

Glossary of Terms and Acronyms

Virtual Multimedia Resource Function

TERMINOLOGY

Copyright

© Ericsson AB 2016, 2017. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



Contents

| | | |
|----------|---------------------|-----------|
| 1 | Introduction | 1 |
| 2 | Terms | 2 |
| 2.1 | A-E | 2 |
| 2.2 | F-K | 8 |
| 2.3 | L-P | 9 |
| 2.4 | Q-T | 15 |
| 2.5 | U-Z | 19 |
| | Glossary | 22 |





1 Introduction

This document defines the terms and acronyms used in this library.

The defined terms, definitions, acronyms, and abbreviations are sorted in alphabetical order. Some of them can have more than one definition.

2 Terms

In the following sections, terms and definitions used in Virtual Multimedia Resource Function (vMRF) CPI are defined.

2.1 A-E

| | |
|------------------------|--|
| 1+n redundancy | A redundancy scheme used in the VNF where SC functions are active in only one VM at a time, and all other VMs serve as standby. |
| 3GPP | 3rd Generation Partnership Project. 3GPP® is a body that produces standards and specifications for third-generation systems. |
| Access network | A network from which the individual users connect to the core network through the P-CSCF. Private overlapping address spaces can be used in access networks. |
| Access transfer | Transfer at the IMS-level of one or more media paths of an ongoing IMS session on one UE between access and CS networks. |
| ACL | Access Control List. A list of permissions attached to an object. An ACL specifies which users, entities, or system processes are granted access to objects, and what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. |
| Action | An executable operation triggered by setting attributes on an MO. Each action is defined in the related MOC description. |
| AF | Application Function. An element of the service layer architecture offering applications that require information about the characteristics of the IP-connectivity session used to access such applications. |



| | |
|--------------------|---|
| Alarm | <p>Issued by the system to indicate an unexpected behavior of malfunction requiring corrective action by the user. An alarm at least has the states “raised” (initial detection of the fault) and “cleared” (when the fault no longer exists). An alarm can also change state regarding perceived severity. Alarms are also called “stateful” alarms to emphasize that they have a state. An active alarm is an alarm that has been issued but not cleared.</p> <p>All alarm state changes, including cleared state, are recorded in the Alarm Log. Each alarm has an alarm Operating Instructions document. It describes the possible fault reasons, fault locations, and the potential service impact. It also describes the procedures required to eliminate the problem and eventually clear the alarm.</p> |
| APN | <p>Access Point Name. The APN is the name of a gateway between a GPRS, 3G, or 4G mobile network and another computer network, frequently the public Internet.</p> <p>A mobile device making a data connection must be configured with an APN to present to the carrier. The carrier examines this identifier to determine what type of network connection to create, for example: what IP addresses to assign to the wireless device, what security methods to use, and how, or if, it to connect to a private customer network.</p> |
| Application | <p>A service enabler deployed by service providers, manufacturers, or users. Individual applications are often enablers for a wide range of services.</p> |
| ARP | <p>Address Resolution Protocol. A telecommunications protocol used for resolution of network layer addresses into link layer addresses.</p> |
| AS | <p>Application Server. A SIP-based server that provides value added IM services and resides either in the home network of the user or in a third-party location.</p> |
| ATCF | <p>Access Transfer Control Function. The ATCF is a logical entity and coordinates the access transfer of a session between access and CS networks.</p> |
| Attribute | <p>Represents the configuration. The read-only attributes in the MOs describe configuration state and operational values. The writable attributes control the operation and configuration for the particular network resource. Each attribute is defined in the related MOC description.</p> |



| | |
|----------------------------|---|
| Authentication | The process of verifying the identity of an entity. |
| Authorization | The granting of permission based on authenticated identification. |
| BFD | Bidirectional Forwarding Detection. A network protocol used to detect faults between two forwarding engines connected by a link. |
| C-RACF | Core Resource and Admission Control Function. Acts as the mediator between SCF and transport functions for QoS-related transport. C-RACF resides in the core network and makes decisions according to defined policies based on resource status in the transport layer and also based on use information, SLA, network policy rules, and service priorities. |
| CAC | Call Admission Control. A validation process in communication systems that confirms that there are sufficient resources for a proposed connection before the connection is accepted and established. |
| Cardinality | Cardinality in the MOM means the number of elements of MOs in a parent-child relationships, and in associations between MOs. |
| Cloud Administrator | The role of the cloud service provider who provides the cloud service to the end user. |
| Codec latching | During transcoding, if a subsequent SDP offer is received from either side after a previous SDP offer/answer exchange and the new SDP offer contains a single codec that is the same as currently negotiated for the side on which the new offer was received, then the same codec parameters that resulted from the previous SDP offer/answer negotiation are used when forwarding the subsequent SDP offer. |
| Codec lockdown | During transcoding, the locking down to a single codec when an answer contains multiple codecs from the offer. |
| Compute host | A compute host (or simply host) is the whole server entity providing computing resources, composed of the underlying hardware platform: processor, memory, I/O devices, and disk. |
| Compute node | See compute host. |



| | |
|----------------------|--|
| Control plane | The IP traffic between users or IMS core network nodes to control, for example, sessions, dialogs, and registration states. Realized by SIP. Compare with media plane. |
| Core network | Central part of a multimedia network including, for example, databases, SIP servers, media servers, and media gateways. Compare with IMS Core Network. |
| Counter | An entity that accumulates the measured values of a certain monitored item as the time passes. The counter value is incremented, never decremented, until it is restarted. |
| CPI | Customer Product Information. Documentation for an ME, delivered in the Active Library Explorer. |
| CS network | The IP network between the MSC and the P-CSCF (ATCF), which is used in the transfer of a session between the LTE network and CS network. |
| CSCF | Call Session Control Function. Several roles of SIP servers or proxies that are collectively called Call Session Control Function. A CSCF is used to process SIP signalling packets in the IMS. See P-CSCF, I-CSCF, and S-CSCF for details regarding the different CSCF types within IMS. |
| CSR | Customer Service Request. Used during the trouble reporting process to describe the problems identified. |
| Data model | A mapping of the contents of an information model into a form that is specific to a particular type of data store or repository. A data model is basically the rendering of an information model according to a specific set of mechanisms for representing, organizing, storing, and handling data. In contrast to an information model, a data model includes implementation and protocol-specific details. That is, rules that explain how to map MOs onto lower-level protocol constructs. |
| DDoS | Distributed Denial of Service. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted server. When a server is overloaded with connections, new connections can no longer be accepted. |



Defense in depth

A security approach where the security mechanisms are implemented in layers from the outermost part of the network to the inner part of the network. An example is from the user host and access network through the perimeter firewalls and routers to the core of the core network. Each layer must be protected from the attacks.

Derived data type

Data type enhanced with extra restrictions and properties. Derived string data types contain, for example, length and content constraints. Derived integer data types contain extra range constraints. Each derived data type is defined in the related MOC description.

DHCP

Dynamic Host Configuration Protocol. DHCP is a protocol for plug-and-play configuration of IP hosts. IP hosts query a DHCP server using the DHCP.

Dialog

A dialog represents a peer-to-peer SIP relationship between two user agents. A dialog is identified by a call identifier, local tag, and a remote tag. An early dialog exists until a final response has been received at which point a stable session exists.

DN

Distinguished Name. The name of an object tree that is shared between the system and the Management System. The DN is in 3GPP format (from root to leaf). The DN is used to identify an MO uniquely in the system. It gives the path of the MO in the tree of objects. The system uses 3GPP formatted DNs where each relative DN part consists of the MOC name equal the MO identity. If the key attribute name is not equal to the MOC name plus ID, then the key attribute name is also appended to the MOC name separated by a dot.

DNS

Domain Name System. A logical node that maintains information associated with hostnames within a naming domain or subdomain. A DNS offers the mapping of names to addresses and the mapping of addresses to names.

DNS SRV record

A DNS Resource Record for specifying the domain name of a server.

DoS

Denial of Service. A DoS attack occurs when a single system floods the bandwidth or resources of a targeted server. When a server is overloaded with connections, new connections can no longer be accepted.



| | |
|-----------------------------------|---|
| DSCP | Differentiated Services Code Point. DSCP is a value in an IP packet header. It is used to specify a particular QoS behavior for the packet. DSCP is defined in RFC 2472 . |
| E-CSCF | Emergency Call Session Control Function. A CSCF used for handling emergency calls. |
| Early media | Early media refers to media (for example, audio and video) that is exchanged before a particular session is accepted by the called user. Early media is defined in RFC 3959 . |
| ECIM | Ericsson Common Information Model. Controls the MOM structure. The ECIM is based on the CIM standard. |
| ECLI | Ericsson Command-Line Interface. A terminal-based command-line interface that is used to monitor and manage the ME. The ECLI is based on industry de facto standard patterns. |
| Emergency bearer | A bearer that is used for emergency services. For P-CSCF, an emergency bearer is a configurable IP subnet. |
| Emergency registration | A registration initiated by UE for emergency calls, that has an “sos” URI parameter present in the Contact header. |
| End-to-end security | Media protection extending between two UEs without being terminated by any intermediary. |
| End User | The role of the vMRF operator, who is assumed to be a cloud service consumer. Also referred to as tenant. |
| Enumeration | Integer-name pairs defining a fixed set of named values for an attribute, return value, or action parameter. Each enumeration is defined in the MOM. |
| Ericsson NETCONF interface | A machine to machine interface for configuration management of the ME, using the NETCONF protocol over the Secure Shell. |
| Event | Occurrence of significance to users, the MEs under surveillance and network management specifications. Events do not have states. |



2.2

F-K

Firewall

A network security system that controls the incoming and outgoing network traffic. Traffic is filtered by analyzing the data packets and determining whether they are to be allowed through, based on an applied rule set.

Flavor

Virtual resource templates in OpenStack that define RAM size, number of vCPU cores, and so on, for running VNFs.

Foreign network

The network of another carrier or a separate portion within the network of the carrier. The foreign network can either be a trusted SIP network, or an untrusted SIP network.

FTP

File Transfer Protocol. A protocol for reliable transfer of text and binary files between computers. Specified in [RFC 959](#).

Gauge

An entity that shows the current measured value of a certain monitored item. A gauge value can be incremented and decremented.

GP

Granularity Period. The time between the initiation of two successive gatherings of measurement data.

HA

High Availability. A system or component that is continuously operational for a desirably long length of time. Availability is measured relative to 100% operational status.

Heartbeats

Used by a Management System to monitor the interface over which the alarms or alerts are to be sent. Heartbeats are needed because a management system cannot assume that a “silent” ME behaves properly. The Heartbeat event is reported as an SNMP notification at regular intervals.

HOT

Heat Orchestration Template. In OpenStack, HOT is a file that defines the infrastructure for a cloud application in a textual format.

HPLMN

Home Public Land Mobile Network. The home telecommunications network providing mobile cellular services. Defined in [3GPP TR 21.905](#).



| | |
|--------------------------|---|
| HSS | Home Subscriber Server. An IMS database that contains subscription-related information (subscriber profiles), user authentication and authorization, and information about the subscriber location and IP information. |
| Hypervisor | A hypervisor, or VMM, is a piece of software, firmware, or hardware that creates and runs VMs. |
| I-CSCF | Interrogating Call Session Control Function. Acts as an inbound SIP proxy server in the IMS. During IMS registrations, the I-CSCF queries the HSS to select the appropriate S-CSCF that can serve the UE. During IMS sessions, the I-CSCF acts as the entry point to terminating session requests. The I-CSCF routes the incoming session requests to the S-CSCF of the called party. |
| IMS | IP Multimedia Subsystem. An architectural framework for delivering IP Multimedia services as defined by 3GPP 23:288 . |
| IMS core network | The central part of the IMS network architecture. The IMS core can include databases (HSS), SIP call/session servers (CSCF), ASs, media resource functions (MRFC and MRFP), and PSTN gateways. An IMS core network is typically separated from access networks (where users reside) and other operator IP Multimedia networks by an SBG. |
| Information model | An abstraction and representation of the entities (or MOs) in a managed environment, their properties, attributes, and operations, as well as the way that they relate to each other. It is independent of any specific repository, software use, protocol, or platform. |
| IP host | An endpoint that terminates the IP layer (L3) in an IP network (in contrast to a router, which is a transit node). |
| IP interface | An interface terminating the IP Layer 3 (L3). The IP interface has an associated IP address. |
| 2.3 L-P | |
| L1 | Layer 1. Physical layer is the first (lowest) layer of the OSI model. The implementation of this layer is often termed PHY. The physical layer consists of the basic networking hardware transmission technologies of a network. |



| | |
|------------------------|---|
| L2 | Layer 2. The data link layer is the OSI protocol layer. L2 transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The data link layer provides functions and procedures to transfer data between network entities. The data link layer can provide the means to detect and possibly correct errors that can occur in the physical layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the PPP, HDLC, and ADCCP for point-to-point (dual-node) connections. |
| L3 | Layer 3. The network layer is responsible for packet forwarding including routing through intermediate routers. The data link layer is responsible for Media Access Control, flow control, and error checking. The network layer provides functions and procedures for transferring variable length data sequences from a source to a destination host through one or more networks. The network layer maintains the quality of service functions. |
| L4 | Layer 4. The transport layer provides convenient services such as connection-oriented data stream support, reliability, flow control, and multiplexing. |
| LAN | Local Area Network. A computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media. |
| Load balancing | The distribution of processing and communications activity evenly across a network so that no single node is overwhelmed. |
| Logical network | A way to group a set of subnets and subnet segments together. Normally the subnets and subnet segments grouped have a common use. Each of these logical networks contains several subnets used in the associated network. |
| LOTG | Linux® Open Telecom Cluster. A custom Ericsson operating system distribution based on GNU/Linux. The LOTG provides a Linux cluster with high-availability characteristics. |
| LTE | Long Term Evolution. A standard for wireless communication of high-speed data for mobile phones and data terminals. |



| | |
|----------------------------------|--|
| MAC | Media Access Control. MAC is a data communication protocol that is a sublayer of the OSI data link layer (L2). The MAC sublayer provides addressing and channel access control mechanisms. The MAC mechanisms allow several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, for example, Ethernet. |
| Malicious traffic | Traffic that can harm the network, the network core nodes, or user entities. Examples of traffic considered malicious by the SBG are packets using invalid source or destination addresses or ports and packets using IP options. |
| Managed function | The function of a managed element. |
| Managed Object Management | A folder in the Active Library Explorer containing the MOM. |
| ME | Managed Element. Telecommunications equipment that performs managed element functions, that is, provides support and services to the user. A managed element communicates with a manager (directly or indirectly) over one or more interfaces being monitored or controlled. |
| Measurement job | The execution of measurement data collection, aggregation, and reporting in PM XML files is performed by measurement jobs. |
| Media | IP traffic containing audio, video, fax, and so on. Some packets not containing actual payload (for example, RTCP packets or TCP segments for connection establishment) are considered media as they are prerequisites for, or closely coupled to, the payload. |
| Media anchoring | Forcing media to take a certain path by altering source or destination address and port in SDP. |
| Media plane | Media traffic between network entities. Compare with control plane. |
| MGW | Media Gateway. A translation device or service that converts digital media streams between disparate telecommunications networks. |



| | |
|-------------|--|
| MIB | Management Information Base. A set of managed objects in a management domain, together with their attributes, constitutes a management domain MIB. MIB is also used in SNMP for trap and counter-definition. |
| MIM | Management Information Model. Describes MOCs, their associations, attributes, and operations. |
| MO | <p>Managed Object. A resource within the telecommunications environment that can be managed using OAMP application protocols.</p> <p>The MO is a software object that encapsulates the manageable characteristics and behavior of a particular hardware or software resource. An MO is an instance of a MOC. An MO normally has attributes that provide information used to characterize the MOs that belong to the MOC. An MO can also have actions that allow the user to perform operations on the underlying implementation.</p> |
| MOC | Managed Object Class. A description of all the common characteristics for several MOs, such as attributes, operations, notifications, and behavior. |
| MOM | Managed Object Model. A structured collection of configuration information that defines the O&M capability on an ME. The MOM is defined as a set of MOCs. The MOCs contain attributes representing the configuration that can be performed by the user, and actions representing the operations that can be started by the user. The MOM is a static blueprint for the creation of the actual object model. |
| MTAS | Multimedia Telephony Application Server. Application server that supports IMS-based multimedia services. |
| MTU | Maximum Transmission Unit. The size (in bytes) of the largest protocol data unit that the communication layer can pass onwards. |
| NAPT | Network Address Port Translation. A method by which many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports. NAPT is defined in RFC3022 . |
| NAT | Network Address Translation. A network protocol used in IPv4 networks that allows multiple devices to connect to a public network using the same public IPv4 address. NAT modifies the IP address information in IPv4 headers when passing through a routing device. |



| | |
|-----------------|---|
| NBI | Northbound Interface. The interface to a management system and a CLI client. The protocols used are ECLI, NETCONF, SFTP, and SNMP. |
| ND | Neighbor Discovery. A method for mapping an IPv6 address to the corresponding MAC address. |
| NE | Network Element. An NE provides telecommunications and support functions, and is managed by a telecommunications operations support system. |
| NETCONF | Network Configuration. NETCONF is a network management protocol developed in the IETF. It uses an XML-based data encoding for the configuration data and the protocol messages. The NETCONF protocol operations are realized on top of a simple RPC layer. |
| Next hop | A node through which IP traffic is routed. A next hop is needed when an IP source address and an IP destination address are not in the same subnet. A next hop is used when IP routing is needed to send an IP packet from the source to the destination. Separate next hops are normally configured for media transport and for SIP signaling. A next hop address is normally associated with one route but can also be associated with more than one route. |
| NF | Network Function. An NF is a functional block within a network infrastructure that has well-defined external interfaces and well-defined functional behavior. In practical terms, an NF is often a network node or physical appliance. |
| NFV | Network Functions Virtualization. NFV is the principle of separating network functions from the hardware they run on by using virtual hardware abstraction. |
| NFVI | Network Function Virtualization Infrastructure. NFVI is the totality of all hardware and software components that build up the environment in which VNFs are deployed. |
| NIC | Network Interface Controller. A NIC is a device in a compute node that provides a physical interface with the infrastructure network. |
| NMC | Network Management Center. One or more locations from which network monitoring and control, or network management, is exercised over a telecommunication network. |



| | |
|-------------------------|--|
| NNI | Network-to-Network Interface. An interface that specifies signaling and management functions between two networks. |
| Notification | A general term for a message that carries an alarm or alert instance. |
| NTP | Network Time Protocol. NTP is a protocol built on top of TCP/IP that is used to synchronize computer clock times in a network of computers. Defined IETF RFC 1119 . |
| O&M | Operation & Maintenance. O&M provides the processes, activities, tools, standards, and so on, involved with operating, and maintaining any system. |
| OAM | Operations, Administration, and Maintenance. OAM provides the processes, activities, tools, standards, and so on, involved with operating, administering, managing and maintaining any system. |
| OSPF | Open Shortest Path First. A link-state routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system. It is defined as OSPF Version 2 in RFC 2328 for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 . |
| OSS | Operations Support System. Systems dealing with the telecom network to support processes such as maintaining network inventory, provisioning services, configuring network components, and managing faults. |
| P-CSCF | Proxy Call Session Control Function. The first contact point for the UE within the IMS core network. The P-CSCF performs several tasks, for example: forwards the SIP register request received from the UE to the correct destination, forwards SIP messages received from the UE to the SIP server (for example, S-CSCF), forwards SIP requests or responses to the UE, detects and handles emergency session establishment, and generates CDRs. |
| Payload function | The payload function of a vMRF VM processes user plane traffic and H.248 signaling traffic. |
| PCP | Priority Code Point. Priority marking in an Ethernet frame. |



| | |
|------------------------------|---|
| Pinhole | A set of criteria defining a media stream that is let through the dynamic pinhole firewall. The criteria include local IP address and port, direction of media, and transport protocol. The criteria can also include remote IP address and port for media source filtering and bandwidth for policing. |
| PLMN | Public Land Mobile Network. A telecommunications network providing mobile cellular services. Defined in 3GPP TR 21.905 . |
| PNF | Physical Network Function. A PNF is an implementation of an NF using a tightly coupled software and hardware system. |
| Priority call | A call that is given priority over other calls. A priority call can be a call from a priority subscribed user or a call received that indicates priority using the RPH in SIP. |
| Proactive transcoding | A service where proactive measures are taken, when processing an SDP offer, to allow transcoding to be invoked at the reception of the SDP answer. Transcoding is only activated in the case the B-party does not support any codec that the A-party listed in the SDP offer. Based on local policy, more codecs can be inserted in the forwarded offer and transcoding is then invoked if one of the added codecs is selected by the answerer. |
| Q-T | |
| Realm | A realm represents a network the vMRF is connected to. It can be an access network, a core network, or a foreign network. For each realm defined in the vMRF there must be a corresponding realm defined in the MTAS configuration. |
| Role | Role is equivalent to the user occupation within an organization, for example, System Administrator. A user can have one or more roles. |
| Route | Routes represent the paths IP packets travel on their way to a specific destination network (IP subnet). A route is defined by the destination network and the next hops to use when forwarding packets to this network. |
| RTCP | RTP Control Protocol. A protocol that monitors the quality of service and to conveys information about the participants in ongoing sessions. |

2.4



| | |
|------------------------|--|
| RTP | Real-Time Transport Protocol. A standardized transport protocol for delivering audio and video over IP networks as defined by RFC3550 . |
| Rule | When applied to user authorization, rules specify the permissions to a set of resources within a ME. The authorization rules depend on predefined roles. Roles and authorization rules are defined to build a Role-Based Access Control (RBAC) model for controlling access to Managed Element resources. |
| Rx | An interface used by a P-CSCF for policy control (resource and QoS authorization) in an access network. |
| S-CSCF | Serving Call Session Control Function. Acts as a registrar server, and in some cases as a redirect server. It is the central point for IMS service control over the ISC reference point. Moreover, the S-CSCF facilitates the routing path for mobile originated or mobile terminated session requests. The S-CSCF provides initial filter criteria processing logic that enables IMS service control. It also interacts with the Media Resource Function over the Mr interface for playing tones and announcements. |
| SA | Security Association. The establishment of shared security attributes between two network entities to support secure communication. An SA can include attributes such as: cryptographic algorithm and mode; traffic encryption key; and parameters for the network data to be passed over the connection. |
| SC function | System Controller function. The SC function is responsible for processing O&M traffic and for the VNF internal clustering function that is needed for scaling out and scaling in. The SC function is present in all VMs, but it is active in only one VM at a time, and all other VMs in the VNF serve as standby SC VMs. |
| Scaling | The ability to dynamically extend or reduce resources granted to the VNF. This includes scaling up and down, and scaling out and in. |
| Scaling out/in | The ability to scale by adding or deleting resource instances (for example, VMs). |
| Scaling up/down | The ability to scale by changing allocated resource, for example, increase or decrease memory, vCPU capacity, or storage size. |



| | |
|--------------|---|
| SCTP | Stream Control Transmission Protocol. A transport layer protocol for transmitting multiple streams of data at the same time between two endpoint. It provides a combination of service features from UDP and TCP: it is message-oriented like UDP and ensures reliable, in-sequence transport of messages with congestion control like TCP. SCTP is defined in RFC 4960 . |
| SDES | Security Description for SDP. A way to negotiate cryptographic parameters for media streams between SDP and SRTP. It has been proposed for standardization to the IETF in July 2006 (refer to RFC 4568). |
| SDP | Session Description Protocol. A format for describing streaming media initialization parameters as defined by RFC 4566 . |
| SF | System Functions. Common system functions and resources for the management entity such as Fault Management (FM), Performance Management (PM), and Security Management (SecM). System Functions is one of the first-level branches in the MOM. |
| SFTP | Secure File Transfer Protocol. A network protocol for secure file transfer over secure shell. |
| SIP | Session Initiation Protocol. A signaling communications protocol for controlling multimedia communication sessions such as voice and video calls over IP networks. |
| SRTCP | Secure Real-Time Control Protocol. A profile of RCTP to provide encryption, message authentication and integrity, and replay protection to the RCTP data. |
| SRTP | Secure Real-Time Transport Protocol. A profile of RTP to provide encryption, message authentication and integrity, and replay protection to the RTP data in both unicast and multicast applications. |
| SSH | Secure Shell. A cryptographic network protocol for secure data communication, remote command line logon, remote command execution, and other secure network services. The secure shell exists between two networked computers that connect, using a secure channel over an insecure network. The secure shell is implemented by a server and a client (running SSH server and SSH client programs, respectively). |
| SSL | Secure Socket Layer. A commonly used protocol for managing the security of a message transmission on the internet. |



| | |
|-----------------------------|---|
| Struct | Struct is a compound data type in the MOM that groups element members of different types. |
| Subnet | A subnet is defined as a contiguous IP address range. A subnet is an IP address or IP prefix, which is the first address in the subnet, and an address mask that specifies the size of the subnet. For example, the 10.10.10.0/24 subnet has the IP prefix 10.10.10.0 and the mask is 24 bits, thus allowing 256 addresses in the subnet. |
| TCP | Transmission Control Protocol. Part of the TCP/IP protocol stack. It provides connection-oriented communication to move data across the network. The protocol supports byte-oriented transfer of data between the applications, and is a reliable end-to-end transport protocol between the TCP processes. |
| TLS | Transport Layer Security. A cryptographic protocol that is designed to provide communication security. In vMRF, it is used to secure the transport layer for the LDAP protocol. |
| Topology hiding | Topology hiding is a feature that hides the network address topology of one network from another. Deletion, modification, and insertion of certain information is done to achieve topology hiding. |
| Transaction | For administration, configuration changes are applied through atomic transactions. |
| Transcoding | Conversion from one encoding format to another. vMRF supports basic transcoding allowing for calls between two endpoints that do not support a common codec. |
| Transport Management | Transport-related functions and resources, for example, load sharing between all configured and available blades in the cluster, and distribution of incoming traffic to the system. Transport is one of the first-level branches in the MOM. |
| Trap | An unacknowledged SNMP message that carries a notification or heartbeat. |
| Trombone | Media path that is routed out from a node and back to the same point in the network (hairpinning). |



2.5

U-Z

UDP

User Datagram Protocol. Supports the transmission of messages to other hosts on an IP network without prior communications to set up special transmission channels or data paths. UDP messages are referred to as datagrams. The protocol is defined in [RFC 768](#).

UE

User Equipment. A device allowing a user to access network services. For example a PC with proper software or a SIP-telephone. Defined in [3GPP TR 21.905](#).

UNI

User-to-Network Interface. A demarcation point between the responsibility of the service provider and the responsibility of the subscriber.

Upgrade

A product or product version that is created to provide an increased level of functionality or performance to a user. Upgrade is also the operation to replace a previous product or product version with a new product or product version that provides an increased level of functionality.

UTC

Coordinated Universal Time. UTC is the time-scale maintained by the BIPM, with assistance from the IERS. UTC forms the basis of a coordinated dissemination of standard frequencies and time signals. It corresponds exactly in rate with International Atomic Time (TAI) but differs from it by an integer number of seconds.

VC

Virtualization Container. A VC is a partition of a compute node that provides an isolated virtualized computation environment. Examples of VCs include VM and OS container.

VM

Virtual Machine. A VM is a virtualized computation environment. A VM has all the virtualized counterparts (processor, memory, storage, interfaces, ports) of a physical computer and is generated by a hypervisor, by partitioning the underlying physical resources and allocating them to VMs. VMs are capable of hosting a VNFC.

vMRF

The Virtual Multimedia Resource Function is a VNF running in a cloud environment. The vMRF provides media-related functions, such as, stream mixing and playing of tones and announcements. The vMRF is controlled by the MTAS through H.248.



| | |
|--------------|--|
| VNF | Virtual Network Function. Network function virtualization is a concept that uses virtualization of entire classes of network node functions into building blocks that may connect, or chain together, to create communication services. vMRF can contain one or more VNFs. A single VNF contains multiple VMs. |
| VNFC | Virtualized Network Function Component. A VNFC is an internal component of a VNF providing a defined subset of the functionality of that VNF. |
| VNFCI | Virtualized Network Function Component Instance. A VNFCI is an instance of a VNFC deployed in a specific VC instance. It has a life cycle dependency with its parent VNF instance. |
| VNFD | Virtual Network Function Descriptor. Links to scripts for initiation and termination, description of internal and external connectivity, and dependencies between VNFCs. |
| VNFI | Virtualized Network Function Instance. A VNFI is a runtime instantiation of the VNF software, resulting from completing the instantiation of its components and of the connectivity between them. This is achieved using the VNF deployment and operational information captured in the VNFD, as well as additional runtime instance-specific information and constraints. |
| vNIC | Virtualized Network Interface Controller. A vNIC is created for a VM by a hypervisor. |
| VPLMN | Visited Public Land Mobile Network. VPLMN is the PLMN on which the mobile subscriber has roamed when leaving their HPLMN. |
| VR | Virtual Router. A VR is a VNF, a software-based routing framework that allows packet routing and forwarding. To be able to handle multiple IP domains in the same router, the router can be divided into different VRs. Each VR is handling a separate IP domain. To each VR, routes and IP interfaces are connected. |
| VRRP | Virtual Router Redundancy Protocol. VRRP is a protocol that provides for automatic assignment of available IP routers to participating hosts. VRRP increases the availability and reliability of routing paths using automatic default gateway selections on an IP subnetwork. In vMRF, L3 redundancy is provided by VRRP. |

**WCG**

Web Communication Gateway. A WCG converts between web client signalling (for example, HTTP REST) and SIP (for example, registration, session setup, and session modification signaling).

The WCG abstracts the complexity of the IMS signalling protocol from the client developer by providing an SDK API for client application development.

WCG sends converted client signaling over the Gm reference point to the SBG (P-CSCF).

Web client

A browser-based client uses HTTP REST or other equivalent signalling to interact with the WCG for registration and session control. The web client can use any media protocol supported by the IMS and normally use RTP for audio and video call.

WCG sends converted client signaling over the Gm reference point to SBG (P-CSCF).

Wildcard

A character that substitutes for another character or character range in a regular expression.



Glossary

3DES

Triple Data Encryption Standard

3GPP

3rd Generation Partnership Project

A-RACF

Access Resource and Admission Control Function

AA

Authentication Authorization

AAA

AA-Answer

AAAA

Authentication, Authorization, Accounting, and Auditing

AAR

AA-Request

ABNF

Augmented Backus-Naur Form

ACA

Accounting-Answer

ACL

Access Control List

ACR

Accounting-Request

ADCCP

Advanced Data Communication Control Procedures

AES

Advanced Encryption Standard

AF

Application Function

AKA

Authentication and Key Agreement

ALB

Abstract Load Balancer

AMF

Availability Management Framework

AMR

Adaptive Multi-Rate

AMR-NB

Adaptive Multi-Rate Narrowband

AMR-WB

Adaptive Multi-Rate Wideband

ANSI

American National Standards Institute

API

Application Programming Interface

APN

Access Point Name

ARP

Address Resolution Protocol

AS

Application Server

ASA

Abort-Session-Answer

ASCII

American Standard Code for Information Interchange

ASI

Additional System Information

ASN.1

Abstract Syntax Notation One

ASR

Abort-Session-Request

**ATCF**

Access Transfer Control Function

ATGW

Access Transfer Gateway

ATM

Asynchronous Transfer Mode

ATU-STI

Access Transfer Update - Session Transfer Identifier

AVC

Attribute Value Change

AVP

Attribute-Value Pair

Audio-Visual Profile

AVPF

Extended Audio Video Profile for RTCP Feedback

BFD

Bidirectional Forwarding Detection

BIPM

Bureau International DES Poids et Mesures

BRF

Backup and Restore Framework

BRM

Backup and Restore Management

BSP

Blade Server Platform

BT

Business Trunking

C-RACF

Core Resource and Admission Control Function

CA

Certificate Authority

CAC

Call Admission Control

CBA

Component Based Architecture

CC

Cumulative Counter

CEA

Capabilities-Exchange-Answer

CER

Capabilities-Exchange-Request

CertM

Certificate Management

CIM

Common Information Model

CLB

Converged SIP/HTTP Load Balancer

CLI

Command-Line Interface

CLM

Cluster Management

CM

Configuration Management

CMP

Certificate Management Protocol

CMPv2

Certificate Management Protocol version 2

CMX

Component Main Switch

CMXB

Component Main Switch Board

CN

Common Name

CNB

Collapsed Northbound

codec

Coder-Decoder

COTS

Commercial-Off-The-Shelf



CPE
Customer-Premises Equipment

CPI
Customer Product Information

CPU
Central Processing Unit

CRC
Cyclic Redundancy Check

CRM
Customer Relationship Management

CRV
Call Reference Value

CS
Circuit Switched

CS-ACELP
Conjugate Structure Algebraic Code Excited
Linear Prediction

CSCF
Call Session Control Function

CSR
Customer Service Request

Certificate Signing Request

CUA
Capabilities Update Answer

CUR
Capabilities Update Request

DAD
Optimistic Duplicate Address Detection

DBN
Database Network

DBS
Database Service

DCN
Data Communication Network

DDoS
Distributed Denial of Service

DER
Discrete Event Registration

DES
Data Encryption Standard

DF
Don't Fragment

DHCP
Dynamic Host Configuration Protocol

DiffServ
Differentiated Services

DMX
Distributed Main Switch

DMXC
Distributed Main Switch Controller

DMZ
Demilitarized Zone

DN
Distinguished Name

DNS
Domain Name System

DoS
Denial of Service

DPA
Disconnect Peer Answer

DPR
Disconnect Peer Request

DR
Disaster Recovery

DRA
Diameter Routing Agent

DRBD
Distributed Replicated Block Device

DSA
Digital Signature Algorithm

DSCP
Differentiated Services Code Point

**DST**

Daylight Saving Time

DTLS

Datagram Transport Layer Security

DTMF

Dual-Tone Multifrequency

DTMF-S

DTMF Sender

DTMF-R

DTMF Receiver

DTX

Discontinuous Transmission

DU

Destination Unreachable

DWA

Device Watchdog Answer

DWR

Device Watchdog Request

E-CSCF

Emergency Call Session Control Function

e2e

End-to-end

EBNF

Extended Backus-Naur Form

EBS

Ericsson Blade System

EC

Emergency Call

ECDSA

Elliptic Curve Digital Signature Algorithm

ECGI

E-UTRAN Cell Global Identifier

ECIM

Ericsson Common Information Model

ECLI

Ericsson Command-Line Interface

ECM

Ericsson Cloud Manager

ECMP

Equal-Cost Multipath routing

EJB

Enterprise JavaBeans

ECS

Ericsson Cloud System

EFR

Enhanced Full Rate

EPC

Evolved Packet Core

EPS

Evolved Packet System

ETSI

European Telecommunications Standards Institute

eVIP

Evolved Virtual Internet Protocol

EWMA

Exponentially Weighted Moving Average

FEE

Front-End Element

FIFO

First In First Out

FM

Fault Management

FNI

Foreign Network Identifier

FOSS

Free Open Source Software

FQDN

Fully Qualified Domain Name

FS

Function Specification

**FTP**

File Transfer Protocol

FW

Firewall

GCP

Gateway Control Protocol (H.248)

GE

Gigabit Ethernet Interface

GP

Granularity Period

GSM

Global System for Mobile Communications

GW

Gateway

GUI

Graphical User Interface

HA

High Availability

HDLC

High-Level Data Link Control

HCM

Health Check Management

HLR

Home Location Register

HOT

Heat Orchestration Template

HPLMN

Home PLMN

HSS

Home Subscriber Server

HTML

Hypertext Markup Language

HTTP

Hypertext Transfer Protocol

HTTPS

Hypertext Transfer Protocol Secure

HW

Hardware

I-CSCF

Interrogating Call Session Control Function

I/O

Input/Output

IANA

Internet Assigned Numbers Authority

IAP

Interception Access Point

ICE

Interactive Connectivity Establishment

ICID

IMS Charging Identifier

ICMP

Internet Control Message Protocol

ICSI

IMS Communication Service Identifier

ID

Identity

IEEE

Institute of Electrical and Electronics Engineers

IEPS

International Emergency Preference Scheme

IERS

International Earth Rotation Service

IETF

Internet Engineering Task Force

IKE

Internet Key Exchange

IMI

Integrated Management Interface

IMM

Information Model Management

**IMS**

IP Multimedia Subsystem

INAP

Intelligent Network Application Protocol

IOI

Inter-Operator Identifier

IOPS

Input/Output Operations Per Second

IP

Internet Protocol

IP-CAN

IP Connectivity Access Network

IP-PBX

IP Private Branch Exchange

IPsec

Internet Protocol Security

IPv4

IP version 4

IPv6

IP version 6

IPVS

Internet Protocol Virtual Server

IPX

Internet Packet Exchange

IRP

Integration Reference Point

ISDN

Integrated Services Digital Network

ISO

International Organization for Standardization

ISP

In-Service Performance

ISUP

Integrated Services Digital Network User Part

ITU

International Telecommunication Union
Telecommunications Standardization Sector

ITU-T

International Telecommunication Union –
Telecommunications

IVR

Interactive Voice Response

IWD

Interwork Description

IWF

Interworking Function

KPI

Key Performance Indicator

KQI

Key Quality Indicator

L1

Layer 1 (according to the OSI layered model)

L2

Layer 2 (according to the OSI layered model)

L3

Layer 3 (according to the OSI layered model)

L4

Layer 4 (according to the OSI layered model)

LAN

Local Area Network

LBE

Load Balancer Element

LBaaS

Load-Balancing-as-a-Service

LCT

Local Craft Terminal

LDAP

Lightweight Directory Access Protocol

LDAPS

LDAP over SSL



LDIF
LDAP Data Interchange Format

LDN
Local Distinguished Name

LEA
Law Enforcement Agency

LKF
License Key File

LM
License Management

LOTC
Linux Open Telecom Cluster

LTE
Long Term Evolution

MAC
Media Access Control

MAF
Middleware Agnostic Framework

MBS
Maximum Burst Size

MD5
Message-Digest algorithm 5

MDF
Model Delivery Function

ME
Managed Element

MG
Media Gateway

MGC
Media Gateway Controller

MGCF
Media Gateway Control Function

MGW
Media Gateway

MIA
Manual Intervention Allowed

MIB
Management Information Base

MIM
Management Information Model

MMAS
Multimedia Application Server

MO
Managed Object

MOC
Managed Object Class

MOM
Managed Object Model

MRF
Multimedia Resource Function

MS
Mobile Station

MSC
Mobile Switching Center

MSD
Master Slave Determination

MSISDN
Mobile Subscriber ISDN Number

MSS
Mobile Softswitch Solution

MTAS
Multimedia Telephony Application Server

MTP
Message Transfer Part

MTU
Maximum Transmission Unit

MW
Middleware

NAI
Network Access Identifier

NAPT
Network Address Port Translation

**NAT**

Network Address Translation

NB

Narrowband

NBI

Northbound Interface

ND

Neighbor Discovery

NE

Network Element

NeLS

Network License Server

NETCONF

Network Configuration

NF

Network Function

NFV

Network Function Virtualization

NFVI

Network Functions Virtualization Infrastructure

NIC

Network Interface Controller

NMC

Network Management Center

NMS

Network Management System

NNI

Network-to-Network Interface

NPLI

Network Provided Location Information

NTP

Network Time Protocol

O&M

Operation and Maintenance

OAM

Operations, Administration, and Maintenance

OAMP

Operations, Administration, Maintenance, and Provisioning

OID

Object Identifier

OLP

Overload Protection

OPI

Operating Instructions

OS

Operating System

OSI

Open Systems Interconnection

OSPF

Open Shortest Path First

OSS

Operations Support System

OVA

Open Virtualized Architecture

OVF

Open Virtualization Format

P-CSCF

Proxy Call Session Control Function

PAI

P-Asserted-Identity

PAM

Pluggable Authentication Module

PANI

P-Access-Network-Info

PBX

Private Branch Exchange

PC

Personal Computer

Probable Cause

PCFA

P-Charging Function Address

**PCM**

Pulse Code Modulation

PCMU

Pulse Code Modulation, μ -law

PCP

Priority Code Point

PCRE

Perl Compatible Regular Expressions

PCV

P-Charging-Vector

PDB

Parameter Database

PDF

Probability Density Function

Portable Document Format

PDN

Packet Data Networks

PDU

Protocol Data Unit

PI

Performance Indicator

PKCS

Public-Key Cryptography Standards

PKI

Public-Key Infrastructure

PL

Payload

PLC

Packet Loss Concealment

PLMN

Public Land Mobile Network

PM

Performance Management

PNF

Physical Network Function

PNI

Private Network Interface

PoC

Push to Talk over Cellular

POSIX

Portable Operating System Interface

PPI

P-Preferred-Identity

PPP

Point-to-Point Protocol

PS

Packet Switched

PSI

Public Service Identity

PSK

Preshared Key

PSTN

Public Switched Telephone Network

PXE

Preboot eXecution Environment

QoS

Quality of Service

RA

Registration Authority

RAA

Re-Auth-Answer

RACF

Resource and Admission Control Function

RACS

Resource and Admission Control Subsystem

RAM

Random-Access Memory

RAR

Re-Auth-Request

RBAC

Role-Based Access Control



RBS
Radio Base Station

RCA
Root Cause Analysis

RDN
Relative Distinguished Name

RFC
Request for Comments

ROP
Report Output Period

RPC
Remote Procedure Call

RPH
Resource-Priority Header

RPM
RedHat® Package Manager

RR
Resource Records

RRT
Realm Routing Table

RSA
Rivest, Shamir and Adleman

RSIP
Realm Specific Internet Protocol

RTCP
RTP Control Protocol

RTP
Real-Time Transport Protocol

RTT
Round-Trip Time

S-CSCF
Serving Call Session Control Function

SA
Security Association

Support Agent

SAF
Service Availability Forum

SAVP
Secure Audio Video Profile

SB-ADPCM
Sub-Band Adaptive Differential Pulse Code Modulation

SC
System Controller

SCC-AS
Service Centralization and Continuity Application Server

SCCP
Signalling Connection Control Part

SCEP
Simple Certificate Enrollment Protocol

SCF
Service Control Functions

SCTP
Stream Control Transmission Protocol

SCX
System Control Switch

SCXB
System Control Switch Board

SDES
Security Description for SDP

SDK
Software Development Kit

SDP
Session Description Protocol

Software Delivery Package

SE
Security Element

SecM
Security Management



SELinux

Security-Enhanced Linux

SF

System Functions

SFTP

Secure File Transfer Protocol

SHA

Secure Hash Algorithm

SI

Service Instance

Status Inspection

SID

Silence Insertion Descriptor

SIP

Session Initiation Protocol

SIP-I

SIP with encapsulated ISUP

SIP-T

SIP for Telephones

SLA

Service Level Agreement

SMMSL

SIP Message Manipulation Scripting Language

SNMP

Simple Network Management Protocol

SoC

Statement of Compliance

SPDF

Service-Based Policy Decision Function

SPL

Service Priority Level

SPLMN

Serving PLMN

SR

Site Router

SRTCP

Secure Real-Time Control Protocol

SRTP

Secure Real-Time Transport Protocol

SRTP-DTLS

Secure Real-Time Transport Protocol
Datagram Transport Layer Security

SRV

Service

SRVCC

Single Radio Voice Call Continuity

SS7

Signalling System No. 7

SSCF

Service Specific Coordination Functions

SSCOP

Service Specific Connection Oriented Protocol

SSH

Secure Shell

SSHFS

SSH Filesystem

SSL

Secure Socket Layer

STA

Session-Termination-Answer

STR

Session-Termination-Request

SU

Service Unit

SW

Software

SwIM

Software Inventory Management

SwM

Software Management

**TBAC**

Target-Based Access Control

TC

Textual Convention

TCAP

Transaction Capabilities Application Part

TCP

Transmission Control Protocol

TDM

Time Division Multiplexing

TDMA

Time Division Multiple Access

TGRP

Trunk Group

TIPC

Transparent Inter-Process Communication

TISPAN

Telecoms & Internet converged Services & Protocols for Advanced Networks

TLS

Transport Layer Security

TrFO

Transcoder Free Operation

TrGW

Transition Gateway

TS

Technical Specification

TTC

Telecommunication Technology Committee

TTL

Time To Live

UCF

Upgrade Control File

UDA

User-Data-Answer

UDP

User Datagram Protocol

UDPTL

UDP Transport Layer

UDR

User-Data-Request

UE

User Equipment

UG

User Guide

ULN

Unique Logical Name

UML

Unified Modeling Language

UMTS

Universal Mobile Communication System

UNI

User-to-Network Interface

UP

Upgrade Package

URI

Uniform Resource Identifier

URL

Uniform Resource Locator

URN

Uniform Resource Name

USM

User-based Security Model

UTC

Coordinated Universal Time

UTF

Unicode Transformation Format

VC

Virtualization Container

vCPU

Virtual CPU



VDU
Virtualization Deployment Unit

VIP
Virtual Internet Protocol

VLAN
Virtual LAN

VM
Virtual Machine

vMRF
Virtual Multimedia Resource Function

VNF
Virtualized Network Function

VNFC
Virtualized Network Function Component

VNFCI
Virtualized Network Function Component Instance

VNFD
Virtualized Network Function Descriptor

VNFI
Virtualized Network Function Instance

VNFM
Virtualized Network Function Manager

vNIC
Virtualized Network Interface Controller

VoIP
Voice over IP

VoLTE
Voice over LTE

VMDK
Virtual Machine Disk

VMM
Virtual Machine Monitor

VPLMN
Visited - Public Land Mobile Network

VPN
Virtual Private Network

VR
Virtual Router

VRRP
Virtual Router Redundancy Protocol

WB
Wideband

WCDMA
Wideband Code Division Multiple Access

WCG
Web Communication Gateway

xDSL
Digital Subscriber Line

XML
Extensible Markup Language

XSD
XML Schema Definition