ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.8081/Y.1353

(09/2010)

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

Packet over Transport aspects – Ethernet over Transport 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)

Recommendation ITU-T G.8081/Y.1353

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS 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
MULTIMEDIA 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
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
Ethernet over Transport aspects	**G.8000–G.8099**
MPLS over Transport aspects	G.8100–G.8199
Quality and availability targets	G.8200–G.8299
Service Management	G.8600–G.8699
ACCESS NETWORKS	G.9000–G.9999

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

Recommendation ITU-T G.8081/Y.1353

Terms and definitions for Automatically Switched Optical Networks (ASON)

Summary

Recommendation ITU-T G.8081/Y.1353 provides terms, definitions, and abbreviations used in automatically switched optical network (ASON) Recommendations. It contains a list of the definitions and abbreviations introduced in Recommendations associated with Automatically Switched Optical Networks, and can be considered a companion document to Recommendations ITU-T G.780/Y.1351 and ITU-T G.870/Y.1352. The goal of this Recommendation is to be a single normative source for terms in this subject area.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.8081/Y.1353	2004-06-13	15
1.1	ITU-T G.8081/Y.1353 (2004) Amend. 1	2006-06-06	15
1.2	ITU-T G.8081/Y.1353 (2004) Amend. 2	2007-07-29	15
2.0	ITU-T G.8081/Y.1353	2008-03-29	15
3.0	ITU-T G.8081/Y.1353	2010-09-22	15

Keywords

Acronyms, automatically switched optical network (ASON), terminology, terms.

CONTENTS

Page

Recommendation ITU-T G.8081/Y.1353

Terms and definitions for Automatically Switched Optical Networks (ASON)

1 Scope

This Recommendation contains a complete listing of the terms, definitions, and abbreviations introduced in the Recommendations associated with automatically switched optical networks.

2 References

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

[ITU-T G.780]   Recommendation ITU-T G.780/Y.1351 (2008), *Terms and definitions for synchronous digital hierarchy (SDH) networks.*

[ITU-T G.800]   Recommendation ITU-T G.800 (2007), *Unified functional architecture of transport networks.*

[ITU-T G.805]   Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks.*

[ITU-T G.806]   Recommendation ITU-T G.806 (2009), *Characteristics of transport equipment – Description methodology and generic functionality.*

[ITU-T G.852.2]   Recommendation ITU-T G.852.2 (1999), *Enterprise viewpoint description of transport network resource model.*

[ITU-T G.870]   Recommendation ITU-T G.870/Y.1352 (2008), *Terms and definitions for optical transport networks (OTN).*

[ITU-T G.7712]   Recommendation ITU-T G.7712/Y.1703 (2008), *Architecture and specification of data communication network.*

[ITU-T G.7713]   Recommendation ITU-T G.7713/Y.1704 (2009), *Distributed call and connection management (DCM).*

[ITU-T G.7713.1]   Recommendation ITU-T G.7713.1/Y.1704.1 (2003), *Distributed Call and Connection Management (DCM) based on PNNI.*

[ITU-T G.7713.2]   Recommendation ITU-T G.7713.2/Y.1704.2 (2003), *Distributed Call and Connection Management: Signalling mechanism using GMPLS RSVP-TE.*

[ITU-T G.7713.3]   Recommendation ITU-T G.7713.3/Y.1704.3 (2003), *Distributed Call and Connection Management: Signalling mechanism using GMPLS CR-LDP.*

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

[ITU-T G.7714.1]   Recommendation ITU-T G.7714.1/Y.1705.1 (2010), *Protocol for automatic discovery in SDH and OTN networks.*

[ITU-T G.7715]   Recommendation ITU-T G.7715/Y.1706 (2002), *Architecture and requirements for routing in the automatically switched optical networks.*

[ITU-T G.7715.1]	Recommendation ITU-T G.7715.1/Y.1706.1 (2004), *ASON routing architecture and requirements for link state protocols*.
[ITU-T G.7715.2]	Recommendation ITU-T G.7715.2/Y.1706.2 (2007), *ASON routing architecture and requirements for remote route query*.
[ITU-T G.7716]	Recommendation ITU-T G.7716/Y.1707 (2010), *Architecture of control plane operations*.
[ITU-T G.8080]	Recommendation ITU-T G.8080/Y.1304 (2006), *Architecture for the automatically switched optical network (ASON)* and its amendments.
[ITU-T M.3010]	Recommendation ITU-T M.3010 (2000), *Principles for a telecommunications management network*.
[ITU-T M.3013]	Recommendation ITU-T M.3013 (2000), *Considerations for a telecommunications management network*.
[ITU-T M.3100]	Recommendation ITU-T M.3100 (2005), *Generic network information model*.
[ITU-T X.25]	Recommendation ITU-T 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 X.700]	Recommendation ITU-T X.700 (1992), *Management framework for Open Systems Interconnection (OSI) for CCITT applications*.
[ITU-T Y.1311]	Recommendation ITU-T Y.1311 (2002), *Network-based VPNs – Generic architecture and service requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere.

3.1.1 Terms defined in [ITU-T G.780]

– data communications channel (DCC)
– embedded control channel (ECC)
– layer
– network node interface (NNI)
– protection

3.1.2 Terms defined in [ITU-T G.805]

– access group (AG)
– access point (AP)
– administrative domain
– client-server relationship
– connection termination point (CTP)
   NOTE – [ITU-T G.805] uses the acronym TCP for this term.
– layer network
– link
– link connection

- management domain
- network connection
- partitioning
- port
- subnetwork connection
- trail
- trail termination
- transport
- transport network
- unidirectional access point
- unidirectional connection
- unidirectional connection point
- unidirectional port
- unidirectional trail

3.1.3 Terms defined in [ITU-T G.806]

- client/server layer
- continuity supervision
- management information (MI)
- management point (MP)

3.1.4 Terms defined in [ITU-T G.870]

- entity
- local craft terminal
- management communications
- optical channel (OCh)
- optical channel data unit (ODUk)
- optical channel transport unit (OTUk)
- OTN network element (O.NE)
- optical overhead signal (OOS)
- optical supervisory channel (OSC)
- optical transport network (OTN)
- optical transport network node interface (ONNI)
- restoration
- resource
- transport entity

3.1.5 Terms defined in [ITU-T G.7712]

- data communication network (DCN)
- dual interfaces
- signalling communication network (SCN)

3.1.6   Terms defined in [ITU-T M.3010]

–   data communication function (DCF)

–   mediation device (MD)

–   network element (NE)

–   network element function (NEF)

–   operations system (OS)

–   operations system function (OSF)

–   Q interface

–   q reference points

–   reference point (RP)

3.1.7   Terms defined in [ITU-T M.3013]

–   message communication function (MCF)

–   workstation function (WSF)

3.1.8   Terms defined in [ITU-T M.3100]

–   management interface

–   managed entity

3.1.9   Term defined in [ITU-T X.25]

–   closed user group

3.1.10   Term defined in [ITU-T X.700]

–   managed object (MO)

3.1.11   Term defined in [ITU-T Y.1311]

–   virtual private network (VPN)

3.2   Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1   access group container (AGC): An AGC is a single layer entity that contains access groups, link resource managers (LRMs), and termination and adaptation performers (TAPs). It is similar to subnetworks defined by [ITU-T G.805] except that it is not recursively defined, may or may not be a matrix (it does not have to be specified), and has no defined subnetwork connections. See [ITU-T G.8080].

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

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

3.2.4   allocated (resource) label range: An allocated (resource) label range is the set of labels that can be used by the adaptation function of a particular link to carry user traffic. It is a subset of the potential resource label range. The allocated labels are entities that can be referenced in the transport plane name space. Each allocated label is associated with one or multiple subnetwork point (SNP) IDs that exist in the control plane name space (1:n relationship). Termination and adaptation performers (TAPs) hold this binding information.

3.2.5   assigned SNPs: The assigned subnetwork points (SNPs) are those SNPs out of the set of potential SNPs that have been assigned to a particular connection. This means that the associated label corresponds to a configured label.

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

3.2.7   automatically switched optical network (ASON): An automatically switched transport network (ASTN) that is applied to connection oriented circuit or packet transport networks, as defined in [ITU-T G.805].

3.2.8   automatic switched transport network (ASTN): An ASTN is a transport network where configuration connection management is implemented by means of a control plane.

3.2.9   call: A call is 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.

3.2.10   call admission control: Call admission control is a policy function invoked by an originating role in a network and may involve cooperation with the terminating role in the network. See [ITU-T G.8080].

3.2.10.1   originating call admission function: The originating call admission function is responsible for checking that a valid called user name and parameters has been provided. See [ITU-T G.8080].

3.2.10.2   terminating call admission function: The terminating call admission function is responsible for checking that the called party is entitled to accept the call, based on the calling party and called party service contracts. See [ITU-T G.8080].

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

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

3.2.12.1   calling/called party call controller: The calling/called party call controller is associated with an end of a call and may be co-located with end systems or located remotely and acts as a proxy on behalf of end systems. This controller acts in one or both of two roles, one to support the calling party and the other to support the called party. See [ITU-T G.8080].

3.2.12.2   network call controller (NCC): 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. See [ITU-T G.8080].

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

3.2.13   call segment: A call segment is an association between two call control entities (as per Rec. ITU-T Q.2982, which is equivalent to [ITU-T G.8080] call controllers). Each call segment has zero or more associated connections. Call segments between network call control entities have zero or more supporting calls.

3.2.14 commissioning: The act of specifying parameters necessary to create a control plane instance. These parameters are fundamental to the continued operation of the control plane instance and cannot be changed without significant impact to the control plane instance. Therefore, commissioning is only done during the initialization phase of the control plane lifecycle. Note that commissioning is focused on the commissioning on the control plane component and not the data/transport plane resource.

3.2.15 component: A component is 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.

3.2.16 configured (resource) label: A configured (resource) label is a label that has been configured in the transport plane in support of a connection. For each configured label, a forwarding table entry exists on the receiving end of the link such that packets can be forwarded based on the label value of the received packet.

3.2.17 connection: A connection is a concatenation of link connections and subnetwork connections (as described in [ITU-T G.805]) that allows the transport of user information between the ingress and egress points of a subnetwork.

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

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

3.2.20 connection controller interface (CCI): A CCI is an interface between a subnetwork in the transport plane and the control plane. See [ITU-T G.8080].

3.2.21 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 G.805] the CP refers to the binding between two points.)

3.2.22 connection termination point (CTP): A connection termination point represents the signal state at the CP. Also see [ITU-T M.3100].

3.2.23 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.

3.2.24 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 set-up.

3.2.25 CR-LDP peers: Constraint-based routing label distribution protocol (CR-LDP) peers is two protocol controllers implementing CR-LDP that have established communication with each other.

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

3.2.27 discovery agent (DA): The "federation" of discovery agents operates in the transport plane name space, and provides for separation between that space and the control plane names. The federation has knowledge of connection points (CPs) and termination connection points (TCPs) in the network, while a local DA has knowledge of only those points assigned to it. See [ITU-T G.8080].

3.2.28 domain: A domain represents a collection of entities that are grouped for a particular purpose. See [ITU-T G.8080].

3.2.28.1 control domain: A control domain is 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.

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

3.2.28.3 rerouting domain: A rerouting domain is 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.

3.2.28.4 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 ITU-T G.805 administrative domain.

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

3.2.30 E-NNI: An E-NNI is a bidirectional interface between control plane entities belonging to different domains.

3.2.31 E-NNI transport resource name: The E-NNI SNPP link may be assigned a name for the network call controllers to specify E-NNIs. These names must be globally unique and are assigned by the automatically switched optical network (ASON). Multiple names may be assigned to the SNPP link. See [ITU-T G.8080].

3.2.32 federation: Federation is a community of domains that cooperates for the purposes of connection management, and is illustrated using the cooperation between connection controllers. See [ITU-T G.8080].

3.2.33 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.

3.2.34 hard rerouting service: A hard rerouting service offers a failure recovery mechanism for calls and is always in response to a failure event. See [ITU-T G.8080].

3.2.35 Hello: Hello is a message sent by a signalling protocol controller to advertise its presence to other signalling protocol controllers.

3.2.36 hierarchical routing: Hierarchical routing is 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 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 G.8080].

3.2.36.1 routing adjacency (RAdj): The RAdj is a logical association between two routing controllers.

3.2.36.2 source routing: Source routing is 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 versus source routing. In order to reduce the amount of network topology each controller needs to share, only that portion of the topology that applies to its own routing area is made available. See [ITU-T G.8080].

3.2.36.3 step-by-step routing: Step-by-step routing is 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 G.8080].

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

3.2.38 interface: In the context of this Recommendation, interfaces represent logical relationships between automatically switched optical network (ASON) 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.

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

3.2.40 label: This term is the same as an SNP.

3.2.41 link resource manager (LRM): A LRM is an architecture component. Two LRM components are used – the LRMA and LRMZ. The LRM components are responsible for the management of a subnetwork point pool (SNPP) link, including the allocation and un-allocation of subnetwork point (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. See [ITU-T G.8080].

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

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

3.2.44 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 M.3010] are performed in the management plane: performance management; fault management; configuration management; accounting management and security management.

3.2.45 multi-homed: A user is considered to be multi-homed when there are two or more subnetwork point pool (SNPP) links connecting the access group container to the network.

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

3.2.47 network-layer interworking function: A network-layer interworking function provides interoperability between nodes that support incompatible network-layer protocols.

3.2.48 node: In the context of this Recommendation, the term "node" is used to signify a subnetwork or a routing area.

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

3.2.50 permanent connection (PC): A PC is a connection type that is provisioned by manual action or via the management system.

3.2.51 policy: A policy is the set of rules applied to interfaces at the system boundary, which filter messages into an allowed set.

3.2.52 port controller: Port controller is a class of component that implements the set of rules applied to a system.

3.2.53 potential (resource) label range: A potential (resource) label range is the range of resource labels in the transport plane name space that an adaptation function supports to distinguish different information flows.

3.2.54 potential SNPs: Potential subnetwork points (SNPs) are those SNPs that are associated with a (resource) label.

3.2.55 protocol controller (PC): A PC is a component, which provides the function of mapping the parameters of the abstract interfaces of the control components into messages that are carried by a protocol to support interconnection via an interface. Protocol controllers are a sub-class of policy ports. See [ITU-T G.8080].

3.2.56 provisioning: The act of specifying the parameters necessary when assigning/deassigning network resources to/from the control plane or to invoke/remove services provided by a control plane instance. These parameters are specific to a resource or service request, causing changes to these parameters to only impact a specific resource or service request. Therefore, provisioning is allowed in the initialization and operations phases of the control plane lifecycle.

3.2.57 proxy call: A call in which the calling/called party call controller which is not coincident with the user interacts with the network call controller by means of a call protocol. See [ITU-T G.8080].

3.2.58 remote route query: A remote route query is an operation where a routing controller communicates with another routing controller, which does not have the same set of layer resources, in order to compute a routing path in a collaborative manner.

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

3.2.60 route: Route is a sequence of subnetwork point (SNP) names, subnetwork point pool (SNPP) names, routing area names, and/or transport resource identifiers that are used by the control plane to create a network connection.

3.2.61 route query requester: A route query requester is a connection controller or routing controller that sends a route query message to a routing controller requesting for one or more routing paths that satisfies a set of routing constraints.

3.2.62 route query responder: A route query responder is a routing controller that performs path computation upon reception of a route query message from a routing controller or connection controller, sending a response back at the end of computation.

3.2.63 routing: Routing is the control plane function used to select paths for the establishment of connections through one or more operator networks.

3.2.64 routing area (RA): 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. See [ITU-T G.8080].

3.2.65 routing controller (RC): The RC is 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 G.8080].

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

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

3.2.68 routing level: A routing level is a relationship between a routing area (RA) and a containing RA or contained RAs. The containment hierarchy of routing areas creates routing levels.

3.2.69 routing performer (RP): RP is a computational viewpoint object that is associated with a routing area and provides an abstraction of the routing service for the routing area.

3.2.70 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.

3.2.71 shared risk group (SRG): An SRG is a group of resources that share a common risk component whose failure can cause the failure of all the resources in the group.

3.2.72 SNPP alias: A subnetwork point pool (SNPP) alias is an alternate SNPP name for the same SNPP link that is generated from another SNPP name space. If present in a routing area, it is available to the routing controller (RC) that is associated with the routing area (RA).

3.2.73 SNP identifier: A subnetwork point (SNP) identifier is used for link connection assignment and, in some cases, routing. The SNP identifier is derived from the subnetwork point pool (SNPP) identifier concatenated with a locally significant SNP index. When the identifier is routable, it is an SNPP address. When it is not routable, the identifier is an SNP name.

3.2.74 SNPP identifier: A subnetwork point pool (SNPP) identifier is an instance of an identifier for an SNPP. When the identifier is routable, it is an SNPP address. When it is not routable, the identifier is an SNPP name. The constituents of an SNPP identifier may include routing area (RA) IDs, a subnetwork id and resource context identifiers. See [ITU-T G.8080].

3.2.75 soft permanent connection (SPC): An SPC is a user-to-user connection whereby the user-to-network portion of the end-to-end connection is established by the network management system as a permanent connection (PC). The network portion of the end-to-end connection is established as a switched connection using the control plane. In the network portion of the connection, requests for establishment of the connection are initiated by the management plane and set-up by the control plane.

3.2.76 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.

3.2.77 subnetwork: A subnetwork is 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.

3.2.78 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.

3.2.79 subnetwork point (SNP): The SNP is an abstraction that represents an actual or potential underlying connection point (CP) (or connection termination point (CTP)) or an actual or potential termination connection point (TCP) or trail termination point (TTP). Several SNPs (in different subnetwork partitions) may represent the same TCP or CP.

3.2.80 subnetwork point pool (SNPP): An SNPP is a set of subnetwork points that are grouped together for the purposes of routing. An SNP pool has a strong relationship to link ends (see [ITU-T G.852.2]).

3.2.81 subnetwork point pool link (SNPP link): An SNPP link is an association between SNPPs on different subnetworks.

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

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

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

3.2.85 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 G.805] the TCP refers to the binding between two points.)

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

3.2.87 trail termination point (TTP): A trail termination point represents the signal state at a TCP. Also see [ITU-T M.3100].

3.2.88 transitional SNPP link: A subnetwork point pool (SNPP) link with an SNPP in a subnetwork in one layer, and an SNPP in a subnetwork of a different layer. It may also be an SNPP link with an SNPP in a subnetwork in one sublayer and an SNPP in a subnetwork of a different sublayer, where both sublayers are in the same layer. See [ITU-T G.8080].

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

3.2.90 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.

3.2.91 user-network interface for the control plane (UNI): An UNI is a bidirectional signalling interface between service requester and service provider control plane entities.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

ACC-n   A-end CC at domain n

AD   Administrative Domain

AE-DCF   Automatic Encapsulating Data Communication Function

AESA   ATM End System Address

AG   Access Group

AGC   Access Group Container

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

ASON   Automatically Switched Optical Network

ASTN   Automatic Switched Transport Network

CAC   Call Admission Control

CallC   Call Controller

CC   Connection Controller

CC-a   A-end Connection Controller

CCC   Calling/Called Party Call Controller

CCC-a   A-end CCC

CCC-z   Z-end CCC

CCI   Connection Controller Interface

CC-z   Z-end Connection Controller

CoS   Class of Service

CP   Connection Point

CPS   Connection Point Status

CTP   Connection Termination Point

DA   Discovery Agent

DCM   Distributed Call and Connection Management

E-NNI   External Network-Network Interface (physical or logical reference point, based upon context)

GoS   Grade of Service

ID   Identifier

I-NNI	Internal Network-Network Interface (physical or logical reference point, based upon context)
LAD	Layer Adjacency Discovery
LAPD	Link Access Procedure D-channel
LCP	Link Control Protocol
LLCF	Link Layer Convergence Function
LRM	Link Resource Manager
LSP	Label Switched Path
LSPDU	Link State Protocol Data Unit
MI	Management Information
MO	Managed Object
MP	Management Plane
NC	Network Connection
NCC	Network Call Controller
NCCI	Network Call Correlation Identifier
NCC-n	NCC in domain n
NNI	Network-to-Network Interface or Network Node interface, based upon context
PC	Permanent Connection
PC	Protocol Controller
PNNI	Private Network-Network Interface
PPP	Point-to-Point Protocol
RA	Routing Area
RAdj	Routing Adjacency
RC	Routing Controller
RCD	Routing Control Domain
RDB	Routing Information Database
RI	Routing Information
RP	Routing Performer
SC	Switched Connection
SC-a	A-end user Signalling Controller
SC-z	Z-end user Signalling Controller
SLA	Service Level Agreement
SN	Subnetwork
SNCr	Subnetwork Controller
SNP	Subnetwork Point
SNPP	Subnetwork Point Pool
SPC	Soft Permanent Connection

SRG	Shared Risk Group
TAP	Termination and Adaptation Performer
TCC-n	Transit CC in domain n
TLV	Type, Length, Value
T-MPLS	Transport-MPLS
TSC-n	Transit Signalling Controller in domain n
TSN-n	Transit SN in domain n
UNI	User Network Interface (physical or logical reference point, based upon context)
UNI-C	Customer side of UNI
UNI-N	Network side of UNI
VPN	Virtual Private Network
ZSC-n	Z-end Signalling Controller in domain n
ZSN-n	Z-end SN in domain n

Appendix I

List of source Recommendations

(This appendix does not form an integral part of this Recommendation)

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

Recommendation ITU-T	Latest version
G.7713/Y.1704	05/2009
G.7713.1/Y.1704.1	03/2003
G.7713.2/Y.1704.2	03/2003
G.7713.3/Y.1704.3	03/2003
G.7714/Y.1705	08/2005
G.7714.1/Y.1705.1	06/2010
G.7715/Y.1706	06/2002
G.7715.1/Y.1706.1	02/2004
G.7715.2/Y.1706.2	02/2007
G.7716/Y.1707	01/2010
G.8080/Y.1304	06/2006

Appendix II

Related definitions found in documents from other organizations

(This appendix does not form an integral part of this Recommendation)

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

Term	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.	[b-IETF RFC 3209]
address	An IPv6-layer identifier for an interface or a set of interfaces.	[b-IETF RFC 2460]
address prefix	A string of zero or more bits up to a maximum of 152 bits that is the lead portion of one or more ATM addresses.	[b-BBF 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.	[b-IETF RFC 2328]
adjacency (2)	The relationship between two communicating neighbouring peer nodes.	[b-BBF 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".	[b-IETF RFC 2205]
Adspec	An Adspec is a data element (object) in a Path message that carries a package of OPWA advertising information. See "OPWA".	[b-IETF 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.	[b-BBF 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.	[b-BBF 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, ...).	[b-BBF af-pnni-0055.002]
ARPANET leader	The control information on an ARPANET message at the host-IMP interface.	[b-IETF 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).	[b-IETF RFC 791]

Term	Definition	Source document
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.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
Autonomous System (AS) (1)	A group of routers exchanging routing information via a common routing protocol. Abbreviated as AS.	[b-IETF 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.	[b-IETF 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.	[b-IETF 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.	[b-BBF af-cs-0173.000]
blockade state	Blockade state helps to solve a "killer reservation" problem. See "killer reservation".	[b-IETF 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.	[b-BBF 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".	[b-IETF RFC 2205]

Term	Definition	Source document
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.	[b-IETF RFC 2328]
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.	[b-IETF RFC 4201]
bypass	A bypass represents the connectivity between two ports in the complex node representation. A bypass is always an exception.	[b-BBF af-pnni-0055.002]
check-pointable FT label	An FT label which is secured by using the check-pointing techniques.	[b-IETF RFC 3479]
check-pointing	A process of message exchanges that confirm receipt and processing (or secure storage) of specific protocol messages.	[b-IETF RFC 3479]
Connection and LSP	"Connection" and "LSP" is interchangeable where the meaning is clear from the context.	[b-IETF RFC 4803]
cross-connect	The conceptual connection between a set of in-segments and out-segments.	[b-IETF RFC 4803]
C-type	The class type of an object; unique within class-name. See "class-name".	[b-IETF RFC 2205]
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.	[b-IETF RFC 4204]
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.	[b-IETF RFC 1661]

Term	Definition	Source document
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".	[b-IETF RFC 1812]
Dedicated LSP protection	Set if a protecting LSP does not allow sharing of the recovery resources nor the transport of extra-traffic (implying in the present context, duplication of the signal over both working and protecting LSPs as in 1+1 dedicated protection).	[b-IETF RFC 4872]
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.	[b-BBF 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.	[b-IETF RFC 1812]
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".	[b-IETF 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.	[b-IETF 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.	[b-BBF 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.	[b-BBF 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).	[b-BBF af-pnni-0055.002]
DestAddress	The IP destination address; part of session identification. See "session".	[b-IETF RFC 2205]
destination	The destination address, an Internet header field.	[b-IETF 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.	[b-BBF af-cs-0173.000]

Term	Definition	Source document
Dijkstra's algorithm	An algorithm that is sometimes used to calculate routes given a link and nodal state topology database.	[b-BBF af-pnni-0055.002]
distinct style	A (reservation) style attribute. Separate resources are reserved for each different sender. See also "shared style".	[b-IETF RFC 2205]
DLCI	A label used in Frame Relay networks to identify frame relay circuits.	[b-IETF RFC 3031]
domain	Synonymous with PNNI Routing Domain.	[b-BBF 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.	[b-BBF af-cs-0173.000]
Don't Fragment (DF)	The Don't Fragment bit carried in the flags field.	[b-IETF RFC 791]
downstream	Towards the data receiver(s).	[b-IETF RFC 2205]
DstPort	The IP (generalized) destination port used as part of a session. See "generalized destination port".	[b-IETF RFC 2205]
edge node	The source node or the destination node of a call in a particular rerouting domain.	[b-BBF af-cs-0173.000]
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.	[b-IETF RFC 3032]
Element Management System (EMS)	A terminal, network element, or system that provides specific services to manage specific Network Elements.	[b-OIF-SMI-01.0]
end system	A system on which connection termination points are located.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
entry policing	Traffic policing done at the first RSVP- (and policing-) capable router on a data path.	[b-IETF RFC 2205]
Error_Spec	Object that carries the error report in a PathErr or ResvErr message.	[b-IETF RFC 2205]
exception	A connectivity advertisement in a PNNI complex node representation that represents something other than the default node representation.	[b-BBF 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.	[b-BBF 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".	[b-IETF RFC 2205]

Term	Definition	Source document
explicitly routed LSP	An LSP whose path is established by a means other than normal IP routing.	[b-IETF RFC 3209]
explicitly routed LSP (ERLSP)	An explicitly routed LSP (ERLSP) is referred to as a GMPLS tunnel. It consists of in-segment(s) and/or out-segment(s) at the egress/ingress LSRs, each segment being associated with one GMPLS-enabled interface. These are also referred to as tunnel segments.	[b-IETF RFC 4802]
Extended Tunnel ID	A 32-bit (or 16-byte) identifier used in the SESSION that remains constant over the life of the tunnel.	[b-IETF RFC 4872]
exterior	Denotes that an item (e.g., link, node, or reachable address) is outside of a PNNI routing domain.	[b-BBF af-pnni-0055.002]
Exterior Gateway Protocol (EGP)	A protocol that distributes routing information to the gateways (routers) which connect autonomous systems. See "IGP".	[b-IETF RFC 1812]
Exterior Gateway Protocol version 2 (EGP-2)	An EGP routing protocol developed to handle traffic between autonomous systems in the Internet.	[b-IETF 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.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
exterior route	A route which traverses an exterior link.	[b-BBF 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.	[b-IETF RFC 2205]
Fixed Filter (FF) style	Fixed Filter reservation style, which has explicit sender selection and distinct attributes.	[b-IETF RFC 2205]
flags	An Internet header field carrying various control flags.	[b-IETF RFC 791]
flooding	The part of the OSPF protocol that distributes and synchronizes the link-state database between OSPF routers.	[b-IETF RFC 2328]
flow descriptor	The combination of a flowspec and a filterspec.	[b-IETF 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.	[b-IETF RFC 2205]
foreign address	An address or address prefix that does not match any of a given node's summary addresses.	[b-BBF af-pnni-0055.002]

Term	Definition	Source document
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.	[b-IETF 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.	[b-IETF 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).	[b-IETF 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.	[b-IETF 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.	[b-IETF RFC 1812]
fragment offset	This Internet header field indicates where in the Internet datagram a fragment belongs.	[b-IETF 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.	[b-IETF 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.	[b-IETF 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 labelled IP datagram, the Frame Payload consists of the label stack entries and the IP datagram.	[b-IETF RFC 3032]
FT label	A label for which some fault tolerant operation is used.	[b-IETF RFC 3479]
Full LSP rerouting	Set if a primary working LSP is dynamically recoverable using (non pre-planned) head-end rerouting.	[b-IETF RFC 4872]
Gateway-to-Gateway Protocol (GGP)	The protocol used primarily between gateways to control routing and other gateway functions.	[b-IETF RFC 791]

Term	Definition	Source document
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".	[b-IETF RFC 1812]
generalized destination port	The component of a session definition that provides further transport or application protocol layer demultiplexing beyond DestAddress. See "session".	[b-IETF RFC 2205]
generalized source port	The component of a filter spec that provides further transport or application protocol layer demultiplexing beyond the sender address.	[b-IETF 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).	[b-BBF af-cs-0173.000]
header	Control information at the beginning of a message, segment, datagram, packet or block of data.	[b-IETF RFC 791]
Hello Packet	A type of PNNI routing packet that is exchanged between neighbouring logical nodes.	[b-BBF 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.	[b-IETF 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.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
horizontal link	A link between two logical nodes that belong to the same peer group.	[b-BBF af-pnni-0055.002]
host	Any node that is not a router.	[b-IETF RFC 2460]
identification	An Internet header field carrying the identifying value assigned by the sender to aid in assembling the fragments of a datagram.	[b-IETF RFC 791]
IGP Area	OSPF area or IS-IS level	[b-IETF RFC 4972]
incarnation number	Identify the instance of a rerouting connection.	[b-BBF af-cs-0173.000]

Term	Definition	Source document
incoming interface	The interface on which data packets are expected to arrive, and on which Resv messages are sent.	[b-IETF 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.	[b-BBF af-cs-0173.000]
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.	[b-BBF 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.	[b-OIF-UNI-01.0]
initial connection	The first incumbent connection (no rerouting operation has ever occurred).	[b-BBF 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.	[b-IETF RFC 3032]
in-segment	This is analogous to a GMPLS Label on an interface.	[b-IETF RFC 4803]
inside link	Synonymous with horizontal link.	[b-BBF af-pnni-0055.002]
instance ID	A subset of an object's attributes which serve to uniquely identify a MIB instance.	[b-BBF 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.	[b-IETF RFC 2205]
Inter-area TE LSP	A TE LSP whose path transits across at least two different IGP areas.	[b-IETF RFC 4736]
Inter-AS MPLS TE LSP	A TE LSP whose path transits across at least two different Autonomous Systems (ASes) or sub-ASes (BGP confederations).	[b-IETF RFC 4736]
inter-domain interface	An interface at the ingress or egress of a rerouting domain.	[b-BBF af-cs-0173.000]
Inter-domain PNNI interface	A PNNI interface at the ingress or egress of a rerouting domain.	[b-BBF af-cs-0173.000]
Inter-domain rerouting service	A rerouting service for a call across multiple rerouting domains.	[b-BBF af-cs-0173.000]
interface (1)	A node's attachment to a link.	[b-IETF RFC 2460]

Term	Definition	Source document
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.	[b-IETF RFC 2328]
interface bounded Hello session	A Hello session in which local and remote addresses of the interface in question are used in the source and destination fields of the Hello packet, respectively.	[b-IETF RFC 4558]
interface IP address	The IP address and network prefix length that is assigned to a specific interface of a router.	[b-IETF RFC 1812]
Interface Message Processor (IMP)	The packet switch of the ARPANET.	[b-IETF RFC 791]
interior	Denotes that an item (e.g., link, node, or reachable address) is inside of a PNNI routing domain.	[b-BBF af-pnni-0055.002]
Interior Gateway Protocol (IGP) (1)	The routing protocol spoken by the routers belonging to an autonomous system.	[b-IETF RFC 2328]
Interior Gateway Protocol (IGP) (2)	A protocol that distributes routing information with an Autonomous System (AS). See "EGP".	[b-IETF RFC 1812]
internal reachable ad	An address of a destination that is directly attached to the logical node advertising the address.	[b-BBF af-pnni-0055.002]
Internet Address (1)	A four-octet (32-bit) source or destination address consisting of a Network field and a Local Address field.	[b-IETF 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.	[b-IETF 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.	[b-IETF RFC 791]
Internet datagram	The unit of data exchanged between a pair of Internet modules (includes the Internet header).	[b-IETF RFC 791]
Internet fragment	A portion of the data of an Internet datagram with an Internet header.	[b-IETF RFC 791]
Internet Header Length (IHL)	The length of the Internet header measured in 32 bit words.	[b-IETF RFC 791]
Internet Protocol (IP)	The network layer protocol for the Internet. It is a packet switching, datagram protocol defined in [b-IETF RFC 791]. IP does not provide a reliable communications facility; that is, there is no end-to-end of hop-by-hop acknowledgments.	[b-IETF RFC 1812]

Term	Definition	Source document
Intra-area TE LSP	A TE LSP whose path does not transit across areas.	[b-IETF RFC 4736]
intra-domain interface	An interface within a rerouting domain.	[b-BBF af-cs-0173.000]
intra-domain rerouting service	A rerouting service for a call within a rerouting domain.	[b-BBF af-cs-0173.000]
IP control channel	The communication channel over which IP packets are transported between two devices.	[b-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.	[b-IETF 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.	[b-IETF 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.	[b-IETF RFC 1812]
IPv4 (or IPv6) tunnel endpoint address	IPv4 (or IPv6) address of the egress node for the tunnel.	[b-IETF RFC 4872]
IPv4 (or IPv6) tunnel sender address	IPv4 (or IPv6) address for a sender node.	[b-IETF RFC 4872]
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.	[b-IETF RFC 2205]
label	A short fixed-length physically contiguous identifier which is used to identify a FEC, usually of local significance.	[b-IETF RFC 3031]
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.	[b-IETF RFC 3036]
label merging	The replacement of multiple incoming labels for a particular FEC with a single outgoing label	[b-IETF RFC 3031]
label stack	An ordered set of labels.	[b-IETF RFC 3031]

Term	Definition	Source document
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.	[b-IETF 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.	[b-IETF RFC 3031]
label switched hop	The hop between two MPLS nodes, on which forwarding is done using labels.	[b-IETF RFC 3031]
Label Switched Path (1)	A Label Switched Path (LSP) is modelled as a connection consisting of one or more incoming segments (in-segments) and/or one or more outgoing segments (out-segments) at an LSR.	[b-IETF RFC 4803]
Label Switched Path (2)	The path through one or more LSRs at one level of the hierarchy followed by a packets in a particular FEC.	[b-IETF RFC 3031]
label switching router	An MPLS node which is capable of forwarding native L3 packets.	[b-IETF 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.	[b-IETF RFC 3031]
layer 3	The protocol layer at which IP and its associated routing protocols operate link layer synonymous with layer 2.	[b-IETF RFC 3031]
LDP FT enhancements	The extensions to LDP.	[b-IETF 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.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
Li	Li is a logical control plane entity that is associated to a single data plane (abstract) node. The Li is identified by the TE Router_ID.	[b-IETF RFC 4652]

Term	Definition	Source document
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.	[b-IETF RFC 2460]
link (2)	Synonymous with logical link.	[b-BBF af-pnni-0055.002]
link (3)	Aggregation token. See "aggregation token".	[b-BBF af-pnni-0055.002]
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.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
link MTU	The maximum transmission unit, i.e., maximum packet size in octets, that can be conveyed over a link.	[b-IETF RFC 2460]
link property correlation	A procedure to correlate the local and remote properties of a TE link.	[b-IETF 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.	[b-IETF RFC 2328]
link state parameter	Information that captures an aspect or property of a link.	[b-BBF 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.	[b-IETF RFC 791]
Local Policy Module (LPM)	The function that exerts policy control.	[b-IETF RFC 2205]
local repair	Local repair allows RSVP to rapidly adapt its reservations to changes in routing.	[b-IETF RFC 2205]
logical (network) interface	A logical path, distinguished by a unique IP address, to a connected network.	[b-IETF RFC 1812]
logical group node	An abstract representation of a lower level peer group as a single point.	[b-BBF af-pnni-0055.002]
Logical Interface Handle (LIH)	The LIH is used to help deal with non-RSVP clouds.	[b-IETF RFC 2205]
logical link	An abstract representation of the connectivity between two logical nodes.	[b-BBF af-pnni-0055.002]

Term	Definition	Source document
logical node	A lowest-level node or a logical group node.	[b-BBF af-pnni-0055.002]
logical node ID	A string of bits that unambiguously identifies a logical node within a routing domain.	[b-BBF 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.	[b-IETF RFC 3031]
loop prevention	A method of dealing with loops in which data is never transmitted over a loop.	[b-IETF 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.	[b-IETF RFC 2328]
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.	[b-BBF af-pnni-0055.002]
LSP association	An object used to associate the working and protection LSPs.	[b-IETF RFC 4872]
LSP and Connection	"Connection" and "LSP" is interchangeable where the meaning is clear from the context.	[b-IETF RFC 4803]
LSP ID	A 16-bit identifier used in the SENDER_TEMPLATE and FILTER_SPEC that can be changed to allow a sender to share resources with itself. The LSP ID is used to differentiate LSPs that belong to the same LSP Tunnel (as identified by its Tunnel ID).	[b-IETF RFC 4872]
LSP protection with extra-traffic	Set if a protecting LSP is a dedicated primary LSP that allows for extra-traffic transport and thus precludes any sharing of the recovery resources between more than one <sender;receiver> pair. This type includes 1:N LSP protection with extra-traffic.	[b-IETF RFC 4872]
LSP tunnel	An LSP which is used to tunnel below normal IP routing and/or filtering mechanisms.	[b-IETF RFC 3209]
management system	A generic term for an EMS or NMS.	[b-OIF-SMI-01.0]
martian filtering	A packet that contains an invalid source or destination address is considered to be martian and discarded.	[b-IETF 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.	[b-IETF RFC 1812]
membership scope	The level of routing hierarchy within which advertisement of a given address is constrained.	[b-BBF af-pnni-0055.002]
merge point	A node at which label merging is done.	[b-IETF RFC 3031]

Term	Definition	Source document
merge policing	Traffic policing that takes place at data merge point of a shared reservation.	[b-IETF 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.	[b-IETF RFC 2205]
MIB attribute	A single piece of configuration, management, or statistical information which pertains to a specific part of the PNNI protocol operation.	[b-BBF 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.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
module	An implementation, usually in software, of a protocol or other procedure.	[b-IETF 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.	[b-IETF 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.	[b-IETF 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.	[b-IETF RFC 3031]
MPLS egress node	An MPLS edge node in its role in handling traffic as it leaves an MPLS domain.	[b-IETF RFC 3031]
MPLS ingress node	An MPLS edge node in its role in handling traffic as it enters an MPLS domain	[b-IETF RFC 3031]
MPLS label	A label which is carried in a packet header, and which represents the packet's FEC	[b-IETF 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.	[b-IETF RFC 3031]
multicast	A packet that is destined for multiple hosts. See "broadcast".	[b-IETF 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.	[b-IETF RFC 1812]

Term	Definition	Source document
multiplex capability	The ability to multiplex/demultiplex a data stream into sub-rate streams for switching purposes.	[b-IETF RFC 4204]
MultiProtocol Label Switching	An IETF working group and the effort associated with the working group.	[b-IETF RFC 3031]
native address	An address or address prefix that matches one of a given node's summary addresses.	[b-BBF af-pnni-0055.002]
neighbour node	A node that is directly connected to a particular node via a logical link.	[b-BBF 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.	[b-IETF RFC 2328]
neighbours	Nodes attached to the same link.	[b-IETF RFC 2460]
network	An IP network/subnet/supernet. It is possible for one physical network to be assigned multiple IP network/subnet numbers.	[b-IETF RFC 2328]
Network Administrator (NA)	A person who is authorized to use a Management System.	[b-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.	[b-OIF-SMI-01.0]
network layer	Synonymous with layer 3.	[b-IETF 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.	[b-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.	[b-IETF 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.	[b-IETF RFC 1812]
next hop	The next router in the direction of traffic flow.	[b-IETF RFC 2205]
NHOP	An object that carries the Next Hop information in RSVP control messages.	[b-IETF 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.	[b-BBF af-pnni-0055.002]
nodal constraint	A restriction on the use of nodes for path selection for a specific connection.	[b-BBF af-pnni-0055.002]

Term	Definition	Source document
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.	[b-BBF af-pnni-0055.002]
nodal state parameter	Information that captures an aspect or property of a node.	[b-BBF af-pnni-0055.002]
node (1)	A device that implements IPv6.	[b-IETF RFC 2460]
node (2)	A router or host system.	[b-IETF RFC 2205]
node (3)	Synonymous with logical node.	[b-BBF 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.	[b-IETF RFC 4204]
Node-ID based Hello Session	A Hello session in which local and remote Node-IDs are used in the source and destination fields of the Hello packet, respectively.	[b-IETF RFC 4558]
non-branching node	A node that cannot currently support additional branching points for point-to-multipoint calls.	[b-BBF 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.	[b-IETF 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.	[b-IETF RFC 2205]
nucleus	The interior reference point of a logical node in the PNNI complex node representation.	[b-BBF af-pnni-0055.002]
null	A value of all zeros.	[b-BBF 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.	[b-IETF RFC 791]
object	An element of an RSVP control message; a type, length, value triplet.	[b-IETF RFC 2205]
octet	An eight-bit byte.	[b-IETF 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".	[b-IETF RFC 2205]

Term	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.	[b-IETF RFC 4209]
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.	[b-IETF RFC 2328]
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.	[b-OIF-UNI-01.0]
options	The Internet header Options field may contain several options, and each option may be several octets in length.	[b-IETF 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.	[b-IETF RFC 1812]
outgoing interface	Interface through which data packets and Path messages are forwarded.	[b-IETF 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.	[b-BBF 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.	[b-OIF-UNI-01.0]

Term	Definition	Source document
out-segment	This is analogous to a GMPLS Label on an interface.	[b-IETF RFC 4803]
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.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
packet (1)	An IPv6 header plus payload.	[b-IETF RFC 2460]
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.	[b-IETF 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.	[b-IETF 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".	[b-IETF 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".	[b-IETF 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.	[b-IETF 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.	[b-BBF 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.	[b-BBF 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.	[b-IETF RFC 1812]

Term	Definition	Source document
path constraint	A bound on the combined value of a topology metric along a path for a specific connection.	[b-BBF af-pnni-0055.002]
path scope	The highest level of PNNI hierarchy used by a path.	[b-BBF af-pnni-0055.002]
path state	Information kept in routers and hosts about all RSVP senders.	[b-IETF 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.	[b-BBF af-cs-0141.000]
PathErr	Path Error RSVP control message.	[b-IETF RFC 2205]
PathTear	Path Teardown RSVP control message.	[b-IETF RFC 2205]
peer	The other end of the point-to-point link.	[b-IETF 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.	[b-BBF af-pnni-0055.002]
peer group identifier	A string of bits that is used to unambiguously identify a peer group.	[b-BBF 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.	[b-BBF af-pnni-0055.002]
peer group level	The number of significant bits in the peer group identifier of a particular peer group.	[b-BBF af-pnni-0055.002]
peer node	A node that is a member of the same peer group as a given node.	[b-BBF af-pnni-0055.002]
PHOP	An object that carries the Previous Hop information in RSVP control messages.	[b-IETF RFC 2205]
physical link	A real link which attaches two switching systems.	[b-BBF 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.	[b-IETF 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.	[b-IETF RFC 1812]
Pi	Pi is a physical (bearer/data/transport plane) node.	[b-IETF RFC 4652]

Term	Definition	Source document
PNNI protocol entity	The body of software in a switching system that executes the PNNI protocol and provides the routing service.	[b-BBF af-pnni-0055.002]
PNNI routing control channel	VCCs used for the exchange of PNNI routing protocol messages.	[b-BBF af-pnni-0055.002]
PNNI routing domain	A group of topologically contiguous systems which are running one instance of PNNI routing.	[b-BBF af-pnni-0055.002]
PNNI routing hierarchy	The hierarchy of peer groups used for PNNI routing.	[b-BBF 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.	[b-BBF 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.	[b-BBF 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".	[b-IETF RFC 1812]
point-to-point networks	A network that joins a single pair of routers. A 56 kbit/s serial line is an example of a point-to-point network.	[b-IETF RFC 2328]
police	See "traffic policing".	[b-IETF 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.	[b-IETF RFC 2205]
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.	[b-IETF 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.	[b-OIF-UNI-01.0]
port (2)	The point of attachment of a link to a node.	[b-BBF af-pnni-0055.002]
port (3)	An interface that terminates a data link.	[b-IETF RFC 4204]
port identifier	The identifier assigned by a logical node to represent the point of attachment of a link to that node.	[b-BBF af-pnni-0055.002]
pre-planned LSP rerouting without extra-traffic	Set if a protecting LSP is a secondary LSP that allows sharing of the pre-reserved recovery resources between one or more than one <sender;receiver> pair. When the secondary LSPs resources are not pre-reserved for a single <sender;receiver> pair, this type is referred to as "shared mesh" recovery	[b-IETF RFC 4872]
previous hop	The previous router in the direction of traffic flow. Resv messages flow towards previous hops.	[b-IETF RFC 2205]

Term	Definition	Source document
previously labelled IP datagram	An IP datagram which had already been labelled before it was received by a particular LSR.	[b-IETF RFC 3032]
protocol	In this document, the next higher level protocol identifier, an Internet header field.	[b-IETF RFC 791]
protocol ID	The component of session identification that specifies the IP protocol number used by the data stream.	[b-IETF RFC 2205]
QoS	Quality of Service.	[b-IETF RFC 2205]
reachable address prefix	A prefix on a 20-octet ATM address indicating that all addresses beginning with this prefix are reachable.	[b-BBF 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.	[b-BBF 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 behaviour.	[b-BBF af-pnni-0055.002]
recovery LSP/span	A recovery LSP/span is an LSP/span used to transport "normal" user traffic when the working LSP/span fails. Additionally, the recovery LSP/span may transport "extra" user traffic (i.e., pre-emptable traffic) when normal traffic is carried over the working LSP/span.	[b-IETF RFC 4427]
recovery path	The path by which traffic is restored after the occurrence of a fault. In other words, the path on which the traffic is directed by the recovery mechanism. The recovery path is established by MPLS means. The recovery path can either be an equivalent recovery path and ensure no reduction in quality of service, or be a limited recovery path and thereby not guarantee the same quality of service (or some other criteria of performance) as the working path. A limited recovery path is not expected to be used for an extended period of time. Synonyms for a recovery path are: back-up path, alternative path, and protection path.	[b-IETF RFC 3469]
rendez-vous node	A node that terminates the rerouting request for an alternative connection segment	[b-BBF af-cs-0173.000]

Term	Definition	Source document
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.	[b-BBF af-cs-0173.000]
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.	[b-BBF af-cs-0173.000]
rerouting node	A node that initiates the establishment of an alternate connection segment to a predetermined rendez-vous node.	[b-BBF af-cs-0173.000]
reservation state	Information kept in RSVP-capable nodes about successful RSVP reservation requests.	[b-IETF RFC 2205]
reservation style	Describes a set of attributes for a reservation, including the sharing attributes and sender selection attributes.	[b-IETF RFC 2205]
rest	The local address portion of an Internet Address.	[b-IETF 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.	[b-BBF af-pnni-0055.002]
Resv message	Reservation request RSVP control message.	[b-IETF RFC 2205]
ResvConf	Reservation Confirmation RSVP control message, confirms successful installation of a reservation at some upstream node.	[b-IETF RFC 2205]
ResvErr	Reservation Error control message, indicates that a reservation request has failed or an active reservation has been pre-empted.	[b-IETF RFC 2205]
ResvTear	Reservation Teardown RSVP control message, deletes reservation state.	[b-IETF RFC 2205]
Reverse Path Forwarding (RPF)	A method used to deduce the next hops for broadcast and multicast packets.	[b-IETF RFC 1812]
Ri	Ri is a logical control plane entity that is associated to a control plane "router". The latter is the source for topology information that it generates and shares with other control plane "routers". The Ri is identified by the (advertising) Router_ID	[b-IETF RFC 4652]
router (1)	A node that forwards IPv6 packets not explicitly addressed to itself.	[b-IETF RFC 2460]

Term	Definition	Source document
router (2)	A level three Internet Protocol packet switch. Formerly called a gateway in much of the IP literature.	[b-IETF 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	[b-IETF 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.	[b-IETF RFC 2328]
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.	[b-BBF af-pnni-0055.002]
routing constraint	A generic term that refers to either a topology constraint or a path constraint.	[b-BBF 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.	[b-IETF RFC 2205]
RSVP_HOP	Object of an RSVP control message that carries the PHOP or NHOP address of the source of the message.	[b-IETF 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).	[b-BBF 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).	[b-BBF af-cs-0141.000]
scope (1)	The set of sender hosts to which a given reservation request is to be propagated.	[b-IETF 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.	[b-BBF af-pnni-0055.002]
SE style	Shared explicit reservation style, which has explicit sender selection and shared attributes.	[b-IETF 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.	[b-IETF RFC 2205]

Term	Definition	Source document
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.	[b-IETF 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.	[b-IETF RFC 2205]
sequence numbered FT label	An FT label which is secured using the sequence number in the FT Protection TLV.	[b-IETF 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.	[b-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.	[b-IETF RFC 2205]
shared style	A (reservation) style attribute: all reserved senders share the same reserved resources. See also "distinct style".	[b-IETF RFC 2205]
signal type	A SDH/SONET signal type, such as STS-1.	[b-OIF-UNI-01.0]
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.	[b-IETF 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.	[b-IETF 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.	[b-IETF RFC 1812]

Term	Definition	Source document
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).	[b-BBF af-cs-0173.000]
soft state	Control state in hosts and routers that will expire if not refreshed within a specified amount of time.	[b-IETF RFC 2205]
source	The source address, an Internet header field.	[b-IETF 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.	[b-BBF af-cs-0173.000]
source route	As used in this document, a hierarchically complete source route.	[b-BBF 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".	[b-IETF 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.	[b-IETF RFC 1812]
split system	A switching system which implements the functions of more than one logical node.	[b-BBF af-pnni-0055.002]
spoke	In the complex node representation, this represents the connectivity between the nucleus and a specific port.	[b-BBF af-pnni-0055.002]
stack	Synonymous with label stack.	[b-IETF RFC 3031]
style	Object of an RSVP message that specifies the desired reservation style.	[b-IETF RFC 2205]
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.	[b-IETF 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.	[b-IETF 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.	[b-IETF RFC 3784]

Term	Definition	Source document
summary address	An address prefix that tells a node how to summarize reachability information.	[b-BBF af-pnni-0055.002]
switched path	Synonymous with label switched path.	[b-IETF 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.	[b-BBF af-pnni-0055.002]
TCP segment	The unit of data exchanged between TCP modules (including the TCP header).	[b-IETF RFC 791]
TE LSP head-end	Head/source of the TE LSP.	[b-IETF RFC 4736]
TE LSP tail-end	Tail/destination of the TE LSP.	[b-IETF RFC 4736]
Time to Live (TTL) (1)	An Internet header field which indicates the upper bound on how long this Internet datagram may exist.	[b-IETF 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.	[b-IETF RFC 1812]
TIME_VALUES	Object in an RSVP control message that specifies the time period timer used for refreshing the state in this message.	[b-IETF RFC 2205]
topology aggregation	The process of summarizing and compressing topology information at a hierarchical level to be advertised at the level above.	[b-BBF af-pnni-0055.002]
topology attribute	A generic term that refers to either a link attribute or a nodal attribute.	[b-BBF af-pnni-0055.002]
topology constraint	A topology constraint is a generic term that refers to either a link constraint or a nodal constraint.	[b-BBF af-pnni-0055.002]
topology database	The database that describes the topology of the entire PNNI routing domain as seen by a node.	[b-BBF af-pnni-0055.002]
topology metric	A generic term that refers to either a link metric or a nodal metric.	[b-BBF af-pnni-0055.002]
topology state parameter	A generic term that refers to either a link parameter or a nodal parameter.	[b-BBF 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.	[b-IETF RFC 791]

Term	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.	[b-BBF 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.	[b-BBF 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.	[b-BBF 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).	[b-BBF 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.	[b-IETF RFC 2205]
traffic engineered tunnel (TE tunnel)	A set of one or more LSP Tunnels which carries a traffic trunk.	[b-IETF 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.	[b-IETF 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.	[b-IETF RFC 3209]

Term	Definition	Source document
Transmission Control Protocol (TCP)	A host-to-host protocol for reliable communication in Internet environments.	[b-IETF 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.	[b-IETF RFC 4204]
transport network address	Address of an entity (e.g., a TNE) within the transport network.	[b-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.	[b-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.	[b-OIF-UNI-01.0]
Trivial File Transfer Protocol (TFTP)	A simple file transfer protocol built on UDP.	[b-IETF 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.	[b-IETF RFC 3032]
TSpec	A traffic parameter set that describes a flow. The format of a Tspec is opaque to RSVP.	[b-IETF RFC 2205]
tunnel ID	A 16-bit identifier used in the SESSION that remains constant over the life of the tunnel.	[b-IETF RFC 4872]
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.	[b-IETF RFC 1812]
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.	[b-IETF RFC 2205]
UNI signalling channel	This is the logical communication channel between the UNI-C and the UNI-N over which UNI signalling messages are sent.	[b-OIF-UNI-01.0]
UNI-C	The logical entity that terminates UNI signalling on the client device side.	[b-OIF-UNI-01.0]
UNI-N	The logical entity that terminates UNI signalling on the transport network side.	[b-OIF-UNI-01.0]
uplink	Represents the connectivity from a border node to an upnode.	[b-BBF 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.	[b-BBF af-pnni-0055.002]

Term	Definition	Source document
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 "tunnelled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself.	[b-IETF RFC 2460]
upstream	Towards the traffic source. RSVP Resv messages flow upstream.	[b-IETF 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.	[b-IETF RFC 791]
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.	[b-OIF-UNI-01.0]
User Datagram Protocol (UDP)	A user-level protocol for transaction-oriented applications.	[b-IETF RFC 791]
User Network Interface (UNI)	The user-network interface is the service control interface between a client device and the transport network.	[b-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.	[b-IETF 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.	[b-IETF 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.	[b-IETF RFC 3031]
VPI/VCI	A label used in ATM networks to identify circuits	[b-IETF RFC 3031]
working LSP/span	A working LSP/span is an LSP/span transporting "normal" user traffic.	[b-IETF RFC 4427]
working path	The protected path that carries traffic before the occurrence of a fault. The working path can be of different kinds; a hop-by-hop routed path, a trunk, a link, an LSP or part of a multipoint-to-point LSP. Synonyms for a working path are primary path and active path.	[b-IETF RFC 3469]

Appendix III

Related abbreviations and acronyms found in documents
from other organizations

(This appendix does not form an integral part of this Recommendation)

In the table below, a term followed by a number in ( ) indicates that the term has multiple meanings defined by different documents.

AA	Administrative Authority (a three octet-field in the GOSIP version 2.0 NSAP address format)	[b-IETF RFC 1195]
ABR	Area Border Router	[b-IETF RFC 4736]
AFI	Authority and Format Identifier (the first octet of all OSI NSAP addresses – identifies format of the rest of the address)	[b-IETF RFC 1195]
AS	Autonomous System	[b-IETF RFC 3945]
ASP	ATM Service Provider	[b-BBF af-pnni-0055.002]
ATC	ATM Transfer Capability	[b-BBF af-pnni-0055.002]
AW	Administrative Weight	[b-BBF af-pnni-0055.002]
BGP	Border Gateway Protocol	[b-BBF af-pnni-0055.002]
CA	Certification Authority	[b-OIF-SMI-01.0]
CAC	Connection Admission Control	[b-BBF af-pnni-0055.002]
CBC	Cipher Block Chaining	[b-OIF-SMI-01.0]
CDV	Cell Delay Variation	[b-BBF af-pnni-0055.002]
CLNP	ConnectionLess Network Protocol (ISO 8473, the OSI connectionless network layer protocol – very similar to IP)	[b-IETF RFC 1195]
CLR	Cell Loss Ratio	[b-BBF af-pnni-0055.002]
CLR0	Cell Loss Ratio objective for CLP=0 traffic	[b-BBF af-pnni-0055.002]
COA	Connection Available	[b-BBF af-cs-0148.000]
CO-BI	Connection-Oriented Bearer-Independent	[b-BBF af-cs-0141.000]
COPS	Common Open Policy Service	[b-IETF RFC 2749]
CR-LDP	Constraint-based Routing LDP	[b-IETF RFC 3945]
CR-LSP	Constraint-based Router Label Switched Path	[b-IETF RFC 3212]
CRM	Cell Rate Margin	[b-BBF af-pnni-0055.002]
CSPF	Constraint-based Shortest Path First	[b-IETF RFC 3945]
DCC	Data Communication Channel	[b-OIF-UNI-01.0]
DFI	DSP Format Identifier	[b-IETF RFC 1195]
DLCI	Data Link Connection Identifier	[b-BBF af-cs-0141.000]
DSP	Domain Specific Part	[b-BBF af-pnni-0055.002]
DSS	Digital Signature Standard	[b-OIF-SMI-01.0]
DTL	Designated Transit List	[b-BBF af-pnni-0055.002]
ERLSP	Explicitly Routed LSP	[b-IETF RFC 4802]
ERO	Explicit Route Object	[b-IETF RFC 4736]
ESI	End System Identifier	[b-BBF af-pnni-0055.002]

ES-IS	End System to Intermediate System Routing Exchange Protocol (ISO 9542 – OSI protocol between routers and end systems)	[b-IETF RFC 1195]
ESP	Encapsulating Security Payload	[b-OIF-SMI-01.0]
FA	Forwarding Adjacency	[b-IETF RFC 3945]
FEC	Forwarding Equivalence Class	[b-IETF RFC 4201]
FRTT	Fixed Round Trip Time	[b-BBF af-cs-0173.000]
FSC	Fibre-Switch Capable	[b-IETF RFC 4202]
FTN	FEC to NHLFE Map	[b-IETF RFC 4201]
GCAC	Generic Connection Admission Control	[b-BBF af-pnni-0055.002]
GFR	Guaranteed Frame Rate	[b-BBF af-cs-0173.000]
GLB	Greatest Lower Bound	[b-IETF RFC 2205]
GMPLS	Generalized Multi-Protocol Label Switching	[b-OIF-UNI-01.0]
GSMP	Generic Switch Management Protocol	[b-OIF-UNI-01.0]
ICD	International Code Designator (ISO standard for identifying organizations)	[b-IETF RFC 1195]
ICMP	Internet Control Message Protocol	[b-OIF-SMI-01.0]
ID	Identifier	[b-BBF af-pnni-0055.002]
IDI	Initial Domain Identifier	[b-BBF af-pnni-0055.002]
IDP	Initial Domain Part	[b-BBF af-pnni-0055.002]
IDRP	Inter Domain Routing Protocol	[b-BBF af-pnni-0055.002]
IE	Information Element	[b-BBF af-pnni-0055.002]
IG	Information Group	[b-BBF af-pnni-0055.002]
IGP	Interior Gateway Protocol	[b-IETF RFC 4201]
IISP	Interim Inter-switch Signalling Protocol	[b-BBF af-cs-0141.000]
IKE	Internet Key Exchange	[b-OIF-SMI-01.0]
ILM	Incoming Label Map	[b-IETF RFC 4201]
ILMI	Interim Local Management Interface	[b-BBF af-pnni-0055.002]
IP (1)	Internetwork Protocol (an Internet Standard Network Layer Protocol)	[b-IETF RFC 1195]
IP (2)	Internet Protocol	[b-OIF-SMI-01.0]
IPCC	IP Control Channel	[b-OIF-UNI-01.0]
Ipsec	IP Security	[b-OIF-SMI-01.0]
IS	Intermediate System (the OSI term for a router)	[b-IETF RFC 1195]
ISH	An Hello packet defined by ISO 9542 (ES-IS protocol). (not the same as IS-IS Hello)	[b-IETF RFC 1195]
ISI	Internal Signalling Interface	[b-OIF-UNI-01.0]
IS-IS	Intermediate System to Intermediate System Routeing Exchange Protocol (the ISO protocol for routing within a single routing domain)	[b-IETF RFC 1195]
IS-IS Hello	An Hello packet defined by the IS-IS protocol (a type of packet used by the IS-IS protocol)	[b-IETF RFC 1195]
L2	Layer 2	[b-IETF RFC 4201]
L2SC	Layer-2 Switch Capable	[b-IETF RFC 4202]

L3	Layer 3	[b-IETF RFC 4201]
LDP	Label Distribution Protocol	[b-OIF-UNI-01.0]
LGN	Logical Group Node	[b-BBF af-pnni-0055.002]
LMP	Link Management Protocol	[b-OIF-UNI-01.0]
LOH	Line Overhead	[b-OIF-UNI-01.0]
LSA	Link State Advertisement	[b-IETF RFC 3945]
LSC	Lambda Switch Capable	[b-IETF RFC 4201]
LSP (1)	Link State Packet (a type of packet used by the IS-IS protocol)	[b-IETF RFC 1195]
LSP (2)	Label Switched Path	[b-IETF RFC 3945]
LSR	Label Switching Router	[b-IETF RFC 4201]
LTE	Line Terminating Equipment	[b-OIF-UNI-01.0]
LUB	Least Upper Bound	[b-IETF RFC 2205]
MAC	Message Authentication Code	[b-OIF-SMI-01.0]
maxCR	Maximum Cell Rate	[b-BBF af-pnni-0055.002]
maxCTD	Maximum Cell Transfer Delay	[b-BBF af-pnni-0055.002]
MCR	Minimum Cell Rate	[b-BBF af-pnni-0055.002]
MIB	Management Information Base	[b-BBF af-cs-0141.000]
MOA	MODIFICATION ACKNOWLEDGE Message	[b-BBF af-cs-0148.000]
MOD	MODIFICATION REQUEST Message	[b-BBF af-cs-0148.000]
MOR	MODIFICATION REJECT Message	[b-BBF af-cs-0148.000]
MPLS	Multi-Protocol Label Switching	[b-OIF-UNI-01.0]
NCCI	Network Call Correlation Identifier	[b-BBF af-cs-0173.000]
ND	Neighbour Discovery	[b-OIF-UNI-01.0]
NHLFE	Next Hop Label Forwarding Entry	[b-IETF RFC 4201]
NLPID	Network Layer Protocol ID (a one-octet field identifying a network layer protocol)	[b-IETF RFC 1195]
NNI	Network-to-Network Interface	[b-BBF af-pnni-0055.002]
Non-FT	Not fault tolerant	[b-IETF RFC 3479]
NSAP	Network Service Access Point (a conceptual interface point at which the network service is made available)	[b-IETF RFC 1195]
O	Optional (may be selected to suit the implementation, provided that any requirements applicable to the options are observed)	[b-BBF 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"	[b-BBF af-cs-0148.000]
OSPF	Open Shortest Path First	[b-BBF af-pnni-0055.002]
OUI	Organizational Unique Identifier	[b-BBF af-cs-0141.000]
OXC	Optical Cross-Connect	[b-IETF RFC 3945]
PCR	Peak Cell Rate	[b-BBF af-pnni-0055.002]
PDP	Policy Decision Point	[b-IETF RFC 2753]
PEP	Policy Enforcement Point	[b-IETF RFC 2753]
PG	Peer Group	[b-BBF af-pnni-0055.002]
PGL	Peer Group Leader	[b-BBF af-pnni-0055.002]

PGLE	Peer Group Leader Election	[b-BBF af-pnni-0055.002]
PICS	Protocol Implementation Conformance Statement	[b-BBF af-cs-0141.000]
PIN	Policy Ignorant Node	[b-IETF RFC 2753]
PNNI	Private Network-Network Interface	[b-BBF af-cs-0141.000]
PSC	Packet Switch Capable	[b-IETF RFC 4201]
PTSE	PNNI Topology State Element	[b-BBF af-pnni-0055.002]
PTSP	PNNI Topology State Packet	[b-BBF af-pnni-0055.002]
PVCC	Permanent Virtual Channel Connection	[b-BBF af-pnni-0055.002]
PXC	Photonic Cross-Connect	[b-IETF RFC 3945]
QoS	Quality of Service	[b-BBF af-pnni-0055.002]
RAIG	Resource Availability Information Group	[b-BBF af-pnni-0055.002]
RCC	Routing Control Channel	[b-BBF 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)	[b-IETF RFC 1195]
RDF	Rate Decrease Factor	[b-BBF af-pnni-0055.002]
RIF	Rate Increase Factor	[b-BBF af-pnni-0055.002]
RM	Resource Management	[b-BBF af-cs-0173.000]
RSVP	Resource reSerVation Protocol	[b-OIF-UNI-01.0]
RSVP-TE	RSVP with Traffic Engineering extensions	[b-OIF-UNI-01.0]
SAAL	Signalling ATM Adaptation Layer	[b-BBF af-pnni-0055.002]
SCR	Sustainable Cell Rate	[b-BBF af-pnni-0055.002]
SEL	NSAP Selector (the last octet of NSAP addresses, also called NSEL)	[b-IETF RFC 1195]
SHA	Secure Hash Algorithm	[b-OIF-SMI-01.0]
S/MIME	Secure Multipurpose Internet Mail Extensions	[b-OIF-SMI-01.0]
SNPA	Subnetwork Point of Attachment (a conceptual interface at which a subnetwork service is provided)	[b-IETF RFC 1195]
Soft	PVC Soft Permanent Virtual Connection	[b-BBF af-cs-0141.000]
SPD	Security Policy Database	[b-OIF-SMI-01.0]
SPF	Shortest Path First	[b-IETF RFC 4202]
SSCOP	Service Specific Connection Oriented Protocol	[b-BBF af-pnni-0055.002]
SSCS	Service Specific Convergence Sublayer	[b-BBF af-pnni-0055.002]
SSH	Secure Shell	[b-OIF-SMI-01.0]
SSL	Secure Sockets Layer	[b-OIF-SMI-01.0]
STE	Section Terminating Equipment	[b-OIF-UNI-01.0]
SVC (1)	Switched Virtual Connection	[b-BBF af-pnni-0055.002]
SVC (2)	Switched Virtual Circuit	[b-BBF af-cs-0173.000]
SVCC	Switched Virtual Channel Connection	[b-BBF af-pnni-0055.002]
SVP	Switched Virtual Path	[b-IETF RFC 4201]
SVPC	Switched Virtual Path Connection	[b-BBF af-pnni-0055.002]
TAS	Transported Address Stack	[b-BBF af-cs-0173.000]
TBE	Transit Buffer Exposure	[b-BBF af-pnni-0055.002]

TCP	Transmission Control Protocol (an Internet Standard Transport Layer Protocol)	[b-IETF RFC 1195]
TCP/IP	The protocol suite based on TCP, IP, and related protocols (the Internet standard protocol architecture)	[b-IETF RFC 1195]
TE	Traffic Engineering	[b-IETF RFC 3945]
TLV (1)	Type Length Value	[b-BBF af-cs-0173.000]
TLV (2)	Type-Length-Value encoding	[b-OIF-UNI-01.0]
TTL (1)	Time-To-Live	[b-IETF RFC 4201]
TTL (2)	Trace Transit List	[b-BBF af-cs-0141.000]
UBR	Unspecified Bit Rate	[b-BBF af-pnni-0055.002]
UDP	User Datagram Protocol	[b-OIF-SMI-01.0]
ULIA	Uplink Information Attribute	[b-BBF af-pnni-0055.002]
UNI	User to Network Interface	[b-BBF af-cs-0173.000]
UNI-N	UNI Signalling Agent – Network	[b-OIF-UNI-01.0]
UNI-C	UNI Signalling Agent – Client	[b-OIF-UNI-01.0]
VC	Virtual Circuit	[b-IETF RFC 4201]
VCC	Virtual Channel Connection	[b-BBF af-pnni-0055.002]
VCI	Virtual Channel Identifier	[b-BBF af-cs-0141.000]
VF	Variance Factor	[b-BBF af-pnni-0055.002]
VP	Virtual Path	[b-BBF af-pnni-0055.002]
VPC	Virtual Path Connection	[b-BBF af-pnni-0055.002]
VPI	Virtual Path Identifier	[b-BBF af-pnni-0055.002]

Bibliography

[b-BBF af-cs-0141.000]	ATM Forum Technical Committee (2000), *PNNI Addendum for Path and Connection Trace, Version 1.0.*
[b-BBF af-cs-0148.000]	ATM Forum Technical Committee (2000), *Modification of Traffic Descriptor for an Active Connection.*
[b-BBF af-cs-0173.000]	ATM Forum Technical Committee (2001), *Domain-based rerouting for active point-to-point calls, Version 1.0.*
[b-BBF af-pnni-0055.002]	ATM Forum Technical Committee (2002), *Private Network-Network Interface Specification v.1.1.*
[b-IETF RFC 791]	IETF RFC 791 (1981), *Internet Protocol.*
[b-IETF RFC 1195]	IETF RFC 1195 (1990), *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments.*
[b-IETF RFC 1661]	IETF RFC 1661 (1994), *The Point-to-Point Protocol (PPP).*
[b-IETF RFC 1812]	IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers.*
[b-IETF RFC 2205]	IETF RFC 2205 (1997), *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification.*
[b-IETF RFC 2328]	IETF RFC 2328 (1998), *OSPF Version 2.*
[b-IETF RFC 2460]	IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification.*
[b-IETF 2749]	IETF 2749 (2000), *COPS usage for RSVP.*
[b-IETF RFC 2753]	IETF RFC 2753 (2000), *A Framework for Policy-based Admission Control.*
[b-IETF RFC 3031]	IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture.*
[b-IETF RFC 3032]	IETF RFC 3032 (2001), *MPLS Label Stack Encoding.*
[b-IETF RFC 3036]	IETF RFC 3036 (2001), *LDP Specification.*
[b-IETF RFC 3209]	IETF RFC 3209 (2001), *RSVP-TE: Extensions to RSVP for LSP Tunnels.*
[b-IETF RFC 3212]	IETF RFC 3212 (2002), *Constraint-Based LSP Setup using LDP.*
[b-IETF RFC 3469]	IETF RFC 3469 (2003), *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery.*
[b-IETF RFC 3479]	IETF RFC 3479 (2003), *Fault Tolerance for the Label Distribution Protocol (LDP).*
[b-IETF RFC 3784]	IETF RFC 3784 (2004), *Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE).*
[b-IETF RFC 3945]	IETF RFC 3945 (2004), *Generalized Multi-Protocol Label Switching (GMPLS) Architecture.*
[b-IETF RFC 4201]	IETF RFC 4201 (2005), *Link Bundling in MPLS Traffic Engineering (TE).*
[b-IETF RFC 4202]	IETF RFC 4202 (2005), *Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS).*

[b-IETF RFC 4204]	IETF RFC 4204 (2005), *Link Management Protocol (LMP)*.
[b-IETF RFC 4209]	IETF RFC 4209 (2005), *Link Management Protocol (LMP) for Dense Wavelength Division Multiplexing (DWDM) Optical Line Systems*.
[b-IETF RFC 4427]	IETF RFC 4427 (2006), *Recovery (Protection and Restoration) Terminology for Generalized Multi-Protocol Label Switching (GMPLS)*.
[b-IETF RFC 4558]	IETF RFC 4558 (2006), *Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement*.
[b-IETF RFC 4652]	IETF RFC 4652 (2006), *Evaluation of Existing Routing Protocols against Automatic Switched Optical Network (ASON) Routing Requirements*.
[b-IETF RFC 4736]	IETF RFC 4736 (2006), *Reoptimization of Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Loosely Routed Label Switched Path (LSP)*.
[b-IETF RFC 4802]	IETF RFC 4802 (2007), *Generalized Multiprotocol Label Switching (GMPLS) Traffic Engineering Management Information Base*.
[b-IETF RFC 4803]	IETF RFC 4803 (2007), *Generalized Multiprotocol Label Switching (GMPLS) Label Switching Router (LSR) Management Information Base*.
[b-IETF RFC 4872]	IETF RFC 4872 (2007), *RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery*.
[b-IETF RFC 4972]	IETF RFC 4972 (2007), *Routing Extensions for Discovery of Multiprotocol (MPLS) Label Switch Router (LSR) Traffic Engineering (TE) Mesh Membership*.
[b-OIF-SMI-01.0]	OIF Forum (2003), *Security for Management Interfaces to Network Elements*.
[b-OIF-UNI-01.0]	OIF Forum (2001), *User Network Interface (UNI) 1.0 Signaling Specification*.

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
IPTV over NGN	Y.1900–Y.1999
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
Future networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999

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   Terminals and subjective and objective assessment methods

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