Secure Multicast

First Published: February 27, 2006
Last Updated: October 2, 2011

Secure Multicast is a set of features that are necessary to secure IP multicast group traffic that originates on or flows through a Cisco IOS device. Secure Multicast combines the keying protocol Group Domain of Interpretation (GDOI) with IP security (IPsec) encryption to provide users with an efficient method to secure IP multicast group traffic. Secure Multicast 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.

Secure Multicast provides the following benefits:

- Protection of multicast traffic without any form of additional encapsulation.
- Scalability: one-to-many and many-to-many relationships.
- Manageability: easier configuration and enhanced manageability.
- Native IPsec encapsulation for IP multicast traffic.
- Centralized key and policies distribution mechanism through GDOI key server.
- Simplified troubleshooting.
- Extensible standard-based framework is used.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Secure Multicast" section on page 47.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

- Prerequisites for Secure Multicast, page 2
- Restrictions for Secure Multicast, page 2
- Information About Secure Multicast, page 2
- How to Configure Secure Multicast, page 7
- Configuration Examples for Secure Multicast, page 14
- Additional References, page 17
- Command Reference, page 18
- Glossary, page 47
- Feature Information for Secure Multicast, page 47

Prerequisites for Secure Multicast

- You should be knowledgeable about IPsec and Internet Key Exchange (IKE).
- You should know how to configure multicast routing on a Cisco IOS global router.
- When configuring the IKE policy, the IKE lifetime should be set to the minimum of 5 minutes so that unnecessary resources are not wasted on the maintenance of the IKE security association (SA). After the registration IKE SA is established, the rekeys no longer have to be maintained.

Restrictions for Secure Multicast

- A router can be a group member or a key server, but it cannot be configured for both at the same time.
- Cisco Express Forwarding (CEF) switching is not supported.
- The following platforms can be configured only as shown:
  - Cisco 800 through the 830 series routers: by a group member only.
  - Cisco 850 and 870 series routers: by a group member only.
- Public key infrastructure (PKI) is recommended for group members that have dynamic IP addresses.
- Network Address Translation-Traversal (NAT-T) will work only from the group member to the key server. NAT-T will not work if there is a NAT device between group members.

Information About Secure Multicast

To configure the Secure Multicast feature, you should understand the following concepts:

- Secure Multicast and Internet Standards, page 3
- How Protocol Messages Work with the Cisco IOS, page 4
- End-User Considerations, page 5
- Secure Multicast: Typical Scenarios, page 5

Secure Multicast and Internet Standards

Secure Multicast relies on the following two Internet standards: GDOI and IPsec.

GDOI

GDOI is defined as the Internet Security Association Key Management Protocol (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 or 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 IETF RFC 3547. The topology shown in Figure 1 and the corresponding explanation show how this protocol works.

Figure 1 Protocol Flows That Are Necessary for Group Members to Participate in a Group

The above topology in Figure 1 shows the protocol flows that are necessary for group members to participate in a group:

1. Group members register with the key server. The key server 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 new IPsec policy and keys to use when old IPsec SAs expire. Rekey messages are sent in advance of the SA expiration time to ensure that valid group keys are always available.

IPsec

IPsec is a well-known RFC that defines an 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 IETF RFC 2401.

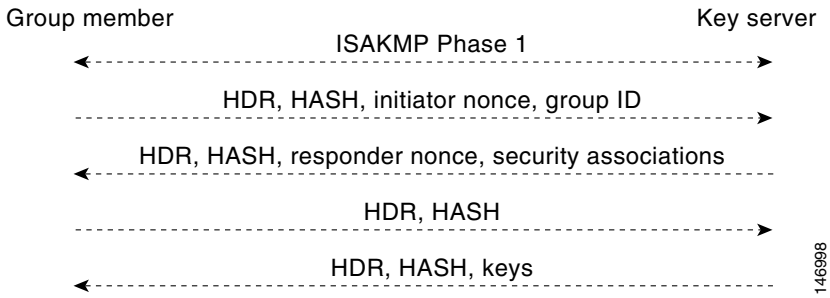
How Protocol Messages Work with the Cisco IOS

Secure Multicast uses the GDOI protocol (IETF RFC 3547) to distribute the policy and keys for the group. The GDOI protocol is between a key server and a group member. The key server creates and maintains the policy and keys, and it downloads the policy and keys to the authenticated group members. The group members are authenticated by the key server and communicate with other authenticated group members that are in the same group using the IPsec SAs that the group members have received from the key server.

The GDOI protocol is protected by an ISAKMP Phase 1 exchange. The GDOI key server and the GDOI group member must have the same ISAKMP policy. This Phase 1 ISAKMP policy should be strong enough to protect the GDOI protocol that follows. The GDOI protocol is a four-message exchange that follows the Phase 1 ISAKMP policy. The Phase 1 ISAKMP exchange can be main mode or aggressive mode.

Figure 2 shows the ISAKMP Phase 1 exchange.

Figure 2 ISAKMP Phase 1 Exchange



The above messages (the ISAKMP Phase 1 messages and the four GDOI protocol messages) are referred to as the GDOI registration, and the entire exchange that is shown above is a unicast exchange between the group member and the key server.

After the registration is successful, the key server sends a multicast rekey to all the group members that have registered within a group. During the registration, the group member receives the address of the multicast group and registers with the multicast group that is required to receive the multicast rekeys.)

Note The GDOI protocol uses User Datagram Protocol (UDP) port 848 (with NAT-T, it floats to 4848).

Key Server

The responsibilities of the key server include maintaining the policy and creating and maintaining the keys for the group. When a group member registers, the key server downloads this policy and the keys to the group member. The key server also rekeys the group before existing keys expire.

The key server has two modes: servicing registration requests and sending rekeys. A group member can register at any time and receive the most current policy and keys. When a group member registers with the key server, the key server verifies the group ID that the group member is attempting to join. If this ID is a valid group ID, the key server sends the SA policy to the group member. After the group member acknowledges that it can handle the downloaded policy, the key server downloads the respective keys.

There are two types of keys that the key server can download: the key encryption key (KEK) and the traffic encryption key (TEK). The TEK becomes the IPsec SA with which the group members within the same group communicate. The KEK encrypts the rekey message.

The GDOI server sends out rekey messages either because of an impending IPSec SA expiration or because the policy has changed on the key server (using command-line interface [CLI]). The rekey messages may also be retransmitted periodically to account for possible packet loss. Packet loss can occur because rekey messages are sent without the use of any reliable transport. There is no efficient feedback mechanism by which receivers can indicate that they did not receive a rekey message, so retransmission seeks to bring all receivers up to date.

Group Member

The group member registers with the key server to get the IPsec SA or SAs that are necessary to communicate with the group. The group member provides the group ID to the key server to get the respective policy and keys for this group. These keys are refreshed periodically, and before the current IPsec SAs expire, so that there is no loss of traffic.

End-User Considerations

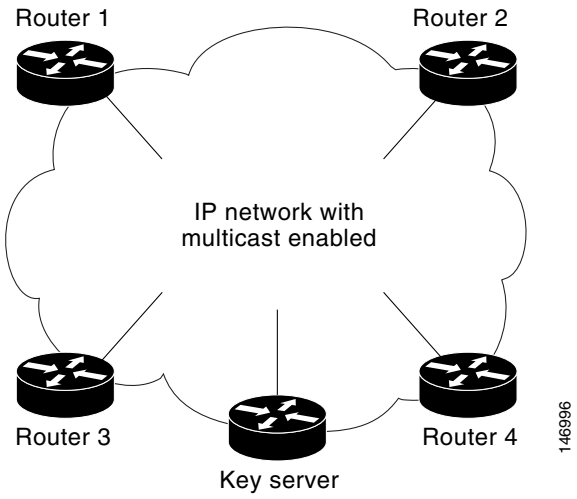
Secure Multicast can be used with all modes of multicast. The **rekey retransmit** command should be used whenever the Protocol Independent Multicast-sparse mode (PIM-SM) is configured because the PIM-SM shortest path tree (SPT) can be torn down if it does not receive continuing traffic. When traffic resumes, PIM-SM must reestablish the SPT. Retransmitting rekey packets increases the chance that group members will receive the rekeys when PIM-SM is setting up the SPT.

Secure Multicast: Typical Scenarios

IP Network with Multicast Enabled

IP multicast-enabled networks can transport encrypted multicast traffic natively over an IP core. An IP multicast encryption-enabled router can forward IP multicast packets to the core network, which is careful to distribute the multicast packets only to other customer edge (CE) devices that belong to the same customer. However, with secure multicast, the IP multicast traffic is protected with encryption in case packets are erroneously delivered. (See Figure 3 below.)

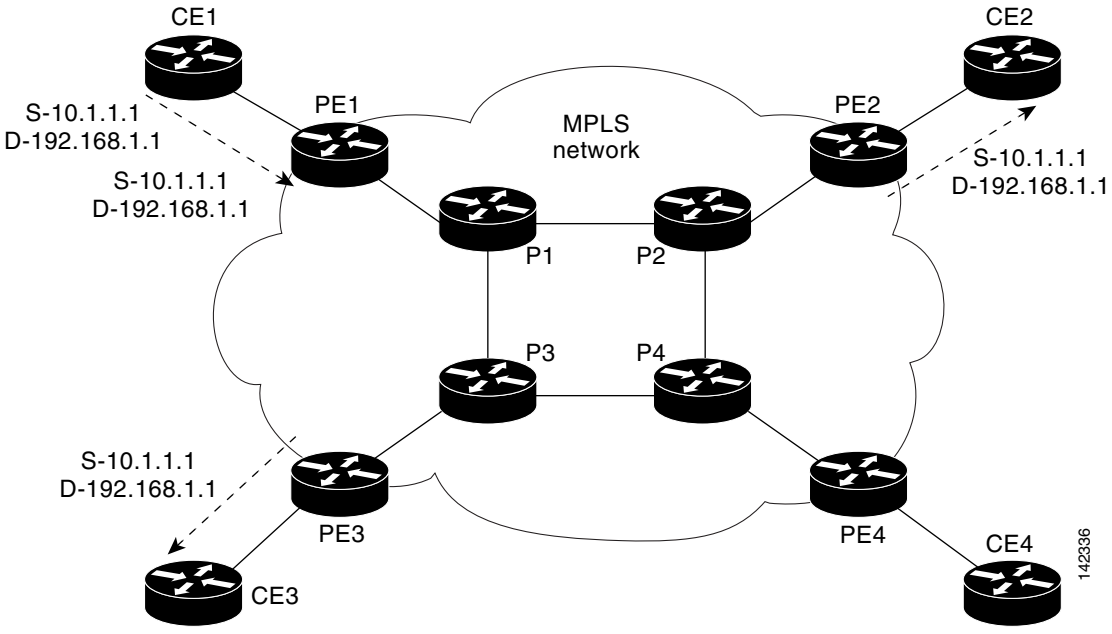
Figure 3 IP Network with Multicast Enabled



Multicast VPN over an MPLS Network

Figure 4 is an example of multicast virtual private network (VPN) packets that are being sent over a Multiprotocol Label Switching (MPLS) network.

Figure 4 Multicast VPN over an MPLS Network



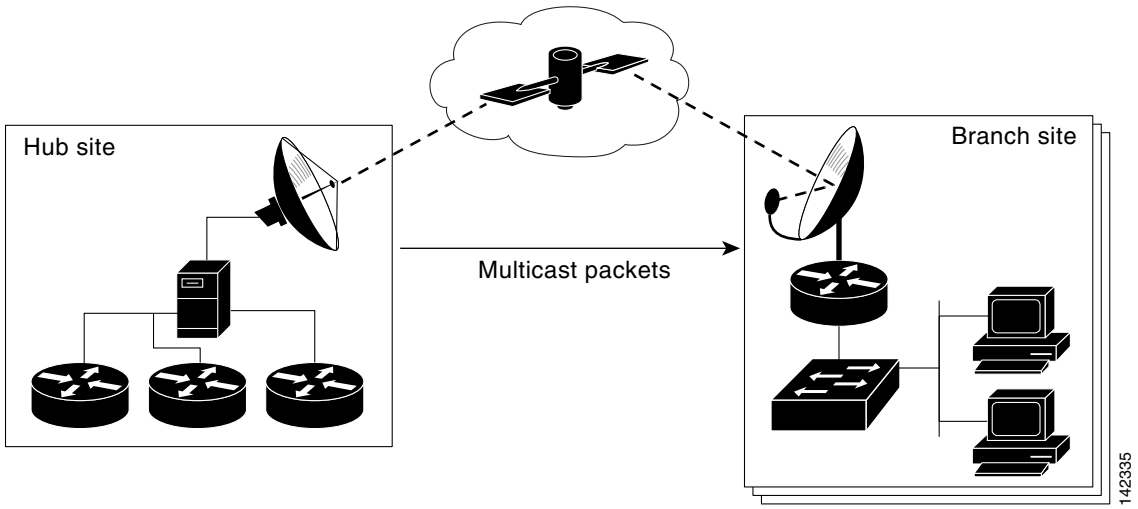
In Figure 4, a customer within an MPLS network has four CE devices attached to the MPLS network. One multicast sender (IP address 10.1.1.1) is sending packets on the IP multicast address 192.168.1.1. These packets are encrypted by CE1 before distribution into the provider edge (PE) network. Router PE1 creates a VPN packet, which is forwarded to P1. The multicast VPN packet code on P1 forwards the

packet toward both CE2 and CE3 because systems behind those routers have joined the 192.168.1.1 group and are "listening" for those packets. Devices CE2 and CE3 will decrypt the IP multicast packets and further distribute them in the network.

IP Multicast over Satellite

Figure 5 is an example of encrypted IP packets that are being sent over satellite links.

Figure 5 IP Multicast over Satellite



In Figure 5, a router in a hub has encrypted IP multicast packets and forwarded them to the satellite sending unit. The satellite sending unit transmits the IP packets to the satellite, where the satellite retransmits the IP packet toward the dish antennas located at branch sites. At each branch, a router decrypts the IP multicast packets and forwards the packet into the branch network.

How to Configure Secure Multicast

This section includes the following required and optional tasks:

- Configuring a Key Server, page 7 (required)
- Configuring Group Members, page 11 (required)
- Clearing a Group Member Registration with a Key Server, page 13 (optional)
- Verifying Secure Multicast, page 14 (optional)

Configuring a Key Server

To configure a key server, perform the following steps.

Prerequisites

Before creating the GDOI group, you must first configure IKE and the IPsec transform set, and you must create an IPsec profile. For information about how to configure IKE and the IPsec transform set and to create an IPsec profile, see the "Related Documents" subsection of the "Additional References" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** {*group-name*}
4. **identity number** {*number*}

   or

   identity address ipv4 {*address*}
5. **server local**
6. **authorization address ipv4** {*access-list-name* | *access-list-number*}
7. **rekey algorithm** {*type-of-encryption-algorithm*}
8. **rekey lifetime** {**seconds** *number-of-seconds*}
9. **rekey retransmit** {*number-of-seconds*} [**number** *number-of-retransmissions*]
10. **rekey authentication** {**mypubkey** | **pubkey**} {**rsa** *key-name*}
11. **rekey address ipv4** {*access-list-number* | *access-list-name*}
12. **registration interface** *type slot/port*
13. **sa ipsec** {*sequence number*}
14. **profile** {*ipsec-profile-name*}
15. **match address** {**ipv4** *access-list-number* | *access-list-name*}
16. **exit**
17. **exit**
18. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto gdoi group** {*group-name*} **Example:** `Router (config)# crypto gdoi group gdoigroupname`	Identifies a GDOI group and enters GDOI group configuration mode.

Step 4	**identity number** {*number*}
	
	or
	
	identity address ipv4 {*address*}
	
	Example:
	`Router (config-gdoi-group)# identity number 3333`
	
	or
	
	`Router (config-gdoi-group)# identity address ipv4 10.2.2.2`
		Identifies a GDOI group number or address.

Step 5	**server local** **Example:** `Router (config-gdoi-group)# server local`	Designates a device as a GDOI key server and enters GDOI local server configuration mode.
Step 6	**authorization address ipv4** {*access-list-name* | *access-list-number*} **Example:** `Router (gdoi-local-server)# authorization address ipv4 99`	(Optional) Specifies a list of addresses for a GDOI group.
Step 7	**rekey algorithm** {*type-of-encryption-algorithm*} **Example:** `Router (gdoi-local-server)# rekey algorithm 3des-cbc`	(Optional) Defines the type of encryption algorithm used for a GDOI group. • If this command is not configured, the default value of 3des-cbc takes effect.
Step 8	**rekey lifetime** {**seconds** *number-of-seconds*} **Example:** `Router (gdoi-local-server)# rekey lifetime seconds 300`	(Optional) Limits the number of seconds that any one encryption key should be used. • If this command is not configured, the default value of 86400 seconds takes effect.
Step 9	**rekey retransmit** {*number-of-seconds*} [**number** *number-of-retransmissions*] **Example:** `Router (gdoi-local-server)# rekey retransmit 10 number 3`	(Optional) Specifies the number of times the rekey message is retransmitted. • If this command is not configured, there will be no retransmits.

	Command or Action	Purpose
Step 10	**rekey authentication** {**mypubkey** | **pubkey**} {**rsa** *key-name*} **Example:** `Router (gdoi-local-server)# rekey authentication mypubkey rsa mykeys`	(Optional) Specifies the keys to be used for a rekey to GDOI group members. • This command is optional if rekeys are not required. If rekeys are required, this command is required.
Step 11	**rekey address ipv4** {*access-list-number* | *access-list-name*} **Example:** `Router (gdoi-local-server)# rekey address ipv4 101`	(Optional) Specifies the source or destination information of the rekey message. • If rekeys are not required, this command is optional. If rekeys are required, this command is required.
Step 12	**registration interface** *type slot*/*port* **Example:** `Router (gdoi-local-server)# registration interface Ethernet 0/0`	(Optional) Specifies the interface to be used for a GDOI registration.
Step 13	**sa ipsec** {*sequence-number*} **Example:** `Router (gdoi-local-server)# sa ipsec 1`	Specifies the IPsec security association (SA) policy information to be used for a GDOI group and enters GDOI SA IPsec configuration mode.
Step 14	**profile** {*ipsec-profile-name*} **Example:** `Router (gdoi-sa-ipsec)# profile gdoi-p`	Defines the IPsec SA policy for a GDOI group.
Step 15	**match address** {**ipv4** *access-list-number* | *access-list-name*} **Example:** `Router (gdoi-sa-ipsec)# match address ipv4 102`	Specifies an IP extended access list for a GDOI registration.
Step 16	**exit** **Example:** `Router (gdoi-sa-ipsec)# exit`	Exits GDOI SA IPsec configuration mode.
Step 17	**exit** **Example:** `Router (gdoi-local-server)# exit`	Exits GDOI local server configuration mode.
Step 18	**exit** **Example:** `Router (config-gdoi-group)# exit`	Exits GDOI group configuration mode.

Troubleshooting Tips

If **debug crypto gdoi** debugging is turned on, you may see "No Pubkey." This means that the Rivest, Shamir, and Adelman (RSA) keys were never generated.

What to Do Next

Configure group members (See "Configuring Group Members.")

Configuring Group Members

To configure group members, perform the following steps.

Prerequisites

Before configuring a group member, you must first configure IKE policy. For more information, see the reference to configuring IKE policy in the "Related Documents" subsection of the "Additional References" section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** {*group-name*}
4. **identity number** {*number*}

   or

   identity address ipv4 {*address*}
5. **server address ipv4** {*address*}
6. **exit**
7. **crypto map** *map-name seq-num* [**gdoi**]
8. **set group** {*group-name*}
9. **exit**
10. **exit**
11. **interface** *type slot/port*
12. **crypto map** *map-name*
13. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**crypto gdoi group** {*group-name*} **Example:** `Router (config)# crypto gdoi group groupname`	Identifies a GDOI group and enters GDOI group configuration mode.

Step 4	**identity number** {*number*}
	or
	identity address ipv4 {*address*}
	
	Example:
	`Router (config-gdoi-group)# identity number 3333`
	or
	`Router (config-gdoi-group)# identity address ipv4 10.2.2.2`
		Enters a GDOI group number or address.

Step 5	**server address ipv4** {*address*} **Example:** `Router (config-gdoi-group)# server address ipv4 10.0.5.2`	Specifies the address of the server a GDOI group is trying to reach. • To disable the address, use the **no** form of the command.
Step 6	**exit** **Example:** `Router (config-gdoi-group)# exit`	Exits GDOI group configuration mode.
Step 7	**crypto map** *map-name seq-num* [**gdoi**] **Example:** `Router (config)# crypto map testmap 10 gdoi`	Creates or modifies a GDOI crypto map entry and enters crypto map configuration mode. **Note** This new crypto map remains disabled until a valid group is configured.
Step 8	**set group** {*group-name*} **Example:** `Router (config-crypto-map)# set group gdoigroupname`	Sets the GDOI crypto map to the GDOI group that has already been defined.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Router (config-crypto-map)# exit`	Exits crypto map configuration mode.
Step 10	**exit** **Example:** `Router (config-gdoi-group)# exit`	Exits GDOI group configuration mode.
Step 11	**interface** *type slot/port* **Example:** `Router (config)# interface Ethernet 0/0`	Configures an interface type and enters interface configuration mode.
Step 12	**crypto map** *map-name* **Example:** `Router (config-if)# crypto map testmap`	Applies a previously defined crypto map set to an interface.
Step 13	**exit** **Example:** `Router (config-if)# exit`	Exits interface configuration mode.

Clearing a Group Member Registration with a Key Server

To clear a group member registration with a key server, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear crypto gdoi**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear crypto gdoi** **Example:** `Router# clear crypto gdoi`	Clears current group member registration with the key server and starts a new registration. • All current group-member policy is deleted. A new registration is started.

Verifying Secure Multicast

To verify your Secure Multicast configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto gdoi**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto gdoi** **Example:** `Router# show crypto gdoi`	Displays information about a GDOI configuration.

Configuration Examples for Secure Multicast

This section provides the following configuration examples:

- Key Server: Example, page 14
- Group Member: Example, page 15

Key Server: Example

The following example shows information about a key server:

```
Router# show running config

Building configuration...

Current configuration : 2669 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
```

```
!
resource policy
!
clock timezone PST 0
ip subnet-zero
no ip routing
!
!
crypto isakmp policy 1
authentication pre-share
crypto isakmp key key1 address 10.0.3.1
crypto isakmp key key1 address 10.0.3.2
crypto isakmp key key1 address 10.0.4.2
!
!
crypto ipsec transform-set gdoi-p esp-3des esp-sha-hmac
!
crypto ipsec profile gdoi-p
 set security-association lifetime seconds 3600  set transform-set gdoi-p
!
crypto gdoi group gdoigroupname
 identity number 3333
 server local
  rekey address ipv4 102
  rekey lifetime seconds 36000
  ! Create a RSA key with "crypto key gen rsa gen label mykeys" before configuring the
following command.
  rekey authentication mypubkey rsa mykeys
  sa ipsec 1
   profile gdoi-p
   match address ipv4 101
!
interface Ethernet0/0
 ip address 10.0.5.2 255.0.0.0
 no ip route-cache
!
! The following is a list of access controls to be downloaded from the key server to the
group members. It tells them which traffic will be encrypted.
access-list 101 permit ip host 10.0.1.2 host 239.251.5.1
access-list 101 permit ip host 10.0.1.2 239.251.7.0 0.0.0.255
access-list 101 permit ip 10.0.1.0 0.0.0.255 239.251.6.0 0.0.0.255
! The following access control list determines to which multicast addresses the rekeys are
to be sent.
access-list 102 permit udp host 10.0.5.2 eq 848 host 239.251.1.2 eq 848
```

Group Member: Example

The following output example shows information about a GDOI group member:

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
```

```
resource policy
!
clock timezone PST -8
ip subnet-zero
!
!
ip multicast-routing
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key key1 address 10.0.5.2
!
crypto gdoi group diffint
 identity number 3333
 server address ipv4 10.0.5.2
!
!
crypto map diffint 10 gdoi
 set group diffint
!
!
interface Loopback0
 ip address 10.65.9.2 255.255.255.255
 ip pim sparse-dense-mode
!
interface Ethernet0/0
 ip address 10.0.3.2 255.255.255.0
 ip mtu 1000
 ip pim sparse-dense-mode
 no ip route-cache
 crypto map diffint
!
interface Ethernet1/0
 ip address 10.0.1.1 255.255.255.0
 ip pim sparse-dense-mode
 no ip route-cache
!
router eigrp 10
 network 10.0.0.0
 auto-summary
 no eigrp log-neighbor-changes
!
!
ip classless
no ip http server
no ip http secure-server
!
ip pim bidir-enable
ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery scope 16
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Additional References

The following sections provide references related to Secure Multicast.

Related Documents

Related Topic	Document Title
Cisco IOS commands (listed in an index)	*Cisco IOS Master Commands List*, Release 12.4
Cisco IOS security commands	*Cisco IOS Security Command Reference*, Release 12.4T
Configuring IKE and IKE policy	"Configuring Internet Key Exchange for IPSec VPNs" section of the *Cisco IOS Security Configuration Guide*, Release 12.4.
Configuring an IPsec transform	"Configuring Security for VPNs with IPSec" section of the *Cisco IOS Security Configuration Guide*, Release 12.4.

Standards

Standard	Title
No new or modified standards are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3547	The Group Domain of Interpretation

Technical Assistance

Description	Link
The Cisco Technical Support Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

New Commands

- **authorization address ipv4**
- **clear crypto gdoi**
- **crypto gdoi group**
- **debug crypto gdoi**
- **identity address ipv4**
- **identity number**
- **match address (GDOI local server)**
- **profile (GDOI local server)**
- **registration interface**
- **rekey address ipv4**
- **rekey algorithm**
- **rekey authentication**
- **rekey lifetime**
- **rekey retransmit**
- **sa ipsec**
- **server address ipv4**
- **server local**
- **set group**
- **show crypto gdoi**

Modified Commands

- **crypto map (global IPSec)**

authorization address ipv4

To specify a list of addresses for a Group Domain of Interpretation (GDOI) group, use the **authorization address ipv4** command in GDOI local server configuration mode. To remove an address from the group, use the **no** form of this command.

authorization address ipv4 {*access- list-name* | *access-list number*}

no authorization address ipv4 {*access- list-name* | *access-list number*}

Syntax Description

access-list-name	A hostname or distinguished name (DN).
access-list number	Standard IP access list number. Value: 1 through 99

Command Default

A list of addresses is not specified.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If the identity of the Internet Key Exchange (IKE) authentication matches an entry in the access control list, the address is authorized.

Examples

The following example shows that access list number 99 has been specified to be part of a GDOI group:

```
authorization address ipv4 99
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

clear crypto gdoi

To clear the current registration of a Group Domain of Interpretation (GDOI) group member with the key server, use the **clear crypto gdoi** command in privileged EXEC mode.

clear crypto gdoi

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If this command is issued on the group member, the policy of the group member is deleted, and the group member reregisters with the key server

If this command is issued on the key server, the policy of the key server is deleted.

Examples

The following example shows that current group member registration is to be cleared:

```
clear crypto gdoi
```

crypto gdoi group

To identify a Group Domain of Interpretation (GDOI) group and enter GDOI group configuration mode, use the **crypto gdoi group** command in global configuration mode. To disable a GDOI group, use the **no** form of this command.

crypto gdoi group {*group-name*}

no crypto gdoi group {*group-name*}

Syntax Description

group-name	Name of the group. The group name is limited to 80 characters.

Command Default

A GDOI group is not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

There are more options for configuring a group on a key server than there are for configuring a group member. The group is identified by an identity and by the server. If the crypto GDOI group is a group member, the address of the server is specified. If the crypto GDOI group is a key server, "server local" is specified, which indicates that this is the key server.

Examples

The following example shows how to configure a GDOI group for a key server:

```
crypto gdoi group gdoigroupname
 identity number 4444
 server local
```

The following example shows how to configure a GDOI group for a group member:

```
crypto gdoi group gdoigroupname
 identity number 3333
 server address ipv4 10.0.5.2
```

crypto map (global IPSec)

To enter crypto map configuration mode and create or modify a crypto map entry, to create a crypto profile that provides a template for configuration of dynamically created crypto maps, or to configure a client accounting list, use the **crypto map** command in global configuration mode. To delete a crypto map entry, profile, or set, use the **no** form of this command.

crypto map *map-name seq-num* [**ipsec-manual**]

crypto map *map-name seq-num* [**ipsec-isakmp**] [**dynamic** *dynamic-map-name*] [**discover**] [**profile** *profile-name*]

crypto map *map-name* [**client-accounting-list** *aaalist*]

crypto map *map-name seq-num* [**gdoi**]

no crypto map *map-name seq-num*

Note Issue the **crypto map** *map-name seq-num* command without a keyword to modify an existing crypto map entry.

Syntax Description

map-name	Name that identifies the crypto map set. This is the name assigned when the crypto map was created.
seq-num	Sequence number you assign to the crypto map entry. See additional explanation for using this argument in the "Usage Guidelines" section.
ipsec-manual	(Optional) Indicates that Internet Key Exchange (IKE) will not be used to establish the IP Security (IPSec) security associations (SAs) for protecting the traffic specified by this crypto map entry.
ipsec-isakmp	(Optional) Indicates that IKE will be used to establish the IPSec SAs for protecting the traffic specified by this crypto map entry.
dynamic	(Optional) Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. If you use this keyword, none of the crypto map configuration commands will be available.
dynamic-map-name	(Optional) Specifies the name of the dynamic crypto map set that should be used as the policy template.
discover	(Optional) Enables peer discovery. By default, peer discovery is not enabled.
profile	(Optional) Designates a crypto map as a configuration template. The security configurations of this crypto map will be cloned as new crypto maps are created dynamically on demand.
profile-name	(Optional) Name of the crypto profile being created.
client-accounting-list	(Optional) Designates a client accounting list.
aaalist	(Optional) List name.
gdoi	(Optional) Indicates that the key management mechanism is Group Domain of Interpretation (GDOI).

Defaults

No crypto maps exist.

Peer discovery is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3 T	The following keywords and arguments were added: • **ipsec-manual** • **ipsec-isakmp** • **dynamic** • *dynamic-map-name*
12.0(5)T	The **discover** keyword was added to support Tunnel Endpoint Discovery (TED).
12.2(4)T	The **profile** *profile-name* keyword and argument combination was introduced to allow the generation of a crypto map profile that is cloned to create dynamically created crypto maps on demand.
12.2(11)T	Support was added for the Cisco 1760, Cisco AS5300, Cisco AS5400, and Cisco AS5800 platforms.
12.2(15)T	The **client-accounting-list** keyword and *aaalist* argument were added.
12.4(6)T	The **gdoi** keyword was added.

Usage Guidelines

Use this command to create a new crypto map entry, to create a crypto map profile, or to modify an existing crypto map entry or profile.

After a crypto map entry has been created, you cannot change the parameters specified at the global configuration level because these parameters determine which of the configuration commands are valid at the crypto map level. For example, after a map entry has been created using the **ipsec-isakmp** keyword, you cannot change it to the option specified by the **ipsec-manual** keyword; you must delete and reenter the map entry.

After you define crypto map entries, you can assign the crypto map set to interfaces using the **crypto map** (interface IPSec) command.

Crypto Map Functions

Crypto maps provide two functions: filtering and classifying traffic to be protected and defining the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed (via IKE) on behalf of that traffic.

IPSec crypto maps define the following:

- What traffic should be protected
- To which IPSec peers the protected traffic can be forwarded—these are the peers with which an SA can be established
- Which transform sets are acceptable for use with the protected traffic

- How keys and security associations should be used or managed (or what the keys are, if IKE is not used)

Multiple Crypto Map Entries with the Same Map Name Form a Crypto Map Set

A crypto map set is a collection of crypto map entries, each with a different *seq-num* argument but the same *map-name* argument. Therefore, for a given interface, you could have certain traffic forwarded to one IPSec peer with specified security applied to that traffic and other traffic forwarded to the same or a different IPSec peer with different IPSec security applied. To accomplish differential forwarding you would create two crypto maps, each with the same *map-name* argument, but each with a different *seq-num* argument. Crypto profiles must have unique names within a crypto map set.

Sequence Numbers

The number you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower *seq-num* is evaluated before a map entry with a higher *seq-num*; that is, the map entry with the lower number has a higher priority.

For example, consider a crypto map set that contains three crypto map entries: mymap 10, mymap 20, and mymap 30. The crypto map set named "mymap" is applied to serial interface 0. When traffic passes through serial interface 0, the traffic is evaluated first for mymap 10. If the traffic matches any access list permit statement entry in the extended access list in mymap 10, the traffic will be processed according to the information defined in mymap 10 (including establishing IPSec SAs when necessary). If the traffic does not match the mymap 10 access list, the traffic will be evaluated for mymap 20, and then mymap 30, until the traffic matches a permit entry in a map entry. (If the traffic does not match a permit entry in any crypto map entry, it will be forwarded without any IPSec security.)

Dynamic Crypto Maps

Refer to the "Usage Guidelines" section of the **crypto dynamic-map** command for a discussion on dynamic crypto maps.

Crypto map entries that reference dynamic map sets should be the lowest priority map entries, allowing inbound SA negotiation requests to try to match the static maps first. Only after the request does not match any of the static maps, do you want it to be evaluated against the dynamic map set.

To make a crypto map entry referencing a dynamic crypto map set the lowest priority map entry, give the map entry the highest *seq-num* of all the map entries in a crypto map set.

Create dynamic crypto map entries using the **crypto dynamic-map** command. After you create a dynamic crypto map set, add the dynamic crypto map set to a static crypto map set with the **crypto map** (global IPSec) command using the **dynamic** keyword.

TED

TED is an enhancement to the IPSec feature. Defining a dynamic crypto map allows you to dynamically determine an IPSec peer; however, only the receiving router has this ability. With TED, the initiating router can dynamically determine an IPSec peer for secure IPSec communications.

Dynamic TED helps to simplify IPSec configuration on the individual routers within a large network. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms that are required.

Note TED helps only in discovering peers; otherwise, TED does not function any differently from normal IPSec. Thus, TED does not improve the scalability of IPSec (in terms of performance or the number of peers or tunnels).

Crypto Map Profiles

Crypto map profiles are created using the **profile** *profile-name* keyword and argument combination. Crypto map profiles are used as configuration templates for dynamically creating crypto maps on demand for use with the Layer 2 Transport Protocol (L2TP) Security feature. The relevant SAs the crypto map profile will be cloned and used to protect IP traffic on the L2TP tunnel.

Note The **set peer** and **match address** commands are ignored by crypto profiles and should not be configured in the crypto map definition.

Examples

The following example shows the minimum required crypto map configuration when IKE will be used to establish the SAs:

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
```

The following example shows the minimum required crypto map configuration when the SAs are manually established:

```
crypto transform-set someset ah-md5-hmac esp-des
crypto map mymap 10 ipsec-manual
 match address 102
 set transform-set someset
 set peer 10.0.0.5
 set session-key inbound ah 256 9876543210987654987654321098765 4
 set session-key outbound ah 256 fedcbafedcbafedcfedcbafedcbafedc
 set session-key inbound esp 256 cipher 0123456789012345
 set session-key outbound esp 256 cipher abcdefabcdefabcd
```

The following example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows SAs to be established between the router and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the remote peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” which can be used to process inbound SA negotiation requests that do not match “mymap” entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in “mydynamicmap,” for a flow permitted by the access list 103, IPSec will accept the request and set up SAs with the remote peer without previously knowing about the remote peer. If the request is accepted, the resulting SAs (and temporary crypto map entry) are established according to the settings specified by the remote peer.

The access list associated with “mydynamicmap 10” is also used as a filter. Inbound packets that match any access list permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists associated with static crypto maps entries.) Outbound packets that match a permit statement without an existing corresponding IPSec SA are also dropped.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
```

```
crypto map mymap 20 ipsec-isakmp
 match address 102
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.3
crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
!
crypto dynamic-map mydynamicmap 10
 match address 103
 set transform-set my_t_set1 my_t_set2 my_t_set3
```

The following example configures TED on a Cisco router:

```
crypto map testtag 10 ipsec-isakmp dynamic dmap discover
```

The following example configures a crypto profile to be used as a template for dynamically created crypto maps when IPSec is used to protect an L2TP tunnel:

```
crypto map l2tpsec 10 ipsec-isakmp profile l2tp
```

The following example configures a crypto map for a GDOI group member:

```
crypto map diffint 10 gdoi
 set group diffint
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto isakmp profile	Audits IPSec user sessions.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
debug crypto isakmp	Applies a previously defined crypto map set to an interface.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new SAs for this crypto map entry, or that IPSec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate IPSec SAs should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec SAs.
set session-key	Specifies the IPSec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

debug crypto gdoi

To display information about a Group Domain of Interpretation (GDOI) configuration, use the **debug crypto gdoi** command in privileged EXEC mode. To disable crypto gdoi debugging, use the **no** form of this command.

debug crypto gdoi

no debug crypto gdoi

Syntax Description

This command has no arguments or keywords.

Command Default

Debugging is turned off.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Using this command displays various GDOI debugs.

Examples

The following example shows group member registration debug output:

```
00:00:40: GDOI:(0:0:N/A:0):GDOI group diffint
00:00:40: %CRYPTO-5-GM_REGSTER: Start registration for group diffint using address
10.0.3.1
00:00:40: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
00:00:40: GDOI:(0:1001:HW:0:3333):beginning GDOI exchange, M-ID of 1167145075
00:00:40: GDOI: Group Number is 3333
00:00:40: GDOI:(0:1001:HW:0:3333):GDOI: GDOI ID sent successfully
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI SA Payload, message ID + 1167145075
00:00:40: GDOI:(0:1001:HW:0):processing GDOI SA KEK Payload
00:00:40: GDOI:(0:0:N/A:0):    KEK_ALGORITHM 5
00:00:40: GDOI:(0:0:N/A:0):    KEY_LENGTH 24
00:00:40: GDOI:(0:0:N/A:0):    KEY_LIFETIME 299
00:00:40: GDOI:(0:0:N/A:0):    SIG_HASH_ALG 2
00:00:40: GDOI:(0:0:N/A:0):    SIG_ALG 1
00:00:40: GDOI:(0:0:N/A:0):    SIG_KEY_LEN 94
00:00:40: GDOI:(0:0:N/A:0): Completed KEK Processing
00:00:40: GDOI:(0:1001:HW:0):processing GDOI SA TEK Payload
00:00:40: GDOI:(0:1001:HW:0:3333): Completed TEK Processing
00:00:40: GDOI:(0:1001:HW:0):processing GDOI SA TEK Payload
00:00:40: GDOI:(0:1001:HW:0:3333): Completed TEK Processing
00:00:40: GDOI:(0:1001:HW:0:3333):GDOI ACK sent successfully by GM
00:00:40: GDOI:received payload type 18
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI Seq Payload, message_id  1167145075
00:00:40: GDOI:(0:1001:HW:0:3333):Completed SEQ Processing for seq 0
00:00:40: GDOI:received payload type 17
```

```
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI KD Payload, message_id  1167145075
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI Key Packet, message_id  38649336
00:00:40: GDOI:(0:1001:HW:0:3333):procesing TEK KD: spi is 56165461, spi
00:00:40: GDOI:(0:1001:HW:0:3333):TEK Integrity Key 20 bytes
00:00:40: GDOI:(0:1001:HW:0:3333):Completed KeyPkt Processing
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI Key Packet, message_id  38649336
00:00:40: GDOI:(0:1001:HW:0:3333):procesing TEK KD: spi is 56165522, spi
00:00:40: GDOI:(0:1001:HW:0:3333):TEK Integrity Key 20 bytes
00:00:40: GDOI:(0:1001:HW:0:3333):Completed KeyPkt Processing
00:00:40: GDOI:(0:1001:HW:0:3333):processing GDOI Key Packet, message_id  38649336
00:00:40: GDOI:(0:1001:HW:0:3333): Processing KEK KD
00:00:40: GDOI:(0:1001:HW:0:3333):KEK Alg Key 32 bytes
00:00:40: GDOI:(0:1001:HW:0:3333):KEK Sig Key 94 bytes
00:00:40: GDOI:(0:1001:HW:0:3333):Completed KeyPkt Processing
00:00:40: %GDOI-5-GM_REGS_COMPL: Registration complete for group diffint using address
10.0.3.1

enc(config-if)#
00:00:40: GDOI:(0:0:N/A:0):Registration installed 2 new ipsec SA(s) for group diffint.
```

The following output example shows key server registration debugs:

```
00:00:40: GDOI:(0:1001:HW:0):processing GDOI ID payload, message ID = 1167145075
00:00:40: GDOI:(0:1001:HW:0):The GDOI ID is a Number: 3333
00:00:40: GDOI:(0:0:N/A:0): Adding KEK Policy to the current ks_group
00:00:40: GDOI:(0:0:N/A:0):Setting MULTICAST TEK rekey lifetime 30
00:00:40: GDOI:(0:0:N/A:0):Setting MULTICAST TEK rekey lifetime 30
00:00:40: GDOI:(0:1001:HW:0:3333):GDOI SA sent successfully by KS
00:00:40: GDOI:(0:1001:HW:0:3333):GDOI KD sent successfully by KS
```

The following output example shows group member rekey debugs:

```
00:02:00: GDOI:(0:1002:HW:0):Received Rekey Message!
00:02:00: GDOI:(0:1002:HW:0):Signature Valid!
00:02:00: GDOI:received payload type 18
00:02:00: GDOI:(0:1002:HW:0):processing GDOI Seq Payload, message_id  0
00:02:00: GDOI:(0:1002:HW:0):Completed SEQ Processing for seq 8
00:02:00: GDOI:(0:1002:HW:0):processing GDOI SA Payload, message ID + 0
00:02:00: GDOI:(0:1002:HW:0):processing GDOI SA KEK Payload
00:02:00: GDOI:(0:1002:HW:0):    KEK_ALGORITHM 5
00:02:00: GDOI:(0:1002:HW:0):    KEY_LENGTH 24
00:02:00: GDOI:(0:1002:HW:0):    KEY_LIFETIME 219
00:02:00: GDOI:(0:1002:HW:0):    SIG_HASH_ALG 2
00:02:00: GDOI:(0:1002:HW:0):    SIG_ALG 1
00:02:00: GDOI:(0:1002:HW:0): Completed KEK Processing
00:02:00: GDOI:(0:1002:HW:0):processing GDOI SA TEK Payload
00:02:00: GDOI:(0:1002:HW:0): Completed TEK Processing
00:02:00: GDOI:(0:1002:HW:0):processing GDOI SA TEK Payload
00:02:00: GDOI:(0:1002:HW:0): Completed TEK Processing
00:02:00: GDOI:received payload type 17
00:02:00: GDOI:(0:1002:HW:0):processing GDOI KD Payload, message_id  0
00:02:00: GDOI:(0:1002:HW:0):processing GDOI Key Packet, message_id  38649336
00:02:00: GDOI:(0:1002:HW:0):procesing TEK KD: spi is 49193284, spi
00:02:00: GDOI:(0:1002:HW:0):TEK Integrity Key 20 bytes
00:02:00: GDOI:(0:1002:HW:0):Completed KeyPkt Processing
enc(config-if)#
00:02:00: GDOI:(0:1002:HW:0):processing GDOI Key Packet, message_id  38649336
00:02:00: GDOI:(0:1002:HW:0):procesing TEK KD: spi is 49193345, spi
00:02:00: GDOI:(0:1002:HW:0):TEK Integrity Key 20 bytes
00:02:00: GDOI:(0:1002:HW:0):Completed KeyPkt Processing
00:02:00: GDOI:(0:1002:HW:0):processing GDOI Key Packet, message_id  38649336
00:02:00: GDOI:(0:1002:HW:0): Processing KEK KD
00:02:00: GDOI:(0:1002:HW:0):Completed KeyPkt Processing
```

identity address ipv4

To identify a Group Domain of Interpretation (GDOI) group address, use the **identity address ipv4** command in GDOI group configuration mode. To remove the group address, use the **no** form of this command.

identity address ipv4 {*address*}

no identity address ipv4 {*address*}

Syntax Description

address	IP address of the group.

Command Default

A group address is not identified.

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command or the **identity number** command is required for a GDOI configuration.

Examples

The following example shows that the identity address is 10.2.2.2:

```
identity address ipv4 10.2.2.2
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group.
identity number	Identifies a GDOI group number.

identity number

To identify a Group Domain of Interpretation (GDOI) group number, use the **identity number** command in GDOI group configuration mode. To remove the group number, use the **no** form of this command.

identity number {*number*}

no identity number {*number*}

Syntax Description

number	Number of the group.

Command Default

A GDOI group number is not identified.

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command or the **identity address ipv4** command is required for a GDOI configuration.

Examples

The following example shows the group number is 3333:

```
identity number 3333
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
identity address ipv4	Identifies a GDOI group address.

match address (GDOI local server)

To specify an IP extended access list for a Group Domain of Interpretation (GDOI) registration, use the **match address** command in GDOI SA IPsec configuration mode. To disable the access list, use the **no** form of this command.

match address {**ipv4** *access-list-number* | *access-list-name*}

no match address {**ipv4** *access-list-number* | *access-list-name*}

Syntax Description

ipv4	Specifies that IPv4 packets should be matched.
access-list-number | *access-list-name*	Access list number or name. This value should match the access-list number or name of the extended access list that is being matched. The range is 100 through 199 or 2000 through 2699 for an expanded range.

Command Default

No access lists are matched to the GDOI entry.

Command Modes

GDOI SA IPsec configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example shows that the IP extended access list is 102:

```
match address ipv4 102
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

profile (GDOI local server)

To define the IP security (IPsec) security association (SA) policy for a Group Domain of Interpretation (GDOI) group, use the **profile** command in GDOI SA IPsec configuration mode. To disable the IPsec SA policy that was defined, use the **no** form of this command.

profile {*ipsec-profile-name*}

no profile {*ipsec-profile-name*}

Syntax Description

ipsec-profile-name	Name of the IPsec profile.

Command Default

An IPsec SA policy is not defined for the GDOI group.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example shows that the IPsec SA policy has been defined as "group1234":

```
profile group1234
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

registration interface

To specify the interface to be used for a Group Domain of Interpretation (GDOI) registration, use the **registration interface** command in GDOI local server configuration mode. To disable an interface, use the **no** form of this command.

registration interface *type slot/port*

no registration interface *type slot/port*

Syntax Description

type	Type of interface (see Table 1 below).
slot/port	Slot and port number of the interface.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Table 1 lists the types of interface that may be used for the *type* argument.

Table 1 Type of Interface

Interface	Description
Async	Async interface
BVI	Bridge-Group Virtual Interface
CDMA-1x	Code division multiple access 1x interface
CTunnel	CTunnel interface
Dialer	Dialer interface
Ethernet	Institute of Electrical and Electronics Engineers (IEEE) Standard 802.3
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink group interface
Null	Null interface
Serial	Serial
Tunnel	Tunnel interface

Table 1 Type of Interface (Continued)

Interface	Description
Vif	Pragmatic General Multicast (PGM) Multicast Host interface
Virtual-PPP	Virtual PPP interface
Virtual-Template	Virtual Template interface
Virtual-TokenRing	Virtual TokenRing

Examples

The following example shows that the interface is Ethernet 0/0:

```
registration interface Ethernet 0/0
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey address ipv4

To specify the source or destination information of the rekey message, use the **rekey address ipv4** command in GDOI local server configuration mode. To remove a source or destination address, use the **no** form of this command.

rekey address ipv4 {*access-list-number* | *access-list-name*}

no rekey address ipv4 {*access-list-number* | *access-list-name*}

Syntax Description

access-list-number	IP access list number. The number can be from 100 through 199, or it can be in the expanded range of 2000 through 2699.
access-list-name	Access list name.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

The source is usually the key server interface from which the message leaves, and the destination is the multicast address on which the group members receive the rekeys. For example:

```
access-list 101 permit 121 permit udp host 10.0.5.2 eq 848 host 192.168.1.2. eq 848
```

Examples

The following example shows that the rekey address is access list “101”:

```
rekey address ipv4 101
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.

rekey algorithm

To define the type of encryption algorithm used for a Group Domain of Interpretation (GDOI) group, use the **rekey algorithm** command in GDOI local server configuration mode. To disable an algorithm that was defined, use the **no** form of this command.

rekey algorithm {*type-of-encryption-algorithm*}

no rekey algorithm {*type-of-encryption-algorithm*}

Syntax Description

type-of-encryption-algorithm	Type of encryption algorithm used (see Table 2). The default algorithm is 3des-cbc. • The rekey algorithm is used to encrypt the rekey message that is sent from the key server to the multicast group.

Command Default

If this command is not configured, the default value of 3des-cbc takes effect. However, the default is used only if the commands required for a rekey to occur are specified (see the Note below in "Usage Guidelines").

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Table 1 lists the types of encryption algorithms that may be used.

Table 2 Types of Encryption

Encryption Type	Description
3des-cbc	Cipher Block Chaining mode of the Triple Data Encryption Standard (3des).
aes 128	128-bit Advanced Encrytion Standard (AES).
aes 192	192-bit AES.
aes 256	256-bit AES.
des-cbc	Cipher Block Chaining mode of the Data Encryption Standard (des).

Note At a minimum, the following commands are required for a rekey to occur:

rekey address ipv4 {*access-list-number* | *access-list-name*}

rekey authentication {**mypubkey** | **pubkey**} {*rsa key-name*}

If the **rekey algorithm** command is not configured, the default of 3des-cbc is used if the above minimum rekey configuration is met.

Examples

The following example shows that the 3des-cbc encryption standard is used:

```
rekey algorithm 3des-cbc
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
rekey address ipv4	Specifies the source or destination information of the rekey message.
rekey authentication	Specifies the keys to be used to a rekey to GDOI group members.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey authentication

To specify the keys to be used for a rekey to Group Domain of Interpretation (GDOI) group members, use the **rekey authentication** command in GDOI local server configuration mode. To disable the keys, use the **no** form of this command.

rekey authentication {**mypubkey** | **pubkey**} {**rsa** *key-name*}

no rekey authentication {**mypubkey** | **pubkey**} {**rsa** *key-name*}

Syntax Description

mypubkey	Keypair associated with this device.
pubkey	Public key associated with a different device.
rsa	Identifies an Rivest, Shamir, and Adelman (RSA) keypair.
key-name	Key to be used for rekey.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

If rekeys are not required, this command is optional. If rekeys are required, this command is required.

For this command to work, Rivest, Shamir, and Adelman (RSA) keys must be generated first on the router using the following command:

crypto key generate rsa {**general keys**} [**label** *key-label*]

For example:

```
crypto key generate rsa general keys label group_1234_key_name
```

Examples

The following example shows that the keypair to be used for a rekey is RSA “group_1234_key_name”:

```
rekey authentication mypubkey rsa group_1234_key_name
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration.
crypto key generate rsa	Generates RSA key pairs.

rekey lifetime

To limit the number of seconds for which any one encryption key should be used, use the **rekey lifetime** command in GDOI local server configuration mode. To disable the number of seconds that were set, use the **no** form of this command.

rekey lifetime {**seconds** *number-of-seconds*}

no rekey lifetime {**seconds** *number-of-seconds*}

Syntax Description

number-of-seconds	Lifetime in seconds. Value: 300 through 86400 seconds.

Command Default

If this command is not configured, the default value of 86400 seconds takes effect.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This **rekey** command is not used often. When this rekey limit is sent, a new key encryption key is sent to the group member so that the next rekey after this one will be encrypted with the new key encryption key.

Examples

The following example shows that the rekey lifetime has been set to 600 seconds:

```
rekey lifetime seconds 600
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

rekey retransmit

To specify the number of times the rekey message is retransmitted, use the **rekey retransmit** command in GDOI local server configuration mode. To disable the number of times that were specified, use the **no** form of this command.

rekey retransmit {*number-of-seconds*} [**number** *number-of-retransmissions*]

no rekey retransmit {*number-of-seconds*} [**number** *number-of-retransmissions*]

Syntax Description

number-of-seconds	Number of seconds that the rekey message is retransmitted. Range: 10 through 60. Default=10.
number *number-of-retransmissions*	Number of times the message may be retransmitted. Range: 1 through 10. Default: 2.

Command Default

If this command is not configured, the number of seconds defaults to 10 and the number of transmissions defaults to 2.

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use this command if you are concerned about network loss. Using this command ensures that the rekey message is resent the number of times specified in the retransmit command.

Examples

The following example shows that the rekey message may be retransmitted twice for 15 seconds each time:

```
rekey retransmit 15 number 2
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

sa ipsec

To specify the IP security (IPsec) security association (SA) policy information to be used for a Group Domain of Interpretation (GDOI) group and to enter GDOI SA IPsec configuration mode, use the **sa ipsec** command in GDOI local server configuration mode. To remove the policy information that was specified, use the **no** form of this command.

sa ipsec {*sequence-number*}

no sa ipsec {*sequence-number*}

Syntax Description

sequence-number	Sequence number of the IPsec SA.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

IPsec and SA policy information must be specified using this command if the traffic encryption key policy has to be defined.

Examples

The following example shows that three IPsec SA policy numbers (1, 2, and 3) have been specified:

```
sa ipsec 1
  profile gdoi-p
  match address ipv4 120
sa ipsec 2
  profile gdoi-q
  match address ipv4 121
sa ipsec 3
  profile gdoi-r
  match address ipv4 122
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
match address	Specifies an IP extended access list for a GDOI registration.
profile	Defines the IPsec SA policy for a GDOI group.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

server address ipv4

To specify the address of the server that a Group Domain of Interpretation (GDOI) group is trying to reach, use the **server address ipv4** command in GDOI group configuration mode. To disable the address, use the **no** form of this command.

server address ipv4 {*address* | *hostname*}

no server address ipv4 {*address* | *hostname*}

Syntax Description

address	IP address of the server.
hostname	Hostname of the server.

Command Default

None

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **server address ipv4** command can be used only on a group member. This command must be specified or the group configuration on the group member is not complete.

Examples

The following example shows that the GDOI group is trying to reach the server with the IP address "10.34.255.57":

```
server address ipv4 10.34.255.57
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

server local

To designate a device as a Group Domain of Interpretation (GDOI) key server and enter GDOI local server configuration mode, use the **server local** command in GDOI group configuration mode. To remove a device as a key server, use the **no** form of this command.

server local

no server local

Syntax Description

This command has no arguments or keywords.

Command Default

A device is not designated as a GDOI key server.

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used on the key server to specify the key server policy that will be downloaded to the group members that are registered with the key server.

Examples

The following example shows that the device has been designated as a GDOI key server:

```
server local
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.

set group

To set the Group Domain of Interpretation (GDOI) crypto map to the GDOI group that has already been defined, use the **set group** command in crypto map configuration mode. To remove the GDOI crypto map, use the **no** form of this command.

set group {*group-name*}

no set group {*group-name*}

Syntax Description

group-name	Name of the GDOI group.

Command Default

None

Command Modes

crypto map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command must be configured for the GDOI crypto map to be complete.

Note This crypto map is specifically a GDOI crypto map, that is, the crypto map must be named as a GDOI crypto map, as in this example: **crypto map test 10 gdoi**

Examples

The following example shows that the group name is "hsrp-group":

```
set group hsrp-group
```

Related Commands

Command	Description
crypto map	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, indicates that the key management mechanism is GDOI, or configures a client accounting list.

show crypto gdoi

To display information about a Group Domain of Interpretation (GDOI) configuration, use the **show crypto gdoi** command in privileged EXEC mode.

show crypto gdoi

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following output displays information about a configuration for a GDOI group member:

```
Router# show crypto gdoi

Group Information
   Group Name                : diffint
   Group Identity            : 3333
   Group Members Registered  : 0
   Group Server              : 10.0.5.2


   Group Name                : test
   Group Identity            : 4444
   Group Members Registered  : 0
   Group Server              : 10.0.5.2
```

The following output displays information about a configuration for a GDOI key server:

```
Router# show crypto gdoi

Group Information
   Group Name                : diffint
   Group Identity            : 3333
   Group Members Registered  : 1
   Group Server              : Local
   Group Rekey Lifetime      : 300 secs
   Group Rekey
       Remaining Lifetime    : 84 secs
   IPSec SA Number           : 1
     IPSec SA Rekey Lifetime : 120 secs
     Profile Name            : gdoi-p
   SA Rekey
       Remaining Lifetime    : 64 secs
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1

   Group Member List for Group diffint :
   Member ID                 : 10.0.3.1
```

```
Group Name                  : test
Group Identity              : 4444
Group Members Registered    : 0
Group Server                : Local
Group Rekey Lifetime        : 600 secs
IPSec SA Number             : 1
  IPSec SA Rekey Lifetime   : 120 secs
  Profile Name              : gdoi-p
access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
access-list 120 permit ip host 10.0.100.2 host 192.168.1.1
```

The fields in the above displays are self-explanatory.

Glossary

DOI—Domain of Interpretation. For Internet Security Association Key Management Protocol (ISAKMP), a value in the security association (SA) payload that describes in which context the key management message is being sent (IPsec or Group Domain of Interpretation).

GDOI—Group Domain of Interpretation. For ISAKMP, a means of distributing and managing keys for groups of mutually trusted systems.

group member—Device (Cisco IOS router) that registers with a group that is controlled by the key server for purposes of communicating with other group members.

group security association—SA that is shared by all group members in a group.

IPsec—IP security. Data encryption protocol for IP packets that are defined in a set of RFCs (see IETF RFC 2401).

ISAKMP—Internet Security Association and Key Management Protocol. Protocol that provides a framework for cryptographic key management protocols.

key encryption key. Key used to protect the rekey between the key server and group members.

key server—A device (Cisco IOS router) that distributes keys and policies to group members.

SA—security association. SA that is shared by all group members in a group.

traffic encryption key. Key that is used to protect the rekey between group members.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.

Feature Information for Secure Multicast

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for Secure Multicast

Feature Name	Releases	Feature Information
Secure Multicast	12.4(6)T	The Secure Multicast feature provides a secure means of distributing and managing IP security (IPsec) keys for groups of mutually trusted systems. The following commands were introduced or modified by this feature: authorization address ipv4, clear crypto gdoi, crypto map (global IPsec), debug crypto gdoi, identity address ipv4, identity number, match address (GDOI local server), registration interface, rekey address ipv4, rekey algorithm, rekey authentication, rekey lifetime, rekey retransmit, sa ipsec, server address ipv4, server local, set group, and show crypto gdoi.