enable (TN3270)

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

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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-config** 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 (TN3270)	Enables security on the TN3270 server.
disable (TN3270)	Turns off security in the TN3270 server.

encapsulation alc

To specify that the P1024B Airline Control (ALC) protocol will be used on the serial interface, use the **encapsulation alc** command in interface configuration mode. To remove ALC protocol handling from the serial interface, and return the default encapsulation high-level data link control (HDLC) to the interface, use the **no** form of this command.

encapsulation alc

no encapsulation alc

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation alc** command causes any agent-set control unit (ASCU) configuration to be removed from the interface. As each ASCU defined on the interface is removed it is also unlinked from the ASCU circuit it belongs to. All data frames queued for sending to the ASCU are destroyed.

This command must be entered prior to any ASCU configuration. Note that all timer and counter values are applicable to all ASCUs on the interface.

Examples

The following example specifies that the ALC protocol is used:

```
encapsulation alc
```

Related Commands

Command	Description
show interfaces	Displays statistics for the interfaces configured on a router or access server.

encapsulation bstun

To configure block serial tunnel (BSTUN) on a particular serial interface, use the **encapsulation bstun** command in interface configuration mode. To disable the BSTUN function on the interface, use the **no** form of this command.

encapsulation bstun

no encapsulation bstun

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation bstun** command must be configured on an interface before any further BSTUN or Bisync commands are configured for the interface.

You must use this command to enable BSTUN on an interface. Before using this command, perform the following two tasks:

- Enable BSTUN on a global basis by identifying BSTUN on IP addresses. The command is **bstun peer-name**.
- Define a protocol group number to be applied to the interface. Packets travel only between interfaces that are in the same protocol group. The command is **bstun protocol-group**.

After using the **encapsulation bstun** command, use the **bstun group** command to place the interface in the previously defined protocol group.

Examples

The following example configures the BSTUN function on serial interface 0:

```
interface serial 0
 no ip address
 encapsulation bstun
```

Related Commands

Command	Description
bstun group	Specifies the BSTUN group to which the interface belongs.
bstun peer-name	Enables the BSTUN function.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.

encapsulation sdlc

To configure an Synchronous Data Link Control (SDLC) interface, use the **encapsulation sdlc** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

encapsulation sdlc

no encapsulation sdlc

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation sdlc** command must be used to configure an SDLC interface if you plan to implement data-link switching plus (DLSw+) or Frame Relay access support.

SDLC defines two types of network nodes: primary and secondary. Primary nodes poll secondary nodes in a predetermined order. Secondaries then send if they have outgoing data. When configured as primary and secondary nodes, Cisco routers are established as SDLC stations. Use the **sdlc role** interface configuration command to establish the role as primary or secondary.

In the IBM environment, a front-end processor (FEP) is the primary station and establishment controllers (ECs) are secondary stations. In a typical scenario, an EC may be connected to dumb terminals and to a Token Ring network at a local site. At the remote site, an IBM host connects to an IBM FEP, which can also have links to another Token Ring LAN. Typically, the two sites are connected through an SDLC leased line.

If a router is connected to an EC, it takes over the function of the FEP, and must therefore be configured as a primary SDLC station. If the router is connected to a FEP, it takes the place of the EC, and must therefore be configured as a secondary SDLC station.

Examples

The following example configures an SDLC interface:

```
interface serial 2/6
 no ip address
 encapsulation sdlc
```

Related Commands

Command	Description
sdlc role	Establishes the router to be either a primary or secondary SDLC station.

encapsulation sdlc-primary

To configure the router as the primary Synchronous Data Link Control (SDLC) station if you plan to configure the SDLC Logical Link Control (SDLLC) media translation feature, use the **encapsulation sdlc-primary** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

encapsulation sdlc-primary

no encapsulation sdlc-primary

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation sdlc-primary** or **encapsulation sdlc-secondary** command must be used to configure an SDLC interface. To use the **encapsulation sdlc-primary** command, first select the interface on which you want to enable SDLC. Then establish the router as a primary station. Next, assign secondary station addresses to the primary station using the **sdlc address** command.

SDLC defines two types of network nodes: primary and secondary. Primary nodes poll secondary nodes in a predetermined order. Secondaries then send if they have outgoing data. When configured as primary and secondary nodes, Cisco routers are established as SDLC stations.

In the IBM environment, a front-end processor (FEP) is the primary station and establishment controllers (ECs) are secondary stations. In a typical scenario, an EC may be connected to dumb terminals and to a Token Ring network at a local site. At the remote site, an IBM host connects to an IBM FEP, which can also have links to another Token Ring LAN. Typically, the two sites are connected through an SDLC leased line.

If a router is connected to an EC, it takes over the function of the FEP, and must therefore be configured as a primary SDLC station. If the router is connected to an FEP, it takes the place of the EC, and must therefore be configured as a secondary SDLC station.

Examples

The following example shows how to configure serial interface 0 on your router to allow two SDLC secondary stations to attach through a modem-sharing device (MSD) with addresses C1 and C2:

```
! enter a global command if you have not already
interface serial 0
 encapsulation sdlc-primary
 sdlc address c1
 sdlc address c2
```

Related Commands

Command	Description
encapsulation sdlc-secondary	Configures the router as a secondary SDLC station if you plan to configure the SDLLC media translation feature.
sdlc address	Assigns a set of secondary stations attached to the serial link.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

encapsulation sdlc-secondary

To configure the router as a secondary Synchronous Data Link Control (SDLC) station if you plan to configure the SDLC Logical Link Control (SDLLC) media translation feature, use the **encapsulation sdlc-secondary** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

encapsulation sdlc-secondary

no encapsulation sdlc-secondary

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An **encapsulation sdlc-primary** or **encapsulation sdlc-secondary** command must be used to configure an SDLC interface. To use the **encapsulation sdlc-secondary** command, select the interface on which you want to enable SDLC. Then establish the router as a secondary station. Next, assign secondary station addresses to the primary station using the **sdlc address** command.

SDLC defines two types of network nodes: primary and secondary. Primary nodes poll secondary nodes in a predetermined order. Secondaries then send if they have outgoing data. When configured as primary and secondary nodes, Cisco devices are established as SDLC stations.

In the IBM environment, a front-end processor (FEP) is the primary station and establishment controllers (ECs) are secondary stations. In a typical scenario, an EC may be connected to dumb terminals and to a Token Ring network at a local site. At the remote site, an IBM host connects to an IBM FEP, which can also have links to another Token Ring LAN. Typically, the two sites are connected through an SDLC leased line.

If a router is connected to an EC, it takes over the function of the FEP, and must therefore be configured as a primary SDLC station. If the router is connected to a FEP, it takes the place of the EC, and must therefore be configured as a secondary SDLC station.

Examples

The following example establishes the router as a secondary SDLC station:

```
interface serial 0
 encapsulation sdlc-secondary
```

Related Commands

Command	Description
encapsulation sdlc-primary	Configures the router as the primary SDLC station if you plan to configure the SDLLC media translation feature.
sdlc address	Assigns a set of secondary stations attached to the serial link.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

encapsulation stun

To enable serial tunnel (STUN) encapsulation on a specified serial interface, use the **encapsulation stun** command in interface configuration mode.

encapsulation stun

Syntax Description

This command has no arguments or keywords.

Defaults

STUN encapsulation is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to enable STUN on an interface. Before using this command, perform the following two tasks:

- Enable STUN on a global basis by identifying STUN on IP addresses. The command is **stun peer-name**.
- Define a protocol group number to be applied to the interface. Packets travel only between interfaces that are in the same protocol group. The command is **stun protocol-group**.

After using the **encapsulation stun** command, use the **stun group** command to place the interface in the previously defined protocol group.

To disable stun encapsulation, configure the default interface encapsulation using the **encapsulation** command and specify HDLC as the encapsulation type

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

Examples

This partial configuration example shows how to enable serial interface 5 for STUN traffic:

```
! sample stun peer name and stun protocol-group global commands
stun peer-name 10.108.254.6
stun protocol-group 2 sdlc
!
interface serial 5
! sample ip address command
no ip address
! enable the interface for STUN; must specify encapsulation stun
! command to further configure the interface
encapsulation stun
! place interface serial 5 in previously defined STUN group 2
stun group 2
! enter stun route command
stun route 7 tcp 10.108.254.7
```

Related Commands

Command	Description
stun group	Places each STUN-enabled interface on a router in a previously defined STUN group.
stun peer-name	Enables STUN for an IP address.
stun protocol-group	Creates a protocol group.

encapsulation uts

To specify that the P1024C Universal Terminal Support (UTS) protocol will be used on the serial interface, use the **encapsulation uts** command in interface configuration mode. To remove P1024C UTS protocol handling from the serial interface and return the default encapsulation high-level data link control (HDLC) to the interface, use the **no** form of this command.

encapsulation uts

no encapsulation uts

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **encapsulation uts** command causes any agent-set control unit (agent-set control unit (ASCU)) configuration to be removed from the interface. As each ASCU defined on the interface is removed it is also unlinked from the ASCU circuit it belongs to. All data frames queued for sending to the ASCU are destroyed.

This command must be entered prior to any ASCU configuration. Note that all timer and counter values are applicable to all ASCUs on the interface.

Examples

The following example specifies that the P1024C UTS protocol is used:

```
encapsulation uts
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on a router or access server.

encryptorder

To specify the security encryption algorithm for the Secure Socket Layer (SSL) Encryption Support feature, use the **encryptorder** command in profile configuration mode.

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

Syntax Description

RC4	(Optional) Specifies the RC4 encryption algorithm.
RC2	(Optional) Specifies the RC2 encryption algorithm.
RC5	(Optional) Specifies the RC5 encryption algorithm.
DES	(Optional) Specifies the DES encryption algorithm.
3DES	(Optional) Specifies the 3DES 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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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
```

ethernet-transit-oui

To choose the Organizational Unique Identifier (OUI) code to be used in the encapsulation of Ethernet Type II frames across Token Ring backbone networks, use the **ethernet-transit-oui** command in subinterface configuration mode. Various versions of this OUI code are used by Ethernet/Token Ring translational bridges. To return the default OUI code, use the **no** form of this command.

ethernet-transit-oui [**90-compatible** | **standard** | **cisco**]

no ethernet-transit-oui

Syntax Description

90-compatible	(Optional) Default OUI form.
standard	(Optional) Standard OUI form.
cisco	(Optional) Cisco's OUI form.

Defaults

The default OUI form is 90-compatible.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Before using this command, you must have completely configured your router using multiport source bridging and transparent bridging.

The **standard** keyword is used when you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity.

Table 12 shows the actual OUI codes used, when they are used, and how they compare to Software Release 9.0-equivalent commands.

Table 12 Bridge OUI Codes

Keyword	OUI Used	When Used/Benefits	Software Release 9.0 Command Equivalent
90-compatible	0000F8	By default, when talking to other Cisco routers. Provides the most flexibility.	**no bridge old-oui**

Table 12 Bridge OUI Codes (continued)

Keyword	OUI Used	When Used/Benefits	Software Release 9.0 Command Equivalent
cisco	00000C	Provided for compatibility with future equipment.	None
standard	000000	When talking to IBM 8209 bridges and other vendor equipment. Does not provide for as much flexibility as the other two choices.	**bridge old-oui**

Specify the **90-compatible** keyword when talking to our routers. This keyword provides the most flexibility. When **90-compatible** is specified or the default is used, Token Ring frames with an OUI of 0x0000F8 are translated into Ethernet Type II frames and Token Ring frames with the OUI of 0x000000 are translated into Subnetwork Access Protocol (SNAP)-encapsulated frames. Specify the **standard** keyword when talking to IBM 8209 bridges and other vendor equipment. This OUI does not provide for as much flexibility as the other two choices. The **cisco** keyword oui is provided for compatibility with future equipment.

Do not use the **standard** keyword unless you are forced to interoperate with other vendor equipment, such as the IBM 8209, in providing Ethernet and Token Ring mixed media bridged connectivity. Only use the **standard** keyword only when you are transferring data between IBM 8209 Ethernet/Token Ring bridges and routers running the source-route translational bridging (SR/TLB) software (to create a Token Ring backbone to connect Ethernets).

Use of the **standard** keyword causes the OUI code in Token Ring frames to always be 0x000000. In the context of the **standard** keyword, an OUI of 0x000000 identifies the frame as an Ethernet Type II frame. (Compare with 90-compatible, where 0x000000 OUI means SNAP-encapsulated frames.)

If you use the **90-compatible** keyword, the router, acting as an SR/TLB, can distinguish immediately on Token Ring interfaces between frames that started on an Ethernet Type II frame and those that started on an Ethernet as a SNAP-encapsulated frame. The distinction is possible because the router uses the 0x0000F8 OUI when converting Ethernet Type II frames into Token Ring SNAP frames, and leaves the OUI as 0x000000 for Ethernet SNAP frames going to a Token Ring. This distinction in OUIs leads to efficiencies in the design and execution of the SR/TLB product; no tables need to be kept to know which Ethernet hosts use SNAP encapsulation and which hosts use Ethernet Type II.

The IBM 8209 bridges, however, by using the 0x000000 OUI for all the frames entering the Token Ring, must take extra measures to perform the translation. For every station on each Ethernet, the 8209 bridges attempt to remember the frame format used by each station, and assume that once a station sends out a frame using Ethernet Type II or 802.3, it will always continue to do so. It must do this because in using 0x000000 as an OUI, there is no way to distinguish between SNAP and Type II frame types. Because the SR/TLB router does not need to keep this database, when 8209 compatibility is enabled with the **standard** keyword, the SR/TLB chooses to translate all Token Ring SNAP frames into Ethernet Type II frames as described earlier in this discussion. Because every nonroutable protocol on Ethernet uses either non-SNAP 802.3 (which traverses fully across a mixed IBM 8209/ router Token Ring backbone) or Ethernet Type II, this results in correct inter connectivity for virtually all applications.

Do not use the **standard** keyword OUI if you want SR/TLB to output Ethernet SNAP frames. Using either the **90-compatible** or **cisco** keyword OUI does not present such a restriction, because SNAP frames and Ethernet Type II-encapsulated frames have different OUI codes on Token Ring networks.

Examples

The following example specifies standard OUI form:

```
interface tokenring 0
 ethernet-transit-oui standard
```

Related Commands

Command	Description
source-bridge transparent	Establishes bridging between transparent bridging and SRB.

exception slot

To provide a core dump of a Cisco Mainframe Channel Connection (CMCC) adapter, use the **exception slot** command in global configuration mode. To disable the core dump, use the **no** form of this command.

exception slot [*slot*] *protocol***://***host***/***filename*

no exception slot [*slot*] *protocol***://***host***/***filename*

Syntax Description

slot	(Optional) Slot number of the CMCC adapter. If no *slot* value is specified, all installed CMCC adapters will output a core dump when they halt unexpectedly.
protocol	Protocol for transferring the file. Currently, the only allowed value is FTP. The colon and two slash marks are required.
host	Name or IP address of the host that receives the core dump information. The slash mark is required.
filename	Filename on the host that receives the core dump information. The maximum name length is 31 characters. When written to the host, the *slot* argument is automatically appended, where *slot* is the slot number.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is supported only on the Cisco 7000 with RSP7000 and Cisco 7500 series routers.

You must configure FTP services on the router before you can create a CMCC adapter core dump.

Do not exceed your host limits on filename length. Two characters are added to the filename, *slot*, where *slot* is the slot number.

Examples

The following example shows how to configure a router to perform a CMCC adapter core dump. Assuming the Channel Interface Processor (CIP) is installed in slot 3, the filename cipdump.3 will be written to the host.

```
ip domain-name cisco.com
ip name-server 168.69.161.21
```

```
ip ftp username tech1
ip ftp password tech1
exception slot ftp://168.18.2.196/cipdump
```

Related Commands

Command	Description
ip domain-name	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
ip ftp username	Configures the username for FTP connections.
ip ftp password	Specifies the password to be used for FTP connections.

frame-relay map bridge broadcast

To bridge over a Frame Relay network, use the **frame-relay map bridge broadcast** command in interface configuration mode. To delete the mapping entry, use the **no** form of this command.

frame-relay map bridge *dlci* **broadcast**

no frame-relay map bridge *dlci* **broadcast**

Syntax Description

dlci	Data Link Connection Identifier (DLCI) number. The valid range is from 16 to 1007.

Defaults

No mapping entry is established.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Bridging over a Frame Relay network is supported on networks that do and do not support a multicast facility.

The following example allows bridging over a Frame Relay network:

```
frame-relay map bridge 144 broadcast
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.

frame-relay map bstun

To configure block serial tunnel (BSTUN) over Frame Relay for pass-through, use the **frame-relay map bstun** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

frame-relay map bstun *dlci*

no frame-relay map bstun *dlci*

Syntax Description

dlci	Frame Relay DLCI number on which to support pass-through.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Direct encapsulation over Frame Relay is supported only for an encapsulation type of cisco, configured using the **encapsulation frame-relay** command.

Examples

The following example maps BSTUN traffic to DLCI number 16:

```
frame-relay map bstun 16
```

Related Commands

Command	Description
bstun lisnsap	Configures a service access point (SAP) on which to listen for incoming calls.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
encapsulation frame-relay	Enables Frame Relay encapsulation.

frame-relay map llc2

To configure block serial tunnel (BSTUN) over Frame Relay when using Bisync local acknowledgment, use the **frame-relay map llc2** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

frame-relay map llc2 *dlci*

no frame-relay map llc2 *dlci*

Syntax Description

dlci	Frame Relay data-link connection identifier (DLCI) number on which to support local acknowledgment.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Direct encapsulation over Frame Relay is supported only for an encapsulation type of cisco, configured using the **encapsulation frame-relay** command.

Examples

The following example maps BSTUN traffic to data-link connection identifier (DLCI) number 16:

```
frame-relay map dlci 16
```

Related Commands

Command	Description
bstun lisnsap	Configures a service access point (SAP) on which to listen for incoming calls.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
encapsulation frame-relay	Enables Frame Relay encapsulation.

frame-relay map rsrb

To specify the data-link connection identifier (DLCI) number onto which the remote source-route bridging (RSRB) traffic is to be mapped, use the **frame-relay map rsrb** command in interface configuration mode. To cancel the RSRB map, use the **no** form of this command.

frame-relay map rsrb *dlci*

no frame-relay map rsrb

Syntax Description

dlci	Frame Relay DLCI.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Direct encapsulation over Frame Relay is supported only for an encapsulation type of cisco, configured using the **encapsulation frame-relay** command.

Examples

The following example shows RSRB traffic mapped to DLCI number 30:

```
frame-relay map rsrb 30
```

Related Commands

Command	Description
encapsulation frame-relay	Enables Frame Relay encapsulation.

fras backup dlsw

To configure an auxiliary route between the end stations and the host for use as a backup when the data-link connection identifier (DLCI) connection to the Frame Relay network is lost, use the **fras backup dlsw** command in interface configuration mode. To cancel the backup configuration, use the **no** form of this command.

fras backup dlsw *virtual-mac-address target-ring-number host-mac-address* [**retry** *retry-number*]

no fras backup dlsw *virtual-mac-address target-ring-number host-mac-address* [**retry** *retry-number*]

Syntax Description

virtual-mac-address	12-digit hexadecimal string used as a source MAC address for all packets going to the host.
target-ring-number	Number configured in the **source-bridge ring-group** command. This is a virtual ring. The valid range is from 1 to 4095.
host-mac-address	Destination MAC address of the host.
retry *retry-number*	(Optional) Number of attempts by the end station to reconnect to the primary Frame Relay interface before activating the backup link. The range is from 1 to 5 retries. If the **retry** option is not specified, the default number of retries is 5.

Defaults

Frame Relay access support (FRAS) dial backup over data-link switching plus (DLSw+) is disabled. The default number of retries is 5.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configure DLSw+ as normally required. Specify the optional keyword **dynamic** at the end of the **dlsw remote-peer** configuration command to enable the peer relationship to be established only when needed (for example, when the **fras backup dlsw** command becomes active).

Examples

The following example configures FRAS dial backup over DLSw+:

```
fras backup dlsw 4000.1000.2000 200 1000.5aed.1f53
```

Related Commands

Command	Description
dlsw local-peer	Defines the parameters of the DLSw+ local peer.
dlsw remote-peer tcp	Identifies the IP address of a peer with which to exchange traffic using TCP.
frame-relay lmi-type	Selects the LMI type.
frame-relay map llc2	Configures BSTUN over Frame Relay when using Bisync local acknowledgment.
fras map llc	Associates an LLC connection with a Frame Relay DLCI.
show fras	Displays notification that the FRAS dial backup over DLSw+ feature is active, information about the connection state in FRAS, and information about current BNN, boundary access node (BAN), and dial backup.
source-bridge ring-group	Defines or removes a ring group from the configuration.

fras ban

To associate bridging over a Frame Relay network using boundary access node (BAN), use the **fras ban** command in interface configuration mode. To cancel each association, use the **no** form of this command.

fras ban *local-ring bridge-number ring-group ban-dlci-mac* **dlci** *dlci1* [*dlci2 … dlci5*] [**bni** *mac-addr*]

no fras ban *local-ring bridge-number ring-group ban-dlci-mac* **dlci** *dlci1* [*dlci2 … dlci5*] [**bni** *mac-addr*]

Syntax Description

local-ring	Decimal number from 1 to 4095 describing the Token Ring interface.
bridge-number	Decimal number from 1 to 15 that uniquely identifies a bridge connecting two rings.
ring-group	Decimal number from 1 to 4095 representing a collection of Token Ring interfaces on one or more routers.
ban-dlci-mac	Frame Relay BAN permanent virtual circuit (PVC) MAC address.
dlci *dlci1* [*dlci2 … dlci5*]	Frame Relay data-link connection identifier (DLCI). The **dlci** keyword precedes the list of one or more DLCI numbers. If you need more than one DLCI number for load balancing, you can configure up to five DLCI numbers, separated by spaces. Each DLCI number must be unique and must be a decimal in the range from 16 through 1007.
bni *mac-addr*	(Optional) Boundary node identifier (BNI) MAC address of the NCP that receives frames from the router.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Multiple **fras ban** commands may be configured; however, each **fras ban** command must use a unique DLCI MAC address.

You must configure the **source-bridge ring-group** command in global configuration mode prior to configuring the **fras ban** command.

Examples

The following example shows Frame Relay access support (FRAS) BAN support for Token Ring and serial interfaces:

```
source-bridge ring-group 200
!
interface serial 0
 mtu 4000
 encapsulation frame-relay ietf
 frame-relay lmi-type ansi
 frame-relay map llc2  16
 frame-relay map llc2  17
 fras ban 120 1 200 4000.1000.2000 dlci 16 17
!
interface tokenring 0
 source-bridge 100 5 200
```

Related Commands

Command	Description
source-bridge ring-group	Defines or removes a ring group from the configuration.

fras ddr-backup

To configure an auxiliary interface for use as a backup when the primary Frame Relay link to the Frame Relay WAN fails, use the **fras ddr-backup** command in interface configuration mode. To cancel the backup configuration, use the **no** form of this command.

fras ddr-backup interface *interface dlci-number*

no fras ddr-backup

Syntax Description

interface *interface*	Interface over which the backup connection is made.
dlci-number	Data-link connection identifier (DLCI) number of the session.

Defaults

Frame Relay access support (FRAS) DLCI backup is disabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures FRAS DLCI backup on serial interface 1:

```
fras ddr-backup interface serial 1 188
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show fras	Displays notification that the FRAS dial backup over data-link switching plus (DLSw+) feature is active, information about the connection state in FRAS, and information about current boundary network node (BNN), boundary access node (BAN), and dial backup.

fras map llc

To associate an Logical Link Control (LLC) connection with a Frame Relay data-link connection identifier (DLCI), use the **fras map llc** command in interface configuration mode. To disable the association, use the **no** form of this command.

fras map llc *lan-lsap* **serial** *interface* **frame-relay dlci** *dlci fr-rsap*

no fras map llc *lan-lsap* **serial** *interface* **frame-relay dlci** *dlci fr-rsap*

Syntax Description

lan-lsap	Logical Link Control, type 2 (LLC2) LAN service access point (SAP) that is the local SAP address of the router.
serial *interface*	Serial interface on which Frame Relay is configured.
frame-relay dlci *dlci*	Frame Relay DLCI.
fr-rsap	LLC2 Frame Relay SAP that is the destination SAP of the router on the Frame Relay side.

Defaults

The default state is Frame Relay access support (FRAS) boundary network node (BNN) enhancement is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the destination SAP specified by the end station is equal to the *lan-lsap* value, the router associates the LLC (LAN) connection with the Frame Relay DLCI.

The MAC address and the SAP address of the end station are no longer required for the BNN enhanced configuration.

Examples

In the FRAS BNN enhancement, the revised **fras map llc** command achieves the same result as using multiple **fras map llc** commands in the original FRAS BNN implementation. The following example provides one map definition for both end stations:

```
fras map llc 4 Serial 0 frame-relay dlci 16 04
```

Related Commands

Command	Description
show fras	Displays notification that the FRAS dial backup over data-link switching plus (DLSw+) feature is active, information about the connection state in FRAS, and information about current BNN, BAN, and dial backup.
show llc2	Displays the LLC2 connections active in the router.

fras map sdlc

To associate an Synchronous Data Link Control (SDLC) link with a Frame Relay data-link connection identifier (DLCI), use the **fras map sdlc** command in interface configuration mode. To cancel the association, use the **no** form of this command.

fras map sdlc *sdlc-address* **serial** *port* **frame-relay** *dlci fr-lsap fr-rsap* [**pfid2** | **afid2** | **fid4**]

no fras map sdlc *sdlc-address* **serial** *port* **frame-relay** *dlci fr-lsap fr-rsap* [**pfid2** | **afid2** | **fid4**]

Syntax Description

sdlc-address	SDLC address of the downstream service access point (SAP) device in hexadecimal.
serial *port*	Serial interface on which Frame Relay is configured.
frame-relay *dlci*	Frame Relay DLCI.
fr-lsap	Local service access point (SAP) address of the logical link connection on the Cisco Frame Relay Access Device (CFRAD).
fr-rsap	Destination SAP address on the host.
pfid2	(Optional) format indicator 2 (FID2) Systems Network Architecture (SNA) transmission header for SNA peripheral traffic.
afid2	(Optional) FID2 transmission header for Advanced Peer-to-Peer Networking (APPN) traffic.
fid4	(Optional) Transmission header used on SNA subarea flows.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can map multiple SDLC links to a DLCI.

Examples

The following example associates an SDLC link with a Frame Relay DLCI:

```
fras map sdlc c1 serial 0 frame-relay 200 4 4
```

Related Commands

Command	Description
frame-relay map llc2	Configures block serial tunnel (BSTUN) over Frame Relay when using Bisync local acknowledgment.

fras-host ban

To enable the Frame Relay access support (FRAS) Host function for boundary access node (BAN), use the **fras-host ban** command in interface configuration mode. To disable the FRAS Host BAN functionality, use the **no** form of this command.

fras-host ban *interface* **hmac** *hmac* [**bni** *bni*]

no fras-host ban

Syntax Description

interface	Associated Frame Relay interface or subinterface.
hmac *hmac*	MAC address of the Channel Interface Processor (CIP) adapter or LAN-attached host.
bni *bni*	(Optional) Boundary node identifier MAC address. The default *bni* value is 4FFF.0000.0000.

Defaults

The FRAS Host function for BAN is disabled for the Frame Relay subinterface.

The default *bni* value is 4FFF.0000.0000.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables the FRAS Host function for BAN:

```
fras-host ban Serial0 hmac 4001.3745.0001
```

Related Commands

Command	Description
fras ban	Associates bridging over a Frame Relay network using BAN.
fras-host bnn	Enables the FRAS Host function for boundary network node (BNN).
fras-host dlsw-local-ack	Enables Logical Link Control, type 2 (LLC2) local termination for FRAS Host connections using the virtual Token Ring.
interface virtual-tokenring	Creates a virtual Token Ring interface.

fras-host bnn

To enable the Frame Relay access support (FRAS) Host function for boundary network node (BNN), use the **fras-host bnn** command in interface configuration mode. To disable the FRAS Host function, use the **no** form of this command.

fras-host bnn *interface* **fr-lsap** *sap* **vmac** *virt-mac* **hmac** *hmac* [**hsap** *hsap*]

no fras-host bnn

Syntax Description

interface	Associated Frame Relay interface or subinterface.
fr-lsap *sap*	Logical Link Control, type 2 (LLC2) service access point (SAP). The destination SAP on inbound BNN frames received from Frame Relay.
vmac *virt-mac*	Used in combination with the data-link connection identifier (DLCI) number to form a unique MAC address. The first 4 bytes of the MAC address are formed by the Virtual Media Access Control (VMAC) and the last 2 bytes are formed from the DLCI number. The last 2 bytes of the VMAC must be configured as zeros.
hmac *hmac*	MAC address of the Channel Interface Processor (CIP) adapter or LAN-attached host.
hsap *hsap*	(Optional) Host SAP. If this keyword value is not specified, the host SAP value used will match the **fr-lsap** value.

Defaults

FRAS Host for BNN is disabled for the Frame Relay subinterface.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables the FRAS Host function for BNN:

```
fras-host bnn Serial0 fr-lsap 04 vmac 4005.3003.0000 hmac 4001.3745.0001
```

Related Commands

Command	Description
fras-host ban	Enables the FRAS Host function for boundary access node (boundary access node (BAN)).
fras-host dlsw-local-ack	Enables LLC2 local termination for FRAS Host connections using the virtual Token Ring.
fras map sdlc	Associates an Synchronous Data Link Control (SDLC) link with a Frame Relay DLCI.
interface virtual-tokenring	Creates a virtual Token Ring interface.

fras-host dlsw-local-ack

To enable Logical Link Control, type 2 (LLC2) local termination for Frame Relay access support (FRAS) Host connections using the virtual Token Ring, use the **fras-host dlsw-local-ack** command in interface configuration mode. To disable LLC2 local termination, use the **no** form of this command.

fras-host dlsw-local-ack

no fras-host dlsw-local-ack

Syntax Description

This command has no arguments or keywords.

Defaults

The default state is FRAS Host LLC2 local termination disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example enables LLC2 local termination for FRAS Host connections using the virtual Token Ring:

```
fras-host dlsw-local-ack
```

Related Commands

Command	Description
dlsw local-peer	Defines the parameters of the data-link switching plus (DLSw+) local peer.
fras-host ban	Enables the FRAS Host function for boundary access node (BAN).
fras-host bnn	Enables the FRAS Host function for boundary network node (BNN).
interface virtual-tokenring	Creates a virtual Token Ring interface.

generic-pool

To specify whether leftover logical unit (LU)s will be made available to TN3270 sessions that do not request a specific LU or LU pool through TN3270E, use the **generic-pool** command in TN3270 server configuration mode. To selectively remove the permit or deny condition of generic pool use, use the **no** form of this command.

generic-pool {**permit** | **deny**}

no generic-pool

Syntax Description

permit	Leftover LUs should be made available to TN3270 users wanting generic sessions. This value is the default.
deny	Leftover LUs should not be given to a generic pool. The physical unit (PU) is not automatically fully populated with 255 LOCADDR definitions. The default is the value configured in TN3270 server configuration mode.

Defaults

In TN3270 server configuration mode, generic pool use is permitted.

In PU configuration mode, the default is the value configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface.

A leftover LU is defined as one for which all of the following conditions are true:

- The system services control point (SSCP) did not send an activate logical unit (ACTLU) during PU startup.
- The PU controlling the LU is capable of carrying product set ID (PSID) vectors on network management vector transport (NMVT) messages, thus allowing dynamic definition of dependent LU (DDDLU) operation for that LU.

All LUs in the generic pool are, by definition, DDDLU capable.

Values entered for the **generic-pool** in the TN3270 server configuration mode apply to all PUs for that TN3270 server but can be changed in PU configuration mode.

In PU configuration mode, a **no generic-pool** command will restore the **generic-pool** value entered in TN3270 command mode.

In TN3270 server configuration mode, the **no generic-pool** command reverts to the default, which permits generic pool use.

The command takes effect immediately. If the **generic-pool deny** command is specified on a PU, no further dynamic connections to it will be allowed. Existing sessions are unaffected, but as they terminate the LUs will not become available for dynamic connections.

Similarly, if the **generic-pool permit** command is specified, any inactive LUs are immediately available for dynamic connections. Moreover, any active LUs that were dynamic previously (before the **generic-pool deny** command was issued) return to being dynamic.

Examples

The following example permits generic LU pool use:

```
generic-pool permit
```

Related Commands

Command	Description
client ip lu	Defines a specific LU or range of LUs to a client at the IP address or subnet.

idle-time

To specify seconds of logical unit (LU) inactivity, from both host and client, before the TN3270 session is disconnected, use the **idle-time** command in TN3270 server configuration mode. To cancel the idle time period and return to the default, use the **no** form of this command.

idle-time *seconds*

no idle-time

Syntax Description

seconds	Idle time in seconds, from 0 to 65535. A value of 0 means the session is never disconnected.

Defaults

The default in TN3270 server configuration mode is that the session is never disconnected (0).

The default in PU configuration mode is the value configured in TN3270 server configuration mode.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **idle-time** command is valid only on the virtual channel interface, and can be entered in either TN3270 server configuration mode or PU configuration mode. A value entered in TN3270 mode applies to all PUs for that TN3270 server, except as overridden by values entered in PU configuration mode.

A **no idle-time** command entered in PU configuration mode will restore the idle-time value entered in TN3270 command mode.

The **idle-time** command affects active and future TN3270 sessions. For example, if the **idle-time** value is reduced from 900 seconds to 600 seconds, sessions that have been idle for 600 to 900 seconds are immediately disconnected.

Note For the purposes of idle-time logic, TIMING-MARKs generated by the keepalive logic do not constitute "activity."

In TN3270 server configuration mode, the **idle-time** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **idle-time** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **idle-time** command applies only to the specified PU.

In DLUR PU configuration mode, the **idle-time** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **idle-time** command applies only to the specified PU.

Examples

The following command sets an idle-time disconnect value of 10 minutes:

```
idle-time 600
```

The following command entered in TN3270 server configuration mode sets the default idle-time disconnect value to 0, or never disconnect:

```
no idle-time
```

Related Commands

Command	Description
keepalive (TN3270)	Specifies how many seconds of inactivity elapse before transmission of a DO TIMING-MARK or Telnet no operation (nop) to the TN3270 client.
timing-mark	Selects whether a WILL TIMING-MARK is sent when the host application needs an SNA response (definite or pacing response).

interface bvi

To create the bridge-group virtual interface (BVI) that represents the specified bridge group to the routed interface and links the corresponding bridge group to the other routed interfaces, use the **interface bvi** command in global configuration mode. To delete the BVI, use the **no** form of this command.

interface bvi *bridge-group*

no interface bvi *bridge-group*

Syntax Description

bridge-group	Bridge-group number specified in the **bridge protocol** command.

Command Default

No BVI is created.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	Support for the *sub slot interface* argument was removed for dynamic interfaces.

Usage Guidelines

You must enable integrated routing and bridging (IRB) before attempting to create a BVI.

When you intend to bridge and route a given protocol in the same bridge group, you must configure the network-layer attributes of the protocol on the BVI. Do not configure protocol attributes on the bridged interfaces. Bridging attributes cannot be configured on the BVI.

Examples

The following example creates a bridge group virtual interface and associates it with bridge group 1:

```
Router(config)# bridge 1 protocol ibm
Router(config)# bridge irb
Router(config)# interface bvi 1
Router(config-if)#
```

Related Commands

Command	Description
bridge irb	Enables Cisco IOS software to route a given protocol between routed interfaces and bridge groups or to route a given protocol between bridge groups.

interface channel

To specify a channel-attached interface and enter interface configuration mode, use the **interface channel** command in global configuration mode.

interface channel *slot/port*

Syntax Description

slot	Slot number where the Cisco Mainframe Channel Connection (CMCC) adapter is located. The slash mark is required.
port	Interface where the CMCC adapter is located.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to enter interface configuration mode for a CIP in slot 2 and begin configuring port 0:

```
interface channel 2/0
```

Related Commands

Command	Description
channel-protocol	Defines a data rate of either 3 MBps or 4.5 MBps for Parallel Channel Interfaces.
claw (primary)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in IP datagram mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
cmpc	Configures a Cisco Multipath Channel (CMPC or CMPC+) read subchannel and a CMPC (or CMPC+) write subchannel.
csna	Configures Systems Network Architecture (SNA) support on a CMCC physical channel interface and specifies the path and device/subchannel on a physical channel of the router to communicate with an attached mainframe.

Command	Description
keylen	Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode.
maximum-lus	Specifies the maximum number of LLC2 sessions supported on the CMCC adapter.
offload (primary)	Configures an Offload device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of an Offload backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.
tg (CMPC)	Defines LLC connection parameters for the CMPC TG.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

interface virtual-tokenring

To create a virtual Token Ring interface, use the **interface virtual-tokenring** command in global configuration mode. To cancel the configuration, use the **no** form of this command.

interface virtual-tokenring *number*

no interface virtual-tokenring

Syntax Description

number	Number of the virtual Token Ring.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the virtual Token Ring interface:

```
interface virtual-tokenring 0
```

Related Commands

Command	Description
source-bridge	Configures an interface for SRB.
fras ban	Associates bridging over a Frame Relay network using boundary access node (BAN).
fras-host bnn	Enables the FRAS Host function for boundary network node (BNN).

interface vlan

To create a dynamic Switch Virtual Interface (SVI) or configure a Route Switch Module (RSM), use the **interface vlan** command in global configuration mode.

Configuring on an RSM

To configure a Token Ring or Ethernet interface on the RSM, use the **interface vlan** command in global configuration mode.

interface vlan *vlanid* **type** {**trbrf** | **ethernet**}

Creating a Dynamic Switch Virtual Interface

To create or access a dynamic SVI, use the **interface vlan** command in global configuration mode. Use the **no** form of this command to delete an SVI.

interface vlan *vlanid*

no interface vlan *vlanid*

Syntax Description

vlanid	Unique VLAN ID number (1 to 4094) used to create or access a VLAN.
type trbrf	Configures a Token Ring interface on the RSM.
type ethernet	Configures an Ethernet interface on the RSM.

Defaults

Configuring on an RSM

RSM interfaces are not configured.

Creating a Dynamic Switch Virtual Interface

Fast EtherChannel is not specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3(5)T	This command was introduced.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to create Layer 2 VLANs when you create an SVI.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Configuring on an RSM

Valid Token Ring VLAN ID numbers are 2 through 1000.

Routing or bridging to a Token Ring VLAN (TrBRF) on the RSM is done by creating a logical interface to a TrBRF VLAN on the RSM with the **interface vlan** command. The TrBRF VLAN must be defined on the Supervisor module prior to creating the TrBRF interface on the RSM.

Creating a Dynamic Switch Virtual Interface

SVIs are created the first time that you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* value corresponds to the VLAN tag that is associated with the data frames on an Inter-Switch Link (ISL), the 802.1Q-encapsulated trunk, or the VLAN ID that is configured for an access port. A message displays whenever you create a new VLAN interface, so that you can check if you entered the correct VLAN number.

If you delete an SVI by entering the **no interface vlan** *vlan-id* command, the associated initial domain part (IDP) pair is forced into an administrative down state and is marked as deleted. The deleted interface will not be visible in the **show interface** command.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but much of the previous configuration is gone.

VLANs 1006 to 1014 are internal VLANs on the Cisco 7600 series router and cannot be used for creating new VLANs.

Examples

Configuring on an RSM

The following example show how to configure an RSM Token Ring interface with VLAN 998:

```
Router(config)# interface vlan 998 type trbrf
 ip address 10.5.5.1 255.255.255.0
```

Creating a Dynamic Switch Virtual Interface

The following example shows the output when you enter the **interface vlan** *vlan-id* command for a new VLAN number:

```
Router(config)# interface vlan 23
% Creating new VLAN interface.
```

Related Commands

Command	Description
clear drip counters	Clears DRiP counters.
show drip	Displays the status of the DRiP database.

ip precedence (TN3270)

To specify the precedence level for voice over IP traffic in the TN3270 server, use the **ip precedence** command in TN3270 server configuration mode. To remove the precedence value, use the **no** form of this command.

ip precedence {**screen** | **printer**} *value*

no ip precedence {**screen** | **printer**}

Syntax Description

screen	Specifies that the precedence is for screen devices.
printer	Specifies that the precedence is for printer devices.
value	Sets the precedence priority. A value from 0 to 7, with 7 being the highest priority. The default is 0.

Defaults

The default is a precedence value of 0 for both screens and printers.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. Precedence values applied in TN3270 PU configuration mode override values applied in TN3270 server configuration mode.

You can enter new or different values for IP precedence without first using the **no** form of this command.

During initial Telnet negotiations to establish, or bind, the session an IP precedence value of 0 and IP ToS value of 0 is used. These values are used until the bind takes place. When the session is a type 2 bind, the TN3270 client is assumed to be a screen; otherwise the client is assumed to be a printer.

In TN3270 server configuration mode, the **ip precedence** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **ip precedence** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **ip precedence** command applies only to the specified PU.

In DLUR PU configuration mode, the **ip precedence** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **ip precedence** command applies only to the specified PU.

Examples

The following example assigns a precedence value of 3 to printers:

```
ip precedence printer 3
```

Related Commands

Command	Description
ip tos	Specifies the ToS level for IP traffic in the TN3270 server.

ip tos

To specify the type of service (ToS) level for IP traffic in the TN3270 server, use the **ip tos** command in TN3270 server configuration mode. To remove the ToS value, use the **no** form of this command.

ip tos {**screen** | **printer**} *value*

no ip tos {**screen** | **printer**}

Syntax Description

screen	Specifies that the ToS is for screen devices.
printer	Specifies that the ToS is for printer devices.
value	Sets the ToS priority. A value from 0 to 15. The default is 0.

Defaults

The default is a ToS value of 0 for both screens and printers.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. ToS values applied in TN3270 PU configuration mode override values applied in TN3270 server configuration mode.

The default ToS values for screen and printer are 0. However, RFC 1349 recommends different default values. Specifically, the RFC recommends a default minimize screen delay value of 8 and a default maximize printer throughput value of 4. You must configure these values using the **ip tos** command if you want to comply to the defaults as stated in the RFC.

Table 13 shows the values described in RFC 1349.

Table 13 ToS Defined Values

Value	Definition	Action
0	All normal.	Use default metric.
8	Minimize delay.	Use delay metric.
4	Maximize throughput.	Use default metric.
2	Maximize reliability.	Use reliability metric.
1	Minimize monetary cost.	Use cost metric.
Other	Not defined.	Reserved for future use.

During initial Telnet negotiations to establish, or bind, the session, an IP precedence value of 0 and IP ToS value of 0 is used. These values are used until the bind takes place. When the session is a type 2 bind, the TN3270 client is assumed to be a screen; otherwise the client is assumed to be a printer.

When you use the **no** form of the command, the ToS value is set to 0 for that configuration mode or the value set at a previous (higher) configuration mode is used. For example, if you are at the TN3270 PU configuration mode and issue a **no ip tos screen** command, any value you configured previously at the TN3270 server configuration mode will take effect.

You can enter new or different values for ToS without first using the **no** form of this command.

In TN3270 server configuration mode, the **ip tos** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **ip tos** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **ip tos** command applies only to the specified PU.

In DLUR PU configuration mode, the **ip tos** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **ip tos** command applies only to the specified PU.

Examples

In the following example, the TN3270 server ToS screen value is set to 10 and a specific PU ToS screen value is set to 0:

```
interface channel 3/2
  tn3270-server
   ip tos screen 8
   ip tos printer 4
  up PUS2
   ip tos screen 0
```

Related Commands

Command	Description
ip precedence (TN3270)	Specifies the precedence level for IP traffic in the TN3270 server.

keepalive (TN3270)

To specify how many seconds of inactivity elapse before the TN3270 server sends a DO TIMING-MARK or Telnet no operation (nop) to the TN3270 client, use the **keepalive** command in TN3270 server configuration mode. To cancel the keepalive period and return to the previously configured siftdown value or the default, use the **no** form of this command.

keepalive *seconds* [**send** {**nop** | **timing-mark** [*max-response-time*]}]

no keepalive

Syntax Description

seconds	Number of elapsed seconds (from 0 to 65535) before the TN3270 server sends a DO TIMING-MARK or Telnet **nop** command to the TN3270 client. A value of 0 means no keepalive signals are sent. The default is 1800 seconds (30 minutes).
send nop	(Optional) Sends the Telnet command for no operation to the TN3270 client to verify the physical connection. No response is required by the client.
send timing-mark [*max-response-time*]	(Optional) Number of seconds (from 0 to 32767) within which the TN3270 server expects a response to the DO TIMING-MARK from the TN3270 client. The default is 30 seconds if the keepalive interval is greater than or equal to 30 seconds. If the value of the keepalive interval is less than 30 seconds, then the default *max-response-time* value is the value of the interval. The value of the *max-response-time* should be less than or equal to the *interval* value.

Defaults

The default behavior is to send timing marks with a keepalive interval of 1800 seconds (30 minutes). If you specify only the keepalive interval, the TN3270 server sends timing marks.

The default value of the **send timing-mark** *max-response-time* command is 30 seconds if the keepalive interval is greater than or equal to 30 seconds. If the value of the keepalive interval is less than 30 seconds, then the default *max-response-time* value is the value of the interval.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The **send** {**nop** | **timing-mark** [*max-response-time*]} keywords and argument were added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **keepalive** command is valid only on the virtual channel interface. This command can be entered in one of four command modes (TN3270 configuration, listen-point configuration, listen-point PU configuration, or PU configuration mode). A value entered in TN3270 mode applies to all PUs for that TN3270 server, except as overridden by values entered in the other supported configuration modes. A **no keepalive** command entered in a subsequent configuration mode will restore the **keepalive** value entered in the previous command mode.

In Cisco IOS releases prior to 12.0(5)T in which the **keepalive** command is supported, you cannot specify the period of time in which the client must respond to the DO TIMING-MARK before the TN3270 server disconnects the session. By default in prior releases, if the client does not reply within 30 minutes of sending the DO TIMING-MARK, the TN3270 server disconnects the TN3270 session. (The DO TIMING-MARK is a Telnet protocol operation that does not affect the client operation.)

With the addition of the **send timing-mark** *max-response-time* keywords in Cisco IOS Release 12.0(5)T, you can specify the period of time in which the client must respond to the DO TIMING-MARK before being disconnected by the server. If you do not specify a value for the *max-response-time* argument, the default value is determined by the size of the keepalive interval. The default is 30 seconds if the keepalive interval is greater than or equal to 30 seconds. If the value of the keepalive interval is less than 30 seconds, then the default *max-response-time* is the value of the interval.

If the IP path to the client is broken, the TCP layer will detect the failure to acknowledge the DO TIMING-MARK and initiate disconnection. This action usually takes much less than 30 seconds.

The **keepalive** command affects active and future TN3270 sessions. For example, reducing the keepalive interval to a lower nonzero value causes an immediate burst of DO TIMING-MARKs on those sessions that have been inactive for a period of time greater than the new, lower value.

Use the **keepalive send nop** command when you are using older TN3270 clients that do not support TIMING-MARK or are DOS-based clients. When you use the **keepalive send nop** command to monitor the client connection, no response is required by the client to the TN3270 server. However, the TCP/IP stack can detect that the physical connection still exists. This command is useful for those clients that can be swapped out when a DO TIMING-MARK has been sent by the TN3270 server. If the client is swapped out and cannot respond to the DO TIMING-MARK from the TN3270 server, the session is disconnected. However, if the client is swapped out and the Telnet **nop** command is sent by the server, the physical connection is still verifiable by the TCP/IP stack and the client remains connected to the server.

If your client supports the use of timing marks and is not subject to being swapped out, then using timing marks is preferable to the Telnet **nop** command for keepalive monitoring. The required response by TN3270 clients to timing marks sent by the server provides a better indication of the health of the client/server connection.

In TN3270 server configuration mode, the **keepalive** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **keepalive** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **keepalive** command applies only to the specified PU.

In DLUR PU configuration mode, the **keepalive** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **keepalive** command applies only to the specified PU.

Examples

The following example specifies that the TN3270 server sends a DO TIMING-MARK in 15-minute (900-second) intervals and the client must respond within 30 seconds (the default value for the **timing-mark** *max-response-time* command when not specified):

```
keepalive 900
```

The following example entered in TN3270 server configuration mode specifies that the TN3270 server sends a DO TIMING-MARK in 30-minute (1800-second) intervals (the default interval) and the client must respond within 30 seconds (the default for the **timing-mark** *max-response-time* command when not specified):

```
no keepalive
```

The following example specifies that the TN3270 server sends a DO TIMING-MARK in 40-minute (2400-second) intervals and the client must respond within 1 minute (60 seconds):

```
keepalive 2400 send timing-mark 60
```

Consider the following example in which the **keepalive** command is configured in more than one command mode. In this example the **keepalive** command is configured in TN3270 server configuration mode, and then in listen-point physical unit (PU) configuration mode. The **keepalive** command values specified under the listen-point PU override the **keepalive** 300 value specified under the tn3270-server for PU1. In this example, all other PUs except PU1 use the value of the **keepalive 300** command specified in TN3270 server configuration mode.

```
tn3270-server
keepalive 300
listen-point 10.10.10.1 tcp-port 40
  pu PU1 94223456 tok 1 08
    keepalive 10 send timing-mark 5
  pu PU2 94223457 tok 2 12
```

Related Commands

Command	Description
idle-time	Specifies how many seconds of LU inactivity, from both host and client, before the TN3270 session is disconnected.
timing-mark	Selects whether a WILL TIMING-MARK is sent when the host application needs an SNA response (definite or pacing response).

keylen

To specify the maximum bit length for the encryption keys for Secure Socket Layer (SSL) Encryption Support, use the **keylen 128** command in profile configuration mode. 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**]

Syntax Description

40	Specifies the bit length for the encryption keys to 40.
128	Specifies the bit length for the encryption keys to 128. The default is 40 bits.

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.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

The length is optional on the **no** form of this command. Entering the **no** form of this command with no length 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
```

lan

To configure an internal LAN on a Cisco Mainframe Channel Connection (CMCC) adapter interface and enter internal LAN configuration mode, use the **lan** command in interface configuration mode. To remove an internal LAN interface, use the **no** form of this command.

lan *type lan-id*

no lan *type lan-id*

Syntax Description

type	Interface type for this internal LAN: **tokenring**.
lan-id	Number from 0 to 31 that uniquely identifies the internal LAN on this CMCC adapter. This value must be unique between all internal LANs of the same interface type on a CMCC adapter.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Token Ring is the only type of internal LAN supported.

This command is valid only on the virtual channel interface. All internal adapters configured on the internal LAN must be removed before the internal LAN can be removed.

A CMCC internal LAN can be configured as a SRB LAN. This allows Logical Link Control (LLC) packets to be bridged between the CMCC adapter and Cisco IOS, providing a means to link the internal LAN to Cisco IOS Systems Network Architecture (SNA) features such as source-route bridging (SRB), data-link switching plus (DLSw+), remote source-route bridging (RSRB), SDLC Logical Link Control (SDLLC), Qualified Logical Link Control (QLLC), Advanced Peer-to-Peer Networking (APPN), and source-route translational bridging (SR/TLB).

An internal LAN can be configured only on a virtual channel interface of a CMCC adapter. You enter first internal LAN configuration mode by issuing the command for an internal LAN that already exists or when you first configure an internal LAN. In internal LAN configuration mode, the router prompt appears as follows:

```
router (cfg-lan-type x) #
```

In this syntax, *type* is the specified internal LAN type and *x* is the specified value for the *lan-id*.

Examples

The following example shows how to configure an internal LAN Token Ring with a LAN ID of 20 on the channel interface 1/2:

```
interface channel 1/2
 lan tokenring 20
```

Related Commands

Command	Description
adapter	Configures internal adapters.
locaddr-priority	Assigns an RSRB priority group to an input interface.
sap-priority	Defines a priority list on an interface.
show extended channel lan	Displays the internal LANs and adapters configured on a CMCC adapter.
source-bridge	Configures an interface for SRB.

lan-name

To specify a name for the LAN that is attached to the interface, use the **lan-name** command in interface configuration mode. This name is included in any Alert sent to the Systems Network Architecture (SNA) host when a problem occurs on this interface or LAN. To revert to the default name, use the **no** form of this command.

lan-name *lan-name*

no lan-name *lan-name*

Syntax Description

lan-name	Name used to identify the LAN when you send Alerts to the SNA host. The default LAN name is the name of the interface.

Defaults

The default name used for the LAN is the name of the interface.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example identifies a LAN:

```
lan-name LAN1
```

Related Commands

Command	Description
show sna	Displays the status of the SNA Service Point feature.

link (TN3270)

To define and activate a link to a host, use the **link** command in Dependent Logical Unit Requestor (DLUR) service access point (SAP) configuration mode. To delete the link definition, use the **no** form of this command.

link *name* [**rmac** *rmac*] [**rsap** *rsap*]

no link *name*

Syntax Description

name	Link name, from one to eight alphanumeric characters. The first character must be alphabetic. The name must be unique within the Dependent Logical Unit Requestor (DLUR) function.
rmac *rmac*	(Optional) Remote MAC address of the form *xxxx.xxxx.xxxx* in hexadecimal. If not specified, a loopback link to another service access point (SAP) on the same internal LAN adapter is assumed.
rsap *rsap*	(Optional) Remote SAP address, 04 to FC in hexadecimal. The *rsap* value should be an even number and should be a multiple of 4, but the latter requirement is not enforced. The default value for the *rsap* argument is 04.

Defaults

No DLUR link is defined.
The default remote SAP address is 04 (hexadecimal).

Command Modes

DLUR SAP configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. The combination of the *rmac* and *rsap* value must be unique within the DLUR SAP function. These values can be changed only by deleting the link definition, using the **no link** command, and recreating the link definition.

For a link via a channel on this Cisco Mainframe Channel Connection (CMCC) adapter, the TN3270 server and the hosts should open different adapters. Using different adapters avoids any contention for SAP numbers, and is also necessary if you configure duplicate MAC addresses for fallback Cisco Systems Network Architecture (CSNA) or Cisco Multipath Channel (CMPC) access to the host.

Examples

The following example defines a link name and a remote SAP address:

```
link LINK5 rsap 08
```

The following example shows different adapter numbers configured on the same internal LAN to avoid SAP contention. The host uses SAP 4 on Token Ring adapter 0.

```
lan tokenring 0
 adapter 0 4000.0000.0001
 adapter 1 4000.0000.0002
tn3270-server
 dlur ...
 lsap token-adapter 1
  link HOST rmac 4000.0000.0001 rsap 4
```

Related Commands

Command	Description
adapter	Configures internal adapters.
client pool	Nails clients to pools.
lsap	Creates a SAP in the SNA session switch and enters DLUR SAP configuration mode.

listen-point

To define an IP address for the TN3270 server, use the **listen-point** command in TN3270 server configuration mode. To remove a listen-point for the TN3270 server, use the **no** form of this command.

listen-point *ip-address* [**tcp-port** *number*]

no listen-point *ip-address* [**tcp-port** *number*]

Syntax Description

ip-address	IP address that the clients should use as the host IP address to map to logical unit (LU) sessions under this physical unit (PU) and listen point.
tcp-port *number*	(Optional) Port number used for the listen operation. The default value is 23.

Defaults

The default **tcp-port** *number* is 23.

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **listen-point** command to create a unique listen point for every IP address and TCP-port pair. In this mode, the IP address and the TCP port are no longer configured in the PU. Configure the PUs under the appropriate listen point. The other siftdown configuration commands remain the same.

For example, in the old configuration the following statements were used to configure the IP address and TCP port in the PU:

```
tn3270-server
  pu PU1 94223456 10.10.10.1 tok 1 08
   tcp-port 40
   keepalive 10
```

In the new listen-point configuration, the following statements are used to configure the IP address and TCP port at the listen point:

```
tn3270-server
  listen-point 10.10.10.1 tcp-port 40
   pu PU1 94223456 tok 1 08
    keepalive 10
```

You can also use the listen-point configuration to assign the same IP address to multiple PUs. In the old configuration the following statements were used:

```
tn3270-server
  pu PU1 94201231 10.10.10.2 tok 1 10
  pu PU2 94201232 10.10.10.3 tok 1 12
  pu PU3 94201234 10.10.10.3 tok 1 14
  pu PU4 94201235 10.10.10.4 tok 1 16
   tcp-port 40
  pu PU5 94201236 10.10.10.4 tok 2 08
```

In the new listen point configuration, the old statements are replaced by the following configuration commands. In this example, PU2 and PU3 are grouped into one listen point because they have the same IP address. Note that even though PU4's IP address is identical to PU5's IP address, they are not configured within the same listen point because the listen point indicates a unique IP address and TCP port pair. If you do not specify the TCP port, the default port value is 23.

```
tn3270-server
 listen-point 10.10.10.2
  pu PU1 94201231 tok 1 10
 listen-point 10.10.10.3
  pu PU2 94201232 tok 1 12
  pu PU3 94201234 tok 1 14
 listen-point 10.10.10.4
  pu PU5 94201236 tok 2 08
 listen-point 10.10.10.4 tcp-port 40
  pu PU4 94201235 tok 1 16
```

The next example shows how the configuration changes for a Dependent Logical Unit Requestor (DLUR) PU. In this mode, the DLUR PU is no longer configured under DLUR, but is configured in the listen point.

In the old configuration, the following statements were used:

```
tn3270-server
 dlur NETA.RTR1 NETA.HOST
  dlus-backup NETA.HOST
  lsap token-adapter 15 08
   link MVS2TN rmac 4000.b0ca.0016
  pu PU1 017ABCDE 10.10.10.6
```

These statements are replaced by the following statements in the new listen-point configuration. The keyword **dlur** differentiates the listen point direct PU from the listen point DLUR PU. The DLUR configuration must be completed before you configure the PU in the listen point. Any siftdown commands configured within the scope of the listen point are automatically inherited by the PUs that are configured within the scope of that listen point. To override the siftdown configurations, you can explicitly configure the siftdown configuration commands within the scope of the listen-point PU.

```
tn3270-server
 dlur NETA.RTR1 NETA.HOST
  dlus-backup NETA.HOST
  lsap token-adapter 15 08
   link MVS2TN rmac 4000.b0ca.0016
 listen-point 10.10.10.6
  pu PU1 017ABCDE dlur
```

Examples

The following example of the **listen-point** command shows PU7 grouped into the listen point at IP address 10.10.10.1 and TCP port 40:

```
tn3270-server
listen-point 10.10.10.1 tcp-port 40
 pu PU7 94201237 tok 1 17
```

Related Commands

Command	Description
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.
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.

llc2 ack-delay-time

To set the amount of time the Cisco IOS software waits for an acknowledgment before sending the next set of information frames, use the **llc2 ack-delay-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 ack-delay-time *milliseconds*

no llc2 ack-delay-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software allows incoming information frames to stay unacknowledged. The minimum is 1 ms and the maximum is 60000 ms. The default is 100 ms.

Defaults

100 ms

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Upon receiving an information frame, each Logical Link Control, type 2 (LLC2) station starts a timer. If the timer expires, an acknowledgment will be sent for the frame, even if the number of received frames in the **llc2 ack-max** command has not been reached. Experiment with the value of the **llc2 ack-delay-time** command to determine the configuration that balances acknowledgment network overhead and quick response time (by receipt of timely acknowledgments).

Use this command in conjunction with the **llc2 ack-max** command to determine the maximum number of information frames the Cisco IOS software can receive before sending an acknowledgment.

Examples

In the following example, the software allows a 100-ms delay before I-frames must be acknowledged:

```
! enter a global command, if you have not already
interface tokenring 0
! sample ack-max command
 llc2 ack-max 3
! allow a 100 millisecond delay before I-frames must be acknowledged
 llc2 ack-delay-time 100
```

At time 0, two information frames are received. The **llc2 ack-max** amount of three has not been reached, so no acknowledgment for these frames is sent. If a third frame, which would force the software to send an acknowledgment, is not received in 100 ms, an acknowledgment will be sent anyway, because the l**lc2 ack-delay** timer expires. At this point, because all frames are acknowledged, the counter for the ack-max purposes will be reset to zero.

Related Commands

Command	Description
llc2 ack-max	Controls the maximum amount of information frames the Cisco IOS software can receive before it must send an acknowledgment.
show llc2	Displays the LLC2 connections active in the router.

llc2 ack-max

To control the maximum amount of information frames the Cisco IOS software can receive before it must send an acknowledgment, use the **llc2 ack-max** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 ack-max *packet-count*

no llc2 ack-max *packet-count*

Syntax Description

packet-count	Maximum number of packets the software will receive before sending an acknowledgment. The minimum is 1 packet and the maximum is 127 packets. The default is 3 packets.

Defaults

Three packets

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An Logical Link Control, type 2 (LLC2)-speaking station can send only a predetermined number of frames before it must wait for an acknowledgment from the receiver. If the receiver waits until receiving a large number of frames before acknowledging any of them, and then acknowledges them all at once, overhead is reduced on the network.

For example, an acknowledgment for five frames can specify that all five have been received, as opposed to sending a separate acknowledgment for each frame. To keep network overhead low, make this parameter as large as possible.

However, some LLC2-speaking stations expect this number to be low. Some NetBIOS-speaking stations expect an acknowledgment to every frame. Therefore, for these stations, this number is best set to 1. Experiment with this parameter to determine the best configuration.

Examples

In the following example, the software is configured to receive up to seven frames before it must send an acknowledgment. Seven frames is the maximum allowed by Systems Network Architecture (SNA) before a reply must be received:

```
! enter a global command, if you have not already
interface tokenring 0
! receive up to seven frames before sending an acknowledgment
```

```
 llc2 ack-max 7
! sample delay-time command
 llc2 ack-delay-time 100
```

Related Commands

Command	Description
llc2 ack-delay-time	Sets the amount of time the Cisco IOS software waits for an acknowledgment before sending the next set of information frames.
llc2 local-window	Controls the maximum number of information frames the Cisco IOS software sends before it waits for an acknowledgment.
show llc2	Displays the LLC2 connections active in the router.

llc2 adm-timer-value

To control the amount of time the Cisco IOS software waits for, in Asynchronous Disconnect Mode (ADM) before giving up, use the **llc2 adm-timer-value** command in interface configuration mode. To restore the default configuration, use the **no** form of this command.

llc2 adm-timer-value *milliseconds*

no llc2 adm-timer-value *milliseconds*

Syntax Description

milliseconds	Time period in milliseconds (ms) the software waits for in ADM. The range is from 0 to 60000 ms. The default is 60000 ms.

Command Default

The default is 60000 ms.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on the feature set, platform, and hardware.

Usage Guidelines

The command **llc2 adm-timer-value** command is used to clear out the Logical Link Control (LLC) sessions that are left in the ADM State for a defined time period, so that the router does not hang.

Examples

This example shows how to control the waiting time with the **llc2 adm-timer-value** command:

```
Router (config-if)# llc2 adm-timer-value 3
```

Related Commands

Command	Description
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.
llc2 xid-neg-val-time	Controls the frequency of XID transmissions by the Cisco IOS software.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 dynwind

To enable dynamic window congestion management, use the **llc2 dynwind** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

llc2 dynwind [**nw** *nw-number*] [**dwc** *dwc-number*]

no llc2 dynwind [**nw** *nw-number*] [**dwc** *dwc-number*]

Syntax Description

nw *nw-number*	(Optional) Specifies a number of frames that must be received to increment the working window value by 1. The default is 4.
dwc *dwc-number*	(Optional) Specifies the number by which the working window value is divided when Systems Network Architecture (SNA) occurs. Valid numbers are 1, 2, 4, 8, and 16; 1 is a special value that indicates that the working window value should be set to 1 when backward explicit congestion notification (BECN) is indicated. The default is 1.

Defaults

The default *nw-number* value is 4.
The default *dwc-number* value is 1.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies that to increment the working window six frames must be received, and the working window value should be set to 1 when BECN occurs:

```
llc2 dynwind nw 6 dwc 1
```

llc2 idle-time

To control the frequency of polls during periods of idle time (no traffic), use the **llc2 idle-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 idle-time *milliseconds*

no llc2 idle-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds that can pass with no traffic before the Logical Link Control, type 2 (LLC2) station sends a Receiver Ready frame. The minimum is 1 ms and the maximum is 60000 ms. The default is 10000 ms.

Defaults

10000 ms

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Periodically, when no information frames are being sent during an LLC2 session, LLC2 stations are sent a Receiver Ready frame to indicate that they are available. Set the value for this command low enough to ensure a timely discovery of available stations, but not too low, or you will create a network overhead with too many Receiver Ready frames.

Examples

In the following example, the Cisco IOS software waits 20,000 ms before sending a Receiver Ready (“are you there”) frame:

```
! enter a global command, if you have not already
interface tokenring 0
! wait 20000 milliseconds before sending receiver-ready frames
 llc2 idle-time 20000
```

Related Commands

Command	Description
llc2 tbusy-time	Controls the amount of time the Cisco IOS software waits until repolling a busy remote station.
llc2 tpf-time	Sets the amount of time the Cisco IOS software waits for a final response to a poll frame before resending the poll frame.
show llc2	Displays the LLC2 connections active in the router.

llc2 local-window

To control the maximum number of information frames the Cisco IOS software sends before it waits for an acknowledgment, use the **llc2 local-window** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 local-window *packet-count*

no llc2 local-window *packet-count*

Syntax Description

packet-count	Maximum number of packets that can be sent before the software must wait for an acknowledgment. The minimum is 1 packet and the maximum is 127 packets. The default is 7 packets.

Defaults

Seven packets.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An Logical Link Control, type 2 (LLC2)-speaking station can send only a predetermined number of frames before it must wait for an acknowledgment from the receiver. Set this number to the maximum value that can be supported by the stations with which the router communicates. Setting this value too large can cause frames to be lost, because the receiving station may not be able to receive all of them.

Examples

In the following example, the software will send as many as 30 information frames through Token Ring interface 1 before it must receive an acknowledgment:

```
! enter a global command, if you have not already
interface tokenring 1
 llc2 local-window 30
```

Related Commands

Command	Description
llc2 ack-max	Controls the maximum amount of information frames the Cisco IOS software can receive before it must send an acknowledgment.
show llc2	Displays the LLC2 connections active in the router.

llc2 n1

To specify the maximum size of an I-frame, use the **llc2 n1** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 n1 *bytes*

no llc2 n1

Syntax Description

bytes	Maximum size of an I-frame. The valid range is from 1 to 4105 bytes. The default is 4105 bytes.

Defaults

The default maximum I-frame size is 4105 bytes.

Command Modes

Internal adapter configuration

Command History

Release	Modification
12.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example sets the maximum I-frame size to 2057 bytes:

```
! enter a global command, if you have not already
interface tokenring 1
! maximum I-frame size of 2057 bytes
 llc2 n1 2057
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 n2

To control the amount of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations, use the **llc2 n2** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 n2 *retry-count*

no llc2 n2

Syntax Description

retry-count	Number of times the software retries operations. The minimum is 1 retry and the maximum is 255 retries. The default is 8 retries.

Defaults

Eight retries

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An Logical Link Control, type 2 (LLC2) station must have some limit to the number of times it will resend a frame when the receiver of that frame has not acknowledged it. After the software is told that a remote station is busy, it will poll again based on the *retry-count* value. When this retry count is exceeded, the LLC2 station terminates its session with the other station. Set this parameter to a value that balances between frame checking and network performance.

Examples

In the following example, the software will resend a frame up to four times through Token Ring interface 1 before it must receive an acknowledgment. Because you generally do not need to change the retry limit, this example shows you how to reset the limit to the default of 8.

```
! enter a global command, if you have not already
interface tokenring 1
! retry value of 8
 llc2 n2 8
```

Related Commands

Command	Description
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.
llc2 tbusy-time	Controls the amount of time the Cisco IOS software waits until repolling a busy remote station.
llc2 trej-time	Controls the amount of time the Cisco IOS software waits for a correct frame after sending a reject command to the remote LLC2 station.
show llc2	Displays the LLC2 connections active in the router.

llc2 nw

To increase the window size for consecutive good I-frames received, use the **llc2 nw** internal adapter configuration command. To revert to the default setting, use the **no** form of this command.

llc2 nw *window-size-increase*

no llc2 nw

Syntax Description

window-size-increase	Number of frames to increase the window size for consecutive good I-frames received (0 is disabled). The allowed range is from 1 to 7. The default is 0.

Defaults

0 (disabled).

Command Modes

Internal adapter configuration

Command History

Release	Modification
11.0	This command was introduced.
12.1	The allowed range was changed to from 0 to 31.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the window size for Token Ring interface 1 is increased by 1 frame when consecutive good I-frames are received:

```
! enter a global command, if you have not already
interface tokenring 1
! increase window size by 1
 llc2 nw 1
```

Related Commands

Command	Description
show llc2	Displays the LLC2 connections active in the router.
llc2 nw	Invokes dynamic windowing logic for a link station when the router receives an RNR from the remote link station.

llc2 recv-window

To control the number of frames in the receive window, use the **llc2 recv-window** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 recv-window *frame-count*

no llc2 recv-window

Syntax Description

frame-count	Specifies the number of frames in the receive window. The default is 7.

Defaults

Seven frames.

Command Modes

Internal adapter configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the receive window for Token Ring interface 1 contains 11 frames:

```
! enter a global command, if you have not already
interface tokenring 1
! 11 frames in the receive window
 llc2 recv-window 11
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 rnr-activated

To invoke dynamic windowing logic for a link station when the router receives an RNR from the remote link station, use the **llc2 rnr-activated** internal adapter configuration command. To disable dynamic windowing logic, use the **no** form of this command.

llc2 rnr-activated

no llc2 rnr-activated

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Internal adapter configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **llc2 nw** command must be enabled before the **llc2 rnr-activated** command can be configured.

Examples

In the following example, the **llc2n rnr-activated** command is enabled on Adapter 0 4000.cafe.0000:

```
interface Channel4/2
 max-llc2-rcvbuffs 750
lan TokenRing 12
 source-bridge 16 1 500
 adapter 0 4000.cafe.0000
  llc2 Nw 31
  llc2 rnr-activated
 adapter 1 4000.cafe.0001
```

Related Commands

Command	Description
llc2 nw	Increases the window size for consecutive good I-frames received.
max-llc2-rcvbuffs	Configures the number of receive DMA buffers that are used by the LLC2 stack on the CIP/XCPA.

llc2 send-window

To control the number of frames in the send window, use the **llc2 send-window** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 send-window *frame-count*

no llc2 send-window

Syntax Description

frame-count	Specifies the number of frames in the send window. The default is 7.

Defaults

Seven frames.

Command Modes

Internal adapter configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

In the following example, the send window for Token Ring interface 1 contains 11 frames:

```
! enter a global command, if you have not already
interface tokenring 1
! 11 frames in the send window
 llc2 send-window 11
```

Related Commands

Command	Description
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 t1-time

To control the amount of time the Cisco IOS software will wait before resending unacknowledged information frames, use the **llc2 t1-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 t1-time *milliseconds*

no llc2 t1-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software waits before resending unacknowledged information frames. The minimum is 1 ms and the maximum is 60000 ms. The default is 1000 ms.

Defaults

1000 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in conjunction with the **llc2 n2** command to provide a balance of network monitoring and performance. Ensure that enough time is allowed to account for the round trip between the router and its Logical Link Control, type 2 (LLC2)-speaking stations under heavy network loading conditions.

Examples

In the following example, the software will wait 4000 ms before resending an unacknowledged frame through Token Ring interface 2:

```
! enter a global command, if you have not already
interface tokenring 2
! wait 4000 milliseconds before retransmitting a frame through tokenring 2
 llc2 t1-time 4000
```

Related Commands

Command	Description
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
llc2 tpf-time	Sets the amount of time the Cisco IOS software waits for a final response to a poll frame before resending the poll frame.
llc2 xid-retry-time	Sets the amount of time the Cisco IOS software waits for a reply to XID frames before dropping the session.
show llc2	Displays the LLC2 connections active in the router.

llc2 tbusy-time

To control the amount of time the Cisco IOS software waits until repolling a busy remote station, use the **llc2 tbusy-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 tbusy-time *milliseconds*

no llc2 tbusy-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software waits before repolling a busy remote station. The minimum is 1 ms and the maximum is 60000 ms. The default is 9600 ms.

Defaults

9600 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

An Logical Link Control, type 2 (LLC2) station can to notify other stations that it is temporarily busy, so the other stations will not attempt to send any new information frames. The frames sent to indicate this are called Receiver Not Ready (RNR) frames. Change the value of this parameter only to increase the value for LLC2-speaking stations that have unusually long busy periods before they clear their busy status. Increasing the value will prevent the stations from timing out.

Examples

In the following example, the software will wait up to 12,000 ms before attempting to poll a remote station through Token Ring interface 0 to learn the station's status:

```
! enter a global command, if you have not already
interface tokenring 0
! wait 12000 milliseconds before polling a station through tokenring 0
 llc2 tbusy-time 12000
```

Related Commands

Command	Description
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
llc2 idle-time	Controls the frequency of polls during periods of idle time (no traffic).
show llc2	Displays the LLC2 connections active in the router.

llc2 tpf-time

To set the amount of time the Cisco IOS software waits for a final response to a poll frame before resending the poll frame, use the **llc2 tpf-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 tpf-time *milliseconds*

no llc2 tpf-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) the software waits for a final response to a poll frame before resending the poll frame. The minimum is 1 ms and the maximum is 60000 ms. The default is 1000 ms.

Defaults

1000 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When a command is sent that must receive a response, a poll bit is sent in the frame. This is the receiving station's clue that the sender is expecting some response from it, be it an acknowledgment of information frames or an acknowledgment of more administrative tasks, such as starting and stopping the session. Once a sender gives out the poll bit, it cannot send any other frame with the poll bit set until the receiver replies with a frame containing a final bit set. If the receiver is faulty, it may never return the final bit to the sender. Therefore, the sender could be waiting for a reply that will never come. To avoid this problem, when a poll-bit-set frame is sent, a transmit-poll-frame (TPF) timer is started. If this timer expires, the software assumes that it can send another frame with a poll bit.

Usually, you will not want to change this value. If you do, the value should be larger than the T1 time, set with the **llc2 t1-time** command. The T1 time determines how long the software waits for receipt of an acknowledgment before sending the next set of frames.

Examples

Although you generally will not want to change the transmit-poll-frame (TPF) time, this example sets the TPF time to 3000 ms. Because the TPF time should be larger than the Logical Link Control, type 2 (LLC2) T1 time, this example shows the TPF time as double the LLC2 T1 time.

```
! enter a global command, if you have not already
interface tokenring 0
```

```
! send a poll bit set through tokenring 0 after a 3000 ms delay
 llc2 tpf-time 3000
! wait 1500 milliseconds for an acknowledgment before resending I-frames
 llc2 t1-time 1500
```

Related Commands

Command	Description
llc2 idle-time	Controls the frequency of polls during periods of idle time (no traffic).
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.
show llc2	Displays the LLC2 connections active in the router.

llc2 trej-time

To control the amount of time the Cisco IOS software waits for a correct frame after sending a reject command to the remote Logical Link Control, type 2 (LLC2) station, use the **llc2 trej-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 trej-time *milliseconds*

no llc2 trej-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software waits for a resend of a rejected frame before sending a reject command to the remote station. The minimum is 1 milliseconds (ms) and the maximum is 60000 ms. The default is 3200 ms.

Defaults

3200 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When an LLC2 station sends an information frame, a sequence number is included in the frame. The LLC2 station that receives these frames will expect to receive them in order. If it does not, it can reject a frame and indicate which frame it is expecting to receive instead. Upon sending a reject, the LLC2 station starts a reject timer. If the frames are not received before this timer expires, the session is disconnected.

Examples

In the following example, the software will wait up to 1000 ms to receive a previously rejected frame before resending its reject message to the station that sent the frame:

```
! enter a global command, if you have not already
interface tokenring 0
! wait 1000 milliseconds before resending a reject message through tokenring 0
 llc2 trej-time 1000
```

Related Commands

Command	Description
llc2 n2	Controls the number of times the Cisco IOS software retries sending unacknowledged frames or repolls remote busy stations.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

llc2 xid-neg-val-time

To control the frequency of exchange of identification (XID) transmissions by the Cisco IOS software, use the **llc2 xid-neg-val-tim** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 xid-neg-val-time *milliseconds*

no llc2 xid-neg-val-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms)) after which the software sends XID frames to other Logical Link Control, type 2 (LLC2)-speaking stations. The minimum is 0 ms and the maximum is 60000 ms. The default is 0 ms.

Defaults

0 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Do not change the **llc2 xid-neg-val-time** value unless requested by your technical support representative.

LLC2-speaking stations can communicate XID frames to each other. These frames identify the stations at a higher level than the MAC address and also can contain information about the configuration of the station. These frames are typically sent only during setup and configuration periods when it is deemed that sending them is useful. The greatest frequency at which this information is transferred is controlled by this timer.

Examples

The following example shows how to reset the frequency of XID transmissions to the default of 0 ms:

```
! enter a global command, if you have not already
interface tokenring 0
! set the frequency of XID transmissions to 0
 llc2 xid-neg-val-time 0
```

Related Commands

Command	Description
llc2 xid-retry-time	Sets the amount of time the Cisco IOS software waits for a reply to XID frames before dropping the session.
show llc2	Displays the LLC2 connections active in the router.

llc2 xid-retry-time

To set the amount of time the Cisco IOS software waits for a reply to exchange of identification (XID) frames before dropping the session, use the **llc2 xid-retry-time** command in internal adapter configuration mode. To revert to the default setting, use the **no** form of this command.

llc2 xid-retry-time *milliseconds*

no llc2 xid-retry-time *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) the software waits for a reply to XID frames before dropping a session. The minimum is 1 ms and the maximum is 60000 ms. The default is 60000 ms.

Defaults

60000 ms.

Command Modes

Internal adapter configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Set this value greater than the value of the T1 time or the time the software waits for an acknowledgment before dropping the session. T1 time is set with the **llc2 t1-time** command.

Examples

The following example sets the software to wait up to 60,000 ms for a reply to XID frames it sent to remote stations (which resets the value to its default):

```
! enter a global command, if you have not already
interface tokenring 0
! wait 60000 milliseconds for a reply to XID frames
 llc2 xid-retry-time 60000
```

Related Commands

Command	Description
llc2 t1-time	Controls the amount of time the Cisco IOS software will wait before resending unacknowledged information frames.

Command	Description
llc2 xid-neg-val-time	Controls the frequency of XID transmissions by the Cisco IOS software.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

lnm alternate

Note Effective with Cisco IOS release 12.3(4)T, the **lnm alternate** command is no longer available in Cisco IOS 12.3T releases.

To specify the threshold reporting link number, use the **lnm alternate** command in interface configuration mode. In order for a LAN Reporting Manager (LRM) to change parameters, it must be attached to the reporting link with the lowest reporting link number, and that reporting link number must be lower than this threshold reporting link number. To restore the default of 0, use the **no** form of this command.

lnm alternate *number*

no lnm alternate

Syntax Description

number	Threshold reporting link number. It must be in the range from 0 to 3.

Defaults

The default threshold reporting link number is 0.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

LAN Network Manager (LNM) employs the concepts of reporting links and reporting link numbers. A reporting link is simply a connection (or potential connection) between an LRM and a bridge. A reporting link number is a unique number used to identify a reporting link. An IBM bridge allows four simultaneous reporting links numbered 0 to 3. Only the LRM attached to the lowest number connection is allowed to change any parameters, and then only when that connection number falls below a certain configurable number. In the default configuration, the LRM connected through link 0 is the only LRM allowed to change parameters.

Note Setting the threshold reporting link number on one interface in a source-route bridge will cause it to appear on the other interface of the bridge, because the command applies to the bridge itself and not to either of the interfaces.

Examples

The following example permits LRMs connected through links 0 and 1 to change parameters:

```
! provide appropriate global configuration command if not currently in your config.
!
! permit 0 and 1
lnm alternate 1
```

The following example permits all LRMs to change parameters in the Cisco IOS software:

```
! provide appropriate global configuration command if not currently in your config.
!
! permit 0, 1, 2, and 3
lnm alternate 3
```

Related Commands

Command	Description
lnm password	Sets the password for the reporting link.

lnm crs

Note Effective with Cisco IOS release 12.3(4)T, the **lnm crs** command is no longer available in Cisco IOS 12.3T releases.

To monitor the current logical configuration of a Token Ring, use the **lnm crs** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm crs

no lnm crs

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Configuration Report Server service tracks the current logical configuration of a Token Ring and reports any changes to LAN Network Manager (LNM). It also reports on various other activities such as the change of the Active Monitor on a Token Ring.

For more information about the Active Monitor, refer to the *IBM Token Ring Architecture Reference Manual* or the IEEE 802.5 specification.

Examples

The following example disables monitoring of the current logical configuration of a Token Ring:

```
interface tokenring 0
 no lnm crs
```

Related Commands

Command	Description
lnm rem	Monitors errors reported by any station on the ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm disabled

Note Effective with Cisco IOS release12.3(4)T, the **lnm disable** command is no longer available in Cisco IOS 12.3T releases.

To disable LAN Network Manager (LNM) functionality, use the **lnm disabled** command in global configuration mode. To restore LNM functionality, use the **no** form of this command.

lnm disabled

no lnm disabled

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Under some circumstances, you can disable all LNM server functions on the router without having to determine whether to disable a specific server, such as the ring parameter server or the ring error monitor on a given interface.

This command can be used to terminate all LNM server input and reporting links. In normal circumstances, this command should not be necessary because it is a superset of the functions normally performed on individual interfaces by the **no lnm rem** and **no lnm rps** commands.

Examples

The following example disables LNM functionality:

```
lnm disabled
```

Related Commands

Command	Description
lnm pathtrace-disabled	Disables pathtrace reporting to LNM stations.
lnm rem	Monitors errors reported by any station on the ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm express-buffer

Note Effective with Cisco IOS release 12.3(4)T, the **lnm express-buffer** command is no longer available in Cisco IOS 12.3T releases.

To enable the LAN Network Manager (LNM) Ring Parameter Server (RPS) express buffer function, use the **lnm express-buffer** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm express-buffer

no lnm express-buffer

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The RPS express buffer function allows the router to set the express buffer bit to ensure priority service for frames required for ring station initiation. When this function is enabled, the router sets the express buffer bit in its initialize ring station response, which allows Token Ring devices to insert into the ring during bursty conditions.

Examples

The following example enables the LNM RPS express buffer function:

```
lnm express-buffer
```

lnm loss-threshold

Note Effective with Cisco IOS release 12.3(4)T, the **lnm loss-threshold** command is no longer available in Cisco IOS 12.3T releases.

To set the threshold at which the Cisco IOS software sends a message informing all attached LAN Network Manager (LNM)s that it is dropping frames, use the **lnm loss-threshold** command in interface configuration mode. To return to the default value, use the **no** form of this command.

lnm loss-threshold *number*

no lnm loss-threshold

Syntax Description

number	Single number expressing the percentage loss rate in hundredths of a percent. The valid range is from 0 to 9999. The default is

Defaults

10 (0.10 percent).

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The software sends a message to all attached LNMs whenever it begins to drop frames. The point at which this report is generated (threshold) is a percentage of the number of frames dropped compared with the number of frames forwarded.

When setting this value, remember that 9999 would mean 100 percent of your frames could be dropped before the message is sent. A value of 1000 would mean 10 percent of the frames could be dropped before sending the message. A value of 100 would mean 1 percent of the frames could be dropped before the message is sent.

Examples

In the following example, the loss threshold is set to 0.02 percent:

```
interface tokenring 0
 lnm loss-threshold 2
```

lnm password

Note Effective with Cisco IOS release 12.3(4)T, the **lnm password** command is no longer available in Cisco IOS 12.3T releases.

To set the password for the reporting link, use the **lnm password** command in interface configuration mode. To return the password to its default value of 00000000, use the **no** form of this command.

lnm password *number string*

no lnm password *number*

Syntax Description

number	Number of the reporting link to which to apply the password. This value must be in the range from 0 to 3.
string	Password you enter at the keyboard. In order to maintain compatibility with LAN Network Manager (LNM), the parameter *string* should be a six- to eight-character string of the type listed in the "Usage Guidelines" section.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

LNM employs the concepts of reporting links and reporting link numbers. A reporting link is simply a connection (or potential connection) between a LAN Reporting Manager (LRM) and a bridge. A reporting link number is a unique number used to identify a reporting link. An IBM bridge allows four simultaneous reporting links numbered 0 to 3. Only the LRM attached to the lowest number connection is allowed to change any parameters, and then only when that connection number falls below a certain configurable number. In the default configuration, the LRM connected through link 0 is the only LRM allowed to change parameters.

Each reporting link has its own password. Passwords are used not only to prevent unauthorized access from an LRM to a bridge, but also to control access to the different reporting links. This is important because of the different abilities associated with the various reporting links.

Characters allowable in the *string* are the following:

- Letters
- Numbers
- Special characters @, #, $, or %

Passwords are displayed only through use of the privileged EXEC **show running-config** command.

Note Two parameters in an IBM bridge have no corresponding parameter in the Cisco IOS software. This means that any attempt to modify these parameters from LNM will fail and display an error message. The LNM names of these two parameters are *route active status* and *single route broadcast mode*.

Examples

In the following example, the password Zephyr@ is assigned to reporting link 2:

```
! provide appropriate global configuration command if not currently in your config.
!
lnm password 2 Zephyr@
```

Related Commands

Command	Description
lnm alternate	Specifies the threshold reporting link number. In order for an LRM to change parameters, it must be attached to the reporting link with the lowest reporting link number, and that reporting link number must be lower than this threshold reporting link number.

lnm pathtrace-disabled

Note Effective with Cisco IOS release 12.3(4)T, the **lnm pathtrace-dsiabled** command is no longer available in Cisco IOS 12.3T releases.

To disable pathtrace reporting to LAN Network Manager (LNM) stations, use the **lnm pathtrace-disabled** command in global configuration mode. To restore pathtrace reporting functionality, use the **no** form of this command.

lnm pathtrace-disabled [**all** | **origin**]

no lnm pathtrace-disabled

Syntax Description

all	(Optional) Disable pathtrace reporting to the LNM and originating stations.
origin	(Optional) Disable pathtrace reporting to originating stations only.

Defaults

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Under some circumstances, such as when new hardware has been introduced into the network and is causing problems, the automatic report pathtrace function can be disabled. The new hardware may be setting bit-fields B1 or B2 (or both) of the routing control field in the routing information field embedded in a source-route bridged frame. This condition may cause the network to be flooded by report pathtrace frames if the condition is persistent. The **lnm pathtrace-disabled** command, along with its options, allows you to alleviate network congestion that may be occurring by disabling all or part of the automatic report pathtrace function within LNM.

Examples

The following example disables all pathtrace reporting:

```
lnm pathtrace-disabled
```

Related Commands

Command	Description
lnm disabled	Disables LNM functionality.

lnm rem

Note Effective with Cisco IOS release 12.3(4)T, the **lnm rem** command is no longer available in Cisco IOS 12.3T releases.

To monitor errors reported by any station on the ring, use the **lnm rem** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm rem

no lnm rem

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Ring Error Monitor (REM) service monitors errors reported by any station on the ring. It also monitors whether the ring is in a functional state or in a failure state.

Examples

The following example shows the use of the **lnm rem** command:

```
interface tokenring 0
 lnm rem
```

Related Commands

Command	Description
lnm crs	Monitors the current logical configuration of a Token Ring.
lnm rps	Ensures that all stations on a ring are using a consistent set of reporting parameters.

lnm rps

Note Effective with Cisco IOS release 12.3(4)T, the **lnm rps** command is no longer available in Cisco IOS 12.3T releases.

To ensure that all stations on a ring are using a consistent set of reporting parameters, use the **lnm rps** command in interface configuration mode. To disable this function, use the **no** form of this command.

lnm rps

no lnm rps

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Ring Parameter Server (RPS) service ensures that all stations on a ring are using a consistent set of reporting parameters and are reporting to LAN Network Manager (LNM) when any new station joins a Token Ring.

Examples

The following example shows the use of the **lnm rps** command:

```
interface tokenring 0
 lnm rps
```

Related Commands

Command	Description
lnm crs	Monitors the current logical configuration of a Token Ring.
lnm rem	Monitors errors reported by any station on the ring.

lnm snmp-only

Note Effective with Cisco IOS release 12.3(4)T, the **lnm snmp-only** command is no longer available in Cisco IOS 12.3T releases.

To prevent any LAN Network Manager (LNM) stations from modifying parameters in the Cisco IOS software, use the **lnm snmp-only** command in global configuration mode. To allow modifications, use the **no** form of this command.

lnm snmp-only

no lnm snmp-only

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring a router for LNM support is very simple. It happens automatically as a part of configuring the router to act as a source-route bridge. Several commands are available to modify the behavior of the LNM support, but none of them are necessary for it to function.

Because there is now more than one way to remotely change parameters in the Cisco IOS software, this command was developed to prevent them from detrimentally interacting with each other.

This command does not affect the ability of LNM to monitor events, only to modify parameters in the Cisco IOS software.

Examples

The following command prevents any LNM stations from modifying parameters in the software:

```
lnm snmp-only
```

lnm softerr

Note Effective with Cisco IOS release 12.3(4)T, the **lnm softerr** command is no longer available in Cisco IOS 12.3T releases.

To set the time interval in which the Cisco IOS software will accumulate error messages before sending them, use the **lnm softerr** command in interface configuration mode. To return to the default value, use the **no** form of this command.

lnm softerr *ten-illiseconds*

no lnm softerr

Syntax Description

ten-milliseconds	Time interval in tens of milliseconds between error messages. The valid range is from 0 to 65535.

Defaults

200 ms (2 seconds).

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.3(4)T	This command is no longer available in Cisco IOS 12.3T releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

All stations on a Token Ring notify the ring error monitor (REM) when they detect errors on the ring. To prevent an excessive number of messages, error reports are not sent immediately, but are accumulated for a short period of time and then reported. A station learns this value from a router (configured as a source-route bridge) when it first enters the ring.

Examples

The following example changes the error-reporting frequency to once every 5 seconds:

```
lnm softerr 500
```

Related Commands

Command	Description
lnm rem	Monitors errors reported by any station on the ring.

locaddr-priority

To assign a remote source-route bridging (RSRB) priority group to an input interface, use the **locaddr-priority** command in interface configuration mode. To remove the RSRB priority group assignment from the interface, use the **no** form of this command.

locaddr-priority *list-number*

no locaddr-priority *list-number*

Syntax Description

list-number	Priority list number of the input interface.

Defaults

No RSRB priority group is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must use the **priority-list protocol** command to assign priorities to the ports as shown in Table 14.

Table 14 Common RSRB Services and Their Port Numbers

Service	Port
RSRB high priority	1996
RSRB medium priority	1987
RSRB normal priority	1988
RSRB low priority	1989

Examples

In the following example, Token Ring interface 0 is assigned the RSRB priority group 1; LU 01 is assigned a medium priority and maps to TCP port 1996; LU 02 has been assigned a normal priority and maps to TCP port 1987; LU 03 has been assigned a low priority and maps to TCP port 1988; and LU 04 has been assigned high priority and maps to TCP port 1989:

```
source-bridge ring-group 2624
source-bridge remote-peer 2624 tcp 10.0.0.1
source-bridge remote-peer 2624 tcp 10.0.0.2 local-ack priority
locaddr-priority-list 1 01 medium
```

```
locaddr-priority-list 1 02 normal
locaddr-priority-list 1 03 low
locaddr-priority-list 1 04 high
!
priority-list 1 protocol ip low tcp 1996
priority-list 1 protocol ip high tcp 1987
priority-list 1 protocol ip medium tcp 1988
priority-list 1 protocol ip normal tcp 1989
!
interface tokenring 0
 source-bridge 2576 8 2624
 locaddr-priority 1
```

Related Commands

Command	Description
locaddr-priority-list	Maps LUs to queueing priorities as one of the steps to establishing queueing priorities based on LU addresses.
priority-list protocol	Establishes queueing priorities based on the protocol type.

locaddr-priority-list

To map logical units (LUs) to queueing priorities as one of the steps to establishing queueing priorities based on LU addresses, use the **locaddr-priority-list** command in global configuration mode. To remove that priority queueing assignment, use the **no** form of this command. You use this command in conjunction with the **priority list** command.

locaddr-priority-list *list-number address-number queue-keyword* [**dsap** *ds*] [**dmac** *dm*] [**ssap** *ss*] [**smac** *sm*]

no locaddr-priority-list *list-number address-number queue-keyword* [**dsap** *ds*] [**dmac** *dm*] [**ssap** *ss*] [**smac** *sm*]

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the LU address priority list selected by the user.
address-number	Value of the LOCADDR= parameter on the LU macro, which is a 1-byte address of the LU in hexadecimal.
queue-keyword	Enables a priority queue type: Valid queue keyword values and their equivalent priority queue type level are: • **high**—Priority queue type is high. • **medium**—Priority queue type is medium. • **normal**—Priority queue type is normal. • **low**—Priority queue type is low.
dsap *ds*	(Optional) Indicates that the next argument, *ds*, represents the destination service access point address. The argument *ds* is a hexadecimal value.
dmac *dm*	(Optional) Indicates that the next argument, *dm*, is the destination MAC address. The argument *dm* is written as a dotted triple of four-digit hexadecimal numbers.
ssap *ss*	(Optional) Indicates that the next argument, *ss*, is the source service access point address. If this is not specified, the default is all source service access point addresses.
smac *sm*	(Optional) Indicates that the next argument, *sm*, is the source MAC address, written as a dotted triple of four-digit hexadecimal numbers. If this is not specified, the default is all source MAC addresses.

Defaults

No mapping.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The following keywords were added: • **ssap** • **smac**
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to map LUs to queueing priorities. Once you establish the priority for each LU, you can assign a priority to a TCP port. Hence you establish a mapping between the LUs and queueing priorities, and queueing priorities and TCP ports.

It is preferable to prioritize NetBIOS traffic below Systems Network Architecture (SNA) traffic, but by default NetBIOS traffic is assigned the high priority on TCP port 1996.

Examples

In the following example, Token Ring interface 0 is assigned the remote source-route bridging (RSRB) priority group 1; LU 01 is assigned a medium priority and maps to TCP port 1996; LU 02 has been assigned a normal priority and maps to TCP port 1987; LU 03 has been assigned a low priority and maps to TCP port 1988; and LU 04 has been assigned high priority and maps to TCP port 1989:

```
source-bridge ring-group 2624
source-bridge remote-peer 2624 tcp 10.0.0.1
source-bridge remote-peer 2624 tcp 10.0.0.2 local-ack priority
locaddr-priority-list 1 01 medium
locaddr-priority-list 1 02 normal
locaddr-priority-list 1 03 low
locaddr-priority-list 1 04 high
!
priority-list 1 protocol ip low tcp 1996
priority-list 1 protocol ip high tcp 1987
priority-list 1 protocol ip medium tcp 1988
priority-list 1 protocol ip normal tcp 1989
!
interface tokenring 0
 source-bridge 2576 8 2624
 locaddr-priority 1
```

The following example shows how to establish queueing priorities based on the address of the serial link on a serial tunnel (STUN) connection. Note that you must use the **priority-group** command in interface configuration mode to assign a priority group to an input interface.

```
stun peer-name 10.108.254.6
stun protocol-group 1 sdlc
locaddr-priority-list 1 02 high
locaddr-priority-list 1 03 high
locaddr-priority-list 1 04 medium
locaddr-priority-list 1 05 low
!
interface serial 0
 no ip address
 encapsulation stun
```

```
stun group 1
stun route address 4 interface serial 0 direct
locaddr priority 1
priority-group 1
```

Related Commands

Command	Description
locaddr-priority	Assigns an RSRB priority group to an input interface.
priority-list protocol	Establishes queueing priorities based on the protocol type.

lsap

To create a service access point (SAP) in the Systems Network Architecture (SNA) session switch and enter Dependent Logical Unit Requestor (DLUR) SAP configuration mode, use the **lsap** DLUR configuration command. To delete a SAP and all SNA session switch links using the internal LAN interface, use the **no** form of this command.

lsap *type adapter-number* [*lsap*]

no lsap *type adapter-number* [*lsap*]

Syntax Description

type	Internal adapter type on the Channel Interface Processor (CIP) card, which corresponds to the value specified in the **lan** internal LAN configuration command. The currently supported value for the *type* argument is **token-adapter**.
adapter-number	Internal adapter interface on the CIP card, which is the same value specified in the **adapter** internal LAN configuration command.
lsap	(Optional) Local SAP number, 04 to FC, in hexadecimal. The value must be even number and should normally be a multiple of four. It must be an unique within the internal adapter in that no other 802.2 clients of that adapter, in the router or in a host, should be allocated the same SAP. The default value is C0.

Defaults

The default value for the *lsap* argument is hexadecimal C0.

Command Modes

DLUR configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **lsap** command is valid only on the virtual channel interface. If the SAP in the SNA session switch function is already created, the **lsap** command with no arguments puts you in DLUR SAP configuration mode.

The **lsap** command can be entered only in DLUR configuration mode.

The **lsap** command uses values that are defined in two other commands: the **lan** internal LAN configuration command and the **adapter** internal LAN configuration command. The **lan** *type* and **adapter** *adapter-number* values configured on the Cisco Mainframe Channel Connection (CMCC) internal LAN interface are used in the **lsap** command. However, the **lan** *type* keyword is a little different.

Where the value for the *type* argument on the **lan** command is **tokenring**, the corresponding value for the *type* argument on **lsap** is **token-adapter**. This emphasizes that the number that follows is an **adapter** number, not a **lan** number.

The **no lsap** command hierarchically deletes any links using it. Any sessions using those links are lost.

Examples

The following example defines an adapter type, an adapter number, and a local SAP:

```
lsap token 0 B0
```

Related Commands

Command	Description
adapter	Configures internal adapters.
client pool	Nails clients to pools.
keylen	Specifies the maximum bit length for the encryption keys for SSL Encryption Support.

lu deletion

To specify whether the TN3270 server sends a REPLY-PSID poweroff request to virtual telecommunications access method (VTAM) to delete the corresponding logical unit (LU) when a client disconnects, use the **lu deletion** command in TN3270 server configuration mode. To remove LU deletion from the current configuration scope, use the **no** form of this command.

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. The default is never.
named	Delete only named LUs 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.

Dependent Logical Unit Requestor (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 into Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to add the **named** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 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 Dependent Logical Unit Requestor (DLUR) PUs using dynamic LU naming:

```
tn3270-server
listen-point 172.18.4.18
pu pu1 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.

lu termination

To specify whether a TERMSELF or UNBIND request/response unit (RU) is sent by the TN3270 server when a client turns off a device or disconnects, use the **lu termination** command in TN3270 server configuration mode. To remove LU termination from the current configuration scope, use the **no** form of this command.

lu termination {**termself** | **unbind**}

no lu termination

Syntax Description

termself	Orders termination of all sessions and session requests associated with a logical unit (LU) upon disconnect.
unbind	Requests termination of the session by the application upon LU disconnect. This value is the default.

Defaults

unbind is the default.

Command Modes

TN3270 server configuration
Listen-point configuration
Listen-point PU configuration
Dependent Logical Unit Requestor (DLUR) PU configuration
PU configuration

Note The **lu termination** command is a siftdown command, so it can be used at any of the configuration command modes shown. The most recent **lu termination** 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 into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **termself** keyword when you want to be sure that the application terminates the session when the LU disconnects. This is important for certain applications such as Customer Information Control System (CICS).

If you use the **unbind** keyword for session termination with applications such as CICS, virtual telecommunications access method (VTAM) security problems can arise. When CICS terminates a session from an UNBIND request, the application may reestablish a previous user's session with a new user, who is now assigned to the same freed LU.

In TN3270 server configuration mode, the **lu termination** command applies to all PUs supported by the TN3270 server.

In listen-point configuration mode, the **lu termination** command applies to all PUs defined at the listen point.

In listen-point PU configuration mode, the **lu termination** command applies only to the specified PU.

In DLUR PU configuration mode, the **lu termination** command applies to all PUs defined under DLUR configuration mode.

In PU configuration mode, the **lu termination** command applies only to the specified PU.

Examples

Following is an example of the **lu termination** configuration command to force termination of the session when an LU disconnects for any PUs supported by the TN3270 server:

```
tn3270-server
 lu termination termself
```