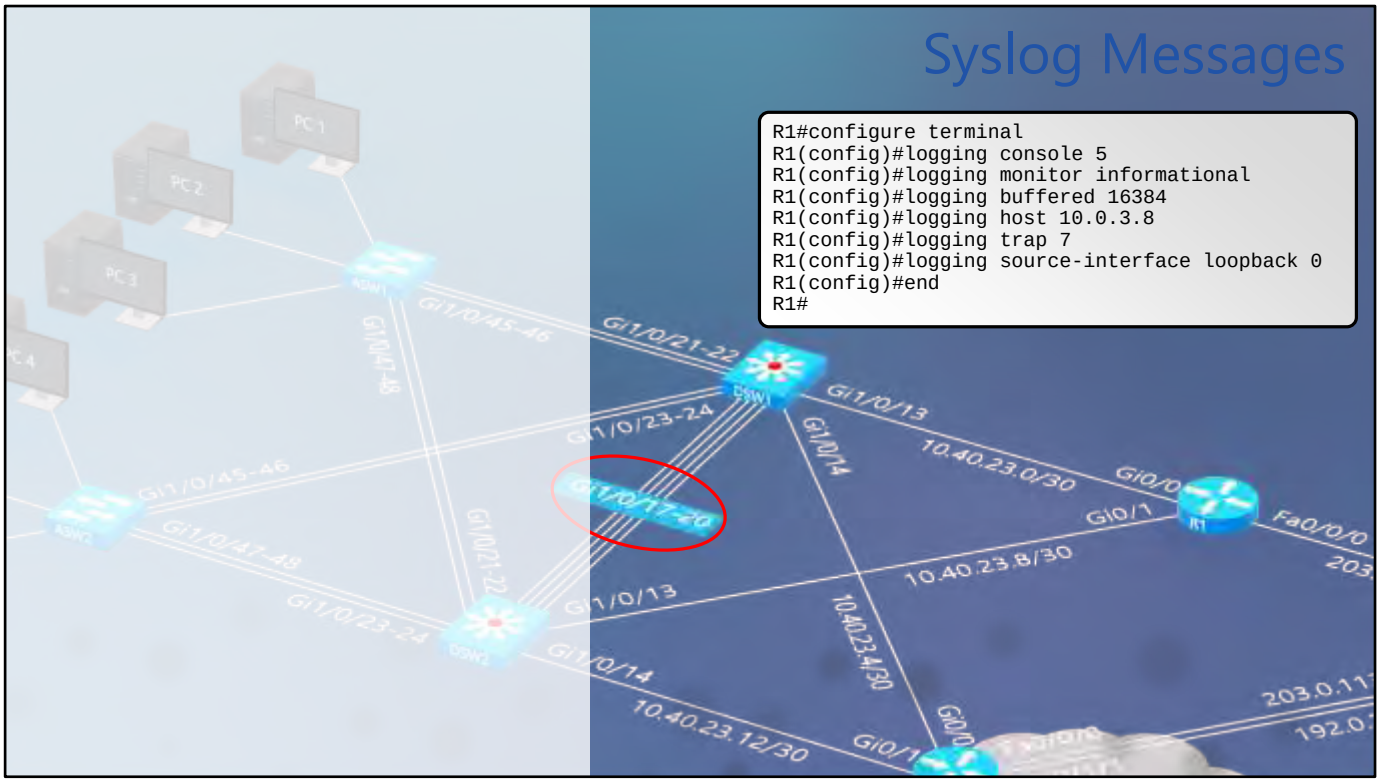
Syslog

```
R1#show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 56 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 56 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (8192 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 59 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (8192 bytes):

*Sep 19 11:31:36.883: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-table
No such file or directory
*Sep 19 11:31:38.711: %PLATFORM-3-PACONFIG: Exceeds 600 bandwidth points for slots
0, 1, 3 & 5
*Sep 19 11:31:51.699: %LINEPROTO-5-UPDOWN: Line protocol on Interface VoIP-Null0,
changed state to up
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog Messages

```
R1#configure terminal
R1(config)#logging console 5
R1(config)#logging monitor informational
R1(config)#logging buffered 16384
R1(config)#logging host 10.0.3.8
R1(config)#logging trap 7
R1(config)#logging source-interface loopback 0
R1(config)#end
R1#
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog

```
R1#show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

    Console logging: level notifications, 59 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level informational, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 0 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (8192 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level debugging, 65 message lines logged
        Logging to 10.0.3.8  (udp port 514, audit disabled,
              link up),
              5 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
        Loopback0

Log Buffer (16384 bytes):

***output omitted***
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Syslog and TLS

- Uses TLS to secure communication between client and server
  - Certificates
- Default port is
  - TCP 6514
- RFC 5425
- R2(config)#logging host 10.0.3.8 *vrf mgmt* transport tcp port 6514

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs, Conditional Debugs, Ping, and Traceroute

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

- Show commands are a snap-shot in time
  - Information provided at the moment you executed the command
- Debugs are real-time
  - Information provided as changes occur
    - Automatically sent to
      - Console
      - Monitor
      - Buffer

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

Example:

show ip route will not show you adds and deletes from the routing table

debug ip routing will show you adds and deletes from the routing table

```
R1#show ip route
…output omitted…

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.1/32 is directly connected, GigabitEthernet1/0
C        10.0.14.0/24 is directly connected, GigabitEthernet0/0
L        10.0.14.1/32 is directly connected, GigabitEthernet0/0
D        10.0.24.0/24 [90/3072] via 10.0.14.4, 00:23:29, GigabitEthernet0/0
                      [90/3072] via 10.0.12.2, 00:23:29, GigabitEthernet1/0
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.13.13.0/24 is directly connected, GigabitEthernet2/0
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

Example:

show ip route will not show you adds and deletes from the routing table

debug ip routing will show you adds and deletes from the routing table

```
R1#debug ip routing
IP routing debugging is on
R1#
*Sep 12 14:48:45.551: RT: updating eigrp 10.0.44.0/24 (0x0):
    via 10.0.14.4 Gi0/0  1048578

*Sep 12 14:48:45.555: RT: add 10.0.44.0/24 via 10.0.14.4, eigrp metric [90/3072]
*Sep 12 14:48:45.583: RT: updating eigrp 10.0.44.0/24 (0x0):
    via 10.0.14.4 Gi0/0  1048578

*Sep 12 14:48:45.587: RT: updating eigrp 10.0.44.0/24 (0x0):
    via 10.0.12.2 Gi1/0  1048578

*Sep 12 14:48:45.591: RT: rib update return code: 19
R1#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

Example:

show ip route will not show you adds and deletes from the routing table

debug ip routing will show you adds and deletes from the routing table

```
R1#show ip route
…output omitted…

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C        10.0.12.0/24 is directly connected, GigabitEthernet1/0
L        10.0.12.1/32 is directly connected, GigabitEthernet1/0
C        10.0.14.0/24 is directly connected, GigabitEthernet0/0
L        10.0.14.1/32 is directly connected, GigabitEthernet0/0
D        10.0.24.0/24 [90/3072] via 10.0.14.4, 00:26:48, GigabitEthernet0/0
                      [90/3072] via 10.0.12.2, 00:26:48, GigabitEthernet1/0
D        10.0.44.0/24 [90/3072] via 10.0.14.4, 00:02:34, GigabitEthernet0/0
      13.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        13.13.13.0/24 is directly connected, GigabitEthernet2/0
…output omitted…
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

- Invokes Process switching on the device
  - CPU needs to process the packet
  - Could slow down the device as it processes and generates debugs
- RISKS
  - Turning to many on at the same time
  - Leaving debugs enabled
- Use **undebug all (u all)** to disable all debugs that might be enabled

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Debugs

CISCO WARNING:

Use debug commands with caution. In general, it is recommended that these commands only be used under the direction of your router technical support representative when troubleshooting specific problems.

Enabling debugging can disrupt operation of the router when internetworks are experiencing high load conditions. Hence, if logging is enabled, the access server can intermittently freeze as soon as the console port gets overloaded with log messages.

Source: many cisco documents at www.cisco.com

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Conditional Debugs

Provides debug filtering to limit the output generated

***this list will vary based on device and IOS version

```
R1#debug condition ?
  application  Application
  called       called number
  calling      calling
  cpl          Cisco Provisioning Language debugging
  glbp         interface group
  interface    interface
  ip           IP address
  mac-address  MAC address
  match-list   apply the match-list
  profile      Media Services Profile
  standby      interface group
  username     username
  vcid         VC ID
  voice-port   voice-port number
  vrf          Virtual Routing and Forwarding
  xconnect     Xconnect conditional debugging on segment pair
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Conditional Debugs

```
R1#debug ip packet
IP packet debugging is on
R1#
*Sep 12 15:16:00.523: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:16:00.531: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending full packet
*Sep 12 15:16:02.691: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:16:02.695: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 12 15:16:02.931: IP: s=10.0.12.1 (local), d=224.0.0.10 (GigabitEthernet1/0), len 60, sending broad/multicast
*Sep 12 15:16:02.939: IP: s=10.0.12.1 (local), d=224.0.0.10 (GigabitEthernet1/0), len 60, sending full packet
*Sep 12 15:16:03.015: IP: s=10.0.12.2 (GigabitEthernet1/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:16:03.019: IP: s=10.0.12.2 (GigabitEthernet1/0), d=224.0.0.10
, len 60, input feature, packet consumed, MCI Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 12 15:16:04.419: IP: s=13.13.13.1 (local), d=13.13.13.3 (GigabitEthernet2/0), len 59, sending
*Sep 12 15:16:04.427: IP: s=13.13.13.1 (local), d=13.13.13.3 (GigabitEthernet2/0), len 59, sending full packet
*Sep 12 15:16:04.675: IP: s=13.13.13.3 (GigabitEthernet2/0), d=13.13.13.1, len 40, rcvd 0
*Sep 12 15:16:04.679: IP: s=13.13.13.3 (GigabitEthernet2/0), d=13.13.13.1, len 40, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 12 15:16:04.943: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:16:04.951: IP: s=10.0.14.1 (local), d=224.0.0.10
R1#(GigabitEthernet0/0), len 60, sending full packet
R1#u all
All possible debugging has been turned off
R1#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Conditional Debugs

```
R1#debug condition interface gigabitEthernet 0/0
Condition 1 set
R1#debug ip packet
IP packet debugging is on
R1#
*Sep 12 15:17:58.251: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:17:58.255: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
R1#
*Sep 12 15:17:59.495: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:17:59.503: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending full packet
R1#
*Sep 12 15:18:03.131: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:18:03.135: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
R1#
*Sep 12 15:18:04.227: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:18:04.235: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending full packet
R1#
*Sep 12 15:18:08.043: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, rcvd 0
*Sep 12 15:18:08.047: IP: s=10.0.14.4 (GigabitEthernet0/0), d=224.0.0.10, len 60, input feature, packet consumed, MCI
Check(101), rtype 0, forus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Sep 12 15:18:08.971: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending broad/multicast
*Sep 12 15:18:08.979: IP: s=10.0.14.1 (local), d=224.0.0.10 (GigabitEthernet0/0), len 60, sending full packet
R1#u all
All possible debugging has been turned off
R1#
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Ping

A tool that can be used to test connectivity between two devices

Character	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
Q	Source quench (destination too busy).
M	Could not fragment.
?	Unknown packet type.
&	Packet lifetime exceeded.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Traceroute

A tool that can be used to verify the path that traffic takes through the network.

Character	Description
nn msec	For each node, the round-trip time in milliseconds for the specified number of probes
*	The probe timed out
A	Administratively prohibited (example, access-list)
Q	Source quench (destination too busy)
I	User interrupted test
U	Port unreachable
H	Host unreachable
N	Network unreachable
P	Protocol Unreachable
T	Timeout
?	Unknown packet type

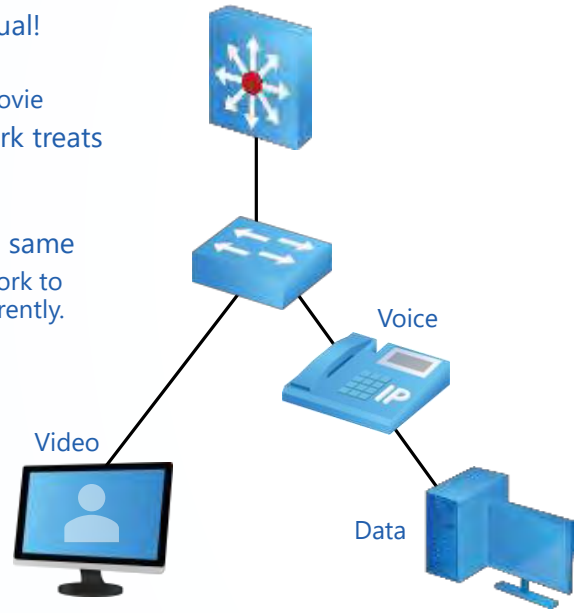
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Quality of Service (QoS) Overview

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

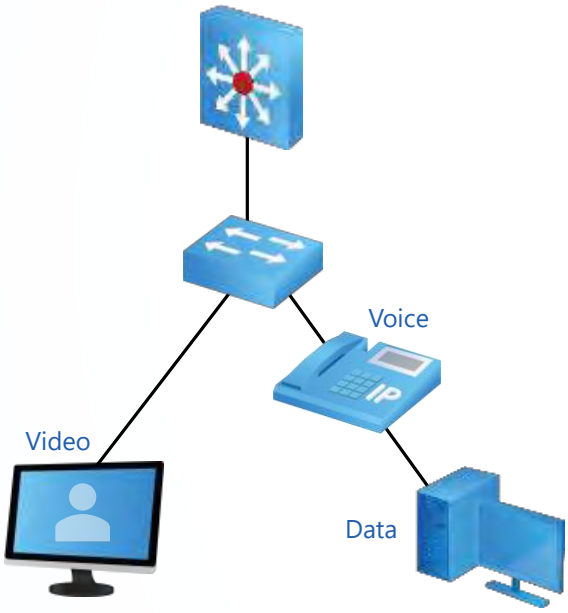
Quality of Service Overview

- All packets are not equal!
  - CEO on a VOIP call
  - You downloading a movie
- By default your network treats the packets the same.
  - Best-Effort
- But… They are not the same
  - QoS allows your network to treat the packets differently.



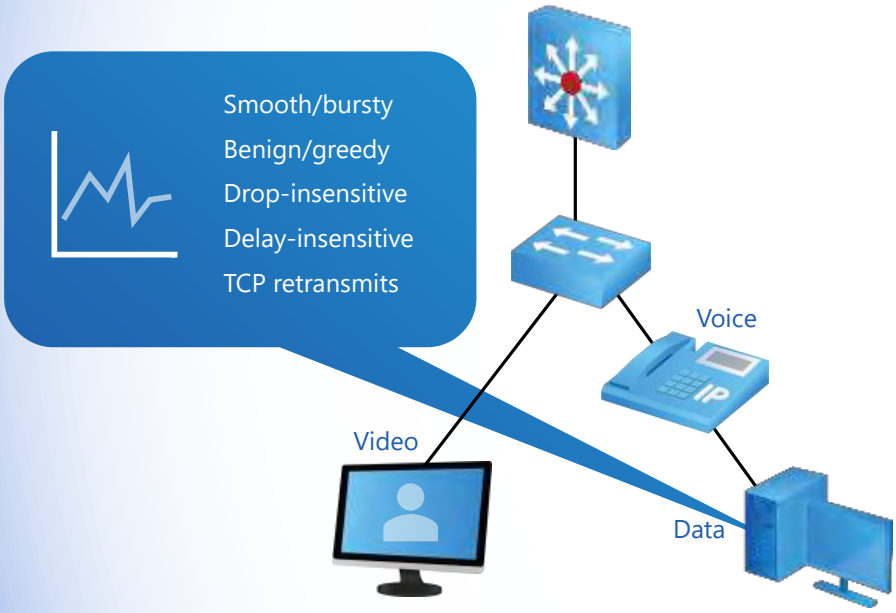
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Quality of Service Overview



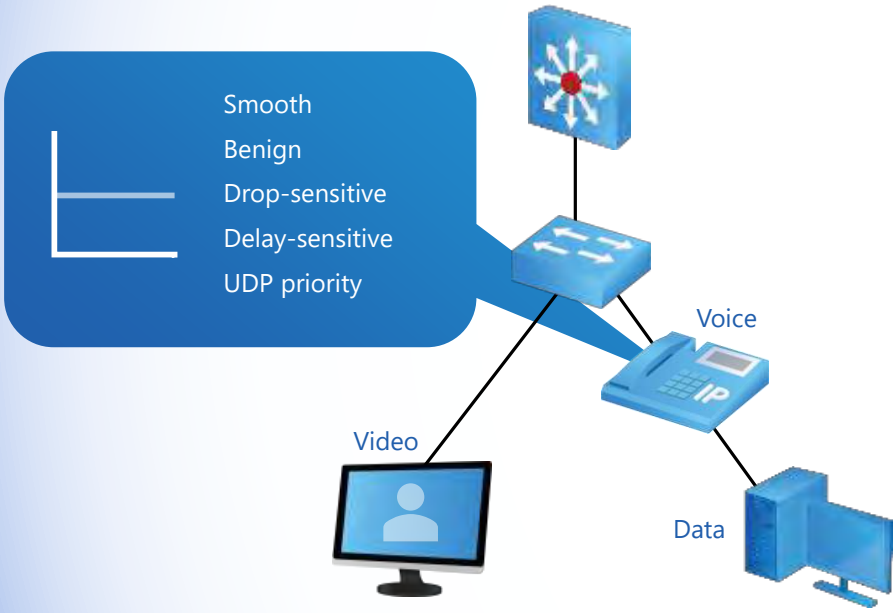
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Quality of Service Overview

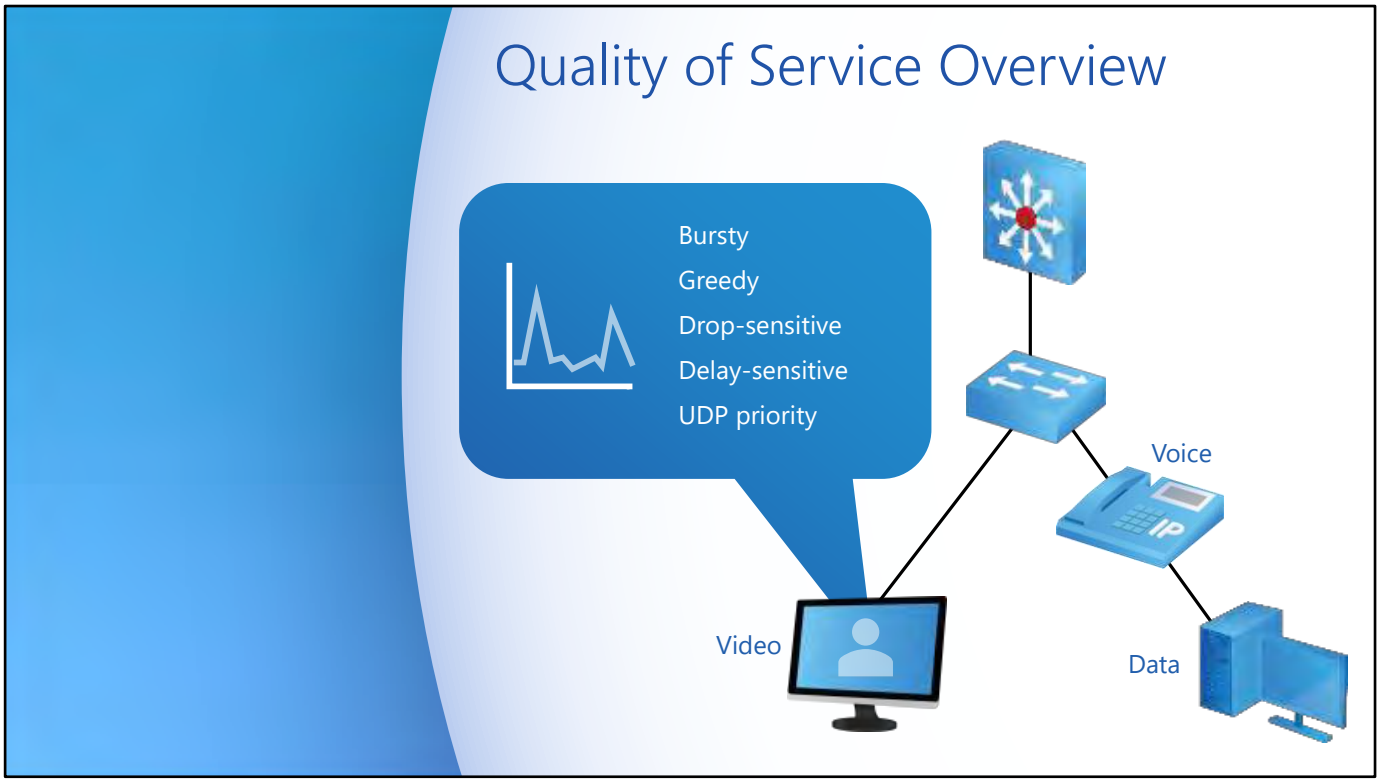


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Quality of Service Overview



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



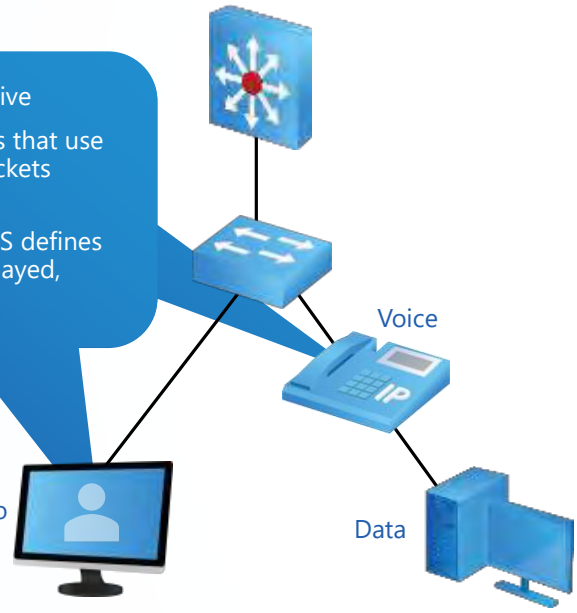
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Quality of Service Overview

Voice & Video are sensitive

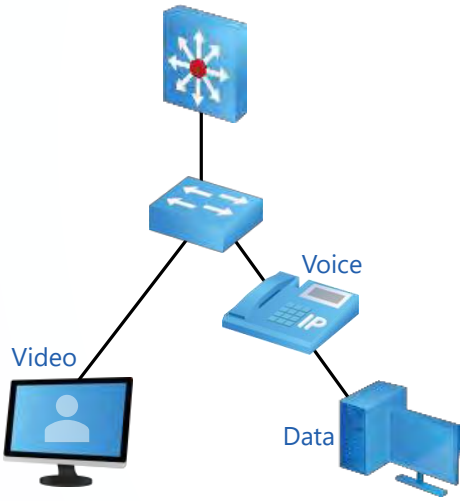
Unlike other applications that use TCP, Voice and Video packets **can't be retransmitted**

If there's congestion, QoS defines what gets expedited, delayed, and dropped



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

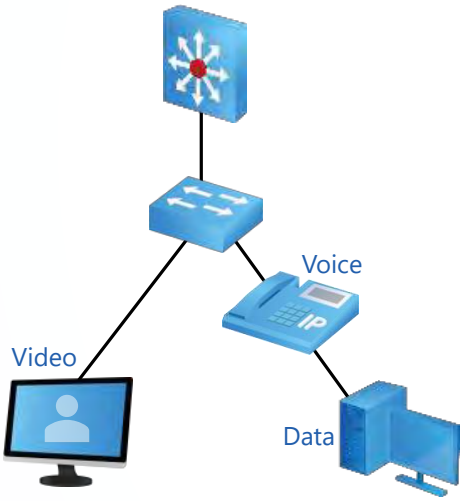
Quality of Service Overview



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Quality of Service Terminology

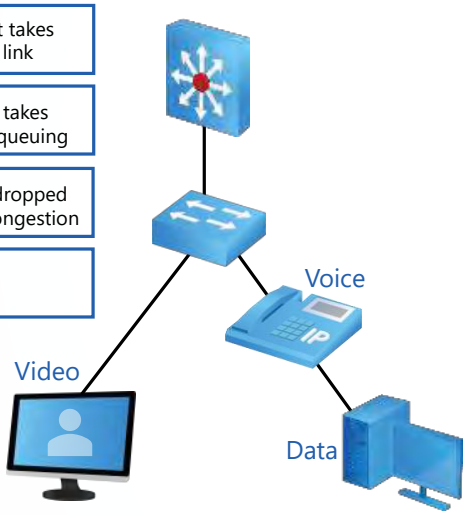
- Bandwidth
- Delay
- Jitter
- Loss
- Recommendations for VOIP



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Quality of Service Terminology

Bandwidth	Amount of data that can be transmitted over a link
Delay	Amount of time it takes traffic to traverse link
Jitter	Variation in time it takes over a link due to queuing
Loss	Amount of traffic dropped in transit due to congestion
Recommendations for VOIP	Delay: <150 ms Jitter: <30 ms Loss: <1%



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Best Effort vs QoS

Devices by default use FIFO

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Best Effort vs QoS

Devices by default use FIFO

Devices compete for bandwidth

Packets are sent to Queue

No guarantee

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

QoS Mechanisms

Classification

Identify within the chassis the different types of traffic

Marking

Modify/Alter the type of service byte in the IPv4 header or **802.1p field** within an 802.1q trunk to encode the classification into the packet or frame header

Congestion Management

Queuing techniques which will manage how traffic is handled when congestion occurs

Traffic Policing

Mark or drop excess traffic

Causes TCP retransmissions

Does not introduce delay or jitter

Performed near source

Traffic Shaping

Queue / slow down / delay excess traffic

Accomplished with buffering

Introduces delay and jitter

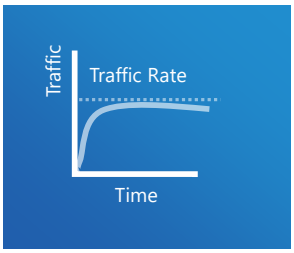
WRED

A technique for Congestion Avoidance

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

QoS Mechanisms



Traffic Policing

Mark or drop excess traffic

Causes TCP retransmissions

Does not introduce delay or jitter

Performed near source

Traffic Shaping

Queue / slow down / delay excess traffic

Accomplished with buffering

Introduces delay and jitter

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

ToS and CoS Markings

Marking is possible in the IPv4, IPv6 and 802.1q headers

Layer 3 marking is called Type of Service (ToS) or (DSCP)

Layer 2 wired marking is called Class of Service (COS)

Layer 2 Wireless is Traffic Identifier (TID)

MPLS has an MPLS EXP value

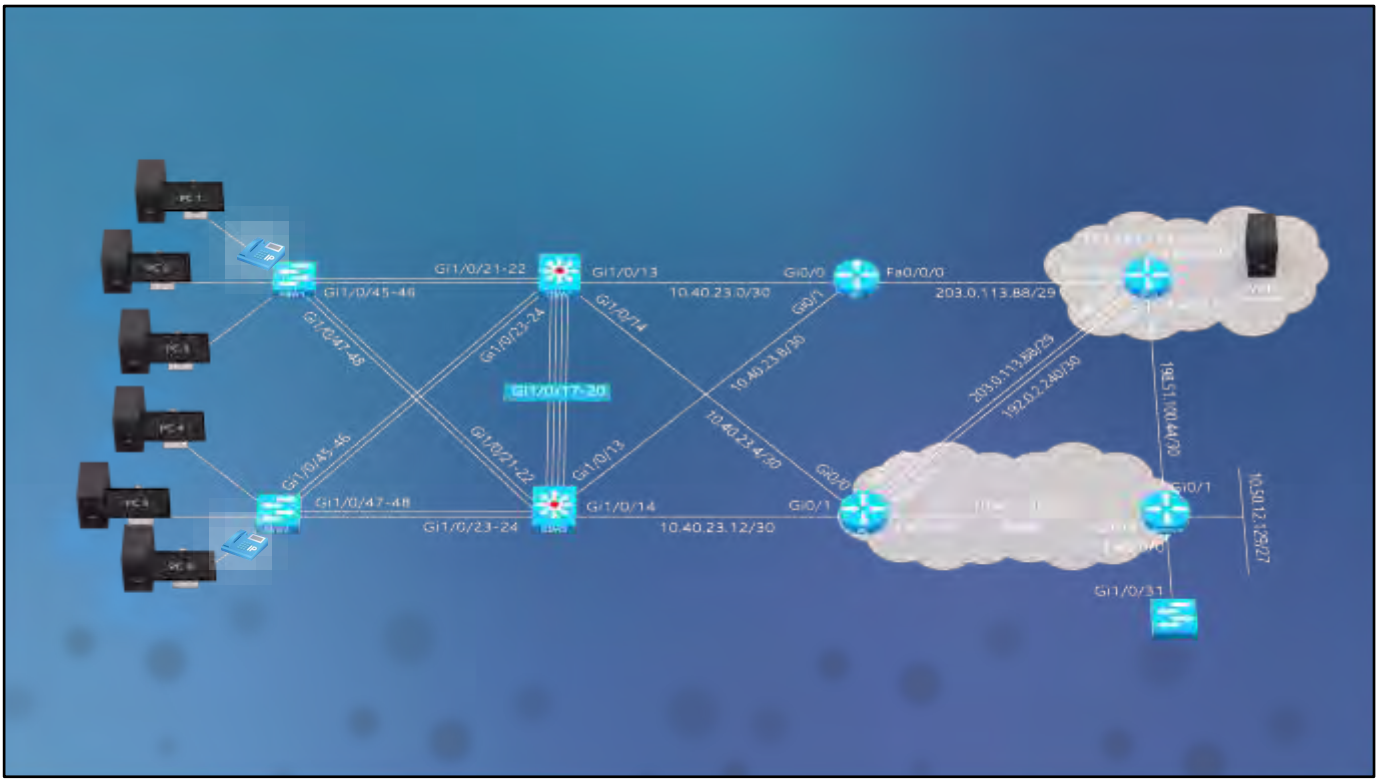
Version	**IHL**	**Service Type**	**Total Length**	
Identification			Flag	Fragment Offset
TTL		Protocol	Checksum	
Source Address				
Destination Address				
Options				Padding

802.1p CoS marking

Destination Address	Source Address	802.1Q VLAN Tag	Type/Len	Data	Frame Check

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

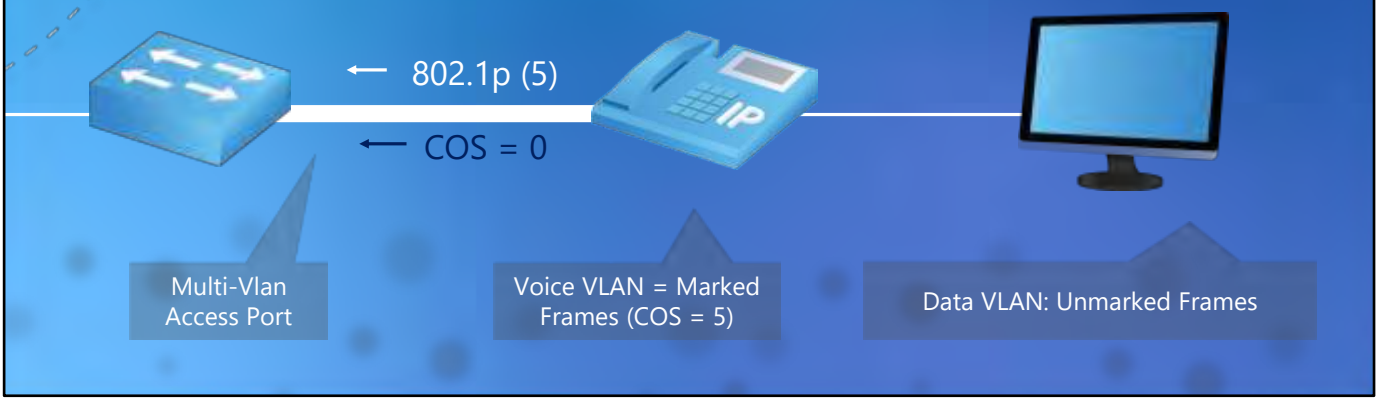


©2023 by StormWind LLC. All rights reserved.

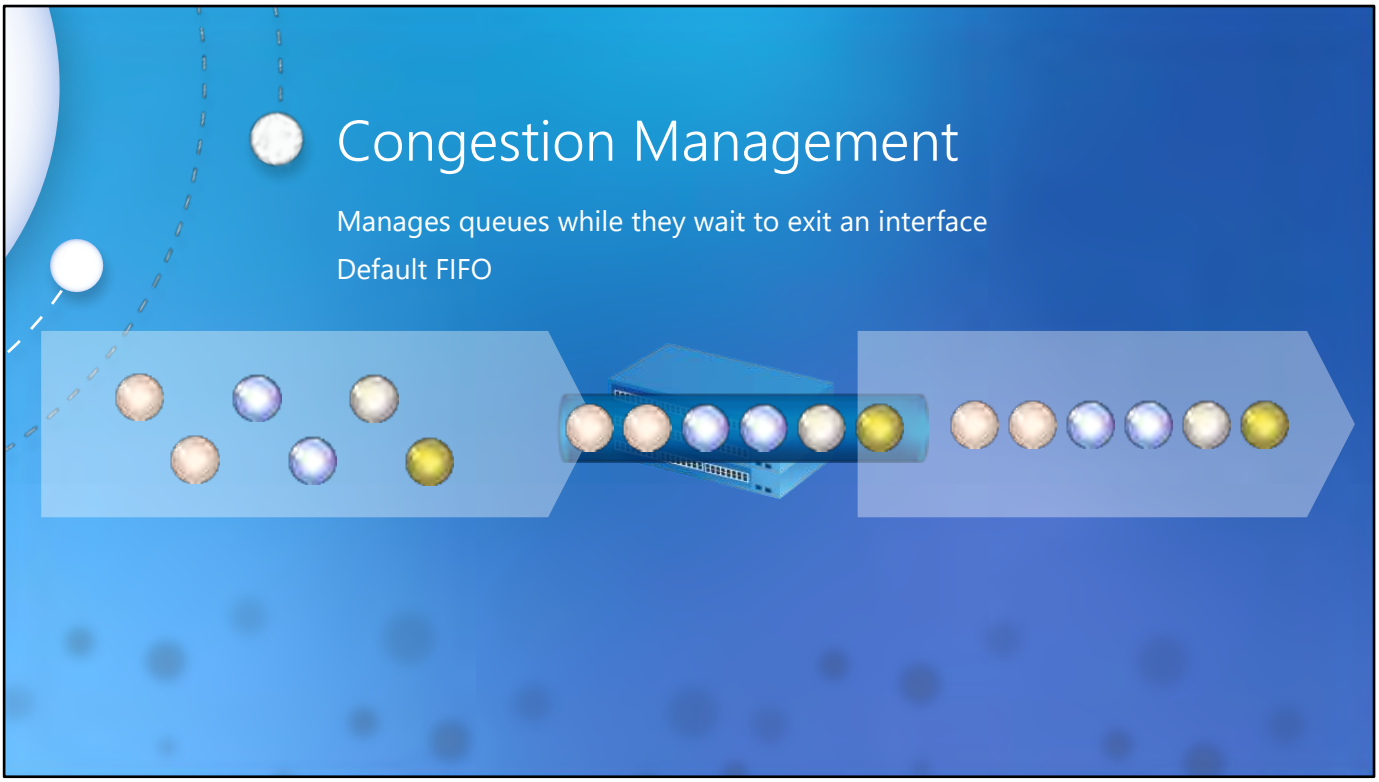
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Trust Boundary

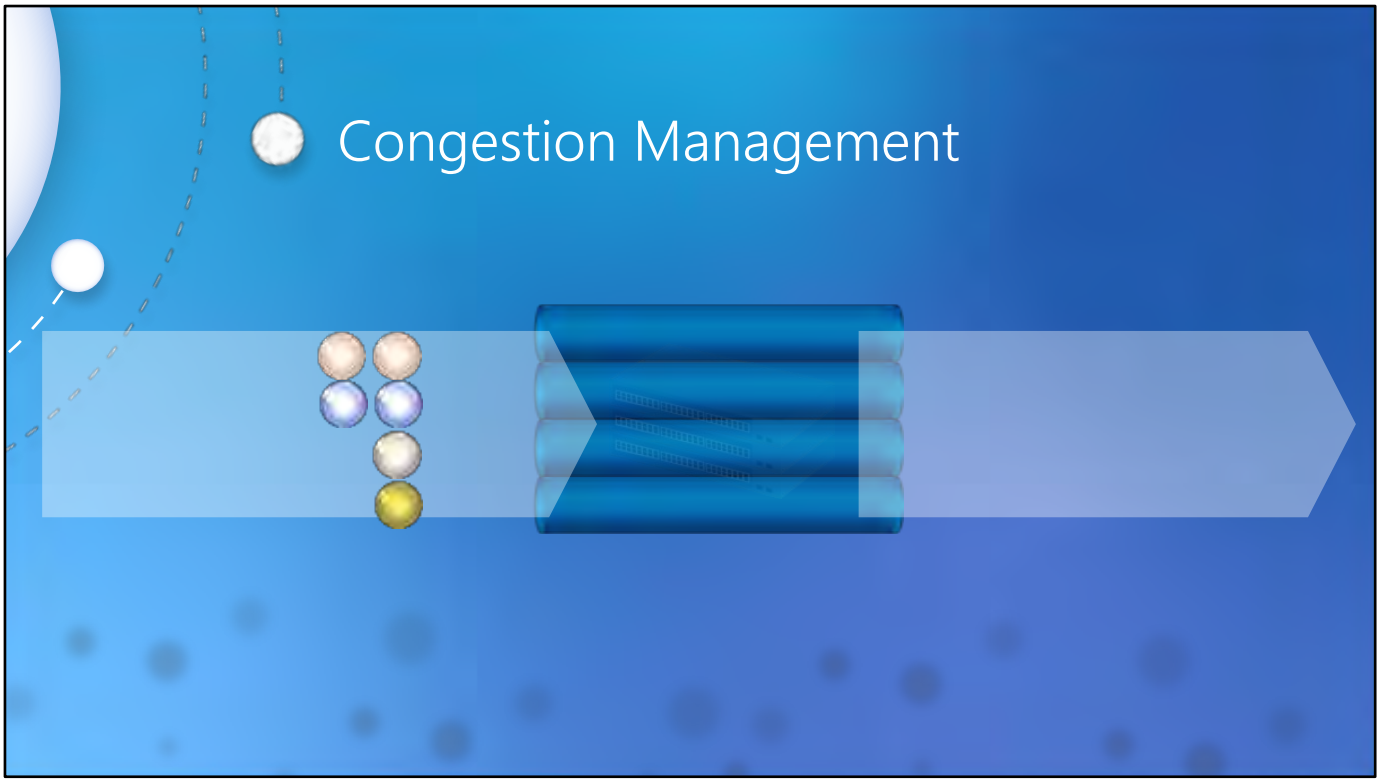
Traffic sent from the IP phone to the switch is trusted to ensure that voice traffic is properly prioritized.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Congestion Management

Queuing system will need a **Classifier** to choose what traffic is placed into each queue

Scheduler performs **Prioritization** specifying one queue is more preferred over another

Example: Round Robin takes turns processing each queue in order by packets or bytes

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Congestion Management Queueing

Queueing	Description
First-In-First-Out (FIFO)	*Default* queuing method, where packets are processed and forwarded out an interface in the order they arrive, without any specific prioritization.
Priority Queuing (PQ)	Uses *4 priority based queues* and assigns different priority levels to traffic classes, and high-priority traffic is forwarded ahead of lower-priority traffic.
Weighted Fair Queuing (WFQ)	A flow-based queuing method that *uses store and forwarding queues* and allocates bandwidth proportionally to different flows based on their weight.
Class-Based Weighted Fair Queuing (CBWFQ)	Extends WFQ by allowing you to define traffic classes based on various criteria. You can then allocate bandwidth and apply QoS policies to each class. Adding an LLQ *provides guaranteed bandwidth and strict-priority servicing to a specified class of traffic such as voice.*
Custom Queuing (CQ)	allows you to configure a specific number of queues and allocate bandwidth to each queue manually. So, you can *specify the number of bytes in a specific queue that should be delt with before working on the next queues*.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Weighted Random Early Detection

Congestion avoidance feature of QoS

- When a queue is filling up WRED can determine which packets are high priority and which packets are low priority.
  - It will then selectively drop based on a weighting
    - The lower priority packets are dropped before the queue fills up

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

MQC uses three main configuration elements:

class-map = Identify traffic to match

policy-map = Define what happens to the traffic that matches (create a schedular)

service-policy = Applies policy to interface

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

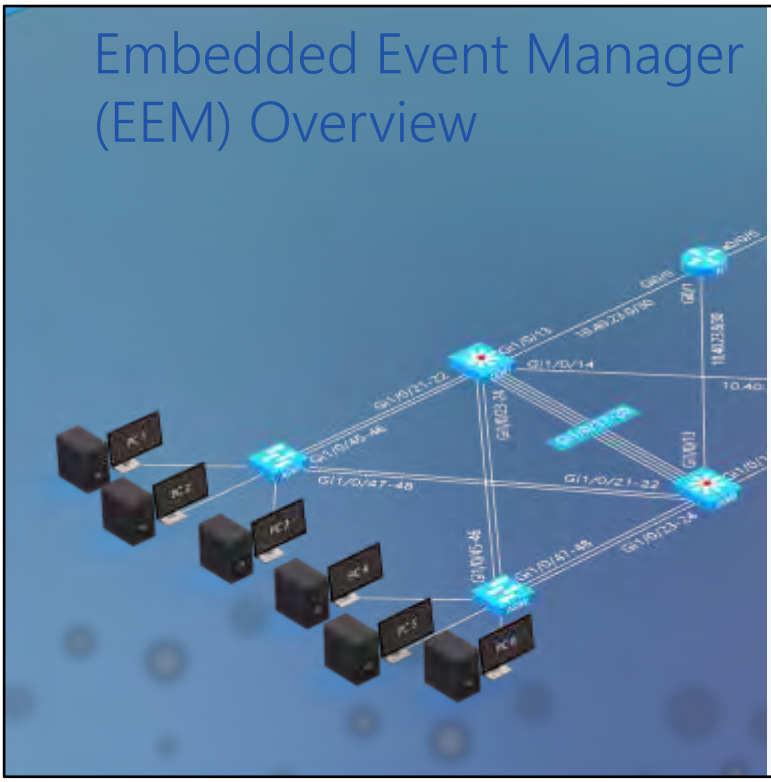
ENCOR Automation Preparation

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Embedded Event Manager (EEM)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

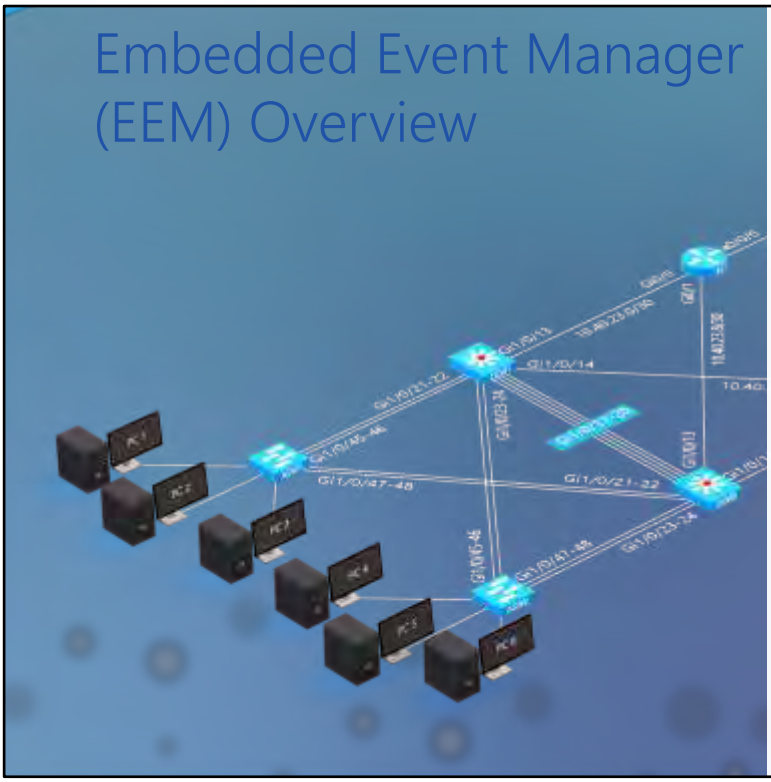
Embedded Event Manager (EEM) Overview



- A tool that provides automated event detection and recovery
- EEM Policy
  - Defines Event and Action to be taken
    - Applet
      - Defined in CLI
    - Script
      - Defined in TCL (Tool Command Language)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Embedded Event Manager (EEM) Overview



The creation of an EEM policy involves:

- Naming and registering the applet
- Selecting the event for which the applet is run and defining the event detector options associated with logging and responding to the event.
- Choosing the actions to be performed when the event occurs.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EEM Event Detectors

Determines when the event occurs

- Application-Specific Event
- CLI Event
- Counter Event
- Custom CLI Event
- Enhanced Object Tracking Event
- GOLD Event
- IP SLA Event
- NetFlow Event
- None Event
- OIR Event
- Resource Event
- RF Event
- RPC Event
- Routing Event
- SNMP Event
- SNMP Notification Event
- SNMP Object Event
- Syslog Event
- Systems Manager Event
- Timer Event
- Watchdog System Monitor Event (for Cisco IOS)

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

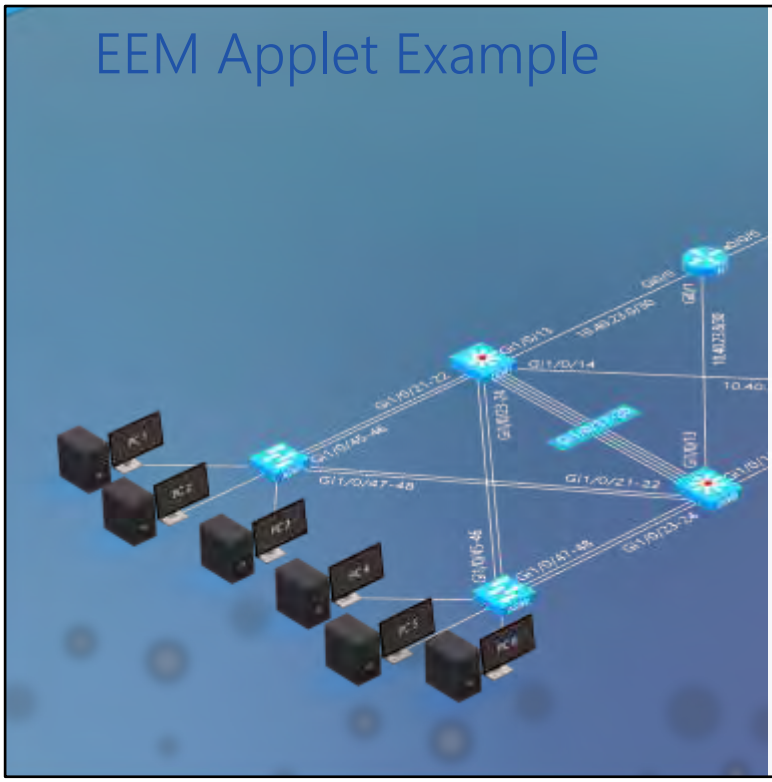
EEM Actions

Corrective actions that occur when an event detector reports an event

- Executing a Cisco IOS command-line interface (CLI) command.
- Generating a CNS event for upstream processing by Cisco CNS devices.
- Setting or modifying a named counter.
- Switching to a secondary processor in a fully redundant hardware configuration.
- Requesting system information when an event occurs.
- Sending a short e-mail.
- Manually running an EEM policy.
- Publishing an application-specific event.
- Reloading the Cisco software.
- Generating an SNMP trap.
- Generating prioritized syslog messages.
- Reading the state of a tracked object.
- Setting the state of a tracked object.
- Print text in the terminal window.

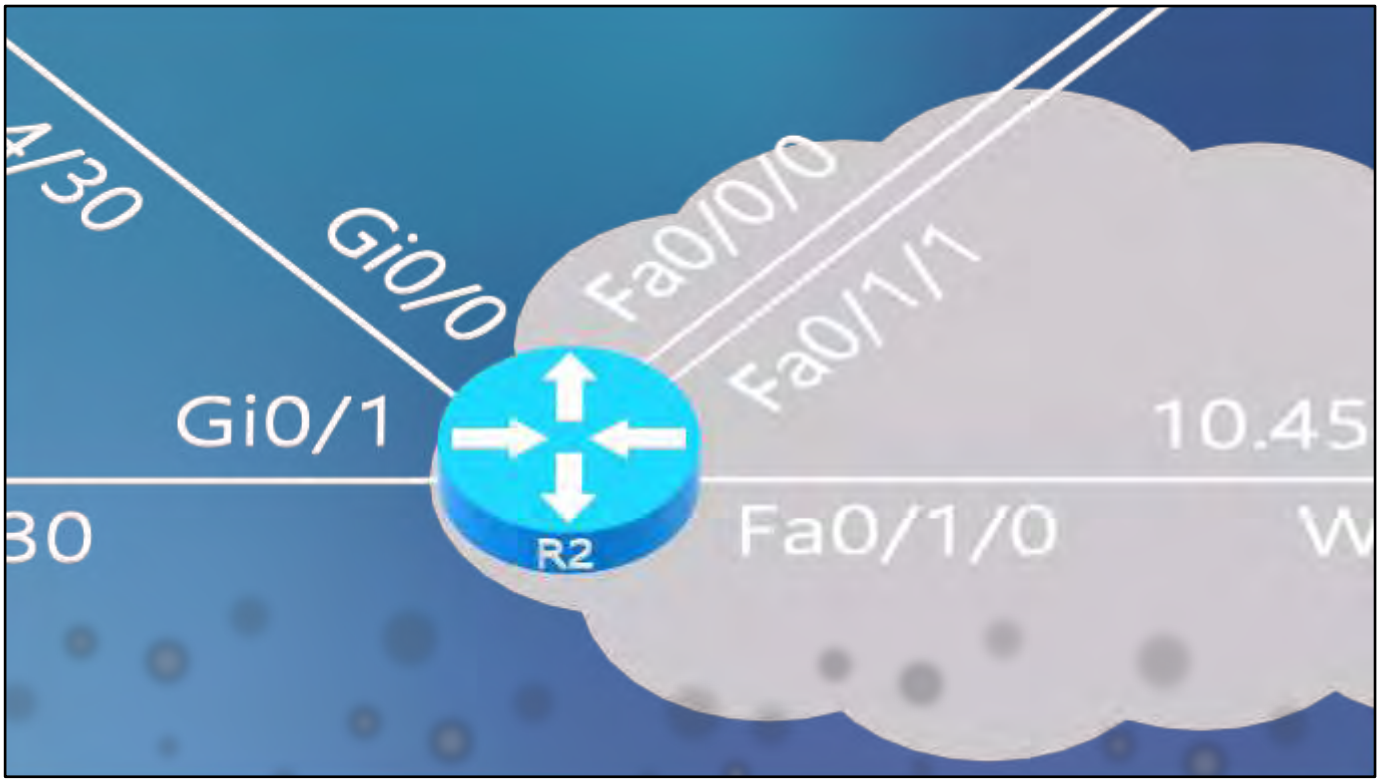
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EEM Applet Example



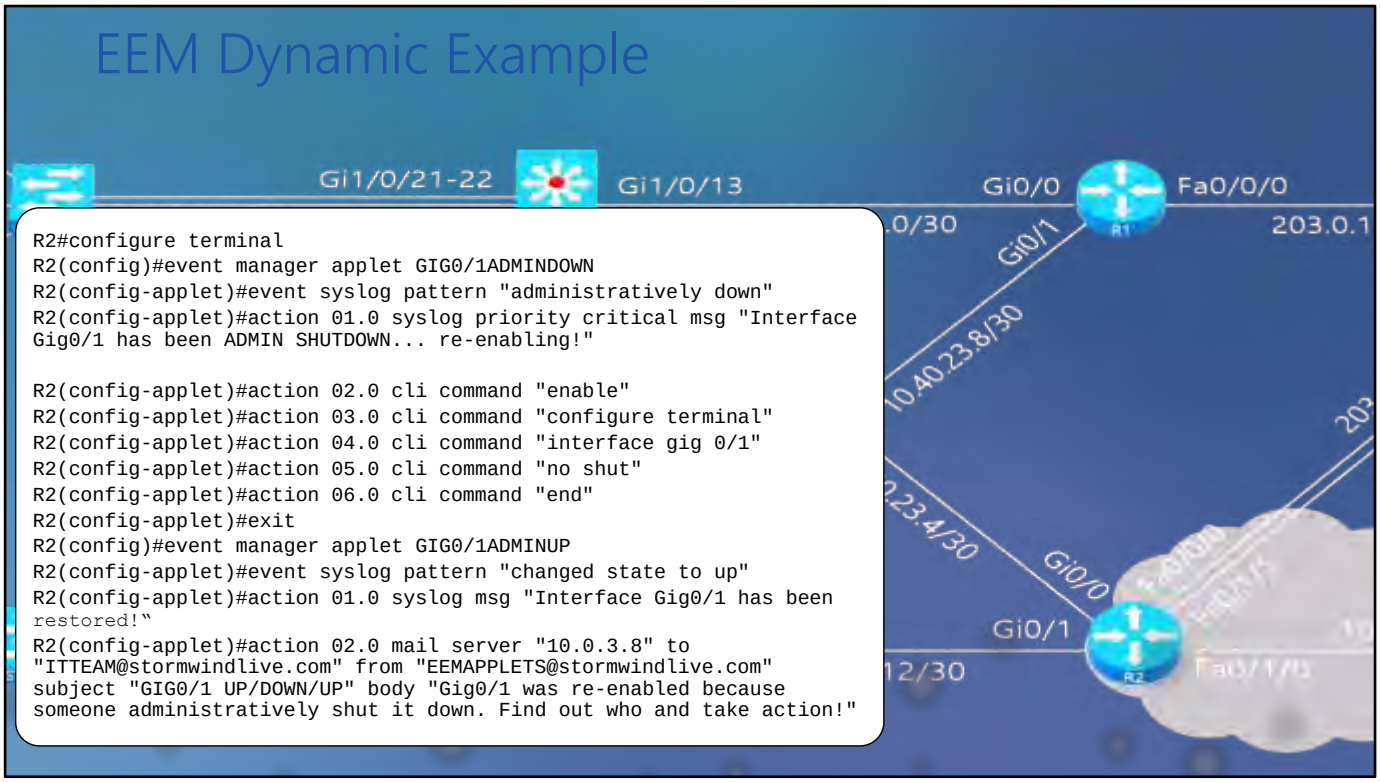
- Name and register the applet
- Event
  - Specify the event criteria to trigger the applet to run
  - Only 1 is allowed per applet configuration
- Action
  - Specify the action to perform when the EEM applet is triggered
  - Multiple actions are allowed per applet configuration

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EEM Dynamic Example




```
R2#configure terminal
R2(config)#event manager applet GIG0/1ADMINDOWN
R2(config-applet)#event syslog pattern "administratively down"
R2(config-applet)#action 01.0 syslog priority critical msg "Interface
Gig0/1 has been ADMIN SHUTDOWN... re-enabling!"

R2(config-applet)#action 02.0 cli command "enable"
R2(config-applet)#action 03.0 cli command "configure terminal"
R2(config-applet)#action 04.0 cli command "interface gig 0/1"
R2(config-applet)#action 05.0 cli command "no shut"
R2(config-applet)#action 06.0 cli command "end"
R2(config-applet)#exit
R2(config)#event manager applet GIG0/1ADMINUP
R2(config-applet)#event syslog pattern "changed state to up"
R2(config-applet)#action 01.0 syslog msg "Interface Gig0/1 has been
restored!"
R2(config-applet)#action 02.0 mail server "10.0.3.8" to
"ITTEAM@stormwindlive.com" from "EEMAPPLETS@stormwindlive.com"
subject "GIG0/1 UP/DOWN/UP" body "Gig0/1 was re-enabled because
someone administratively shut it down. Find out who and take action!"
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EEM Manual Example with PUTs

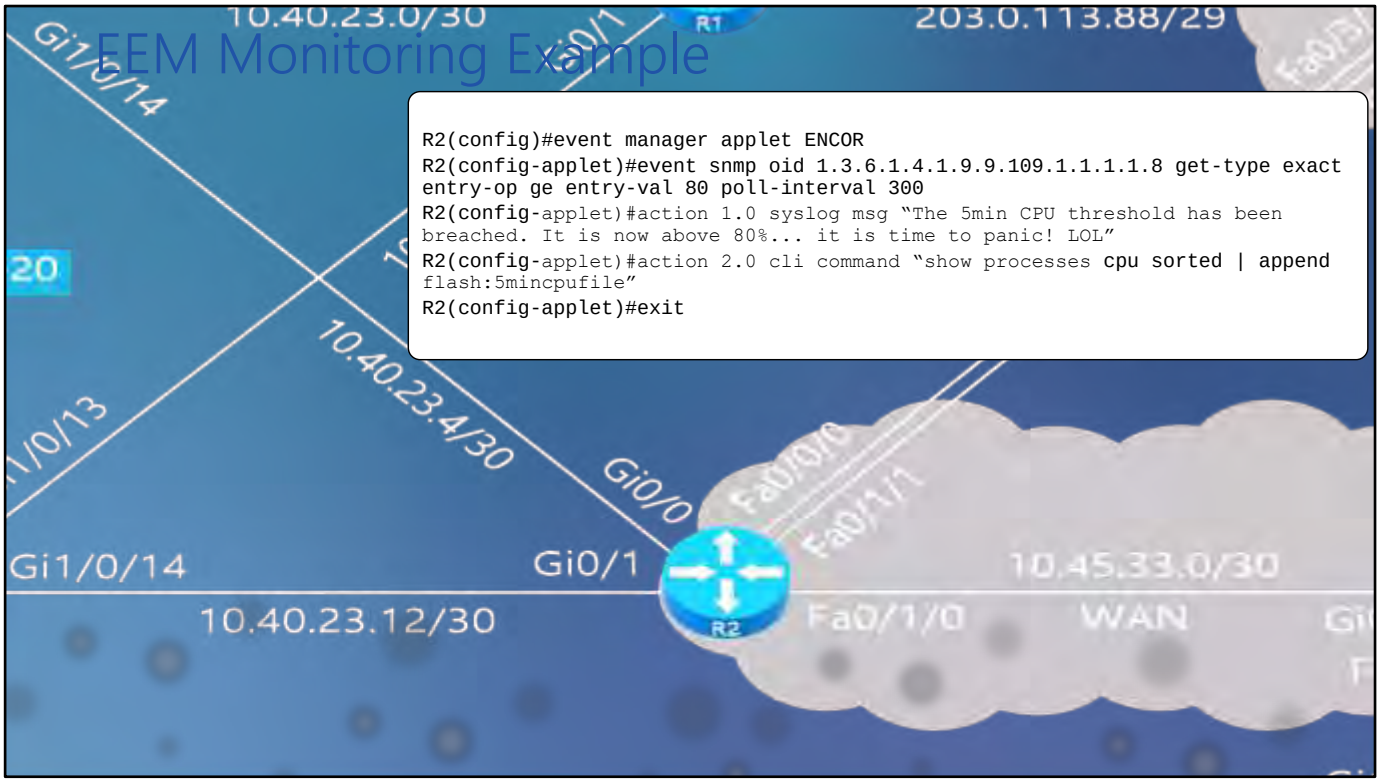
```
R2#config terminal
R2(config)#event manager applet EXAMPLE_MANUAL_POLICY
R2(config-applet)# event none
R2(config-applet)# action 01.0 syslog msg "My example manual-policy has been triggered!!!"
R2(config-applet)# action 02.0 cli command "enable"

R2(config-applet)# action 03.0 cli command "configure terminal"
R2(config-applet)# action 04.0 cli command "interface gig 0/1"
R2(config-applet)# action 05.0 cli command "shut"
R2(config-applet)# action 06.0 cli command "end"
R2(config-applet)# action 07.0 cli command "copy run flash:/config.txt"
R2(config-applet)# action 08.0 puts "Interface gig 0/1 is now disabled because someone ran
the manual policy!!!"
R2(config-applet)# end
R2#
R2#event manager run EXAMPLE_MANUAL_POLICY
R2#
Interface gig 0/1 is now disabled because someone ran the manual policy!!!

R2#
*Jul  8 12:22:31.073: %HA_EM-6-LOG: EXAMPLE_MANUAL_POLICY: My example manual-policy has
been triggered!!!
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EEM Monitoring Example

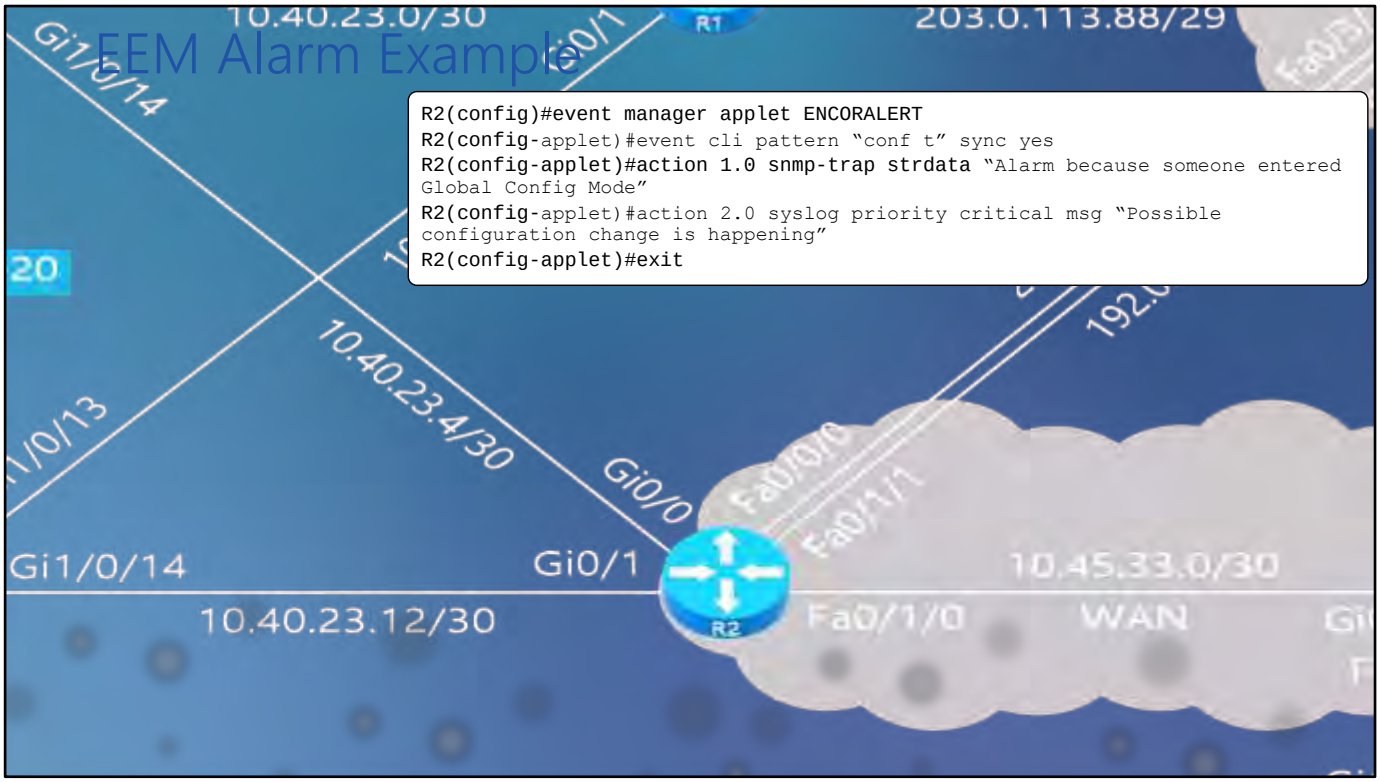
```
R2(config)#event manager applet ENCOR
R2(config-applet)#event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.8 get-type exact
entry-op ge entry-val 80 poll-interval 300
R2(config-applet)#action 1.0 syslog msg "The 5min CPU threshold has been
breached. It is now above 80%... it is time to panic! LOL"
R2(config-applet)#action 2.0 cli command "show processes cpu sorted | append
flash:5mincpufile"
R2(config-applet)#exit
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EEM Alarm Example

```
R2(config)#event manager applet ENCORALERT
R2(config-applet)#event cli pattern "conf t" sync yes
R2(config-applet)#action 1.0 snmp-trap strdata "Alarm because someone entered Global Config Mode"
R2(config-applet)#action 2.0 syslog priority critical msg "Possible configuration change is happening"
R2(config-applet)#exit
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

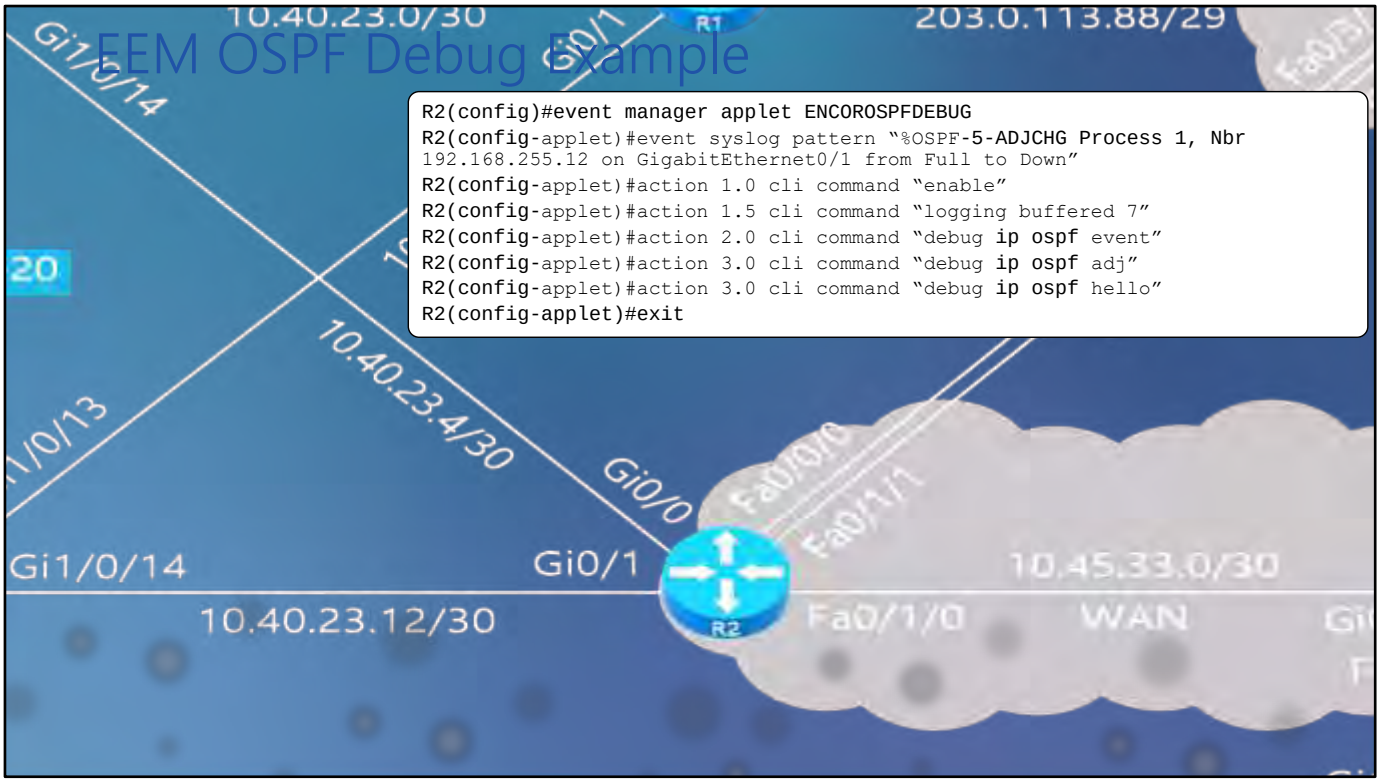
IPSLA and Tracking Object Example

```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 8.8.8.8
R1(config-ip-sla-echo)#frequency 5
R1(config-ip-sla-echo)#exit
R1(config)#ip sla  schedule 1 start-time now life forever
R1(config)#
R1(config)#track 15 ip sla 1 reachability
R1(config-track)#exit
R1(config)#
R1(config)#event manager applet TRACKIPSLA
R1(config-applet)#event track 15 state down
R1(config-applet)#action 1.0 syslog msg "THE IPSLA PROBE IS BROKEN!!!!"
priority 1
R1(config-applet)#exit
R1(config)#end

.....Connectivity to 8.8.8.8 fails.....

R1#
.Oct 16 12:31:49.343: %TRACK-6-STATE: 15 ip sla 1 reachability Up -> Down
R1#
.Oct 16 12:31:49.343: %HA_EM-1-LOG: TRACKIPSLA: THE IPSLA PROBE IS BROKEN!!!!
R1#
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EEM OSPF Debug Example

```
R2(config)#event manager applet ENCOROSPFDEBUG
R2(config-applet)#event syslog pattern "%OSPF-5-ADJCHG Process 1, Nbr
192.168.255.12 on GigabitEthernet0/1 from Full to Down"
R2(config-applet)#action 1.0 cli command "enable"
R2(config-applet)#action 1.5 cli command "logging buffered 7"
R2(config-applet)#action 2.0 cli command "debug ip ospf event"
R2(config-applet)#action 3.0 cli command "debug ip ospf adj"
R2(config-applet)#action 3.0 cli command "debug ip ospf hello"
R2(config-applet)#exit
```



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

DNA Center Overview

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Cisco DNA Center

Central management plane for building and operating the fabric

Controller-based SDN solution

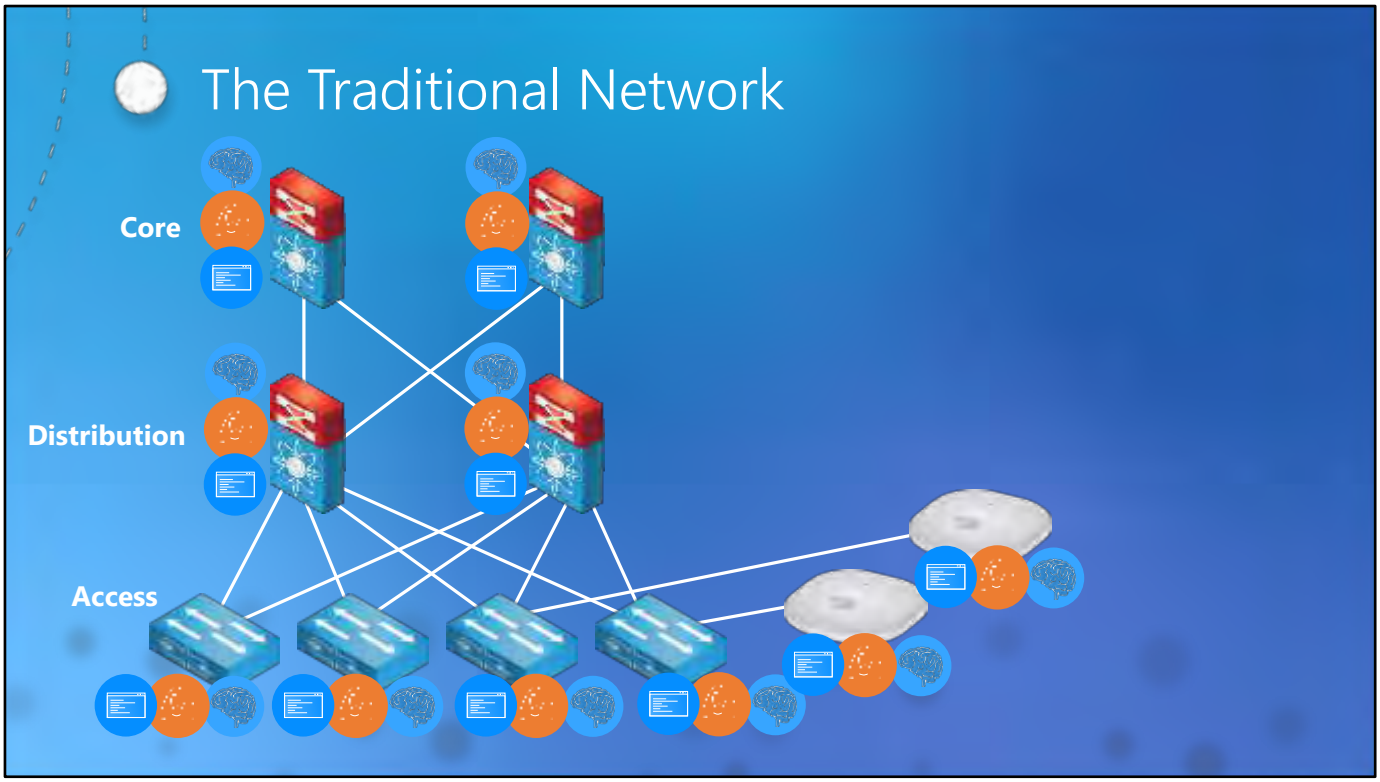
Provides:

Automation, Policy, Assurance, Integration

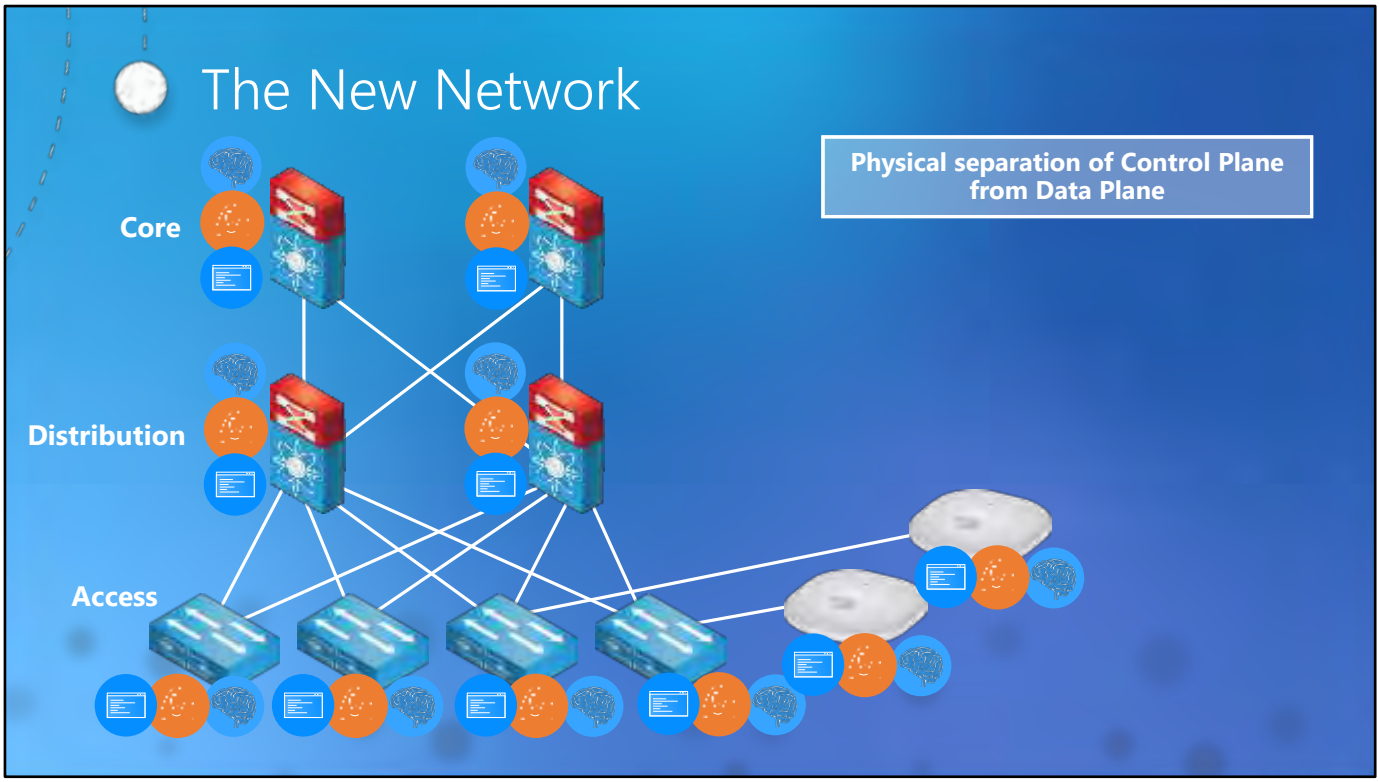
Responsible for:

Forwarding configuration
Policy distribution
Device management
Analytics

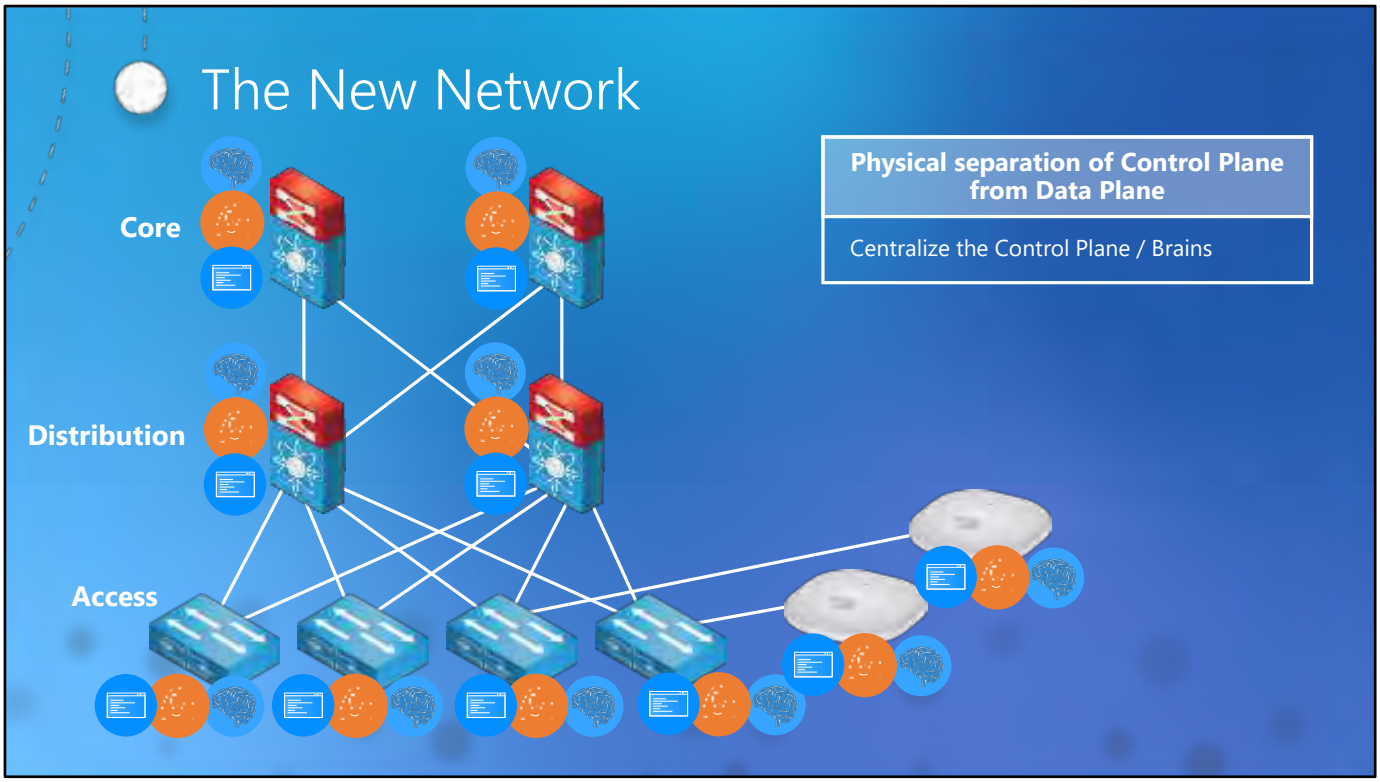
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



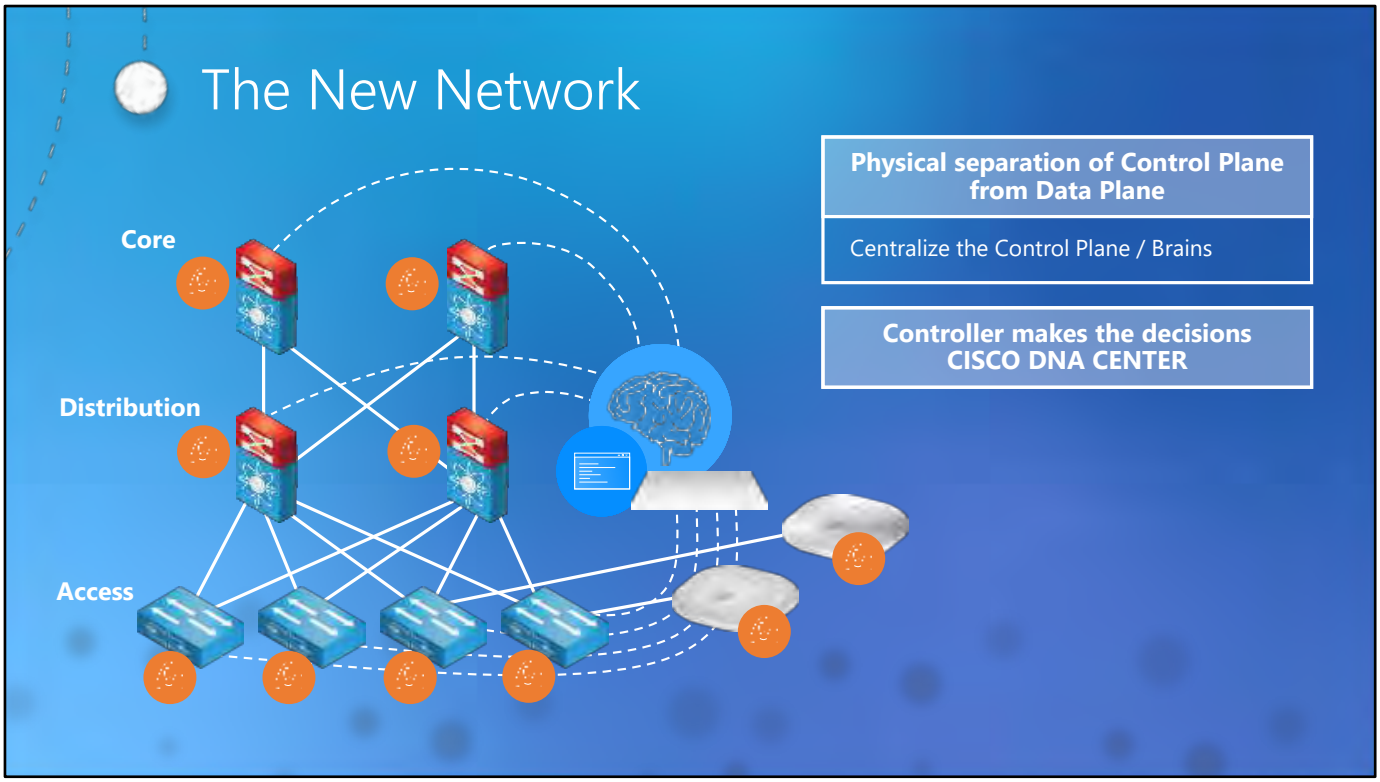
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

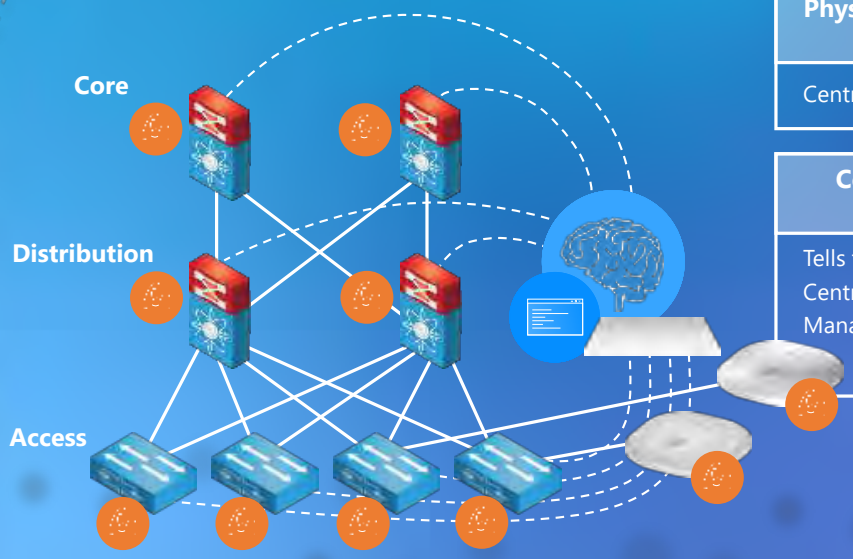


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

The New Network



Physical separation of Control Plane from Data Plane

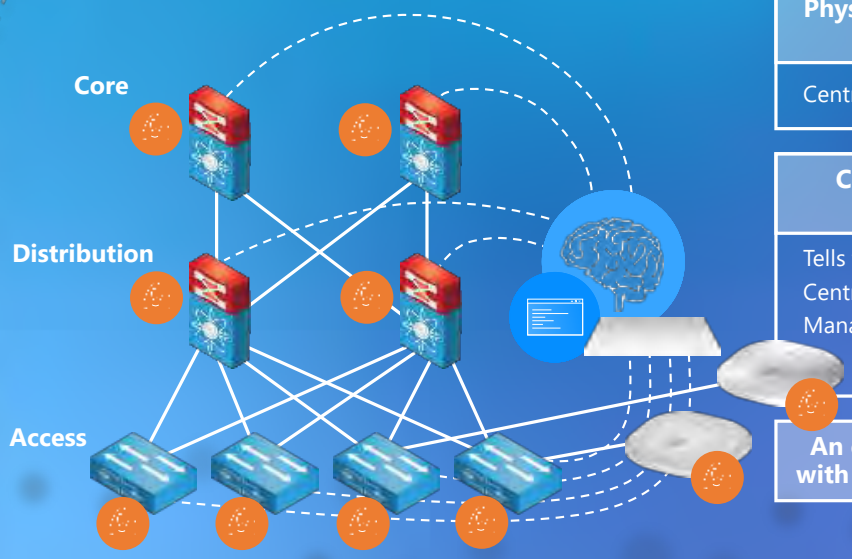
Centralize the Control Plane / Brains

Controller makes the decisions CISCO DNA CENTER

Tells the data plane what to do
Centralizing policy and control
Manage multiple devices at the same time
As a single entity

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

The New Network



Physical separation of Control Plane from Data Plane

Centralize the Control Plane / Brains

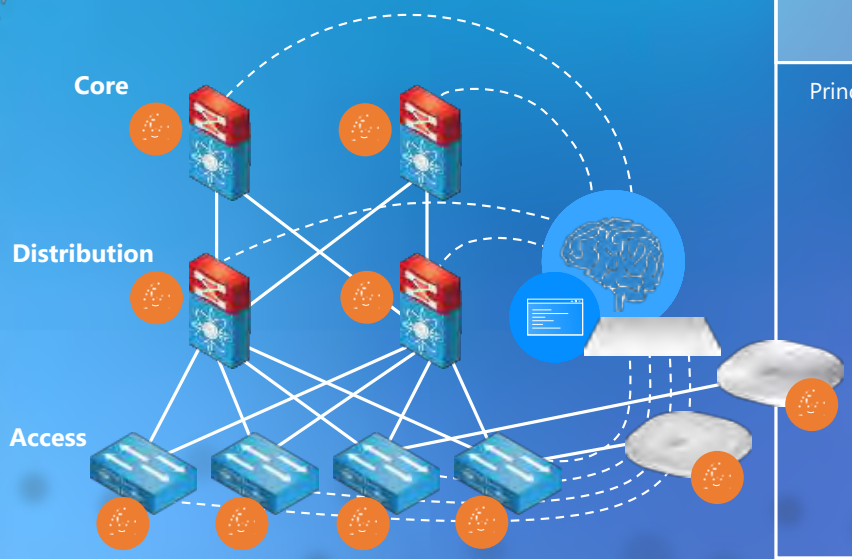
Controller makes the decisions CISCO DNA CENTER

Tells the data plane what to do
Centralizing policy and control
Manage multiple devices at the same time
As a single entity

An entire network can be modified with policies using a click of a button

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

The New Network



Cisco DNA Center

Principles of DNA:
- Policy
- Security
- Automation
- Analytics
- Open platform
- Cloud
- Physical and Virtual Infrastructure

Benefits of DNA:
- IT agility and scale
- Reduced risk
- Improved user experience
- Investment protection
- Ease of updates

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

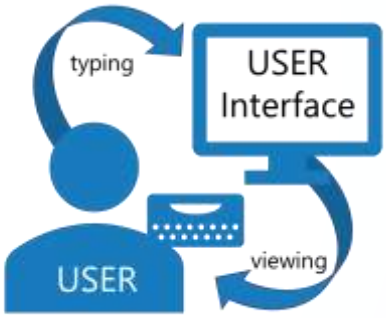
What is an API?

How software can talk to other software.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

What is an API?

How software can talk to other software.

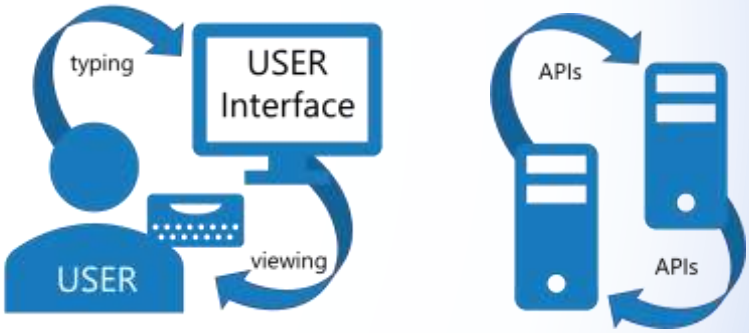


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

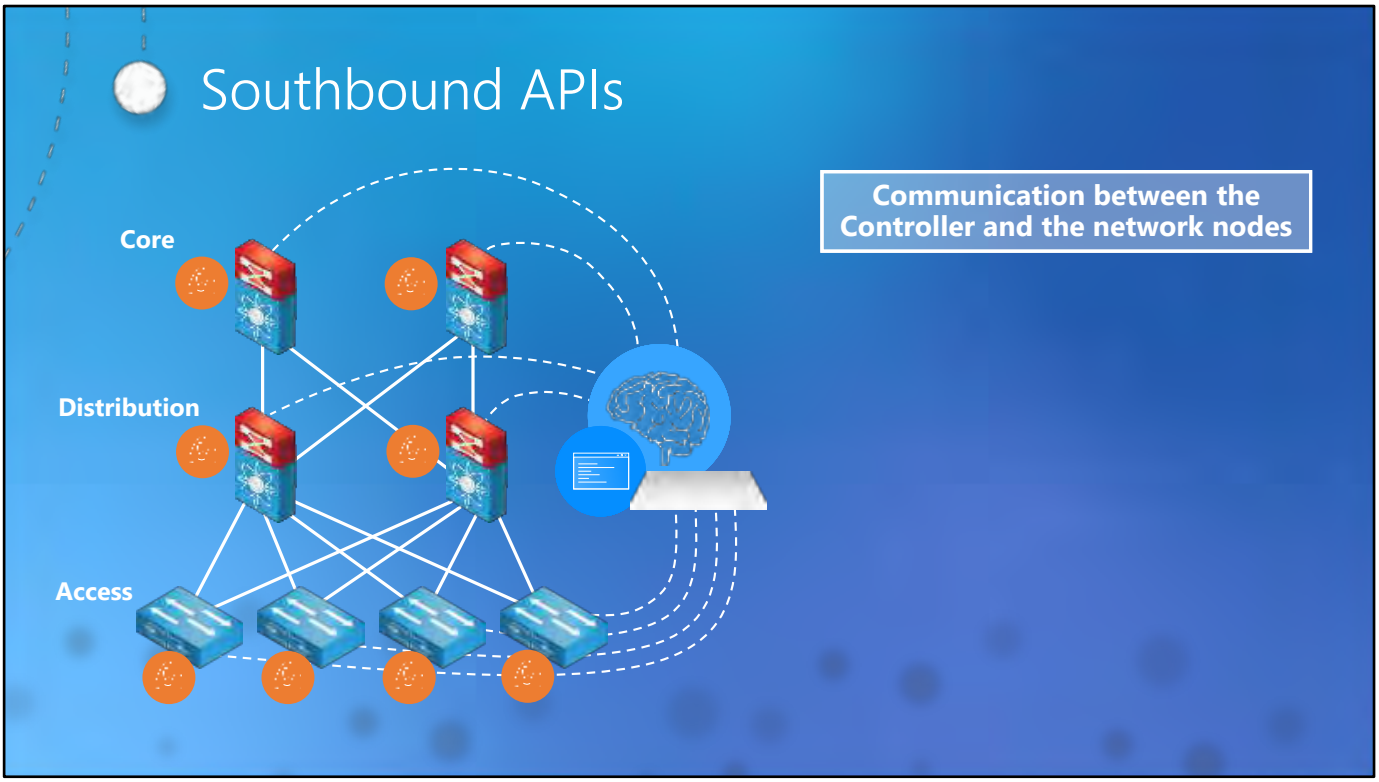
What is an API?

How software can talk to other software.

The user interface of software systems

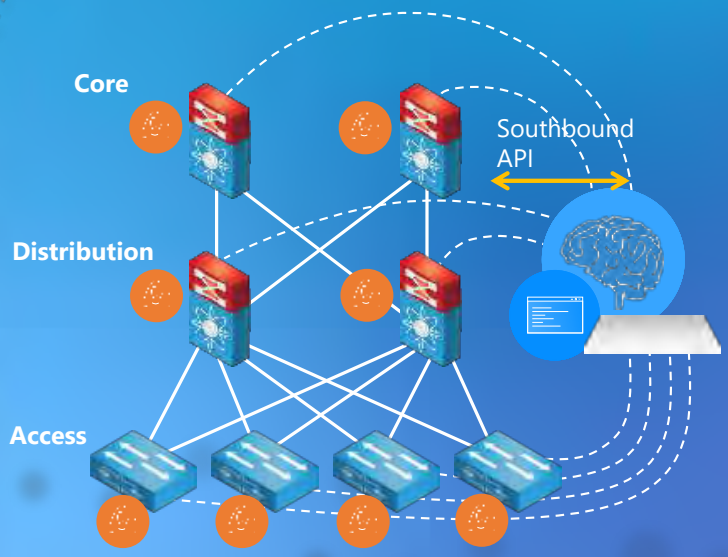


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Southbound APIs

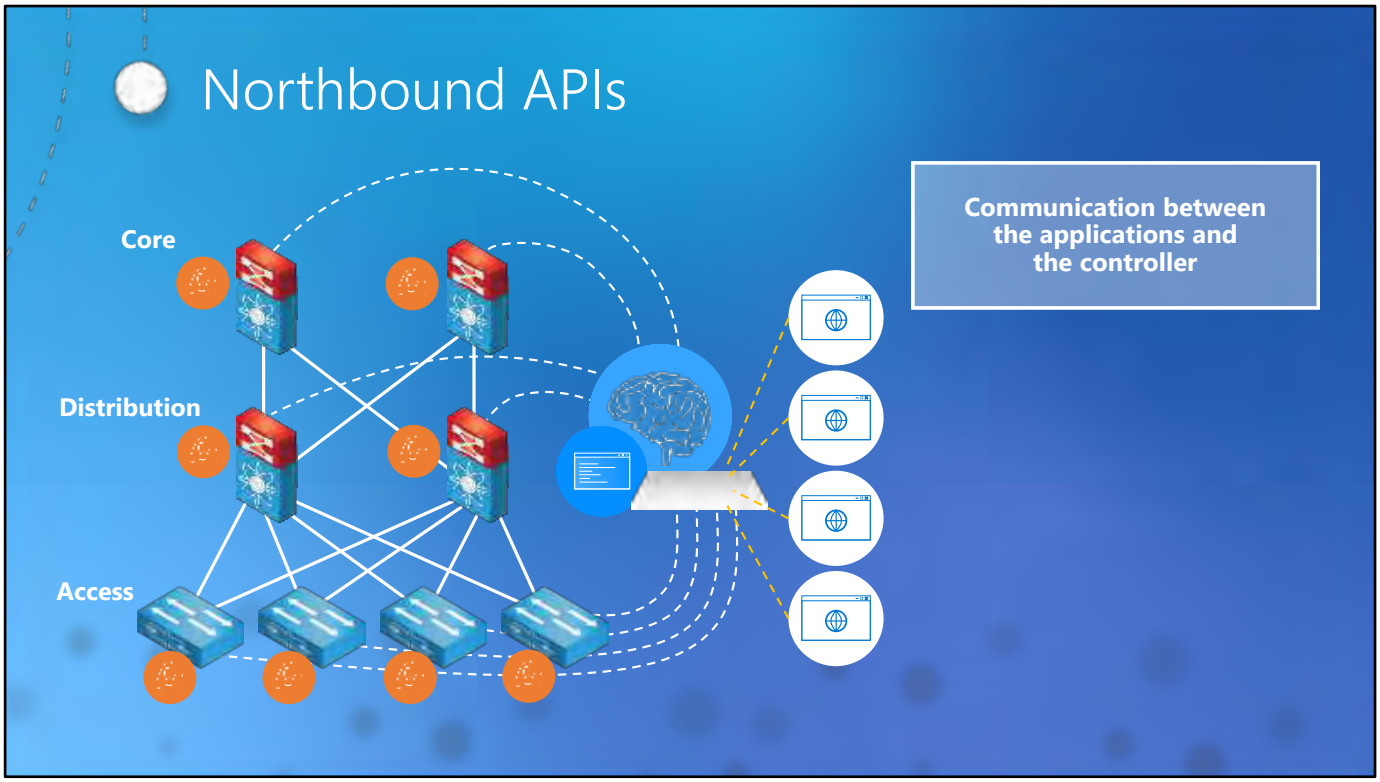


Communication between the Controller and the network nodes

APIs

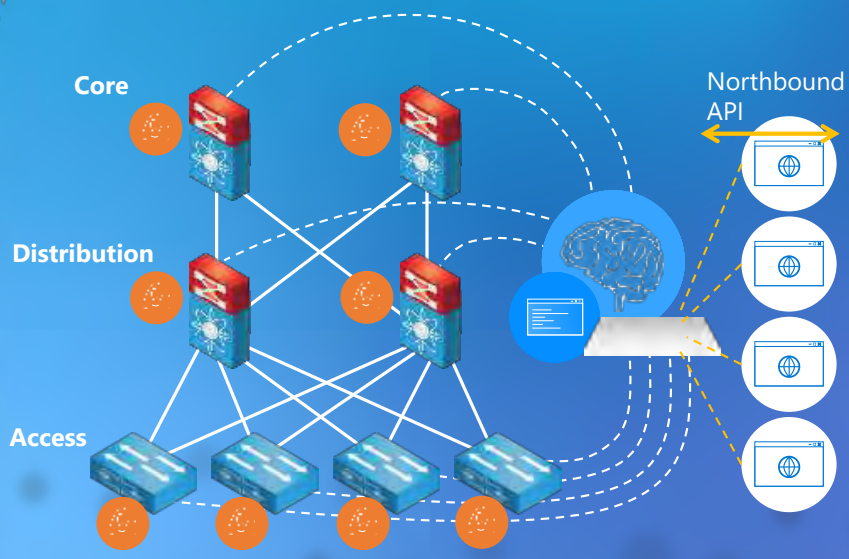
OpenFlow	FTP
NETCONF	SFTP
OpFlex	Telnet
SNMP	SSH
CLI	RESTCONF

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Northbound APIs



Communication between the applications and the controller

- REST APIs
  - HTTP methods - GET, POST, PUT, DELETE
- XML
- SNMP
- Syslog
- LDAP
- RADIUS

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

REST APIs (Structure)

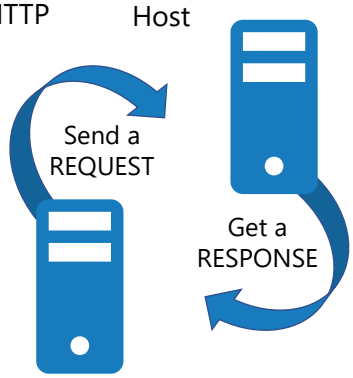
https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

Type of HTTP

Server / Host

Resource

Parameters



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

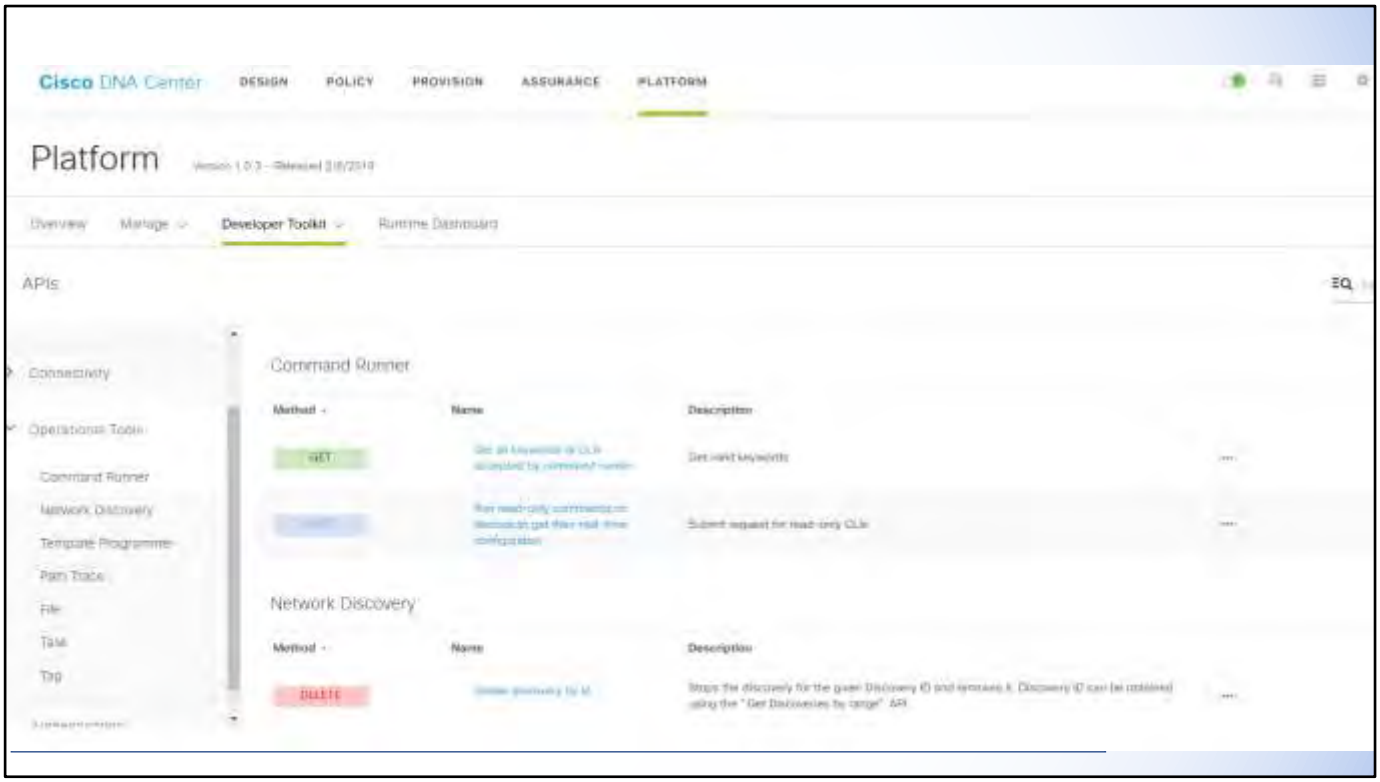
REST APIs (Verbs)

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

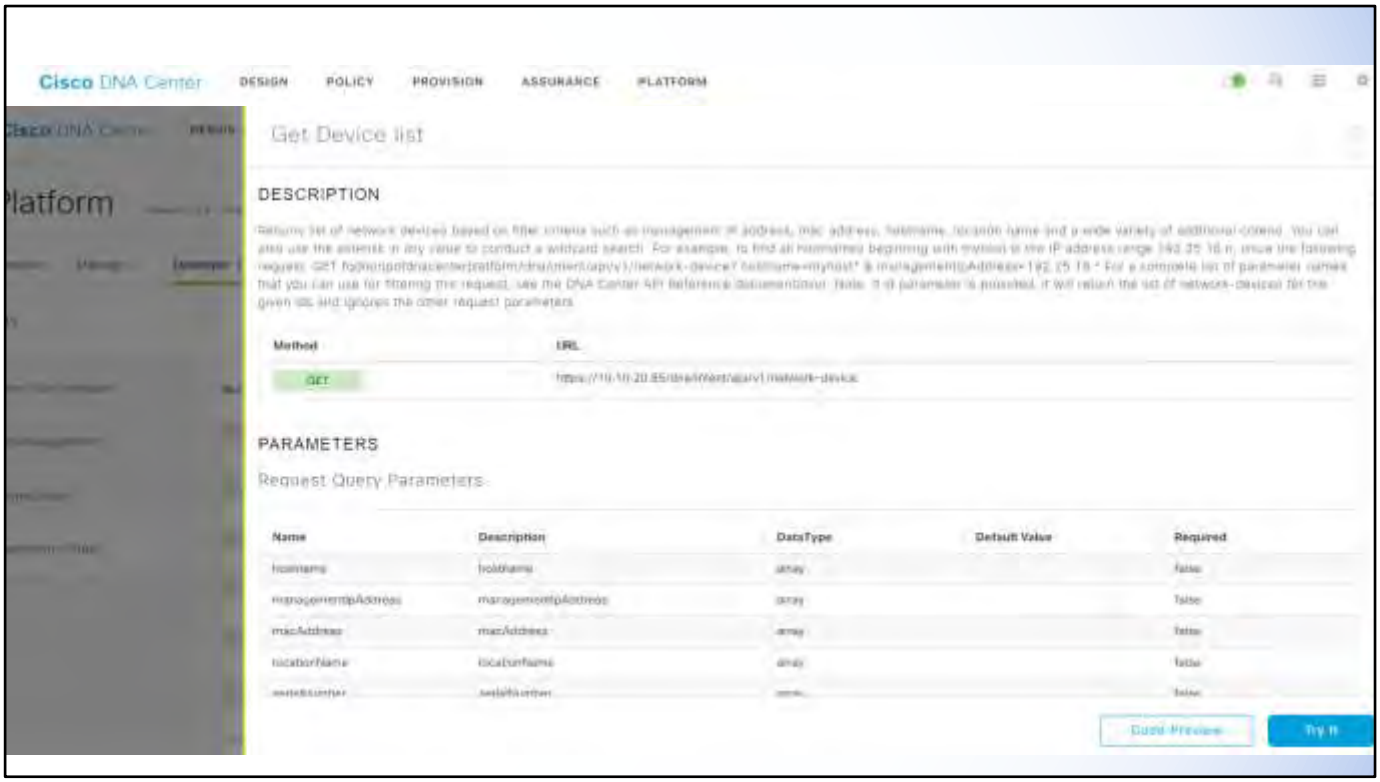
ameters

HTTP Verb	Purpose (CRUD)	Description
GET	Read	"GET" information from the endpoint Ex: Retrieve all action movies from the movie database
POST	Create	Add new information to the endpoint Ex: Create a new movie entry in the movie database
PUT	Update	Replace or modify or create information on the endpoint Ex: Modify the description of the movie in the movie database
DELETE	Delete	Remove information from the endpoint Ex: Delete a movie from the movie database

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

HTTP(s) Messages

Field	Value	Example
Start-Line	Request / Status	(GET /hello.htm HTTP/1.1) / (HTTP/1.1 200 OK)
Headers	General / Request / Response / Entity	Content-Type: application/json Date: Tue, 25 Jul 2017 18:26:00 GMT
Empty-Line	An empty line	Indicating the end of the header fields
Body	HTML, XML, etc.	<html> <body> Hello, World! </body> </html>

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Example REST Headers

Header	Example Value	Purpose
Content-type	application/json	Specify the format of data in the body
Accept	application/json	Specify the request format for returned data
Authorize	Basic dmFncmFudDp2YWdyYW50	Provide credentials to authorize the request
Date	Tue, 25 Jul 2017 18:26:00 GMT	Date and time of the message

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

REST API Security

Encryption

Use HTTPs not HTTP

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

Authenticate the REST API call

Authentication Type	**Description**
None	API is public and anybody can use it
Basic HTTP	Username and Password are passed in an encoded string
Token	A static secret generated and retrieved from the API developer portal (Secure Vault)
Oauth	A dynamic method of retrieving and using access tokens from an identity provider

©2023 by StormWind LLC. All rights reserved.

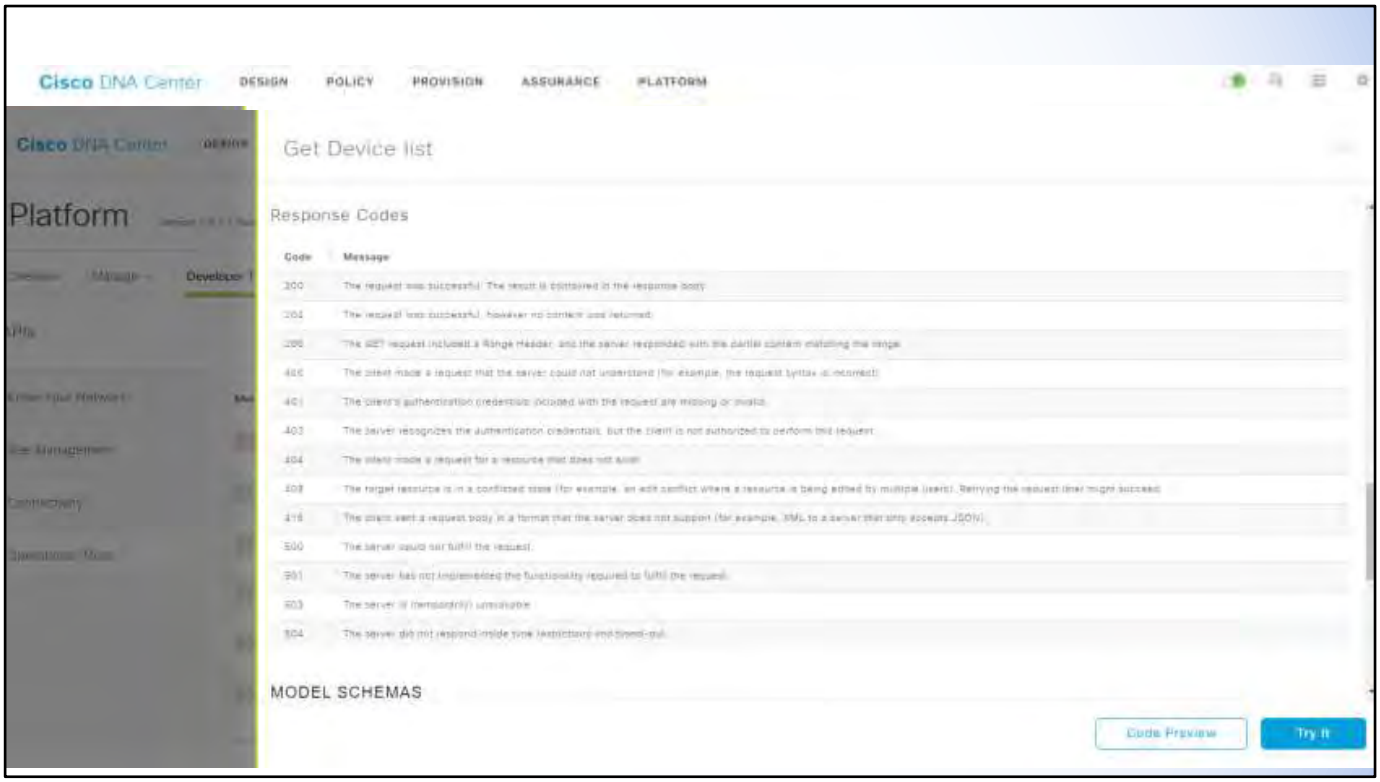
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

REST API Response Codes

Common Ones We Should Know

Status Code	Status Message	Meaning
200	Ok	All looks good
201	Created	New resource created
204	No Content	No body content to send for this request, but the headers may be useful
400	Bad Request	Request was invalid
401	Unauthorized	Authentication missing or incorrect
403	Forbidden	Request was understood, but not allowed
404	Not found	Resource not found
405	Method Not Allowed	Method is known by the server but is not supported by the target resource
500	Internal Server Error	Something wrong with server
503	Service Unavailable	Server is unavailable to complete request
504	Gateway Timeout	Server is unable to respond in the amount of time

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Response Codes

Code	Message
200	The request was successful. The result is contained in the response body.
204	The request was successful, however no content was returned.
206	The GET request included a Range Header, and the server responded with the partial content matching the range.
400	The client made a request that the server could not understand (for example, the request syntax is incorrect).
401	The client's authentication credentials included with the request are missing or invalid.
403	The server recognizes the authentication credentials, but the client is not authorized to perform this request.
404	The client made a request for a resource that does not exist.
409	The target resource is in a conflicted state (for example, an edit conflict where a resource is being edited by multiple users). Retrying the request later might succeed.
415	The client sent a request body in a format that the server does not support (for example, XML to a server that only accepts JSON).
500	The server could not fulfill the request.
501	The server has not implemented the functionality required to fulfill the request.
503	The server is (temporarily) unavailable.
504	The server did not respond inside time restrictions and timed-out.

MODEL SCHEMAS

Code Preview | Try It

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

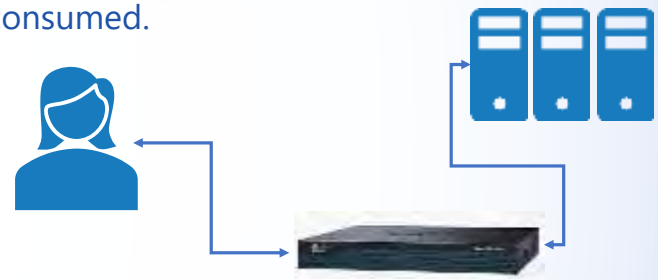
Data Formats

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Data Formats

How the information is presented so it can be consumed.

- CLI
- JSON
- XML
- YAML

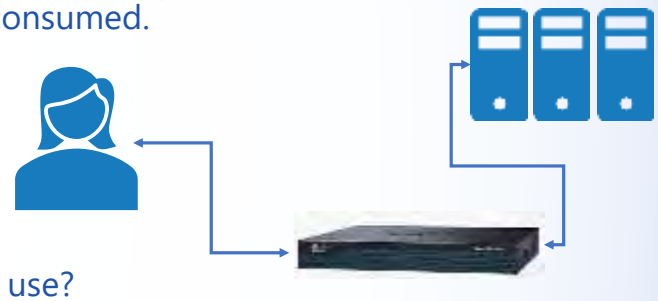


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Data Formats

How the information is presented so it can be consumed.

- CLI
- JSON
- XML
- YAML



What do you use?

- Depends on who or what is consuming it.
- CLI great for you and I
- JSON, XML, YAML great for devices

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

JSON vs XML vs YAML

JSON


```
{
  "Cisco-IOS-XE-interfaces-oper:interfac
    "name": "GigabitEthernet2",
    "interface-type": "iana-iftype-ether
    "admin-status": "if-state-down",
    "oper-status": "if-oper-state-no-pas
    "last-change": "2019-11-22T18:42:47.
    "if-index": 2,
    "phys-address": "00:50:56:bb:77:1a",
    "speed": "1024000000",
    "statistics": {
      "discontinuity-time": "2019-11-22T
      "in-octets": "0",
      "in-unicast-pkts": "0",
      "in-broadcast-pkts": "0",
      "in-multicast-pkts": "0",
      "in-discards": 0,
      "in-errors": 0,
      "in-unknown-protos": 0,
      "out-octets": 0,
      "out-unicast-pkts": "0",
      "out-broadcast-pkts": "0",
      "out-multicast-pkts": "0",
      "out-discards": "0",
      "out-errors": "0",
      "rx-pps": "0",
      "rx-kbps": "0",
      "tx-pps": "0",
      "tx-kbps": "0",
      "num-flows": "0"
```


XML


```
<interface xmlns="http://cisco.com/ns
xmlns:interfaces-ios-xe-oper="http://
interfaces-oper">
    <name>GigabitEthernet2</name>
    <interface-type>iana-iftype-ether
    <admin-status>if-state-down</admi
    <oper-status>if-oper-state-no-pas
    <last-change>2019-11-22T18:42:47.
    <if-index>2</if-index>
    <phys-address>00:50:56:bb:77:1a</
    <speed>1024000000</speed>
    <statistics>
        <discontinuity-time>2019-11-
22T18:41:30.000142+00:00</discontinui
        <in-octets>0</in-octets>
        <in-unicast-pkts>0</in-unicas
        <in-broadcast-pkts>0</in-broa
        <in-multicast-pkts>0</in-mult
        <in-discards>0</in-discards>
        <in-errors>0</in-errors>
        <in-unknown-protos>0</in-unkn
        <out-octets>0</out-octets>
        <out-unicast-pkts>0</out-unic
        <out-broadcast-pkts>0</out-br
        <out-multicast-pkts>0</out-mu
        <out-discards>0</out-discards
        <out-errors>0</out-errors>
        <rx-pps>0</rx-pps>
        <rx-kbps>0</rx-kbps>
```


YAML


```
---
Cisco-IOS-XE-interfaces-oper:interface:
  name: GigabitEthernet2
  interface-type: iana-iftype-ethernet-csmacd
  admin-status: if-state-down
  oper-status: if-oper-state-no-pass
  last-change: '2019-11-22T18:42:47.000421+00:00'
  if-index: 2
  phys-address: 00:50:56:bb:77:1a
  speed: '1024000000'
  statistics:
    discontinuity-time: '2019-11-22T18:41:30.000159+00:00'
    in-octets: '0'
    in-unicast-pkts: '0'
    in-broadcast-pkts: '0'
    in-multicast-pkts: '0'
    in-discards: 0
    in-errors: 0
    in-unknown-protos: 0
    out-octets: 0
    out-unicast-pkts: '0'
    out-broadcast-pkts: '0'
    out-multicast-pkts: '0'
    out-discards: '0'
    out-errors: '0'
    rx-pps: '0'
    rx-kbps: '0'
    tx-pps: '0'
    tx-kbps: '0'
    num-flows: '0'
```


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

JSON

JavaScript Object Notation

Human readable data format for applications
to store, transfer, and read data


```
{
  "Cisco-IOS-XE-interfaces-oper:interface": {
    "name": "GigabitEthernet2",
    "interface-type": "iana-iftype-ethernet-csmacd",
    "admin-status": "if-state-down",
    "oper-status": "if-oper-state-no-pass",
    "last-change": "2019-11-22T18:42:47.000421+00:00",
    "if-index": 2,
    "phys-address": "00:50:56:bb:77:1a",
    "speed": "1024000000",
    "statistics": {
      "discontinuity-time": "2019-11-22T18:41:30.000159+00:00",
      "in-octets": "0",
      "in-unicast-pkts": "0",
      "in-broadcast-pkts": "0",
      "in-multicast-pkts": "0",
      "in-discards": 0,
      "in-errors": 0,
      "in-unknown-protos": 0,
      "out-octets": 0,
      "out-unicast-pkts": "0",
```


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

JSON Web Token

- Compact / Self-Contained way to securely transmit information between parties as a JSON object.
  - Open Standard (RFC 7519)
- Can be sent through
  - URL
  - POST parameter
  - Inside an HTTP header
- Contains all needed information
  - A database does not need to be queried more than once by the sender
  - The recipient does not need to call a server to validate the token

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

JSON Web Token Example

Encoded

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
zdWIiOiIwMTAyMDMwNDA1MDYwNzA4MDkiLCJuYW1
lIjoiRU5DT1IgRVhBTSBFWEFNUExFIiwiaWF0Ijo
xNTE2MjM5MDIyfQ.ZxdxzQENoCwaddMwpR6G2pIW
21gvSQ9PzBsVQxFnLH0

Decoded

Header: Algorithm & Token Type

{
"alg": "HS256",
"typ": "JWT"
}

Payload: Data

{
"sub": "0102030405060708090",
"name": "ENCOR EXAM EXAMPLE",
"iat": 1516239022
}

Verify Signature

HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
iwillpassencorexam
) ☑ secret base64 encoded

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

JSON Web Token Example

Encoded

Decoded

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

JSON Web Token Example

Encoded

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
zdWIiOiIwMTAyMDMwNDA1MDYwNzA4MDkiLCJuYW1
lIjoiRU5DT1IgRVhBTSBFWEFNUExFIiwiaWF0Ijo
xNTE2MjM5MDIyfQ.ZxdxzQENoCwaddMwpR6G2pIW
21gvSQ9PzBsVQxFnLH0

Decoded

Header: Algorithm & Token Type

{
"alg": "HS256",
"typ": "JWT"
}

Payload: Data

{
"sub": "0102030405060708090",
"name": "ENCOR EXAM EXAMPLE",
"iat": 1516239022
}

Verify Signature

HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
iwillpassencorexam
) ☑ secret base64 encoded

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Data Modeling

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

What is a Data Model?

A data model describes how data is represented, structured, and accessed.

It is well understood and agreed upon

- Typically standardized to ensure consistency and scalability.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

What is a YANG Data Model?

… a data modeling language used to model configuration and state data manipulated by the Network Configuration Protocol (NETCONF), NETCONF remote procedure calls, and NETCONF notifications.

… used to model data for the NETCONF protocol.

https://tools.ietf.org/html/rfc6020

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

What is a YANG Data Model?

XML

DATA

JSON
XML
YAML

```
<interface xmlns="http://cisco.com/ns/yang/Cisco-
IOS-XE-interfaces-oper"  xmlns:interfaces-ios-xe-
oper="http://cisco.com/ns/yang/Cisco-IOS-XE-
interfaces-oper">
    <name>GigabitEthernet2</name>
    <interface-type>iana-iftype-ethernet-
csmacd</interface-type>
    <admin-status>if-state-down</admin-status>
    <oper-status>if-oper-state-no-pass</oper-
status>
    <last-change>2019-11-
22T18:42:47.000404+00:00</last-change>
    <if-index>2</if-index>
    <phys-address>00:50:56:bb:77:1a</phys-address>
    <speed>1024000000</speed>
    <statistics>
        <discontinuity-time>2019-11-
22T18:41:30.000142+00:00</discontinuity-time>
        <in-octets>0</in-octets>
        <in-unicast-pkts>0</in-unicast-pkts>
        <in-broadcast-pkts>0</in-broadcast-pkts>
        <in-multicast-pkts>0</in-multicast-pkts>
        <in-discards>0</in-discards>
        <in-errors>0</in-errors>
        <in-unknown-protos>0</in-unknown-protos>
        <out-octets>0</out-octets>
```

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

JSON vs XML vs YAML

JSON


```
{
  "Cisco-IOS-XE-interfaces-oper:interfac
    "name": "GigabitEthernet2",
    "interface-type": "iana-iftype-ether
    "admin-status": "if-state-down",
    "oper-status": "if-oper-state-no-pas
    "last-change": "2019-11-22T18:42:47.
    "if-index": 2,
    "phys-address": "00:50:56:bb:77:1a",
    "speed": "1024000000",
    "statistics": {
      "discontinuity-time": "2019-11-22T
      "in-octets": "0",
      "in-unicast-pkts": "0",
      "in-broadcast-pkts": "0",
      "in-multicast-pkts": "0",
      "in-discards": 0,
      "in-errors": 0,
      "in-unknown-protos": 0,
      "out-octets": 0,
      "out-unicast-pkts": "0",
      "out-broadcast-pkts": "0",
      "out-multicast-pkts": "0",
      "out-discards": "0",
      "out-errors": "0",
      "rx-pps": "0",
      "rx-kbps": "0",
      "tx-pps": "0",
      "tx-kbps": "0",
      "num-flows": "0"
```


XML


```
<interface xmlns="http://cisco.com/ns
xmlns:interfaces-ios-xe-oper="http://
interfaces-oper">
    <name>GigabitEthernet2</name>
    <interface-type>iana-iftype-ether
    <admin-status>if-state-down</admi
    <oper-status>if-oper-state-no-pas
    <last-change>2019-11-22T18:42:47.
    <if-index>2</if-index>
    <phys-address>00:50:56:bb:77:1a</
    <speed>1024000000</speed>
    <statistics>
        <discontinuity-time>2019-11-
22T18:41:30.000142+00:00</discontinui
        <in-octets>0</in-octets>
        <in-unicast-pkts>0</in-unicas
        <in-broadcast-pkts>0</in-broa
        <in-multicast-pkts>0</in-mult
        <in-discards>0</in-discards>
        <in-errors>0</in-errors>
        <in-unknown-protos>0</in-unkn
        <out-octets>0</out-octets>
        <out-unicast-pkts>0</out-unic
        <out-broadcast-pkts>0</out-br
        <out-multicast-pkts>0</out-mu
        <out-discards>0</out-discards
        <out-errors>0</out-errors>
        <rx-pps>0</rx-pps>
        <rx-kbps>0</rx-kbps>
```


YAML

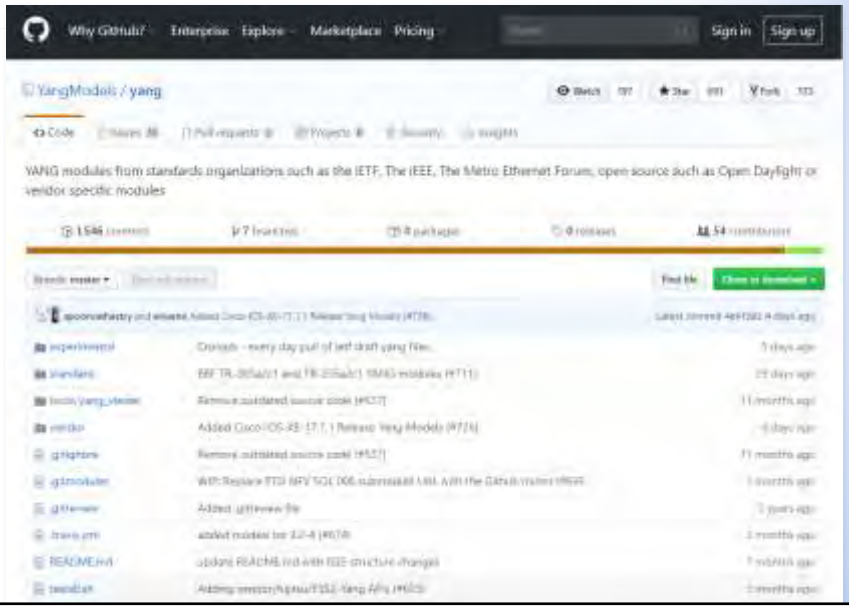

```
---
Cisco-IOS-XE-interfaces-oper:interface:
  name: GigabitEthernet2
  interface-type: iana-iftype-ethernet-csmacd
  admin-status: if-state-down
  oper-status: if-oper-state-no-pass
  last-change: '2019-11-22T18:42:47.000421+00:00'
  if-index: 2
  phys-address: 00:50:56:bb:77:1a
  speed: '1024000000'
  statistics:
    discontinuity-time: '2019-11-22T18:41:30.000159+00:00'
    in-octets: '0'
    in-unicast-pkts: '0'
    in-broadcast-pkts: '0'
    in-multicast-pkts: '0'
    in-discards: 0
    in-errors: 0
    in-unknown-protos: 0
    out-octets: 0
    out-unicast-pkts: '0'
    out-broadcast-pkts: '0'
    out-multicast-pkts: '0'
    out-discards: '0'
    out-errors: '0'
    rx-pps: '0'
    rx-kbps: '0'
    tx-pps: '0'
    tx-kbps: '0'
    num-flows: '0'
```


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

YANG Models

https://github.com/YangModels/yang



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

YANG Models

Data Model = YANG

JSON
XML
YAML

ietf-interfaces@2018-02-20.yang

```
          leaf out-errors {
            type yang:counter32;
            status deprecated;
            description
              "For packet-oriented interfaces, the number of
outbound
               packets that could not be transmitted because of
errors.
               For character-oriented or fixed-length interfaces,
the
               number of outbound transmission units that could
not be
               transmitted because of errors.
               Discontinuities in the value of this counter can
occur
               at re-initialization of the management system and
at
               other times as indicated by the value of
               'discontinuity-time'.";
            reference
              "RFC 2863: The Interfaces Group MIB - ifOutErrors";
          }
        }
      }
    }
}
```

Module

- Define the hierarchy of data that can be used for NETCONF based operations
- Module that is a self—contained top- level hierarchy of nodes
- Uses containers to group related nodes
- Lists to identify nodes that are stored in sequence
- Each individual attribute of a node is represented by a leaf
- Every leaf must have an associated type

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Exploring a Model as a Tree

ietf-interfaces@2018-02-20.yang

Data Model = YANG

JSON
XML
YAML

```
module: ietf-interfaces
  +--rw interfaces
  |  +--rw interface* [name]
  |     +--rw name                        string
  |     +--rw description?                string
  |     +--rw type                        identityref
  |     +--rw enabled?                    boolean
  |     +--rw link-up-down-trap-enable?   enumeration {if-mib}?
  |     +--ro admin-status                enumeration {if-mib}?
  |     +--ro oper-status                 enumeration
  |     +--ro last-change?                yang:date-and-time
  |     +--ro if-index                    int32 {if-mib}?
  |     +--ro phys-address?               yang:phys-address
  |     +--ro higher-layer-if*            interface-ref
  |     +--ro lower-layer-if*             interface-ref
  |     +--ro speed?                      yang:gauge64
  |     +--ro statistics
  |        +--ro discontinuity-time    yang:date-and-time
  |        +--ro in-octets?            yang:counter64
  |        +--ro in-unicast-pkts?      yang:counter64
  |        +--ro in-broadcast-pkts?    yang:counter64
  |        +--ro in-multicast-pkts?    yang:counter64
  |        +--ro in-discards?          yang:counter32
  |        +--ro in-errors?            yang:counter32
  |        +--ro in-unknown-protos?    yang:counter32
  |        +--ro out-octets?           yang:counter64
  |        +--ro out-unicast-pkts?     yang:counter64
  |        +--ro out-broadcast-pkts?   yang:counter64
  |        +--ro out-multicast-pkts?   yang:counter64
  |        +--ro out-discards?         yang:counter32
  |        +--ro out-errors?           yang:counter32
  x--ro interfaces-state
     x--ro interface* [name]
```

Python YANG Library

pip install pyang

pyang -f tree *yang_file_name*

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Exploring a Model as a Tree

ietf-interfaces@2018-02-20.yang

Module Name

Container

List

Leaf

Container

List

Data Types

```
module: ietf-interfaces
  +--rw interfaces
     +--rw interface* [name]
        +--rw name                          string
        +--rw description?                  string
        +--rw type                          identityref
        +--rw enabled?                      boolean
        +--rw link-up-down-trap-enable?     enumeration {if-mib}?
        +--ro admin-status                  enumeration {if-mib}?
        +--ro oper-status                   enumeration
        +--ro last-change?                  yang:date-and-time
        +--ro if-index                      int32 {if-mib}?
        +--ro phys-address?                 yang:phys-address
        +--ro higher-layer-if*              interface-ref
        +--ro lower-layer-if*               interface-ref
        +--ro speed?                        yang:gauge64
        +--ro statistics
           +--ro discontinuity-time     yang:date-and-time
           +--ro in-octets?             yang:counter64
           +--ro in-unicast-pkts?       yang:counter64
…output omitted…
  x--ro interfaces-state
     x--ro interface* [name]
        x--ro name                  string
        x--ro type                  identityref
        x--ro admin-status          enumeration {if-mib}?
        x--ro oper-status           enumeration
        x--ro last-change?          yang:date-and-time
        x--ro if-index              int32 {if-mib}?
        x--ro phys-address?         yang:phys-address
        x--ro higher-layer-if*      interface-state-ref
        x--ro lower-layer-if*       interface-state-ref
        x--ro speed?                yang:gauge64
```

Module

- Define the hierarchy of data that can be used for NETCONF based operations
- Uses containers to group related nodes
- Lists to identify nodes that are stored in sequence
- Each individual attribute of a node is represented by a leaf
- Every leaf must have an associated data type

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Yang Data Model and Data Formats

ietf-interfaces@2018-02-20.yang

Data Model = YANG

DATA

Data Format
JSON
XML
YAML

```
module: ietf-interfaces
  +--rw interfaces
  |  +--rw interface* [name]
  |     +--rw name                        string
  |     +--rw description?                string
  |     +--rw type                        identityref
  |     +--rw enabled?                    boolean
  |     +--rw link-up-down-trap-enable?   enumeration {if-mib}?
  |     +--ro admin-status                enumeration {if-mib}?
  |     +--ro oper-status                 enumeration
  |     +--ro last-change?                yang:date-and-time
  |     +--ro if-index                    int32 {if-mib}?
  |     +--ro phys-address?               yang:phys-address
  |     +--ro higher-layer-if*            interface-ref
  |     +--ro lower-layer-if*             interface-ref
  |     +--ro speed?                      yang:gauge64
  |     +--ro statistics
  |        +--ro discontinuity-time    yang:date-and-time
  |        +--ro in-octets?            yang:counter64
  |        +--ro in-unicast-pkts?      yang:counter64
  |        +--ro in-broadcast-pkts?    yang:counter64
  |        +--ro in-multicast-pkts?    yang:counter64
  |        +--ro in-discards?          yang:counter32
  |        +--ro in-errors?            yang:counter32
  |        +--ro in-unknown-protos?    yang:counter32
  |        +--ro out-octets?           yang:counter64
  |        +--ro out-unicast-pkts?     yang:counter64
  |        +--ro out-broadcast-pkts?   yang:counter64
  |        +--ro out-multicast-pkts?   yang:counter64
  |        +--ro out-discards?         yang:counter32
  |        +--ro out-errors?           yang:counter32
  x--ro interfaces-state
```

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Yang Data Model and Data Formats

JSON

Data Model = YANG

DATA

JSON


```
{
  "Cisco-IOS-XE-interfaces-oper:interface": {
    "name": "GigabitEthernet2",
    "interface-type": "iana-iftype-ethernet-csmacd",
    "admin-status": "if-state-down",
    "oper-status": "if-oper-state-no-pass",
    "last-change": "2019-11-22T18:42:47.000421+00:00",
    "if-index": 2,
    "phys-address": "00:50:56:bb:77:1a",
    "speed": "1024000000",
    "statistics": {
      "discontinuity-time": "2019-11-22T18:41:30.000159+00:00",
      "in-octets": "0",
      "in-unicast-pkts": "0",
      "in-broadcast-pkts": "0",
      "in-multicast-pkts": "0",
      "in-discards": 0,
      "in-errors": 0,
      "in-unknown-protos": 0,
      "out-octets": 0,
      "out-unicast-pkts": "0",
      "out-broadcast-pkts": "0",
      "out-multicast-pkts": "0",
      "out-discards": "0",
      "out-errors": "0",
      "rx-pps": "0",
      "rx-kbps": "0",
      "tx-pps": "0",
      "tx-kbps": "0",
      "num-flaps": "0",
      "in-crc-errors": "0"
    },
```

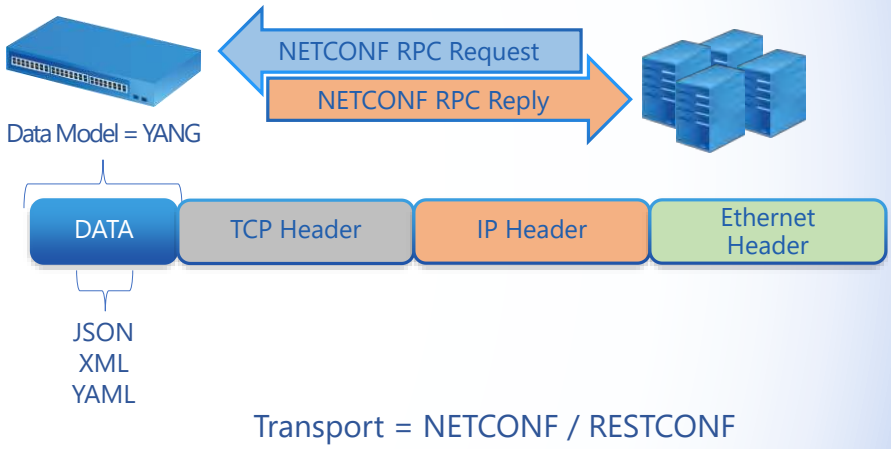

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NetConf / RestConf

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Transferring the Data



Transport = NETCONF / RESTCONF

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF / RESTCONF Overview

NETCONF

- Provides mechanisms to install, manipulate, and delete the configuration of network devices
- Uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages
- Operations are realized as remote procedure calls (RPCs)

RESTCONF

- Provides mechanisms to install, manipulate, and delete the configuration of network devices
- An HTTP-based protocol (REST APIs)
- Uses the datastore concepts defined in the Network Configuration Protocol (NETCONF)

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

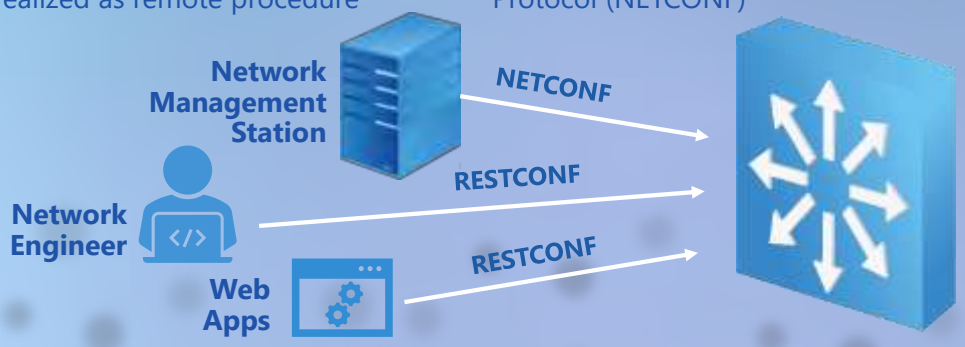
NETCONF / RESTCONF Overview

NETCONF

- Provides mechanisms to install, manipulate, and delete the configuration of network devices
- Uses an Extensible Markup Language (XML)-based data encoding for the configuration data as well as the protocol messages
- Operations are realized as remote procedure calls (RPCs)

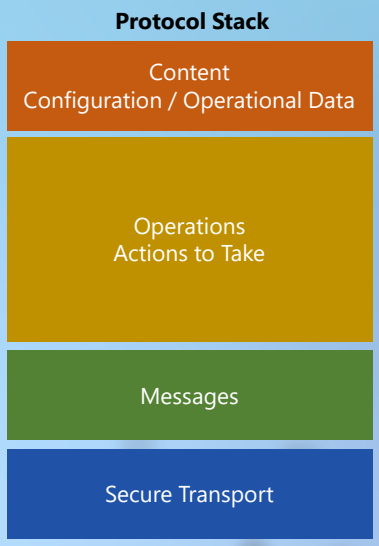
RESTCONF

- Provides mechanisms to install, manipulate, and delete the configuration of network devices
- An HTTP-based protocol (REST APIs)
- Uses the datastore concepts defined in the Network Configuration Protocol (NETCONF)

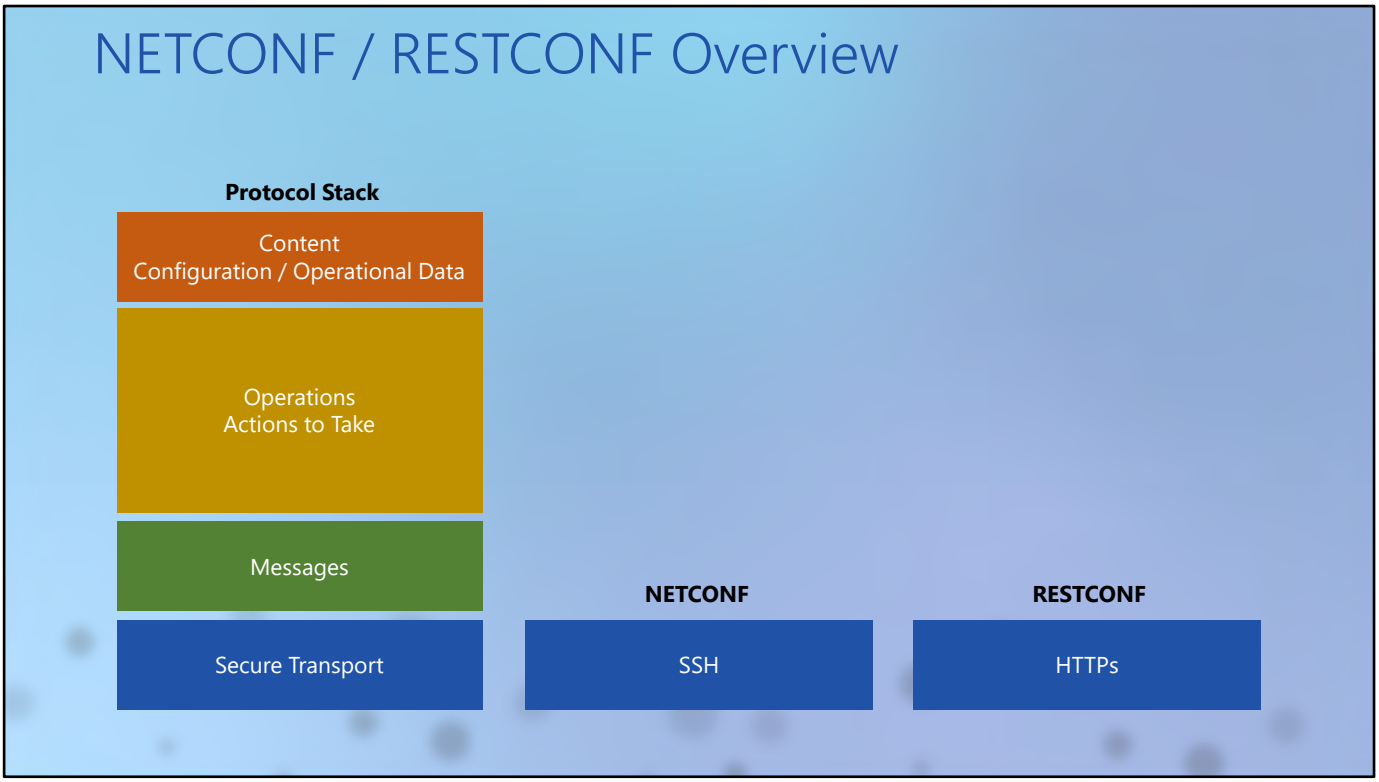


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

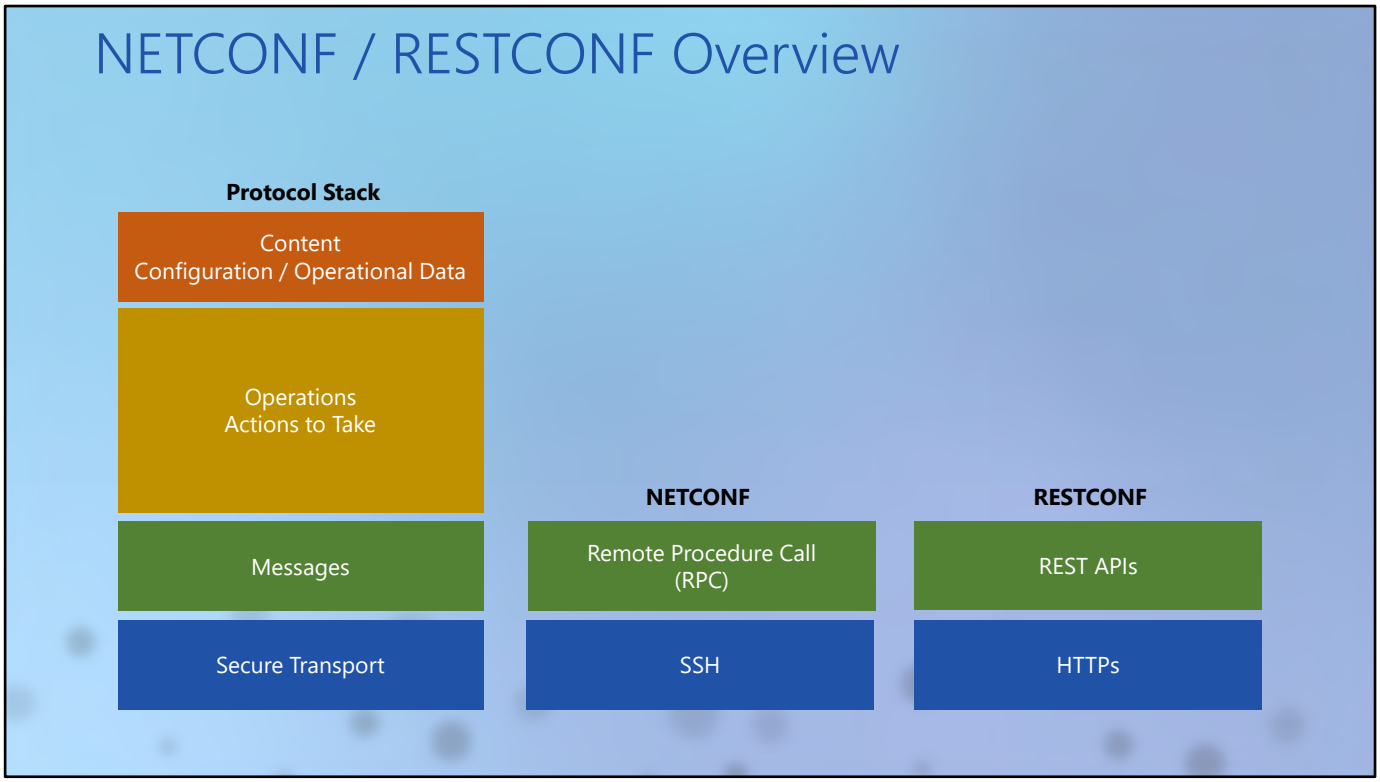
NETCONF / RESTCONF Overview



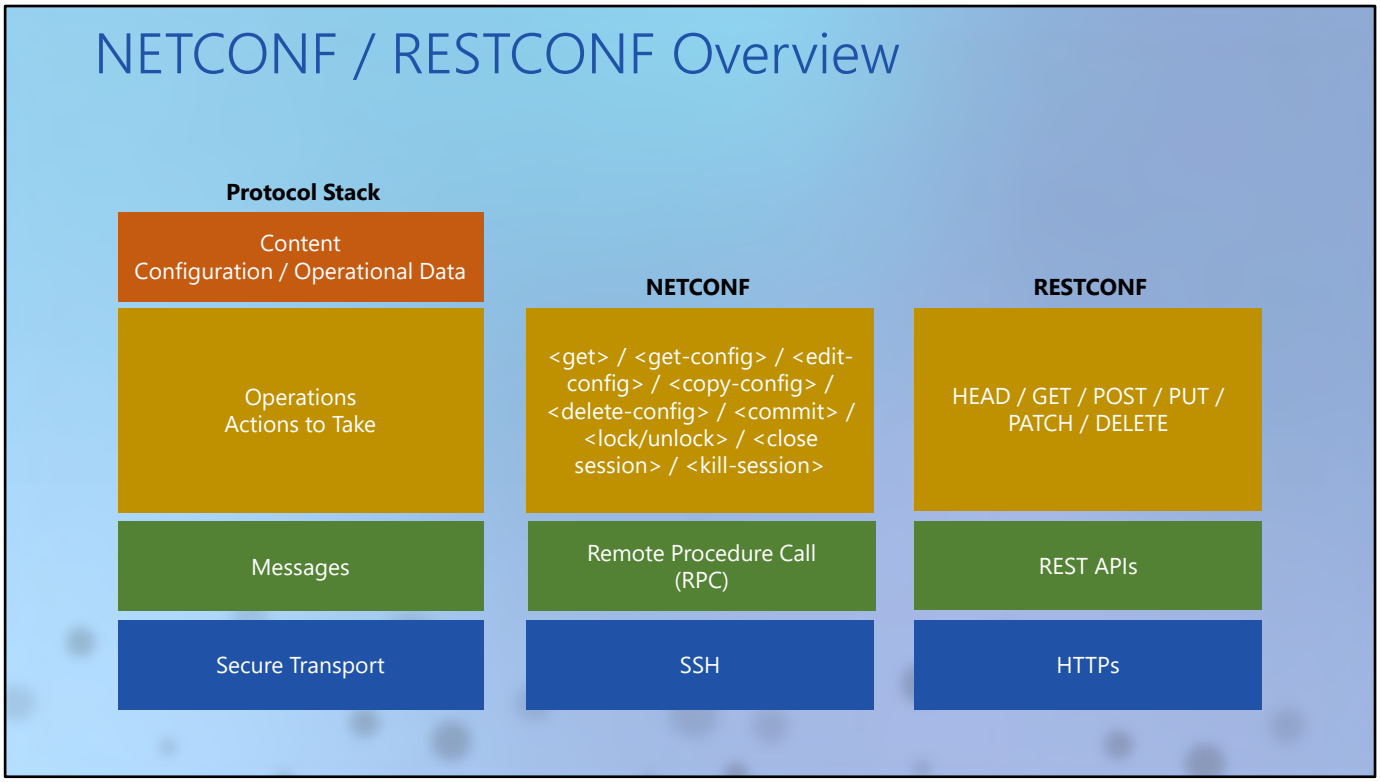
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF / RESTCONF Overview

Protocol Stack	NETCONF	RESTCONF
Content Configuration / Operational Data	DATA formatted as XML	DATA formatted as XML / JSON
Operations Actions to Take	<get> / <get-config> / <edit-config> / <copy-config> / <delete-config> / <commit> / <lock/unlock> / <close session> / <kill-session>	HEAD / GET / POST / PUT / PATCH / DELETE
Messages	Remote Procedure Call (RPC)	REST APIs
Secure Transport	SSH	HTTPs

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF DATA STORES

A conceptual place to store and access information

- Running configuration datastore
- Startup configuration datastore
- Candidate datastore

Definition from: https://tools.ietf.org/html/rfc6241

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF DATA STORES

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface>
          <name/>
        </interface>
      </interfaces>
    </filter>
  </get-config>
</rpc>
```

A conceptual place to store and access information

- Running configuration datastore
- Startup configuration datastore
- Candidate datastore

Definition from: https://tools.ietf.org/html/rfc6241

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF on IOS-XE

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
                                                  :yang:ietf-interfaces">
  </get-config>
</rpc>
```

RPC

Global Config Mode:

netconf-yang

NETCONF listens on any IP address assigned to the system.

When enabled, NETCONF runs on port 830 and uses SSH for transport.

SSH is enabled automatically when the NETCONF feature is enabled.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF on IOS-XE

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
                                                  yang:ietf-interfaces">

</rpc>
```

RPC Operation

Global Config Mode:

netconf-yang

NETCONF listens on any IP address assigned to the system.

When enabled, NETCONF runs on port 830 and uses SSH for transport.

SSH is enabled automatically when the NETCONF feature is enabled.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF on IOS-XE

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
                                                    ietf-interfaces">
    </
  </ge
</rpc>
```

The Data Store we are getting the information from.

Global Config Mode:

netconf-yang

NETCONF listens on any IP address assigned to the system.

When enabled, NETCONF runs on port 830 and uses SSH for transport.

SSH is enabled automatically when the NETCONF feature is enabled.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF on IOS-XE

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface>
          <name/>
        </inte
      </interf
    </filter>
  </get-config
</rpc>
```

A filter restricting what we want to get from the data store.

Global Config Mode:

netconf-yang

NETCONF listens on any IP address assigned to the system.

When enabled, NETCONF runs on port 830 and uses SSH for transport.

SSH is enabled automatically when the NETCONF feature is enabled.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF on IOS-XE

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface>
          <name/>
        </interfa
      </interfac
    </fil
  </get-c
</rpc>
```

A further filter restricting what we specifically want to get from the data store.

Global Config Mode:

netconf-yang

NETCONF listens on any IP address assigned to the system.

When enabled, NETCONF runs on port 830 and uses SSH for transport.

SSH is enabled automatically when the NETCONF feature is enabled.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

NETCONF on IOS-XE

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface>
          <name/>
        </interface>
      </interfaces>
    </filter>
  </get-config>
</rpc>
```

All the XML tags needed to close out our code.

Global Config Mode:

netconf-yang

NETCONF listens on any IP address assigned to the system.

When enabled, NETCONF runs on port 830 and uses SSH for transport.

SSH is enabled automatically when the NETCONF feature is enabled.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

Server / Host

Parameters

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

Type of HTTP

Resource

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

The hostname or IP address and port number of the device running the RESTCONF agent you want to connect to.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

The connection point for RESTCONF requests.

Typically = RESTCONF

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

The storage location that contains the information you want to retrieve or configure.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

```
module: ietf-interfaces
  +--rw interfaces
  |  +--rw interface* [name]
  |     +--rw name                        string
  |     +--rw description?                string
  |     +--rw type                        identityref
  |     +--rw enabled?                    boolean
  |     +--rw link-up-down-trap-enable?   enumeration {if-mib}?
  |     +--ro admin-status                enumeration {if-mib}?
  |     +--ro oper-status                 enumeration
  |     +--ro last-change?                yang:date-and-time
***output omitted***
  |        +--ro out-broadcast-pkts?   yang:counter64
  |        +--ro out-multicast-pkts?   yang:counter64
  |        +--ro out-discards?         yang:counter32
  |        +--ro out-errors?           yang:counter32
  x--ro interfaces-state
     x--ro interface* [name]
        x--ro name               string
        x--ro type               identityref
        x--ro admin-status       enumeration {if-mib}?
        x--ro oper-status        enumeration
        x--ro last-change?       yang:date-and-time
        x--ro if-index           int32 {if-mib}?
        x--ro phys-address?      yang:phys-address
***output omitted***
```

The YANG module that has the information you want to retrieve or configure.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

```
module: ietf-interfaces
  +--rw interfaces
  |  +--rw interface* [name]
  |     +--rw name                        string
  |     +--rw description?                string
  |     +--rw type                        identityref
  |     +--rw enabled?                    boolean
  |     +--rw link-up-down-trap-enable?   enumeration {if-mib}?
  |     +--ro admin-status                enumeration {if-mib}?
  |     +--ro oper-status                 enumeration
  |     +--ro last-change?                yang:date-and-time
***output omitted***
  |        +--ro out-broadcast-pkts?   yang:counter64
  |        +--ro out-multicast-pkts?   yang:counter64
  |        +--ro out-discards?         yang:counter32
  |        +--ro out-errors?           yang:counter32
  x--ro interfaces-state
     x--ro interface* [name]
        x--ro name               string
        x--ro type               identityref
        x--ro admin-status       enumeration {if-mib}?
        x--ro oper-status        enumeration
        x--ro last-change?       yang:date-and-time
        x--ro if-index           int32 {if-mib}?
        x--ro phys-address?      yang:phys-address
***output omitted***
```

The container in the YANG module that has the information you want to retrieve or configure.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

```
module: ietf-interfaces
  +--rw interfaces
  |  +--rw interface* [name]
  |     +--rw name                        string
  |     +--rw description?                string
  |     +--rw type                        identityref
  |     +--rw enabled?                    boolean
  |     +--rw link-up-down-trap-enable?   enumeration {if-mib}?
  |     +--ro admin-status                enumeration {if-mib}?
  |     +--ro oper-status                 enumeration
  |     +--ro last-change?                yang:date-and-time
***output omitted***
  |        +--ro out-broadcast-pkts?   yang:counter64
  |        +--ro out-multicast-pkts?   yang:counter64
  |        +--ro out-discards?         yang:counter32
  |        +--ro out-errors?           yang:counter32
  x--ro interfaces-state
     x--ro interface* [name]
        x--ro name               string
        x--ro type               identityref
        x--ro admin-status       enumeration {if-mib}?
        x--ro oper-status        enumeration
        x--ro last-change?       yang:date-and-time
        x--ro if-index           int32 {if-mib}?
        x--ro phys-address?      yang:phys-address
***output omitted***
```

The leaf in the container in the YANG module that has the specific information you want to retrieve or configure.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF URLs

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

```
module: ietf-interfaces
  +--rw interfaces
  |  +--rw interface* [name]
  |     +--rw name                        string
  |     +--rw description?                string
  |     +--rw type                        identityref
  |     +--rw enabled?                    boolean
  |     +--rw link-up-down-trap-enable?   enumeration {if-mib}?
  |     +--ro admin-status                enumeration {if-mib}?
  |     +--ro oper-status                 enumeration
  |     +--ro last-change?                yang:date-and-time
***output omitted***
  |        +--ro out-broadcast-pkts?   yang:counter64
  |        +--ro out-multicast-pkts?   yang:counter64
  |        +--ro out-discards?         yang:counter32
  |        +--ro out-errors?           yang:counter32
  x--ro interfaces-state
     x--ro interface* [name]
        x--ro name               string
        x--ro type               identityref
        x--ro admin-status       enumeration {if-mib}?
        x--ro oper-status        enumeration
        x--ro last-change?       yang:date-and-time
        x--ro if-index           int32 {if-mib}?
        x--ro phys-address?      yang:phys-address
***output omitted***
```

Filters that can be used to control the results that are returned.

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RESTCONF on IOS-XE

https://<NAME:PORT>/<ROOT>/<DATASTORE>/<YANG MODULE:CONTAINER>/<LEAF>?<OPTIONS>

```
module: ietf-interfaces
  +--rw interfaces
  |  +--rw interface* [name]
  |     +--rw name                        string
  |     +--rw description?                string
  |     +--rw type                        identityref
  |     +--rw enabled?                    boolean
  |     +--rw link-up-down-trap-enable?   enumeration {if-mib}?
  |     +--ro admin-status                enumeration {if-mib}?
  |     +--ro oper-status                 enumeration
  |     +--ro last-change?                yang:date-and-time
***output omitted***
  |        +--ro out-broadcast-pkts?   yang:counter64
  |        +--ro out-multicast-pkts?   yang:counter64
  |        +--ro out-discards?         yang:counter32
  |        +--ro out-errors?           yang:counter32
  x--ro interfaces-state
     x--ro interface* [name]
        x--ro name               string
        x--ro type               identityref
        x--ro admin-status       enumeration {if-mib}?
        x--ro oper-status        enumeration
        x--ro last-change?       yang:date-and-time
        x--ro if-index           int32 {if-mib}?
        x--ro phys-address?      yang:phys-address
***output omitted***
```

HTTPS (port 443)
    ip http secure-server

listens on any IP address assigned to the system

Enable RESTCONF
    R1(config)#restconf

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Python Exam Prep

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

What is Python?

A programming language that is:

- Powerful
- Fast
- User friendly
- Easily integrated
- Open
  - Windows, MAC, Linux, Routers, Switches, etc…

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Why Python for Network Folks?

Programmatically manage, monitor, and maintain our networks

- Eliminate the CLI

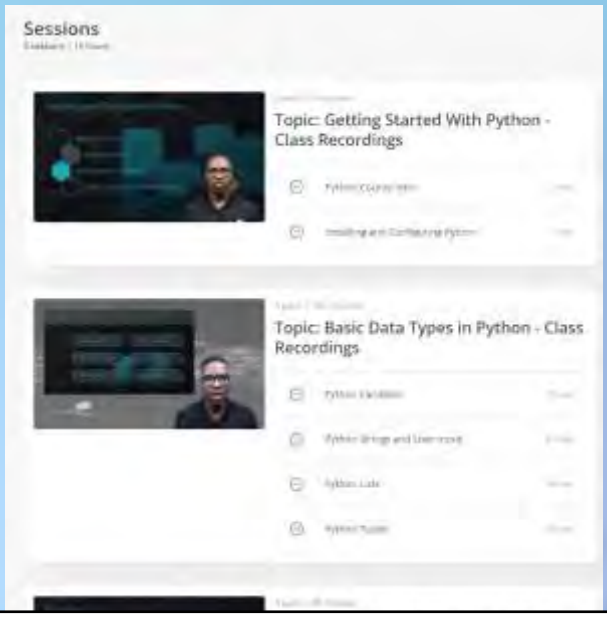
www.python.org

- For the latest and greatest information

©2023 by StormWind LLC. All rights reserved.

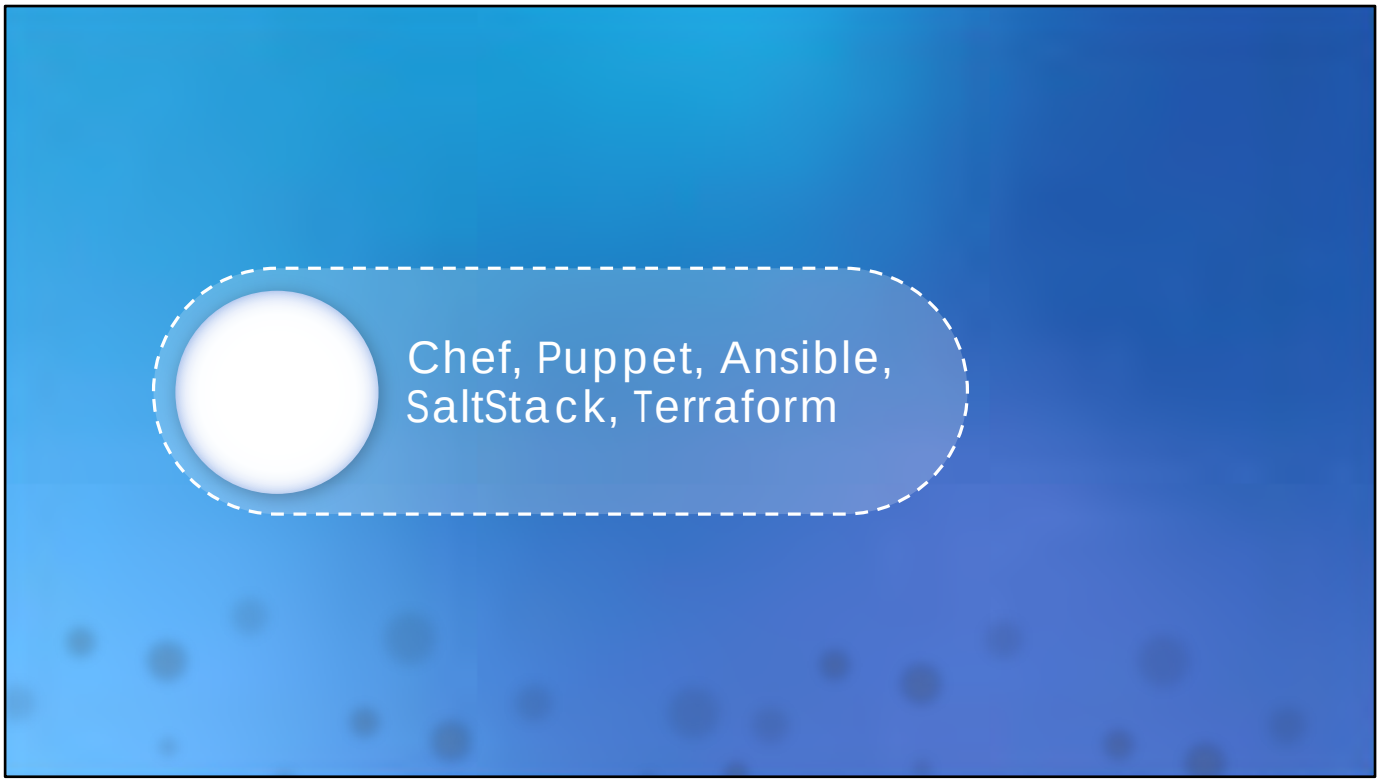
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Why Python for Network Folks?



Take the StormWind Course:
Python Foundations

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Chef, Puppet, Ansible, SaltStack

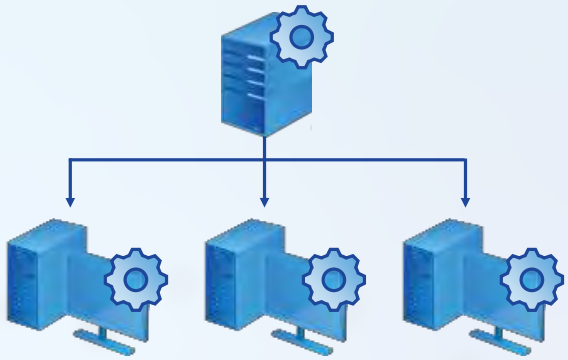
Configuration Management and Automation Tools

- Automate deployment and configuration of resources
- Reduce manual effort and administrative burden
- Improve consistency across resources
- Assist in tracking changes across networks

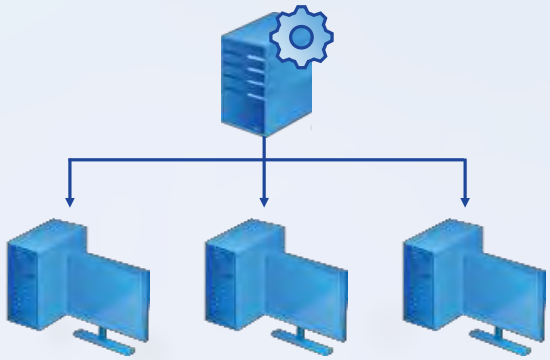
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Agent vs Agentless

Agent-based tools require agent software to be installed on managed systems



Agentless systems do not require additional software to be installed on managed systems



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Common Configuration Management Tools

Puppet

Chef

SaltStack

Ansible

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Common Configuration Management Tools

Factor	Puppet	Chef	Ansible	SaltStack	Terraform
Agent / Server	Both Required	Both Required	No / No	Optional	No / No
Scripting Language	Ruby-based	Ruby	YAML	YAML	HCL
Architecture	Puppet masters and agents	Chef server and Chef clients	Control station and remote hosts	Salt master and minions	Control station and remote hosts
Procedural or Declarative	Declarative	Procedural	Procedural	Declarative	Declarative
Push or Pull Model	Pull	Pull	Push	Push	Push
Terminology	Modules and manifests	Cookbooks and recipes	Playbooks and plays	Pillars and grains	Configurations and Documents
Mutable or Immutable	Mutable	Mutable	Mutable	Mutable	Immutable
Agentless version	Puppet Bolt	N/A	Yes	Salt SSH	Yes
Orchestration or Configuration Management	Configuration Management	Configuration Management	Both	Both	Orchestration
Protocols and Ports	TCP 8140	TCP 10002	SSH 22	TCP 4505 / 4506	SSH 22

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

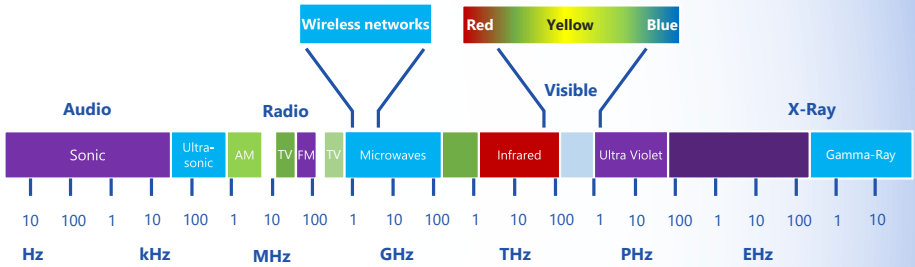
ENCOR Wireless Preparation

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Layer 1 Wireless

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

RF Fundamentals - RF Spectrum



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

802.11 Specifications

Protocol	Frequency Band	Bandwidth
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz, 5GHz	450 Mbps
802.11ac (5)	5 GHz	6.933Mbps (~7 Gbps)
802.11ax (6/6E)	2.4 GHz, 5GHz, 6GHz(6E)	9-10ish Gbps
802.11be (7)	2.4GHz, 5GHz, 6GHz	46ish Gbps

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Signal Measurements You May See:

mW (1mW = 0 dBm)

Most accurate
Loots of 00's
    Ex: -60 dBm = .000001

dBm

Decibels to a milliwatt
Commonly measured from -30 to -100

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

dBm

Easiest and most consistent

Strength of the signal

Power of 3 (approx.)

+3 db equals a doubling of signal strength
-3 db loss equals to a halving of signal strength

RSSI (not standardized)

Received Signal Strength Indicator
- 0-60
- 0-255

Handled differently by different vendors

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

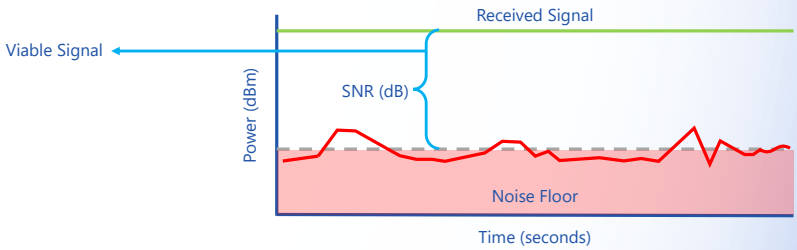
Signal Strength	Node Connectivity		Required for
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/ VoWi-Fi, Streaming Video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, Web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Signal to Noise Ratio

Difference between the received signal and the noise floor

Noise floor – background



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Calculating SNR

Signal subtract Noise

Signal -65 dBm

RSSI (Received Signal Strength Indicator)

Noise -90 dBm

SNR (dB) = RSSI dBm- Noise dBm

*Sometimes you may have to do conversions

(-65) – (-90) = 25 dB

©2023 by StormWind LLC. All rights reserved.

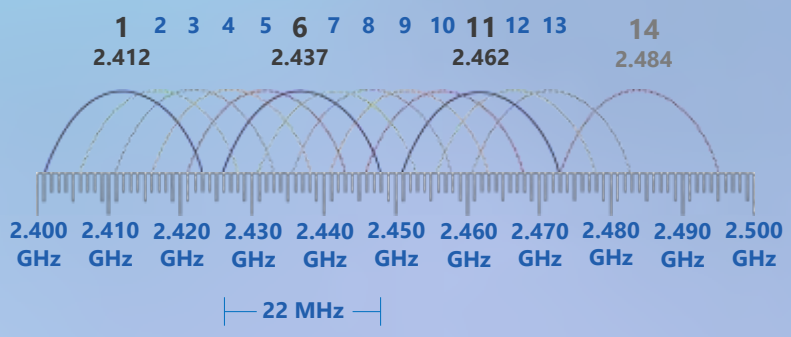
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SNR	
> 40 dB	Excellent quality, highest data rates.
25-40 dB	Very good quality, high data rates. **VOICE Minimum 25**
15-25 dB	Fair quality, good data rates. **DATA Minimum 20**
10-15 dB	Ok quality, lower data rates.
0-10 dB	Low to no signal, very low data rate to nothing

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IEEE Standards: 2.4 Gz Channel Use

Channel	GHz	Channel	GHz
1	2.412	8	2.447
2	2.417	9	2.452
3	2.422	10	2.457
4	2.427	11	2.462
5	2.432	12	2.467
6	2.437	13	2.472
7	2.442	14	2.484



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

IEEE Standards: 5 GHz Channel Use

5 GHz

U-NII-1		U-NII-2	
Channel	**GHz**	**Channel**	**GHz**
36	5.180	52	5.260
40	5.200	56	5.280
44	5.220	60	5.300
48	5.240	64	5.320

U-NII-2 Extended	
Channel	**GHz**
100	5.500
104	5.520
108	5.540
112	5.560
116	5.580
120	5.600
124	5.620
128	5.640
132	5.660
136	5.680
140	5.700

U-NII-3	
Channel	**GHz**
149	5.745
153	5.765
157	5.785
161	5.805

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

5Ghz Interference Sources

- Weather / Hospital / Airplane Radar can be an issue
  - Mostly in the UNI-II and UNI II Extended
    - Stay off those channels
  - Disable DFS Channels
    - DFS rules only apply to the 5.250 – 5.725 Ghz band

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Antenna Types

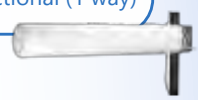
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AP Antenna Options

Antennas only divert, direct, or concentrate radio energy in som direction

Ceiling Mount Omni

Yagi Directional (1 way)



Patch Directional

Dipole (Omni)

Diversity Patch Directional

Parabolic Dish (directional)

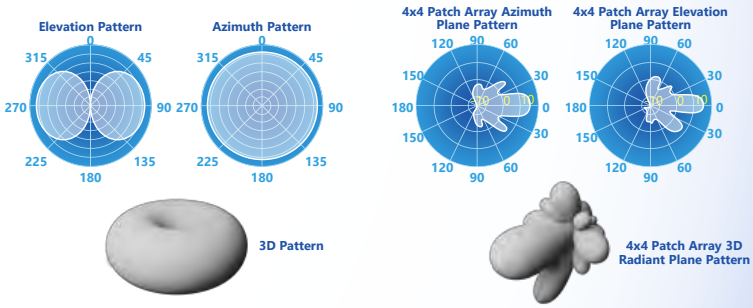
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Radiation Patterns

Directional (angular) dependence of the strength of the radio waves from the antenna or other source.

- The shape of the transmission pattern
- Direction concentrates the signal to a certain extent, thereby adding some gain to the signal in that direction



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Gain

How well the antenna converts input power into radio waves headed in a specified direction.

In a receiving antenna, how well the antenna converts radio waves arriving from a specified direction into electrical power.

When no direction is specified, gain is understood to refer to the peak value of the gain, the gain in the direction of the antenna's main lobe

Higher gain = better quality signal

- Every antenna gain is measured against an isotropic antenna
  - Theoretical antenna used as a standard baseline
- Gain is measured in decibels and is displayed as dBi
  - Decibels (dB) against that isotropic (i) antenna

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

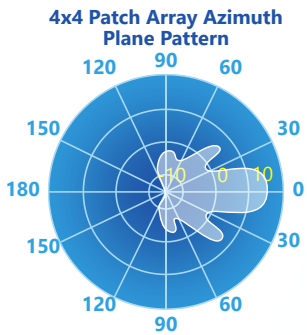
Beamwidth

Angle from which the majority of the antenna's power radiates.

Varies base on design of antenna

May be azimuth or elevation

The main lobe

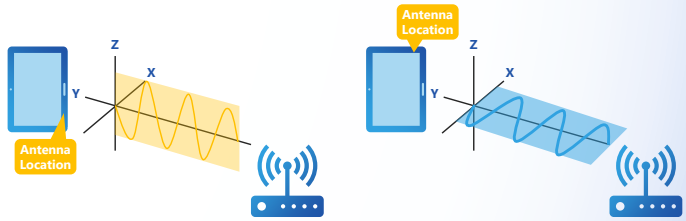


©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Polarization

- The Orientation of the signal as it leaves the antenna
- All antennas have some polarization (ex. Horizontal / Vertical)
  - Certain antennas are more sensitive to these waves than other antennas
- Regardless of sensitivity, antennas with the same polarization have the best communication path
  - Polarization can affect AP-to-client and AP-to-AP signal quality

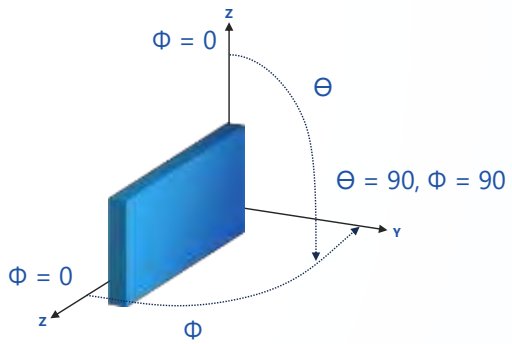


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Plane Patterns

azimuth ="the horizon" or "the horizontal"

elevation = "the vertical"

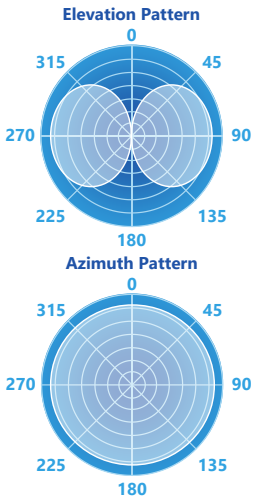


©2023 by StormWind LLC. All rights reserved.

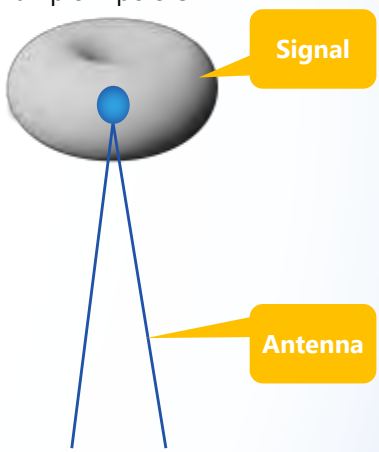
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Omnidirectional

360-degree radiation pattern



Example Dipole Omni

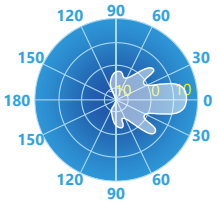


©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

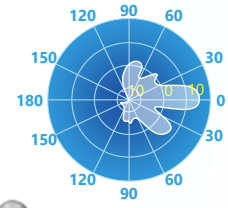
Directional

- Different styles and shapes
- Directs energy in one direction
  - Same energy but all focused in one area

4x4 Patch Array Azimuth Plane Pattern



4x4 Patch Array Elevation Plane Pattern



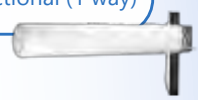
4x4 Patch Array 3D Radiant Plane Pattern

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AP Antenna Options

Ceiling Mount Omni

Yagi Directional (1 way)



Patch Directional

Dipole (Omni)

Diversity Patch Directional

Parabolic Dish (directional)

Antennas only divert, direct, or concentrate radio energy in som direction

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Effective Isotropic Radiated Power

- Measured power radiated in a direction by an ideal isotropic antenna
- Accounts for connection Loss
- EIRP= Tx Power + Tx Antenna – Tx Cable

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Calculating EIRP

Tranmitter: Input power, measured in dBm

Decibels relative to milliwatt

Cable loss: Power loss over length, measured in dB

Antenna: Gain, energy focused into direction, measured in dBi

Compared to isotropic radiator (all directions at once)

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

EIRP Example

Tranmitter input: 20 dBm
Antenna gain: 12 dBi
Cable loss: -6 dB

EIRP= Tx Power + Tx Antenna – Tx Cable

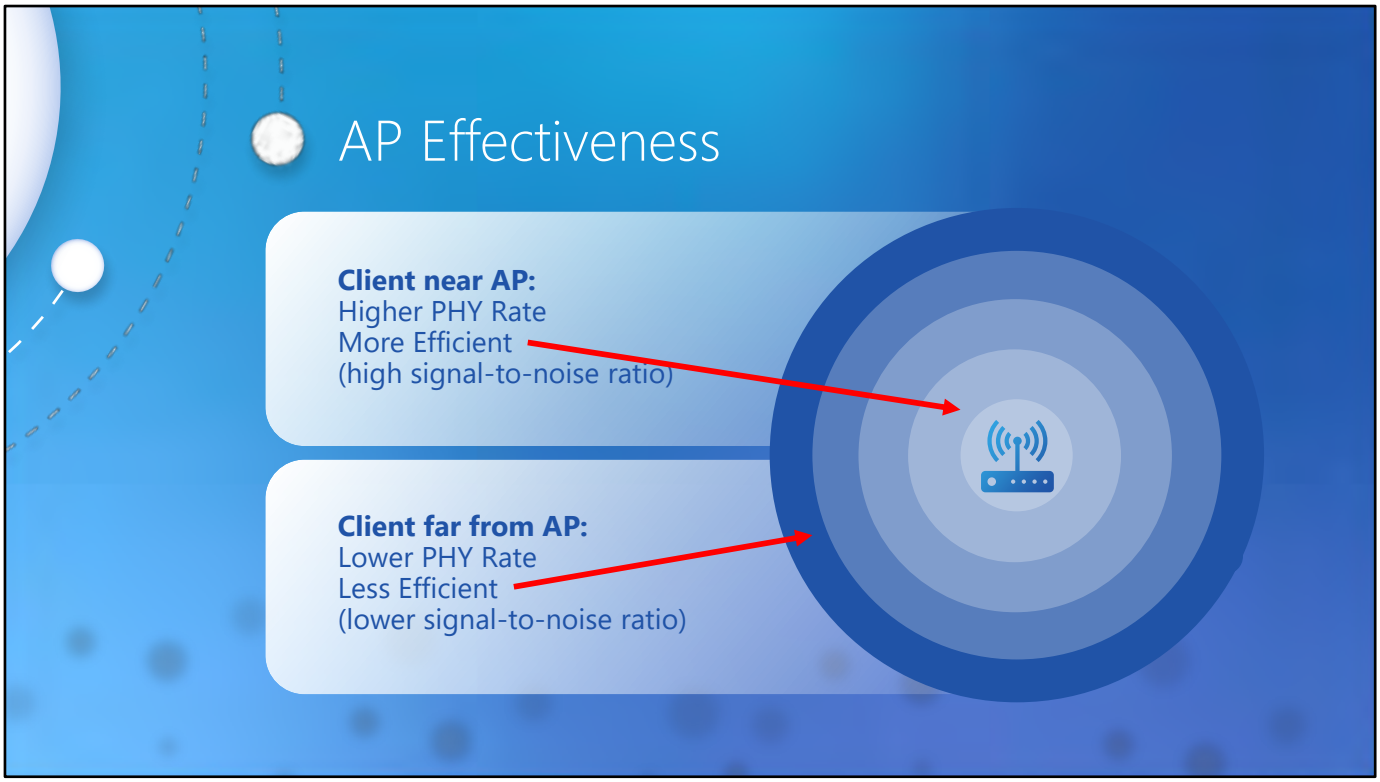
EIRP= 20 dBm + 12 dBi + 6 dB

EIRP= 26 dBm

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Wireless AP Placement

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

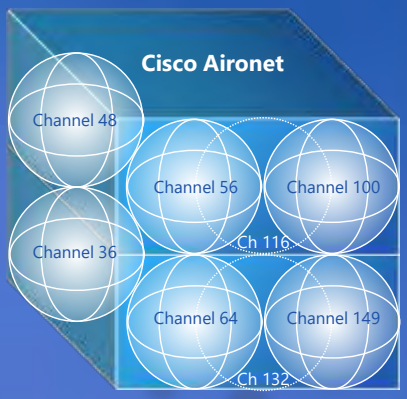
Ensuring Coverage

Overlapping cells

Separate non-touching channels

- Rooms
  - Start at edges working in to fill in dead zones — **2nd Floor**
  - Omnidirectional?
- Client Density
  - How many — **1st Floor**
- Directional Antennas
  - for specified coverage

Overlap can be 50% because of channel separation. The minimum should be 15%



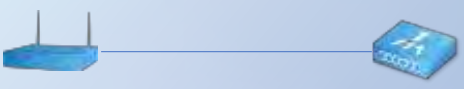
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AP Discovery and Join Process

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Process Steps

1. AP sends CAPWAP discovery request to WLC
2. Any and all WLCs that receive the discovery request respond with CAPWAP discovery response
3. AP chooses the WLCs from the response that were sent and sends a CAPWAP join request to the WLC it has chosen.
4. WLC affirms the process with a CAPWAP join response



1. Discovery Request →
2. Discovery Response ←

3. Join Request →
4. Join Response ←

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Two protocols for the phases

- CAPWAPP (modern)
  - Control and provision of wireless access points
- LWAPP
  - Lightweight Access Point Protocol

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Discovery Phase

Broadcast message on local network
- UDP 5246 (CAPWAP Discovery message)

Previously joined WLCs
- Up to 8 older WLC ip addresses can be checked

Using DHCP option 43
- If DHCP is used: One or more WLCs can be listed

DNS records
- Define Cisco-capwap-controller.local_domain IP address record

Manual configuration
- capwap ap ip address <ipaddress> <subnet>
- capwap ap default-gateway <ipaddress>
- capwap ap controller ip address <ipaddress>

**If you do not tell the LAP where the controller is via DHCP option 43, Domain Name System (DNS) resolution of Cisco-capwap-controller.local_domain, or statically configure it, the LAP does not know where in the network to find the management interface of the controller.*

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Option 43 configuration

When DHCP servers are programmed to offer WLAN Controller IP addresses as Option 43 for Cisco Aironet LAPs, the sub-option TLV block is defined in this way:

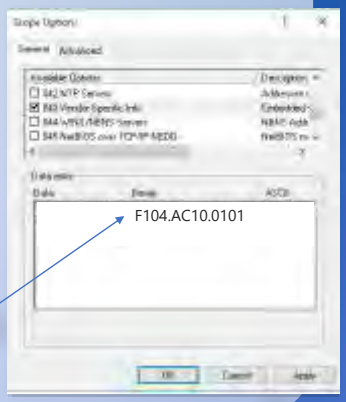
Type - 0xf1 (decimal 241).

Length - Number of controller IP addresses * 4.

Value - List of the WLC management interfaces, typically translated to hexadecimal values.

Cisco IOS option 43

option 43 hex F104.AC10.0101 ← Hex value



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Figuring out TLV for option 43

Type= F1 (always)

Length = Number of controller management IP address (x 4)… In this case lets say 1 controller

- If 1 ip address then 1 x 4 = 04
- If 2 ip addresses then 2 x 4 = 08

Value = IP address of the controller (sequentially in hex)

- To do this convert IP address to binary lets say 172.16.1.1
- Start from left to right (make life easy on yourself)
  - 172 = 10101100
  - 16 = 00010000
  - 1 = 00000001
  - 1= 00000001
- Then back to Hex
  - Break into 4 bits

1010 = A	1100 = C
0001 = 1	0000 = 0
0000 = 0	0001= 1
0000 = 0	0001= 1

Putting it all together

F1	04	AC100101

Configuration:

Configure option 43
Hex F104.AC10.0101

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

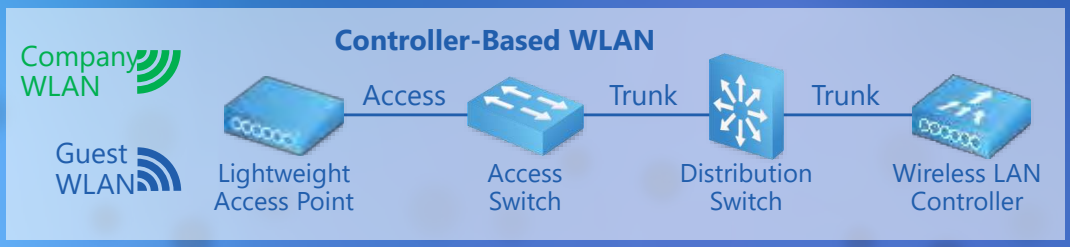
Discovery outside of a LAN

Use an IP helper address

- Similar to DHCP relay agent

DSW1 (config)# interface vlan #

DSW1 (config-if)# ip helper-address XXX.XXX.XXX.XXX



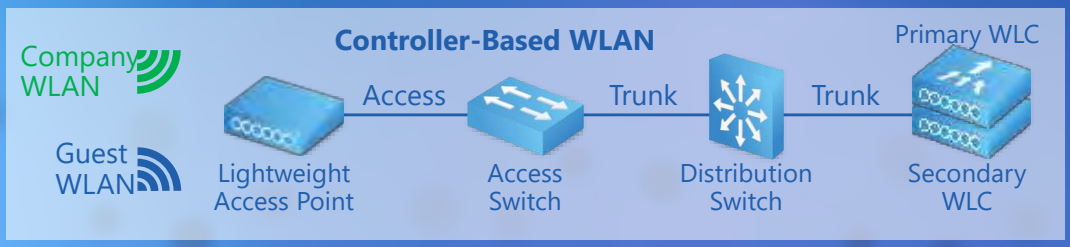
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Join Phase

Encrypted tunnel is created between AP-manager and AP

AP decision process priority

1. WLC it has joined before
2. Primary controller
3. WLC with lowest number of APs



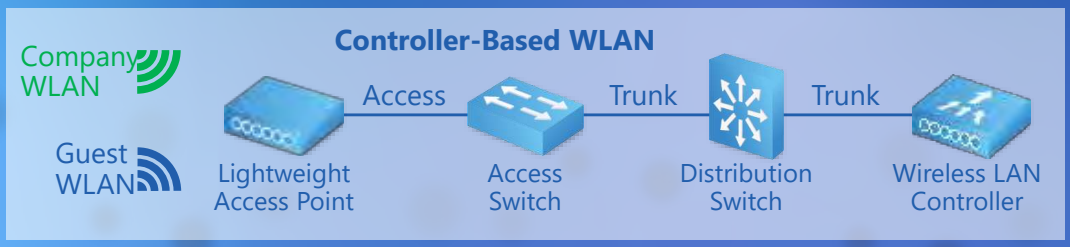
©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

After the Discover and Join Process

Additional steps to functionality

1. Image match between AP and WLC
   Compatibility
2. Configuration check
   Updates?
3. Registration



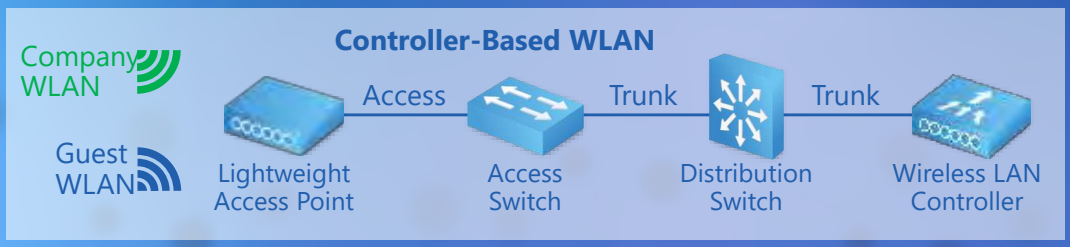
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Architecture Deployment Models

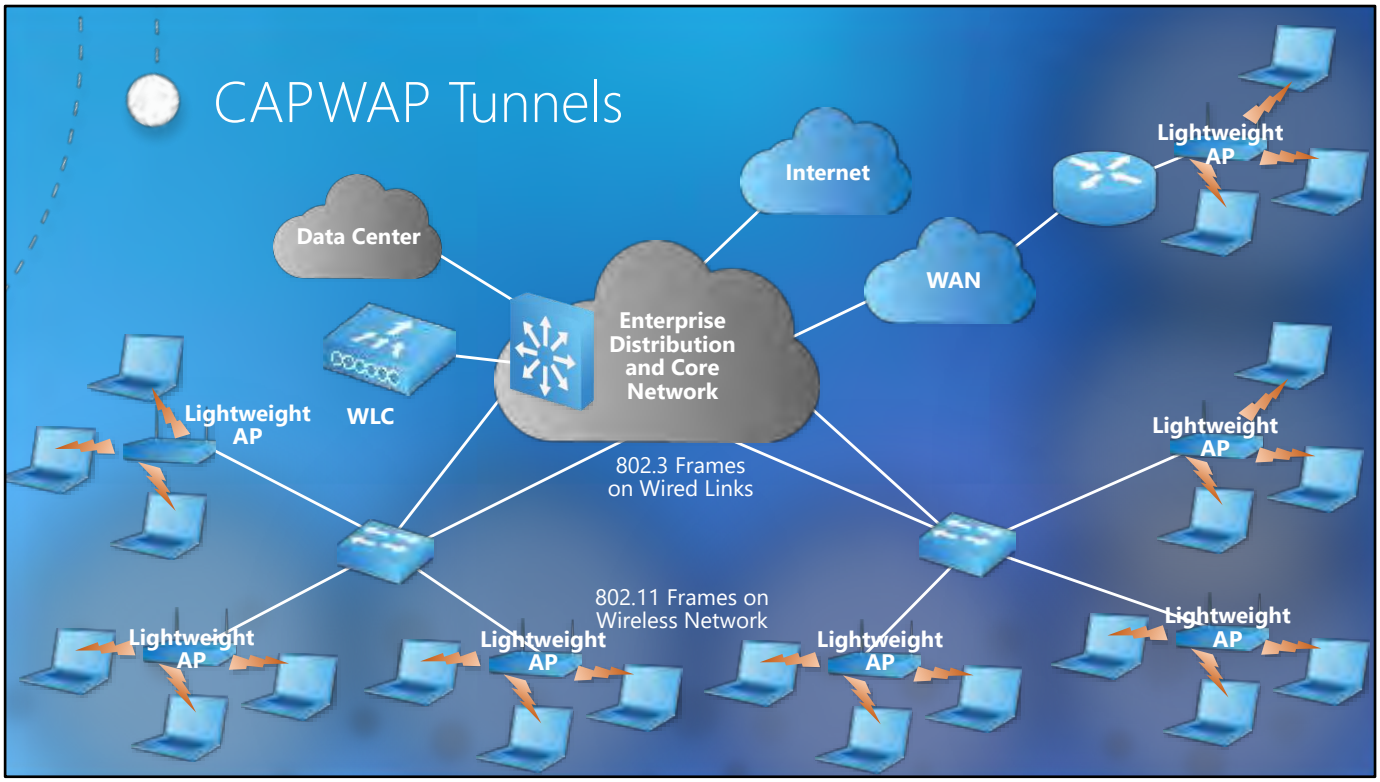
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Controller-Based Configuration

- Centralized configuration management
- CAPWAP tunnels run management traffic to controller



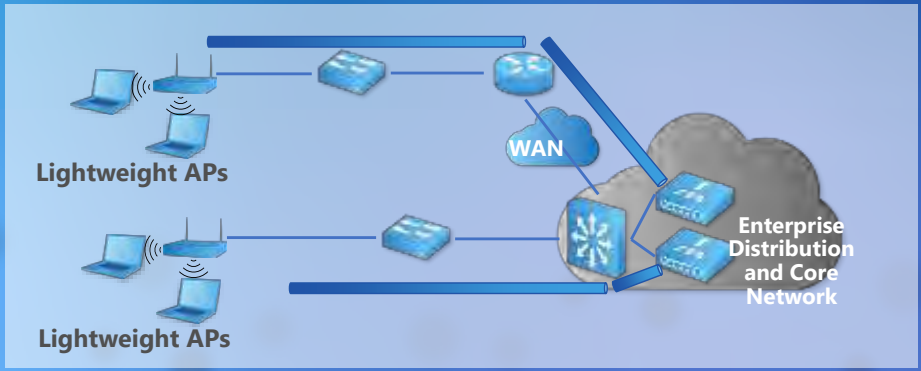
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Centralized

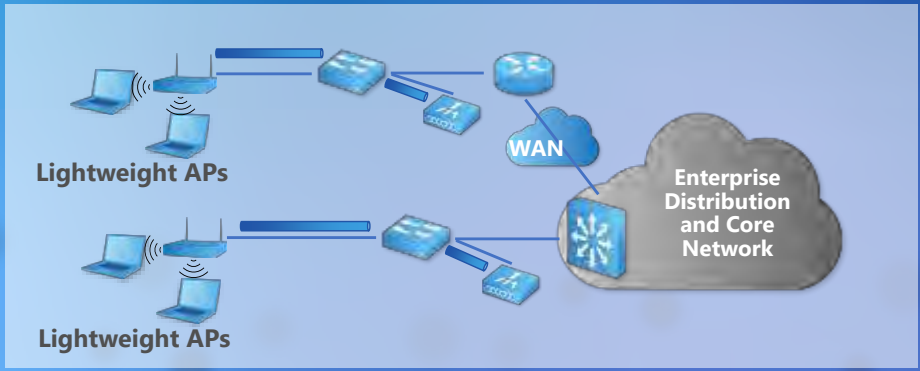
- Wireless LAN controllers are centrally located
- CAPWAP Tunnels are used to transport management packets



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Distributed

- WLCs are at individual sites
- Expensive solution



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Lightweight APs

Used by both Distributed and Centralized

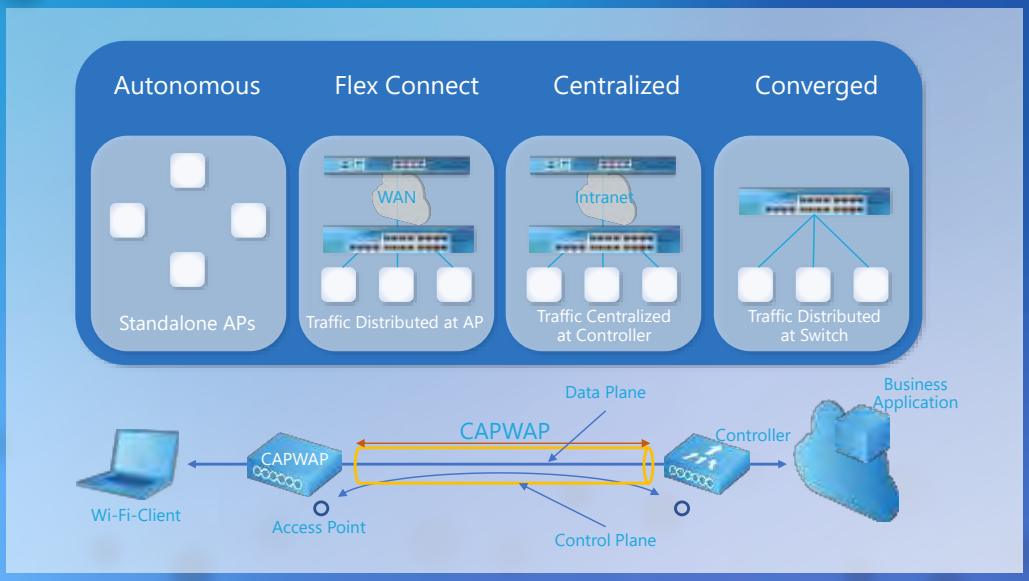
Types	Characteristics
Lightweight APs	Rely on central WLAN controller Controller configures the APs Updates dynamically as conditions change.

Local Mode (Default) → Requires WLC Connectivity

FlexConnect Mode → Can still function if WLC connection is interrupted

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

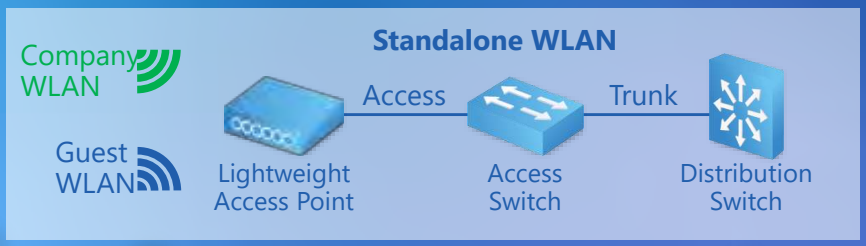
AP Review



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Controller-less Configuration

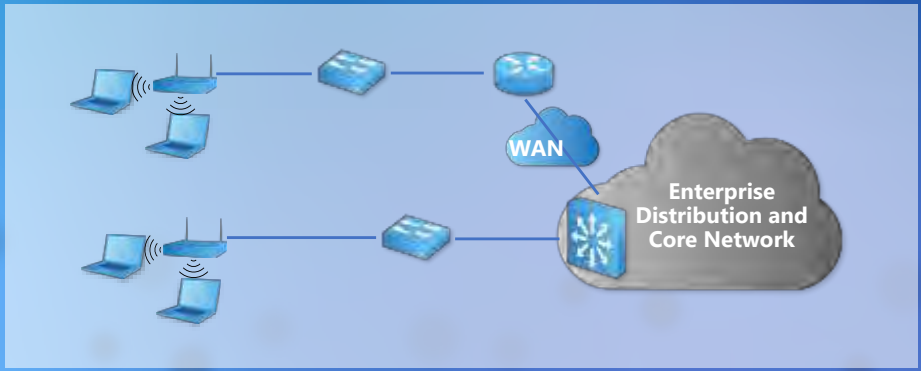
- Trunk for the win
- Small deployments



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Controller-less

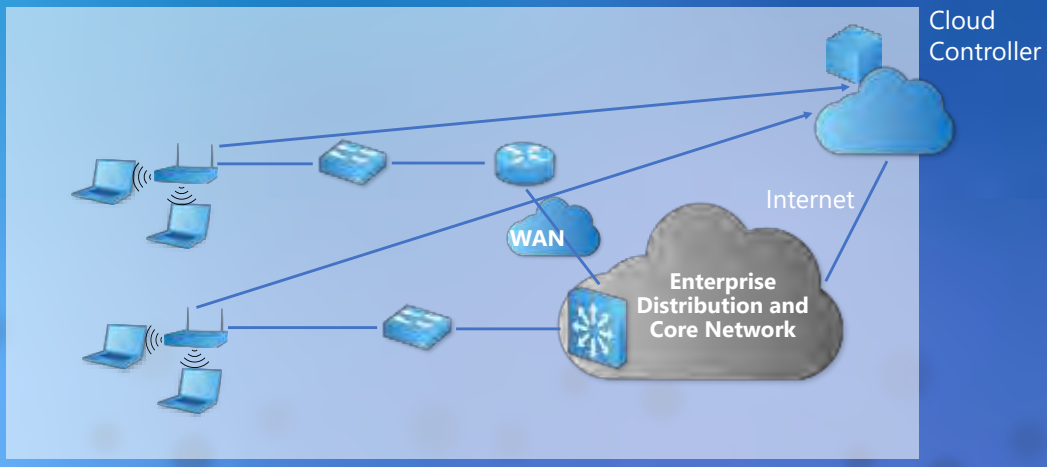
- No WLC's
- AP OS handles requests etc.



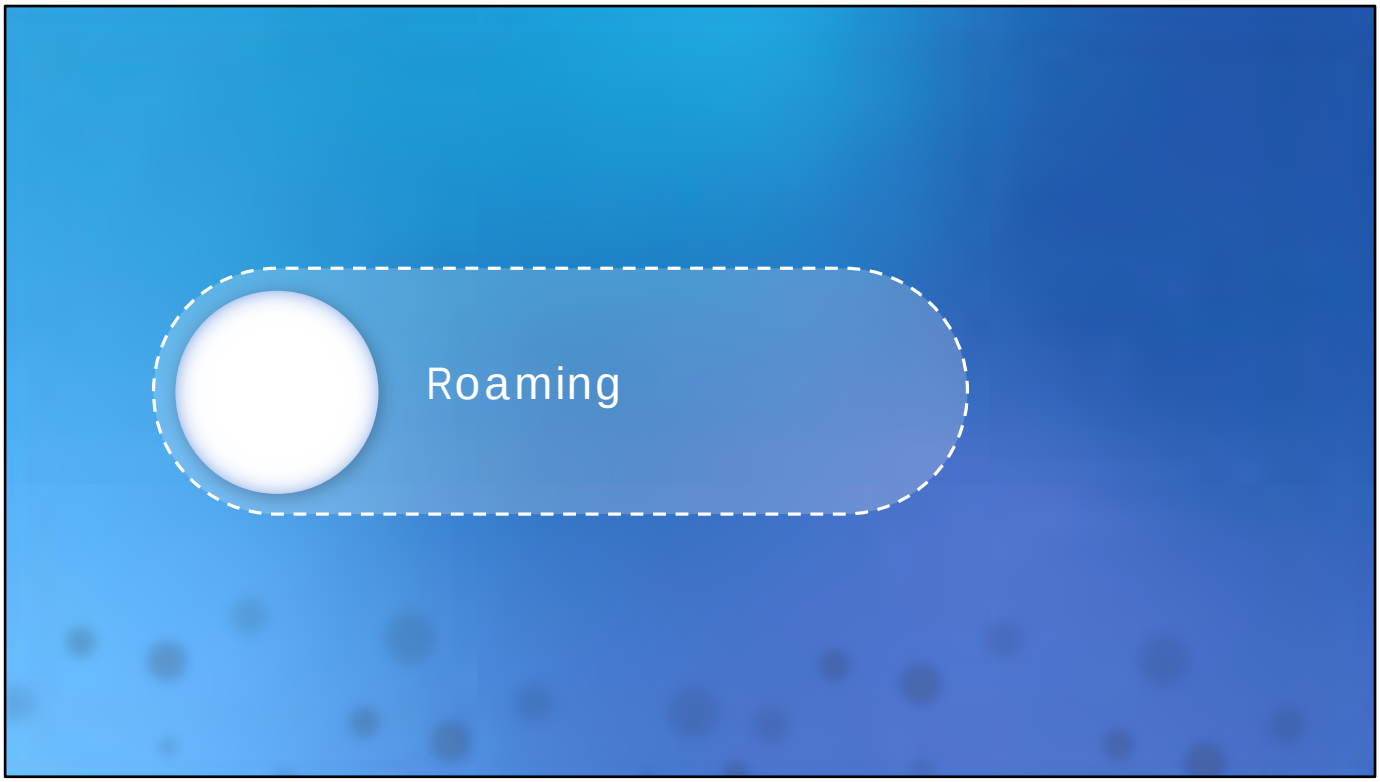
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Cloud

Cloud based controller



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



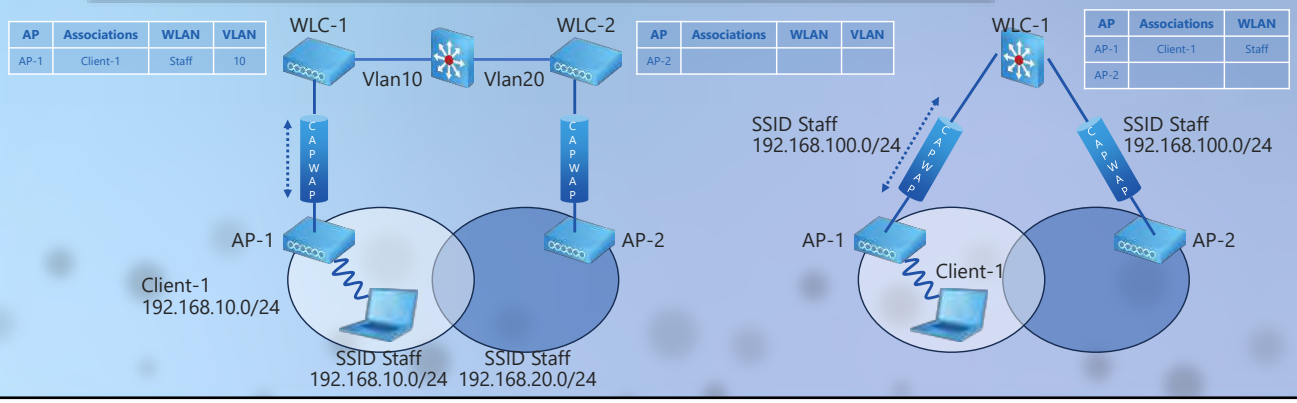
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Inter and Intra Controller Roaming

Inter : Between WLC's

All controllers within a mobility group must be configured with the same virtual interface IP address. Otherwise, the handoff does not complete, and the client loses connectivity for a period of time.

Intra : within a single WLC



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

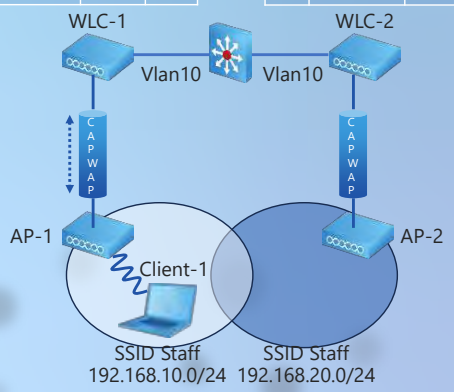
Layer 2 Roaming

Client roaming between WLC's within the same subnet

>20 ms

AP	Associations	WLAN	VLAN
AP-1	Client-1	Staff	10

AP	Associations	WLAN	VLAN
AP-2			



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

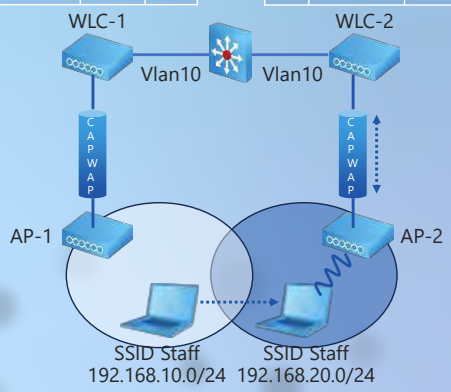
Layer 2 Roaming

Client roaming between WLC's within the same subnet

>20 ms

AP	Associations	WLAN	VLAN
AP-1		Staff	

AP	Associations	WLAN	VLAN
AP-2	Client-1	Staff	10



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Layer 3 Roaming

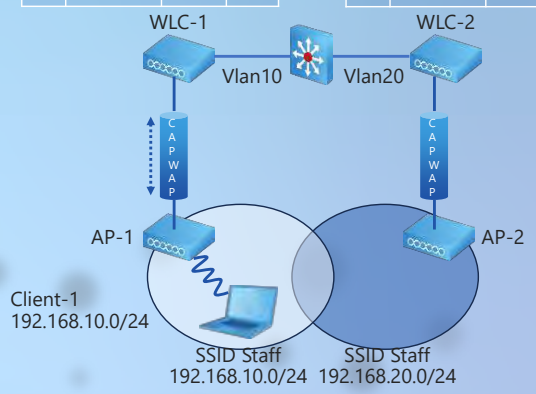
Originally controller (anchor controller)

A WLC can be configured as a static anchor for a WLAN, directing guest clients to it via Layer 3 roaming tunnels. *special circumstance*

Reassociated client (foreign controller)

AP	Associations	WLAN	VLAN
AP-1	Client-1	Staff	10

AP	Associations	WLAN	VLAN
AP-2			



1. Original controller marks the client with an "Anchor" entry in its own client database.
2. The database entry is copied to the new controller client database and marked with a "Foreign" entry in the new controller.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Layer 3 Roaming

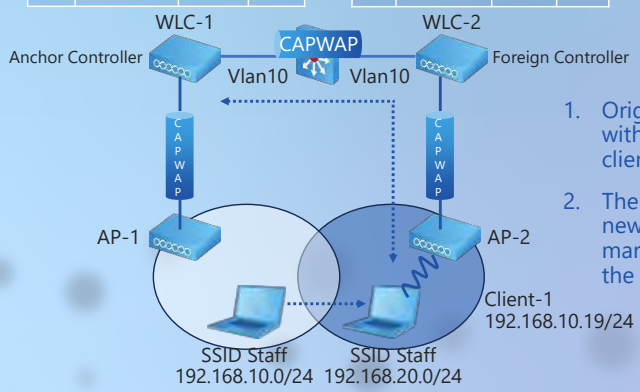
Originally controller (anchor controller)

A WLC can be configured as a static anchor for a WLAN, directing guest clients to it via Layer 3 roaming tunnels. *special circumstance*

Reassociated client (foreign controller)

AP	Associations	WLAN	VLAN
WLC-2	Client-1 Mobile	Staff	10

AP	Associations	WLAN	VLAN
AP-2	Client-1	Staff	



1. Original controller marks the client with an "Anchor" entry in its own client database.
2. The database entry is copied to the new controller client database and marked with a "Foreign" entry in the new controller.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SDA Roaming

SD-Access deployments

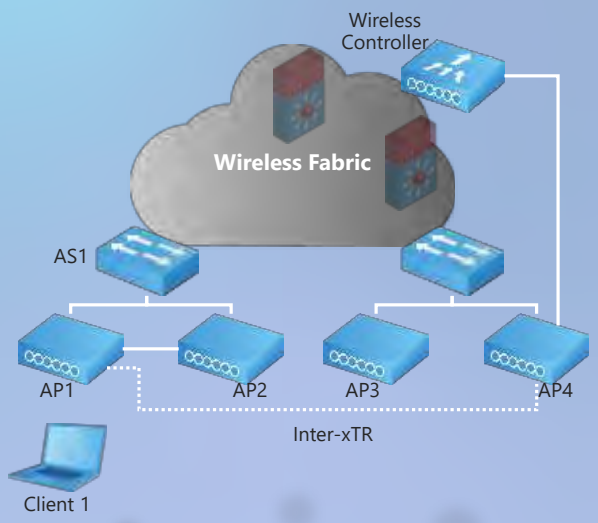
Inter-xTR

Across fabric switches

Intra-xTR

Within a single fabric switch

***xTR stands for an access-switch that is a fabric edge node**



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

AP Modes

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Client-Serving AP modes

These modes allow APs to provide networking to clients

- Local
- FlexConnect
- Bridge (Mesh)
- Flex+Bridge

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Local Mode

- Default mode for lightweight APs
- Two CAPWAP tunnels to the WLC
  - Data and Management
- AP directly to WLC
- Requires a reliable connection to the WLC
  - No connection no access

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

FlexConnect Mode

- Data traffic can be switched locally
  - Does not need to go back to the controller
  - Allows wireless data traffic to egress at the switch port of the access point
- Still managed by the WLC
- Can still function if not connected to WLC
  - To a point
  - Understand the FlexConnect Feature Matrix for AireOS - Cisco

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Bridge or Mesh Mode

- Dedicated point-to-point / multipoint between networks
- Extend networks
  - Indoor or outdoor mesh networks

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Flex+Bridge

FlexConnect features assigned to mesh APs

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Network Management Cisco AP Mode

Modes that provide dedicated management tools

- Monitor
- Rogue Detector
- SE-Connect
- Sniffer

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Monitor Mode

Does not transmit

No SSID's
Listener only

Monitors the WiFi channel for

IDS Events
Rogue access points
Location-based services

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Rogue Detector

- Dedicated rogue detector
  - Wired and wireless
- Mac address comparison (wired vs wireless)
- AP can still broadcast SSID
  - Serve clients
  - Wireless connections are valid

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

SE-Connect

- Dedicated connection to Cisco CleanAir
  - Spectrum analysis
    - Cisco Spectrum Expert
    - MetaGeek Chanalyzer
- Used to discover interference

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Sniffer

- Dedicated traffic receiver
- Traffic is forwarded to a network analyzer
  - Wireshark
  - OmniPeek
- No broadcasts
- No Client dconnects
- Troubleshooting tool

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Features

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Aggressive Load Balancing

- Configured on WLC
  - Can be a single controller
- Allows the Lightweight Access Points to load-balance clients among APs
- Works at the association phase
  - If conditions are met (too busy)
    - Code 17 is sent (some OS's may ignore): Find another AP
    - You can also enable or disable load balancing on a particular WLAN,
      - Useful for a select group of clients, such as time-sensitive voice clients.

Voice clients does not authenticate when delay is configured to more than 300 ms
To avoid: Configure Central-authentication, local-switching WLAN with Cisco Centralized Key Management (CCKM),a pagent router between an AP and WLC with a delay of 600 ms (300 ms UP and 300 ms DOWN), and try associating the voice client.

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Peer to Peer Blocking (P2P)

- Allows more control of how traffic is directed
  - Bridged locally within controller, dropped by the controller, forwarded to the upstream VLAN
- Applied to individual WLANs
- Does not apply to multicast traffic
- Local and central switched WLANs
  - Disabled: (default value) bridges traffic locally within the controller
  - Drop: Controller discards P2P traffic
  - Forward-UpStream: Packets are forwarded on the upstream VLAN, upstream device decides
  - **For FlexConnect local switching, select Drop from the P2P Blocking drop-down list and select the FlexConnect Local Switching check box.*

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Dynamic Channel Assignment

- Part of Cisco Radio Resource Management (RRM)
- Dynamically changes Channels based on Cost metric
  - RSSI based metric which combines AP load, Co-channel interference, Adjacent channel interference and non wi-fi sourced interference
- Configured under 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz)
  - **Automatic** will run every 10 minutes by default. The anchor point is used to set the time of day the algorithm would start.
    - For less frequent channel changes, increase the interval.
    - Keep in mind that clients will be disconnected briefly for a channel change.
  - **Freeze** does not run the DCA algorithm unless triggered.
  - **Off** disables the use of RRM and its auto-rf capabilities.

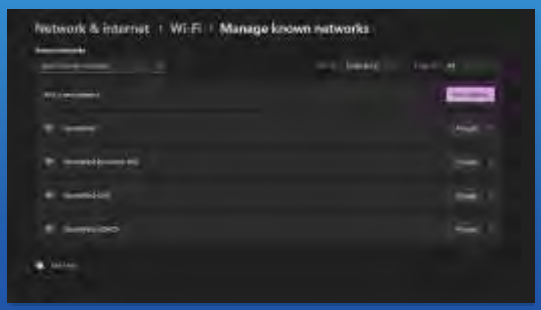
©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

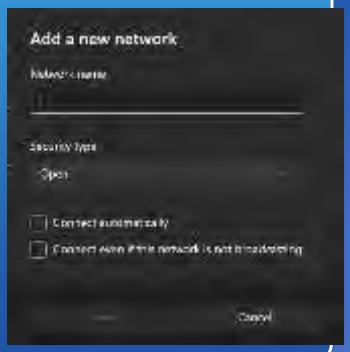
Manually adding a Wireless SSID to a client

Many Enterprise environments do not broadcast SSIDs for security reasons.

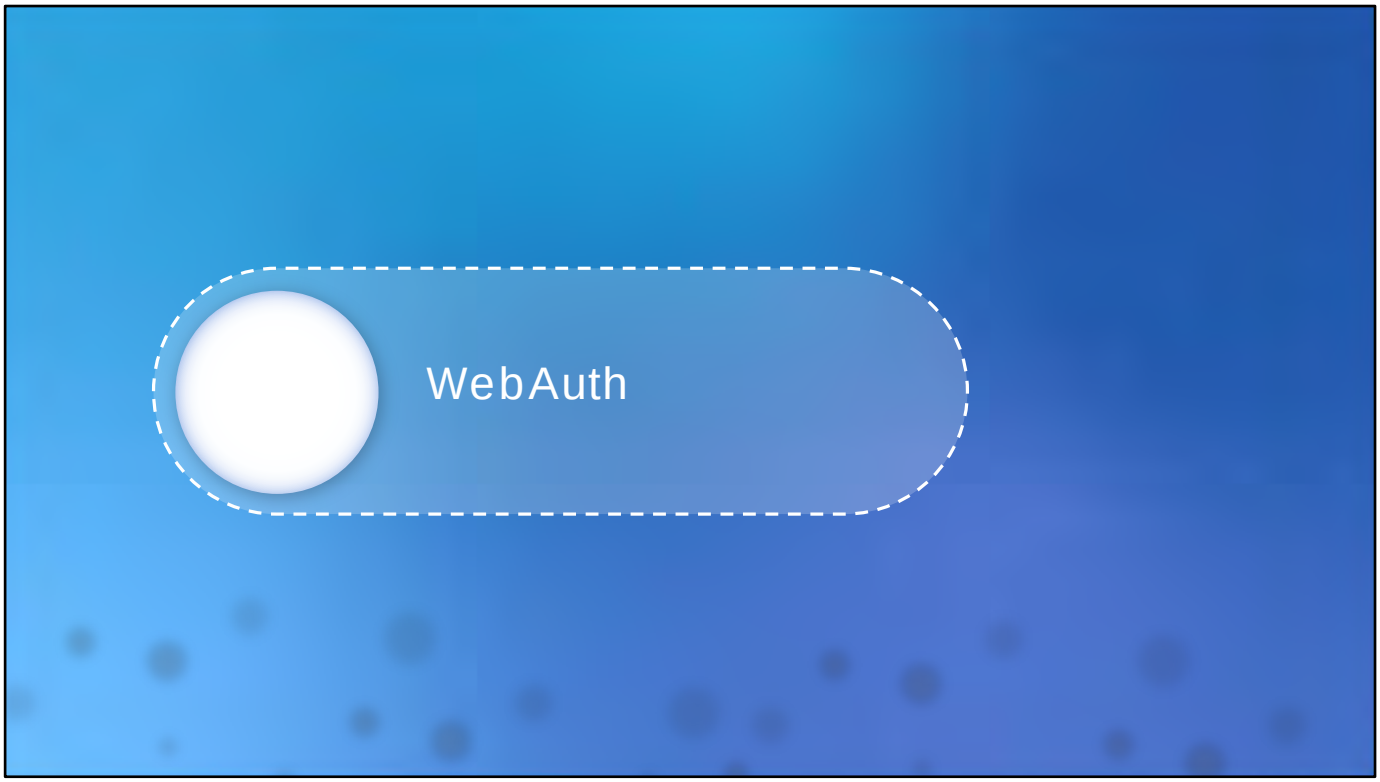
Manually add a SSID to a client

Example: Windows 11





©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Web Auth Authentication Types

Webauth:

- Basic web authentication method where the controller presents a policy page with the user name and password.
- You need to enter the correct credentials to access the network.

Authbypass:

- The controller uses the MAC address as the client identity
- Validates this with the authentication server that has a database of client MAC addresses that are allowed network access.

Consent (web-passthrough):

- The controller redirects you to a usage policy page without prompting you to enter any credentials for user authentication.
- To access the network, you must accept the policy.

Webconsent:

- This is a combination of webauth and consent web authentication types in which the controller redirects you to a usage policy page with Accept or Deny buttons along with user name or password.
- You need to enter the correct credentials and accept the usage policy to access the network

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Web Auth Roles

Client:

Requests access to the WLAN and its services and responds to requests from the controller.

Access Point:

Connects directly to a switch through a wired Ethernet connection and provides wireless connection to client devices.

Restricts IP traffic except DHCP and DNS packets until the guest provides valid credentials.

Controller:

Manages the access points and clients.

The WLC intercepts HTTP requests from the client and redirects the client to a login page for authentication.

It authenticates the user after validating the credentials entered by the user against the local database or the external server.

The controller hosts the virtual interface used for guest connectivity.

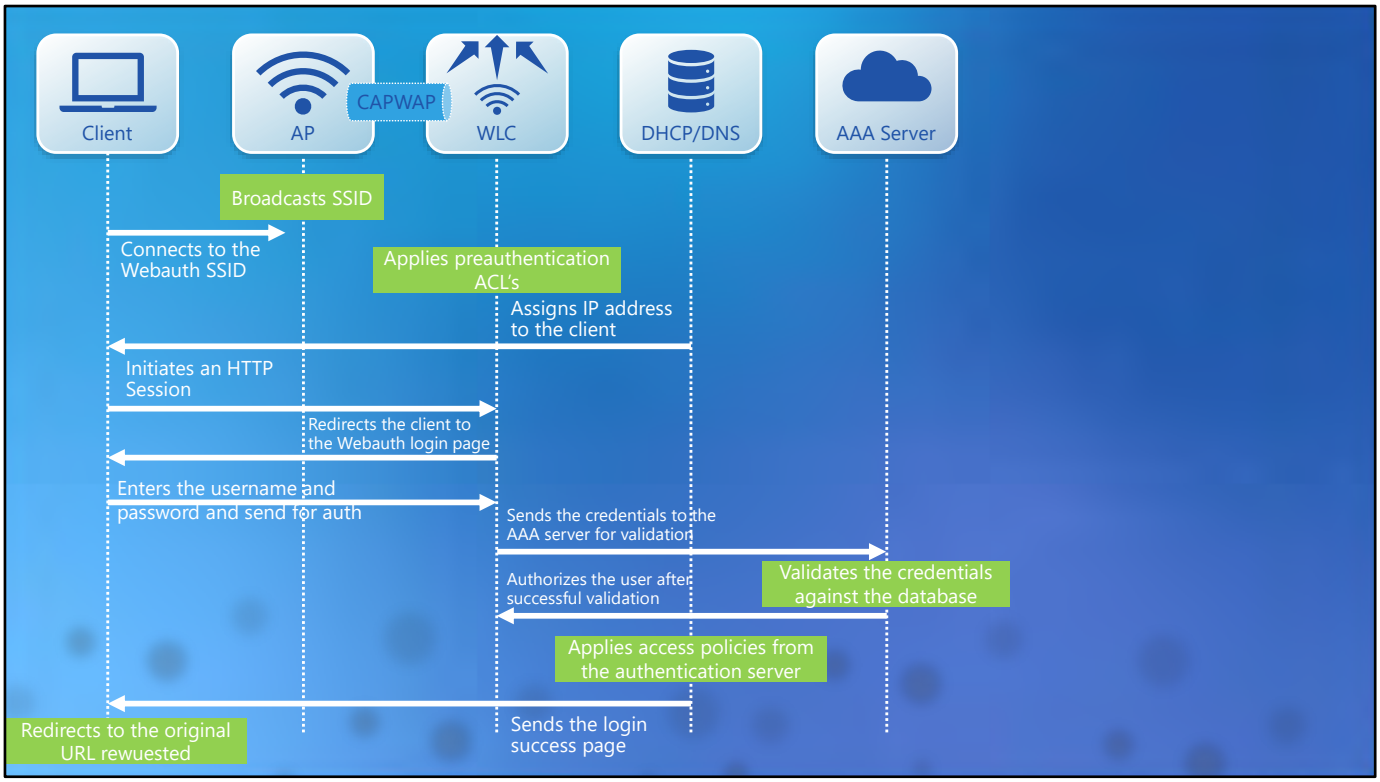
Authentication server:

Authenticates the client.

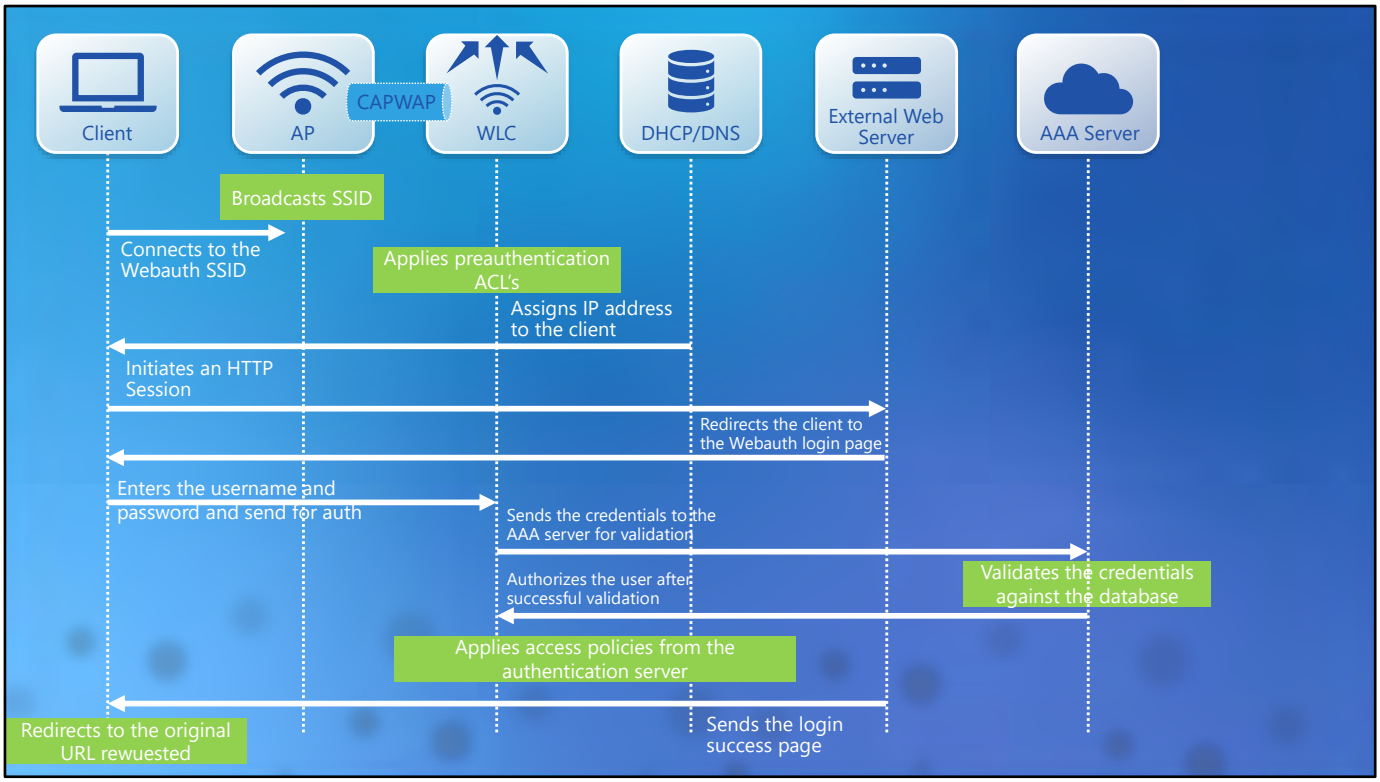
Validates the identity of the client and notifies the controller that the client is authorized to access the network and its services

©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.



©2023 by StormWind LLC. All rights reserved.

No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

Web Auth Features

- Secure HTTP Access
- WLC Certificate Validation
- Custom Webauth login portals
  - Webauth Bundle is a GNU Tar file
    - HTML and GIF Files
- Custom web browser banners
  - CLI configuration
  - When not configured on username / password appear in the login screen
- Custom authentication proxy web pages
- Preauthentication ACLs and URL filters

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.

The Virtual IP address for Web Auth

- (IPv4 or IPv6) Used only in communications between the controller and wireless clients.
  - redirect address for the web authentication login page.
  - Configure a non-routable IP address for the virtual interface
    - not overlapping with the network infrastructure addresses.
  - Use one of the options proposed in RFC 5737, for example, 192.0.2.0/24, 198.51.100.0/24, and 203.0.113.0/24 networks

©2023 by StormWind LLC. All rights reserved.
No part of this book may be reproduced in any written, electronic, recording, or photocopying without written permission of StormWind LLC.