# X.25 Suppression of Security Signaling Facilities

The X.25 Suppression of Security Signaling Facilities feature allows the X.25 Call Redirection/Call Deflection Notification (CRCDN) and Called Line Address Modified Notification (CLAMN) security signaling facilities to be disabled (suppressed) in X.25 Call and Call Confirm packets (respectively) sent by an X.25-class service. This feature may be required when connecting to equipment that implements a proprietary or nonstandard X.25 service that does not accept X.25 security signaling facilities.

### Feature Specifications for the X.25 Suppression of Security Signaling Facilities

| **Feature History** | |
|---|---|
| Release | Modification |
| 12.2(13)T | This feature was introduced. |
| Supported Platforms | |
| Cisco Catalyst 4000 Gateway, Cisco 800 series, Cisco 805 router, Cisco 1400 series, Cisco 1600 series, Cisco 1600R series, Cisco 1710 router, Cisco 2500 series, Cisco 2610 to 2613 series, Cisco 2620 and 2621 routers, Cisco 2650 and 2651 routers, Cisco 2691 router, Cisco 3620 router, Cisco 3631 router, Cisco 3640 router, Cisco 3660 router, Cisco 3725 router, Cisco 3745 router, Cisco 5300 series, Cisco 5350 router, Cisco 5400 series, Cisco 5800 series, Cisco 5850 router, Cisco 7100 series, Cisco 7200 series, Cisco 7400 series, Cisco 8850-RPM, IGX8400-URM, Cisco MC3810 router, Cisco uBR 7200 router | |

### Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

### Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or Cisco Feature Navigator.



# Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

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.

# Information About the X.25 Suppression of Security Signaling Facilities Feature

## X.25 Security Facilities Suppression Scenarios

X.25 networks encode security facilities in X.25 Call, Call Confirm, and Clear packets to notify both stations participating in the setup of a switched virtual circuit (SVC) of events that may result in a station connecting to an unexpected partner.

**Note** This document refers to Call packets and Call Confirm packets. These names differ from those standardized by X.25. The standard distinguishes between a Call packet sent by the DTE station (a Call Request) and one sent by the DCE station (an Incoming Call), and similarly between a Call Confirm packet sent by the DTE (a Call Accepted) and one sent by the DCE (a Call Connected). The packets are encoded identically and, in many cases, the processing that X.25 does is identical; however, there are cases where the behavior is predicated on the station type receiving or sending the packet.

For example, when an X.25 Call is redistributed by a network through a hunt group, a standard implementation will encode a CRCDN facility in the forwarded call. Thus, the receiver is notified that the Call packet was redistributed by a hunt group and is notified of the original destination address. A standard network will also, if such a Call is accepted by a returned Call Confirm packet, encode a CLAMN facility when forwarding the Call Confirm packet. This encoding notifies the originator that the accepting destination was reached by distribution through a hunt group, and may also encode the destination address of the accepting station. Both stations receive notification of what happened so each can decide to either proceed with the SVC, if the resulting connection is permissible, or to clear the channel if not.

## When Suppressing the Security Signaling Facilities Is Necessary

**Danger** X.25 security signaling facilities are used to explicitly notify the connecting stations of events that may raise security issues if they were not signaled. Suppression of these facilities should only be configured when the attached equipment and network configurations are sufficiently secure that the signaled information is unnecessary.

There are many X.25 implementations that will not operate as intended if presented with X.25 features or facilities beyond a narrow set of those that occur most commonly. The security signaling facilities are less common, and there are a significant number of X.25 implementations that will not proceed with an SVC that encodes them during Call setup. This can cause connection failures when Cisco equipment is used to implement an X.25 hunt group. There are two security facilities that the Cisco hunt group feature encodes: An X.25 Call packet forwarded out from a hunt group has the CRCDN facility encoded in the packet and, when accepted, the returning X.25 Call Confirm packet has the CLAMN facility encoded in the packet.

Both the originator of the Call packet and the destination it reaches should be notified of the hunt group event, thus allowing each side to clear the SVC if communication is not permitted by the station's security policy. For this reason, the Cisco implementation of hunt groups is designed to signal both stations participating in

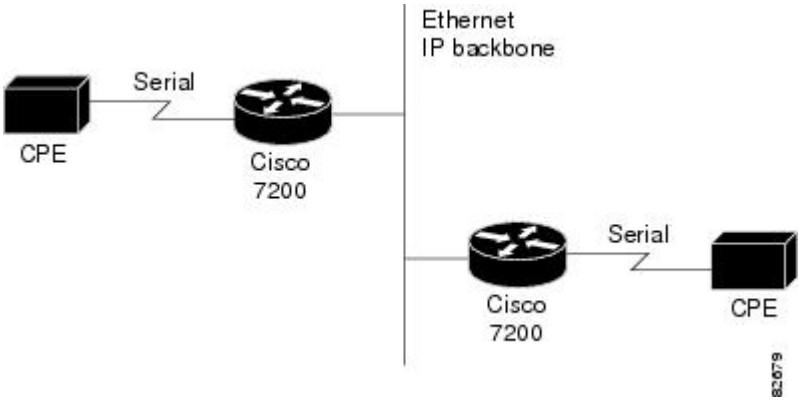
the Call setup using the X.25-designated CRCDN and CLAMN facilities. The X.25 Suppression of Security Signaling Facilities feature allows this signaling to be suppressed by the CRCDN facility in a Call packet. The **no x25 security crcdn** command introduced in this feature provides this function, and there are no implications for correct protocol behavior by using it.

X.25 operation can also be modified to suppress a CLAMN facility in X.25 Call Confirm packets when the **no x25 security clamn** command is configured to disable that signaling. Configuring suppression of the CLAMN security signaling facility has an implication for correct protocol behavior: The X.25 Recommendations specify that the CLAMN facility must be present in a Call Confirm packet if that packet encodes a destination address that is not the null address and that differs from the address encoded in the Call packet. When X.25 is configured to suppress the encoding of a CLAMN facility, it will also suppress the encoding of the destination address. That is, when the address block is encoded in the Call Confirm packet, the destination address will be encoded as the null address (zero digits) because no representation should be made as to what destination was reached.

An X.25 profile may also be configured to suppress the X.25 security signaling facilities. This profile can be useful if the network administrator wants to localize the suppression of these facilities. For example, a hunt group that switches a connection using X.25 over TCP/IP (XOT) may be configured so that the security signaling facilities are not transmitted to either hop participating in the Call setup.

As another example, some telephone company data communications networks (telco DCNs) use a nonstandard X.25 implementation that blends elements of the 1980 and 1984 International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendations. The figure below shows a portion of a telco DCN network where X.25 devices, also called CPE, are connected to Cisco routers and the IP backbone network using serial links.

***Figure 1: DCN Network Devices Connected to a Cisco IP Backbone Network***




Early equipment in the telco DCN conformed to the ITU-T 1980 X.25 Recommendation, and Cisco provides support for this standard. However, substantial ITU-T 1984 X.25 Recommendation elements, such as maximum packet sizes of 2048 and 4096 and X.25 Annex G operation, have since been incorporated into the DCN. This mix of ITU-T 1980 and 1984 X.25 Recommendations in the telco DCN has resulted in a design requirement that would allow the CPE to operate according to the ITU-T 1984 X.25 Recommendation, but with a modification that would allow suppressing security signaling facilities encoded by the Cisco hunt group feature. Because the ITU-T 1980 X.25 Recommendation does not define these security signaling facilities, the Cisco X.25 implementation can now be configured to suppress them in the packets where they would otherwise be encoded.

# How to Suppress the X.25 Security Signaling Facilities

## Disabling the X.25 Security Signaling Facilities

To disable the X.25 CLAMN and CRCDN signaling facilities, perform the following steps:

### SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface serial** *interface-number*
4. **encapsulation x25**
5. **no x25 security crcdn**
6. **no x25 security clamn**
7. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables higher privilege levels, such as privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure** {**terminal** | **memory** | **network**}<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface serial** *interface-number*<br><br>**Example:**<br>`Router(config)# interface serial 0` | Enters interface configuration mode. |
| **Step 4** | **encapsulation x25**<br><br>**Example:**<br>`Router(config-if) encapsulation x25` | Enables the default X.25 DTE operation mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **no x25 security crcdn**<br><br>**Example:**<br><br>`Router(config-if) no x25 security crcdn` | Disables the CRCDN security signaling facility in X.25 Call packets transmitted. |
| **Step 6** | **no x25 security clamn**<br><br>**Example:**<br><br>`Router(config-if) no x25 security clamn` | Disables the CLAMN security signaling facility in X.25 Call Confirm packets and suppresses any destination address. |
| **Step 7** | **exit**<br><br>**Example:**<br><br>`Router(config-if) exit` | Ends interface configuration mode.<br><br>• Enter the **exit** command once more to exit global configuration mode. |

### Troubleshooting Tips

Use the **debug x25** EXEC command to determine when the X.25 facilities are present and when they are suppressed by the configured feature.

# Configuration Example for Suppressing X.25 Security Signaling Facilities

The following example shows how to suppress both the CRCDN and CLAMN security signaling facilities:

```
interface serial 0
  no ip address
  encapsulation x25
  no x25 security crcdn
  no x25 security clamn
```

# Additional References

**Related Documents**

| Related Topic | Document Title |
|---|---|
| X.25 commands | *Cisco IOS Wide-Area Networking Command Reference* , Release 12.2 |

| Related Topic | Document Title |
|---|---|
| X.25 configuration tasks | *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2 |

### Standards

| Standards[1] | Title |
|---|---|
| ITU-T X.25 | • *ITU-T 1980 X.25 Recommendation*<br>• *ITU-T 1984 X.25 Recommendation*<br>• *ITU-T 1988 X.25 Recommendation*<br>• *ITU-T 1993 X.25 Recommendation* |

1 Not all supported standards are listed.

### MIBs

| MIB | MIBs Link |
|---|---|
| None | To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:<br>http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml |

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

### RFCs

| RFCs | Title |
|---|---|
| None | -- |

### Technical Assistance

| Description | Link |
|---|---|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/public/support/tac/home.shtml |