INTERNATIONAL TELECOMMUNICATION UNION

ITU-T G.8081/Y.1353

(06/2004)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Digital networks – General aspects

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION NETWORKS

Internet protocol aspects – Transport

Terms and definitions for Automatically Switched Optical Networks (ASON)

ITU-T Recommendation G.8081/Y.1353

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TESTING EQUIPMENTS	G.500–G.599
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DIGITAL TERMINAL EQUIPMENTS	G.7000–G.7999
DIGITAL NETWORKS	G.8000–G.8999
General aspects	**G.8000–G.8099**
Design objectives for digital networks	G.8100–G.8199
Quality and availability targets	G.8200–G.8299
Network capabilities and functions	G.8300–G.8399
SDH network characteristics	G.8400–G.8499
Management of transport network	G.8500–G.8599
SDH radio and satellite systems integration	G.8600–G.8699
Optical transport networks	G.8700–G.8799

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation G.8081/Y.1353

Terms and definitions for Automatically Switched Optical Networks (ASON)

Summary

This Recommendation provides terms, definitions, and abbreviations used in Automatically Switched Optical Network (ASON) Recommendations. It contains a list of the definitions and abbreviations introduced in Recommendations associated with Automatically Switched Optical Networks, and can be considered a companion document to ITU-T Recs G.780/Y.1351 and G.870/Y.1352. The goal of this Recommendation is to be a single normative source for terms in this subject area.

Source

ITU-T Recommendation G.8081/Y.1353 was approved on 13 June 2004 by ITU-T Study Group 15 (2001-2004) under the ITU-T Recommendation A.8 procedure.

Keywords

Acronyms, ASON, Automatically Switched Optical Network, terminology, terms.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation G.8081/Y.1353

Terms and definitions for Automatically Switched Optical Networks (ASON)

1 Scope

This Recommendation contains a complete listing of the terms, definitions, and abbreviations introduced in the Recommendations associated with Automatically Switched Optical Network.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- ITU-T Recommendation G.780/Y.1351 (2004), *Terms and definitions for synchronous digital hierarchy (SDH) networks*.
- ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.
- ITU-T Recommendation G.807/Y.1302 (2001), *Requirements for automatic switched transport networks (ASTN)*.
- ITU-T Recommendation G.852.2 (1999), *Enterprise viewpoint description of transport network resource model*.
- ITU-T Recommendation G.870/Y.1352 (2004), *Terms and definitions for Optical Transport Networks (OTN)*.
- ITU-T Recommendation G.7713/Y.1704 (2001), *Distributed Call and Connection Management (DCM)* plus Amd.1 (2004).
- ITU-T Recommendation G.7713.1/Y.1704.1 (2003), *Distributed Call and Connection Management (DCM) based on PNNI*.
- ITU-T Recommendation G.7713.2/Y.1704.2 (2003), *Distributed Call and Connection Management: Signalling mechanism using GMPLS RSVP-TE*.
- ITU-T Recommendation G. 7713.3/Y.1704.3 (2003), *Distributed Call And Connection Management: Signalling mechanism using GMPLS CR-LDP*.
- ITU-T Recommendation G.7714/Y.1705 (2001), *Generalized automatic discovery techniques*.
- ITU-T Recommendation G.7714.1/Y.1705.1 (2003), *Protocol for automatic discovery in SDH and OTN networks*.
- ITU-T Recommendation G.7715/Y.1706 (2002), *Architecture and requirements for routing in the automatically switched optical networks*.
- ITU-T Recommendation G.7715.1/Y.1706.1 (2004), *ASON routing architecture and requirements for link state protocols*.

– ITU-T Recommendation G.8080/Y.1304, (2001), *Architecture for the automatically switched optical network (ASON)* plus Amd.1 (2003).

– ITU-T Recommendation M.3010 (2000), *Principles for a telecommunications management network*.

3 Definitions

3.1 Terms defined in other Recommendations

This Recommendation uses following terms defined in other ITU-T Recommendations.

3.1.1 Terms defined in ITU-T Rec. G.780/Y.1351

– Data Communications Channel (DCC)
– Embedded Control Channel (ECC)
– Link Capacity Adjustment Scheme (LCAS)
– Network Node Interface (NNI)
– Protection

3.1.2 Terms defined in ITU-T Rec. G.805

– Access Group (AG)
– Access Point (AP)
– Administrative domain
– Client-server Relationship
– Connection
– Connection Point (CP)
– Connection Termination Point (CTP)
– Layer network
– Link
– Link Connection
– Management domain
– Network Connection
– Termination Connection Point
– Partitioning
– Port
– Subnetwork
– Subnetwork connection
– Trail
– Trail termination
– Transport
– Unidirectional access point
– Unidirectional connection
– Unidirectional connection point
– Unidirectional port
– Unidirectional trail

3.1.3 Term defined in ITU-T Rec. G.806

– Client/server Layer

3.1.4 Terms defined in ITU-T Rec. G.870/Y.1352

– Entity
– General Communication Channel (GCC)
– General Management Communications Overhead (COMMS OH)
– Layer
– Local craft terminal
– Management communications
– Management Information (MI)
– Management Point (MP)
– Optical Channel (OCh)
– Optical Channel Data Unit (ODUk)
– Optical Channel Transport Unit (OTUk)
– Optical Network Element (ONE)
– Optical Overhead Signal (OOS)
– Optical Supervisory Channel (OSC)
– Optical Transport Network (OTN)
– Optical transport network node interface (ONNI)
– Restoration
– Resource
– Transport entity
– Transport Network

3.1.5 Terms defined in ITU-T Rec. G.7712/Y.1703

– Data Communication Network (DCN)
– Dual interfaces
– Signalling Communication Network (SCN)

3.1.6 Terms defined in ITU-T Rec. M.3010

– Data Communication Function (DCF)
– Mediation Device (MD)
– Network Element (NE)
– Network Element Function (NEF)
– Operations System (OS)
– Operations System Function (OSF)
– Q-interface
– q reference points
– Reference Point (RP)

3.1.7 Terms defined in ITU-T Rec. M.3013

– Message Communication Function (MCF)
– WorkStation Function (WSF)

3.1.8 Terms defined in ITU-T Rec. M.3100

– Management interface
– Connection Termination Point (CTP)
– Managed entity
– Trail Termination Point (TTP)

3.1.9 Term defined in ITU-T Rec. X.700

– Managed Object (MO)

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 Access Group Container (AGC): An AGC is a single layer entity that contains access groups, LRMs, and TAPs. It is similar to G.805 subnetworks except that it is not recursively defined, may or may not be a matrix (it does not have to be specified), and has no defined subnetwork connections. Multiple AGCs from different layers may be co-incident in the same equipment. See ITU-T Rec. G.8080/Y.1304.

3.2.2 address: An address is a string of symbols that is valid regardless of the location of the source but changes if the destination moves. An address is used for the purpose of routing. Source and destination addresses must be globally unique.

3.2.3 agent: Within this Recommendation, the term agent is used to describe the entity that represents certain attributes and behaviour of a resource. The agent allows interaction between various resources and management and control functions. More than one agent may represent a resource.

3.2.4 Automatic Encapsulating Data Communication Function (AE-DCF): An AE-DCF automatically encapsulates packets when necessary so that they may be routed by NEs that would otherwise be unable to forward them. An AE-DCF also features a matching de-encapsulation function to restore the packet back to its original form once it has traversed incompatible NEs.

3.2.5 Automatic Switched Transport Network (ASTN): A transport network where configuration connection management is implemented by means of a control plane.

3.2.6 call: An association between endpoints that supports an instance of a service.

3.2.7 call control: Call control is a signalling association between one or more user applications and the network to control the set-up, release, modification and maintenance of sets of connections. See ITU-T Rec. G.8080/Y.1304.

3.2.8 call admission control: Call admission control is a policy function invoked by an Originating role in a network and may involve cooperation with the terminating role in the network. See ITU-T Rec. G.8080/Y.1304.

3.2.8.1 originating call admission function: The originating call admission function is responsible for checking that a valid called user name and parameters has been provided. See ITU-T Rec. G.8080/Y.1304.

3.2.8.2 terminating call admission function: The terminating call admission function is responsible for checking that the called party is entitled to accept the call, based on the calling party and called party service contracts. See ITU-T Rec. G.8080/Y.1304.

3.2.9 call controller: Calls are controlled by means of call controllers. There are two types of call controller components.

3.2.9.1 calling/called party call controller: This is associated with an end of a call and may be co-located with end systems or located remotely and acts as a proxy on behalf of end systems. This controller acts in one, or both, of two roles, one to support the calling party and the other to support the called party.

3.2.9.2 Network call controller: A network call controller provides two roles, one for support of the calling party and the other to support the called party.

A calling party call controller interacts with a called party call controller by means of one or more intermediate network call controllers. See ITU-T Rec. G.8080/Y.1304.

3.2.10 call segment: An association between two call control entities (call controllers), using a telecommunication service to concatenate a call.

3.2.11 signalling controller: A signalling controller contains the functions of connection control and/or call control.

3.2.12 connection admission control: Connection admission control is essentially a process that determines if there are sufficient resources to admit a connection (or re-negotiates resources during a call). See ITU-T Rec. G.8080/Y.1304.

3.2.13 Connection Controller (CC): A component in the ASON control plane. The connection controller is responsible for coordination among the link resource manager, routing controller, and both peer and subordinate connection controllers for the purpose of the management and supervision of connection set-ups, releases and the modification of connection parameters for existing connections. See ITU-T Rec. G.8080/Y.1304.

3.2.14 Connection Controller Interface (CCI): An interface between a subnetwork in the transport plane and the control plane. See ITU-T Rec. G.8080/Y.1304.

3.2.15 Discovery Agent (DA): The "federation" of discovery agents operates in the transport plane name space, and provides for separation between that space and the control plane names. The federation has knowledge of Connection Points (CPs) and Termination Connection Points (TCPs) in the network, while a local DA has knowledge of only those points assigned to it.

3.2.16 domain: A domain represents a collection of entities that are grouped for a particular purpose. See ITU-T Rec. G.8080/Y.1304.

3.2.16.1 control domain: A control domain is an architectural construct that encapsulates and hides the detail of a distributed implementation of a particular group of architectural component of one or more types. The entities that are grouped in a control domain are components of the control plane. See ITU-T Rec. G.8080/Y.1304.

3.2.16.2 rerouting domain: A group of call and connection controllers that share control of domain-based rerouting. A rerouting domain must be entirely contained within a routing domain or area. A routing domain may fully contain several rerouting domains. See ITU-T Rec. G.8080/Y.1304.

3.2.17 E-NNI transport resource name: The ENNI SNPP Link may be assigned a name for the network call controllers to specify E-NNIs. These names must be globally unique and are assigned by the ASON network. Multiple names may be assigned to the SNPP link.

3.2.18 federation: A community of domains that cooperates for the purposes of connection management, and is illustrated using the cooperation between connection controllers. See ITU-T Rec. G.8080/Y.1304.

3.2.19 hard rerouting: In hard rerouting, the original connection segment is released prior to the creation of an alternative connection segment. This is known as break-before-make. See ITU-T Rec. G.8080/Y.1304.

3.2.20 hard rerouting service: A hard rerouting service offers a failure recovery mechanism for calls and is always in response to a failure event. See ITU-T Rec. G.8080/Y.1304.

3.2.21 IP routing interworking function: An IP routing interworking function allows IP topology or routes to be passed from one IP routing protocol to a different incompatible IP routing protocol. For example, an IP routing interworking function may form a gateway between an Integrated IS-IS routed DCN and an OSPF routed DCN.

3.2.22 local CP-ID: A CP-ID that has local significance to the discovery agent transmitting the discovery messages.

3.2.23 local TCP-ID: A TCP-ID that has local significance to the discovery agent transmitting the discovery messages.

3.2.24 management plane: The management plane performs management functions for the transport plane, the control plane and the system as a whole. It also provides coordination between all the planes. The following management functional areas identified in ITU-T Rec. M.3010 are performed in the management plane: performance management; fault management; configuration management; accounting management; security management.

3.2.25 multi-homing: Multiple links between an end-point and one or more transport networks. Multi-homing may be used, for example, for load balancing or protection via diverse routes.

3.2.26 name: A name, or identifier, is a location independent string with respect to both a source and a destination. If a string is the name of a destination, it remains unchanged if the destination moves. It is valid regardless of the source attempting communication with the destination.

3.2.27 network-layer interworking function: A network-layer interworking function provides interoperability between nodes that support incompatible network-layer protocols. An example of a network-layer interworking function is static GRE tunnels, or an AE-DCF.

3.2.28 Permanent Connection (PC): A PC is a connection type that is provisioned by the management system.

3.2.29 policy: The set of rules applied to interfaces at the system boundary, which filter messages into an allowed set. Policy is implemented by "Port Controller" components.

3.2.30 port controller: A class of component that implements the set of rules applied to a system.

3.2.31 proxy call: The calling/called party call controller interacts with the network call controller by means of a call protocol, but is not coincident with the user. See ITU-T Rec. G.8080/Y.1304.

3.2.32 Protocol Controller (PC): A component, which provides the function of mapping the parameters of the abstract interfaces of the control components into messages that are carried by a protocol to support interconnection via an interface. Protocol Controllers are a sub-class of policy ports, and provide all the functions associated with those components. See ITU-T Rec. G.8080/Y.1304.

3.2.33 route: a sequence of transport resource identifiers that are used by the control plane to create a network connection. These may include addresses that are routable for SNPs, SNPPs, and RAs. Names for SNPs, SNPPs, and RAs may also be used in a route but require resolution to an address or proper context in order to be routable.

3.2.34 routing: The control plane function used to select paths for the establishment of connections through one or more operator networks. See ITU-T Rec. G.807/Y.1302.

3.2.34.1 hierarchical routing: One of the three basic forms of algorithm for dynamic path control. This uses the decomposition of a layer network into a hierarchy of subnetworks. Connection controllers are related to one another in a hierarchical manner. Each subnetwork has its own dynamic connection control that has knowledge of the topology of its subnetwork but has no

knowledge of the topology of subnetworks above or below itself in the hierarchy (or other subnetworks at the same level in the hierarchy). See ITU-T Rec. G.8080/Y.1304.

3.2.34.2 source routing: One of the three basic forms of algorithm for dynamic path control. Its connection control process is implemented by a federation of distributed connection and routing controllers and connection controllers operate on routing areas. The signal flow for source (and step-by-step) routing is illustrated in Figure 27/G.8080/Y.1304. In order to reduce the amount of network topology each controller needs to have available, only that portion of the topology that applies to its own routing area is made available. See ITU-T Rec. G.8080/Y.1304.

3.2.34.3 step-by-step routing: One of the three basic forms of algorithm for dynamic path control. In this form of routing there is further reduction of routing information in the nodes, and this places restrictions upon the way in which routing is determined across the subnetwork. A similar process of obtaining one link at a time as that of source routing is followed when connecting across the second routing Area. See ITU-T Rec. G.8080/Y.1304.

3.2.35 Routing Adjacency (RAdj): A logical association between two routing controllers.

3.2.36 routing area: A routing area is defined by a set of subnetworks, the SNPP links that interconnect them, and the SNPPs representing the ends of the SNPP links exiting that routing area. A routing area may contain smaller routing areas interconnected by SNPP links.

3.2.37 Routing Controller (RC): A component with the roles to:

– respond to requests from connection controllers for path (route) information needed to set up connections. This information can vary from end-to-end (e.g., source routing) to next hop;

– respond to requests for topology (SNPs and their abstractions) information for network management purposes. See ITU-T Rec. G.8080/Y.1304.

3.2.38 Routing Control Domain (RCD): An abstract entity that hides the details of the RC distribution.

3.2.39 Routing Information Database (RDB): A repository for the local topology, network topology, reachability, and other routing information that is updated as part of the routing information exchange and may additionally contain information that is configured.

3.2.40 routing level: A routing level is a relationship between an RA and a containing RA or contained RAs. The containment hierarchy of routing areas creates routing levels.

3.2.41 Routing Performer (RP): A computational viewpoint object that is associated with a routing area and provides an abstraction of the routing service for the routing area.

3.2.42 service level agreement: A service level agreement is a contract between two parties such as a service provider and a customer. It defines the services available to the customer, and the grade of service of those services as offered to the customer. It also usually describes the service guarantee and potential penalties in case of service degradation or failure. See ITU-T Rec. G.807/Y.1302.

3.2.43 Shared Risk Group (SRG): A group of resources that share a common risk component whose failure can cause the failure of all the resources in the group.

3.2.44 SNPP Alias: An SNPP alias is an alternate SNPP name for the same SNPP link that is generated from another SNPP name space. If present in a routing area, it is available to the RC that is associated with RA.

3.2.45 Soft Permanent Connection (SPC): An SPC is a user-to-user connection whereby the user-to-network portion of the end-to-end connection is established by the network management system as a PC. The network portion of the end-to-end connection is established as a switched connection using the control plane. In the network portion of the connection, requests for

establishment of the connection are initiated by the management plane and set-up by the control plane.

3.2.46 soft rerouting service: Soft rerouting service is a mechanism for the rerouting of a call for administrative purposes (e.g., path optimization, network maintenance, and planned engineering works). When a rerouting operation is triggered (generally via a request from the management plane) and sent to the location of the rerouting components, the rerouting components establish a rerouting connection to the location of the rendez-vous components. Once the rerouting connection is created, the rerouting components use the rerouting connection and delete the initial connection. This is known as make before-break. See ITU-T Rec. G.8080/Y.1304.

3.2.47 SNP identifier: An SNP identifier is used for link connection assignment and, in some cases, routing. The SNP identifier is derived from the SNPP identifier concatenated with a locally significant SNP index. When the identifier is routable, it is an SNPP address. When it is not routable, the identifier is an SNP name.

3.2.48 SNPP identifier: An instance of an identifier for an SNPP. When the identifier is routable, it is an SNPP address. When it is not routable, the identifier is an SNPP name. The constituents of an SNPP identifier may include RA IDs, a subnetwork id, and resource context identifiers.

3.2.49 Subnetwork Point (SNP): The SNP is an abstraction that represents an actual or potential underlying CP (or CTP) or an actual or potential TCP (or TTP). Several SNPs (in different subnetwork partitions) may represent the same TCP or CP.

3.2.50 Subnetwork Point Pool (SNPP): A set of subnetwork points that are grouped together for the purposes of routing. An SNP pool has a strong relationship to Link Ends (See ITU-T Rec. G.852.2).

3.2.51 Subnetwork Point Pool link (SNPP link): An association between SNPPs on different subnetworks.

3.2.52 supplementary services: Within a transport network, supplementary services are considered to be the set of services that are provided to end users over and above connection management.

3.2.53 Switched Connection (SC): An SC is any connection that is established, as a result of a request from the end user, between connection end-points using a signalling/control plane and involves the dynamic exchange of signalling information between signalling elements within the control plane(s).

3.2.54 Termination and Adaptation Performer (TAP): The TAP is physically located on the equipment providing the adaptation and termination function. It provides a control plane view of the link connection, and hides any hardware and technology-specific details of the adaptation and termination control.

3.2.55 third party signalling: A party that acts on behalf of a user and exchanges information between the user and the control plane for the purpose of connection supervision.

3.2.56 transport plane: The transport plane provides bidirectional or unidirectional transfer of user information, from one location to another. It can also provide transfer of some control and network management information. The transport plane is layered; it is equivalent to the "Transport Network" defined in ITU-T Rec. G.805.

3.2.57 UNI transport resource name: The UNI SNPP Link requires a name for the calling party call controller and network call controller to specify destinations. These names must be globally unique and are assigned by the ASON network. Multiple names may be assigned to the SNPP link. This enables a calling/called party to associate different applications with specific addresses over a common link.

3.2.58 Virtual Private Network (VPN): A set of virtually dedicated transport resources, supporting a closed user group, over transport links that are shared between multiple users.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

AD	Administrative Domain
AE-DCF	Automatic Encapsulating Data Communication Function
AESA	ATM End System Address
AG	Access Group
AGC	Access Group Container
ASON	Automatically Switched Optical Network
ASTN	Automatic Switched Transport Network
CAC	Call Admission Control
CallC	Call Controller
CC	Connection Controller
CCC	Calling/Called Party Call Controller
CCI	Connection Controller Interface
DA	Discovery Agent
E-NNI	External Network-Network Interface
GoS	Grade of Service
ID	Identifier
I-NNI	Internal Network-Network Interface
LRM	Link Resource Manager
LSP	Label Switched Path
LSPDU	Link State Protocol Data Unit
NC	Network Connection
NCC	Network Call Controller
NCCI	Network Call Correlation Identifier
NNI	Network-to-Network Interface
NNI	Network Node Interface
PC	Permanent Connection
PC	Protocol Controller
PNNI	Private Network-Network Interface
RA	Routing Area
RAdj	Routing Adjacency
RC	Routing Controller
RCD	Routing Control Domain

RDB	Routing Information Database
RI	Routing Information
RP	Routing Performer
SC	Switched Connection
SLA	Service Level Agreement
SNCr	SubNetwork Controller
SNP	Subnetwork Point
SNPP	Subnetwork Point Pool
SPC	Soft Permanent Connection
SRG	Shared Risk Group
TAP	Termination and Adaptation Performer
TLV	Type, Length, Value
UNI	User Network Interface
VPN	Virtual Private Network

Appendix I

List of Source Recommendations

The abbreviations and terms were taken from the Recommendations listed below. Where the definitions were not a part of an explicit Definitions clause in the source Recommendation, the source Recommendation is referenced in a Note following the definition. After this Recommendation is finally approved, Corrigenda or revisions to the original sources of these terms will be proposed to replace the definitions in those Recommendations by references to this Recommendation (except where the definition is part of the source Recommendation text and not in a definitions clause). The end result should be a single normative definition for each term in this subject area, contained in this Recommendation.

ITU-T Recommendation	Latest version
G.7713/Y.1704	12/01
G.7713.1/Y.1704.1	03/03
G.7713.2/Y.1704.2	03/03
G.7713.3/Y.1704.3	03/03
G.7714/Y.1705	11/01
G.7714.1/Y.1705.1	04/03
G.7715/Y.1706	06/02
G.7715.1/Y.1706.1	02/04
G.807/Y.1302	07/01
G.8080/Y.1304	11/01
G.8080/Y.1304 Amd.1	03/03
G.7713/Y.1704 Amd.1	06/04

Appendix II

Related definitions found in documents from other organizations

NOTE – In the table below, a term followed by a number in ( ) indicates that the term has multiple definitions.

No.	Terms	Definition	Source document
1	abstract node	A group of nodes whose internal topology is opaque to the ingress node of the LSP. An abstract node is said to be simple if it contains only one physical node.	RFC 3209
2	address	An IPv6-layer identifier for an interface or a set of interfaces.	RFC 2460
3	address prefix	A string of 0 or more bits up to a maximum of 152 bits that is the lead portion of one or more ATM addresses.	af-pnni-0055.002
4	adjacency (1)	A relationship formed between selected neighbouring routers for the purpose of exchanging routing information. Not every pair of neighbouring routers become adjacent.	RFC 2328
5	adjacency (2)	The relationship between two communicating neighbouring peer nodes.	af-pnni-0055.002
6	admission control	A traffic control function that decides whether the packet scheduler in the node can supply the requested QoS while continuing to provide the QoS requested by previously-admitted requests. See also "policy control" and "traffic control".	RFC 2205
7	Adspec	An Adspec is a data element (object) in a Path message that carries a package of OPWA advertising information. See "OPWA".	RFC 2205
8	aggregation token	A number assigned to an outside link by the border nodes at the ends of the outside link. The same number is associated with all uplinks and induced uplinks associated with the outside link. In the parent and all higher-level peer group, all uplinks with the same aggregation token are aggregated.	af-pnni-0055.002
9	alternate routing	A mechanism that supports the use of a new path after an attempt to set up a connection along a previously selected path fails.	af-pnni-0055.002
10	ancestor node	A logical group node that has a direct parent relationship to a given node (i.e., it is the parent of that node, or the parent's parent, ...).	af-pnni-0055.002
11	ARPANET leader	The control information on an ARPANET message at the host-IMP interface.	RFC 791
12	ARPANET message	The unit of transmission between a host and an IMP in the ARPANET. The maximum size is about 1012 octets (8096 bits).	RFC 791

No.	Terms	Definition	Source document
13	ATM anycast capability	The ability to allow an application to request a point-to-point connection to a single ATM end system that is part of an ATM group.	af-pnni-0055.002
14	ATM service provider network	Any ATM network that provides transit services for users or other ATM networks belonging to different administrative entities.	af-pnni-0055.002
15	Autonomous System (AS) (1)	A group of routers exchanging routing information via a common routing protocol. Abbreviated as AS.	RFC 2328
16	Autonomous System (AS) (2)	An Autonomous System (AS) is a connected segment of a network topology that consists of a collection of subnetworks (with hosts attached) interconnected by a set of routes. The subnetworks and the routers are expected to be under the control of a single operations and maintenance (O&M) organization.Within an AS, routers may use one or more interior routing protocols, and sometimes several sets of metrics. An AS is expected to present to other ASs an appearance of a coherent interior routing plan, and a consistent picture of the destinations reachable through the AS. An AS is identified by an autonomous system number.	RFC 1812
17	auto-refresh loop	An auto-refresh loop is an error condition that occurs when a topological loop of routers continues to refresh as existing reservation state even though all receivers have stopped requesting these reservations. See 3.4 for more information.	RFC 2205
18	availability of a rerouting service	A rerouting service is available at a node if the node supports the service (i.e., is capable of providing the service) and the network policy allows the service to be requested. A rerouting service is available within a rerouting domain if the service is available for a call at both the source node and the destination node of this rerouting domain.	af-cs-0173.000
19	blockade state	Blockade state helps to solve a "killer reservation" problem. See 2.5 and 3.5, and "killer reservation".	RFC 2205
20	border node	A logical node that is in a specified peer group, and has at least one link that crosses the peer group boundary.	af-pnni-0055.002
21	branch policing	Traffic policing at a multicast branching point on an outgoing interface that has "less" resources reserved than another outgoing interface for the same flow. See "traffic policing".	RFC 2205

No.	Terms	Definition	Source document
22	broadcast networks	Networks supporting many (more than two) attached routers, together with the capability to address a single physical message to all of the attached routers (broadcast). Neighbouring routers are discovered dynamically on these nets using OSPF's Hello Protocol. The Hello Protocol itself takes advantage of the broadcast capability. The OSPF protocol makes further use of multicast capabilities, if they exist. Each pair of routers on a broadcast network is assumed to be able to communicate directly. An Ethernet is an example of a broadcast network.	RFC 2328
23	bypass	A bypass represents the connectivity between two ports in the complex node representation. A bypass is always an exception.	af-pnni-0055.002
24	check-pointable FT label	An FT label which is secured by using the check-pointing techniques.	RFC 3479
25	check-pointing	A process of message exchanges that confirm receipt and processing (or secure storage) of specific protocol messages.	RFC 3479
26	child node	A node at the next lower level of the hierarchy which is contained in the peer group represented by the logical group node currently referenced. This could be a logical group node, or a physical node.	af-pnni-0055.002
27	child peer group	A child peer group of a peer group is any one containing a child node of a logical group node in that peer group. A child peer group of a logical group node is the one containing the child node of that logical group node.	af-pnni-0055.002
28	class-name	The class of an object. See "object".	RFC 2205
29	client-layer	A layer acting as a client with regard to transport services provided by a server layer (in this case, the transport network). Example of a client layer is IP.	OIF-UNI-01.0
30	client-layer address	An address used in client-layer protocols. Example is IP addressing in IP clients connected to the transport network.	OIF-UNI-01.0
31	common peer group	The lowest level peer group in which a set of nodes is represented. A node is represented in a peer group either directly or through one of its ancestors.	af-pnni-0055.002
32	complex node representation	A collection of nodal state parameters that provide detailed state information associated with a logical node.	af-pnni-0055.002
33	connected (sub)network	A connected (sub)network is an IP subnetwork to which a router is interfaced, or a connected network if the connected network is not subnetted. See also "connected network".	RFC 1812
34	connected network	A network prefix to which a router is interfaced is often known as a local network, or the subnetwork of that router. However, these terms can cause confusion and, therefore, we use the term connected network in this memo.	RFC 1812

No.	Terms	Definition	Source document
35	connection	A circuit connecting an ingress TNE port and an egress TNE port across the transport network for transporting user signals. The connection may be unidirectional or bidirectional. (This is referred to as "network connection" in ITU terminology, see Appendix I.)	OIF-UNI-01.0
36	connection scope	The level of routing hierarchy within which a given connection request to a group address is constrained.	af-pnni-0055.002
37	connection segment	A portion of a connection or an entire connection. In this document a connection segment spans an entire rerouting domain.	af-cs-0173.000
38	connection trace	A control plane mechanism that determines the logical nodes and logical links traversed by existing connections and parties that have already been established, and supporting mechanisms that provide this information to network management systems.	af-cs-0141.000
39	crankback	A mechanism for partially releasing a connection setup in progress which has encountered a failure. This mechanism allows PNNI to perform alternate routing.	af-pnni-0055.002
40	C-type	The class type of an object; unique within class-name. See "class-name".	RFC 2205
41	datagram (1)	The unit of transmission in the network layer (such as IP). A datagram may be encapsulated in one or more packets passed to the data link layer.	RFC 1661
42	datagram (2)	The unit transmitted between a pair of Internet modules. Data, called datagrams, from sources to destinations. The Internet Protocol does not provide a reliable communication facility. There are no acknowledgments either end-to-end or hop-by-hop. There is no error nor retransmissions. There is no flow control. See IP.	RFC 1812
43	default node representation	A single value for each nodal state parameter giving the presumed value between any entry or exit to the logical node and the nucleus.	af-pnni-0055.002
44	default route	A routing table entry that is used to direct any data addressed to any network prefixes not explicitly listed in the routing table.	RFC 1812
45	dense mode	In multicast forwarding, two paradigms are possible: in dense mode forwarding, a network multicast is forwarded as a data link layer multicast to all interfaces except that on which it was received, unless and until the router is instructed not to by a multicast routing neighbour. See "Sparse Mode".	RFC 1812

No.	Terms	Definition	Source document
46	designated router	Each broadcast and NBMA network that has at least two attached routers has a designated router. The designated router generates an LSA for the network and has other special responsibilities in the running of the protocol. The designated router is elected by the Hello Protocol. The designated router concept enables a reduction in the number of adjacencies required on a broadcast or NBMA network. This in turn reduces the amount of routing protocol traffic and the size of the link-state database.	RFC 2328
47	designated transit list	A list of node and optionally link Ids that completely specify a path across a single PNNI peer group.	af-pnni-0055.002
48	DestAddress	The IP destination address; part of session identification. See "session".	RFC 2205
49	destination	The destination address, an Internet header field.	RFC 791
50	destination node	The last node in a particular rerouting domain to process the original SETUP message for a particular point-to-point call/connection.	af-cs-0173.000
51	Don't Fragment (DF)	The Don't Fragment bit carried in the flags field.	RFC 791
52	Dijkstra's algorithm	An algorithm that is sometimes used to calculate routes given a link and nodal state topology database.	af-pnni-0055.002
53	distinct style	A (reservation) style attribute; separate resources are reserved for each different sender. See also "shared style".	RFC 2205
54	domain	Synonymous with PNNI routing domain.	af-pnni-0055.002
55	domain-based rerouting	A rerouting mechanism that replaces a connection segment within a rerouting domain between the source node and the destination node of a connection. With the domain-based rerouting feature, connections are not rerouted across an inter-domain interface.	af-cs-0173.000
56	downstream	Towards the data receiver(s).	RFC 2205
57	DstPort	The IP (generalized) destination port used as part of a session. See "generalized destination port".	RFC 2205
58	Designated Transport List (DTL) originator	The first lowest-level node within the entire PNNI routing domain to build the initial DTL stack for a given connection.	af-pnni-0055.002
59	Designated Transport List (DTL) terminator	The last lowest-level node within the entire PNNI routing domain to process the connection (and thus the connection's DTL).	af-pnni-0055.002
60	edge node	The source node or the destination node of a call in a particular rerouting domain.	af-cs-0173.000
61	Exterior Gateway Protocol (EGP)	A protocol that distributes routing information to the gateways (routers) which connect autonomous systems. See IGP.	RFC 1812
62	Exterior Gateway Protocol version 2 (EGP-2)	This is an EGP routing protocol developed to handle traffic between autonomous systems in the Internet.	RFC 1812

No.	Terms	Definition	Source document
63	Element Management System (EMS)	A terminal, network element, or system that provides specific services to manage specific network elements.	Security Mgmt-IA
64	end system	A system on which connection termination points are located.	af-pnni-0055.002
65	entry border node	The node which receives a call over an outside link. This is the first node within a peer group to see this call.	af-pnni-0055.002
66	entry policing	Traffic policing done at the first RSVP- (and policing-) capable router on a data path.	RFC 2205
67	Error_Spec	Object that carries the error report in a PathErr or ResvErr message.	RFC 2205
68	exception	A connectivity advertisement in a PNNI complex node representation that represents something other than the default node representation.	af-pnni-0055.002
69	exit border node	The node that will progress a call over an outside link. This is the last node within a peer group to see this call.	af-pnni-0055.002
70	explicit sender selection	A (reservation) style attribute; all reserved senders are to be listed explicitly in the reservation message. See also "wildcard sender selection".	RFC 2205
71	explicitly routed LSP	An LSP whose path is established by a means other than normal IP routing.	RFC 3209
72	exterior	Denotes that an item (e.g., link, node, or reachable address) is outside of a PNNI routing domain.	af-pnni-0055.002
73	exterior link	A link which crosses the boundary of the PNNI routing domain. The PNNI protocol does not run over an exterior link.	af-pnni-0055.002
74	exterior reachable address	An address that can be reached through a PNNI routing domain, but which is not located in that PNNI routing domain	af-pnni-0055.002
75	exterior route	A route which traverses an exterior link.	af-pnni-0055.002
76	Fixed Filter (FF) style	Fixed filter reservation style, which has explicit sender selection and distinct attributes.	RFC 2205
77	FilterSpec	Together with the session information, defines the set of data packets to receive the QoS specified in a flowspec. The filterspec is used to set parameters in the packet classifier function. A filterspec may be carried in a FILTER_SPEC or SENDER_TEMPLATE object.	RFC 2205
78	flags	An Internet header field carrying various control flags.	RFC 791
79	flooding	The part of the OSPF protocol that distributes and synchronizes the link-state database between OSPF routers.	RFC 2328
80	flow descriptor	The combination of a flowspec and a filterspec.	RFC 2205

No.	Terms	Definition	Source document
81	Flowspec	Defines the QoS to be provided for a flow. The flowspec is used to set parameters in the packet scheduling function to provide the requested quality of service. A flowspec is carried in a FLOWSPEC object. The flowspec format is opaque to RSVP and is defined by the Integrated Services Working Group.	RFC 2205
82	foreign address	An address or address prefix that does not match any of a given node's summary addresses.	af-pnni-0055.002
83	forwarder	The logical entity within a router that is responsible for switching packets among the router's interfaces. The Forwarder also makes the decisions to queue a packet for local delivery, to queue a packet for transmission out on another interface, or both.	RFC 1812
84	forwarding	Forwarding is the process a router goes through for each packet received by the router. The packet may be consumed by the router, it may be output on one or more interfaces of the router, or both. Forwarding includes the process of deciding what to do with the packet as well as queuing it up for (possible) output or internal consumption.	RFC 1812
85	Forwarding Information Base (FIB)	The table containing the information necessary to forward IP Datagrams, in this document, is called the Forwarding Information Base. At minimum, this contains the interface identifier and next hop information for each reachable destination network prefix.	RFC 1812
86	fragment	An IP datagram that represents a portion of a higher layer's packet that was too large to be sent in its entirety over the output network.	RFC 1812
87	fragment offset	This Internet header field indicates where in the Internet datagram a fragment belongs.	RFC 791
88	frame	The unit of transmission at the data link layer. A frame may include a header and/or a trailer, along with some number of units of data.	RFC 1661
89	FT label	A label for which some fault tolerant operation is used.	RFC 3479
90	general purpose serial interface	A physical medium capable of connecting exactly two systems and, therefore, configurable as a point-to-point line, but also configurable to support link layer networking using protocols such as X.25 or Frame Relay. A link layer network connects another system to a switch, and a higher communication layer multiplexes virtual circuits on the connection. See "point-to-point line".	RFC 1812
91	generalized destination port	The component of a session definition that provides further transport or application protocol layer demultiplexing beyond DestAddress. See "session".	RFC 2205
92	generalized source port	The component of a filterspec that provides further transport or application protocol layer demultiplexing beyond the sender address.	RFC 2205

No.	Terms	Definition	Source document
93	Gateway-to-Gateway Protocol (GGP)	The protocol used primarily between gateways to control routing and other gateway functions.	RFC 791
94	GLB	Greatest Lower Bound	RFC 2205
95	hard rerouting	A rerouting operation where the original connection segment is released before the establishment of an alternative connection segment (i.e., break-before-make).	af-cs-0173.000
96	header	Control information at the beginning of a message, segment, datagram, packet or block of data.	RFC 791
97	Hello Packet	A type of PNNI routing packet that is exchanged between neighbouring logical nodes.	af-pnni-0055.002
98	Hello Protocol	The part of the OSPF protocol used to establish and maintain neighbour relationships. On broadcast networks the Hello Protocol can also dynamically discover neighbouring routers.	RFC 2328
99	hierarchically complete source route	A stack of DTLs representing a route across a PNNI routing domain such that a DTL is included for each hierarchical level between and including the current level and the lowest visible level in which the source and destination are reachable.	af-pnni-0055.002
100	hop-by-hop route	A route that is created by having each switch along the path use its own routing knowledge to determine the next hop of the route, with the expectation that all switches will choose consistent hops such that the call will reach the desired destination. PNNI does not use hop-by-hop routing.	af-pnni-0055.002
101	horizontal link	A link between two logical nodes that belong to the same peer group.	af-pnni-0055.002
102	host	Any node that is not a router.	RFC 2460
103	ICMP	Internet Control Message Protocol, implemented in the Internet module, the ICMP is used from gateways to hosts and between hosts to report errors and make routing suggestions.	RFC 791
104	identification	An Internet header field carrying the identifying value assigned by the sender to aid in assembling the fragments of a datagram.	RFC 791
105	incarnation number	Identify the instance of a rerouting connection.	af-cs-0173.000
106	incoming interface	The interface on which data packets are expected to arrive, and on which Resv messages are sent.	RFC 2205
107	incumbent connection	An incumbent connection refers to an active connection segment that is in the process of being replaced by an alternate connection segment.	af-cs-0173.000
108	induced uplink	An uplink "A" that is created due to the existence of an uplink "B" in the child peer group represented by the node that created uplink "A". Both "A" and "B" group in which uplink "A" is seen.	af-pnni-0055.002

No.	Terms	Definition	Source document
109	in-fibre signalling	In-fibre signalling refers to the transport of signalling traffic over a communication channel embedded in the data-bearing physical link.	OIF-UNI-01.0
110	initial connection	The first incumbent connection (no rerouting operation has ever occurred).	af-cs-0173.000
111	inside link	Synonymous with horizontal link.	af-pnni-0055.002
112	instance ID	A subset of an object's attributes which serve to uniquely identify a MIB instance.	af-pnni-0055.002
113	integrity	Object of an RSVP control message that contains cryptographic data to authenticate the originating node and to verify the contents of an RSVP message.	RFC 2205
114	inter-domain interface	An interface at the ingress or egress of a rerouting domain.	af-cs-0173.000
115	inter-domain PNNI interface	A PNNI interface at the ingress or egress of a rerouting domain.	af-cs-0173.000
116	inter-domain rerouting service	A rerouting service for a call across multiple rerouting domains.	af-cs-0173.000
117	interface (1)	A node's attachment to a link.	RFC 2460
118	interface (2)	The connection between a router and one of its attached networks. An interface has state information associated with it, which is obtained from the underlying lower level protocols and the routing protocol itself. An interface to a network has associated with it a single IP address and mask (unless the network is an unnumbered point-to-point network). An interface is sometimes also referred to as a link.	RFC 2328
119	interface IP address	The IP address and network prefix length that is assigned to a specific interface of a router.	RFC 1812
120	Interface Message Processor (IMP)	The packet switch of the ARPANET.	RFC 791
121	interior	Denotes that an item (e.g., link, node, or reachable address) is inside of a PNNI routing domain.	af-pnni-0055.002
122	Interior Gateway Protocol (IGP) (1)	The routing protocol spoken by the routers belonging to an autonomous system. Each autonomous system has a single IGP. Separate autonomous systems may be running different IGPs.	RFC 2328
123	Interior Gateway Protocol (IGP) (2)	A protocol that distributes routing information with an Autonomous System (AS). See "EGP".	RFC 1812
124	internal reachable ad	An address of a destination that is directly attached to the logical node advertising the address.	af-pnni-0055.002
125	Internet address (1)	A four octet (32 bits) source or destination address consisting of a network field and a local address field.	RFC 791
126	Internet address (2)	An assigned number that identifies a host in an Internet. It has two parts: an IP address and a prefix length. The prefix length indicates how many of the most specific bits of the address constitute the network prefix.	RFC 1812

No.	Terms	Definition	Source document
127	Internet datagram	The unit of data exchanged between a pair of Internet modules (includes the Internet header).	RFC 791
128	Internet fragment	A portion of the data of an Internet datagram with an Internet header.	RFC 791
129	Internet Header Lengh (IHL)	The Internet header field Internet Header Length is the length of the Internet header measured in 32-bit words.	RFC 791
130	intra-domain interface	An interface within a rerouting domain.	af-cs-0173.000
131	intra-domain rerouting service	A rerouting service for a call within a rerouting domain.	af-cs-0173.000
132	Internet Protocol (IP)	The network layer protocol for the Internet. It is a packet switching, datagram protocol defined in RFC 791. IP does not provide a reliable communications facility; that is, there are no end-to-end of hop-by-hop acknowledgments.	RFC 1812
133	IP control channel	The communication channel over which IP packets are transported between two devices. Implementation Agreement OIF-UNI-01.0 UNI 1.0 Signalling Specification 12.	OIF-UNI-01.0
134	IP datagram	An IP datagram is the unit of end-to-end transmission in the Internet Protocol. An IP datagram consists of an IP header followed by all of higher-layer data (such as TCP, UDP, ICMP, and the like). An IP datagram is an IP header followed by a message. An IP datagram is a complete IP end-to-end transmission unit. An IP datagram is composed of one or more IP fragments. In this memo, the unqualified term datagram should be understood to refer to an IP datagram.	RFC 1812
135	IP fragment	An IP fragment is a component of an IP datagram. An IP fragment consists of an IP header followed by all or part of the higher-layer of the original IP datagram. One or more IP fragments comprises a single IP datagram. In this memo, the unqualified term fragment should be understood to refer to an IP fragment.	RFC 1812
136	IP packet	An IP datagram or an IP fragment. In this memo, the unqualified term packet should generally be understood to refer to an IP packet.	RFC 1812
137	killer reservation problem	The killer reservation problem describes a case where a receiver attempting and failing to make a large QoS reservation prevents smaller QoS reservations from being established. See 2.5 and 3.5 for more information.	RFC 2205
138	Label Distribution Protocol (LDP)	A new protocol defined for distributing labels. It is the set of procedures and messages by which Label Switched Routers (LSRs) establish Label Switched Paths (LSPs) through a network by mapping network-layer routing information directly to data-link layer switched paths.	RFC 3036

No.	Terms	Definition	Source document
139	Label Switched Path (LSP)	The path created by the concatenation of one or more label switched hops, allowing a packet to be forwarded by swapping labels from an MPLS node to another MPLS node.	RFC 3209
140	LDP FT enhancements	The extensions to LDP.	RFC 3479
141	leadership priority	The priority with which a logical node wishes to be elected peer group leader of its peer group. Generally, of all nodes in a peer group, the one with the highest leadership priority will be elected as peer group leader.	af-pnni-0055.002
142	level	Level is the position in the PNNI hierarchy at which a particular node or peer group exists. A level that has a smaller numerical value implies greater topology aggregation, and is hence called a 'higher level' in the PNNI hierarchy throughout this document. Conversely, a level that has a larger numerical value implies less topology aggregation, and is hence called a 'lower level' in the PNNI hierarchy throughout this document.	af-pnni-0055.002
143	Logical Interface Handle (LIH)	The LIH is used to help deal with non-RSVP clouds. See 2.9 for more information.	RFC 2205
144	link (1)	A communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6. Examples are Ethernets (simple or bridged); PPP links; X.25, Frame Relay, or ATM networks; and Internet (or higher) layer "tunnels", such as tunnels over IPv4 or IPv6 itself.	RFC 2460
145	link (2)	Synonymous with logical link.	af-pnni-0055.002
146	link (3)	Aggregation token. See "aggregation token".	af-pnni-0055.002
147	link (4)	Attribute A link state parameter that is considered individually to determine whether a given link is acceptable and/or desirable for carrying a given connection.	af-pnni-0055.002
148	link constraint	A restriction on the use of links for path selection for a specific connection.	af-pnni-0055.002
149	link metric	A link parameter that requires the values of the parameter for all links along a given path to be combined to determine whether the path is acceptable and/or desirable for carrying a given connection.	af-pnni-0055.002
150	link MTU	The maximum transmission unit, i.e., maximum packet size in octets, that can be conveyed over a link.	RFC 2460
151	Link State Advertisement (LSA)	Unit of data describing the local state of a router or network. For a router, this includes the state of the router's interfaces and adjacencies. Each link state advertisement is flooded throughout the routing domain. The collected link state advertisements of all routers and networks forms the protocol's link state database. Throughout this memo, link state advertisement is abbreviated as LSA.	RFC 2328

No.	Terms	Definition	Source document
152	link state parameter	Information that captures an aspect or property of a link.	af-pnni-0055.002
153	local address	The address of a host within a network. The actual mapping of an Internet local address on to the host addresses in a network is quite general, allowing for many to one mappings.	RFC 791
154	local repair	Local repair allows RSVP to rapidly adapt its reservations to changes in routing.	RFC 2205
155	logical [network] interface	A logical path, distinguished by a unique IP address, to a connected network.	RFC 1812
156	logical group node	An abstract representation of a lower level peer group as a single point.	af-pnni-0055.002
157	logical link	An abstract representation of the connectivity between two logical nodes.	af-pnni-0055.002
158	logical node	A lowest-level node or a logical group node.	af-pnni-0055.002
159	logical node ID	A string of bits that unambiguously identifies a logical node within a routing domain.	af-pnni-0055.002
160	lower-level protocols	The underlying network access protocols that provide services to the Internet Protocol and in turn the OSPF protocol. Examples of these are the X.25 packet and frame levels for X.25 PDNs, and the ethernet data link layer for ethernets.	RFC 2328
161	lowest-level node	A leaf in the PNNI routing hierarchy; an abstraction representing a single instance of the PNNI routing protocol. Lowest-level nodes are created in a switching system via configuration. They are not created dynamically.	af-pnni-0055.002
162	Local Policy Module (LPM)	The function that exerts policy control.	RFC 2205
163	LSP	A Label Switched Path.	RFC 3209
164	LSP tunnel	An LSP which is used to tunnel below normal IP routing and/or filtering mechanisms.	RFC 3209
165	LUB	Least Upper Bound.	RFC 2205
166	management system	A generic term for an EMS or NMS.	Security Mgmt-IA
167	martian filtering	A packet that contains an invalid source or destination address is considered to be martian and discarded.	RFC 1812
168	membership scope	The level of routing hierarchy within which advertisement of a given address is constrained.	af-pnni-0055.002
169	merge policing	Traffic policing that takes place at data merge point of a shared reservation.	RFC 2205
170	merging	The process of taking the maximum (or more generally the least upper bound) of the reservations arriving on outgoing interfaces, and forwarding this maximum on the incoming interface. See 2.2 for more information.	RFC 2205
171	More Fragments (MF)	The more-fragments flag carried in the Internet header flags field.	RFC 791

No.	Terms	Definition	Source document
172	MIB attribute	A single piece of configuration, management, or statistical information which pertains to a specific part of the PNNI protocol operation.	af-pnni-0055.002
173	MIB instance	An incarnation of an MIB object that applies to a specific part, piece, or aspect of the PNNI protocol's operation.	af-pnni-0055.002
174	MIB object	A collection of attributes that can be used to configure, manage, or analyse an aspect of the PNNI protocol's operation.	af-pnni-0055.002
175	module	An implementation, usually in software, of a protocol or other procedure.	RFC 791
176	more-fragments flag	A flag indicating whether or not this Internet datagram contains the end of an Internet datagram, carried in the internet header flags field.	RFC 791
177	Maximum Transmission Unit (MTU)	The size of the largest packet that can be transmitted or received through a logical interface. This size includes the IP header but does not include the size of any link layer headers or framing.	RFC 1812
178	multicast	A packet that is destined for multiple hosts. See "broadcast".	RFC 1812
179	multicast address	A special type of address that is recognizable by multiple hosts. A multicast address is sometimes known as a functional address or a group address.	RFC 1812
180	native address	An address or address prefix that matches one of a given node's summary addresses.	af-pnni-0055.002
181	neighbour node	A node that is directly connected to a particular node via a logical link.	af-pnni-0055.002
182	neighbouring routers	Two routers that have interfaces to a common network. Neighbour relationships are maintained by, and usually dynamically discovered by, OSPF's Hello Protocol.	RFC 2328
183	neighbours	Nodes attached to the same link.	RFC 2460
184	network	An IP network/subnet/supernet. It is possible for one physical network to be assigned multiple IP network/subnet numbers. These are considered to be separate networks. Point-to-point physical networks are an exception – they are considered a single network no matter how many (if any at all) IP network/subnet numbers are assigned to them.	RFC 2328
185	Network Administrator (NA)	A person who is authorized to use a management system. (Refer to [T1M1] for the many roles that may exist for a NA.) Implementation Agreement: Security for Management Interfaces to Network Elements – SMI-01.0.	Security Mgmt-IA

No.	Terms	Definition	Source document
186	Network Element (NE)	Any device implementing one or more of the OIF's UNI or NNI control protocols. It may also support other interfaces or services. In this IA, a networking component with its own OAM&P interfaces (e.g., a signalling control or transport component), is considered a NE.	Security Mgmt-IA
187	Network Management System (NMS)	A terminal, network element, or system that provides services to manage a network element. It may be an overall management system that manages multiple EMSs and network elements, including non-optical network elements.	Security Mgmt-IA
188	network mask	A 32-bit number indicating the range of IP addresses residing on a single IP network/subnet/supernet. This specification displays network masks as hexadecimal numbers. For example, the network mask for a class C IP network is displayed as 0xffffff00. Such a mask is often displayed elsewhere in the literature as 255.255.255.0.	RFC 2328
189	network prefix	The portion of an IP address that signifies a set of systems. It is selected from the IP address by logically ANDing a subnet mask with the address, or (equivalently) setting the bits of the address not among the most significant bits of the address to zero.	RFC 1812
190	next hop	The next router in the direction of traffic flow.	RFC 2205
191	NFB	The number of fragment blocks in the data portion of an Internet fragment. That is, the length of a portion of data measured in 8 octet units.	RFC 791
192	NHOP	An object that carries the next hop information in RSVP control messages.	RFC 2205
193	nodal attribute	A nodal state parameter that is considered individually to determine whether a given node is acceptable and/or desirable for carrying a given connection.	af-pnni-0055.002
194	nodal constraint	A restriction on the use of nodes for path selection for a specific connection.	af-pnni-0055.002
195	nodal metric	A nodal parameter that requires the values of the parameter for all nodes along a given path to be combined to determine whether the path is acceptable and/or desirable for carrying a given connection.	af-pnni-0055.002
196	nodal state parameter	Information that captures an aspect or property of a node.	af-pnni-0055.002
197	node (1)	A device that implements IPv6.	RFC 2460
198	node (2)	A router or host system.	RFC 2205
199	node (3)	Synonymous with logical node.	af-pnni-0055.002
200	non-branching node	A node that cannot currently support additional branching points for point-to-multipoint calls.	af-pnni-0055.002

No.	Terms	Definition	Source document
201	non-broadcast networks	Networks supporting many (more than two) routers, but having no broadcast capability. Neighbouring routers are maintained on these nets using OSPF's Hello Protocol. However, due to the lack of broadcast capability, some configuration information may be necessary to aid in the discovery of neighbours. On non-broadcast networks, OSPF protocol packets that are normally multicast need to be sent to each neighbouring router, in turn. An X.25 Public Data Network (PDN) is an example of a non-broadcast network.	RFC 2328
202	non-FT label	Not fault tolerant.	RFC 3479
203	non-RSVP clouds	Groups of hosts and routers that do not run RSVP. Dealing with nodes that do not support RSVP is important for backwards compatibility. See 2.9.	RFC 2205
204	nucleus	The interior reference point of a logical node in the PNNI complex node representation.	af-pnni-0055.002
205	null	A value of all zeros.	af-pnni-0055.002
206	object	An element of an RSVP control message; a type, length, value triplet.	RFC 2205
207	octet	An eight bit byte.	RFC 791
208	optical transport network or transport network	An optical transport network is an abstract representation, which is defined by a set of access points (ingress/egress) and a set of network services. The actual implementation is assumed to be composed of a set of transparent or opaque transport network elements such as OEO or all optical Cross-Connects, Add/Drop Multiplexers (ADM), etc., that are interconnected using point-to-point optical links (single channel or wavelength division multiplexed optical line systems). In this document, the term "Transport Network" is used interchangeably with "Optical Transport Network". Furthermore, these terms are used to refer to the service provider transport network and not the user or client transport network.	OIF-UNI-01.0
209	options	The internet header options field may contain several options, and each option may be several octets in length.	RFC 791
210	One Pass With Advertising (OPWA)	Describes a reservation setup model in which (Path) messages sent downstream gather information that the receiver(s) can use to predict the end-to-end service. The information that is gathered is called an advertisement. See also "Adspec".	RFC 2205

No.	Terms	Definition	Source document
211	originate	Packets can be transmitted by a router for one of two reasons: 1) the packet was received and is being forwarded; or 2) the router itself created the packet for transmission (such as route advertisements). Packets that the router creates for transmission are said to originate at the router.	RFC 1812
212	Open Shortest Path First (OSPF)	OSPF runs in one of two modes over non-broadcast networks. The first mode, called non-broadcast multi-access or NBMA, simulates the operation of OSPF on a broadcast network. The second mode, called point-to-multipoint, treats the non-broadcast network as a collection of point-to-point links. Non-broadcast networks are referred to as NBMA networks or point-to-multipoint networks, depending on OSPF's mode of operation over the network.	RFC 2328
213	outgoing interface	Interface through which data packets and path messages are forwarded.	RFC 2205
214	outlier	A node whose exclusion from its containing peer group would significantly improve the accuracy and simplicity of the aggregation of the remainder of the peer group topology.	af-pnni-0055.002
215	out-of-fibre signalling	Out-of-fibre signalling refers to the transport of signalling traffic over a dedicated communication link, separate from the data-bearing link, between the signalling entities.	OIF-UNI-01.0
216	outside link	A link to a lowest-level outside node. In contrast to an inside link (i.e., horizontal link) or an uplink, an outside link does not form part of the PNNI topology and is, therefore, not used in path computation.	af-pnni-0055.002
217	outside node	A node which is participating in PNNI routing, but which is not a member of a particular peer group.	af-pnni-0055.002
218	packet (1)	An IPv6 header plus payload.	RFC 2460
219	packet (2)	The basic unit of encapsulation, which is passed across the interface between the network layer and the data link layer. A packet is usually mapped to a frame; the exceptions are when data link layer fragmentation is being performed, or when multiple packets are incorporated into a single frame.	RFC 1661
220	packet (3)	A packet is the unit of data passed across the interface between the Internet layer and the link layer. It includes an IP header and data. A packet may be a complete IP datagram or a fragment of an IP datagram.	RFC 1812
221	packet classifier	Traffic control function in the primary data packet forwarding path that selects a service class for each packet, in accordance with the reservation state set up by RSVP. The packet classifier may be combined with the routing function. See also "traffic control".	RFC 2205

No.	Terms	Definition	Source document
222	packet scheduler	Traffic control function in the primary data packet forwarding path that implements QoS for each flow, using one of the service models defined by the Integrated Services Working Group. See also " traffic control".	RFC 2205
223	padding	The internet header padding field is used to ensure that the data begins on a 32 bit word boundary. The padding is zero.	RFC 791
224	parent node	The logical group node that represents the containing peer group of a specific node at the next higher level of the hierarchy.	af-pnni-0055.002
225	parent peer group	The parent peer group of a peer group is the one containing the logical group node representing that peer group. The parent peer group of a node is the one containing the parent node of that node.	af-pnni-0055.002
226	path	The sequence of routers and (sub-)networks that a packet traverses from a particular router to a particular destination host. Note that a path is unidirectional; it is not unusual to have different paths in the two directions between a given host pair.	RFC 1812
227	path constraint	A bound on the combined value of a topology metric along a path for a specific connection.	af-pnni-0055.002
228	path scope	The highest level of PNNI hierarchy used by a path.	af-pnni-0055.002
229	path state	Information kept in routers and hosts about all RSVP senders.	RFC 2205
230	path trace	A control plane mechanism that determines the logical nodes and logical links traversed by new connections and parties in the process of being established, and supporting mechanisms that provide this information to network management systems.	af-cs-0141.000
231	PathErr	Path error RSVP control message.	RFC 2205
232	PathTear	Path teardown RSVP control message.	RFC 2205
233	peer	The other end of the point-to-point link.	RFC 1661
234	peer group	A set of logical nodes which are grouped for purposes of creating a routing hierarchy. PTSEs are exchanged among all members of the group.	af-pnni-0055.002
235	peer group identifier	A string of bits that is used to unambiguously identify a peer group.	af-pnni-0055.002
236	peer group leader	A node of a peer group that performs the extra work of collecting, aggregating, and building data that will be suitable to represent the entire peer group as a single node. This representation is made available in the parent node.	af-pnni-0055.002
237	peer group level	The number of significant bits in the peer group identifier of a particular peer group.	af-pnni-0055.002
238	peer node	A node that is a member of the same peer group as a given node.	af-pnni-0055.002

No.	Terms	Definition	Source document
239	PHOP	An object that carries the Previous Hop information in RSVP control messages.	RFC 2205
240	physical link	A real link which attaches two switching systems.	af-pnni-0055.002
241	physical network	A physical network is a network (or a piece of an Internet) which is contiguous at the link layer. Its internal structure (if any) is transparent to the Internet layer. In this memo, several media components that are connected using devices such as bridges or repeaters are considered to be a single physical network since such devices are transparent to the IP.	RFC 1812
242	physical network interface	This is a physical interface to a connected network and has a (possibly unique) link-layer address. Multiple physical network interfaces on a single router may share the same link-layer address, but the address must be unique for different routers on the same physical network.	RFC 1812
243	PNNI protocol entity	The body of software in a switching system that executes the PNNI protocol and provides the routing service.	af-pnni-0055.002
244	PNNI routing control channel	VCCs used for the exchange of PNNI routing protocol messages.	af-pnni-0055.002
245	PNNI routing domain	A group of topologically contiguous systems which are running one instance of PNNI routing.	af-pnni-0055.002
246	PNNI routing hierarchy	The hierarchy of peer groups used for PNNI routing.	af-pnni-0055.002
247	PNNI Topology State Element (PTSE)	A collection of PNNI information that is flooded among all logical nodes within a peer group.	af-pnni-0055.002
248	PNNI topology state packet	A type of PNNI routing packet that is used for flooding PTSEs among logical nodes within a peer group.	af-pnni-0055.002
249	point-to-point line	A physical medium capable of connecting exactly two systems. In this document, it is only used to refer to such a line when used to connect IP entities. See "general purpose serial interface".	RFC 1812
250	point-to-point networks	A network that joins a single pair of routers. A 56 Kb serial line is an example of a point-to-point network.	RFC 2328
251	police	See "traffic policing".	RFC 2205
252	policy control	A function that determines whether a new request for quality of service has administrative permission to make the requested reservation. Policy control may also perform accounting (usage feedback) for a reservation.	RFC 2205
253	policy data	Data carried in a path or Resv message and used as input to policy control to determine authorization and/or usage feedback for the given flow.	RFC 2205

No.	Terms	Definition	Source document
254	port	The hardware interface in an optical or user network element that terminates a bidirectional link between network elements. Examples include OC-48 or OC-192 ports in a TNE.	OIF-UNI-01.0
255	port identifier	The identifier assigned by a logical node to represent the point of attachment of a link to that node.	af-pnni-0055.002
256	previous hop	The previous router in the direction of traffic flow. Resv messages flow towards previous hops.	RFC 2205
257	protocol	In this document, the next higher level protocol identifier, an internet header field.	RFC 791
258	protocolId	The component of session identification that specifies the IP protocol number used by the data stream.	RFC 2205
259	QoS	Quality of Service.	RFC 2205
260	reachable address prefix	A prefix on a 20 octet ATM address indicating that all addresses beginning with this prefix are reachable.	af-pnni-0055.002
261	Read-Only (RO)	Attributes which are read-only cannot be written by network management. Only the PNNI protocol entity may change the value of a read-only attribute. Network management entities are restricted to only reading such read-only attributes. Read-only attributes are typically for statistical information, including reporting result of actions taken by auto-configuration.	af-pnni-0055.002
262	Read-Write (RW)	Attributes which are read-write cannot be written by the PNNI protocol entity. Only the network management entity may change the value of a read-write attribute. The PNNI protocol entity is restricted to only reading such read-write attributes. Read-write attributes are typically used to provide the ability for network management to configure, control, and manage a PNNI protocol entity's behaviour.	af-pnni-0055.002
263	rendez-vous node	A node that terminates the rerouting request for an alternative connection segment.	af-cs-0173.000
264	rerouting connection	A rerouting connection refers to an alternate connection segment established to replace an incumbent connection segment, or to recover a failed connection segment.	af-cs-0173.000
265	rerouting domain	A group of topologically contiguous systems that share control of domain-based rerouting. The switching systems at the edges of the rerouting domain coordinate domain-based rerouting operation for all calls/connections traversing the rerouting domain. If a call/connection is rerouted inside the rerouting domain, the domain-based rerouting operation occurs between the edges of the rerouting domain and is entirely contained within the rerouting domain. A rerouting domain must be entirely contained in a PNNI routing domain. A PNNI routing domain may contain several rerouting domains.	af-cs-0173.000

No.	Terms	Definition	Source document
266	rerouting node	A node that initiates the establishment of an alternate connection segment to a predetermined rendez-vous node.	af-cs-0173.000
267	reservation state	Information kept in RSVP-capable nodes about successful RSVP reservation requests.	RFC 2205
268	reservation style	Describes a set of attributes for a reservation, including the sharing attributes and sender selection attributes. See 1.3 for details.	RFC 2205
269	rest	The local address portion of an Internet address.	RFC 791
270	restricted transit node	A node that is to be used for transit by a call only in restricted circumstances. It is free from such restriction when it is used to originate or terminate a call.	af-pnni-0055.002
271	Resv message	Reservation request RSVP control message.	RFC 2205
272	ResvConf	Reservation confirmation RSVP control message, confirms successful installation of a reservation at some upstream node.	RFC 2205
273	ResvErr	Reservation error control message, indicates that a reservation request has failed or an active reservation has been preempted.	RFC 2205
274	ResvTear	Reservation teardown RSVP control message, deletes reservation state.	RFC 2205
275	router (1)	A node that forwards IPv6 packets not explicitly addressed to itself.	RFC 2460
276	router (2)	A level three Internet protocol packet switch. Formerly called a gateway in much of the IP literature.	RFC 2328
277	router (3)	A special-purpose dedicated computer that connects several networks. Routers switch packets between these networks in a process known as forwarding. This process may be repeated several times on a single packet by multiple routers until the packet can be delivered to the final destination – switching the packet from router to router-to-router until the packet gets to its destination.	RFC 1812
278	router ID	A 32-bit number assigned to each router running the OSPF protocol. This number uniquely identifies the router within an autonomous system.	RFC 2328
279	routing computation	The process of applying a mathematical algorithm to a topology database to compute routes. There are many types of routing computations that may be used. The Dijkstra algorithm is one particular example of a possible routing computation.	af-pnni-0055.002
280	routing constraint	A generic term that refers to either a topology constraint or a path constraint.	af-pnni-0055.002
281	Reverse Path Forwarding (RPF)	A method used to deduce the next hops for broadcast and multicast packets.	RFC 1812

No.	Terms	Definition	Source document
282	Rspec	The component of a flowspec that defines a desired QoS. The Rspec format is opaque to RSVP and is defined by the Integrated Services Working Group of the IETF.	RFC 2205
283	RSVP_HOP	Object of an RSVP control message that carries the PHOP or NHOP address of the source of the message.	RFC 2205
284	saved modified trace transit list	The trace transit list information element saved on the node after both ingress and egress data has been encoded in the trace (either successfully or not).	af-cs-0141.000
285	saved original trace transit list	The trace transit list information element saved on the node after the ingress data has been encoded in the trace (either successfully or not).	af-cs-0141.000
286	scope (1)	The set of sender hosts to which a given reservation request is to be propagated.	RFC 2205
287	scope (2)	A scope defines the level of advertisement for an address. The level is a level of a peer group in the PNNI routing hierarchy.	af-pnni-0055.002
288	SE style	Shared explicit reservation style, which has explicit sender selection and shared attributes.	RFC 2205
289	semantic fragmentation	A method of fragmenting a large RSVP message using information about the structure and contents of the message, so that each fragment is a logically complete RSVP message.	RFC 2205
290	sender template	Parameter in a path message that defines a sender; carried in a SENDER_TEMPLATE object. It has the form of a filterspec that can be used to select this sender's packets from other packets in the same session on the same link.	RFC 2205
291	sender Tspec	Parameter in a path message, a Tspec that characterizes the traffic parameters for the data flow from the corresponding sender. It is carried in a SENDER_TSPEC object.	RFC 2205
292	sequence numbered FT label	An FT label which is secured using the sequence number in the FT protection TLV.	RFC 3479
293	service path or trail	The user service path is the logical end-end connection between user interfaces. As such, the service path is realized on top of the optical connections and terminates at client termination points. (This is referred to as "Trail" in ITU terminology).	OIF-UNI-01.0
294	session	An RSVP session defines one simplex unicast or multicast data flow for which reservations are required. A session is identified by the destination address, transport-layer protocol, and an optional (generalized) destination port.	RFC 2205
295	shared style	A (reservation) style attribute: all reserved senders share the same reserved resources. See also "distinct style".	RFC 2205
296	signal type	A SDH/SONET signal type, such as STS-1.	OIF-UNI-01.0

No.	Terms	Definition	Source document
297	silently discard (1)	The implementation discards the packet without further processing. The implementation SHOULD provide the capability of logging the error, including the contents of the silently discarded packet, and SHOULD record the event in a statistics counter.	RFC 1661
298	silently discard (2)	This memo specifies several cases where a router is to silently discard a received packet (or datagram). This means that the router should discard the packet without further processing, and that the router will not send any ICMP error message (see 4.3.2) as a result. However, for diagnosis of problems, the router should provide the capability of logging the error (see 1.3.3), including the contents of the silently discarded packet, and should record the event in a statistics counter.	RFC 1812
299	silently ignore	A router is said to silently ignore an error or condition if it takes no action other than possibly generating an error report in an error log or through some network management protocol, and discarding, or ignoring, the source of the error. In particular, the router does NOT generate an ICMP error message.	RFC 1812
300	soft rerouting	A rerouting operation where the original connection segment is released after the establishment of an alternate connection segment (i.e., make-before-break).	af-cs-0173.000
301	soft state	Control state in hosts and routers that will expire if not refreshed within a specified amount of time.	RFC 2205
302	source	The source address, an Internet header field.	RFC 791
303	source node	The first node in a particular rerouting domain to receive the original SETUP message for a particular point-to-point call/connection.	af-cs-0173.000
304	source route	As used in this document, a hierarchically complete source route.	af-pnni-0055.002
305	sparse mode	In multicast forwarding, two paradigms are possible: in sparse mode forwarding, a network layer multicast datagram is forwarded as a data link layer multicast frame to routers and hosts that have asked for it. The initial forwarding state is the inverse of dense-mode in that it assumes that no part of the network wants the data. See "dense mode".	RFC 1812
306	specific-destination address	This is defined to be the destination address in the IP header unless the header contains an IP broadcast or IP multicast address, in which case the specific-destination is an IP address assigned to the physical interface on which the packet arrived.	RFC 1812
307	split system	A switching system which implements the functions of more than one logical node.	af-pnni-0055.002
308	spoke	In the complex node representation, this represents the connectivity between the nucleus and a specific port.	af-pnni-0055.002
309	style	Object of an RSVP message that specifies the desired reservation style.	RFC 2205

No.	Terms	Definition	Source document
310	subnet	A portion of a network, which may be a physically independent network, which shares a network address with other portions of the network and is distinguished by a subnet number. A subnet is to a network what a network is to an Internet.	RFC 1812
311	subnet number	A part of the Internet address that designates a subnet. It is ignored for the purposes of Internet routing, but is used for intranet routing.	RFC 1812
312	summary address	An address prefix that tells a node how to summarize reachability information.	af-pnni-0055.002
313	switching system	A set of one or more physical devices that act together as a single PNNI network management entity. A switching system contains one or more lowest-level nodes and, when it is acting as a PGL, one or more LGNs.	af-pnni-0055.002
314	Transmission Control Protocol (TCP)	A host-to-host protocol for reliable communication in internet environments.	RFC 791
315	TCP segment	The unit of data exchanged between TCP modules (including the TCP header).	RFC 791
316	Trivial File Transfer Protocol (TFTP)	A simple file transfer protocol built on UDP.	RFC 791
317	time to live (1)	An internet header field which indicates the upper bound on how long this Internet datagram may exist.	RFC 791
318	Time To Live (TTL) (2)	A field in the IP header that represents how long a packet is considered valid. It is a combination hop count and timer value.	RFC 1812
319	TIME_VALUES	Object in an RSVP control message that specifies the time period timer used for refreshing the state in this message.	RFC 2205
320	topology aggregation	The process of summarizing and compressing topology information at a hierarchical level to be advertised at the level above.	af-pnni-0055.002
321	topology attribute	A generic term that refers to either a link attribute or a nodal attribute.	af-pnni-0055.002
322	topology constraint	A topology constraint is a generic term that refers to either a link constraint or a nodal constraint.	af-pnni-0055.002
323	topology database	The database that describes the topology of the entire PNNI routing domain as seen by a node.	af-pnni-0055.002
324	topology metric	A generic term that refers to either a link metric or a nodal metric.	af-pnni-0055.002
325	topology state parameter	A generic term that refers to either a link parameter or a nodal parameter.	af-pnni-0055.002
326	Type Of Service (TOS)	A field in the IP header that represents the degree of reliability expected from the network layer by the transport layer or application.	RFC 1812

No.	Terms	Definition	Source document
327	total length	The internet header field total length is the length of the datagram in octets including internet header and data.	RFC 791
328	trace destination interface PNNI addendum for path and connection trace v1.0	An interface on which a path or connection trace terminates when it completes normally. This interface is defined by any one of three conditions: 1) This interface directly supports the called party number (for path trace and connection trace towards the called party) or calling party number (for connection trace towards the calling party), e.g., soft PVC called or calling party; 2) The next interface which the connection or party traverses (for connection trace), or the next interface on which the connection or party would be progressed towards the called party (for path trace), is not a PNNI interface (e.g., UNI, AINI, B-ICI, IISP); or 3) The next interface which the connection or party traverses (for connection trace), or the next interface on which the connection or party would be progressed towards the called party (for path trace), is administratively designated as a trace destination interface.	af-cs-0141.000
329	trace destination node	The node at which connection trace or path trace is terminated for a given connection, when the trace completes normally. A trace destination node is a node whose outgoing interface for the connection is a trace destination interface.	af-cs-0141.000
330	trace source interface	The interface at the trace source node that is (administratively) designated as the starting point for path or connection trace of a given connection.	af-cs-0141.000
331	trace source node	The node at which connection trace or path trace is initiated for a given connection. This node inserts a new Trace transit list information element into a SETUP or ADD PARTY message (for path trace), or originates a new TRACE CONNECTION message (for connection trace).	af-cs-0141.000
332	traffic control	The entire set of machinery in the node that supplies requested QoS to data streams. Traffic control includes packet classifier, packet scheduler, and admission control functions.	RFC 2205
333	Traffic Engineered Tunnel (TE Tunnel)	A set of one or more LSP tunnels which carries a traffic trunk.	RFC 3209
334	traffic policing	The function, performed by traffic control, of forcing a given data flow into compliance with the traffic parameters implied by the reservation. It may involve dropping non-compliant packets or sending them with lower priority, for example.	RFC 2205

No.	Terms	Definition	Source document
335	traffic trunk	A set of flows aggregated by their service class and then placed on an LSP or set of LSPs called a traffic engineered tunnel.	RFC 3209
336	transport network address	Address of an entity (e.g., a TNE) within the transport network.	OIF-UNI-01.0
337	Transport Network Assigned (TNA) address	An address assigned to a client by the transport service provider, either via a protocol or by configuration.	OIF-UNI-01.0
338	Transport Network Element (TNE)	A network element (within the transport network) having optical interfaces, such as an optical cross-connect (OXC) or an optical add/drop multiplexer.	OIF-UNI-01.0
339	TSpec	A traffic parameter set that describes a flow. The format of a Tspec is opaque to RSVP and is defined by the Integrated Services Working Group.	RFC 2205
340	User Datagram Protocol (UDP)	A user level protocol for transaction oriented applications.	RFC 791
341	UDP encapsulation	A way for hosts that cannot use raw sockets to participate in RSVP by encapsulating the RSVP protocol (raw) packets in ordinary UDP packets. See Appendix C for more information.	RFC 2205
342	User Network Interface (UNI)	The user-network interface is the service control interface between a client device and the transport network.	OIF-UNI-01.0
343	UNI Signalling Channel	This is the logical communication channel between the UNI-C and the UNI-N over which UNI signalling messages are sent.	OIF-UNI-01.0
344	UNI-C	The logical entity that terminates UNI signalling on the client device side.	OIF-UNI-01.0
345	UNI-N	The logical entity that terminates UNI signalling on the transport network side.	OIF-UNI-01.0
346	uplink	Represents the connectivity from a border node to an upnode.	af-pnni-0055.002
347	upnode	The node that represents a border node's outside neighbour in the common peer group. The upnode must be a neighbouring peer of one of the border node's ancestors.	af-pnni-0055.002
348	upper layer	A protocol layer immediately above IPv6. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunneled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself.	RFC 2460
349	upstream	Towards the traffic source. RSVP Resv messages flow upstream.	RFC 2205
350	user (1)	The user of the internet protocol. This may be a higher level protocol module, an application program, or a gateway program.	RFC 791

No.	Terms	Definition	Source document
351	user (2) or client	Network equipment that is connected to the transport network for utilizing optical transport services. Examples of clients include IP routers, ATM switches, Ethernet Switches, SDH/SONET Cross-connects, etc.	OIF-UNI-01.0
352	version	The Version field indicates the format of the internet header.	RFC 791
353	Wavelength Division Multiplexing (WDM)	A technology that allows multiple optical signals operating at different wavelengths to be multiplexed onto a single fibre.	OIF-UNI-01.0
354	WF style	Wildcard Filter reservation style, which has wildcard sender selection and shared attributes.	RFC 2205
355	wildcard sender selection	A (reservation) style attribute: traffic from any sender to a specific session receives the same QoS. See also "explicit sender selection".	RFC 2205

Appendix III

Related abbreviations and acronyms found in documents from other organizations

NOTE – In the list below, a term followed by a number in ( ) indicates that the term has multiple meaning defined by different documents.

AA	Administrative Authority (a three octet field in the GOSIP version 2.0 NSAP address format)	RFC 1195
AAL	ATM Adaptation Layer	af-cs-0148.000
ABR	Available Bit Rate	af-cs-0148.000
ACR	Available Cell Rate	af-cs-0173.000
AD	Administrative Domain	RFC 2753
AES	Advanced Encryption Standard	Security Mgmt-IA
AESA	ATM End System Address	af-cs-0173.000
AFI	Authority and Format Identifier (the first octet of all OSI NSAP addresses – identifies format of the rest of the address)	RFC 1195
AINI	ATM Inter-Network Interface	af-cs-0141.000
ASP	ATM Service Provider	af-pnni-0055.002
ATC	ATM Transfer Capability	af-pnni-0055.002
ATM	Asynchronous Transfer Mode	af-cs-0141.000
AvCR	Available Cell Rate	af-pnni-0055.002
AW	Administrative Weight	af-pnni-0055.002
BGP	Border Gateway Protocol	af-pnni-0055.002
B-ICI	B-ISDN Inter Carrier Interface	af-cs-0141.000
B-ISUP	Broadband ISDN User Part	af-cs-0148.000

B-LLI	Broadband Low Layer Information	af-cs-0173.000
CA	Certification Authority	Security Mgmt-IA
CAC	Connection Admission Control	af-pnni-0055.002
CBC	Cipher Block Chaining	Security Mgmt-IA
CBR	Constant Bit Rate	af-cs-0148.000
CDV	Cell Delay Variation	af-pnni-0055.002
CLNP	ConnectionLess Network Protocol (ISO 8473, the OSI connectionless network layer protocol – very similar to IP)	RFC 1195
CLR	Cell Loss Ratio	af-pnni-0055.002
CLR0	Cell Loss Ratio objective for CLP=0 traffic	af-pnni-0055.002
CMIP	Common Management Information Protocol	Security Mgmt-IA
COA	Connection available	af-cs-0148.000
CO-BI	Connection-Oriented Bearer-Independent	af-cs-0141.000
COPS	Common Open Policy Service	RFC 2749
CORBA	Common Object Request Broker Architecture	Security Mgmt-IA
CRC	Cyclic Redundancy Check	Security Mgmt-IA
CR-LSP	Constraint-based Router Label Switched Path	RFC 3212
CRM	Cell Rate Margin	af-pnni-0055.002
CTD	Cell Transfer Delay	af-cs-0173.000
DCC	Data Communication Channel	OIF-UNI-01.0
DES	Data Encryption Standard	Security Mgmt-IA
DFI	DSP Format Identifier (a one octet field in the GOSIP version 2.0 NSAP address format)	RFC 1195
DH	Diffie-Hellman	Security Mgmt-IA
DLCI	Data Link Connection Identifier	af-cs-0141.000
DSP	Domain Specific Part	af-pnni-0055.002
DSS	Digital Signature Standard	Security Mgmt-IA
DTL	Designated Transit List	af-pnni-0055.002
EMS	Element Management System	Security Mgmt-IA
ES	End System (The OSI term for a host)	RFC 1195
ESI	End System Identifier	af-pnni-0055.002
ES-IS	End System-to-Intermediate System Routing Exchange Protocol (ISO 9542 – OSI protocol between routers and end systems)	RFC 1195
ESP	Encapsulating Security Payload	Security Mgmt-IA
FRTT	Fixed Round Trip Time	af-cs-0173.000
FSM	Finite State Machine	af-cs-0173.000
GCAC	Generic Connection Admission Control	af-pnni-0055.002
GFR	Guaranteed Frame Rate	af-cs-0173.000
GMPLS	Generalized Multi-Protocol Label Switching	OIF-UNI-01.0
GSMP	Generic Switch Management Protocol	OIF-UNI-01.0
ICD	International Code Designator (ISO standard for identifying organizations)	RFC 1195
ICMP	Internet Control Message Protocol	Security Mgmt-IA
ICR	Initial Cell Rate	af-cs-0173.000

ID	Identifier	af-pnni-0055.002
IDI	Initial Domain Identifier	af-pnni-0055.002
IDP	Initial Domain Part	af-pnni-0055.002
IDRP	Inter Domain Routing Protocol	af-pnni-0055.002
IE	Information Element	af-pnni-0055.002
IG	Information Group	af-pnni-0055.002
IISP	Interim Inter-switch Signalling Protocol	af-cs-0141.000
IKE	Internet Key Exchange	Security Mgmt-IA
ILMI	Interim Local Management Interface	af-pnni-0055.002
IP (1)	Internetwork Protocol (an Internet Standard Network Layer Protocol)	RFC 1195
IP (2)	Internet Protocol	Security Mgmt-IA
IPCC	IP Control Channel	OIF-UNI-01.0
IPSec	IP Security	Security Mgmt-IA
IS	Intermediate System (The OSI term for a router)	RFC 1195
ISH	Intermediate System Hello – A Hello packet defined by ISO 9542 (ES-IS protocol) (not the same as IS-IS Hello)	RFC 1195
ISI	Internal Signalling Interface	OIF-UNI-01.0
IS-IS	Intermediate System to Intermediate System routing exchange protocol (the ISO protocol for routing within a single routing domain)	RFC 1195
IS-IS Hello	A Hello packet defined by the IS-IS protocol (a type of packet used by the IS-IS protocol)	RFC 1195
ISO	International Organization for Standardization (an international body which is authorized to write standards of many kinds)	RFC 1195
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector	af-cs-0141.000
IUT	Implementation Under Test	af-cs-0141.000, af-cs-0148.000
KDC	Key Distribution Center	Security Mgmt-IA
LDP	Label Distribution Protocol	OIF-UNI-01.0
LGN	Logical Group Node	af-pnni-0055.002
LMP	Link Management Protocol	OIF-UNI-01.0
LOH	Line Overhead	OIF-UNI-01.0
LSB	Least Significant Bit	af-pnni-0055.002
LSP	Link State Packet (a type of packet used by the IS-IS protocol)	RFC 1195
LTE	Line Terminating Equipment	OIF-UNI-01.0
M	Mandatory requirements (these are to be observed in all cases)	af-cs-0148.000
MAC	Message Authentication Code	Security Mgmt-IA
maxCR	Maximum Cell Rate	af-pnni-0055.002
maxCTD	Maximum Cell Transfer Delay	af-pnni-0055.002
MBS	Maximum Burst Size	af-cs-0148.000
MCR	Minimum Cell Rate	af-pnni-0055.002
MIB	Management Information Base	af-cs-0141.000
MOA	Modification acknowledge message	af-cs-0148.000
MOD	Modification request message	af-cs-0148.000
MOR	Modification reject message	af-cs-0148.000

MPLS	Multi-Protocol Label Switching	OIF-UNI-01.0
MSB	Most Significant Bit	af-pnni-0055.002
MSOH	Multiplex Section Overhead	OIF-UNI-01.0
N/A	Not supported, not applicable, or the conditions for status are not met	af-cs-0148.000
NA	Network Administrator	Security Mgmt-IA
NCCI	Network Call Correlation Identifier	af-cs-0173.000
ND	Neighbour Discovery	OIF-UNI-01.0
NE	Network Element	Security Mgmt-IA
NLPID	Network Layer Protocol ID (A one-octet field identifying a network layer protocol)	RFC 1195
NMS	Network Management System	Security Mgmt-IA
NNI	Network-to-Network Interface	af-pnni-0055.002
nrtVBR	non-real time VBR	af-cs-0148.000
NSAP	Network Service Access Point (a conceptual interface point at which the network service is made available)	RFC 1195
O	Optional (may be selected to suit the implementation, provided that any requirements applicable to the options are observed)	af-cs-0148.000
O.n	Optional, but support is required for either at least one or only one of the options in the group labelled with the same numeral "n".	af-cs-0148.000
OA&M	Operations, Administration & Maintenance	af-cs-0148.000
OC-N	Optical Carrier level N	OIF-UNI-01.0
OH	Overhead	OIF-UNI-01.0
ONE	Optical Network Element	OIF-UNI-01.0
OSI	Open Systems Interconnection (an international standard protocol architecture)	RFC 1195
OSPF	Open Shortest Path First	af-pnni-0055.002
OUI	Organizational Unique Identifier	af-cs-0141.000
PCR	Peak Cell Rate	af-pnni-0055.002
PDP	Policy Decision Point	RFC 2753
PEP	Policy Enforcement Point	RFC 2753
PIN	Policy Ignorant Node	RFC 2753
PG	Peer Group	af-pnni-0055.002
PGL	Peer Group Leader	af-pnni-0055.002
PGLE	Peer Group Leader Election	af-pnni-0055.002
PICS	Protocol Implementation Conformance Statement	af-cs-0141.000
PNNI	Private Network-Network Interface	af-cs-0141.000
PTSE	PNNI Topology State Element	af-pnni-0055.002
PTSP	PNNI Topology State Packet	af-pnni-0055.002
PVC	Permanent Virtual Circuit	af-cs-0173.000
PVCC	Permanent Virtual Channel Connection	af-pnni-0055.002
QoS	Quality of Service	af-pnni-0055.002
RAIG	Resource Availability Information Group	af-pnni-0055.002
RCC	Routing Control Channel	af-pnni-0055.002
RD	Routing Domain (the set of routers and end systems using a single instance of a routing protocol such as IS-IS)	RFC 1195

RDF	Rate Decrease Factor	af-pnni-0055.002
RFC	Request for Comments	Security Mgmt-IA
RIF	Rate Increase Factor	af-pnni-0055.002
RM	Resource Management	af-cs-0173.000
RSA	Rivest, Shamir, and Adleman	Security Mgmt-IA
RSOH	Regenerator Section Overhead	OIF-UNI-01.0
RSVP	Resource reSerVation Protocol	OIF-UNI-01.0
RSVP-TE	RSVP with Traffic Engineering extensions	OIF-UNI-01.0
rtVBR	real time VBR	af-cs-0148.000
S/MIME	Secure Multipurpose Internet Mail Extensions	Security Mgmt-IA
SA	Security Association	Security Mgmt-IA
SAAL	Signalling ATM Adaptation Layer	af-cs-0173.000, af-pnni-0055.002
SAD	Security Association Database	Security Mgmt-IA
SCR	Sustainable Cell Rate	af-pnni-0055.002, af-cs-0148.000
SEL	NSAP Selector (the last octet of NSAP addresses, also called NSEL)	RFC 1195
SHA	Secure Hash Algorithm	Security Mgmt-IA
SNMP	Simple Network Management Protocol	Security Mgmt-IA
SNPA	Subnetwork Point of Attachment (a conceptual interface at which a subnetwork service is provided)	RFC 1195
Soft	PVC Soft Permanent Virtual Connection	af-cs-0141.000
SPD	Security Policy Database	Security Mgmt-IA
SSCOP	Service Specific Connection Oriented Protocol	af-pnni-0055.002
SSCS	Service Specific Convergence Sublayer	af-pnni-0055.002
SSH	Secure Shell	Security Mgmt-IA
SSL	Secure Sockets Layer	Security Mgmt-IA
STE	Section Terminating Equipment	OIF-UNI-01.0
STM-M	Synchronous Transport Module level M	OIF-UNI-01.0
STS-N	Synchronous Transport Signal level N	OIF-UNI-01.0
SUT	System Under Test	af-cs-0141.000
SVC (1)	Switched Virtual Connection	af-pnni-0055.002, af-cs-0141.000
SVC (2)	Switched Virtual Circuit	af-cs-0173.000
SVCC	Switched Virtual Channel Connection	af-pnni-0055.002, af-cs-0173.000
SVPC	Switched Virtual Path Connection	af-pnni-0055.002, af-cs-0173.000
TAS	Transported Address Stack	af-cs-0173.000
TBE (1)	Transit Buffer Exposure	af-pnni-0055.002
TBE (2)	Transient Buffer Exposure	af-cs-0173.000
TCP	Transmission Control Protocol (an Internet Standard Transport Layer Protocol)	RFC 1195
TCP/IP	The protocol suite based on TCP, IP, and related protocols (the Internet standard protocol architecture)	RFC 1195

TGT	Ticket Granting Ticket	Security Mgmt-IA
TL1	Transaction Language 1	Security Mgmt-IA
TLS	Transport Layer Security	Security Mgmt-IA
TLV (1)	Type Length Value	af-cs-0173.000, af-pnni-0055.002
TLV (2)	Type-Length-Value encoding	OIF-UNI-01.0
TNA	Optical-Network Assigned	OIF-UNI-01.0
TTL	Trace Transit List	af-cs-0141.000
UBR	Unspecified Bit Rate	af-cs-0148.000, af-pnni-0055.002
UDP	User Datagram Protocol	Security Mgmt-IA
ULIA	Uplink Information Attribute	af-pnni-0055.002
UNI (1)	User to Network Interface	af-cs-0173.000, af-pnni-0055.002
UNI (2)	User Network Interface	OIF-UNI-01.0
UNI-N	UNI Signalling Agent – Network	OIF-UNI-01.0
UNI-C	UNI Signalling Agent – Client	OIF-UNI-01.0
VBR	Variable Bit Rate	af-pnni-0055.002, af-cs-0148.000
VCC	Virtual Channel Connection	af-pnni-0055.002
VCI	Virtual Channel Identifier	af-pnni-0055.002, af-cs-0141.000
VF	Variance Factor	af-pnni-0055.002
VP	Virtual Path	af-pnni-0055.002
VPC	Virtual Path Connection	af-pnni-0055.002, af-cs-0141.000
VPCI	Virtual Path Connection Identifier	af-cs-0141.000
VPI	Virtual Path Identifier	af-pnni-0055.002, af-cs-0141.000

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	**Y.1300–Y.1399**
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

For further details, please refer to the list of ITU-T Recommendations.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	**Global information infrastructure, Internet protocol aspects and Next Generation Networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2004