IPO WG
Internet Draft
Document: draft-ietf-ipo-ason-02.txt
Category: Informational
Expires: September 2002

O. Aboul-Magd
B. Jamoussi
S. Shew
Nortel Networks

Gert Grammel
Sergio Belotti
Dimitri Papadimitriou
Alcatel

March 2002

Automatic Switched Optical Network (ASON) Architecture and Its Related Protocols

Status of this Memo

1. Abstract

This draft describes the main architectural principles of the automatic switched optical networks (ASON) work that has recently been approved by the ITU-T [2,3]. ASON architecture defines a set of reference points (interfaces) that allows ASON clients to request network services across those reference points.

The protocols that run over ASON interfaces are not specified in [2,3]. IP-based protocols like generalized MPLS (GMPLS) [4], can be considered such that the ASON/ASTN work can benefit from the protocols design work progressing at the IETF. In order to cross-fertilize the discussion the basic concepts are described hereafter.

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 [5].

3. Introduction

The existing transport networks provide SONET/SDH and WDM services whose connections are provisioned via network management. This process is both slow (weeks to months) relative to the switching speed and costly to the network providers.

An automatic switched optical network (ASON) is an optical/transport network that has dynamic connection capability. It encompasses SONET/SDH, wavelength, and potentially fiber connection services in both OEO and all-optical networks. There are a number of added values related to such a capability:

- Traffic engineering of optical channels: Where bandwidth assignment is based on actual demand patterns.

- Mesh network topologies and restoration: Mesh network topologies can in general be engineered for better utilization for a given demand matrix. Ring topologies might not be as efficient due to the asymmetry of traffic patterns.

- Managed bandwidth to core IP network connectivity: A switched optical network can provide bandwidth and connectivity to an IP network in a dynamic manner compared to the relatively static service available today.

- Introduction of new optical services: The availability of switched optical networks will facilitate the introduction of new services at the optical layer. Those services include bandwidth on demand and optical virtual private networks (OVPN).

This draft describes the main ASON architecture principles. This work has recently been approved by the ITU-T.

4. ASON Architecture Principles

This section gives a quick summary of ASON architecture principles as defined in [3]. There is no intention to give a comprehensive account of the architecture. The interested reader may refer to [3] and the references therein.

ASON defines a control plan architecture that allows the setup and teardown of calls (and the connections that support a call) as a result of a user request. To achieve global coverage and the support of multiple client types, the architecture is described in terms of components and a set of reference points and rules must be applied at the interface points between clients and the network and between networks.

4.1 ASON Reference Points

In ASON architecture there is the recognition that the optical network control plan will be subdivided into domains that match the administrative domains of the network. The transport plane is also partitioned to match the administrative domains. Within an administrative domain the control plane may be further subdivided, e.g., by actions from the management plane. This allows the separation of resources into, for example, domains for geographic regions, that can be further divided into domains that contain different types of equipment. Within each domain, the control plane may be further sub divided into routing areas for scalability, which may also be further subdivided into sets of control components. The transport plane resources used by ASON will be partitioned to match the sub divisions created within the control plane.

The interconnection between domains, routing areas and, where required, sets of control components is described in terms of reference points. The exchange of information across these reference points is described by the multiple abstract interfaces between control components. The physical interconnection is provided by one or more of these interfaces. A physical interface is provided by mapping an abstract interface to a protocol. The reference point between an administrative domain and an end user is the UNI. The reference point between domains is the E-NNI. The reference point within a domain between routing areas and, where required, between sets of control components within routing areas is the I-NNI. Figure 1 shows a possible domain subdivisions and the reference points between them

```
+-------+  UNI  +------------+ E-NNI +------------+
|client|-------| Provider A|-------| Provider B| UNI +-------+
+-------+       | Domain "1"|       | Domain "1"|-----|client|
                |  (I-NNI)  |       |   (I-NNI) |     +-------+
                +------------+       +------------+
```

```
                          |          /
                    E-NNI |         /  E-NNI
                          |        /
                        +-----------+
           +------+ UNI | Provider A|
           |client|-----| Domain "2"|
           +------+     |  (I-NNI)  |
                        +-----------+
```

Figure 1: ASON/ASTN Global Architecture

The difference between the I-NNI and the E-NNI is significant. I-NNI is applied in a single routing area where all equipment support the same routing protocol and detailed routing information could be exchanged between the different nodes. On the other hand E-NNI is

mainly concerned with reachability between domain that employs different routing and protection methodologies.

4.2 Call and Connection Control Separation

Call and connection control are treated separately in ASON architecture. 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 is provided at the ingress/egress of the network or at domain boundaries. Call control is applicable at the E-NNI and UNI reference points. Call and connection control separation allows intermediate (relay) network elements to support only procedures needed for the support of switching connections. Access to call information at domain boundaries allows domains that use different protection or restoration mechanisms to inter-work (e.g. a Metro network using UPSR with a backbone network using Mesh Restoration) without the need for all domains to understand all of the possible protection/restoration schemes.

With call and connection control separation a single call may embody a number of connections (more than one) between user applications. This allows for the introduction of enhanced services where a single call is composed of more than one application, e.g. voice and video. There are other situations where this separation between call and connection control is beneficial to the service provider, especially in the areas of restoration and maintenance. In those situations it is cost saving to maintain the call state while restoration actions are underway.

4.3 Policy and Security

According to the ASON architecture policy is defined as the set of rules applied at a system boundary, and implemented by port controller components. System boundaries may be nested to allow for correct modeling of shared policies with any scope. A system is defined as any (arbitrary) collection of components. In general a system boundary will coincide with a domain boundary, this allows the application of a common policy for all interfaces that cross the domain boundary. The nesting of system boundaries allows the application of additional (more stringent) policies if the domain boundaries are between cost centers within a single network (administration) or between different networks (administrations).

Policy is applied at individual interfaces crossing the reference points described before.

4.4 Federation

Connection control across multiple domains requires the cooperation between controllers in the different domains. A federation is defined as the community of domains that co-operate for the purpose of connection management. Two types of federations are defined, joint federation model where one connection controller has authority over connection controllers that reside in different domains. The second model is a co-operative model where there is no concept of a parent connection controller.

5. ASON Control Plane Requirements

A well-designed control plane architecture should give service providers better control of their network, while providing faster and improved accuracy of circuit set-up. The control plane itself should be reliable, scalable, and efficient. It should also be sufficiently generic to support different technologies and differing business needs and different partitions of functions by vendors (i.e., different packaging of the control plane components). In summary, the control plane architecture should:

- Be applicable to a variety of transport network technologies (e.g., SONET/SDH, OTN, PXC). In order to achieve this goal, it is essential that the architecture isolates technology dependent aspects from technology independent aspects, and address them separately.

- Be sufficiently flexible to accommodate a range of different network scenarios. This goal may be achieved by partitioning the control plane into distinct components. This, allows vendors and service providers to decide the location of these components, and also allows the service provider to decide the security and policy control of these components.

The control plane shall support either switched connections (SC) of soft permenant connections (SPC) of basic connection capability in transport networks. These connection capabilities types are:

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

The control of connectivity is essential to the operation of a transport network. The transport network itself can be described as a set of layer networks, each acting as a connecting function whereby associations are created and removed between the inputs and outputs of the function. These associations are referred to as connections. Three types of connection establishment are defined: provisioned, signaled, and hybrid.

Establishment of Provisioned connection is triggered by a management system and is referred to as hard permanent connection. Signaled

connections is established on demand by the communicating end points using a dynamic protocol message exchange in the form of signaling messages. In hybrid connection a network provides a permanent connection at the edge of the network and utilizes a switched connection within the network to provide end-to-end connections between the permanent connections at the network edges.

The most significant difference between the three methods above is the party that sets up the connection. In the case of provisioning, connection set up is the responsibility of the network operator, whilst in the signaled case; connection set-up may also be the responsibility of the end user. Additionally, third party signaling should be supported across a UNI.

6. ASON Functional Architecture

The components of the control plane architecture are:

1. Connection Controller Function (CC): The connection controller is responsible for coordination among the Link Resource Manager, Routing Controller for the purpose of the management and supervision of connection setup, release and modification.

2. Routing Controller (RC): The role of the RC is to respond to requests from CC for route information needed to setup a connection, and to respond to requests for topology information for network management purposes.

3. Link Resource Management (LRM): The LRM component are responsible for the management of subnetwork links including the allocation and de-allocation of resources, providing topology and status information.

4. Traffic Policing (TP): The role of the TP is to check that the incoming user connection is sending traffic according to the parameters agreed upon.

5. Call Controller: There are two types of call controller, a calling/called party call controller and a network call controller. The role of the call control is the generation and processing of call requests.

6. Protocol Controller (PC): The PC provides the function mapping of the parameters of the abstract interfaces of the control components into messages that are carried by a protocol to support interconnection via an interface.

7. ASON Reference Points and GMPLS Protocols

The ASON CP as shown in Figure 1 defines a set of interfaces or reference points:

- User-Network Interface (UNI): UNI runs between the optical client and the network.

- Internal Node-to-Node Interface (I-NNI): I-NNI defines the interface between the signaling network elements within the same domain or between routing areas.

- External Node-to-Node Interface (E-NNI): E-NNI defines the interface between ASON control planes belonging to different domains.

The different ASON interfaces are described in the next few sections. Candidate GMPLS-based protocols for use at the different interfaces are also discussed.

7.1 ASON User-Network Interface

ASON UNI allows ASON client to perform a number of functions including:

- Connection Create: Allows the clients to signal to the network to create a new connection with specified attributes. Those attributes might include bandwidth, protection, restoration, and diversity.

- Connection Delete: Allows ASON clients to signal to the network the need to delete an already existing connection.

- Connection Modify: Allows ASON clients to signal to the network the need to modify one or more attribute for an already existing connection.

- Status Enquiry: Allows ASON clients to enquire the status of an already existing connection.

Other functions that might be performed at the ASON UNI are, client registration, address resolution, neighbor and service discovery. Those functions could be automated or manually configured between the network and its clients.

Client registration and address resolution are tightly coupled to the optical network address scheme. Requirements for optical network addresses and client names are outlined in [6]. In general the client name (or identification) domain and optical address domain are decoupled. The client id should be globally unique to allow for the establishment of end-to-end connections that encompass multiple administration domains. For security, it is required that the nodal addresses used for routing within an optical domain do not cross network boundaries. The notion of closed user groups should also be included in ASON addressing to allow for the offering of OVPN services.

ASON UNI realization requires the implementation of a signaling protocol with sufficient capabilities to satisfy UNI functions. Both LDP [7] and RSVP-TE [8] have been extended to be used the signaling protocol across the ASON UNI. The extensions involve the definition of the necessary TLVs or objects to be used for signaling connection attributes specific to the optical layer. New messages are also defined to allow for connection status enquiry. The Optical Internetworking Forum (OIF) has adopted both protocols in its UNI 1.0 specification [9].

7.2 ASON Internal Node-to-Node Interface

The I-NNI defines the interface between adjacent connection controls (CC) in the same domain or between routing areas. There are two main aspects of I-NNI. Those are signaling and routing.

Path selection and setup through the optical network requires a signaling protocol. Transport networks typically utilize explicit routing, where path selection can be done either by operator or software scheduling tools in management systems. IN ASON, end-to-end optical channels (connections) are requested with certain constraints. Path selection for a connection request should employ constrained routing algorithms that balance multiple objectives:

- Conform to constraints such as physical diversity, etc.

- Load balancing of network traffic to achieve the best utilization of network resources.

- Follow policy decisions on routing such as preferred routes.

To facilitate the automation of the optical connection setup, nodes in the optical network must have an updated view of its adjacencies and of the utilization levels at the various links of the network. This updated view is sometime referred to as state information.

State information dissemination is defined as the manner in which local physical resource information is disseminated throughout the network. First the local physical resource map is summarized into logical link information according to link attributes. This information can then be distributed to the different nodes in the network using the control plane transport network IGP.

ASON I-NNI could be based on two key protocols, IP and MPLS. Since MPLS employs the principle of separation between the control and the forward planes, its extension to support I-NNI signaling is feasible. Generalized MPLS [4] defines MPLS extensions to suit types of label switching other than the in-packet label. Those other types include, time slot switching, wavelength and waveband switching, and position switching between fibers. Both CR-LDP [10] and RSVP-TE [11] have been extended to allow for the request and the binding of generalized labels. With generalized MPLS, a label switched path (LSP) is established with the appropriate encoding type (e.g. SONET,

wavelength, etc.). LSP establishment takes into account specific characteristics that belong to a particular technology.

MPLS traffic engineering requires the availability of routing protocols that are capable of summarizing link state information in their databases. Extensions to IP routing protocols, OSPF and IS-IS, in support of link state information for generalized MPLS are described in [12, 13].

7.3 ASON External Node-to-Node Interface

E-NNI is the external NNI between different domains. Those domains may belong to the same network administration, or to different administrations. In some sense, E-NNI could be viewed as similar to the UNI interface with some routing functions to allow for the exchange of reachability information between different domains.

BGP is the IP based protocol that is commonly deployed between different domains. It could be used to summarize reachability information between different ASON domains in the same manner as it has been in use today for IP networks. BGP is rich in policy which makes a good candidate to satisfy service requirements such as diversity where policies could be used in choosing diverse routes.

8. ASON/ASTN CP Transport Network (signaling Network)

In this section, we detail some architectural considerations for the makeup of the transport network that is used to transport the control plane information. For circuit-based networks, the ability to have an independent transport network for message transportation is an important requirement.

The control network represents the transport infrastructure for control traffic, and can be either in-band or out-of-band. An implication of this is that the control plane may be supported by a different physical topology from that of the underlying ASON. There are fundamental requirements that control networks must satisfy in order to assure that control plane data can be transported in a reliable and efficient manner. In the event of control plane failure (for example, communications channel or control entity failure), while new connection operations will not be accepted, existing connections will not be dropped. Control network failure would still allow dissemination of the failure event to a management system for maintenance purposes. This implies a need for separate notifications and status codes for the control plane and ASON. Additional procedures may also be required for control plane failure recovery.

It is recognized that the inter-working of the control networks is the first step towards control plane inter-working. To maintain a certain level of ease, it's desirable to have a common control network for different domains/sub-networks or types of network.

Typically, control plane and transport functions may co-exist in a network element. However, this may not be true in the case of a third party control. This situation needs further study. Furthermore, addressing issues in the control plane vis- -vis the transport network is also for further study.

ASON CP transport network requirements includes:

- Control plane message transport should be secure. This requirement stems from the fact that the information exchanged over the control plane is service-provider specific and security is of utmost importance.

- Control message transport reliability has to be guaranteed in almost all situations, even during what might be considered catastrophic failure scenarios of the controlled network.

- The control traffic transport performance affects connection management performance. Connection service performance largely depends on its message transport. Time sensitive operations, such as protection switching, may need certain QoS guarantees. Furthermore, a certain level of survivability of the message transport should be provided in case of control network failure.

- The control network needs to be both upward and downward scalable in order for the control plane to be scalable. Downward scalability may be envisioned where the ASON network offers significant static connections, reducing the need for an extended control network.

- The control plane protocols shall not assume that the signaling network topology is identical to that of the transport network. The control plane protocols MUST operate over a variety of signaling network topologies.

Given the above requirements, it is critical that the maintenance of the control network itself not pose a problem to service providers.

As a corollary this means that configuration-intensive operations should be avoided for the control network.

Common channel signaling links are associated with user channels in the following ways:

- Associated, whereby signaling messages related to traffic between two network elements are transferred over signalling links that directly connect the two network elements
- Non-associated, whereby signaling messages between two network elements A and B are routed over several signalling links, whilst traffic signals are routed directly between A and B. The signalling links used may vary with time and network conditions
- Quasi-associated, whereby signaling messages between nodes A and B follow a predetermined routeing path over several signalling links whilst the traffic channels are routed directly between A and B.

Associated signaling may be used where the number of traffic channels between two network elements is large, thereby allowing a single signaling channel to be shared amongst a large number of traffic channels.

Quasi-associated signaling may be used to improve resiliency. For example consider a signaling channel that has failure mechanisms independent of the traffic channels. Failure of the signaling channel will result in loss of signaling capability for all traffic channels even if all the traffic channels are still functional. Quasi-associated signaling mitigates against this by employing alternative signaling routes. In other words the signaling network must be designed such that failure of a signaling link shall not affect the traffic channels associated with that signaling channel.

9. Transport Network Survivability and Protection

This section describes the strategies that can be used to maintain the integrity of an existing call in the event of failures within the transport network. The terms ôProtectionö (replacement of a failed resource with a pre-assigned standby) and ôRestorationö (replacement of a failed resource by re-routing using spare capacity) are used to classify these techniques. In general, protection actions complete in the tens of millisecond range, while restoration actions normally complete in times ranging from hundreds of milliseconds to up to a few seconds

The ASON control plane provides a network operator with the ability to offer a user calls with a selectable class-of-service (CoS), (e.g., availability, duration of interruptions, Errored Seconds, etc). Protection and restoration are mechanisms (used by the network) to support the CoS requested by the user. The selection of the survivability mechanism (protection, restoration or none) for a particular connection that supports a call will be based on; the policy of the network operator, the topology of the network and the capability of the equipment deployed. Different survivability mechanisms may be used on the connections that are concatenated to provide a call. If a call transits the network of more than one operator then each network should be responsible for the survivability of the transit connections. Connection requests at the UNI or E-NNI will contain only the requested CoS, not an explicit protection or restoration type.

The protection or restoration of a connection may be invoked or temporarily disabled by a command from the management plane. These commands may be used to allow scheduled maintenance activities to be performed. They may also be used to override the automatic operations under some exceptional failure conditions.

The Protection or Restoration mechanism should:

- Be independent of, and support any, client type (e.g., IP, ATM, SDH, Ethernet).
- Provide scalability to accommodate a catastrophic failure in a server layer, such as a fiber cable cut, which impacts a large number client layer connections that need to be restored simultaneously and rapidly.
- Utilize a robust and efficient signaling mechanism, which remains functional even after a failure in the transport or signaling network.
- Not rely on functions which are non-time critical to initiate protection or restoration actions. Therefore consideration should be given to protection or restoration schemes that do not depend on fault localization.

10. Relationship to GMPLS Architecture

The relationship between ASON/ASTN control plane architecture and GMPLS-based protocols is established in section 6, where it has been shown how the different GMPLS protocol could be used for the realization of the different ASON/ASTN external interfaces.

Recently, a GMPLS architecture [14] has been introduced. It is important to note that there is no real conflict between GMPLS architecture and the network architecture presented in this draft. ASON/ASTN provides a functional architecture of a control plane that allows the establishment of switched paths in optical networks. It provides the set of external interfaces that are necessary for the ASTN/ASON network to have a global reach. It does that, however, in a protocol independent fashion that can be realized in a different ways provided that its requirements are satisfied.

The GMPLS architecture focuses more on the applications of GMPLS-defined protocols, e.g. CR-LDP for the setup of generalized LSP (GLSP) at the different interfaces of the network, e.g. I-NNI, UNI, etc. It does that in a more comprehensible way than what is described in section 6 of this draft.

11. Other ASON/ASTN Related ITU Activities

This section describes other activities that are currently underway at the ITU and are related to ASON/ASTN architecture.

11.1 Common Equipment Management (G.cemr)

G.cemr [15] recommendation specifies those Equipment Management Functions (EMF) requirements that are common for SDH and OTN. The equipment management function (EMF) provides the means through which a Network Element Level manager manages the Network Element Function (NEF).

These kind of functions are not detailed in the current GMPLS work since it is focused on control plane related aspects. Network

Management aspects are subjects of other working groups in IETF such as OPS WG.

11.1.1 MPLS solution

Element Manager functions are not part of the control plane specifications in GMPLS.

11.1.2 Requirements

- Network management applications shall perform, Fault, Configuration, Accounting, Performance and Service Management (FCAPS).
- Path setup can be triggered by means of a Network Management System using control plane mechanisms
- For path setup control plane and Network management systems shall cooperate to allow path provisioning by network

management as well as provisioning using the control plane.

11.2 Data Communications Network (G.7712/Y.1703)

In [16] the various functions constituting a telecommunications network can be classified into two broad functional groups. One is the transport functional group which transfers any telecommunications information from one point to another point(s). The other is the control functional group which realizes various ancillary services and operations and maintenance functions.

The Data Communications Network (DCN) provides transport for the applications associated with the control functional group. Examples of such applications that are transported by the DCN are: transport network operations/management applications, DCN operations/management applications, Automatic Switched Transport Services (ASTN) control plane applications, voice communications, etc.

The IP-based DCN provides Layer 1 (physical), Layer 2 (data-link) and Layer 3 (network) functionality and consists of routing/switching functionality interconnected via links. These links can be implemented over various interfaces, including WAN interfaces, LAN interfaces, and ECCs.

This recommendation provides the architecture requirements for an IP-based DCN, the requirements for inter-working between an IP-based DCN and an OSI-based DCN, and the IP-based DCN interface specifications.

11.2.1 GMPLS solution

Since in GMPLS the signaling and management plane are independent from each other, different kinds of networks can be used for both tasks. Today GMPLS itself can be managed by the use of GMPLS MIB (draft-nadeau-mpls-gmpls-te-mib-00.txt and referenced). In the view of GMPLS each node is capable to process signaling and routing

messages whereby the topology of the transport network and the control-plane network are the same.

11.2.2 Requirements

- The management and signaling functions shall be decoupled from each other
- the DCN shall support in-fiber-in-band, in-fiber-out-of-band and out-of-fiber/out-of-band signaling for any kind of

technology
- DCN shall be dimensioned to support fast restoration by providing fast transport of restoration messages.
- DCN shall be IP based and support IP addressing.
- IP routing mechanisms (OSPF, IS-IS) shall be used

11.3 Distributed Connection Management (G.7713/Y.1704)

G.7713/Y.1704 [17] Recommendation covers the areas associated with the signalling aspects of automatic switched transport network, such as attribute specifications, the message sets, the interface requirements, the DCM state diagrams, and the interworking functions for the distributed connection management

11.3.1 GMPLS solution

In GMPLS a permanent communication between the Network devices is established which is anyhow necessary to exchange reachability and traffic-engineering information (e.g. routing protocol provides reachability and TE attributes information). Link bundling plays a key role by augmenting the scalability of the routing protocol. A user device or a management station can optionally trigger a connection setup and initiates a control plane action.

1. In a first phase the edge device (where the Trail Termination is located) has to determine the route (trail) either by a route calculation (e.g. explicit route computation through C-SPF) or by receiving a pre-calculated route from an external device e.g. a Traffic Engineering Tool.
2. Then it signals the trail request to the involved nodes across the network, reserving the bandwidth without allocating it.
3. When bandwidth reservation has been performed the trail is implemented.

Some optimizations have also been added in order to speed up the process of implementing the connection. The full procedure is explained in more detail in draft-ietf-mpls-generalized-signaling-05.txt.

11.3.2 Requirements

GMPLS control plane components could be applied to ASTN to achieve a distributed connection control taking into account draft-ietf-mpls-generalized-signaling-05.txt.

11.4 Generalized Automatic Discovery (G.7714/Y.1705)

G.7714/Y.1705 [18] describes the specifications for automatic discovery (referred to as auto-discovery) to aid distributed connection management (DCM) and routing in the context of automatically switched transport networks (ASTN/ASON). In this recommendation, three major instances of discovery are addressed, (a) adjacency discovery (b) neighbor discovery (c) service discovery. In addition, the results of neighbor discovery are also used for establishing logical adjacencies between nodes at the control plane.

11.4.1 Adjacency Discovery

Adjacency discovery is described as the process of verifying physical connectivity between two ports on adjacent network elements over a specific physical layer. Depending on the physical packaging of the functions within a network element, two types of associations need to be discovered as part of adjacency discovery.

11.4.2 GMPLS Solution

Optical Link Interface (OLI) concept and requirement are proposed in conjunction with LMP-WDM protocol to cover the functions provided by adjacency discovery. From the GMPLS perspective, information exchange occurs between a ôpassiveö and an ôactiveö element, such as between a DWDM (OLS) system and an OXC. Ongoing work with ITU referred to as G.VBI (Virtual Backplane Interface) will complete the picture.

11.4.3 Requirements

- Adjacency discovery should be provided through a simple protocol mechanism for reporting the health and properties of OLSs based on a well-defined set of parameters.

- It should be extensible so that we can start with a set of most-needed parameters initially, and be able to extend later by adding new parameter types and new parameters within a type.

- The initial focus is on SONET and SDH equipment. However, the OLI must be extensible to support other types of equipment such as Ethernet and G.709 OTN.

- The adjacency must be reliable, not only assume a one-to-one relationship between OLS and client i.e., an OLS client will most likely be attached to multiple different OLSs, and a single OLS may have multiple different clients at a single location.

11.4.4 Neighbor Discovery

[18] Recommendation provides the requirements and message sets for the automatic neighbor for the User-to-Network Interface (UNI),

Internal Node-to-Node Interface (I-NNI), External Node-to-Node Interface (E-NNI) and Physical Interface (PI). The requirements in this Recommendation specify the discovery process across these interfaces that aid automated connection management.

11.4.5 GMPLS solution

MPLS is based on an IP-based control plane incorporating protocols defined for routing and neighbor discovery defined in OSPF and IS-IS. To achieve a single control plane across multiple technology layers a single method for neighbor discovery and routing is mandatory. LMP extensions for neighbor discovery have solved the ôpotentialö problem of the usage of a routing protocol at the UNI (when considering for instance OIF UNI 1.0 specification)

11.4.6 Requirements

- Neighbor Discovery shall be used to detect and maintain Node adjacencies. For this the mechanisms already defined at the IETF for OSPF and IS-IS shall be used.
- Topology information and resource information shall be decoupled. While topology information remains unchanged, resource utilization can change dynamically when setting up new path. To support this concept the links between two adjacent nodes shall be bundled. In case of any single link failure within the bundle, the topology information remains stable while the capacity information may change.
- The control plane shall detect changes in the resources and enable timely reaction if established path or network resources are affected by this change.

11.4.7 Service Discovery

[18] provides the requirements and message sets for the automatic service discovery for the User-to-Network Interface (UNI), Internal Node-to-Node Interface (I-NNI), External Node-to-Node Interface (E-NNI) and Physical Interface (PI). The requirements in this Recommendation specifies the discovery process across these interfaces that aid automated connection management.

11.4.8 GMPLS solution

GMPLS focuses on intra-domain implementation on which OIF based itÆs UNI specification. OIF-UNI GMPLS profile can be considered when discussing about UNI implementations. Extensions of LMP enables the exchange of service discovery information at the UNI 1.0 specification.

11.4.9 Requirements

- Service discovery mechanisms shall be aligned with the mechanisms provided by GMPLS such that a seamless integration of UNI and NNI can be supported.

11.5 OTN routing (G.rtg)

A first outline has been presented during the last ITU Q14/SG15 meeting, however one doesnÆt expect to see a more complete specification prior to Mid-2002.

11.5.1 GMPLS solution

GMPLS is supposed to be based on OSPF/IS-IS routing mechanisms and more explicitly to the traffic engineering extensions of these protocols like e.g. CSPF. See also: ôdraft-kompella-ospf-gmpls-extensions-01.txt OSPF Extensions in Support of Generalized MPLSö and ôdraft-ietf-isis-gmpls-extensions-02.txt IS-IS Extensions in Support of Generalized MPLSö. Today on-going work related to GMPLS/BGP has started as well in order to cover inter-domain routing specification for non-packet based networks (such as draft-parent-optical-bgp-00.txt) It allows also to use explicit or implicit routing.

11.5.2 Requirements

- Support of explicit and implicit routing
- Support of OSPF and ISIS routing protocols for intra-domain and subsequently BGP for inter-domain routing
- Support of constrained based routing in order to e.g. Conform to constraints such as physical diversity, Achieve traffic engineering objectives in the transport network. Examples are to adhere to operator policies on routing such as preferred routes or to conform to network specific constraints

11.6 OTN Connection Admission Control (G.cac)

Connection admission control (CAC) is necessary for authentication of the user and controlling access to network resources. 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 to allow a new connection. à If there is, the CAC may permit the connection request to proceed, alternatively, if there is not, it shall notify the originator of the connection request that the request has been denied. Connections may be denied on the basis of available free capacity or alternatively on the basis of prioritisation. CAC policies are outside the scope of standardisation.ö

11.6.1 GMPLS solution

Call admission control in the sense of authentication and access control is not explicitly addressed in GMPLS since a trusted relation in a single operator, multi-vendor network is assumed. The

work related to connection admission is performed e.g. in OIF. Related issues like security of signaling protocols is already included in RSVP-TE and CR-LDP. However, if a given LSP can not be established through the network (for reasons as diverse as resource unavailability, overbooking, control-plane congestion, etc.) it is simply rejected.

11.6.2 Requirements

None

11.7 OTN Link Management (G.lm)

No ITU-T contribution available prior to October 2001.

11.7.1 GMPLS solution

The Link Management Protocol defined in draft-ietf-ccamp-lmp-00.txt is used to manage the resources available between two nodes and to check the connections. It is closely related to the unnumbered interface and bundling concepts described in ôdraft-kompella-mpls-bundle-05.txt Link Bundling in MPLS Traffic Engineeringö.

11.7.2 Requirements

- Link management shall form a consistent network level resource view between adjacent nodes.
- The use of link management shall decouple resource information from topology information which is bound to the bundling concept.
- LMP as under definition in IETF (draft-ietf-ccamp-lmp-00.txt) shall be considered for G.lm.

12. Security Considerations

This draft does not introduce any unknown security issues.

13. References

1 Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

2 Mayer, M. Ed., "Requirements for Automatic Switched Transport Networks (ASTN)", ITU G.8070/Y.1301, V1.0, May 2001.

3 M. Mayer, Ed., "Architecture for Automatic Switched Optical Networks (ASON)", ITU G.8080/Y1304, V1.0, October 2001

4 Ashwood-Smith, P. et. al., "Generalized MPLS- Signaling Functional Description", draft-ietf-mpls-generalized-signaling-04.txt, work in progress, May. 2001

5 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

6 Lazar, M. et. al., "Alternate Addressing Proposal", OIF Contribution, OIF2001.21, January 2001.

7 Aboul-Magd, O. et. al., "LDP Extensions for Optical User Network Interface (O-UNI) Signaling", draft-ietf-mpls-ldp-uni-optical-01.txt, work in progress, July 2001.

8 Yu, J., et. al., "RSVP Extensions in Support of OIF Optical UNI Signaling", draft-yu-mpls-rsvp-oif-uni-00.txt, work in progress, Dec. 2000.

9 Rajagopalan, B. Editor, "User Network Interface (UNI) 1.0 Signaling Specifications", OIF Contribution, OIF2000.125.7, October 2001

10 Ashoowd-Smith, P. et. al., "Generalized MPLS Signaling: CR-LDP Extensions", draft-ietf-mpls-generalized-cr-ldp-03.txt, work in

progress, May 2001

11 Ashwood-Smith, P. et. al., "Generalized MPLS Signaling: RSVP-TE Extensions", draft-ietf-mpls-generalized-rsvp-te-03.txt, work in progress, May 2000.

12 Kompella, K. et. al., "IS-IS Extensions in Support of Generalized MPLS", draft-ietf-isis-gmpls-extensions-01.txt, work in progress, Nov. 2000.

13 Kompella, K. et. al., "OSPF Extensions in Support of Generalized MPLS", draft-kompella-ospf-gmpls-extensions-01.txt, work in progress, Nov. 2000.

14 Mannie, E., Ed., "Generalized Multi-Protocol Lable Switching (GMPLS) Architecture" draft-ietf-ccamp-gmpls-architecture-00.txt, work in progress, June 2001.

15 Draft New RecommendationG.cemr, Common Equipment Management Function Requirements, ITU, June 2001

16 C. Daloia, Ed., "Architecture and Specification of Data Communication Network", ITU G.7712/Y.1703, October 2001

17 Z. Lin, Ed., "Distributed Call and Connection Management", ITU G.7713/Y.1704, October 2001

18 S. Sankaranarayanan, Ed., "Generalized Automatic Discovery Techniques", ITU G.7714/Y.1705, October 2001.

14. Author's Addresses

Osama Aboul-Magd
Nortel Networks
P.O. Box 3511, Station C
Ottawa, Ontario, Canada
K1Y-4H7
Phone: 613-763-5827
E.mail: Osama@nortelnetworks.com

Bilel Jamoussi

Nortel Networks
600 Technology Park Drive
Billerica, MA 01821, USA
Phone: 978-288-4506
Email: jamoussi@nortelnetworks.com

Stephen Shew
Nortel Networks
P.O. Box 3511, Station C
Ottawa, Ontario, Canada
K1Y-4H7
Phone: 613-763-2462
Email: sdshew@nortelnetworks.com

Gert Grammel
Alcatel
Via Trento 30,
I-20059 Vimercate, Italy
Phone: +39 039 686-4453
Email: gert.grammel@netit.alcatel.it

Sergio Belotti
Alcatel
Via Trento 30,
I-20059 Vimercate, Italy
Phone: +39 039 686-7060
Email: sergio.belotti@netit.alcatel.it

Dimitri Papadimitriou
Alcatel
Francis Wellesplein 1,
B-2018 Antwerpen, Belgium
Phone: +32 3 240-8491
Email: Dimitri.Papadimitriou@alcatel.be

Full Copyright Statement