



Terminal Line Security for PAD Connections

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

This document describes the Terminal Line Security for PAD Connections feature in 12.2(13)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 5](#)
- [Supported Standards, MIBs, and RFCs, page 7](#)
- [Prerequisites, page 7](#)
- [Configuration Tasks, page 7](#)
- [Monitoring and Maintaining X.25 CUG Support on Terminal Lines, page 9](#)
- [Configuration Examples, page 9](#)
- [Command Reference, page 10](#)
- [Glossary, page 11](#)

Feature Overview

X.25 closed user group (CUG) service is a network service that allows subscribers to be segregated into private subnetworks with limited outgoing and incoming access. A data terminal equipment (DTE) device becomes a member of a CUG by subscription; the DTE must obtain membership from its network service for the set of CUGs to which it needs access.

The Terminal Line Security for PAD Connections feature allows a CUG service to be configured on terminal lines, enabling terminal lines to participate in X.25 CUG security for packet assembler/disassembler (PAD) connections. A CUG service can be applied to console lines, auxiliary lines, and tty and vty devices. Configuring a CUG service on terminal lines allows you to specify CUG



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

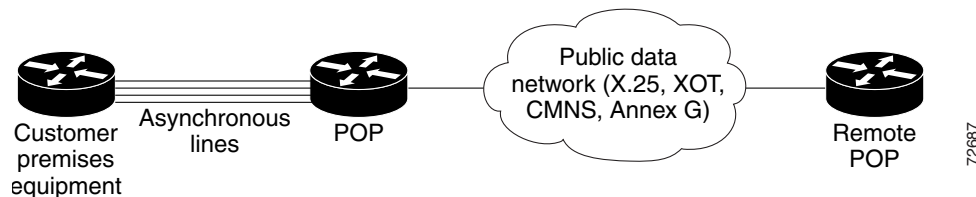
© 2007 Cisco Systems, Inc. All rights reserved.

protection for lines that are part of the point of presence (POP). Before the introduction of this feature, a CUG service could be configured only on X.25 synchronous data communications equipment (DCE) interfaces.

A line configured for CUG service will apply CUG security to PAD, X.28 mode, and protocol translation sessions. The Terminal Line Security for PAD Connections feature ensures that CUG protection is applied to incoming calls destined for the terminal line and call requests specified from the line. This feature also supports the signaling of the CUG selection facility in call requests that originated on the line and incoming calls received on an X.25 service that are terminated by the line.

Figure 1 shows a typical topology in which CUG service would be configured on asynchronous terminal lines.

Figure 1 Network Topology with Asynchronous Lines Configured for CUG Service



Security Considerations



Caution

X.25 CUG security relies on the correct, complementary configuration of CUG sets at all the boundaries between client premises equipment (CPE) and POPs. Any POP that is connected to a CPE device that is not configured for CUG security has compromised the X.25 network security because that CPE device will be considered a trusted host, even though it is not secure.

PAD Call Behavior When a Line Is Configured for CUG Subscription

This section describes the overall behavior of PAD-initiated calls when a terminal line or an X.25 interface is configured for CUG subscription.

The **x25 map pad** and **x25 facility cug** commands can be used to cause a CUG selection facility to be encoded in calls placed within the networks. The following rules describe which CUG selection facility is encoded in the call:

- A call initiated using the **pad** command or in X.28 mode without a CUG subscription set encodes the interface CUG selection facility, if one was specified.
- A call initiated using the **pad** command with the **/use-map** option encodes the CUG selection facility for the matching map entry, if one was specified.
- A call initiated in X.28 mode with a specified CUG encodes the specified X.28 CUG.

The following sections provide examples that illustrate the behavior of PAD-initiated calls.

PAD Call Behavior When Only the Line is Configured for CUG Service

This section describes PAD call behavior when only the line is configured for CUG service.

Configuration A

In the following example, a line is configured for CUG subscription, and the interface on which the resulting call is to be placed is configured with the **x25 facility cug** and **x25 map pad** commands. CUG subscription is not configured on the interface.

```
interface Serial1
  encapsulation x25 dce
  x25 facility cug 99
  x25 map pad 1221 cug 10 no-outgoing
  x25 map pad 1222 cug 99
  x25 map pad 1234 cug 10
!
line tty 1
  x25 subscribe cug-service
  x25 subscribe local-cug 99 network-cug 9999 preferential
  x25 subscribe local-cug 10 network-cug 100
  x25 subscribe local-cug 20 network-cug 200
!
[...]
!
x25 route ^12..$ interface Serial1
[...]
```

When the line initiates an X.28 mode or PAD call without a CUG subscription set, the line will decode the interface's CUG selection facility, and the network will encode the line's signaled CUG selection facility. The **x25 facility cug** command implicitly identifies the local CUG to use for PAD-originated calls.

[Table 1](#) shows the CUG value sent when a line initiates a PAD or an X.28 mode call without a CUG subscription set.

Table 1 CUG Value Sent for Line-Initiated Calls Without a CUG Subscription

User Command	Result
pad 1234	Call 1234, CUG 9999 sent on Serial 1.
*1234	Call 1234, CUG 9999 sent on Serial 1.

Using configuration A, if a call is initiated on a line using the **pad** command with the **/use-map** option, the line will decode the matching map entry's CUG, and the network will encode the line's signaled CUG selection facility. The map's CUG identifies the local CUG to use for PAD-originated calls and overrides the interface's CUG selection facility on a per-call basis.

If the **pad** command is used with the **/use-map** option, the interface on which the resulting call is to be placed must have a matching X.25 map statement for the PAD call and must permit outgoing calls. Any CUG specified in the map statement must identify the local CUG ID to be used for generating the call.

[Table 2](#) shows the values sent when a line initiates a PAD call with the **/use-map** option.

Table 2 CUG Value Sent for Line-Initiated PAD Calls Initiated with the /use-map Option

User Command	Result
pad 1234 /use-map	Call 1234, CUG 100 sent on Serial 1.
pad 1221 /use-map	Call is cleared, outgoing calls are barred.
pad 1255 /use-map	Call is cleared (no matching map found on Serial 1).

Using configuration A, if an X.28 mode call specifies a CUG, the line will decode the specified CUG, and the network will encode the line's signaled CUG selection facility. The X.28 mode commands do not use X.25 map statements when originating calls.

Table 3 shows the CUG value sent when a line initiates a call using an X.28 interface with CUG specified.

Table 3 CUG Value Sent for Line-Initiated Calls Using an X.28 Mode with CUG Specified

User Command	Result
*g10-1234	Call 1234, CUG 100 sent on Serial 1.

PAD Call Behavior When Both a Line and an Interface Are Configured for CUG Service

This section describes PAD call behavior when a line and an interface are both configured for CUG service.

Configuration B

In the following example a line and an interface are configured for CUG subscription:

```
interface Serial1
  encapsulation x25 dce
  x25 subscribe cug-service
  x25 subscribe local-cug 5599 network-cug 9999 preferential
  x25 subscribe local-cug 5510 network-cug 100
  x25 subscribe local-cug 5520 network-cug 200
  x25 facility cug 99
  x25 map pad 1234 cug 10
  x25 map pad 1221 cug 10 no-outgoing
  x25 map pad 1222 cug 99
!
line tty 1
  x25 subscribe cug-service
  x25 subscribe local-cug 10 network-cug 100
  x25 subscribe local-cug 20 network-cug 200
  x25 subscribe local-cug 99 network-cug 9999 preferential
!
[...]
!
x25 route ^12..$ interface Serial1
[...]
```

Table 4 shows examples of line-initiated PAD commands and the CUG values sent when the terminal line and the X.25 interface are both configured for CUG subscription.

Table 4 CUG Values Sent for Line-Initiated Calls When the Line and Interface Are Configured for CUG Subscription

User Command	Result
pad 1234	Call 1234, CUG 5599 sent on Serial 1.
pad 1221	Call 1221, CUG 5599 sent on Serial 1.
pad 1222	Call 1222, CUG 5599 sent on Serial 1.
pad 1234 /use-map	Call 1234, CUG 5510 send on Serial 1.

Table 4 *CUG Values Sent for Line-Initiated Calls When the Line and Interface Are Configured for CUG Subscription*

User Command	Result
pad 1221 /use-map	Call is cleared, outgoing calls are barred
pad 1222 /use-map	Call 1222, CUG 5599 sent on Serial 1

Benefits

Before the introduction of this feature, CUG functionality required all CPE devices to be attached to the router at an X.25 synchronous DCE interface. The Terminal Line Security for PAD Connections feature extends the existing X.25 CUG functionality to terminal lines, allowing PAD access devices (console lines, auxiliary lines, and tty and vty devices) to be configured for CUG security enforcement.

Restrictions

The CUG selection facility suppression options are not available for terminal lines because incoming PAD calls are terminated by the terminal line.

Related Documents

For information about X.25 CUGs, refer to the following documents:

- “Configuring X.25 and LAPB” chapter, *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.2
- “X.25 and LAPB Commands” chapter, *Cisco IOS Wide-Area Networking Command Reference*, Release 12.2

For information about PAD connections, refer to the following documents:

- “Configuring the Cisco PAD Facility for X.25 Connections” chapter, *Cisco IOS Terminal Services Configuration Guide*, Release 12.2
- *Cisco IOS Terminal Services Command Reference*, Release 12.2

Supported Platforms

- Cisco 1400 series
- Cisco 1600 series
- Cisco 1700 series
- Cisco 2500 series
- Cisco 2600 series
- Cisco 2600XM
- Cisco 2691
- Cisco 3600 series

- Cisco 3725
- Cisco 3745
- Cisco 7100 series
- Cisco 7200 series
- Cisco 800 series
- Cisco AS5300
- Cisco AS5350
- Cisco AS5400 series
- Cisco AS5800
- Cisco AS5850
- Cisco IAD2400 series
- Cisco MC3810
- Cisco uBR7200 Series
- Universal Router Module (URM) for Cisco IGX 8400

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>

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, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

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://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

No new or modified RFCs are supported by this feature.

Prerequisites

The tasks in this document assume a basic understanding of the X.25 CUG service and how it works.

Configuration Tasks

See the following sections for configuration tasks for the Terminal Line Security for PAD Connections feature. Each task in the list is identified as either required or optional.

- [Configuring X.25 CUG Support on Terminal Lines](#) (required)
- [Verifying X.25 CUG Support on Terminal Lines](#) (optional)

Configuring X.25 CUG Support on Terminal Lines

To configure X.25 CUG support on terminal lines, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# line [aux console tty vty] <i>line-number</i> [<i>ending-line-number</i>]	Identifies a specific line or range of lines for configuration and enters line configuration mode.
Step 2	Router(config-line)# x25 subscribe cug-service [incoming-access outgoing-access]	Enables and controls standard CUG behavior. CUG protection will be applied to PAD calls destined for and originated on the line. Note The CUG selection facility suppression option is not available for terminal lines because incoming PAD calls are terminated by the line.
Step 3	Router(config-line)# x25 subscribe local-cug <i>number</i> network-cug <i>number</i> [no-incoming no-outgoing preferential]	Configures subscription to a specific CUG and maps the desired local CUG number to its corresponding network CUG. This command can be entered as many times as needed to configure the access needs of a line.

Verifying X.25 CUG Support on Terminal Lines

To verify support for X.25 CUG service on terminal lines, perform the following steps:

- Step 1** Enter the **show running-config** command to verify that the configuration is correct.
- Step 2** Enter the **show line** command to display the configured CUG capability in the Capabilities field:

```
Router# show line vty 2
```

```
Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
    132 VTY - - - - - 0 0 0/0 -
```

```
Line 132, Location: "", Type: ""
```

```
Length: 24 lines, Width: 80 columns
```

```
Baud rate (TX/RX) is 9600/9600
```

```
Status: No Exit Banner
```

```
Capabilities: CUG Security Enabled
```

```
Modem state: Idle
```

```
Group codes: 0
```

```
Special Chars: Escape Hold Stop Start Disconnect Activation
                ^x none - - none
```

```
Timeouts: Idle EXEC Idle Session Modem Answer Session Dispatch
            00:10:00 never none not set
```

```
Idle Session Disconnect Warning
```

```
never
```

```
Login-sequence User Response
```

```
00:00:30
```

```
Autoselect Initial Wait
```

```
not set
```

```
Modem type is unknown.
```

```
Session limit is not set.
```

```
.
```

```
.
```

```
.
```

- Step 3** Enter the **show x25 cug** command with the **local-cug** keyword to display information about all local CUGs configured on the router:

```
Router# show x25 cug local-cug
```

```

X.25 Serial1/1, 3 CUGs subscribed with no public access
  local-cug 99 <-> network-cug 9999, no-incoming, preferential
  local-cug 100 <-> network-cug 1000
  local-cug 101 <-> network-cug 1001
PROFILE cugs, 2 CUGs subscribed with with incoming public access
  local-cug 1 <-> network-cug 10, no-outgoing
  local-cug 2 <-> network-cug 20, no-incoming, preferential
Line: 129 aux 0 , 1 CUGs subscribed with outgoing public access
  local-cug 1 <-> network-cug 10
Line: 130 vty 0 , 4 CUGs subscribed with incoming and outgoing public access
  local-cug 1 <-> network-cug 10
  local-cug 50 <-> network-cug 5, preferential
  local-cug 60 <-> network-cug 6, no-incoming
  local-cug 70 <-> network-cug 7, no-outgoing
Line: 131 vty 1 , 1 CUGs subscribed with no public access
  local-cug 1 <-> network-cug 10

```

Step 4 Enter the **show x25 cug** command with the **network-cug** keyword to display information about all network CUGs configured on the router. The following sample output displays the local CUGs associated with network CUG 10:

```

Router# show x25 cug network-cug 10

PROFILE cugs, 2 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1 , no-outgoing
Line: 129 aux 0 , 1 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1
Line: 130 vty 0 , 4 CUGs subscribed with incoming and outgoing public access
  network-cug 10 <-> local-cug 1
Line: 131 vty 1 , 1 CUGs subscribed with no public access
  network-cug 10 <-> local-cug 1

```

Monitoring and Maintaining X.25 CUG Support on Terminal Lines

To monitor and maintain X.25 CUG support on terminal lines, use the following command in privileged EXEC mode:

Command	Purpose
Router# debug pad	Displays debug messages for all PAD connections.

Configuration Examples

This section provides the following configuration example:

- [Configuring X.25 CUG Support on Terminal Lines](#)

Configuring X.25 CUG Support on Terminal Lines Example

The following example shows the configuration of CUG behavior on asynchronous line 1 and virtual terminal lines 0 to 9. The user of async line 1 has only outgoing access to CPE that is subscribed to the corporate CUG designated for finance (CUG 1101) but can receive calls from those same CUG members or from the open network (that is, calls from a network X.25-class service that are destined for the line and have no CUG restriction).

The users of virtual terminal lines 0 to 9 have access only within the corporate CUGs designated for engineering (CUGs 1102 or 1103). Any call from a network X.25-class service destined for the line will be refused unless the inbound POP validates it as a member of one of those two CUGs.

```
Line 1
Location Company A. Finance Connection
x25 subscribe cug-service incoming-access
x25 subscribe local-cug 1 network-cug 1101 preferential
!
line vty 0 9
Location Company A. Engineering Access
x25 subscribe cug-service
x25 subscribe local-cug 2 network-cug 1102 preferential
x25 subscribe local-cug 3 network-cug 1103
!
```

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Wide-Area Networking Command Reference* at http://www.cisco.com/en/US/docs/ios/wan/command/reference/wan_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug pad**
- **show line**
- **show x25 cug**
- **x25 subscribe cug-service**
- **x25 subscribe local-cug**

Glossary

call request—An X.25 call packet sent from a DTE to a DCE that initiates a connection to a destination DTE.

closed user group selection facility—A specific encoding element that can be presented in a call request or incoming call. A CUG selection facility in a call request allows the source DTE to identify the CUG within which it is placing the call. A CUG selection facility in an incoming call allows the destination DTE to identify the CUG to which both DTEs belong.

CPE—customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company, installed at customer sites, and connected to the telephone company network. This equipment is available for customer modification and is considered insecure by the network.

CUG—closed user group. A collection of DTE devices for which the network controls access among members and between members and nonmembers. A DTE may subscribe to zero, one, or more CUGs. A DTE that does not subscribe to a CUG is referred to as being in the open part of the network.

DCE—data communications equipment. A network connection where a subscriber can be attached. A DCE is configured with the operational details for which a given subscriber (DTE) has contracted.

DTE—data terminal equipment. A network subscriber that can be reached at a specific network attachment point. A network identifies each DTE device by assigning an X.121 address.

incoming call—An X.25 call packet sent from a DCE to a DTE that presents a connection requested by the source DTE.

PAD—packet assembler/disassembler. Device used to connect simple devices (like character-mode terminals) that do not support the full functionality of a particular protocol to a network. PADs buffer data and assemble and disassemble packets sent to such end devices.

POP—point of presence. In the context of a public data network, a POP is the part of the network to which CPE is attached. A POP is configured and controlled by the public network and serves as the boundary equipment between the trusted network and insecure client attachments.

preferential closed user group—The CUG that is assumed when a CUG is not specified in call setup. A DTE that subscribes to more than one CUG and does not have incoming or outgoing access must designate a preferred CUG.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

