Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications

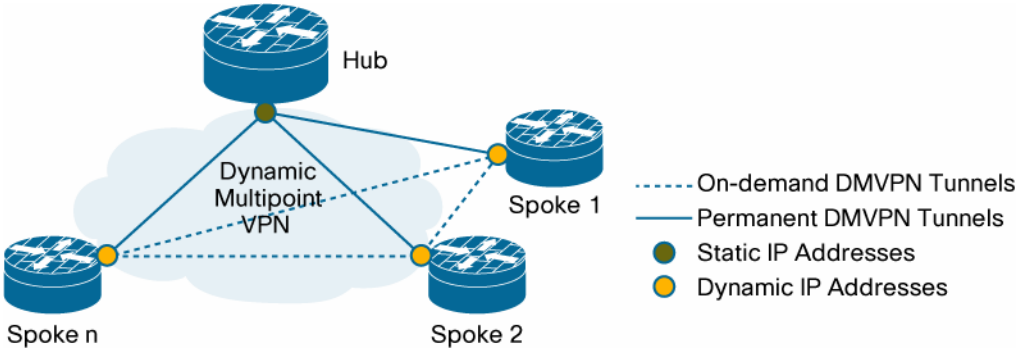
Product Overview

Cisco® Dynamic Multipoint VPN (DMVPN) is a Cisco IOS® Software-based security solution for building scalable enterprise VPNs that support distributed applications such as voice and video (Figure 1).

Cisco DMVPN is widely used to combine enterprise branch, teleworker, and extranet connectivity. Major benefits include:

- On-demand full mesh connectivity with simple hub-and-spoke configuration
- Automatic IP Security (IPsec) triggering for building an IPsec tunnel
- "Zero-touch" deployment for adding remote sites
- Reduced latency and bandwidth savings

Figure 1. Cisco Dynamic Multipoint VPN



Cisco DMVPN can be deployed in conjunction with Cisco IOS Firewall and Cisco IOS IPS, as well as quality of service (QoS), IP Multicast, split tunneling, and routing-based failover mechanisms. Large-scale, highly available Cisco DMVPN deployments are made possible by load balancing multiple Cisco DMVPN hubs.

Applications

Cisco DMVPN is the preferred solution for organizations requiring encrypted WAN connectivity between remote sites. Factors include the cost-driven use of the Internet to replace or provide backup for private leased lines and Frame Relay links, and regulatory pressures requiring encryption of private WAN links.

- **Medium-sized and large enterprises:** In industries such as finance, insurance, or retail, numerous sites are typically connected to the corporate headquarters. Critical applications such as bank ATMs and point of sale (POS) machines are deployed over these connections. Cisco DMVPN allows these sites to connect over the Internet, providing privacy and data integrity while meeting the performance requirements of business-critical applications.
- **Enterprise small office/home office (SOHO):** Cisco DMVPN provides enhanced integration with QoS that can be used to support both voice and data for employees accessing the network from a SOHO environment.

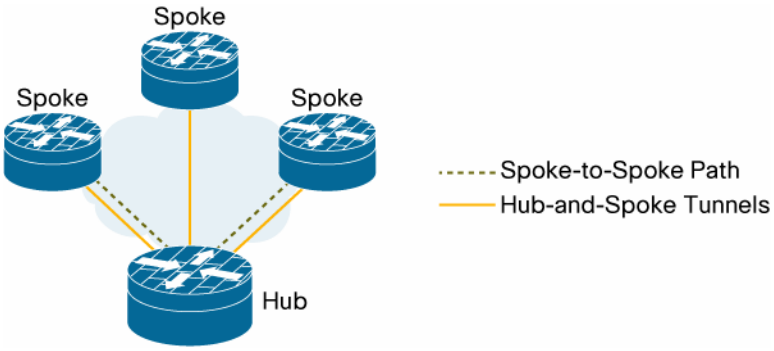
- **Enterprise extranet:** Large enterprises frequently require connectivity to many business partners. Cisco DMVPN can be used to secure traffic between the enterprise and various partner sites, providing network segregation by helping to ensure that no spoke-to-spoke traffic is allowed, even through the hub.
- **Enterprise WAN connectivity backup:** Cisco DMVPN can be used as a backup solution for private WANs, allowing remote sites to connect securely to the enterprise head-office over Internet links.
- **Service provider VPN services:** Cisco DMVPN enables service providers to offer managed VPN services. Traffic from multiple customers can be aggregated in a single provider edge router, and kept isolated using features such as Virtual Routing and Forwarding (VRF).

Deployment Scenarios

Cisco DMVPN can be deployed in two ways:

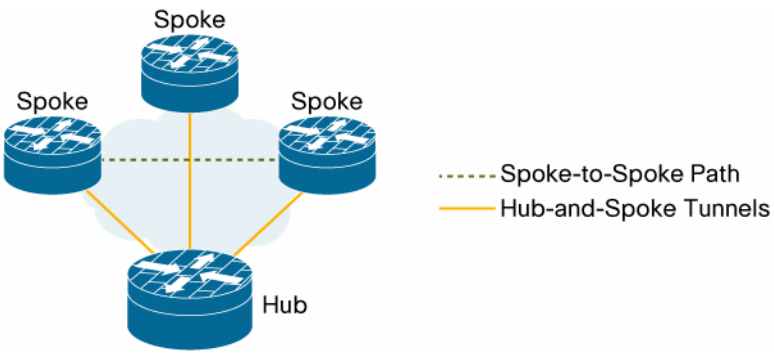
Hub-and-spoke deployment model: In this traditional topology, remote sites (spokes) are aggregated into a headend VPN device at the corporate headquarters (hub). Traffic from any remote site to other remote sites would need to pass through the headend device. Cisco DMVPN supports dynamic routing, QoS, and IP Multicast while significantly reducing the configuration effort. Figure 2 shows a hub-and-spoke model.

Figure 2. Cisco DMVPN Hub-and-Spoke Deployment Model



Spoke-to-spoke deployment model: Cisco DMVPN allows the creation of a full-mesh VPN, in which traditional hub-and-spoke connectivity is supplemented by dynamically created IPsec tunnels directly between the spokes. With direct spoke-to-spoke tunnels, traffic between remote sites does not need to traverse the hub; this eliminates additional delays and conserves WAN bandwidth. Spoke-to-spoke capability is supported in a single-hub or multihub environment. Multihub deployments provide increased spoke-to-spoke resiliency and redundancy. Figure 3 shows a spoke-to-spoke model.

Figure 3. Cisco DMVPN Spoke-to-Spoke Deployment Model



The 80:20 traffic rule can be used to determine which model to use:

- If 80 percent or more of the traffic from the spokes are directed into the hub network itself, deploy the hub-and-spoke model.
- If more than 20 percent of the traffic is meant for other spokes, consider the spoke-to-spoke model.

For networks with a high volume of IP Multicast traffic, the hub-and-spoke model is usually preferred.

Architecture

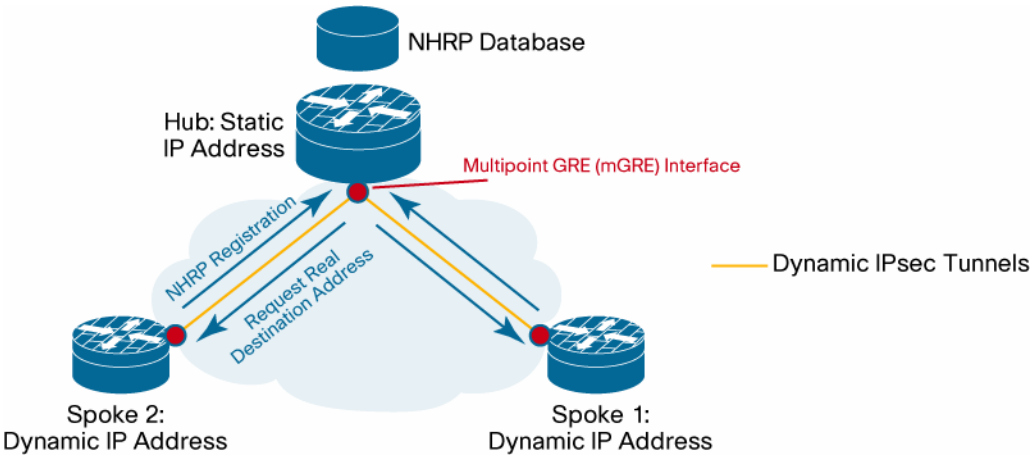
Medium-sized and large-scale site-to-site VPN deployments require support for advanced IP network services such as:

- IP Multicast: Required for efficient and scalable one-to-many (i.e., Internet broadcast) and many-to-many (i.e., conferencing) communications, and commonly needed by voice, video, and certain data applications
- Dynamic routing protocols: Typically required in all but the smallest deployments or wherever static routing is not manageable or optimal
- QoS: Mandatory to ensure performance and quality of voice, video, and real-time data applications

Traditionally, supporting these services required tunneling IPsec inside protocols such as Generic Route Encapsulation (GRE), which introduced an overlay network, making it complex to set up and manage, and limiting the scalability of the solution. Indeed, traditional IPsec only supports IP Unicast, making it inefficient to deploy applications that involve one-to-many and many-to-many communications.

Cisco DMVPN combines GRE tunneling and IPsec encryption with Next-Hop Resolution Protocol (NHRP) routing in a manner that meets these requirements while reducing the administrative burden (Figure 4).

Figure 4. Cisco DMVPN Architecture



Key components include:

- **Multipoint GRE (mGRE) tunnel interface:** Allows a single GRE interface to support multiple IPsec tunnels, simplifying the size and complexity of the configuration.
- **Dynamic discovery of IPsec tunnel endpoints and crypto profiles:** Eliminates the need to configure static crypto maps defining every pair of IPsec peers, further simplifying the configuration.
- **NHRP:** Allows spokes to be deployed with dynamically assigned public IP addresses (i.e., behind an ISP's router). The hub maintains an NHRP database of the public interface addresses of the each spoke. Each spoke registers its real address when it boots; when it needs to build direct tunnels with other spokes, it queries the NHRP database for real addresses of the destination spokes.

Features and Benefits

Table 1 lists the features and benefits of Cisco DMVPN.

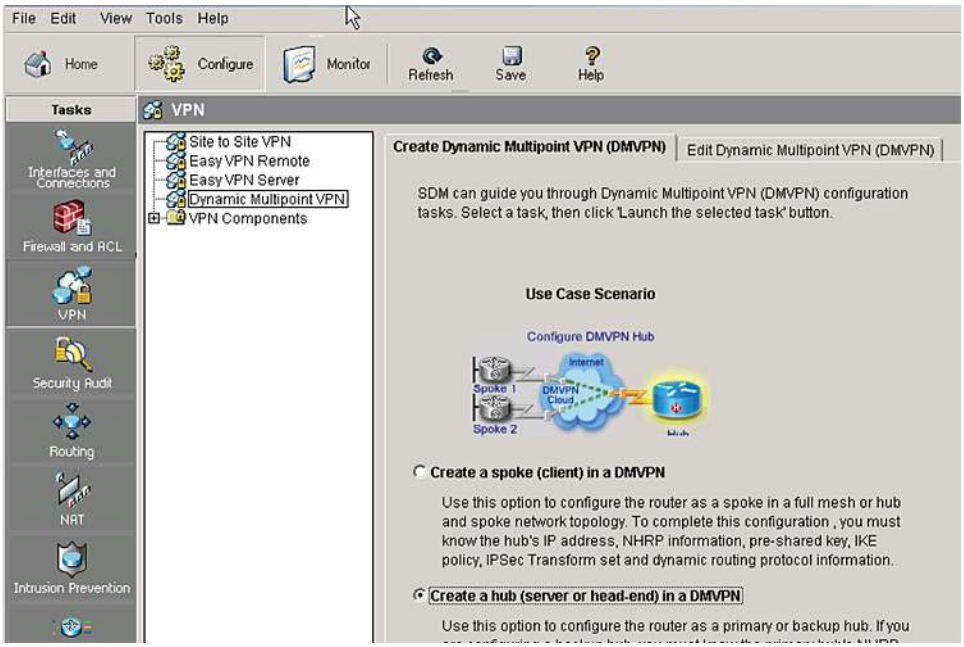
Table 1. Cisco DMVPN Features and Benefits

Feature	Description and Benefit
Dynamic Routing over VPN	• Enables IP routing tables to be securely distributed between the branch site and the corporate headend over encrypted tunnels. Allows improved reachability without needing to manually define allowed routes. • Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) routing protocols are supported.
Reduced Configuration Overhead	• DMVPN eliminates the need to configure crypto maps tied to the physical interface, dramatically simplifying the number of lines of configuration required for a VPN deployment (e.g., for a 1000-site deployment, DMVPN reduces the configuration effort at the hub from 3900 lines to 13 lines). • Adding new spokes to the VPN requires no changes at the hub. • Simplifies configuration of split tunneling. Centralized configuration change at the hub controls the split tunneling behavior. In traditional IPsec, all the spokes need to be modified.
Zero-Touch Deployment	• Cisco DMVPN can be deployed in zero-touch deployment models using Easy Secure Device Deployment for secure PKI-based device provisioning. Devices can be bootstrapped remotely, avoiding the need for extensive staging operations.
Dynamic Spoke-to-Spoke Tunnels	• Direct spoke-to-spoke tunnels eliminate the need for spoke-to-spoke traffic to traverse the hub. • Reduces latency for voice over IP (VoIP) deployments over DMVPN and improves effective throughput of the hub router. • Tunnels are created dynamically when required and torn down after use, allowing the system to scale better (i.e., smaller spokes can participate in the virtual full mesh).
Dynamic Addressing for Spoke Routers	• Spoke routers can use dynamic IP addresses, a frequent requirement for Internet connections over cable and DSL.
Network Address Translation (NAT) Traversal	• DMVPN supports spoke routers running NAT or behind dynamic NAT devices, enabling enhanced security for branch subnets.
IP Multicast Support	• DMVPN supports IP Multicast traffic (between hub and spokes); native IPsec supports only IP Unicast. This provides efficient and scalable distribution of one-to-many and many-to-many traffic.
QoS Support	Cisco DMVPN supports the following advanced QoS mechanismis: • Traffic shaping at hub interfaces on a per-spoke or per-spoke-group basis. • Hub-to-spoke and spoke-to-spoke QoS policies. • Dynamic QoS policies wherein QoS templates are attached automatically to tunnels as they come up. • Per-spoke QoS policing, allowing spokes to be differentiated, and protecting the network from being overrun by bandwidth hungry spokes.
High Availability	• Cisco DMVPN enables routing-based failover. • Dual WAN links and hub redundancy provide higher availability. DMVPN supports dual-hub designs, where each spoke is peered with two hubs, providing rapid failover. • Mulitiple hub topologies allow uninterrupted spoke-to-spoke communication in the event of any single hub failure.
Scalability	• DMVPN scales to thousands of spokes using server load balancing (SLB). Encryption can be integrated within the SLB device or distributed to dedicated headend VPN routers. Tunnels are load balanced over available hubs. • Performance can be scaled incrementally by adding hubs. • Hierarchical hub deployments allow enhanced scalability.
Manageability	• Manageability support is provided through IPsec (including VRF-aware IPsec) MIB, NHRP MIB, and command-line interface (CLI).
VRF Awareness	• VRF-aware DMVPN deployed at the provider edge hubs allows segregation of customer traffic.
Multiprotocol Label Switching (MPLS) Support (2547oDMVPN)	• MPLS networks can be encrypted over DMVPN tunnels.

Ease of Deployment and Management

Cisco Router and Security Device Manager (SDM) provides advanced wizards to make it easy to configure Cisco DMVPN (Figure 5). Cisco SDM is included in Cisco router security bundles and is an effective tool to configure DMVPN for small deployments or pilot/test environments.

Figure 5. Cisco Router and Security Device Manager: Wizard-Based Management



Cisco Security Manager provides enterprise-class scalable Cisco DMVPN configuration on a wide range of Cisco routers for medium-sized or large installations requiring multispoke management. Some of the DMVPN features supported in Cisco Security Manager include:

- DMVPN SLB deployment models involving distributed or integrated encryption
- VRF-aware DMVPN
- EIGRP, OSPF, Routing Information Protocol (RIP)v2, and on-demand routing (ODR)

Cisco IOS Software CLI provides configuration, monitoring, and debugging capabilities for Cisco DMVPN hub-and-spoke and spoke-to-spoke configurations.

System Requirements

Tables 2 and 3 list the hardware and software requirements to install and use Cisco DMVPN.

Table 2. Cisco Hardware Platforms That Support Cisco DMVPN

Platform	VPN Acceleration Module
Cisco 870 Series Integrated Services Routers*	Onboard encryption
Cisco 1801, 1802, 1803, 1811, 1812, 1841, 2800, 3825, and 3845 Integrated Services Routers	Onboard encryption
Cisco 1841 Integrated Services Routers	Advanced Integration Module (AIM)-VPN/SSL-1
Cisco 2800 Series Integrated Services Routers	AIM-VPN/SSL-2
Cisco 3825 Integrated Services Routers	AIM-VPN/SSL-3
Cisco 3845 Integrated Services Routers	AIM-VPN/SSL-3
Cisco 1900, 2900, and 3900 Next Generation Integrated Services Routers	Onboard encryption
Cisco 7200 Series Routers	VPN Acceleration Module 2+ (VAM2+)
Cisco 7200VXR Routers with Network Processing Engine NPE-G2	VPN Services Adapter (VSA)
Cisco 7301 Routers	VAM2+
Cisco 7600 Series Routers	IPsec VPN Shared Port Adapter (SPA)
Cisco Catalyst 6500 Series Switches	IPsec VPN SPA
Cisco ASR 1000 Series Routers	Onboard encryption

* Functions as DMVPN spoke only.

Table 3. Cisco DMVPN Software Requirements

Hardware	Cisco 870, 1800, 1900, 2800, 2900, 3800, 3900, 7200 Series and Cisco 7301 routers
Cisco IOS Software Release	• Cisco IOS Software Release 12.3(2)T or later recommended for Cisco 870, 1800, 2800, 3800, and 7200 Series Routers and Cisco 7301 Routers • Cisco IOS Software Release 15.0 or later recommended for Cisco 1900, 2900 and 3900 Series Routers • Cisco IOS Software Release 12.2(18)SXE2 or later for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers • Cisco IOS XE Release 2.0.0 or later for Cisco ASR 1000 Series Routers
Cisco IOS Software Feature Set	• Advanced Security or higher • Cisco ASR 1000 Series Routers also require VPN license

Ordering Information

All Cisco router security bundles include support for Cisco Easy VPN. For a list of router security bundles, visit http://www.cisco.com/go/securitybundles.

To place an order, visit the Cisco Ordering Home Page. To download software, visit the Cisco Software Center at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml.

Cisco and Partner Services for the Branch

Services from Cisco and our certified partners can help you transform the branch experience and accelerate business innovation and growth in the Borderless Network. We have the depth and breadth of expertise to create a clear, replicable, optimized branch footprint across technologies. Planning and design services align technology with business goals and can increase the accuracy, speed, and efficiency of deployment. Technical services help improve operational efficiency, save money, and mitigate risk. Optimization services are designed to continuously improve performance and help your team succeed with new technologies.

For More Information

Visit the Cisco Software Center to download Cisco IOS Software. See the System Requirements section above to determine which Cisco IOS Software Release to download and install.

For more information about Cisco DMVPN, visit http://www.cisco.com/go/dmvpn, contact your local Cisco account representative, or send e-mail to ask-stg-ios-pm@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-468520-01 08/09