In this chapter, you learn about the following:

- How MPLS provides security (VPN separation, robustness against attacks, core hiding, and spoofing protection)
- How the different Inter-AS and Carrier's Carrier models work, and how secure they are compared to each other
- Which security mechanisms the MPLS architecture does not provide
- How MPLS VPNs compare in security to ATM or Frame Relay VPNs.

CHAPTER 3

MPLS Security Analysis

VPN users have certain expectations and requirements for their VPN service. In a nutshell, they want their service to be both private and secure. In other words, they want their VPN to be as secure as with dedicated circuits while gaining the scalability benefits of a shared infrastructure. Both concepts, of privacy and security, are not black and white, and need to be defined for a real world implementation.

This chapter defines typical VPN security requirements, based on the threat model developed in the previous chapter, and discusses in detail how MPLS can fulfill them. The typical VPN security requirements are

- VPN separation (addressing and traffic)
- Robustness against attacks
- Hiding of the core infrastructure
- Protection against VPN spoofing

We also explain which security features MPLS VPNs do not provide, and compare the security capabilities of MPLS VPNs with Layer 2–based VPN services such as ATM and Frame Relay.

NOTE This chapter analyses the *architecture* of MPLS/VPN networks, that is, how the standards define the architecture and protocols. In other words, for this chapter, we assume that the MPLS core is configured and operated correctly. Implementation issues are discussed in Chapter 4, “Secure MPLS VPN Designs,” and Chapter 5, “Security Recommendations.” Operational aspects are covered in Chapter 8, “Secure Operation and Maintenance of an MPLS Core.”

VPN Separation

The most important security requirement for VPN users is typically that their traffic be kept separate from other VPN traffic and core traffic. This refers to both its traffic not being seen in other VPNs, and also other VPNs traffic or core traffic not intruding into their VPN. Referring to the threat model from the previous chapter, this section analyses a threat against a VPN, specifically intrusions into and from other VPNs.

Another requirement is that each VPN be able to use the complete IP address space without affecting or being affected by other VPNs or the core.

NOTE The CE-PE links belong logically to the VPN, even though they are usually addressed with provider address space. The reason provider address space is used is that management from the NOC requires unique CE addresses.

The service provider has the requirement that the core remain separate from the VPNs in the sense that the address space in use does not conflict with any VPN and that VPN traffic remains separate on the core from the control plane traffic on the core.

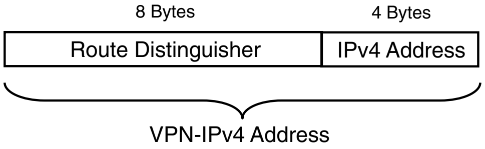
In other words, a given VPN must be completely separate from other VPNs or the core in terms of traffic separation and address space separation. We will now analyze how the standard, RFC 2547bis, meets these requirements. In the first section, we see how it achieves address space separation, and in the following section how data and control traffic are kept architecturally separate—between VPNs, but also between a VPN and the core.

NOTE Again, this chapter assumes that the network is securely implemented and operated, and the analysis concentrates completely on the standard.

Address Space Separation

To be able to distinguish between addresses from different VPNs, RFC 2547bis does not use standard IPv4 (or IPv6) addressing on the control plane for VPNs on the core. Instead, the standard introduces the concept of the *VPN-IPv4 or VPN-IPv6 address family.* A VPN-IPv4 address consists of an 8-byte *route distinguisher (RD)* followed by a 4-byte IPv4 address, as shown in Figure 3-1. Similarly, a VPN-IPv6 address consists of an 8-byte *route distinguisher (RD)* followed by a 16-byte IPv6 address.[1]

Figure 3-1 *Structure of VPN-IPv4 Addresses*

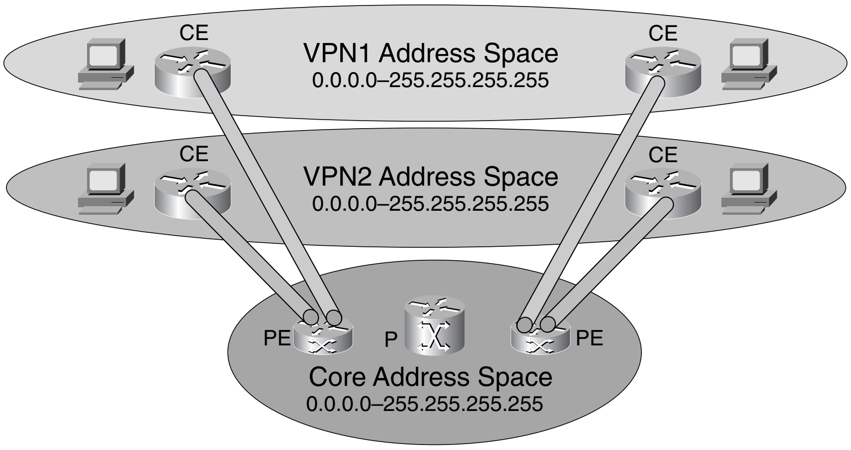


The purpose of the RD is to allow the entire IPv4 space to be used in different contexts (for VPNs, in our example). On a given router, a single RD can define a VPN routing/forwarding instance (VRF), in which the entire IPv4 address space may be used independently.

NOTE RFC 2547bis defines a semantic for RDs, but this serves only administrative purposes, to make it easier to select unique RDs. For security considerations, it is only important to understand that the RD makes the IPv4 routes of a VPN unique on the MPLS VPN core.

Due to the architecture of MPLS IP VPNs, only the PE routers have to know the VPN routes. Because PE routers use VPN-IPv4 addresses exclusively for VPNs, the address space is separated between VPNs. In addition, because they use IPv4 internally in the core, which is a different address family from the VPN-IPv4 address family, the core also has independent address space from the VPNs. This provides a clear separation between VPNs, and between VPNs and the core. Figure 3-2 illustrates how different address spaces are used on an MPLS IP VPN core.

Figure 3-2 *Address Planes in an MPLS VPN Network*



There is one special case in this model. The attachment circuit on a PE, which connects a VPN CE, is part of the VRF of that VPN and thus belongs to the VPN. However, the address of this PE interface is part of the VPN-IPv4 address space of the VPN and therefore not accessible from other interfaces on the same PE, from other core routers, or from other VPNs.

For practical purposes, this means that address space separation between VPNs and between a VPN and the core is still perfect because this PE interface to the CE belongs to the VPN and is treated as a VPN address. However, this also means that addresses exist in the VPN that belong to a PE. Consequently, a PE can by default be reached from a VPN, which might be used to attack that PE. This is a very important case and is discussed in detail in Chapter 5, “Security Recommendations.”

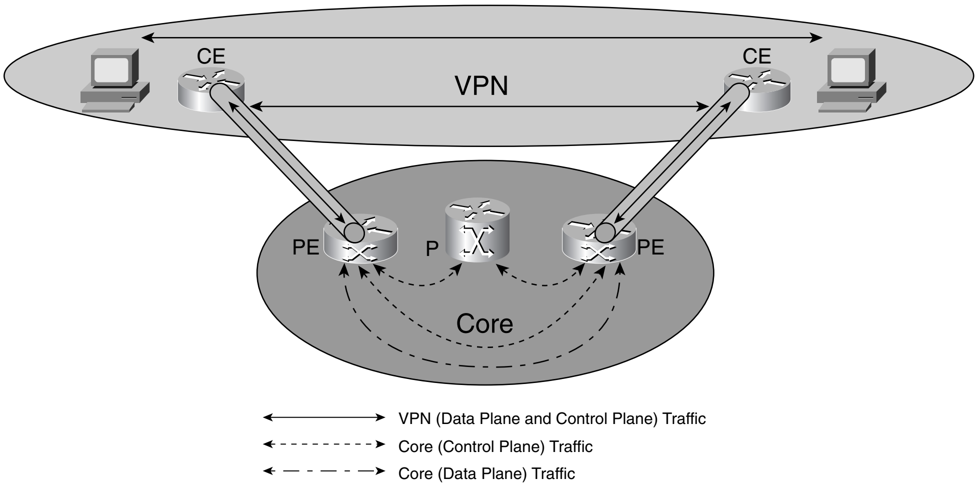
NOTE All security mechanisms explained in this chapter work only when configured correctly and when the network is correctly implemented. Operational and implementation issues are discussed in later chapters. Here, we concentrate on the standards.

Traffic Separation

VPN traffic consists of VPN data plane and control plane traffic. For the sake of this discussion, both will be examined together. The VPN user's requirement is that their traffic (both types) does not mix with other VPNs' traffic or core traffic, that their packets are not sent to another VPN, and that other VPNs cannot send traffic into their VPN.

On the service provider network, this definition needs to be refined because VPN traffic will obviously have to be transported on the MPLS core. Here, we distinguish between control plane and data plane traffic, where the control plane is traffic originating and terminating within the core and the data plane contains the traffic from the various VPNs. This VPN traffic is encapsulated, typically in an LSP, and sent from PE to PE. Due to this encapsulation, the core never sees the VPN traffic. Figure 3-3 illustrates the various traffic types on the MPLS VPN core.

Figure 3-3 *Traffic Separation*


CE
CE
VPN
PE
P
PE
Core
VPN (Data Plane and Control Plane) Traffic
Core (Control Plane) Traffic
Core (Data Plane) Traffic

VPN traffic consists of traffic from and to end stations in a VPN and traffic between CEs (for example, if IPsec is implemented between the CEs).

Each interface can only belong to one single VRF, depending on its configuration. So for VPN customer "red," connected to the PE on a fast Ethernet interface, the interface command **ip vrf forwarding** *VPN* determines the VRF. Example 3-1 shows the configuration for this.

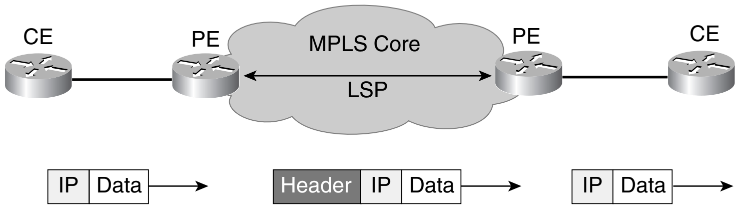
Example 3-1 *VRF Configuration of an Interface*

```
interface FastEthernet1/0
 ip vrf forwarding red
 ip address 1.1.1.1 255.255.255.0
```

Traffic separation on a PE router is implemented differently, depending on the type of interface on which the packet enters the router.

- **Non-VRF interface**—If the packet enters on an interface associated with the global routing table (no **ip vrf forwarding** command), the forwarding decision is made based on the global routing table, and the packet is treated like a normal IP packet. Only core traffic uses non-VRF interfaces, thus no further separation is required. (Inter-AS and Carrier's Carrier scenarios make an exception to this rule and are discussed later in this chapter.)
- **VRF interface**—If the packet enters on an interface linked to a VRF using the **ip vrf forwarding** *VPN* command, then a forwarding decision is made based on the *forwarding table* (or *forwarding information base, FIB*) of that VRF. The next hop from a PE perspective always points to another PE router, and the FIB entry contains the encapsulation method for the packet on the core. Traffic separation between various VPNs is then achieved by encapsulating the received packet with a VPN-specific header. There are various options for how to encapsulate and forward VPN packets on the core—through a *Label Switch Path (LSP)*,[2] an *IPsec* tunnel,[3] an *L2TPv3* tunnel,[4] or a simple *IPinIP* or *GRE* tunnel.[5] All of the methods keep various VPNs separate, either by using different tunnels for different VPNs or by tagging each packet with a VPN-specific header. Figure 3-4 shows how packets are encapsulated within the MPLS core.

Figure 3-4 *Encapsulation on the Core*



P routers have no active role in keeping traffic from VPNs separate: they just connect the PE routers together through LSPs or the other methods just described. It is one of the key advantages of the MPLS VPN architecture that P routers do not keep VPN-specific information. This aids the scalability of the core, but it also helps security because by not having visibility of VPNs the P routers also have no way to interfere with VPN separation. Therefore, P routers have no impact on the security of an MPLS core.

NOTE In this chapter, as always, we assume correct operation and implementation. It is conceivable to construct a P router with the capability to also modify VPN traffic. However, this would constitute an operational mistake. (Current IOS and IOS-XR versions used for P routers do not permit modification of the tunnel content.) It is also possible for a service provider to use a packet generator to produce crafted packets and insert them into the core—anything can be faked that way. As mentioned before, the service provider must be trusted by the VPN users, or VPN-specific security such as IPsec is required.

In summary, VPN users can expect their VPN to be separate from other VPNs and the core because

- An interface on a PE (for example, the interface holding the user's attachment circuit) can only belong to a single VRF or the core.
- The attachment circuit (PE-CE link) to this interface belongs logically to the VPN of the user. No other VPN has access to it.
- On the PE the address information of the VPN is held as VPN-IPv4 addresses, making each VPN unique through unique route distinguishers. VPN-IPv4 addresses are only held on PE routers and route reflectors.
- VPN traffic is forwarded through the core through VPN-specific paths or tunnels, typically tagging each packet with a VPN-specific label.
- P routers have no knowledge of VPNs, thus they cannot interfere with VPN separation.

The service provider can expect its core to be separate from the VPNs because

- PE and P addresses are IPv4 addresses. VPNs use exclusively VPN-IPv4 addresses and cannot access PE and P routers. (Exception: The attachment circuit on the PE, which needs to be secured. See Chapter 4, "Secure MPLS VPN Designs.")

For more technical details on how VPN separation is technically implemented, please refer to RFC 2547bis.

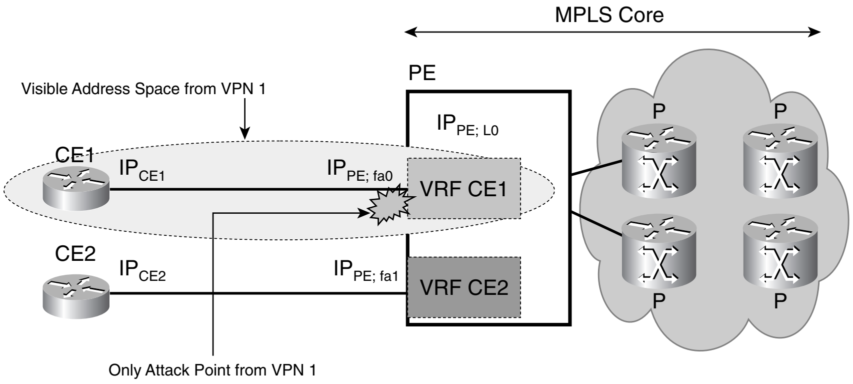
Robustness Against Attacks

Over the last years, there have been an increasing number of attacks not only against application servers, but also directly against networking infrastructure. Service providers, therefore, have to be extremely careful about securing their core network well. The drastic effects of DoS attacks are mostly understood, but on MPLS VPN networks there is an additional, much more serious danger: if an attacker can control a PE device, the security of any VPN on the MPLS core can be compromised, whether connected to this PE or not. It is therefore of paramount importance for the service provider, but also for the VPN users, that the core, specifically the PEs, are properly secured and not attackable.

Where an MPLS Core Can Be Attacked

As the previous section shows, VPNs are separated from each other and from the core. This also limits potential attack points: Figure 3-5 illustrates the only interface point where a VPN can "see" the core and send packets to a core device: this is the PE router because the attachment circuit between CE and PE belongs to the VPN. Therefore, the only attack points seen from a VPN are all the PE interfaces that connect to CEs of that VPN. In the figure, VPN 1 can only see the PE interface it connects to and no other interface on that PE. Note that there is an attack point for each CE-PE connection, so that all of those PE interfaces must be protected from the entire VPN space. A VPN can*not* see any other interface on the PE, nor any core routers (for example, P routers or route reflectors).

Figure 3-5 *Visible Address Space from a VPN*



NOTE A CE router is *always* untrusted, even if the CE is managed by the service provider. The reason is that the CE is usually placed on customer premises and could, for example, be replaced by another router or even, in some cases, a workstation. A PE router, on the other hand, is *always* trusted, and *must* be trusted, because an intruder on a PE could jeopardize the security of *all* VPNs. This implies that a PE must always be in a physically secured environment.

Each VPN can see and, by default, reach all of its PE peer addresses. These are the only direct attack points in an MPLS VPN environment, and this needs to be examined in more detail. How can a PE router be attacked from the outside?

NOTE P routers cannot be directly attacked from a VPN because they are not reachable from there.

How an MPLS Core Can Be Attacked

In principle, a PE can be attacked with either transit traffic (not destined to the PE itself) or with targeted traffic to the PE. Traffic that is destined to a router is generally also called *receive traffic.*

Transit traffic is usually less of a problem because routers are designed to forward traffic fast. A router must, of course, be appropriately dimensioned to handle all potential transit traffic, which is a question of network design. This will be covered in detail in Chapter 4, "Secure MPLS VPN Designs," and Chapter 5, "Security Recommendations." However, certain forms of packets cannot be handled in hardware and can cause additional load on a router. Therefore, floods with such packets can lead to a DoS situation on the router.

Packets with *IP options* are one example. A packet with IP options has a variable IP header length and cannot, therefore, be looked up in current ASICs (microchips). This means that IP option packets must be switched in software, which lowers the performance of the router. Ways to protect against this are explained in Chapter 5.

Receive traffic, or traffic destined to the PE, is more of a concern because it affects the PE more directly. Two forms of attack are possible with receive traffic:

- **DoS**—In this case, an attacker tries to consume all resources on a PE router. This could be done, for example, by sending too many routing updates to the router, consuming all available memory.
- **Intrusion**—Here an attacker attempts to use a legal channel to configure the PE router. Examples are password guessing attacks against the telnet or SSH port, or SNMP writes to the router.

How the Core Can Be Protected

All of the potential attacks can be well controlled by appropriate configuration. In short, the recommendation is to block via an *access control list (ACL)* all access to all reachable PE interfaces. If routing is required, the routing port should be the only port on the PE not blocked by the interface ACL. Now an attacker can only attack the routing protocol directly, and that needs to be secured separately.

NOTE Theoretically, if the PE is correctly configured, it should not be necessary to configure interface ACLs to protect it. However, in practice, two types of security problems arise: 1) operational issues, such as an erroneous AAA configuration or a weak password, and 2) implementation issues, where the operating system may have a security vulnerability. For better protection, it is therefore always recommended not to rely on a single layer of defense, but to configure additional security measures, such as interface ACLs in this example.

Following these recommendations, the PE will exclusively accept packets on the port for the routing protocol. This can also be secured, as explained in detail in Chapter 5. Any other packet destined to the PE will be dropped by the ACLs.

For overall security, of course all of the interfaces into the core need to be considered. Up to here we have covered the PE-CE interfaces. Another important point to control is the access to the Internet, and the question is whether an MPLS core or its VPNs can be attacked from the Internet.

If Internet access is provided in a VRF as if it were just another VPN, then all the above considerations apply equally to the Internet access: the Internet PE has to be dimensioned correctly, secured with ACLs, and the routing has to be secured separately.

If Internet is provided from the global routing table, then this access has to be secured in a different way. How Internet can be provisioned, what the security consequences are, and how to secure it is discussed in the Chapter 4.

NOTE This chapter discusses only architectural security of MPLS, that is, whether an MPLS/VPN core *can* be secured. In real life the question arises whether the service provider actually implements and operates the core correctly. Overall security also depends on correct operation and implementation of the core. This is discussed in detail in Chapters 4 and 8.

Assuming proper implementation and operation, an MPLS VPN core provides a very high level of security: First of all, the interface into the core is limited to peering PE addresses only, and these can be secured well. This way, an MPLS/VPN core has considerably less exposure to attacks from the outside than a traditional IP backbone, where every interface on every core router might be a target for an attack. One of the key advantages of MPLS, then, is that it has small, well securable edges to the outside, making it easier to secure.

A traditional IP core, in comparison, is by default quite open, and each network element is reachable from the outside. This can in principal be limited by various means, such as ACLs or some core hiding techniques. But the advantage in an MPLS core is that the majority of the core is unreachable by architecture. Note that this depends how Internet routing is carried on the core: if it is carried in the global table, the risks of traditional IP cores apply as well. The key to security on an MPLS core is limited access to the global routing table from the outside. Chapter 4, “Secure MPLS VPN Designs,” discusses the various options on Internet provisioning in detail.

Hiding the Core Infrastructure

Traditional Layer 2 VPNs such as Frame Relay or ATM have the characteristic that the VPN user cannot “see” the core infrastructure. In these cases, the reason is that the user connects a Layer 3 device to a Layer 2 network, such that the Layer 2 infrastructure is mostly hidden to the user. In general, most VPN users prefer to have details of the core hidden to them.

MPLS VPN networks hide most of their core infrastructure in the architecture. As shown previously in Figure 3-5, only the peering PE addresses are exposed to the VPN user; P routers are completely hidden. It is important to understand that the hiding of the core is not due to ACLs but to the intrinsic way of handling separate address spaces on an MPLS core: even if an address of a P router would be known to an outsider, this address does not belong to the address space of the VPN user, and therefore it not reachable.

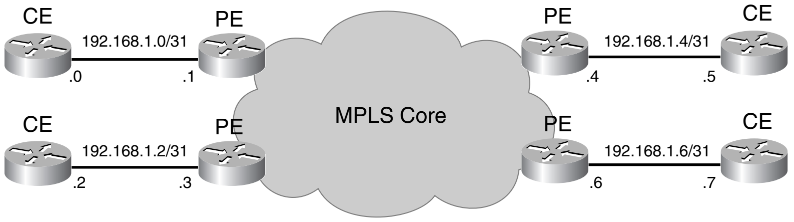
The only exception to this is the peering address of the PE router. However, the address space of the CE-PE attachment circuits belongs to the VPN, not to the core. In fact, the same CE-PE address space could be used in several VPNs without address conflicts. Therefore, even though a PE address might be visible to the VPN, strictly speaking, no core information is passed to the outside because the address in question is VPN address space.

However, in reality, the reason to keep core infrastructure hidden is to avoid attacks against it. Therefore, considering which address space the PE peering address belongs to can be seen as mainly academic.

There is, however, a way to completely hide the PE routers from the VPN user: by using unnumbered address space and static routing between PE and CE. Here, an ACL could be applied to all PE peering interfaces of that VRF (where they exist), dropping any IP packet to the PEs' peering addresses (don't forget that *all* PE peering addresses toward *all* CEs of the VPN have to be secured this way).

In many cases, there are advantages to keeping the attachment circuit numbered—to monitor the health of the link, for example. Figure 3-6 shows a numbering scheme for such a case.

Figure 3-6 *PE-CE Addressing*



NOTE **Recommendation**

All attachment circuits of a given VPN should be addressed out of a contiguous supernet to simplify aggregation and protection of the PE via an ACL.

Example 3-2 shows how to implement this complete access control to the PE.

Example 3-2 *ACL to Protect PE Peering Interfaces*

```
access-list 101 remark 192.168.1.0/24 is the space used for PE-CE addressing
access-list 101 remark throughout this particular VPN, which is connected to
access-list 101 remark interface serial 0/1.
access-list 101 deny ip any 192.168.1.0 0.0.0.255
access-list 101 remark The next line permits transit traffic (important!)
access-list 101 permit ip any any
!
interface serial 0/1

ip access-group 101 in
```

In this example, the first line in the ACL covers all the PE-CE address space of that particular VPN. Note the following:

- In many real life implementations, this would require more lines to cover all the PE-CE address spaces (attachment circuits).
- Don’t forget the last line: it permits all transit traffic.
- Other PE addresses, which do not belong to the VPN, do *not* have to be included, nor does any P addressing, because they are not reachable by architecture.
- This example assumes static routing (that is, no routing protocol) between CE and PE. If routing is required, the specific protocol must be permitted in the above ACL.
- The ACL as described here also blocks access to the interfaces of the CEs that are facing the PEs (see Figure 3-6). For example, 192.168.1.5 belongs to a CE, but this address is blocked by the ACL. Therefore, other CEs cannot ping that address. Also, a ping from this CE across the MPLS core would not work because return packets would be blocked, unless another source IP was chosen manually for the ping (using extended ping). This might not be desirable if, for example, a network management station pings these CE interfaces. To avoid that, you can either list all PE addresses of the VPN separately as host entries (/32) or ping loopback addresses on the CEs instead.

Implementing Example 3-2 for a given VPN, the core is entirely protected from that VPN.

Should routing be required, then the required ports need to be permitted from the CE and only the CE. This is described in more detail with examples in Chapter 5, “Security Recommendations.” In this case, the peering PE address is not hidden, but as mentioned before, the address space belongs to the VPN.

Regarding core hiding, the main goal of service providers is to provide higher resistance against attacks. The previous section shows that even with the peering PE address exposed, sufficient security can be achieved.

VPN users asking for core hiding usually want to keep the network as simple as possible. The fact that a routing relationship with the PEs might be required is usually not seen as a strong impediment against using an MPLS service.

Protection Against Spoofing

When the Internet was in its early stages, the source address of a packet itself was considered sufficient to prove that the packet was really sent by this IP address. In early versions of UNIX, there is a whole command suite, the so-called "r-commands," such as **rlogin**, **rcp**, **rsh**, and so on, which rely on the IP address for authentication.

Today, IP address spoofing is an everyday occurrence in various types of attacks, and engineers have learned not to rely on the IP source address.

Since MPLS is a Layer 3 technology, users are concerned about spoofing on the MPLS network, both on the IP level and with the labels used by the MPLS protocols. Questions asked include "Can another VPN user spoof my IP address range to get into my VPN?" and "Can someone spoof VPN labels to intrude into my VPN?"

These questions can be easily answered:

- **IP address spoofing**—As discussed previously and shown in Figure 3-2, each VPN can use the entire theoretical IP address space, from 0.0.0.0 to 255.255.255.255. A certain VPN site or host may indeed spoof IP addresses, but the spoofing will remain local to that VPN. This is, in fact, a strength of MPLS VPNs: the VPN user may use the entire address space, including fake addresses, and the VPN behaves like a physical network with just that VPN user. This is possible because the PE routers keep all packets within the VRF context, such that even fake packets cannot "escape" that VPN context. Therefore, IP address spoofing in a VPN does not affect VPN separation.
- **Label spoofing**—Within the MPLS core, packets of different VPNs are distinguished by prepending a VPN label to the packet. A malicious VPN user may try to create specifically crafted packets with a fake VPN label and insert those into the MPLS core, trying to get those packets into another VPN. This is also impossible because PEs do not accept labeled packets from CEs. Therefore, such a faked packet would simply be dropped by the PE.

NOTE The Inter-AS and Carriers' Carrier topologies are an exception to this rule because they do allow labeled packets to be sent to a PE router from the outside. These cases are discussed in the following sections in more detail.

But what if the packet with a spoofed VPN label is inserted within the core? Then this packet may really be routed to a random VPN, assuming the attacker knows (or can guess) some internal details of the MPLS core, such as VPN label numbers and egress PE label numbers.

The assumption made in this chapter is that the MPLS network is an integer (in other words, that the core is secure). This assumption includes the fact that the only interfaces into the network are the PE-CE interfaces. This may seem an unrealistic assumption at first, but in fact, any VPN technology is insecure if someone can insert packets in the core, because it would allow, for example, the insertion of random ATM cells with crafted virtual path and circuit information, and the same effect: getting packets into another VPN.

Therefore, the MPLS core is treated as a zone of trust where packets can only enter on well-known interfaces. See Chapter 1, "MPLS VPN Security: An Overview," for more details on zones of trust and this concept.

NOTE In a standard MPLS VPN network consisting of a single AS, as defined in RFC 2547, a VPN user can assume a "virtually private" service with full separation, but the user has to trust the service provider to configure and operate the MPLS core correctly. Configuration mistakes or operational mistakes on the side of the service provider may break the security of the VPN. Also, data in transit are not encrypted and can be sniffed anywhere between the CEs. (This is discussed in more detail in Chapter 6, "How IPsec Complements MPLS.")

Assuming that packets can only enter the MPLS core through defined PE-CE interfaces, spoofing is not possible. RFC 2547, the first version of the standard for BGP/MPLS IP VPNs, describes only IP interfaces into the core, which allows this relatively simple security analysis.

RFC 2547bis, the second version of the standard, however, adds another form of interface—the Inter-AS and Carriers' Carrier architectures—which allow labeled packets entering the core. This changes the security exposure significantly and is therefore discussed in the following two sections in more detail.

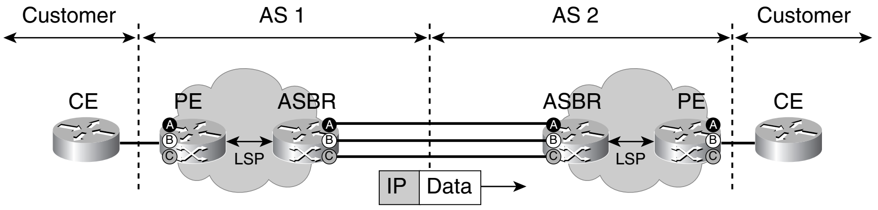
Specific Inter-AS Considerations

The drawback of RFC 2547 is that it requires a single *autonomous system* (AS) to provide VPNs across it. RFC 2547bis allows VPNs to be provided across several ASs and thus several service providers. The standard describes three basic models for Inter-AS connectivity (models A, B, and C) that have different security properties.

Model A: VRF-to-VRF Connections at the AS Border Routers

This model is the simplest one, as it uses interfaces or subinterfaces between *autonomous system border routers (ASBRs)* to keep the VPNs separate. Figure 3-7 shows this principle: the two ASBRs each hold a VRF for each VPN that is shared between the autonomous systems. The ASBRs are then connected, and subinterfaces are used to link the VRFs directly.

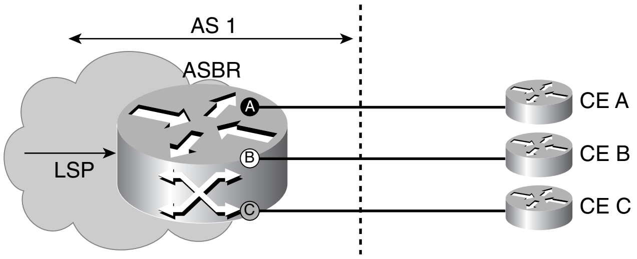
Figure 3-7 *Inter-AS Model A*



This model is equivalent in security to the standard RFC 2547 implementation because all external interfaces (seen from either AS) are IP interfaces.

In fact, an ASBR in this model behaves exactly like a normal PE router, and the configuration on an ASBR is also exactly the same as if it connected to a CE router in each VRF. Figure 3-8 shows how an ASBR in this model sees the other connections around it.

Figure 3-8 *Inter-AS Model A: How an ASBR Sees Its Peers*



Therefore, all the considerations from the previous sections apply also in this model: there is strict separation between VRFs, label spoofing is impossible because no labeled packets are accepted by the ASBR from the other ASBR, and the other AS cannot "see" the core.

A further advantage of Inter-AS model A is that existing provisioning systems require little or no changes to support this model because the ASBR is essentially a normal PE, with attachment circuits to untrusted routers. To the provisioning system, such an Inter-AS connection looks like a number of normal CE connections.

For the same reasons, this model is also the easiest in other aspects, such as quality of service (QoS): everything that is possible on a subinterface can be supported automatically in this model. Because consistent QoS is important, especially when several service providers are involved in the provisioning of a VPN, it is important to have clear interfaces.

A service provider can deploy this model without further security implications over the standard MPLS VPN model, just as it would deploy more CE connections.

A VPN user in a single-AS RFC 2547 network has to trust the service provider for correct implementation and operation of the core. In Inter-AS model A, the user must trust *all* service providers that provide parts of the user's MPLS VPN in this way, but there is no further risk of interference with third parties. The only potential risk is that a service provider connects the VPNs from the other service provider wrongly, but this problem also exists in standard single-AS MPLS networks and has to be controlled operationally.

Inter-AS model A is the most secure interconnection model, but it has scalability issues on the ASBR: the ASBR must be configured with all shared VPNs (VPNs spanning more than one AS) and thus hold all VPN routes of shared VPNs. VPNs that exist only on one AS do not need to be kept on the ASBR. Furthermore, the interface between the ASBRs is not very flexible: a new subinterface must be configured on both sides for each new shared VPN.

The limiting scalability factor in Inter-AS model A is the number of interfaces or subinterfaces required, the number of VRFs required, and the memory required to hold all the routes from the various shared VPNs. Only Inter-AS model A has VRFs configured, so VRF memory is a deciding factor between the different Inter-AS types.

Two more MPLS interconnection models are defined in RFC 2547bis, with the goal of making the interconnection between ASs more scalable. Model B removes the need for separate subinterfaces, and model C even removes the need for configuring VRFs on the ASBRs. Both models are more scalable than model A, but this scalability has security consequences.

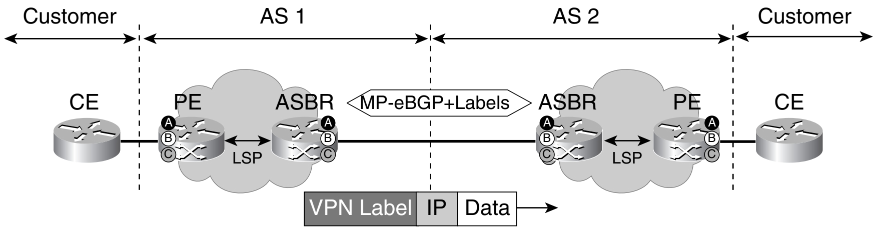
Model B: EBGP Redistribution of Labeled VPN-IPv4 Routes from AS to Neighboring AS

Model B removes the need for separate (sub-) interfaces per shared VPN on the ASBR. Here, only a single interface is required between the ASBRs. To be able to still distinguish the data packets from each VPN, packets must now be labeled on the data plane. This essentially creates a type of "tunnel" for each VPN on the single connection, defined by the label. These labels could be configured manually, but for ease of use, the control plane controls the labels in use. The *Multi-Protocol Exterior Border Gateway Protocol (MP-eBGP)* is used to pass VPN routes between ASBRs, and it assigns the labels to be used for each VPN prefix.

How Model B Works

Figure 3-9 illustrates model B: On the control plane, a single instance of MP-eBGP is used, exchanging all VPN-IPv4 routes, together with the required parameters (RD, label, and so on). On the data plane, all VPN packets are labeled to distinguish the VPN they belong to. In model B, the ASBR still needs to keep all VPN routes of the exchanged VPNs, as in model A, but here there is only a single interconnection.

Figure 3-9 *Inter-AS Model B*



The standard for Multi-Protocol extensions for BGP (MP-BGP) is defined in RFC 2858. Although BGP only uses IPv4, MP-BGP uses the concept of an *address family* to enable BGP to carry VPN-IPv4 routes as a new address type. For this purpose, MP-BGP introduces two new attribute types, MP_REACH_NLRI and MP_UNREACH_NLRI, to announce and withdraw multiprotocol *Network Layer Reachability Information* (NLRI). The NLRI contains the VPN-IPv4 prefix (which in turn contains the RD) and the label. Example 3-3 shows how VPN label information can be seen on an ASBR.

Example 3-3 **show ip bgp vpnv4 vrf A labels**

```
PE#  sh ip bgp vpnv4 vrf A labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (A)
   10.10.10.10/32   192.168.10.10   10/12
```

This model makes the security between the service providers somewhat more complex. For the VPN user, however, nothing changes in comparison to model A: The VPN user must still trust both service providers, but third parties still can not interfere with this solution.

Security of Model B

To analyze the security between service providers, we examine the data plane and control plane separately.

On the control plane, there is a single MP-eBGP session between ASBRs, nothing else. Specifically, there is no *Tag Distribution Protocol (TDP)* or *Label Distribution Protocol (LDP)* running between ASBRs. This session can be and should be secured as any other BGP session: peer authentication with *message digest 5 (MD5)*, maximum route limits per peer and per VRF, dampening, and so on. In addition, prefix filters can be deployed to control which routes can be received from the other AS. Details on how to secure such BGP sessions are discussed in Chapter 5, "Security Recommendations."

With the Chapter 5 recommendations implemented on the two ASBRs, the MP-eBGP control plane does not increase the security exposure over model A and can be considered sufficiently secure for both service provider and VPN user.

On the data plane, labeled packets are exchanged. The label is derived from the MP-eBGP session; therefore, the ASBR announcing a VPN-IPv4 prefix controls and assigns the label for each prefix it announces. On the data plane, the incoming label is then checked to verify that this label on the data plane has really been assigned on the control plane. Therefore, it is impossible to introduce fake labels from one AS to another.

This control on the data plane means that packets with labels that were not assigned to the other ASBR will be dropped; however, it is *not* possible to check *which* of the correctly assigned labels is being used.

As an example, assume that an ASBR has announced two prefixes: one from VPN A with label 20, and another prefix from VPN B with label 21. On the data plane, packets with labels other than 20 or 21 can be dropped, but it is not possible to verify that a packet with label 21 really belongs to VRF B.

However, in reality, this does not add a new security exposure: each service provider involved in the provisioning of a VPN has the power to make each VPN insecure (which is not a specific MPLS problem). This does not change when VPNs are shared. As previously mentioned, the VPN user must trust all service providers involved in the provisioning of the VPN.

NOTE Current versions of IOS (as of February, 2005) do not check the front label of an incoming packet on the data plane if the incoming interface terminates in the global routing table. The front label is only checked if the incoming interface terminates on a VRF (such as in the CsC case). Therefore, an additional security issue currently exists for Inter-AS case B: since the top label is currently unchecked, packets might enter an LSP to a PE router. At the penultimate router, the top label is popped and the resulting packet is presented to the egress PE, which would route it normally. This cannot happen accidentally and would be hard to execute deliberately. Also, such an attack could only come from the other service provider core, not from any of its connected customers.

There is one more potential issue to look at: Layer 2 security. All the considerations so far have been exclusively on Layer 3 and above. However, for a Layer 3 service such as MPLS VPNs to be secure, the lower layers must be secure as well. We have already discussed one Layer 1 issue: a wiretap on core lines or CE-PE lines reveals VPN data, unless encryption is used on top of MPLS.

A potential Layer 2 issue relates to using a shared switch to interconnect various MPLS networks in the Inter-AS model: if the connection between the ASBRs is provided (for example, on an Ethernet switch), Layer 2 security must be taken into consideration. This type of security threat is detailed in Chapter 4, “Secure MPLS/VPN Designs.” (A quick summary here: VLANs can usually be assumed to be separate from other traffic on the switch, but within a VLAN there are security issues such as a third party inserting labeled traffic.

NOTE Never connect ASBRs over a shared Layer 2 infrastructure such as an *Internet Exchange Point (IXP)*. Use a private connection, or at least a private VLAN.

In comparison with model A, model B is more scalable in that it requires only one connection between the ASBRs over which all VPNs are propagated. For this to work, MP-eBGP must be run between the ASBRs, and traffic is exchanged with labels. This can be secured adequately, but with more configuration the likelihood of error and a subsequent security breach increases.

Model B still requires each ASBR to hold the VPN routes for each shared VPN, and this is another scalability concern. To solve this issue, model C was invented.

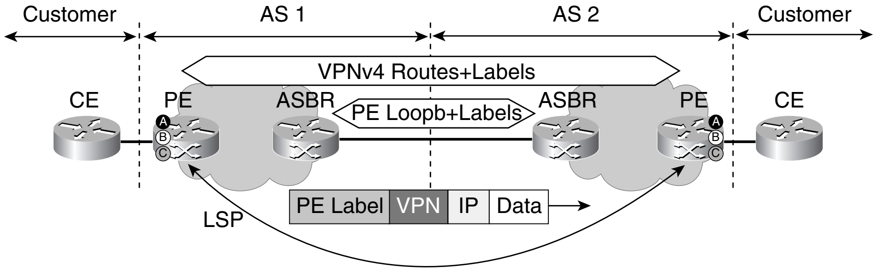
Model C: Multihop eBGP Redistribution of Labeled VPN-IPv4 Routes Between Source and Destination ASs, with eBGP Redistribution of Labeled IPv4 Routes from AS to Neighboring AS

Model C was introduced in RFC 2547bis to remove the requirement to hold VPN-specific information on the ASBR. In this model, the VPN-specific information is propagated between the ingress PE on AS 1 and the egress PE on AS 2 directly. To improve scalability further, it allows the usage of *route reflectors (RRs)*.[6]

How Model C Works

Figure 3-10 depicts model C without RRs. The PEs of both autonomous systems have visibility of each other through a multihop MP-BGP connection, and they exchange the VPN-specific information (VPN-IPv4 NLRIs, labels, and so on) end to end, using the loopback addresses of the PEs without involving the ASBRs. This means that the ASBRs do not need to hold VPN-specific information.

Figure 3-10 *Inter-AS Model C, Without Route Reflectors*

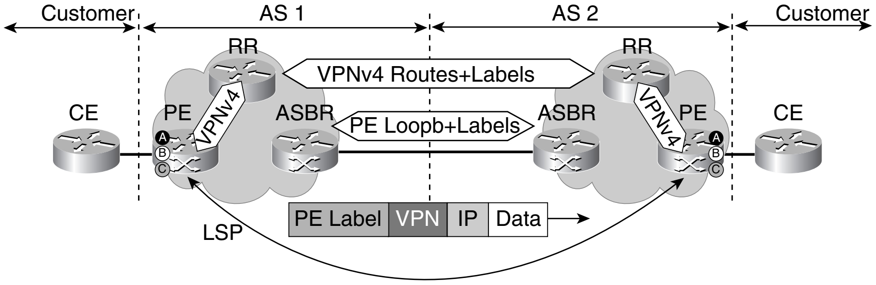


The ASBRs need only to exchange host routes (/32) to the PE routers involved in the VPN, with the labels needed to get there. In this way they facilitate the multihop BGP connection between the PE routers on both sides.

A Label Switch Path (LSP) is built from the ingress PE router in AS 1 to the egress PE in AS 2 (using loopback addresses). VPN traffic uses this LSP to reach the other AS. As far as the data plane is concerned, the ASBRs act as P routers, with no knowledge about the VPNs concerned. Also, between ASBRs the VPN traffic looks like traffic between P routers: each data packet is prepended with the VPN label and then with an egress-PE label.

Model C can be further scaled by using route reflectors in each AS. Figure 3-11 depicts this mode of operation. Because many networks require RRs internally, MPLS VPN model C also usually uses RRs.

Figure 3-11 *Inter-AS Model C, with Route Reflectors*



Here, the PEs in both autonomous systems maintain an MP-BGP peering only with the RRs in their own AS. The RRs in turn maintain an external MP-BGP peering. LSPs are established end to end from ingress PE to egress PE, as before.

Security of Model C

The security of this model is considerably more open than in models A and B.

On the control plane, model C has two interfaces between autonomous systems:

- The ASBRs exchange IPv4 routes with labels via eBGP. The purpose is to propagate the PE loopback addresses to the other AS so that LSPs can be established end to end. This route exchange and the whole BGP session can be controlled as in standard BGP. On this connection, no VPN information is passed on—only information relevant to the two ASs. Details on how to secure this connection are explained in Chapter 5, "Security Recommendations."
- The RRs exchange VPN-IPv4 routes with labels via multihop MP-eBGP. The prefixes exchanged can be controlled through route maps, equally the route targets. This makes it possible to ensure that only the required VPNs are exchanged, and within the VPNs, only specific prefixes.

On the data plane, the traffic exchanged between the ASBRs contains two labels:

- **VPN label**—Is set by the ingress PE to identify the VPN
- **PE label**—Specifies the LSP to the egress PE

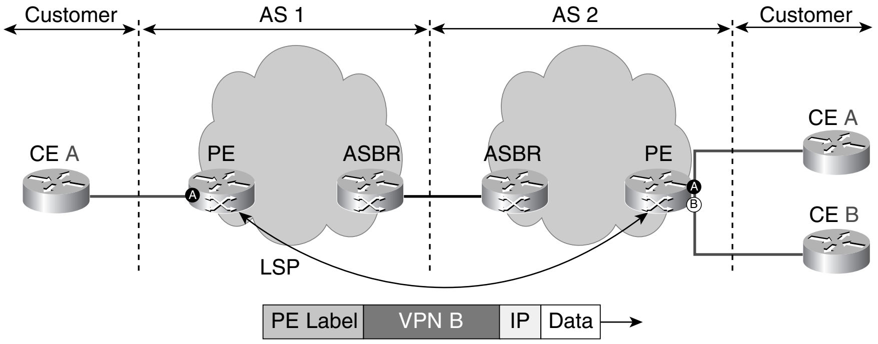
Model C is considerably more open in terms of security than the previous models, for the following reasons:

- To be able to establish end-to-end LSPs, the service provider must be able to reach all PEs of the other AS, which hold connections of shared VPNs. This can be a considerable number of PEs, exposing important parts of the normally internal infrastructure of an AS to the other AS. This also means that considerations that are usually local to an AS in terms of addressing need to be coordinated with the other AS. It also means that traffic can be sent to a number of internal addresses from the outside, making possible attacks from the outside. The recommendation is to filter IP packets into the core as tightly as possible to prevent these issues. Labeled packets cannot be filtered currently.

- The ASBR does not hold any VPN information. This is a scalability advantage, but at the same time it prevents the ASBR from checking the VPN label for its validity. This means that it is impossible to verify the VPN label in the data path. (In model B, the ASBR holds this information and can therefore validate the VPN label.) The egress PE cannot verify the packet anymore because at this point the origin of the packet can no longer be determined.

Considering these reasons, a potential attack could be AS 1 sending labeled traffic into AS 2, where the top label represents the label to a valid egress PE in AS 2. AS 1 holds PE labels for all those PEs in AS 2, on which it has shared VPNs. However, because the VPN label cannot be checked by the ASBR, AS 1 could send packets with random VPN labels into AS 2 without AS 2 having a way to block this. Figure 3-12 illustrates this vulnerability. AS 1 has an LSP to the egress PE in AS 2. This PE has two VPNs configured: VPN A, which is shared with AS 1, and VPN B, which is not shared with AS 1. By sending the packet shown in Figure 3-12 with a VPN label for VPN B, the packet will be forwarded into VPN B. At the time of writing this book there was no solution to this issue.

Figure 3-12 *Case C Security Issue*



But how dangerous is this issue? First of all, AS 1 would need to know the VPN label for VPN B. The MPLS VPN network does not expose the label externally, so there are two ways of getting it: by espionage, or simply by trying the entire label space. A label has 20 bits, yielding 2^{20} = 1,048,576 potential label values. Assuming a single packet attack with a 500-byte packet size, in the worst case an attacker would need to send 524 MB, which would take approximately 7 minutes on a 10 Mbps link, and 9 hours on a 128 k link. Note that in practice this number would be statistically smaller, and also, label numbering is not random, so intelligent guessing could reduce this number significantly.

Then, a malicious user in AS 1 could only send traffic into the VPN, but not receive a reply. However, there are a large number of examples in the history of security where a single unidirectional packet was enough to propagate a worm, for example. So while this limits the scope of an attack, it does not rule it out. In any case, the potential attacker would not receive feedback as to whether the attack was successful.

Therefore, it is not easy to carry out a sophisticated attack against a VPN from a given AS. But a single-packet unidirectional attack, as frequently used in the propagation of worms, is possible, even though statistically unlikely.

The consequence of this is that in model C the service providers must trust each other also in areas that are not shared. Therefore, model C is most commonly used today where a single operator uses several ASs on the backbone. In this case, implicit trust exists between the ASs because they have the same operational control.

As in model B, Layer 2 security between the ASBRs is extremely important. Therefore, here again is the recommendation from the previous section:

NOTE **Recommendation**

Never connect ASBRs over a shared Layer 2 infrastructure such as an *Internet Exchange Point (IXP)*. Use a private connection, or at least a private VLAN.

Since the various Inter-AS connectivity options are confusing and their differences often subtle, the next section puts all options in context for easy comparison.

Comparison of Inter-AS Security Considerations

Table 3-1 compares the three Inter-AS connectivity options in simple terms.

Table 3-1 *Properties of Inter-AS Models*

	Model A	**Model B**	**Model C**
Required protocols between ASBRs	None (although intra-VRF routing is typically used)	MP-eBGP	eBGP
Complexity	Simple	More complex	Very complex
Scalability	Not very scalable	More scalable: one ASBR interconnection only	Very scalable: ASBRs don't carry VPN information
Visibility of other AS	None	ASBR only	All PEs, which carry shared VPNs and route reflectors
VPN user must trust	All service providers	All service providers	All service providers
Service provider must trust	Nobody	Nobody	The other service provider

So which Inter-AS option is the right one for you? Here are some decision guidelines, from a security perspective:

- If the number of shared VPNs and prefixes is small, consider model A. ("Small" is a relative term, depending on your ASBR capabilities.) It is simple, most provisioning systems easily support it, and it is the most secure option because of its simplicity: the more complex a solution, the more risk for errors and security issues. Model A has almost nothing to configure and no global protocols running (only possibly inside the VRFs). In security, nothing can beat simplicity! If the number of VPNs and prefixes is too large for model A, consider one of the other models.
- If you are peering with another operator, that is, the other AS is not under your direct control and you cannot fully trust it, use model B. If you cannot fully trust the other side, you need to control the interface. Model B has a clear-cut interface, which is relatively easy to control. Model C is not recommended here.
- If you are a single operator controlling all involved ASs, feel free to use model C. In this case, all your ASs behave a bit like a single AS, where ingress and egress PEs are in direct contact. The boundaries between ASs are less clear, but if there is one operator for all ASs, this is controllable.

NOTE As a general security guideline, never use a new technology or protocol without a good reason. Adding complexity usually reduces security. So if in doubt, use the simpler model!

A number of risks exist in any environment and are independent of the Inter-AS model:

- Service provider 1 sends faked or crafted IP packets into any shared VPN on AS 2: this cannot be prevented. The VPN user must trust both service providers.
- Service provider 1 can bring a fake CE into any shared VPN, endangering the integrity of that VPN: this also cannot be prevented. Again, the service providers are trusted.
- A service provider can sniff traffic on any trunk, endangering the confidentiality of the VPN data. Here, too, the VPN user must trust the provider.

This appears to be quite an insecure model, but in fact the same risks exist in any VPN technology, although sometimes these trust issues are not clear. The service provider must always be trusted. The only solution if the service provider cannot be trusted is to provide additional security on top of MPLS, such as through IPsec. Chapter 6, "How IPsec Complements MPLS," describes this option.

Another model involving several providers is the Carrier's Carrier model. It allows a hierarchical structure, where a service provider resells a service from an MPLS provider. The next section covers this case.

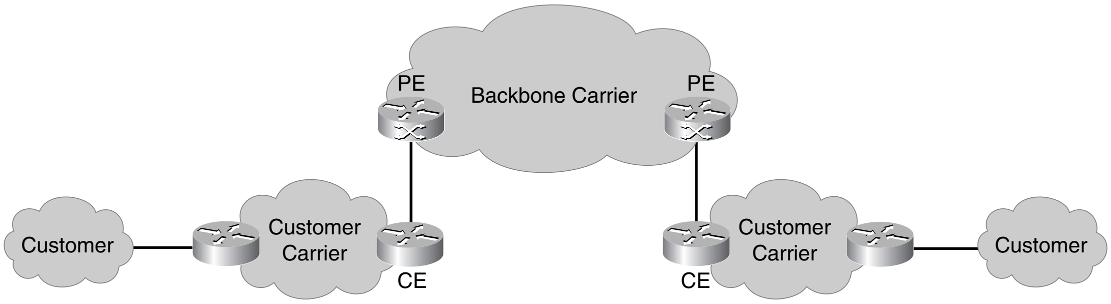
Specific Carrier's Carrier Considerations

The *Carrier's Carrier (CsC)* architecture is described in RFC 2547bis, and can best be described as hierarchical MPLS VPNs: CsC provides an MPLS VPN service that other carriers use to resell their services.

How CsC Works

Figure 3-13 shows how the CsC architecture looks. The first-level service provider is commonly called the *backbone carrier*; the second-level provider is called the *customer carrier*.

Figure 3-13 *CsC*



From a security point of view, the model is similar to standard RFC 2547 networks, with the exception that here on the interface between PE and CE, labeled packets instead of IP packets are exchanged. Although in the standard RFC 2547 network, all labeled packets can be discarded on ingress into the MPLS core, this model allows them.

There are two main cases for the application of CsC:

- The customer carrier is an Internet service provider (ISP).
- The customer carrier is an MPLS VPN provider.

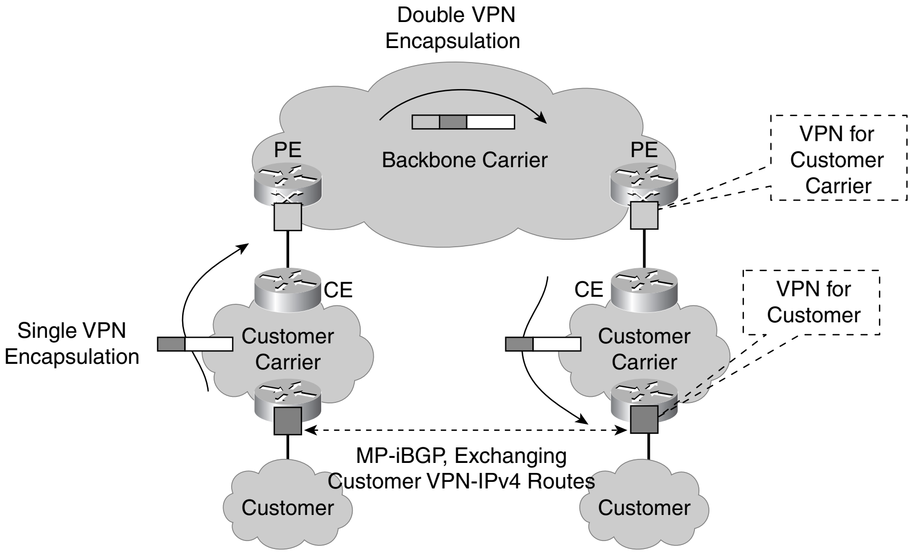
If the customer carrier is an ISP, Internet traffic will be sent across the entire ISP network (spanning several VPN sites). For this to work, each router on the path must know all Internet routes. This includes the ISP's routers, but also the backbone carrier's PEs. For the backbone carrier, this does not scale: the PE would need to keep the entire Internet routing table for each VRF.

The solution is to use LSPs over the backbone carrier's network, essentially tunneling the Internet traffic over the core. This way, the PEs only need to know the address of the LSP endpoints, instead of the entire Internet routing table. In this solution the PE passes prefixes with a label to the CE, so the CE must be able to receive prefixes with labels and must be able to send labeled packets.

If the customer carrier is an MPLS VPN provider, the requirement is to connect VPN users transparently on several sites of the customer carrier's network. This can also be done with standard RFC 2547 MPLS, but it would require the backbone carrier also to configure on the core a VRF per customer of the customer carrier: essentially the VPN user would have to be configured on both the customer carrier network as well as the backbone carrier network. In addition, this does not scale well.

The solution is to exchange only *Interior Gateway Protocol (IGP)* loopback addresses with labels over the backbone, such that the CE will impose a new label for the traffic between sites. This way, the PEs from the customer carrier run MP-iBGP (interior BGP) sessions directly, and the backbone never sees the VPN user information. Figure 3-14 shows this behavior.

Figure 3-14 *CsC: Hierarchical VPN*



The original IP packet from the customer is encapsulated with a VPN label on the customer carrier's network. For this purpose, the customer's carrier has a VPN configured for each customer. This is exactly as in normal RFC 2547. The backbone carrier again configures a VPN for each customer's carrier on the customer's PE, the effect of which is that packets are again encapsulated on the backbone carrier's network.

There are several ways to configure the CsC solution for each case, but they are not discussed here because they do not differ from a security point of view: for security considerations, the important point is that the CE-PE interface now allows labeled packets. Therefore, CsC—like Inter-AS—is an exception to the general rules discussed in previous sections.

Security of CsC

To examine the security of the CsC solution, we address again both the control plane and the data plane. The interface between customers and the customer's carrier is a standard RFC 2547 interface and follows the considerations of the previous sections. The new part in the CsC architecture is the connection between the backbone PE and the customer carrier CE.

On the control plane, this interface has two basic options:

- To configure an Interior Gateway Protocol (IGP) with LDP or TDP. The IGP distributes the routes, while the LDP/TDP distributes labels for those routes.
- To configure BGP with label distribution, which combines the two tasks in one protocol.

All of these protocols can be appropriately secured, and this is described in detail in Chapter 5. The key concept is to ensure that the control connection is made with a known peer. This can be done using the MD5 authentication, which is available for all these protocols.

Label distribution on this interface is controlled in all cases by the backbone carrier. RFC 2547bis states for the CsC case: "The PE must not distribute the same label to two different CEs" (with some exceptions) for the control plane. For the data plane, it specifies that "when the PE receives a labeled packet from a CE, it must verify that the top label is one that was distributed to that CE."

This means the backbone carrier issues the label uniquely and then, on the data plane, controls all packets so that they use only the label(s) issued to them. This makes spoofing from the customer carrier impossible.

Attacks against the backbone carrier can be carried out with the protocols in use (IGP plus LDP/TDP or BGP), so they must be secured against DoS attacks and against propagation of false information. The backbone cannot be attacked through the exchanged packets, however, because the packets sent from the CE to the PE are not interpreted. Only label swapping takes place, which, again, is controlled by the backbone carrier. RFC 2547bis states for this case that packets cannot break the VPN separation if "it is known that such packets will leave the backbone before the IP header or any labels lower in the stack will be inspected." This is the case on the backbone level.

In CsC Layer 2, as in the Inter-AS architecture, security is paramount for any critical interface. Therefore, we repeat this warning:

NOTE Never connect PEs and CEs over a shared Layer 2 infrastructure such as an Internet Exchange Point (IXP). Use a private connection, or at least a private VLAN.

The Carrier's Carrier architecture provides a secure way to operate multilevel VPNs, assuming correct implementation and operation. It is the backbone carrier that assigns and polices policy for the customer carrier, as the customer carrier does for its customers. On both levels the "customer" has no way to break the VPN separation of the level above. On both levels the lower level needs to trust the upper level to correctly implement and operate the network. For the end customer, this trust is transitive: the customer needs to trust the customer carrier, and implicitly also the backbone carrier.

Security Issues Not Addressed by the MPLS Architecture

In discussions about MPLS security, a number of questions typically arise that are outside the scope of the MPLS architecture. This means these issues have nothing to do with the standards and cannot, therefore, be controlled by the architecture. The following list describes these issues and explains why they are outside the scope of the architecture.

- **Protection against misconfiguration or operational mistakes**—The standards describe the architecture. This whole chapter examined MPLS VPNs based on this architecture. This architecture can also be misapplied, leading to security issues. Here's an example: As long as the PE is configured correctly according to the standard, the solution is secure. However, any operator could misconfigure a PE, breaking the security. This is not an architectural issue, but an operational issue. These problems are discussed in Chapter 8, "Secure Operation and Maintenance of an MPLS Core."
- **VPN data confidentiality, integrity, and origin authentication**—There is no guarantee to VPN users that packets do not get read or corrupted when in transit over the MPLS core. MPLS as such does not provide any of the above services. It is important to understand that a service provider has the technical possibility to sniff VPN data, and VPN users can either choose to trust the service provider(s) not to use their data inappropriately, or they can encrypt the traffic over the MPLS core, for example with IPsec, as described in Chapter 6, "How IPsec Complements MPLS."
- **Attacks from the Internet through an MPLS backbone**—If the MPLS backbone provides an Internet access to a VPN, attacks from the Internet into this VPN are

outside the scope of MPLS. The task of the MPLS core is to forward packets from the Internet to the VPN and vice versa. This includes potential attacks. It is, however, within the scope of MPLS security to make sure that an attack against a given VPN does not affect other VPNs or the core itself. (This is discussed in Chapter 4.) Also outside the scope of the MPLS architecture is any kind of firewalling required for such cases.

- **Customer network security**—Every attack that originates in a customer VPN and terminates in that same VPN is outside the scope of MPLS security. The MPLS VPN architecture forwards packets between VPN sites; it is not concerned with the nature of these packets, which could also be attack packets. This also includes IP spoofing within a VPN.

NOTE When discussing the security of MPLS VPN networks, take care to maintain a balanced view of the overall risks to a customer. For example, it is in relative terms close to irrelevant to argue about chances of an attacker sniffing a core line, if the customer network has unsecured wireless access points; it is also not important to worry about a service provider misconfiguring a PE, when attackers have uncontrolled physical access to hosts in an enterprise. Security is a question of balance: there is no point in putting extra secure locks on the door of your house if the windows are left open.

Comparison to ATM/FR Security

Many enterprises have been using VPN services based on ATM or Frame Relay (FR) in the past and are considering moving to MPLS VPNs. Unfortunately, the discussion about this topic has often been emotional and unbalanced.

New MPLS users are often concerned about the fact that an MPLS VPN service has a control plane on Layer 3. However, as shown in the previous sections, Layer 3 services can also be correctly secured and are fit to provide VPN services.

ATM/FR might be perceived as more secure because they are mostly not vulnerable to Layer 3 attacks (also ATM/FR switches typically have a Layer 3 control plane such as telnet). However, the security of Layer 2 in those technologies is typically assumed rather than actually proven. As we discuss in various parts of this book, Layer 2 has its own security issues that have to be considered. Many ATM/FR users are asking very hard questions about MPLS VPN security, while never having questioned whether a flood of signaling packets to an ATM switch might not affect that switch. It is good to discuss security of a technology, but it should be discussed in a balanced way.

This section discusses the features of both technologies and compares them.

VPN Separation

A VPN user requires his VPN to be separate from other VPNs and the core. In Layer 2 technologies, this is achieved implicitly by layering: the core exclusively uses Layer 2, so that the Layer 3 information of a VPN is separate. In MPLS VPNs, separation is achieved logically, by maintaining separate contexts on a provider router. Both ways are different, but both achieve the same result: each VPN can use the entire IP address space in their VPN, and it is impossible to send packets into other VPNs on the same core.

Misconfigurations are a problem in both technologies: an ATM circuit can be misconfigured, connecting a VPN router to a router from another company. Because many topologies are hub-and-spoke with default routing, this might lead to serious security breaches.

On the MPLS side, misconfigurations can equally break security. For example, a wrong route target on a PE router can bring a CE into a wrong VPN. You can argue about which misconfigurations are worse or more likely, but the fact is that if the core is misconfigured, VPN separation might be broken—in any VPN technology.

Robustness Against Attacks

VPN users demand a stable service, and most of all a service that cannot be attacked from the outside. For many VPN users, it would not be acceptable if a VPN service could be affected by a DoS attack from the outside. Even worse, an attacker gaining control of a network element could control any VPN. Therefore, any VPN technology must be resistant against attacks.

MPLS VPNs have been heavily scrutinized for the Layer 3 control plane and their frequent accessibility from the Internet. The issue was raised that given enough time, a good hacker would get access to a PE router over the Internet.

As shown previously in this chapter, an MPLS core has few and well-defined interface points to the outside. An MPLS core is not at all comparable to a traditional IP core, where every router was accessible (assuming the MPLS core has no global interfaces to the outside, only VRF interfaces). Rather, only single interfaces can be reached, and those can be very well secured. Therefore, it is very difficult to attack an MPLS network directly. An attack using transit traffic is the only possibility, and it might lead to a DoS condition. However, this can be controlled through appropriate dimensioning of the routers and architectural decisions, as is discussed in Chapter 4, in the section "Internet Access."

ATM or Frame Relay networks are also resistant against attack, assuming correct implementation. However, ATM switches and Frame Relay switches also have Layer 3 control planes (for example, telnet), and can be attacked if not appropriately secured. Frame Relay links depend on correct dimensioning of parameters such as Committed and Extended Information Rate (CIR/EIR). Misconfigurations of any of the above protocols or parameters can also result in a degradation or loss of service.

As long as both types of VPN technologies are configured correctly, they cannot be easily attacked.

Hiding the Core Infrastructure

In Layer 2 networks, the core is usually hidden because the VPN user works on Layer 3. Also, MPLS VPN cores are hidden to the VPN user, although using a different method: most addresses are hidden by architecture; the only visible part is the peering PE address. This address is, however, part of the VPN address space, so that in reality no core information is visible to the outside.

The fact that the PE router is reachable on this single interface is an exception to this rule. However, this usually is not a problem per se, but only in connection with attacks against the PE. As shown previously, this is very difficult if the PE is properly secured.

Impossibility of VPN Spoofing

As shown earlier in this chapter, it is impossible for an outsider to spoof another VPN, or the core, because a VPN user is always treated in his own context. Also, in ATM or Frame Relay, there are no known ways to spoof VPN signaling mechanisms such as the Virtual Path/Circuit Identifier (VPI/VCI) to spoof another VPN.

CE-CE Visibility

There is one area where ATM/Frame Relay point-to-point services do have an advantage over MPLS IP VPNs: Because the former are Layer 2 services, CEs can establish a direct Layer 3 adjacency and "see" the other CE. For example, the *Cisco Discovery Protocol (CDP)* can be used to find out basic properties of the peer router. This includes addressing of the Layer 3 link, so that a CE is able to verify to some extent the identity of the CE on the other end of the point-to-point link.

This is not possible in MPLS IP VPNs, and a given CE has no direct visibility of other CEs in his VPN. The reason for this is the connection model of MPLS IP VPNs: Although ATM and Frame Relay provide mostly point-to-point connections, where such a check is possible, MPLS IP VPNs provide connectivity from a CE to a "cloud." This avoids the overlay issue of having to establish a tunnel between all CEs (the so-called n^2 issue), but it has the disadvantage of losing the direct peering information.

This problem is not only theoretical. There is a real issue when a service provider accidentally or maliciously adds a CE to a wrong VPN by configuring wrong *route targets (RTs)*. The VPN to which this CE has been added has no easy means to find the bogus CE. It can only monitor traffic, control routing, and watch the used IP address space. This must be controlled by the service provider operationally. See Chapter 8, "Secure Operation and Maintenance of an MPLS Core," for more information on this important issue.

Other MPLS services, such as the *Pseudo Wire Emulation (PWE)*, also implement point-to-point services based on Layer 2, where direct CE-CE visibility is possible.

Comparison of VPN Security Technologies

Table 3-2 compares all the aspects of VPN security for the different VPN technologies.

Table 3-2 *Security Comparison Between MPLS and ATM/Frame Relay*

	MPLS	**ATM/Frame Relay**
VPN separation	Yes	Yes
Robustness against attacks	Yes	Yes
Hiding of the core infrastructure	Yes	Yes
Impossibility of VPN spoofing	Yes	Yes
CE-CE visibility	Not in MLPS IP VPNs Yes for MPLS pseudo wire emulation	Yes

Overall, at the time of writing this book, the industry had mostly accepted that both MPLS and ATM/Frame Relay can be operated securely. It was also common understanding that operational issues such as misconfigurations are an issue for any VPN technology.

Summary

In this chapter, we defined common requirements that VPN users have for a VPN service and examined MPLS IP VPNs against these requirements.

The result is that, based on the architecture described in RFC 2547bis, MPLS IP VPNs can be provided securely, meaning that:

- VPNs are separated (addressing and traffic).
- The core cannot be easily attacked.
- VPN spoofing is impossible.
- The core is invisible to the VPN user.

MPLS VPNs provide mostly equivalent security compared to traditional Layer 2 VPNs such as ATM and Frame Relay.

We have also examined Inter-AS and Carrier's Carrier architectures on their architectural security. While CsC networks are quite secure, care must be taken with Inter-AS scenarios when connecting different carriers: not all architectures provide the same level of security between providers.

There are also a number of issues that MPLS VPNs do not address. Among those are the internal security of a VPN, attacks from the Internet into a VPN, and VPN data confidentiality. These issues are independent of MPLS and have to be solved separately.

MPLS VPN networks are only secure when the network implementation is correct and when the network is operated correctly. How to control operations is discussed in Chapter 8, "Secure Operation and Maintenance of an MPLS Core." How to design and implement an MPLS core such that VPN services are secure is the subject of the next chapter.

Footnotes

[1] We will generally refer to IPv4 in this book; IPv6 is supported in the same way as IPv4, as a different address family.

[2] See RFC 2547bis.

[3] See draft-ietf-l3vpn-ipsec-2547 (work in progress).

[4] See draft-townsley-l2tpv3-mpls (work in progress).

[5] See draft-ietf-l3vpn-gre-ip-2547 (work in progress).

[6] For general considerations about route reflectors, consult *Cisco ISP Essentials*, ISBN 1-58705-041-2; *MPLS and VPN Architectures*, ISBN 1-58705-002-1.