IETF   Ping Pan
Internet Draft   (Infinera)
                                                            Lyndon Ong
                                                               (Ciena)
                                                         Shane Amante
                                                             (Level 3)

Expires: April 31, 2012   October 31, 2011

              Software-Defined Network (SDN) Use Case for
                    Bandwidth on Demand Applications

            draft-pan-sdn-bod-problem-statement-and-use-case-01.txt

Status of this Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79. This document may not be modified,
   and derivative works of it may not be created, and it may not be
   published except as an Internet-Draft.

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79. This document may not be modified,
   and derivative works of it may not be created, except to publish it
   as an RFC and to translate it into languages other than English.

   This document may contain material from IETF Documents or IETF
   Contributions published or made publicly available before November
   10, 2008. The person(s) controlling the copyright in some of this
   material may not have granted the IETF Trust the right to allow
   modifications of such material outside the IETF Standards Process.
   Without obtaining an adequate license from the person(s) controlling
   the copyright in such materials, this document may not be modified
   outside the IETF Standards Process, and derivative works of it may
   not be created outside the IETF Standards Process, except to format
   it for publication as an RFC or to translate it into languages other
   than English.

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 obsoleted 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

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

This Internet-Draft will expire on January 31, 2012.

Copyright Notice

Abstract

Bandwidth on Demand services are offered by network operators in
industry and research sectors to support the needs of selected
customers needing high bandwidth point-to-point connections.

Without a standard interface for controlling the use of network
resources, user applications and services are subject to limits of
layering, security and interoperability across multiple vendors of
network equipment.

In this document, we argue the necessity in providing network
information to the applications, thereby enabling the applications
to directly provision network elements associated with the relevant
applications.

Table of Contents

1. Introduction

   Bandwidth on Demand services are offered by network operators in
   industry and research sectors to support the needs of selected
   customers needing high bandwidth point-to-point connections. Such
   services take advantage of dynamic control of the underlying network
   to set up forwarding and resource allocation as requested by the
   customer. Some control is given directly to the customer via a
   portal so that there is no need to go through an intermediate
   stage of service order provisioning on the part of the network
   operator.

   Currently such services are often based on management interfaces to
   vendor equipment that are vendor-specific, and as a result the
   operator must redesign its supporting control application for each
   vendor domain, or limit their offering to a single vendor domain.

   In this document, we propose that providing a common interface to
   networks of different vendors and technologies would enable the
   network provider to offer Bandwidth on Demand and other services
   that are faster to deploy across a wide range of network equipment
   by using additional network information.

   Here are some of the 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 [RFC2119].

2. Related Work

   There has been much work in this area in recent years. OpenFlow has
   defined an architecture for offering virtualized network control
   through a centralized controller and proxies called FlowVisors.
   These allow users to configure forwarding of packets within slices
   of the network partitioned off for their use. The controller is
   designed to control each network element directly through a
   dedicated control interface. It is not designed to work with
   existing control plane protocols.

   More generally, TMF has developed models and interfaces for
   operations and administration of networks through the north-bound
   interface provided by the element management system. These
   interfaces are not intended for real-time control of the network
   element and need to take into account variations in the design and
   features of different types of equipment.

   PCE is a client-server protocol that operates in MPLS networks that
   enables the network operators to compute and potentially provision
   optimal point-to-point and point-to-multipoint connections. However,
   PCE does not interface with applications to optimize traffic from
   user applications.

3. Problem Definition

   Figure 1 illustrates the relationship between application and
   network today, where customer control of bandwidth on demand is
   provided through applications created by the network operator
   supporting the user interface, features and backend accounting for
   the service. Such applications are used in single domain
   deployments and have limited visibility of underlying IP/MPLS and
   Transport networks and, most importantly, resource availability on
   those networks.

```
        +-------------+                +-------------+
        | Application |                | Application |
        |     #1      |                |     #2      |
        +-------------+                +-------------+
              |                              |
              |                              |
              |                              |
    +------------------+           +------------------+
    |   Network        |           |   Network        |
    |   Domain #1      |           |    Domain #2     |
    +------------------+           +------------------+
```
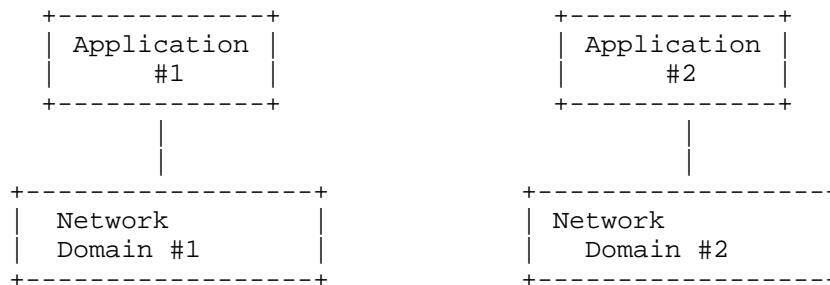
Figure 1: Application to network relationship today

This presents a number of challenges and problems. Without a
standard interface to the network elements that comprise one or more
network domains and their associated control software, each
bandwidth on demand supporting application must be built for a
specific set of vendor equipment and is not easily generalizable to
different vendors or even different equipment offered by a single
vendor. While signaling interfaces such as the UNI could offer
standardized access to network control, such interfaces have not
been adopted because they provide minimal security and functionality
and are designed for more of a peer relationship between network
elements, traditionally at only a single (peer) layer of the
network.

Similarly, bandwidth on demand applications must be designed for a
single technology, which restricts the range of use and potential
users. If Domain #1 uses SDH, for example, and Domain #2 uses OTN
it may be necessary to design supporting Application #2 from scratch
even though Application #1 has been successfully offering service.
Ideally the interface should allow some level of technology
independence, as well as potentially integration to permit control
of multiple layers simultaneously (esp. packet and circuit).

Third, the application is generally limited to simple services
connecting a source to destination, because interfaces hide network
topology and do not allow visualization of the topology for
different customer views. For some services users may wish to
exercise control over path routing aspects such as shared risk,
required latency characteristics or inclusion or exclusion of areas
for policy reasons.

4. The Role of an SDN Layer

   To solve the above problem, the proposal is to introduce a software-
   driven network (SDN) layer (as shown in Figure 2), that is
   responsible for network virtualization, programmability and
   monitoring, between supporting applications and the network.

```
      +-------------+    +-------------+    +-------------+
      | Application |    | Application |    | Application |
      |     #1      |    |     #2      |    |     #3      |
      +-------------+    +-------------+    +-------------+
            |                  |                  |
            |                  |                  |
      +-------------------------------------------------+
      |                    SDN Layer                    |
      |     (Network virtualization, programmability    |
      |                 and Monitoring)                 |
      +-------------------------------------------------+
            |                              |
            |                              |
      +------------------+        +------------------+
      | Physical Network |        | Physical Network |
      |    Domain #1     |        |    Domain #2     |
      +------------------+        +------------------+
```
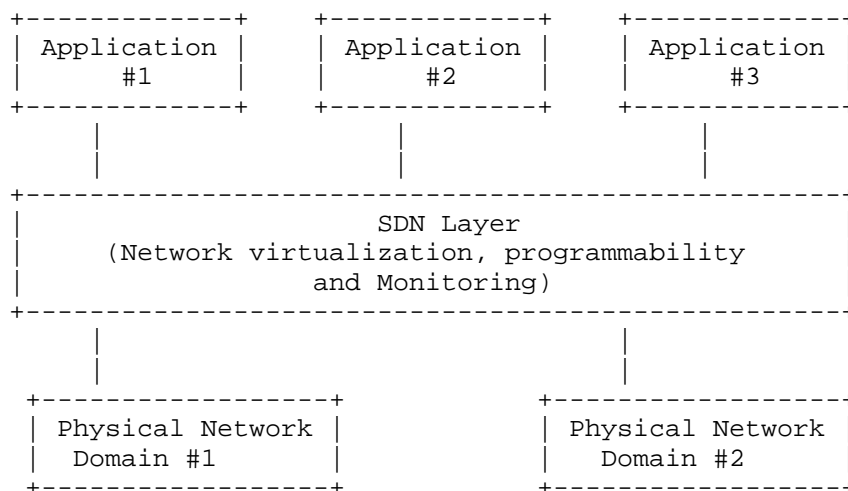
           Figure 2: Application to network relationship for SDN

   The purpose of the SDN Layer is to enable the applications
   supporting bandwidth on demand services to access information about
   and control (aggregate) traffic flows at various layers of the
   network through a standard, secure and customizable interface.
   Applications can visualize the traffic flows at the network layer,
   and manage the mapping or binding between its traffic flows from
   edge-to-edge through the associated networks.

   The implementation of an SDN Layer involves interfacing among
   different types of applications and different types of network
   domains, based on technology or vendor, administrative or policy
   control. Standardized interfaces must be defined to support this.

   The architecture should be agnostic as to the type of network
   control plan used in a supporting domain. The focus of work should

be on providing richer access to control of network resources rather
than on the scheme for network control used in the domain.

5. Use Cases

5.1. Scheduled/ Dynamic Bandwidth On-Demand Service

Figure 3 illustrates the flow of a scheduled or dynamic bandwidth
service. In the simplest case, connectivity may already be provided
between user-specified endpoints, however the bandwidth allocated
between endpoints can be varied within some overall limit based on a
predefined schedule or on spontaneous customer request. Note that
allowing bandwidth to be partitioned so that a scheduling
application has control over some pre-allocated set of resources is
necessary to support the scheduled BoD service. Also, the SDN layer
ideally hides the specific technology used to support the
connection, offering control of the service with associated rate,
latency and recovery features.

In more sophisticated services, the customer may be allowed to
create new connections within a specified set of endpoints and
delete such connections when the connectivity is no longer required.

```
    User
    Req's      +------------+
 -------->| Controller |
           +------------+
                |
                |  <----- North-bound protocol to adjust connections
                |
             \|/
        +---------+                      +--------+
        |   PE1   |                      |   PE2  |
        |         |==== Provisioned Connection ===>|        |
        +---------+                      +--------+
```

              Figure 3: Scheduled/Dynamic BoD Service

5.2. Multi-Layer BoD Support

```
User
Req's      +------------+
-------->| Controller |
           +------------+
                |
                |   <----- North-bound protocol to map packets to circuits
                |
              \|/
      +-------------------+                   +-------------------+
Pkt   |        PE1        |     Transport     |        PE2        | Pkt
====>| Classifer<->Tunnel |<=== Circuit ===>| Classifer<->Tunnel |====>
      +-------------------+                   +-------------------+
```
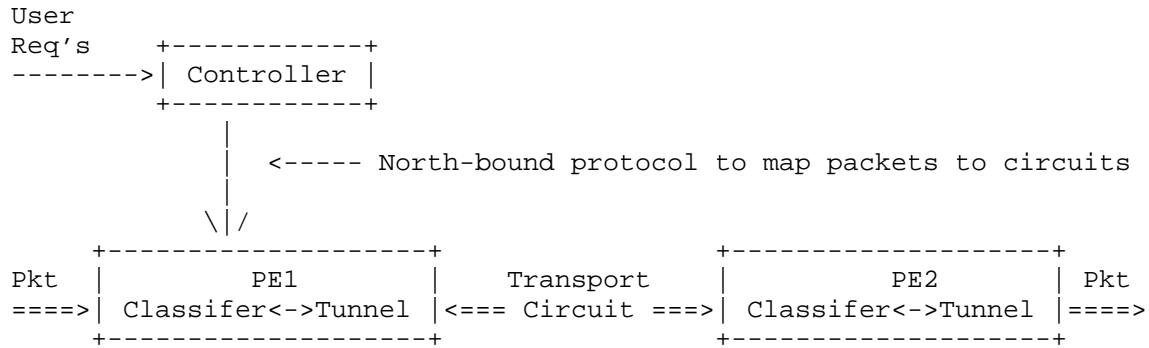
                  Figure 4: Multi-Layer BoD service

   Figure 4 illustrates a BoD service that supports multi-layer network
   control. This extends allows the network operator's supporting
   applications to combine control of packet forwarding through
   guaranteed bandwidth tunnels that connect sites in a (virtual)
   private network as requested dynamically by the BoD customer.
   Different transport network technologies may be used to provide the
   server layer transport functions so that the application can evolve
   easily with new transport technologies.

5.3. Virtualized Network Service

```
   User
   Req's      +------------+
   -------->| Controller |
            +------------+
              /|\   |
Topology --->|    |<----- North-bound protocol to adjust connections
Gathering    |    |
             |   \|/
            +---------+                            +--------+
            |    PE1   |                           |   PE2   |
            |         |==== Provisioned Connection ===>|        |
            +---------+                            +--------+
```
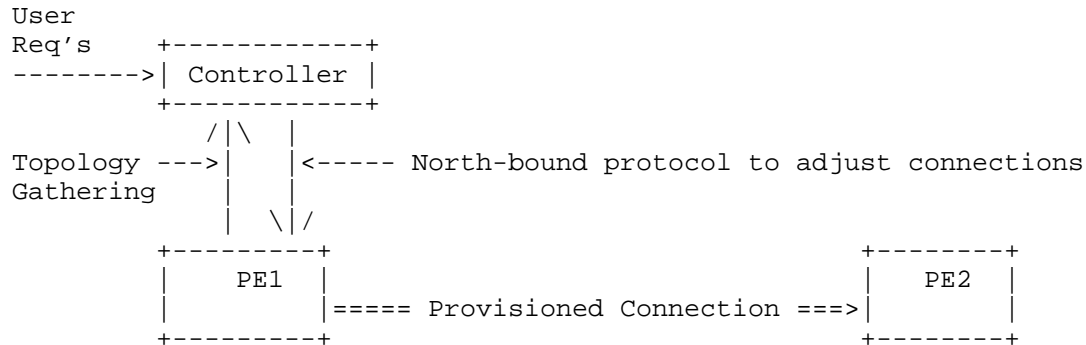
                  Figure 5: Virtualized network service

Figure 5 illustrates the flow of a virtualized network service that
offers some degree of topology visibility and control in addition to
the features of scheduled or dynamic BoD. For some customers it may
be desirable to provide visibility into the topology of the
resources they control, in order for the customer so they may
control the physical and/or virtual topology of the resources used
within their dedicated domain.

If this topology information is provided together with associated
cost, latency, SRLG, etc. for the links and nodes in the topology,
the customer is provided with additional flexibility to manipulate
routing of their data flows so as to balance the cost, latency,
energy efficiency or survivability using knowledge of client
applications and their particular needs and priorities.

At this time such visibility is not possible to provide, as
protocols provide either no visibility into topology or full
visibility into topology. For security reasons it is likely that a
supporting network operator will want to limit visibility and
control to some virtualized topology using functionality provided by
the SDN orchestrator.

5.4. BoD Actions Supported by the SDN Orchestrator

The following summarizes actions that would be supported by
the SDN orchestrator as part of a BoD service:

- increase or decrease bandwidth on an existing path between
  two, or more, network clients;

- dynamically learn if resources are available, (e.g.: bandwidth,
  latency, SRLG, etc.) to create a path between two, or more,
  network clients;

- create a path and assign associated characteristics, (e.g.:
  bandwidth, latency, SRLG, etc.) that connect two, or more, network
  clients;

- configure mapping of packets, Ethernet frames, OTN frames, etc.
  from a client interface into a specified network path (or paths)
  connecting the appropriate ingress and egress client interfaces;

- configure some partition of network resources (e.g., links and
  link capacity connecting some set of nodes and client endpoints)
  to be controlled by a specific application;

- provide real or virtual topology information (links, nodes and
  associated information such as costs, latency, etc.) for this
  partition to the associated application.

6. Security Consideration

   TBD

7. IANA Considerations

   This document has no actions for IANA.

8. Normative References

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

   [2]   Crocker, D. and Overell, P.(Editors), "Augmented BNF for
          Syntax Specifications: ABNF", RFC 2234, Internet Mail
          Consortium and Demon Internet Ltd., November 1997.

9. Acknowledgments

   This work is based on the conversation with many people, including
   Thomas Nadeau and Benson Schliesser.

Authors' Addresses

   Ping Pan
   Email: ppan@infinera.com

   Lyndon Ong
   Email: lyong@ciena.com

   Shane Amante
   Email: shane@level3.net