Provider Provisioned VPN WG
Internet Draft
Expiration Date: May 2002

Hamid Ould-Brahim
Nortel Networks

Yakov Rekhter
Juniper Networks

- Editors

Don Fedyk
Peter Ashwood-Smith
Nortel Networks

Eric C. Rosen
Cisco Systems

Eric Mannie
Ebone

Luyuan Fang
AT&T

John Drake
Calient Networks

Yong Xue
UUNET/WorldCom

Riad Hartani
Caspian Networks

Dimitri Papadimitrio
Alcatel

November 2001

BGP/GMPLS Optical/TDM VPNs

draft-ouldbrahim-bgpgmpls-ovpn-02.txt

Status of this Memo

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.

Abstract

Consider a service provider network that offers Optical/TDM Virtual Private Network service. An important goal of such service is the ability to support what is known as "single end provisioning", where addition of a new port to a given Optical/TDM VPN would involve configuration changes only on the devices connected to that port. Another important goal in the Optical/TDM VPN service is the ability to establish/terminate an optical connection between a pair of (existing) ports within an Optical/TDM VPN without involving configuration changes in any of the provider devices.

In this document we describe a set of mechanisms that accomplishes these goals.

1. Sub-IP Summary ID

This ID targets the PPVPN working group as it deals with a VPN solution similar to port-based VPNs. It describes an approach to allow service providers to offer optical VPN service. A pair of client devices (a router, a SONET/SDH cross-connect, or an Ethernet switch) could be connected through the service provider network via an optical connection. It is this optical connection that forms the basic unit of service that the service provider network offers.

RELATED DOCUMENTS

draft-ouldbrahim-ovpn-requirements-00.txt. Others can be found in the "references" section.

WHERE DOES IT FIT IN THE PICTURE OF THE SUB-IP WORK

Fits the PPVPN box.

WHY IS IT TARGETED AT THIS WG

This WG is looking at port based VPN over an IP/MPLS infrastructure. This work is exactly a port-based optical VPN using IP related building blocks.

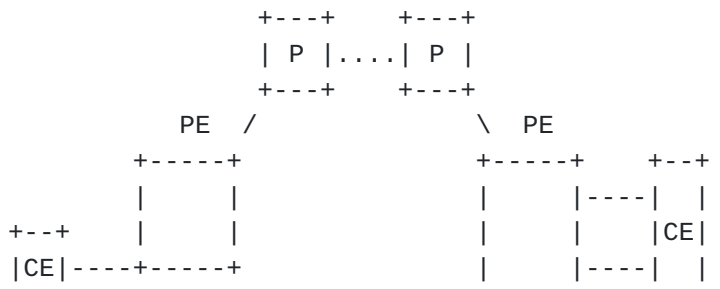
JUSTIFICATION

The current PPVPN chairs have already discussed this work and are considering expanding the PPVPN charter to include OVPN as part of PPVPN mandate.

2. Optical/TDM VPN Reference Model

Consider a service provider network that consists of devices such as Optical Network Element (ONE) which may be Optical Cross Connects (OXCs). Following the framework suggested in [PPVPN-FRAMEWORK], we partition these devices into P (provider) ONEs and PE (provider edge) ONEs. The P ONEs are connected only to the ONEs within the provider's network. The PE ONEs are connected to the ONEs within the provider network, as well as to the devices outside of the provider network. We'll refer to such other devices as Client Edge Devices (CEs). An example of a CE would be a router, or a SONET/SDH cross-connect, or an Ethernet switch.

While the rest of this document mostly focuses on the scenarios where the service provider network consists of ONEs and ports are connected via optical connections, the mechanisms described in this document could be applied in an environment, where the service provider network consists of SONET/SDH cross connects and CE ports being either SONET/SDH or Ethernet.



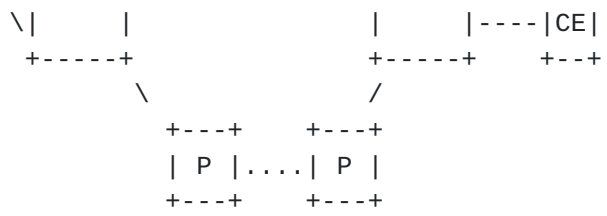


Figure 1 Optical VPN Reference Model

A CE is connected to a PE ONE via one or more links, where each link may consists of one or more channels or sub-channels (e.g., wavelength or wavelength and timeslot respectively). In the context of this document a link is a logical construct that is used to represent grouping on a per VPN basis of physical resources used to connect a CE to a PE ONE.

For purpose of this discussion we assume that all the channels within a given link have shared similar characteristics (e.g., bandwidth, encoding, etc_), and can be interchanged from the CEs point of view. Channels on different links of a CE need not have the same characteristics.

There may be more than one link between a given CE PE ONE pair. A CE may be connected to more than one PE ONE (with at least one port per each PE ONE). And, of course, a PE ONE may have more than one CE connected to it.

If a CE is connected to a PE ONE via multiple links and all these links belong to the same VPN, then for the purpose of OVPN these links could be treated as a single link using the link bundling constructs [LINK-BUNDLING].

In general a link may have only data bearing channels, or only control bearing channels, or both. For the purpose of this discussion we assume that for a given CE - PE ONE pair at least one of the links between them has at least one data bearing channel, and at least one control bearing channel, or there is an IP connectivity between the CE and the PE that could be used for exchanging control information (more on this in Section 4).

A link has two end-points - one on CE and one on PE ONE. In the context of this document we'll refer to the former as "CE port", and to the latter as "PE ONE port". From the above it follows that a CE is connected to a PE ONE via one or more ports, where each port may consists of one or more channels or sub-channels (e.g., wavelength or wavelength and timeslot respectively), and all the channels within a given port have shared similar characteristics (e.g., bandwidth, encoding,

etc_), and can be interchanged from the CEs point of view. Channels on different ports of a CE need not have the same characteristics. Just like links, in the context of this document ports are logical construct that

are used to represent grouping of physical resources on a per OVPN basis that are used to connect a CE to a PE ONE.

At any given point in time, a given port on a PE ONE is associated with at most one OVPN, or to be more precise with at most one Port Information Table (although different ports on a given PE ONE could be associated with different OVPNs, or to be more precise with different Port Information Tables) This association is established and maintained by the service provider provisioning system.

A pair of CEs could be connected through the service provider network via an optical connection. It is precisely this optical connection that forms the basic unit of the OVPN service that the service provider network offers. If a port by which a CE is connected to a PE ONE consists of multiple channels (e.g., multiple wavelengths), the CE could establish optical connection to multiple other CEs over this single port.

An important goal in the OVPN service is the ability to support what is known as "single end provisioning", where addition of a new port to a given OVPN would involve configuration changes only on the PE ONE that has this port and on the CE that is connected to the PE ONE via this port. Another important goal in the OVPN service is the ability to establish/terminate an optical connection between a pair of (existing) ports within an OVPN without involving configuration changes in any of the provider's ONEs. The mechanisms outlined in this document aim at achieving these goals. Specifically, as part of the Optical VPN service offering, these mechanisms (1) enable the service provider to restrict the set of ports that a given port could be connected to, (2) enable the service provider to provide a CE with the information about the ports that the CE could be connected, (3) enable a CE to establish the actual connections to a subset of ports provided by (2). Finally, the mechanisms allow different OVPN topologies to be supported ranging from hub-and-spoke to complete mesh.

The service provider does not initiate the creation of an optical circuit between a pair of PE ONE ports. This is done rather by the CEs, which attach to the ports. However, the SP, by using the mechanisms outlined in this document, restricts the set of other PE ONE ports which may be the remote endpoints of optical circuits that have the given port as the local endpoint. Subject to these restrictions, the CE-to-CE connectivity is under the control of the CEs themselves. In other words, SP allows an OVPN to have a certain set of

topologies (expressed as a port-to-port connectivity matrix), and CE-initiated signaling is used to choose a particular topology from that set.

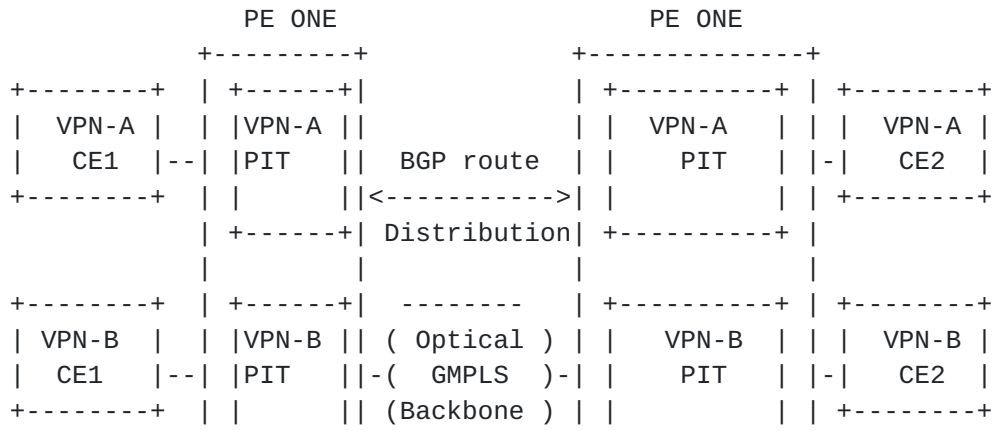
Since this model involves minimal provisioning changes when changing the connectivity among the ports within a OVPN on the providers network and the OVPNs themselves are controlled by the CEs, the tariff structure may be on a port basis or alternatively tariffs could be triggered on the basis of signaling mechanisms.

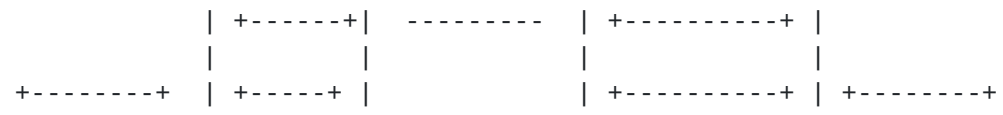
Finally, it is assumed that CE-to-CE optical connectivity is based on GMPLS [GMPLS].

3. Overview of operations

This document assumes that within a given OVPN each port on a CE that connects the CE to a PE ONE has an identifier that is unique within that OVPN (but need not be unique across several OVPNs). One way to accomplish this is to assign each port an IP address that is unique within a given OVPN, and use this address as a port identifier. Another way to accomplish this is to assigned each port on a CE an index that is unique within that CE, assign each CE an IP address that is unique within a given OVPN, and then use a tuple <port index, CE IP address> as a port identifier.

This document assumes that within a service provider network, each port on a PE ONE has an identifier that is unique within that network. One way to accomplish this would be to assign each port on a PE ONE an index that is unique within that PE ONE, assign each PE ONE an IP address that is unique within the service provider network (in the case of multi-provider operations, the address has to be unique across all the providers involved), and then use a tuple <port index, PE ONE IP address> as a port identifier within the provider network.





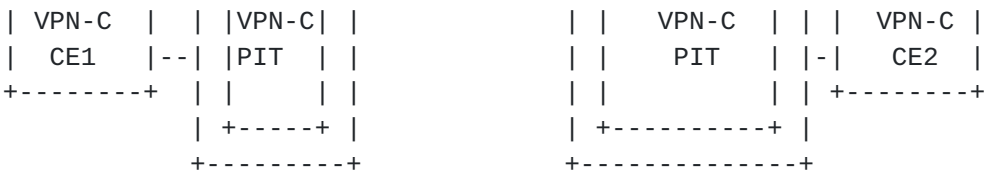


Figure 2 OVPN Components

As a result, each link connecting the CE to the PE ONE is associated with a CE port that has a unique identifier within a given OVPN, and with a PE port that has a unique identifier within the service provider network. We'll refer to the former as the customer port identifier (CPI), and to the latter as the provider port identifier (PPI).

This document assumes that in addition to PPI, each port on PE ONE has also an identifier that is unique within the OVPN of that port. One way to accomplish this is to assign each port an IP address that is unique within a given OVPN, and use this address as a port identifier. Another way to accomplish this is to assigned each port an index that is unique within a given PE ONE, assign each PE ONE an IP address that is unique within a given OVPN (but need not be unique within the service provider network), and then use a tuple <port index, PE ONE IP address> acts as a port identifier. We'll refer to such port identifier as VPN-PPI. Note that PE ONE IP address used for VPN-PPI need not be the same as PE ONE IP address used for PPI. If for a given port on a PE its PPI and VPN-PPI are both unnumbered, then they both could use exactly the same port index.

Note that IP addresses used for CPIs, PPIs and VPN-PPIs could be either IPv4 or IPv6 addresses.

For a given link connecting a CE to a PE ONE, if CPI is an IP address, then VPN-PPI has to be an IP address as well. And if CPI is an <port index, CPI IP address>, then VPN-PPI has to be an <port index, PE ONE IP address>. However, for a given port on PE ONE, whether VPN-PPI of that port is an IP address or an <port index, PE ONE IP address> is independent of whether PPI of that port is an IP address or an <port index, PE ONE IP address>.

This document assumes that assignment of PPIs is controlled solely by the service provider (without any coordination with the OVPN customers), while assignment of CPIs and VPN-PPIs is controlled solely by the OVPN that the CPIs and VPN-PPIs belong to. And, of course, each OVPN could assign its CPIs and VPN-

PPIs on its own, without any coordination with other OVPNs.

Each PE ONE maintains a Port Information Table (PIT) for each OVPN that has at least one port on that PE ONE. A PIT contains a list of <CPI, PPI> tuples for all the ports within its OVPN.

A PIT on a given PE ONE is populated from two sources: the information related to the CEs' ports attached to the ports on that PE ONEs (this information could be optionally received from the CEs), and the information received from other PE ONEs. We'll refer to the former as the "local" information, and to the latter as the "remote" information.

The local information is propagated to other PE ONEs by using BGP with multi-protocol extensions. To restrict the flow of this information to only the PITs within a given OVPN, we use BGP route filtering based on the Route Target Extended Community [BGP-COMM], as follows.

Each PIT on a PE ONE is configured with one or more Route Target Communities, called "export Route Targets", that are used for tagging the local information when it is exported into provider's BGP. The granularity of such tagging could be as fine as a single <PPI, CPI> pair. In addition, each PIT on a PE ONE is configured with one or more Route Target Communities, called "import Route Targets", that restrict the set of routes that could be imported from provider's BGP into the PIT to only the routes that have at least of these Communities.

When a service provider adds a new OVPN port to a particular PE ONE, this port is associated at provisioning time with a PIT on that PE ONE, and this PIT is associated (again at provisioning time) with that OVPN.

Once a port is configured on the PE ONE, the CE that is attached via this port to the PE ONE MAY pass to the PE ONE the CPI information of that port. This document assumes that this is accomplished by using BGP (however, the document doesn't preclude the use of other mechanisms).

This information, combined with the PPI information available to the PE ONE, enables the PE ONE to create a tuple <CPI, PPI> for such port, and then use this tuple to populate the PIT of the OVPN associated with that port.

In order to establish an optical connection, a CE needs to identify all other CEs in the CE's OVPN it wants to connect to. A CE may already have obtained the CE list through configuration or through some other schemes (such schemes are outside the scope of this draft).

It is also desirable, that the service provider, as a value added service, may provide a CE with a list of all other CEs in the CE's OVPN. This is accomplished by passing the information

stored in the PE ONE PITs to the attached CE. This document assumes that this is accomplished by using BGP Multi-protocol extensions (however this draft doesn't preclude other mechanisms to be used). Although optional, this draft recommends the PE to signal to the attached CEs the remote CPIs it learnt from the remote CEs part of the same OVPN. A CE may decide to initiate an optical connection request to a remote CE only when it learn the CPI of the remote CE from the PE. This has the benefit to avoid rejecting connection request while the PE is populating the PITs.

Once a CE obtains the information about the CPIs of other ports within the same OVPN, which we'll refer to as "target ports", the CE uses a (subset of) GMPLS signaling, as described in Section 4, to request the provider network to establish an optical connection to a target port. Note that this draft assumes that GMPLS is only used to establish optical connections between client devices.

The request originated by the CE contains the CPI of the port on the CE that CE wants to use for the optical connection, and the CPI of the target port. When the PE ONE attached to the CE that originated the request receives the request, the PE ONE identifies the appropriate PIT, and then uses the information in that PIT to find out the PPI associated with the CPI of the target port carried in the request. The PPI should be sufficient for the PE ONE to establish an optical connection. Ultimately the request reaches the CE associated with the target CPI (note that the request still carries the CPI of the CE that originated the request). If the CE associated with the target CPI accepts the request, the optical connection is established.

Note that a CE need not establish an optical connection to every target port that CE knows about - it is a local to the CE matter to select a subset of target ports to which the CE will try to establish optical connections.

A port, in addition to its CPI and PPI may also have other information associated with it that describes characteristics of the channels within that port, such as encoding supported by the channels, bandwidth of a channel, total unreserved bandwidth within the port, etc. This information could be further augmented with the information about certain capabilities of the Service Provider network (e.g., support RSOH DCC transparency, arbitrary concatenation, etc_). This information is used to ensure that ports at each end of an optical connection have compatible characteristics, and that

there are sufficient unallocated resources to establish an optical connection. Distribution of this information (including the mechanisms for distributing this information) is identical to the distribution of the <CPI, PPI> information. Distributing

changes to this information due to establishing/terminating of optical connections is identical to the distribution of the <CPI, PPI> information, except that thresholds should be used to contain the volume of control traffic caused by such distribution.

It may happen that for a given pair of ports within an OVPN, each of the CEs connected to these ports would concurrently try to establish an optical connection to the other CE. If having a pair of optical connections between a pair of ports is viewed as undesirable, the a way to resolve this is have CE with the lower value of CPI is required to terminate the optical connection originated by the CE. This option could be controlled by configuration on the CE devices.

4. Signaling between CE and PE (Simple UNI -SUNI)

Signaling between CE and PE uses a (proper) subset of GMPLS signaling [GMPLS].

For the purpose of GMPLS signaling between CE and PE, this document assumes that there is an IP control channel between the CE and the PE. This channel could be either a single IP hop, or an IP private network, or even an IP VPN. We'll refer to the CE's address of this channel as the CE Control Channel Address (CE-CC-Addr), and to the PE's address of this channel as the PE Control Channel Address (PE-CC-Addr). Both CE-CC-Addr and PE-CC-Addr are required to be unique within the OVPN they belong to, but are not required to be unique across multiple OVPNs. Assignment of CE-CC-Addr and PE-CC-Addr are controlled by the OVPN these addresses belong to.

Multiple ports on a CE could share the same control channel only as long as all these ports belong to the same OVPN. Likewise, multiple ports on a PE could share the same control channel only as long as all these ports belong to the same OVPN.

When a CE sends an RSVP Path message to a PE, the source IP address in the IP packet that carries the message is set to the appropriate CE-CC-Addr, and the destination IP address in the packet is set to the appropriate PE-CC-Addr. When the PE sends back to the CE the corresponding Resv message, the source IP address in the IP packet that carries the message is set to the PE-CC-Addr, and the destination IP address is set to the CE-CC-Addr.

Likewise, when a PE sends an RSVP Path message to a CE, the

source IP address in the IP packet that carries the message is set to the appropriate PE-CC-Addr, and the destination IP address in the packet is set to the appropriate CE-CC-Addr. When the CE sends back to the PE the corresponding Resv

message, the source IP address in the IP packet that carries the message is set to the CE-CC-Addr, and the destination IP address is set to the PE-CC-Addr.

In addition to being used for IP addresses in the IP packet that carries RSVP messages between CE and PE, CE-CC-Addr and PE-CC-Addr are also used in the Next/Previous Hop Address field of the IF_ID RSVP_HOP object that is carried between CEs and PEs.

In the case where a link between CE and PE is a numbered non-bundled link, the CPI and VPN-PPI of that link are used for the Type 1 or 2 TLVs of the IF_ID RSVP HOP object that is carried between the CE and PE. In the case where a link between CE and PE is an unnumbered non-bundled link, the CPI and VPN-PPI of that link are used for the IP Address field of the Type 3 TLV. In the case where a link between CE and PE is a bundled link, the CPI and VPN-PPI of that link are used for the IP Address field of the Type 3 TLVs.

When a CE originates a Path message to establish a connection from a particular port on that CE to a particular target port the CE uses the CPI of its port in the Sender Template object. If the CPI of the target port is an IP address, then the CE uses it in the Session object. And if the CPI of the target port is a <port index, IP address> tuple, then the CE uses the IP address part of the tuple in the Session object, and the whole tuple as the Unnumbered Interface ID subobject in the ERO. When the Path message arrives at the ingress PE, the PE selects the PIT associated with the OVPN, and then uses this PIT to map CPIs carried in the Session and the Sender Template objects to the appropriate PPIs. Once the mapping is done, the ingress PE replaces CPIs with these PPIs. As a result, the Session and the Sender Template objects that are carried in the GMPLS signaling within the service provider network carry PPIs, and not CPIs. At the egress PE, the PE performs the reverse mapping _ it maps PPIs carried in the Session and the Sender Template object into the appropriate CPIs, and then sends the Path message to the CE that has the target port.

5. Encoding

This section specifies encoding of various information defined in this document.

5.1 Encoding of channel characteristics in GMPLS Signaling

[TBD]

5.2 Encoding of CPI, PPI, and channel characteristics in BGP

5.2.1 Encoding of CPI and PPI information in BGP

The <CPI, PPI> mapping is carried using the Multiprotocol Extensions BGP [RFC2858]. [RFC2858] defines the format of two BGP attributes, MP_REACH_NLRI and MP_UNREACH_NLRI that can be used to announce and withdraw the announcement of reachability information. We introduce a new address family identifier (AFI) for OVPN (to be assigned by the IANA), a new subsequent address family identifier (to be assigned by the IANA), and also a new NLRI format for carrying the CPI and PPI information.

One or more <PPI, CPI> tuples could be carried in the above mentioned BGP attributes.

The format of encoding a single <PPI, CPI> tuple is shown in Figure 3 below:

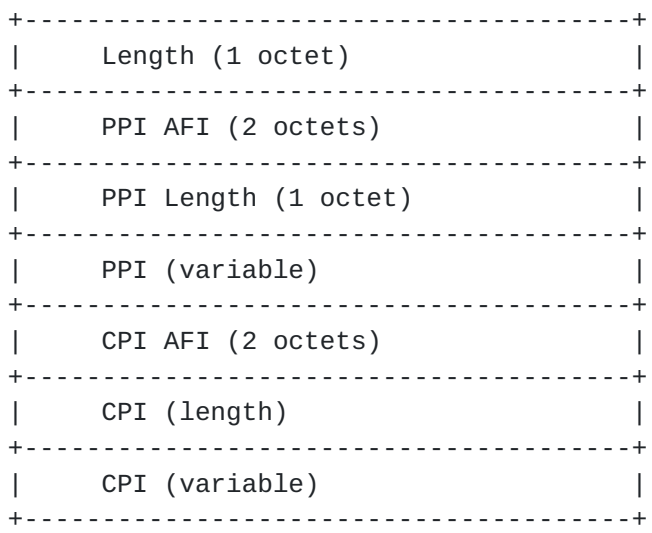


Figure 3: NLRI BGP encoding

The use and meaning of these fields are as follows:

Length:

A one octet field whose value indicates the length of the <PPI, CPI> Information tuple in octets.

PPI AFI:

A two octets field whose value indicates address family identifier of PPI

PPI Length:

A one octet field whose value indicates the length of of the PPI field

PPI field:

A variable length field that contains the value of the PPI (either an address or <port index, address> tuple

CPI AFI field:

A two octets field whose value indicates address family of the CPI.

CPI Length:

A once octet field whose value indicates the length of the CPI field.

CPI (variable):

A variable length field that contains the CPI value (either an address or <port index, address> tuple.

5.2.2 Encoding channel characteristics in BGP

[TBD]

6. One vs more than one OVPN

The solution described in this document requires each customer port to be in at most one OVPN, or to be more precise requires each customer port connected to a given PE to be associated with at most one PIT on that PE. It has been asserted that this requirement is too restrictive, as it doesn't allow to realize certain connectivity scenarios. To understand why this assertion is incorrect we'd like to make several observations.

First, the solution described in this document allows control connectivity between customers' ports at the granularity of individual ports. This is because each local port on a PE could have its own PIT, and the granularity of the information that is used to populate this PIT could be as fine as a single remote port (port on some other PE).

Second, ports that are present in a given PIT need not have the same administrative control. For example, some ports in a given PIT may belong to the same organization (have the same

administrative control) as the local ports associated with that PIT, while some other ports in exactly the same PIT may belong to organizations different from the one associated with the

local ports. In that sense, a single PIT could combine both an Intranet and an Extranet.

As a result, it should be abundantly obvious to the informed reader that the solution described in this document allows to realize any arbitrary inter-port connectivity matrix. Therefore, no other solution could be less restrictive than then one described in this document.

7. Exchanging VPN-ID between CE and PE

The solution described in this document assumes that an association of a particular port on a CE with a particular OVPN (or to be more precise with a particular PIT on a PE) is done by the OVPN service provider, as part of the provisioning the port on the PE (associating the PE's port with a particular PIT, and connecting the CE's port with the PE's port). Once this association is established, the CE could request establishment of an optical connection to any customer's port present in the PIT. Important to note that in order to select a particular port within the PIT for the purpose of establishing a connection to that port the only information that the CE needs to identify that port is the CPI of that port. Also important to note that the CPI is either an IP address, or a combination of <port index, IP address>, but it doesn't include any such thing as VPN-ID.

Therefore, the solution described in this document doesn't involve exchanging VPN-IDs between CE and PE in (GMPLS) signaling. Moreover, the lack of exchanging VPN-ID in signaling has no adverse effect on the ability to support any arbitrary inter-port connectivity matrix, and more generally on the flexibility of the solution described here.

8. Other issues

Since the protocol used to populate a PIT with remote information is BGP, since BGP works across multiple routing domains, and since GMPLS signaling isn't restricted to a single routing domain, it follows that the mechanisms described in this document could support an environment that consists of multiple routing domains.

The mechanisms described in this document allow for a wide range of choices with respect to addresses used for CPI, PPI, and VPN-PPI. For example, one could use either IPv4 addresses,

or IPv6 addresses, or NSAPs. Different OVPN customers of a given service provider may use different types of addresses. Moreover, different OVPNs attaching to the same PE ONE may use

different addressing schemes. The types of addresses used for PPIs within a given service provider network are independent from the type of addresses used for CPI and VPN-PPI by the OVPN customers of that provider.

While in the context of this document a CE is a device that uses the Optical/TDM VPN service, such a device, in turn, could be used to offer VPN services (e.g., RFC2547, Virtual Routers, Layer 2 VPNs) to other devices (thus becoming a PE with respect to these devices). Moreover, a CE device that uses the Optical VPN service could, in turn be used to offer Optical/TDM services to other devices (thus becoming a PE ONE with respect to these devices).

9. Security Considerations

Since association of a particular port with a particular OVPN (or to be more precise with a particular PIT) is done by the service provider as part of the service provisioning process (and thus can't be altered via signaling between CE and PE), and since signaling between CE and PE is assumed to be over a private network (and thus can't be spoofed by entities outside the private network), the solution described in this document doesn't require authentication in signaling.

10. References

[BGP-COMM] Ramachandra, Tappan, "BGP Extended Communities Attribute", February 2000, work in progress.

[Framework] Rajagopalan, B. et al., "IP over Optical Networks: A Framework ", November 2000, work in progress.

[GMPLS] Ashwood-Smith, P., Berger, L. et al., "Generalized MPLS -Signaling Functional Description", November 2000, work in progress.

[LINK-BUNDLING] Kompella, K., Rekhter, Y., Berger, L., "Link Bundling in MPLS Traffic Engineering", work in progress.

[OVPN-REQ] Ould-Brahim, H., Rekhter, Y., et al., "Service Requirements for Optical Virtual Private Networks", work in progress, July 2001.

[PPVPN-FRAMEWORK] Callon, R., Suzuki, M., Gleeson, B., Malis, A., Muthukrishnanm K, Rosen, E., Sargor, C., Yu, J., _A Framework for Provider Provisioned Virtual Private

Networks_, draft-ietf-ppvpn-framework-01.txt

[RFC-2858] Bates, Chandra, Katz, and Rekhter, "Multiprotocol Extensions for BGP4", RFC2858, June 2000.

[RFC-2026] Bradner, S., "The Internet Standards Process -- Revision 3", RFC2026, October 1996.

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

[VPN-BGP] Ould-Brahim H., Gleeson B., Ashwood-Smith P., Rosen E., Rekhter Y., Declerq J., Fang L., Hartani R., "Using BGP as an Auto-Discovery Mechanism for Network-based VPNs", work in progress, July 2001.

11. Acknowledgments.

The authors would like to thank Osama Aboul-Magd, Penno Reinaldo, Erning Ye, Bryan Gleeson, and Dave Allan for reviewing the draft and providing comments.

12. Author's Addresses

Hamid Ould-Brahim
Nortel Networks
P O Box 3511 Station C
Ottawa ON K1Y 4H7 Canada
Phone: +1 (613) 765 3418
Email: hbrahim@nortelnetworks.com

Yakov Rekhter
Juniper Networks
1194 N. Mathilda Avenue
Sunnyvale, CA 94089
Email: yakov@juniper.net

Don Fedyk
Nortel Networks
600 Technology Park
Billerica, Massachusetts
01821 U.S.A

Phone: +1 (978) 288 3041

Email: dfedyk2nortelnetworks.com

Peter Ashwood-Smith
Nortel Networks
P.O. Box 3511 Station C,
Ottawa, ON K1Y 4H7, Canada
Phone: +1 613 763 4534
Email: petera@nortelnetworks.com

Eric C. Rosen
Cisco Systems, Inc.
250 Apollo drive
Chelmsford, MA, 01824
E-mail: erosen@cisco.com

Eric Mannie
Ebone (GTS)
Terhulpsesteenweg 6A
1560 Hoeilaart
Belgium
Phone: +32 2 658 56 52
Email: eric.mannie@gts.com

Luyuan Fang
AT&T
200 Laurel Avenue
Middletown, NJ 07748
Email: Luyuanfang@att.com
Phone: +1 (732) 420 1920

John Drake
Calient Networks
5853 Rue Ferrari
San Jose, CA 95138
USA
Phone: +1 408 972 3720
Email: jdrake@calient.net

Yong Xue
UUNET/WorldCom
Ashburn, Virginia
(703)-886-5358
yxue@uu.net

Riad Hartani
Caspian Networks

170 Baytech Drive
San Jose, CA 95143
Phone: 408 382 5216

Email: riad@caspiannetworks.com

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

Full Copyright Statement