An ADTRAN White Paper

Private IP Service
BGP/MPLS VPN Networks
Until the advent of business communications over the Internet, a clear distinction between private and public networks was present. Private networks based on technologies like Frame Relay and point-to-point circuits inherently provided network security because the general public did not have access to a particular customer’s data. Frame Relay, although not commonly thought of in this manner, can really be considered a type of Virtual Private Network (VPN) because of the nature in which the Permanent Virtual Circuits (PVCs) connect locations together through a provider’s network.

With the advent of business communications over the Internet, private data is now transferred over a public network using another type of VPN. In this model, the virtual nature of the network comes into play because a company does not have dedicated paths or dedicated PVCs for data; instead, all traffic is routed over the Internet from one location to another. This model requires the data to be encrypted to prevent unauthorized users from capturing the data—a task not easily accomplished in Frame Relay, ATM, or point-to-point networks.

Three Broad Categories of VPNs Exist Today:
Traditional access, Customer Premises Equipment (CPE)-based, and Network-based. Furthermore, just because a service is defined as a VPN does not mean encryption is a requirement. The connectivity model is the determining factor as to whether encryption is needed. Only one of the VPNs listed below requires the use of encryption for secure communication.

Traditional Access VPNs
- Frame Relay
- ATM

CPE-based VPNs (Internet-based connectivity, needs encryption)
- IPSec (Layer 3)
- PPTP or L2TP (Layer 2)

Service Provider VPNs (Network-based)
- Private IP networks based around Border Gateway Protocol (BGP) and Multiprotocol Label Switching (MPLS)
Advantages and Disadvantages of VPNs

All three types have advantages and disadvantages as highlighted in Table 1. The last type, Service Provider VPNs, is an emerging category of service provided by carriers to create a network that combines the best aspects of both traditional access and CPE-based VPNs.

<table>
<thead>
<tr>
<th>Traditional Access VPNs</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Widely available</td>
<td>High cost for mesh networks</td>
</tr>
<tr>
<td></td>
<td>Private network</td>
<td>Higher cost than CPE-based VPN approach</td>
</tr>
<tr>
<td></td>
<td>In-network Quality of Service (QoS) support (ATM)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Level Agreements (SLAs) available</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPE-based VPNs</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lower monthly cost</td>
<td>No in-network QoS support</td>
</tr>
<tr>
<td></td>
<td>Secure communication over any Internet connection</td>
<td>Everyone has access to data (even though its encrypted)</td>
</tr>
<tr>
<td></td>
<td>No additional network costs for mesh networks</td>
<td>More complex to set up CPE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No latency guarantee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Potentially greater CPE requirements depending on the network size</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Generally no SLAs available</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Provider VPNs</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Easy, flexible connectivity</td>
<td>No support for IP Multicast traffic today</td>
</tr>
<tr>
<td></td>
<td>Lower monthly cost</td>
<td>Connections between service providers can be problematic</td>
</tr>
<tr>
<td></td>
<td>In-network QoS available</td>
<td>Implications of many VPN Routing and Forwarding tables (VRFs) on a single Provider Edge (PE) router not widely tested (more details on VRFs and PEs will follow)</td>
</tr>
<tr>
<td></td>
<td>Secure communications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SLAs available</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Generally a managed service offering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Generally no additional CPE requirements</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Types of VPNs
Some new terms must be defined in order to understand the concept of the BGP/MPLS VPN.

- **Customer Edge Router (CE):** Router located on the customer premise that terminates the connection to the carrier.
- **Provider Edge Router (PE):** Router located at the ingress or egress point in the provider’s network that terminates the connection to the CE router. It runs BGP on the core side of the router.
- **Provider Router (P):** Routers inside the service provider’s network running BGP and MPLS.

Even though the local loop connects the customer’s site via Frame Relay, the traditional concepts of Frame Relay with PVCs in the network to each site stop here. The first departure from Frame Relay lies in the fact that generally only one PVC is present on the local loop, regardless of whether the site is a branch or the host site. That single PVC connects the CE router to the ingress PE router. From the core side of the ingress PE router to the core side of the egress PE router, the Frame Relay PVC and corresponding Data Link Connection Identifier (DLCI) no longer exist in the network.
How is Traffic Routed in the Core?
Since no PVCs exist in the core, how does the traffic know where to go? The answer lies in the combination of MPLS for label switching and BGP for routing. To understand this process, a further explanation of the network in Figure 1 is necessary.

The network in Figure 1 represents two different customers’ networks—represented by the BLUE and GREEN CE routers. The GREEN customer only has access to GREEN routers and similarly, the BLUE customer has access only to the BLUE routers. So how does the network restrict the traffic such that the BLUE and GREEN customers do not see each other’s traffic? A new concept known as VPN Routing and Forwarding Table (VRF) is used in the PE routers to establish a unique routing table for each customer. This concept, combined with Label Switched Paths (see Switching Labels section on page 8), creates a logical separation of customer networks. Figure 2 illustrates the VRF concept.

VRF tables are independent. The GREEN and BLUE customers, while physically connected to the same PE router, would never be able to route between each other’s network or even know other networks exist. If connectivity between these customers was desirable, the PE router’s VRF tables could be configured accordingly.

The PE routers maintain BGP sessions with each other and convey customer-specific route information and MPLS labels between PEs (VRFs). This is accomplished by adding properties to an advertised route, called Route Distinguishers, which instruct the PE to associate a route with a specific VRF. The PE routers are BGP peers with other PE routers. The P routers typically run an Interior Gateway Routing Protocol (IGP), like Open Shortest Path First (OSPF), within the core to provide the IP routed backbone between all P and PE routers. The P routers do not have knowledge of customer routes. They simply provide paths between PE routers.
More information on ADTRAN’s NetVanta routers is included at the conclusion of this document.) If multiple routers sit behind the CE router, it may be advantageous to use a routing protocol. This is more common in a large branch site or a host site where multiple networks exist behind the CE router. With a routing protocol running on the CE router, as new networks are added, they are automatically advertised to the PE router, via the CE router, and hence distant networks will now know of the new networks. While BGP provides some definite advantages in this situation, BGP is not absolutely required. (See When is BGP Needed in a CE Router? section on page 7.)

A common misnomer is that BGP is a requirement at the CE router. Table 2 summarizes four major carriers’ service offerings relative to MPLS/BGP VPNs. In each case, no carrier mandates BGP be used at the CE router. In fact, the only place in the network where BGP is mandatory is on the PE router’s interface that is connected to the MPLS core. Even if a different routing protocol is used on the CE router, route redistribution is used to allocate the CE router’s routes into the BGP routing table on the core side of the PE router.

As a result of BGP running in the core, core redundancy is also present as shown in Figure 2. With each PE router having connections to multiple P routers and similarly with each P router having multiple connections to other P routers, if a failure of a P router in the core occurs, BGP will automatically re-route the traffic within the network.

<table>
<thead>
<tr>
<th>Table 2. MPLS/BGP VPN Service Offerings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Private IP Network Available</td>
</tr>
<tr>
<td>BGP Required</td>
</tr>
<tr>
<td>Routing Protocols Supported</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Layer 2 Access</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Access Speed</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Internet Access via Private IP</td>
</tr>
<tr>
<td>Optional In-network QoS Support</td>
</tr>
</tbody>
</table>

Is BGP Support Required on the CE Router?
How do the CE and PE routers communicate which routes to advertise into the MPLS/BGP core? In typical hub-and-spoke topology, it does not matter just so long as the PE router has knowledge of the attached customer network(s). This can be a simple static route on the PE router pointing to the CE router along with a default route on the CE router pointing to the PE router, or any dynamic routing protocol (RIP, OSPF, BGP, etc.) peered between the CE router and PE router allowing the CE router to convey its local network(s) to the PE router and allowing the PE router to convey distant customer networks to the CE router.

Typically at a branch or remote site, a single router is present with a switch and multiple devices connected to the switch (a stub VPN). A routing protocol in this case does not benefit the customer since there is only one network with which to connect. (It is important to be able to identify stub and non-stub VPN sites to determine if ADTRAN’s NetVanta® routers are suitable for an application. A stub VPN is most commonly used at a branch site. In a stub VPN, ADTRAN’s NetVanta router is generally suitable.
When is BGP Support Needed in a CE Router?

There are situations where BGP provides advantages over static routing. Three common scenarios exist that require BGP and are generally associated with the host site requirements (non-stub VPN site). Two situations are illustrated in Figure 2 at the BLUE host site CE router. The first case is where multiple connections exist between the CE router and PE router(s) for redundancy, extra capacity, or tariff benefits. It is more likely that a second connection would be to a second PE router or a second carrier. This architecture is called a multi-homed network, meaning the CE router has multiple connections. In a multi-homed architecture, BGP affords a network administrator great control over how traffic flows over the two connections. BGP is more suited to this type of route control over other routing protocols.

The second situation is one where a Disaster Recovery (DR) site is present. In this example, the DR site is at a different location than the primary host site. Much like the first scenario where BGP has well defined control over routes, BGP benefits this situation as well because of its ability to control routing. Routing Information Protocol (RIP) can be used in this situation as well, but many people think RIP is not a robust routing protocol and can have an impact on bandwidth because of the mandatory 30-second routing table updates regardless of network topology changes. OSPF is not well suited for this situation because of the additional complexity with OSPF areas.

The third situation where BGP is needed is when multiple networks exist behind the CE router. This is illustrated in Figure 2 at the BLUE host site with routers or Layer 3 switches behind the CE router. If additional networks are added behind the CE router, BGP running on the CE router will automatically notify the PE router of the new networks, allowing all other CE routers in the network to know of the new networks without any configuration changes to any CE routers. While RIP and OSPF will work to advertise routes, the service provider must configure the PE router to run multiple routing protocols. In a spoke where no other routers are present (a stub VPN), a routing protocol does not benefit a customer on the CE router.

One less common scenario in which a customer might choose to use BGP on the CE router is for controlling which routes are advertised to the PE router. This will not likely be a common scenario with stub VPNs.
Any-to-Any Connectivity

Because the connectivity between sites is established with a VRF table, connectivity between any two sites in the same customer’s network is easily accomplished, creating an Intranet. To realize this, additional routes in the VRF table are installed and then advertised to the PE router’s BGP peers. A more traditional Frame Relay approach to this same type of connectivity would require a completely meshed Frame Relay network with many PVCs, the number growing exponentially as the number of branch sites increases. This solution becomes costly and does not scale well.

From a CPE-based VPN perspective, a mesh network is possible as well, but instead of PVCs to each site, an IPSec/L2TP/PPTP tunnel is required. The monthly recurring costs stays the same regardless of the number of tunnels present, assuming enough bandwidth is available to support the connectivity, but CPE costs could increase substantially to deploy a product that can support enough tunnels.

A hub-and-spoke model where branch sites only have connectivity back to the host site is nothing more than a trivial case of a mesh network. Hub-and-spoke connectivity is still the most common approach according to the service providers surveyed, even though a mesh network is easily obtained.

Switching Labels

Since PVCs are not present in the core, how is the traffic sent from one location to another? The answer lies in MPLS labels and Label Switch Paths (LSPs). An LSP is simply the path packets take to cross the MPLS core to reach the destination PE router. Figure 3 illustrates an example of two LSPs.

Once the traffic hits the source PE router, using the VRF table for a particular customer, two labels are applied to the packet. The “bottom” label is the label for the destination PE router and corresponding VRF table. The “top” label is the next P router along the path to the destination PE router. As the next P router is reached, the top label is popped off and replaced with a label representing the next P router. Once the final P router is reached along the path to the destination PE router, no top label is applied leaving only the label representing the destination PE router. Once a packet reaches the destination PE router, the bottom label is stripped off leaving the original packet in tact. Looking up the packet’s destination in the VRF table allows the PE router to forward the packet to the destination CE router and ultimately to the host on the destination LAN. Note that any remaining MPLS labels are removed by the destination PE router and are not present on either local loop. As such, MPLS support is not required on any CE router.
If multiple paths are present from one PE to another how is the best path chosen? BGP’s metrics define the best path. Alternatively, if a customer requests a specific QoS, data flows over a specific path that is engineered to provide that level of QoS.

Traffic Prioritization

Neither a CPE-based VPN nor traditional Frame Relay-based VPN have in-network QoS support generally available. While it is true that routers and VPN appliances can selectively mark outbound packets with a priority higher than general traffic, these markings are not guaranteed to be honored once the traffic leaves the local loop and enters the Internet or service provider’s network. If an ATM-based VPN is present, QoS is available as part of the ATM protocol, but ATM connections are not commonly found in Enterprise-class networks with connection speeds of less than T3.

The ability to prioritize traffic is another benefit of BGP/MPLS VPNs. Part of the standard allows the reservation of a certain Local Service Provider (LSP) through the network with a given QoS. Using a technology called Resource Reservation Protocol (RSVP), a request of each router along the path in the core can reserve resources to guarantee a specific level of QoS. In order for the PE router to know which traffic is destined for the priority path, the CE router marks priority packets using DiffServ, a technology present in ADTRAN NetVanta® routers.

Internet Connectivity with Private IP

Today, when a customer needs Internet connectivity, the carriers surveyed do not offer a direct Internet connection via their Private IP network. This is because of the need to redistribute all Internet routes into each VRF table, which substantially increases the number of routes in the VRF table and potentially results in reduced PE router performance.

Connecting a customer’s network to the Internet is accomplished in the same way that is commonly found in existing Frame Relay or Point-to-Point networks today with a separate connection and firewall at the host site. In this architecture, Internet traffic is backhauled over the Private IP network. If the host site firewall is not configured properly, only that customer’s network is affected because of the inherent security found in the Private IP core by virtue of the VRF tables in the PE routers.

Summary

Private IP networks offer many benefits over more traditional methods of connectivity. The benefits of Private IP service include lower monthly cost, equivalent security, easier management and configuration of routers at the customer premise, and the availability of QoS inside the service provider’s network. Additional benefits include the ability to connect any site together with any other site just by changing routing information on the service provider’s PE router. This reduces cost to the customer and network complexity by eliminating the need for PVC, point-to-point, or IPSec/L2TP/PPTP tunnels to each site.

The ADTRAN Advantage

ADTRAN’s NetVanta routers are well positioned to support a variety of connectivity options into a carrier’s private IP network. The NetVanta 3000 Series is designed for customers with bandwidth needs up to three T1s. The NetVanta 4000 Series includes connectivity options for aggregating up to eight T1s together, while the NetVanta 5000 Series includes support for dual DS3s. All NetVanta routers are based on the ADTRAN Operating System (OS), a common operating system across all NetVanta routers, switches, and security appliance products. ADTRAN OS supports common routing protocols such as RIP and OSPF, and provides for Frame Relay, PPP, Multilink PPP, and PPPoE connectivity. Management of ADTRAN’s NetVanta routers is based around the industry’s de facto standard Command Line Interface (CLI), minimizing the need to retrain IT staff. In addition to the CLI, the NetVanta 3000 Series includes a built-in web-based Graphical User Interface (GUI) for configuration and SNMP support for third party SNMP management platforms.

In addition, ADTRAN’s NetVanta router products are part of an overall network security solution. By including a stateful inspection firewall as part of the standard feature package, network security is enhanced without costly add-ons. Optional IPSec-based VPN support is also available for customers who need a hybrid network infrastructure model to support mobile users or gateway-to-gateway VPNs.

Finally, every ADTRAN NetVanta product includes no cost pre- and post-sale technical support and software updates for the life of the product without requiring a costly maintenance contract. For more information on ADTRAN’s complete family of NetVanta LAN-to-WAN products, see ADTRAN’s Dare to Compare web site at: www.dare2compare.adtran.com
ADTRAN, Inc.
Attn: Enterprise Networks
901 Explorer Boulevard
Huntsville, AL 35806

P.O. Box 140000
Huntsville, AL 35814-4000

256 963-8000 voice
256 963-8699 fax

General Information
800 9ADTRAN
info@adtran.com
www.adtran.com

Pre-Sales
Technical Support
800 615-1176 toll-free
application.engineer@adtran.com
www.adtran.com/support

Where to Buy
877 280-8416 toll-free
channel.sales@adtran.com
www.adtran.com/where2buy

Post-Sales
Technical Support
888 423-8726
support@adtran.com
www.adtran.com/support

ACES Installation & Maintenance Service
888 874-ACES
aces@adtran.com
www.adtran.com/support

International Inquiries
256 963 8000 voice
256 963-6300 fax
international@adtran.com
www.adtran.com/international

For the regional office nearest you, visit:
www.adtran.com/regional

To download a searchable version of the 2005 ADTRAN Enterprise Networks Catalog, visit:
www.adtran.com/ecatalog

About ADTRAN®
ADTRAN, Inc. is one of the world’s most successful network access equipment suppliers, with a 17-year history of profitability and a portfolio of more than 1,300 solutions for use in the last mile of today’s telecommunications networks. Widely deployed by carriers and enterprises, ADTRAN solutions enable voice, data, video, and Internet communications across copper, fiber, and wireless network infrastructures. ADTRAN solutions are currently in use by every major domestic service provider and many international ones, as well as by thousands of public, private and governmental organizations worldwide.

ADTRAN, Inc.
901 Explorer Boulevard
Huntsville, Alabama 35806
P.O. Box 140000
Huntsville, Alabama 35814-4000

800 9ADTRAN
256 963-8000 voice
256 963-8004 fax
info@adtran.com e-mail
www.adtran.com website

ADTRAN, Inc. is committed to utilize Minority Business Enterprises (MBE), Woman-Owned Business Enterprises (WBE) and Disabled Veteran Business Enterprises (DVBE) whenever possible and practical for procurements supporting ADTRAN and our customers.

Copyright © 2005
ADTRAN, Inc. All rights reserved. ADTRAN and NetVanta are registered trademarks of ADTRAN, Inc. All other trademarks and registered trademarks are the property of their respective owners.

EN683A