Carrier Optical Services Requirements

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or rendered obsolete by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.
Abstract
This Internet Draft describes the major carrier’s service requirements for the automatic switched optical networks (ASON) from both an end-user’s as well as an operator’s perspectives. Its focus is on the description of the service building blocks and service-related control plane functional requirements. The management functions for the optical services and their underlying networks are beyond the scope of this document and will be addressed in a separate document.

Table of Contents
1. Introduction 3
  1.1 Justification 3
  1.2 Conventions used in this document 3
  1.3 Value Statement 3
  1.4 Scope of This Document 4
2. Abbreviations 5
3. General Requirements 5
  3.1 Separation of Networking Functions 5
  3.2 Network and Service Scalability 6
  3.3 Transport Network Technology 6
  3.4 Service Building Blocks 7
4. Service Model and Applications 7
  4.1 Service and Connection Types 7
  4.2 Examples of Common Service Models 8
5. Network Reference Model 9
  5.1 Optical Networks and Subnetworks 9
  5.2 Network Interfaces 9
  5.3 Intra-Carrier Network Model 11
  5.4 Inter-Carrier Network Model 12
6. Optical Service User Requirements 13
  6.1 Common Optical Services 13
  6.2 Optical Service Invocation 14
  6.3 Bundled Connection 16
  6.4 Levels of Transparency 17
  6.5 Optical Connection granularity 17
  6.6 Other Service Parameters and Requirements 18
7. Optical Service Provider Requirements 19
  7.1 Access Methods to Optical Networks 19
  7.2 Dual Homing and Network Interconnections 19
  7.3 Inter-domain connectivity 20
1. Introduction

Next generation WDM-based optical transport network (OTN) will consist of optical cross-connects (OXC), DWDM optical line systems (OLS) and optical add-drop multiplexers (OADM) based on the architecture defined by the ITU Rec. G.872 in [G.872]. The OTN is bounded by a set of optical channel access points and has a layered structure consisting of optical channel, multiplex section and transmission section sub-layer networks. Optical networking encompasses the functionalities for the establishment, transmission, multiplexing, switching of optical connections carrying a wide range of user signals of varying formats and bit rate.

The ultimate goal is to enhance the OTN with an intelligent optical layer control plane to dynamically provision network resources and to provide network survivability using ring and mesh-based protection and restoration techniques. The resulting intelligent networks are
called automatic switched optical networks or ASON [G.8080].

The emerging and rapidly evolving ASON technologies are aimed at providing optical networks with intelligent networking functions and capabilities in its control plane to enable wavelength switching, rapid optical connection provisioning and dynamic rerouting. The same technology will also be able to control TDM based SONET/SDH optical transport network as defined by ITU Rec. G.803 [G.803]. This new networking platform will create tremendous business opportunities for the network operators and service providers to offer new services to the market.

1.1. Justification

The charter of the IPO WG calls for a document on "Carrier Optical Services Requirements" for IP/Optical networks. This document addresses that aspect of the IPO WG charter. Furthermore, this document was accepted as an IPO WG document by unanimous agreement at the IPO WG meeting held on March 19, 2001, in Minneapolis, MN, USA. It presents a carrier and end-user perspective on optical network services and requirements.

1.2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.3. Value Statement

By deploying ASON technology, a carrier expects to achieve the following benefits from both technical and business perspectives:

- Rapid Circuit Provisioning: ASON technology will enable the dynamic end-to-end provisioning of the optical connections across the optical network by using standard routing and signaling protocols.

- Enhanced Survivability: ASON technology will enable the network to dynamically reroute an optical connection in case of a failure using mesh-based network protection and restoration techniques, which greatly improves the cost-effectiveness compared to the current line and ring protection schemes in the SONET/SDH network.

- Cost-Reduction: ASON networks will enable the carrier to better utilize the optical network, thus achieving significant unit cost
reduction per Megabit due to the cost-effective nature of the optical transmission technology, simplified network architecture and reduced operation cost.

- Service Flexibility: ASON technology will support provisioning of an assortment of existing and new services such as protocol and bit-rate independent transparent network services, and bandwidth-on-demand services.

- Enhanced Interoperability: ASON technology will use a control plane utilizing industry and international standards architecture and protocols, which facilitate the interoperability of the optical network equipment from different vendors.

In addition, the introduction of a standards-based control plane offers the following potential benefits:

- Reactive traffic engineering at optical layer that allows network resources to be dynamically allocated to traffic flow.

- Reduce the need for service providers to develop new operational support systems software for the network control and new service provisioning on the optical network, thus speeding up the deployment of the optical network technology and reducing the software development and maintenance cost.

- Potential development of a unified control plane that can be used for different transport technologies including OTN, SONET/SDH, ATM and PDH.

1.4. Scope of This Document

This document is aimed at providing, from the carrier’s perspective, a service framework and associated requirements in relation to the optical services to be offered in the next generation optical networking environment and their service control and management functions. As such, this document concentrates on the requirements driving the work towards realization of ASON. This document is intended to be protocol-neutral.

Every carrier’s needs are different. The objective of this document is NOT to define some specific service models. Instead, some major service building blocks are identified that will enable the carriers to mix and match them in order to create the best service platform most suitable to their business model. These building blocks include
generic service types, service enabling control mechanisms and service control and management functions. The ultimate goal is to provide the requirements to guide the control protocol developments within IETF in terms of IP over optical technology.

In this document, we consider IP a major client to the optical network, but the same requirements and principles should be equally applicable to non-IP clients such as SONET/SDH, ATM, ITU G.709, etc.

2. Abbreviations

ASON     Automatic Switched Optical Networking
ASTN     Automatic Switched Transport Network
CAC     Connection Admission Control
E-NNI    Exterior NNI
E-UNI    Exterior UNI
IWF     Inter-Working Function
I-NNI    Interior NNI
I-UNI    Interior UNI
NNI     Node-to-Node Interface
NE     Network Element
OTN     Optical Transport Network
OLS     Optical Line System
PI     Physical Interface
SLA    Service Level Agreement
UNI     User-to-Network Interface

3. General Requirements

In this section, a number of generic requirements related to the service control and management functions are discussed.

3.1. Separation of Networking Functions

It makes logical sense to segregate the networking functions within each layer network into three logical functional planes: control plane, data plane and management plane. They are responsible for providing network control functions, data transmission functions and network management functions respectively. The crux of the ASON network is the networking intelligence that contains automatic routing, signaling and discovery functions to automate the network control functions.

Control Plane: includes the functions related to networking control capabilities such as routing, signaling, and policy control, as well
as resource and service discovery. These functions are automated.

Data Plane (transport plane): includes the functions related to bearer channels and signal transmission.

Management Plane: includes the functions related to the management functions of network element, networks and network resources and services. These functions are less automated as compared to control plane functions.

Each plane consists of a set of interconnected functional or control entities, physical or logical, responsible for providing the networking or control functions defined for that network layer.

The separation of the control plane from both the data and management plane is beneficial to the carriers in that it:

- Allows equipment vendors to have a modular system design that will be more reliable and maintainable thus reducing the overall systems ownership and operation cost.

- Allows carriers to have the flexibility to choose a third party vendor control plane software systems as its control plane solution for its switched optical network.

- Allows carriers to deploy a unified control plane and OSS/management systems to manage and control different types of transport networks it owes.

- Allows carriers to use a separate control network specially designed and engineered for the control plane communications.

The separation of control, management and transport function is required and it shall accommodate both logical and physical level separation.

Note that it is in contrast to the IP network where the control messages and user traffic are routed and switched based on the same network topology due to the associated in-band signaling nature of the IP network.
3.2. Network and Service Scalability

Although specific applications or networks may be on a small scale, the control plane protocol and functional capabilities shall not limit large-scale networks.

In terms of the scale and complexity of the future optical network, the following assumption can be made when considering the scalability and performance that are required of the optical control and management functions. - There may be up to hundreds of OXC nodes and the same order of magnitude of OADMs per carrier network.

- There may be up to thousands of terminating ports/wavelength per OXC node.

- There may be up to hundreds of parallel fibers between a pair of OXC nodes.

- There may be up to hundreds of wavelength channels transmitted on each fiber. In relation to the frequency and duration of the optical connections:

  - The expected end-to-end connection setup/teardown time should be in the order of seconds.

  - The expected connection holding times should be in the order of minutes or greater.

  - The expected number of connection attempts at UNI should be in the order of 100’s.

- There may be up to millions of simultaneous optical connections switched across a single carrier network. Note that even though automated rapid optical connection provision is required, but the carriers expect the majority of provisioned circuits, at least in short term, to have a long lifespan ranging from months to years.

3.3. Transport Network Technology

Optical services can be offered over different types of underlying optical transport technologies including both TDM-based SONET/SDH network and WDM-based OTN networks.

For this document, standards-based transport technologies SONET/SDH as defined in the ITU Rec. G.803 and OTN implementation framing as defined in ITU Rec. G.709 shall be supported.
Note that the service characteristics such as bandwidth granularity and signaling framing hierarchy to a large degree will be determined by the capabilities and constraints of the server layer network.

3.4. Service Building Blocks

The primary goal of this document is to identify a set of basic service building blocks the carriers can mix and match them to create the best suitable service models that serve their business needs.

The service building blocks are comprised of a well-defined set of service capabilities and a basic set of service control and management functions, which offer a basic set of services and additionally enable a carrier to define enhanced services through extensions and customizations. Examples of the building blocks include the connection types, provisioning methods, control interfaces, policy control functions, and domain internetworking mechanisms, etc.

4. Service Model and Applications

A carrier’s optical network supports multiple types of service models. Each service model may have its own service operations, target markets, and service management requirements.

4.1. Service and Connection Types

The optical network is primarily offering high bandwidth connectivity in the form of connections, where a connection is defined to be a fixed bandwidth connection between two client network elements, such as IP routers or ATM switches, established across the optical network. A connection is also defined by its demarcation from ingress access point, across the optical network, to egress access point of the optical network.

The following connection capability types must be supported:

- Uni-directional point-to-point connection
- Bi-directional point-to-point connection
- Uni-directional point-to-multipoint connection

For point-to-point connection, the following three types of network connections based on different connection set-up control methods
shall be supported:

- Permanent connection (PC): Established hop-by-hop directly on each ONE along a specified path without relying on the network routing and signaling capability. The connection has two fixed end-points and fixed cross-connect configuration along the path and will stays permanently until it is deleted. This is similar to the concept of PVC in ATM.

- Switched connection (SC): Established through UNI signaling interface and the connection is dynamically established by network using the network routing and signaling functions. This is similar to the concept of SVC in ATM.

- Soft permanent connection (SPC): Established by specifying two PC at end-points and let the network dynamically establishes a SC connection in between. This is similar to the SPVC concept in ATM.

The PC and SPC connections should be provisioned via management plane to control interface and the SC connection should be provisioned via signaled UNI interface.

4.2. Examples of Common Service Models

Each carrier can defines its own service model based on it business strategy and environment. The following are three service models that carriers may use:

4.2.1. Provisioned Bandwidth Service (PBS)

The PBS model provides enhanced leased/private line services provisioned via service management interface (MI) using either PC or SPC type of connection. The provisioning can be real-time or near real-time. It has the following characteristics:

- Connection request goes through a well-defined management interface

- Client/Server relationship between clients and optical network.

- Clients have no optical network visibility and depend on network intelligence or operator for optical connection setup.
4.2.2. Bandwidth on Demand Service (BDS)

The BDS model provides bandwidth-on-demand dynamic connection services via signaled user-network interface (UNI). The provisioning is real-time and is using SC type of optical connection. It has the following characteristics:

- Signaled connection request via UNI directly from the user or its proxy.
- Customer has no or limited network visibility depending upon the control interconnection model used and network administrative policy.
- Relies on network or client intelligence for connection set-up depending upon the control plane interconnection model used.

4.2.3. Optical Virtual Private Network (OVPN)

The OVPN model provides virtual private network at the optical layer between a specified set of user sites. It has the following characteristics:

- Customers contract for specific set of network resources such as optical connection ports, wavelengths, etc.
- Closed User Group (CUG) concept is supported as in normal VPN.
- Optical connection can be of PC, SPC or SC type depending upon the provisioning method used.
- An OVPN site can request dynamic reconfiguration of the connections between sites within the same CUG.
- Customer may have limited or full visibility and control of contracted network resources depending upon the customer service contract.

At minimum, the PBS, BDS and OVPN service models described above shall be supported by the control functions.
5. Network Reference Model

This section discusses major architectural and functional components of a generic carrier optical network, which will provide a reference model for describing the requirements for the control and management of carrier optical services.

5.1. Optical Networks and Subnetworks

As mentioned before, there are two main types of optical networks that are currently under consideration: SDH/SONET network as defined in ITU Rec. G.803, and OTN as defined in ITU Rec. G.872.

We assume an OTN is composed of a set of optical cross-connects (OXC) and optical add-drop multiplexer (OADM) which are interconnected in a general mesh topology using DWDM optical line systems (OLS).

It is often convenient for easy discussion and description to treat an optical network as a subnetwork cloud, in which the details of the network become less important, instead focus is on the function and the interfaces the optical network provides. In general, a subnetwork can be defined as a set of access points on the network boundary and a set of point-to-point optical connections between those access points.

5.2. Network Interfaces

A generic carrier network reference model describes a multi-carrier network environment. Each individual carrier network can be further partitioned into domains or sub-networks based on administrative, technological or architectural reasons. The demarcation between (sub)networks can be either logical or physical and consists of a set of reference points identifiable in the optical network. From the control plane perspective, these reference points define a set of control interfaces in terms of optical control and management functionality. The following figure 5.1 is an illustrative diagram for this.
The network interfaces encompass two aspects of the networking functions: user data plane interface and control plane interface. The former concerns about user data transmission across the physical network interface and the latter concerns about the control message exchange across the network interface such as signaling, routing, etc. We call the former physical interface (PI) and the latter control plane interface. Unless otherwise stated, the control interface is assumed in the remaining of this document.

5.2.1. Control Plane Interfaces

Control interface defines a relationship between two connected network entities on both side of the interface. For each control interface, we need to define an architectural function each side plays and a controlled set of information that can be exchanged across the interface. The information flowing over this logical interface may include, but not limited to:

- Endpoint name and address
- Reachability/summarized network address information
- Topology/routing information
- Authentication and connection admission control information
- Connection management signaling messages
- Network resource control information

Different types of the interfaces can be defined for the network control and architectural purposes and can be used as the network reference points in the control plane. In this document, the following set of interfaces are defined as shown in Figure 5.1:

The User-Network Interface (UNI) is a bi-directional signaling interface between service requester and service provider control entities. We further differentiate between interior UNI (I-UNI) and exterior UNI (E-UNI) as follows:

- E-UNI: A UNI interface for which the service request control entity resides outside the carrier network control domain.
- I-UNI: A UNI interface for which the service requester control entity resides within the carrier network control domain.

The reason for doing so is that we can differentiate a class of UNI where there is trust relationship between the client equipment and the optical network. This private nature of UNI may have similar functionality to the NNI in that it may allow for controlled routing information to cross the UNI. Specifics of the I-UNI are currently under study.

The Network-Network Interface (NNI) is a bi-directional signaling interface between two optical network elements or sub-networks.

We differentiate between interior (I-NNI) and exterior (E-NNI) NNI as follows:

- E-NNI: A NNI interface between two control plane entities belonging to different control domains.
- I-NNI: A NNI interface between two control plane entities within the same control domain in the carrier network.

It should be noted that it is quite common to use E-NNI between two sub-networks within the same carrier network if they belong to different control domains. Different types of interface, interior vs. exterior, have different implied trust relationship for security and access control purposes. Trust relationship is not binary, instead a policy-based control mechanism need to be in place to restrict the
type and amount of information that can flow across each type of
interfaces depending on the carrier’s service and business requirements.
Generally, two networks have a trust relationship if they belong to
the same administrative domain.

Interior interface examples include an I-NNI between two optical
network elements in a single control domain or an I-UNI interface
between the optical transport network and an IP client network owned
by the same carrier. Exterior interface examples include an E-NNI
between two different carriers or an E-UNI interface between a
carrier optical network and its customers.

The control plane shall support the UNI and NNI interface described
above and the interfaces shall be configurable in terms of the type
and amount of control information exchange and their behavior shall
be consistent with the configuration (i.e., exterior versus interior
interfaces).

5.3. Intra-Carrier Network Model Intra-carrier network model is
concerned about the network service control and management issues
within networks owned by a single carrier.

5.3.1. Multiple Sub-networks

Without loss of generality, the optical network owned by a carrier
service operator can be depicted as consisting of one or more optical
sub-networks interconnected by direct optical links. There may be
many different reasons for more than one optical sub-networks: It may
be the result of using hierarchical layering, different technologies
across access, metro and long haul (as discussed below), or a result
of business mergers and acquisitions or incremental optical network
technology deployment by the carrier using different vendors or
technologies.

A sub-network may be a single vendor and single technology network.
But in general, the carrier’s optical network is heterogeneous in
terms of equipment vendor and the technology utilized in each sub-
network.
5.3.2. Access, Metro and Long-haul networks

Few carriers have end-to-end ownership of the optical networks. Even if they do, access, metro and long-haul networks often belong to different administrative divisions as separate optical sub-networks. Therefore Inter-(sub)-networks interconnection is essential in terms of supporting the end-to-end optical service provisioning and management. The access, metro and long-haul networks may use different technologies and architectures, and as such may have different network properties.

In general, an end-to-end optical connection may easily cross multiple sub-networks with the following possible scenarios:
Access -- Metro -- Access
Access -- Metro -- Long Haul -- Metro -- Access

5.3.3. Implied Control Constraints

The carrier’s optical network is in general treated as a trusted domain, which is defined as a network under a single technical administration with implied trust relationship. Within a trusted domain, all the optical network elements and sub-networks are considered to be secure and trusted by each other at a defined level. In the intra-carrier model interior interfaces (I-NNI and I-UNI) are generally assumed.

One business application for the interior UNI is the case where a carrier service operator offers data services such as IP, ATM and Frame Relay over its optical core network. Data services network elements such as routers and ATM switches are considered to be internal optical service client devices. The topology information for the carrier optical network may be shared with the internal client data networks.

5.4. Inter-Carrier Network Model

The inter-carrier model focuses on the service and control aspects between different carrier networks and describes the internetworking relationship between them.
5.4.1. Carrier Network Interconnection

Inter-carrier interconnection provides for connectivity among different optical network operators. To provide the global reach end-to-end optical services, the optical service control and management between different carrier networks become essential. The normal connectivity between the carriers may include:

Private Peering: Two carriers set up dedicated connection between them via a private arrangement.

Public Peering: Two carriers set up a point-to-point connection between them at a public optical network access points (ONAP)

Due to the nature of the automatic optical switched network, it is possible to support the distributed peering for the IP client layer network where the connection between two distant IP routers can be connected via an optical connection.

5.4.2. Implied Control Constraints

In the inter-carrier network model, each carrier’s optical network is a separate administrative domain. Both the UNI interface between the user and the carrier network and the NNI interface between two carrier’s networks are crossing the carrier’s administrative boundary and therefore are by definition exterior interfaces.

In terms of control information exchange, the topology information shall not be allowed to across both E-NNI and E-UNI interfaces.

6. Optical Service User Requirements

This section describes the user requirements for optical services, which in turn impose the requirements on service control and management for the network operators. The user requirements reflect the perception of the optical service from a user’s point of view.

6.1. Common Optical Services

The basic unit of an optical service is a fixed-bandwidth optical connection between connected parties. However different services are created based on its supported signal characteristics (format, bit rate, etc), the service invocation methods and possibly the
associated Service Level Agreement (SLA) provided by the service provider.

At present, the following are the major optical services provided in the industry:

- SONET/SDH, with different degrees of transparency
- Optical wavelength services: opaque or transparent
- Ethernet at 1 Gbps and 10 Gbps
- Storage Area Networks (SANs) based on FICON, ESCON and Fiber Channel

The services mentioned above shall be provided by the optical transport layer of the network being provisioned using the same management, control and data planes.

Opaque Service refers to transport services where signal framing is negotiated between the client and the network operator (framing and bit-rate dependent), and only the payload is carried transparently. SONET/SDH transport is most widely used for network-wide transport. Different levels of transparency can be achieved in the SONET/SDH transmission and is discussed in Section 6.4.

Transparent Service assumes protocol and rate independency. However, since any optical connection is associated with a signal bandwidth, for transparent optical services, knowledge of the maximum bandwidth is required.

Ethernet Services, specifically 1Gb/s and 10Gbs Ethernet services, are gaining more popularity due to the lower costs of the customers’ premises equipment and its simplified management requirements (compared to SONET or SDH).

Ethernet services may be carried over either SONET/SDH (GFP mapping) or WDM networks. The Ethernet service requests will require some service specific parameters: priority class, VLAN Id/Tag, traffic aggregation parameters.

Storage Area Network (SAN) Services. ESCON and FICON are proprietary versions of the service, while Fiber Channel is the standard alternative. As is the case with Ethernet services, SAN services may be carried over either SONET/SDH (using GFP mapping) or WDM networks.
Currently SAN services require only point-to-point connections, but it is envisioned that in the future they may also require multicast connections.

The control plane shall provide the carrier with the capability functionality to to provision, control and manage all the services listed above.

6.2. Optical Service Invocation

As mentioned earlier, the methods of service invocation play an important role in defining different services.

6.2.1. In this scenario, users forward their service request to the provider via a well-defined service management interface. All connection management operations, including set-up, release, query, or modification shall be invoked from the management plane.

6.2.2. In this scenario, users forward their service request to the provider via a well-defined UNI interface in the control plane (including proxy signaling). All connection management operation requests, including set-up, release, query, or modification shall be invoked from directly connected user devices, or its signaling representative (such as a signaling proxy).

In summary the following requirements for the control plane have been identified:

The control plane shall support action results codes as responses to any requests over the control interfaces.

The control plane shall support requests for connection set-up, subject to policies in effect between the user and the network.

The control plane shall support the destination client device’s decision to accept or reject connection creation requests from the initiating client’s device.

- The control plane shall support requests for connection set-up across multiple subnetworks over both Interior and Exterior Network Interfaces.

- NNI signaling shall support requests for connection set-up, subject to policies in effect between the subnetworks.
- Connection set-up shall be supported for both uni-directional and bi-directional connections.

- Upon connection request initiation, the control plane shall generate a network unique Connection-ID associated with the connection, to be used for information retrieval or other activities related to that connection.

- CAC shall be provided as part of the control plane functionality. It is the role of the CAC function to determine if there is sufficient free resource available downstream to allow a new connection.

- When a connection request is received across the NNI, it is necessary to ensure that the resources exist within the downstream subnetwork to establish the connection.

- If sufficient resources are available, the CAC may permit the connection request to proceed.

- If sufficient resources are not available, the CAC shall send an appropriate notification upstream towards the originator of the connection request that the request has been denied.

- Negotiation for connection set-up for multiple service level options shall be supported across the NNI.

- The policy management system must determine what kind of connections can be set up across a given NNI.

- The control plane elements need the ability to rate limit (or pace) call setup attempts into the network.

- The control plane shall report to the management plane, the Success/Failures of a connection request

- Upon a connection request failure, the control plane shall report to the management plane a cause code identifying the reason for the failure.

Upon a connection request failure:

- The control plane shall report to the management plane a cause code identifying the reason for the failure

- A negative acknowledgment shall be returned across the NNI

- Allocated resources shall be released.
Upon a connection request success:

- A positive acknowledgment shall be returned when a connection has been successfully established.

- The positive acknowledgment shall be transmitted both downstream and upstream, over the NNI, to inform both source and destination clients of when they may start transmitting data.

The control plane shall support the client’s request for connection tear down.

NNI signaling plane shall support requests for connection tear down by connection-ID.

The control plane shall allow either end to initiate connection release procedures.

NNI signaling flows shall allow any end point or any intermediate node to initiate the connection release over the NNI.

Upon connection teardown completion all resources associated with the connection shall become available for access for new requests.

The management plane shall be able to tear down connections established by the control plane both gracefully and forcibly on demand.

Partially deleted connections shall not remain within the network.

End-to-end acknowledgments shall be used for connection deletion requests.

Connection deletion shall not result in either restoration or protection being initiated.

Connection deletion shall at a minimum use a two pass signaling process, removing the cross-connection only after the first signaling pass has completed.

The control plane shall support management plane and client’s device request for connection attributes or status query.

The control plane shall support management plane and neighboring device (client or intermediate node) request for connection attributes or status query.
The control plane shall support action results code responses to any requests over the control interfaces.

The management plane shall be able to query on demand the status of the connection.

The UNI shall support initial registration of the UNI-C with the network via the control plane.

The UNI shall support registration and updates by the UNI-C entity of the clients and user interfaces that it controls.

The UNI shall support network queries of the client devices.

The UNI shall support detection of client devices or of edge ONE failure.

6.3. Bundled Connection

Bundled connections differ from simple basic connections in that a connection request may generate multiple parallel connections bundled together as one virtual connection.

Multiple point-to-point connections may be managed by the network so as to appear as a single compound connection to the end-points. Examples of such bundled connections are connections based on virtual concatenation, diverse routing, or restorable connections.

The actions required to manage compound connections are the same as the ones outlined for the management of basic connections.

6.4. Levels of Transparency

Opaque connections are framing and bit-rate dependent - the exact signal framing is known or needs to be negotiated between network operator and its clients. However, there may be multiple levels of transparency for individual framing types. Current transport networks are mostly based on SONET/SDH technology. Therefore, multiple levels have to be considered when defining specific optical services.

The example below shows multiple levels of transparency applicable to SONET/SDH transport.

- Bit transparency in the SONET/SDH frames. This means that the OXC
will not terminate any byte in the SONET OH bytes.

- SONET Line and section OH (SDH multiplex and regenerator section OH) are normally terminated and the network can monitor a large set of parameters.

However, if this level of transparency is used, the TOH will be tunneled in unused bytes of the non-used frames and will be recovered at the terminating ONE with their original values.

- Line and section OH are forwarded transparently, keeping their integrity thus providing the customer the ability to better determine where a failure has occurred, this is very helpful when the connection traverses several carrier networks.

- G.709 OTN signals

6.5. Optical Connection granularity

The service granularity is determined by the specific technology, framing and bit rate of the physical interface between the ONE and the client at the edge and by the capabilities of the ONE. The control plane needs to support signaling and routing for all the services supported by the ONE.

The physical connection is characterized by the nominal optical interface rate and other properties such as protocol supported. However, the consumable attribute is bandwidth. In general, there should not be a one-to-one correspondence imposed between the granularity of the service provided and the maximum capacity of the interface to the user. The bandwidth utilized by the client becomes the logical connection, for which the customer will be charged.

In addition, sub-rate interfaces shall be supported by the optical control plane such as VT /TU granularity (as low as 1.5 Mb/s)

The control plane shall support the ITU Rec. G.709 connection granularity for the OTN network.

The control plane shall support the SDH and SONET connection granularity.

In addition, 1 Gb and 10 Gb granularity shall be supported for 1 Gb/s and 10 Gb/s (WAN mode) Ethernet framing types, if implemented in the hardware.
For SAN services the following interfaces have been defined and shall be supported by the control plane if the given interfaces are available on the equipment:
- FC-12
- FC-50
- FC-100
- FC-200

Therefore, sub-rate fabric granularity shall support VT-x/TU-1n granularity down to VT1.5/TU-11, consistent with the hardware.

Encoding of service types in the protocols used shall be such that new service types can be added by adding new code point values or objects.

6.6. Other Service Parameters and Requirements

6.6.1. Classes of Service

We use "service level" to describe priority related characteristics of connections, such as holding priority, set-up priority, or restoration priority. The intent currently is to allow each carrier to define the actual service level in terms of priority, protection, and restoration options. Therefore, individual carriers will determine mapping of individual service levels to a specific set of quality features.

Specific protection and restoration options are discussed in Section 10. However, it should be noted that while high grade services may require allocation of protection or restoration facilities, there may be an application for a low grade of service for which preemptable facilities may be used.

Multiple service level options shall be supported and the user shall have the option of selecting over the UNI a service level for an individual connection.

The control plane shall be capable of mapping individual service classes into specific protection and / or restoration options.
6.6.2. Connection Latency

Connection latency is a parameter required for support of time-sensitive services like Fiber Channel services. Connection latency is dependent on the circuit length, and as such for these services, it is essential that shortest path algorithms are used and end-to-end latency is verified before acknowledging circuit availability.

The control plane shall support latency-based routing constraint (such as distance) as a path selection parameter.

6.6.3. Diverse Routing Attributes

The ability to route service paths diversely is a highly desirable feature. Diverse routing is one of the connection parameters and is specified at the time of the connection creation. The following provides a basic set of requirements for the diverse routing support.

Diversity between two links being used for routing should be defined in terms of link disjointness, node disjointness or Shared Risk Link Groups (SRLG) that is defined as a group of links which share some risky resources, such as a specific sequence of conduits or a specific office. A SRLG is a relationship between the links that should be characterized by two parameters:

- Type of Compromise: Examples would be shared fiber cable, shared conduit, shared right-of-way (ROW), shared link on an optical ring, shared office - no power sharing, etc.)

- Extent of Compromise: For compromised outside plant, this would be the length of the sharing.

The control plane routing algorithms shall be able to route a single demand diversely from N previously routed demands in terms of link disjoint path, node disjoint path and SRLG disjoint path.
7. Optical Service Provider Requirements

This section discusses specific service control and management requirements from the service provider’s point of view.

7.1. Access Methods to Optical Networks

Multiple access methods shall be supported:

- Cross-office access (User NE co-located with ONE) In this scenario the user edge device resides in the same office as the ONE and has one or more physical connections to the ONE. Some of these access connections may be in use, while others may be idle pending a new connection request.

- Direct remote access

In this scenario the user edge device is remotely located from the ONE and has inter-location connections to the ONE over multiple fiber pairs or via a DWDM system. Some of these connections may be in use, while others may be idle pending a new connection request.

- Remote access via access sub-network

In this scenario remote user edge devices are connected to the ONE via a multiplexing/distribution sub-network. Several levels of multiplexing may be assumed in this case. This scenario is applicable to metro/access subnetworks of signals from multiple users, out, of which only a subset have connectivity to the ONE.

All of the above access methods must be supported.

7.2. Dual Homing and Network Interconnections

Dual homing is a special case of the access network. Client devices can be dual homed to the same or different hub, the same or different access network, the same or different core networks, the same or different carriers. The different levels of dual homing connectivity result in many different combinations of configurations. The main objective for dual homing is for enhanced survivability.

The different configurations of dual homing will have great impact on admission control, reachability information exchanges, authentication, neighbor and service discovery across the interface.

Dual homing must be supported.
7.3. Inter-domain connectivity

A domain is a portion of a network, or an entire network that is controlled by a single control plane entity. This section discusses the various requirements for connecting domains.

7.3.1. Multi-Level Hierarchy

Traditionally current transport networks are divided into core inter-city long haul networks, regional intra-city metro networks and access networks. Due to the differences in transmission technologies, service, and multiplexing needs, the three types of networks are served by different types of network elements and often have different capabilities. The diagram below shows an example three-level hierarchical network.

```
+--------------+
|              |
+-------------+   Haul       +-------------+
|              | Subnetwork   |             |
+-------+------+                            +-------+------+
|              |                            |              |
| Core Long    |                            | Core Long    |
+-------+------+
Regional     Regional
+-------+------+
Subnetwork   Subnetwork
+-------+------+
| Metro/Access|                            | Metro/Access|
+-------------+                            +-------------+
|              |                            |              |
```

Figure 2 Multi-level hierarchy example

Functionally we can often see clear split among the 3 types of networks: Core long-haul network deals primarily with facilities transport and switching. SONET signals at STS-1 and higher rates constitute the units of transport. Regional networks will be more closely tied to service support and VT-level signals need to be also switched. As an example of interaction a device switching DS1 signals interfaces to other such devices over the long-haul network via STS-1 links. Regional networks will also groom traffic of the Metro networks, which generally have direct interfaces to clients, and support a highly varied mix of services. It should be noted that, although not shown in Figure 2, metro/access subnetworks may have interfaces to the core network, without having to go through a
Routing and signaling for multi-level hierarchies shall be supported to allow carriers to configure their networks as needed.

7.3.2. Network Interconnections

Subnetworks may have multiple points of inter-connections. All relevant NNI functions, such as routing, reachability information exchanges, and inter-connection topology discovery must recognize and support multiple points of inter-connections between subnetworks. Dual inter-connection is often used as a survivable architecture.

Such an inter-connection is a special case of a mesh network, especially if these subnetworks are connected via an I-NNI, i.e., they are within the same administrative domain. In this case the control plane requirements described in Section 8 will also apply for the inter-connected subnetworks, and are therefore not discussed here.

However, there are additional requirements if the interconnection is across different domains, via an E-NNI. These additional requirements include the communication of failure handling functions, routing, load sharing, etc. while adhering to pre-negotiated agreements on these functions across the boundary nodes of the multiple domains. Subnetwork interconnection may also be achieved alternatively via a separate subnetwork. In this case, the above requirements stay the same, but need to be communicated over the interconnecting subnetwork, similar to the E-NNI scenario described above.

7.4. Bearer Interface Types

All the bearer interfaces implemented in the ONE shall be supported by the control plane and associated signaling protocols.

The following interface types shall be supported by the signaling protocol:

- SDH
- SONET
- 1 Gb Ethernet, 10 Gb Ethernet (WAN mode)
- 10 Gb Ethernet (LAN mode)
- FC-N (N= 12, 50, 100, or 200) for Fiber Channel services
- OTN (G.709)
- PDH
7.5. Names and Address Management

7.5.1. Address Space Separation

To ensure the scalability of and smooth migration toward to the optical switched network, the separation of three address spaces are required:
- Internal transport network addresses
- Transport Network Assigned (TNA) address
- Client addresses.

7.5.2. Directory Services

Directory Services shall be supported to enable operator to query the optical network for the optical network address of a specified user. Address resolution and translation between various user edge device names and corresponding optical network addresses shall be supported. UNI shall use the user naming schemes for connection request.

7.5.3. Network element Identification

Each network element within a single control domain shall be uniquely identifiable. The identifiers may be re-used across multiple domains. However, unique identification of a network element becomes possible by associating its local identity with the global identity of its domain.

7.6. Policy-Based Service Management Framework

The IPO service must be supported by a robust policy-based management system to be able to make important decisions.

Examples of policy decisions include: - What types of connections can be set up for a given UNI?

- What information can be shared and what information must be restricted in automatic discovery functions?

- What are the security policies over signaling interfaces?
- What border nodes should be used when routing depend on factors including, but not limited to source and destination address, border nodes loading, time of connection request.

Requirements: - Service and network policies related to configuration and provisioning, admission control, and support of Service Level Agreements (SLAs) must be flexible, and at the same time simple and scalable.

- The policy-based management framework must be based on standards-based policy systems (e.g. IETF COPS).

- In addition, the IPO service management system must support and be backwards compatible with legacy service management systems.

7.7. Support of Hierarchical Routing and Signaling

The routing protocol(s) shall support hierarchical routing information dissemination, including topology information aggregation and summarization.

The routing protocol(s) shall minimize global information and keep information locally significant as much as possible.

Over external interfaces only reachability information, next routing hop and service capability information should be exchanged. Any other network related information shall not leak out to other networks.

8. Control Plane Functional Requirements for Optical Services

This section addresses the requirements for the optical control plane in support of service provisioning.

The scope of the control plane include the control of the interfaces and network resources within an optical network and the interfaces between the optical network its client networks. In other words, it include NNI and UNI aspects.

8.1. Control Plane Capabilities and Functions

The control capabilities are supported by the underlying control functions and protocols built in the control plane.
8.1.1. Network Control Capabilities

The following capabilities are required in the network control plane to successfully deliver automated provisioning for optical services:
- Neighbor, service and topology discovery
- Address assignment and resolution
- Routing information propagation and dissemination
- Path calculation and selection
- Connection management

These capabilities may be supported by a combination of functions across the control and the management planes.

8.1.2. Control Plane Functions for network control

The following are essential functions needed to support network control capabilities:
- Signaling
- Routing
- Automatic resource, service and neighbor discovery

Specific requirements for signaling, routing and discovery are addressed in Section 9.

The general requirements for the control plane functions to support optical networking and service functions include: - The control plane must have the capability to establish, teardown and maintain the end-to-end connection, and the hop-by-hop connection segments between any two end-points.

- The control plane must have the capability to support traffic-engineering requirements including resource discovery and dissemination, constraint-based routing and path computation.

- The control plane shall support network status or action result code responses to any requests over the control interfaces.

- The control plane shall support resource allocation on both UNI and NNI.

- Upon successful connection teardown all resources associated with
the connection shall become available for access for new requests.

- The control plane shall support management plane request for connection attributes/status query.
- The control plane must have the capability to support various protection and restoration schemes for the optical channel establishment.
- Control plane failures shall not affect active connections.
- The control plane shall be able to trigger restoration based on alarms or other indications of failure.

8.2. Signaling Network

The signaling network consists of a set of signaling channels that interconnect the nodes within the control plane. Therefore, the signaling network must be accessible by each of the communicating nodes (e.g., OXCs).

- The signaling network must terminate at each of the nodes in the transport plane.
- The signaling network shall not be assumed to have the same topology as the data plane, nor shall the data plane and control plane traffic be assumed to be congruently routed. A signaling channel is the communication path for transporting control messages between network nodes, and over the UNI (i.e., between the UNI entity on the user side (UNI-C) and the UNI entity on the network side (UNI-N)). The control messages include signaling messages, routing information messages, and other control maintenance protocol messages such as neighbor and service discovery. There are three different types of signaling methods depending on the way the signaling channel is constructed: - In-band signaling: The signaling messages are carried over a logical communication channel embedded in the data-carrying optical link or channel. For example, using the overhead bytes in SONET data framing as a logical communication channel falls into the in-band signaling methods.
- In fiber, Out-of-band signaling: The signaling messages are carried over a dedicated communication channel separate from the optical data-bearing channels, but within the same fiber. For example, a dedicated wavelength or TDM channel may be used within the same fiber as the data channels.
Out-of-fiber signaling: The signaling messages are carried over a dedicated communication channel or path within different fibers to those used by the optical data-bearing channels. For example, dedicated optical fiber links or communication path via separate and independent IP-based network infrastructure are both classified as out-of-fiber signaling.

In-band signaling may be used over a UNI interface, where there are relatively few data channels. Proxy signaling is also important over the UNI interface, as it is useful to support users unable to signal to the optical network via a direct communication channel. In this situation a third party system containing the UNI-C entity will initiate and process the information exchange on behalf of the user device. The UNI-C entities in this case reside outside of the user in separate signaling systems.

In-fiber, out-of-band and out-of-fiber signaling channel alternatives are usually used for NNI interfaces, which generally have significant numbers of channels per link. Signaling messages relating to all of the different channels can then be aggregated over a single or small number of signaling channels.

The signaling network forms the basis of the transport network control plane.

- The signaling network shall support reliable message transfer.
- The signaling network shall have its own OAM mechanisms.
- The signaling network shall use protocols that support congestion control mechanisms.

In addition, the signaling network should support message priorities. Message prioritization allows time critical messages, such as those used for restoration, to have priority over other messages, such as other connection signaling messages and topology and resource discovery messages.

The signaling network must be highly scalable, with minimal performance degradations as the number of nodes and node sizes increase.

The signaling network shall be highly reliable and implement failure recovery.

Security and resilience are crucial issues for the signaling network will be addressed in Section 10 and 11 of this document.
8.3. Control Plane Interface to Data Plane

In the situation where the control plane and data plane are provided by different suppliers, this interface needs to be standardized. Requirements for a standard control -data plane interface are under study. Control plane interface to the data plane is outside the scope of this document.

8.4. Management Plane Interface to Data Plane

The management plane is responsible for identifying which network resources that the control plane may use to carry out its control functions. Additional resources may be allocated or existing resources deallocated over time.

Resources shall be able to be allocated to the control plane for control plane functions include resources involved in setting up and tearing down calls and control plane specific resources. Resources allocated to the control plane for the purpose of setting up and tearing down calls include access groups (a set of access points), connection point groups (a set of connection points). Resources allocated to the control plane for the operation of the control plane itself may include protected and protecting control channels.

Resources allocated to the control plane by the management plane shall be able to be de-allocated from the control plane on management plane request.

If resources are supporting an active connection and the resources are requested to be de-allocated by management plane, the control plane shall reject the request. The management plane must either wait until the resources are no longer in use or tear down the connection before the resources can be de-allocated from the control plane. Management plane failures shall not affect active connections.

Management plane failures shall not affect the normal operation of a configured and operational control plane or data plane.

8.5. Control Plane Interface to Management Plane

The control plane is considered a managed entity within a network. Therefore, it is subject to management requirements just as other managed entities in the network are subject to such requirements.
8.5.1. Soft Permanent Connections (Point-and click provisioning)

In the case of SPCs, the management plane requests the control plane to set up / tear down a connection just like what we can do over a UNI.

The management plane shall be able to query on demand the status of the connection request. The control plane shall report to the management plane, the Success/Failures of a connection request. Upon a connection request failure, the control plane shall report to the management plane a cause code identifying the reason for the failure.

8.5.2. Resource Contention resolution Since resources are allocated to the control plane for use, there should not be contention between the management plane and the control plane for connection set-up. Only the control plane can establish connections for allocated resources. However, in general, the management plane shall have authority over the control plane.

The control plane shall not assume authority over management plane provisioning functions.

In the case of network failure, both the management plane and the control plane need fault information at the same priority.

The control plane needs fault information in order to perform its restoration function (in the event that the control plane is providing this function). However, the control plane needs less granular information than that required by the management plane. For example, the control plane only needs to know whether the resource is good/bad. The management plane would additionally need to know if a resource was degraded or failed and the reason for the failure, the time the failure occurred and so on.

The control plane shall not assume authority over management plane for its management functions (FCAPS).

The control plane shall be responsible for providing necessary statistic data such as call counts, traffic counts to the management plane. They should be available upon the query from the management plane.

Control plane shall support policy-based CAC function either within the control plane or provide an interface to a policy server outside
Topological information learned in the discovery process shall be able to be queried on demand from the management plane.

The management plane shall be able to tear down connections established by the control plane both gracefully and forcibly on demand.

8.6. Control Plane Interconnection

When two (sub)networks are interconnected on transport plane level, so should be two corresponding control network at the control plane. The control plane interconnection model defines the way how two control networks can be interconnected in terms of controlling relationship and control information flow allowed between them.

8.6.1. Interconnection Models

There are three basic types of control plane network interconnection models: overlay, peer and hybrid, which are defined by the IETF IPO WG document [IPO_frame].

Choosing the level of coupling depends upon a number of different factors, some of which are:

- Variety of clients using the optical network
- Relationship between the client and optical network
- Operating model of the carrier

Overlay model (UNI like model) shall be supported for client to optical control plane interconnection

Other models are optional for client to optical control plane interconnection

For optical to optical control plane interconnection all three models shall be supported
9. Requirements for Signaling, Routing and Discovery

9.1. Requirements for information sharing over UNI, I-NNI and E-NNI

There are three types of interfaces where the routing information dissemination may occur: UNI, I-NNI and E-NNI. Different types of interfaces shall impose different requirements and functionality due to their different trust relationships. Over UNI, the user network and the transport network form a client-server relationship. Therefore, the transport network topology shall not be disseminated from transport network to the user network.

Information flows expected over the UNI shall support the following:
- Call control
- Resource Discovery
- Connection Control
- Connection Selection

Address resolution exchange over UNI is needed if an addressing directory service is not available.

Information flows over the I-NNI shall support the following:
- Resource Discovery
- Connection Control
- Connection Selection
- Connection Routing

Information flows over the E-NNI shall support the following:
- Call Control
- Resource Discovery
- Connection Control
- Connection Selection
- Connection Routing

9.2. Signaling Functions

Call and connection control and management signaling messages are used for the establishment, modification, status query and release of an end-to-end optical connection.
9.2.1. Call and connection control

To support many enhanced optical services, such as scheduled bandwidth on demand and bundled connections, a call model based on the separation of the call control and connection control is essential. The call control is responsible for the end-to-end session negotiation, call admission control and call state maintenance while connection control is responsible for setting up the connections associated with a call. A call can correspond to zero, one or more connections depending upon the number of connections needed to support the call.

This call model has the advantage of reducing redundant call control information at intermediate (relay) connection control nodes, thereby removing the burden of decoding and interpreting the entire message and its parameters. Since the call control is provided at the ingress to the network or at gateways and network boundaries. As such the relay bearer needs only provide the procedures to support switching connections.

Call control is a signaling association between one or more user applications and the network to control the set-up, release, modification and maintenance of sets of connections. Call control is used to maintain the association between parties and a call may embody any number of underlying connections, including zero, at any instance of time.

Call control may be realized by one of the following methods:

- Separation of the call information into parameters carried by a single call/connection protocol
- Separation of the state machines for call control and connection control, whilst signaling information in a single call/connection protocol
- Separation of information and state machines by providing separate signaling protocols for call control and connection 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. Note that a call being allowed to proceed only indicates that the call may proceed to request one or more connections. It does not imply that any of those connection requests will succeed. Call admission control may also be invoked at other network boundaries.
Connection control is responsible for the overall control of individual connections. Connection control may also be considered to be associated with link control. The overall control of a connection is performed by the protocol undertaking the set-up and release procedures associated with a connection and the maintenance of the state of the connection.

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). This is usually performed on a link-by-link basis, based on local conditions and policy. Connection admission control may refuse the connection request.

Control plane shall support the separation of call control and connection control.

Control plane shall support proxy signaling.

Inter-domain signaling shall comply with g.8080 and g.7713 (ITU).

The inter-domain signaling protocol shall be agnostic to the intra-domain signaling protocol within any of the domains within the network.

Inter-domain signaling shall support both strict and loose routing.

Inter-domain signaling shall not be assumed necessarily congruent with routing.

It should not be assumed that the same exact nodes are handling both signaling and routing in all situations.

Inter-domain signaling shall support all call management primitives:
- Per individual connections
- Per groups of connections

Inter-domain signaling shall support inter-domain notifications.

Inter-domain signaling shall support per connection global connection identifier for all connection management primitives.

Inter-domain signaling shall support both positive and negative responses for all requests, including the cause, when applicable.

Inter-domain signaling shall support all the connection attributes representative to the connection characteristics of the individual
Inter-domain signaling shall support crank-back and rerouting.

Inter-domain signaling shall support graceful deletion of connections including of failed connections, if needed.

9.3. Routing Functions

Routing includes reachability information propagation, network topology/resource information dissemination and path computation. In optical network, each connection involves two user endpoints. When user endpoint A requests a connection to user endpoint B, the optical network needs the reachability information to select a path for the connection. If a user endpoint is unreachable, a connection request to that user endpoint shall be rejected. Network topology/resource information dissemination is to provide each node in the network with stabilized and consistent information about the carrier network such that a single node is able to support constrain-based path selection.

A mixture of hop-by-hop routing, explicit/source routing and hierarchical routing will likely be used within future transport networks. Using hop-by-hop message routing, each node within a network makes routing decisions based on the message destination, and the network topology/resource information or the local routing tables if available. However, achieving efficient load balancing and establishing diverse connections are impractical using hop-by-hop routing. Instead, explicit (or source) routing may be used to send signaling messages along a route calculated by the source. This route, described using a set of nodes/links, is carried within the signaling message, and used in forwarding the message.

Hierarchical routing supports signaling across NNIs. It allows conveying summarized information across I-NNIs, and avoids conveying topology information across trust boundaries. Each signaling message contains a list of the domains traversed, and potentially details of the route within the domain being traversed.

All three mechanisms (Hop-by-hop routing, explicit / source-based routing and hierarchical routing) must be supported. Messages crossing trust boundaries must not contain information regarding the details of an internal network topology. This is particularly important in traversing E-UNIs and E-NNIs. Connection routes and identifiers encoded using topology information (e.g., node identifiers) must also not be conveyed over these boundaries.
Requirements for routing information dissemination:

Routing protocols must propagate the appropriate information efficiently to network nodes.

The following requirements apply:

The inter-domain routing protocol shall comply with G.8080 (ITU).

The inter-domain routing protocol shall be agnostic to the intra-domain routing protocol within any of the domains within the network.

The inter-domain routing protocol shall not impede any of the following routing paradigms within individual domains:

- Hierarchical routing
- Step-by-step routing
- Source routing

The exchange of the following types of information shall be supported by inter-domain routing protocols

- Inter-domain topology
- Per-domain topology abstraction
- Per domain reachability information
- Metrics for routing decisions supporting load sharing, a range of service granularity and service types, restoration capabilities, diversity, and policy.

Inter-domain routing protocols shall support per domain topology and resource information abstraction.

Inter-domain protocols shall support reachability information aggregation.

A major concern for routing protocol performance is scalability and stability issues, which impose following requirements on the routing protocols:

- The routing protocol performance shall not largely depend on the scale of the network (e.g. the number of nodes, the number of links, end user etc.). The routing protocol design shall keep the network size effect as small as possible.
- The routing protocols shall support following scalability techniques:

1. Routing protocol shall support hierarchical routing information dissemination, including topology information aggregation and summarization.

2. The routing protocol shall be able to minimize global information and keep information locally significant as much as possible (e.g., information local to a node, a sub-network, a domain, etc). For example, a single optical node may have thousands of ports. The ports with common characteristics need not to be advertised individually.

3. Routing protocol shall distinguish static routing information and dynamic routing information. Static routing information does not change due to connection operations, such as neighbor relationship, link attributes, total link bandwidth, etc. On the other hand, dynamic routing information updates due to connection operations, such as link bandwidth availability, link multiplexing fragmentation, etc.

4. The routing protocol operation shall update dynamic and static routing information differently. Only dynamic routing information shall be updated in real time.

5. Routing protocol shall be able to control the dynamic information updating frequency through different types of thresholds. Two types of thresholds could be defined: absolute threshold and relative threshold. The dynamic routing information will not be disseminated if its difference is still inside the threshold. When an update has not been sent for a specific time (this time shall be configurable the carrier), an update is automatically sent. Default time could be 30 minutes.

All the scalability techniques will impact the network resource representation accuracy. The tradeoff between accuracy of the routing information and the routing protocol scalability should be well studied. A routing protocol shall allow the network operators to adjust the balance according to their networks’ specific characteristics.
9.4. Requirements for path selection

The path selection algorithm must be able to compute the path, which satisfies a list of service parameter requirements, such as service type requirements, bandwidth requirements, protection requirements, diversity requirements, bit error rate requirements, latency requirements, including/excluding area requirements. The characteristics of a path are those of the weakest link. For example, if one of the links does not have link protection capability, the whole path should be declared as having no link-based protection. The following are functional requirements on path selection.

- Path selection shall support shortest path as well as constraint-based routing.

- Various constraints may be required for constraint based path selection, including but not limited to:
  - Cost
  - Load Sharing
  - Diversity
  - Service Class

- Path selection shall be able to include/exclude some specific locations, based on policy.

- Path selection shall be able to support protection/restoration capability. Section 10 discusses this subject in more detail.

- Path selection shall be able to support different levels of diversity, including diversity routing and protection/restoration diversity.

- Path selection algorithms shall provide carriers the ability to support a wide range of services and multiple levels of service classes. Parameters such as service type, transparency, bandwidth, latency, bit error rate, etc. may be relevant.

- Path selection algorithms shall support a set of requested routing constraints, and constraints of the networks. Some of the network constraints are technology specific, such as the constraints in all-optical networks addressed in [John_Angela_IPO_draft]. The requested constraints may include bandwidth requirement, diversity requirements, path specific requirements, as well as restoration requirements.
9.5. Automatic Discovery Functions

This section describes the requirements for automatic discovery to aid distributed connection management (DCM) in the context of automatically switched transport networks (ASTN/ASON), as specified in ITU-T recommendation G.807. Auto-discovery is applicable to the User-to-Network Interface (UNI), Network-Node Interfaces (NNI) and to the Transport Plane Interfaces (TPI) of the ASTN.

Automatic discovery functions include neighbor, resource and service discovery.

9.5.1. Neighbor discovery

This section provides the requirements for the automatic neighbor discovery for the UNI and NNI and TPI interfaces. This requirement does not preclude specific manual configurations that may be required and in particular does not specify any mechanism that may be used for optimizing network management.

Neighbor Discovery can be described as an instance of auto-discovery that is used for associating two subnet points that form a trail or a link connection in a particular layer network. The association created through neighbor discovery is valid so long as the trail or link connection that forms the association is capable of carrying traffic. This is referred to as transport plane neighbor discovery. In addition to transport plane neighbor discovery, auto-discovery can also be used for distributed subnet controller functions to establish adjacencies. This is referred to as control plane neighbor discovery. It should be noted that the Sub network points that are associated, as part of neighbor discovery do not have to be contained in network elements with physically adjacent ports. Thus neighbor discovery is specific to the layer in which connections are to be made and consequently is principally useful only when the network has switching capability at this layer. Further details on neighbor discovery can be obtained from ITU-T draft recommendations G.7713 and G.7714.

Both control plane and transport plane neighbor discovery shall be supported.

9.5.2. Resource Discovery

Resource discovery can be described as an instance of auto-discovery that is used for verifying the physical connectivity between two ports on adjacent network elements in the network. Resource
discovery is also concerned with the ability to improve inventory management of network resources, detect configuration mismatches between adjacent ports, associating port characteristics of adjacent network elements, etc.

Resource discovery happens between neighbors. A mechanism designed for a technology domain can be applied to any pair of NEs interconnected through interfaces of the same technology. However, because resource discovery means certain information disclosure between two business domains, it is under the service providers’ security and policy control. In certain network scenario, a service provider who owns the transport network may not be willing to disclose any internal addressing scheme to its client. So a client NE may not have the neighbor NE address and port ID in its NE level resource table.

Interface ports and their characteristics define the network element resources. Each network can store its resources in a local table that could include switching granularity supported by the network element, ability to support concatenated services, range of bandwidths supported by adaptation, physical attributes signal format, transmission bit rate, optics type, multiplexing structure, wavelength, and the direction of the flow of information. Resource discovery can be achieved through either manual provisioning or automated procedures. The procedures are generic while the specific mechanisms and control information can be technology dependent.

Resource discovery can be achieved in several methods. One of the methods is the self-resource discovery by which the NE populates its resource table with the physical attributes and resources. Neighbor discovery is another method by which NE discovers the adjacencies in the transport plane and their port association and populates the neighbor NE. After neighbor discovery resource verification and monitoring must be performed to verify physical attributes to ensure compatibility. Resource monitoring must be performed periodically since neighbor discovery and port association are repeated periodically. Further information can be found in [GMPLS-ARCH].

Resource discovery shall be supported.

9.5.3. Service Discovery

Service Discovery can be described as an instance of auto-discovery that is used for verifying and exchanging service capabilities that are supported by a particular link connection or trail. It is assumed that service discovery would take place after two Sub Network
Points within the layer network are associated through neighbor discovery. However, since service capabilities of a link connection or trail can dynamically change, service discovery can take place at any time after neighbor discovery and any number of times as may be deemed necessary.

Service discovery is required for all the optical services supported.

10. Requirements for service and control plane resiliency

Resiliency is a network capability to continue its operations under the condition of failures within the network. The automatic switched Optical network assumes the separation of control plane and data plane. Therefore the failures in the network can be divided into those affecting the data plane and those affecting the control plane. To provide enhanced optical services, resiliency measures in both data plane and control plane should be implemented. The following failure handling principles shall be supported.

The control plane shall provide the failure detection and recovery functions such that the failures in the data plane within the control plane coverage can be quickly mitigated.

The failure of control plane shall not in any way adversely affect the normal functioning of existing optical connections in the data plane.

10.1. Service resiliency

In circuit-switched transport networks, the quality and reliability of the established optical connections in the transport plane can be enhanced by the protection and restoration mechanisms provided by the control plane functions. Rapid recovery is required by transport network providers to protect service and also to support stringent Service Level Agreements (SLAs) that dictate high reliability and availability for customer connectivity.

The choice of a protection/restoration mechanism is a tradeoff between network resource utilization (cost) and service interruption time. Clearly, minimizing service interruption time is desirable, but schemes achieving this usually do so at the expense of network resources, resulting in increased cost to the provider. Different protection/restoration schemes differ in the spare capacity requirements and service interruption time.

In light of these tradeoffs, transport providers are expected to
support a range of different levels of service offerings, characterized by the recovery speed in the event of network failures. For example, a provider’s highest offered service level would generally ensure the most rapid recovery from network failures. However, such schemes (e.g., 1+1, 1:1 protection) generally use a large amount of spare restoration capacity, and are thus not cost effective for most customer applications. Significant reductions in spare capacity can be achieved by protection and restoration using shared network resources.

Clients will have different requirements for connection availability. These requirements can be expressed in terms of the "service level", which can be mapped to different restoration and protection options and priority related connection characteristics, such as holding priority (e.g. pre-emptable or not), set-up priority, or restoration priority. However, how the mapping of individual service levels to a specific set of protection/restoration options and connection priorities will be determined by individual carriers.

In order for the network to support multiple grades of service, the control plane must support differing protection and restoration options on a per connection basis.

In order for the network to support multiple grades of service, the control plane must support setup priority, restoration priority and holding priority on a per connection basis.

In general, the following protection schemes shall be considered for all protection cases within the network:
- Dedicated protection: 1+1 and 1:1
- Shared protection: 1:N and M:N.
- Unprotected

In general, the following restoration schemes should be considered for all restoration cases within the network:
- Shared restoration capacity.
- Un-restorable

Protection and restoration can be done on an end-to-end basis per connection. It can also be done on a per span or link basis between two adjacent network nodes. Specifically, the link can be a network link between two nodes within the network where the P&R scheme operates across a NNI interface or a drop-side link between the edge device and a switch node where the P&R scheme operates across a UNI interface. End-to-end Path protection and restoration schemes operate between access points across all NNI and UNI interfaces supporting the connection.
In order for the network to support multiple grades of service, the control plane must support differing protection and restoration options on a per link or span basis within the network.

In order for the network to support multiple grades of service, the control plane must support differing protection and restoration options on a per link or span basis for dropped customer connections.

The protection and restoration actions are usually triggered by the failure in the networks. However, during the network maintenance affecting the protected connections, a network operator need to proactively force the traffic on the protected connections to switch to its protection connection. Therefore, in order to support easy network maintenance, it required that management initiated protection and restoration be supported.

To support the protection/restoration options: The control plane shall support configurable protection and restoration options via software commands (as opposed to needing hardware reconfigurations) to change the protection/restoration mode.

The control plane shall support mechanisms to establish primary and protection paths.

The control plane shall support mechanisms to modify protection assignments, subject to service protection constraints.

The control plane shall support methods for fault notification to the nodes responsible for triggering restoration / protection (note that the transport plane is designed to provide the needed information between termination points. This information is expected to be utilized as appropriate.)

The control plane shall support mechanisms for signaling rapid re-establishment of connection connectivity after failure.

The control plane shall support mechanisms for reserving bandwidth resources for restoration.

The control plane shall support mechanisms for normalizing connection routing (reversion) after failure repair.

The signaling control plane should implement signaling message priorities to ensure that restoration messages receive preferential treatment, resulting in faster restoration.

Normal connection management operations (e.g., connection deletion)
shall not result in protection/restoration being initiated.

Restoration shall not result in miss-connections (connections established to a destination other than that intended), even for short periods of time (e.g., during contention resolution). For example, signaling messages, used to restore connectivity after failure, should not be forwarded by a node before contention has been resolved.

In the event of there being insufficient bandwidth available to restore all connections, restoration priorities / pre-emption should be used to determine which connections should be allocated the available capacity.

The amount of restoration capacity reserved on the restoration paths determines the robustness of the restoration scheme to failures. For example, a network operator may choose to reserve sufficient capacity to ensure that all shared restorable connections can be recovered in the event of any single failure event (e.g., a conduit being cut). A network operator may instead reserve more or less capacity than required to handle any single failure event, or may alternatively choose to reserve only a fixed pool independent of the number of connections requiring this capacity (i.e., not reserve capacity for each individual connection).

10.2. Control plane resiliency

The control plane may be affected by failures in signaling network connectivity and by software failures (e.g., signaling, topology and resource discovery modules).

Fast detection and recovery from failures in the control plane are important to allow normal network operation to continue in the event of signaling channel failures.

The optical control plane signal network shall support protection and restoration options to enable it to self-healing in case of failures within the control plane. The control plane shall support the necessary options to ensure that no service-affecting module of the control plane (software modules or control plane communications) is a single point of failure. The control plane shall provide reliable transfer of signaling messages and flow control mechanisms for easing any congestion within the control plane. Control plane failures shall not cause failure of established data plane connections. Control network failure detection mechanisms shall distinguish between control channel and software process failures.
When there are multiple channels (optical fibers or multiple wavelengths) between network elements and / or client devices, failure of the control channel will have a much bigger impact on the service availability than in the single case. It is therefore recommended to support a certain level of protection of the control channel. Control channel failures may be recovered by either using dedicated protection of control channels, or by re-routing control traffic within the control plane (e.g., using the self-healing properties of IP). To achieve this requires rapid failure detection and recovery mechanisms. For dedicated control channel protection, signaling traffic may be switched onto a backup control channel between the same adjacent pairs of nodes. Such mechanisms protect against control channel failure, but not against node failure.

If a dedicated backup control channel is not available between adjacent nodes, or if a node failure has occurred, then signaling messages should be re-routed around the failed link / node.

Fault localization techniques for the isolation of failed control resources shall be supported.

Recovery from signaling process failures can be achieved by switching to a standby module, or by re-launching the failed signaling module.

Recovery from software failures shall result in complete recovery of network state.

Control channel failures may occur during connection establishment, modification or deletion. If this occurs, then the control channel failure must not result in partially established connections being left dangling within the network. Connections affected by a control channel failure during the establishment process must be removed from the network, re-routed (cranked back) or continued once the failure has been resolved. In the case of connection deletion requests affected by control channel failures, the connection deletion process must be completed once the signaling network connectivity is recovered.

Connections shall not be left partially established as a result of a control plane failure. Connections affected by a control channel failure during the establishment process must be removed from the network, re-routed (cranked back) or continued once the failure has been resolved. Partial connection creations and deletions must be completed once the control plane connectivity is recovered.
11. Security Considerations

In this section, security considerations and requirements for optical services and associated control plane requirements are described.

11.1 Optical Network Security Concerns
Since optical service is directly related to the physical network which is fundamental to a telecommunications infrastructure, stringent security assurance mechanism should be implemented in optical networks. When designing equipment, protocols, NMS, and OSS that participate in optical service, every security aspect should be considered carefully in order to avoid any security holes that potentially cause dangers to an entire network, such as Denial of Service (DoS) attack, unauthorized access, masquerading, etc.

In terms of security, an optical connection consists of two aspects. One is security of the data plane where an optical connection itself belongs, and the other is security of the control plane.

11.0.1. Data Plane Security

- Misconnection shall be avoided in order to keep the user’s data confidential. For enhancing integrity and confidentiality of data, it may be helpful to support scrambling of data at layer 2 or encryption of data at a higher layer.

11.0.2. Control Plane Security

It is desirable to decouple the control plane from the data plane physically.

Additional security mechanisms should be provided to guard against intrusions on the signaling network. Some of these may be done with the help of the management plane.

- Network information shall not be advertised across exterior interfaces (E-UNI or E-NNI). The advertisement of network information across the E-NNI shall be controlled and limited in a configurable policy based fashion. The advertisement of network information shall be isolated and managed separately by each administration.

- The signaling network itself shall be secure, blocking all unauthorized access. The signaling network topology and addresses shall not be advertised outside a carrier's domain of trust.

- Identification, authentication and access control shall be
rigorously used for providing access to the control plane.

- Discovery information, including neighbor discovery, service discovery, resource discovery and reachability information should be exchanged in a secure way. This is an optional NNI requirement.

- UNI shall support ongoing identification and authentication of the UNI-C entity (i.e., each user request shall be authenticated).

- The UNI and NNI should provide optional mechanisms to ensure origin authentication and message integrity for connection management requests such as set-up, tear-down and modify and connection signaling messages. This is important in order to prevent Denial of Service attacks. The NNI (especially E-NNI) should also include mechanisms to ensure non-repudiation of connection management messages.

- Information on security-relevant events occurring in the control plane or security-relevant operations performed or attempted in the control plane shall be logged in the management plane.

- The management plane shall be able to analyze and exploit logged data in order to check if they violate or threat security of the control plane.

- The control plane shall be able to generate alarm notifications about security related events to the management plane in an adjustable and selectable fashion.

- The control plane shall support recovery from successful and attempted intrusion attacks.

- The desired level of security depends on the type of interfaces and accounting relation between the two adjacent sub-networks or domains. Typically, in-band control channels are perceived as more secure than out-of-band, out-of-fiber channels, which may be partly colocated with a public network.

11.1. Service Access Control

From a security perspective, network resources should be protected from unauthorized accesses and should not be used by unauthorized entities. Service Access Control is the mechanism that limits and controls entities trying to access network resources. Especially on the public UNI, Connection Admission Control (CAC) functions should also support the following security features:
- CAC should be applied to any entity that tries to access network resources through the public UNI (or E-UNI). CAC should include an authentication function of an entity in order to prevent masquerade (spoofing). Masquerade is fraudulent use of network resources by pretending to be a different entity. An authenticated entity should be given a service access level in a configurable policy basis.

- Each entity should be authorized to use network resources according to the service level given.

- With help of CAC, usage based billing should be realized. CAC and usage based billing should be enough stringent to avoid any repudiation. Repudiation means that an entity involved in a communication exchange subsequently denies the fact.

12. Acknowledgements
The authors of this document would like to acknowledge the valuable inputs from John Strand, Yangguang Xu, Deborah Brunhard, Daniel Awduche, Jim Luciani, Lynn Neir, Wesam Alanqar, Tammy Ferris, Mark Jones and Gerry Ash.

References


[G.dcm] ITU-T New Recommendation G.dcm, "Distributed Connection Management (DCM)".


[ipo-impairments] J. Strand et al., "Impairments and Other
Constraints on Optical Layer Routing", draft-ietf-ipo-impairments-00.txt, work in progress.


[oif2001.188.0] R. Graveman et al.,"OIF Security requirement", oif2001.188.0.a"
Author’s Addresses

Yong Xue
UUNET/WorldCom
22001 Loudoun County Parkway
Ashburn, VA 20147
Phone: +1 (703) 886-5358
Email: yong.xue@wcom.com

Monica Lazer
AT&T
900 ROUTE 202/206N PO BX 752
BEDMINSTER, NJ 07921-0000
mlazer@att.com

Jennifer Yates,
AT&T Labs
180 PARK AVE, P.O. BOX 971
FLORHAM PARK, NJ 07932-0000
jyates@research.att.com

Dongmei Wang
AT&T Labs
Room B180, Building 103
180 Park Avenue
Florham Park, NJ 07932
mei@research.att.com

Ananth Nagarajan
Sprint
9300 Metcalf Ave
Overland Park, KS 66212, USA
ananth.nagarajan@mail.sprint.com

Hirokazu Ishimatsu
Japan Telecom Co., LTD
2-9-1 Hatchobori, Chuo-ku,
Tokyo 104-0032 Japan
Phone: +81 3 5540 8493
Fax: +81 3 5540 8485
EMail: hirokazu@japan-telecom.co.jp

Olga Aparicio
Cable & Wireless Global
11700 Plaza America Drive
Reston, VA 20191
### Appendix A Commonly Required Signal Rate

The table below outlines the different signal rates and granularities for the SONET and SDH signals.

<table>
<thead>
<tr>
<th>SDH name</th>
<th>SONET name</th>
<th>Transported signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS64</td>
<td>STS-192</td>
<td>STM-64 (STS-192) signal without termination of any OH.</td>
</tr>
<tr>
<td>RS16</td>
<td>STS-48</td>
<td>STM-16 (STS-48) signal without termination of any OH.</td>
</tr>
<tr>
<td>MS64</td>
<td>STS-192</td>
<td>STM-64 (STS-192); termination of RSOH (section OH) possible.</td>
</tr>
<tr>
<td>MS16</td>
<td>STS-48</td>
<td>STM-16 (STS-48); termination of RSOH (section OH) possible.</td>
</tr>
<tr>
<td>VC-4-64c</td>
<td>STS-192c-64c SPE</td>
<td>VC-4-64c (STS-192c-SPE); termination of RSOH (section OH), MSOH (line OH) and VC-4-64c TCM OH possible.</td>
</tr>
<tr>
<td>VC-4-16c</td>
<td>STS-48c-16c SPE</td>
<td>VC-4-16c (STS-48c-SPE); termination of RSOH (section OH), MSOH (line OH) and VC-4-16c TCM OH possible.</td>
</tr>
<tr>
<td>VC-4-4c</td>
<td>STS-12c-4c SPE</td>
<td>VC-4-4c (STS-12c-SPE); termination of RSOH (section OH), MSOH (line OH) and VC-4-4c TCM OH possible.</td>
</tr>
<tr>
<td>VC-4</td>
<td>STS-3c-4c SPE</td>
<td>VC-4 (STS-3c-SPE); termination of RSOH (section OH), MSOH (line OH) and VC-4 TCM OH possible.</td>
</tr>
<tr>
<td>VC-3</td>
<td>STS-1-3 SPE</td>
<td>VC-3 (STS-1-SPE); termination of RSOH (section OH), MSOH (line OH) and VC-3 TCM OH possible.</td>
</tr>
</tbody>
</table>

Note: In SDH it could be a higher order or lower order VC-3, this is
identified by the sub-addressing scheme. In case of a lower order VC-3 the higher order VC-4 OH can be terminated.

<table>
<thead>
<tr>
<th>VC-2</th>
<th>VT6-SPE</th>
<th>VC-2 (VT6-SPE); termination of RSOH (section OH), MSOH (line OH), higher order VC-3/4 (STS-1-SPE) OH and VC-2 TCM OH possible.</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>VT3-SPE</td>
<td>VT3-SPE; termination of section OH, line OH, higher order STS-1-SPE OH and VC3-SPE TCM OH possible.</td>
</tr>
<tr>
<td>VC-12</td>
<td>VT2-SPE</td>
<td>VC-12 (VT2-SPE); termination of RSOH (section OH), MSOH (line OH), higher order VC-3/4 (STS-1-SPE) OH and VC-12 TCM OH possible.</td>
</tr>
<tr>
<td>VC-11</td>
<td>VT1.5-SPE</td>
<td>VC-11 (VT1.5-SPE); termination of RSOH (section OH), MSOH (line OH), higher order VC-3/4 (STS-1-SPE) OH and VC-11 TCM OH possible.</td>
</tr>
</tbody>
</table>

The tables below outline the different signals, rates and granularities that have been defined for the OTN in G.709.

<table>
<thead>
<tr>
<th>OTU type</th>
<th>OTU nominal bit rate</th>
<th>OTU bit rate tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTU1</td>
<td>255/238 * 2 488 320 kbit/s</td>
<td>20 ppm</td>
</tr>
<tr>
<td>OTU2</td>
<td>255/237 * 9 953 280 kbit/s</td>
<td></td>
</tr>
<tr>
<td>OTU3</td>
<td>255/236 * 39 813 120 kbit/s</td>
<td></td>
</tr>
</tbody>
</table>

NOTE - The nominal OTUk rates are approximately: 2,666,057.143 kbit/s (OTU1), 10,709,225.316 kbit/s (OTU2) and 43,018,413.559 kbit/s (OTU3).

<table>
<thead>
<tr>
<th>ODU type</th>
<th>ODU nominal bit rate</th>
<th>ODU bit rate tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>ODU1</td>
<td>239/238 * 2 488 320 kbit/s</td>
<td>20 ppm</td>
</tr>
<tr>
<td>ODU2</td>
<td>239/237 * 9 953 280 kbit/s</td>
<td></td>
</tr>
<tr>
<td>ODU3</td>
<td>239/236 * 39 813 120 kbit/s</td>
<td></td>
</tr>
</tbody>
</table>

NOTE - The nominal ODUk rates are approximately: 2,498,775.126 kbit/s (ODU1), 10 037 273.924 kbit/s (ODU2) and 40 319 218.983 kbit/s (ODU3). ODU Type and Capacity (G.709)

<table>
<thead>
<tr>
<th>OPU type</th>
<th>OPU Payload nominal bit rate</th>
<th>OPU Payload bit rate</th>
<th>OPU Payload bit rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPU1</td>
<td>2488320 kbit/s</td>
<td>20 ppm</td>
<td></td>
</tr>
<tr>
<td>OPU2</td>
<td>238/237 * 9953280 kbit/s</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPU3</td>
<td>238/236 * 39813120 kbit/s</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NOTE - The nominal OPUk Payload rates are approximately:
2,488,320.000 kbit/s (OPU1 Payload), 9,995,276.962 kbit/s (OPU2 Payload) and 40,150,519.322 kbit/s (OPU3 Payload).

Appendix B: Protection and Restoration Schemes

For the purposes of this discussion, the following protection/restoration definitions have been provided:

Reactive Protection: This is a function performed by either equipment management functions and/or the transport plane (i.e. depending on if it is equipment protection or facility protection and so on) in response to failures or degraded conditions. Thus if the control plane and/or management plane is disabled, the reactive protection function can still be performed. Reactive protection requires that protecting resources be configured and reserved (i.e. they cannot be used for other services). The time to exercise the protection is technology specific and designed to protect from service interruption.

Proactive Protection: In this form of protection, protection events are initiated in response to planned engineering works (often from a centralized operations center). Protection events may be triggered manually via operator request or based on a schedule supported by a soft scheduling function. This soft scheduling function may be performed by either the management plane or the control plane but could also be part of the equipment management functions. If the control plane and/or management plane is disabled and this is where the soft scheduling function is performed, the proactive protection function cannot be performed. [Note that in the case of a hierarchical model of subnetworks, some protection may remain available in the case of partial failure (i.e. failure of a single subnetwork control plane or management plane controller) relates to all those entities below the failed subnetwork controller, but not its parents or peers.] Proactive protection requires that protecting resources be configured and reserved (i.e. they cannot be used for other services) prior to the protection exercise. The time to exercise the protection is technology specific and designed to protect from service interruption.

Reactive Restoration: This is a function performed by either the management plane or the control plane. Thus if the control plane and/or management plane is disabled, the restoration function cannot be performed. [Note that in the case of a hierarchical model of
subnetworks, some restoration may remain available in the case of partial failure (i.e. failure of a single subnetwork control plane or management plane controller) relates to all those entities below the failed subnetwork controller, but not its parents or peers.)

Restoration capacity may be shared among multiple demands. A restoration path is created after detecting the failure. Path selection could be done either off-line or on-line. The path selection algorithms may also be executed in real-time or non-real time depending upon their computational complexity, implementation, and specific network context.

- Off-line computation may be facilitated by simulation and/or network planning tools. Off-line computation can help provide guidance to subsequent real-time computations.

- On-line computation may be done whenever a connection request is received.

Off-line and on-line path selection may be used together to make network operation more efficient. Operators could use on-line computation to handle a subset of path selection decisions and use off-line computation for complicated traffic engineering and policy related issues such as demand planning, service scheduling, cost modeling and global optimization.

Proactive Restoration: This is a function performed by either the management plane or the control plane. Thus if the control plane and/or management plane is disabled, the restoration function cannot be performed. [Note that in the case of a hierarchical model of subnetworks, some restoration may remain available in the case of partial failure (i.e. failure of a single subnetwork control plane or management plane controller) relates to all those entities below the failed subnetwork controller, but not its parents or peers.)

Restoration capacity may be shared among multiple demands. Part or all of the restoration path is created before detecting the failure depending on algorithms used, types of restoration options supported (e.g. shared restoration/connection pool, dedicated restoration pool), whether the end-end call is protected or just UNI part or NNI part, available resources, and so on. In the event restoration path is fully pre-allocated, a protection switch must occur upon failure similarly to the reactive protection switch. The main difference between the options in this case is that the switch occurs through actions of the control plane rather than the transport plane. Path selection could be done either off-line or on-line. The path selection algorithms may also be executed in real-time or non-real time depending upon their computational complexity, implementation, and specific network context.
- Off-line computation may be facilitated by simulation and/or network planning tools. Off-line computation can help provide guidance to subsequent real-time computations.

- On-line computation may be done whenever a connection request is received.

Off-line and on-line path selection may be used together to make network operation more efficient. Operators could use on-line computation to handle a subset of path selection decisions and use off-line computation for complicated traffic engineering and policy related issues such as demand planning, service scheduling, cost modeling and global optimization.

Control channel and signaling software failures shall not cause disruptions in established connections within the data plane, and signaling messages affected by control plane outages should not result in partially established connections remaining within the network.

Control channel and signaling software failures shall not cause management plane failures.

Appendix C Interconnection of Control Planes

The interconnection of the IP router (client) and optical control planes can be realized in a number of ways depending on the required level of coupling. The control planes can be loosely or tightly coupled. Loose coupling is generally referred to as the overlay model and tight coupling is referred to as the peer model. Additionally there is the augmented model that is somewhat in between the other two models but more akin to the peer model. The model selected determines the following:

- The details of the topology, resource and reachability information advertised between the client and optical networks

- The level of control IP routers can exercise in selecting paths across the optical network

The next three sections discuss these models in more details and the last section describes the coupling requirements from a carrier’s perspective.
C.1. Peer Model (I-NNI like model)

Under the peer model, the IP router clients act as peers of the optical transport network, such that single routing protocol instance runs over both the IP and optical domains. In this regard the optical network elements are treated just like any other router as far as the control plane is concerned. The peer model, although not strictly an internal NNI, behaves like an I-NNI in the sense that there is sharing of resource and topology information.

Presumably a common IGP such as OSPF or IS-IS, with appropriate extensions, will be used to distribute topology information. One tacit assumption here is that a common addressing scheme will also be used for the optical and IP networks. A common address space can be trivially realized by using IP addresses in both IP and optical domains. Thus, the optical networks elements become IP addressable entities.

The obvious advantage of the peer model is the seamless interconnection between the client and optical transport networks. The tradeoff is that the tight integration and the optical specific routing information that must be known to the IP clients.

The discussion above has focused on the client to optical control plane inter-connection. The discussion applies equally well to inter-connecting two optical control planes.

C.2. Overlay (UNI-like model)

Under the overlay model, the IP client routing, topology distribution, and signaling protocols are independent of the routing, topology distribution, and signaling protocols at the optical layer. This model is conceptually similar to the classical IP over ATM model, but applied to an optical sub-network directly.

Though the overlay model dictates that the client and optical network are independent this still allows the optical network to re-use IP layer protocols to perform the routing and signaling functions.

In addition to the protocols being independent the addressing scheme used between the client and optical network must be independent in the overlay model. That is, the use of IP layer addressing in the clients must not place any specific requirement upon the addressing used within the optical control plane.

The overlay model would provide a UNI to the client networks through which the clients could request to add, delete or modify optical
connections. The optical network would additionally provide reachability information to the clients but no topology information would be provided across the UNI.

C.3. Augmented model (E-NNI like model)

Under the augmented model, there are actually separate routing instances in the IP and optical domains, but information from one routing instance is passed through the other routing instance. For example, external IP addresses could be carried within the optical routing protocols to allow reachability information to be passed to IP clients. A typical implementation would use BGP between the IP client and optical network.

The augmented model, although not strictly an external NNI, behaves like an E-NNI in that there is limited sharing of information.

Generally in a carrier environment there will be more than just IP routers connected to the optical network. Some other examples of clients could be ATM switches or SONET ADM equipment. This may drive the decision towards loose coupling to prevent undue burdens upon non-IP router clients. Also, loose coupling would ensure that future clients are not hampered by legacy technologies.

Additionally, a carrier may for business reasons want a separation between the client and optical networks. For example, the ISP business unit may not want to be tightly coupled with the optical network business unit. Another reason for separation might be just pure politics that play out in a large carrier. That is, it would seem unlikely to force the optical transport network to run that same set of protocols as the IP router networks. Also, by forcing the same set of protocols in both networks the evolution of the networks is directly tied together. That is, it would seem you could not upgrade the optical transport network protocols without taking into consideration the impact on the IP router network (and vice versa).

Operating models also play a role in deciding the level of coupling. [Freeland] gives four main operating models envisioned for an optical transport network: - ISP owning all of its own infrastructure (i.e., including fiber and duct to the customer premises)

- ISP leasing some or all of its capacity from a third party

- Carriers carrier providing layer 1 services

- Service provider offering multiple layer 1, 2, and 3 services over a common infrastructure
Although relatively few, if any, ISPs fall into category 1 it would seem the mostly likely of the four to use the peer model. The other operating models would lend themselves more likely to choose an overlay model. Most carriers would fall into category 4 and thus would most likely choose an overlay model architecture.