# Authorization for Protocol Translation

In releases of Cisco IOS software prior to 12.3(2)T, protocol translation sessions established using one-step protocol translation are set up without an authorization request being issued first. The Authorization for Protocol Translation feature adds an option to require that an authorization request is issued as a prerequisite to establishing a protocol translation session. This feature improves authentication, authorization, and accounting (AAA) support for protocol translation.

**Feature History for the Authorization for Protocol Translation Feature**

| Release | Modification |
|---|---|
| Cisco IOS XE Gibraltar 16.10.1 | This feature was introduced. |

### 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.

## Contents




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

# Prerequisites for Authorization for Protocol Translation

Packet assembler/disassembler (PAD) must be configured. For more information on configuring PAD, refer to Configuring the Cisco PAD Facility for X.25 Connections.

A TACACS+ server must be configured to perform authorization. For more information about configuring authorization, refer to the "Configuring Authorization" chapter in the *Cisco IOS Security Configuration Guide*.

# Restrictions for Authorization for Protocol Translation

This feature is supported only for protocol translation sessions in which the incoming protocol is TCP or X.25, and in which the outgoing protocol is TCP, X.25, or autocommand.

For incoming X.25 sessions, this feature is restricted to switched virtual circuits (SVCs) only; permanent virtual circuits (PVCs) may be used only for the outgoing side.

If the **pvc** keyword is specified in the **translate** command, the **authorize** and **login** keywords may not be used.

# Information About Authorization for Protocol Translation

To configure the Authorization for Protocol Translation feature, you must understand the following concepts:

- AAA Authorization and the Authorization Packet, page 2
- Benefits of Authorization for Protocol Translation, page 2

## AAA Authorization and the Authorization Packet

Once authorization is enabled, authorization occurs before access to the connection is granted. If authentication is configured, authorization occurs after authentication.

During authorization, a TACACS+ authorization packet is generated. This authorization packet contains the following attribute-value (AV) pairs:

- service—A new value, translate, has been added to the existing service AV pair defined in the args section. This AV pair is marked as mandatory.
- azn-tag—This new attribute contains the authorization tag assigned to the command. The azn-tag attribute may contain a series of lowercase alphanumeric ASCII characters up to 64 bytes in length. Allowable characters are digits, lowercase letters, the hyphen, and the underscore. This AV pair is marked as mandatory.

## Benefits of Authorization for Protocol Translation

Releases of Cisco IOS software prior to 12.3(2)T did not allow authorization of protocol translation sessions established using one-step protocol translation. The Authorization for Protocol Translation feature introduces the ability to configure one-step protocol translation sessions for AAA authorization using TACACS+. This feature improves AAA support for protocol translation sessions.

# How to Configure Authorization for Protocol Translation

This section contains the following procedures:



## Configuring Authorization for Protocol Translation for a TCP-to-X.25 Protocol Translation Session

Perform this task to enable AAA authorization of a TCP-to-X.25 protocol translation session.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network** {**default** | *list-name*} *method1* [*method2*...]
4. **translate tcp** *incoming-address* [*incoming-options*] **x25** *outgoing-address* [*outgoing-options*] [*global-options*] **authorize** *method-list tag*

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **aaa authorization network** {**default** \| *list-name*} *method1* [*method2...*]<br><br>**Example:**<br>`Router(config)# aaa authorization network mylist group tacacs+` | Sets parameters that restrict user access to a network. |
| **Step 4** | **translate tcp** *incoming-address* [*incoming-options*] **x25** *outgoing-address* [*outgoing-options*] [*global-options*] **authorize** *method-list tag*<br><br>**Example:**<br>`Router(config)# translate tcp 10.60.155.63 pvc 3 dynamic x25 12345678 authorize mylist 05149c3` | Translates a connection request to another protocol connection type when receiving a TCP connection request to a particular destination address or host name.<br>• **authorize**—Enables AAA authorization for a protocol translation session.<br>• *method-list*—The list of authorization methods defined with the **aaa authorization** command using the **network** keyword. The *method-list* argument may have the value of *list-name* or **default**.<br>• *tag*—An alphanumeric string of up to 64 characters. The *tag* argument need not be unique; more than one instance of the **translate** command can specify identical values for the *tag* argument.<br>**Note** The *tag* argument is not interpreted by the router. The *tag* argument simply identifies the translate command or the resource being accessed by the protocol translation session to the authorization server. |

# Configuring Authorization for Protocol Translation for an X.25-to-TCP Protocol Translation Session

Perform this task to enable AAA Authorization of an X.25-to-TCP protocol translation session.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa authorization network** {**default** | *list-name*} *method1* [*method2...*]
4. **translate x25** *incoming-address* [*incoming-options*] **tcp** *outgoing-address* [*outgoing-options*] [*global-options*] **authorize** *method-list tag*

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa authorization network** {**default** \| *list-name*} *method1* [*method2...*]<br><br>**Example:**<br>`Router(config)# aaa authorization network mylist group tacacs+` | Sets parameters that restrict user access to a network. |
| **Step 4** | **translate x25** *incoming-address* [*incoming-options*] **tcp** *outgoing-address* [*outgoing-options*] [*global-options*] **authorize** *method-list tag*<br><br>**Example:**<br>`Router(config)# translate x25 12345678 tcp 10.60.155.63 login authorize mylist 73234r45` | Translates a connection request to another protocol connection type when receiving an X.25 connection request to a particular destination address or host name.<br>• **authorize**—Enables AAA authorization for a protocol translation session.<br>• *method-list*—The list of authorization methods defined with the **aaa authorization** command using the **network** keyword. The *method-list* argument may have the value of *list-name* or **default**.<br>• *tag*—An alphanumeric string of up to 64 characters. The *tag* argument need not be unique; more than one instance of the **translate** command can specify identical values for the *tag* argument. |

# Configuration Examples for Authorization for Protocol Translation

This section contains the following configuration example:


- Configuring Translation Authorization for a TCP-to-X.25 Protocol Translation Session: Example, page 6
- Configuring Translation Authorization for an X.25-to-TCP Protocol Translation Session: Example, page 7

# Configuring Translation Authorization for a TCP-to-X.25 Protocol Translation Session: Example

The following example uses an authorization method list named mygroup. Serial interfaces 2/0 and 2/1 connect to X.25 hosts, each of which provides multiple services at different X.25 subaddresses. Some of the translate statements specify unique authorization tags so the services can be individually controlled; others specify generic tags (perhaps because they are less critical, such as a monitoring service rather than one which permits configuration changes).

```
aaa authorization network mygroup group tacacs+
x25 routing
!
interface Ethernet0/0
 ip address 10.60.155.30 255.255.255.0
!
interface Serial2/0
 encapsulation x25 dce
 x25 ltc 30
!
interface Serial2/1
 encapsulation x25 dce
 x25 ltc 30
!
x25 route ^13033 interface Serial2/0
x25 route ^13133 interface Serial2/1
!
translate tcp 10.60.155.36 port 2001 x25 1303301 login authorize mygroup a-port01
translate tcp 10.60.155.36 port 2002 x25 1303302 login authorize mygroup a-port02
translate tcp 10.60.155.36 port 2003 x25 1303303 login authorize mygroup monitor
translate tcp 10.60.155.36 port 2004 x25 1303304 login authorize mygroup monitor
translate tcp 10.60.155.36 port 2005 x25 13033 pvc 1 login authorize mygroup a-admin01
!
translate tcp 10.60.155.36 port 2101 x25 1313301 login authorize mygroup b-port01
translate tcp 10.60.155.36 port 2102 x25 1313302 login authorize mygroup b-port02
translate tcp 10.60.155.36 port 2103 x25 1313303 login authorize mygroup monitor
translate tcp 10.60.155.36 port 2104 x25 1313304 login authorize mygroup monitor
```

With this configuration, the router accepts Telnet requests to 10.60.155.36 at any of the TCP ports listed. The user is required to log in, then the router sends an authorization request specifying “translate” as the value of the “service” AV pair, and the authorization tag from the corresponding **translate** command as the value of the “azn-tag” AV pair. The user id and remote address of the Telnet session are also included in the authorization request. If the authorization server approves the request, the connection to the specified X.25 address is attempted; if the request is denied, the Telnet connection is closed.

The authorization server would not be able to distinguish between connections to 10.60.155.36 port 2003 and 10.60.155.36 port 2104, because they specify the same authorization tag.

# Configuring Translation Authorization for an X.25-to-TCP Protocol Translation Session: Example

The following example uses the default authorization method list. Incoming PAD calls to the router on serial interface 1/1 are translated to Telnet calls to various destinations based on the X.25 subaddress. Use of the first two translate statements is restricted to users that are approved by the authorization server for access to group1; the third translate statement will complete the connection only if the authorization server grants access to group2.

```
aaa authorization network default group tacacs+
!
interface Serial1/1
 encapsulation x25
 x25 address 5551088
!
translate x25 555108801 tcp 10.60.155.1 login authorize default group1
translate x25 555108802 tcp 10.60.155.2 login authorize default group1
translate x25 555108803 tcp 10.60.155.3 login authorize default group2
```

# Additional References

The following sections provide additional information related to the Authorization for Protocol Translation feature.

## Related Documents

| Related Topic | Document Title |
|---|---|
| Information on configuring PAD | The "Configuring the Cisco PAD Facility for X.25 Connections" chapter in the *Cisco IOS Terminal Services Configuration Guide* |
| Additional PAD commands: complete command syntax, command mode, defaults, usage guidelines and examples | *Cisco IOS Terminal Services Command Reference*, Release 12.3 |
| Additional information about configuring authorization | "Configuring Authorization" chapter in the *Cisco IOS Security Configuration Guide* |
| Additional authentication commands: complete command syntax, command mode, defaults, usage guidelines and examples | *Cisco IOS Security Command Reference*, Release 12.3 |

## Standards

| Standards | Title |
|---|---|
| None | — |

## MIBs

| MIBs | MIBs Link |
|---|---|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

## 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, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/public/support/tac/home.shtml |

# 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 Terminal Services Command Reference* at http://www.cisco.com/en/US/docs/ios/termserv/command/reference/tsv_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.*

- **aaa authorization**
- **translate tcp**
- **translate x25**