OPEN NETWORKING
FOUNDATION

Requirements Analysis for Transport OpenFlow/SDN

V1.0
August 20, 2014

ONF TR-508

ONF Document Type: TR (Technical Recommendation)
ONF Document Name: TR_Requirements Analysis for Transport OpenFlow/SDN_v.1.0

Disclaimer

THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE.

Any marks and brands contained herein are the property of their respective owners.

Open Networking Foundation
2275 E. Bayshore Road, Suite 103, Palo Alto, CA 94303
www.opennetworking.org

1 Introduction

This document provides a set of architectural and protocol requirements and considerations based upon well-established transport network attributes and derived from analysis of the Optical Transport WG Use Case document [1], as well as from other documents produced within ONF and from other organizations (in particular, the Security Requirements document [2] and the OIF Carrier WG Transport SDN Requirements document [3]].)

Beginning with a summary of transport network attributes, this document identifies requirements and considerations that are relevant to the OT WG Architecture, OT WG Information Model, and OpenFlow/SDN protocols. A focus of the document is on requirements impacting the OpenFlow-switch protocol, which forms the basis for extensions recommended in [4].

1.1 Terms and Abbreviations

OT WG	Optical Transport Working Group
OTN	Optical Transport Network
OAM	Operations, Administration and Maintenance
MPLS-TP	MPLS-Transport Profile
EMS/NMS	Element/Network Management System
ASON/GMPLS	Automatic Switched Optical Network/Generalized MultiProtocol Label Switching
SLA	Service Level Agreement
NE	Network Element

1.2 Conventions

This document uses the keywords "may" and "must" to qualify optional and mandatory requirements.

2 Transport Network Attributes

This section provides a high-level summary of transport network attributes for background and as a basis for subsequent requirements sections.

2.1 Overview of Transport Network Attributes

The global transport network is provided by a number of interconnected but independent transport networks, each run by a different network operator. Each of these transport networks may cover a large geographic area and contain a variety of transport equipment and systems. These networks offer connectivity services to large numbers of clients. Traffic from the users is collected and aggregated for transport across the network. The transport network is designed with the intention of assuring that traffic from one user does not impact the service provided to other users.

The transport network may consist of many different technologies, such as OTN, Ethernet, and MPLS-TP. These different technologies provide independent layer networks. Transport network architectures and protocols are designed to provide client/server independence so that the network operator is free to choose the most appropriate server technology to support the client service(s) they offer. Different server layers may be used in different parts of the network; the client is unaware of the particular server layer that is being used. This independence also allows a wide variety of clients to be supported across a common infrastructure and allows new types of clients to be supported without changes to the infrastructure.

Within the transport network, the forwarding of the data flows within a connection is independent from the control/management mechanisms used to setup the connection (e.g., signaling and routing functions.) The topology of the transport network is not assumed to be congruent with the topology of the communications network supporting its control/management messaging.

Service providers that use transport equipment have business models that vary according to a combination of factors, including leasing versus ownership of resources, services provided, and what is sold (revenue source). Especially given the high volumes of data carried by optical transport network connections, safeguarding the transport network against attacks that may compromise its control/management plane, or seek unauthorized use of its resources, is deemed essential. A strong abstraction barrier is supported in the controller plane between users and providers. User transport resource name and address spaces are assumed, by default, to be independent of provider transport resource name and address spaces. Users do not inherently have visibility of provider transport resource names, addresses, or other information (such as detailed node information, network topology, etc.).

2.2 Connection Management

Connectivity is the basic service provided by a transport network. Connection management functions include: path computation, connection creation, connection modification, connection teardown, and configuration and activation of OAM and survivability mechanisms.

These connection management functions could be operated under instructions from a centralized system (e.g., SDN controller, EMS/NMS) or from a distributed control plane (such as ASON/GMPLS). The connection management function is integrated with the OSS infrastructure so that functions such as inventory and service assurance/fault management are fully aware of the status of the connections.

Failure in the controller/management/control plane system or its communication to the transport network is designed to avoid affecting established transport connection (connection persistence).

2.3 Transport Network Maintenance and Service Assurance

The transport network is capable of monitoring the performance of both the connectivity services that it provides and the basic network infrastructure. This monitoring allows assessment of compliance with SLAs, or evaluation of resource utilization.

To provide service level assurance and to facilitate maintenance of infrastructure, the transport network uses OAM monitoring that shares fate with the monitored traffic.

The network elements (NEs) within a transport network have different capacities and capabilities (e.g., the layer networks/technologies supported) and are of different vintages. To simplify the operation of such a diverse network, OAM and the associated operational standards are designed to be as common as possible across the layer networks and vintages.

Common OAM is used for the maintenance of both the client service and the infrastructure. The information derived from this OAM may be used as a trigger for recovery actions in either the infrastructure or the service. OAM also provides alarm suppression and supports fault localization.

2.4 Transport Network Operations

Transport network elements and the connections they provide are supported by an extensive OSS infrastructure. The OSS supports operational functions that are necessary to run the network including:

- Fault management, including dispatch of staff to repair faults
- Network configuration
- Inventory management
- Network planning (involving monitoring of inventory and service demands to stimulate reconfiguration of the infrastructure or the deployment of new resources). The time frame ranges from seconds (if the network capacity is in place) to years if major new construction is required.

2.5 Transport Network Protection and Restoration

The transport network provides a range of survivability mechanisms (both restoration and protection). Common types of protection include linear 1+1, 1:1, 1:n and ring. If used, these protection schemes must be configured and activated when a connection is set up. The coordination of protection across multiple layers in the transport network must also be considered.

3 Generic Requirements

This section uses the generic transport network attributes summarized in the previous section, Optical Transport Use Cases, and OIF Carrier Requirements considerations to derive a set of high level generic requirements.

3.1 Use-Case Derived Requirements

The OT WG Use Case document [1] describes a number of example use cases for SDN in optical transport networks. The use cases are written in a protocol-independent manner, and describe not only the use of interfaces but also actions taken by the switch, controller and application that are beyond the scope of the interface protocols themselves. This section uses the work on use cases to identify requirements on the SDN controller and network elements to support transport network attributes.

3.1.1 Transport Network Maintenance and Service Assurance

Performance monitoring may be performed to support proactive maintenance, fault localization or as input to SLA assurance. Indications of performance degradation may be an indication of impending failure of the related connection.

R-2.2.1.1: The SDN controller must be able to provide notification of performance degradation. The SDN Controller must be able to provide a report with details of the performance degradation on request. Such a report may involve the analysis of parameters retrieved from, or reported by, one or more network elements. The SDN controller may also have the capability to (re)configure the network to compensate for performance degradation.

R-2.2.1.2: If a network element is capable of detecting performance degradation, it must notify the SDN controller when the degradation exceeds a preset threshold. This threshold may be preset within the equipment or it may be configured during installation or operation.

R-2.2.1.3: If a network element supports performance monitoring of individual or sets of parameters, the network element must notify the SDN controller when any of the parameters exceeds a predefined range. The range may be preset within the equipment or it may be configured during installation or operation.

3.1.2 Transport Network Operations

R-2.2.2.1: The SDN controller must be able to retrieve or be provided with information about the network that it is controlling, including, as appropriate:

- Sub-elements that may be present within the network element (e.g. shelves and plug-in units)
- Capabilities that are supported (e.g. client/server adaptations, ITU-T application codes),
- Component usage state, e.g. active, idle, busy.
- Link characteristics that include, but are not limited to: link loss, distance and latency. These may be provided either by the network element, by specialized test equipment, or configured directly in the SDN controller.
- Network topology involving knowledge of the network topology under its control. This may be provided directly to the controller by a manager, or by invoking discovery protocols that may be supported by the network elements.

3.1.3 Transport Network Restoration and Recovery

The precise allocation of responsibility and actions taken by an SDN controller upon the occurrence of transport network failure(s) depends on the maximum time that a service may be disrupted before recovery and overall availability. There are three possibilities depending on the desired service level/SLA and performance:

a) The connection is recovered by normal maintenance/repair actions. Depending on the location and type of failure, recovery may take hours to days.
b) The connection is recovered by the SDN controller establishing a new connection in order to replace the failed connection.

c) The recovery action is delegated to autonomous protection/restoration mechanisms within the transport network. In this case when the original connection is set up, it may include the configuration of the required protection/restoration resources as well.

R-2.2.3.1: It must be possible for the operator to configure the controller and network element to take the appropriate actions upon occurrence of transport network failure (as in (a), (b) and (c) above) according to the desired service level/SLA.

R-2.2.3.2: When recovery action has been delegated by the SDN controller to autonomous protection/restoration mechanisms within the transport network, the controller must be notified of any change in state of the working or protection entities. Depending on the desired service level/SLA and the expected repair time, the SDN controller may set up a new protection/recovery path. When both the working and protection entities fail and further autonomous recovery is not supported, the SDN controller may establish a new connection to recover the service.

3.2 OIF Carrier Requirements Considerations

The OIF Carrier WG Requirements on Transport Networks in SDN Architectures [3] identifies basic requirements on the controller northbound and southbound interfaces.

The control communications network must be designed and dimensioned to provide adequate QoS (e.g., throughput and latency) and to be highly secure and robust. When designing the control network the latency, availability and security threats to which a carrier WAN are subject must be considered. The other main concern is the ability of the SDN architecture to accommodate the diversity to be expected (heterogeneity) within a carrier network environment. Aspects of this include the ability to deal with multiple administrative domains, support multiple technologies and protocol environments, and fit into the framework of other major carrier initiatives such as Network Functions Virtualization.

3.3 Requirements for support of Operator Business Practices

This section identifies a set of generic requirements for support of operator's business and operations needs, including support of virtual network services as described in [1].

R-3.1.1: Support for service provider/network operator commercial and operational practices, which include:

- Protection of commercial business operating practices and resources from external scrutiny or control (i.e., boundaries of policy and information sharing);
- Protection of the security and reliability of the transport network;
- Capability to support a “pay for service” commercial model (e.g., value added services must be verifiable and billable).

R-3.1.2: Support for accommodation of transport network operator-specific criteria and attributes including cost metrics, performance, and survivability characteristics.

R-3.1.3: Support for provision of virtual network services including:

- Support for service negotiation.

- Support for multiple service levels and service level attributes.
- e.g., directionality, connectivity (point-to-point, point-to-multipoint, etc.), committed bandwidth, class of service characteristics.
- Support for specifying service start and end times.

3.4 Deployment Requirements

This section identifies requirements on the deployment of Transport SDN over a control communications infrastructure. Source: OIF Carrier Requirements [3]

R-3.2.1: The network supporting Transport SDN controller communications (e.g., controller-NE, inter-controller) must be capable of delivering controller messages with performance, reliability and survivability suitable for meeting carrier network needs. This implies that the SDN controller communications network must:

- be designed with sufficient bandwidth to accommodate scaling requirements,
- support functionality such as congestion and flow control to avoid message loss and queuing delays,
- support connectivity between the community of controllers and their subtending network elements, and
- support redundancy and recovery capabilities to be able to restore connectivity in the event of failures.

3.5 Architectural Requirements

The main sources for the following requirements include the OIF Carrier Requirements [3] and the Use Case document [1].

R-3.3.1: The architecture must provide support for transport network infrastructure heterogeneity; i.e., the use of different technologies, control plane mechanisms and protocols in different domains of a carrier transport network.

R-3.3.2: The architecture must provide support for a transport network that is partitioned into multiple administrative domains.

R-3.3.3: The architecture must provide support for scalability across a carrier transport network, including scalability in number of systems, number of domains, and geographic scalability to global reach.

- Scalability and isolation of domains implies the ability to offer abstracted or virtualized views of network resources through a northbound interface from the controller.

These requirements drive the architecture to support network virtualization and both hierarchal and peer relationships between controllers in order to allow heterogeneity, partitioning and scalability. Hierarchical and peer controller organization is supported in the base ONF architecture [5] as well as the Optical Transport WG architecture [6].

3.6 Information Model Requirements

To effect the control of the transport network by the SDN controller, information will be exchanged in the interfaces between a SDN controller and the controlled network, or between SDN controllers in hierarchical relationship, or between SDN controllers in peer relationship. To facilitate the design of specific control protocol(s), e.g. OF-switch protocol, a protocol-neutral transport information model has been specified in [8].

R-3.4.1: The protocol-neutral transport information model must support the configuration and assurance requirements enumerated above.

R-3.4.2: The protocol-neutral transport information model must support the notification requirements enumerated above.

R-3.4.3: The design of the protocols used for the control of the transport network must be capable of supporting the information elements and actions identified in the protocol-neutral transport information model.

4 Protocol Requirements

In this section, OF-switch protocol requirements relevant to supporting SDN for transport are identified and categorized according to their support for the transport network attributes enumerated above. Requirements on other protocols (e.g., OF-Config) are for further study.

4.1 Connection Management Requirements

Sources: Use Case document [1], OIF Carrier Requirements [3].

R-4.1.1: The OF-switch protocol must be capable of creating, deleting and modifying flows for different transport technologies

a) This includes support of match and action capabilities for different circuit transport layers:
    i. L0 OTN Signal
        1. Match extensions that identify a signal using the attributes of an OCh (i.e. Grid, Channel Spacing, center frequency, channel mask)
        2. Action extensions that update these attributes (as allowed by hardware)
    ii. L1 OTN Signal
        1. Match extensions that identify a signal using the attributes of an ODUj/k (i.e. ODU type, ODU Tributary Slot, ODU Tributary Port Number)
        2. Action extensions that update these attributes (as allowed by hardware).

b) This includes support of port attributes for different circuit transport layers:
    i. L0 OTN Signal

1. Port capability extensions to identify the capabilities of OTS and OPS ports. This includes understanding the signals supported and granularity of switching available.

ii. L1 OTN Signal

1. Port capability extensions to identify the capabilities of OTU ports. This includes understanding the signals supported and granularity of switching available.

R-4.1.2: The OF-switch protocol must be capable of conveying to the controller information affecting path computation:

a) This includes support of port characteristics affecting path computation:

i. L0 OTN

1. signal characteristics impacting compatibility (e.g., ITU-T application code support)
2. connectivity constraints (e.g., inability to get from an ingress port to a set of egress ports)

ii. L1 OTN

1. Client signals and adaptation methods supported by the port

R-4.1.3: The OF-switch protocol must support specification of transport layering relationships for flow handling (e.g., adaptation of one signal to another using client/server model)

a) Including mapping of incoming packet flows into transport connections and mapping of incoming transport connection traffic into individual egress packet flows.

4.2 Transport Network Maintenance and Service Assurance Requirements

This section identifies requirements for support of carrier transport network environments. Source: OIF Carrier Requirements [3].

R-4.2.1: The OF-switch protocol must support procedures to maintain connection persistence in the event of controller plane failures and the ability to recover from such failures without disruption of customer traffic.

R-4.2.2: The OF-switch protocol must support reporting of faults in the data plane to the SDN Controller.

R-4.2.3: The OF-switch protocol must support reporting of performance monitoring information from the data plane, such as threshold crossing alerts.

R-4.2.4: The OF-switch protocol must provide a mechanism for filtering of notifications to the SDN controller.

4.3 Transport Network Operations Requirements

Source: Use Case document [1] and OIF Carrier Requirements [3].

R-4.3.1: The OF-switch protocol must support SDN controller establishment or validation of a global view (for some value of globe) of the network topology and resources under its control; e.g.,

a) Be capable of passing discovered adjacency information for each port of each OpenFlow Logical Switch in the topology (which may be physical or abstract network topology) up to the SDN Controller.
b) Be capable of passing transmitted and expected identity and support updates to discovered adjacency passed to the SDN Controller.
c) Be capable of configuring, retrieving, or triggering existing neighbor/link discovery mechanisms within the NE.

R-4.3.2: The OF-switch protocol must support procedures for resynchronizing state information between switch and controller in the event of a failure of the controller, the control network, or the switch.

4.4 Transport Network Restoration and Protection Requirements

Source: Use Case document [1] and OIF Carrier Requirements [3].

R-4.4.1: The OF-switch protocol must be capable of specifying protection behavior to be applied by the switch to a flow or set of flows (including no protection).

a. As discussed previously, this includes the ability to support pre-specified, autonomously carried out actions at the switch, when responsibility is delegated by the controller.
b. Commonly used protection behaviors to be supported include:
    i. 1+1 protection
    ii. 1:n and m:n protection
    iii. Ring and other protection mechanisms

5 Security Requirements

Overall ONF Security Requirements are defined in [2]. This section identifies impacts of optical transport network OpenFlow/SDN on the overall requirements. Previous work on transport network control plane security provides useful references as well [7].

R-5.1. Overall Security Requirements defined in [2] apply.
R-5.2. Security Requirements must take into account geographic distribution of controller and network elements.
R-5.3. Security Requirements must take into account partitioning of carrier transport networks into multiple administrative domains.

6 References

[1] OpticalTransport_UseCases, onf2013.128, http://login.opennetworking.org/bin/c5i?mid=4&rid=5&gid=0&k1=137.

[2] ONF Security Requirements Document, onf2014.134, http://login.opennetworking.org/bin/c5i?mid=4&rid=5&gid=0&k1=558&tid=1401743220

[3] OIF Carrier WG Requirements on Transport Networks in SDN Architectures, http://www.oiforum.com/public/documents/OIF_Carrier_WG_Requirements_on_Transport_Networks_in_SDN_Architectures_Sept2013.pdf

[4] OpticalTransport_Protocol_Recommendations, onf2014.228, Work in progress, http://login.opennetworking.org/bin/c5i?mid=4&rid=7&cid=1&gid=0&k1=687&k2=2&k3=9&tid=1401743326

[5] ONF Architecture, TR_SDN_ARCH_1.0, https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf

[6] SDN Architecture for Transport Networks, onf2014.301, Work in progress, http://login.opennetworking.org/bin/c5i?mid=4&rid=5&gid=0&k1=776&tid=1401238295.

[7] OIF-SEP-03.2, Security Extension for E-NNI and UNI IA, http://www.oiforum.com/public/documents/OIF_SEP_03.2.pdf

[8] [8] Optical Transport Information Model, onf2014.251, Work in progress, http://login.opennetworking.org/bin/c5i?mid=4&rid=5&gid=0&k1=710&tid=1401238533

LIST OF CONTRIBUTORS

The DOC3 Design team responsible for the writing of this document included:

- Jia He
- Dave Hood
- Young Lee
- Lyndon Ong
- Karthik Sethuraman
- Vishnu Shukla
- Eve Varma

Special thanks to Italo Busi, Paul Doolan and Kam Lam for their comments.