International Telecommunication Union

ITU-T G.8081/Y.1353

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Amendment 1

(06/2006)

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

Ethernet over Transport aspects – 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)

Amendment 1

ITU-T Recommendation G.8081/Y.1353 (2004) – Amendment 1

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
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
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
ETHERNET OVER TRANSPORT ASPECTS	G.8000–G.8999
General aspects	**G.8000–G.8099**
MPLS over Transport aspects	G.8100–G.8199
Quality and availability targets	G.8200–G.8299
ACCESS NETWORKS	G.9000–G.9999

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)

Amendment 1

Summary

This amendment identifies modifications to definitions and abbreviations listed in ITU-T Rec. G.8081/Y.1353 (06/2004), and presents additional terminology definitions and abbreviations to be inserted into ITU-T Rec. G.8081/Y.1353.

Source

Amendment 1 to ITU-T Recommendation G.8081/Y.1353 (2004) was approved on 6 June 2006 by ITU-T Study Group 15 (2005-2008) under the ITU-T Recommendation A.8 procedure.

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)

Amendment 1

1 Introduction

Certain terms and abbreviations have been modified, defined or used since the approval of ITU-T Rec. G.8081/Y.1353 (06/2004); and, to some existing terms, consistent definitions have recently been formulated. All of the above should or could be reflected in ITU-T Rec. G.8081/Y.1353. This amendment indicates modifications to ITU-T Rec. G.8081/Y.1353 (06/2004).

2 Changes to definitions in ITU-T Rec. G.8081/Y.1353 (06/2004)

2.1 Clause 3.1

a) Delete the following terms in clause 3.1.2:

- Connection Point (CP)
- Termination Connection Point
- Subnetwork

b) Add the term "Continuity Supervision" in clause 3.1.3.

c) Delete the following terms in clause 3.1.8:

- Connection Termination Point (CTP)
- Trail Termination Point (TTP)

d) Insert new subclauses as follows:

3.1.10 Terms defined in ITU-T Rec. X.25

– Closed User Group.

3.1.11 Terms defined in ITU-T Rec. Y.1311

– Virtual Private Network (VPN).

2.2 Clause 3.2

a) Insert the following terms according to alphabetic order, and renumber all the terms accordingly:

Automatically Switched Optical Network (ASON): An Automatically Switched Transport Network (ASTN) that is applied to connection oriented circuit switched networks (described by ITU-T Rec. G.805) such as SDH transport networks, as defined by ITU-T Rec. G.803; or, Optical Transport Networks, as defined by ITU-T Rec. G.872, etc.

component: An abstract representation of a functional entity. In this Recommendation, components do not represent instances of implementation code. They are used to construct scenarios to explain the operation of the architecture.

Connection Point (CP): For the purposes of this Recommendation, a connection point represents the north input port of an Adaptation function. (Note that in ITU-T Rec. G.805 the CP refers to the binding between two points.)

Connection Termination Point (CTP): A connection termination point represents the signal state at the CP. Also, see ITU-T Rec. M.3100.

control plane: The control plane performs the call control and connection control functions. Through signalling, the control plane sets up and releases connections, and may restore a connection in case of a failure. The control plane also performs other functions in support of call and connection control, such as routing information dissemination.

control plane configured protection: Control plane configured protection refers to the configuration and use of transport plane protection capabilities. Configuration of protection is done by the control plane as opposed to the management plane. Control plane components associated with a protected connection are responsible for use of the protected connection. In the event of a failure, the control plane protection action does not involve rerouting or additional connection setup.

CR-LDP peers: Two protocol controllers implementing CR-LDP that have established communication with each other.

CR-LDP session: The control communication instance between two CR-LDP peers.

downstream on demand: A label advertisement procedure by which the upstream node is responsible for requesting the label mapping.

E-NNI: A bidirectional interface between control plane entities belonging to different domains.

I-NNI: A bidirectional interface between control plane entities belonging to one or more domains having a trusted relationship.

interface: In the context of this Recommendation, interfaces represent logical relationships between ASTN control plane entities and are defined by the information flow between these entities. Such a relationship allows distribution of these entities in support of different equipment implementations and network architectures.

hello: A message sent by a signalling protocol controller to advertise its presence to other signalling protocol controllers.

label: This term is the same as an SNP.

Link Resource Manager (LRM): An architecture component. Two LRM components are used – the LRMA and LRMZ. The LRM components are responsible for the management of an SNPP link, including the allocation and un-allocation of SNP link connections, providing topology and status information. An SNPP link is managed by a pair of LRMA and LRMZ components, each one managing an end of the link. Requests to allocate SNP link connections are only directed to the LRMA. Since an SNPP link can be either public or private, a LRM can also be either public or associated to exactly one VPN. See ITU-T Rec. G.8080/Y.1304.

node: In the context of this Recommendation, the term "node" is used to signify a subnetwork or a Routing Area.

ordered control mode: A node initiates the transmission of a label mapping only when the label mapping from the downstream node is received.

restoration: Restoration is the action of replacing a connection in a call by rerouting the connection.

routing domain: A type of control domain where the criterion for membership is a common routing capability. It may contain zero or more rerouting domains.

subnetwork: A topological component used to effect routing of a specific characteristic information. For the purposes of this Recommendation, a subnetwork is bounded by subnetwork points.

Subnetwork Connection (SNC): A subnetwork connection is a dynamic relation between two (or more, in the case of broadcast connections) subnetwork points at the boundary of the same subnetwork.

transport domain: A transport domain is a set of transport resources that are grouped as a result of some criteria. This grouping is established by operator policies. An example is the G.805 administrative domain.

transport resource identifier: Transport resource identifiers are used by control plane components to refer to transport plane resources. This name space is operator assigned and is independent of SNPP identifier spaces.

Termination Connection Point (TCP): For the purposes of this Recommendation, a termination connection point represents the output of a trail termination function or the input to a trail termination sink function. (Note that in ITU-T Rec. G.805 the TCP refers to the binding between two points).

Trail Termination Point (TTP): A trail termination point represents the signal state at a TCP. Also, see ITU-T Rec. M.3100.

User-Network Interface for the control plane (UNI): A bidirectional signalling interface between service requester and service provider control plane entities.

b) In subclause 3.2.34, delete the words "See ITU-T Rec. G.807/Y.1302."

c) Delete the following items:

3.2.57 UNI transport resource name

3.2.58 Virtual Private Network (VPN)

2.3 Terms to be modified in ITU-T Rec. G.8081/Y.1353 (06/2004)

The table below lists changes to definitions of related terms in ITU-T Rec. G.8081/Y.1353:

Original term	Replacement text
3.2.6 call: An association between endpoints that supports an instance of a service.	**3.2.6 call**: An association between two or more users and one or more domains that support an instance of a service through one or more domains. Within domains, the association is supported by network entities that contain call state. Between a user and a network call control entity and between network call control entities, there are call segments. The call consists of a set of concatenated call segments.
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.	**3.2.9.2 Network call controller**: A network call controller provides three roles, one for support of the calling party, another to support the called party and a third to support calls across domain boundaries. 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.

Original term	Replacement text
3.2.10 call segment: An association between two call control entities (call controllers), using a telecommunication service to concatenate a call.	**3.2.10 call segment**: An association between two call control entities (as per ITU-T Rec. Q.2982, which is equivalent to G.8080/Y.1304 call controllers). Each call segment has zero or more associated connections. Call segments between network call control entities have zero or more supporting calls.
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.	**3.2.16.1 control domain**: A type of transport domain where the criterion for membership is the scope of a control plane component that is responsible for the transport resources within the transport domain.
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.	**3.2.16.2 rerouting domain**: A type of routing control domain whose control components at the edge of the domain coordinate rerouting operations for all calls/connections that traverse the rerouting domain.
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. 8080/Y.1304.	**3.2.19 hard rerouting**: A failure recovery function in a rerouting domain that attempts to create another connection to the destination at the edge of the rerouting domain. This is performed in response to the failure of an existing connection, and the rerouted connection replaces the connection that contained the failure.
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.	**3.2.24 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. The TMN architecture is described in ITU-T Rec. M.3010; additional details of the management plane are provided by the M-series Recommendations.
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.	**3.2.25 multi-homed**: A user is considered to be multi-homed when there are two or more SNPP links connecting the access group container to the network. SNPP links associated with the same UNI reference point, if on the network side, are within the scope of a common network call controller component. Further, there is also a service agreement between the user and the network such that the network offers reliability, diversity, or other service characteristic between connections on different multi-homed SNPP links.

Original term	Replacement text
3.2.28 Permanent Connection (PC): A PC is a connection type that is provisioned by the management system.	**3.2.28 Permanent Connection (PC)**: A PC is a connection type that is provisioned by manual action or via the management system.
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.	**3.2.33 route**: A sequence of SNP names, SNPP names, routing area names, and/or transport resource identifiers that are used by the control plane to create a network connection.
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.	**3.2.34.1 hierarchical routing**: One of the three basic forms of algorithm for dynamic path control. A node contains a routing controller, connection controllers and link resource managers for a single level in a routing area hierarchy. The decomposition of routing areas follows the decomposition of a layer network into a hierarchy of subnetworks (in line with the concepts described in ITU-T Rec. G.805). Connection controllers are related to one another in a hierarchical manner. Each routing area has its own dynamic connection control that has knowledge of the topology of its routing area but has no knowledge of the topology of routing areas above or below itself in the hierarchy, or other routing areas 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.	**3.2.34.2 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. The significant difference is that connection controllers invoke a different sequence of path computation functions between routing levels for hierarchical vs. source routing. 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.	**3.2.34.3 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.

Original term	Replacement text
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.	**3.2.36 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. The limit of subdivision results in a routing area that contains a subnetwork.
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.	**3.2.37 Routing Controller (RC)**: A component with the roles to: – respond to requests for path (route) information needed to set up connections. This information can range from end-to-end path details to a next hop. The route can be computed by one or more cooperating RCs; – 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.	**3.2.38 Routing Control Domain (RCD)**: A type of control domain where the criterion for membership is a common routing capability. It may contain zero or more rerouting domains.
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.	**3.2.42 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. Service level agreements and related policies are outside the scope of this Recommendation.
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.	**3.2.46 soft rerouting**: Soft rerouting is a function that reroutes a connection for administrative purposes. The original connection is not taken out of service until the rerouted connection is established.

3 Additions to clause 4

In clause 4, insert the following abbreviations in alphabetical order:

ACC-n	A-end CC at domain n
AGC-a	A-end AGC
AGC-z	Z-end AGC
ARC	Alarm Reporting Control
ASC-n	A-end signalling controller in domain n
ASN-n	A-end SN in domain n
CC-a	A-end Connection Controller
CC-z	Z-end Connection Controller
CCC-a	A-end CCC
CCC-z	Z-end CCC
CoS	Class of Service
DCM	Distributed Call and Connection Management
DT	Discovery Trigger
LAD	Layer Adjacency Discovery
LAPD	Link Access Procedure D-channel
LCP	Link Control Protocol
LLCF	Link Layer Convergence Function
MI	Management Information
MO	Managed Object
MP	Management Plane
NCC-n	NCC in domain n
PPP	Point-to-Point Protocol
SC-a	A-end user signalling controller
SC-z	Z-end user signalling controller
SN	SubNetwork
TCC-n	Transit CC in domain n
TCE	Transport Entity Capability Exchange
TSC-n	Transit Signalling Controller in domain n
TSN-n	Transit SN in domain n
UNI-C	The user side of UNI, UNI-C (for client)
UNI-N	The network side of UNI, UNI-N (for network)
ZSC-n	Z-end signalling controller at domain n
ZSN-n	Z-end SN in domain n

4 Appendix I – List of source Recommendations

Update the table in Appendix I as follows:

ITU-T Recommendation	Latest version
G.7713/Y.1704	05/06
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	08/05
G.7714.1/Y.1705.1	04/03
G.7715/Y.1706	06/02
G.7715.1/Y.1706.1	02/04
G.8080/Y.1304	06/06

5 Editorial changes

5.1 Clause 2 – References

a) Add the following two references in clause 2:

– ITU-T Recommendation X.25 (1996), *Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit*.

– ITU-T Recommendation Y.1311 (2002), *Network-based VPNs – Generic architecture and service requirements*.

b) Delete the following reference:

– ITU-T Recommendation G.807/Y.1302 (2001), *Requirements for automatic switched transport networks (ASTN)*.

c) Update the title of the referred ITU-T Rec. G.7714/Y.1705 as follows:

– ITU-T Recommendation G.7714/Y.1705 (2005), *Generalized automatic discovery for transport entities*.

5.2 Editorial changes to Appendices II and III

In Appendix II, to delete reference numbers and words from the text of some definitions (which were included in the original text of those definitions).

To sort all items alphabetically with additions and updates to Appendices II and III based on newly available RFCs.

The updated Appendices II and III are as follows:

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.

Terms	Definition	Source document
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
address	An IPv6-layer identifier for an interface or a set of interfaces.	RFC 2460
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
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
adjacency (2)	The relationship between two communicating neighbouring peer nodes.	af-pnni-0055.002
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
Adspec	An Adspec is a data element (object) in a Path message that carries a package of OPWA advertising information. See "OPWA".	RFC 2205
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
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
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
ARPANET leader	The control information on an ARPANET message at the host-IMP interface.	RFC 791
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
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
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

Terms	Definition	Source document
Autonomous System (AS) (1)	A group of routers exchanging routing information via a common routing protocol. Abbreviated as AS.	RFC 2328
Autonomous System (AS) (2)	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
auto-refresh loop	An auto-refresh loop is an error condition that occurs when a topological loop of routers continues to refresh existing reservation state even though all receivers have stopped requesting these reservations.	RFC 2205
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
blockade state	Blockade state helps to solve a "killer reservation" problem. See "killer reservation".	RFC 2205
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
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
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

Terms	Definition	Source document
bundled link	A TE link such that, for the purpose of GMPLS signalling, a combination of <TE link identifier, label> is not sufficient to unambiguously identify the appropriate resources used by an LSP. In this situation, the link bundling construct assumes that the set of resources that form the TE link could be partitioned into disjoint subsets, such that (a) the partition is minimal, and (b) within each subset, a label is sufficient to unambiguously identify the appropriate resources used by an LSP. We refer to such subsets as "component links", and to the whole TE link as a "bundled link". Furthermore, we restrict the identifiers that can be used to identify component links such that they are unique for a given node. On a bundled link, a combination of <component link identifier, label> is sufficient to unambiguously identify the appropriate resources used by an LSP.	RFC 4201
bypass	A bypass represents the connectivity between two ports in the complex node representation. A bypass is always an exception.	af-pnni-0055.002
check-pointable FT label	An FT label which is secured by using the check-pointing techniques.	RFC 3479
check-pointing	A process of message exchanges that confirm receipt and processing (or secure storage) of specific protocol messages.	RFC 3479
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
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
class-name	The class of an object. See "object".	RFC 2205
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
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
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
complex node representation	A collection of nodal state parameters that provide detailed state information associated with a logical node.	af-pnni-0055.002
component link	A subset of resources of a TE Link such that (a) the partition is minimal, and (b) within each subset a label is sufficient to unambiguously identify the appropriate resources used by an LSP.	RFC 4201
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

Terms	Definition	Source document
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
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.	OIF-UNI-01.0
connection scope	The level of routing hierarchy within which a given connection request to a group address is constrained.	af-pnni-0055.002
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
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
control channel	A pair of mutually reachable interfaces that are used to enable communication between nodes for routing, signalling, and link management.	RFC 4204
conventional maximum frame payload size	The maximum frame payload size allowed by data link standards. For example, the Conventional Maximum Frame Payload Size for Ethernet is 1500 bytes.	RFC 3032
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
C-type	The class type of an object; unique within class-name. See "class-name".	RFC 2205
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
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
data link	A pair of interfaces that are used to transfer user data. Note that in GMPLS, the control channel(s) between two adjacent nodes are no longer required to use the same physical medium as the data links between those nodes.	RFC 4204
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
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

Terms	Definition	Source document
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
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
Designated Transit List (DTL)	A list of node and optionally link Ids that completely specify a path across a single PNNI peer group.	af-pnni-0055.002
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
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
DestAddress	The IP destination address; part of session identification. See "session".	RFC 2205
destination	The destination address, an Internet header field.	RFC 791
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
Dijkstra's algorithm	An algorithm that is sometimes used to calculate routes given a link and nodal state topology database.	af-pnni-0055.002
distinct style	A (reservation) style attribute. Separate resources are reserved for each different sender. See also "shared style".	RFC 2205
DLCI	A label used in Frame Relay networks to identify frame relay circuits.	RFC 3031
domain	Synonymous with PNNI Routing Domain.	af-pnni-0055.002
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
Don't Fragment (DF)	The Don't Fragment bit carried in the flags field.	RFC 791
downstream	Towards the data receiver(s).	RFC 2205
DstPort	The IP (generalized) destination port used as part of a session. See "generalized destination port".	RFC 2205
edge node	The source node or the destination node of a call in a particular rerouting domain.	af-cs-0173.000

Terms	Definition	Source document
effective maximum frame payload size for labeled packets	This is either the Conventional Maximum Frame Payload Size or the True Maximum Frame Payload Size, depending on the capabilities of the equipment on the data link and the size of the data link header being used.	RFC 3032
Element Management System (EMS)	A terminal, network element, or system that provides specific services to manage specific Network Elements.	OIF-SMI-01.0
end system	A system on which connection termination points are located.	af-pnni-0055.002
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
entry policing	Traffic policing done at the first RSVP- (and policing-) capable router on a data path.	RFC 2205
Error_Spec	Object that carries the error report in a PathErr or ResvErr message.	RFC 2205
exception	A connectivity advertisement in a PNNI complex node representation that represents something other than the default node representation.	af-pnni-0055.002
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
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
explicitly routed LSP	An LSP whose path is established by a means other than normal IP routing.	RFC 3209
exterior	Denotes that an item (e.g., link, node, or reachable address) is outside of a PNNI routing domain.	af-pnni-0055.002
Exterior Gateway Protocol (EGP)	A protocol that distributes routing information to the gateways (routers) which connect autonomous systems. See "IGP".	RFC 1812
Exterior Gateway Protocol version 2 (EGP-2)	An EGP routing protocol developed to handle traffic between autonomous systems in the Internet.	RFC 1812
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
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
exterior route	A route which traverses an exterior link.	af-pnni-0055.002
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
Fixed Filter (FF) style	Fixed Filter reservation style, which has explicit sender selection and distinct attributes.	RFC 2205
flags	An Internet header field carrying various control flags.	RFC 791

Terms	Definition	Source document
flooding	The part of the OSPF protocol that distributes and synchronizes the link-state database between OSPF routers.	RFC 2328
flow descriptor	The combination of a flowspec and a filterspec.	RFC 2205
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
foreign address	An address or address prefix that does not match any of a given node's summary addresses.	af-pnni-0055.002
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 on another interface, or both.	RFC 1812
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
forwarding equivalence class	A group of IP packets which are forwarded in the same manner (e.g., over the same path, with the same forwarding treatment).	RFC 3031
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
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
fragment offset	This Internet header field indicates where in the Internet datagram a fragment belongs.	RFC 791
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
frame merge	Label merging, when it is applied to operation over frame-based media, so that the potential problem of cell interleave is not an issue.	RFC 3031
frame payload	The contents of a data link frame, excluding any data link layer headers or trailers. When a frame is carrying an unlabeled IP datagram, the Frame Payload is just the IP datagram itself. When a frame is carrying a labeled IP datagram, the Frame Payload consists of the label stack entries and the IP datagram.	RFC 3032
FT label	A label for which some fault tolerant operation is used.	RFC 3479

Terms	Definition	Source document
Gateway-to-Gateway Protocol (GGP)	The protocol used primarily between gateways to control routing and other gateway functions.	RFC 791
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
generalized destination port	The component of a session definition that provides further transport or application protocol layer demultiplexing beyond DestAddress. See "session".	RFC 2205
generalized source port	The component of a filter spec that provides further transport or application protocol layer demultiplexing beyond the sender address.	RFC 2205
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
header	Control information at the beginning of a message, segment, datagram, packet or block of data.	RFC 791
Hello Packet	A type of PNNI routing packet that is exchanged between neighbouring logical nodes.	af-pnni-0055.002
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
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
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
horizontal link	A link between two logical nodes that belong to the same peer group.	af-pnni-0055.002
host	Any node that is not a router.	RFC 2460
identification	An Internet header field carrying the identifying value assigned by the sender to aid in assembling the fragments of a datagram.	RFC 791
incarnation number	Identify the instance of a rerouting connection.	af-cs-0173.000
incoming interface	The interface on which data packets are expected to arrive, and on which Resv messages are sent.	RFC 2205
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

Terms	Definition	Source document
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
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
initial connection	The first incumbent connection (no rerouting operation has ever occurred).	af-cs-0173.000
initially labeled IP datagram	Suppose that an unlabeled IP datagram is received at a particular LSR, and that the LSR pushes on a label before forwarding the datagram. Such a datagram will be called an Initially Labeled IP Datagram at that LSR.	RFC 3032
inside link	Synonymous with horizontal link.	af-pnni-0055.002
instance ID	A subset of an object's attributes which serve to uniquely identify a MIB instance.	af-pnni-0055.002
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
inter-domain interface	An interface at the ingress or egress of a rerouting domain.	af-cs-0173.000
Inter-domain PNNI interface	A PNNI interface at the ingress or egress of a rerouting domain.	af-cs-0173.000
Inter-domain rerouting service	A rerouting service for a call across multiple rerouting domains.	af-cs-0173.000
interface (1)	A node's attachment to a link.	RFC 2460
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
interface IP address	The IP address and network prefix length that is assigned to a specific interface of a router.	RFC 1812
Interface Message Processor (IMP)	The packet switch of the ARPANET.	RFC 791
interior	Denotes that an item (e.g., link, node, or reachable address) is inside of a PNNI routing domain.	af-pnni-0055.002
Interior Gateway Protocol (IGP) (1)	The routing protocol spoken by the routers belonging to an autonomous system.	RFC 2328
Interior Gateway Protocol (IGP) (2)	A protocol that distributes routing information with an Autonomous System (AS). See "EGP".	RFC 1812
Internet Header Length (IHL)	The length of the Internet header measured in 32 bit words.	RFC 791
internal reachable ad	An address of a destination that is directly attached to the logical node advertising the address.	af-pnni-0055.002

Terms	Definition	Source document
Internet Address (1)	A four-octet (32-bit) source or destination address consisting of a Network field and a Local Address field.	RFC 791
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
Internet Control Message Protocol (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
Internet datagram	The unit of data exchanged between a pair of Internet modules (includes the Internet header).	RFC 791
Internet fragment	A portion of the data of an Internet datagram with an Internet header.	RFC 791
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 is no end-to-end of hop-by-hop acknowledgments.	RFC 1812
intra-domain interface	An interface within a rerouting domain.	af-cs-0173.000
intra-domain rerouting service	A rerouting service for a call within a rerouting domain.	af-cs-0173.000
IP control channel	The communication channel over which IP packets are transported between two devices.	OIF-UNI-01.0
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
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
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
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.	RFC 2205
label	A short fixed-length physically contiguous identifier which is used to identify a FEC, usually of local significance.	RFC 3031

Terms	Definition	Source document
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
label merging	The replacement of multiple incoming labels for a particular FEC with a single outgoing label	RFC 3031
label stack	An ordered set of labels.	RFC 3031
label swap	The basic forwarding operation consisting of looking up an incoming label to determine the outgoing label, encapsulation, port, and other data handling information.	RFC 3031
label swapping	A forwarding paradigm allowing streamlined forwarding of data by using labels to identify classes of data packets which are treated indistinguishably when forwarding.	RFC 3031
label switched hop	The hop between two MPLS nodes, on which forwarding is done using labels.	RFC 3031
Label Switched Path (LSP)	The path through one or more LSRs at one level of the hierarchy followed by a packets in a particular FEC.	RFC 3031
label switching router	An MPLS node which is capable of forwarding native L3 packets.	RFC 3031
layer 2	The protocol layer under layer 3 (which therefore offers the services used by layer 3). Forwarding, when done by the swapping of short fixed length labels, occurs at layer 2 regardless of whether the label being examined is an ATM VPI/VCI, a frame relay DLCI, or an MPLS label.	RFC 3031
layer 3	The protocol layer at which IP and its associated routing protocols operate link layer synonymous with layer 2.	RFC 3031
LDP FT enhancements	The extensions to LDP.	RFC 3479
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
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
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
link (2)	Synonymous with logical link.	af-pnni-0055.002
link (3)	Aggregation token. See "aggregation token".	af-pnni-0055.002

Terms	Definition	Source document
\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
link constraint	A restriction on the use of links for path selection for a specific connection.	af-pnni-0055.002
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
link MTU	The maximum transmission unit, i.e., maximum packet size in octets, that can be conveyed over a link.	RFC 2460
link property correlation	A procedure to correlate the local and remote properties of a TE link.	RFC 4204
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 form the protocol's link state database. Throughout this memo, link state advertisement is abbreviated as LSA.	RFC 2328
link state parameter	Information that captures an aspect or property of a link.	af-pnni-0055.002
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
local repair	Local repair allows RSVP to rapidly adapt its reservations to changes in routing.	RFC 2205
logical group node	An abstract representation of a lower level peer group as a single point.	af-pnni-0055.002
logical (network) interface	A logical path, distinguished by a unique IP address, to a connected network.	RFC 1812
Logical Interface Handle (LIH)	The LIH is used to help deal with non-RSVP clouds.	RFC 2205
logical link	An abstract representation of the connectivity between two logical nodes.	af-pnni-0055.002
logical node	A lowest-level node or a logical group node.	af-pnni-0055.002
logical node ID	A string of bits that unambiguously identifies a logical node within a routing domain.	af-pnni-0055.002
loop detection	A method of dealing with loops in which loops are allowed to be set up, and data may be transmitted over the loop, but the loop is later detected.	RFC 3031
loop prevention	A method of dealing with loops in which data is never transmitted over a loop.	RFC 3031
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

Terms	Definition	Source document
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
Local Policy Module (LPM)	The function that exerts policy control.	RFC 2205
LSP tunnel	An LSP which is used to tunnel below normal IP routing and/or filtering mechanisms.	RFC 3209
management system	A generic term for an EMS or NMS.	OIF-SMI-01.0
martian filtering	A packet that contains an invalid source or destination address is considered to be martian and discarded.	RFC 1812
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
membership scope	The level of routing hierarchy within which advertisement of a given address is constrained.	af-pnni-0055.002
merge point	A node at which label merging is done.	RFC 3031
merge policing	Traffic policing that takes place at data merge point of a shared reservation.	RFC 2205
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.	RFC 2205
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
MIB instance	An incarnation of a MIB object that applies to a specific part, piece, or aspect of the PNNI protocol's operation.	af-pnni-0055.002
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
module	An implementation, usually in software, of a protocol or other procedure.	RFC 791
More-Fragments (MF) 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
MPLS domain	A contiguous set of nodes which operate MPLS routing and forwarding and which are also in one Routing or Administrative Domain.	RFC 3031
MPLS edge node	An MPLS node that connects an MPLS domain with a node which is outside of the domain, either because it does not run MPLS, and/or because it is in a different domain. Note that if an LSR has a neighbouring host which is not running MPLS, that LSR is an MPLS edge node.	RFC 3031
MPLS egress node	An MPLS edge node in its role in handling traffic as it leaves an MPLS domain.	RFC 3031

Terms	Definition	Source document
MPLS ingress node	An MPLS edge node in its role in handling traffic as it enters an MPLS domain	RFC 3031
MPLS label	A label which is carried in a packet header, and which represents the packet's FEC	RFC 3031
MPLS node	A node which is running MPLS. An MPLS node will be aware of MPLS control protocols, will operate one or more L3 routing protocols, and will be capable of forwarding packets based on labels. An MPLS node may optionally be also capable of forwarding native L3 packets.	RFC 3031
multicast	A packet that is destined for multiple hosts. See "broadcast".	RFC 1812
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
multiplex capability	The ability to multiplex/demultiplex a data stream into sub-rate streams for switching purposes.	RFC 4204
MultiProtocol Label Switching	An IETF working group and the effort associated with the working group.	RFC 3031
native address	An address or address prefix that matches one of a given node's summary addresses.	af-pnni-0055.002
neighbour node	A node that is directly connected to a particular node via a logical link.	af-pnni-0055.002
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
neighbours	Nodes attached to the same link.	RFC 2460
network	An IP network/subnet/supernet. It is possible for one physical network to be assigned multiple IP network/subnet numbers.	RFC 2328
Network Administrator (NA)	A person who is authorized to use a Management System.	OIF-SMI-01.0
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.	OIF-SMI-01.0
network layer	Synonymous with layer 3.	RFC 3031
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.	OIF-SMI-01.0
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.	RFC 2328
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

Terms	Definition	Source document
next hop	The next router in the direction of traffic flow.	RFC 2205
NHOP	An object that carries the Next Hop information in RSVP control messages.	RFC 2205
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
nodal constraint	A restriction on the use of nodes for path selection for a specific connection.	af-pnni-0055.002
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
nodal state parameter	Information that captures an aspect or property of a node.	af-pnni-0055.002
node (1)	A device that implements IPv6.	RFC 2460
node (2)	A router or host system.	RFC 2205
node (3)	Synonymous with logical node.	af-pnni-0055.002
Node_Id	For a node running OSPF, the LMP Node_Id is the same as the address contained in the OSPF Router Address TLV. For a node running IS-IS and advertising the TE Router ID TLV, the Node_Id is the same as the advertised Router ID.	RFC 4204
non-branching node	A node that cannot currently support additional branching points for point-to-multipoint calls.	af-pnni-0055.002
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
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.	RFC 2205
nucleus	The interior reference point of a logical node in the PNNI complex node representation.	af-pnni-0055.002
null	A value of all zeros.	af-pnni-0055.002
Number of Fragment Blocks (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
object	An element of an RSVP control message; a type, length, value triplet.	RFC 2205
octet	An eight-bit byte.	RFC 791
One Pass With Advertising (OPWA)	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

Terms	Definition	Source document
opaque	A device is called X-opaque if it examines or modifies the X aspect of the signal while forwarding an incoming signal from input to output.	RFC 4209
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
options	The Internet header Options field may contain several options, and each option may be several octets in length.	RFC 791
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
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
outgoing interface	Interface through which data packets and Path messages are forwarded.	RFC 2205
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
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
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
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
packet (1)	An IPv6 header plus payload.	RFC 2460

Terms	Definition	Source document
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
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
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
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
padding	The Internet header Padding field is used to ensure that the data begins on 32-bit word boundary. The padding is zero.	RFC 791
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
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
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
path constraint	A bound on the combined value of a topology metric along a path for a specific connection.	af-pnni-0055.002
path scope	The highest level of PNNI hierarchy used by a path.	af-pnni-0055.002
path state	Information kept in routers and hosts about all RSVP senders.	RFC 2205
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
PathErr	Path Error RSVP control message.	RFC 2205
PathTear	Path Teardown RSVP control message.	RFC 2205
peer	The other end of the point-to-point link.	RFC 1661
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

Terms	Definition	Source document
peer group identifier	A string of bits that is used to unambiguously identify a peer group.	af-pnni-0055.002
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
peer group level	The number of significant bits in the peer group identifier of a particular peer group.	af-pnni-0055.002
peer node	A node that is a member of the same peer group as a given node.	af-pnni-0055.002
PHOP	An object that carries the Previous Hop information in RSVP control messages.	RFC 2205
physical link	A real link which attaches two switching systems.	af-pnni-0055.002
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
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
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
PNNI routing control channel	VCCs used for the exchange of PNNI routing protocol messages.	af-pnni-0055.002
PNNI routing domain	A group of topologically contiguous systems which are running one instance of PNNI routing.	af-pnni-0055.002
PNNI routing hierarchy	The hierarchy of peer groups used for PNNI routing.	af-pnni-0055.002
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
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
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
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
police	See "traffic policing".	RFC 2205
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

Terms	Definition	Source document
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
port (1)	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
port (2)	The point of attachment of a link to a node.	af-pnni-0055.002
port (3)	An interface that terminates a data link.	RFC 4204
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
previous hop	The previous router in the direction of traffic flow. Resv messages flow towards previous hops.	RFC 2205
previously labeled IP datagram	An IP datagram which had already been labeled before it was received by a particular LSR.	RFC 3032
protocol	In this document, the next higher level protocol identifier, an Internet header field.	RFC 791
protocol ID	The component of session identification that specifies the IP protocol number used by the data stream.	RFC 2205
QoS	Quality of Service.	RFC 2205
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
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
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 behavior.	af-pnni-0055.002
rendez-vous node	A node that terminates the rerouting request for an alternative connection segment	af-cs-0173.000
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

Terms	Definition	Source document
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
rerouting node	A node that initiates the establishment of an alternate connection segment to a predetermined rendez-vous node.	af-cs-0173.000
reservation state	Information kept in RSVP-capable nodes about successful RSVP reservation requests.	RFC 2205
reservation style	Describes a set of attributes for a reservation, including the sharing attributes and sender selection attributes.	RFC 2205
rest	The local address portion of an Internet Address.	RFC 791
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
Resv message	Reservation request RSVP control message.	RFC 2205
ResvConf	Reservation Confirmation RSVP control message, confirms successful installation of a reservation at some upstream node.	RFC 2205
ResvErr	Reservation Error control message, indicates that a reservation request has failed or an active reservation has been pre-empted.	RFC 2205
ResvTear	Reservation Teardown RSVP control message, deletes reservation state.	RFC 2205
Reverse Path Forwarding (RPF)	A method used to deduce the next hops for broadcast and multicast packets.	RFC 1812
router (1)	A node that forwards IPv6 packets not explicitly addressed to itself.	RFC 2460
router (2)	A level three Internet Protocol packet switch. Formerly called a gateway in much of the IP literature.	RFC 2328
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
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

Terms	Definition	Source document
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
routing constraint	A generic term that refers to either a topology constraint or a path constraint.	af-pnni-0055.002
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
RSVP_HOP	Object of an RSVP control message that carries the PHOP or NHOP address of the source of the message.	RFC 2205
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
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
scope (1)	The set of sender hosts to which a given reservation request is to be propagated.	RFC 2205
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
SE style	Shared explicit reservation style, which has explicit sender selection and shared attributes.	RFC 2205
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
sender template	Parameter in a Path message that defines a sender; carried in a SENDER_TEMPLATE object. It has the form of a filter spec that can be used to select this sender's packets from other packets in the same session on the same link.	RFC 2205
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
sequence numbered FT label	An FT label which is secured using the sequence number in the FT Protection TLV.	RFC 3479
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.	OIF-UNI-01.0
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
shared style	A (reservation) style attribute: all reserved senders share the same reserved resources. See also "distinct style".	RFC 2205
signal type	A SDH/SONET signal type, such as STS-1.	OIF-UNI-01.0

Terms	Definition	Source document
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
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 as a result. However, for diagnosis of problems, the router 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 1812
silently ignore	A router is said to silently ignore an error or condition if it asks 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
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
soft state	Control state in hosts and routers that will expire if not refreshed within a specified amount of time.	RFC 2205
source	The source address, an Internet header field.	RFC 791
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
source route	As used in this document, a hierarchically complete source route.	af-pnni-0055.002
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 no part of the network wants the data. See "dense mode".	RFC 1812
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
split system	A switching system which implements the functions of more than one logical node.	af-pnni-0055.002
spoke	In the complex node representation, this represents the connectivity between the nucleus and a specific port.	af-pnni-0055.002
stack	Synonymous with label stack.	RFC 3031
style	Object of an RSVP message that specifies the desired reservation style.	RFC 2205

Terms	Definition	Source document
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
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
sub-TLVs	Similar to regular TLVs. They use the same concepts as regular TLVs. The difference is that TLVs exist inside IS-IS packets, while sub-TLVs exist inside TLVs. TLVs are used to add extra information to IS-IS packets. Sub-TLVs are used to add extra information to particular TLVs.	RFC 3784
summary address	An address prefix that tells a node how to summarize reachability information.	af-pnni-0055.002
switched path	Synonymous with label switched path.	RFC 3031
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
TCP segment	The unit of data exchanged between TCP modules (including the TCP header).	RFC 791
Time to Live (TTL) (1)	An Internet header field which indicates the upper bound on how long this Internet datagram may exist.	RFC 791
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
TIME_VALUES	Object in an RSVP control message that specifies the time period timer used for refreshing the state in this message.	RFC 2205
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
topology attribute	A generic term that refers to either a link attribute or a nodal attribute.	af-pnni-0055.002
topology constraint	A topology constraint is a generic term that refers to either a link constraint or a nodal constraint.	af-pnni-0055.002
topology database	The database that describes the topology of the entire PNNI routing domain as seen by a node.	af-pnni-0055.002
topology metric	A generic term that refers to either a link metric or a nodal metric.	af-pnni-0055.002
topology state parameter	A generic term that refers to either a link parameter or a nodal parameter.	af-pnni-0055.002
total length	The Internet header field Total Length is the length of the datagram in octets including Internet header and data.	RFC 791

Terms	Definition	Source document
trace destination interface	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
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
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
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
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
Traffic Engineered Tunnel (TE Tunnel)	A set of one or more LSP Tunnels which carries a traffic trunk.	RFC 3209
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
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
Transmission Control Protocol (TCP)	A host-to-host protocol for reliable communication in Internet environments.	RFC 791
transparent	A device is called X-transparent if it forwards incoming signals from input to output without examining or modifying the X aspect of the signal.	RFC 4204

Terms	Definition	Source document
transport network address	Address of an entity (e.g., a TNE) within the transport network.	OIF-UNI-01.0
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
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
Trivial File Transfer Protocol (TFTP)	A simple file transfer protocol built on UDP.	RFC 791
true maximum frame payload size	The maximum size frame payload which can be sent and received properly by the interface hardware attached to the data link.	RFC 3032
TSpec	A traffic parameter set that describes a flow. The format of a Tspec is opaque to RSVP.	RFC 2205
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
User Datagram Protocol (UDP)	A user-level protocol for transaction-oriented applications.	RFC 791
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.	RFC 2205
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
UNI-C	The logical entity that terminates UNI signalling on the client device side.	OIF-UNI-01.0
UNI-N	The logical entity that terminates UNI signalling on the transport network side.	OIF-UNI-01.0
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
uplink	Represents the connectivity from a border node to an upnode.	af-pnni-0055.002
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
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
upstream	Towards the traffic source. RSVP Resv messages flow upstream.	RFC 2205
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

Terms	Definition	Source document
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
VC merge	Label merging where the MPLS label is carried in the ATM VCI field (or combined VPI/VCI field), so as to allow multiple VCs to merge into one single VC.	RFC 3031
virtual circuit	A circuit used by a connection-oriented layer 2 technology such as ATM or Frame Relay, requiring the maintenance of state information in layer 2 switches.	RFC 3031
VP merge	Label merging where the MPLS label is carried in the ATM VPI field, so as to allow multiple VPs to be merged into one single VP. In this case two cells would have the same VCI value only if they originated from the same node. This allows cells from different sources to be distinguished via the VCI.	RFC 3031
VPI/VCI	A label used in ATM networks to identify circuits	RFC 3031
WF style	Wildcard Filter reservation style, which has wildcard sender selection and shared attributes.	RFC 2205
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 table 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
AD	Administrative Domain	RFC 2753
AFI	Authority and Format Identifier (the first octet of all OSI NSAP addresses – identifies format of the rest of the address)	RFC 1195
AS	Autonomous System	RFC 3945
ASP	ATM Service Provider	af-pnni-0055.002
ATC	ATM Transfer Capability	af-pnni-0055.002
AW	Administrative Weight	af-pnni-0055.002
BGP	Border Gateway Protocol	af-pnni-0055.002
CA	Certification Authority	OIF-SMI-01.0
CAC	Connection Admission Control	af-pnni-0055.002
CBC	Cipher Block Chaining	OIF-SMI-01.0

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
COA	Connection Available	af-cs-0148.000
CO-BI	Connection-Oriented Bearer-Independent	af-cs-0141.000
COPS	Common Open Policy Service	RFC 2749
CR-LDP	Constraint-based Routing LDP	RFC 3945
CR-LSP	Constraint-based Router Label Switched Path	RFC 3212
CRM	Cell Rate Margin	af-pnni-0055.002
CSPF	Constraint-based Shortest Path First	RFC 3945
DCC	Data Communication Channel	OIF-UNI-01.0
DFI	DSP Format Identifier	RFC 1195
DLCI	Data Link Connection Identifier	af-cs-0141.000
DSP	Domain Specific Part	af-pnni-0055.002
DSS	Digital Signature Standard	OIF-SMI-01.0
DTL	Designated Transit List	af-pnni-0055.002
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	OIF-SMI-01.0
FA	Forwarding Adjacency	RFC 3945
FEC	Forwarding Equivalence Class	RFC 4201
FSC	Fibre-Switch Capable	RFC 4202
FRTT	Fixed Round Trip Time	af-cs-0173.000
FTN	FEC to NHLFE Map	RFC 4201
GCAC	Generic Connection Admission Control	af-pnni-0055.002
GFR	Guaranteed Frame Rate	af-cs-0173.000
GLB	Greatest Lower Bound	RFC 2205
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	OIF-SMI-01.0
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
IGP	Interior Gateway Protocol	RFC 4201

IISP	Interim Inter-switch Signalling Protocol	af-cs-0141.000
IKE	Internet Key Exchange	OIF-SMI-01.0
ILM	Incoming Label Map	RFC 4201
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	OIF-SMI-01.0
IPCC	IP Control Channel	OIF-UNI-01.0
Ipsec	IP Security	OIF-SMI-01.0
IS	Intermediate System (the OSI term for a router)	RFC 1195
ISH	An 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 Routeing Exchange Protocol (the ISO protocol for routing within a single routing domain)	RFC 1195
IS-IS Hello	An Hello packet defined by the IS-IS protocol (a type of packet used by the IS-IS protocol)	RFC 1195
L2	Layer 2	RFC 4201
L2SC	Layer-2 Switch Capable	RFC 4202
L3	Layer 3	RFC 4201
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
LSA	Link State Advertisement	RFC 3945
LSC	Lambda Switch Capable	RFC 4201
LSP (1)	Link State Packet (a type of packet used by the IS-IS protocol)	RFC 1195
LSP (2)	Label Switched Path	RFC 3945
LSR	Label Switching Router	RFC 4201
LTE	Line Terminating Equipment	OIF-UNI-01.0
LUB	Least Upper Bound	RFC 2205
MAC	Message Authentication Code	OIF-SMI-01.0
maxCR	Maximum Cell Rate	af-pnni-0055.002
maxCTD	Maximum Cell Transfer Delay	af-pnni-0055.002
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
NCCI	Network Call Correlation Identifier	af-cs-0173.000
ND	Neighbour Discovery	OIF-UNI-01.0
NHLFE	Next Hop Label Forwarding Entry	RFC 4201

NLPID	Network Layer Protocol ID (a one-octet field identifying a network layer protocol)	RFC 1195
NNI	Network-to-Network Interface	af-pnni-0055.002
Non-FT	Not fault tolerant	RFC 3479
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
OSPF	Open Shortest Path First	af-pnni-0055.002
OXC	Optical Cross-Connect	RFC 3945
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
PSC	Packet Switch Capable	RFC 4201
PTSE	PNNI Topology State Element	af-pnni-0055.002
PTSP	PNNI Topology State Packet	af-pnni-0055.002
PVCC	Permanent Virtual Channel Connection	af-pnni-0055.002
PXC	Photonic Cross-Connect	RFC 3945
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
RIF	Rate Increase Factor	af-pnni-0055.002
RM	Resource Management	af-cs-0173.00
RSVP	Resource reSerVation Protocol	OIF-UNI-01.0
RSVP-TE	RSVP with Traffic Engineering extensions	OIF-UNI-01.0
SAAL	Signalling ATM Adaptation Layer	af-pnni-0055.002
SCR	Sustainable Cell Rate	af-pnni-0055.002
SEL	NSAP Selector (the last octet of NSAP addresses, also called NSEL)	RFC 1195
SHA	Secure Hash Algorithm	OIF-SMI-01.0
S/MIME	Secure Multipurpose Internet Mail Extensions	OIF-SMI-01.0
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	OIF-SMI-01.0
SPF	Shortest Path First	RFC 4202
SSCOP	Service Specific Connection Oriented Protocol	af-pnni-0055.002
SSCS	Service Specific Convergence Sublayer	af-pnni-0055.002
SSH	Secure Shell	OIF-SMI-01.0
SSL	Secure Sockets Layer	OIF-SMI-01.0
STE	Section Terminating Equipment	OIF-UNI-01.0
SVC (1)	Switched Virtual Connection	af-pnni-0055.002
SVC (2)	Switched Virtual Circuit	af-cs-0173.000
SVCC	Switched Virtual Channel Connection	af-pnni-0055.002
SVP	Switched Virtual Path	RFC 4201
SVPC	Switched Virtual Path Connection	af-pnni-0055.002
TAS	Transported Address Stack	af-cs-0173.000
TBE	Transit Buffer Exposure	af-pnni-0055.002
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
TE	Traffic Engineering	RFC 3945
TLV (1)	Type Length Value	af-cs-0173.000
TLV (2)	Type-Length-Value encoding	OIF-UNI-01.0
TTL (1)	Time-To-Live	RFC 4201
TTL (2)	Trace Transit List	af-cs-0141.000
UBR	Unspecified Bit Rate	af-pnni-0055.002
UDP	User Datagram Protocol	OIF-SMI-01.0
ULIA	Uplink Information Attribute	af-pnni-0055.002
UNI	User to Network Interface	af-cs-0173.000
UNI- N	UNI Signalling Agent – Network	OIF-UNI-01.0
UNI-C	UNI Signalling Agent – Client	OIF-UNI-01.0
VC	Virtual Circuit	RFC 4201
VCC	Virtual Channel Connection	af-pnni-0055.002
VCI	Virtual Channel Identifier	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
VPI	Virtual Path Identifier	af-pnni-0055.002

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 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	Telecommunication management, including TMN and network maintenance
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, open system communications and security
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, 2006