Q&A

Cisco IOS Secure Multicast

This section introduces a foundational technology and Cisco Systems® innovation—Cisco IOS® Secure Multicast—and discusses positioning and advantages of VPN solutions over native IP Security (IPsec), generic routing encapsulation (GRE), and Easy VPN.

Q. What is Cisco IOS Secure Multicast?

A. Cisco IOS Secure Multicast is a set of hardware and software features necessary to secure IP Multicast group traffic originating on or flowing through a Cisco IOS device. Combining the keying protocol Group Domain of Interpretation (GDOI) with hardware-based IPsec encryption, it provides users an efficient method to secure IP Multicast group traffic. It enables the router to apply encryption to nontunneled (that is, "native") IP Multicast packets and eliminates the requirement to configure tunnels to protect multicast traffic. It relies on two technologies:

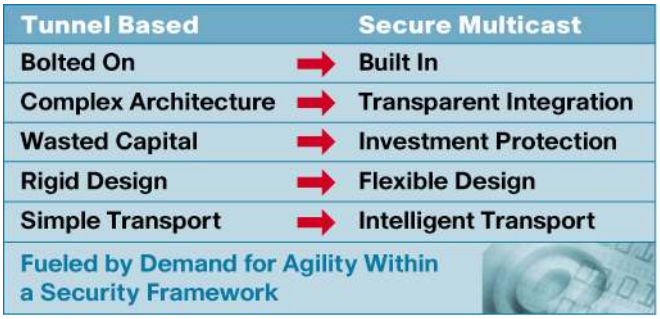
- **Group Domain of Interpretation**—GDOI is defined as the ISAKMP Domain of Interpretation (DOI) for group key management. In a group management model, the GDOI protocol operates between a group member and a group controller/key server (GCKS), which establishes security associations among authorized group members. The ISAKMP defines two phases of negotiation. GDOI is protected by a Phase 1 ISAKMP security association; the Phase 2 exchange is defined in RFC 3547.
- **IP Security**—IPsec is a well-known protocol that defines architecture to provide various security services for traffic at the IP layer. The components and how they fit together with each other and into the IP environment are described in RFC 2401. A variety of IP Multicast applications benefit from the encryption of native IP Multicast packets.

Q. What are the benefits of Cisco IOS Secure Multicast deployments?

A. Cisco IOS Secure Multicast can be used to protect native multicast traffic, originating from various applications such as voice, video, etc. without the use of tunnels. It is typically used in private WAN deployment, and it provides the following benefits:

- Includes native IPsec encapsulation for IP Multicast traffic without requiring GRE
- Allows for one-to-many and many-to-many relationships
- Provides easier configuration and enhanced manageability
- Distributes centralized key and policies through GDOI key server
- Simplifies troubleshooting
- Uses extensible standards-based framework

Figure 1. Cisco IOS Secure Multicast Differentiators



All contents are Copyright © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Q. What are the various deployments of Cisco IOS Secure Multicast?

A. Cisco IOS Secure Multicast is a foundational technology that can be used in many deployment scenarios. In network scenarios other than an IPsec remote-access network, it is more efficient to apply encryption to nontunneled (that is, "native") IP Multicast packets. Encapsulating IP Multicast packets as IP Multicast packets allows IP Multicast routing (for example, Protocol Independent Multicast [PIM]) to route the packets, regardless of the fact that the content is encrypted. A native IP Multicast encapsulation also avoids the needless packet replication that occurs when encapsulating IP Multicast packets using unicast tunnels.

The most commonly used scenarios include the following:

- Encryption of IP Multicast packets sent over satellite links
- Encryption in Hoot and Holler audio conferencing
- Cisco IOS Secure Multicast router control traffic
- Secure real-time content replication
- Secure Multicast VPN (mVPN)
- Dynamic Multipoint VPN (DMVPN)
- Details of Cisco IOS Secure Multicast topologies and configurations can be accessed in the Cisco IOS Secure Multicast white paper at: http://www.cisco.com/go/multicast

Q. What are the technical benefits of Cisco IOS Secure Multicast?

A. The benefits of Cisco IOS Secure Multicast follow:

- Avoids complexity of network overlays (IPsec over IP)
  - Requires conversion of only one network layer
  - Reduces extra penalty on hub CPU
  - Eliminates suboptimal routing, and reduces latency and bandwidth overhead
- Eliminates needless replication
  - Takes advantage of IP Multicast core infrastructure
  - Minimizes encapsulation and encryption
  - Saves hub CPU resources and bandwidth overhead
- Requires no point-to-point tunnels for multicast traffic
  - Reduces number of IPsec security associations (just 1 instead of ~N2)
  - Scalable by design, saving hub CPU resources
  - Simplifies troubleshooting (manage N entities instead of ~N2)
- Offers other benefits
  - Offers extra security for PIM control packets
  - Offers extensible framework: Multiprotocol Label Switching (MPLS) customer edge to customer edge starting today (mVPN); MPLS VPN provider edge and provider replication future

Q. What is GDOI, and how is it related to Cisco IOS Secure Multicast?

A. Refer to the question, "What is Cisco IOS Secure Multicast?" earlier in the document.

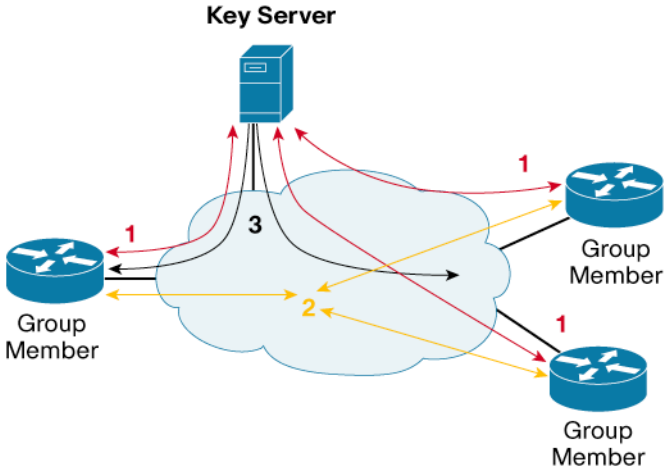
© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

The topology in Figure 2 shows the protocol flows that are necessary for group members to participate in a group:

1. Group members register with the key server, which authenticates and authorizes the group members and downloads the IPsec policy and keys that are necessary for them to encrypt and decrypt IP Multicast packets.
2. Group members exchange IP Multicast packets that are encrypted using IPsec.
3. As needed, the key server pushes a rekey message to the group members. The rekey message contains a new IPsec policy and keys to use when old IPsec security associations expire. Rekey messages are sent in advance of the security-association expiration time to ensure that valid group keys are always available.

   GDOI is implemented in the Cisco® feature Cisco IOS Secure Multicast.

Figure 2. Protocol Flows That Are Necessary for Group Members to Participate in a Group



POSITIONING OF CISCO IOS SECURE MULTICAST TO OTHER IPSEC SOLUTIONS

Q. What are the differences between Cisco IOS Secure Multicast and native IPsec?

A. Cisco IOS Secure Multicast is a foundational technology that has several applications—in fact, it is used with Cisco IPsec solutions such as DMVPN as well. Cisco IOS Secure Multicast has the following advantages over native IPsec:

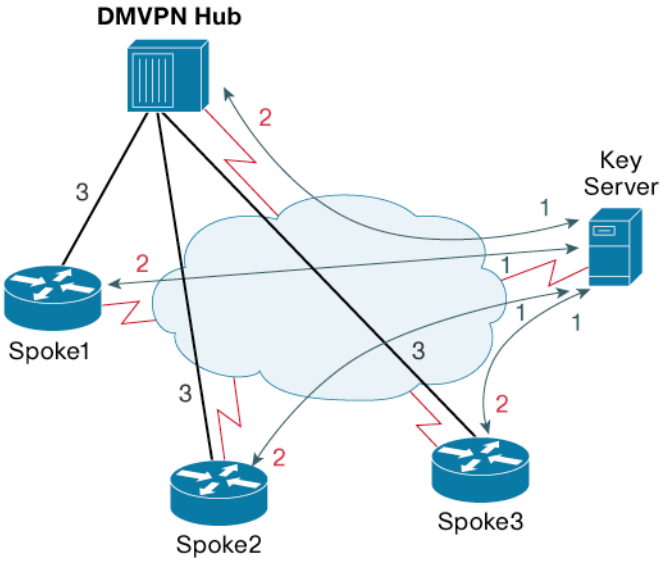
- Unlike native IPsec, Cisco IOS Secure Multicast alleviates the need for tunnels, thus enabling protection of “native” multicast traffic.
- Unlike native IPsec, Cisco IOS Secure Multicast preserves the original context of (source, group [S,G]) for a multicast application, such that the context is preserved before encryption, after encryption, transit, and after decryption, enabling Cisco IOS Secure Multicast to take advantage of the underlying network for multicast replication.
- Unlike native IPsec, Cisco IOS Secure Multicast is a group or community of interest, making it easier to manage.
- Unlike native IPsec, Cisco IOS Secure Multicast, through the role of key server, enables pushing both the keys and policies for all registered and authenticated members.
- Unlike native IPsec, Cisco IOS Secure Multicast supports unicast, multicast, and dynamic routing.

Q. What are the differences between DMVPN and Cisco IOS Secure Multicast?

A. DMVPN and Cisco IOS Secure Multicast are complementary. In fact, Cisco IOS Secure Multicast when used in a DMVPN environment can aid in the deployments of voice, video, and VPN (Figure 3).

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Figure 3. Application Scenario: Integration of GDOI with DMVPN



- DMVPN hub and all spokes are configured as group members. All group members register with the key server.
- The key server distributes group and IPsec policy information to all group members.
- A spoke-to-hub tunnel is established using NHRP. All packets traveling via the DMVPN tunnel are now encrypted using the group key.
- The spoke sends NHRP resolution request to the hub for any spoke-spoke communication
- Upon receiving NHRP resolution reply from the hub, the spoke sends traffic directly to their spokes with group key encryption.

Benefit: Using Cisco IOS Secure Multicast functionality in a DMVPN network eliminates the delay caused by IPsec negotiation.

Note: Multicast traffic will still be forwarded to hub for any spoke to spoke connectivity even with this deployment.

DMVPN provides spoke-to-hub and spoke-to-spoke connectivity solutions using multipoint GRE (MGRE) and Next Hop Resolution Protocol (NHRP) functions. If spoke-to-spoke direct connectivity is enabled in the network, the spoke maintains a permanent IPsec tunnel to the hub, but the spoke-to-spoke IPsec tunnel is dynamic (on demand). Whenever spoke-to-spoke connectivity is desired, the originating spoke sends a NHRP resolution request to the hub, and the destination spoke and hub responds with nonbroadcast multi-access address (NBMA) mapped to the destination NHRP address. When the mapping is received, the spoke initiates a dynamic IPsec tunnel with the destination spoke using the same MGRE interface. Traffic then starts passing through this dynamic tunnel. However, until this dynamic tunnel is built, traffic continues to pass through the hub. To get any response from the destination spoke, the same procedure is initiated by the destination spoke toward the originating spoke.

The creation of a dynamic tunnel keeps the hub from being bombarded with spoke-to-spoke traffic, but it introduces some delay in setting up the tunnel. Though this delay exists for any direct communications between spokes, certain real-time applications such as voice would want to avoid that. Using Cisco IOS Secure Multicast—GDOI—technology eliminates the delay caused by IPsec negotiation, which is the major contributor to the overall delay. It is important to note that when group keying is applied to the tunnel in a DMVPN context, all tunnel traffic is encrypted with the group key. In other words, the traffic is more than multicast.

Q. What are the differences between Cisco IOS Secure Multicast and Easy VPN?

A. The differences vary, depending on the type of Easy VPN, whether it is legacy Easy VPN—Easy VPN over Internet—or the Easy VPN with a virtual tunnel interface (VTI). When Easy VPN is used with VTI between site-to-site gateways over a private network, Cisco IOS Secure Multicast and Easy VPN are complementary. However, there is no relationship between Cisco IOS Secure Multicast and Easy VPN when Easy VPN is used to connect to a corporate gateway over an Internet.

Q. What customers would be interested in deploying Cisco IOS Secure Multicast?

A. Customers interested in a VPN installation that involves the following would want to deploy Cisco IOS Secure Multicast:

- Securing multicast—and of course, unicast—traffic
- Deploying voice with VPN with a solution such as DMVPN

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

- Protecting and securing multicast control traffic
- Encrypting IP Multicast packets sent over satellite links
- Encrypting multicast packets in a MVPN environment

Q. What customers would be interested in an alternate Cisco VPN solution?

A. Customers interested in a VPN for basic connectivity without any of the features listed previously would want to deploy Cisco IOS Secure Multicast. Examples include:

- Easy VPN and VTI
- IPsec

Customers interested in multicast and routing protocols should deploy:

- DMVPN with Cisco IOS Secure Multicast

Q. What is GDOI, and how is it different from Internet Key Exchange (IKE)?

A. GDOI is a key management protocol, similar to IKE, but GDOI is used for providing key management for native multicast traffic and IKE is suitable for providing key management for unicast traffic. Table 1 compares GDOI and IKE.

Table 1. Comparison of GDOI and IKE

	IKEv1	IKEv2	GDOI
RFC Documents	2407, 2408, 2409	**RFC 4306**	**RFC 3547**
UDP Port	500 and 4500	500 and **4500**	848
Phases	2, Ph. 1 (6/3 messages), Ph. 2 (3 messages)	2, Ph. 1 (4 messages), Ph. 2 (2 messages)	2, Ph. 1 (6/3 messages), Ph. 2 (4 messages)
Authentication Type	Signature, PSK, and PKI	**Signature, PSK, and PKI**	**Signature, PSK, and PKI**
Security-Association Negotiation	Responder selects initiator's proposal	**Same as IKEv1, proposal structure simplified**	**Not negotiated, GODI is used to push keys and policies**
Identity Hiding	Yes in MM, No in AM	**Yes**	**Yes in MM, No is AM**
Keepalives	No	**Yes**	**No**
Anti-DoS	No	**Yes**	**Yes**
UDP/NAT	No	**Yes**	**No**
Reliability	No	**Yes**	Yes
PFS	Yes	**Yes**	**Yes**
EAP/CP	No	**Yes**	**No**

Q. What are Cisco IOS Secure Multicast Support, Scalability, and Management options?

A. This section covers:

- Cisco IOS Secure Multicast support questions (multicast, voice over IP [VoIP], MPLS, routing protocols supported, quality of service [QoS], and NAT)
- Cisco IOS Secure Multicast configuration questions
- Cisco IOS Secure Multicast scalability questions
- Cisco IOS Secure Multicast management (MIBs, monitor individual connections, and enhanced command-line interface [CLI])

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

- Cisco IOS Secure Multicast availability and resiliency questions (failover mechanisms, resiliency, and dual hubs)

CISCO IOS SECURE MULTICAST SUPPORT QUESTIONS

Q. What images are recommended for Cisco IOS Secure Multicast?

A. The following images are recommended:

For Cisco 830 through Cisco 7200VXR/7300 routers:

- Cisco IOS Software Mainline: None
- Cisco IOS T-train: 12.4(6)T

For Cisco Catalyst 6500 or Catalyst 7600:

- None, this feature is not supported

Cisco IOS Secure Multicast introduces two new taxonomies: key server and group member. Cisco IOS Secure Multicast is supported on the entire access Cisco line of VPN router products, which range in application from small business up to large VPN tunnel aggregation points at a large enterprise central site. The following lists show the range of products available.

Key server platforms:

- Cisco 1800, 2800, and 3800 Series Integrated Services Routers
- Cisco 7206VXR Router

Group member platforms:

- Cisco 830 through 7200VXR/7300 routers

Q. How is Cisco IOS Secure Multicast configured with mVPN?

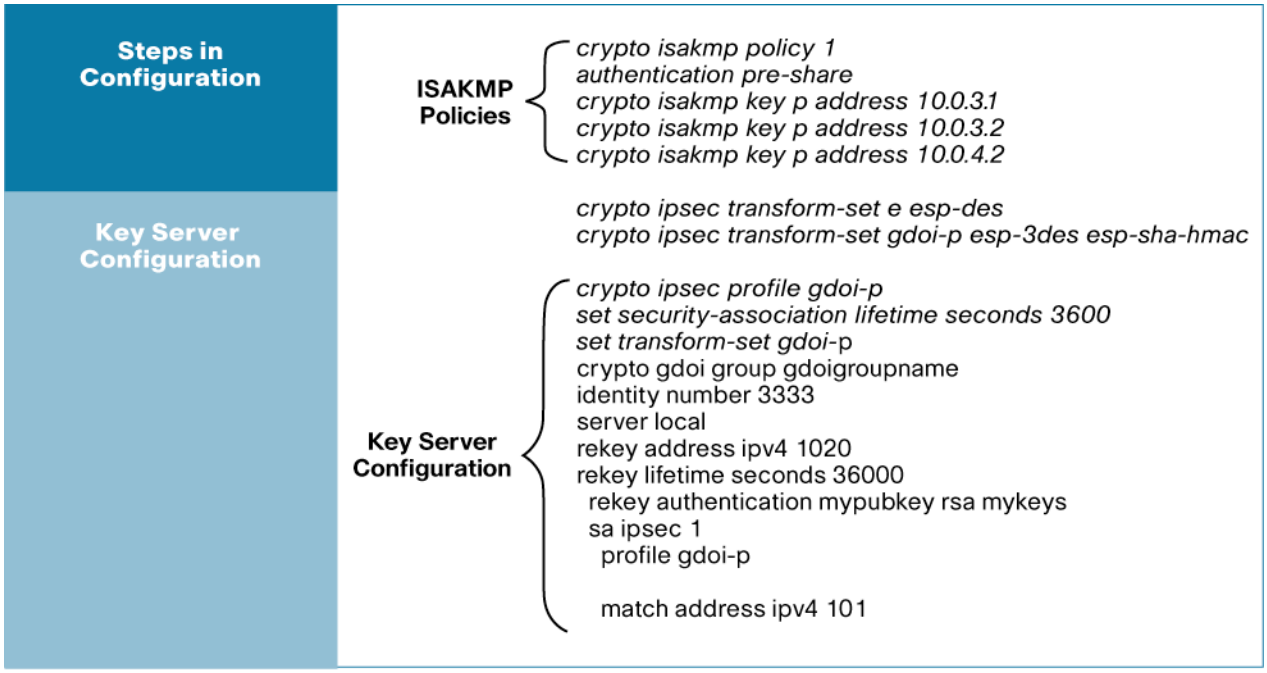
A. Refer to Appendix A in the deployment guide in the “Deployment Guide” section http://www.cisco.com/go/multicast.

Q. What is the key server configuration?

A. Figure 4 shows the key server configuration.

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Figure 4. Cisco IOS CLI Configuration for Key Server



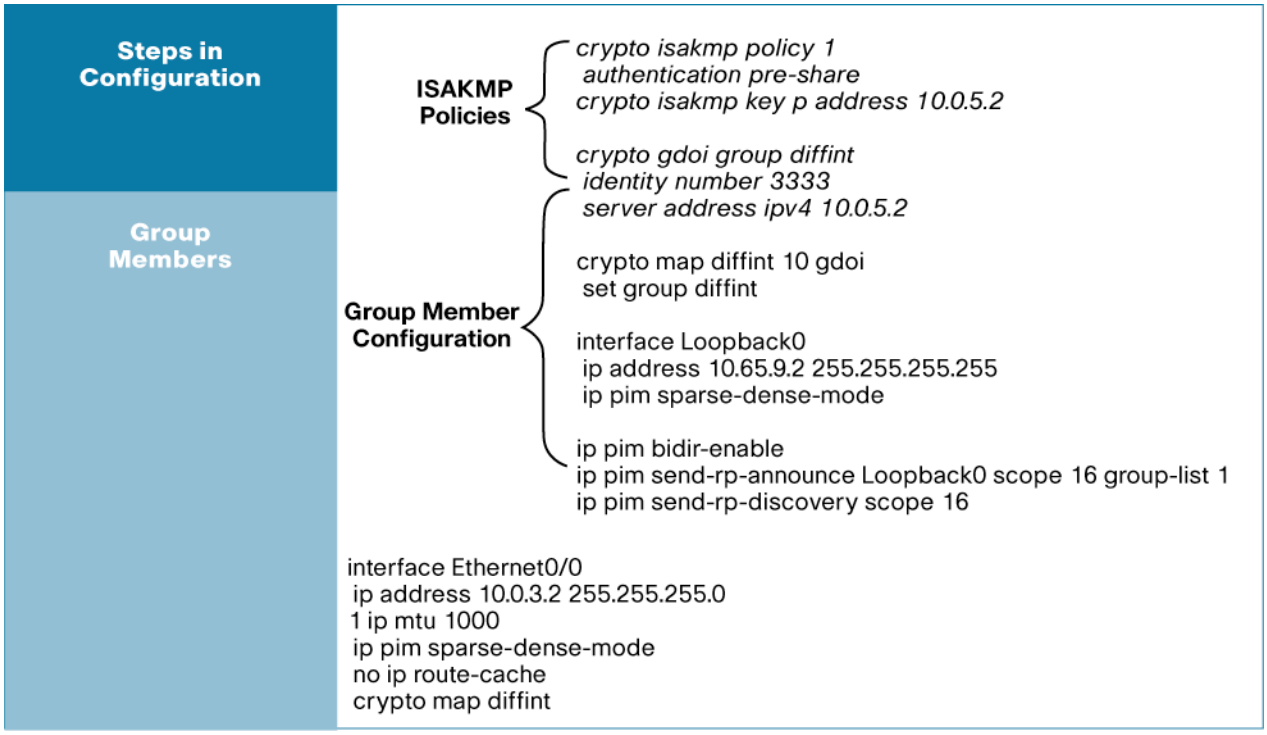

```
! The following line is the access control list downloaded from the key server to the group member
! This line tells the group members which encrypted traffic is acceptable in this SSM configuration.
access list 101 permit ip host 10.0.1.1 host 192.168.5.1

!The following line is the rekey access control list to which multicast addresses the rekeys are to be sent.
access list 102 permit udp host 10.0.5.2 eq 848 host 192.168.1.2 eq 848
```

Q. What is the group member configuration?

A. Figure 5 gives the group member configuration.

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Figure 5. Cisco IOS CLI Group Member Configuration



Q. What routing protocols are supported for DMVPN?

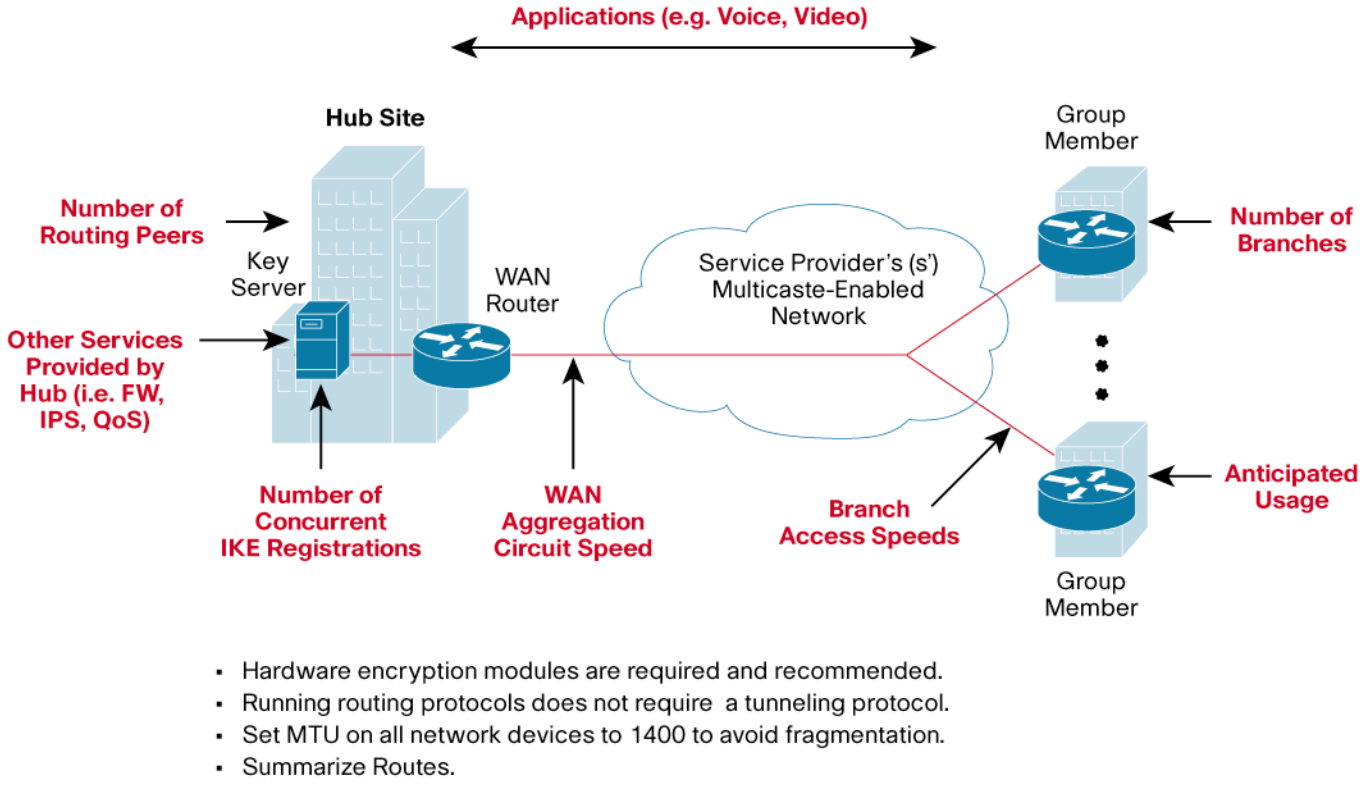
A. Enhanced Interior Gateway Routing Protocol (EIGRP), On-Demand Routing (ODR), and Open Shortest Fast Path (OSPF) are supported. Intermediate System-to-Intermediate System (IS-IS) is not supported because it does not use IP as its network or transport protocol. Border Gateway Protocol (BGP) is supported, but requires specification of all the neighbors individually in the configuration.

Q. What are the general design considerations of Cisco IOS Secure Multicast?

A. Refer to Figure 6.

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Figure 6. General Design Considerations for Cisco IOS Secure Multicast



Q. What are the best practices for Cisco IOS Secure Multicast?

A. Cisco IOS Secure Multicast provides the following elements:

- For multicast control traffic, enable PIM sparse mode.
- Set up digital certificates and public key infrastructure (PKI) for group member authentication.

Q. How is voice supported in a Cisco IOS Secure Multicast network?

A. VoIP is an application that is very sensitive for end-to-end delay. Cisco IOS Secure Multicast provides VoIP with security and optimized path across the network. Because there is no hub, the group member can select the optimum path and lower delay for switching the voice packets. The setup time is practically nil for the direct path between the group members, making it transparent for the end user.

In a DMVPN scenario, the application of secure multicast with DMVPN reduces the time lag during spoke-to-spoke tunnel setup, and enhances the quality of voice calls over the VPN network.

Q. How are QoS parameters configured in a Cisco IOS Secure Multicast network?

A. Cisco IOS Secure Multicast does not introduce logical tunnels, so every Cisco QoS router command is available for the user. The QoS parameters in DMVPN and GDOI networks should fall back to what is supportable with DMVPN.

Q. How are individual connections at the key server monitored?

A. Several CLI commands are available to monitor the group members; an example of a command is **show crypto group**.

Q. What is the support for Cisco IOS Secure Multicast and MIBs?

A. A Cisco IOS Secure Multicast MIB is currently on the roadmap.

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

ENTERPRISE-CLASS TELEWORKER SOLUTION

Q. What is the ECT solution?

A. The Cisco Enterprise Class Teleworker (ECT) solution is the Cisco IT implementation of an internal teleworker solution for Cisco employees to work from the comfort of their homes with complete access to corporate resources. Currently used by more than 2000 company employees, Cisco ECT spans multiple company locations in the United States and overseas. Cisco ECT offers several unique features, such as providing complete support for IP telephony, layers of telephony, and access to video-on-demand (multicast) applications with layers of security.

For complete details about Cisco ECT, visit the ECT Website at http://www.cisco.com/go/ect. Following is a list of white papers outlining the solution. They can be accessed from the Website.

- **DMVPN Enterprise Class Teleworker Guide**—This document describes the deployment of DMVPN and various aspects of the Cisco ECT solution in a consolidated way.
- **Layered Security in a VPN Deployment**—This document describes the deployment of different aspects of layers of security in the Cisco ECT network.
- **Deployment of Secure Sockets Layer VPNs**—This document gives topology and configuration guidance and tried and tested scenarios of DMVPN with SSL VPN.
- **Cisco IOS IPsec High Availability**—This document gives topology and configuration guidance and tried and tested scenarios of IPsec high availability, which has been used in the management gateways to provide transparent connectivity to network management.
- **Secure Voice and Wireless in a VPN Deployment**—This document describes the deployment of voice and wireless applications in a Cisco ECT network.
- **Integrated Easy VPN and Dynamic Multipoint VPN**—This document describes the deployment of Easy VPN client on the same hub as DMVPN hubs used in the Cisco ECT solution.

Q. What are the layers of security in the Cisco ECT solution?

A. There are multiple layers of security.

- Router antitheft protection
- Maintenance of customer premises equipment (CPE) configuration integrity; Cisco AutoSecure; supported platforms: Cisco 831 Ethernet Broadband Router, Cisco 836 ADSL over ISDN Broadband Router, and Cisco 837 ADSL Broadband Router*
- Maintenance of client integrity—"Loss of private key"
- Perimeter integrity—Firewall access control and stateful inspection
- Client (router) authentication—PKI authentication, authorization, and accounting (PKI-AAA) integration
- User authentication—Based on Authentication Proxy feature (Auth-Proxy), integrated with AAA and Secure Address Resolution Protocol (Secure-ARP) (in DHCP)
- Port authentication—Standard 802.1x VLAN authentication for Cisco 831, 836, and 837 Broadband Routers; Cisco 1701 ADSL Security Access Router; Cisco 1711 and 1712 Security Access Routers; and Cisco 1721, 1751, 1751-V, and 1760 Modular Access Routers
- Data authentication and confidentiality
- Host protection—Network Admission Control (NAC) (antivirus) protection
- Encrypted RSA private key
- Intrusion prevention systems (IPS) – Dynamic IPS
- Easy secure device deployment using transitive trusted introduction

Refer to *"Layered Security in a VPN Deployment"* under *Deployment Guides* for a detailed explanation of the ECT layers of security at http://www.cisco.com/go/ect.

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

Q. What are the authentication methods in the ECT solution?

A. Standards 802.1x and authproxy are some of the authentication methods. This is answered in the layers of security already and described in detail in the *ECT Deployment Guide* under *Deployment Guides* at http://www.cisco.com/go/ect.

Q. What components are involved in the management of Cisco ECT?

A. From a provisioning and management perceptive, the components include:

- AAA for device authentication for PKI-AAA integration
- Cisco IOS Software Certificate Server for PKI deployment
- Cisco CNS 2100 Series Intelligence Engine as an event notification engine and configuration engine
- Cisco IP Solution Center for provisioning and management of the network
- Easy, secure device deployment registrar for easy, secure remote bootstrapping of new spokes

Q. How is Cisco IOS Secure Multicast related to Cisco ECT?

A. Cisco IOS Secure Multicast can be implemented as a part of managed services in Cisco ECT.

When Cisco IOS Secure Multicast is used with Cisco ECT, users must be aware that their connection shares keying material with other ECT users. That is, there is not the same level of privacy as a Cisco ECT solution using IKE to generate keys between each spoke and the hub.

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.

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.
168 Robinson Road
#28-01 Capital Tower
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 Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus 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

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0601R)

Printed in the USA C67-34151200 03/06

© 2006 Cisco Systems, Inc. All rights reserved.
Important notices, privacy statements, and trademarks of Cisco Systems, Inc. can be found on cisco.com.