

Cisco Unified VPN Suite

Introduction

Virtual Private Networking (VPN) technology creates “private networks” over a public infrastructure. VPNs use protocol-specific encapsulations to separate user data on a shared network infrastructure, including the service provider (SP) networks, to form a “tunnel” between endpoints. Such endpoints can exist between an enterprise headquarters and a branch site, between disparate core networks in a service provider network, or extending network infrastructure globally.

The most common types of Layer 2 (L2) access are Leased Lines, Frame Relay, and Asynchronous Transfer Mode (ATM), while Ethernet, wireless and broadband continue to become more widespread.

Service providers with IP or MPLS cores can either terminate the access VPN or transport them transparently. Termination of the access VPN can limit the customers’ ability to manage the network internally, while transporting the access VPN incorrectly makes the network appear to be a virtual pipe or tunnel. Transporting access VPN over an IP or MPLS core requires new L2 tunneling mechanisms, which are part of the overall Cisco Unified VPNSuite.

Cisco Unified VPN Suite addresses the needs of differing packet-based service provider infrastructures with two distinct, new L2 tunneling protocols: Any Transport over MPLS (AToM) for MPLS-based core networks, and Layer 2 Tunneling Protocol

version 3 (L2TPv3) for “Native IP”-based core networks. Both protocols provide high-speed any site to-any site Layer 2 connectivity, and support Layer 2 attachment technologies (i.e.: Frame Relay, Ethernet, HDLC and ATM).

Cisco Unified VPN Suite also includes Layer 3 or IP VPN technologies such as IPsec, GRE, and MPLS/BGP VPNs. These technologies support the transport of IP packets as part of a VPN over IP/MPLS core. These L3 VPN techniques operate at the IP layer, providing an intelligent control plane to manage customer traffic and complex routing.

Benefits of Cisco Unified VPN Suite

- One network, any access
- Complete set of protocols, platforms, and provisioning capabilities
- Reduced cost of ownership
- Flexibility, scale, and services required by service providers and large enterprises

Feature Compatibility

Cisco Unified VPNSuite is available using IP /MPLS core networks, allowing various other value-add Cisco IOS features to be leveraged. Related Cisco IOS Software features include Multicast, Netflow, and MPLS-based Traffic Engineering or IP-based Quality of Service.



Scalability

Cisco Unified VPN Suite can add new sites and Customer Edge (CE) to Customer Edge circuits without provisioning every Provider Edge (PE) on the backbone, or interrupting network service to expand pre-provisioned PEs.

With Cisco Unified VPN Suite, only the PEs on which the service is offered require configuration. The MPLS or IP-based core can remain transparent. The only routers that need to be configured are those edge PE routers that the VPN transverses. Signaling will process the remaining data.

Simplification

Core routers must store a minimal amount of forwarding information, because Cisco Unified VPN Suite eliminates the need for core routers to store VPN information.

Cisco Unified VPN Suite integrates with existing networks, which simplifies migration. Below, find descriptions of the two tunneling mechanisms that provide transport capabilities for access services over MPLS or IP.

AToM

AToM provides Layer 2 access across an MPLS-enabled core network, extending the benefits of an MPLS-based core. Similar to its Native IP counterpart, L2TPv3, AToM enables service providers to offer scalable connectivity and to support existing services, while gaining the benefits of a consolidated core and enhancing network scalability. Service providers can combine the benefits of AToM and MPLS Traffic Engineering to differentiate application data and maintain the service levels that are supported in legacy ATM and Frame Relay networks.

L2TPv3

L2TPv3 provides service providers that run Native IP core networks with the ability to offer high-speed, Layer 2 tunneling capabilities. This allows service providers to further consolidate multiple networks that support differing services (i.e., Frame Relay or ATM) into a common IP infrastructure.

Further benefits include connecting MPLS islands, or allowing Transparent LAN Service (TLS) connectivity in the emerging Metro Ethernet environment.

MPLS VPN

Multiprotocol Label Switching Protocol Virtual Private Network (MPLS VPN) VPN is an application of the MPLS with IP VPN routing/forwarding that enables service providers to deliver advanced VPN transport services over existing network infrastructure. It relies on MPLS to extend the reach of VPNs over multiple network architectures (i.e., IP, ATM, Frame Relay, and hybrid networks).

MPLS VPN uses an efficient encapsulation method to enable VPN in a service provider network (public or private). It assumes minimum complexity, and requires little or no IP routing expertise from the CE users. The CE router usually needs minimal IP configuration or routing information to bring new sites into a VPN, and it does not have to maintain a point-to-point circuit in full-mesh connectivity. The service provider has the only provisioning and management tool necessary to run the network.



MPLS VPN enables VPN service providers to support large-scale VPN services (up to millions of VPNs per service provider). It also allows them to support a diverse population of customers, where some VPNs would consist of just a few sites, while others would have thousands of sites per VPN. This scenario enables connectivity to a large number of sites for enterprises, Inter-provider VPNs, and carrier of carriers.

IPsec VPN

Cisco IOS Software IPsec VPN deployments can be divided into four categories, based on the deployment scenario and the protocols: (1) site-to-site, (2) hub-and-spoke, (3) full mesh with TED, and (4) client/server. IPsec VPN is commonly used in enterprise networks.

GRE

Generic Routing Encapsulation (GRE) tunnels provide a designated pathway across the shared Wide Area Network (WAN) and encapsulate traffic with new packet headers, which ensures delivery to specific destinations. The network is private because traffic can enter a tunnel only at an endpoint. Tunnels do not provide true confidentiality (as does encryption), but can carry encrypted traffic. IPsec can be used to encrypt data before it enters and after it leaves the GRE tunnel.

Summary

Cisco Unified VPN Suite is the next step in WAN, Metro-Ethernet, and IP VPN technologies, and will address issues facing both service provider and enterprise customers. It provides one network with any access.

Cisco continues to be the leader in providing L2 and L3 VPN technologies to meet networking and security needs, through its complete set of protocols, platforms, and provisioning capabilities.

Industry Standard Support

L2TPv3 implements the “*Layer Two Tunneling Protocol ‘L2TP’*” Internet Draft from IETF,
<http://www.ietf.org/internet-drafts/draft-ietf-l2tpext-l2tp-base-01.txt>

AToM implements the following Internet Drafts from IETF:

“*Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks,*”
<http://www.ietf.org/internet-drafts/draft-martini-l2circuit-encap-mpls-04.txt>

“*Transport of Layer 2 Frames Over MPLS,*”
<http://www.ietf.org/internet-drafts/draft-martini-l2circuit-trans-mpls-08.txt>

MPLS VPN

Cisco IOS Software implements MPLS VPN as defined in IETF RFC 2547bis.

IPsec VPN

IPSec is documented in a series of Internet Drafts available at <http://www.ietf.org/html.charters/ipsec-charter.html>.

The overall IPsec implementation is per the latest version of the Security Architecture for the Internet Protocol Internet Draft (RFC2401). Cisco IOS IPsec implements RFC 2402 (*IP Authentication Header*) though RFC 2410 (*The NULL Encryption Algorithm and Its Use With IPsec*).

GRE

Cisco IOS Software implements GRE as defined in RFC 1701.

Cisco IOS Software Release and Platform Support Information

Unified VPN Suite provides the widest selection of VPN technologies on the widest range of routers and switches available from a single vendor through Cisco IOS Software.

L2TPv3

Release 12.0(18)ST supports L2TPv3 tunneling at the port level, like-interfaces on each end of the tunnel, on the Cisco 12000, Cisco 7500, and Cisco 7200 Series Routers.

Release 12.0(19)ST supports L2TPv3 tunneling for Frame Relay point-to-point subinterfaces with each Frame Relay Private Virtual Circuit mapped to a unique tunnel on the Cisco 12000, Cisco 7500 and Cisco 7200 Series Routers.

Release 12.0(21)ST supports 802.1q VLAN, L2TPv3 tunneling for 802.1Q point-to-point subinterfaces on Cisco 12000, Cisco 7500 and Cisco 7200 Series Routers.

Release 12.0(19)SP supports L2TPv3 tunneling at the port level for like interfaces on each end of the tunnel and L2TPv3 tunneling for 802.1q for point-to-point subinterfaces on Cisco 10720 Series Routers.

AToM

Release 12.1(9)E supports Ethernet over MPLS is supported on Cisco 7600 Series Routers. The Cisco 7200, 7500, and 12000 Series Routers are planned for support with Release 12.0(21)ST.

Release 12.0(11)ST supports ATM over MPLS on Cisco 12000 Series Internet Routers.

Future releases of 12.0ST will support Frame Relay over MPLS, ATM Cell Relay over MPLS, and PPP over MPLS.

MPLS VPN

Release 12.2 supports MPLS VPN features on Cisco 3600, 4500, 7200, and 7500 Series Routers.

Release 12.0(10)T supports MPLS VPN on Cisco 12000 Series Internet Routers

IPsec VPN

Release 12.x and 12.1E support IPsec VPN.

GRE

Early releases of Cisco IOS Software supported GRE, and significant enhancements were implemented in Release 12.0.

For More Information

For more information, please email unified-vpns@cisco.com. Or contact your Cisco account manager or global service manager.



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 Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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: 65 317 7777
Fax: 65 317 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**

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 © 1992–2002 Cisco Systems, Inc. All rights reserved. CCIP, the Cisco *Powered Network* mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, 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, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, 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. (0201R) 201777/ETMG 02/02