NOKIA

# NSP
# Network Services Platform

## Network Functions Manager - Packet (NFM-P)

Release 17.3

# Glossary

**3HE-11991-AAAA-TQZZA**

**Issue 1**

**March 2017**

**Legal notice**

# Contents



# 1 About this document

## 1.1 Purpose

The *NSP NFM-P Glossary* defines terms, acronyms, and initialisms used in the *NFM-P* documentation.

Glossary entries that are marked with an asterisk (*) are reproduced with permission from *LTE – The UMTS Long Term Evolution: A Pocket Dictionary of Acronyms*, © 2009 Stefania Sesia, Issam Toufik, and Matthew Baker, available at http://www.wiley.com/go/sesia_theumts.

## 1.2 Document support

**Customer documentation and product support URLs:**

- Customer Documentation Welcome Page
- Technical support
- Documentation feedback

# Glossary

## Numerics

**10/100/1000Base-FX**
A networking standard that supports data transfer rates of up to 1000 Mb/s over two optical fibers.

**10/100/1000Base-TX**
An Ethernet technology that supports data transfer rates of up to 1000 Mb/s using twisted-pair copper wire.

**10/100Base-TX**
An Ethernet standard that supports data transfer rates of up to 100 Mb/s using two pairs of data-grade, twisted-pair copper wire.

**100Base-T**
An Ethernet standard that supports data transfer rates of up to 100 Mb/s using twisted-pair copper wire.

**1830 PSS**
1830 Photonic Service Switch
A photonic switching device that has advanced "CWDM" (p. 30) , "DWDM" (p. 37) , and "OTN" (p. 89) capabilities.

**1830 PSS-1**
1830 Photonic Service Switch, 1-slot
A single-slot 1830 PSS that is typically deployed as a CE access device.

**1830 PSS-16**
1830 Photonic Service Switch, 16-slot
A 16-slot 1830 PSS that is typically deployed for service delivery between metropolitan and core networks.

**1830 PSS-32**
1830 Photonic Service Switch, 32-slot
A 32-slot 1830 PSS that is typically deployed in a core network.

**1830 PSS-4**
1830 Photonic Service Switch, 4-slot
A four-slot 1830 PSS that is typically deployed near the edge of a metropolitan network for the aggregation of "CWDM" (p. 30) and "DWDM" (p. 37) traffic.

**1830 VWM**
1830 Versatile WDM Module
A passive add-on shelf unit that provides "WDM" (p. 130) extension to a network element.

**3-plus-tag**
A descriptor for Ethernet frames with three or more VLAN ID tags.

**3GPP**
3rd Generation Partnership Project
The joint standardization partnership responsible for standardizing UMTS, HSPA, and LTE.

**5-tuple**
Information that defines a TCP/IP connection, including source IP address, destination IP address, source port number, destination port number, and the protocol in use.

**6over4 tunneling**
6over4 tunneling is a network mechanism that is part of the transition from IPv4 usage to the adoption of IPv6. The mechanism enables IPv6 packet transmission through a multicast-enabled IPv4 network.

**6PE**
IPv6 provider edge
6PE allows IPv6 domains to communicate over an MPLS IPv4 network without requiring explicit IPv6 transport.

**6VPE**
IPv6 VPN provider edge
6VPE allows IPv6 VPNs to communicate over an MPLS IPv4 network without requiring explicit IPv6 transport.

**7210 SAS-D**
7210 Service Access Switch - Demarcation
An intelligent Ethernet edge-demarcation device that extends enhanced Carrier Ethernet VPN service delivery to the CE.

**7210 SAS-E**
7210 Service Access Switch - Ethernet
A Carrier Ethernet CLE device that can also be deployed as a cost-effective CE aggregation device for smaller networks.

**7210 SAS-K**
7210 Service Access Switch, chassis type K
A Gigabit Ethernet switch typically used for L2 services and mobile backhaul applications. The switch provides aggregation and demarcation for VLL and VPLS services managed to the customer edge.

**7210 SAS-M**
7210 Service Access Switch - MPLS
A CE device that provides MPLS-enabled metropolitan and WAN Carrier Ethernet service delivery, Ethernet-based mobile backhaul, and residential service access.

**7210 SAS-Mxp**
7210 Service Access Switch, chassis type Mxp
An Ethernet access device that provides IP and MPLS-enabled metropolitan and WAN Carrier Ethernet service delivery, Ethernet-based mobile backhaul, and residential service access.

**7210 SAS-R**
7210 Service Access Switch, chassis type R
An Ethernet switch capable of MPLS and MPLS-TP service transport. With multiple IMM card slots and two CPM slots, the 7210 SAS-R supports redundant switching capacity and is suitable for aggregating 1-Gig and 10-Gig rings in access Ethernet networks.

**7210 SAS-Sx**
7210 Service Access Switch, chassis type Sx

An Ethernet access device that provides IP and MPLS-enabled service delivery, Ethernet-based mobile backhaul, and residential service access. The 7210 SAS-Sx can operate in two modes:

- Standalone mode, in which the NE is managed as an IP/MPLS-enabled service aggregation device at the customer edge.
- Satellite mode, in which the NE is connected by the uplink port to an SR device, and is managed as a shelf unit of the SR device to provide port expansion.

**7210 SAS-T**
7210 Service Access Switch, chassis type T
An Ethernet access device that provides demarcation for services managed to the customer edge and Ethernet aggregation in smaller network locations.

**7210 SAS-X**
7210 Service Access Switch - MPLS Extended
An MPLS-enabled Ethernet aggregation device for small and medium-sized networks that provides business, mobile backhaul, and residential services. It is similar to the 7210 SAS-M, but has 10Gb/s uplink ports, enhanced traffic management, greater scalability, and hierarchical QoS functions.

**7301 ASAM**
7301 Advanced Services Access Manager
A high-bandwidth, multimedia-ready DSLAM that provides DSL-based high-speed data transmission between a residential subscriber host and an ATM network.

**7450 ESS**
7450 Ethernet Service Switch
An Ethernet switch that enables the delivery of metro Ethernet services and high-density service-aware Ethernet aggregation over IP/MPLS networks.

**7701 CPAA**
7701 Control Plane Assurance Appliance
A mountable two-unit computing platform that passively monitors a network to collect and analyze routing data. The 7701 CPAA is the hardware component with which the CPAM interacts.

**7705 SAR**
7705 Service Aggregation Router
A router that provides IP/MPLS and PW aggregation functions.

**7705 SAR-A**
7705 Service Aggregation Router, chassis type A

A 7705 SAR-A router with two variants:

- passively cooled chassis with 12 Ethernet ports and 8 T1/E1 ports
- passively cooled chassis with 12 Ethernet ports and no T1/E1 ports

**7705 SAR-Ax**
7705 Service Aggregation Router, chassis type Ax
The 7705 SAR-Ax is designed mainly as a platform for indoor small cell application. The 7705 SAR-Ax transports all types of data from a mobile cell site to a higher aggregation point of presence or to the Evolve packet core (EPC) over a packet switched network or unsecure ISP. The 7705 SAR-Ax also targets fixed and vertical networks.

**7705 SAR-F**
7705 Service Aggregation Router– fixed form-factor chassis

**7705 SAR-H**
7705 Service Aggregation Router– hardened
A 7705 SAR-H router that is temperature and EMC–hardened to the following specifications: IEEE1613 and IEC61850-3.

**7705 SAR-Hc**
7705 Service Aggregation Router– hardened compact
A 7705 SAR-Hc router is a compact version of the 7705 SAR-H.

**7705 SAR-M**
7705 Service Aggregation Router, chassis type M

A 7705 SAR router with four variants:

- actively cooled chassis with 16 T1/E1 ports, 7 Ethernet ports, and 1 hot-insertable module slot
- actively cooled chassis with 0 T1/E1 ports, 7 Ethernet ports, and 1 hot-insertable module slot
- passively cooled chassis with 16 T1/E1 ports, 7 Ethernet ports, and 0 module slots
- passively cooled chassis with 0 T1/E1 ports, 7 Ethernet ports, and 0 module slots

**7705 SAR-W**
7705 Service Aggregation Router, chassis type W
A 7705 SAR-W router is a passively cooled, universal AC and DC powered unit, equipped with five Gigabit Ethernet ports (three SFP ports and two RJ-45 Power over Ethernet (PoE) ports).

**7705 SAR-Wx**
7705 Service Aggregation Router, chassis type Wx

A 7705 SAR-Wx router is a passively cooled, universal AC powered unit; there are three variants:

- AC power input connector, five Gigabit Ethernet data ports (three SFP ports and two RJ-45 Ethernet ports), and an RJ-45 alarm input connector

- AC power input connector, five Gigabit Ethernet data ports (three SFP ports, one RJ-45 Ethernet port, and one RJ-45 Ethernet port with PoE+), and an RJ-45 alarm input connector
- AC power input connector, four Gigabit Ethernet data ports (three SFP ports and one RJ-45 port), one RJ-45 4-pair xDSL port, and an RJ-45 alarm input connector

**7710 SR**
7710 Service Router
A 10-Gbyte version of the 7750 SR that provides granular lower-speed private data services with SLAs.

**7750 SR**
7750 Service Router
A high-capacity router that provides scalable, high-speed private data services. It is typically deployed in a core network.

**7750 MG**
7750 Mobile Gateway
An LTE gateway based on the 7750 SR. The 7750 MG can be configured as a "PGW" (p. 92) or an "SGW" (p. 109) .

**7950 XRS**
7950 Extensible Routing System
A large-scale routing system designed for core deployments. The system is based on the SROS and is available in a 20-slot chassis.

**802.1ag**
An IEEE standard that specifies protocols, procedures, and managed objects to support transport fault management in Ethernet services. The standard includes specifications for path discovery and verification, and detection and isolation of connectivity faults.

**802.1D**
An IEEE standard that specifies a general method for the operation of MAC bridges, including the STP.

**802.1p**
An IEEE standard to provide QoS in Ethernet networks. The standard uses packet tags that define up to eight traffic classes, and enables a switch to transmit packets based on the priority value.

**802.1Q**
An IEEE standard that defines the operation of VLAN bridges, and the operation and administration of VLAN topologies in a bridged LAN.

**802.1w**
An IEEE standard that defines the requirements for a MAC bridge to provide rapid reconfiguration capability.

**802.1X**
An IEEE standard for transmitting EAP authentication messages over a LAN. The client EAP messages are encapsulated in Ethernet frames and transported to a network

access point, which is typically a port on an edge device, and then to an authentication device such as a RADIUS server.

**9400 NEM**
9400 Network Element Manager
The 9400 NEM is a configuration tool for eNodeB devices.

**9412 eNodeB**
See "eNodeB" (p. 40) .

**9471 WMM**
9471 Wireless Mobility Manager
An MME based on an ATCA Linux platform.

**9500 MPR**
9500 Microwave Packet Radio
A microwave radio transmission device that aggregates, in a unified Ethernet convergence layer, the native IP packet streams of services in a TDM mobile backhaul network.

**9500 MPRe**
9500 Microwave Packet Radio (Ethernet)
The 9500 MPRe is a 9500 MPR variant that is a standalone outdoor application of the "MPT-MC" (p. 75) with no shelf unit. The 9500 MPRe provides fixed or mobile Ethernet backhaul and supports converged metropolitan MPLS networks.

**9926 DBS**
9926 Distributed Base Station
See "eNodeB" (p. 40) .

**9952 WPS**
9952 Wireless Provisioning System
The 9952 WPS is an LTE software tool for creating CM XML "WO" (p. 131) files for LTE NE configuration management.

**9958 WTA**
9958 Wireless Trace Analyzer
The 9958 WTA is a client-based tool that performs end–to–end analysis of call-trace data gathered from the eNodeB and 9471 WMM.

**9959 NPO**
9959 Network Performance Optimizer
The 9959 NPO is an EMS that monitors LTE RAN networks and provides the NFM-P with QoS support, alarm management, and statistics.

## A

**AA**
application assurance
A technology that enables policy-based deep packet inspection of subscriber traffic for application-layer subscriber management.

**AAA**
authentication, authorization, and accounting
The functions of user security protocols such as RADIUS and TACACS+.

**AAL-5**
ATM adaptation layer type 5
AAL-5 supports the conversion of “VBR” (p. 125) , delay-tolerant, connection-oriented traffic such as signaling and control data, and network management data. AAL-5 traffic requires minimal sequencing and minimal error detection.

**ABM**
advanced bandwidth manager
A system that performs bandwidth reservation tasks and provides session admission control for VoIP, VoD, or any IP-based application that requires a bandwidth guarantee.

**ABR**
area border router
A router on the border of one or more OSPF areas that connects the areas to the backbone network. The ABR is considered to be a member of the OSPF backbone and the attached areas. The router maintains routing tables that describe both the backbone topology and the topologies of other areas.

**ABS**
anti-breakdown system
An overload protection process on the 7750 MG. ABS contains internal parameters that monitor signaling latency and memory utilization on each ISM-MG. The parameters each have a high and low threshold value.
When the high threshold value is reached, the ABS signals the corresponding application protocol handler, which decides whether the packet is selectively discarded.
When the memory utilization drops below the low threshold value, the ABS stops passing the signal to the application handler, which prevents the packets from being discarded.

**ACK**
acknowledge
An ACK is an acknowledgment signal that confirms the receipt of a data packet.

**ACL**
access control list
An ACL, which is also called a filter policy, is a template applied to a service or port to control ingress or egress network traffic based on IP and MAC criteria.

**ACR**
accounting requests

**AD**
administrative domain
A group of hosts, routers, and the interconnecting networks, that are managed by a single administrative authority.

**AD**
add drop

**ADC**
application detection and control
ADC detects and reports the stop and start of specified application traffic to the PCRF, and applies the appropriate enforcement actions.

**adjacency**
An adjacency is a close link-state relationship between compatible neighboring routers that allows them to share routing information and forward network traffic. In OSPF, routers become fully adjacent when their compatibility is confirmed and they synchronize their link-state databases. In IS-IS, adjacencies proceed in stages from Down to Up; they are Up when their compatibility is confirmed. IS-IS adjacencies are level 1 or level 2, depending on the level capability of the routers.

**ADM**
add/drop multiplexer
A device installed at an intermediate point on a transmission line that enables new signals to be added in the line and existing signals to be dropped. Add/drop multiplexing can be done with optical or electrical signals.

**admission control**
Admission control is a validation process that matches the availability of network resources with the service authorization level of an end user to establish a network connection.

**ADT**
add drop through

**AFI**
Address Family Identifier
MP-BGP uses routing tables identified by the Address Family Identifier and Subsequent Address Family Identifier (SAFI).

**AGW**
access gateway

**AH**
Authentication Header
A member of the IPsec protocol suite. AH is a transport-layer protocol that provides data confidentiality, origin authentication, integrity checking, and replay protection. The communicating systems use a shared key to encrypt and decipher data. AH is similar to “ESP” (p. 41) , but provides IP header protection by default.

**AHPHG**
High Power High Gain Amplifier

**AHPLG**
High Power Low Gain Amplifier

**AINS**
Automatic IN-Service
An 1830 PSS shelf option that allows newly provisioned entities to be inserted at a later time without generating alarms.

**AIS**
alarm indication signal
A signal that a system transmits after some part of a communication link fails.

**AISG**
Air Interface Standards Group
The AISG is a non-profit consortium that develops international standards for wireless antenna line devices.

**alarm**
An alarm is a notification that the NFM-P generates based on a set of conditions; for example, SNMP traps from NEs and NFM-Pevents. NFM-P alarms are displayed in the client GUI client alarms window, and are also available through the XML APIinterface. NFM-P alarms follow the X.733 standard.

**ALD**
antenna line device

**ALG**
Application Layer Gateway.
A security component that augments a NAT configuration in a network. It allows the configuration of NAT traversal filters that allow address and port translation for specified application layer protocols.

**ALPFGT**
Low Power Fixed Gain Amplifier card with total power monitoring

**ALPHG**
Low Power High Gain Amplifier card

**AMBR**
aggregated maximum bit rate
The upper limit on the aggregate bit rate that is provided across all non-GBR bearers. See 3GPP TS23.401 Section 4.7.3.

**AMI**
alternate mark inversion
A type of line encoding that prevents line capacitance charging. AMI uses alternate positive and negative pulses of the same amplitude to represent a binary 1 and a zero-amplitude state to represent a binary 0.

**AMR**
adaptive multi-rate

**ANCP**
Access Node Control Protocol

ANCP is an IP-based protocol used in DSL networks. ANCP operates between a DSLAM and a core network device to provide SAP-level rate management. ANCP is an extension of GSMP.

**ANL**
Access Network Location
ANLs are potential congestion points in the network.

**ANM**
Any rate pluggable I/O card

**ANR**
automatic neighbor relation
An eNodeB function that automatically determines the optimal neighbor relations for UE hand-off.

**ANSI**
American National Standards Institute

**AOS**
Nokia OmniSwitch

**AP**
access point
A device that allows wireless devices to connect to a wired network using Wi-Fi.

**APAC**
Asia Pacific and China

**API**
application programming interface
A set of programming functions that provide an interface between software applications. An API translates high-level program code into low-level computer instructions.

**Apipe**
ATM pipe
A type of VLL service that provides a point-to-point ATM service between users who connect to NEs directly or through an ATM access network. One endpoint of an Apipe uses ATM encapsulation, and the other endpoint uses ATM or frame relay encapsulation.

**APN**
access point name
Identifies a “GGSN” (p. 46) or “PGW” (p. 92) . It includes a network identifier that defines the “PDN” (p. 91) to which the “UE” (p. 123) requests connectivity, and may also include an operator identifier that specifies in which “PLMN” (p. 94) the PGW or GGSN is located. See 3GPP TS23.003 Sections 9 and 19.4.2.2.*

**APN AMBR**
access point name aggregate maximum bit rate
The maximum available bit rate for an LTE user for accessing services on a specific PDN APN.

**application server**
A software product that provides Java EE services for Java applications, such as JMS or transaction support. The product may include clustering technology to allow communication among multiple JVMs in a network.

**APR**
automatic power reduction
A function that automatically reduces the output power of an optical amplifier to prevent human exposure to hazardous output levels.

**APS**
automatic protection switching
The capability of a transmission system to detect a failure on a working line and to switch automatically to a protection line to recover the traffic.

**AQP**
application QoS policy
An AQP defines the application policy rules (in terms of matches and actions) when actions that require application awareness are to be performed on the traffic.

**arbiter**
An arbiter is an object in a policer control policy that controls the amount of bandwidth that may be distributed to a set of child policers. The root arbiter represents the parent policer. The maximum traffic rate defined for the root arbiter specifies the decrement rate for the parent policer that governs the overall aggregate traffic rate of every child policer associated with the policy instance. The root arbiter also contains the parent policer MBS configuration parameters that the system uses to individually configure the priority thresholds for each policer instance. Child policers may be associated directly with the root arbiter, or with one of the tier 1 or tier 2 arbiters created under the root arbiter.

**area**
In the OSPF protocol, network management and scalability can be simplified by partitioning a network into regions. These OSPF network regions are called areas. Each area, also called a routing sub-domain, maintains detailed routing information about its own internal composition, and also maintains routing information which allows it to reach other areas.

**ARP**

ARP is expanded two ways:

1. Address Resolution Protocol

   ARP is a TCP/IP protocol used to convert an IP address into a physical address, such as an Ethernet address.

2. allocation and retention priority

   An EPS bearer QoS parameter that prioritizes bearer establishment or modification requests when resources are limited. An ARP can determine that existing bearers with a relatively low priority should be dropped to free up needed resources. An ARP can also determine whether a bearer should be dropped by another bearer with a higher priority. See 3GPP TS 23.203

**AS**

AS is expanded two ways:

1. autonomous system

   An AS is a collection of routers under one administrative entity that cooperates by using a common IGP (such as OSPF). AS is synonymous with the ISO term “routing domain”. Routing between autonomous systems is done with an inter-AS or interdomain EGP, such as BGP-4.

2. alarm surveillance

   AS is an application that receives, stores, displays, and manages real-time alarms. The AS tool consists of an IM to receive, filter, and store alarms; and a USM to display and manage alarm information.

**ASAP**
alarm severity assignment profile
The condition severities on an 1830 PSS OCS device are managed using ASAP.

**ASAP MDA**
any service, any port MDA
An MDA that supports channelization down to the DS0 level and accepts one OC-3 /STM-1 SFP module. The MDA is based on a programmable data path architecture that enables enhanced L1 and L2 data path functions, such as ATM TM features, MDA-based channel and port queuing, and multilink applications such as IMA and PPP.

**ASBR**
autonomous system boundary router
In OSPF, an ASBR is a router that exchanges information with devices from other ASs. ASBRs are also used to import routing information about RIP, direct, or static routes from non-OSPF attached interfaces.

**ASCII**
American Standard Code for Information Interchange
ASCII is a collection of 7-bit character sets allowing per-country definitions, called variants.

**ASE**
Amplified Spontaneous Emissions

**AS-MAC**
asynchronous-MAC

**ASM**
Any-Source Multicast
Any-Source Multicast is the IP multicast service model defined in RFC 1112, host extensions for IP Multicasting. An IP datagram is transmitted to a host group which is a set of zeros and is identified by a single IP destination address (224.0.0.0 through 239.255.255.255 for IPv4). End hosts are able to join or leave a group any time as there

is no restriction to the location or number. This model supports multicast groups with a number of senders. Any end host can be transmitted to a host group even if it is not a member of that group.

**ASN**
autonomous system number

**ASN.1**
abstract syntax notation one

**ASO**
application service option
ASOs are used to define service provider and customer network functions that are common among sets of subscribers. ASOs prevent subscribers from requiring each subscriber-specific entry in the application QoS policies for standard network services.

**ATCA**
Advanced Telecommunications Computing Architecture
ATCA is an industry initiative developed by the PCI Industrial Computer Manufacturers Group. It is designed to meet the needs of both network equipment manufacturers, who require platform reuse, lower costs, faster time-to-market, and multi-source flexibility, and carriers and service providers, who require reduced capital and operational expenditures.

**ATM**
asynchronous transfer mode
A transport and switching mechanism that employs 53-byte cells as a basic unit of transfer. Information is routed through the network in the cell using addressing information contained in the header.

**AU**
administrative unit
*See* “AU-N” (p. 17) .

**AU-N**
administrative unit - level *N*
A managed entity within the SDH structure that is the top of the STM-1 configuration hierarchy.
AU-3 has the payload pointer for each payload envelope that is consolidated with the respective payload in one unit. An STM-1 frame has three payload envelopes; therefore, the frame has three AU-3 units. AU-4 applies to the entire STM-1 payload. The AU-4 structure is the only AU in an STM-1 frame.

**AUG**
administrative unit group
One or more AUs that occupy fixed, defined positions in an STM payload.

**autosigned**
A method of automatically signing SSL and PKI certificates, rather than forcing the manually signing certificates each time there is an SSL or PKI transaction.

**AUX**
auxiliary

**auxiliary database**
See “NFM-P auxiliary database” (p. 80).

**auxiliary server**
See “NFM-P auxiliary server” (p. 81).

**AVCN**
Attribute value change notification

**AVP**
attribute value pair
A fundamental data representation that consists of an attribute name and a value. The Diameter protocol consists of a header followed by one or more AVPs. An AVP includes a header and is used to encapsulate protocol-specific data and AAA information.

## B

**B-component**
The VLAN component within a Backbone Edge Bridge that relays frames between Customer Backbone Ports and Provider Network Ports.

**B-MAC**
backbone or provider MAC

**B-TAG**
backbone VLAN tag

**B-VID**
backbone VLAN Id

**B-VLAN**
backbone VLAN

**B-VPLS**
backbone VPLS

**B-VSI**
backbone Virtual Switch Instance. Also referred to as a B-Site.

**backpressure**
A technique for ensuring that a transmitting port does not send too much data to a receiving port at a specific time. When the buffer capacity of a receiving port is exceeded, the port sends a jam message to the transmitting port to halt transmission.

**BBU**
base band unit

**BCB**
backbone core bridge

**BCD**
binary-coded decimal
A binary-coded notation in which each of the decimal digits is represented by a binary numeral; a code compression scheme in which two binary bits replace the three-zone bits and four binary bits replace the nine data bits.

**BCP**
Bridging Control Protocol
A protocol that configures, enables, and disables the bridge protocol modules on both ends of a point-to-point link.

**bearer**
A bearer is an IP packet flow that has a QoS configuration between a gateway and the “UE” (p. 123) .

**BEB**
backbone edge bridge

**BER**
bit error rate
The percentage of bits that have errors relative to the total number of bits received in a transmission.

**BERT**
bit error rate tester
BERT is a device that determines the BER on a communication channel.

**BFD**
bidirectional forwarding detection
BFD is a protocol to detect faults in the bidirectional path between two forwarding devices.

**BGP**
Border Gateway Protocol
BGP is an IETF standard EGP used to propagate routing information between autonomous systems.

**BGP AD**
BGP Auto Discovery
BGP AD enables a VPLS PE router to discover other PE routers that are part of the same VPLS domain.

**BGP AS**
border gateway protocol autonomous system
BGP is an IETF standard EGP used to propagate routing information between autonomous systems.

**BGP LS**
border gateway protocol link state
BGP LS is a BGP address family that distributes IGP topology information to external traffic engineering servers to assist in calculating paths.

**BGP-4**
Border Gateway Protocol 4
A BGP that supports CIDR addressing, which increases the number of available IP addresses.

**binding**
A collection of configuration parameters, including at least an IP address, associated with a DHCP client. DHCP servers manage bindings.

**BITS**
Building Integrated Timing Supply
BITS is a method of distributing precision timing in a network.

**black hole**
In networking, black holes refer to places in a network where incoming or outgoing traffic is silently discarded at the routing level without informing the source that the data did not reach its intended recipient. For example, you can configure NFM-P VPLS sites to allow customers under DOS, DDOS, and worm attacks to send all traffic to a null route to quarantine the hostile traffic.

**BOF**
boot option file
A file that specifies the runtime image, configuration files, and other operational parameters during system initialization.

**BOM**
byte order mark
The byte order mark is a unicode character used to signal the byte order of a text file or stream.

**BPDU**
bridge protocol data unit
BPDU is the frame used by LAN bridges that support 802.1D STP to communicate with each other.

**BRAS**
broadband remote access server

**bridge**
Bridges connect two or more network segments which increases the network diameter. Bridges also help regulate traffic. They can send and receive transmissions but a bridge does not originate any traffic of its own other than a special Ethernet frame that allows it to communicate with other bridges.

**broadcast TV**
See "BTV" (p. 21) .

**BSA**
broadband service aggregator
A high-speed Ethernet aggregation device that supports hundreds of ports, tens of thousands of filter policies, and tens of thousands of queues to aggregate subscriber traffic. The 7450 ESS is a BSA.

**BSM**
bootstrap message
A PIM message that CBSRs exchange during the BSR election process.

**BSR**

BSR is expanded two ways:

1. bootstrap router

   A BSR is a PIM router that manages RP and group information in a multicast network.

2. broadband service router

   A BSR terminates L2 access services and routes over IP/MPLS, supporting hundreds of ports and sophisticated QoS for services and for differentiating content and source. An example of a BSR is the 7750 SR.

**BTS**
base transceiver station
In a “RAN” (p. 98) , the BTS is the terminating point of the radio interface.

**BTV**
broadcast television
The transmission of television signals that are available to all users. This television service is used on cable, satellite, and off-air systems. BTV is typically part of a triple play service offering.

**bundle**
A bundle consists of all baud channels of a packet handler access point interface to a specific connection-related function to which users are connected.

## C

**C**
client port

**C-MAC**
customer MAC

**c-plane**
See “control plane” (p. 28) .

**C-RP**
candidate rendezvous point
A router that is configured as a potential RP. If the current RP fails, the C-RP participates in an automated RP election process.

**C-XMA**
compact XMA
In the 7950 XRS, an XMA that operates at half capacity. See also “XMA” (p. 133) .

**CAC**
Connection Admission Control

**CAD**
Channel Add Drop

**CALEA**
communications assistance for law enforcement act
CALEA is a United States federal law that enables the government to intercept wire and electronic communications and call-identifying information under certain circumstances; for example, to protect national security.

**CAM**
content-addressable memory
CAM is a type of computer memory typically used where high-speed searches are required. CAM compares search terms to the memory contents and returns the storage address of any matches, along with additional data if so designed.

**CBP**
customer backbone port
A CBP is a Backbone Edge Bridge Port that can receive and transmit frames for multiple customers, and can translate or assign B-MAC, B-VID, and I-SID on the basis of the received I-SID. This is an I-tagged interface. In the context of SR PBB this is the B-Site “port” that is connected to the I-Site.

**CBR**
constant bit rate
CBR is an ATM service category that is used to carry traffic characterized by a service bit rate specified by a constant value and an evenly-spaced cell stream.

**CBS**
committed burst size
The CBS is the maximum number of bytes that can be transmitted at the link speed and that conform to the CIR.

**CBSR**
candidate bootstrap router
A router that is configured as a potential BSR. If the current BSR fails, the CBSR participates in an automated BSR election process.

**CC**

CC can be expanded in the following ways:

1. content of communication
2. continuity check

   A continuous flow of OAM cells generated by an ATM switch to check connectivity in the forward direction of a VCC or a VPC between two points in the network.
3. credit control

**CCA**

CCA can be expanded in two ways:

1. credit control answer

   The CCA is a message that is used between the credit control server and the Diameter credit control client to acknowledge a CCR.

2. cross-connect adapter

   See “VSM-CCA” (p. 129) .

**CCAG**
cross-connect aggregation group
VSM-CCAs are placed in a CCAG. A CCAG provides a mechanism to aggregate multiple CCAs into one forwarding group. The CCAG uses conversation hashing to dynamically distribute cross-connect traffic to the active CCAs in the aggregation group. In the event that an active CCA fails or is removed from the group, the conversation hashing function redistributes the traffic over the remaining active CCAs within the group. The conversation hashing mechanism for a CCAG is identical to that used by Ethernet LAGs.

**CCF**
charging control function

**CCFH**
credit control failure handling
The CCFH AVP establishes the behavior of the credit-control client in fault conditions. The CCFH value may be configured locally or received from the credit-control server or Diameter home AAA server. The CCFH value received from the Diameter home AAA server overrides the locally configured value, while the CCFH value received from the credit-control server in the CCA message overrides any existing value.
The CCFH AVP offers different failure handling options, including terminate, continue, and retry and terminate.

**CCM**

CCM is expanded in two ways:

1. continuity check message

   In a CFM enabled network, CCM is a multicast PDU transmitted periodically by a MEP to assure the continuity over the MA to which the transmitting MEP belongs.

2. chassis control module

   In the 7950 XRS, a module that houses all management connections and supports operator access to the routing system. CCMs include an LCD touch-screen that supports interfaces for functions such as alarm management and timing management. Each 7950 XRS includes two CCMs that are physically connected to a CPM.

**CCR**
credit control request

The credit control request is a message used between the Diameter credit control client and the credit control server to request credit authorization for a service.

**CCR-A**
credit control request answer

**CCR-U**
credit control request update

**CDC-F**
colorless, directionless, and contentionless flexible grid

**CDF**
charging data function

**CDR**
charging data record
A CDR represents a formatted collection of information about a chargeable event and is used by telecom providers for user billing.

**CE**
customer edge
A customer device with the required functions to access the services that are made available by a provider.

**CEM**
circuit emulation
CEM is an encapsulation mode that emulates circuit characteristics of SONET or SDH packets.

**certified directory**
The certified directory contains image and configuration files that are certified by an authorized user as the default files for the switch. If the switch reboots, the switch reloads the files in the certified directory. If a switch is running from the certified directory, you cannot save any changes made in the running configuration. If the switch reboots, the changes made to switch parameters are lost. To save running configuration changes, the switch must be running from the working directory. See also "working directory" (p. 131) .

**CES**
circuit emulation service
A device function that enables the encapsulation of TDM frames in protocol packets that are tunneled through a core network.

**CESoETH**
circuit emulation service over Ethernet
See "CES" (p. 24)

**cflowd**
Enabling cflowd allows for the collection and analysis of traffic flow samples through a router. It is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, and SLA measurement.

**CFM**
connectivity fault management

**CFOADM**
"CWDM" (p. 30) Fixed Optical Add Drop Multiplexer

**CFP**
compact form factor pluggable

**CGF**
charging gateway function
The CGF listens to GTP messages sent from the GSNs on TCP or UDP port 3386 and gathers charging information in discreet records called CDRs from both SGSNs and GGSNs. The CGF compiles the CDRs into files and stores them until forwarding them to one or more billing networks.

**CGI**
cell global identity

**CHAP**
Challenge Handshake Authorization Protocol
CHAP is a secure method for connecting to a system.

**cHDLC**
Cisco HDLC data encapsulation
cHDLC is a Cisco variation of HDLC encapsulation, a bit-oriented synchronous data link layer protocol. HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums. cHDLC also uses a control protocol to maintain serial link keep-alives. You can only configure Cisco HDLC on IES SAPs.

**checkpoint (regular)**
A checkpoint is a snapshot of a network at a particular point in time. The checkpoint may be as simple as a checkpoint of existences, or as complex as a complete copy of the topology, which models the existence of an object and its attributes.
See also "reference" (p. 99) .

**child form**
A child form is a form that is opened from another form. Typically, you must save the child form configuration, and also save or apply the changes from the parent.

**CIDR**
classless interdomain routing
An address aggregation process that simplifies routing.

**CIR**
committed information rate
The CIR is the guaranteed minimum rate of throughput between two end-user devices over a network under normal operating circumstances. This rate, measured in bits or kb/s, is used in congestion control procedures.

**circuit**
A circuit is a communications connection between two points. It has a line interface from which it transmits and receives data and signaling. A circuit is also known as a port, channel, or timeslot. An electronic circuit is one or more electronic components connected together to perform a specific function.

**CIST**
common and internal spanning tree
The CIST instance is the spanning tree calculated by the MSTP region IST and the network CST. The CIST is represented by the single spanning tree flat mode instance. By default, all VLANs are associated with the CIST until they are mapped to an MSTI.
See "STP flat mode" (p. 116) .

**CIT**
Craft interface terminal
A local interface between the user and an NE. It is used to issue commands to the local system or, by way of a remote login, to another system on the same fiber as the local system.

**class of service**
See "CoS" (p. 28) .

**CLE/ODNC**
critical link event/OAM discovery not completed

**CLEI**
common language equipment identifier
CLEI codes identify telecommunications equipment in networks. The CLEI code uses a 10-character structure, as outlined in the Telcordia specification. These characters define equipment by specifying basic product type, features, source document, and associated drawings and versions. A CLEI code is unique to a specific piece of equipment and cannot be assigned to any other part.

**CLI**
command line interface
A CLI is an interface that allows an operator to interact with a system by typing commands at a prompt.

**client delegate server**
See "NFM-P client delegate server" (p. 81).

**CLLI**
common language location identifier
A CLLI is a standardized, 11-character code used to identify the geographic location of an NE.

**CLM**
customer license manager
A designated role within a customer organization that is responsible for the administration, purchase, return, and request of temporary, permanent, and emergency RAN license entitlements via OLCS and the LKDI web tool.

**CM**
configuration management
Modification of network elements in the LTE RAN.

**CMA**
compact media adapter
Similar to an MDA, but smaller.

**CMAS**
confederation member autonomous system
A subdivision of an AS that is recognized only by other peers within the confederation. Within the confederation, a BGP peer treats only the peers in its CMAS as internal peers. Peers in different CMASs are external peers.

**CMG**
cloud mobile gateway
The software-only version of the 7750 MG.
Formerly known as the VMG.

**CMM**
chassis management module
Switches that operate in a stack, in a primary or secondary management role.

**CNM**
customer network manager
A data integration system that integrates data from the fault, performance, order management, and provisioning systems of a service provider into a near real-time view for the enterprise customer.

**CNM toolkit**
The CNM toolkit is comprised of a servlet and related files that provide a simplified distributed interface to the XML APImodule. The servlet is invoked by CNM applications from a web browser.

**CNO-ULI**
core network overload - user location information
CNO-ULI allows network operators to deploy differentiated charging and other business logic based on location, without incurring massive network signaling load.

CNO-ULI constitutes two parts:

- ULI change reporting when the E-RAB/RAB/user plane is established
- presence reporting area information reporting

**CO**
central office
See “NOC” (p. 82) .

**COF**
Channel optical filter

**combo port**
A port that is shared between a 10/100/1000 RJ-45 copper connection and a fiber 1 Gb/s connection. The copper or fiber connection can be used, but not both at the same time. If the fiber connection fails, the copper connection automatically becomes active. Combo ports are also known as hybrid ports.

**confederation**
In BGP, a confederation is an AS that has been subdivided into smaller ASs called CMASs. A confederation appears to be a single AS to other ASs and is recognized only by other confederation members.

**control plane**
The portion of the telecommunications network that is involved with signaling and control, including the management of sessions and services. See also “c-plane” (p. 21) .

**CoS**
class of service
CoS is the degree of importance assigned to traffic. There are standard and premium classes of services. During queuing and forwarding, service points give preferential treatment to traffic that originates on elements configured for premium CoS.

**CPAM**
Control Plane Assurance Manager
A system that captures and displays 7701 CPAA IGP topology information. The CPAM and NFM-P products are integrated and share the platform resources.

**CPB**
Commissioning and Power Balancing

**CPE**

CPE can be expanded in two ways:

1. customer premises equipment

   Network equipment that resides on the customer’s premises.

2. customer provider edge

**CPG**
client protection group

**Cpipe**
A Cpipe, or circuit emulation VLL service, provides a point-to-point CEM service between users who connect to devices in an IP/MPLS network directly. The endpoints of a Cpipe uses CEM encapsulation.

**CPM**
control processing module
A CPM is in a device such as the 7750 SR that uses hardware filters to perform traffic management and queuing functions to protect the control plane.

**CPU**
central processing unit

**CRC**
cyclic redundancy check
CRC checks transmission errors applied to a block of information. CRC involves a bit string (computed from the data to transmit) associated with each transmitted block, and ensures the check on reception.

**credit control**
A mechanism that interacts with a subscriber account in real time, and controls or monitors the charges that are associated with service usage. Credit control checks to see if credit is available, reserves credit, deducts credit from a subscriber account when the service is completed, and refunds unused reserved credit.

**cron**
A time-based scheduling service in a UNIX-based OS.

**CSA**
Convergent Security Asset
A security solution package that offers single sign-on and access control mechanisms at different levels to provide a highly secure operating environment. The CSA includes an entry-level login and password mechanism.

**CSFB**
circuit switched fallback
CSFB allows UE in an LTE network to use non-LTE RAT for services, such as SMS, when the LTE network does not provide that service.

**CSFP**
compact small form factor pluggable
A type of SFP transceiver with two bidirectional channels in a conventional SFP module. See also “SFP” (p. 109) .

**CSG**
closed subscriber group
A closed subscriber group that identifies a group of subscribers who are permitted to access a group of cells which have restricted access. A CSG can consist of group of friends or employees that are allowed to connect to either a single small cell hosted by a residential customer or a group of small cells hosted by a business. A CSG ID is used to identify a unique group of subscribers. A CSG list is created based on input from the host of a single or group of small cells and operator. The CSG access list is referred to by the 9471 WMM to validate subscriptions at a CSG cell where it performs access or handover when UE connects to a small cell.

**CSM**
control switching module
A CSM is part of the 7705 SAR that uses hardware filters to perform traffic management and queuing functions to protect the control plane.

**CSNP**
complete sequence number PDU
A PDU sent by a designated router to ensure database synchronization.

**CSPF**
constrained shortest path first
CSPF is a component of constraint-based routing that uses a TED to find the shortest path through an MPLS domain that meets established constraints. The ingress router determines the physical path for each LSP by applying the CSPF algorithm to the TED information. Input to the CSPF algorithm includes topology link-state information learned from the IGP, LSP administrative attributes, and network resource attributes that are carried by IGP extensions and stored in the TED.
As CSPF considers each candidate NE and link for a new LSP, it accepts or rejects a specific path component based on resource availability and whether selecting the component violates policy constraints. The output of the CSPF calculation is an explicit route that consists of a sequence of router addresses. The explicit route is passed to the signaling component, which establishes forwarding states in the routers along the LSP.

**CST**
common spanning tree
The CST is the overall network spanning tree topology resulting from STP, RSTP, and/or MSTP calculations to provide a single data path through the network.

**CSU**
channel service unit
A CSU connects a digital phone line coming in from the phone company to network access equipment located on the customer premises. A CSU may also be built into the network interface of the network access equipment.

**CSV**
comma separated value
CSV is a way of recording parameters and values in text format that separates values with a delimiter, such as a comma or tab.

**CTg**
call trace geographic
Complete call trace data collection of call flow, geolocation, neighbor relation, and user experience data.

**CTP**
connection termination point

**customer**
In the NFM-P, a customer is the entity that pays for a network service, such as an IES, a VPLS, or a VPRN. The service is a means of transport for the application content, such as HSI or VoIP, that the customer offers to end users.

**CVLAN**
customer VLAN

**CWDM**
Coarse wavelength division multiplexing
CWDM is the method of combining multiple signals on laser beams at various wavelengths for transmission along fiber optic cables. The number of channels is fewer

than in dense wavelength division multiplexing, or “DWDM” (p. 37) , but more than in standard wavelength division multiplexing, or “WDM” (p. 130) .

**CWR8**
8–Channel colorless wavelength router card, 44 channel

**CWR8-88**
8–Channel colorless wavelength router card, 88 channel

## D

**DAPI**
Destination Access Point Identifier

**data-MDT**
data multicast distribution tree
A data-MDT is a tunnel for high-bandwidth source traffic through the P-network to interested PE routers. Data-MDTs do not broadcast customer multicast traffic to all PE routers in a multicast domain. Data-MDTs are only supported for VPRN services.

**DB**
database

**DCCA**
diameter credit-control application
A networking protocol for the diameter application that is used for real-time credit control of user services.

**DCE**
data communication equipment
A device that communicates with a DTE device in RS-232C communications.

**DCP**

DCP can be expanded in two ways:

1. data collection and processing
2. Distributed CPU Protection

   A control traffic rate limiting protection mechanism for the CPM/CFM that operates on the line cards (hence ‘distributed’). CPU protection protects the CPU of the node that it is configured on from a DOS/DDOS attack by limiting the amount of traffic coming in from one of its ports and destined to the CPM (to be processed by its CPU) using a combination of the configurable limits.

**DDN**
downlink data notification
A message sent from an SGW to an SGSN or 9471 WMM over the S11 or S4 interface when data is received from a UE. The DDN and DDN Ack alert the SGSN or 9471 WMM of the UE reachability and service requests.

**DDoS**
distributed denial of service

A DoS attack that occurs from more than one source at the same time. See also "DoS" (p. 34) .

**de-mux**
See "demultiplexer" (p. 31) .

**default SAP**
A SAP that forwards VLAN traffic with any encapsulation value. Default SAPs are indicated by the 4095 or * VLAN ID tag.

**degree-2**
A bidirectional network configuration from east to west or west to east.

**DEI**
drop eligible indicator
The DEI bit is a one-bit field in an Ethernet frame that indicates whether a frame can be dropped when traffic congestion occurs.

**demultiplexer**
A device that separates signals that have been combined as a single signal by a multiplexer for transmission over a communications channel.

**deprecate**
As a class evolves over releases, its API, methods, and parameters may change. As the old transitions to the new, both versions must be maintained for a period. To deprecate an API, method, class, or parameter, the older version is marked as deprecated, but continues to work.

**DES**
data encryption standard
An unclassified U.S. government-sanctioned encryption and decryption technology that uses 56-bit encryption, with 8-bit error detection.

**device**
A generic term for an NE such as a router, switch, or bridge; the term is typically used to describe the NE in a non-network context.

**DF**
don't fragment
A bit in an IPv4 header that controls the fragmentation of a datagram.

**DGE**
dynamic gain equalizer

**DHCP**
Dynamic Host Configuration Protocol
An Internet protocol to automate the configuration of computers that use TCP/IP. The DHCP can be used to automatically assign IP addresses, deliver TCP/IP stack configuration parameters such as the subnet mask and default router, and provide other configuration information such as the addresses for printer, time, and news servers.

**DHCP client**
An Internet host that uses DHCP to obtain configuration parameters, such as a network address, from a DHCP server.

**DHCP relay**
DHCP relay allows a router to intercept a DHCP broadcast packet and forward the packet to a specific DHCP server.

**DHCP relay agent**
A router used to interconnect DHCP clients with a DHCP server that is connected to another LAN segment or network. A DHCP relay agent can also be used to insert client circuit information.

**DHCP server**
A server that stores network addresses and delivers configuration parameters to DHCP clients.

**DHCP snooping**
DHCP snooping provides network security by monitoring and analyzing DHCP messages from hosts outside the managed network that can cause traffic attacks within the managed network. DHCP snooping builds and maintains a binding table that contains information such as MAC addresses and IP addresses that correspond to the hosts that are connected from outside the managed network.

**Diameter**
A base foundation protocol that provides transfer of Diameter messages, negotiation capabilities, routing capabilities, and error handling. Diameter is a type of AAA protocol.

**Diffie-Hellman key exchange**
A key agreement algorithm used by two parties to agree on a shared secret.

**Dijkstra**
Routing algorithm used by IS-IS and OSPF that uses the length of path to determine a shortest-path spanning tree. Sometimes also called SPF.

**DLCI**
data link connection identifier
A DLCI is a 10-bit routing address of the virtual circuit at the UNI or the NNI that identifies a frame as being from a specific PVC. DLCIs are used to multiplex several PVCs over one physical link.

**DM**
delay measurement
Ethernet delay measurement measures frame delay and frame delay variations by sending periodic frames to the peer “MEP” (p. 71) and receiving frames from the peer “MEP” (p. 71) during the diagnostic interval.

**DMM**
delay measurement message

**DNS**
domain name system
A system that translates host names to IP addresses.

**DNU**
do not use

**DoD**
downstream on demand
DoD is a type of LDP that allows LDP peers to request label bindings only for specific FECs, in order to reduce the amount of label information that is exchanged compared to LDP DU. See also “DU” (p. 36) and “LDP” (p. 63) .

**DOIC**
diameter overload indication conveyance

**DoS**
denial of service
A type of attack on a network that involves flooding the network with dummy data packets to render the network incapable of transmitting legitimate traffic.

**Dot1N**
802.1 level *N*
See “802.1D” (p. 9) , “802.1p” (p. 9) , “802.1Q” (p. 9) , “802.1w” (p. 9) , and “802.1X” (p. 9) .

**DP**
drop precedence
Attribute of a packet which affects the probability of the packet being dropped within a CoS.

**DPA**
diameter proxy agent

**DPD**
dead peer detection
A method that is used to detect a dead IKE peer by using IPsec traffic patterns.

**DPI**
deep packet inspection
A computer network packet inspection process that evaluates the data of a packet. The data is examined for protocol non-compliance and for intrusions such as viruses and spam. If the data passes inspection, the packet passes; otherwise, it is routed to a different destination.

**DPR**
disconnect peer request

**DR**
designated router

A DR is a PIM-enabled router that manages multicast stream delivery for a group of receiver hosts in a multicast network. DRs exchange information regarding multicast sources and dynamically adjust to changes in source availability.

**DRA**
Diameter routing agent
A functional element that ensures that all Diameter sessions established over reference points, such as the Gx, for a specific IP-CAN session, reach the same PCRF when there are multiple and separately addressable PCRFs that are deployed in a Diameter realm. The DRA tracks the status of PCRFs that are assigned to specific UEs and IP-CAN sessions across reference points, such as the Gx.

**DRC**
Disaster recovery center—a backup site.

**DRMP**
diameter routing message priority
The DRMP defines a mechanism that allows diameter nodes, such as the PGW, to indicate the relative priority of diameter transactions using the DRMP AVP. In cases where the DOIC is only run between the DRAs and the diameter servers, the DRA can use the DRMP AVP information to differentiate request message priorities when making throttling decisions when in overload.

**DRR**
deficit round robin
A DRR scheduler is designed to address the limitations of WRR scheduling by implementing a scheduling algorithm that is based on the bytes sent on an egress link. The DRR scheduling algorithm maintains a quantum value that defines the total number of credits for each CoS queue and a credit counter that is decremented each time a byte is taken from the queue for transmission. The purpose of the credit counter is to track the use of bandwidth by a CoS queue relative to the amount of bandwidth that has been allocated to the queue.

**DRX**
discontinuous reception
A system used in cellular networks to prolong “UE” (p. 123) battery life by dividing UE devices into paging channels that are only paged by the designated network devices.

**DS Lite**
Dual-Stack Lite
DS Lite allows an Internet service provider to omit the deployment of any IPv4 address to the customer's CPE. Only global IPv6 addresses are provided.

**DS-N**
digital signal - level *N*
A digital signaling rate of *N* Mb/s; for example, the DS-1 rate is 1.544 Mb/s.

**DSAP**
destination service access point

**DSC**
Dynamic Services Controller.
The DSC is a network component that acts as the PCRF in an LTE network.

**DSCP**
differentiated services code point
A six-bit value encoded in the type of service field of an IP packet header, which identifies CoS and the DP the packet receives.

**DSL**
digital subscriber line
A DSL is a single twisted pair that supports full-duplex transmission at a bit rate of 160 kb/s (144 kb/s for 2B+D data, 12 kb/s for framing and error correction, and 4 kb/s for the embedded operation channel).

**DSL module**
A module card that can be configured on the 7705 SAR-M/ME. The DSL module includes eight xDSL lines.

**DSLAM**
digital subscriber line access multiplexer
A DSLAM is multiplexing equipment that a telecom operator uses to provide DSL services to end users.

**DSU**
data service unit
A DSU adapts the physical interface on a DTE device to a transmission facility such as T1 or E1. The DSU is also responsible for signal timing.

**DTD**
document type definition
The DTD defines the document structure and legal elements for a set of XML code.

**DTE**
data terminal equipment
A device that communicates with a DCE device in RS-232-C.

**DTE**
data terminating entity

**DU**
downstream unsolicited
An MPLS LDP technique, where LSRs distribute bindings to LSRs that have not explicitly requested them.

**DUS**
do not use for synchronization

**DVD**
digital versatile disk
An optical digital disk that stores up to 4.7 GBytes of data. A DVD can be recorded on both sides and in dual layers.

**DVD-ROM**
digital versatile disk - read-only memory
A read-only DVD that is used to store data and software, as well as audio and video content.

**DWDM**
dense wavelength division multiplexing
In DWDM, the channels that are transported simultaneously over one fiber at different wavelengths without interaction, are closely spaced (100 GHz or below). Each channel is usually Time Division Multiplexed.

**dynamic host**
A host that is temporarily configured on the SAP. The NFM-P learns dynamic hosts when the DHCP lease populate function is enabled.

## E

**e-BGP**
See "EBGP" (p. 37) .

**E-CSCF**
emergency call session control function

**E-LSP**
EXP inferred LSP

**E-SNCP**
Electrical-Subnetwork Connection Protection

**E1**
A European standard for high-speed voice and data transmission at 2.048 Mb/s.

**E3**
A wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mb/s. E3 lines can be leased for private use from common carriers.

**EAP**
Extensible Authentication Protocol
EAP provides a generalized framework for different types of authentication methods. This allows access devices to hand off authentication packets to an authentication system, such as a RADIUS server, without knowing the authentication method used.

**EAS**
Ethernet Access Switch

**EBGP**
Exterior Border Gateway Protocol
A BGP session established between routers in different ASs. EBGPs communicate among different network domains.

**EBI**
EPS bearer ID

**EC**
Equipment controller

**eCCM-U**
enhanced core controller module
The eCCM-U is an eNodeB component that provides the backhaul interface, call processing, data switching, routing, alarms, and frequency/timing.

**eCEM-U**
enhanced channel element module
The eCEM-U is an eNodeB component that provides baseband signal processing and supports data, control, and timing interfaces to the “BTS” (p. 21) .

**ECGI**
E-UTRAN cell global identifier

**ECMP**
equal-cost multipath routing
Technique used by OSPF and IS-IS routing protocols to balance the load of Internet traffic.

**ECT**
equal cost tree
Algorithm as defined by 802.1aq where the shortest paths have to follow a subset of the equal cost shortest paths to any destination.

**ED**
Edge device

**EDFA**
Erbium doped fiber amplifier

**edge**
In the context of an NFM-P map, an object which links two vertex objects. Physical links and service tunnels are examples of edges.

**EDPS**
event-driven processing server
A server that is used by the 5750 SSC to access network equipment or mediate with other network management systems to access network equipment.

**EFM**
Ethernet in the First Mile
EFM refers to the IEEE Std 802.3ah-2004 standard, an amendment to the Ethernet standard. The EFM standard was approved by the IEEE Standards Board in June 2004, and officially published on 7 September 2004.
The EFM amendment deals with a set of additional specifications, allowing users to run the Ethernet protocol over previously unsupported media, such as single pairs of telephone wiring and single strands of single-mode fiber.

**EGP**
Exterior Gateway Protocol

A generic term for a routing protocol that is used to exchange routing information between two hosts in a network of ASs. An EGP is typically used between hosts on the Internet to share routing table information.

**Egress secondary shaper**
A control mechanism to prevent downstream packet overruns without affecting the class-based scheduling behavior on a port, typically on an HSMDA.

**eHRPD**
evolved high rate packet data
Connects the 3GPP2 HRPD access network to the 3GPP EPC IP environment through PMIP.

**EIC**
equipment ID code
A character, or group of characters, used to identify or name equipment.

**EIR**
excess information rate
The EIR is the excess bandwidth that a frame relay network attempts to carry for a given connection.

**EIS**
enhanced Internet service
EIS enhances the Internet service model by catering to the needs of QoS-sensitive applications by providing value-added Internet services that improve delivery performance.

**EJB**
Enterprise Java Beans
Used to describe a session bean, which is a Java object tied into system services to provide session management functions. EJB technology is the part of the Java server-side architecture.

**EM**
element manager

**EMG**
egress multicast group
A group of destination SAPs that receives packets in a single transmission. The advantage of an EMG is the elimination of packet loopbacks to multiple SAPs.

**eMLPP**
enhanced multi-level precedence and pre-emption
Specifies levels of precedence for call setup and continuity for HO.

**eMPS**
enhanced multimedia priority service
eMPS applies to first responders who are required to have priority treatment as per government mandates. In case of disasters resulting in network overload, signaling for emergency responders should not be dropped. The PGW sees the UE as the regular UE

in the initial attachment, but the PCRF later updates the eMPS status to the PGW through a bearer modification request.

**EMS**
element management system
An application that manages one or more NEs.

**eNB**
See “eNodeB” (p. 39) .

**encapsulation**
Encapsulation is the addition of information to the beginning and end of data. Encapsulation is used by layered network protocols as data moves from one stack down to the next. Header and trailer information is added to the data at each layer. Encapsulation is also used to bridge connections between different types of networks.

**eNodeB**
Evolved NodeB
The eNodeB is an enhanced BTS system for UE access to the LTE RAN network and LTE services in the 700 MHz spectrum. There are different hardware configurations available for the eNodeB, involving compact configuration (9412 eNodeB) or distributed configuration using remote radio heads (9926 DBS, also known as 9926 BBU). NFM-P customer documentation refers to the 9926 DBS and 9412 eNodeB collectively as the eNodeB.

**ePC**
evolved packet core
The core network in the LTE and SAE system. The ePC provides the overall control of the UE and establishment of the bearers. The main logical NEs of the ePC are the PGW, SGW, and MME.

**ePDG**
evolved packet data gateway
The ePDG is part of the SAE that interfaces with untrusted non-3GPP networks that require secure access, such as Wi-Fi. The ePDG secures the data transmission with UE connected to the EPC, and acts as a secure termination node for IPsec tunnels that are established with the UE.

**Epipe**
A type of VLL service that provides a point-to-point Ethernet service. One endpoint of an Epipe uses Ethernet encapsulation, and the other endpoint uses Ethernet, ATM, or frame relay encapsulation. Also known as an Ethernet VLL service.

**EPS**

EPS is expanded two ways:

1. equipment protection switching
2. evolved packet system

   The LTE and SAE together, comprising both an evolved core network and an evolved radio access network.

**EPT**
Engineering and Planning Tool

**E-RAB**
E-UTRAN radio access bearer
The concatenation of an S1 bearer and the corresponding radio bearer. See 3GPP TS23.401.

**ERP**
Ethernet ring protection
Ethernet Ring Protection (ERP) as specified in ITU-T G.8032, is a protection mechanism for Ethernet ring topologies that provides a resilient Ethernet network. ERP provides sub-50ms protection and recovery switching for Ethernet traffic in a ring topology, and, at the same time, ensures that loops are not formed at the Ethernet layer.

**ERPS**
Ethernet ring protection switching

**ESI**
Ethernet segment identifier

**ESM**
See “RSM” (p. 102) .

**ESNCP**
Electrical sub-block network connection protection

**ESP**
encapsulating security payload
A member of the IPsec protocol suite. ESP is a transport-layer protocol that provides data confidentiality, origin authentication, integrity checking, and replay protection. The communicating systems use a shared key to encrypt and decipher data. ESP is similar to “AH” (p. 12) , but provides IP header protection only in tunnel mode.

**ESS**
extended service switch
A network switch, for example, the 7450 ESS, that supports the creation of Ethernet services such as VPLS and VLL.

**EtherType**
A field in the Ethernet frame header that is used to indicate the version of Ethernet protocol.

**ETR**
extended temperature range

**eUTRAN**
evolved Universal Terrestrial Radio Access Network
The eUTRAN consists of eNodeBs that provide the user-plane and control-plane protocol terminations towards the UE. The eNodeBs can be interconnected with each other using the X2 interface. The eNodeBs are connected to the EPS through the S1 interface.

**eVOA**
electrical variable optical attenuator

**EVPL**
Ethernet virtual private line
An EVPL is a data service, defined by the Metro Ethernet Forum that provides a point-to-point Ethernet connection between UNIs.

**EVPN**
Ethernet virtual private network
EVPN is an Ethernet Layer 2 VPN bridging solution that enables you to connect a group of dispersed customer sites that uses BGP as the control-plane for MAC address signaling over the core.

**EXP**
experimental field
A field in an IP packet header that is reserved for experimental use.

## F

**FA**
foreign agent
A router on the visited network of an MNN which provides routing services to the MNN while registered. The FA detunnels and delivers datagrams to the MNN that were tunneled by the HA of the MNN.

**failover**
Failover is the process of changing the roles of a redundant system, for example, when the standby database takes over the role of a failed active database.

**fallback**
Fallback is the process of reversing configuration deployments using the activation manager.

**Fast Ethernet**
A LAN transmission standard that provides a data rate of 100 Mb/s.

**fault**
A fault is a failure or defect in a network, causing the network, or part of the network, to malfunction.

**FC**
flow control
Flow control is the procedure that shuts down transmission when a receiving station is unable to store the data it is receiving.

**FC**
forwarding class
See “forwarding class” (p. 44) .

**FCAPS**

FCAPS is the acronym for a broad categorization of network and service management activities that includes:

- fault management
- configuration management
- accounting/administration management
- performance management
- security management

**FCC**
fast channel change
FCC is an HDTV function that provides bursts of cached unicast traffic via separate video servers to provide channel changes in under a second.

**FD**
frequency diversity
Two ODUs simultaneously transmit packets on different frequencies. On the receive side, two ODUs receive the packets on two frequencies but only the best signal, as determined by factors such as BER and loss of signal, is processed by the 9500 MPR.

**FDB**

FDB is expanded two ways:

1. filtering database
2. forwarding database

**FDL**
facilities data link
Used in ESF to support the communication of network information in the form of in-service monitoring and diagnostics.

**FDN**
fully distinguished name

**FEC**
forwarding equivalency class
A group of IP packets that are forwarded in the same manner, for example, over the same path, with the same forwarding treatment.

**FIB**
forwarding information base
FIB is the set of information that represents the best forwarding information for a destination. A device derives FIB entries from the reachability information held in the RIB, which is subject to administrative routing.

**FIC**
frame ID code
A field in a channel frame that identifies the position of the frame in the frame sequence.

**FIPS**
Federal Information Processing Standards
A cryptographic certification standard that defines the requirements for products to become FIPS-140-2 certified.

**flash memory**
A rewritable memory chip that retains its content without power.

**flow description**
A flow description defines the filters for service data flow, such as the source and destination IP address, port numbers, and the protocol.

**FM**
fault management

**FF**
Flex framer

**flowspec**
The use of BGP to distribute traffic flow specifications (flow routes) throughout a network. A flow route carries the description of a flow, such as source IP address, destination IP address or TCP/UDP port number, and a set of actions to take on packets that match the flow.

**FOADM**
Fixed optical add/drop multiplexer/multiplexing

**forwarding class**
A forwarding class, also called a CoS, provides to NEs a method to weigh the relative importance of one packet over another in a different forwarding class. Each forwarding class is important only in relation to other forwarding classes.
Queues are created for a specific forwarding class to determine the manner in which the queue output is scheduled into the switch fabric and the type of parameters the queue accepts. The forwarding class of the packet, along with the in-profile or out-of-profile state, determines how the packet is queued and handled (the per-hop behavior at each hop along its path to a destination egress point).

**FPE**
Forward Path Extension
FPE refers to the functionality where traffic is passed internally from egress to ingress for the purpose of traffic pre-processing.

**FPGA**
field programmable gate array
A high density programmable hardware device capable of supporting different applications

**Fpipe**
A type of VLL service that provides a point-to-point frame relay service between users over an IP/MPLS network. Both endpoints of an Fpipe use frame relay encapsulation. An Fpipe connects users through frame relay PVCs. An Fpipe is also known as a frame relay VLL service.

**FQDN**
fully qualified domain name

**FR**
frame relay
A standard for high-speed data communication that offers transmission speeds of at least 2.048 Mb/s. The main application of FR is LAN interconnection.

**FRF.5**
Frame Relay/ATM PVC Network Interworking Implementation Agreement
A standard that provides network interworking function, allowing frame relay users to communicate over an intermediate ATM network.

**FRR**
fast reroute

**FRU**
Field replaceable unit
An FRU is a component that you can replace on-site with minimal or no service interruption. A fan unit is an example of an FRU.

**FT**
fault tolerance or fault-tolerant
Fault tolerance enables a system to continue operating properly in the event of the failure of some of its components. When the operating quality decreases at all, the decrease is proportional to the severity of the failure.
TCP fault tolerance allows reliable two-way network communication using links that may be imperfect or overloaded. It does this by requiring the communication endpoints to expect packet loss, duplication, reordering and corruption, so that these conditions do not affect data integrity.

**FTP**
File Transfer Protocol
FTP is the Internet standard client-server protocol for transferring files from one computer to another. FTP generally runs over TCP or UDP.

**FUA**
fixed uplink allocation

**FUI**
final unit indication
The FUI indicates that the given quota is the final quota from the server.

**fVOA**
fast variable optical attenuator

**FXO**
Foreign Exchange Office

**FXS**
Foreign Exchange Subscriber

## G

**Ga**
The interface between the “PGW” (p. 92) and the “OFCS” (p. 84) .

**GARP**
Generic Attribute Registration Protocol (formerly Group Address Registration Protocol)
A LAN protocol that defines procedures by which end stations and switches can register and de-register attributes (such as network identifiers or addresses) with each other. By this means, every NE has a record or list of all the other NEs that can be reached at any given time.

**GBE**
Gigabit Ethernet
A transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs) that provides a data rate of one billion bits (one Gigabit) per second. Gigabit Ethernet is defined in the IEEE 802.3 standard and is currently used as the backbone in many enterprise networks.

**GBEH**
Gigabit Ethernet Hardened
The 1830 PSS-1 GBEH is a temperature-hardened edge device that provides up to 10 GBE services over an 11G optical channel.

**GBR**
guaranteed bit rate
The GBR indicates the guaranteed number of bits delivered to the network within a period of time.

**generic NE**
generic network element
An NE, typically a non-Nokia device, for which the NFM-P provides limited management support using SNMP.

**GERAN**
GSM Edge Radio Access network
Supports enhanced data rates for global evolution (EDGE), and provides both the radio coverage and intelligent network services. It consists of the Base Transceiver Station (BTS), the Base Station Controller (BSC), the Transcoding and Rate Adaptation Unit (TRAU), a key component in handling and routing information, and the Operation and Maintenance Center (OMC-B).

**GGSN**
gateway GPRS support node
GGSN provides network access to external hosts that need to communicate with mobile subscribers. GGSN is the gateway between the GPRS wireless data network and other external PDNs such as radio networks, IP networks, or private networks.

**GIF**
graphics interchange format
GIF is a graphics file format that supports up to 256 colors.

**Gig**
gigabit
Approximately 1 000 000 000 bits. The exact number is $2^{30}$, or 1 073 741 824 bits. The term is used to mean either value.

**Gig Ethernet**
See "Gigabit Ethernet" (p. 46) .

**Gigabit Ethernet**
An Ethernet interface with a peak data rate of 1000 Mb/s.

**GigE**
See "Gigabit Ethernet" (p. 47) .

**Global MEG**
Global Maintenance Entity Group
A Global MEG is a virtual object that contains more than one MEG. See also "MEG" (p. 71) .

**GMPLS**
generalized multi-protocol label switching
The GMPLS protocol reroutes traffic dynamically around a failure. After a failure in the network is fixed, the connection is returned to its original route automatically, or on-demand, depending on the connection settings.

**GMPLS-UNI**
generalized multi-protocol label switching-user network interface
GMPLS-UNI permits dynamic provisioning of optical transport connections between IP routers and optical network elements in order to reduce the operational time and administrative overhead required to provision new connectivity. See also "MPLS" (p. 74) .

**Gn**

Gn is:

- the interface between the "PGW" (p. 92) and the "SGSN" (p. 109)
- the interface between "GSN" (p. 49) s within a "PLMN" (p. 94)

**GNE**

GNE can be expanded in two ways:

1. See "generic NE" (p. 46) .
2. Gateway Network Element
   The NFM-P can manage a network consisting of one or more 1830 PSS NEs while being connected to a single 1830 PSS NE called the GNE. The GNE manages the connectivity to all other 1830 PSS NEs in the network.

**GNI**
Gigabit Ethernet Network Interface

**GNSS**
global navigation satellite system
A satellite navigation system is a system of satellites that provides autonomous geo-spatial positioning with global coverage. It allows small electronic receivers to determine their location (longitude, latitude, and altitude) to high precision, using time signals transmitted along a line of sight by radio from satellites. The signals also allow the electronic receivers to calculate the current local time to high precision, which allows time synchronization. A satellite navigation system with global coverage may be termed a global navigation satellite system or GNSS.

**golden configuration**
A golden configuration is an NE that is configured to be a standard against which other NE configurations can be compared.

**Gp**

Gp is:

- the interface between the "PGW" (p. 92) and the "SGSN" (p. 109)
- the interface between "GSN" (p. 49) s in different "PLMN" (p. 94) s

**GPON module**
gigabit passive optical network module
A module card that can be configured on the 7705 SAR-M/ME. The GPON module is a 1-port optical network terminal which serves as an Ethernet connection point for transmitting data over a GPON network.

**GPRS**
General Packet Radio Service
A mobile data service extension to the GSM system. It is often described as "2.5G". See 3GPP TS43.064 and TS23.060.*

**GPS**
global positioning system

**GPV**
get parameter values
Type of TR-069 RPC method.

**GQP**
Generic QoS Profile

**GR**
graceful restart
Many Internet routers implement a separation of control and forwarding functions. These routers can continue to forward data while the control software is restarted or reloaded. This function is called graceful restart. A successful graceful restart requires the use of a GR helper.

**GR helper**
graceful restart helper
A GR helper is a neighboring router that is configured to cooperate during a graceful restart. The GR helper monitors the network topology for any changes and, if there are none, advertises that the router performing the graceful restart is still active.

**Gr interface**
generic requirement interface
The Gr interface is a General Packet Radio Service which is located between the Serving General Packet Radio Service Support Node and the Home Location Register.

**GRE**
generic routing encapsulation
A protocol for the encapsulation of an arbitrary network-layer protocol over another arbitrary network-layer protocol.

**GRT**
global route table

**GSM**
Global System for Mobile communications; a type of 2G network.

**GSMP**
General Switch Management Protocol
GSMP is an ATM and TCP/IP protocol designed to control a label switch. This protocol allows a controller to establish and release connections across the switch. For example, adding and deleting leaves on a multicast connection, managing switch ports, and requesting configuration information and statistics.
ANCP is an extension of GSMP.

**GSN**
GPRS support node
A GSN is an NE that supports the use of GPRS in a GSM core network.

**GTP**
GPRS tunneling protocol

GTP is the protocol between GSNs in the UMTS/GPRS backbone network. GTP is the standard that specifies interfaces for the GPRS within the 3GPP system:

- the Gn and Gp interfaces of the GPRS
- the Iu, Gn, and Gp interfaces of the UMTS system.

**GTP-C**
GTP-control plane
This protocol tunnels signaling messages between the "SGSN" (p. 109) and "MME" (p. 73) over the S3 interface, between the "SGSN" (p. 109) and "SGW" (p. 109) over the S4 interface, between the "SGW" (p. 109) and "PGW" (p. 92) over the S5 /S8interface, and between "MME" (p. 73) s over the S10 interface. See 3GPP TS 23.401 Section 5.1.1.*

**GTP-U**
GTP-user plane
This protocol tunnels user data between the eNodeB and the "SGW" (p. 109) , as well as between the "SGW" (p. 109) and the "PGW" (p. 92) in the backbone network. GTP encapsulates all end-user IP packets. See 3GPP TS23.401 Section 5.1.2.1.*

**GUI**
graphical user interface
A GUI is a computer user interface that incorporates graphics to make software easier to use.

**GVRP**
GARP VLAN registration protocol
GVRP is a standards-based Layer 2 network protocol for automatic configuration of VLAN information on switches.

**Gx**
The Diameter reference point between the "PCRF" (p. 91) and the "PCEF" (p. 90) on the "PGW" (p. 92) that transfers policy and charging rules from the "PCRF" (p. 91) to "PCEF" (p. 90) .

**Gy**
The reference point between the "PGW" (p. 92) and the "OCS" (p. 84) .

## H

**H-VPLS**
hierarchical virtual private LAN service

**HA**

HA is expanded two ways:

1. high-availability
2. home agent

   A router on the home network of an MNN, which tunnels datagrams for delivery to the MNN when it is away from home, and maintains current location (IP address) information for the MNN.

**HCM**
high capacity multiplexing
HCM is a rate adaption and sub-rate multiplexing scheme that provides a bandwidth granularity of 800bit/s throughout a network. HCM multiplexes multiple V.24 lines into a single G.703 time slot.

**HDD**
hard disk drive

**HDLC**
high-level data link control

HDLC is a bit-oriented synchronous data link layer protocol. It specifies a data encapsulation mode on synchronous serial links using frame characters and checksums.

**HIP**
horizontal integration protocol
A mechanism for connecting external systems to the NFM-P. HIP supports network discovery, alarm forwarding, and alarm management.

**HI component**
horizontal integration component

**HMAC**
key-hash message authentication code
HMAC is a type of message authentication code that is calculated using MD5 and a secret key. It simultaneously verifies the data integrity and the authenticity of a message. The resulting algorithm is termed HMAC-MD5 or HMAC-SHA-1.

**HO**
handover

**HO-ODUk**
The higher-order ODU (HO-ODU) transparently carries several multiplexed lower-order ODUs.

**Hop**
The number of hops in a path indicates the number of full or fractional links a path traverses to get from source to destination. Each link is one hop.

**host**
A host is a device that has at least one static or dynamic IP address. The term typically applies to an end-user device, such as a PC, VoIP phone, or set-top box, rather than an NE in a transport network.

**HPCFAP**
high power connection fuse and alarm panel

**Hpipe**
A type of VLL service that provides point-to-point HDLC service over an MPLS network.

**HQoS**
hierarchical quality of service
HQoS provides the ability to perform rate limiting across multiple queues from multiple SAPs.

**HSB**
hot standby
One ODU transmits or receives packets on a single frequency. A second ODU is in standby mode and takes over if the other ODU fails.

**HSDPA**
high speed data-link packet access

**HSGW**
HRPD service gateway
The HRPD service gateway is in HRPD network, and provides interworking between the HRPD and ePC networks. The HSGW connects to the PGW by the S2a reference point.

**HSI**
high-speed Internet access
HSI is a broadband Internet access service that is typically part of a triple play service.

**HSMDA**
high scale Ethernet MDA
The HSMDA is an MDA for the 7450 ESS and 7750 SR. The HSMDA extends subscriber and service density capabilities of first and second generation IOMs by adding an MDA level of ingress and egress queues, shapers, and schedulers.

**HSPA**
high-speed packet access

**HSS**
home subscriber server
The HSS is a user database that supports the IMS network entities that handle calls. It contains subscriber profiles, performs authentication and authorization of the user, and can provide information about the subscriber's location and IP information.

**HSU**
high capacity subscriber unit

**HTML**
hypertext markup language
Language for writing hypertext documents, often for use in a web environment.

**HTTP**
Hypertext Transfer Protocol
A set of rules for exchanging text, graphics, sound, video, and other multimedia files on the Web.

**HTTP POST**
In HTML, you can specify a GET or POST submission method for a form. The method is specified inside a FORM element using the METHOD attribute. The difference between METHOD=”GET” (default) and METHOD=”POST” is primarily defined by form data encoding.

**HTTPS**
Secure Hypertext Transfer Protocol
A protocol built into a Web browser that provides encryption and decryption of Web page requests and responses. Also known as HTTP over SSL.

**HVPLS**
hierarchical virtual private LAN service

**hybrid port**
See “combo port” (p. 27) .

## I

**I-component**
An S-VLAN component with PIP

**I-PMSI**
inclusive provider multicast service interface

**I-SID**
I-component service instance identifier

**I-TAG**
service instance TAG

**I-VPLS**
I-component VPLS (or I-SID VPLS)

**I-VSI**
I-component virtual switch instance. Also referred to as an I-Site.

**I/O**
input/output
Connections between a system and its controlled devices (output) and incoming statuses (input).

**I/O module**
See “IOM” (p. 56) .

**IB-RCC**
In-band ring control connection

**IBGP**
Interior Border Gateway Protocol
IBGP is a type of BGP used within a single AS. IBGP is a protocol for exchanging routing information between gateways within an autonomous network. The routing information can then be used by IP or other network protocols to specify how to route packets.

**ICAP**
Internet Content Adaptation Protocol
ICAP is a protocol defined in the IETF RFC 3507 that provides simple object-based content processing for HTTP services. An ICAP client passes an HTTP message to an ICAP server that processes the message and sends a response to the client. A typical ICAP function is to enable parental control of Internet content viewed by children.

**ICB**
inter-chassis backup

**ICE**
in case of emergency

**ICMP**
Internet Control Message Protocol
ICMP is a protocol that sends and receives the control and error messages used to manage the behavior of the TCP/IP stack. ICMP is defined in RFC 792.

**ICR**
inter-chassis redundancy
ICR provides a baseline requirement for providing stateful redundancy on broadband subscriber management equipment, such as routers, gateways, and remote access servers. The redundancy mitigates against network outages and protects routers against link and chassis failures.

**ID**
identifier or identification

**IdP**
identity provider
IdP is responsible for acting as the access management authority for SSO-enabled applications and their users.

**IE**
information element
An element of a signaling message whose contents are for a specific signaling purpose

**IED**
intelligent electronic device
A packet-based remote monitoring and control device used in “SCADA” (p. 106) networks

**IEEE**
Institute of Electrical and Electronics Engineers

**IES**
Internet enhanced service
IES is a routed connectivity service in which a host communicates with an IP router interface to send and receive Internet traffic. An IES has one or more logical IP router interfaces, each with a SAP that acts as the access point to the network. IES allows customer-facing IP interfaces to participate in the same routing instance that is used for core network routing. The IP addressing scheme for a customer must be unique among the provider addressing schemes in the network and possibly in the entire Internet. The usable IP address space may be limited. A portion of the service provider address is reserved for service IP provisioning and allows administration by a separate but subordinate address authority.

**IETF**
Internet Engineering Task Force
The IETF is the organization that manages the standards and specifications for IP and related protocols.

**IGH**
interface group handler

IGH is a fate-sharing group that provides the ability to group multiple IP links and POS links so that if a specified number of links go out of service for any reason, the rest of the links in the IGH also go out of service and can be rerouted to an alternate path.

**IGMP**
Internet Group Management Protocol.
IGMP is an IP extension that hosts use to report their multicast group membership to neighboring multicast routers.

**IGMP snooping**
IGMP snooping enables a device that relays an IGMP packet to read the IGMP message and thus identify hosts that are members of multicast groups. The device forwards the returning multicast packets to only the hosts in the multicast group.

**IGP**
Interior Gateway Protocol
Generic term applied to any protocol used to propagate network reach and routing information within an AS.

**IGP administrative domain**
An IGP administrative domain is a collection of routers under one administrative entity that cooperates by using a common IGP (such as OSPF). Routing between IGP administrative domains is done with an inter-AS or interdomain EGP, such as BGP-4.

**IKE**
Internet key exchange
Protocol used to establish a security association in the IPsec protocol suite using the Diffie-Hellman Key exchange to establish a shared secret session.
IKE is an IPsec standard protocol used to ensure security for VPN negotiation and remote host or network access. Specified in IETF Request for Comments (RFC) 2409, IKE defines an automatic means of negotiation and authentication for IPsec SAs. IKE protocol ensures security for SA communication without the preconfiguration that would otherwise be required.

**ILA**
in-line amplifier

**ILM**
incoming label map

**ILMI**
interim local management interface
An interim standard defined by the ATM Forum that allows UNI management information to be exchanged between an end user and a public or private network, or between a public network and a private network, including setting and capturing physical layer, ATM layer, virtual path, and virtual circuit parameters on ATM interfaces. ILMI uses SNMP messages without UDP and IP, and organizes managed objects into MIBs.

**IMA**
inverse multiplexing over ATM

A cell-based protocol where an ATM cell stream is inverse-multiplexed and de-multiplexed in a cyclical fashion among ATM-supporting paths to form a higher bandwidth logical link, where the logical link concept is referred to as an IMA group.

**IME**
interface management entity
Software components that execute the ILMI protocol.

**IMEI**
international mobile equipment identity
A unique number that is allocated to each mobile station. It is implemented by the mobile station manufacturer. See 3GPP TS 22.016.*

**IMEISV**
international mobile equipment identifier and software version
A unique number that is allocated to each mobile station. It is implemented by the mobile station manufacturer. The software version number identifies the software version number of the mobile equipment.

**IMM**
integrated media module
A circuit board that uses the same chassis card slots as an IOM, but combines IOM 3 and high-bandwidth MDA functions in one unit. The IMM does not accept plug-in MDAs because the MDA functions are built into the IMM.

**IMPM**
ingress multicast path management

**IMS**
Internet protocol multimedia subsystem
An architectural framework for delivering Internet Protocol (IP) multimedia services via UTRAN and E-UTRAN. See 3GPP TS23.228 and TS23.406.*

**IMSI**
international mobile subscriber identity
A unique number associated with each mobile phone user. It is stored in the SIM inside the phone and is sent by the phone to the network. It is primarily intended for obtaining information on the use of the PLMN by subscribers. It is also used for other functions, such as to compute the Paging Occasions (PO) in LTE. See 3GPP TS22.016 and TS23.003.*

**Interlaken**
Interlaken is a narrow, high-speed, channelized chip-to-chip interface.

**intermediate system**
A device such as a router that forwards traffic between end systems.

**IOM**
input/output module

A circuit board that contains two independent data paths, with each path connected to an MDA. IOMs implement queuing and IP and MPLS functions. IOMs are available in several variants, such as the IOM 2 and IOM 3, that provide enhancements to the original IOM functions.

**IP**
Internet Protocol
IP is the network layer of the TCP/IP protocol suite. It is a connectionless, best-effort packet-switching protocol defined by the IETF.

**IP precedence**
A three-bit field in an IP packet header that specifies the level of service a packet is to receive in a network. IP precedence bits are the least significant bits of the DSCP field.

**IP-CAN**
IP connectivity access network
The IP-CAN defines the network that connects an IMS subscriber to IMS services. Typically, the IP-CAN is a GPRS that is supported by GERAN or UTRAN functions.

**IPCC**
Internet Protocol Communication Channel

**IPCP**
IP control protocol
IPCP assigns DNS and NBNS addresses to the UE.

**IPDR**
Internet Protocol Detail Record
An IPDR is a type of data record that contains information about IP service usage and traffic flows. The information in a record is typically used by an OSS for purposes such as billing and traffic analysis.

**IPFIX**
Internet Protocol Flow Information eXport
IPFIX is an IETF standard that defines how IP flow information is to be formatted and transferred from a flow exporter, such as a managed NE, to a flow collector, such as a “NFM-P C flowd auxiliary server” (p. 81).

**Ipipe**
A type of VLL service that provides point-to-point IP connectivity and allows service interworking between different Layer 2 technologies. One endpoint of an Ipipe uses Ethernet encapsulation and the other endpoint uses Ethernet, ATM, frame relay, cHDLC, or PPP encapsulation. An Ipipe is also called an IP interworking VLL service.

**IPsec**
Internet protocol security
A structure of open standards to ensure private and secure communication over IP networks using cryptographic security services.

**IPTV**
Internet-based television transmission

**IPv4**
Internet Protocol version 4
The version of IP in use since the 1970s. IPv4 addresses are 32 bits. IPv4 headers vary in length and are at least 20 bytes.

**IPv6**
Internet Protocol version 6
The version of IP that succeeds IPv4. IPv6 addresses are 128 bits. IPv6 headers are 40 bytes.

**IRAT**
inter-radio access technology
IRAT refers to functions, particularly “SON” (p. 112) functions, that interface between radio technologies such as “LTE” (p. 67) and “UTRAN” (p. 124) .

**IRI**
intercept related information
Data about the targeted communication event, including the destination of a voice call, the source of a call, and the time of the call.

**IRICC**
intercept related information and content of communication
Data about the call and the data containing the call content.

**IS**
See “intermediate system” (p. 56) .

**ISID**
Service Identifier

**IS-IS**
intermediate system to intermediate system
IS-IS is an ISO standard link-state routing protocol. Integrated IS-IS allows IS-IS to be used for route determination in IP networks.

**ISA**
integrated services adapter
An ISA is an MDA for the 7450 ESS and 7750 SR. As a resource adapter, there are no external interface ports on the ISA. Any IOMs on a system in which the ISA is installed are used to switch traffic internally to the ISA.

**ISA-AA**
integrated services adapter - application assurance
ISA-AA is an application assurance function that is configured for 7450 ESS and 7750 SR ISAs. See “AA” (p. 10) and “ISA” (p. 58) .

**ISA-IPsec**
integrated services adapter - IP security
ISA-IPsec is a IP security function that is configured in the for 7450 ESS and 7750 SR ISAs. On an NE, the ISA-IPsec acts as a concentrator to gather and terminate encrypted

IPsec tunnels on an IES or VPRN service. This allows a network provider to offer a secure global service when the hosts are in an uncontrolled or unsecure part of a network.

**ISA-L2TP/LNS**
integrated services adapter - L2TP network server
ISA-LNS is a L2TP network server function that is configured on the 7450 ESS and 7750 SR. Any IOMs on a system in which the ISA-LNS is installed are used to switch traffic internally to the ISA-LNS.

**ISA-NAT**
integrated services adapter - network address translation
ISA-NAT is a NAT function that is configured on 7450 ESS and 7750 SR ISAs. See "NAT" (p. 79) and "ISA" (p. 58) .

**ISA-TMS**
integrated services adapter - threat management system
The ISA-TMS is a 7750 SR MDA.

**ISA-WLAN**
integrated services adapter - wireless local area network
The ISA-WLAN is a WLAN function that is configured for 7450 ESS and 7750 SR ISAs. See "WLAN GW" (p. 131) and "ISA" (p. 58) .

**ISC**
integrated services card

**ISL**
inter-switch link

**ISO**
International Standards Organization

**ISSU**
in-service software upgrade

**IST instance**
internal spanning tree instance
The IST instance determines and maintains the CST topology between MSTP switches that belong to the same MSTP region. The IST is a CST that only applies to MSTP region switches while, at the same time, the IST represents the region as a single spanning tree bridge to the network CST.

**IT**
information technology

**ITL**
Interleaver

**ITU**
See "ITU-T" (p. 59) .

**ITU-T**
International Telecommunication Union - Telecommunication Standardization Sector

**IWF**
interworking function
IWF provides seamless packet transmission between two protocol stacks. For example, IWF can connect an ATM endpoint with a frame relay endpoint using mappings between the two protocol stacks.

## J

**J0 byte**
The J0 byte refers to the numeric value for a SONET section trace to verify the physical connectivity of data links. The J0 byte traces the origin of an STS frame as it travels across a SONET network. The value for the J0 byte parameter is inserted continuously at the source and is checked against the value expected by the receiver. After the data links have been verified, they can be grouped to form a single traffic engineering link.

**JAAS**
Java authentication and authorization service
A set of packages that enable services to authenticate and enforce access controls on users.

**Java**
An object-oriented programming language that creates portable code to support interaction among different objects.

**Java EE**
Java Enterprise Edition
A set of services, APIs, and protocols that provide the functions to develop multi-tiered, web-based application components. Java EE is overseen by a partnership of enterprise software and computer vendors, and is available for a range of platforms.

**JDBC**
Java Database Connectivity
An application-programming interface that has the same characteristics as Open Database Connectivity, but is specifically designed for use by Java database applications.

**JMS**
Java Message Service
JMS is an API that combines Java technology with enterprise messaging. The JMS API defines a common set of interfaces for creating applications using reliable asynchronous communication among components in a distributed computing environment. The applications are portable to different enterprise systems.

**JNLP**
Java Network Launching Protocol
JNLP enables an application to be launched on a client desktop by using resources that are hosted on a remote web server. Java Plug-in software and Java Web Start software

are considered JNLP clients because they can launch remotely hosted applets and applications on a client desktop.

**JRMP**
Java Remote Method Protocol
A proprietary wire-level protocol that transports Java RMI.

**JVM**
Java virtual machine
A software abstraction layer that enables Java software to run on any processor architecture.

## K

**KCI**
key capacity indicator

**keystore**
A Java security framework class that represents an in-memory collection of keys and trusted certificates.

**KPI**
key performance indicator
A statistic counter used to monitor network performance.

## L

**L**
line port

**L-LSP**
label only inferred LSP

**L0**
Optical layer 0
The optical layer 0 comprises of the OCH, OTU, or ODU trails between WDM or photonic network elements.

**L1**
Optical layer 1
The optical layer 1 comprises of the optical cross connection system between OCS or switching network elements.

**L1**
Layer 1
The physical layer of the OSI model that includes network hardware and physical cabling required to transmit raw bits and perform requests from the data link layer.

**L2**
Layer 2

The data link or MAC layer of the OSI model. In networking, it is a communications protocol that contains the physical address of a client or server station that is inspected by a bridge or switch.

**L2PT**
Layer 2 protocol tunneling
L2PT allows L2 PDUs to tunnel through a network.

**L2TP**
Layer 2 Tunneling Protocol
L2TP is a session-layer protocol that extends the PPP model by allowing L2 and PPP endpoints to reside on different devices that are interconnected by a PSN. L2TP extends the PPP sessions between the CPE and PPP/L2TP termination point (LNS), via an intermediate LAC. See also "LNS" (p. 65) and "LAC" (p. 61) .

**L3**
Layer 3
The network layer of the OSI model. In networking, it is a communications protocol that contains the logical address of a client or server station that is inspected by a router, which forwards the address through the network. L3 contains a type field so that traffic can be prioritized and forwarded based on the message type as well as the network destination.

**LAC**
L2TP access concentrator
The LAC is the initiator of an L2TP tunnel. See also "LNS" (p. 65) and "L2TP" (p. 62) .

**LACP**
Link Aggregation Control Protocol
LACP is used to detect whether all local members of a LAG are physically connected to the remote ports that are part of the far end of the LAG.

**LACPDU**
link aggregation control protocol data unit

**LAG**
link aggregation group
A LAG increases the bandwidth available between two NEs by grouping up to eight ports into one logical link. The aggregation of multiple physical links allows for load sharing and offers seamless redundancy. If one of the links fails, traffic is redistributed over the remaining links. Up to eight links can be supported in a single LAG, and up to 64 LAGs can be configured on a device.

**LAI**
location area identity
The LAI consists of the PLMN and LAC.

**LAIS**
line alarm indication signal
A SONET signal that indicates a general line fault.

**LAN**
local area network
A LAN is a group of computers or associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area, for example, within an office building.

**Layer 2**
See “L2” (p. 61) .

**Layer 3**
See “L3” (p. 62) .

**LBM**
loopback message
A loopback message is generated by a “MEP” (p. 71) to a peer “MEP” (p. 71) or an intervening “MIP” (p. 72) .

**LB-VM**
load balancer VM

**LCP**
Link Control Protocol
LCP establishes, configures and tests data-link Internet connections before establishing communications over a point to point link.

**LD**
Line driver

**LDAP**
Lightweight Directory Access Protocol
LDAP is a networking protocol for querying and modifying directory services that run over TCP/IP.

**LDP**
Label Distribution Protocol
LDP is a signaling protocol used for MPLS path setup and teardown. An LDP is used by LSRs to indicate to other LSRs of the meaning of labels used to forward traffic. LDP is defined in RFC 3036. See also “DoD” (p. 34) and “DU” (p. 36) .

**lease**
For DHCP, the amount of time that a specific IP address is valid for a computer.

**LED**
light-emitting diode

**LER**
label edge router
An LER is a router at the edge of a service-provider network that forwards IP packets using LSPs.

**level**
In the IS-IS link-state protocol, level indicates the type of adjacency that can be formed between routers. Routers are assigned a capability for level 1, level 2, or both level 1

and 2. Level 1 routers can form adjacencies with other level 1-capable routers, and forward traffic within an area. Level 2 routers can form adjacencies with level 2-capable routers, and forward traffic between areas. Traffic that moves from one area to another is forwarded through routers that have both level 1 and 2 capability.

**level 1 and level 2 intermediate system**
These systems deliver and receive NPDUs from other systems, and relay NPDUs from other source systems to other destination systems. Level 1 systems route directly to systems within their own area, and route towards a level 2 system. A level 2 systems route towards another destination area or another routing area. Level 2 systems constitute the ISIS backbone area.

**LFA**
Loop-free alternate
A method of IP re-routing that finds a backup routing path by calculating a loop-free alternate backup path for each hop. The backup paths are included in the routing base in case of a failed link.
Topology independent LFA (TI-LFA) uses segment routing to determine a backup path that is independent of the network topology.

**LFI**
link fragmentation and interleaving
LFI interleaves high priority traffic within a stream of fragmented lower priority traffic. LFI helps avoid excessive delays to high priority, delay-sensitive traffic over a low-speed link.

**LH**
Long haul

**LI**
lawful intercept
A method to monitor target subscriber voice and data communications over an IP network by authorized agencies.

**LIC**
location ID code
A field in a SONET frame that identifies the location of an MDL.

**lightRadio Wi-Fi**
lightRadio Wi-Fi is a solution that allows the offloading of traffic or data to a wireless network using RADIUS authentication, GRE tunnels, and WLAN GWs.

**Linux**
A UNIX-like OS developed using the open-source software development and distribution model. Linux has an independently developed kernel, so is not a UNIX variant. “RHEL” (p. 100) is a commercial Linux version.

**LKDI**
license key delivery infrastructure
An Nokia web service that you can use to create and download LTE RAN license files for import into the NFM-P

**LLC**
logical link control
LLC is the upper sublayer of the ISO model data link layer. LLC governs packet transmission as specified by IEEE 802.2.

**LLD**
link layer discovery

**LLDP**
Link Layer Discovery Protocol
LLDP, defined by IEEE 802.1AB, is a standard that provides a solution for the configuration issues caused by expanding LANs. LLDP defines a standard information advertising and discovery method for Ethernet devices. The protocol runs in the datalink layer only, which allows NEs running different network-layer protocols to learn about each other.

**LLDPDU**
Link Layer Discovery Protocol data unit
See also “LLDP” (p. 65) .

**LLID**
Logical Link Identifier
A means for a service provider to track a subscriber, based on a virtual port (the LLID).

**LM**
loss measurement
Ethernet loss measurement is used to count the number of service frames which are not successfully delivered to the specified destinations.

**LMI**
local management interface
LMI is a signaling standard that is used between routers and FR switches. LMI communication takes place between a router and the first FR switch in the signaling path and involves the exchange of keep-alive, addressing, and virtual circuit status information.

**LMP**
link management protocol
LMP is used to establish and maintain an “IPCC” (p. 57) between adjacent peers.

**LMT**
local maintenance terminal

**LNS**
L2TP network server
The LNS is the server, which waits for L2TP tunnels. See also “LAC” (p. 62) and “L2TP” (p. 62) .

**load balancing**
Load balancing is the distribution of network traffic among the ports by a device so that no single port is overwhelmed, and network bandwidth is optimized.

**LOC**
loss of clock
A field in a SONET frame that indicates the loss of the line clock signal.

**LOF**
loss of frame
A field in a SONET frame that indicates the loss of a line frame in the frame sequence.

**LOS**
loss of signal
A field in a SONET frame that indicates the loss of line signaling.

**LOS**
line of sight
The propagation characteristic of high-frequency radio is called line-of-sight. Any obstruction between a transmitting antenna and a receiving antenna will block a signal. The ability to visually see a transmitting antenna roughly corresponds to the ability to receive a radio signal from it.

**LO–ODUk**
Lower Order–Optical Data Unit–k (k=1 to 8)

**LPE**
logical provider edge
A set of devices in a provider network that implement the functions of a service, such as VPLS.

**LPS**
learned port security
A mechanism for authorizing source learning of MAC addresses on Ethernet and Gigabit Ethernet ports.

**LRDI**
line remote defect indication
A field in a channel frame that indicates a remote LOF, LOC, or LOS.

**LS**
Link State

**LSA**
link state advertisement
LSA describes the local state of a device or network, including the state of the device’s interfaces and adjacencies. Each LSA is flooded throughout the routing domain. The collected LSAs of all devices and networks form the protocol’s topological database.

**LSDB**
link state database
A link state database, or topological database, contains the collection of LSAs received from all of the routers in an AS. The collected LSAs of all of the devices and networks form the protocol's LSDB. The LSDB is updated on a continuous basis as LSAs are advertised and when the network topology is updated.

**LSP**
label switched path
LSPs support MPLS functions and allow network operators to perform traffic engineering.

There are three types of LSPs:

- static LSP

  A static LSP specifies a static path. All devices that the LSP traverses must be configured manually with labels. No signaling is required.

- signaled (dynamic) LSP

  A signaled LSP is set up using a signaling protocol. The signaling protocol facilitates path selection and allows labels to be assigned from an ingress device to an egress device. Signaling is triggered by the ingress router; only the ingress router requires configuration.

- bypass-only LSP

  A bypass-only LSP has manually configured bypass tunnels on PLR NEs and is used exclusively for bypass protection.

- segment routing TE LSP

  A segment routing TE LSP is established with trafic engineering and protection requirements based on different parameters, such as hop limit, IGP shortcut , BGP shortcut and maximum segment routing labels.

- Point-to-Multipoint LSP

  A Point-to-Multipoint LSP allows the source of multicast traffic to forward packets to one or many multicast receivers over a network without requiring a multicast protocol, such as PIM, to be configured in the network.

**LSP classifier**
A method of filtering IP traffic flows on to an LSP.

**LSP path**
An LSP associated with an MPLS path. This path could be an actual route, or a configured route. A configured route can be primary, secondary, or standby. An LSP could have at most one actual route, one primary route, and multiple standby or secondary routes.

**LSR**
label switched router
An LSR is an MPLS NE that runs MPLS control protocols and is capable of forwarding packets based on labels. An MPLS NE may also be capable of forwarding native Layer 3 packets.

**LTE**
Long Term Evolution
LTE is a standard for wireless mobile broadband networks. LTE networks can offer higher data throughput to mobile terminals than other technologies. LTE is the accepted evolution path for GSM, WCDMA, and CDMA networks. LTE is developed and maintained by the 3GPP standards body.

**LTN**
LSP ID to NHLFE
"LSP" (p. 66) ID to Next Hop Label Forwarding Entry

**LTR**
Link Trace Response

## M

**MA**
maintenance association
MA is a set of MEPs, each configured with the same ID and MD level.

**MAC**
media access control
MAC is a sublayer of the data link layer, defined in IEEE 802.2 specifications that accesses the LAN medium. The MAC layer handles the recognition and identification of individual network devices. Every computer and network device has a MAC address that is hardware-encoded.

**MAC pinning**
MAC pinning is a restriction on a MAC entry in the MAC forwarding table such that it cannot be relearned on another port within the lifetime of the entry. The entry can still age.

**MAF**

MAF can be expanded in two ways:

1. management access filter

   A filter that specifies the type of management access and underlying connection protocol usage for an NE, as well as the IP addresses and ports that can access the device.

2. 9471 MME application function

**MAID**
maintenance association ID
A MAID is a unique identifier for the MA. The MAID has two parts, the maintenance domain name and the MA name.

**main server**
See "NFM-P main server" (p. 81).

**MAN**
metropolitan area network
A telecommunications network that covers a geographic area such as a city or suburb.

**mask**
A filter that selectively includes or excludes certain values. For example, when you define a database field, you can assign a mask that indicates the type of value for the field. Values that do not conform to the mask cannot be entered.

**MBB**
make before break

**MBMS**
multimedia broadcast multicast service
A "P2MP" (p. 89) interface specification for RAN and core network broadcast and multicast services.

**MBS**
maximum burst size
MBS refers to the number of cells that can be sent at PCR and still conform to the SCR.

**MC**
multichassis
A redundancy configuration that includes two peer NEs.

**MC APS**
multi chassis automatic protection switching

**MC LAG**
multi chassis link aggregation group

**MC MLPPP**
multiclass MLPPP
Fragmentation of packets of various priorities into multiple classes, allowing high-priority packets to be sent between fragments of lower priorities. See "MLPPP" (p. 73) .

**MC mobile group**
A child group object of an MC peer group. When you create an MC mobile group, the NFM-P automatically creates the child group members using the peer objects in the MC peer group.

**MC peer group**
An NFM-P object that defines the relationship between two peer NEs to provide system redundancy in an Ethernet network. An MC peer group configuration includes a list of protocols and objects with state information that is to be synchronized between the peers.

**MCC**
mobile country code
A three-digit code defined in ITU-T Recommendation E212 that identifies a country or group of networks.

**MCFR**
Fragmentation of packets of various priorities into multiple classes, allowing high-priority packets to be sent between fragments of lower priorities. See "MLFR" (p. 73) .

**MCM**
MDA carrier module
A hardware component of a 7450 ESS or 7750 SR that plugs into a card slot and accepts the installation of one or more MDAs.

**MCS**

MCS can be expanded in two ways:

1. multichassis synchronization
2. MC mobile interface

**MCS Database**
multi chassis synchronization database
A database that contains the dynamic state information created on any of the NEs by any application using its services. The individual entries in the MCS Database are always paired by peering-relation, sync-tag and application-id. At any time, the specific entry is related to the single redundant-pair objects (such as two saps on two different NEs), and hence stored in a local MCS Database of the respective NEs.

**MCT**
microwave craft terminal
A type of local craft terminal. An MCT can provision or manage an NE remotely over a network connection, or directly over a local connection. A local connection allows on-site management of the NE. An MCT includes the terminal and the software required to perform NE management.

**MD**
maintenance domain
An MD is a network or part of a network for which faults in connectivity can be managed using the IEEE 802.1ag standard protocols. Each MD can include multiple MAs.

**MD4H**
multi-service dual-module unit with four temperature-hardened client ports per module
The 1830 PSS-1 MD4H is a temperature-hardened one-RU edge device that supports two PSS1MD4 OTs, four multi-service client ports, and two 2.7-Gb line ports on each OT.

**MD5**
message digest 5
MD5 is a security algorithm that takes an input message of arbitrary length and produces as an output a 128-bit message digest of the input. MD5 is intended for digital signature applications, where a large file must be compressed securely before being encrypted.

**MDA**
media dependent adapter
An MDA is a pluggable interface module that distributes traffic between the network and the system IOM. Also referred to as a daughter card.

**MDCR**
minimum desired cell rate
MDCR is equivalent to MIR.

**MDDB**
multidrop data bridge

An MDDB broadcasts a single stream from a "SCADA" (p. 106) master to multiple remote devices and allows communication from individual remote devices back to the master.

**MDI/MDIX**
medium-dependent interface/medium-dependent interface crossed
A type of Ethernet port connection that uses twisted-pair cabling, as specified in the IEEE 802.3 standard. Network adapter cards on computers typically connect to a network using RJ-45 interface ports that use pins 1 and 2 to transmit, and pins 3 and 6 to receive. Uplink ports on hubs and switches use the same pin assignments. Normal ports on hubs and switches use the opposite pin assignment: pins 1 and 2 are used to receive, and pins 3 and 6 are used to transmit. Such ports are called MDIX ports.

**MDL**
message data link
A data transmission path that is used to communicate identification or test signal information at the data link layer.

**MDT**
multicast distribution tree
An MDT is a group of network paths in a multicast domain that originate at a common multicast source and terminate at CE devices.

**ME**
metro Ethernet

**MED**
multi-exit discriminator
An attribute that is used by an external AS to determine the preferred route into the AS that is advertising the attribute.

**MEF**
Metro Ethernet Forum

**MEG**
maintenance entity group
An MD is a network, or part of a network, that is provisioned with a set of maintenance entity groups, or MEGs, which are groups of service sites. Typically, a MEG represents one service and consists of a group of MEPs. A MEG can be associated with only one service, while one service can be associated with multiple MEGs.

**menu bar**
The menu bar is a tool on the GUI that organizes tasks across broad headings. You can perform functions on the application by selecting an action from the menu bar.

**MEP**
maintenance entity point
In a CFM enabled network MEPs can be any SAP or SDP binding in a service and associated to a MA. A set of MEPs configured with the same MA ID defines a MA. CFM tests detect connectivity failures between any pair of local and remote MEPs in a MA.

**Mesh**
A type of network configuration that combines ROADMs to support mesh channel connectivity between the ROADMs without O-E-O for transmission. It is operated as a single NE with as many as four degrees (bidirectional DWDM interfaces) that comprise two lines for the east and two for the west.

**MF bit**
more fragments bit
A bit in an IP header that indicates the occurrence of data fragmentation and signals that at least one packet fragment follows. When a packet becomes fragmented, the MF bit in the current packet is set to 1. The MF bit is reset in the last packet of the fragmented datagram to indicate that there are no more fragments.

**MG-VM**
mobile gateway VM
Provides services that include 3GPP control and data plane call processing, PCEF, and application assurance, in which the PCEF is enhanced with ADC for application detection and control and L7 service classification for policy charging control. The MG-VM supports all 3GPP gateway functions, including SGW, PGW/GGSN, and SAE-GW. Supported service functions depend on the configurable personality of the MG-VM.

**MHF**
MIP half function
In a CFM enabled network MIP half-function objects allow MIPs to be recognized as MIPs on one MD level and MEPs on a higher level.

**MI**
management interface

**MIB**
management information base
A formal description of a set of network objects that can be managed using SNMP.

**MIF**
9471 WMM interface function

**MIM**
management information model

**MIP**

MIP is expanded two ways:

1. maintenance domain intermediate point

   In a CFM enabled network a MIP is an intermediate point between 2 MEPs and consists of 2 MHFs.

2. mobile Internet Protocol

   An IETF communications protocol that allows mobile device users to move between networks while retaining the same permanent IP address.

**MIR**
minimum information rate
MIR is the minimum data transfer rate for a path, such as a frame relay, VPC, or VCC path.

**mirror service**
A mirror service is a type of service that copies the packets from a specific customer service to a destination outside the service for troubleshooting or surveillance purposes.

**MLD**
Multicast Listener Discovery Protocol
MLD is an asymmetric protocol used by IPv6 routers to discover the presence of NEs that wish to receive multicast packets on their directly-attached links, and to discover which multicast addresses are of interest to those neighboring NEs.

**MLDP**
Multicast Label Distribution Protocol
MLDP provides extensions to "LDP" (p. 63) for the setup of "P2MP" (p. 89) "LSP" (p. 66)s in "MPLS" (p. 74) networks.

**MLD snooping**
Multicast listener discovery snooping is essentially the IPv6 version of IGMP snooping.

**MLFR**
An aggregation of multiple physical links into a single logical bundle to improve bandwidth between two peer systems. See "FR" (p. 45) .

**MLPPP**
multilink PPP
An aggregation of multiple physical links into a single logical bundle to improve bandwidth between two peer systems. See "PPP" (p. 95) .

**MME**
mobility management entity
The control NE that processes the signaling between the UE and the core network. The MME also provides VLR functions for the EPS and supports functions related to bearer and connection management.

**MMRP**
Multiple MAC Registration Protocol

**MMS**
multimedia messaging service
A method to send multimedia content messages to and from mobile devices.

**MNC**
mobile network code
A two- or three-digit code defined in ITU-T Recommendation E212 that together with the MCC identifies a network.

**MNN**
mobile network node
A node that is located inside a mobile network.

**MNO**
mobile network operator
A telecommunications company that provides mobile services to subscribers. An MNO typically holds a radio spectrum license.

**MOBIKE**
mobility and multihoming Internet key exchange
The MOBIKE protocol is a mobility and multihoming extension to the IKEv2.
Base IKEv2 procedures allow a UE and EPDG to establish a set of SAs between single UE and EPDG IP addresses. However, since the UE typically uses an IP address allocated by the access network (perhaps by the WiFi AP), there are mobility scenarios wherein this “outer” IP address may change. Using the base IKEv2 protocol, the UE would have to delete and re-establish a new set of SAs with the EPDG using this new source address.
MOBIKE allows one or both of the IKEv2 endpoints to change the IP address used for its side of the SA without re-establishing the SA. MOBIKE can be used for both mobility and multihoming scenarios. Multihoming means that the IKEv2 endpoint may have multiple IP addresses and be connected to multiple interfaces. The IKEv2 endpoint can use MOBIKE to switch to a different IP interface after the IKEv2 SA and IPsec SAs have been established. For example, it may choose to try a new IP interface if it notices that it cannot reach its peer using the current IP interface.
In the mobility case, the UE informs the EPDG that is has moved and would like to use a new source IP address. MOBIKE does not change the EPDG IP address.

**MOC**
managed object class

**monitoring key**
A monitoring key groups services that share a common allowed usage. A monitoring key identifies a usage monitoring control instance. Many PCC rules share the same monitoring key.

**MP**
Multi Point

**MP-BGP**
Multiprotocol Border Gateway Protocol
An enhanced BGP that carries IP multicast routes. MP-BGP carries two sets of routes: one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by PIM to build multicast data distribution trees.

**MPH**
MME packet handler service
The MPH service terminates the external signaling SCTP, UDP, and TCP stacks on the 9471 WMM to offload the MIF service from this function.

**MPLS**
multiprotocol label switching
MPLS is a technology in which forwarding decisions are based on fixed-length labels inserted between the data link layer and network layer headers to increase forwarding performance and flexibility in path selection.

**MPLS-TP**
multiprotocol label switching - transport profile
MPLS-TP is a set of MPLS protocol functions that enables the use of MPLS in transport networks and applications. MPLS-TP enables MPLS to be deployed in a statically configured transport network without the need for a dynamic control plane.

**MPT**
microwave packet transport
MPT is a microwave dish which connects to a 9500 MPR MSS via a GigE interface located on a 4+4 × Ethernet EAS module of a 9500 MPR MSS.

**MPT-ACC**
microwave packet transport-access

**MPT-HC**
microwave packet transport-high capacity

**MPT-HL**
microwave packet transport-high capacity long haul
MPT-HL provides full indoor RF transceiver packages connecting to ports on an Ethernet Access Switch (EAS) module.

**MPT-HQAM**
microwave packet transport-hierarchical quadrature amplitude modulation

**MPT-MC**
microwave packet transport-medium capacity

**MPT-XP**
microwave packet transport-eXtreme power

**MR**
mobile router
A device that has one or more subnets that connects to an IP host. The MR hides its mobility from the hosts on the HRPD network. The hosts on the subnets are fixed in relationship to the MR and move homogeneously, or as a whole. The MR connects the mobile network to the Internet.

**MRP**
Multiple Registration Protocol

**MRRU**
maximum received reconstructed unit
MRRU is the maximum frame size that can be reconstructed from multilink fragments.

**MS**
mobile station

An MS comprises all user equipment and software needed for communication with a mobile network. In 3G systems it is often referred to as UE.

**MS-PW**
multi-segment pseudowire
MS-PW routing allows inter-domain routed services to dynamically maintain paths using "S-PE" (p. 104) and "T-PE" (p. 117) NEs.

**MSAP**
managed service access point
See also "SAP" (p. 105) .

**MSCC**
multiple services credit control
An AVP in CCA and CCR messages that is used to grant and report quota for each rating group. When the MSCC AVP is included in CCA messages, it represents quota that is granted. When it is included in CCR messages, it represents usage that is reported. If the quota or usage is reported for more than one rating group, multiple MSCC AVPs are present in the message.

**MSDP**
Multicast Source Discovery Protocol
MSDP allows PIM-SM domains to communicate with each other using their own RPs. MSDP also enables multiple RPs in a single PIM-SM domain to establish MDSP mesh-groups, and can be used between anycast RPs to synchronize information about the active sources being served by each anycast RP peer.

**MSE**
mean squared error

**MSISDN**
mobile station international subscriber directory number
The telephone number of a mobile user. The MSISDN is included in the EPS bearer context. See 3GPP TS 23.003 Section 3.3.*

**MSM**
mobility service module

**MSP**
multiplex section protection

**MSS**

MSS can be expanded in two ways:

- Microwave Service Switch

  The MSS is a multiservice aggregation switch in which TDM traffic is circuit-emulated according to MEF 8. Inverse Multiplexing over ATM (IMA) is terminated, aggregated natively, then converted into packet using PWE3 (IETF RFC 4717).
- Maximum Segment Size

  The largest amount of data that a device can receive in a TCP segment.

**MSTI**
multiple spanning tree instance
An enhancement to the IEEE 802.1Q CST. An MSTI is a single spanning tree instance that represents a group of VLANs.

**MSTP**
Multiple Spanning Tree Protocol
An RSTP that allows different spanning trees to co-exist on the same Ethernet switched network.

**MTC**
machine-type communications
MTC specifies machine-to-machine communications and is a 3GPP standard.

**MTOSI**
multi-technology operations systems interface
A TMF team creating new standards for OSSs to simplify integration between different vendor systems by using a common open interface.

**MTSO**
Mobile Telephone Switching Office

**MTU**
maximum transmission unit
MTU is the largest unit of data that can be transmitted over a specific interface type in one packet. The MTU can change over a network.

**multi-tier model**
Logical partitioning of software products to enable distributed implementations and modular deployments. Logical partitioning can be from three layers (user interface, application server or middleware, database server) to five or more layers. One model uses the client, presentation, business, integration, and resource layers to define software components.

**multicast CAC**
multicast connection admission control
Multicast CAC manages the amount of bandwidth consumed by BTV distribution services to avoid network congestion and maintain QoS standards. The multicast CAC function is supported on any IGMP and PIM interface, and in the case of BTV distribution, on VPLS SAPs and SDPs where IGMP snooping is enabled.

**multicast routing**
Multicast routing delivers source traffic to multiple receivers without any additional burden to the source or the receivers. Multicast packets are replicated in the network by routers that are enabled with PIM, which results in the efficient delivery of data to multiple receivers.
Multicast routing is based on an arbitrary group of receivers that expresses an interest in receiving a specific data stream. The group does not have physical boundaries—the hosts can be located anywhere on the Internet. The hosts must join the group using IGMP to receive the data stream.

**MVAC8B**
Multiple Variable Attenuator Card Bidirectional
The bidirectional card is used to control the power level and insert WaveTracker keys on optical signals received from client equipment.

**MVPLS**
management virtual private LAN service
An MVPLS is created to run RSTP and manage traffic on the associated VPLS. An MVPLS is required to remove topology loops when redundant spoke SDPs or L2 access interfaces have been created for HVPLS configurations. RSTP must be run on the redundant spoke SDPs or L2 access interfaces to block some of them from passing traffic. VPLS that have redundant spoke SDPs or L2 access interfaces that are managed by the MVPLS also have their traffic blocked appropriately.

**MVPN**
A multicast "VPN" (p. 128) is an IP VPN service that supports the transmission of IP multicast packets between sites.

**MVR**
multicast VLAN registration
See "MVR VPLS" (p. 77) .

**MVR by proxy**
A 7450 ESS feature that allows multicast VPLS traffic to be copied to an SAP other than the SAP from which the IGMP message originated.

**MVR VPLS**
Also known as a multicast VPLS, an MVR VPLS distributes multicast traffic through a network. An MVR VPLS also acts as a user VPLS when it contains SAPs that receive multicast traffic.
MVR on VPLS allows multiple subscriber hosts to remain in separate VLANs while sharing a single multicast VPLS. The 7450 ESS uses MVR on VPLS and IGMP snooping to provide BTV services.

**MVRF**
The multiple virtual routing and forwarding feature provides the ability to configure separate virtual routing instances on the same NE. See "VRF" (p. 128) .

**MVRP**
Multi-VLAN Registration Protocol

**MW**
microwave

**MWA**
microwave-aware

## N

**N-PE**
network-facing provider edge
A device that implements the control and signaling functions of an LPE.

**NA**
Neighbor Advertisement

**NAI**
network access identifier
The NAI is used to address a user in a specific Internet domain. The format of an NAI is similar to that of an address. It is comprised of a user portion that identifies the individual node and a realm portion that identifies an administrative domain in the Internet. The two portions are separated by an @ sign. The ROAMOPS working group is in liaison with bodies such as the ITU and 3GPP in order to integrate NAI with variables such as the E.164 telephone number range and the IMSI.

**NAPT**
network address port translation
An enhancement of regular “NAT” (p. 78) that allows a large number of devices on a private network to simultaneously “share” a single inside global address by changing the port numbers used in TCP and UDP messages.

**NAS**
non-access stratum
A functional layer in the UMTS and LTE wireless telecom protocol stacks between the core network and UE, used to direct communication sessions and to maintain steady communications with the UE as it changes locations.

**NAT**
network address translation
NAT is a method by which IP addresses are mapped from one group to another group; the method is transparent to end users. Many network addresses and their TCP/UDP ports are translated into a network address and its TCP/UDP ports. As a result, a realm with private addresses can be connected to an external realm with globally unique registered addresses, typically the Internet.

**NB-IoT**
NarrowBand Internet of Things
NB-IoT is a lower power WAN radio technology 3GPP standard developed to connect IoT user devices and services on established mobile networks. NB-IoT improves the power consumption of the devices and increases coverage, system capacity, and spectrum efficiency.

**NBNS**
NetBIOS name server

**ND**
node discovery

**navigation tree**
The navigation tree displays a view of all managed equipment, services, and protocols, and allows you to navigate through these components.

**NE**
network element
A physical device, such as a router, switch, or bridge, that participates in a network.

**NE WO**
network element work order
See "WO" (p. 131) .

**NEBS**
Network Equipment Building Standards
The requirement for equipment deployed in a central office environment. Covers spatial, hardware, craftsperson interface, thermal, fire resistance, handling and transportation, earthquake and vibration, airborne contaminants, grounding, acoustical noise, illumination, electromagnetic compatibility, and electrostatic discharge requirements.

**neighbor**
An adjacent system reachable by traversing a single sub-network by a PDU

**NEMO**
network mobility
A mobile network that can change its connection point to the Internet. MRs within the NEMO provide the connection to the Internet by maintaining a tunnel with an HA that resides in the home network of the MNN and the NEMO. While the MR changes its link locations, it obtains new IP addresses from the visited links. Traffic generated by the MNNs inside the NEMO network is forwarded by the MR to the HA through the tunnel. Packets from the Internet that are destined for the NEMO network are tunneled by the HA to the MR, then forwarded to the final destination inside the NEMO network.

**NETCONF**
Network Configuration Protocol

**NEtO**
Network Element Overview
A GUI-based 9500 MPR NE manager.

**network topology**
The layout of a network, which can include the way in which NEs are connected and how they communicate.

**NFM-P**
Network Functions Manager - Packet
The NFM-P is an advanced IP/MPLS and mobile network management system developed using a modular, scalable architecture. The system provides multiple GUI, web, and OSS interfaces, and can be integrated with other management systems.

**NFM-P analytics server**
The NFM-P analytics server is an NFM-P system component that uses business intelligence software, aggregated statistics, and raw data to generate reports about network conditions and trends. The reports are accessible from the NFM-P Analytics application. An analytics server requires an NFM-P auxiliary database as a data store.

**NFM-P auxiliary database**
An NFM-P auxiliary database is an optional, horizontally scalable NFM-P system component that increases the data throughput and storage for demanding operations such as statistics or NFM-P analytics data collection. An auxiliary database is deployed as a distributed database on separate stations in a cluster configuration to provide fault tolerance and enable load balancing.

**NFM-P auxiliary server**
An NFM-P auxiliary server is an optional NFM-P system component on a dedicated station that accepts processing requests from, and is directed by, an NFM-P main server. Auxiliary server deployment is supported only in a distributed NFM-P system.

**NFM-P C flowd auxiliary server**
An NFM-P C flowd auxiliary server is an optional NFM-P system component on a dedicated station that collects AA Cflowd statistics data from managed NEs. The server forwards the collected data in “IPDR” (p. 57) format to an OSS or third-party system for processing.

**NFM-P client**
An NFM-P client interacts with an NFM-P main server. An NFM-P GUI client provides a graphical interface for network and NFM-Pmanagement. An NFM-P OSS client is a third-party application that uses the XML API for network and NFM-P management.

**NFM-P client delegate server**
An NFM-P client delegate server supports simultaneous NFM-P client GUI sessions using one client software installation. Local and remote client GUI users on separate terminals connect to an NFM-P main server through a client delegate server using display redirection or a remote access server.

**NFM-P database**
The NFM-P database stores network data-model objects and configuration information.

**NFM-P main server**
An NFM-P main server mediates between the NFM-P database and other components, NFM-P clients, and the managed network.

**NFM-P server cluster**
A logical grouping of the components in an NFM-P system. Each component in a system belongs to the same server cluster, which is identified by the NFM-P domain name specified during system installation.

**NFM-T**
The NFM-T provides unified optical end-to-end network management and operational support for all network element products in the Nokia’s optics portfolio.

**NFV**
Network function virtualization
Allows network administrators to uncouple network functions from underlay hardware NEs so that the functions can run as software images.

**NGE**
Network Group Encryption

A mechanism for the end-to-end encryption of MPLS-based traffic. NGE is supported on 7705 SAR devices.

**NG MVPN**
next generation MVPN
Transports user traffic over M-LSPs and GRE tunnels using BGP for signaling multicast information.

**NI**
network ID

**NIST**
National Institute of Standards and Technology

**NLOS**
non-line-of-sight
A radio transmission across a path that is partially obstructed, usually by an object.

**NLRI**
network layer reachability information

**NMS**
network management system
A system that manages at least part of a network. An NMS is typically a reasonably powerful and well equipped computer that communicates with external agents to monitor and manage network resources.

**NNI**

NNI is expanded two ways:

1. network-to-network interface

   An NNI is a standard interface between two ATM devices or two frame relay devices.

   An NNI is also a port that resides on a PE bridge or a transit bridge, and connects to a service provider network.

2. network node interface

   NNI is the interface between two ATM network devices that operate under different administrative domains, such as a vendor ATM switch and an ATM switch from another vendor.

**NOC**
network operations center
The group that is responsible for the configuration and monitoring of the network and service elements using network switching equipment and management systems.

**NPDU**
network protocol data unit

**NRC-P**
Packet Network Resource Controller

**nrt-VBR**
non real-time variable bit rate
nrt-VBR is an ATM service category that guarantees low cell loss and low delay for applications, such as video and frame relay, which are characterized by an on/off source with known, predictable transmission patterns. During the on period, cells are transmitted at the peak information rate. No cells are transmitted during the off period. nrt-VBR allows statistical multiplexing gains using the traffic descriptors (PCR and SCR). It does not provide delay commitments.

**NSAPI**
network service access point identifier

**NSG**
network services gateway
The NSG is a network element representing the network forwarding plane for customer network services at the remote business location. The VNS solution manages NSGs at each enterprise site to act as a CPE, allowing it to create overlay VPNs to network customer sites and data centers.

**NSR**
non-stop routing
Non-stop routing prevents the outage of the control plane of a router due to the introduction of fault tolerance.

**NSSA**
not-so-stubby-area
NSSA is an OSPF area type where OSPF propagates any external routes that it obtains from the AS.

**NSWO**
non-seamless WLAN offload

**NTP**
Network Time Protocol
An Internet protocol that network devices use to synchronize their clocks.

## O

**O-GLSP**
optical-generalized label switched path

**OADM card**
optical add/drop multiplexer card
An MDA that can be configured on the 7705 SAR to add or drop specific wavelengths while allowing others to pass through. This card comes in 1, 2, 4, or 8-channel variants.

**OAM**
operations, administration, and maintenance
A general term used to describe the costs, tasks involved, or other aspects of operating, administering, and managing a telecommunications network. The NFM-P provides a series of OAM tools to monitor and administer the network.

**OAMPDU**
operations, administration, and maintenance protocol data unit

**OAM-VM**
operations, administration, and management VM

**OC-N**
optical carrier - level *N*
An optical SONET signal carried at the speed of *N*, for example, OC-12 is a signal at 622.08 Mb/s.

**OCH**
Optical channel
An optical wavelength band for WDM optical communications.

**OCS**
online charging system
A charging system that records accounting information for network resource usage. The OCS performs real-time credit control, including the management of transactions and subscriber accounts. The OCS authorizes the network, upon request, to grant resource usage to a subscriber. See 3GPP TS 32.240 for more information.

**OCS**
optical core switch

**ODU**
optical channel data unit
outdoor unit

**ODUk**
The Optical Data Unit (ODU) provides end-to-end bandwidth management for a sub-wavelength signal in the electronic domain. The ODU is a fixed-sized container with in-band OAM tools for quality supervision and SLA assurance. The ODU functions as primary bearer for client traffic.

**OEO**
optical-to-electrical to optical
The process of converting an optical signal to an electrical equivalent and then back to optical data.

**OFCS**
offline charging system
A charging system that records charging information and sends the data from the network to an external billing system, after the resource usage has occurred. The OFCS relies on clients in the NE that initiate, modify, and terminate charging reporting based on a set of parameters that are relevant to each NE. See 3GPP TS 32.240 for more information.

**OID**
object identifier

An OID is a sequence of integers that uniquely identifies a MIB object. Each MIB object has an OID. A management system uses an OID to request an object value from a MIB. The OID defines a path to the object through a tree-like structure called the OID tree, or registration tree.

**OIPS**
Open Interfaces Professional Support
The Nokia OIPS portfolio provides OSS developers with network management integration solutions for the NFM-P. OSS integration initiatives include project review, design consultation, development support, and training for integration projects.

**OLC**
object life cycle
The OLC state specifies whether a service or network object is in maintenance or in-service mode to filter alarms. The default value of the OLC state for NEs can be specified in the discovery rules.

**OLP**
optical line protection
OLP protects the path between two adjacent network element degrees by splitting the fibers and selecting from two transmission fibers.

**OMC**
Optical Management Console

**OMD**
Optical multiplexer/demultiplexer

**OMSP**
Optical multiplex section protection

**OOS**
out of service

**OPEX**
operating expenditures

**OPR**
Optical power receive

**OPS**
An optical circuit pack that provides WDM protection.

OPS is expanded in two ways:

1. off-premise station
2. optical protection switch

**OPSA**
Optical protection switch - advanced card

**OPT**
Optical power transmit

**Option 82**
See “Relay Information Option” (p. 99) .

**OPTSG**
OPU1 Timing Slot Group

**OPUk**
Optical Channel Payload Unit-k (k=1,2, or 3)

**Oracle Advanced Security**
A security option for the Oracle database product that provides security features to protect enterprise networks and securely extend corporate networks to the Internet. Oracle Advanced Security combines message encryption, database encryption, strong authentication, and authorization to address customer privacy and compliance requirements.

**ORF**
outbound route filtering
ORF is used to reduce the amount of time required to filter routes from a BGP peer.

**ORR**
Optimal Route Reflection
BGP Optimal Route Reflection (BGP-ORR) can be configured on a route reflector to advertise the best path to the BGP-ORR client groups.

**OS**

OS is expanded in two ways:

1. operating system
2. OmniSwitch

   A Nokia family of devices. These devices support L2 forwarding and L3 routing, and have an extensive array of networking features.

**OS 10K**
OmniSwitch 10K
The OS 10K is a high-capacity, high-performance modular Ethernet LAN switch that provides 5.12 terabits per second of switching performance. The OS 10K has a 12 slot chassis configuration: 4 slots for CMM/fabric cards; and 8 slots for XNI or GNI cards that provide Ethernet, GigE, and 10 GigE capabilities.

**OS 6250**
OmniSwitch 6250
Layer 2+ Fast Ethernet Stackable LAN family of switches which includes the OS 6250SME (small and medium enterprise) for the enterprise segment, and the OS 6250M, for the Metro access segment.

**OS 6400**
OmniSwitch 6400
The OS 6400 family of devices is a set of stackable Layer 2+ GigE LAN switches.

**OS 6450**
OmniSwitch 6450
The OS 6450 family of devices is a set of stackable GigE LAN switches available in 10-, 24-, or 48-ports variants, with optional upgrade paths for 10 GigE stacking, 10 GigE uplinks, and metro Ethernet services.

**OS 6850**
OmniSwitch 6850
The OS 6850 family of devices is a set of stackable Ethernet switches that provides wire-rate L2 forwarding and L3 routing with advanced service support.
This family includes the OS 6850E, an enhanced chassis that has a different form factor, updated transceiver support, and a different stacking mode.

**OS 6850E**
OmniSwitch 6850E
See "OS 6850" (p. 87) .

**OS 6855**
OmniSwitch 6855
The OS 6855 is a stackable, hardened Ethernet switch that has up to 24 Gigabit copper and fiber ports; it is designed to operate reliably in harsh electrical and severe temperature environments.

**OS 6900**
OmniSwitch 6900
The OS 6900 is a family of standalone aggregation switches.

**OS 9600**
OmniSwitch 9600
The OS 9600 is a five-slot Ethernet switch that supports one CMM and four network interface modules. It offers a wide range of GigE and 10GigE interfaces, and supports power-over-Ethernet for devices such as IP telephones, WLAN access points and video cameras. The OS 9600 supports up to two load-sharing power supplies.

**OS 9700**
OmniSwitch 9700
The OS 9700 family of devices is a set of high-density ten-slot Ethernet switches that use two slots for control and eight for network interfaces. Designed for smart continuous switching operation, the two center slots are dedicated to CMMs that support redundancy. The OS 9700 supports up to three power supplies.
This family includes the OS 9700E, which offers eight slots for Gigabit and 10-GigE network interface modules. The remaining two slots are reserved for redundant CMMs.

**OS 9700E**
OmniSwitch 9700E
See "OS 9700" (p. 87) .

**OS 9800**
OmniSwitch 9800

The OS 9800 family of devices is a set of high performance 18-slot switches. 16 slots are reserved for Gigabit and 10-GigE network interface modules. The remaining two slots are reserved for primary and redundant CMMs. The OS 9800 supports up to four power supplies.
This family includes the OS 9800E, which offers 16 slots for Gigabit and 10-GigE network interface modules. The remaining two slots are reserved for redundant CMMs.

**OS 9800E**
OmniSwitch 9800E
See "OS 9800" (p. 87) .

**OSC**
optical supervisory channel
A designated optical channel used to carry communications related to maintenance and operational functions of the network rather than customer traffic.

The OSC supports the following communications:
- NE-to-NE
- interworking
- client LAN
- orderwire communication

**OSI**
open systems interconnection
A reference model of protocols organized in seven layers. OSI standards and applications facilitate the interworking of equipment from different manufacturers.

**OSPF**
open shortest path first
OSPF is an IETF standard link-state routing protocol used to determine the most direct path for a transmission in IP networks.

**OSS**
operations support system
A network management system supporting a specific management function, such as alarm surveillance and provisioning, in a service provider network.

**OSSI**
operations support system interface
A set of APIs that allow OSSs to manipulate a well defined set of managed objects that are identified by management applications to automate operational procedures and allow flow-through provisioning.

**OT**
Optical Transponder
A circuit pack that performs "OEO" (p. 84) conversion. OTs perform frequency adaptation between 1830 PSS equipment and external equipment that is not optically compatible with 1830 PSS transport. It provides retiming, reshaping, and re-

amplification, or 3R, functions and performs fault management and non-intrusive performance monitoring on the “SONET” (p. 112) / “SDH” (p. 107) and WaveWrapper signals.

**OTDR**
Optical time domain reflectometer

**OTN**
Optical Transport Network
A fiber-optic network, such as an SDH or SONET network, that is designed to transport customer traffic,

**OTT**
Over The Top
OTT services are services used in addition to the network services provided by the service provider, also called “value added” services. An example is Skype.

**OTU**
optical transport unit

**OUI**
organizationally unique identifier
A three-octet field in a SNAP header that identifies an organization.

## P

**P**
provider core

**P-CSCF**
proxy-call session control function

An IMS SIP server that is the first point of contact in a VoLTE call. The P-CSCF has the following functions:

- forwards SIP messages to other IMS nodes and to the UE
- interacts with the PCRF for billing and policy rules
- maintains a security association with the UE
- detects and forwards emergency calls to the local E-CSCF

**P-GW**
See “PGW” (p. 92) .

**P2MP**
point to multi-point

**PAE**
port access entity
A logical entity that supports the IEEE 802.1X protocol that is associated with a port.

**PAP**
Password Authentication Protocol
A protocol to communicate with a security server for a user authentication.

**PAT**
program association table

**PBB**
provider backbone bridge or provider backbone bridging

**PBBN**
provider backbone bridged network

**PBN**
provider bridge network

**PBS**
peak burst size
The maximum number of bytes that can be sent at the network interface speed without exceeding the PIR.

**PC**
personal computer

**PCC**
policy and charging control
PCC encompasses flow-based charging, including charging control and online credit control and policy control (e.g. gating control, QoS control, QoS signaling). See 3GPP TS23.203.*

**PCC**
"PCE" (p. 89) Client

**PCE**
IP Path Computational Engine

**PCEF**
policy and charging enforcement function
This encompasses SDF detection, policy enforcement and flow-based charging functions. See 3GPP TS23.203 Section 6.2.2.*

**PCEP**
"PCE" (p. 90) Protocol

**PCI**
physical cell identification
PCI prevents signal collision during UE handover between wireless cells of eNodeBs.

**PCMD**
per-call measurement data
In a CDMA network, PCMD is the data associated with a call, such as the subscriber identifier, start time, duration, type, system identifiers, and call geometry parameters. The data is used for operations such as call hand-off, tracking, and traffic analysis.

**PCO**
protocol configuration options

The PCO provides additional optional information about the destination network to which the UE is connecting. The PCO information element transfers parameters, such as external network protocol options, between the UE and the PDN APN, which are sent transparently through the MME and the SGW. The PCO may include the address allocation preference indicating that the UE prefers to obtain an IP address only after the default bearer activation. See 3GPP TS23.401.

**PCP**
port control protocol
Port control protocol allows an IPv4 or IPv6 host to control how incoming IPv4 or IPv6 packets are translated and forwarded by a NAT or firewall, and also allows a host to optimize its outgoing NAT keepalive messages.

**PCR**

PCR is expanded in two ways:

1. peak cell rate

   PCR is the cell rate, in cells per second, that the endpoint may never exceed.

2. program clock reference

**PCRF**
policy control and charging rules function
Enables operators to have rules-based, real-time dynamic control over bandwidth, charging, and usage in an LTE network.

**PD**
powered device
Any device that uses a PoE data cable as the only source of power.

**PDF**
portable document format
The file format in Adobe Acrobat document exchange technology.

**PDH**
plesiochronous digital hierarchy
A technology used in telecommunications networks to transport large quantities of data over digital transport equipment such as fiber optic and microwave radio systems.

**PDN**
packet data network
The network through which a UE obtains a packet data connection to the Internet.

**PDP**
packet data protocol
In UMTS, the PDP uses a packet data connection over which the user equipment and the network exchange IP packets. The use of the packet data connections is restricted to specific services. The services can be accessed using access points.

**PDSN**
public data switched network

**PDU**
protocol data unit
A PDU is a message of a specific protocol comprising payload and protocol-specific control information, typically contained in a header. PDUs pass over the protocol interfaces which exist between the layers of protocols, as indicated in the OSI model.

**PE**
provider edge
The name of the device or set of devices at the edge of the provider network with the functions required to interface with the customer network and the MPLS network.

**PE bridge**
An Ethernet switch that resides on the edge of the service provider network. The PE bridge interconnects customer networks with service provider networks. A switch is a PE bridge when the switch transports packets between a customer-facing port and a network port or between two customer-facing ports.

**PECF**
policy enforcement and charging function

**PEM**
power entry module

**PEQ**
power equalization module
The 7950 XRS power supply which provides DC power to the chassis.

**PF**
power filter

**PFS**
perfect forwarding secrecy
A key-establishment protocol for secure VPN communications. PFS requires the use of public key cryptography. No key used for the transfer of data may be used to derive keys for future transmission. Diffie-Hellman key exchange is a cryptographic protocol that provides perfect forward secrecy.

**PGW**
packet data network gateway
The gateway that terminates the interface towards the PDN. If a UE is accessing multiple PDNs, there may be more than one PGW for that UE.

**PHY**
physical
PHY refers to the physical layer, or L1 of the OSI model.

**Pi**
The reference point between the PGW and the PDSN.

**PIC**
prefix independent convergence

PIC is a method for speeding up convergence of the FIB under failover conditions in large networks, by using a hierarchical path structure in the FIB.

**PID**

PID is expanded in two ways:

1. protocol identification

   A two-octet field in a SNAP header that specifies the protocol type.

2. packet identification

**PIM**
protocol independent multicast
PIM is a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN or the Internet. It is termed protocol-independent because PIM does not include its own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols such as BGP, IS-IS, OSPF, RIP, or static.

**PIM snooping**
PIM snooping for VPLS allows a VPLS PE router to build multicast states by snooping PIM protocol packets that are sent over the VPLS. The VPLS PE then forwards multicast traffic based on the multicast states.

**PIM-SM**
PIM sparse mode

**PIM-SSM**
PIM-source specific multicast

**ping**
packet Internet groper
An ICMP echo message and its reply. Often used in IP networks to test the reachability of a network device.

**PIP**
provider instance port
A PIP is a backbone edge bridge port that can transmit or receive frames from one or multiple customers, adding or removing I-TAGs. In the context of SR PBB, it could be the I-Site “port” that is connected to the B-Site.

**PIR**
peak information rate
The PIR is the peak data transfer rate for a path, such as a frame relay, VPC, VCC, or DE service path. The PIR is the PCR converted to kb/s.

**PKI**
public key infrastructure
PKI represents the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke public key certificates based on public-key cryptography.

**PLAR**
Private Line Automatic Ringdown

**PLMN**
public land mobile network
Typically the mobile network run by one network operator in one country. See 3GPP TS23.002 Section 3.1.*

**PLR**
point-of-local-repair
A functional NE in a path in which a manual bypass is implemented for a defective NE in the path.

**PM**
path monitoring
For an optical channel data unit.

**PMC**
packet microwave card

**PMIP**
proxy mobile IP
A network-based mobility management protocol. It is an amendment to mobile IPv6 which allows mobility control to be moved from the mobile node to a proxy in the network.

**PMIPv6**
proxy mobile IPv6
A network-based mobility management protocol. It allows mobility control to be moved from a mobile NE to a proxy in the network.

**PMSI**
provider multicast service interface

**PMT**
program map table

**POA**
program off-air

**PoE**
power over Ethernet
A technology that provides in-line power directly from switch Ethernet ports. PDs such as IP phones, wireless LAN stations, Ethernet hubs, and other access points can be plugged directly into an Ethernet port. The Ethernet port provides both electrical power and data flow.

**PoE Plus**
power over Ethernet plus
A technology that provides greater in-line power over Ethernet than PoE.

**PoE+**
See “PoE Plus” (p. 94) . See also “PoE” (p. 94) .

**POS**
packet over SONET
A technology that allows IP packets to be sent directly over SONET/SDH frames.

**PPP**
Point-to-Point Protocol
PPP is a protocol for communication between two computers using a serial interface, typically a PC connected by phone line to a server. PPP uses IP. It is considered as a member of the TCP/IP suite of protocols.

**PPP Magic Numbers**
Magic numbers are identifiers which are inserted into PPP control packets and are sent to the other end of the link in the form of an echo. The echo-request should be answered with an echo-reply containing the magic number of the other end. See "PPP" (p. 95) .

**PPPoE**
Point-to-Point Protocol over Ethernet
See also "PPP" (p. 95) .

**PPPRF**
Point-to-Point Protocol over Radio Frequency
See also "PPP" (p. 95) .

**PPTP**
Point-to-Point Tunneling Protocol
A protocol that provides VPN connections for home or mobile users to gain secure access to an enterprise network. Encrypted payload is transported over a GRE tunnel that is negotiated over a TCP control channel.

**prefix**
The first 64 bits of an IPv6 address that identify the network to which a host belongs. The IPv6 prefix is analogous to the IPv4 subnet mask.

**primary CMM**
primary chassis management module
When switches operate in a stack, one switch in the stack, known as the primary CMM, always performs the primary management role.

**property form identifier link**
A window identifier link is a unique internal address that the NFM-P assigns to a form or window.

**PS FCI**
Packet Switched Furnish Charging Information
Specific information about an online charging session. PS FCI includes charging information per rating group when it is sent by the OCS. See 3GPP 32.298.

**PSE**
power source equipment
PSE provides power to a single link section. The PSE main functions include searching the PD, optionally classifying the PD, supplying power to the link section if the PD is

detected, monitoring the power on the link section, and scaling power back to detect level when power is no longer requested or required.

**pseudonode**
A pseudonode is the LAN identifier for a broadcast subnetwork (ISIS).

**pseudowire**
A mechanism that emulates the essential attributes of a service such as ATM, frame relay, or Ethernet over a PSN.

**PSI**
program specific information

**PSN**
packet-switched network
A data-transmission network that uses the packet-switching technique. Unlike circuit switching, packet switching allocates multiplexing and switching resources only when data is present. There are public and private packet-switched networks.

**PSN**
pseudonode number
A one-octet field in an ISIS header that specifies the virtual node identifier in a type 24 TLV.

**PSNP**
partial sequence number PDU
A PDU that is sent by a router, which has established an adjacency with a neighboring router, to transmit link-state information to ensure synchronization of routing tables throughout the network.

**PSS**
Photonic Service Switch

**PST**
Primary state

**PTB**
Packet Too Big
A PTB message is sent when a router receives a packet with a size that exceeds the MTU of the link.

**PTP**
Precision Time Protocol
A time synchronization protocol for networks.

**PVC**
permanent virtual circuit
A PVC is an ATM end-to-end logical connection that extends between host interfaces on a network. A single PVC may pass through several ATM switching devices.

**PVP**
permanent virtual path
A permanent ATM connection that is used to carry one or more PVCs.

**PVST**
Per-VLAN spanning tree
PVST maintains a spanning tree instance for each VLAN configured in the network to help load balance L2 traffic without causing spanning tree loops.

**PW**
See “pseudowire” (p. 96) .

**PWRSV**
Power-save mode

**PXC**
Photonic Cross Connect

## Q

**QAM**
quadrature amplitude modulation

**QCI**
quality of service class identifier
A parameter of the QoS profile of an EPS bearer. It is a scalar quantity that refers to access-device-specific parameters that control bearer-level packet forwarding treatment, for example, scheduling weights, admission thresholds, queue management thresholds, and link layer protocol configuration. See 3GPP TS23.401 Section 4.7.3 and TS23.203 Annex J.*

**QinQ**
QinQ is a type of Ethernet encapsulation in which a second 802.1Q VLAN tag is added to an 802.1Q frame. Service providers can then use VLAN IDs to segregate customer services and still allow customers to assign their own VLAN IDs without the possibility of ID duplication.

**QL**
quality level

**QoE**
quality of experience

**QoS**
quality of service
QoS is a term for the set of parameters and their values that determine the performance of a virtual circuit. A service level is typically described in terms of network delay, bandwidth, and jitter.

**QPPB**
QoS policy propagation via BGP
QPPB is a mechanism that allows propagation of QoS policy and classification by the sending party, based on access lists, community lists and AS paths, thereby helping to classify based on destination instead of source address.

**QSFP**
Quad Small Form-factor Pluggable
QSFP ports allow a single port to serve as four independent port connections, to increase port density on a device. See also "SFP" (p. 109).

**QSFP+**
Quad Small Form-factor Pluggable (enhanced)
An enhanced version of QSFP that supports data rates up to 10 Gb/s. See also "QSFP" (p. 97).

## R

**R-APS**
ring automatic protection switching

**R-VPLS**
routed VPLS
A routed VPLS connector joins an L3 access interface on an IES or VPRN service to a VPLS service on the same site.

**RAB**
radio access bearer

**RADIUS**
remote authentication dial-in user service
A remote user authentication, authorization, and accounting protocol.

**RAE**
remote antenna extension

**RAM**
random access memory
A group of memory chips that function as the primary workspace of the computer. Each byte of storage in the chip can be directly accessed without regard to the bytes before or after it.

**RAN**
radio access network

**RAT**
radio access technology
The RAT is the type of radio technology used in a radio access network (RAN) to access the core network (CN), e.g. UMTS, GSM, CDMA2000.

**rating group**
An AVP, within the MSCC AVP, that is used to indicate service. Each quota allocated to a Diameter credit control session has a unique rating group value.

**RCA**
root cause analysis
Problem solving methods used to determine the root cause of a problem.

**RD**
route distinguisher
An eight-byte BGP field that allows an operator to create a distinct route to a common IP address prefix.

**RDI**
remote defect indication
A signal sent to transmitting equipment by receiving equipment when defects are detected on an incoming signal.

**RED**
random early detection
RED is an algorithm that detects and avoids traffic congestion in a PSN. Incoming congestion is detected by calculating the average queue size. If the gateway decides that the average queue size exceeds a predetermined threshold, it either randomly drops packets arriving at the gateway, or sets a bit in the packet headers. The packet transmission rate is reduced until all the packets reach their destination.

**reference**
A reference is used by the CPAM to determine the existence of an object, and determines the color of objects and links on the GUI topology maps.
See "checkpoint (regular)" (p. 25) .

**Relay Information Option**
The Relay Information Option is defined in RFC 3046 and allows a DHCP relay agent to append to the relayed DHCP request information that identifies where the originating DHCP request was sent. Also known as Option 82.

**residential subscriber**
See "subscriber" (p. 116) .

**resync**
An OSS operation that maintains a local mirror of NFM-P state information, such as inventory or current alarm states, performs a resync when it knows or suspects that the locally stored state information is out of sync with the state information stored in the NFM-P. The OSS does this by requesting information via the XML API. An OSS that does not monitor events periodically performs resyncs to maintain synchronization with the NFM-P. An OSS that does monitor events requires a resync in situations where there are missed events.

**RET**

RET is expanded two ways:

1. retransmission
2. remote electrical tilt

**RF**
radio frequency

**Rf**

Rf is:

- the reference point between an "IMS" (p. 56) element and the "OCS" (p. 84)
- the interface between the "SGW" (p. 109) and the "CCF" (p. 23)

**RFC**
request for comments
A document that describes a technology specification. RFCs are used by the IETF and other standards bodies.

**RFM**
radio frequency module

**RG**
rating group

**RHEL**
Red Hat Enterprise Linux
RHEL is the supported "Linux" (p. 64) distribution for NFM-P deployment.

**RIB**
routing information base
A router database that contains the routing information necessary for packet forwarding.

**ring group**
A group of network devices that connect to each other in a ring topology for the efficient distribution of multicast or broadcast network traffic.

**RIP**
Routing Information Protocol
RIP is a Bellman-Ford routing protocol based on distance vector algorithms, which measure the shortest path between two points on a network in terms of the number of hops between those points. Various forms of RIP distribute routing information in IP, XNS, IPX, and VINES networks.
See also "OSPF" (p. 88) .

**RJ-45**
registered jack 45
A telephone connector that holds up to eight wires. RJ-45 plugs and sockets are used in Ethernet and Token Ring Type 3 devices.

**RMI**
remote method invocation
A standard for distributed objects written in Java. RMI is a remote procedure call that allows Java objects to be managed remotely.

**RMON**
remote network monitoring

**RMS**
resource management server

A server that tracks the use of services in a network by an end host. An RMS can enforce quotas, ensure that specific service levels are met, optimize resources, manage IP addresses, and generate real-time active session reports.

**RNC**
radio network controller
Controls radio resource management in the radio access networks of universal mobile telecommunications systems. An RNC is equipment in the UTRAN radio network subsystem that manages the use of radio resources.

**RNCV**
ring node connectivity verification

**ROADM**
Reconfigurable Optical Add/Drop Multiplexer
An optical network element with a configuration that can be changed remotely. This remote reconfigurability reduces “OPEX” (p. 85) when operating a “DWDM” (p. 37) network. “OPEX” (p. 85) is reduced because the ROADM eases network provisioning and line tuning at both the initial installation and any upgrades (to increase the capacity or re-allocate resources to a new demand matrix).

**root bridge**
The bridge with the highest priority ID, selected as the root in a spanning tree.

**route flapping**
A routing problem caused by network problems where an advertised route between two devices changes back and forth between two different paths.

**router**
An interface device that connects two networks. It maintains configuration tables and uses various network protocols to select cost-effective routes that move data between a source and destination device. Also called a device.

**routing domain**
In OSPF, a routing domain is an OSPF area. In IS-IS, a routing domain does not map to the ISIS area, but is a group of routers that participate in an ISIS level, that are visible to each other in their link state database.

**routing instance**
The configuration of a router, including information such as protocols, interfaces, routing, and policies.

**routing protocol**
A routing protocol is used to determine the correct route for packets within IP and IP /MPLS networks.

**RP**
rendezvous point
An RP is a PIM-enabled router that is elected by PIM as a central distribution source for multicast groups in a multicast domain.

**RPC**
remote procedure call
An RPC is a procedure call between applications that run on the same or different stations.

**RPF**
reverse path forwarding
A mechanism used by PIM to forward multicast packets down a distribution tree.

**RPL**
ring protection link
Loop avoidance in an Ethernet Ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links which is designated as the RPL.

**RPS**
radio protection switching

**RRH**
remote radio head

**RS-232-C**
recommended standard - 232 - current
The physical interface and protocol used to connect serial devices.

**RSA**
Rivest, Shamir, Adleman
RSA is an algorithm for public key encryption in which a public key consists of the product of two prime numbers and an auxiliary value.

**RSHG**
residential split horizon group
A type of SHG with dual-pass queue optimization. Downstream broadcast and multicast traffic are not supported. SAPs associated with an RSHG are lightweight SAPs.

**RSM**
residential subscriber management
A versatile TPSDA model, sometimes called enhanced subscriber management, which supports a variety of delivery configurations, such as one VLAN per host, one VLAN per application, one VLAN for all applications, and one VLAN per service provider per application. See “subscriber” (p. 116) .

**RSRP**
reference signal received power

**RSRQ**
reference signal received quality

**RSTP**
Rapid Spanning Tree Protocol
RSTP is an enhanced version of STP, as defined in IEEE standard 802.1w-2001 and incorporated in IEEE standard 802.1D-2004. RSTP supersedes STP for standards

conformance. RSTP provides faster automatic reconfiguration for route failures than STP by facilitating a rapid change in port roles.

**RSVP**
Resource Reservation Protocol
RSVP is a network-control protocol in the IP suite that is used for communicating application QoS requirements to intermediate transit NEs in a network. RSVP uses a soft-state mechanism to maintain path and reservation states on each NE in the reservation path.

**RSVP-TE**
resource reservation protocol-traffic engineering
RSVP-TE is an extension of RSVP that is described in RFC 3209. RSVP-TE allows the establishment of LSPs based on network constraints such as available bandwidth and explicit hops.

**RT**
route target or retransmission
In BGP/MPLS VPNs, an RT is an attribute that identifies a set of sites.

**rt-VBR**
real-time variable bit rate
rt-VBR is a variant of the VBR service category available only for VPC paths and VCC paths. It allows statistical multiplexing gains using the traffic descriptors (PCR and SCR), and provides delay commitments. rt-VBR supports variable bit rate traffic with sustained and peak traffic parameters, which require strict delay control, such as packetized voice or video.
An rt-VBR is an ATM service category that guarantees very low cell loss and very low delay for time-sensitive applications such as voice and video, which are characterized by unpredictable, bursty transmission patterns.
rt-VBR is a variant of the VBR service category that is only available for VPC and VCC paths. nrt-VBR is the other variant of VBR available for these paths.

**RTM**
routing table manager
An RTM is an application that operates in a multiprotocol network to create and maintain a RIB that contains all active static routes in the network. The RTM calculates the best routes from the RIB and stores the information in the FIB.

**RTU**
remote terminal unit
A remote monitoring and control device used in industrial networks. An RTU, also called a slave or remote, typically uses RS-232 links back to the master.

**RUC**
rack user commissioning
An RUC is an eNodeB component that is comprised of front and back RUC cards and a fan rack.

**RVPLS**
Routed VPLS

Routed VPLS allows a VPLS instance to be associated with an IES IP interface. Traffic with a destination MAC matching that of the associated IP interface is routed based on the IP forwarding table; all other traffic is forwarded based on the VPLS forwarding table.

**rwa**
read-write access

## S

**S-GW**
See "SGW" (p. 109) .

**S-PE**
switching-provider edge
In "MS-PW" (p. 76) routing, switching-provider edge NEs are automatically created to forward inter-domain traffic between "T-PE" (p. 117) NEs.

**S-PMSI**
selective provider multicast service interface

**S1**
The interface between an eNodeB and the Core Network (CN). See 3GPP TS36.300 Section 19 and TS36.410 to TS36.414.*

**S1-U**
S1-user plane
Provides non-guaranteed delivery of user plane "PDU" (p. 91) s between the eNodeB and the "SGW" (p. 109) . It is built on "IP" (p. 57) transport, and "GTP-U" (p. 49) is used on top of "UDP" (p. 123) / "IP" (p. 57) to carry the user plane "PDU" (p. 91) s between the eNodeB and the "SGW" (p. 109) . It supports inter-eNodeB path switching during handover. See 3GPP TS36.300 Section 19.1 and TS36.414.*

**S11**
The interface between the "SGW" (p. 109) and the "MME" (p. 73) .

**S12**
The interface between the "SGW" (p. 109) and the "RNC" (p. 101) .

**S2a**
A reference point that provides the user plane with control and mobility support between trusted non- "3GPP" (p. 5) "IP" (p. 57) access and the mobile gateway.
The interface between the PGW and the TWAN.

**S2b**
A reference point that provides the user plane with control and mobility support between the "ePDG" (p. 40) and the mobile gateway.

**S4**
An interface between the "SGW" (p. 109) and "SGSN" (p. 109) that provides control and mobility support between the "GPRS" (p. 48) core and the "3GPP" (p. 5) anchor function of the "SGW" (p. 109) .

**S5**
The interface between the “SGW” (p. 109) and the “PGW” (p. 92) in the same “PLMN” (p. 94) .*

**S6b**
The Diameter interface between the “PGW” (p. 92) and the “3GPP” (p. 5) “AAA” (p. 10) server/proxy.

**S8**
The interface between the “SGW” (p. 109) and the “PGW” (p. 92) in different “PLMN” (p. 94) s.*

**SA**
security association
The establishment of shared security information between two IPsec peers to support secure communication.

**SAA**
service assurance agent
The SAA is a tool that allows operators to configure a number of different tests that can be used to provide performance information such as delay, jitter, loss of services, or network segments. The test results are saved in SNMP tables or summarized XML files.

**SAE**
system architecture evolution
The part of the evolved packet system (EPS), which involves non-radio aspects. It includes the evolved packet core (ePC) network, and accompanies LTE.*

**SAE-GW**
SGW combined with PGW/GGSN

**SAFI**
Subsequent Family Address Identifier
See “AFI” (p. 12).
BGP messages in which AFI=1 and SAFI=66 are "MDT-SAFI" messages.

**SAII**
Source Attachment Individual Identifier

**SAM-L**
security assertion markup language
An XML-based standard for exchanging authentication and authorization data between security domains, such as identity providers (producers of assertions) and service providers (consumers of assertions). SAM-L is a product of the OASIS Security Services Technical Committee.

**SaMOG**
S2a Mobility Over GTP
*See* “TWAG” (p. 122)

**SAP**
service access point

A SAP is a point of communication exchange between an application and the LLC, or between layers of software.

**SAS**
service assurance system
SAS refers to the grouping of OAM diagnostic tests into test suites for end-to-end testing of customer services. SAS test suites can be scheduled. They can provide more network monitoring and troubleshooting capability than individual OAM activities.

**SC**
service component
An SC is a customer service that is a component of a composite service.

**SC AP**
Small Cell Access Point
The SC AP is a low-powered wireless device that is part of the Small Cells solution. The SC AP provides high-performance data and voice communications services, and is designed to improve coverage and increase network capacity. The SC AP has reduced radius and user capacity in comparison to a macro cell. An SC AP can occasionally be referred to as a Femto: an older name that has been discontinued, yet survived in some areas of the NFM-P client GUI.

**SC GW**
Small Cell Gateway
The SC GW is an NE that is part of the Small Cells solution, and interconnects the SC APs and the mobile core network. The SC GW performs software management, fault management, performance management, and backup and restore functions. An SC GW can occasionally be referred to as an FGW (Femto Gateway): an older name that has been discontinued, yet survived in some areas of the NFM-P client GUI.

**SCADA**
Supervisory Control And Data Acquisition
An industrial data management system that monitors and controls IEDs

**SCATCA**
Small Cell ATCA
The SCATCA is a Small Cells logical object that represents the hardware chassis in which the blade-based SC GWs are installed. The SCATCA object includes the ATCA chassis, two shelf management cards and two switching blades.

**SCP**

SCP is expanded two ways:

1. secure copy protocol

   The SCP securely transfers files between local and remote hosts, or between two remote hosts, using SSH2.

2. service connection point

   An SCP is a type of connector endpoint in a composite service. It can be a SAP, service interface, or network port, depending on the device.

**SCR**
sustainable cell rate
An upper limit on the conforming average rate of an ATM connection. An SCR uses a time scale that is long relative to the time scale of the PCR.

**SCTE35**
society of cable telecommunications engineers

**SCTP**
Stream Control Transmission Protocol
A transport layer protocol, similar to TCP and UDP. Like TCP, SCTP ensures that data is transported across the network sequentially and without error. SCTP is also similar to TCP in that a relationship is created between the endpoints of an SCTP session before the data is transmitted, and this relationship is maintained until the data transmission is completed.
Unlike TCP, SCTP provides multi-streaming and multi-homing, which increase performance and reliability of the Diameter application message exchange.
Multi-streaming allows data to be partitioned into multiple streams that can be delivered independently, so that message loss in any of the streams only affects delivery within that stream.
Multi-homing is the ability of an SCTP endpoint to support multiple IP addresses, which can mean greater survivability of the session in the presence of network failures. In a single-homed session, the failure of a local LAN access can isolate the end system, while failures within the core network can disrupt transport until the IP routing protocols reconverge around the point of failure. With multi-homed SCTP, redundant LANs can be used to reinforce the local access and, in the core network, the risk of failure from one address can be reduced.

**Sd**
The interface between the PCRF and the TDF/SSG.

**SDC**
service data container

**SDF**
service data flow
An aggregate set of packet flows that match a set of filters based on packet headers, such as source and destination IP addresses, in a policy and charging control rule. See 3GPP TS23.203.*

**SDH**
synchronous digital hierarchy
SDH is a hierarchical set of digital transport structures, standardized for the transport of suitably adapted payloads over physical transmission networks. SDH is a standard for communicating digital information over optical fiber and microwaves. SDH was developed to replace the PDH system for transporting large amounts of telephone and data traffic.

**SDI**
serial data interface

An SDI is an MDA configurable on the 7705 SAR-8/18. It can be configured to operate in access mode for a V35, RS232, or X.21 interface.

**SDM**
subscriber data management
SDM is a central repository used by carriers to consolidate and manage subscriber data across multiple domains. The data can include subscriber presence, preferences, authentication, services, identities, and location.

**SDP**
service distribution point
The NFM-P uses this term interchangeably with service tunnel.

**SDRAM**
synchronous dynamic random-access memory
The NFM-P uses this term interchangeably with service tunnel.

**SDU**
service data unit
An SDU is a unit of information from an upper-layer protocol that defines a service request to a lower-layer protocol.

**secondary CMM**
secondary chassis management module
When switches operate in a stack, one of the switches in the stack operates in a secondary management role. This switch serves as a backup, and is always ready to perform the primary management role if the primary CMM fails or is taken offline.

**section**
A single fiber run that an NE or optical regenerator terminates. The main functions of the section layer are to properly format the SONET frames and to convert the electrical signals to optical signals.

**SEG**
security gateway
A SEG is one or both ends of an IPsec tunnel.

**service class indicator**
A 3GPP standard that identifies the service class associated with downlink user plane packets, so that the GERAN can optimize the deployment of radio resources for packet-switched traffic.

**service tunnel**
A service tunnel acts as a logical way of unidirectionally directing traffic from one device to another device. The service tunnel is provisioned to a specific encapsulation method, such as GRE, and the services are mapped to the service tunnel. A distributed service spans more than one router. Distributed services use Service Distribution Points to direct traffic to another router through a service tunnel.

**service-level agreement**
See “SLA” (p. 110) .

**SES**
severely errored second
A one-second interval during which the error ratio on a transmission line is greater than a specified limit, and transmission performance is significantly degraded.

**set-top box**
A set-top box is a type of residential subscriber end-user device that receives network traffic. An example of a set-top box is a consumer device that converts BTV IP data into video and audio signals for a television.

**SFC**

SFC is expanded two ways:

1. Static Filter CWDM

   A static filter card used with a CWDM circuit pack.

2. Service Function Chain

**SFD**
Static Filter DWDM
A static filter card used with a DWDM circuit pack.

**SFM**
Switch Fabric Module

**SFP**
Small Form-factor Pluggable
A high-speed, compact, and hot-swappable optical modular transceiver.

**SFP+**
Small Form-factor Pluggable (enhanced)
An enhanced version of SFP that supports data rates up to 10 Gb/s. See also “SFP” (p. 109) .

**SFTP**
Secure File Transfer Protocol
A secure file transfer protocol is included with version 2 of the SSH application.

**SGi**
The reference point between the PGW and the PDN.

**SGSN**
serving GPRS support node
SGSN mediates access to network resources, on behalf of mobile subscribers, and implements the packet scheduling policy between different QoS classes. SGSN establishes the Packet Data Protocol context with the GGSN upon activation. See also “GGSN” (p. 46) .

**SGW**
serving gateway
The SGW is positioned at the edge of the eUTRAN and terminates the connection from the eNodeB.

**SHA**
secure hash algorithm
A NIST standard hash algorithm, also known as SHA-1.

**SHCV**
subscriber host connectivity verification
A method of using periodic ARP requests and DHCP snooping to maintain connectivity state information for the subscriber hosts on a SAP.

**SHG**
split horizon group
A group of SAPs or spoke SDPs. Members of the group cannot send traffic to each other.

**SID**
Segment Identifier
SIDs are used in segment routing.

**SIP**
session initiation protocol
An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.

**SLA**
service-level agreement
An SLA is a service contract, between a network service provider and a customer, which guarantees a specific QoS level. SLAs specify criteria such as network availability and data delivery reliability.

**SLM**
synthetic loss measurement
Ethernet synthetic loss measurement is used to count the number of synthetic "LM" (p. 65) frames which are not successfully delivered to the specified destinations.

**SLOF**
section loss of frame
A field in a SONET channel frame that indicates the loss of a frame in the section frame sequence.

**SLOS**
section loss of signal
A field in a SONET channel frame that indicates the loss of section signaling.

**Smart SFP RMD**
The Gigabit Ethernet demarcation device managed by 1830 PSS to provide the customers service visibility at the network edge demarcation in applications like business Ethernet and carrier wholesale, and mobile backhaul.

**SMI**
structure of management information

A description of the common structure and identification scheme for the definition of information used to manage TCP/IP-based internetworks. Formal descriptions of the structure are provided using ASN.1. SMI, which is defined in RFC 1155.

**SMM**
Site Monitoring Module

**SMS**
short message service
A communication service component of the GSM mobile communication system, using standardized communications protocols that allow the exchange of short text messages between mobile devices.

**SMTP**
simple mail transfer protocol
An application in the TCP/IP suite that manages the sending and receiving of e-mail messages.

**SNAP**
subnetwork access protocol
An Internet protocol that operates between a network entity in the subnetwork and a network entity in the end system. The SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks. The SNAP entity in the end system uses the subnetwork services and performs three key functions: data transfer, connection management, and QoS selection.

**SNCI**
subnetwork connection (protection) inherent monitoring

**SNCN**
subnetwork connection (protection) non-intrusive monitoring

**SNCNC**
subnetwork connection non-intrusive monitoring client protection

**sniffer**
A software tool that is used to monitor and analyze network traffic for troubleshooting or surveillance purposes.

**SNMP**
Simple Network Management Protocol
A protocol used for the transport of network management information between a network manager and an NE. SNMP is the most commonly used standard for interworking devices.

**SNMP trap**
An SNMP trap is an unsolicited notification that indicates that the SNMP agent on an NE has detected an event, and that the network management domain should be aware of the event. SNMP trap information typically includes alarm and status information, and standard SNMP messages.

**SNMP trap log ID**
SNMP trap log ID is the ID of a log. A valid log ID must exist for alarms and traps to be sent to the trap receiver.

**SNTP**
Simple Network Time Protocol
A rudimentary version of NTP with only the features that devices commonly require.

**SOAP**
Simple Object Access Protocol
An XML-based protocol for the exchange of information in a decentralized, distributed environment.

**SON**
self-organizing network
SON is a 3GPP standard for LTE RAN that includes functions such as self-optimization, self-healing, “ANR” (p. 14) , and “PCI” (p. 90) .

**SONET**
synchronous optical network
SONET is an ANSI standard for fiber optic transmission of high-speed digital traffic. SONET allows internetworking of transmission products from multiple vendors and defines a physical interface, optical line rates known as OC signals, frame format, and an OAM protocol. The base rate is 51.84 Mb/s (OC-1), and higher rates are multiples of the base rate.
SONET uses synchronous high-speed signals and provides easy access to low-speed signals by mapping them into VTs.
SONET is a North American standard that is technically consistent with SDH, which is an international standard.

**SPB**
shortest path bridging
SPB, defined in IEEE 802.1aq, simplifies how customers create and configure networks—across the enterprise and for the cloud— by requiring service provisioning only at the edge of the network. It uses IS-IS to dynamically build the topology between NEs, enabling multipath routing and virtually eliminating human error.

**SPF**
shortest path first
SPF is an algorithm used by IS-IS and OSPF to make routing decisions based on the state of network links.

**spoofing**
A technique used to gain unauthorized access to devices, whereby the intruder sends messages using a source IP address that appears to come from a trusted host.

**SPT**
shortest path tree
SPT is an algorithm used by PIM to make routing decisions based on the state of network links.

**SPV**
set parameter values
Type of TR-069 RPC method.

**SQL**
structured query language
A specialized language for accessing relational databases.

**SR**

SR is expanded in three ways:

1. short reach

   An optical interface specification for distances of less than 2 km.

2. service router

   A network router, for example, the 7750 SR, that supports the creation of IP and MPLS network-layer services such as IES and VPRN services.

3. segment routing

   Segment routing adds to the IS-IS and OSPF routing protocols the ability to perform shortest path routing and source routing using the concept of abstract segment.

**SR TE**
segment routing with traffic engineering

**SRLG**
shared risk link group
A situation in which links in a group share a common attribute, whose failure may affect all of the links in the set.

**SRRP**
Subscriber Routed Redundancy Protocol
A set of functions and messaging protocols that allows a system to create a set of redundant gateway IP addresses shared by local and remote NEs.

**srTCM**
single rate three color marking

**SSAP**
source service access point

**SSD**
source statistics descriptor
The characteristic of traffic in the conversational UMTS traffic class. The SSD can be either speech or unknown.

**SSG**
service selection gateway
The SSG provides policy-driven traffic steering and service chaining, which provides the network carrier with the ability to quickly introduce new services and the flexibility to introduce value-added services to the user traffic path.

**SSH**
secure shell
The SSH protocol is used to protect communication between two hosts by encrypting a Telnet, FTP, or SCP connection between the NEs. Both ends of the connection are authenticated, and passwords are encrypted.

**SSH2**
SSH version 2
SSH2 is a more secure, efficient, and portable version of SSH that includes SCP. See “SSH” (p. 113) .

**SSID**
Service Set Identifier
An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must use the same SSID in order to communicate with each other.

**SSL**
secure socket layer
The SSL is a protocol developed by Netscape for transmitting private documents using the Internet. Many web sites use the protocol to obtain confidential user information, such as credit card numbers. The protocol is also used for data encryption, server authentication, and message integrity between NFM-P servers and single-user GUI clients, as well as between NFM-P servers and client delegate servers.

**SSLF**
section synchronization line failure
A SONET alarm that indicates a failure of the frame synchronization for a section.

**SSM**
source-specific multicast
An extension of PIM that enables a receiving client to obtain content directly from the source rather than from the shared RP.

**SSM**
synchronous status message

**SSO**
single sign on

**SST**
secondary state

**SSU**
synchronization supply unit
A timing synchronization unit that filters and distributes synchronization signals to local equipment.

**STa**
The interface between the 3GPP AAA proxy/server and theTWAN. The STa reference point is used to authenticate and authorize the UE, to transport PMIPv6, and to transport charging-related information and information about IP mobility mode selection.

**standby**
A standby database or standby server is an NFM-P component that is not currently in service, but provides protection for the active system. For example, the standby server is a system that can read and write to the active database. However, it is in standby mode, and ignores events from the network. An NFM-P client cannot connect to a standby server.

**static host**
See "static subscriber host" (p. 114) .

**static MAC**
A MAC address that is manually configured in a FIB, rather than dynamically learned. Static MAC addresses are assigned to network objects such as SAPs, SDPs (service circuits), or endpoints.

**static subscriber host**
A host that is explicitly configured on a SAP rather than through a dynamic learning process.

**station**
A generic term for a physically discrete piece of processing or transmission equipment, for example, a personal computer or mobile communication relay agent. See also "workstation" (p. 131) .

**statistics**
Statistics are the quantitative data collected by the NFM-P for entities such as equipment, network protocols, interfaces, and alarms.

**STB**
See "set-top box" (p. 109) .

**STE**
section terminating equipment
SONET equipment that originates, accesses, modifies, or terminates section header information.

**STM**

STM is expanded two ways:

1. service test manager

   An NFM-P facility that allows the manual creation and automatic generation of tests and test suites. STM tests and test suites can be run on demand or scheduled to run periodically on services and service transport components for SLA QoS validation and troubleshooting.

2. synchronous transfer mode

   The synchronous end-to-end transmission of data or voice containers in a network. STM is a component of SDH.

**STM-N**
synchronous transfer mode - level *N*
An SDH signal carried at the speed of *N*; for example, STM-4 is a signal at 622.08 Mb/s.

**STP**
Spanning Tree Protocol
The STP is specified in IEEE 802.1D. This protocol automatically ensures a loop-free topology in any interconnection of Ethernet LAN or WAN devices.

**STP 1x1 mode**
The STP 1x1 mode is a proprietary implementation of the STP that applies a single spanning tree instance per VLAN.

**STP flat mode**
The STP flat mode applies a single spanning tree instance per switch. In the STP flat mode, when you choose MSTP as the STP mode, you can configure MSTIs in addition to the CST instance. Each MSTI is mapped to a set of VLANs. Therefore, flat mode supports the forwarding of VLAN traffic over separate data paths.

**strict priority**
In strict priority scheduling, each CoS queue associated with the egress port is serviced in priority order from highest 7 to lowest 0. All traffic for a specific CoS is transmitted before the scheduler proceeds to the next highest priority queue. The purpose of strict priority scheduling is to ensure lower latency and priority transmission of critical traffic by always transmitting higher priority traffic before lower priority traffic.

**STS**
synchronous transport signal
The electrical equivalent of the SONET optical signal. In SDH, STS is known as STM.

**subscriber**
In the NFM-P, a subscriber represents a unique identifier that associates a group of end-user devices with policies and resources.

**subscriber host**
In the NFM-P, a subscriber host is an end device, such as a set-top box, that receives the network traffic. See also “host” (p. 51) .

**subscriber instance**
In the NFM-P, a subscriber instance refers to the instantiation of a specific subscriber and the associated policies on a device. A subscriber may have multiple subscriber instances in a network, but only one instance on a specific NE.

**SVLAN**
service provider VLAN

**sVOA**
slow variable optical attentuator

**switch**
Switches are Layer 2 devices that make it possible for several users to send information over a network at the same time without slowing each other down. Switches allow different NEs to communicate directly with one another in an efficient manner.

**switch fabric processor**
A processor that handles traffic passing through the switch fabric.

**switchover**
Switchover is the process of switching the roles of a redundant system; for example, switching the roles of an active and standby database. A switchover is reversible.

**SWm**
The reference point between the EPDG and 3GPP AAA server. SWm uses Diameter protocol for communication.

**SWu**
The reference point between the UE and EPDG. SWu uses the IPsec tunnel to carry bearer traffic between the UE and EPDG.

**SWw**
The interface between the UE and the TWAN.

**SYN**
synchronize
SYN is a message that is sent by TCP during the initiation of a new connection to synchronize the TCP packet sequence numbers on the connecting computers. The SYN is acknowledged by a SYN/ACK from the responding computer.

**SYN/ACK**
synchronize acknowledged
An SYN/ACK is a message that is sent by TCP during the initiation of a new connection in response to a synchronization attempt from another computer.

**SyncE**
See “Synchronous Ethernet” (p. 117) .

**Synchronous Ethernet**
An ITU-T standard for transmitting clock signals over an Ethernet network. Clock signals are traceable to an external master clock that meets certain accuracy requirements.

## T

**T-LDP**
Targeted-Label Distribution Protocol
An LDP session between indirect connect peers.

**T-PE**
termination-provider edge
In “MS-PW” (p. 76) routing, termination-provider edge NEs are the endpoints of the MS-PW service. T-PEs are configured with PW SDPs that connect to “S-PE” (p. 104) NEs.

**T1**
A 1.544-Mb/s point-to-point dedicated digital circuit provided by the telephone companies in North America.

**TAC**

TAC is expanded two ways:

1. technical assistance center

   The front end, or customer-facing, product support structure in which the first- and second-level support reside.

2. tracking area code

**TACACS+**
terminal access controller access control system
A remote user authentication, authorization, and accounting protocol.

**TAF**
time-average-factor
Specifies a weight factor between the previous shared buffer average utilization and current shared buffer instantaneous utilization when a new shared buffer average utilization is calculated.

**TAI**
tracking area identity
An identity used to identify tracking areas, composed of a TAC, an MNC, and an MCC. See 3GPP TS23.003 Section 19.4.2.3.

**TAII**
Target Attachment Individual Identifier

**TCA**
Threshold-crossing alert
A TCA occurs when a statistics counter value crosses the defined threshold during a 15-min interval.

**TCE**
trace-collection entity

**TCN**
topology change notification
A bridge uses TCN BPDUs to notify the root bridge about a detected topology change.

**TCP**
Transmission Control Protocol
TCP is a protocol used, along with the IP, to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

**TCP/IP**
transmission control protocol/Internet protocol

TCP/IP is a set of protocols that link different computers across many kinds of networks. It is commonly used over subnetworks, including Ethernet, ATM, frame relay, and leased line. TCP corresponds to the network layer and transport layer of the OSI model. It is a multivendor, non-proprietary standard.

**TDF**
traffic detection function
TDF enables carriers to create personalized application-based services that match subscriber preferences, such as gaming, social networking, and video streaming, by allowing operators to identify subscribers and their applications, content use, and devices. The personalized service also allows for individualized subscriber pricing plans.

**TDM**
time division multiplexing
Multiplexing in which a separate periodic time interval is allocated to each tributary channel in a common aggregated channel.

**TE**
traffic engineering
The process of selecting the paths from one node to another to provide efficient and reliable network operations while considering bandwidth availability and traffic characteristics in an MPLS network.

**TED**
traffic engineering database
A TED is a database used by CSPF for storing route constraint information.

**TEI**
transport error indicator

**telco**
telephone company
A company that provides local, or local and long-distance, telephone services.

**Telnet**
Telnet is an application in the TCP/IP suite that provides remote terminal connection service. It allows a user at one site to interact with a timesharing system at another site as though the user terminal directly connects to the remote system.

**TI-LFA**
See “LFA” (p. 64).

**tiered architecture**
Tiered architecture refers to the way in which the GUI and the network management components use a Java-based technology that provides distributed, secure, and scalable applications. The tiered architecture allows for scaling and fair load balancing, which improves performance.

**TISPAN**
telecommunications and Internet converged services and protocols for advanced networking

TISPAN is the ETSI core competence center for all aspects of standardization for fixed and converged networks, including NGNs. TISPAN defines standards for service aspects, architectural aspects, protocol aspects, QoS support, security-related matters, and mobility aspects within fixed networks to meet the business requirements and commercial objectives of the ETSI members. ETSI TISPAN writes the key standard specifications that define the fixed and converged networks as well as the NGN architecture.

**TLS**
LDAPv3 Transport Layer Security

**TLV**
type length value
Traffic engineering information is carried by signaling objects, such as LDPs. The type, length, and values of this traffic engineering information is specified in the TLV.

**TMA**
tower mounted amplifier
A tower mounted amplifier is a low-noise amplifier for “BTS” (p. 21) .

**TMF**
telemanagement forum
A non-profit global organization that provides leadership, strategic guidance, and practical solutions to improve the management and operation of information and communications services.

**TMN**
telecommunications management network
A TMN is an industry-standard model defined by the ITU-T for the layering of management functions in telecommunications networks.
TMN is a network that interfaces with a telecommunications network at several points to receive information from, and to control the operation of, the telecommunications network. A TMN may use parts of the managed telecommunications network to provide for the TMN communications.

**TMS**
threat management system
A TMS is a server that identifies and removes network and application-layer attacks without interrupting the flow of legitimate traffic.

**TNC**
tech non-conformant

**TOA**
transport stream off-air

**TOADM**
tunable optical add/drop multiplexer
A tunable “ROADM” (p. 101) that yields the ultimate in operational flexibility, especially when used in conjunction with transponders with tunable wavelength lasers.

**ToS**
type of service
An eight-bit field in an IP packet header that contains a three-bit IP precedence value or six-bit DSCP value. This value is used to identify the level of service that a packet receives in the network.

**TPMR**
two port MAC relay

**TPS**
transmission protection switching

**TPSDA**
triple play service delivery architecture
A model of service delivery for triple play that attempts to guarantee delay, jitter, and packet loss characteristics. TPSDA provides QoS customization for high-speed Internet data services with per-user bandwidth controls.

**transit bridge**
An Ethernet switch that resides inside the service provider network and provides a connection between multiple provider networks. The transit bridge uses the same SVLAN on two or more network ports. This SVLAN does not terminate on the switch. Traffic that ingresses a network port is switched to other network ports. The same switch can also function as both a PE bridge and a transit bridge.

**transit SAP**
An access interface on a VLL or VPLS that forwards traffic with any encapsulation values transparently through the service.

**transit service**
A service tunnel that uses transit SAPs to pass traffic for existing VLL or VPLS data services or composite services.

**transport tunnel**
Routers are connected to physical links that are used to carry traffic. When a service is set up using MPLS, transport LSP tunnels are set up between Provider Edge routers. Each service or customer sends traffic through a service tunnel within the transport LSP tunnel. Transport tunnel LSPs are identified by MPLS labels that are swapped at each intermediate NE, or transit LSR, along the LSP from the ingress to the egress of the MPLS network.

**TRDU**
transceiver duplexer unit

**triple play**
Triple play refers to the offering of voice, video and data applications over the same network connection. Triple play services are available through technologies that range from DSL to broadband wireless connections.

**trTCM**
two rate three color marking

**TRU**
top rack unit

**TTL**
time-to-live
A field in an IP header that specifies the maximum number of hops for a data packet before the packet expires and is discarded.

**TU-N**
tributary unit - level *N*
The basic unit of an SDH payload, which includes management overheads and synchronization data. The TU consists of a virtual container and a TU pointer. It provides a unit of bandwidth that is required to convey a T1- or E1-framed carrier.

**TUG**
tributary unit group
A TUG consists of identical TUs. A multiplexing scheme that is used to assemble the TUs into a higher unit of bandwidth.

**tunnel**
A method of setting up a communication session between two or more points that hides the complexity of the underlying technologies.

**tuple**
In programming languages, a tuple is an ordered set of values. The delimiter for each value is often a comma, depending on the rules of the specific language. As a data type, a tuple can be used to pass a string of parameters from one program to another.

**TWAG**
trusted WLAN access gateway
A trusted WLAN access gateway that interfaces with the PGW using the S2a interface. In a trusted access, the UE is connected through a TWAG in the Wi-Fi core, and the TWAG is connected with the PGW using a secure GTP tunnel. The TWAG also acts as a DHCP server for the UE.

**TWAMP**
two-way active measurement protocol
Two-way Active Measurement Protocol (TWAMP), based on the One-way Active Measurement Protocol (OWAMP), adds two-way or round-trip measurement capabilities. The TWAMP measurement architecture is usually comprised of two hosts with specific roles. Devices that implement TWAMP provide the capability to identify performance issues on all IP network segments. TWAMP initiates a control session between any two points in the network using TCP and then sends a test session using UDP packets. The UDP test packets are sent from the client and are reflected by the server, providing a round-trip measurement.

**TWAN**
trusted WLAN access network
The TWAN provides access for UEs across a trusted non-3GPP access network. When the WLAN is considered as trusted by the network operator, the TWAN is interfaced with

the EPC as a trusted non-3GPP access to the PGW using the S2a interface, and to the 3GPP AAA server/proxy using the STa interface.

**TWL**
TWAMP Light
TWAMP Light tests target Layer 3 interfaces. See "TWAMP" (p. 122).

**Tx**
transmit

## U

**u-plane**
See "user plane" (p. 124) .

**UBR**
unspecified bit rate
UBR is an ATM service category that is used for applications, which do not require guarantees of low cell loss or low delay. Specifically, UBR does not include the notion of a per-connection negotiated bandwidth. No numerical commitments are made with respect to the cell loss ratio experienced by a UBR connection, or as to the cell transfer delay experienced by cells on the connection. UBR emulates the connectionless services provided by conventional bridged and routed data networks. It provides best effort delivery.

**UCT**
universal coordinated time
UCT is also known as Greenwich Mean Time.

**UDP**
User Datagram Protocol
A minimal transport protocol above the IP network layer that does not guarantee datagram delivery. The UDP is used by applications that do not require the level of service of TCP or that need to use communications services, such as multicast or broadcast delivery, which are not available from TCP.

**UE**
user equipment
The mobile unit, which allows a user to access network services. The UE connects to the UTRAN or eUTRAN through a radio interface.

**UI**
user interface
See "GUI" (p. 50) .

**UIC**
unit ID code
A field in an MDL message that identifies the CSU or DSU of the originating equipment.

**ULI**
user location information

**UMTS**
Universal Mobile Telecommunication System

**UNI**
user-network interface
UNI is an interface point between ATM end users and a private ATM switch, or between a private ATM switch and the public carrier ATM network. The physical and protocol specifications of the ATM Forum UNI documents define the standard for a connection between end stations and a local ATM network switch.
A switch UNI is a port that resides on a PE bridge and that connects to a customer network and carries customer traffic. The UNI may consist of a single port or a group of ports, and can accept tagged or untagged traffic.

**UNIVTRM**
universal transmission

**UNIX**
A multi-user, multitasking OS on which Linux is modeled.

**URPF**
Unified reverse path forwarding

**URL**
uniform resource locater

**user plane**
The portion of a telecommunications network that is involved with user traffic, including voice, data, and video. See also “u-plane” (p. 123) .

**user VPLS**
A VPLS that contains SAPs that receive multicast traffic from an MVR VPLS.

**USM**
user service manager
A GUI application for a management system. It usually functions as a manager towards an information manager application, but it may also connect directly with the managed system.

**USRPNL**
user interface panel

**USU**
used service unit

**UTC**
Coordinated Universal Time
primary time standard by which the world regulates clocks and time

**UTRAN**
universal terrestrial radio access network
UTRAN consists of RNCs and NodeBs of a UMTS network. UTRAN allows connectivity between the UE and the core network.

## V

**VACM**
view-based access control model
A model of the access control subsystem of an SNMP engine, which defines a set of services that an application can use for checking access rights.

**VAS**
vendor-specific attribute
An attribute that is set by a remote-server vendor to allow a vendor-specific extension of existing remote server attributes.

**VBR**
variable bit rate
VBR is an ATM service category that provides guaranteed low cell loss and low delay for applications such as video and frame relay, and is characterized by an on/off source with known, predictable transmission patterns. During the on period, cells are transmitted at the peak information rate. No cells are transmitted during the off period.
VBR supports VBR data traffic with average and peak traffic parameters.
VBR is intended for applications that generate bursty traffic at a rate that varies with time. There are two service categories in VBR. The first is rt-VBR and is used by real-time applications. The second one is nrt-VBR and is intended for non-real-time applications.
See also "nrt-VBR" (p. 82) and "rt-VBR" (p. 103) .

**VC**
virtual connection
A technique ensuring that packets are delivered to the correct recipient in the same order as they were submitted.

**VCC**
virtual channel connection
A VCC is the series of cross-connections used to traverse an ATM network end-to-end. This ATM concept describes a type of path through an ATM network, defined by its VPI and VCI values.
VCCs represent a specific instance of a PVC, SPVC, or SVC. They are formed as a concatenation of one-hop connections that are cross-connected on workgroup switches. VCCs are unidirectional. They do not use bandwidth if there is no data to transmit.

**VCI**
virtual channel identifier
The VCI is part of the address of a VCC. The complete address of the VCC consists of the VCI and the VPI. A unique numerical tag, as defined by a 16-bit field in the ATM cell header, identifies a virtual channel, over which the cell is to travel. VCIs are assigned for one hop only. Each switch cross-connects cells from one VC to the next, reassigning VCIs.

**vertex**
In the context of an NFM-P map, an object other than a link between objects. Network elements and NE groups are examples of vertexes.

**VHO**
video head end office
The VHO is where the video server complex resides.

**VID**
VLAN Identifier
A VID is a 12-bit field in an Ethernet frame that uniquely identifies the VLAN to which the frame belongs.

**VINES**
virtual networking system

**virtual link**
Virtual links connect separate elements of a backbone, and function as if they are unnumbered point-to-point networks between two devices. A virtual link uses the intra-area routing of its transit area (the non-backbone area that both devices share) to forward packets.

**VLAN**
virtual LAN
A logical grouping of two or more NEs, which are not necessarily on the same physical network segment, but which share the same IP network number.

**VLAN stacking**
VLAN stacking provides a mechanism to tunnel multiple customer VLANs through a service provider network, using one or more stacked VLANs that use 802.1Q double-tagging or VLAN translation. VLAN stacking allows service providers to offer their customers TLS. This service is multipoint to support multiple customer sites or networks, which are distributed over the edges of a service provider network.

**VLAN uplink**
A logical object in the NFM-P that is automatically created between SAPs on two NEs which have a physical link and are on the same service. VLAN uplinks are also automatically created when the underlying transport mechanism is a transit service or composite transit service, rather than a direct physical link.

**VLL**
virtual leased line
A virtual leased line is a type of VPN where IP traffic is transported in a point-to-point manner.

**VLR**
Visitor Location Register
A database that stores information about all the mobiles under the jurisdiction of a Mobile Switching Centre (MSC), which the database serves. See 3GPP TS23.002 Section 4.1.1.2.*

**VM**
virtual machine

**VMG**
Virtual Mobile Gateway

The software-only version of the 7750 SR MG. Also known as CMG (cloud mobile gateway).

**VMM**
Virtual Mobility Manager
The software-only version of the 9471 WMM.

**VNF**
Virtual Network Function
A virtualized network element that represents a physical node.

**VNFC**
Virtual Network Function Component

**VoD**
video on demand
An application that provides a specific, non-broadcast video stream to an end user. Triple play service sometimes includes VoD.

**VoIP**
Voice over Internet Protocol
A telephone service that uses the Internet as a global telephone network. VoIP is typically part of a triple play service.

**VoLTE**
voice over LTE
Voice and SMS services over an LTE network using IMS.

**VPA**
VLAN port assignment
By default, all switch ports on an OmniSwitch are non-mobile ports that are manually assigned to a specific VLAN and can only belong to one VLAN at a time. When a port is defined as a mobile port, switch software compares traffic coming in on the port with configured VLAN rules. If any of the mobile port traffic matches any of the VLAN rules, the port and the matching traffic become a member of that VLAN.

**VPC**
virtual path connection
A VPC is a series of linked VPs that extend between the point where the VCI values are assigned and the point where those values are translated or removed.
A VPC carries VCCs between sites. VPC traffic is carried on full ATM trunks. VPCs use physical bandwidth only when the end devices pass traffic over the network; they do not use bandwidth if there is no data to transmit.
A VPC is a concatenation of VP links. The endpoints of a VPC are the points at which the ATM payload is passed to, or received from, the users of the ATM layer.

**VPI**
virtual path identifier
The VPI is an 8-bit field in the ATM cell header, which indicates the virtual path over which the cell should be routed.

The VPI is assigned on a connection set up by the devices at the two ends of a hop. Multihop VPC paths use multiple VPIs to go from source to destination. Each switch that the VPC traverses cross-connects the VPC from one port and VPI to another port and VPI.

**VPLS**
virtual private LAN service
A VPLS is a type of VPN in which a number of sites are connected in a single bridged domain over an IP/MPLS network. The services may be from different locations, but in a VPLS, they appear to be on the same LAN.
When implemented with Layer 2 interfaces, this service is called VPLS. When implemented with Layer 3 interfaces, this service is called an IP-VPN.

**VPM**
VLAN port membership
Mobile ports on an OmniSwitch can join more than one VLAN. However, certain rules, such as MAC address rules, can limit port membership to one VLAN.

**VPN**
virtual private network
A private network that is configured within a public network (a carrier network or the Internet) takes advantage of the economies of scale and management facilities of large networks. VPNs are used by enterprises to create WANs that span large geographic areas in order to provide site-to-site connections to branch offices, and to allow mobile users to dial up their company LANs.

**VPRN**
virtual private routed network
A network exhibiting at least some of the characteristics of a private network, even though it uses the resources of a public switched network.

**VQM**
video quality monitoring
VQM monitors video quality in the stages of transmission just prior reaching the STB.

**VRF**
virtual routing and forwarding
A logical or virtual routing function, with an associated routing table, which can be instantiated in a device capable of supporting IP VPN services.

**VRID**
virtual router ID
A number that is used with an IP address to uniquely identify the virtual router created using VRRP. Only one VRID can be used in a VLAN.

**VRRP**
Virtual Router Redundancy Protocol
VRRP is a protocol to provide redundancy in statically defined routed networks, rather than in dynamically defined networks, such as RIP and OSPF. VRRP is an election protocol that dynamically assigns responsibility for one or more virtual router(s) to the

VRRP router(s), allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers.

**VRS**
Virtual Routing and Switching
VRS is a service solution is implemented and monitored by the VSD.

**VSAP**
Virtualized Services Assurance Platform
VSAP provides the network management component for the Nokia Data Centers Service Delivery solution. VSAP provides network management functionality using web-based applications. The applications provide inventory management, network fault monitoring, troubleshooting purposes, and policy creation. The applications are external to the NFM-P client GUI and do not require a local client installation.

**VSC**
Virtualized Services Controller
The VSC is the data center network control plane. The VSC manages virtual routing and switching elements to program the network forwarding plane. The VSC communicates with the VSD policy engine using XMPP.

**VSD**
Virtualized Services Directory
The VSD is a policy-based system which can be used for creating virtualized services and provisioning them on the 7850 VSG. It has a web-based UI for administrator and tenant onboarding. The VSD is responsible for user management databases, policy creation, and cross-system interfaces. The VSD represents the user- or service-based outward functionality of the data center network.

**VSI**
virtual switch instance

**VSM-CCA**
versatile service module cross-connect adapter
The VSM-CCA is a type of MDA for the 7450 ESS and 7750 SR that provides an extra set of egress and ingress forwarding paths through a set of virtual ports. This design eliminates the need for a physical port MAC address, cable, or other MDA-specific component.

**VSP**
Virtualized Services Platform
VSP is a software-defined networking solution that provides data center network virtualization and manages connectivity between compute resources.

**VSR**
Virtual Service Router
A software-only version of the 7750 SR.

**VT**
virtual trunk

An aggregation of ATM VCs. All connections on a VT map to a single VPC with a public network-assigned VPI.

**VT-N**
virtual tributary - level *N*
A SONET format for mapping a lower-rate signal into a SONET payload; for example, VT1.5 is used to transport a DS-1 signal.

**VTG**
virtual tributary group
One or more virtual tributaries of the same rate that are bundled into an STS-1 payload.

**VTL**
velocity template language

**VTS**
virtual time-slot
1830 PSS-1 GBE Edge Device has a fixed assignment of 10 virtual time slots to each line port.

**VWM**
Versatile WDM Module
See "1830 VWM" (p. 5) .

**VXLAN**
Virtual Extensible LAN

## W

**WAN**
wide-area network
A geographically dispersed, long-haul telecommunications network that usually consists of backbone links. A WAN may be privately owned or leased. The term usually connotes the inclusion of public networks that are highly regulated, and provides superior reliability and resilience.

**WDM**
Wavelength Division Multiplexing
Several signals (or channels) are transported simultaneously over one fiber but at different wavelengths without interaction. Each channel is usually "TDM" (p. 119) . The capacity of a WDM system is thus given by the number of wavelengths × the bit rate of the "TDM" (p. 119) channel.

**web services**
Web services are network functions that can be accessed through a standard interface. For example, the XML metalanguage and the SOAP protocol allow the definition and transmission of messages between software components that run on heterogeneous platforms. This allows development teams to independently build components that run as distributed, independent implementations, linked only by their XML interfaces.

**WFF**
weighting factor file

**WFQ**
weighted fair queuing
Weighted fair queuing classifies all current traffic flows on an interface. Packets are sorted into flows based on a number of criteria such as MAC addresses, IP addresses, ports, priority codes (e.g., DiffServ, 802.11p), VLANs, and even DLCIs. These flows are then assigned to either a low-volume or high-volume queue. Interactive traffic, such as Telnet, is almost always placed in the low-volume queue; high-volume flows, such as FTP or HTTP, are placed in high-volume queues. The low-volume and high-volume queues are then serviced in a WRR manner, meaning that 20 low-volume packets might be processed for every high-volume packet. This type of queuing is weighted, but it allows each queue fair access to the interface.

**Wi-Fi offload**
Wi-Fi offload is a process by which traffic or data on a cellular network is offloaded to an available wireless network.

**window**
A window is a form, panel of information, equipment drawing, or graphic that appears on a screen. A window commonly allows an operator to enter data and initiate functions, but some windows only display information.

**WLAN GW**
wireless local area network gateway
A WLAN is a network to which users can establish a wireless connection via an access point within the coverage area.

**WO**
work order
A WO is an XML file that contains eNodeB configuration data. WOs are created by the "9952 WPS" (p. 10) and deployed by the NFM-P to eNodeBs.

**workflow**
The NFM-P workflow is a defined series of tasks that describe how to install, configure, create, and manage services.

**working directory**
The working directory contains image and configuration files that may or may not be the same as the files in the certified directory. The working directory is a holding place for new files. Files in the working directory must be tested before they can be committed to the certified directory. You can save configuration changes to the working directory. See also "certified directory" (p. 24) .

**working panel**
The working panel is a component of the NFM-P GUI that can include windows, drawings, and configuration forms.

**workstation**
A computer system with a local set of input and output devices, such as a keyboard and monitor.

**WPP**
web portal protocol
The WPP is used for web portal authentication of WLAN users (DHCP host) and runs between a BNG and a web portal server.

**WR2-88**
2-degree, 88-channel wavelength router card

**WRED**
weighted random early detection
WRED is a variation of RED, but instead of dropping packets randomly when there is high traffic congestion, the packets are dropped based on traffic priority.

**WRR**
weighted round robin
This queuing technique creates a number of queues and allows a user to assign incoming traffic to each queue by some distinguishing factor. This could be service class, address, protocols, or any other number of factors. To ensure each queue is serviced fairly, the user defines a weighting for each queue. Like round robin queuing, the scheduler visits each queue in turn. However, the weighting impacts the number of packets released from each queue when it is visited.
The primary problem with WRR is that it operates at the packet level. This means that if the queues contain packets of differing average lengths, the packet percentages won't be realized as bandwidth percentages.

**WTOCM**
Wavelength Tracker Optical Channel Monitoring card

**WTR**
wait to restore
A period of time that must elapse after a failed working line has recovered, before switching back to the working line from the protection line.

## X

**X.25**
An ITU-T data communications protocol and interface for public packet-switched communication between a network user and the network.

**X.733**
X.733 is the standard that describes the alarm reporting function.

**X2**
The interface used to interconnect eNodeBs. See 3GPP S36.300 Section 20 and TS36.420 to TS36.424.*

**XC**
Cross Connect

**XCM**
XMA Control Module

In the 7950 XRS, an interface module that is inserted into one of the I/O slots on the 7950 XRS shelf. An XCM includes two input slots for XMA or C-XMA cards.

**XFP**
10 Gigabit Small Form Factor Pluggable

**XMA**
XRS Media Adapter
In the 7950 XRS, an interface module that is installed on an XCM. An XMA card slot is also configurable with a C-XMA, which operates at half the capacity of an XMA.

**XMDA**
extended media dependent adapter.
See "MDA" (p. 70) .

**XML**
extensible markup language
XML defines the syntax to customize markup languages. The markup languages are used to create, manage, and transmit documents across the web.

**XML API**
NFM-P Extensible Markup Language Application Program Interface
An NFM-P software module that provides an interface for NFM-P communication with OSS applications.

**XML-JMS**
extensible markup language Java Message Service
The OSS client sends requests and receives responses using raw XML over a JMS queue. The requests and responses do not use SOAP headers.

**XNI**
10 Gigabit Network Interface

**XNS**
Xerox network standard
The term for the suite of Internet protocols developed by researchers at the Xerox Corporation.

**XPIC**
Cross Polarization Interference Cancellation
The 9500 MPR has XPIC capabilities that double the potential capacity of a microwave path. It allows the assignment of the same frequency to both the vertical and horizontal polarization on a path.

## Z

**ZIC**
Zero Install Craft
The ZIC interface provides a web-based user interface, called WebUI, to access the 1830 PSS. WebUI supports provisioning, administration, performance monitoring, and NE alarm and condition display.

**zone**
A portion of the namespace defined by the “DNS” (p. 33) protocol over which a system or organization has authority. The DNS namespace is a hierarchical concatenation of zone identifiers in a tree structure, with the highest-level zone as the rightmost. A period serves as the separator between two zones in a namespace.