NSP
Network Services Platform
Release 26.4

Glossary

3HE-29827-AAAA-TQZZA
Issue 1
April 2026

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

About this document

Purpose

The *NSP Glossary* is intended to expand acronyms and define unique terms that are used throughout NSP guides and products. This guide is not intended to define industry-standard terms and will only provide spell-outs in those cases.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to Documentation Feedback.

1 Glossary

Numerics

1.1 10/100/1000Base-FX

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

1.2 10/100/1000Base-TX

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

1.3 10/100Base-TX

An Ethernet standard supporting data transfer rates of up to 100 Mb/s using two pairs of data-grade, twisted-pair copper wire.

1.4 100Base-T

An Ethernet standard supporting data transfer rates of up to 100 Mb/s using twisted-pair copper wire.

1.5 1830 VWM

1830 Versatile WDM

A passive add-on shelf unit that provides 1.1014 “WDM” (p. 193) extension to a network element.

1.6 3-plus-tag

A descriptor for Ethernet frames with three or more VLAN ID tags.

1.7 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.

1.8 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.

1.9 6PE

IPv6 provider edge

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

1.10 6VPE

IPv6 VPN provider edge

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

1.11 7210 SAS-D

7210 Service Access System - Demarcation

An intelligent Ethernet edge-demarcation device that extends enhanced Carrier Ethernet VPN service delivery to the CE.

1.12 7210 SAS-Dxp

7210 Service Access System - Dxp

An intelligentEthernet demarcation/access device that supports 2 x 1GE/10GE SFP+ ports, 4 x 100/1000 SFP ports, and 6 x 10/100/1000 Base-T ports. The 7210 SAS-Dxp can be used in locations where they currently use a 7210 SAS-D, with the additional capability of 10GE uplinks and a higher capacity to address the growing bandwidth needs of service aggregation in access networks..

1.13 7210 SAS-E

7210 Service Access System - Ethernet

A Carrier Ethernet CLE device that can also be deployed as a cost-effective CE aggregation device for smaller networks.

1.14 7210 SAS-K

7210 Service Access System, 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.

1.15 7210 SAS-M

7210 Service Access System - MPLS

A CE device that provides MPLS-enabled metropolitan and WAN Carrier Ethernet service delivery, Ethernet-based mobile backhaul, and residential service access.

1.16 7210 SAS-Mxp

7210 Service Access System, 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.

1.17 7210 SAS-R

7210 Service Access System, 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.

1.18 7210 SAS-S

7210 Service Access System, chassis type S

An Ethernet access device that provides IP and MPLS-enabled service delivery, Ethernet-based mobile backhaul, and residential service access. The 7210 SAS-S is similar to the 7210 SAS-Sx, but with a reduced set of hardware features.

The 7210 SAS-S 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.

1.19 7210 SAS-Sx

7210 Service Access System, 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 is similar to the 7210 SAS-S, but with an enhanced set of hardware features.

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.

1.20 7210 SAS S/Sx VC

7210 Service Access System, chassis type Virtual Chassis

An Ethernet 7210 SAS-S/Sx VC supports stacking of the SAS-S/Sx variants. It includes support for virtual chassis/stacking with 7210 SAS-Sx/S 1/10GE platforms for EPIPE, VPLS, RVPLS services with IP/MPLS.

To simplify the operations and management, the stack of nodes is presented as a virtual chassis, with a single IP address to use for managing the platform.

1.21 7210 SAS-T

7210 Service Access System, chassis type T

An Ethernet access device that provides demarcation for services managed to the customer edge and Ethernet aggregation in smaller network locations.

1.22 7210 SAS-X

7210 Service Access System - 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.

1.23 7250 IXR

7250 Interconnect Router

An SR-based router suitable for interconnect applications in core, metro, and datacenter networks.

1.24 7250 IXR (non-SR OS)

7250 Interconnect Router, Release earlier than 19.x

The term 7250 IXR (non-SR OS) is used in the NFM-P documentation to describe 7250 IXR NEs that are not SR OS based, that is, 7250 IXR NEs running an NE release earlier than 19.x.

1.25 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.

1.26 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.

1.27 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.

1.28 7705 SAR

7705 Service Aggregation Router

A router that provides IP/MPLS and PW aggregation functions.

1.29 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

1.30 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 over a packet switched network or unsecure ISP. The 7705 SAR-Ax also targets fixed and vertical networks.

1.31 7705 SAR-F

7705 Service Aggregation Router– fixed form-factor chassis

1.32 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.

1.33 7705 SAR-Hc

7705 Service Aggregation Router– hardened compact

A 7705 SAR-Hc router is a compact version of the 7705 SAR-H.

1.34 7705 SAR Hx

7705 Service Aggregation Router, chassis type Hx

Hardened modular router with passive cooling for field deployments.

1.35 7705 SAR-M

7705 Service Aggregation Router, chassis type M

The 7705 SAR-M has the following:

- 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

1.36 7705 SAR Mx

7705 Service Aggregation Router, chassis type Mx

Hardened modular router with active cooling for field deployments.

1.37 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).

1.38 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

1.39 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.

Routers and other network hardware are referred to as devices or NEs in the NSP documentation.

1.40 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.

1.41 802.1ag

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.

1.42 802.1D

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

1.43 802.1p

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.

1.44 802.1Q

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

1.45 802.1w

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

1.46 802.1X

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.

1.47 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.

The 9500 MPR has been renamed Wavence starting in Release 18.

1.48 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 with no shelf unit. The 9500 MPRe provides fixed or mobile Ethernet backhaul and supports converged metropolitan MPLS networks.

The 9500 MPRe has been renamed Wavence SA starting in Release 18.

A

1.49 A

The A resource record defines the IPv4 host address that corresponds with the host FQDN.

1.50 AA

application assurance

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

1.51 AAA

authentication, authorization, and accounting

The functions of user security protocols such as RADIUS and TACACS+.

1.52 AAAA

The AAAA resource record defines the IPv6 host address that corresponds with the host FQDN.

1.53 AAL-5

ATM adaptation layer type 5

AAL-5 supports the conversion of 1.976 “VBR” (p. 186) , 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.

1.54 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.

1.55 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.

1.56 AC

Attachment circuit

An attachment circuit is the circuit connecting PE and CE equipment in an MPLS VPN.

1.57 ACK

acknowledge

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

1.58 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.

1.59 AD

administrative domain

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

1.60 adaptor

An adaptor provides mapping between a specific device and an application interface to enable model-driven mediation.

1.61 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.

1.62 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.

1.63 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.

1.64 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.

1.65 AES CTR

advanced encryption standard counter

AES CTR is a cryptography suite. It allows for decoding to be run in parallel on devices with many cores, and does not have padding of AES blocks.

1.66 AF

application function

The AF is an element that offers applications dynamic policy and/or charging control over the IP-CAN user plane behavior. The AF communicates with the PCRF to transfer dynamic session information that is required for PCRF decisions, and IP-CAN information and bearer-level event notifications.

1.67 AFI

Address Family Identifier

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

1.68 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 1.294 “ESP” (p. 80) , but provides IP header protection by default.

1.69 AIM

Automated intelligent management

The Nokia AIM device is a component of the MAGc-a2 compound node, along with the MAG-c and HP server.

1.70 AIS

alarm indication signal

A signal that a system transmits after some part of a communication link fails.

1.71 AISG

Air Interface Standards Group

The AISG is a non-profit consortium that develops international standards for wireless antenna line devices.

1.72 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.

1.73 ALMP

Auto-Learn MAC Protect

ALMP is used to prevent loops or MAC spoofing attacks.

1.74 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.

1.75 Analytics

Analytics generates reports and dashboard views of network conditions using raw and aggregated data. The NSP Analytics reports and information are in the **Data Collection and Analysis, Analytics Reports** view.

For more information, see the *NSP Analytics Report Catalog*.

1.76 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.

1.77 ANL

Access Network Location

ANLs are potential congestion points in the network.

1.78 AP

access point

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

1.79 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.

1.80 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.

1.81 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.

1.82 APR

automatic power reduction

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

1.83 APS

automatic protection switching

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

1.84 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.

1.85 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.

1.86 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.

1.87 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

1.88 artifact

An NSP artifact is one of a range of objects that evolves with the NSP product. The following are examples of NSP artifacts:

- workflows, actions, and Jinja templates
- configuration, service, or ZTP intent types
- operation types

Artifacts are provided for download in artifact bundles (zip files).

1.89 Artifact Administrator

Prior to NSP Release 23.11, the Artifact Administrator application, formerly called Artifact Manager or Common Artifact Manager (CAM), facilitated the tracking and management of NSP artifacts and artifact bundles.

Starting in Release 23.11, artifact management functions are available from the **Artifacts** views.

See “Artifacts” in the *NSP Network Automation Guide*.

1.90 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.

1.91 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.

1.92 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.

1.93 ASCII

American Standard Code for Information Interchange

ASCII is a collection of 7-bit character sets allowing per-country definitions, called variants.

1.94 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.

1.95 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.

1.96 ASR

Abort-Session-Request

The ASR command is sent by the CRF to notify the AF that the bearer for the established session has become unavailable.

1.97 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.

1.98 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.

1.99 AU

administrative unit

See 1.100 “AU-N” (p. 50) .

1.100 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.

1.101 AUG

administrative unit group

One or more AUs that occupy fixed, defined positions in an STM payload.

1.102 auto-signed

Refers to a security certificate that is signed locally, rather than by a certification authority, or CA. An auto-signed certificate provides limited external security, and is typically used only for inter-system access in an isolated environment.

1.103 auxiliary database

See 1.629 “NSP auxiliary database” (p. 132).

1.104 auxiliary server

See 1.612 “NFM-P auxiliary server” (p. 130).

1.105 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

1.106 B-component

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

1.107 BSF

binding support function

The binding support function (BSF), which is co-located with session management function (SMF), is used to discover the PCF serving the UE based on the UE IP address. This is done using the service operation, Nbsf_Management_Discovery, where the query parameters of the GET request contain the IP address of the UE. The IP domain attribute may be used in the query of the same UE IP address and may be used in a different IP domain. If a matching PDU session is found, the BSF returns the PCF identity either as an FQDN or IP address. The BSF may also return a PCRF identify using the Diameter host and realm. The UE IP address is served by the PCRF.

1.108 B-VSI

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

1.109 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.

1.110 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.

1.111 BCP

Bridging Control Protocol

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

1.112 bearer

A bearer is an IP packet flow that has a QoS configuration between a gateway and the 1.962 “UE” (p. 183) .

1.113 BER

bit error rate

The percentage of bits that have errors relative to the total number of bits received in a transmission.

1.114 BERT

bit error rate tester

BERT is a device that determines the BER on a communication channel.

1.115 BFD

bidirectional forwarding detection

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

1.116 BFER

bit forwarding egress router

In a BIER-enabled multicast network, a BFER removes the 1.124 “BIER” (p. 54) header from the packets before they leave the BIER domain.

1.117 BFIR

bit forwarding ingress router

In a BIER-enabled multicast network, a BFIR adds a 1.124 “BIER” (p. 54) header to packets. This header contains information about the set of BFERs to which a copy of the packet is to be delivered.

1.118 BFR

bit forwarding router

In a BIER-enabled multicast network, a BFR is any router that forwards traffic using 1.124 “BIER” (p. 54) header information (BIER bit-strings).

1.119 BGP

Border Gateway Protocol

BGP is an IETF standard EGP used to propagate routing information between autonomous systems.

1.120 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.

1.121 BGP AS

border gateway protocol autonomous system

BGP is an IETF standard EGP used to propagate routing information between autonomous systems.

1.122 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.

1.123 BGP-4

Border Gateway Protocol 4

A BGP that supports CIDR addressing, which increases the number of available IP addresses.

1.124 BIER

Bit Index Explicit Replication

BIER is a routing protocol proposed by the IETF and described in RFC 8279, used for forwarding multicast packets.

1.125 bill shock prevention

Bill shock occurs when a subscriber is unknowingly charged for a service that requires additional charges. Bill shock prevention service allows network operators to notify roaming subscribers of service costs in real time, and require their acceptance of the charges before a connection is made.

1.126 binding

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

1.127 BITS

Building Integrated Timing Supply

BITS is a method of distributing precision timing in a network.

1.128 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.

1.129 BMP

BGP Monitoring Protocol

BMP is used to monitor BGP sessions.

1.130 BOF

boot option file

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

1.131 BOM

byte order mark

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

1.132 BPDU

bridge protocol data unit

BPDU is the frame used by LAN bridges that support 802.1D STP to communicate with each other.

1.133 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.

1.134 broadcast TV

See 1.139 “BTV” (p. 56) .

1.135 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.

1.136 BSID

base station identifier

BSID is the base station identification of a UE.

1.137 BSM

bootstrap message

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

1.138 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.

1.139 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.

1.140 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

1.141 c-plane

See 1.192 “control plane” (p. 64) .

1.142 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.

1.143 C-XMA

compact XMA

In the 7950 XRS, an XMA that operates at half capacity. See also 1.1034 “XMA” (p. 196) .

1.144 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.

1.145 CAK

connectivity association key

A connectivity association key is a component of MACsec, securing control plane traffic.

1.146 CAM

CAM can be expanded in several ways:

- 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.
- cooperative awareness message
- common artifact manager
  One of several out-of-date terms for the Artifacts views in the NSP UI; see also 1.89 “Artifact Administrator” (p. 48)

1.147 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.

1.148 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.

1.149 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.

1.150 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.

1.151 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

1.152 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 1.1006 “VSM-CCA” (p. 191) .

1.153 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.

1.154 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.

1.155 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.

1.156 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.

1.157 Cdbx

cloud database interface

The local interface which represents the connectivity between the MG-VM and the database VM.

1.158 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.

1.159 CE

customer edge

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

1.160 CEM

circuit emulation

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

1.161 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 1.1022 “working directory” (p. 194) .

1.162 CES

circuit emulation service

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

1.163 CESoETH

circuit emulation service over Ethernet

See 1.162 “CES” (p. 60)

1.164 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.

1.165 CFM

Connectivity fault management

Ethernet Connectivity Fault Management in NSP is implemented based on the IEEE 802.1ag OAM standard. This standard describes protocols for detecting, isolating and reporting connectivity faults in an Ethernet network.

1.166 CGNAT

carrier grade network address translation

CGNAT, sometimes also referred to as CGN, LSN, or BB-NAT, enables translation of end users' private IPv4 addresses into one public IPv4 address.

1.167 CHAP

Challenge Handshake Authorization Protocol

CHAP is a secure method for connecting to a system.

1.168 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.

1.169 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 1.758 “reference” (p. 153) .

1.170 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.

1.171 CIDR

classless interdomain routing

An address aggregation process that simplifies routing.

1.172 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.

1.173 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.

1.174 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 1.900 “STP flat mode” (p. 174) .

1.175 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.

1.176 class of service

See 1.193 “CoS” (p. 64) .

1.177 classic mediation

Classic mediation comprises the following functions:

- mediation services for SNMP-managed Nokia NEs via the 1.611 “NFM-P” (p. 130) component
- control-plane management services for network infrastructure management and service assurance functions via the 1.194 “CPAM” (p. 65)

1.178 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.

1.179 CLI

command line interface

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

1.180 client delegate server

See 1.614 “NFM-P client delegate server” (p. 130).

1.181 CLLI

common language location identifier

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

1.182 CLM

Centralized License Manager

The Nokia Centralized License Manager (CLM) is available as an independent or an NSP-integrated deployment. It is a tool that provides simplification of network function license management. CLM is used to manage a pool of licenses for supported network functions as well as the NSP Routing key. Using CLM, operators can flexibly control license entitlement and monitor license pool usage for their managed network functions.

1.183 CMA

compact media adapter

Similar to an MDA, but smaller.

1.184 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.

1.185 CN telemetry

Cloud native telemetry

Cloud native telemetry provides microservice based statistics collection in NSP.

1.186 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.

1.187 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.

1.188 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

1.189 CO

central office

See 1.622 “NOC” (p. 131) .

1.190 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.

1.191 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.

1.192 control plane

The portion of the telecommunications network that is involved with signaling and control, including the management of sessions and services. See also 1.141 “c-plane” (p. 57) .

1.193 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.

1.194 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.

1.195 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

   Network equipment that resides on the customer side of the boundary between their network and the service provider's network.

1.196 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.

1.197 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.

1.198 CR

Custom resource

CR files provide information to CN telemetry microservices to enable interworking between the NSP and the NE for device telemetry.

1.199 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.

1.200 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.

1.201 CRL

certificate revocation list

CRL allows the network operator to check if a certificate has been revoked by the issuer CA. CRL can be used for CA certificates (root CA and sub CAs). CRL offers the option to configure an offline certificate revocation list file. CRL is configured per CA profile entry in the system.

Automatic CRL updates can be configured by providing a number of URLs where the system can automatically download a new CRL list for a given CA profile. The CRL file is automatically downloaded from a list of configured HTTP URLs either periodically or before the CRL expires. If the downloaded CRL is more recent than the existing one, then the existing one will be replaced.

1.202 cron

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

1.203 Cross Domain Coordinator

Prior to NSP Release 23.11, the Cross Domain Coordinator application enabled the automatic discovery of cross domain links between IP and optical networks.

Starting in Release 23.11, these functions are available from the **IP/Optical Coordination** views.

See the *NSP IP/Optical Coordination Guide*.

1.204 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.

1.205 CSFP

compact small form factor pluggable

A type of SFP transceiver with two bidirectional channels in a conventional SFP module. See also1.837 “SFP” (p. 165) .

1.206 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.

1.207 CSNP

complete sequence number PDU

A PDU sent by a designated router to ensure database synchronization.

1.208 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.

1.209 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.

1.210 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.

1.211 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.

1.212 CTg

call trace geographic

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

1.213 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.

1.214 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 1.267 “DWDM” (p. 76) , but more than in standard wavelength division multiplexing, or 1.1014 “WDM” (p. 193) .

D

1.215 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.

1.216 DCCA

diameter credit-control application

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

1.217 DCE

data communication equipment

A device that communicates with a DTE device in RS-232C communications.

1.218 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.

1.219 DDoS

distributed denial of service

A DoS attack that occurs from more than one source at the same time. See also 1.245 “DoS” (p. 73) .

1.220 DEM

Dynamic Experience Management

DEM is a congestion detection and mitigation solution for mobile, Wi-Fi, and fixed networks.

1.221 de-mux

See 1.225 “demultiplexer” (p. 69) .

1.222 default SAP

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

1.223 degree-2

A bidirectional network configuration from east to west or west to east.

1.224 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.

1.225 demultiplexer

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

1.226 deprecated

Features, functions or equipment for which future support discontinuation is planned are deprecated. Deprecation is intended to give customers time to plan to use alternatives before the feature, function or equipment is removed.

For example, 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.

1.227 DES

data encryption standard

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

1.228 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.

1.229 Device Administrator

Prior to NSP Release 23.11, the Device Administrator application provided the ability to discover and manage model-based devices using mediation policies and network rules.

Starting in Release 23.11, device discovery and management functions are available from the **Device Discovery** and **Device Management** views.

See the *NSP Device Management Guide*.

1.230 DF

don’t fragment

A bit in an IPv4 header that controls the fragmentation of a datagram.

1.231 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.

1.232 DHCP client

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

1.233 DHCP relay

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

1.234 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.

1.235 DHCP server

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

1.236 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.

1.237 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.

1.238 Diffie-Hellman key exchange

A key agreement algorithm used by two parties to agree on a shared secret.

1.239 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.

1.240 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.

1.241 DM

delay measurement

Ethernet delay measurement measures frame delay and frame delay variations by sending periodic frames to the peer 1.546 “MEP” (p. 120) and receiving frames from the peer 1.546 “MEP” (p. 120) during the diagnostic interval.

1.242 DNAI

data network access identifier

The DNAI identifies the user plane access to one or more data networks where applications reside, particularly in support of MEC.

1.243 DNS

domain name system

A system that translates host names to IP addresses.

1.244 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 1.262 “DU” (p. 75) and 1.474 “LDP” (p. 109) .

1.245 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.

1.246 Dot1N

802.1 level *N*

See 1.42 “802.1D” (p. 41) , 1.43 “802.1p” (p. 41) , 1.44 “802.1Q” (p. 41) , 1.45 “802.1w” (p. 41) , and 1.46 “802.1X” (p. 41) .

1.247 DP

drop precedence

Attribute of a packet which affects the probability of the packet being dropped within a CoS.

1.248 DPD

dead peer detection

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

1.249 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.

1.250 DR

DR can be expanded in the following ways:

1. designated router

   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.

2. disaster recovery

   A disaster-recovery (DR) NSP deployment consists of identical primary and standby NSP clusters and ancillary components in separate data centers. One cluster has what is called the primary role, and processes all client requests.

   The standby NSP cluster in a DR deployment operates in warm standby mode. If a primary cluster failure is detected, the standby automatically initializes as the primary, and fully assumes the primary role. Nokia encourages combining DR with high-availability (HA) for a robust and efficient network redundancy and resiliency solution.

1.251 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.

1.252 DRX

discontinuous reception

A system used in cellular networks to prolong 1.962 “UE” (p. 183) battery life by dividing UE devices into paging channels that are only paged by the designated network devices.

1.253 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.

1.254 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.

1.255 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.

1.256 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).

1.257 DSL module

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

1.258 DSLAM

digital subscriber line access multiplexer

A DSLAM is multiplexing equipment that a telecom operator uses to provide DSL services to end users.

1.259 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.

1.260 DTD

document type definition

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

1.261 DTE

data terminal equipment

A device that communicates with a DCE device in RS-232-C.

1.262 DU

downstream unsolicited

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

1.263 dual management

Dual management is no longer supported as of NSP Release 24.

With dual management, a device could be discovered and managed in both NFM-P and NSP, that is, both classic and MDM management. Using dual management, gRPC telemetry could be enabled on classic devices. All other management was through NFM-P.

Starting in Release 24, classic devices can be discovered and managed in NSP using a unified discovery rule. CN telemetry is available on classic devices if the unified discovery rule includes GRPC mediation; see the *NSP Device Management Guide*. Cloud native accounting telemetry can be enabled on classic devices.

1.264 dual stack

A dual-stack device is a device that can communicate using both IPv4 and IPv6.

1.265 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.

1.266 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.

1.267 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.

1.268 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

1.269 e-BGP

See 1.273 “EBGP” (p. 77) .

1.270 E1

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

1.271 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.

1.272 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.

1.273 EBGP

Exterior Border Gateway Protocol

A BGP session established between routers in different ASs. EBGPs communicate among different network domains.

1.274 ECMP

equal-cost multipath routing

Technique used by OSPF and IS-IS routing protocols to balance the load of Internet traffic.

1.275 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.

1.276 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.

1.277 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.

1.278 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.

1.279 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.

1.280 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.

1.281 EIC

equipment ID code

A character, or group of characters, used to identify or name equipment.

1.282 EIR

excess information rate

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

1.283 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.

1.284 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.

1.285 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.

1.286 eMLPP

enhanced multi-level precedence and pre-emption

Specifies levels of precedence for call setup and continuity for HO.

1.287 EMS

element management system

An application that manages one or more NEs.

1.288 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.

1.289 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.

1.290 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.

1.291 ESA

Extended Services Appliance

The Extended Services Appliance (ESA) is specialized hardware that hosts ESA Virtual Machines (ESA-VMs). Each ESA-VM is configured as an integrated service type. ESA extends the proven Integrated Services Adapter (ISA) system implementation architecture and related control processing module (CPM) functions on the 7750 SR systems to include ESA-VM-based virtual ISA (v-ISA) functionality.

1.292 ESAT

Ethernet satellites

The Ethernet satellite support feature allows the following chassis to act as a port extension for the 7750 SR or 7950 XRS host:

- 7210 SAS-Sx
- 7210 SAS-S
- 7250 IXR-X1/7250 IXR-Xs
- 7250 IXR-e 24SFP+ 8SFP28 2QSFP28

In this configuration, the host node performs all configuration and management functions. Management of the satellite node is not required when it is configured in an Ethernet satellite operations mode. A direct, non-switched, Ethernet connection between the 7750 SR or 7950 XRS host and the Ethernet satellite must be provided. The use of active Layer 2 switching devices in the path between the host and satellite is not supported.

1.293 ESM

See 1.787 “RSM” (p. 157) .

1.294 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 1.68 “AH” (p. 45) , but provides IP header protection only in tunnel mode.

1.295 ESS

extended service switch

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

1.296 ETH-BN

Ethernet bandwidth notification

ETH-BN enables the detection and extraction of ETH-BN messages to the CSM. If the ETH-BN indicates a new throughput value, the CSM programs the new value into the egress-rate of the port.

1.297 ETH-ED

Ethernet-expected defect

The ITU-T Y.1731 standard defines the method by which CCM-enabled MEPs can communicate during expected periods of interruption to peers including the specific ETH-ED sub-code options.

1.298 ETH-LMM

Ethernet-loss measurement message

The ITU-T Y.1731 standard defines the method by which Ethernet frame loss measurement statistics are collected to determine the unidirectional frame loss between point-to-point ETH-CFM MEP peers.

1.299 EtherType

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

1.300 ETree

Ethernet tree

An ETree is a VPN service in which each AC is designated either a root or a leaf. Roots can communicate with leaves or other roots; leaves can only communicate with roots.

1.301 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.

1.302 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.

1.303 EXP

experimental field

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

F

1.304 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.

1.305 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.

1.306 fallback

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

1.307 Fast Ethernet

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

1.308 fault

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

1.309 Fault Management

Prior to NSP Release 23.11, the Fault Management application provided alarm monitoring, correlation, and troubleshooting for the most unhealthy network elements (NE) in the network.

Starting in Release 23.11, alarm information is found in the **Network Map and Health, Current Alarms** view.

See the *NSP Network and Service Assurance Guide* for more information.

1.310 FC

FC can be expanded the following ways:

- flow control
  Flow control is the procedure that shuts down transmission when a receiving station is unable to store the data it is receiving.
- forwarding class
  See 1.325 “forwarding class” (p. 85) .

1.311 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

1.312 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.

1.313 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.

1.314 FDB

FDB is expanded two ways:

1. filtering database
2. forwarding database

1.315 FDL

facilities data link

Used in ESF to support the communication of network information in the form of in-service monitoring and diagnostics.

1.316 Feature package

The purchase of one or more NSP feature packages grants the right to download, install, and use the software that enables the associated NSP applications and functions.

See the *NSP System Architecture Guide* for more information about feature packages.

1.317 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.

1.318 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.

1.319 FIC

frame ID code

A field in a channel frame that identifies the position of the frame in the frame sequence.

1.320 FIPS

Federal Information Processing Standards

A cryptographic certification standard that defines the requirements for products to become FIPS-140-2 certified.

1.321 FIR

Fair Information Rate

FIR allows the QoS scheduling priority to be modified independently from the marking/drop precedence of the packets being scheduled from a queue.

1.322 flash memory

A rewritable memory chip that retains its content without power.

1.323 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.

1.324 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.

1.325 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).

1.326 FP

Forwarding Plane

In routing, a forwarding plane, sometimes called the data plane or user plane, defines the part of the router architecture that determines where packets are forwarded to when arriving on an inbound interface. Nokia uses this term with a numeric identifier to distinguish its family of network processors, for example FP3 and FP4 network processors.

1.327 FP4

A high-capacity chipset used in selected models and releases of Nokia network equipment.

1.328 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.

1.329 FPGA

field programmable gate array

A high density programmable hardware device capable of supporting different applications

1.330 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.

1.331 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.

1.332 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.

1.333 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.

1.334 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.

1.335 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.

1.336 FUI

final unit indication

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

G

1.337 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.

1.338 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.

1.339 GBR

guaranteed bit rate

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

1.340 generic NE

generic network element

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

1.341 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).

1.342 GIF

graphics interchange format

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

1.343 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.

1.344 Gig Ethernet

See 1.345 “Gigabit Ethernet” (p. 87) .

1.345 Gigabit Ethernet

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

1.346 GigE

See 1.345 “Gigabit Ethernet” (p. 88) .

1.347 Global MEG

Global Maintenance Entity Group

A Global MEG is a virtual object that contains more than one MEG. See also 1.544 “MEG” (p. 120) .

1.348 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.

1.349 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 1.566 “MPLS” (p. 123) .

1.350 GNE

See 1.340 “generic NE” (p. 87) .

1.351 gNMI

gRPC Network Management Interface

gNMI is a mechanism, carried by 1.359 “GRPC” (p. 90), that allows for viewing real-time operational data and managing configuration of devices.

gNMI is used by NSP to keep the NSP functions in sync with changes from SR OS NEs (via ON_CHANGE events) as well as to collect telemetry records.

1.352 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.

1.353 golden configuration

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

1.354 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.

1.355 GPV

get parameter values

Type of TR-069 RPC method.

1.356 GR

GR can be expanded in two ways:

- 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.
- geo-redundancy
  GR is an essential element of a disaster-recovery redundancy model. See 1.250 “DR” (p. 73).

1.357 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.

1.358 GRE

generic routing encapsulation

A protocol for the encapsulation of an arbitrary network-layer protocol over another arbitrary network-layer protocol.

1.359 GRPC

Google Remote Procedure Call

GRPC is the underlying protocol used for gNMI.

1.360 Group Manager

Prior to NSP Release 23.11, the Group Manager application provided a centralized resource that allowed administrators to configure groups of managed objects for use in NSP.

Starting in Release 23.11, these functions are available from the **Map Layouts and Groups** views.

See the *NSP System Administrator Guide*.

1.361 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.

1.362 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.

1.363 GUI

graphical user interface

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

1.364 GVRP

GARP VLAN registration protocol

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

H

1.365 HA

HA is expanded two ways:

1. high-availability

   HA is a local fault recovery mechanism within a multi-node NSP cluster. HA uses Kubernetes pod replicas to ensure minimal downtime in the event of an essential pod failure within the cluster. HA can be combined with disaster recovery (DR) to provide robust network resiliency and redundancy.

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.

1.366 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.

1.367 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.

1.368 heartbeat

Keep-alive messages that are exchanged between the UE and the application server in the Internet cloud. The message exchange maintains an active application session and prevents the expiration of NAT mapping, which causes IP session disconnection.

1.369 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.

1.370 HO-ODUk

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

1.371 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.

1.372 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.

1.373 Hpipe

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

1.374 HQoS

hierarchical quality of service

HQoS provides the ability to perform rate limiting across multiple queues from multiple SAPs.

1.375 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.

1.376 HSI

high-speed Internet access

HSI is a broadband Internet access service that is typically part of a triple play service.

1.377 HSM

hardware security module

An HSM is a certified system for MACsec key generation.

1.378 HSMDA

high scale Ethernet MDA

The HSMDA is an MDA for the 7450 ESS-7/12 and 7750 SR-7/12/12e, Release 20.10 and earlier. 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.

1.379 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.

1.380 HTML

hypertext markup language

Language for writing hypertext documents, often for use in a web environment.

1.381 HTTP

Hypertext Transfer Protocol

A set of rules for exchanging text, graphics, sound, video, and other multimedia files on the Web.

1.382 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.

1.383 HTTPS

HTTP Secure

An extension of HTTP that provides encryption and decryption of Web page requests and responses for secure browser communication over a network. HTTPS is secured using the 1.935 “TLS” (p. 179) protocol, so is sometimes called HTTP over TLS.

1.384 hybrid port

See 1.190 “combo port” (p. 64) .

I

1.385 ICM

Infrastructure Configuration Management

ICM is an alternative term for Device Configuration, which is available from the Device Management views.

Device configuration allows a network engineer to define reusable configuration templates covering such areas as card, port, QoS, security, and routing policy configurations.

You must enable the `networkInfrastructureManagement-deviceConfig` installation option to see and use device configuration in NSP.

1.386 I-VSI

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

1.387 I/O

input/output

Connections between a system and its controlled devices (output) and incoming statuses (input).

1.388 I/O module

See 1.420 “IOM” (p. 100) .

1.389 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.

1.390 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.

1.391 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.

1.392 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.

1.393 IdP

identity provider

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

1.394 IE

information element

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

1.395 IED

intelligent electronic device

A packet-based remote monitoring and control device used in 1.813 “SCADA” (p. 162) networks

1.396 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.

1.397 I-ES

Interconnect Ethernet Segment

An I-ES is a virtual ethernet segment that allows DC GWs with two BGP instances to handle VXLAN access networks.

1.398 IETF

Internet Engineering Task Force

The IETF is the organization that manages the standards and specifications for IP and related protocols.

1.399 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.

1.400 IGMP

Internet Group Management Protocol.

IGMP is an IP extension that hosts use to report their multicast group membership to neighboring multicast routers.

1.401 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.

1.402 IGP

Interior Gateway Protocol

Generic term applied to any protocol used to propagate network reach and routing information within an AS.

1.403 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.

1.404 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.

1.405 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.

1.406 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.

1.407 IME

interface management entity

Software components that execute the ILMI protocol.

1.408 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.*

1.409 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.

1.410 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.*

1.411 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.*

1.412 Insights Administrator

Prior to NSP Release 23.11, the Insights Administrator application enabled the management of YANG-based telemetry in the NSP user interface.

Starting in Release 23.11, these functions are available from the **Data Collection and Analysis**, **Management** views.

See the *NSP Data Collection and Analysis Guide*.

1.413 Insights Viewer

Prior to NSP Release 23.11, the Insights Viewer utility enabled the charting of real-time telemetry data.

Starting in Release 23.11, these functions are available from the **Data Collection and Analysis**, **Visualizations** views.

See the *NSP Data Collection and Analysis Guide*.

1.414 Installation option

An NSP installation option enables a specific NSP function that is required by one or more feature packages. You specify and configure installation options in the NSP configuration file during system deployment or reconfiguration.

1.415 intent

An intent is an instance of an intent type. The intent provides inputs to the intent type and executes the configuration.

1.416 Intent Manager

Prior to NSP Release 23.11, the Intent Manager application enabled the creation and execution of intent types and intents in the NSP user interface.

Starting in Release 23.11, these functions are available from the **Network Intents** views.

See the *NSP Network Automation Guide*.

1.417 Intent type

An intent type is a detailed specification for a desired network configuration. The intent type includes the YANG model and scripts and templates for the configuration to be performed.

For example, an intent type for service creation defines the parameters for the service and provides mapping for device models. When you create an intent using an intent type, you create an instance of the intent type with any required inputs provided.

1.418 Interlaken

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

1.419 intermediate system

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

1.420 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.

1.421 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.

1.422 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.

1.423 IP Optical Coordination

NSP function that provides coordination between IP and optical network domains, including discovery of cross-domain links between IP and optical networks. Available from the IP/Optical Coordination views in the NSP UI.

1.424 IP/MPLS Optimization

Prior to NSP Release 23.11, the IP/MPLS Optimization application provided a view of the IGP topology and PCE LSPs.

Starting in Release 23.11, these functions are available from the **Path Control** views.

See the *NSP Path Control and Simulation Guide*.

1.425 IP/MPLS Simulation

Prior to NSP Release 23.11, the IP/MPLS Simulation application provided the ability to simulate changes in the IP topology.

Starting in Release 23.11, these functions are available from the **Path Simulation** views.

See the *NSP Path Control and Simulation Guide*.

1.426 IPCP

IP control protocol

IPCP assigns DNS and NBNS addresses to the UE.

1.427 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.

1.428 IPFIX

Internet Protocol Flow Information eXport

IPFIX is an IETF standard that defines how IP flow data are to be formatted and transferred from a flow exporter such as a managed NE to a collector such as an 1.631 “NSP Flow Collector” (p. 133).

1.429 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.

1.430 IPsec

Internet protocol security

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

1.431 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.

1.432 IPv6

Internet Protocol version 6

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

1.433 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.

1.434 IRICC

intercept related information and content of communication

Data about the call and the data containing the call content.

1.435 IS

See 1.419 “intermediate system” (p. 100) .

1.436 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.

1.437 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.

1.438 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 1.50 “AA” (p. 43) and 1.437 “ISA” (p. 102) .

1.439 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.

1.440 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.

1.441 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 1.598 “NAT” (p. 128) and 1.437 “ISA” (p. 102) .

1.442 ISA-TMS

integrated services adapter - threat management system

The ISA-TMS is a 7750 SR MDA.

1.443 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 1.1019 “WLAN GW” (p. 194) and 1.437 “ISA” (p. 102) .

1.444 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.

1.445 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

1.446 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.

1.447 JAAS

Java authentication and authorization service

A set of packages that enable services to authenticate and enforce access controls on users.

1.448 Java

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

1.449 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.

1.450 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.

1.451 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.

1.452 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.

1.453 JRMP

Java Remote Method Protocol

A proprietary wire-level protocol that transports Java RMI.

1.454 JVM

Java virtual machine

A software abstraction layer that enables Java software to run on any processor architecture.

K

1.455 Kafka

Apache Kafka is an open-source distributed event streaming platform.

1.456 keystore

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

1.457 KPI

key performance indicator

A statistic counter used to monitor network performance.

L

1.458 L0

Optical layer 0

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

1.459 L1

L1 can refer to two terms:

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

1.460 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.

1.461 L2PT

Layer 2 protocol tunneling

L2PT allows L2 PDUs to tunnel through a network.

1.462 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 L2TP access concentrator. See also 1.491 “LNS” (p. 111) and 1.464 “LAC” (p. 108) .

1.463 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.

1.464 LAC

LAC can be expanded in the following ways:

- L2TP access concentrator
  The LAC is the initiator of an L2TP tunnel. See also 1.491 “LNS” (p. 111) and 1.462 “L2TP” (p. 107) .
- local access control
- location area code

1.465 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.

1.466 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.

1.467 LAIS

line alarm indication signal

A SONET signal that indicates a general line fault.

1.468 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.

1.469 Layer 2

See 1.459 “L1” (p. 107) .

1.470 Layer 3

See 1.463 “L3” (p. 107) .

1.471 LBM

loopback message

A loopback message is generated by a 1.546 “MEP” (p. 120) to a peer 1.546 “MEP” (p. 120) or an intervening 1.551 “MIP” (p. 121) .

1.472 LCP

Link Control Protocol

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

1.473 LDAP

Lightweight Directory Access Protocol

LDAP is a networking protocol for querying and modifying directory services that run over TCP/IP.

1.474 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 1.244 “DoD” (p. 72) and 1.262 “DU” (p. 75) .

1.475 lease

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

1.476 LER

label edge router

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

1.477 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.

1.478 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.

1.479 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.

1.480 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.

1.481 LI

LI can be expanded in two ways:

- lawful intercept

  A method to monitor target subscriber voice and data communications over an IP network by authorized agencies. Available in NFM-P only.

- logical inventory

1.482 LIC

location ID code

A field in a SONET frame that identifies the location of an MDL.

1.483 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.

1.484 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. 1.766 “RHEL” (p. 154) is a commercial Linux version.

1.485 LLC

logical link control

LLC is the upper sublayer of the OSI model data link layer. LLC governs packet transmission as specified by IEEE 802.2.

1.486 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.

1.487 LLDPDU

Link Layer Discovery Protocol data unit

See also 1.486 “LLDP” (p. 111) .

1.488 LLID

Logical Link Identifier

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

1.489 LM

loss measurement

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

1.490 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.

1.491 LNS

L2TP network server

The LNS is the server, which waits for L2TP tunnels. See also 1.464 “LAC” (p. 108) and 1.462 “L2TP” (p. 107) .

1.492 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.

1.493 LOC

loss of clock

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

1.494 local storage

Storage that is dynamically provisioned for a specific node and accessible only by the pods running on that node. Local storage is used when only a single pod requires access to the persistent volume.

1.495 LOF

loss of frame

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

1.496 LOS

LOS can be expanded in two ways:

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

1.497 LPE

logical provider edge

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

1.498 LPS

learned port security

A mechanism for authorizing source learning of MAC addresses on Ethernet and Gigabit Ethernet ports.

1.499 LRDI

line remote defect indication

A field in a channel frame that indicates a remote LOF, LOC, or LOS.

1.500 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.

1.501 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.

1.502 LSP

label switched path

LSPs support MPLS functions and allow network operators to perform traffic engineering.

There are several 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.

1.503 LSP classifier

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

1.504 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.

1.505 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.

1.506 LTN

LSP ID to NHLFE

1.502 “LSP” (p. 113) ID to Next Hop Label Forwarding Entry

M

1.507 MA

maintenance association

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

1.508 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.

1.509 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.

1.510 MACsec

Media Access Control Security

MACsec provides secure communication for almost all types of traffic on Ethernet links.

1.511 MAF

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.

1.512 MAG-c

Multi-Access Gateway controller

The MAG-c is a component of the Nokia CUPS solution.

1.513 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.

1.514 main server

See 1.616 “NFM-P main server” (p. 130).

1.515 MAN

metropolitan area network

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

1.516 master node

Master node is a term previously used for the control-plane node in a Kubernetes cluster. The control-plane node manages the overall state of the cluster.

1.517 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.

1.518 MBH

microwave backhaul

Microwave backhaul refers to the transportation of traffic (voice, video and data) between distributed sites and a more centralized point of presence via a radio link

1.519 MBS

maximum burst size

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

1.520 MC

multichassis

A redundancy configuration that includes two peer NEs.

1.521 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 1.559 “MLPPP” (p. 122) .

1.522 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.

1.523 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.

1.524 MCC

mobile country code

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

1.525 MCFR

Fragmentation of packets of various priorities into multiple classes, allowing high-priority packets to be sent between fragments of lower priorities. See 1.558 “MLFR” (p. 122) .

1.526 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.

1.527 MCS

MCS can be expanded in two ways:

1. multichassis synchronization
2. MC mobile interface

1.528 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.

1.529 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.

1.530 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.

1.531 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.

1.532 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.

1.533 MDC

Model Driven Configurator

Model Driven Configurator, previously called Modeled Device Configurator, allows for viewing the state and configuration of model-based devices in NSP, and for editing the device configuration.

1.534 MDCR

minimum desired cell rate

MDCR is equivalent to MIR.

1.535 MDDB

multidrop data bridge

An MDDB broadcasts a single stream from a 1.813 “SCADA” (p. 162) master to multiple remote devices and allows communication from individual remote devices back to the master.

1.536 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.

1.537 MDL

message data link

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

1.538 MDM

model-driven mediation

A mediation framework that manages network devices using adaptors. The MDM framework supports Nokia and third-party devices.

With MDM, the data objects that make up an NE and its capabilities are defined using YANG models. MDM provides the translation and abstraction required for automated applications to interact with the NE YANG model, allowing management of NEs without the need for the NFM-P.

1.539 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.

1.540 MEC

multi-access edge computing

MEC is an ETSI-defined cloud-based IT service environment located at the edge of a network. Traffic and services are moved from a centralized cloud to the edge of the network, closer to the customer. Data is collected and processed at the network edge, instead of the cloud, which reduces latency and brings real-time, high-bandwidth performance to applications.

1.541 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.

1.542 mediation address

Virtual IP addresses that NSP uses for mediation traffic between NEs and NSP applications.

1.543 mediator

Mediators serve as communication proxies between the Network Intents component of NSP and other systems, such as NSP components that manage network devices, or external controllers. The use of a mediator removes the need for Network Intents to provide authentication credentials to reach the desired endpoint.

1.544 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.

1.545 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.

1.546 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.

1.547 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.

1.548 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.

1.549 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.

1.550 MIB

management information base

A formal description of a set of network objects that can be managed using SNMP.

1.551 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.

1.552 MIR

minimum information rate

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

1.553 mixed mode

Mixed mode can refer to the following parameters in NFM-P:

- Mixed Mode State on Chassis Enabled

  This parameter allows the support of features on 7450 ESS or 7750 SR devices that are not available on the device when the parameter is not enabled. See the *NSP NFM-P Classic Management User Guide* for details.

- Management Operational Mode

  The Management Operational Mode parameter is read-only in NFM-P. It shows the value of the `configuration-mode` parameter on the NE, if applicable:

  - classic: router configuration changes can be made via classic CLI and SNMP management interfaces
  - modelDriven: router configuration changes can be made via model-driven management interfaces (NETCONF with 'Nokia' YANG models, MD-CLI, or gRPC), but not using classic interfaces
  - mixed: router configuration changes can be made using classic and model-driven management interfaces (with some restrictions and limitations)

  NSP manages devices with `configuration-mode` set to “modelDriven” or “mixed” as MDM devices.

  NFM-P management of devices with `configuration-mode` set to “modelDriven” or “mixed” is not supported as of Release 24.11 or earlier.

  The discovery of mixed mode is supported from NFM-P 25.4 release onwards.

1.554 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.

1.555 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.

1.556 MLDP

Multicast Label Distribution Protocol

MLDP provides extensions to 1.474 “LDP” (p. 109) for the setup of P2MP LSPs in 1.566 “MPLS” (p. 123) networks.

1.557 MLD snooping

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

1.558 MLFR

An aggregation of multiple physical links into a single logical bundle to improve bandwidth between two peer systems. See 1.331 “FR” (p. 85) .

1.559 MLPPP

multilink PPP

An aggregation of multiple physical links into a single logical bundle to improve bandwidth between two peer systems. See 1.721 “PPP” (p. 146) .

1.560 MMS

multimedia messaging service

A method to send multimedia content messages to and from mobile devices.

1.561 MNC

mobile network code

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

1.562 MNN

mobile network node

A node that is located inside a mobile network.

1.563 MNO

mobile network operator

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

1.564 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.

1.565 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.

1.566 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.

1.567 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.

1.568 MPR

microwave packet radio

MPR devices are renamed to Wavence starting in Release 18.

1.569 MPT

microwave packet transport

An MPT is an outdoor microwave radio which forms the radio component of a Wavence SM or Wavence SA unit.

1.570 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.

1.571 MPTCP

multipath transmission control protocol

MPTCP is a TCP connection that uses many paths to maximize resource usage and increase redundancy.

1.572 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.

1.573 MRRU

maximum received reconstructed unit

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

1.574 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.

1.575 MS-PW

multi-segment pseudowire

MS-PW routing allows inter-domain routed services to dynamically maintain paths using 1.801 “S-PE” (p. 160) and 1.916 “T-PE” (p. 176) NEs.

1.576 MSAP

managed service access point

See also 1.807 “SAP” (p. 161) .

1.577 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.

1.578 MSCP

The MSCP is a communication protocol used by speech servers to provide services such as voice recognition and synthesis.

1.579 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.

1.580 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.*

1.581 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.

1.582 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.

1.583 MSTP

Multiple Spanning Tree Protocol

An RSTP that allows different spanning trees to co-exist on the same Ethernet switched network.

1.584 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.

1.585 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.

1.586 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.

1.587 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.

1.588 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.

1.589 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.

1.590 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.

1.591 MVPN

A multicast 1.997 “VPN” (p. 189) is an IP VPN service that supports the transmission of IP multicast packets between sites.

1.592 MVR

multicast VLAN registration

1.593 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.

1.594 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.

1.595 MVRF

The multiple virtual routing and forwarding feature provides the ability to configure separate virtual routing instances on the same NE. See 1.1000 “VRF” (p. 190) .

N

1.596 N-PE

network-facing provider edge

A device that implements the control and signaling functions of an LPE.

1.597 NAPT

network address port translation

An enhancement of regular 1.598 “NAT” (p. 128) 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.

1.598 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.

1.599 Nbsf

The Nbsf service is used by the BSF to provide a PDU session binding function. It ensures that an AF request for a PDU session reaches the PCF that has the PDU session information. The Nbsf service configuration defines the TCP port used for service access. The Nbsf service allows NF consumers to retrieve, update, and remove the binding information.

1.600 navigation tree

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

1.601 NE

network element

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

1.602 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.

1.603 NECG

NSP NFM-P Network Element Compatibility Guide

The NECG is a reference guide that provides information about which NE software releases are supported by specific versions of the NFM-P. You can consult the latest version before performing upgrades or changes to your network environment to avoid service disruptions and ensure support for all managed devices. The guide is delivered biweekly on the Nokia Doc Center outside of the public HTML collection.

1.604 neighbor

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

1.605 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.

1.606 NetLoc

Network-provided location information for IMS

NetLoc refers to a situation where the network may require the cellphone ID for purposes such as lawful interception or charging. Cellphone ID information, provided by the UE, cannot be trusted as it is coming from the untrusted WLAN, therefore, the network provides the cellphone ID.

1.607 NEtO

Network Element Overview

A GUI-based Wavence NE management system.

1.608 Network Supervision

Prior to NSP Release 23.11, the Network Supervision application provided a dashboard to monitor the health of core, access, transport, and optical NEs, and virtual NFs using pre-defined KPIs and alarms.

Starting in Release 23.11, NE information is found in the **Object Troubleshooting, Network Element** view.

See the *NSP Network and Service Assurance Guide* for more information.

1.609 network topology

The general layout of a network in terms of, for example, NE interconnection, grouping, or communication protocol.

1.610 NF

network function

A processing function in a network, defined by 3GPP. An NF can be implemented as a network element or software instance running on hardware, or as a virtualized function instantiated on a platform, such as on a cloud infrastructure.

1.611 NFM-P

Network Functions Manager - Packet

The NFM-P is an advanced IP/MPLS and mobile network management system that has a modular, scalable architecture. The system provides multiple GUI, web, and OSS interfaces, and can integrate with other management systems.

1.612 NFM-P auxiliary server

An NFM-P auxiliary server is a scalable NFM-P system component that performs routine functions such as statistics collection. Auxiliary server deployment is supported only in a distributed NFM-P system.

1.613 NFM-P client

An NFM-P client is an entity that interacts with an NFM-P main server to perform network management operations. For example, an NFM-P GUI client uses an NFM-P graphical interface, an NFM-P OSS client uses an NFM-P API or similar mechanism, and an NFM-P application client uses NFM-P browser-based applications.

1.614 NFM-P client delegate server

An NFM-P client delegate server is a scalable NFM-P component that can host multiple concurrent GUI client sessions. A client delegate server has one NFM-P client software instance that is invoked by local and remote NFM-P users.

1.615 NFM-P main database

An NFM-P main database is a mandatory NFM-P system component that acts as the main NFM-P data store.

1.616 NFM-P main server

An NFM-P main server is the processing engine that co-ordinates and performs NFM-P network management operations that include responding to 1.613 “NFM-P client” (p. 130) requests, and mediation between the managed network and other entities.

1.617 NGE

Network Group Encryption

A mechanism for the end-to-end encryption of MPLS-based traffic.

1.618 N:K

A resource deployment redundancy model where N represents the active (primary) resource, and K represents the standby (secondary) resource that is activated when the active resource (N) fails. For deployments that do not require zone level failure (when half of all resources are impacted), the overhead of computing resources can be reduced by creating a shared pool of standby resources that can be used for processing sessions that are impacted due to limited scope failure.

1.619 NLOS

non-line-of-sight

A radio transmission across a path that is partially obstructed, usually by an object.

1.620 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.

1.621 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.

1.622 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.

1.623 node

In an NSP cluster, a cluster node (or cluster member) is a Kubernetes worker node VM. On NSP

cluster nodes, the NSP software runs in pods that are devoted to distinct NSP services and are distributed among VMs in the cluster.

1.624 NRC-P

Network Resource Controller — Packet

Former NSP module; NRC-P function is realized by the Path Control function in NSP.

1.625 NRC-X

Network Resource Controller — Cross Domain

Former NSP module; this function is realized by the 1.423 “IP Optical Coordination” (p. 100) function in NSP.

See 1.423 “IP Optical Coordination” (p. 100).

1.626 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.

1.627 NSD

Network Services Director

Former module of NSP; NSD functionality is realized by the Service Management function.

1.628 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.

1.629 NSP auxiliary database

An NSP auxiliary database is a scalable NSP system component that increases the data throughput and storage for demanding operations such as statistics collection. An auxiliary database can be deployed on one station, or as a distributed database on separate stations to provide fault tolerance and enable load balancing.

1.630 NSP cluster

One or more VMs which together host the NSP software and functions.

An NSP cluster may consist of one member, or three or more members that each host a portion of the installed NSP software. See 1.623 “node” (p. 131) for more information.

1.631 NSP Flow Collector

An NSP Flow Collector is a scalable internal NSP system function that collects flow statistics data from managed NEs for processing by consumers such as NSP Analytics or OSS applications. Flow data collection by the Flow Collectors is enabled using an installation option and addressing parameters in the NSP configuration.

1.632 NSR

non-stop routing

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

1.633 NSSA

not-so-stubby-area

NSSA is an OSPF area type where OSPF propagates any external routes that it obtains from the AS.

1.634 NTP

Network Time Protocol

An Internet protocol that network devices use to synchronize their clocks.

O

1.635 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.

1.636 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.

1.637 OAuth

OAuth is an open-standard authorization protocol that allows resource owners to authorize third-party access to their server resources without providing authorization credentials. Access tokens are issued to third-party clients by an authorization server with approval from the resource owner. The access tokens are used by the third party to access the protected resources of the resource server. OAuth is commonly used to allow websites access to information on other websites without giving them passwords.

1.638 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.

1.639 OCH

optical channel

An optical wavelength band for WDM optical communications.

1.640 OCSP

online certificate status protocol

OCSP is a method of checking the state of a certificate. Unlike the CRL, which relies on checking against an offline file, the OCSP provides online information regarding the revocation status of a certificate. Like the CRL, the network operator can define an OCSP server per CA profile configuration.

1.641 ODU

optical channel data unit

outdoor unit

1.642 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.

1.643 OEO

optical-to-electrical to optical

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

1.644 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.

1.645 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.

1.646 OLP

optical line protection

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

1.647 ONIE

Open Network Install Environment

An open source initiative which enables automatic installation of a Network Operating System (NOS).

ONIE provides the following services:

- Installing and reinstalling an OS
- Booting in rescue mode
- Formatting the system

1.648 OPS

An optical circuit pack that provides WDM protection.

OPS is expanded in two ways:

1. off-premise station
2. optical protection switch

1.649 Option 82

See 1.759 “Relay Information Option” (p. 153) .

1.650 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.

1.651 ORF

outbound route filtering

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

1.652 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.

1.653 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.

1.654 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: 8 slots for XNI or GNI cards that provide Ethernet, GigE, and 10 GigE capabilities.

1.655 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.

1.656 OS 6350

OmniSwitch 6350

Stackable family is a series of fixed-configuration Gigabit Ethernet switches available as 10-, 24- and 48- port, Power-over-Ethernet (PoE) and non-PoE models to create the exact network for your small business. The network capabilities of the OmniSwitch 6350 family include advanced security, quality of service and high availability features for your business-class data, voice and wireless technologies.

1.657 OS 6400

OmniSwitch 6400

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

1.658 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.

1.659 OS 6450 M/X

OmniSwitch 6450 M/X

See 1.658 “OS 6450 ” (p. 137).

1.660 OS 6465

OmniSwitch 6465

OS 6465 devices are shock-resistent, fully managed, gigabit Ethernet switches offering high security, reliability, performance, and easy management. With support for MACSec on all ports, OS 6465 enables end-to-end encrypted networks. The OS 6465 family offers advanced system and network-level resiliency features and convergence through standardized protocols in a space-efficient form factor.

1.661 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.

1.662 OS 6850E

OmniSwitch 6850E

See 1.661 “OS 6850” (p. 137) .

1.663 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.

1.664 OS 6860

OmniSwitch 6860

The OS 6860 is a family of stackable high-density Gigabit and 10 Gigabit L2/L3 switches that can be positioned as edge, aggregation, or data center devices, or in a small enterprise network core.

1.665 OS 6860E

OmniSwitch 6860E

The OS 6860E is a family of high-density Gigabit and 10 Gigabit L2/L3 switches that provide application monitoring and enforcement, deep packet inspection, and advanced security.

1.666 OS 6865

OmniSwitch 6865

The OS 6865 is a stackable 1-GigE and 10-GigE L2/L3 hardened Ethernet switch suitable for outdoor installations. It is designed to operate in harsh environments and severe temperatures.

1.667 OS 6900

OmniSwitch 6900

The OS 6900 is a family of standalone aggregation switches.

1.668 OS 9600

OmniSwitch 9600

The OS 9600 is a five-slot Ethernet switch that supports 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.

1.669 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.

1.670 OS 9700E

OmniSwitch 9700E

See 1.669 “OS 9700” (p. 139) .

1.671 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.

1.672 OS 9800E

OmniSwitch 9800E

See 1.671 “OS 9800” (p. 139) .

1.673 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

1.674 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.

1.675 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.

1.676 OSS

operations support system

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

1.677 OSSI

operations support system interface

An API endpoint that allows an OSS to manipulate managed objects and allow flow-through provisioning.

1.678 OTN

Optical Transport Network

A fiber-optic network, such as an SDH or SONET network, that is designed to transport customer traffic,

1.679 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.

1.680 OUI

organizationally unique identifier

A three-octet field in a SNAP header that identifies an organization.

P

1.681 PAE

port access entity

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

1.682 PAP

Password Authentication Protocol

A protocol to communicate with a security server for a user authentication.

1.683 parameter

A parameter is a value that is passed to a function or method for use in its operation.

The NSP documentation also uses the term parameter to describe attributes, or properties of objects.

1.684 PBS

peak burst size

The maximum number of bytes that can be sent at the network interface speed without exceeding the PIR.

1.685 PCC

PCC can be expanded in two ways:

- 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.*
- path computation client

1.686 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.

1.687 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

1.688 PD

powered device

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

1.689 PDF

portable document format

The file format in Adobe Acrobat document exchange technology.

1.690 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.

1.691 PDN

packet data network

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

1.692 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.

1.693 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.

1.694 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.

1.695 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.

1.696 PEQ

power equalization module

The 7950 XRS power supply which provides DC power to the chassis.

1.697 PFCP

packet forwarding control protocol

PFCP is a message delivery protocol that is used on the interface between the control plane and user plane functions in a CUPS context.

1.698 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.

1.699 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.

1.700 PGW-C

packet data network gateway - control plane

The PGW that exists in the control plane.

1.701 PGW-U

packet data network gateway - user plane

The PGW that exists in the user plane.

1.702 PHY

physical

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

1.703 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.

1.704 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

1.705 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.

1.706 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.

1.707 ping

packet Internet groper

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

1.708 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.

1.709 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.

1.710 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.

1.711 PLMN

public land mobile network

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

1.712 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.

1.713 PM

PM is expanded in two ways:

1. path monitoring

   For an optical channel data unit.

2. performance monitoring

1.714 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.

1.715 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.

1.716 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.

1.717 PoE Plus

power over Ethernet plus

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

1.718 PoE+

See 1.717 “PoE Plus” (p. 146) . See also 1.716 “PoE” (p. 146) .

1.719 POS

packet over SONET

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

1.720 PPI

paging policy indicator

The PPI indicates paging policy differentiation when the SMF initiates paging in the AMF. Paging is a process in which the network informs the UE, which may be in an idle state, that there is an incoming data transmission.

1.721 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.

1.722 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 1.721 “PPP” (p. 146) .

1.723 PPPoE

Point-to-Point Protocol over Ethernet

See also 1.721 “PPP” (p. 146) .

1.724 PPPRF

Point-to-Point Protocol over Radio Frequency

See also 1.721 “PPP” (p. 146) .

1.725 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.

1.726 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.

1.727 property form identifier link

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

1.728 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.

1.729 pseudonode

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

1.730 pseudowire

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

1.731 PSK

pre-shared key

The pre-shared key is a component of MACsec.

1.732 PSN

PSN can be expanded in two ways:

- 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.

- pseudonode number

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

1.733 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.

1.734 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.

1.735 PTP

Precision Time Protocol

A time synchronization protocol for networks.

1.736 PVC

PVC can be expanded in two ways:

1. 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.

2. persistent volume claim

   The PVC is the amount of disk space that a Kubernetes pod claims for it to use during its life.

1.737 PVP

permanent virtual path

A permanent ATM connection that is used to carry one or more PVCs.

1.738 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.

1.739 PW

See 1.730 “pseudowire” (p. 147) .

Q

1.740 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.*

1.741 QER

QoS enforcement rule

The QER is an enforcement rule for processing data traffic that instructs the user plane function to enforce QoS policing on the packets, within the context of CUPS. The QER is a rule that is provisioned by the Sx reference point when it establishes a session between the control and user plane functions.

1.742 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.

1.743 QMA

Quick-locking SMA

A QMA is a type of RF coaxial connector; see 1.851 “SMA” (p. 167).

1.744 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.

1.745 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.

1.746 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 1.837 “SFP” (p. 165).

1.747 QSFP+

Quad Small Form-factor Pluggable (enhanced)

An enhanced version of QSFP that supports data rates up to 10 Gb/s. See also 1.746 “QSFP” (p. 150).

R

1.748 RAA

Re-Auth Answer

An RAA message is sent by the PCEF to the PCRF to acknowledge that the PCEF has executed the new PCC rules that were carried in an RAR message sent by the PCRF.

1.749 RADIUS

remote authentication dial-in user service

A remote user authentication, authorization, and accounting protocol.

1.750 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.

1.751 RAR

Re-Auth-Request

An RAR command is sent by the CRF to notify the AF that the bearer for the established session has become unavailable.

An RAR command is also sent by the PCRF to the PCEF to execute new PCC rules when an event-trigger event occurs. The RAR message carries the new PCC rules.

1.752 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.

1.753 RBAC

role-based access control

RBAC is a method of controlling network access based on user roles within an organization. It provides employees with access rights to only those resources that they need to do their jobs and prevents them from accessing information that doesn't pertain to them.

1.754 RCA

root cause analysis

Problem solving methods used to determine the root cause of a problem.

1.755 RD

route distinguisher

An eight-byte BGP field that allows an operator to create a distinct route to a common IP address prefix.

1.756 RDI

remote defect indication

A signal sent to transmitting equipment by receiving equipment when defects are detected on an incoming signal.

1.757 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.

1.758 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 also 1.169 “checkpoint (regular)” (p. 61) .

1.759 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.

1.760 residential subscriber

See 1.903 “subscriber” (p. 174) .

1.761 Resource Administrator

Prior to NSP Release 23.11, the Resource Administrator utility managed resource pools and monitored pool usage.

Starting in Release 23.11, these functions are available from the **Resource Management** views.

See the *NSP System Administrator Guide*.

1.762 RESTCONF

The RESTCONF protocol (RFC 8040) is an HTTP-based protocol that provides an interface for data defined in YANG, using the datastore concepts defined in NETCONF.

1.763 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.

1.764 RET

RET is expanded two ways:

1. retransmission
2. remote electrical tilt

1.765 RFC

request for comments

A document that describes a technology specification. RFCs are used by the IETF and other standards bodies.

1.766 RHEL

Red Hat Enterprise Linux

RHEL is the supported 1.484 “Linux” (p. 110) distribution for NFM-P deployment.

1.767 RIB

routing information base

A router database that contains the routing information necessary for packet forwarding.

1.768 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.

1.769 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 1.675 “OSPF” (p. 140) .

1.770 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.

1.771 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.

1.772 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.

1.773 ROADM

Reconfigurable Optical Add/Drop Multiplexer

An optical network element with a configuration that can be changed remotely. This remote reconfigurability reduces OPEX when operating a 1.267 “DWDM” (p. 76) network. OPEX 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).

1.774 root bridge

The bridge with the highest priority ID, selected as the root in a spanning tree.

1.775 route flapping

A routing problem caused by network problems where an advertised route between two devices changes back and forth between two different paths.

1.776 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.

1.777 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.

1.778 routing instance

The configuration of a router, including information such as protocols, interfaces, routing, and policies.

1.779 routing protocol

A routing protocol is used to determine the correct route for packets within IP and IP/MPLS networks.

1.780 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.

1.781 RPC

remote procedure call

An RPC is a procedure call between applications that run on the same or different stations.

1.782 RPF

reverse path forwarding

A mechanism used by PIM to forward multicast packets down a distribution tree.

1.783 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.

1.784 RS-232-C

recommended standard - 232 - current

The physical interface and protocol used to connect serial devices.

1.785 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.

1.786 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.

1.787 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 1.903 “subscriber” (p. 174) .

1.788 RSRP

reference signal received power

1.789 RSRQ

reference signal received quality

1.790 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.

1.791 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.

1.792 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.

1.793 RT

route target or retransmission

In BGP/MPLS VPNs, an RT is an attribute that identifies a set of sites.

1.794 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.

1.795 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.

1.796 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.

1.797 RVPLS (R-VPLS)

Routed VPLS

Routed VPLS associates an L3 access interface on an IES or VPRN service to a VPLS service on the same site. Traffic with a destination MAC matching that of the associated interface is routed based on the IP forwarding table; all other traffic is forwarded based on the VPLS forwarding table.

1.798 RWO

ReadWriteOnce

A Kubernetes storage access mode. The volume can be mounted as read-write by a single node.

1.799 RWX

ReadWriteMany

A Kubernetes storage access mode. The volume can be mounted as read-write by multiple nodes.

S

1.800 S-NSSAI

single network slice selection assistance information

Identifier of a network slice in the 5G network. The S-NSSAI is sent to the network by the UE to select a network slice. The S-NSSAI is composed of the SST (slice/service type) and an optional SD (slice differentiator).

1.801 S-PE

switching-provider edge

In 1.575 “MS-PW” (p. 124) routing, switching-provider edge NEs are automatically created to forward inter-domain traffic between 1.916 “T-PE” (p. 176) NEs.

1.802 SA

security association

The SA is a security relationship that provides security guarantees for data transmitted among the members, such as IPsec peers, or MACsec CA members.

1.803 SAA

service assurance agent

The SAA is a SROS-based CLI command 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.

1.804 SAK

security association key; see 1.802 “SA” (p. 160)

A security association key is a component of MACsec, securing data plane traffic.

1.805 SAFI

Subsequent Family Address Identifier

See 1.67 “AFI” (p. 45).

BGP messages in which AFI=1 and SAFI=66 are "MDT-SAFI" messages.

1.806 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.

1.807 SAP

service access point

A SAP is a point of communication exchange between an application and the LLC, or between layers of software.

1.808 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.

1.809 SBA

service-based architecture

SBA provides a modular framework where common applications can be deployed using components from different sources. The control plane and common data repositories of a 5G network are delivered by interconnected network functions (NF). Network functions can access each other's services.

1.810 SBFD

Seamless bidirectional forwarding detection

Seamless BFD avoids the negotiation and state establishment for 1.115 "BFD" (p. 53) sessions, primarily by pre-determining the session discriminator and distributing the discriminators to remote network entities. This allows client applications or protocols to more quickly initiate and perform connectivity tests.

1.811 SBI

SBI is expanded two ways:

1. service-based interface

   The API-based communication between two VNFs in the 5G SBA. A VNF can use an API call over the SBI to implement a service or operation.

2. south-bound interface

1.812 SC

service component

An SC is a customer service that is a component of a composite service.

1.813 SCADA

Supervisory Control And Data Acquisition

An industrial data management system that monitors and controls IEDs

1.814 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.

1.815 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.

1.816 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.

1.817 Sd

The interface between the PCRF and the TDF/SSG.

1.818 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.

1.819 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.

1.820 SDK

software development kit

A collection of software development tools to facilitate the creation of applications, including a compiler, debugger and sometimes a software framework. They are normally specific to a hardware platform and operating system combination. See “SDK” in the *NSP Network Automation Guide* to know more.

1.821 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.

1.822 SDP

service distribution point

The NFM-P uses this term interchangeably with service tunnel.

1.823 SDRAM

synchronous dynamic random-access memory

The NFM-P uses this term interchangeably with service tunnel.

1.824 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.

1.825 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.

1.826 SEG

security gateway

A SEG is one or both ends of an IPsec tunnel.

1.827 SEPP

security edge protection proxy

For all 5G interconnect roaming messages, the SEPP is a network function that manages confidentiality or integrity between source and destination networks.

1.828 SEPP

security edge protection proxy

For all 5G interconnect roaming messages, the SEPP is a network function that manages confidentiality or integrity between source and destination networks.

1.829 Service Fulfillment

Prior to NSP Release 23.11, the Service Fulfillment application allowed for service provisioning and activation across networks accessible to the NSP.

Starting in Release 23.11, service management functions are available from the **Service Management** views.

See the *NSP Service Management Guide*.

1.830 service-level agreement

See 1.847 “SLA” (p. 167) .

1.831 Service Supervision

Prior to NSP Release 23.11, the Service Supervision application allowed users to monitor the health of services using KPIs, and monitor the fault status of a network.

Starting in Release 23.11, service information is found in the **Object Troubleshooting, Service** view.

See the *NSP Network and Service Assurance Guide* for more information.

1.832 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.

1.833 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.

1.834 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.

1.835 SFC

SFC is expanded two ways:

1. Static Filter CWDM

   A static filter card used with a CWDM circuit pack.

2. Service Function Chain

   A service function chain uses SDN capabilities to create a service chain of network services, such as firewalls and NAT, that are connected in a virtual chain. Network operators can then set up suites of connected services that use a single network connection. SFC automates the setup of virtual network connections to handle traffic flows for connected services.

1.836 SFD

Static Filter DWDM

A static filter card used with a DWDM circuit pack.

1.837 SFP

Small Form-factor Pluggable

A high-speed, compact, and hot-swappable optical modular transceiver.

1.838 SFP+

Small Form-factor Pluggable (enhanced)

An enhanced version of SFP that supports data rates up to 10 Gb/s. See also 1.837 “SFP” (p. 165)
.

1.839 SFTP

Secure File Transfer Protocol

A secure file transfer protocol is included with version 2 of the SSH application.

1.840 SHA

secure hash algorithm

A NIST standard hash algorithm, also known as SHA-1.

1.841 shared storage

Clustered storage available for access by pods running on any node in the cluster. Shared storage is used when more than one pod requires access to the same persistent volume.

1.842 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.

1.843 SHG

split horizon group

A group of SAPs or spoke SDPs. Members of the group cannot send traffic to each other.

1.844 SID

Segment Identifier

SIDs are used in segment routing.

1.845 SIM

Subscriber Identity Module

The SIM card stores the information needed to identify and authenticate the subscriber of a mobile device.

1.846 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.

1.847 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.

1.848 SLM

synthetic loss measurement

Ethernet synthetic loss measurement is used to count the number of synthetic 1.489 “LM” (p. 111) frames which are not successfully delivered to the specified destinations.

1.849 SLOF

section loss of frame

A field in a SONET channel frame that indicates the loss of a frame in the section frame sequence.

1.850 SLOS

section loss of signal

A field in a SONET channel frame that indicates the loss of section signaling.

1.851 SMA

SubMiniature version A

An SMA is a type of RF coaxial connector.

1.852 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.

1.853 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.

1.854 SMTP

simple mail transfer protocol

An application in the TCP/IP suite that manages the sending and receiving of e-mail messages.

1.855 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.

1.856 sniffer

A software tool that is used to monitor and analyze network traffic for troubleshooting or surveillance purposes.

1.857 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.

1.858 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.

1.859 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.

1.860 SNTP

Simple Network Time Protocol

A rudimentary version of NTP with only the features that devices commonly require.

1.861 SOAP

Simple Object Access Protocol

An XML-based protocol for the exchange of information in a decentralized, distributed environment.

1.862 Software bundle

A software bundle is a set of one or more files that you download and use for product deployment. A software bundle is comprised of one or more compressed archive files.

For NSP cluster deployment, a software bundle consists of a container runtime environment and NSP installation software.

See the *NSP User Guide* for more information about NSP software delivery.

1.863 Software suite

A software suite is a conceptual collection of feature packages. Software suites are not licensed or bundled for delivery, but to create a set of feature packages to meet specific network management requirements.

See the *NSP User Guide* for more information about software suites.

1.864 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.

1.865 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.

1.866 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.

1.867 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.

In IP spoofing, an IP packet is generated with a false source IP address that was not assigned by the PGW in order to hide the identity of the UE or impersonate another computing system.

1.868 SPT

shortest path tree

SPT is an algorithm used by PIM to make routing decisions based on the state of network links.

1.869 SPV

set parameter values

Type of TR-069 RPC method.

1.870 SQL

structured query language

A specialized language for accessing relational databases.

1.871 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.

1.872 SRL OS

See 1.873 “SR Linux OS” (p. 170).

1.873 SR Linux OS

Service Router Linux Operating System

SR Linux OS is the operating system for Linux variants of the 7250 IXR, 7450 ESS, 7750 SR, 7950 XRS, and VSR platforms.

1.874 SR OS

Service Router Operating System

SR OS is the operating system for the 7250 IXR, 7450 ESS, 7750 SR, 7950 XRS, and VSR platforms.

1.875 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.

1.876 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.

1.877 SSC

session and service continuity

SSC ensures uninterrupted service to the user by supporting user plane node reselection when there is UE mobility or high load of the serving user plane node.

1.878 SSD

source statistics descriptor

The characteristic of traffic in the conversational UMTS traffic class. The SSD can be either speech or unknown.

1.879 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.

1.880 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.

1.881 SSH2

SSH version 2

SSH2 is a more secure, efficient, and portable version of SSH that includes SCP. See 1.880 “SSH” (p. 171) .

1.882 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.

1.883 SSL

Secure Sockets Layer

A security protocol that is deprecated by the IETF, and replaced by 1.935 “TLS” (p. 179).

1.884 SSLF

section synchronization line failure

A SONET alarm that indicates a failure of the frame synchronization for a section.

1.885 SSM

SSM can be expanded in the following ways:

- 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.
- synchronous status message

1.886 SSU

synchronization supply unit

A timing synchronization unit that filters and distributes synchronization signals to local equipment.

1.887 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.

1.888 STAR

Self-Tuned Adaptive Routing

A load-balancing and optimal-path-placement algorithm used by the Path Control function in NSP.

1.889 static host

See 1.891 “static subscriber host” (p. 172) .

1.890 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.

1.891 static subscriber host

A host that is explicitly configured on a SAP rather than through a dynamic learning process.

1.892 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 1.1024 “workstation” (p. 194) .

1.893 statistics

Statistics are the quantitative data collected by the NFM-P for entities such as equipment, network protocols, interfaces, and alarms.

1.894 STB

See 1.834 “set-top box” (p. 165) .

1.895 STE

section terminating equipment

SONET equipment that originates, accesses, modifies, or terminates section header information.

1.896 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.

1.897 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.

1.898 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.

1.899 STP 1x1 mode

The STP 1x1 mode is a proprietary implementation of the STP that applies a single spanning tree instance per VLAN.

1.900 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.

1.901 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.

1.902 STS

synchronous transport signal

The electrical equivalent of the SONET optical signal. In SDH, STS is known as STM.

1.903 subscriber

In the NFM-P, a subscriber represents a unique identifier that associates a group of end-user devices with policies and resources.

1.904 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 1.372 “host” (p. 93) .

1.905 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.

1.906 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.

1.907 switch fabric processor

A processor that handles traffic passing through the switch fabric.

1.908 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.

1.909 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.

1.910 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.

1.911 SyncE

See 1.912 “Synchronous Ethernet” (p. 175) .

1.912 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.

1.913 syslog

A message logging standard used by network devices to send event messages to a logging server (syslog). Syslog separates the software that generates the messages, the system that stores them, and the software that reports and analyzes them.

T

1.914 T1

A 1.544-Mb/s point-to-point dedicated digital circuit provided by the telephone companies in North America.

1.915 T-LDP

Targeted-Label Distribution Protocol

An LDP session between indirect connect peers.

1.916 T-PE

termination-provider edge

In 1.575 “MS-PW” (p. 124) routing, termination-provider edge NEs are the endpoints of the MS-PW service. T-PEs are configured with PW SDPs that connect to 1.801 “S-PE” (p. 160) NEs.

1.917 TAC

TAC is expanded in the following 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
3. type allocation code

   The first eight-digit part of the 15-digit IMEI and 16-digit IMEISV codes that is used to uniquely identify wireless devices.

1.918 TACACS+

terminal access controller access control system

A remote user authentication, authorization, and accounting protocol.

1.919 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.

1.920 TCA

Threshold-crossing alert

A TCA occurs when a statistics counter value crosses the defined threshold during a 15-min interval.

1.921 TCE

TCE can be expanded as:

- trace-collection entity
- threshold crossing event; see 1.920 “TCA” (p. 176).

1.922 TCN

topology change notification

A bridge uses TCN BPDUs to notify the root bridge about a detected topology change.

1.923 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.

1.924 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.

1.925 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.

1.926 TDM

time division multiplexing

Multiplexing in which a separate periodic time interval is allocated to each tributary channel in a common aggregated channel.

1.927 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.

1.928 TED

traffic engineering database

A TED is a database used by CSPF for storing route constraint information.

1.929 telco

telephone company

A company that provides local, or local and long-distance, telephone services.

1.930 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.

1.931 Templates

NSP uses intent types to build service and tunnel templates, which are then used to create services and service tunnels

Intent types can be imported into the NSP from the **Artifacts** views, which also imports the models into service management. Users with the NSP programming suite can also create custom intent types within the **Network Intents** views.

Templates serve as a starting point for service or tunnel creation by providing a set of predefined parameters to configure.

1.932 TI-LFA

See 1.479 “LFA” (p. 110).

1.933 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.

1.934 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.

1.935 TLS

TLS is expanded two ways:

1. Transparent LAN Service

   A network service that links remote Ethernet networks to provide the appearance and functions of one contiguous network to users, regardless of the underlying technology.

2. Transport Layer Security

   A security protocol that replaces the deprecated 1.883 “SSL” (p. 172) protocol. TLS provides communication security, privacy, and message integrity over a computer network, and is used in applications such as web browsing, e-mail, and instant messaging.

   The NFM-P uses TLS to encrypt the communication between system components.

1.936 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.

1.937 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.

1.938 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.

1.939 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.

1.940 TOADM

tunable optical add/drop multiplexer

A tunable 1.773 “ROADM” (p. 155) that yields the ultimate in operational flexibility, especially when used in conjunction with transponders with tunable wavelength lasers.

1.941 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.

1.942 T-PDU

The inner IP packet in a GTPv1-U packet.

1.943 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.

1.944 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.

1.945 transit SAP

An access interface on a VLL or VPLS that forwards traffic with any encapsulation values transparently through the service.

1.946 transit service

A service tunnel that uses transit SAPs to pass traffic for existing VLL or VPLS data services or composite services.

1.947 Transport Slice Controller

Prior to NSP Release 23.11, the Transport Slice Controller application was a functional block that provided realization, monitoring, and optimization of transport slices in the network.

Starting in Release 23.11, transport slice controller functions are available from the **Network Map and Health, Overview** view.

See the *NSP Transport Slice Controller Guide*.

1.948 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.

1.949 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.

1.950 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.

1.951 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.

1.952 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.

1.953 tunnel

A method of setting up a communication session between two or more points that hides the complexity of the underlying technologies.

1.954 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.

1.955 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.

1.956 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.

1.957 TWL

TWAMP Light

TWAMP Light tests target Layer 3 interfaces. See 1.956 “TWAMP” (p. 182).

U

1.958 u-plane

See 1.969 “user plane” (p. 184) .

1.959 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.

1.960 UCT

universal coordinated time

UCT is also known as Greenwich Mean Time.

1.961 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.

1.962 UE

user equipment

The mobile unit, which allows a user to access network services. The UE connects to the UTRAN through a radio interface.

1.963 UI

user interface

See 1.363 “GUI” (p. 90) .

1.964 UIC

unit ID code

A field in an MDL message that identifies the CSU or DSU of the originating equipment.

1.965 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.

1.966 UNIX

A multi-user, multitasking OS on which Linux is modeled.

1.967 URR

usage reporting rule

The URR is a usage reporting rule for processing data traffic that instructs the user plane function to measure and report traffic usage, within the context of CUPS. The URR is a rule that is provisioned by the Sx reference point when it establishes a session between the control plane and user plane functions.

1.968 User Manager

Prior to NSP Release 23.11, the User Manager application allowed administrators to perform user session management, user activity logging, user access control, and local user account management..

Starting in Release 23.11, these functions are available in the **Users and System Security** views.

See the *NSP System Administrator Guide*.

1.969 user plane

The portion of a telecommunications network that is involved with user traffic, including voice, data, and video. See also 1.958 “u-plane” (p. 183) .

1.970 user VPLS

A VPLS that contains SAPs that receive multicast traffic from an MVR VPLS.

1.971 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.

1.972 UTC

Coordinated Universal Time

primary time standard by which the world regulates clocks and time

1.973 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

1.974 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.

1.975 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.

1.976 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 1.626 “nrt-VBR” (p. 132) and 1.794 “rt-VBR” (p. 158) .

1.977 VC

virtual connection

A technique ensuring that packets are delivered to the correct recipient in the same order as they were submitted.

1.978 VCB

voice conference bridge

The voice conference bridge application provides a simultaneous communication path between two or more voice circuits. VCBs are deployed in a central location with remote devices connected to the bridge via an NE over an IP/MPLS or TDM network. Inputs to the VCB are 4-wire E&M analog interfaces.

VCBs can be used as a conference bridge with any-to-any connectivity (all branches participate) or as a bridge in broadcast mode where one branch broadcasts to the other branches that are in listen-only mode.

1.979 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.

1.980 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.

1.981 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.

1.982 VHO

video head end office

The VHO is where the video server complex resides.

1.983 VID

VLAN Identifier

A VID is a 12-bit field in an Ethernet frame that uniquely identifies the VLAN to which the frame belongs.

1.984 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.

1.985 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.

1.986 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.

1.987 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.

1.988 VLL

virtual leased line

A virtual leased line is a type of VPN where IP traffic is transported in a point-to-point manner.

1.989 VNF

Virtual Network Function

A virtualized network element that represents a physical node.

1.990 VoD

video on demand

An application that provides a specific, non-broadcast video stream to an end user. Triple play service sometimes includes VoD.

1.991 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.

1.992 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.

1.993 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.

1.994 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.

1.995 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.

1.996 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.

1.997 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.

1.998 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.

1.999 VQM

video quality monitoring

VQM monitors video quality in the stages of transmission just prior reaching the STB.

1.1000 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.

1.1001 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.

1.1002 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.

1.1003 VRS

Virtual Routing and Switching

VRS is a service solution is implemented and monitored by the VSD.

1.1004 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.

1.1005 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.

1.1006 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.

1.1007 VSP

Virtualized Services Platform

VSP is a software-defined networking solution that provides data center network virtualization and manages connectivity between compute resources.

1.1008 VSR

Virtual Service Router

A software-only version of the 7750 SR.

1.1009 VT

virtual trunk

An aggregation of ATM VCs. All connections on a VT map to a single VPC with a public network-assigned VPI.

1.1010 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.

1.1011 VTG

virtual tributary group

One or more virtual tributaries of the same rate that are bundled into an STS-1 payload.

1.1012 VWM

Versatile WDM Module

See 1.5 “1830 VWM” (p. 35) .

W

1.1013 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.

1.1014 WDM

Wavelength Division Multiplexing

Several signals (or channels) are transported simultaneously over one fiber but at different wavelengths without interaction. Each channel is usually 1.926 “TDM” (p. 177) . The capacity of a WDM system is thus given by the number of wavelengths × the bit rate of the 1.926 “TDM” (p. 177) channel.

1.1015 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.

1.1016 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.

1.1017 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.

1.1018 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.

1.1019 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.

1.1020 workflow

A workflow in NSP represents a process to be executed by the NSP. Each workflow consists of at least one task.

Workflows can be configured in the **Workflows** views.

1.1021 Workflow Manager

Prior to NSP Release 23.11, the Workflow Manager application allowed creation and execution of workflows in NSP.

Starting in Release 23.11, these functions are available in the **Workflows** views.

See the *NSP Network Automation Guide*.

1.1022 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 1.161 “certified directory” (p. 60) .

1.1023 working panel

The working panel is a component of the NFM-P GUI that can include windows, drawings, and configuration forms.

1.1024 workstation

A computer system with a local set of input and output devices, such as a keyboard and monitor.

1.1025 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.

1.1026 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.

1.1027 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.

1.1028 WS-NOC

WaveSuite Network Operations Center

The WS-NOC provides unified optical end-to-end network management and operational support for all network element products in the Nokia's optics portfolio.

Formerly known as the NFM-T.

1.1029 WS-RC

WaveSuite Resource Controller

Formerly known as the NRC-T.

1.1030 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

1.1031 X.25

An ITU-T data communications protocol and interface for public packet-switched communication between a network user and the network.

1.1032 X.733

X.733 is the standard that describes the alarm reporting function.

1.1033 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.

1.1034 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.

1.1035 XMDA

extended media dependent adapter.

See 1.532 “MDA” (p. 118) .

1.1036 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.

1.1037 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.

1.1038 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.

1.1039 XNS

Xerox network standard

The term for the suite of Internet protocols developed by researchers at the Xerox Corporation.

1.1040 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.

Y

1.1041 YAML

YAML Ain’t Markup Language

YAML is a data serialization language which is designed to be human-readable.

Z

1.1042 zone

A portion of the namespace defined by the 1.243 “DNS” (p. 72) 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.

1.1043 ZTP

Zero Touch Provisioning

ZTP is an SR OS feature that automatically configures a node by obtaining the required information from the network and provisioning the device with minimal manual intervention and configuration. When new devices that support ZTP are connected and boot up, the device is auto-provisioned.

2 Initialisms

The following table lists acronyms and initialisms used in NSP documentation, along with their expansions. These terms are industry standards, self-explanatory, or defined in other documentation sets for other products. Expansions are provided to assist readers who may be unfamiliar with the terms and who need to look for definitions elsewhere.

Term	Expansion
ACR	accounting requests
AD	add drop
ADP	auto discovery process
ADT	add drop through
AGW	access gateway
AHPHG	High Power High Gain Amplifier
AHPLG	High Power Low Gain Amplifier
ALD	antenna line device
ALPFGT	Low Power Fixed Gain Amplifier card with total power monitoring
ALPHG	Low Power High Gain Amplifier card
AMR	adaptive multi-rate
ANM	Any rate pluggable I/O card
ANSI	American National Standards Institute
AOS	NokiaOmniSwitch
APAC	Asia Pacific and China
ASE	Amplified Spontaneous Emissions
ASL	Application Specific License
AS-MAC	asynchronous-MAC
ASN	autonomous system number
ASN.1	abstract syntax notation one
AUX	auxiliary
AVCN	Attribute value change notification
B-MAC	backbone or provider MAC
BNG	broadband network gateway
B-TAG	backbone VLAN tag

Term	Expansion
B-VID	backbone VLAN Id
B-VLAN	backbone VLAN
B-VPLS	backbone VPLS
BBU	base band unit
BCB	backbone core bridge
BEB	backbone edge bridge
BGP LU	Border Gateway Protocol Labeled Unicast
BNM	bandwidth notification message
BRAS	broadband remote access server
C	client port
C-MAC	customer MAC
CA	certificate authority
CAC	Connection Admission Control
CAD	Channel Add Drop
CBAM	CloudBand Application Manager
CBRS	citizens broadband radio service
CBSD	citizens broadband radio service device
CCF	charging control function
CCR-A	credit control request answer
CCR-I	credit control request initial
CCR-T	credit control request terminate
CCR-U	credit control request update
CDC-F	colorless, directionless, and contentionless flexible grid
CDF	charging data function
CDL	cross-domain link
CFOADM	1.214 “CWDM” (p. 68) Fixed Optical Add Drop Multiplexer
CFP	compact form factor pluggable
CGI	cell global identity

Term	Expansion
CHLI	consecutive high loss interval
CLE/ODNC	critical link event/OAM discovery not completed
CLR	Customer License Repository
CM	configuration management
COF	channel optical filter
CPB	commissioning and power balancing
CPG	client protection group
CPM	control plane module
CPU	central processing unit
CS	circuit switched
CSR	Certificate Signing Request
csros	classic SR OS
CTP	connection termination point
CUPS	control and user plane separation
CVLAN	customer VLAN
CWR8	8–Channel colorless wavelength router card, 44 channel
CWR8-88	8–Channel colorless wavelength router card, 88 channel
DAPI	Destination Access Point Identifier
DB	database
DGE	dynamic gain equalizer
DMM	delay measurement message
DNU	do not use
DOIC	diameter overload indication conveyance
DPA	diameter proxy agent
DPR	disconnect peer request
DSAP	destination service access point
DTE	data terminating entity
DUS	do not use for synchronization

Term	Expansion
E-LAN	Ethernet Local Area Network
E-Line	Ethernet Virtual Private Line
E-LSP	EXP inferred LSP
E-SNCP	Electrical-Subnetwork Connection Protection
EAC	Ethernet Access Card
EAS	Ethernet Access Switch
EC	Equipment controller
ECGI	E-UTRAN cell global identifier
ED	Edge device
EDFA	Erbium doped fiber amplifier
eHA	enterprise Home Agent
EM	element manager
EOP	end-of-packet
EPS	equipment protection switching
EPT	Engineering and Planning Tool
ERO	Explicit Router Object
ERPS	Ethernet ring protection switching
ES	Ethernet Segment
ESI	Ethernet segment identifier
ESNCP	Electrical sub-block network connection protection
ETH-LBM	Ethernet-loopback message
ETR	extended temperature range
eVOA	electrical variable optical attenuator
FBC	flow-based charging
FDN	fully distinguished name
FEP	front end processor
FF	Flex framer
FFD	fast fault detection
FM	fault management

Term	Expansion
FOADM	Fixed optical add/drop multiplexer/multiplexing
FQDN	fully qualified domain name
FRR	fast reroute
FUA	fixed uplink allocation
fVOA	fast variable optical attenuator
FXO	Foreign Exchange Office
FXS	Foreign Exchange Subscriber
GNI	Gigabit Ethernet Network Interface
GPE	Generic Protocol Extension
GPS	global positioning system
GQP	Generic QoS Profile
GRT	global route table
gsros	global SR OS
GSU	Granted-Service-Unit
H-VPLS	hierarchical virtual private LAN service
HDD	hard disk drive
HI component	horizontal integration component
HLI	high loss interval
HO	handover
HPCFAP	high power connection fuse and alarm panel
HSDPA	high-speed data-link packet access
HSPA	high-speed packet access
HSU	high capacity subscriber unit
HVPLS	hierarchical virtual private LAN service
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)
IB-RCC	in-band ring control connection

Term	Expansion
ICB	inter-chassis backup
ICCN	incoming call connected
ICE	in case of emergency
ICRQ	incoming call request
ID	identifier or identification
IEEE	Institute of Electrical and Electronics Engineers
ILA	in-line amplifier
ILM	incoming label map
IMPM	ingress multicast path management
IPCC	Internet Protocol Communication Channel
IPTV	Internet-based television transmission
ISID	Service Identifier
ISC	integrated services card
ISL	inter-switch link
ISO	International Standards Organization
ISSU	in-service software upgrade
IT	information technology
ITL	interleaver
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
JSON	JavaScript Object Notation
KCI	key capacity indicator
KVM	kernel-based virtual machine
L	line port
L-LSP	label only inferred LSP
LACPDU	link aggregation control protocol data unit
LBR	loopback reply
LB-VM	load balancer VM
LCN	Lifecycle change notification

Term	Expansion
LD	Line driver
LED	light-emitting diode
LH	Long haul
LLD	link layer discovery
LMP	Link Management Protocol
LMT	local maintenance terminal
LO–ODUk	Lower Order–Optical Data Unit–k (k=1 to 8)
LS	link state
LTR	link trace response
MBB	make before break
MC APS	multi chassis automatic protection switching
MC LAG	multi chassis link aggregation group
ME	metro Ethernet
MEF	Metro Ethernet Forum
MEI	mobile equipment identity
MI	management interface
MIM	management information model
MMRP	Multiple MAC Registration Protocol
MOC	managed object class
MP	multipoint
MPT-ACC	microwave packet transport-access
MPT-HC	microwave packet transport-high capacity
MPT-HQAM	microwave packet transport-hierarchical quadrature amplitude modulation
MPT-MC	microwave packet transport-medium capacity
MPT-XP	microwave packet transport-eXtreme power
MRP	Multiple Registration Protocol
MSBN	multi-service broadband network
MSB	most significant bit
MSE	mean squared error

Term	Expansion
MSM	mobility service module
MSP	multiplex section protection
msros	model-driven SR OS
MTSO	Mobile Telephone Switching Office
MVRP	Multi-VLAN Registration Protocol
MW	microwave
MWA	microwave-aware
NA	Neighbor Advertisement
NBI	north-bound interface
NBNS	NetBIOS name server
ND	node discovery
NETCONF	Network Configuration Protocol
NI	network ID
NIST	National Institute of Standards and Technology
NLRI	network layer reachability information
NOS	network operating system
NPDU	network protocol data unit
NRC	network resource controller
NSAPI	network service access point identifier
NSP	Network Services Platform
NSWO	non-seamless WLAN offload
O-GLSP	optical-generalized label switched path
OAMPDU	operations, administration, and maintenance protocol data unit
OAM-VM	operations, administration, and management VM
OCS	optical core switch
OFC	OpenFlow Controller
OFS	OpenFlow Switch
OMC	Optical Management Console

Term	Expansion
OMD	optical multiplexer/demultiplexer
OMSP	optical multiplex section protection
OOS	out of service
OPEX	operating expenditures
OPR	optical power receive
OPSA	optical protection switch - advanced card
OPT	optical power transmit
OPTSG	OPU1 Timing Slot Group
OPUk	Optical Channel Payload Unit-k (k=1,2, or 3)
OTDR	optical time domain reflectometer
OTU	optical transport unit
P	provider core
P2MP	point to multi-point
PAT	program association table
PBB	provider backbone bridge or provider backbone bridging
PBBN	provider backbone bridged network
PBN	provider bridge network
PBR	policy-based routing
PC	personal computer
PCE	IP path computational engine
PCEP	Path Computation Element Protocol
PCM	pulse code modulation
PDSN	public data switched network
PECF	policy enforcement and charging function
PEM	power entry module
PF	power filter
PG	postgres
PIM-SM	PIM sparse mode
PIM-SSM	PIM-source specific multicast

Term	Expansion
PLAR	Private Line Automatic Ringdown
PLSP-ID	Path LSP-ID
PMC	packet microwave card
PMSI	provider multicast service interface
PMT	program map table
PON	passive optical network
PS	packet switched
PSI	program specific information
PSS	Photonic Service Switch
PST	Primary state
PWRSV	Power-save mode
PXC	Photonic Cross Connect
QAM	quadrature amplitude modulation
QFI	QoS flow identifier
QL	quality level
QoE	quality of experience
R-APS	ring automatic protection switching
RAB	radio access bearer
RAC	routing area code
RAE	remote antenna extension
RAN	radio access network
RAU	routing area update
REST	Representational state transfer
RF	radio frequency
RFM	radio frequency module
RG	rating group
RMON	remote network monitoring
RNCV	ring node connectivity verification
RPS	radio protection switching
RRH	remote radio head

Term	Expansion
RRO	record route object
rwa	read-write access
S-PMSI	selective provider multicast service interface
SAII	Source Attachment Individual Identifier
SCI	service class indicator
SCM	secure certification mode
SCTE35	society of cable telecommunications engineers
SDC	service data container
SDN	software-defined networking
SFM	Switch Fabric Module
SMM	Site Monitoring Module
SN	sequence number
SNCI	subnetwork connection (protection) inherent monitoring
SNCN	subnetwork connection (protection) non-intrusive monitoring
SNCNC	subnetwork connection non-intrusive monitoring client protection
SRGB	Segment Routing Global Block
SR TE	segment routing with traffic engineering
srTCM	single rate three color marking
SSAP	source service access point
SSO	single sign on
SST	secondary state
SVLAN	service provider VLAN
SVN	software version number
sVOA	slow variable optical attentuator
TAII	Target Attachment Individual Identifier
TAU	tracking area update
TEDB	TE database
TEI	transport error indicator

Term	Expansion
TNC	tech non-conformant
TOA	transport stream off-air
TPM	Template Provisioning Manager
TPMR	two port MAC relay
TPS	transmission protection switching
TRDU	transceiver duplexer unit
trTCM	two rate three color marking
TRU	top rack unit
Tx	transmit
UBT	Ultra Broadband Transceiver
UECM	user equipment context management
UID	Unique ID
ULI	user location information
UMTS	Universal Mobile Telecommunication System
UNIVTRM	universal transmission
UPF	user plane function
URPF	Unified reverse path forwarding
URL	uniform resource locator
usros	unified SR OS
USU	used service unit
UUID	Universally Unique Identifier
UWAN	untrusted wireless access network
vCPAA	virtual control plane assurance adaptor
VINES	virtual networking system
VM	virtual machine
VNFC	Virtual Network Function Component
VNI	VXLAN Network Identifier
VPWS	Virtual Private Wire Service
VSI	virtual switch instance
VSR-I	Virtualized Service Router Integrated

Term	Expansion
VTEP	VLAN tunnel end point
VTL	velocity template language
VXLAN	Virtual Extensible LAN
WFF	weighting factor file
WTOCM	Wavelength Tracker Optical Channel Monitoring card
XC	cross connect
XFP	10 Gigabit Small Form Factor Pluggable
XNI	10 Gigabit Network Interface
YANG	Yet Another Next Generation