



TN3270 Server Connectivity Enhancements

This feature module describes the TN3270 Server Connectivity Enhancements feature. It includes information on the overview and benefits of the new feature, configuration tasks, configuration examples, and new and modified commands.

This document contains the following sections:

- Feature Overview, page 1
- Supported Platforms, page 4
- Supported Standards, MIBs, and RFCs, page 4
- Prerequisites, page 4
- Configuration Tasks, page 5
- Configuration Examples, page 16
- Command Reference, page 22
- Glossary, page 61

Feature Overview

The TN3270 Server Connectivity Enhancements feature in Cisco IOS Release 12.1(5)T contains several TN3270 server configuration enhancements, which are described in this document:

- Dynamic LU Naming, page 1
- Inverse DNS Nailing, page 2
- SSL Encryption Support, page 2

Dynamic LU Naming

The Dynamic LU Naming enhancement allows the user to configure named logical units (LUs) from the TN3270 server side. This enhancement allows the TN3270 server to pass an LU name to the Virtual Telecommunications Access Method (VTAM) software running on the mainframe and have VTAM dynamically create an LU with that name. The LU name is then sent to the mainframe as part of subvector 86 in the Reply PSID NMVT power-on frame. The TN3270 client can connect to any of the available TN3270 servers and the selected server can request a specific LU name for the client. In addition, the LU naming conventions have been modified to allow for more flexibility when specifying lu-seed names.

Inverse DNS Nailing

The Inverse DNS Nailing enhancement enables the TN3270 server to nail a pool of LUs to client machine names or to an entire domain. This enhancement allows dynamic IP addressing on the TN3270 client machines. This addressing is used in network design scenarios, for example, a Dynamic Host Configuration Protocol (DHCP) environment and in individual network configuration scenarios, for example, a machine is moved and needs a new network address.

The Cisco IOS software inverse nailing support uses the Domain Name System (DNS) in routers to look up the symbolic name associated with a client IP address. The TN3270 server uses this symbolic name to assign a predefined LU pool for the user. This eliminates the need for nailed TN3270 clients to have statically defined IP addresses. If you configure inverse DNS nailing on the TN3270 server, you do not need to modify the DNS nailing statements in the router configuration.

SSL Encryption Support

The SSL Encryption Support enhancement allows TN3270 clients and servers to negotiate authentication and encryption schemes using the Secure Socket Layer (SSL) technology. The TN3270 server uses SSL version 3.0 to establish secure sessions.

Benefits

This section describes the benefits of the TN3270 server feature enhancements introduced in Cisco IOS Release 12.1(5)T.

Dynamic LU Naming

- Gives user more control over LU naming from the server side
- Avoids duplicate LU names without requiring manual configuration on the mainframe and router
- Minimizes VTAM configuration
- Offers more flexibility due to modified LU naming convention

Inverse DNS Nailing

- Eliminates the need for nailed TN3270 clients to have statically defined IP addresses
- Enables the TN3270 server to connect with client machine names instead of IP addresses only
- Allows the TN3270 server to work in a DHCP environment
- Enables client nailing by machine name and/or by client domain.

SSL Encryption Support



Note

Only SSL 3.0 is supported

- Provides confidential connections. Session partners can securely send messages.
- Authenticates the message. The partner receiving a message can determine the message's origin.
- Ensures integrity of messages in the data stream.
- Ensures non-repudiation. A message sender cannot falsely deny sending the message.

Restrictions

Dynamic LU Naming

- You must replace the default exit ISTEXCSD with the VTAM User Exit for TN3270 Name Pushing, which you can download from the IBM website: <http://www.ibm.com>. This exit causes VTAM to ignore the LUSEED parameter on the PU statement, and instead use the SLU name sent by the router in the subvector 86 when a client connects in. If you do not configure this exit, VTAM ignores the subvector 86 and the specified LU name.
- If you specify the LUSEED operand for the PU definition in VTAM and the subvector 86 specifies an LU name, the VTAM User Exit for TN3270 Name Pushing ignores the LUSEED operand.
- If you do not specify the LUSEED operand for the PU definition in VTAM, and the subvector 86 is not present, then the VTAM User Exit for TN3270 Name Pushing cannot generate an LU name. VTAM does not log this failure, and the TN3270 server does not receive the ACTLU request. The TN3270 server displays the following message:

```
*Apr 17 12:40:53:%CIP2-3-MSG:slot2 :
%TN3270S-3-NO_DYN_ACTLU_REQ_RCVD
  No ACTLU REQ received on LU JJDL1.6
```

Inverse DNS Nailing

- If there are legacy and inverse DNS nailing statements, the inverse DNS nailing statements take precedence. The TN3270 server attempts an inverse DNS lookup before it checks for any legacy nailing configuration.
- Cisco Systems, Inc. strongly recommends that users configure inverse DNS nailing on a PU that does *not* support generic LUs or a PU that has the **generic-pool** command configured with the **deny** keyword specified.

SSL Encryption Support

- You must be running an IOS image with IPsec support. The strength of the SSL encryption support on the TN3270 server is determined by the strength of the IPsec image.

Related Features and Technologies

The TN3270 Server Connectivity Enhancements feature is an enhancement to the existing TN3270 server feature that is documented in the “TN3270 Server” chapters of the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1 and the *Cisco IOS Bridging and IBM Networking Command Reference, Volume II*, Release 12.1.

Inverse DNS Nailing

- Domain Name System (DNS) technology

SSL Encryption Support

- Secure Socket Layer (SSL) technology

Related Documents

- *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1
- *Cisco IOS Bridging and IBM Networking Command Reference, Volume II*, Release 12.1

Supported Platforms

Router Requirements

The TN3270 Server Connectivity features are supported on the following router platforms:

- Cisco 7500 series—Supports CIP adapters
- Cisco 7200 series—Supports the ECPA and PCPA adapters
- Cisco 7000 series with RSP7000—Supports CIP adapters

You must configure the TN3270 server features on the virtual interface of a CMCC adapter. For a CIP, the virtual interface is either 2. For the CPA adapters, ECPA and PCPA, the virtual interface is port 0.

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.

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB website on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

- No new or modified RFCs are supported by this feature.

Prerequisites

This section describes the prerequisites of the TN3270 server feature enhancements introduced in Cisco IOS release 12.1(5)T. These are divided into router and mainframe prerequisites and then grouped by software (for example, microcode and VTAM) or feature (for example, SSL Encryption Support).

Router Prerequisites

Microcode prerequisites

The Cisco TN3270 server consists of a system image and a microcode image virtually bundled as one combined image. The following versions of hardware microcode are supported for the TN3270 Server Connectivity Enhancements feature on the CIP and CPA in Cisco IOS Release 12.1(5)T:

- CIP hardware microcode—CIP28-1 and later.
- CPA hardware microcode—XCPA28-1 and later.

For additional information about what is supported in the various releases of the Cisco IOS software and the CIP microcode, see the information on Cisco Connection Online (CCO).

Inverse DNS Nailing

- To use inverse DNS Nailing on the TN3270 server, you must specify which DNS servers are required to resolve the TN3270 server client IP addresses. To specify the DNS servers, use the following commands:
 - **ip domain-lookup**
 - **ip domain-name**
 - **ip name-server**

SSL Encryption Support

- You must be running an IOS image with IPsec support. The strength of the SSL encryption support on the TN3270 server is determined by the strength of the IPsec image.
- A server digital certificate loaded on the TN3270 router is required to support TN33270 Server Security Enhancement.

Mainframe prerequisites

VTAM prerequisites

Mainframe hosts using Systems Network Architecture (SNA) with the TN3270 server must be running VTAM V4R2 or later.



Note

You can use VTAM V3R4, but DLUR operation is not supported in V3R4 and proper DDDLU operation may require program temporary fixes (PTFs) to be applied to VTAM.

Dynamic LU Naming

- The TN3270 server creates and deletes LUs dynamically on VTAM by sending Reply PSID poweron and Reply PSID poweroff messages when the named LU is connected and disconnected. In order to properly delete the dynamically created LUs, the following APARS should be applied to VTAM:
 - OW41274
 - OW41686
 - OW40315
- You must replace the default exit ISTEXCSD with the VTAM User Exit for TN3270 Name Pushing, which you can download from the IBM website: <http://www.ibm.com>. This exit causes VTAM to ignore the LUSEED parameter on the PU statement, and instead use the SLU name sent by the router in the subvector 86 when a client connects in. If you do not configure this exit, VTAM ignores the subvector 86 and the specified LU name.

Configuration Tasks

The following sections describe configuration tasks for the TN3270 Server Connectivity Enhancements feature:

- Configuring Dynamic LU Naming, page 6
- Configuring Inverse DNS Nailing, page 8
- Configuring SSL Encryption Support, page 10

See the “Configuration Examples” section on page 16 for sample configurations.

For a complete description of the new or modified TN3270 Server commands in this feature module, refer to the “Command Reference” section on page 22. For a complete description of the rest of the TN3270 Server commands in this feature module, refer to the “TN3270 Server Commands” chapter in the *Cisco IOS Bridging and IBM Networking Command Reference, Volume II*, Release 12.1.

Configuring Dynamic LU Naming

Perform the tasks in the following sections to configure dynamic LU naming according to the type of PU:

- Configuring a Listen-Point PU to Define DLUR PUs using Dynamic LU Naming, page 6
- Configuring a Listen-Point PU to Define Direct PUs using Dynamic LU Naming, page 7


Mainframe Configuration Notes

- You must replace the default exit ISTEXCSD with the VTAM User Exit for TN3270 Name Pushing, which you can download from the IBM website: <http://www.ibm.com>. This exit causes VTAM to ignore the LUSEED parameter on the PU statement, and instead use the SLU name sent by the router in the subvector 86 when a client connects in. If you do not configure this exit, VTAM ignores the subvector 86 and the specified LU name.
- If you specify the LUSEED operand for the PU definition in VTAM and the subvector 86 specifies an LU name, the VTAM User Exit for TN3270 Name Pushing ignores the LUSEED operand.
- If you do not specify the LUSEED operand on the mainframe, and the subvector 86 is not present, then the VTAM User Exit for TN3270 Name Pushing cannot generate an LU name. VTAM does not log this failure, and the TN3270 server does not receive the ACTLU request.

Configuring a Listen-Point PU to Define DLUR PUs using Dynamic LU Naming

To configure a listen-point PU on the internal LAN interface on the CMCC adapter, and to define DLUR PUs using dynamic LU naming, use the following commands beginning in TN3270 configuration mode.

Command	Purpose
Step 1 Router(cfg-tn3270)# listen-point <i>ip-address</i> [tcp-port <i>number</i>]	Specifies the IP address and TCP port number to create a listen point. The default TCP port number is 23. This command changes the configuration mode from TN3270 to listen-point.

Command	Purpose
Step 2 Router(tn3270-lpoint)# pu <i>pu-name idblk-idnum dlur</i> [lu-seed <i>lu-name-stem</i>]	Creates a DLUR PU and enters listen-point PU configuration mode. The lu-seed optional keyword specifies the LU name that the client uses when a specific LU name request is needed.
Step 3 Router(tn3270-lpoint-pu)# lu deletion { always normal non-generic never named }	Specifies whether the TN3270 server sends a REPLY-PSID poweroff request to VTAM to delete the corresponding LU when a client disconnects.  Note You must specify the named option when configuring dynamic LU naming on the PU.

When you use the **pu** command, you enter listen-point PU configuration mode and can use all other commands in this task list. Values that you enter for siftdown commands (such as the **lu deletion** command) in listen-point PU configuration mode will override values that you previously entered in listen-point or TN3270 server configuration mode. For more information about configuring siftdown commands, see the “Configuring TN3270 Siftdown Commands” section in the “Configuring TN3270 Server” chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1.


**Note**

This task table focuses on configuring the Dynamic LU Naming enhancement only. For more complete TN3270 server configuration task information, see the “Configuring TN3270 Server” chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1.

Configuring a Listen-Point PU to Define Direct PUs using Dynamic LU Naming

To configure a listen-point PU on the internal LAN interface on the CMCC adapter and configure direct PUs using dynamic LU naming, use the following commands beginning in listen-point configuration mode.

Command	Purpose
Step 1 Router(cfg-tn3270)# listen-point <i>ip-address</i> [tcp-port [<i>number</i>]]	Specifies the IP address and TCP port number to create a listen point. The default TCP port number is 23. This command changes the configuration mode from TN3270 to listen-point.

Command	Purpose
Step 2 Router(tn3270-lpoint)# pu <i>pu-name idblk-idnum type adapter-number lsap [rmac rmac] [rsap rsap] [lu-seed lu-name-stem]</i>	Creates a direct PU and enters listen-point PU configuration mode. The lu-seed optional keyword specifies the LU name that the client uses when a specific LU name request is needed.
Step 3 Router(tn3270-lpoint-pu)# lu deletion { always normal non-generic never named }	Specifies whether the TN3270 server sends a REPLY-PSID poweroff request to VTAM to delete the corresponding LU when a client disconnects.  Note You must specify the named option when configuring dynamic LU naming on the PU.

When you use the **pu** command, you enter listen-point PU configuration mode and can use all other commands in this task list. Values that you enter for sift-down commands (such as the **lu deletion** command) in listen-point PU configuration mode will override values that you previously entered in listen-point or TN3270 server configuration mode. For more information about configuring sift-down commands, see the “Configuring TN3270 Sift-down Commands” section in the “Configuring TN3270 Server” chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1.

**Note**

This task table focuses on configuring the Dynamic LU Naming enhancement only. For more complete TN3270 server configuration task information, see the “Configuring TN3270 Server” chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1.

Configuring Inverse DNS Nailing

Perform the tasks in the following section to configure the different methods of Inverse DNS Nailing feature:

- Nailing Clients to Pools by IP Address, page 9
- Nailing Clients to Pools by Device Name, page 9
- Nailing Clients to Pools by Device Name using a Domain ID, page 9
- Nailing Clients to Pools by Domain Name, page 10
- Nailing Clients to Pools by Domain Name Using a Domain ID, page 10

**Note**

You can configure Inverse DNS Nailing five different ways by using the same commands. This task table section presents the five different configuration methods as separate task tables.

**Note**

These task tables focus on configuring the Inverse DNS Nailing enhancement. For more complete TN3270 server configuration task information, see the “Configuring TN3270 Server” chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1.

**Note**

Use the **domain-id** command only when you are going to configure the **client pool** command with the **name** keyword and *DNS-domain-identifier* option specified or with the **domain-id** keyword specified.

Nailing Clients to Pools by IP Address

To nail a client to a pool of LUs by IP address, use the following commands beginning in TN3270 configuration mode.

	Command	Purpose
Step 1	Router(cfg-tn3270)# listen-point <i>ip-address</i> [tcp-port <i>number</i>]	Specifies the IP address and TCP port number to create a listen point. The default TCP port number is 23. This command changes the configuration mode from TN3270 to listen-point.
Step 2	Router(tn3270-lpoint)# client ip <i>ip-address</i> [<i>ip-mask</i>] pool <i>poolname</i>	Nails a client located at the IP address to a pool.

Nailing Clients to Pools by Device Name

To nail a client to a pool of LUs by device name, use the following commands beginning in TN3270 configuration mode.

	Command	Purpose
Step 1	Router(cfg-tn3270)# listen-point <i>ip-address</i> [tcp-port <i>number</i>]	Specifies the IP address and TCP port number to create a listen point. The default TCP port number is 23. This command changes the configuration mode from TN3270 to listen-point.
Step 2	Router(tn3270-lpoint)# client name <i>DNS-name</i> pool <i>poolname</i>	Nails a client located at the DNS device name to a pool.

Nailing Clients to Pools by Device Name using a Domain ID

To nail a client to a pool of LUs by device name using a domain id, use the following commands beginning in TN3270 configuration mode.

	Command	Purpose
Step 1	Router(cfg-tn3270)# domain-id <i>DNS-domain-identifier</i> <i>DNS-domain</i>	(Optional) Specifies a domain name suffix to be appended to the configured machine names to form a fully qualified name.
Step 2	Router(cfg-tn3270)# listen-point <i>ip-address</i> [tcp-port <i>number</i>]	Specifies the IP address and TCP port number to create a listen point. The default TCP port number is 23. This command changes the configuration mode from TN3270 to listen-point.
Step 3	Router(tn3270-lpoint)# client name <i>DNS-name</i> <i>DNS-domain-identifier</i> pool <i>poolname</i>	Nails a client located at the IP address to a pool.

Nailing Clients to Pools by Domain Name

To nail a client to a pool of LUs by domain name, use the following commands beginning in TN3270 configuration mode.

	Command	Purpose
Step 1	Router(cfg-tn3270)# listen-point <i>ip-address</i> [tcp-port <i>number</i>]	Specifies the IP address and TCP port number to create a listen point. The default TCP port number is 23. This command changes the configuration mode from TN3270 to listen-point.
Step 2	Router(tn3270-lpoint)# client domain-name <i>DNS-domain</i> pool <i>poolname</i>	Nails a client located at the domain-name to a pool.

Nailing Clients to Pools by Domain Name Using a Domain ID

To nail a client to a pool of LUs by domain name using a domain id, use the following commands beginning in TN3270 configuration mode.

	Command	Purpose
Step 1	Router(cfg-tn3270)# domain-id <i>DNS-domain-identifier</i> <i>DNS-domain</i>	(Optional) Specifies a domain name suffix to be appended to the configured machine names to form a fully qualified name.
Step 2	Router(cfg-tn3270)# listen-point <i>ip-address</i> [tcp-port <i>number</i>]	Specifies the IP address and TCP port number to create a listen point. The default TCP port number is 23. This command changes the configuration mode from TN3270 to listen-point.
Step 3	Router(tn3270-lpoint)# client domain-id <i>DNS-domain-identifier</i> pool <i>poolname</i>	Nails a client located at the domain-id to a pool.

Configuring SSL Encryption Support

Perform the tasks in the following sections to configure the SSL Encryption feature:

- Obtain Server Digital Certificate from Certificate Authority
- Load Server Digital Certificate onto the flash of the TN3270 router

- Configuring Security, page 11 (Required)
- Configuring the Profile, page 11 (Required)
- Configuring the Default Profile, page 12 (Optional)
- Configuring a Listen Point for Security, page 12 (Optional)

Obtaining Server Digital Certificate from Certificate Authority

In order to obtain a sever digital certificate, first create a Certificate Signing Request Pointer to Readme.csr file.

The certificate must be in PEM or Base64 format.

Once you obtain the server digital certificate from a CA such as Verisign, append the private key file onto the end of the digital certificate.

Load Server Digital Certificate onto the flash of the TN3270 router

Digital Certificate must be copied to the flash card on the TN3270 router

e.g. copytftp:servercert.pem slot0:

Configuring Security

To configure security on the TN3270 server, use the following command beginning in TN3270 server configuration mode:

Command	Purpose
Router(cfg-tn3270) # security	Enables security on the TN3270 server and enters TN3270 security configuration mode.

Enabling and Disabling Security

To enable and disable security on the TN3270 server, use the following commands beginning in TN3270 security configuration mode:

Command	Purpose
Router(tn3270-security) # enable	(Optional) Enables security in the TN3270 server.
Router(tn3270-security) # disable	(Optional) Disables the security feature in the TN3270 server.

Configuring the Profile

To configure a security profile on the TN3270 server, use the following command beginning in TN3270 security configuration mode:

Command	Purpose
Router(tn3270-security)# profile <i>profilename</i> { ssl none }	Specifies a name and a security protocol for a security profile.

Configuring the Profile Options

To configure the security profile options, use the following commands beginning in TN3270 profile configuration mode:

Command	Purpose
Router(tn3270-sec-profile)# keylen { 40 128 }	Specifies the maximum bit length for the session encryption key for the TN3270 server.
Router(tn3270-sec-profile)# encryptorder [DES] [3DES] [RC4] [RC2] [RC5]	Specifies the encryption algorithm for the TN3270 SSL Encryption Support.
Router(tn3270-sec-profile)# servercert <i>location</i>	Specifies the location of the TN3270 server's security certificate in the flash memory. This command reads the security certificate from the specified location.
Router(tn3270-sec-profile)# certificate reload	(Optional) Reads the profile security certificate from the file specified in the servercert command.

Configuring the Default Profile

To configure the default security profile name to be applied to the listen-points, use the following command beginning in TN3270 security configuration mode:



Note

The **profile** command must be specified before configuring a default-profile.

Command	Purpose
Router(tn3270-security)# default-profile <i>profilename</i>	Specifies the name of the profile to be applied to the listen-points by default.

Configuring a Listen Point for Security

To configure a listen-point for security, use the following command beginning in TN3270 listen-point configuration mode:



Note

This task table focuses on configuring a listen-point in the SSL Encryption Support enhancement. For more complete TN3270 server configuration task information, see the "Configuring TN3270 Server" chapter in the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.1.

**Note**

The **sec-profile** command is optional if the **default-profile** command has been configured.

Command	Purpose
Router(tn3270-lpoint)# sec-profile <i>profilename</i>	Specifies the security profile to be associated with a listen-point.

Verifying TN3270 Server Connectivity Enhancements

Verifying Dynamic LU Naming on the TN3270 server

Complete the following steps to verify the Dynamic LU Naming enhancement:

- Step 1** Issue the **show extended channel tn3270-server** command. Confirm that lu-deletion is set to **named**.

```
Router# show extended channel 3/2 tn3270-server
```

```
<current stats> < connection stats > <response time(ms)>
server-ip:tcp      lu in-use  connect  disconn  fail    host    tcp
172.28.1.106:23    510      1       12      11     0      54    40
172.28.1.107:23    511      0        0        0     0       0     0
172.28.1.108:23    255      0        0        0     0       0     0
total              1276     1
configured max_lu 20000
idle-time 0          keepalive 1800      unbind-action disconnect
tcp-port 23          generic-pool permit no timing-mark
→ lu-termination unbind lu-deletion named
```

- Step 2** To verify that dynamic LU naming is configured on the TN3270 server, issue the **show extended channel tn3270-server pu** command. Confirm that lu-deletion is set to **named**.

```
Router# show extended channel 6/2 tn3270-server pu pu1
```

```
name(index)  ip:tcp      xid  state  link  destination r-lsap
PU1(1)       172.18.4.18:23  91903315 ACTIVE dlur  NETA.SHPU1

idle-time 0          keepalive 1800      unbind-act discon  generic-poolperm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
→ lu-termination unbind lu-deletion named
```

Verifying Inverse DNS Nailing on the TN3270 server

Complete the following steps to verify the Inverse DNS Nailing enhancement:

- Step 1** To list all nailing statements with a specific nailed-domain name, issue the **show extended channel tn3270-server nailed-domain** command.

```
Router# show extended channel 1/2 tn3270-server nailed-domain .cisco.com
CISCO.COM listen-point 172.18.4.18 pool PCPOOL
```

- Step 2** To list all nailing statements with a specific nailed machine name, issue the **show extended channel tn3270-server nailed-name** command.

```
Router# show extended channel 1/2 tn3270-server nailed-name myclient.cisco.com
MYCLIENT.CISCO.COM    listen-point 172.18.4.18  pool PCPOOL
HISCLIENT.CISCO.COM   listen-point 172.18.4.18  pool UNIXPOOL
HERCLIENT.CISCO.COM   listen-point 172.18.4.19  pool GENERALPOOL
```

Verifying SSL Encryption Support on the TN3270 server

Complete the following steps to verify the SSL Encryption Support enhancement:

- Step 1** To verify the security profile on the TN3270 server, issue the **show extended channel tn3270-server security** command using the **sec-profile** option. Confirm that the status is enabled (status: ENABLE), and that the security certificate is loaded (Certificate Loaded: YES).

```
Router# show extended channel 3/2 tn3270-server security sec-profile cert40
→ status:ENABLE Default Profile: (Not Configured)
Name                Active LUs  keylen encryptorder      Mechanism
→ CERT40             0          40    RC4 RC2 RC5 DES 3DES    SSL
Servercert:slot0:coach188.pem
→ Certificate Loaded:YES Default-Profile:NO
```

- Step 2** To verify the security profile on the TN3270 server listen-point, issue the **show extended channel tn3270-server security** command using the **listen-point** option. Confirm that the status is enabled (status: ENABLE) and that the state is active (State ACTIVE).

```
Router# show extended channel 3/2 tn3270-server security listen-point 172.18.5.188
→ status:ENABLE Default Profile: (Not Configured)
IPaddress    tcp-port  Security-Profile  active-sessions  Type  State
→ 172.18.5.188  23        CERT40            0                 Secure  ACTIVE
Active Sessions using Deleted Profile:0
```

Troubleshooting Tips

Dynamic LU Naming

- You must replace the default exit ISTEXCSD with the VTAM User Exit for TN3270 Name Pushing, which you can download from the IBM website: <http://www.ibm.com>. This exit causes VTAM to ignore the LUSEED parameter on the PU statement, and instead use the SLU name sent by the router in the subvector 86 when a client connects in. If you do not configure this exit, VTAM ignores the subvector 86 and the specified LU name.
- If the LUSEED operand is specified on the mainframe, but the subvector 86 requires an LU name, the VTAM User Exit for TN3270 Name Pushing ignores the LUSEED operand.
- If the LUSEED operand is not specified on the mainframe, and the subvector 86 is not present, then the VTAM User Exit for TN3270 Name Pushing cannot generate an LU name. VTAM does not log this failure, and the TN3270 server does not receive the ACTLU request. The TN3270 server displays the following message:

```
*Apr 17 12:40:53:%CIP2-3-MSG:slot2 :
%TN3270S-3-NO_DYN_ACTLU_REQ_RCVD
  No ACTLU REQ received on LU JJD1.6
```

- Specify the INCLUD0E=YES parameter on VTAM so that the TN3270 server will always receive the LU name generated by the VTAM exit.

Inverse DNS Nailing

- If an inverse DNS lookup fails it could be because the DNS server is unavailable (either because it was not configured, or because it is down). In this case, you cannot tell if the client is nailed because it does not have a name. To complicate the scenario, assume there wasn't a legacy nailing match, but the PU supports LUs that have been assigned from a generic pool. In this situation, the client will disconnect and the router will display the following console message:

```
A connection attempt from client <ip address> was refused because its DNS name could not be obtained.
```

This action removes any potential security risk but presents potential disadvantages—the client could be denied a valid LU, and the generic-pool permit and deny settings may be ignored. For these reasons, it is strongly recommended that users configure the Inverse DNS Nailing enhancement on a PU that does *not* support LUs that have been assigned from a generic pool, or a PU that has the **generic-pool** command configured with the **deny** keyword specified.

- If an inverse DNS lookup succeeds, but the name is not nailed or the client has no machine name, then the client is not nailed and the TN3270 server reverts to the legacy LU nailing process.

Monitoring and Maintaining TN3270 Server Connectivity Enhancements

Dynamic LU Naming

To monitor the status of the Dynamic LU Naming enhancement, use the following commands in EXEC mode:

Command	Purpose
Router# show extended channel tn3270-server	Displays current server configuration parameters and the status of the PUs defined for the TN3270 server.
Router# show extended channel tn3270-server pu client-name	Displays configuration parameters for a PU and all the LUs currently attached to the PU, with the client machine name substituted for the client IP address.

Inverse DNS Nailing

To monitor the status of the Inverse DNS Nailing enhancement, use the following commands in EXEC mode:

Command	Purpose
Router# show extended channel tn3270-server client-name	Displays information about all connected clients with a specific machine name.
Router# show extended channel tn3270-server nailed-domain	Lists all nailing statements with a specific nailed-domain name.

Command	Purpose
Router# show extended channel tn3270-server nailed-name	Lists all nailing statements with a specific nailed-machine name.
Router# show extended channel tn3270-server pu client-name	Displays configuration parameters for a PU and all the LUs currently attached to the PU, with the client machine name substituted for the client IP address.

Configuration Examples

This section provides the following configuration examples:

- Dynamic LU Naming Example, page 16
- Inverse DNS Nailing Examples, page 17
- SSL Encryption Support Examples, page 19

Dynamic LU Naming Example

Router configuration

The following router configuration is an example of the TN3270 server configured with LU pooling. A listen-point PU is configured to define DLUR PUs using dynamic LU naming. Note the following lines in the configuration:

- The **lu deletion** command must be configured with the **named** option.
- The PU pu1 is defined with `lu-seed abc##pqr`. Using hexadecimal numbers for `##`, the LU names for this PU are ABC01PQR, ABC02PQR, ABC03PQR.... up to ABCFFPQR. Similarly, the PU pu2 is defined with `lu-seed pqr###`. Using decimal numbers for `###`, the LU names for this PU are PQR001, PQR002... up to PQR255.

The LUs ABC01PQR through ABC32PQR and PQR100 through PQR199 are allocated to the pool SIMPLE. The LUs ABC64PQR through ABC96PQR and PQR010 through PQR035 are allocated to the pool PCPOOL. The remaining LUs are in the generic pool.

```
tn3270-server
pool simple cluster layout 1s
pool pcpool cluster layout 4s1p
→ lu deletion named
dlur neta.shek neta.mvsd
  lsap tok 15 04
    link she1 rmac 4000.b0ca.0016
listen-point 172.18.4.18
→ pu pu1 91903315 tok 16 08 lu-seed abc##pqr
!
!The following statement allocates LUs ABC01PQR through ABC32PQR to the pool named
!simple.
!
  allocate lu 1 pool simple clusters 50
!
!The following statement allocates LUs ABC64PQR through ABC96PQR to the pool named
!pcpool.
!
  allocate lu 100 pool pcpool clusters 10
pu pu2 91913315 dlur lu-seed pqr###
```

```

!
!The following statement allocates LUs PQR010 through PQR035 to the pool named pcpool.
!
  allocate lu 10 pool pcpool clusters 5
!
!The following statement allocates LUs PQR100 through PQR199 to the pool named simple.
!
  allocate lu 100 pool simple clusters 100

```

Mainframe configuration

The following mainframe configuration is an example of the VTAM configuration that can be used if the TN3270 server is configured with the Dynamic LU Naming enhancement.



Note

PU's are defined with the LUGROUP command. It is not necessary to specify an LUSEED. If the LUSEED operand is specified, it is ignored.



Note

You must specify the INCLUD0E=YES parameter on VTAM so that the TN3270 server receives the LU name generated by the VTAM exit.

```

SWN72022 VBUILD TYPE=SWNET
PU1      PU      ADDR=01,                X
          PUTYPE=2,                      X
          IDBLK=919,                     X
          IDNUM=03315,                   X
          INCLUD0E=YES,                  X
          LUGROUP=MYLUS
*
PU2      PU      ADDR=01,                X
          PUTYPE=2,                      X
          IDBLK=919,                     X
          IDNUM=13315,                   X
          INCLUD0E=YES,                  X
          LUGROUP=MYLUS

```

Inverse DNS Nailing Examples

Nailing Clients to Pools by Device Name, Domain Name, and Domain ID using a Domain ID

The following router configuration shows an example of commands used to define the TN3270 server with LU pools using inverse DNS nailing:

```

tn3270-server
  domain-id 2 .cisco.com
  domain-id 20 .yahoo.com
  pool GENERAL cluster layout 4slp
  pool TEST cluster layout 4slp
  listen-point 172.18.5.168
  pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
    allocate lu 1 pool GENERAL clusters 1
    client name lucy49.cisco.com pool GENERAL
    client name george 20 pool TEST
    client name arthur 20 pool TEST
    client name tyson 20 pool TEST
    client name daisy 20 pool TEST
  listen-point 172.18.5.169
  pu T240CB 91922364 token-adapter 31 12 rmac 4000.4000.0002
    allocate lu 1 pool TEST clusters 50

```

```
client domain-name cisco.com pool GENERAL
client domain-id 20 pool TEST
```

Nailing Clients to Pools by IP Address

The following router configuration shows an example of commands used to define the TN3270 server with LU pools using inverse DNS nailing. In this example, the **client pool** command is configured with the **ip** keyword. The command nails the client at IP address 10.1.2.3 with an IP mask of 255.255.255.0 to the pool named OMAHA:

```
tn3270-server
pool OMAHA cluster layout 10s1p
listen-point 172.18.4.18
→ client ip 10.1.2.3 255.255.255.0 pool OMAHA
```

Nailing Clients to Pools by Device Name

The following router configuration shows an example of commands used to define the TN3270 server with LU pools using inverse DNS nailing. In this example the **client pool** command is configured with the **name** keyword. The command nails the client at device name george-isdn29.cisco.com to the pool named GENERAL:

```
tn3270-server
pool GENERAL cluster layout 4s1p
listen-point 172.18.5.168
pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
allocate lu 1 pool GENERAL clusters 1
→ client name george-isdn29.cisco.com pool GENERAL
```

Nailing Clients to Pools by Device Name using a Domain ID

The following router configuration shows an example of commands used to define the TN3270 server with LU pools using inverse DNS nailing. In this example the **client pool** command is configured with the **name** keyword and the optional *DNS-domain-identifier* argument. The command nails the client at device name lucy-isdn49.cisco.com to the pool named GENERAL:

```
tn3270-server
→ domain-id 23 .cisco.com
pool GENERAL cluster layout 4s1p
listen-point 172.18.5.168
pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
allocate lu 1 pool GENERAL clusters 1
→ client name lucy-isdn49 23 pool GENERAL
```

Nailing Clients to Pools by Domain Name

The following router configuration shows an example of commands used to define the TN3270 server with LU pools using inverse DNS nailing. In this example the **client pool** command is configured with the **domain-name** keyword. The command nails any client at domain name .cisco.com to the pool named GENERAL:

```
tn3270-server
pool GENERAL cluster layout 4s1p
listen-point 172.18.5.168
pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
allocate lu 1 pool GENERAL clusters 1
→ client domain-name .cisco.com pool GENERAL
```

Nailing Clients to Pools by Domain Name Using a Domain ID

The following router configuration shows an example of commands used to define the TN3270 server with LU pools using inverse DNS nailing. In this example the **client pool** command is configured with the **domain-id** keyword. The command nails any client at domain name .cisco.com to the pool named GENERAL:

```
tn3270-server
→ domain-id 23 .cisco.com
   pool GENERAL cluster layout 4slp
   listen-point 172.18.5.168
   pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
   allocate lu 1 pool GENERAL clusters 1
→ client domain-id 23 pool GENERAL
```

SSL Encryption Support Examples

Mainframe configuration

The following mainframe configuration is an example of the VTAM configuration that can be used if the SSL Encryption Support enhancement is configured:

```
example PU definition:
*
BMPU4  PU      ADDR=01,
           PUTYPE=2,
           LOGAPPL=NETTMVSD,
           LUGROUP=BMCL13, LUSEED=BMPU4###,
           PACING=8, VPACING=8,
           IDBLK=919,
           IDNUM=36821
*
BMPU5  PU      ADDR=01,
           PUTYPE=2,
           LOGAPPL=NETTMVSD,
           LUGROUP=BMCL13, LUSEED=BMPU5###,
           PACING=8, VPACING=8,
           IDBLK=919,
           IDNUM=46821
*
*
BMPU6  PU      ADDR=01,
           PUTYPE=2,
           LOGAPPL=NETTMVSD,
           USSTAB=USSTCPMF,
           DLOGMOD=D4C32782,
           PACING=8, VPACING=8,
           IDBLK=919,
           IDNUM=56821
*
BMPU6001 LU    LOCADDR=01
BMPU6002 LU    LOCADDR=02
BMPU6003 LU    LOCADDR=03
BMPU6004 LU    LOCADDR=04
BMPU6005 LU    LOCADDR=05
BMPU6006 LU    LOCADDR=06
BMPU6007 LU    LOCADDR=07
BMPU6008 LU    LOCADDR=08
BMPU6009 LU    LOCADDR=09
BMPU6010 LU    LOCADDR=10
.
.
```

```
BMPU6255 LU    LOCADDR=255
*
```

Simple SSL Encryption Support Example

The following router configuration shows an example of commands used to define a simple configuration of the SSL Encryption Support enhancement. In this configuration, listen-point 172.18.5.187 is a secured listen-point using security profile cert40. Note that the security profile is using all of the default parameters.

```
interface Channel3/2
 ip address 172.18.5.185 255.255.255.248
 no keepalive
 lan TokenRing 15
  source-bridge 15 1 500
  adapter 15 4000.b0ca.0015
 lan TokenRing 16
  source-bridge 16 1 500
  adapter 16 4000.b0ca.0016
 tn3270-server
 security
  profile CERT40 SSL
  servercert slot0:verisign187.pem
 listen-point 172.18.5.187
 sec-profile CERT40
 pu BMPU5    91946821 token-adapter 15 08 rmac 4000.b0ca.0016
```

Complex SSL Encryption Support Example

The following router configuration shows an example of commands used to define a more complex configuration of the SSL Encryption Support enhancement:

- Listen-point 172.18.5.186 is a non-secured listen point.
- Listen-point 172.18.5.187 is a secured listen-point using security-profile cert128 with the encryption order specified and a keylen of 128 which implies strong (domestic) encryption.
- Listen-point 172.18.5.188 is a secured listen-point using security profile cert40 with default security-profile parameters.

```
interface Channel3/2
 ip address 172.18.5.185 255.255.255.248
 no keepalive
 lan TokenRing 15
  source-bridge 15 1 500
  adapter 15 4000.b0ca.0015
 lan TokenRing 16
  source-bridge 16 1 500
  adapter 16 4000.b0ca.0016
 tn3270-server
 security
  profile CERT128 SSL
  servercert slot0:verisign128.pem
  encryptorder RC4 RC2 DES
  keylen 128
  profile CERT40 SSL
  servercert slot0:coach188.pem
 listen-point 172.18.5.186
 pu BMPU4    91946821 token-adapter 15 04 rmac 4000.b0ca.0016
 listen-point 172.18.5.187
 sec-profile CERT128
 pu BMPU5    91956821 token-adapter 15 08 rmac 4000.b0ca.0016
 listen-point 172.18.5.188
 sec-profile CERT40
```

```
pu BMPU6      91966821 token-adapter 15 0C rmac 4000.b0ca.0016
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.1 command reference publications.

- **certificate reload**
- **client pool**
- **default-profile**
- **disable (TN3270)**
- **domain-id**
- **enable (TN3270)**
- **encryptorder**
- **keylen**
- **lu deletion**
- **profile**
- **pu dlur (listen-point)**
- **sec-profile**
- **security (TN3270)**
- **servercert**
- **show extended channel tn3270-server client-name**
- **show extended channel tn3270-server nailed-domain**
- **show extended channel tn3270-server nailed-name**
- **show extended channel tn3270-server pu**
- **show extended channel tn3270-server security**

certificate reload

To load the X.509 digital certificate from the file specified in the **servercert** command, use the **certificate reload** profile command.

certificate reload

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Profile configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines There is not a **no** form for this command.
The TN3270 server must be configured for security.

Examples The following example configures the TN3270 server with SSL Encryption Support to read the profile security certificate from the file specified in the **servercert** command:

```
certificate reload
```

Related Commands	Command	Description
	servercert	Specifies the location of the TN3270 server's X.509 digital certificate in the flash memory.

client pool

To nail clients to pools, use the **client pool** listen-point configuration command. Use the **no** form of this command to remove clients from pools.

client {[**ip** *ip-address* [*ip-mask*]] | [**name** *DNS-name* [*DNS-domain-identifier*]] | [**domain-name** *DNS-domain*] | [**domain-id** *DNS-domain-identifier*]} **pool** *poolname*

no client {[**ip** *ip-address* [*ip-mask*]] | [**name** *DNS-name* [*DNS-domain-identifier*]] | [**domain-name** *DNS-domain*] | [**domain-id** *DNS-domain-identifier*]} **pool** *poolname*

Syntax Description		
ip <i>ip-address</i>		Remote client IP address.
<i>ip-mask</i>		(Optional) Mask applied to the remote device address. The mask is part of the matching function that determines whether a client is governed by the nailing statement. The default is 255.255.255.255. Multiple client IP addresses in the same subnet can be nailed to the same pool.
name <i>DNS-name</i>		Alphanumeric string that specifies a client machine name. The string can contain up to 24 characters. If a valid <i>DNS-domain-identifier</i> is not present, this name must be fully qualified. If this name is not fully qualified, any dot that forms the boundary between the DNS-name and the DNS-domain must be included here if it is not already present in the DNS-domain.
<i>DNS-domain-identifier</i>		(Optional) A numeric identifier that specifies a domain name. The valid value range is 1 to 255. Each domain-id command statement can have only one <i>DNS-domain-identifier</i> value.
domain-name <i>DNS-domain</i>		Alphanumeric string that specifies a domain name suffix, including all dots (.) but not delimited by dots. The string can contain up to 80 characters. All dots must be included when the string is appended to a configured DNS-name. If the DNS-domain starts with a dot, then the dot must be included if it is not already at the end of the DNS-name.
domain-id <i>DNS-domain-identifier</i>		Numeric identifier that specifies that a domain name suffix will be appended to the name configured in the domain-id command. The valid value range is 1 to 255. Each domain-id command statement can have only one <i>DNS-domain-identifier</i> value. The domain-id is originally specified in the domain-id command.
<i>poolname</i>		Specifies a unique pool name. The pool name cannot exceed eight characters.

Defaults No default behavior or values.

Command Modes Listen-point configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated in Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to include the name , domain-name , and domain-id keywords. The name of the command was changed from client ip pool to client pool .

Usage Guidelines

If the pool is configured while LUs are in use, existing clients are allowed to complete their sessions. A pool name can be identical to an LU name. When assigning an LU, the TN3270 server searches the LU name space first for specific requests, such as connections that specify a device name on CONNECT or LU name in the terminal type negotiation. The request is assumed to be directed to the specific LU rather than to the pool. Make sure the LU names do not conflict.

Examples**Nailing Clients to Pools by IP Address**

The following is an example of the **client pool** command with the **ip** keyword configured. The command nails the client at IP address 10.1.2.3 with an IP mask of 255.255.255.0 to the pool named OMAHA:

```
tn3270-server
pool OMAHA cluster layout 10slp
listen-point 172.18.4.18
→ client ip 10.1.2.3 255.255.255.0 pool OMAHA
```

Nailing Clients to Pools by Device Name

The following is an example of the **client pool** command with the **name** keyword configured. The command nails the client at device name george-isdn29.cisco.com to the pool named GENERAL:

```
tn3270-server
pool GENERAL cluster layout 4slp
listen-point 172.18.5.168
pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
allocate lu 1 pool GENERAL clusters 1
→ client name george-isdn29.cisco.com pool GENERAL
```

Nailing Clients to Pools by Device Name using a Domain ID

The following is an example of the **client pool** command with the **name** keyword and the optional *DNS-domain-identifier* argument configured. The command nails the client at device name lucy-isdn49.cisco.com to the pool named GENERAL:

```
tn3270-server
→ domain-id 23 .cisco.com
pool GENERAL cluster layout 4slp
listen-point 172.18.5.168
pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
allocate lu 1 pool GENERAL clusters 1
→ client name lucy-isdn49 23 pool GENERAL
```

Nailing Clients to Pools by Domain Name

The following is an example of the **client pool** command with the **domain-name** keyword configured. The command nails any client at domain name .cisco.com to the pool named GENERAL:

```
tn3270-server
  pool GENERAL cluster layout 4s1p
  listen-point 172.18.5.168
  pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
  allocate lu 1 pool GENERAL clusters 1
→ client domain-name .cisco.com pool GENERAL
```

Nailing Clients to Pools by Domain Name Using a Domain ID

The following is an example of the **client pool** command with the **domain-id** keyword configured. The command nails any client at domain name cisco.com to the pool named GENERAL:

```
tn3270-server
→ domain-id 23 .cisco.com
  pool GENERAL cluster layout 4s1p
  listen-point 172.18.5.168
  pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
  allocate lu 1 pool GENERAL clusters 1
→ client domain-id 23 pool GENERAL
```

Related Commands

Command	Description
listen-point	Defines an IP address for the TN3270 server.
pool	Defines pool names for the TN3270 server and specifies the number of screens and printers in each logical cluster.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host, or enters listen-point PU configuration mode.
pu (listen-point)	Creates a PU entity that has a direct link to a host, or enters listen-point PU configuration mode.
tn3270-server	Starts the TN3270 server on a CMCC adapter or enters TN3270 configuration mode.
domain-id	Specifies a domain name suffix to be appended to the configured machine names to form a fully qualified name.

default-profile

To specify the name of the profile to be applied as a default to all the listening points, use the **default-profile** security command. To disable the default profile specification, use the **no** form of this command.

default-profile *profilename*

no default-profile *profilename*

Syntax Description	<i>profilename</i>	Profile name should already be configured.
Defaults	No default profile.	
Command Modes	Security configuration	
Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines

If this command is configured, this profile name and all of its attributes will be associated with all listen-points that do not specify an individual profile with the **sec-profile** command.

Profile names cannot be duplicated.

Entering the **no** form of this command removes the default specification and any listen-points that do not have the **sec-profile** command specified will revert to a non-secure mode.

This command has no retroactive effect. If a listen-point is specified using the **listen-point** command, and the **sec-profile** command was already configured for that listen-point then all client connections to that listen-point will be secure.

If a listen-point is specified using the listen-point command, and the **default-profile** command is not configured, then all client connections to that listen-point will not be secure. However, if the **default-profile** command is later configured, then all now connections to that listen-point will be secure using the specified **default-profile**. This will not affect the non-secure connections.

The following example specifies DOMESTIC as the default profile name for all clients connecting to listen-point 10.10.10.1 until the **default-profile FOO** command is configured. Once the **default-profile FOO** command is configured, all new client connections will use FOO as the default profile.

```
tn3270
 security
  profile NOSECURITY none
  default-profile DOMESTIC
pu DIRECT 012ABCDE tok 0 04
  default-profile FOO
listen-point 10.10.10.1
```

Related Commands

Command	Description
sec-profile	Specifies the security profile to be associated with a listen-point.
profile	Specifies a name and a security protocol for a security profile.

disable (TN3270)

To disable the security feature in the TN3270 server, use the **disable** (TN3270) security configuration command.

disable

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Security configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines Configuring the **disable** (TN3270) command does not terminate any active secure or non-secure connections. This command specifies that all new connections established with the TN3270 server will be non-secure. If a client initiates a change cipher specification for an existing secure connection then the TN3270 server will process the request.

There is not a **no** form for this command. The **enable** command is equivalent to the **no** form of this command.

Examples The following example turns off the security feature in the TN3270 server so that all new connections established with the TN3270 server will be non-secure:

```
disable
```

Related Commands	Command	Description
	enable (TN3270)	Turns on security in the TN3270 server.

domain-id

To specify a domain name suffix that the TN3270 server appends to a configured machine name to form a fully-qualified name when configuring inverse DNS nailing, use the **domain-id** TN3270 server configuration command. To disable this specification, use the **no** form of this command.

domain-id *DNS-domain-identifier DNS-domain*

no domain-id *DNS-domain-identifier DNS-domain*

Syntax Description

<i>DNS-domain-identifier</i>	A numeric identifier that specifies the domain name. The valid value range is 1 to 255. Each domain-id statement can have only one <i>DNS-domain-identifier</i> value. This identifier is also used in the client pool command.
<i>DNS-domain</i>	An alphanumeric string that specifies a domain name suffix, including all dots (.) but not delimited by dots. The string can contain no more than 80 characters. All dots must be included when the string is appended to a configured DNS-name. If the DNS-domain starts with a dot, then the dot must be included if it is not already at the end of the DNS-name.

Defaults

No default behavior or values.

Command Modes

TN3270 server configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

The user can configure up to 255 domain names, one per statement.

This command must be configured you configure the **client pool** command with either the **domain-id** keyword or the **name** keyword and the optional *DNS-domain-identifier* argument.

Examples

In the following example, the **domain-id** command specifies 23 as the *DNS-domain-identifier* for the .cisco.com domain name. All clients nailed to the pool GENERAL will use .cisco.com as the domain name suffix. For example, the client name ally-isdn1 will become ally-isdn1.cisco.com.

```
tn3270-server
→ domain-id 23 .cisco.com
   pool GENERAL cluster layout 4slp
   listen-point 172.18.5.168
   pu T240CA 91922363 token-adapter 31 12 rmac 4000.4000.0001
   allocate lu 1 pool GENERAL clusters 1
→ client name ally-isdn1 23 pool GENERAL
```

Related Commands

Command	Description
client pool	Nails clients to pools.

enable (TN3270)

To turn on security in the TN3270 server, use the **enable** (TN3270) security configuration mode command.

enable

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Security configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines There is not a **no** form for this command.

If the **security** command has been disabled, then issuing this command does not affect existing connections.

This command is not displayed in the **show running configuration** command output because the security functionality is enabled by default.

Examples The following example turns on security in the TN3270 server:

```
enable
```

Related Commands	Command	Description
	security	Enables security on the TN3270 server.
	disable (TN3270)	Turns off the security feature in the TN3270 server.

encryptorder

To specify the security encryption algorithm for the SSL Encryption Support, use the **encryptorder** profile configuration command.

encryptorder [DES] [3DES] [RC4] [RC2] [RC5]

Syntax Description	Parameter	Description
	DES	Specifies the DES encryption algorithm.
	3DES	Specifies the 3DES encryption algorithm.
	RC4	Specifies the RC4 encryption algorithm.
	RC2	Specifies the RC2 encryption algorithm.
	RC5	Specifies the RC5 encryption algorithm.

Defaults

The default encryption order is RC4, RC2, RC5, DES, 3DES for domestic software. The default encryption order is RC4, RC2, DES for exportable software.

Command Modes

Profile configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

There is not a **no** form for this command.

These algorithms may be entered in any order, but can be specified only once per **encryptorder** command.

Exportable versions of software cannot accept the 3DES or RC5 encryption algorithms.

Examples

The following example specifies RC4, DES, and RC2 as the encryption algorithms:

```
tn3270
 security
  profile DOMESTIC SSL
    encryptorder RC4 DES RC2
```

keylen

To specify the maximum bit length for the session encryption key for the TN3270 server with security, use the **keylen 128** security mode command. To disable this specification and thereby set the key length to the default of 40 bits, use the **no** form of this command or **keylen 40**.

keylen {40 | 128}

no keylen {40 | 128} The length is optional on the no form of this command

Syntax Description

40	Specifies the bit length for the encryption keys to 40.
128	Specifies the bit length for the encryption keys to 128.

Defaults

The default encryption key length is 40 bits.

Command Modes

Profile configuration.

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Exportable software versions cannot accept encryption key lengths greater than 40 bits.

Entering the **no** form of this command resets the length to the default value of 40 bits.

If the key length is changed, all new connections will use the new value. If an active session renegotiates its security specifications, it will use the new key length value.

Examples

The following example specifies the maximum encryption key length value to 128 bits:

```
tn3270-server
 security
  profile DOMESTIC SSL
  encryptorder RC4 DES RC2
  keylen 128
```

lu deletion

To specify whether the TN3270 server sends a REPLY-PSID poweroff request to VTAM to delete the corresponding LU when a client disconnects, use the **lu deletion** TN3270 server configuration command. Use the **no** form of this command to remove LU deletion from the current configuration scope.

lu deletion {**always** | **normal** | **non-generic** | **never** | **named**}

no lu deletion

Syntax Description

always	Always delete dynamic LUs upon disconnect.
normal	Delete screen LUs only upon disconnect.
non-generic	Delete only specified LUs upon disconnect.
never	Never delete LUs upon disconnect.
named	Delete only named LUs only upon disconnect.

Defaults

The default keyword is **never**.

Command Modes

TN3270 server configuration—The **lu deletion** command at this level applies to all PUs supported by the TN3270 server.

Listen-point configuration—The **lu deletion** command at this level applies to all PUs defined at the listen point.

Listen-point PU configuration—The **lu deletion** command at this level applies only to the specified PU.

DLUR PU configuration—The **lu deletion** command at this level applies to all PUs defined under DLUR configuration mode.

PU configuration—The **lu deletion** command at this level applies only to the specified PU.



Note

The **lu deletion** command is a siftdown command, so it can be used at any of the configuration command modes shown. The most recent **lu deletion** command in the PU configuration takes precedence.

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated in to Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to add the named keyword.

Usage Guidelines

Use the **always** keyword of the **lu deletion** command when you have only screen LUs, and they are all different sizes. This prevents screen LUs from attaching to a previously used LU with an incompatible screen size.

Use the **normal** keyword of the **lu deletion** command when you have both screen and printer LUs. This is important because printers are acquired by the host application, and not logged on manually. If VTAM deletes the LU, then there is nothing for a host application (such as CICS) to acquire.

You can use the **non-generic** mode of LU deletion if VTAM can support deletion of specifically-named LUs. (The support of this mode is not currently available in VTAM, as of VTAM version 4.4.1.)

Use the **never** mode of LU deletion when you have only screen LUs and they all use the same screen size.

Use the **named** keyword of the **lu deletion** command when you have configured dynamic LU names from the TN3270 server side.

Examples

Following is an example of the **lu deletion** command specifying that the TN3270 server send a REPLY-PSID poweroff request to delete only screen LUs upon session disconnect for any PUs supported by the TN3270 server:

```
tn3270-server
  lu deletion normal
```

Following is an example of the **lu deletion** command configuring a listen-point PU to define DLUR PUs using dynamic LU naming:

```
tn3270-server
listen-point 172.18.4.18
pu pul 05D9901 dlur
  lu deletion named
```

Related Commands

Command	Description
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
pu (listen-point)	Creates a PU entity that has a direct link to a host and enters listen-point PU configuration mode.

profile

This command creates or modifies a security profile. To create a profile, specify the name of the new profile along with the security type. To modify a security profile, specify the name of the profile without the security type. The security type is only required when creating a profile. Using the security type when modifying a profile will result in an error.

To specify a name and a security protocol for a security profile, use the **profile** configuration command. To remove this name and protocol specification, use the **no** form of this command.

Create a new profile:

```
profile profilename {ssl | none}
```

Modify an existing profile:

```
profile profilename
```

Delete a profile:

```
no profile profilename {ssl | none}
```

Syntax Description		
	<i>profilename</i>	String of alphanumeric characters which specify a name for a security profile. The character range is from 1 to 24. Profile names cannot be duplicated.
	none	Specifies that this profile will not use a security protocol. Sessions using this profile will not use any security.
	ssl	Specifies that this profile will use the ssl 3.0 security protocol. This implies that the initial exchange between the client and the server is the "Client Hello" message.

Defaults No default behavior or values.

Command Modes Security configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines Profile names cannot be duplicated.

Entering the **no** form of this command deletes the profile definition and all of its subcommand definitions (**encryptorder**, **servercert**, **keylen**, **certificate reload** commands). Entering the **no** form of this command deletes the **sec-profile** command specifications on all listen-points where it is currently defined.

Entering the profile command moves the user into the profile configuration mode. Entering the **no** form of the command moves the user into the security configuration mode.

This command has no retroactive effect.

Examples

The following example specifies FOO as the profile name and ssl as the security protocol. When the **no profile FOO** command is configured, all new client connections will be non-secure.

```
tn3270-server
 security
  profile FOO ssl
  keylen 40/128
  servercert slot0:foo
  certificate reload
listen-point 10.10.10.1
 sec-profile FOO
 pu DIRECT 012ABCDE tok 0 04
 no profile FOO
```

Related Commands

Command	Description
security	Enables security on the TN3270 server.
sec-profile	Specifies the security profile to be associated with a listen-point.
default-profile	Specifies the name of the profile to be applied to the listening-points by default.


pu dlur (listen-point)

To create a PU entity that has no direct link to a host or to enter listen-point PU configuration mode, use the **pu dlur** listen-point configuration command. Use the **no** form of this command to remove the PU entity.

```
pu pu-name idblk-idnum dlur [lu-seed lu-name-stem]
```

```
no pu pu-name idblk-idnum dlur [lu-seed lu-name-stem]
```

Syntax Description

<i>pu-name</i>	Name that uniquely identifies this PU.
<i>idblk-idnum</i>	Value for this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server only enforces uniqueness within the set of DLUR PUs.
lu-seed <i>lu-name-stem</i>	<p>(Optional) LU name that the client uses when a specific LU name request is needed. The format is <i>x...x##</i> or <i>x...x###</i> where <i>x...x</i> is an alphanumeric string. When ## is specified, it is replaced with the LU LOCADDR in hexadecimal digits to form the complete LU name. When ### is specified, decimal digits are used, padded with leading zeroes to make three characters. The first <i>x</i> must be alphabetic (A through Z), or one of the following symbols: \$, #, @. The entire string, including the # symbols, must not exceed 8 characters.</p> <p>The # symbols are allowed in the middle of the lu-seed string. For example, NC##RAL or USA###NC are valid strings. The # symbols cannot be the first characters in the string. For example, ##CISCO is not valid because the first character of the LU name cannot be a number. But ####DOT is valid because the # symbols in the second, third and fourth place are used for LU names. There must be at least two to three consecutive # symbols in the string. For example, SH# or CD#D is not valid. A string without # symbols is not valid. For example, CISCONC is not valid. You must not split the # symbols. For example, SH#NC# and SH#D#NC# are not valid.</p>
	
Note	The # sign can signify a value or be used as a symbol

Defaults

No PU is defined.

Command Modes

Listen-point configuration

Command History

Release	Modification
11.2	This command was introduced.
11.2(18)BC	Listen-point PU configuration was added.
12.0(5)T	This command was integrated in Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to add the lu-seed option and <i>lu-name-stem</i> argument. The lu-seed naming format was modified.

Usage Guidelines

If the PU is already created, the **pu dlur** command without any arguments starts listen-point PU configuration mode. In this mode you can modify an existing listen-point DLUR PU entity.

You should define the DLUR before you configure the listen-point DLUR PU.

A typical usage for the IP address is to reserve an IP address for each application. For example, clients wanting to connect to TSO specify an IP address that is defined with PUs that have LOGAPPL=TSO.

If the **lu-seed** option is not configured, the PU name is used as the implicit lu-seed to generate the LU name. If the **lu-seed** option is configured, then there is an explicit LU name.

If the explicit LU names conflict, the TN3270 server will reject the PU configuration. If the implicit LU names (i.e., the PU names) conflict, the TN3270 server will accept the PU definitions, but the LU names will consist of a modified, truncated version of the PU name and the LOCADDR.

Table 1 LU Seed Name Examples

Valid LU Seed Syntax	Invalid LU Seed Syntax
NC##RAL	NC#RAL
USA##NC	#GEORGE
#####	

Examples

The following example defines three PUs in the listen point with an IP address of 172.18.4.18:

```
tn3270-server
listen-point 172.18.4.18
 pu p0 05D99001 dlur
 pu p1 05D99002 dlur
 pu p2 05D99003 dlur
```

The following is an example of the TN3270 server configured with LU pooling. A listen-point PU is configured to define DLUR PUs using the dynamic LU naming. Note that the **lu deletion** command must be configured with the **named** option. The PU pu1 is defined with lu-seed abc##pqr. Using hexadecimal numbers for ##, the LU names for this PU are ABC01PQR, ABC02PQR, ABC0APQR.... up to ABCFFPQR. Similarly, the PU pu2 is defined with lu-seed pqr###. Using decimal numbers for ###, the LU names for this PU are PQR001, PQR002... up to PQR255.

The LUs ABC01PQR through ABC32PQR and PQR100 through PQR199 are allocated to the pool SIMPLE. The LUs ABC64PQR through ABC96PQR and PQR010 through PQR035 are allocated to the pool PCPOOL. The remaining LUs are in the generic pool.:

```
tn3270-server
pool simple cluster layout 1s
pool pcpool cluster layout 4s1p
→ lu deletion named
dlur neta.shek neta.mvsd
  lsap tok 15 04
    link shel rmac 4000.b0ca.0016
listen-point 172.18.4.18
→ pu pu1 91903315 tok 16 08 lu-seed abc##pqr
  allocate lu 1 pool simple clusters 50
  allocate lu 100 pool pcpool clusters 10
→ pu pu2 91913315 dlur lu-seed pqr###
  allocate lu 10 pool pcpool clusters 5
  allocate lu 100 pool simple clusters 100
```

Related Commands

Command	Description
dlur	Enables the SNA session switch function on the CMCC adapter, or enters DLUR configuration mode.
listen-point	Defines an IP address for the TN3270 server.

sec-profile

To specify a security profile to be associated with a listen-point, use the **sec-profile** listen-point configuration command. To remove this specification, use the no form of this command.

sec-profile *profilename*

no sec-profile *profilename*

Syntax Description	<i>profilename</i>	This name is originally specified in the profile command. It consists of a string of alphanumeric characters which specify the security profile name to be associated with a listen-point. The character range is from 1 to 24.
---------------------------	--------------------	--

Defaults No default behavior or values.

Command Modes TN3270 listen-point configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines If this command is not entered or if the **no** form of the command is entered, the security profile reverts to the profile configured in the **default-profile** command. If no default-profile is specified, then the listen-point will accept only non-secure connections

This command has no retroactive effect.

Examples The following example specifies FOO as the security profile name for all new clients connecting to listen-point 10.10.10.1 until the **sec-profile FOO1** command is configured. Once the **sec-profile FOO1** command is configured, all new client connections to 10.10.10.1 will use FOO1 as the profile name.

```
tn3270-server
security
profile FOO ssl
  keylen 40/128
  servercert slot0:foo
  certificate reload
profile FOO1 ssl
  keylen 40
  servercert slot0:foo1
  certificate reload
listen-point 10.10.10.1
sec-profile FOO
pu DIRECT 012ABCDE tok 0 04
Sec-profile F001
```

Related Commands	Command	Description
	profile	Specifies a name and a security protocol for a security profile.
	default-profile	Specifies the name of the profile to be applied to the listening-points by default.

security (TN3270)

To enable or modify security and enter the TN3270 security configuration mode, use the **security** command. To disable security on the TN3270 server, use the **no** form of this command.

security

no security

Syntax Description This command has no arguments or keywords.

Defaults The default is enabled.

Command Modes TN3270 server configuration

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines If the **no** form of this command is configured, any listen-points that contain a security profile definition will be re-configured, and thus no longer secure. Sessions already established on the listen-point will continue to run in the same mode (secure or non-secure) as originally configured. If sessions are active on a listen-point, a message will be sent to the IOS console stating that the listen-point has sessions running with an outdated security specification. A shutdown/restart sequence must be performed on the listen-point if the user wants the sessions on the listen-point to use the new specification.

Entering this command moves the user into the security configuration mode. Entering the **no** form of this command moves the user to a TN3270 server configuration mode.

This command has no retroactive effect.

Examples In the following example, security is enabled on the TN3270 server:

```
tn3270-server
 security
```

Related Commands	Command	Description

servercert

To specify the location of the TN3270 server's security certificate in the router's flash memory, use the **servercert** profile configuration command.

servercert *location*

Syntax Description	<i>location</i>	Hexadecimal string can contain up to 63 characters which specify the location of the server's certificate in the flash memory.
Defaults	No default behavior or values.	
Command Modes	Profile configuration	
Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines

The certificate must be created offline. It cannot be created using the Cisco IOS software. Third party software may be used, or a Windows-based utility that can be downloaded from http://www._____. The certificate should be in PEM or Base64 format. The output from the certificate generation contains two parts: The certificate and the private key. These two files should be concatenated together to create a single certificate file containing the certificate and the private key in PEM or Base64 format.

The resultant file containing the certificate and the private key should be stored on the flash via TFIP, and the location entered here. This certificate is in X.509 format, signed by a Certificate Authority (CA). If the file does not exist in the flash memory when the command is entered, the command is not rejected. An error message is displayed indicating that the file does not exist. The first time this command is configured the certificate is automatically loaded from the specified location. Subsequent changes to the location file will not cause the certificate to be read automatically into system's memory. The certificate reload command must be issued to read the certificate into memory. If the user exits from the profile configuration mode without configuring the **servercert** command, a warning message is displayed. The warning message specifies that it is mandatory to configure a **servercert**.

The following example specifies that slot0:foo is the location of the security certificate:

```
tn3270-server
 security
  profile FOO ssl
  keylen 512
  servercert slot0:foo
  certificate reload
```

Related Commands

Command	Description
profile	Specifies a name and a security protocol for a security profile.

show extended channel tn3270-server client-name

To display information about all connected clients with a specific machine name, use the **show extended channel tn3270-server client-name EXEC** command.

show extended channel *slot*/*virtual channel* tn3270-server client-name *name*

Syntax Description		
	<i>slot</i>	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
	<i>virtual channel</i>	Virtual channel number.
	<i>name</i>	Specifies the client machine name. This name is specified originally in the client pool command.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines There is not a **no** form for this command.

Examples The following is sample output from the **show extended channel tn3270-server client-name** command:

```
Router# show extended channel 4/2 tn3270-server client-name dhcp-rtp-34-40.cisco.com
Note: if state is ACT/NA then the client is disconnected

lu   name      client-name          nail state   model   frames in out  idle for
6    dhcp-rtp-34-40.cisco. N   P-ACTLU  3278S2E  1       0       0:1:59

pu is T240CA, lu is DYNAMIC unbound, negotiated TN3270E
bytes 101 in, 0 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
response time buckets 0 0 0 0 0
average total response time 0 average IP response time 0
number of transactions 0
Note: if state is ACT/NA then the client is disconnected
lu   name      client-name          nail state   model   frames in out  idle for
7    T240DA07 dhcp-rtp-34-40.cisco. N   P-BIND   3278S2E  4       3       0:1:32
pu is T240CA, lu is DYNAMIC unbound, negotiated TN3270E
bytes 199 in, 407 out; RuSize 256 in, 256 out; NegRsp 0 in, 0 out
pacing window 0 in, 0 out; credits 0 in, queue-size 0 in, 0 out
response time buckets 0 0 0 0 0
average total response time 0 average IP response time 0
number of transactions 0
Total 2 clients found using dhcp-rtp-34-40.cisco.com
```

Table 2 describes significant fields in the display.

Table 2 *show extended channel tn3270-server client-name Field Descriptions*

Field	Description
lu <i>locaddr</i>	LOCADDR of the LU.
name <i>lu-name</i>	If the PU is directly connected, then the name shown is the one generated by the seed. If DLUR, then only the unqualified portion is shown. The NETID portion will be the same as the current DLUS.
client-name <i>name</i>	Client's machine name.
nail	Status of LU nailing, either Y or N.
state <i>lu-state</i>	LU state values and their meanings: <ul style="list-style-type: none"> • UNKNOWN—LU in an undefined state. • INACTIVE—LU did not receive ACTLU. • ACT/NA—LU received ACTLU and acknowledged positively. • P-SDT—LU is bound but there is no SDT yet. • ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet has connected and is waiting for ACTLU. • P-NTF/AV—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Awaiting a buffer to send DACTLU response. • P-PSID—Awaiting NMVT Reply PSID response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model <i>model</i>	IBM 3278 model type of client; blank if STATIC LU.
frames in <i>number</i>	Number of frames sent inbound to the host.
frames out <i>number</i>	Number of frames sent outbound from the host.
idle for <i>time</i>	Time the client has been idle. The time is in HH:MM:SS.
pu is <i>pu-name</i>	Name of the PU.
lu is <i>type</i>	Whether LU is DYNAMIC or STATIC.
negotiated <i>type</i>	Whether client is TN3270 or TN3270E.
bytes in / out <i>number/number</i>	Total number of bytes sent to/received from the host.
RuSize in / out <i>number/number</i>	RU size as configured in the bind.

Table 2 *show extended channel tn3270-server client-name Field Descriptions (continued)*

Field	Description
NegRsp in / out <i>number/number</i>	Number of SNA negative responses sent to/received from the host.
pacing window in / out <i>number/number</i>	SNA pacing window as configured in the bind.
credits in <i>number</i>	Number of frames that can be sent inbound without requiring an isolated pacing response.
queue- size in <i>number</i>	Number of SNA frames waiting to be sent to the host that are blocked and are waiting for a pacing response.
queue-size out <i>number</i>	SNA frames not yet acknowledged by an isolated pacing response by the TN3270 server.
response time buckets	Number of transactions in each response-time “bucket” for the specified LU. The bucket boundaries are defined using the response-time group command.
average total response time	Average response time (in tenths of seconds) for the total number of response-time transactions.
average IP response time	Average IP transit response time in tenths of seconds for the total number of response-time transactions.
number of transactions	Total number of response-time transactions across all response-time buckets.

show extended channel tn3270-server nailed-domain

To list all nailing statements with a specific nailed-domain name, use the **show extended channel tn3270-server nailed-domain** EXEC command.

show extended channel *slot/virtual channel* **tn3270-server nailed-domain** *name*

Syntax Description	Parameter	Description
	<i>slot</i>	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
	<i>virtual channel</i>	Virtual channel number.
	<i>name</i>	Specifies the nailed-domain name. This name is specified originally in the client pool command.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines There is not a **no** form for this command.

Examples The following is sample output from the **show extended channel tn3270-server nailed-domain** command:

```
Router# show extended channel 1/2 tn3270-server nailed-domain .cisco.com
CISCO.COM listen-point 172.18.4.18 pool PCPOOL
```

Table 3 describes significant fields in the display.

Table 3 *show extended channel tn3270-server nailed-domain Field Descriptions*

Field	Description
CISCO.COM	Nailed domain name.
listen point <i>ipaddress</i>	Listen point IP address under which the client pool command was configured.
pool <i>poolname</i>	Pool name to which the client is nailed.

show extended channel tn3270-server nailed-name

To list all nailing statements with a specific nailed machine name, use the **show extended channel tn3270-server nailed-name** EXEC command.

show extended channel *slot/virtual channel* **tn3270-server nailed-name** *name*

Syntax Description	Parameter	Description
	<i>slot</i>	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
	<i>virtual channel</i>	Virtual channel number.
	<i>name</i>	Specifies the nailed machine name. This name is specified originally in the client pool command.

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines There is not a **no** form for this command.

Examples The following is sample output from the **show extended channel tn3270-server nailed-name** command:

```
Router# show extended channel 1/2 tn3270-server nailed-name myclient.cisco.com
MYCLIENT.CISCO.COM    listen-point 172.18.4.18  pool PCPOOL
HISCLIENT.CISCO.COM  listen-point 172.18.4.18  pool UNIXPOOL
HERCLIENT.CISCO.COM  listen-point 172.18.4.19  pool GENERALPOOL
```

Table 4 describes significant fields in the display.

Table 4 *show extended channel tn3270-server nailed-name* Field Descriptions

Field	Description
MYCLIENT.CISCO.COM	Fully qualified domain name of nailed client.
listen point <i>ipaddress</i>	Listen point IP address under which the client pool command was configured.
pool <i>poolname</i>	Pool name to which the client is nailed.

show extended channel tn3270-server pu

To display configuration parameters for a PU and all the LUs currently attached to the PU, including the LU cluster layout and pool name, use the **show extended channel tn3270-server pu** EXEC command.

```
show extended channel slot/virtual channel tn3270-server pu pu-name [cluster | client-name]
```

Syntax Description		
<i>slot</i>	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.	
<i>virtual channel</i>	Virtual channel number.	
<i>pu-name</i>	Name that uniquely identifies this PU.	
cluster	(Optional) Display cluster information for the LUs within the pool.	
client-name	(Optional) Display client name information for the LUs within the pool.	

Defaults No default behavior or values.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	11.2(2.1)	ACT/NA replaced ACTIVE status for LU states. A note was added to the output to describe its meaning.
	11.2(18)BC	The cluster keyword was added.
	12.0(5)T	The following fields were added to the output display: <ul style="list-style-type: none"> • lu-termination • lu-deletion
	12.1(5)T	The client-name optional keyword was added.

Usage Guidelines The **show extended channel tn3270-server pu** command is valid only on the virtual channel interface. The display shown depends on whether the PU is a direct PU or a SNA session switch PU.

The output for the **show extended channel tn3270-server pu** command varies based on using the optional **cluster** keyword. Without the **cluster** keyword, the output column headings for the LU information appear as “model,” “frames in out,” and “idle for.”

When you use the **cluster** keyword, the output column headings for the LU information appear as “cluster,” “pool,” and “count.” The cluster heading lists the specific cluster within the pool to which the LU belongs along with the specific cluster layout after the slash.

The pool heading identifies the corresponding pool name, and the count heading identifies the cluster number out of the total number of clusters in the pool.

There is not a **no** form for this command.

Examples

This example shows a sample router configuration and the corresponding output using the **show extended channel tn3270-server pu** command:

```
interface Channel6/1
  no ip address
  no keepalive
  csna E160 40
!
interface Channel6/2
  ip address 172.18.4.17 255.255.255.248
  no keepalive
  lan TokenRing 15
    source-bridge 15 1 500
    adapter 15 4000.b0ca.0015
  lan TokenRing 16
    source-bridge 16 1 500
    adapter 16 4000.b0ca.0016
tn3270-server
  pool PCPOOL cluster layout 4s1p
  pool SIMPLE cluster layout 1a
  pool UNIXPOOL cluster layout 49s1p
  dlur NETA.SHEK NETA.MVSD
  lsap token-adapter 15 04
  link SHE1 rmac 4000.b0ca.0016
  listen-point 172.18.4.18 tcp-port 23
  pu PU1 91903315 dlur
    allocate lu 1 pool PCPOOL clusters 10
    allocate lu 51 pool UNIXPOOL clusters 2
    allocate lu 200 pool SIMPLE clusters 50
  listen-point 172.18.4.19 tcp-port 2023
  pu PU2 91913315 token-adapter 16 08
    allocate lu 1 pool UNIXPOOL clusters 2
    allocate lu 101 pool SIMPLE clusters 100
    allocate lu 201 pool PCPOOL clusters 10
```

Following is an example of the output from the **show extended channel tn3270-server pu** command without the cluster keyword for a PU named PU1:

```
Router# show extended channel 6/2 tn3270-server pu pu1
```

```
name(index)   ip:tcp           xid  state    link  destination r-lsap
PU1(1)        172.18.4.18:23  91903315 ACTIVE  dlur  NETA.SHPU1

idle-time     0      keepalive 1800      unbind-act discon  generic-poolperm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
lu-termination unbind lu-deletion never
bytes 27019 in, 73751 out; frames 1144 in, 869 out; NegRsp 0 in, 0 out
actlus 5, dactlus 0, binds 5
Note: if state is ACT/NA then the client is disconnected

lu  name  client-ip:tcp      nail state  model  frames in out  idle for
1   SHED1001 161.44.100.162:1538 N  ACT/SESS 3278S2E 228 172 0:0:2
51  SHED1051 161.44.100.162:1539 N  ACT/SESS 3278S2E 240 181 0:0:2
151 SHED1151 161.44.100.162:1536 N  ACT/SESS 327802E 212 160 0:0:5
152 SHED1152 161.44.100.162:1537 N  ACT/SESS 3278S2E 220 166 0:0:4
200 SHED1200 161.44.100.162:1557 N  ACT/SESS 3278S2E 244 184 0:0:2
```

Following is an example of the output from the **show extended channel tn3270-server pu** command with the **cluster** keyword for a PU named PU1. In the example below, 1/1a identifies cluster 1 with a layout of 1a, which contains 1 LU of any type.

```
Router# show extended channel 6/2 tn3270-server pu pu1 cluster

name(index)  ip:tcp          xid  state  link  destination  r-lsap
PU1(1)      172.18.4.18:23  91903315 ACTIVE  dlur  NETA.SHPU1

idle-time    0      keepalive 1800      unbind-act discon  generic-poolperm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
lu-termination unbind lu-deletion never
bytes 27489 in, 74761 out; frames 1164 in, 884 out; NegRsp 0 in, 0 out
actlus 5, dacltus 0, binds 5
Note: if state is ACT/NA then the client is disconnected

lu  name  client-ip:tcp      nail state  cluster  pool  count
1  SHED1001 161.44.100.162:1538  N  ACT/SESS 1/4s1p  PCPOOL  1/5
51 SHED1051 161.44.100.162:1539  N  ACT/SESS 1/49s1p UNIXPOOL 1/50
151 SHED1151 161.44.100.162:1536  N  ACT/SESS 1/1a  :GENERIC 1/1
152 SHED1152 161.44.100.162:1537  N  ACT/SESS 1/1a  :GENERIC 1/1
200 SHED1200 161.44.100.162:1557  N  ACT/SESS 1/1a  SIMPLE  1/1
```

**Note**

If the cluster layout is very long, only the first 8 bytes are displayed under the cluster column. The pool called: GENERIC is shown for all LUs that are not allocated to any specific pool name.

Following is an example of the output from the **show extended channel tn3270-server pu** command with the **client-name** keyword for a PU named JADOEPU:

```
Router# show extended channel 1/2 tn3270-server pu jadoepu client-name

name(index)  ip:tcp          xid  state  link  destination  r-lsap
JADOEPU(1)  172.18.5.168:23  91922362 ACTIVE  tok 31 4000.4000.0001 04 10

idle-time    0      keepalive 30      unbind-act discon  generic-pool perm
ip-preced-screen 0 ip-preced-printer 0 ip-tos-screen 0 ip-tos-printer 0
lu-termination unbind lu-deletion never
bytes 824 in, 2619 out; frames 36 in, 39 out; NegRsp 0 in, 0 out
actlus 4, dacltus 0, binds 3
Note: if state is ACT/NA then the client is disconnected

lu  name  client-name      nail state  model frames in out  idle for
1  VINCDP01 never connected  Y  ACT/NA      1  1  2:31:43
2  VINCDP02 never connected  Y  ACT/NA      1  1  2:31:43
5  VINDG005 HERCLIENT.CISCO.COM  Y  ACT/SESS 327904E 22 21 0:0:6
6  VINDG006 HISCLIENT.CISCO.COM  Y  ACT/NA      327904E 12 12 1:44:47

client-ip      mask          nail-type  lu-first  lu-last
10.20.30.40    screen        1          2
20.30.40.50    screen        9          10

client-name      nail-type  lu-first  lu-last
MYCLIENT.CISCO.COM  screen    5          10
.CISCO.COM        screen    11         15
```

Table 5 describes significant fields in the display.

Table 5 *show extended channel tn3270-server pu Field Descriptions*

Field	Description
name (index) <i>pu-name</i> (<i>index</i>)	Name and index of the PU as configured.
ip:tcp <i>ip-addr:tcp-port</i>	IP address and TCP port number configured for the PU.
xid <i>number</i>	Configured XID—idblk and idnum.
state <i>pu-state</i>	Possible pu-state values and their meanings: <ul style="list-style-type: none"> • SHUT—PU is configured but in shut state. • RESET—Link station of this PU is not active. • TEST—PU is sending a TEST to establish link. • XID—TEST is responded, XID is sent. • P-ACTPU—Link station is up but no ACTPU is received. • ACTIVE—ACTPU is received and acknowledged positively. • ACT/BUSY—Awaiting host to acknowledge the SSCP-PU data. • WAIT—Waiting for PU status from CMCC adapter. • UNKNOWN—Direct PU in undefined state. • P-RQACTPU-R—PU is pending request ACTPU response. • P-ACTIVE—DLUR PU and direct PU states disagree. • P-DACTPU—PU is pending DACTPU. • OTHER—State is an undefined value.
link <i>type</i>	LINK type is either internal adapter type and internal adapter number, or dlur if it is a SNA Session Switch PU.
destination <i>mac-address or pu-name</i>	If a direct PU, then it is the destination MAC address, otherwise, it is the name of the partner PU.
r-lsap <i>number number</i>	Remote and local SAP values.
idle-time <i>number</i>	Configured idle-time for this PU.
keepalive <i>number</i>	Configured keepalive for this PU.
unbind-act <i>type</i>	Configured unbind action for LUs on this PU.
generic-pool <i>type</i>	Configured generic-pool for LUs on this PU.
ip-preced-screen <i>number</i>	IP precedence value for screen LUs on this PU.
ip-preced-printer <i>number</i>	IP precedence value for printer LUs on this PU.
ip-tos-screen <i>number</i>	IP Type of Service (TOS) value for screen LUs on this PU.
ip-tos-printer <i>number</i>	IP TOS value for printer LUs on this PU.

Table 5 *show extended channel tn3270-server pu Field Descriptions (continued)*

Field	Description
lu-termination	Value configured in the PU for the lu termination siftdown command. The lu termination command specifies whether a TERMSELF or UNBIND RU is sent by the TN3270 server when a client turns off the device or disconnects. The possible values are: <ul style="list-style-type: none"> • Termself—Termination of all sessions and session requests associated with an LU is ordered upon disconnect. • Unbind—Termination of the session by the application is requested upon LU disconnect.
lu-deletion	Value configured in the PU for the lu deletion siftdown command. The lu deletion command specifies whether the TN3270 server sends a REPLY-PSID poweroff request to VTAM to delete the corresponding LU when a client disconnects. The possible values are: <ul style="list-style-type: none"> • Always—Dynamic LUs for this PU are always deleted upon disconnect. • Normal—Only screen LUs for this PU are deleted upon disconnect. • Non-generic—Only specified LUs for this PU are deleted upon disconnect. • Never—None of the LUs for this PU are ever deleted upon disconnect.
bytes in / out <i>number/number</i>	Total number of bytes sent to/received from the host for this PU.
frames in / out <i>number/number</i>	Total number of frames sent to/received from the host for this PU.
NegRsp in / out <i>number/number</i>	Total number of SNA negative responses sent to/received from the host.
actlus <i>number</i>	Total number of ACTLUs received from the host.
dactlus <i>number</i>	Total number of DACTLUs received from the host.
binds <i>number</i>	Total number of BINDs received from the host.
lu <i>number</i>	LOCADDR of the LU.
name <i>lu-name</i>	Name of the TN3270 LU.
client-name <i>ip-addr:tcpport</i>	Client's IP address and TCP port number.
nail	Status of LU nailing, either Y or N

Table 5 *show extended channel tn3270-server pu Field Descriptions (continued)*

Field	Description
state <i>lu-state</i>	<p>LU states and their meanings:</p> <ul style="list-style-type: none"> • UNKNOWN—LU in an undefined state. • INACTIVE—LU didn't receive ACTLU. • ACT/NA—LU received ACTLU and acknowledged positively. If a client ip address is shown then the client is disconnected. • P-SDT—LU is bound but there is no SDT yet. • ACT/SESS—LU is bound and in session. • P-ACTLU—Telnet has connected and is awaiting ACTLU. • P-NTF/av—Awaiting host notify-available response. • P-NTF/UA—Awaiting host notify-unavailable response. • P-RESET—Waiting for a buffer to send DACTLU response. • P-PSID—Waiting for NMVT Reply psid response. • P-BIND—Waiting for host to send bind. • P-UNBIND—Awaiting host unbind response. • WT-UNBND—Waiting for client to acknowledge disconnection. • WT-SDT—Waiting for client to acknowledge SDT.
model <i>model</i>	IBM 3278 model type of client.
frames in <i>number</i>	Number of frames sent inbound to the host.
frames out <i>number</i>	Number of frames sent outbound from the host.
idle for <i>time</i>	Time the client has been idle. The time is in HH:MM:SS.
client-ip	Remote client IP address.
mask	Current network mask.
nail-type	LU nailing type, screen or printer.
lu-first	First LU address in the range.
lu-last	Last LU address in the range, if one is specified in the client configuration command.
client-name	Client machine name or domain name.
nail-type	LU nailing type, screen or printer.
lu-first	First LU address in the range.
lu-last	Last LU address in the range, if one is specified in the client configuration command.

■ show extended channel tn3270-server pu

Related Commands	Command	Description
	pu (listen-point)	Creates a PU entity that has a direct link to a host, or enters listen-point PU configuration mode.
	pu dlur (listen-point)	Creates a PU entity that has no direct link to a host, or enters listen-point PU configuration mode.
	allocate lu	Assigns LUs to a pool.

show extended channel tn3270-server security

To display information about the TN3270 security enhancement, use the **show extended channel tn3270-server security** EXEC command.

```
show extended channel slot/virtual channel tn3270-server security [[sec-profile profilename]
[listen-point ipaddress [tcp-port number]]]
```

Syntax Description	
<i>slot</i>	Specifies a particular CMCC adapter in the router where <i>slot</i> is the slot number.
<i>virtual channel</i>	Virtual channel number.
sec-profile <i>profilename</i>	(Optional) Alphanumeric name which specifies the security profile name to be associated with a listen-point. The character range is from 1 to 24. This name is specified originally in the profile command.
listen-point <i>ipaddress</i>	(Optional) IP address that the clients should use as the host IP address to map to LU sessions under this PU and listen point.
tcp-port <i>number</i>	(Optional) Port number used for the listen operation. The default value is 23.

Defaults The default **tcp-port** value is 23.

Command Modes EXEC

Command History	Release	Modification
	12.1(5)T	This command was introduced.

Usage Guidelines There is not a **no** form for this command.

Examples The following is sample output from the **show extended channel tn3270-server security** command with the optional **Sec-profile** keyword configured:

```
Router# show extended channel 3/2 tn3270-server security sec-profile cert40
status:ENABLE Default Profile: (Not Configured)
Name           Active LUs  keylen encryptorder      Mechanism
CERT40         0          40      RC4 RC2 RC5 DES 3DES    SSL
Servercert:slot0:coach188.pem
Certificate Loaded:YES Default-Profile:NO
```

The following is sample output from the **show extended channel tn3270-server security** command with the optional **listen-point** keyword configured:

```
Router# show extended channel 3/2 tn3270-server security listen-point 172.18.5.188
status:ENABLE Default Profile: (Not Configured)
IPAddress      tcp-port  Security-Profile  active-sessions  Type      State
172.18.5.188  23       CERT40            0                Secure    ACTIVE
```

Active Sessions using Deleted Profile:0

Table 6 describes significant fields in the display.

Table 6 *show extended channel tn3270-server security Field Descriptions*

Field	Description
status <i>ENABLE/DISABLE</i>	Status of TN3270 server security. (Enable or Disable).
Default Profile (<i>Not configured/configured</i>)	Shows if a default profile is configured. (Not Configured) or (Configured).
Name	Name of the security profile as specified in the profile command.
Active LUs <i>number</i>	Number of active LUs.
keylen <i>bits</i>	Maximum encryption key length in bits.
encryptorder	Order of encryption algorithms. Choices are DES, 3DES, RC4, RC2 or RC5.
Mechanism	Type of security protocol being used. Choices are SSL or none.
Servercert	Location of the TN3270 server's security certificate status in the flash memory.
Certificate Loaded	Security certificate is loaded. YES or NO.
Default-Profile	Default profile is configured. YES or NO.
IPaddress	IP address that the clients should use as the host IP address to map to LU sessions under this PU and listen-point.
tcp-port	Port number used for the listen operation. The default value is 23.
Security-Profile	Name of the security profile as specified in the profile command.
active-sessions	Number of active sessions.
Type	Type of connection.
State	State of the listen-point.
Active Sessions using Deleted Profile:	Number of sessions using a security profile that has been deleted.

Related Commands

Command	Description
sec-profile	Specifies the security profile to be associated with a listen-point.
listen-point	Defines an IP address for the TN3270 server.

Glossary

- DHCP**—Dynamic Host Configuration Protocol (RFC 2131). DHCP clients obtain their IP address assignments and other configuration information from DHCP servers.
- DNS**—Domain Name System. System used for translating names of network nodes into addresses.
- SSL**—Secure Sockets Layer. Encryption technology for the web, used to provide secure transactions.
- DES**—Data Encryption Standard. Standard cryptographic algorithm developed by the U.S. National Bureau of Standards.
- RC2**—A proprietary encryption algorithm provided by RSA Security. RC2 is a block encryption algorithm which supports keys that are from 1 to 128 bytes in length.
- RC4**—A proprietary encryption algorithm provided by RSA Security. RC4 provides 40 and 128 bit encryption.
- TLS**—Transport Layer Security (RFC 2246). An open standard version of SSL.
- DDDLU**—Dynamic Definition of Dependent LU. A feature of VTAM that allows LUs to be created as needed and not be predefined under a switched PU. The CIP TN3270 server supports DDDLU.
- Direct PU**—A PU 2 that has its own LLC2 link to the owning VTAM. Several direct PUs can share a local SAP, but each must have a unique local/remote MAC/SAP quadruple.
- DLUR**—Dependent LU Requester. A feature of APPN that allows traditional 3270 traffic to be routed over the APPN network. The DLUR feature in the CIP creates an LU 6.2 session (pipe) with DLUS (Dependent LU Server) in VTAM (VTAM version 4R2 or higher). DLUR is defined as a separate switched PU to VTAM. All 3270 session control traffic (SSCP-to-PU and SSCP-to-LU) flows over this DLUR-DLUS pipe. Session data traffic, however, can be routed directly from LU to LU using APPN routing. The CIP DLUR is implemented as an APPN end node (EN).
- DLUR PU**—A PU 2 that uses the DLUR-DLUS pipe to send and receive all session control traffic. It does not use its own source SAP because it uses the DLUR SAP. Similarly, it does not have its own LLC session to the mainframe gateway because it rides on top of the DLUR LLC link.
- LU deletion**—A feature of the TN3270 server in Cisco IOS release 12.0(5)T that allows you to specify whether the TN3270 server sends a REPLY-PSID poweroff request to VTAM to delete an LU when a client disconnects.
- LU nailing**—A method by which you can associate a client's connection request with a specific LU. In Cisco IOS release 12.0(5)T, LU nailing is extended to support association of LU pools with a particular client IP address.
- LU pool**—A group of LUs that can contain logical clusters to establish relationships between screen and printer LUs.
- LU termination**—A feature of the TN3270 server in Cisco IOS release 12.0(5)T that supports SNA's TERMSELF RU, which allows the TN3270 server to order termination of all sessions and session requests associated with an LU when users turn off their device or disconnect from the server.
- NMVT**—Network Management Vector Transport. An SNA message consisting of a series of vectors conveying network management information.
- REPLY-PSID**—Request sent to VTAM for a particular product-set identification (PSID). The PSID is used in SNA to identify the hardware and software products that implement a network component.
- Siftdown command**—Command with values that are applied down through several levels of configuration and are optionally altered at each configuration level.
- TERMSELF RU**—An SNA request/response unit that forces termination of all sessions and session requests associated with an LU.

TFTP—Trivial File Transfer Program (RFC 1350). TFTP clients obtain files from TFTP servers without the use of client authentication (username and password).

VTAM—Virtual Telecommunications Access Method. Set of programs that control communications between SNA logical units. VTAM controls data transmission between mainframes and attached devices and performs SNA routing functions. VTAM is now a component of communications server for OS/390 (CS/390).