IPv6 over IPv4 GRE Tunnel Protection

The IPv6 over IPv4 GRE Tunnel Protection feature allows both IPv6 unicast and multicast traffic to pass through a protected generic routing encapsulation (GRE) tunnel.

Prerequisites for IPv6 over IPv4 GRE Tunnel Protection

- To enable this feature, you must configure IPsec tunnel protection on an IPv4 GRE tunnel.
- To enable IPv6 multicast, you must configure IPv6 multicast routing.

Restrictions for IPv6 over IPv4 GRE Tunnel Protection

The IPv6 over IPv4 GRE Tunnel Protection feature supports IPv6 over IPv4 point-to-point GRE tunnel protection and not IPv6 over IPv4 mGRE tunnel protection.

Information About IPv6 over IPv4 GRE Tunnel Protection

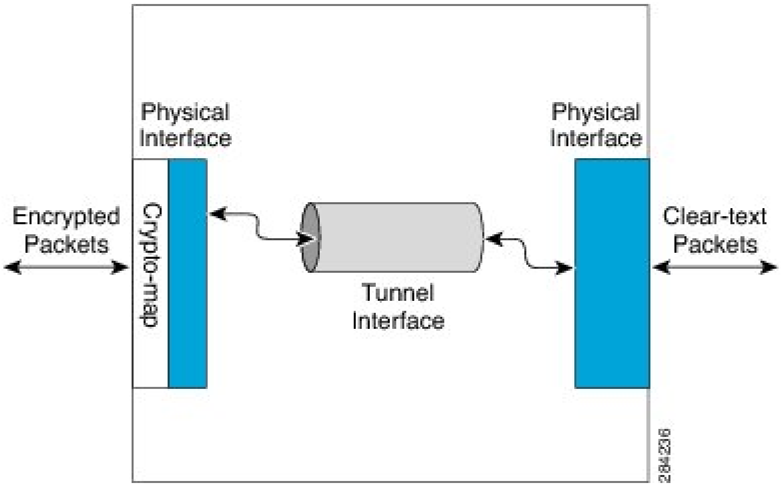
GRE Tunnels with IPsec

Generic routing encapsulation (GRE) tunnels sometimes are combined with IPSec, because IPSec does not support IPv6 multicast packets. This function prevents dynamic routing protocols from running successfully over an IPSec VPN network. Because GRE tunnels do support IPv6 multicast , a dynamic routing protocol can be run over a GRE tunnel. Once a dynamic routing protocol is configured over a GRE tunnel, you can encrypt the GRE IPv6 multicast packets using IPSec.

IPSec can encrypt GRE packets using a crypto map or tunnel protection. Both methods specify that IPSec encryption is performed after GRE encapsulation is configured. When a crypto map is used, encryption is applied to the outbound physical interfaces for the GRE tunnel packets. When tunnel protection is used, encryption is configured on the GRE tunnel interface.

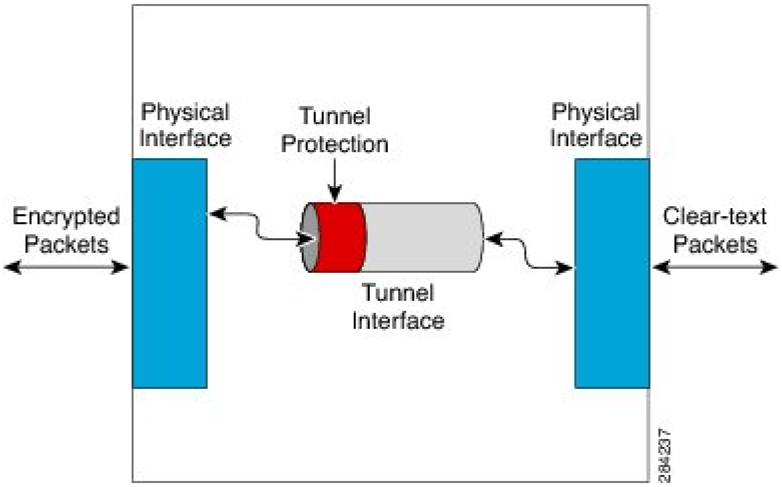
The following figure shows encrypted packets that enter a router through a GRE tunnel interface using a crypto map on the physical interface. Once the packets are decrypted and decapsulated, they continue to their IP destination as clear text.

Figure 1: Using a Crypto Map to Configure IPv6 over IPv4 GRE Tunnel Encryption



The following figure shows encryption using tunnel protection command on the GRE tunnel interface. The encrypted packets enter the router through the tunnel interface and are decrypted and decapsulated before they continue to their destination as clear text.

Figure 2: Using Tunnel Protection to Configure IPv6 over IPv4 GRE Tunnel Encryption



There are two key differences in using the crypto map and tunnel protection methods:

- The IPSec crypto map is tied to the physical interface and is checked as packets are forwarded out through the physical interface. At this point, the GRE tunnel has already encapsulated the packet.

- Tunnel protection ties the encryption functionality to the GRE tunnel and is checked after the packet is GRE encapsulated but before the packet is handed to the physical interface.

How to Configure IPv6 over IPv4 GRE Tunnel Protection

Configuring IPv6 over IPv4 GRE Encryption Using a Crypto Map

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing**
4. **ipv6 unicast-routing**
5. **interface** *type number*
6. **ipv6 address** {**ipv6-address**/*prefix-length* | **prefix-name** *sub-bits*/*prefix-length*}
7. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
8. **tunnel source** {**ip-address** | **ipv6-address** | *interface-typeinterface-number*}
9. **tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
10. **exit**
11. **crypto isakmp policy** *priority*
12. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
13. **hash** {**sha** | **md5**}
14. **group** {**1** | **2** | **5**}
15. **encryption** {**des** | **3des** | **aes 192** | **aes 256**}
16. **exit**
17. **crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**]
18. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
19. **access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]]
20. **crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp** [**dynamic** *dynamic-map-name* | **discover** | **profile** *profile-name*]]
21. **set peer** {*hostname* [**dynamic**] [**default**] | *ip-address* [**default**]}
22. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
23. **match address** [*access-list-id* | *name*]
24. **exit**
25. **interface** *type number*
26. **crypto map** *map-name* [**redundancy** *standby-group-name* [**stateful**]]
27. **end**

DETAILED STEPS

Procedure

	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	**ipv6 multicast-routing** **Example:** `Router(config)# ipv6 multicast-routing`	Enables multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router and enables multicast forwarding. • Enable this command only if you are using IPv6 multicast. If you are using IPv6 unicast, you need not enable this command.
Step 4	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 5	**interface** *type number* **Example:** `Router(config)# interface tunnel 10`	Specifies a tunnel interface and number, and enters interface configuration mode.

Step 6	**ipv6 address** {**ipv6-address/***prefix-length* | **prefix-name** *sub-bits/prefix-length*}
	Example:
	`Router(config-if)# ipv6 address 0:0:0:7272::72/64`
		Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.

Step 7	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
	Example:
	`Router(config-if)# tunnel mode gre ip`
		Sets the encapsulation mode for the tunnel interface.

Step 8	**tunnel source** {**ip-address** | **ipv6-address** | *interface-typeinterface-number*}
	Example:
	`Router(config-if)# tunnel source ethernet0`
		Sets the source address for a tunnel interface.

	Command or Action	Purpose

Step 9	**tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
	Example:
	`Router(config-if)# tunnel destination 172.16.0.12`
		Specifies the destination for a tunnel interface.

Step 10	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 11	**crypto isakmp policy** *priority* **Example:** `Router(config)# crypto isakmp policy 15`	Defines an Internet Key Exchange (IKE) policy, and enters ISAKMP policy configuration mode. • Policy number 1 indicates the policy with the highest priority. The lower the *priority* argument value, the higher the priority.

Step 12	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	Example:
	`Router(config-isakmp-policy)# authentication pre-share`
		Specifies the authentication method within an IKE policy.
		• The **rsa-sig** and **rsa-encr** keywords are not supported in IPv6.

Step 13	**hash** {**sha** | **md5**}
	Example:
	`Router(config-isakmp-policy)# hash md5`
		Specifies the hash algorithm within an IKE policy.

Step 14	**group** {**1** | **2** | **5**}
	Example:
	`Router(config-isakmp-policy)# group 2`
		Specifies the Diffie-Hellman group identifier within an IKE policy.

Step 15	**encryption** {**des** | **3des** | **aes 192** | **aes 256**}
	Example:
	`Router(config-isakmp-policy)# encryption 3des`
		Specifies the encryption algorithm within an IKE policy.

Step 16	**exit** **Example:** `Router(config-isakmp-policy)# exit`	Exits ISAKMP policy configuration mode and enters global configuration mode.
Step 17	**crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**] **Example:** `Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0`	Configures a preshared authentication key.
Step 18	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] **Example:**	Defines a transform set.

	Command or Action	Purpose
	`Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des`	
Step 19	**access-list** *access-list-number* [**dynamic** *dynamic-name* [**timeout** *minutes*]] {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-range-name*] [**fragments**] [**log** [*word*] | **log-input** [*word*]] **Example:** `Router(config)# access-list 110 permit gre host 192.168.0.16 host 172.16.0.12`	Defines an extended IP access list.
Step 20	**crypto map** [**ipv6**] *map-name seq-num* [**ipsec-isakmp** [**dynamic** *dynamic-map-name* | **discover** | **profile** *profile-name*]] **Example:** `Router(config)# crypto map mymap 10 ipsec-isakmp`	Creates a new crypto map entry or profile and enters crypto map configuration mode.

Step 21	**set peer** {*hostname* [**dynamic**] [**default**] | *ip-address* [**default**]}
	Example:
	`Router(config-crypto-map)# set peer 10.0.0.1`
		Specifies an IP Security (IPsec) peer in a crypto map entry.

Step 22	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **Example:** `Router(config-crypto-map)# set transform-set myset0`	Specifies the transform set that can be used with the crypto map entry.
Step 23	**match address** [*access-list-id* | *name*] **Example:** `Router(config-crypto-map)# match address 102`	Specifies an extended access list for a crypto map entry.
Step 24	**exit** **Example:** `Router(config-crypto-map)# exit`	Exits crypto map configuration mode and returns to global configuration mode.
Step 25	**interface** *type number* **Example:** `Router(config)# interface ethernet 1`	Specifies an interface and number and enters interface configuration mode.
Step 26	**crypto map** *map-name* [**redundancy** *standby-group-name* [**stateful**]] **Example:** `Router(config-if)# crypto map mymap`	Applies a previously defined crypto map set to an outbound interface.

	Command or Action	Purpose

Step 27	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuring IPv6 over IPv4 GRE Encryption Using Tunnel Protection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 multicast-routing**
4. **ipv6 unicast-routing**
5. **crypto isakmp policy** *priority*
6. **authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
7. **hash** {**sha** | **md5**}
8. **group** {**1** | **2** | **5**}
9. **encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
10. **exit**
11. **crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**]
12. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
13. **crypto ipsec profile** *profile-name*
14. **set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*]
15. **exit**
16. **interface** *type number*
17. **ipv6 address** {*ipv6-address* / *prefix-length* | *prefix-name sub-bits/prefix-length*}
18. **tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip**[**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
19. **tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
20. **tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
21. **tunnel protection ipsec profile** *name* [**shared**]
22. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 multicast-routing** **Example:** `Router(config)# ipv6 multicast-routing`	Enables multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router and enables multicast forwarding. • Enable this command only if you are using IPv6 multicast. If you are using IPv6 unicast, you do not need to enable this command.
Step 4	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams.
Step 5	**crypto isakmp policy** *priority* **Example:** `Router(config)# crypto isakmp policy 15`	Defines an IKE policy, and enters ISAKMP policy configuration mode. Policy number 1 indicates the policy with the highest priority. The lower the *priority* argument value, the higher the priority.

Step 6	**authentication** {**rsa-sig** | **rsa-encr** | **pre-share**}
	Example:
	`Router(config-isakmp-policy)# authentication pre-share`
		Specifies the authentication method within an Internet Key Exchange (IKE) policy.
		• The **rsa-sig** and **rsa-encr** keywords are not supported in IPv6.

Step 7	**hash** {**sha** | **md5**}
	Example:
	`Router(config-isakmp-policy)# hash md5`
		Specifies the hash algorithm within an IKE policy.

Step 8	**group** {**1** | **2** | **5**}
	Example:
	`Router(config-isakmp-policy)# group 2`
		Specifies the Diffie-Hellman group identifier within an IKE policy.

Step 9	**encryption** {**des** | **3des** | **aes** | **aes 192** | **aes 256**}
	Example:
	`Router(config-isakmp-policy)# encryption 3des`
		Specifies the encryption algorithm within an IKE policy.

Step 10	**exit** **Example:** `Router(config-isakmp-policy)# exit`	Exits ISAKMP policy configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 11	**crypto isakmp key** *enc-type-digit keystring* {**address** *peer-address* [*mask*] | **ipv6** {*ipv6-address*/*ipv6-prefix*} | **hostname** *hostname*} [**no-xauth**] **Example:** `Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0`	Configures a preshared authentication key.
Step 12	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] **Example:** `Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des`	Defines a transform set, and places the router in crypto transform configuration mode.
Step 13	**crypto ipsec profile** *profile-name* **Example:** `Router(config)# crypto ipsec profile ipsecprof`	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters IPsec profile configuration mode.
Step 14	**set transform-set** *transform-set-name* [*transform-set-name2...transform-set-name6*] **Example:** `Router(ipsec-profile)# set transform-set myset0`	Specifies the transform set that can be used with the crypto map entry.
Step 15	**exit** **Example:** `Router(ipsec-profile)# exit`	Exits IPsec profile configuration mode and returns to global configuration mode.
Step 16	**interface** *type number* **Example:** `Router(config)# interface tunnel 1`	Specifies a tunnel interface and number and enters interface configuration mode.

Step 17	**ipv6 address** {*ipv6-address* / *prefix-length* | *prefix-name sub-bits*/*prefix-length*}
	Example:
	`Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127`
		Specifies the IPv6 network assigned to the interface and enables IPv6 processing on the interface.

Step 18	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip**[**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
	Example:
	`Router(config-if)# tunnel mode gre ip`
		Specifies a GRE IPv6 tunnel.

Step 19	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*}
	Example:
	`Router(config-if)# tunnel source 10.0.0.1`
		Specifies the source address or the source interface type and number for the tunnel interface.

	Command or Action	Purpose

Step 20	**tunnel destination** {*hostname* | *ip-address* | *ipv6-address*}
	Example:
	`Router(config-if)# tunnel destination 172.16.0.12`
		Specifies the destination address or hostname for the tunnel interface.

Step 21	**tunnel protection ipsec profile** *name* [**shared**] **Example:** `Router(config-if)# tunnel protection ipsec profile ipsecprof`	Associates a tunnel interface with an IPsec profile. • The *name* argument specifies the name of the IPsec profile; this value must match the *name* specified in the **crypto IPsec profile** *name* command. • The **shared** keyword allows IPsec sessions to be shared between multiple tunnel interfaces configured with the same tunnel source IP. **Note** When you modify the tunnel protection for an IPsec profile, you must shut down the tunnel interface first. After the modification is successful, you must manually turn on the tunnel configuration.

Step 22	**end**
	Example:
	`Router(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for IPv6 over IPv4 GRE Tunnel Protection

Example: Configuring IPv6 over IPv4 GRE Encryption Using a Crypto Map

```
Router> enable
Router# configure terminal
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 unicast-routing
Router(config)# interface tunnel 10
Router(config-if)# ipv6 address my-prefix 0:0:0:7272::72/64
Router(config-if)# tunnel mode gre ip
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 172.16.0.12
Router(config-if)# exit
Router(config)# crypto isakmp policy 15
Router(config-isakmp-policy)# authentication pre-share
Router(config-isakmp-policy)# hash md5
Router(config-isakmp-policy)# group 2
Router(config-isakmp-policy)# encryption 3des
Router(config-isakmp-policy)# exit
Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0
Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des
Router(config)# access-list 110 permit gre host 192.168.0.16 host 172.16.0.12
Router(config)# crypto map mymap 10 ipsec-isakmp
Router(config-crypto-map)# set peer 10.0.0.1
Router(config-crypto-map)# set transform-set myset0
Router(config-crypto-map)# match address 102
Router(config-crypto-map)# exit
Router(config)# interface ethernet1
Router(config-if)# crypto map mymap
Router(config-if)# end
```

Example: Configuring IPv6 over IPv4 GRE Encryption Using Tunnel Protection

The following example configures IPsec tunnel protection on an IPv4 GRE tunnel. IPv6 multicast routing is enabled using the **ipv6 multicast-routing** command.

```
Router> enable
Router# configure terminal
Router(config)# ipv6 multicast-routing
Router(config)# ipv6 unicast-routing
Router(config)# crypto isakmp policy 15
Router(config-isakmp-policy)# authentication pre-share
Router(config-isakmp-policy)# hash md5
Router(config-isakmp-policy)# group 2
Router(config-isakmp-policy)# encryption 3des
Router(config-isakmp-policy)# exit
Router(config)# crypto isakmp key cisco-10 address 172.16.0.12 255.240.0.0
Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des
Router(config)# crypto ipsec profile ipsecprof
Router(ipsec-profile)# set transform-set myset0
Router(ipsec-profile)# exit
Router(config)# interface tunnel 1
Router(config-if)# ipv6 address 3ffe:b00:c18:1::3/127
Router(config-if)# tunnel mode gre ip
Router(config-if)# tunnel source 10.0.0.1
Router(config-if)# tunnel destination 172.16.0.12
Router(config-if)# tunnel protection ipsec profile ipsecprof
Router(config-if)# end
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 Multicast Routing	IPv6 Implementation Guide
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	• *Cisco IOS Security Command Reference Commands A to C* • *Cisco IOS Security Command Reference Commands D to L* • *Cisco IOS Security Command Reference Commands M to R* • *Cisco IOS Security Command Reference Commands S to Z*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 over IPv4 GRE Tunnel Protection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.