Testing MPLS VPNs
Technical Paper

Introduction

Paul Doolan, co-author of a seminal book on IP switching, stated recently that any technology requires ten years to reach maturity. With MPLS now reaching its fifth birthday, it is clear, as Doolan predicted, that the technology and its applications are still evolving.

Virtually all networking technologies have required one or more “killer” applications to stimulate widespread acceptance and deployment. Initially, traffic engineering (TE), which would reduce congestion and costs and improve manageability for service provider (SP) networks, was considered to be the most important application for MPLS.

With the tightening economy in the U.S. and the rest of the world, however, the focus of SPs has shifted to exploring new avenues of revenue generation. The result has been a dramatic increase in interest in the use of MPLS for deployment of Virtual Private Network services (MPLS VPNs) by both SPs and their enterprise customers.
Yakov Rekhter originally proposed the BGP-MPLS VPN concept, extending the existing BGP protocol and using MPLS label technology to allow nested VPN tunnels. Based on this concept, a number of SPs initiated service offerings. These initial offerings were fueled by extensive existing SP deployments of Cisco devices, since Cisco’s proprietary Tag Distribution Protocol (TDP - a predecessor to LDP, one of the standard MPLS protocols) also allowed implementation of BGP-MPLS VPNs. As SPs began to seriously consider BGP-MPLS VPNs, it became clear that other alternatives were also needed.

As MPLS VPN protocol activity increased, a new work group (WG), the Provider Provisioned VPN (PPVPN) WG was created by the Internet Engineering Task Force (IETF). The group’s main task is to define the framework and requirements for specification of VPN service offerings. The recent PPVPN requirements document submitted at the PPVPN WG proposed that an SP must be able to offer QoS service to a customer for at least two generic service types; managed access VPN services or edge-to-edge QoS services.

These two service types have important distinctions. BGP-MPLS VPNs, a Layer 3 service, are considered a managed access VPN service, since VPN services are fully managed by an SP. However, there are many enterprises who wish to manage their own Layer 3 overlays, and many service providers who wish to provide Layer 2 interfaces to such customers. This leads to an edge-to-edge service.

Edge-to-edge services are not a new concept. Enterprises have long built their own wide area networks by purchasing wide area, point-to-point data link layer connectivity from SPs, and then building their own Layer 3 infrastructure on top of that. These services are also being partly defined by the Pseudo-Wire Edge-to-Edge (PWE3) WG at the IETF.

While both of these approaches have their merits and drawbacks, this paper will focus on how implementation of both types of VPNs can be verified in devices and networks.

### VPN Testing

In order to discuss VPN testing, it is necessary first to briefly review some basic concepts of router testing.

Any exchange of information through frames or packets (referred to collectively in this paper as “packets”) requires two packet types -- control packets and data packets. Typically, much device intelligence is vested in the handling of the information carried by control packets. This is accomplished through the device’s “control software”.

Once control packet exchange and control software establish the correct configuration, the device can make proper packet forwarding decisions and data packets can be sent across the network. Thus, device data processing design must include the ability to make a high-volume of forwarding decisions at rates of up to 10 Gigabytes per second.

Further, VPN testing must focus on both control and data processing levels (commonly referred to as Control and Data planes) within switch/routing devices. As will become evident in later discussion, different types of VPNs distribute processing activities differently between these two planes.

### Types of Testing

Typically, any testing discussion must cover the various aspects of each type of testing, namely Conformance, Functional, Performance and Scalability, Interoperability, and Service testing.

Conformance and Functional testing focus on the details of the control and data packets themselves. This type of testing is common at the software development and system integration labs of network equipment manufacturers (NEMs).

As software begins to be integrated with hardware, it is possible to conduct performance and scalability tests on both the control and data planes. For example, the PPVPN Requirements document estimates that a large service provider will require the ability to support 10,000 VPNs within four years and that the number of site interfaces will range from a few to more than 50,000 site interfaces per VPN. Clearly, any device expected to be part of such a network will need to be tested for its ability to support these levels of activity. Performance and scalability testing are generally performed at system integration and pre-deployment labs of NEMs, and also at SP evaluation labs.

Before a device can be deployed in the network, it is also necessary to evaluate whether it will be used in a single- or multi-vendor environment. Multi-vendor networks require interoperability testing to determine the level of interoperability that has been achieved between VPN implementations of various NEMs. Interoperability testing is critical to ensuring that SPs are not limited to use of equipment from a single NEM.

Finally, it is necessary to test the service in the actual network environment. Typically, SPs will initially deploy a particular VPN service in a certain segment of the network, for use between internal sites or by a very small set of customers, for testing purposes. When customers are involved, testing is often based on a Service Level Agreement (SLA) specifying the details of the service and QoS levels.
This paper will focus chiefly on “black box” testing (i.e. all observations are made on an external, third party test tool). The term “Tester T” will be used to refer to a generic tool for testing MPLS VPNs. Tester T must be able to analyze packets and emulate a network of devices, including Customer Edge (CE), Provider Edge (PE), and Provider Core (P) devices.

A CE device is the ‘exit point’ of the customer or enterprise network. A PE device is the first device on the SP network connected to CE devices and P devices are the core devices in the SP network (ref. Figure 1). The device being tested will be referred to as the System Under Test (SUT). Since only a PE device is expected to have VPN functionality, the SUT will always be a PE router.

Layer 2 and Layer 3 VPNs

The remainder of this paper will focus on testing Layer 2 and Layer 3 VPN services running over MPLS-based networks (the concept of layers is taken from the OSI layer model -- Layer 2 is the Data Link Layer, while Layer 3 is the Network Layer). In this context, the phrase “Layer 3 VPN” will denote a VPN service used to carry Layer 3 traffic end-to-end, while “Layer 2 VPN” will denote a VPN service used to carry Layer 2 traffic over an MPLS network.

Layer 3 MPLS VPN testing will be explored first, as Layer 3 MPLS VPNs have been offered for some time by a number of NEMs and SPs. Layer 2 MPLS VPNs are a more recent phenomenon and will be discussed in the final portion of this paper.

Finally, we will not explicitly cover “negative testing” here. Negative testing, or error injection, consists of sending packets into the PE router with incorrect contents or in incorrect sequences to evaluate the robustness of the SUT. This type of testing is a standard part of Conformance and Functionality testing, and can also be used in Stress testing to check the router’s ability to handle errors under high control and data load conditions. It is expected that Tester T is capable of conducting this type of test.

Layer 3 MPLS VPN: BGP-MPLS VPN

The Layer 3 focus of this paper is BGP-MPLS VPNs, as defined in RFC2547bis [BGP-VPN]. In this VPN type, MPLS is used for forwarding packets over the backbone, and BGP is used for distributing routes over the backbone.

This section will first briefly discuss the BGP-MPLS VPN concept and then review testing issues for the most common VPN case, where the VPN is set up between two geographically separate sites, connected to two different PE routers (ref. Figure 2).
PE-CE Connectivity

As with most VPN, the PE router must manage most of the information processing for BGP-MPLS VPNs. An enterprise interested in obtaining BGP-MPLS VPN service from an SP, is referred to as a VPN site. The router in the enterprise network connected to the SP network is called the Customer Edge (CE) router. Thus, a VPN site connects to other sites on the VPN via one or more CE routers (over the SP network). A PE router is attached to a site (S) as the endpoint of an interface or “sub-interface” (e.g. PVC, VLAN, GRE tunnel, etc.) whose other endpoint is a CE device.

This phase of testing checks for interface or sub-interface connectivity.

Tester T must then offer the following capabilities for each interface type:

a. Ability to send and receive data traffic (on each sub-interface if necessary)
b. Ability to run routing protocols, such as BGP-4, OSPF, IS-IS, RIP (on each sub-interface if necessary); static routing is also allowed.

Additionally, Tester T must support all necessary Layer 2 configuration, addressing, and alarms and offer the ability to indicate the health of the Layer 2 link (thus confirming the ability to send and receive data packets).

Maintaining VPN Information on PE

The PE router maintains independent VPN routing and forwarding (VRF) tables for each VPN site it connects with. The VRF table associated with a particular site “S” is populated only with routes that lead to other sites, which have at least one VPN in common with “S”.

A common problem is the overlapping of address space in different customer networks, resulting from enterprises using the private address space recommended by RFC1918. For example, two independent sites connected to the same PE but belonging to separate VPNs might have an overlapping address space. As a result, traffic destined for one site could get sent to the other.

To avoid this, a new type of address was created called the VPN-IPv4 address. This is a 12-byte quantity, beginning with an 8-byte Route Distinguisher (RD) and ending with a 4-byte IPv4 address. Since the RD can be made unique by its structure, the VPN-IPv4 address for every site can be made globally unique.

Because VRF tables are maintained inside the PE router, an external test tool will not typically have access to them. The implementation of VRF tables, however, can be tested through the test for Data Forwarding for VPNs described below.

VPN Site Reachability

One of the extended attributes of BGP, the “Route Target”, is used by BGP to distribute information on sites participating in a particular VPN. When a VPN-IPv4 route is created by a PE router, it is associated with one or more Route Target attributes. Any route associated with a Route Target (“T”) must be distributed to every PE router that has a VRF associated with “T”. In this way, the route is installed in a particular VRF, which is both that particular route’s Route Target and is also one of the “import” targets of that VRF. As a result, controls exist at both ends for two sites participating in a VPN.

If two sites of a VPN attach to PEs which are within the same Autonomous System, the PEs can distribute VPN-IPv4 routes to each other by means of an iBGP connection, either directly or through a route reflector. When a PE router distributes a VPN-IPv4 route via BGP, it uses its own address as the BGP “next hop”. It also assigns and distributes an MPLS label associated with the VPN-IPv4 route, as specified in RFC 3107 [BGP-LBL]. We will refer to this as the “BGP label”.

All of these operations ensure that VPN reachability information of the participating CE devices are available, in an unambiguous, unique fashion to the PE devices. In addition to these steps, it is also necessary to ensure that the PE devices (which are the BGP next hops) are able to send traffic to each other. This is done by using an MPLS LSP between them. The [BGP-VPN] document states that to ensure interoperability among systems which implement this VPN architecture, all systems must support LDP [MPLS-LDP].

Testing of these capabilities is done through basic data forwarding and is discussed in the following sub-heading.
Data Forwarding for VPNs

The CE device in a particular VPN will send an unlabeled IP packet to the PE. When a PE receives a data packet from a CE device, it chooses a particular VRF for look-up of the packet’s destination address. This choice is based on the packet’s incoming sub-interface, since that identifies the site to a VRF association.

The incoming packet will have a BGP next hop and there will be a BGP label for it. This label is pushed onto the packet’s label stack, and becomes the bottom label. This BGP next hop, or the PE router, will also have an MPLS label associated with it, representing the LSP set up between the source and destination PE routers. This label is also pushed onto the packet, creating a two-deep label stack.

MPLS will then carry the packet across the backbone. Once the packet reaches the egress PE, it pops off the MPLS label. The egress PE router’s treatment of the packet will depend on the BGP label. In many cases, the PE will be able to determine, from this label, the sub-interface over which the packet should be transmitted (to a CE device), as well as the proper data link layer header for that interface.

In other cases, the PE may only be able to determine that the packet’s destination address needs to be looked up in a particular VRF before being forwarded to a CE device. Information in the MPLS header itself, and/or information associated with the label, may also be used to provide QoS data on the interface to the CE. When the packet finally gets to a CE device, it will again be an ordinary unlabeled IP packet.

Tester T must perform the following steps to check VRF table implementations and VPN connectivity as part of a basic VPN setup functional test:

a.  Emulate multiple sites (and hence multiple CE routers) in Tester T on one set of interfaces and connect to the SUT
b.  Emulate a network of devices and sites on another set of interfaces and connect to the SUT
c.  Advertise VPN routes from one set of sites to another (populate the SUT’s VRF tables), using iBGP
d.  Set up LSPs between the PEs (which are iBGP peers)
e.  Send traffic over these VPNs from an emulated PE to a particular set of addresses from a simulated VRF. An MPLS label stack will be automatically inserted, based on the entry in the simulated VRF and the LSP label.
f.  Send traffic from a simulated CE and receive packets at an emulated PE containing a two-level label stack. The label stack can be validated in real time using per-stream statistics.
g.  Capture and decode incoming data packets including the label stack
h.  Capture and decode control packets

Both the VRF table and the BGP label for a site should be distinct. Tester T will analyze the traffic streams to and from different sites. For traffic coming to the emulated P routers, Tester T will check to determine that the correct label stacks have been used. For traffic coming to the CE devices, Tester T will check whether traffic is being sent to the correct destination (ref. Figure 3).
At this point, Tester T will have all the information and capabilities required to set up a BGP-MPLS VPN. By repeating some of these steps, Tester T can set up a large number of VPN connections to the SUT, thus stressing the control plane (ref. Figure 4). This can be achieved in two ways:

a. Connecting a large number of emulated CE routers as independent VPN sites, thus forcing large number of VRF tables on the SUT
b. Making one site a member of a large number of VPNs, thus forcing a large VRF table on the SUT

Data stressing can also be performed. Once a particular VPN is set up, data traffic can be sent over this VPN at up to the line rate allowed by the physical connection.

A series of QoS measurements must also be enabled for data traffic. These measurements include:

a. Packet loss
b. Packet delay
c. Packet jitter

These measurements may need to be made on a per VPN or per interface basis.

VPN services will typically be covered under a Service Level Agreement. Service parameters specified may include total bandwidth, availability, and traffic QoS parameters. QoS details may include total network delay, packet loss, and total jitter (if the VPN carries voice traffic). Tester T should have the capability to provide the required measurements at the required granularity level for line rate traffic and high control loads. More detailed discussion on service testing is included later in this paper.

**Layer 2 MPLS VPN**

As the discussion moves to the topic of Layer 2 MPLS VPN testing, it is important to note the distinct difference between Layer 2 VPNs and Layer 3 VPNs, namely that the CE is not involved in Layer 2 VPN creation at all.

In the Layer 2 case, the SP provides only a Layer 2 interface to its customers and the customer is responsible for creating and managing the Layer 3 overlay. Thus, for Layer 2 MPLS VPNs, only the PE needs to be tested, but Layer 2 interactions should be examined in greater depth.

There are no standards yet for Layer 2 MPLS VPNs, but enterprises have long built their own wide-area networks by purchasing wide-area point-to-point data link layer connectivity from service providers, and then building their own layer 3 infrastructure on top of it. Some of the current Internet drafts, which have gained attention, are [Martini-TRANS] and [Kompella]. There have already been a number of public announcements of NEM implementations of the [Martini-TRANS] draft (ref. Figure 5).

The following section describes a test methodology for the [Martini-TRANS], followed by a brief discussion of one for [Kompella].

**PE-CE Connectivity**

In this case, the PE-CE connection need not include routing protocol support. The Layer 2 link must be up and data flow verified. A permanent virtual circuit (PVC) may be used. Testing may simply be used to ensure that data can flow between the PE and CE devices.
Setting up a VPN

In the Layer 2 case, setting up a VPN is similar to establishing a Circuit Emulation Service. The CE to CE connection is considered a Virtual Circuit (VC). Typically, a “VC label” is defined to identify this VC.

The [Martini-TRANS] draft deals with point-to-point transport over MPLS. To transport Layer 2 packets (Protocol Data Units or PDUs) from an ingress PE router (“R1”) to an egress PE router (“R2”) requires the following control plane steps (ref. Figure 6):

a. An MPLS LSP is set up between R1 and R2
b. R1 and R2 establish another LDP session, using the extended discovery mode
c. The VC label is distributed by LDP, running in downstream unsolicited mode
d. A new information element is passed in the LDP protocol exchange to carry additional information about the VC. This is called the Virtual Circuit FEC (Forwarding Equivalence Class) element.
e. At this point, the PEs are ready to start transporting data

This control plane exchange leads to two-level encapsulation of the data packets -- by the VC label and the MPLS LSP label. The [Martini-ENCAP] draft defines data packet encapsulation. In addition, the draft requires a third level of encapsulation called “emulated VC encapsulation”. This level contains the information about the enclosed Layer 2 PDU which is necessary to properly emulate the corresponding Layer 2 protocol. This type of encapsulation is called the “Control Word”.

Thus, when a data packet is sent, it is encapsulated in the following sequence:

<table>
<thead>
<tr>
<th>Tunnel Label</th>
<th>VC Label</th>
<th>Control Word</th>
<th>PDU Payload</th>
</tr>
</thead>
</table>

For Ethernet packets, the Ethernet Header itself is used as the third level of encapsulation instead of the Control Word.

Without going into the complete details of the process used to convert a normal Layer 2 packet into the above format, it is important to note that the content of the Control Word will vary depending on the PDU type (ATM AAL5 PDU, ATM cell, or FR packet).

To test this type of Layer 2 VPN, Tester T will first emulate a network very similar to the one emulated for Layer 3 VPN testing -- a collection of CE, P, and PE devices. Based on Figure 6, for example, one of the test ports needs to emulate a CE (“C1”) and the other test port will emulate an MPLS network of P and PE devices, with another emulated CE connected to the PE (“R2”). The SUT is a PE device (“R1”).

Once these elements are emulated, Tester T will perform the following actions:

a. Set up two LSPs between the PE devices R1 and R2 across the MPLS network, one from R1 to R2 and another from R2 to R1 (this is because MPLS LSPs are unidirectional)
b. Establish an LDP session between R1 and R2 (sing extended discovery), and exchange VC information. At this stage, the VC label and the MPLS labels are available to R1 and R2 and the endpoints are ready to exchange data traffic.
c. Send Layer 2 traffic (Ethernet packets, in this example) from emulated CE1 to R1
d. R1 should forward the Ethernet packets to R2 with two labels attached on top (the Ethernet header remains as is)
e. Tester T should verify the two-deep label stack for correctness
f. Tester T will send traffic with two-deep label stack from R2 to R1, destined for C1
g. The SUT (R1) should strip these two labels and send this traffic to C1
h. Tester T will then check traffic arriving on the port for correctness

Figure 6: Functionality Test Scenario
The scenario can be scaled without the need to significantly increase the number of CE ports, since a very large number of Virtual Circuits can be emulated through a single CE-PE connection.

Assume, for example, that Tester T includes Gigabit Ethernet ports, which can emulate a CE with 2000 VLAN sessions. In that case, using just a few ports, a large number of VCs can be set up per CE port through the SUT (“R1”), as illustrated in Figure 7. Tester T can also be configured so that some of the VCs (e.g. 1,000) from R1 must be set up to a PE (R2), while others (rest 1,000) must be set up to R3.

This will then require four LSPs (two per each PE-PE connection, one in each direction). The important stress scenario here is that the SUT (R1) will be required to be part of 2000x2 LDP extended discovery sessions for setting up the VCs. If more than one emulated CE is connected to R1, this increases the number of sessions by that multiple. Finally, verification data traffic can be sent over each of these VCs.

The [Kompella] draft offers another method of setting up a Layer 2 VPN. It defines usage of the BGP protocol to communicate VPN reachability and VC label information, instead of the LDP protocol, as defined in the [Martini-TRANS]. It also contains a number of recommendations on implementation of such VPNs. The steps defined in the [Kompella] draft will not be discussed in detail here, as the draft is still evolving as of this date.

Verifying Service Level Agreements

Thus far, all of the discussion in this paper has centered on testing of individual devices, with the remainder of the system being emulated by Tester T. It is important to note that some of the elements in the emulated network discussed may be replaced by actual devices, allowing the user to test combinations or networks of various manufacturer’s equipment.

The key application for network testing is verifying Service Level Agreements (SLAs) between SPs and their customers. Various metrics can be measured to determine whether SLA parameters are met.

Service Level Agreements may be defined per access network connection, per VPN, per VPN site, and/or per VPN route. The SP may define both levels and measurement intervals for any or all of the following parameters:

1. QoS and traffic parameters
   - PE to PE round trip delay
   - Jitter (variation of delay)
   - Packet Loss ratio
2. Availability for the site, VPN, or access connection
3. Access Link Load
4. Service activation interval (e.g. time to turn up a new site)
5. Time to repair interval
6. Total traffic offered to the site, route, or VPN
7. Measurement of non-conforming traffic for the site, route, or VPN
8. Router utilization

Using the mechanisms defined previously in this paper, Tester T can be used to set up VPNs, send traffic at up to line rate on the VPNs, and then provide measurements at specified intervals for these SLA parameters.
Service Verification
Tester T must have the following capabilities for SLA measurements:

a. Highly granular traffic measurement, to the degree required by network QoS levels and traffic content
b. Distributed traffic measurement, across geographically distant VPN end points
c. Synchronized measurement capable of correlating traffic sent and received from the test end-points, and creating realistic reports of the state of the VPN and the network
d. Per VPN site or per VPN route measurement capabilities

It is important to note that black box testing does not permit measurement of SUT utilization. This must be done by other means, and this brief preliminary discussion of SLA verification is specific to MPLS VPNs. While this subject requires much more attention, it is also important to include some discussion of Network or Service Restoration testing in this paper.

Service Restoration Verification

When an SP offers a commercial VPN service to an enterprise, it will come with certain availability and QoS guarantees. These require implementation of restoration capabilities in the device and the network, since the link carrying VPN traffic may go down for a variety of reasons.

Network restoration can be implemented in multiple ways. Typically, it will be handled using the underlying protocol infrastructure (MPLS in this case). While various techniques and algorithms may be used, two general methods are device-based and network-based restoration. Device-based techniques offer fast reroute methods. Network-based techniques would provide one or more backup LSPs. Regardless of the method used, it must be assumed that VPN traffic has some alternative path through the network.

Clearly, a key testing issue would be to determine whether the device or network can restore the VPN service within the parametric limits described in the SLA. The following steps describe a method for conducting this type of testing:

a. Tester T emulates a network of devices, where a VPN is to be set up from CE1 adjacent to the SUT (PE router - R1) through an SP network to CE2 behind R2 (Ref. Figure 8)
b. The VPN tunnel is nested inside an LSP (“LSP1”) set up on the path R1-P1-P3-PE2
c. Assume the VPN label is L1, and LSP label is L2 when the traffic leaves the SUT
d. VPN traffic flows from CE1 to CE2
e. Label stack on the traffic is -- Data+L1+L2
f. Another path is available for an LSP from SUT to PE2: R1-P2-PE2 (an LSP may not be set up beforehand, if the SUT supports fast reroute)
g. The link between SUT and P1 is brought down by some method (laser-off may be the fastest way). This results in tear down of LSP1.
h. R1 sets up a new LSP (“LSP2”) through P2 for PE2 using the label “L3” and starts transmitting CE1-CE2 VPN traffic over that LSP

Tester T should perform the following checks:
- Examination of traffic coming to P2 to ensure that it looks like Data+L1+L3
- Measurement of the performance characteristics of the flow and any changes to it, e.g. measurement of the time difference (delay) between the receipt of the last packet over LSP1 and the first packet over LSP, measurement of the jitter of the traffic
- Comparison of the traffic sent out of CE1 and received on CE2 to check for packet loss

The above scenario could also be executed while sending a high volume of control or data traffic to the SUT through other ports. This will emulate realistic network traffic load on the SUT, and test the restoration capacity of the SUT under such conditions.

Figure 8: Service Restoration Test Scenario
Conclusion

It’s clear from the above discussion that MPLS VPN testing is a complicated process, chiefly because of a large number of components involved. However, by extending existing tools, the testing capabilities required for NEM and SP MPLS VPN development and deployment testing can be made available.

To summarize, Tester T must offer the following capabilities:

Functionality

a. Ability to emulate all the network elements of the SP network (P and PE routers) and the Customer edge (CE)
b. Ability to emulate all the required protocols used in the SP network and for the CE-PE connection
c. Ability to fully use all the protocol activity, e.g. to set up MPLS LSPs and VPN tunnels
d. Ability to send traffic up to line-rate over VPN tunnels

Usability

a. Ability to perform highly granular measurement of the packet exchanges in the control and data plane in real-time
b. Ability to decode all the packet exchanges in the control and data plane in real-time
c. Ability to interpret the flow of control and data packets and crate usable information
d. Ability to represent all the information gathered in an intuitive graphical interface and reports for easy interpretation by a user
e. Ability to provide automated ways to conduct all the required functions

Glossary

BGP                Border Gateway Protocol
iBGP               BGP for internal peers in a Service Provider cloud
MP-iBGP            iBGP with Multi-protocol extensions
GRE                Generic Route Encapsulation (a legacy tunneling technique)
LSP                Label Switched Path
MPLS               Multi-protocol Label Switching
PVC                Permanent Virtual Circuit (commonly used term in ATM and Frame Relay world)
QoS                Quality of Service
TE                 Traffic Engineering
VLAN               Virtual Local Area Networks
VPN                Virtual Private Networks -- a way to set up private networks over shared infrastructure

For information about the test tools available from Agilent Technologies, please visit:
www.agilent.com/comms/RouterTester
References

1. [REQMT] Service requirements for Provider Provisioned Virtual Private Networks (draft-ietf-ppvpn-requirements-xx, August 2001, work in progress)


7. [Kompella] MPLS-based Layer 2 VPNs (draft-kompella-ppvpn-12vpn-xx, June 2001)

8. MPLS and VPN Architectures (Jim Guichard & Ivan Pepelnjak, Cisco Press, December 2000)