

# Cisco Unified VPN Suite

## Summary

Virtual private networks (VPNs) continue to be a growing market and have proven to be a solid source of revenue for service providers. Their popularity with enterprises stems from the fact that VPNs allow organizations to share private information over the Internet. For a fraction of the cost of traditional approaches, organizations can confidently share sensitive internal information with remote offices, telecommuters, and business partners.

However, the challenging requirements for VPNs prevent service providers from expanding their addressable market and realizing its full potential, and prevent enterprises from enjoying the full benefit of these services. The crux of the problem is that enterprises with a range of VPN requirements need to work with a range of service providers, and service providers looking to satisfy a range of VPN requirements need to deploy with a range of VPN technologies from several different vendors.

Demand for VPN services based on traditional Layer 2 transports, such as Frame Relay and ATM, continues to grow. For many independent local exchange carrier (ILEC) and Post, Telephone, and Telegraph (PTT) service providers, Layer 2 VPN transports represent a significant portion of their revenue stream. However, these connections are costly, and enterprise customers want more cost-effective options. In response, ILECs and PTTs are building

lower-cost IP networks based on packet technology such as Multiprotocol Label Switching (MPLS), offering Layer 2 and Layer 3 VPN services.

An increasing number of inter-exchange carriers (IXCs) and Internet service providers (ISPs) offer IP-based Layer 3 VPN services. Demand for Layer 3 VPN is climbing because it allows enterprises to exploit the Internet and service providers' IP-based infrastructures for secure, any site-to-any site connectivity. Customers enjoy the cost-effectiveness and reach of IP-based VPNs, while service providers can take advantage of their Layer 3 infrastructure to offer additional IP-based services. IXCs and ISPs are now looking for ways to provide Layer 2 VPN services.

The historical disconnect between Layer 2 and IP-based Layer 3 VPN solutions has forced service providers to build, operate, and maintain separate infrastructures to accommodate various VPN access technologies—a costly proposition. For their part, enterprise customers have had to carefully plan their VPN strategies to account for access technologies available in given geographic areas and specific service provider offerings.

What the market needs is a unified VPN solution that empowers service providers to support a full range of access technologies and VPN service offerings without the burden of separate Layer 2 and Layer 3 infrastructures. Ideally, service providers want to exploit the cost and reach



efficiencies of IP and consolidate their VPN services onto a common, converged IP core network. With such a unified solution, service providers could offer customers whatever VPN option best meets their requirements, and gain the benefits and advantages of an IP-based infrastructure.

The Cisco Unified VPN Suite addresses these market requirements by enabling service providers to integrate their Layer 2 and Layer 3 VPN infrastructures and services. With the Cisco Unified VPN Suite, any access technology—Frame Relay, ATM, Ethernet, or a leased line—can operate over any packet-based core network, whether based on native IP or MPLS. By unifying multiple network layers and providing an integrated set of Cisco IOS<sup>®</sup> Software services and management tools over this infrastructure, the Cisco Unified VPN Suite enables service providers to reach a broader set of potential VPN customers and offer truly global VPNs.

For service providers as well as large enterprises that mirror service providers, the Cisco Unified VPN Suite addresses the crucial requirement for a VPN solution that can accommodate any access technology over a single, converged IP- or MPLS-based network.

#### The Rise of VPNs

The term “virtual private network” covers a range of technologies that allow customers to create logical, private networks over a shared or public infrastructure. VPNs emerged as a significant service with the advent of Frame Relay in the early 1990s. Rather than create private networks based on costly leased point-to-point connections, enterprises could now create the equivalent of a private network by taking advantage of a service provider’s shared infrastructure.

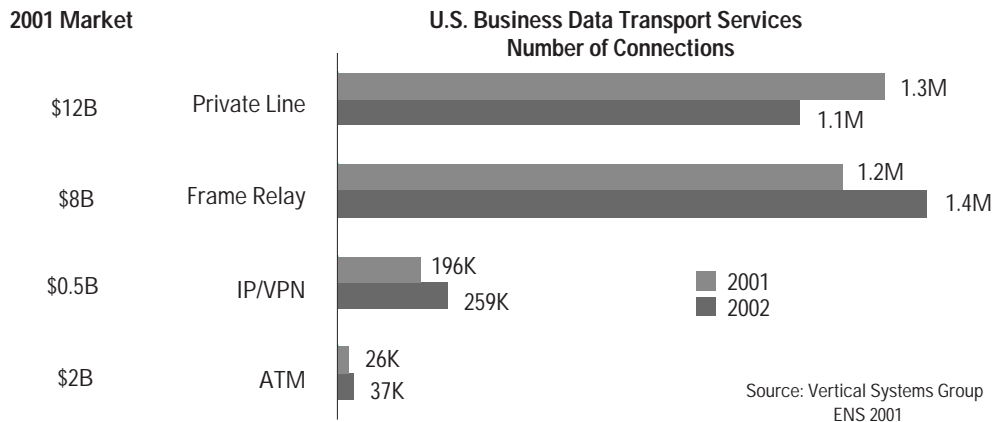
Beyond offering customers simple connectivity, service providers have been able to create Frame Relay-based Layer 2 VPN services through the use of permanent virtual circuits (PVCs). In configuring PVCs, network operators establish the data link connection identifiers (DLCIs) associated with different access devices, creating a tunnel for customer traffic to follow a predetermined path.

Frame Relay has proven attractive because it logically partitions traffic at Layer 2 and provides security equivalent to leased lines—but at a much lower cost. With its ability to support a variety of protocols, such as IP, Novell Internetwork Packet Exchange (IPX), and IBM Systems Network Architecture (SNA), Frame Relay became popular for LAN-to-LAN connections and is still widely used for intranet communications. According to the research firm Vertical Systems, Frame Relay was an \$8 billion market in 2001, with approximately 1.2 million customer connections, projected to grow to 1.4 million connections in 2002 (Figure 1).



Figure 1  
U.S. Access Connection Chart (Source: Vertical Systems Group)

### U.S. Access Connections



- IP comprises more than half of aggregate traffic on private line, frame relay, and ATM networks.
- Erosion of the low speed private line base continues, but growth speed (T1+) connections bolsters revenue.

More recently, service providers began offering ATM-based VPN services as a higher-speed alternative to Frame Relay. In addition, most network operators are using ATM for aggregating and scaling their Frame Relay traffic. Today, many service providers offer Layer 2-based VPNs built using Frame Relay, ATM, or combinations of Frame Relay and ATM.

Despite its benefits, Frame Relay does not lend itself to an open extranet model, so it is not a viable option for supply-chain or enterprise-to-partner communications. Likewise, Frame Relay is not a cost-effective solution for remote users and telecommuters, nor does it address customer need for high-speed data services. Consequently, many enterprises are turning to IP-based VPNs as a more flexible alternative for securely connecting remote sites and users, both internal and external, as well as looking to Ethernet-based metropolitan-area services for high-speed transparent LAN services (TLS).

Currently, the most commonly deployed IP-based VPN technologies are IP Security (IPsec) and MPLS Border Gateway Protocol (BGP)-based VPNs built around the Internet Engineering Task Force (IETF) RFC 2547 bis specification. These technologies can accommodate intranet, extranet, and Internet access applications, addressing an enterprise's need to securely interconnect its geographically dispersed sites, to share company information with trusted partners and suppliers, and to provide connectivity for remote users and telecommuters.

IP-based VPNs offer numerous advantages, and demand for them is growing significantly. IP-based VPNs enable enterprises to take advantage of the flexibility and ubiquity of the Internet and service providers' IP-based backbones for secure any site-to-any site communication. Importantly, IP-based VPNs allow enterprises to use a common transport line for both Internet access and site-to-site communication, a step toward simplifying wide-area communications.

The main drawbacks of IP-based VPNs are that they support IP only and require a Layer 3 infrastructure. Customers with enterprise protocols, such as SNA, continue to look to Layer 2 VPNs to carry this type of traffic. Likewise, some enterprises wish to maintain control over their routing, so they prefer Layer 2 VPNs.



Given the complexity of the current VPN landscape, service providers are wrestling with how best to accommodate legacy access technologies (for example, Frame Relay and ATM) along with new ones (for example, Ethernet today, wireless, and others in the future) while continuing their migration to scalable, cost-effective IP-based backbones.

#### Today's Complex VPN Landscape

Currently, providers that want to offer a full suite of VPN services must build the appropriate infrastructure to support a particular VPN solution, such as Frame Relay/ATM, IPsec, BGP-based, and so on. Because VPN solutions to date have been tied to specific transport technologies, both service providers and customers have had to wrestle with complexity and a lack of flexibility.

Providers must grapple with how to extend the reach and scale of their VPN offerings, while also reducing the time required for service delivery. Providers are unable to offer solutions that preserve their end-user customers' traffic end to end, complicating service management. Enterprises are burdened by the need to plan their VPN strategy around the access technologies they have in common with their prospective service provider(s) at various geographic locations and any suppliers and partners to whom they wish to connect.

For many network operators, the only solution has been to deploy parallel Layer 2 and Layer 3 networks. Needless to say, deploying and maintaining multiple core networks is expensive in terms of both capital outlays and operational overhead. Ideally, service providers would like to move to a single backbone technology. Many service providers are migrating to native IP- or MPLS-based backbones, driven by the lower capital and operational costs afforded by an IP infrastructure. Although IP and IP/MPLS backbones strongly position service providers to offer IP-based VPNs and other value-added IP-based services, to date they have not accommodated customers' Layer 2 services requirements.

As a result, many service providers continue to operate and manage parallel Layer 2 and Layer 3 networks. And those service providers, including IXCs and ISPs, that have built native IP or IP/MPLS core networks and lack a parallel Layer 2 infrastructure find that they are missing revenue opportunities because they cannot address the full range of customer VPN requirements. Similarly, ILECs, PTTs, and other providers that have built up strong Layer 2 access businesses would like to migrate to IP cores in a way that allows them to maintain their lucrative Layer 2 access revenue.

A few service providers have combined IP-based VPN and Frame Relay services in an attempt to offer customers the best of both worlds. Such services allow customers to use Frame Relay for intranets while also providing connectivity to remote users, suppliers, and trading partners across the Internet or shared IP-based networks. However, these solutions are proprietary and media dependent, and do not represent a broadly applicable, standards-based solution that addresses the requirement for a unified VPN architecture.

And although demand for Frame Relay remains strong today, other Layer 2 access technologies are emerging and will continue to emerge. Demand for Ethernet-based metropolitan-area networks is increasing, and wireless access services are expected in the not-too-distant future. Any comprehensive VPN solution must accommodate the range of current and future access technologies, and allow providers to realize the cost benefits of an IP core.



## The Requirement for a Unified VPN Suite

In today's economic climate, service providers are under pressure to reduce costs while increasing revenue. They must protect profitable revenue streams even as they expand into new markets. A key issue for service providers is how to take advantage of their investment in existing network technologies while moving forward to exploit the cost and operational benefits of an IP-based infrastructure.

In particular, service providers want to take advantage of their existing IP infrastructure and to continue their migration to cost-effective IP and IP/MPLS infrastructures without sacrificing revenue from Layer 2 VPN services. New providers that have built out IP or IP/MPLS infrastructures to support Layer 3-based VPN offerings and other IP-based services want to capture some of the revenue from lucrative Layer 2 services.

What service providers need is a VPN architecture that integrates Layer 2 and Layer 3 technologies over a single, converged, packet-based network. Such a unified architecture would enable service providers to accommodate any type of customer access technology over one network. And service providers need a solution that does not require a forklift upgrade or disruption of current network operations or services.

The ability to support Layer 2 and Layer 3 services over a common IP infrastructure would eliminate the need to maintain parallel communications infrastructures. Such an integrated architecture would result in significant cost savings and ease service provisioning and integration.

It would also enable providers to give customers a combination of Layer 2 and Layer 3 VPNs and related services they want, whether managed or unmanaged, customer premises based or provider based. Providers could increase revenue by offering multiple VPN types, expanding into markets they may not currently be addressing, and extending the geographic reach of their VPN coverage. Providers need a standards-based solution that interoperates with their current network infrastructure even as they migrate to an IP-based backbone. Finally, providers need a unified VPN suite that also lets them take advantage of their IP or IP/MPLS infrastructure to deliver additional value-added features and services.

For their part, enterprises want low-cost, secure, any-to-any connectivity. Enterprise customers want a cohesive VPN solution that addresses the connectivity needs of all internal users and also satisfies the need for Internet and extranet access. Customers want the flexibility to interconnect their geographically disparate sites without regard to access technology. Ideally, they want to use the VPN technology most appropriate to a given site, whether it is Frame Relay, IP-based dialup, or outsourced VPNs based on MPLS. And they want this flexibility to extend to VPNs used to connect to suppliers and customers, allowing for any-to-any connectivity regardless of the access technology that the supplier or customer is using.

In addition to any-to-any access without compromise, enterprise customers want providers to offer VPNs with service-level agreements (SLAs), regardless of the VPN technology used. Likewise, enterprise customers are looking to their providers for services, such as security and voice support, to be integrated with their VPNs.

Service providers and enterprise customers alike need a unified VPN architecture that enables support of a full range of VPN access technologies and services on a single, converged, IP-based infrastructure, thus allowing customers to use the VPN option that best meets their needs.



## Cisco Unified VPN Suite—Protocols

The Cisco Unified VPN Suite addresses both service provider and enterprise customer needs for an integrated VPN solution. It defines a single framework that unifies VPN access technologies over a common packet core, enabling providers to create end-to-end VPN solutions with global reach.

Following its tradition of being protocol agnostic, the Cisco Unified VPN Suite encompasses a suite of Layer 2 and Layer 3 VPN offerings that allow providers and their enterprise customers to choose the set of technologies that best meets their requirements and current operating environments. Specifically, the Cisco Unified VPN Suite consists of Layer 2 and Layer 3 VPN protocols, the platforms over which these software capabilities run, and provisioning tools such as those provided as part of the Cisco VPN Solution Center.

In terms of protocols, the Cisco Unified VPN Suite encompasses a suite of Layer 3 and Layer 2 protocols for tunneling and VPN creation. Layer 3 protocols supported include Generic Routing Encapsulation (GRE—RFC 1701) <http://www.ietf.org/rfc/rfc1701.txt?number=1701>, IPsec, and BGP <http://www.ietf.org/rfc/rfc2547.txt?number=2547>. Currently, the key Layer 2 protocols are Layer 2 Tunneling Protocol Version 3 (L2TPv3), which is optimized for native IP networks, and Any Transport over MPLS (AToM) for MPLS-based core networks (see the “AToM Overview” and “L2TPv3 Overview” sections).

## Cisco Unified VPN Suite—Platforms

The Cisco Unified VPN Suite is a fully integrated solution that operates across the broadest range of industry platforms. This extends from access platforms such as the Cisco 800 Series routers up through the carrier-class Internet backbone router—the Cisco 12000 Series Internet routers.

## Cisco Unified VPN Suite—Provisioning

Cisco Easy VPN, a software enhancement based on Cisco's Unified Client Framework, provides a consistent connection and policy and key management method across Cisco routers, security appliances, and VPN clients. This feature allows users to deploy any Cisco Easy VPN-enabled device within a common VPN framework. For remote connections, Cisco Easy VPN enables Cisco routers and security appliances to automatically establish and maintain a VPN tunnel to a Cisco Easy VPN-enabled headend device without complex remote configuration. For headend applications, Cisco Easy VPN accepts incoming calls from remote Cisco Easy VPN-enabled devices and verifies that those connections have up-to-date policies in place before the connection is established. In addition, Cisco IOS Software-based headends can now terminate VPN connections from Cisco VPN Software clients.

In addition, the Cisco Unified VPN Suite encompasses the CiscoWorks VPN/Security Management Solution, an enterprise management tool that allows for the provisioning of IPsec, monitoring, reporting, intrusion detection, and policy management.

Providers can provision and manage services across their integrated VPN infrastructure using the Cisco Virtual Private Network Solution Center (VPNSC) Version 3.0. A carrier-class service and network management system, Cisco VPNSC takes advantage of both Cisco products and partner solutions, such as WANDL, Concord NHM, and Visual Networks. VPNSC provides service activation, monitoring, reporting, intrusion detection, and policy management, ensuring that service providers have the tools they need to deploy a broad range of managed or unmanaged services over Frame Relay, ATM, Packet over SONET (POS), Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), and Ethernet networks.



## Unified VPN Suite

The Cisco Unified VPN Suite goes beyond simple services interworking to provide true unification across three key dimensions:

### Unified Layer 2 and Layer 3 Technologies

The Cisco Unified VPN Suite unifies Layer 2 access with Layer 3 backbones so that a VPN based on any access technology can be transported across an IP or MPLS backbone. The Cisco Unified VPN Suite can also extend the flexibility and reach of VPNs by allowing for the mapping or tunneling of one VPN type to another, simplifying the hand-off of VPN traffic across different underlying technologies and infrastructure types, as well as across service provider boundaries. The Cisco Unified VPN Suite enables service providers to offer truly global VPNs with a consistent set of services from end to end.

### Unified Delivery of IP Services

Delivered through the Cisco IOS Software, the Cisco Unified VPN Suite allows providers to offer customers a consistent set of services across their VPN products. Security, quality of service (QoS), NetFlow, SLAs (via Cisco Service Assurance Agent), MPLS traffic engineering, and so on are among the Cisco IOS services supported. Providers can use these capabilities to guarantee customer SLAs, to offer value-added services such as voice transport, and to build new revenue-generating services. For example, service providers can combine new MPLS-based Layer 2 VPN mechanisms with QoS and traffic engineering to support a virtual leased-line service that mimics existing Layer 2 services, such as Frame Relay and ATM, without compromising the scalability and flexibility of the networks on which they run.

## Cisco Unified VPN Suite—A Phased Strategy

Figure 2

	Phase I 1999–2001	Phase II 2002	Phase III 2003 and beyond ...
KEY FOCUS	Network build out	Unification of Access	Unification of advanced services into single VPN offerings
PROTOCOLS FOR:  Service Providers	Infrastructure investment Frame Relay, ATM, MPLS/IP Guaranteed Bandwidth Services	<b>Access:</b> • AToM for MPLS • L2TP version 3 for IP • IPsec to MPLS	GMPLS IPv6-capable VPNs Dynamic IPsec to MPLS Enhanced high availability for MPLS Enhanced accounting
Enterprise	IPsec remote access, IPsec peer to peer	• Easy VPN	Enhanced cryptography
PROVISIONING APPLICATIONS FOR:  Service Providers	VPN 2.0: MPLS & IPsec VPN	VPN 3.0: MPLS VPN, IPsec VPNs, L2TPv3 SLAs	VPN 4.0 Subscriber Management
Enterprise	CiscoWorks VPN/Security Management Solution	CiscoWorks VPN/Security Management Solution	CiscoWorks VPN/Security Management Solution



As a comprehensive VPN strategy, Cisco is delivering its Unified VPN Suite in phases. In Phase I (1999), Cisco focused on delivering a set of technologies and products that enable service providers to build out and converge on IP and MPLS core infrastructures. Along with these core networks, Cisco also began integrating complementary technologies such as broadband access and IPsec.

In 2002, Cisco is launching Phase II, which layers in Layer 2 access/VPN mechanisms. Phase II deliverables will be provided throughout 2002 and include support for Layer 2 transport across packet-based core networks and access independence, along with the management and control tools providers need to create an integrated Layer 2/Layer 3 VPN infrastructure.

In the third phase of its Unified VPN Suite (2003), Cisco will deliver its unified control plane and integrated signaling, and will enable integration of additional IP services across VPN types. Phase III will also provide support for additional new, emerging access types such as TLS.

#### Cisco Unified VPN Suite Phase I: IP/MPLS Buildout and Layer 3 VPN Offerings

In Phase I, Cisco began delivering the technologies and products that service providers need to build converged IP or MPLS core infrastructures. Service providers are at various stages of that migration, with some having completed it and others still in the process. An IP or MPLS backbone is the foundation upon which a unified VPN architecture can be built.

Along with IP and MPLS core technologies, Cisco in Phase I also delivered the first phase of its access integration with support for dial, broadband, and the first phase of its service integration with support for security. In addition, Cisco delivered a rich set of Layer 3 VPN technologies and solutions, and integrated key elements of these VPN offerings.

Cisco supports Layer 3 VPNs through protocols such as GRE, IPsec, and BGP. In particular, Cisco has worked to integrate its IPsec and MPLS-based VPN offerings to enable service providers to extend secure VPN services beyond the boundaries of their MPLS networks. This integration encompasses technology interworking as well as common management via the Cisco VPN Solution Center.

In general, IP-based VPNs operate by encapsulating customer traffic (data, voice, or video) into IP packets and tunneling those packets over the service provider's IP-based private backbone or across the Internet. Privacy is provided by tunneling or encrypting the customer traffic. In tunneling, a virtual point-to-point connection is established between a sender and receiver; these could be routers at two customer locations or ingress and egress routers on a service provider's network.

For additional security, customer traffic can be encrypted to prevent it from being read by unintended recipients. IPsec is one such encryption technology. Based on IETF standards, IPsec is a set of encryption and tunneling mechanisms designed to securely transport IP traffic across a public, IP-based network. As a security protocol, it provides for the confidentiality, integrity, and authenticity of data communications.

IPsec can be deployed in the last mile, between a customer's site and a service provider's point of presence (POP) (also known as the first mile to a provider's aggregation point), or across a provider's backbone for enterprise site-to-site VPNs. In addition, service providers can use IPsec as an overlay service operating transparently over an IP or MPLS network. Deployed in this way, providers can use IPsec to create a secure, end-to-end connection between customer sites, whether the endpoints are customer premises equipment (CPE) or an individual user's notebook computer.



Whereas end customers as well as service providers can deploy IPsec, BGP-based VPNs are generally implemented by service providers as a managed service. With BGP-based VPNs, MPLS is typically used in conjunction with it to maintain logical separation of customer traffic by encapsulating the traffic in MPLS tunnels known as label switched paths (LSPs). RFC 2547 defines a BGP VPN solution whereby MPLS is used to forward customer traffic using per-customer labels, known as route descriptors. BGP is used for distributing route information across a provider's backbone. With this model, service providers participate in and manage customer routing.

MPLS is a flexible transport in that it can operate over IP, ATM, Frame Relay, and other infrastructures. BGP-based VPNs are particularly attractive to service providers that have implemented MPLS for their traffic engineering, guaranteed bandwidth/QoS, and other features. Providers can take advantage of these capabilities to offer VPNs with strict SLAs, as well as other value-added IP-based services. In addition, the scalability of MPLS allows it to support tens of thousands of VPN groups over the same network, and very large individual VPNs.

Through its integration of IPsec and MPLS, Cisco allows IPsec sessions to be mapped directly into an MPLS VPN. This scenario enables network operators to provide encryption for their MPLS-based VPN service as well as to extend secure VPN service beyond the boundaries of their MPLS network. That is, secure traffic can flow through any number of other service provider networks to reach the customer's branch offices or remote sites anywhere.

The integration of IPsec and BGP VPNs enables service providers to address a broad potential customer base and offer a range of Layer 3 VPN options that meet customer requirements for scalability, security, QoS, manageability, and reliability.

#### Cisco Unified VPN Suite Phase II: Access Independence and Integrated Provisioning

In Phase II of its Unified VPN Suite, Cisco is integrating Layer 2 VPN technologies into its overall VPN solution, enabling service providers to converge their Layer 2 and Layer 3 services on an IP- or MPLS-based infrastructure and support any access over one network. With the Cisco IOS technologies and management tools that Cisco is delivering in Phase II, service providers can take advantage of their investment in IP or MPLS infrastructures to tap into the lucrative Layer 2 access market and position themselves to enter emerging markets with new services, such as TLS and virtual leased lines (VLL).

As part of its Phase II technology rollout, Cisco is introducing two new Layer 2 tunneling technologies: L2TPv3, which is optimized for native IP networks, and AToM for MPLS-based core networks. In addition, Cisco also will be offering unified management via its Cisco VPN Solution Center. As noted earlier, the Cisco VPNSC Version 3.0 will allow service providers to provision and manage services across their unified VPN infrastructure, and will include auditing, accounting, and other functions necessary for services deployment.

L2TPv3 and AToM are IETF standard-track protocols that can be used to encapsulate and tunnel a variety of Layer 2 protocols—including Frame Relay, ATM, Ethernet, HDLC, Synchronous Optical Network (SONET), and PPP—over either IP or MPLS infrastructures. Likewise, Layer 2 VPNs give service providers the flexibility to transport non-IP protocols, such as IPX, SNA, and so on.

An important characteristic of these Layer 2 mechanisms is that they support frame transport rather than frame termination. That is, a customer's traffic is encapsulated and carried end to end across a provider's network, not terminated at the ingress POP. For example, the DLCI assigned to a Frame Relay customer's connection is preserved from ingress to egress across a provider's network. This benefits service providers by making it easier to identify specific customer traffic for management, billing, or other purposes.



Cisco is initially supporting like-to-like connectivity with its Layer 2 tunneling; that is, a single access type, such as Frame Relay, must be supported as the access technology at both the provider network ingress and egress. In future implementations, Cisco will support any-to-any connectivity—allowing disparate access technologies to be used at the ingress and egress. This capability will allow for truly unified VPNs at Layer 2, whereby customers can have any combination of access technologies, such as a Frame Relay site interconnected to sites with ATM and Ethernet, or even to dialup sites, in a single VPN.

L2TP and AToM extend the usability of IP and MPLS networks, respectively, by enabling them to support both Layer 2 and Layer 3 services. Service providers can deploy them in conjunction with Layer 3-based VPNs to offer customers the mix of VPN solutions they may require. For example, network operators have the option to take in IPsec customer traffic and encapsulate it using AToM or L2TPv3 for transport across their backbones. Alternately, providers can offer customers IPsec as a service overlay to their Layer 2-based VPNs.

In addition, Cisco's Layer 2 VPN offerings can be deployed as either CPE-based or provider edge-based solutions, giving providers and enterprises tremendous flexibility. For example, providers can add new sites and customer edge-to-customer edge circuits without having to provision every provider edge on the backbone, and without having to interrupt network service to expand preprovisioned provider edges. With L2TPv3 and AToM, only the provider edges on which the service is offered need to be configured. Service providers can literally bring up a service simply by deploying devices with the tunnel endpoints preconfigured.

These Layer 2 VPN solutions are highly scalable because the provider-edge routers store the forwarding information of only the VPNs to which they connect. Core routers do not store any Layer 2-specific VPN information, so the number of VPNs it services does not affect the service provider core network. Likewise, these Layer 2 VPN options do not require the provider to use any IP addresses, saving on valuable public IP addresses.

In addition, a service provider can upgrade its network to support these Layer 2 VPN technologies without significant disruption of service to the customer. Because L2TPv3 and AToM are transparent to the customers, it appears to customers that they are using a traditional Layer 2 backbone.

### **L2TPv3 Overview**

Layer 2 Tunneling Protocol Version3 (L2TPv3) is emerging as a core tunneling and VPN technology. L2TPv3 is an update to RFC 2661 (L2TPv2), which originally defined a method of tunneling Layer 2 frames across packet-switched data networks. L2TPv3 updates L2TPv2 to support a broader set of Layer 2 encapsulations. Version 3 also specifies a reliable “control connection” for establishment, teardown, and maintenance of individual sessions and for the control connection itself. This setup allows for application of advanced provisioning techniques.

Cisco has been a major contributor to the development of L2TPv3, taking advantage of its earlier work in defining the universal transport interface (UTI). UTI is a prestandard Cisco innovation that specifies a high-speed tunneling encapsulation header for transportation of Layer 2 frames.

L2TP allows a pair of routers connected via an IP network to provide high-speed transparent Layer 2 connectivity between a pair of interfaces. All Layer 2 traffic between two customer network sites is encapsulated in IP packets and sent across an IP network; the routers in the network core treat the traffic as any other IP packet.



Cisco supports numerous L2TP encapsulations, including Ethernet, 802.1Q virtual LANs (VLANs), Frame Relay with subinterface support, and Cisco HDLC. Cisco's implementation also includes raw mode support, which allows tunneling of any type of information that arrives over a given physical interface. Currently, Cisco supports serial, POS, and Ethernet interfaces in raw mode. Service providers can use raw mode to support VLLs, which enterprises often use to connect remote sites together over a clear-channel service.

L2TP-based VPNs provide the flexible connectivity and scalability of IP with the privacy of Frame Relay and ATM, allowing new and extended network services to be delivered over routed IP networks. For example, in the near future L2TP will support TLS connectivity in the emerging metropolitan (metro) Ethernet environment. Likewise, network operators can use L2TP to support traditional Frame Relay, ATM, and leased-line services over their IP infrastructure. If a customer needs only Layer 2 connectivity, the service provider does not need to get involved in enterprise routing policies and security complexities, potentially reducing its operational overhead.

Through its integration of Layer 2 and Layer 3 VPN services, Cisco supports the use of L2TP in conjunction with other protocols, such as IPsec and MPLS. For example, IPsec can be transported as a payload over L2TP. Likewise, providers can use L2TPv3 to interconnect MPLS islands or for IP transit services, eliminating the need to run BGP peering.

### **AToM Overview**

Any Transport over MPLS (AToM) refers to Cisco's implementation of technology defined in the IETF draft "Architecture for Layer 2 VPNs." In essence, AToM does for MPLS-based networks what L2TP does for IP infrastructures. That is, AToM allows for the encapsulation and tunneling of Layer 2 packets across an MPLS network and supports many of the same types of services. For example, IPsec can be transported as a payload over AToM, and AToM can be used to support traditional Frame Relay, ATM, and leased-line services as well as TLS in the metro Ethernet environment.

AToM works by encapsulating customer Layer 2 traffic within MPLS frames and forwarding the frames across an MPLS backbone using LSPs for tunneling. Through the use of MPLS label stacking, a single LSP can carry many emulated virtual circuits, resulting in better scalability than is currently possible with native Frame Relay or ATM services.

Cisco AToM implementation supports encapsulations for Frame Relay, Ethernet, ATM (ATM adaptation layer 5 [AAL5]), PPP, and HDLC. As with L2TP, AToM introduces the opportunity for service providers to offer new services, including VLLs, Ethernet metro connectivity, and Layer 2 aggregation. AToM will be enhanced to allow VPNs to traverse an MPLS cloud to connect Ethernet networks with POS and ATM networks operating in cell mode, and to support TLS.

Importantly, AToM lets service providers extend the benefits of MPLS, including traffic engineering and guaranteed bandwidth/QoS, to Layer 2 service offerings. For example, providers can offer Layer 2 connectivity to Frame Relay and ATM customers and deliver the same service levels supported in legacy Frame Relay and ATM networks.

### **Cisco Unified VPN Suite Phase III: Unified Control Plane and Services Integration**

In Phase III of the delivery of the Cisco Unified VPN Suite, Cisco will deliver a unified control plane and integrated signaling along with further IP services integration. As noted earlier, a unified control plane will provide the consistency of control and topology needed to scale VPN deployments. This unified control plane will support Cisco's Layer 3 tunneling mechanisms, providing for advanced functionality such as endpoint discovery, and policies.



Through the integration of Cisco IOS services, such as QoS, security, and Cisco's Service Assurance Agent, into the Cisco Unified VPN Suite, service providers will be able to deliver a consistent set of services to their customers across an integrated VPN network.

Table 1 Cisco Unified VPN Suite Road Map

L2TPv3	AToM	Platforms	Features
12.0(22)S		Cisco 7200, 7500, 10720, and 12000	Keepalive
12.0(22)S		Cisco 7200, 7500, 10720, and 12000	MTU <sup>1</sup> discovery
Shipping now	12.0(23)S 12.1(9)E	Cisco 7200, 7500, 10720, 12000, and 7600	Point-to-Point Ethernet
Shipping now	12.0(23)S	Cisco 7200, 7500, and 12000	Frame Relay
12.0(23)S	12.0(23)S	Cisco 7200, 7500, and 12000	PPP
Shipping now	12.0(23)S	Cisco 7200, 7500, and 12000	POS
Shipping now	12.0(23)S	Cisco 7200, 7500, and 12000	HDLC
12.0(24)S	12.0(23)S	Cisco 7200, 7500, and 12000	ATM-AAL5
Future	Future		Any to any
Future	Future		TLS
Future	Future		ATM-cell relay

1. Maximum transmission unit

Over the course of 2002 and 2003, Cisco will roll out key elements of its Unified VPN Suite. As noted earlier, the first phase of L2TPv3 and AToM development in Cisco IOS Software supports like-to-like connectivity. This requires the same transport type, such as Frame Relay, at each end of the network. In late 2002, L2TP and AToM will be enhanced with interworking functions that allow providers to connect disparate transport types at each end, such as Frame Relay at one end to Ethernet VLANs at the other.

In terms of L2TPv3 deliverables, Cisco is currently shipping L2TPv3 support in Cisco IOS 12.0(21)S on the Cisco IOS 7200, 7500, 10720, and 12000 platforms. Supported Layer 2 encapsulations include: Frame Relay support on a per-port and per-DLCI basis, Ethernet on a per-port and per-VLAN basis, and raw-mode support for serial, POS, and Ethernet interfaces.

Also in early 2002, Cisco will deliver integration of L2TP with IPsec and MPLS. In mid-2002 Cisco will support L2TP provisioning with VPNSC 3.0 and expand its L2TP support in the 12.0(23)S release of Cisco IOS Software to include an enhanced control plane with support for dynamic discovery of the maximum MTU size, sequencing support to ensure that tunneled ATM and Frame Relay packets are delivered in the proper sequence, and keepalive support, which provides an active method to determine if a tunnel has gone down.

At the same time, Cisco will deliver a unified command-line interface (CLI) for both L2TP and AToM, which will ease management, as well as QoS support for Frame Relay and IEEE802.1p. With this support, the QoS values carried by customer Frame Relay and Ethernet traffic can be mapped to the IP delivery header, ensuring that these QoS values are consistent and accommodated by the L2TP tunnel.

In late 2002, L2TPv3 support in Cisco IOS Software Release 12.0(24)S will include the following:

- Unified control plane
- Layer 2 access interworking
- Transparent LAN services

Also in late 2002, ATM (both AAL5 and cell relay) support for L2TPv3 will be provided. ATM support is part of Phase III.

Cisco will begin rolling out AToM support in Q1 '02, initially delivering encapsulations for Frame Relay, HDLC, and Ethernet in Cisco IOS Software Release 12.0ST. In Q3 '02, Cisco will deliver AToM cell relay encapsulation as well as voice support and integration with BGP MPLS based VPNs. Also in Q3 '02, Cisco will provide provisioning and management support and a generic control plane.

Ethernet over MPLS is supported on Cisco IOS Software Release 12.1(9)E for the Cisco 7600 Series routers and 12.0(22)S for the Cisco 7200, 7500, and 12000 platforms. Ethernet, Frame Relay, PPP, and HDLC support is also available in Cisco IOS 12.0(22)S. ATM over MPLS is supported on Cisco IOS Software Release 12.0(23)S for the Cisco 12000 Series Internet routers. And ATM cell relay over MPLS is scheduled for Q3 CY'02 on the Cisco 7200, 7500, and 12000 platforms.

As part of Phase II, additional Frame Relay, HDLC, Ethernet, and PPP support will be available for the Cisco 2600, 3600, 7600, and 10000 during Q3 CY'02. Phase III will offer any-to-any MPLS in Q4 CY'02 for the Cisco 3600, 7200, 7400, 7500, 7600, 10000, and 12000 platforms.

### Conclusion—An Integrated VPN Solution

Addressing the complexity of today's VPN landscape, the Cisco Unified VPN Suite enables service providers and large enterprises to take advantage of their investment in an IP- or MPLS-based infrastructure to support both Layer 2 and Layer 3 VPN services. By delivering any access-over-one network flexibility, the Cisco Unified VPN Suite allows providers to reduce the total cost of ownership of their core and expand their addressable market without affecting existing revenue-generating services or compromising their ability to roll out new services.

In addition to expanding service providers' market reach, Cisco's VPN architecture accelerates services delivery. By deploying the Cisco Unified VPN Suite, service providers have the tools they need to remain technologically ahead, enabling them to address the most lucrative opportunities in the changing VPN market.



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco Powered Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Net Readiness Scorecard, Networking Academy, and ScriptShare are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, LightStream, MGX, MICA, the Networkers logo, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0303R) 201777/ETMG\_04/03