Serial Tunnel and Block Serial Tunnel Commands

Cisco's serial tunnel (STUN) feature allows Synchronous Data Link Control (SDLC) or High-Level Data Link Control (HDLC) devices to connect to one another through a multiprotocol internetwork rather than through a direct serial link. STUN encapsulates SDLC frames in either the Transmission Control Protocol/Internet Protocol (TCP/IP) or the HDLC protocol. STUN provides a straight passthrough of all SDLC traffic (including control frames, such as Receiver Ready) end-to-end between Systems Network Architecture (SNA) devices.

Cisco's SDLC local acknowledgment provides local termination of the SDLC session so that control frames no longer travel the WAN backbone networks. This means end nodes do not time out, and a loss of sessions does not occur. You can configure your network with STUN, or with STUN and SDLC local acknowledgment. To enable SDLC local acknowledgment, the Cisco IOS software must first be enabled for STUN and routers configured to appear on the network as primary or secondary SDLC nodes. TCP/IP encapsulation must be enabled. Cisco's SDLC transport feature also provides priority queuing for TCP encapsulated frames.

Cisco's block serial tunnel (BSTUN) implementation enables Cisco series 2500, 3600, 4000, 4500, 4700, and 7200 routers to support devices that use the Binary Synchronous Communications (Bisync) datalink protocol and asynchronous security protocols that include Adplex, ADT Security Systems, Inc., Diebold, asynchronous generic, and mdi traffic. Our support of the bisync protocol enables enterprises to transport Bisync traffic and SNA multiprotocol traffic over the same network.

Use the commands in this chapter to configure BSTUN, Bisync, STUN, and SDLC local acknowledgment networks. For STUN and BSTUN configuration information and examples, refer to the "Configuring Serial Tunnel and Block Serial Tunnel" chapter in the *Bridging and IBM Networking Configuration Guide*.

asp addr-offset

Use the **asp addr-offset** interface configuration command to configure an asynchronous port to transmit and receive polled asynchronous traffic through a BSTUN tunnel. Use the **no** form of this command to cancel the specification.

asp addr-offset *address-offset*
no asp addr-offset

Syntax Description

address-offset	Location of the address byte within the polled asynchronous frame being received.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

This command is used to specify the offset from the start of the frame where the address byte is located. This command only applies when the asynchronous-generic protocol has been specified on an interface using a combination of the **bstun protocol-group** global configuration command and the **bstun group** interface configuration command.

Interfaces configured to run the asynchronous-generic protocol have their baud rate set to 9600 bps, use 8 data bits, no parity, 1 start bit, and 1 stop bit. If different line configurations are required, use the **rxspeed**, **txspeed**, **databits**, **stopbits**, and **parity** line configuration commands to change the line attributes.

The addresses of the alarm panels should be used in the address field of the **bstun route address** interface configuration command.

Example

The following example specifies that the first byte in the polled asynchronous frame contains the device address:

```
asp addr-offset 0
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

asp role
asp rx-ift
bstun protocol-group
bstun route

asp role

Use the **asp role** interface configuration command to specify whether the router is acting as the primary end of the polled asynchronous link or as the secondary end of the polled asynchronous link connected to the serial interface and the attached remote device is a security alarm control station. Use the **no** form of this command to cancel the specification.

asp role {**primary** | **secondary**}
no asp role {**primary** | **secondary**}

Syntax Description

primary	Router is the primary end of the polled asynchronous link connected to the serial interface, and the attached remote devices are alarm panels.
secondary	Router is the secondary end of the polled asynchronous link connected to the serial interface, and the attached remote device is a security alarm control station.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

This command enables the interface on which ASP is configured. Configure the interface connected to the alarm console as a secondary router and the interface connected to the alarm panel as a primary router.

The addresses of the alarm panels should be used in the address field of the **bstun route address** interface configuration command.

Example

The following example specifies the router as the primary end of the link:

```
asp role primary
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun route

asp rx-ift

Use the **asp rx-ift** interface configuration command to specify a time period that, by expiring, signals the end of one frame being received and the start of the next. Use the **no** form of this command to cancel the specification.

asp rx-ift *interframe-timeout*
no asp rx-ift

Syntax Description

interframe-timeout	Number of milliseconds between the end of one frame being received and the start of the next frame.

Default

The default timeout value is 40 ms.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

The interframe timeout is useful when different baud rates are used between the router and the alarm console or alarm panel. For example, you might set an interframe timeout of 6 ms if the polled asynchronous protocol is running at 9600 bps, but set the value to 40 ms if the protocol is running at 300 bps.

This command applies only when the asynchronous-generic protocol has been specified on an interface using a combination of the **bstun protocol-group** global configuration command and the **bstun group** interface configuration command.

Interfaces configured to run the asynchronous-generic protocol have their baud rate set to 9600 bps, use 8 data bits, no parity, 1 start bit, and 1 stop bit. If different line configurations are required, use the **rxspeed**, **txspeed**, **databits**, **stopbits**, and **parity** line configuration commands to change the line attributes.

The addresses of the alarm panels should be used in the address field of the **bstun route address** interface configuration command.

Example

The following example sets the interframe timeout value to 6 ms because the polled asynchronous protocol is running at 9600 bps:

```
asp rx-ift 6
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

asp addr-offset
asp role
bstun protocol-group
bstun route

bsc char-set

Use the **bsc char-set** interface configuration command to specify the character set used by the Bisync support feature in this serial interface as either EBCDIC or ASCII. Use the **no** form of this command to cancel the character set specification.

bsc char-set {**ascii** | **ebcdic**}
no bsc char-set {**ascii** | **ebcdic**}

Syntax Description

ascii	ASCII character set.
ebcdic	EBCDIC character set.

Default

EBCDIC

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following command specifies that the ASCII character set will be used:

```
bsc char-set ascii
```

bsc contention

Use the **bsc contention** interface configuration command to specify an address on a contention interface. Use the **no** form of this command to cancel the specification.

bsc contention *address*
no bsc contention

Syntax Description

address	Address assigned to contention interface. The range is 1 to 255. The default is 0x01.

Default

The default address is 0x01 to accommodate backward compatibility to the previous point-to-point contention implementation.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following command specifies address 20 on the remote device:

```
bsc contention 20
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bsc dial-contention

bsc dial-contention

Use the **bsc dial-contention** interface configuration command to specify a router at the central site as a central router with dynamic allocation of serial interfaces. Use the **no** form of this command to cancel the specification. A timeout value is configurable to ensure that an interface does not get locked out because of a device outage during transmission.

bsc dial-contention *time-out*
no bsc dial-contention

Syntax Description

time-out	Amount of time interface can sit idle before it is returned to the idle interface pool. The range is 2 to 30 seconds. The default is 5 seconds.

Default

5 seconds

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

Example

The following command defines a dial-in interface at the central site with an idle timeout of 10 seconds:

```
bsc dial-contention 10
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bsc contention

bsc host-timeout

Use the **bsc host-timeout** interface configuration command to detect deactivation of devices at the host. Use the **no** form of this command to cancel the configuration.

bsc host-timeout *interval*
no host-timeout *interval*

Syntax Description

interval	Timeout interval within which a poll or select for a control unit must be received. If this interval expires, the remote router is sent a teardown peer signal. The range is 30 to 3000 deciseconds. The default is 60 seconds.

Default

The default interval is 60 seconds.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

This command is used to detect deactivation of devices at the host. If the host is told to deactivate or not poll a device it will take time for the signal to propagate the network and get the remote end from polling. The timeout can be used to fine tune the delay in detecting the host outage. The remote peer will stop polling the control unit that has timed out in the interval 1 to 2 times the configured timeout value.

Example

The following example configures a timeout of 50 seconds:

```
bsc host-timeout 500
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bsc secondary
bstun group
bstun protocol-group

bsc pause

Use the **bsc pause** interface configuration command to specify the interval to the tenth of a second, between starts of the polling cycle. Use the **no** form of this command to cancel the specification.

bsc pause *time*
no bsc pause *time*

Syntax Description

time	Interval in tenths of a second. The default value is 10 (1 second). The maximum time is 25.5 seconds.

Default

10 (1 second)

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following command sets the interval to 2 seconds:

```
bsc pause 20
```

bsc poll-timeout

Use the **bsc poll-timeout** interface configuration command to specify the timeout, in tenths of a second, for a poll or select sequence. Use the **no** form of this command to cancel the specification.

bsc poll-timeout *time*
no bsc poll-timeout *time*

Syntax Description

time	Time in tenths of a second. The default value is 10 (1 second).

Default

10 (1 second)

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following command sets the interval to 2 seconds:

```
bsc poll-timeout 20
```

bsc primary

Use the **bsc primary** interface configuration command to specify that the router is acting as the primary end of the Bisync link connected to the serial interface, and that the attached remote devices are Bisync tributary stations. Use the **no** form of this command to cancel the specification.

bsc primary
no bsc primary

Syntax Description

This command has no arguments or keywords.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

The Bisync support feature in the serial interface uses the address of the incoming encapsulation for reply.

Example

The following example specifies the router as the primary role:

```
bsc primary
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun route

bsc retries

Use the **bsc retries** interface configuration command to specify the number of retries performed before a device is considered to have failed. Use the **no** form of this command to cancel the specification.

bsc retries *retries*
no bsc retries *retries*

Syntax Description

retries	Number of retries before a device fails. The default is 5.

Default

5 retries

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following command sets the retry count to 10:

```
bsc retries 10
```

bsc secondary

Use the **bsc secondary** interface configuration command to specify that the router is acting as the secondary end of the Bisync link connected to the serial interface, and the attached remote device is a Bisync control station. Use the **no** form of this command to cancel the specification.

bsc secondary
no bsc secondary

Syntax Description

This command has no arguments or keywords.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

The Bisync support feature in this serial interface uses the address of the poll or selection block in the framing encapsulation. It also generates an end of transmission (EOT) frame preceding each Bisync poll and selection.

Example

The following example specifies the router as the secondary role:

```
bsc secondary
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun route

bsc servlim

Use the **bsc servlim** interface configuration command to specify the number of cycles of the active poll list that are performed between polls to control units in the inactive poll list. Use the **no** form of this command to cancel the specification.

bsc servlim *servlim-count*
no bsc servlim *servlim-count*

Syntax Description

servlim-count	Number of cycles. The range is 1 to 50. The default is 3.

Default

3 cycles

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following command sets the number of cycles to 2:

```
bsc servlim 2
```

bsc spec-poll

Use the **bsc spec-poll** interface configuration command to set specific polls, rather than general polls, used on the host-to-router connection. Use the **no** form of this command to cancel the specification.

bsc spec-poll
no spec-poll

Syntax Description

This command has no arguments or keywords.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Use the **bsc spec-poll** command when a router is connected to a host, and only when that host issues specific polls rather than general polls. Tandem hosts that poll ATM cash machines are typically configured to use specific polls rather than general polls.

Configuring a downstream (control-unit/device connected) router to support specific polling has no effect.

Example

The following commands configure interface serial 0 to use specific poll:

```
interface serial 0
 description Connection to host.
 encapsulation bstun
 bstun group 1
 bsc secondary
 bsc spec-poll
 bsc char-set ebcdic
 bstun route all tcp <ip-addr-of-remote-peer>
```

bstun group

Use the **bstun group** interface configuration command to specify the BSTUN group to which the interface belongs. Use the **no** form of this command to remove the interface from the BSTUN group.

bstun group *group-number*
no bstun group *group-number*

Syntax Description

group-number	BSTUN group to which the interface belongs.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Each BSTUN-enabled interface must be placed in a BSTUN group that was previously defined by the **bstun protocol-group** command. Packets only travel between BSTUN-enabled interfaces that are in the same group.

Example

The following example specifies that serial interface 1 belongs to the previously defined protocol group 1:

```
interface serial 1
 encapsulation bstun
 bstun group 1
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun protocol-group
encapsulation bstun

bstun keepalive-count

Use the **bstun keepalive-count** global configuration command to define the number of times to attempt a peer connection before declaring the peer connection to be down. Use the **no** form of this command to cancel the definition.

bstun keepalive-count *count*
no bstun keepalive-count

Syntax Description

count	Number of connection attempts. The range is between 2 and 10 retries.

Default

No default is specified.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Example

The following example sets the number of times to retry a connection to a peer to 4:

```
bstun keepalive-count 4
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun remote-peer-keepalive

bstun lisnsap

Use the **bstun lisnsap** global configuration command to configure a SAP on which to listen for incoming calls. Use the **no** form of this command to cancel the lisnsap.

bstun lisnsap *sap-value*
no bstun lisnsap

Syntax Description

sap-value	SAP on which to listen for incoming calls. The default is 04.

Default

The default SAP value is 04.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

Changes to the **bstun lisnsap** command configuration will not take effect until after the router has been reloaded.

Example

The following example configures a SAP for listening:

```
bstun lisnsap
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun route (Frame Relay)
frame-relay map bstun
frame-relay map llc2

bstun peer-name

Use the **bstun peer-name** global configuration command to enable the block serial tunneling function. Use the **no** form of this command to disable the function.

bstun peer-name *ip-address*
no bstun peer-name *ip-address*

Syntax Description

ip-address	Address by which this BSTUN peer is known to other BSTUN peers that are using the TCP transport.

Default

No default is specified.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

The IP address defines the address by which this BSTUN peer is known to other BSTUN peers that are using the TCP transport. If this command is unconfigured or the **no** form of this command is specified, all BSTUN routing commands with IP addresses are deleted. BSTUN routing commands without IP addresses are not affected by this command.

Example

The following example enables the block serial tunneling function:

```
bstun peer-name 150.10.254.201
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun protocol-group

bstun protocol-group

Use the **bstun protocol-group** global configuration command to define a BSTUN group and the protocol it uses. Use the **no** form of this command to delete the BSTUN group.

bstun protocol-group *group-number protocol*
no bstun protocol-group *group-number protocol*

Syntax Description

group-number	BSTUN group number. Valid numbers are decimal integers in the range 1 to 255.
protocol	Block serial protocol, selected from the following: **adplex** **adt-poll-select** **adt-vari-poll** **async-generic** **bsc** **bsc-local-ack** **diebold** **mdi**

Default

No defaults are specified.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Interfaces configured to run the Adplex protocol have their baud rate set to 4800 bps, use even parity, 8 data bits, 1 start bit, and 1 stop bit.

Interfaces configured to run the adt-vari-poll and adt-poll-select protocols have their baud rate set to 600 bps, use even parity, 8 data bits, 1 start bit, and 1.5 stop bits. If different line configurations are required, use the **rxspeed**, **txspeed**, **databits**, **stopbits**, and **parity** line configuration commands to change the line attributes.

Interfaces configured to run the asynchronous-generic protocol have their baud rate set to 9600 bps, use no parity, 8 data bits, 1 start bit, and 1 stop bit. If different line configurations are required, use the **rxspeed**, **txspeed**, **databits**, **stopbits**, and **parity** line configuration commands to change the line attributes.

Interfaces configured to run the mdi protocol have their baud rate set to 600 bps, use even parity, 8 data bits, 1 start bit, and 1.5 stop bits. If different line configurations are required, use the **rxspeed**, **txspeed**, **databits**, **stopbits**, and **parity** line configuration commands to change the line attributes. The mdi protocol allows alarm panels to be sent to the the MDI alarm console.

Example

The following example defines BSTUN group 1, specifies that it uses the Bisync protocol, and indicates that frames will be locally acknowledged:

```
bstun protocol-group 1 bsc-local-ack
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun group

bstun remote-peer-keepalive

Use the **bstun remote-peer-keepalive** global configuration command to enable detection of the loss of a peer. Use the **no** form of this command to disable detection.

bstun remote-peer-keepalive *seconds*
no bstun remote-peer-keepalive

Syntax Description

seconds	Keepalive interval, in seconds. The range is 1 to 300 seconds.

Default

30 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Example

In the following example, the remote-peer-keepalive interval is set to 60 seconds:

```
bstun remote-peer-keepalive 60
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun keepalive-count

bstun route

Use the **bstun route** interface configuration command to define how frames will be forwarded from a BSTUN interface to a remote BSTUN peer. Use the **no** form of this command to cancel the definition.

bstun route {**all** | **address** *address-number*} {**tcp** *ip-address* | **interface serial** *number*}
no bstun route {**all** | **address** *address-number*} {**tcp** *ip-address* | **interface serial** *number*}

Syntax Description

all	All BSTUN traffic received on the input interface is propagated, regardless of the address contained in the serial frame.
address	Serial frame that contains a specific address is propagated.
address-number	Poll address, a hexadecimal number from 01 to FF (but not all values are valid). The reply address to be used on the return leg is calculated from the configured poll address.
tcp	TCP encapsulation is used to propagate frames that match the entry.
ip-address	IP address of the remote BSTUN peer.
interface serial	HDLC encapsulation is used to propagate the serial frames.
number	Serial line to an appropriately configured router on the other end.

Default

No defaults are specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

When the ADplex protocol is specified in the **bstun protocol-group** command, ADplex device addresses are limited to the range 1 to 127 because ADplex alarm panels invert the device address in the ADplex frame when responding to alarm console commands.

When the adt-poll-select protocol is specified in the **bstun protocol-group** command, routes for specific addresses cannot be specified on the downstream router (connected to the alarm panel), because no address field is provided within frames that are sent back to the alarm console. The only way to route traffic back to the alarm console is to use the **bstun route all** form of the **bstun route** command. This is also true for the diebold protocol and any other protocol supported by the asynchronous-generic protocol group that does not include a device address in the frame.

When the adt-vari-poll protocol is specified in the **bstun protocol-group** command, ADT device addresses are limited to the range 0 to 255, and address 0 is reserved for use as a broadcast address for adt-vari-poll only. If address 0 is specified in the **bstun route address** form of the **bstun route** command, the address is propagated to all configured BSTUN peers.

It is possible to use both the **all** and the **address** keywords on different **bstun route** commands on the same serial interface. When this is done, the **address** specifications take precedence; if none of these match, then the **all** specification is used to propagate the frame.

Example

In the following example, all BSTUN traffic received on serial interface 0 is propagated, regardless of the address contained in the serial frame:

```
bstun route all interface serial 0
```

bstun route (Frame Relay)

Use the **bstun route** interface configuration command to define how frames will be forwarded from a BSTUN interface to a remote BSTUN peer over Frame Relay. Use the **no** form of this command to cancel the definition.

bstun route {**all** | **address** *cu-address*} **interface serial** *number* **dlci** *dlci rsap* **priority** *priority*
no bstun route {**all** | **address** *cu-address*} **interface serial** *number* **dlci** *dlci rsap*
priority *priority*]

Syntax Description

all	All BSTUN traffic received on the input interface is propagated, regardless of the address contained in the serial frame.
address	Serial frames that contain a specific address are propagated.
cu-address	Control unit address for the Bisync end station.
interface serial *number*	Specify a serial interface on which Frame Relay encapsulation is used to propagate serial frames.
dlci *dlci*	Data-link connection identifier to be used on the Frame Relay interface.
rsap	Remote SAP, to be used when initiating an LLC2 session. This argument is configurable only if the interface group number supports local acknowledgment.
priority *priority*	Priority port to be used for this LLC2 session. Configurable only if the interface group number supports local acknowledgment.

Default

No defaults are specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Example

The following example configures BSTUN over Frame Relay. All BSTUN traffic is propagated to serial interface 0 regardless of the address contained in the serial frame:

```
bstun route all interface serial 0 dlci 16
```

encapsulation bstun

Use the **encapsulation bstun** interface configuration command to configure BSTUN on a particular serial interface. Use the **no** form of this command to disable the BSTUN function on the interface.

encapsulation bstun
no encapsulation bstun

Syntax Description

This command has no arguments or keywords.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

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, complete 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 only travel 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.

Example

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

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

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun group
bstun peer-name
bstun protocol-group

encapsulation stun

Use the **encapsulation stun** interface configuration command to enable STUN encapsulation on a specified serial interface.

encapsulation stun

Syntax Description

This command has no arguments or keywords.

Default

STUN encapsulation is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Use this command to enable STUN on an interface. Before using this command, complete 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 only travel 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.

Example

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 131.108.254.6
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 131.108.254.7
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

stun group
stun peer-name
stun protocol-group

frame-relay map bstun

Use the **frame-relay map bstun** interface configuration command to configure BSTUN over Frame Relay for passthru. Use the **no** form of this command to cancel the configuration.

frame-relay map bstun *dlci*
no frame-relay map bstun *dlci*

Syntax Description

dlci	Frame Relay DLCI number on which to support passthru.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

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

Example

The following example maps BSTUN traffic to DLCI number 16:

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

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun lisnsap
bstun protocol-group
encapsulation frame-relay

frame-relay map llc2

Use the **frame-relay map llc2** interface configuration command to configure BSTUN over Frame Relay when using Bisync local acknowledgement. Use the **no** form of this command to cancel the configuration.

frame-relay map llc2 *dlci*
no frame-relay map llc2 *dlci*

Syntax Description

dlci	Frame Relay DLCI number on which to support local acknowledgement.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

Example

The following example maps BSTUN traffic to DLCI number 16:

```
frame-relay map DLCI 16
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun lisnsap
bstun protocol-group
encapsulation frame-relay

locaddr-priority-list

Use the **locaddr-priority-list** interface configuration command to establish queuing priorities based upon the address of the logical unit (LU). Use the **no** form of this command to cancel all previous assignments.

locaddr-priority-list *list-number address-number queue-keyword*
no locaddr-priority-list

Syntax Description

list-number	Arbitrary integer between 1 and 10 that identifies the LU address priority list.
address-number	Value of the LOCADDR=parameter on the LU macro, which is a 1-byte address of the LU in hexadecimal.
queue-keyword	Priority queue type: **high**, **medium**, **normal**, or **low**.

Default

No queuing priorities are established.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

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

```
stun peer-name 131.108.254.6
stun protocol-group 1 sdlc
!
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
!
 locaddr-priority-list 1 02 high
 locaddr-priority-list 1 03 high
 locaddr-priority-list 1 04 medium
 locaddr-priority-list 1 05 low
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

priority-group

priority-group

Use the **priority-group** interface configuration command to assign a priority group to an interface. Use the **no** form of this command to remove assignments.

priority-group *list-number*
no priority-group *list-number*

Syntax Description

list-number	Priority list number assigned to the interface.

Default

No priority group is assigned.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

The following example shows how to establish queuing priorities based on the address of the serial link on a STUN connection. Note that you must use the **priority-group** interface configuration command to assign a priority group to an output interface.

```
! sample stun peer-name global command
stun peer-name 131.108.254.6
! sample protocol-group command for reference
stun protocol-group 1 sdlc
!
interface serial 0
! disable the ip address for interface serial 0
no ip address
! enable the interface for STUN
encapsulation stun
! sample stun group command
stun group 2
! sample stun route command
stun route address 10 tcp 131.108.254.8 local-ack priority
!
! assign priority group 1 to the input side of interface serial 0
priority-group 1
! assign a low priority to priority list 1 on serial link identified
! by group 2 and address A7
priority-list 1 stun low address 2 A7
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

locaddr-priority-list
priority-list protocol ip tcp
priority-list stun address

priority-list protocol bstun

Use the **priority-list protocol bstun** global configuration command to establish BSTUN queuing priorities based on the BSTUN header. Use the **no** form of this command to revert to normal priorities.

priority-list *list-number* **protocol bstun** *queue* [**gt | lt** *packetsize*]
[**address** *bstun-group bsc-addr*]
no priority-list *list-number* **protocol bstun** *queue* [**gt | lt** *packetsize*]
[**address** *bstun-group bsc-addr*]

Syntax Description

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
queue	Priority queue type: **high**, **medium**, **normal**, or **low**.
gt | lt *packetsize*	(Optional) Output interface examines header information *and* packet size and places packets with the BSTUN header that match criteria (gt or lt specified packet size) on specified output.
address *bstun-group bsc-addr*	(Optional) Output interface examines header information and Bisync address and places packets with the BSTUN header that match Bisync address on the specified output queue.

Default

Prioritize based on BSTUN header.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

In the following example, the output interface examines the header information and places packets with the BSTUN header on the output queue specified as medium.

```
priority-list 1 protocol bstun medium
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

encapsulation bstun

priority-list protocol ip tcp

Use the **priority-list protocol ip tcp** global configuration command to establish BSTUN or STUN queuing priorities based on the TCP port. Use the **no** form of this command to revert to normal priorities.

priority-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*
no priority-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*

Syntax Description

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
queue	Priority queue type: **high**, **medium**, **normal**, or **low**.
tcp-port-number	BSTUN port and priority settings are as follows: High—BSTUN port 1976 Medium—BSTUN port 1977 Normal—BSTUN port 1978 Low—BSTUN port 1979 STUN port and priority settings are as follows: High—STUN port 1994 Medium—STUN port 1990 Normal—STUN port 1991 Low—STUN port 1992

Default

The default is normal queue.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Use the **priority-list stun address** command first. Priority settings created with this command are assigned to SDLC ports.

Note SDLC local acknowledgment with the priority option must be enabled using the **stun route address tcp** command.

Examples

In the following example, queuing priority for address C1 using priority list 1 is set to high. A priority queue of high is assigned to the SDLC port 1994.

```
priority-list 1 stun high address 1 c1
priority-list 1 protocol ip high tcp 1994
```

In the following example, queuing priority for address C1 using priority list 1 is set to high. A priority queue of high is assigned to BSTUN port 1976.

```
priority-list bstun high address 1 c1
priority-list 1 protocol ip high 1976
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

bstun protocol-group
encapsulation bstun
encapsulation stun
priority-group
priority-list stun address
stun route address tcp

priority-list stun address

Use the **priority-list stun address** global configuration command to establish STUN queuing priorities based on the address of the serial link. Use the **no** form of this command to revert to normal priorities.

priority-list *list-number* **stun** *queue* **address** *group-number address-number*
no priority-list *list-number* **stun** *queue-keyword* **address** *group-number address-number*

Syntax Description

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
queue	Priority queue type: **high**, **medium**, **normal**, or **low**.
group-number	Group number that is used in the **stun group** command.
address-number	Address of the serial link. For an SDLC link, the format is a 1-byte hex value (for example, C1). For a non-SDLC link, the address format can be specified by the **stun schema** command.

Default

The default is normal queue.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Note SDLC local acknowledgment with the priority option must be enabled using the **stun route address interface serial** command.

The **priority-list** command is described in greater detail in the "Performance Management Commands" chapter in the *Configuration Fundamentals Command Reference*.

Example

In the following example, queuing priority for address C1 using priority list 1 is set to high:

```
priority-list 1 stun high address 1 c1
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

priority-list protocol ip tcp
stun group
stun route address interface serial
stun schema offset length format

queue-list protocol bstun

Use the **queue-list protocol bstun** global configuration command to customize BSTUN queuing priorities based on the BSTUN header. Use the **no** form of this command to revert to normal priorities.

queue-list *list-number* **protocol bstun** *queue* [**gt** | **lt** *packetsize*]
[**address** *bstun-group bsc-addr*]
no queue-list *list-number* **protocol bstun** *queue* [**gt** | **lt** *packetsize*]
[**address** *bstun-group bsc-addr*]

Syntax Description

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
queue	Priority queue type: **high**, **medium**, **normal**, or **low**.
gt | **lt** *packetsize*	(Optional) Output interface examines header information *and* packet size and places packets with the BSTUN header that match criteria (gt or lt specified packet size) on specified output.
address *bstun-group bsc-addr*	(Optional) Output interface examines header information and Bisync address and places packets with the BSTUN header that match Bisync address on the specified output queue.

Default

Prioritize based on BSTUN header.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

In the following example, the output interface examines the header information and places packets with the BSTUN header on the output queue specified as medium.

```
queue-list 1 protocol bstun medium
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

encapsulation bstun

queue-list protocol ip tcp

Use the **queue-list protocol ip tcp** global configuration command to customize BSTUN queuing priorities based on the TCP port. Use the **no** form of this command to revert to normal priorities.

queue-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*
no queue-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*

Syntax Description

list-number	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
queue	Priority queue type: **high**, **medium**, **normal**, or **low**.
tcp-port-number	BSTUN port and priority settings are as follows: High—BSTUN port 1976 Medium—BSTUN port 1977 Normal—BSTUN port 1978 Low—BSTUN port 1979 STUN port and priority settings are as follows: High—STUN port 1994 Medium—STUN port 1990 Normal—STUN port 1991 Low—STUN port 1992

Default

The default is normal queue.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

In the following example, queuing priority for address C1 using priority list 1 is set to high. A priority queue of high is assigned to BSTUN port 1976.

```
queue-list bstun high address 1 c1
queue-list 1 protocol ip high 1976
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

encapsulation bstun

sdlc virtual-multidrop

Use the **sdlc virtual-multidrop** interface configuration command to allow SDLC broadcast address FF to be replicated for each of the STUN peers, so each of the end stations receive the broadcast frame. Use the **no** form of this command to disable the SDLC broadcast feature.

sdlc virtual-multidrop
no sdlc virtual-multidrop

Syntax Description

This command has no arguments or keywords.

Default

SDLC broadcast is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Example

The following example allows each STUN peer to receive a broadcast frame:

```
sdlc virtual-multidrop
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

stun route address tcp

show bsc

Use the **show bsc** privileged EXEC command to display statistics about the interfaces on which Bisync is configured.

show bsc [**group** *bstun-group-number*] [**address** *address-list*]

Syntax Description

bstun-group-number	BSTUN group number. Valid numbers are decimal integers in the range 1 to 255.
address-list	List of poll addresses.

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Sample Displays

The following is sample output from the **show bsc** command:

```
Router# show bsc

BSC pass-through on Serial4:
HDX enforcement state: IDLE.
Frame sequencing state: IDLE.
Total Tx Counts: 0 frames(total). 0 frames(data). 0 bytes.
Total Rx Counts: 0 frames(total). 0 frames(data). 0 bytes.

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

        Poll address: C3. Select address: E3 *CURRENT-CU*
        State is Active.
        Tx Counts: 1136 frames(total). 0 frames(data). 1136 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

Total Tx Counts: 2273 frames(total). 0 frames(data). 2273 bytes.
Total Rx Counts: 2284 frames(total). 0 frames(data). 11420 bytes.
```

Table 33 describes significant fields shown in the display.

The following is sample output from the **show bsc** command specifying BSTUN group 50:

```
Router# show bsc group 50

BSC local-ack on serial5:
Secondary state is CU_Idle.
```

```
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
        Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.

        Poll address: C3. Select address: E3 *CURRENT-CU*
        State is Active.
        Tx Counts: 1214 frames(total). 0 frames(data). 1214 bytes.
        Rx Counts: 1220 frames(total). 0 frames(data). 6100 bytes.

Total Tx Counts: 2431 frames(total). 0 frames(data). 2431 bytes.
Total Rx Counts: 2442 frames(total). 0 frames(data). 12200 bytes.
```

The following is sample output from the **show bsc** command specifying BSTUN group 50 and poll address C2:

```
Router# show bsc group 50 address C2

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
        Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.

Total Tx Counts: 1217 frames(total). 0 frames(data). 1217 bytes.
Total Rx Counts: 1222 frames(total). 0 frames(data). 6110 bytes.
```

The following is sample output from the **show bsc** command specifying poll address C2:

```
Router# show bsc address C2

BSC pass-through on Serial4:
HDX enforcement state: IDLE.
Frame sequencing state: IDLE.
Total Tx Counts: 0 frames(total). 0 frames(data). 0 bytes.
Total Rx Counts: 0 frames(total). 0 frames(data). 0 bytes.

BSC local-ack on serial5:
Secondary state is CU_Idle.
Control units on this interface:

        Poll address: C2. Select address: E2.
        State is Active.
        Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
        Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.

Total Tx Counts: 1137 frames(total). 0 frames(data). 1137 bytes.
Total Rx Counts: 1142 frames(total). 0 frames(data). 5710 bytes.
```

Table 33 Show BSC Command Field Descriptions

Field	Description
BSC *x* on *interface y*	Indicates whether the router is configured for passthru or local acknowledgment on the indicated interface.
Output queue depth	Packets queued on this interface. This field is only displayed when the value is not zero.

Table 33 Show BSC Command Field Descriptions (Continued)

Field	Description
Frame builder state	Current frame building state. This field is only displayed when the state is not IDLE.
HDX enforcement state	Current half-duplex transmit enforcement state. The possible values are: • IDLE—Waiting for communication activity. • PND_COMP—Waiting for router to transmit. • PND_RCV—Waiting for attached device to respond to transmission.
Frame sequencing state	Frame sequencing state to protect against network latencies. When the router is configured as the primary end of the link, the possible values are: • IDLE—Waiting for a poll. • SEC—In a session with a device. When the router is configured as the secondary end of the link, the possible values are: • IDLE—Waiting for a poll. • PRI—In a session with a device. When the router is configured for point-to-point contention, the possible values are: • IDLE—Waiting for a poll. • PEND—Waiting for the first data frame. • PRI—Connected device is acting as a primary device. • SEC—Connected device is acting as a secondary device.
Total Tx Counts	Total transmit frame count for the indicated interface.
Total Rx Count	Total receive frame count for the indicated interface.
Primary state is …	The current state when the router is configured as the primary end of the link. The possible values are: • TCU_Down—Waiting for the line to become active. • TCU_EOFile—A valid block ending in ETX has been received. • TCU_Idle—Waiting for work or notification of completion of the transmission of EOT. • TCU_InFile—A valid block ending in ETB has been received. • TCU_Polled—A general poll has been issued. • TCU_Selected—A select has been issued. • TCU_SpecPolled—A specific poll has been sent. • TCU_TtdDelay—An ETB block was acknowledged, but the next block to be transmitted has not yet been received. • TCU_TtdSent—A TTD has been transmitted because no data was received by the time the timeout for sending Ttd expired. • TCU_TxEOFile—A block of data ending in ETX has been transmitted. • TCU_TxInFile—A block of data ending in ETB has been transmitted. • TCU_TxRetry—Trying to transmit a frame again.

Table 33 Show BSC Command Field Descriptions (Continued)

Field	Description
Secondary state is …	The current state when the router is configured as the secondary end of the link. The possible values are: • CU_DevBusy—A select has been refused with WACK or RVI. • CU_Down—Waiting for the line to become active. • CU_EOFile—A valid block ending in ETX has been received. • CU_Idle—Waiting for a poll or select action. • CU_InFile—A valid block ending in ETB has been received. • CU_Selected—A select has been acknowledged. • CU_TtdDelay—An ETB block was acknowledged, but the next block to be transmitted has not yet been received. • CU_TtdSent—A TTD has been transmitted because no data was received by the time the timeout for sending Ttd expired. • CU_TxEOFile—A block of data ending in ETX has been transmitted. • CU_TxInFile—A block of data ending in ETB has been transmitted. • CU_TxRetry—Trying to transmit a frame again. • CU_TxSpecPollData—A data frame (typically S/S) has been used to answer a specific poll. • CU_TxStatus—Host has polled for device-specific status.
Poll address	Address used when the host wants to get device information.
Select address	Address used when the host wants to send data to the device.
State is …	Current initialization state of this control unit. The possible values are: • Active—The remote device is active. • Inactive—The remote device is dead. • Initializing—No response from remote device yet.
Tx Counts	Transmit frame count for this control unit.
Rx Counts	Receive frame count for this control unit.
Total Tx Counts	Total transmit frame count for the indicated interface.
Total Rx Counts	Total receive frame count for the indicated interface.

show bstun

Use the **show bstun** privileged EXEC command to display the current status of STUN connections.

show bstun [**group** *bstun-group-number*] [**address** *address-list*]

Syntax Description

group *bstun-group-number*	BSTUN group number. Valid numbers are decimal integers in the range 1 to 255.
address *address-list*	List of poll addresses.

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Sample Displays

The following is sample output from the **show bstun** command with no options:

```
Router# show bstun

This peer: 22.22.1.107
 *Serial0  (group 1 [bsc])
route  transport  address     state     rx_pkts   tx_pkts   drops
all    TCP        22.22.1.108 closed        0         0       0

  Serial4  (group 3 [bsc])
route  transport  address     state     rx_pkts   tx_pkts   drops
C2     TCP        22.22.2.108 closed        0         0       0
C1     TCP        22.22.2.108 closed        0         0       0
40     TCP        22.22.1.108 closed        0         0       0

  Serial5  (group 50 [bsc])
route  transport  address     state     rx_pkts   tx_pkts   drops
C2     TCP        22.22.2.108 open          4         4       0
C3     TCP        22.22.2.108 open          3         3       0
```

The following is sample output from the **show bstun** command specifying BSTUN group 3:

```
Router# show bstun group 3

This peer: 22.22.1.107
  Serial4  (group 3 [bsc])
route  transport  address     state     rx_pkts   tx_pkts   drops
C2     TCP        22.22.2.108 closed        0         0       0
C1     TCP        22.22.2.108 closed        0         0       0
40     TCP        22.22.1.108 closed        0         0       0
```

The following is sample output from the **show bstun** command specifying BSTUN group 3 and poll address C1:

```
Router# show bstun group 3 address C1

This peer: 22.22.1.107
  Serial4  (group 3 [bsc])
route  transport  address     state     rx_pkts   tx_pkts   drops
C1     TCP        22.22.2.108 closed        0         0       0
```

The following is sample output from the **show bstun** command specifying poll address C2:

```
Router# show bstun address C2

This peer: 22.22.1.107
  Serial4  (group 3 [bsc])
route  transport  address     state     rx_pkts   tx_pkts   drops
C2     TCP        22.22.2.108 closed        0         0       0

  Serial5  (group 50 [bsc])
route  transport  address     state     rx_pkts   tx_pkts   drops
C2     TCP        22.22.2.108 open          4         4       0
```

Table 34 describes significant fields shown in the output.

Table 34 Show BSTUN Command Field Descriptions

Field	Description
This peer	Lists the peer name or address. The interface name (as defined by the **description** command), its BSTUN group number, and the protocol associated with the group are shown on the next header line.
route	Bisync control unit address.
transport	Description of link, either a serial interface using serial transport (indicated by IF followed by interface name), or a TCP connection to a remote router (TCP followed by IP address).
address	Address or the word *all* if the default forwarding entry is specified, followed by a repeat of the group number given for the interface.
state	State of the link: open is the normal, working state; direct indicates a direct link to another line, as specified with the **direct** keyword on the **bstun route** command.
rx_pkts	Number of received packets.
tx_pkts	Number of transmitted packets.
drops	Number of packets that had to be dropped for whatever reason.

show stun

Use the **show stun** privileged EXEC command to display the current status of STUN connections.

show stun

Syntax Description

This command has no arguments or keywords.

Command Mode

Privileged EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Sample Display

The following is sample output from the **show stun** command:

```
Router# show stun

This peer: 131.108.10.1
Serial0 -- 3174 Controller for test lab (group 1 [sdlc])
                          state   rx-pkts  tx-pkts  drops  poll
  7[ 1] IF Serial1         open     20334    86440      5  8P
 10[ 1] TCP 131.108.8.1    open      6771     7331      0
all[ 1] TCP 131.108.8.1    open    612301  2338550   1005
```

In the display, the first entry reports proxy polling is enabled for address 7 and serial 0 is running with modulus 8 on the primary side of the link. The link has received 20,334 packets, transmitted 86,440 packets, and dropped 5 packets.

Table 35 describes significant fields shown in the output.

Table 35 Show STUN Command Field Descriptions

Field	Description
This peer	Lists the peer name or address. The interface name (as defined by the **description** command), its STUN group number, and the protocol associated with the group are shown on the header line.
STUN address	Address or the word *all* if the default forwarding entry is specified, followed by a repeat of the group number given for the interface.
Type of link	Description of link, either a serial interface using serial transport (indicated by IF followed by interface name), or a TCP connection to a remote router (TCP followed by IP address).
state	State of the link: open is the normal, working state; direct indicates a direct link to another line, as specified with the **direct** keyword on the **stun route** command.
rx_pkts	Number of received packets.
tx_pkts	Number of transmitted packets.

Table 35 Show STUN Command Field Descriptions (Continued)

Field	Description
drops	Number of packets that for whatever reason had to be dropped.
poll	Report of the proxy poll parameters, if any. P indicates a primary and S indicates a secondary node. The number before the letter is the modulus of the link.

stun group

Use the **stun group** interface configuration command to place each STUN-enabled interface on a router in a previously defined STUN group. Use the **no** form of this command to remove an interface from a group.

stun group *group-number*
no stun group *group-number*

Syntax Description

group-number	Integer in the range 1 to 255.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Before using this command, complete the following steps:

Step 1 Enable STUN on a global basis with the **stun peer-name** command.

Step 2 Define the protocol group in which you want to place this interface with the **stun protocol-group** command.

Step 3 Enable STUN on the interface using the **encapsulation stun** command.

Packets only travel between STUN-enabled interfaces that are in the same group. Once a given serial link is configured for the STUN function, it is no longer a shared multiprotocol link. All traffic that arrives on the link is transported to the corresponding peer as determined by the current STUN configuration.

Example

The following example places serial interface 0 in STUN group 2, which is defined to run the SDLC transport:

```
! sample stun peer-name global command
stun peer-name 131.108.254.6
! sample protocol-group command telling group 2 to use the SDLC protocol
stun protocol-group 2 sdlc
!
interface serial 0
! sample ip address subcommand
 no ip address
! sample encapsulation stun subcommand
 encapsulation stun
! place interface serial0 in previously defined STUN group 2
 stun group 2
! enter stun route command
 stun route 7 tcp 131.108.254.7
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

encapsulation stun
priority-list stun address
stun peer-name
stun protocol-group

stun keepalive-count

Use the **stun keepalive-count** global configuration command to define the number of times to attempt a peer connection before declaring the peer connection to be down. Use the **no** form of this command to cancel the definition.

stun keepalive-count *count*
no stun keepalive-count

Syntax Description

count	Number of connection attempts. The range is between 2 and 10 retries.

Default

No default is specified.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

The following example sets the number of times to retry a connection to a peer to 4:

```
stun keepalive-count 4
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

stun remote-peer-keepalive

stun peer-name

Use the **stun peer-name** global configuration command to enable STUN for an IP address. Use the **no** form of this command to disable STUN for an IP address.

stun peer-name *ip-address* **cls**
no stun peer-name *ip-address* **cls**

Syntax Description

ip-address	IP address by which this STUN peer is known to other STUN peers.

Default

STUN is disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Use this command to enable any further STUN features. After using this command, complete the following steps:

Step 1 Define the protocol group in which you want to place this interface with the **stun protocol-group** command.

Step 2 Enable STUN on the interface using the **encapsulation stun** command.

Step 3 Place the interface in a STUN group with the **stun group** command.

Example

The following example assigns IP address 131.108.254.6 as the STUN peer:

```
stun peer-name 131.108.254.6 cls
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

encapsulation stun
stun group
stun protocol-group

stun protocol-group

Use the **stun protocol-group** global configuration command to create a protocol group. Use the **no** form of this command to remove an interface from the group.

stun protocol-group *group-number* {**basic** | **sdlc** [**sdlc-tg**] | **schema**}
no stun protocol-group

Syntax Description

group-number	Integer in the range 1 to 255.
basic	Indicates a non-SDLC protocol.
sdlc	Indicates an SDLC protocol.
sdlc-tg	(Optional) Identifies the group as part of an SNA transmission group.
schema	Indicates a custom protocol.

Default

No protocol group established.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Use the **sdlc** keyword to specify an SDLC protocol. You must specify either the **sdlc** or the **sdlc-tg** keyword before you can enable SDLC local acknowledgment. SDLC local acknowledgment is established with the **stun route address tcp** command.

Use the **basic** keyword to specify a non-SDLC protocol, such as HDLC.

Use the **schema** keyword to specify a custom protocol. The custom protocol must have been previously created with the **stun schema** command.

Use the optional **sdlc-tg** keyword, in conjunction with the **sdlc** keyword, to establish an SNA transmission group. A transmission group is a set of protocol groups providing parallel links to the same pair of IBM establishment controllers. This provides redundancy of paths. In case one or more links go down, an alternate path will be used. All STUN connections in a transmission group must connect to the same IP address. SDLC local acknowledgment must be enabled.

Note If you specify the keyword **sdlc** in the **stun protocol group** command string, you cannot specify the **stun route all** command on that interface.

Examples

The following example specifies that group 7 will use the SDLC STUN protocol to route frames within that group:

```
stun protocol-group 7 sdlc
```

The following example specifies that group 5 use the basic protocol, wherein the serial addressing is unimportant and you have a point-to-point link:

```
stun protocol-group 5 basic
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

encapsulation stun
stun route address interface serial
stun route address tcp
stun schema offset length format

stun quick-response

Use the **stun quick-response** global configuration command to enable STUN quick-response, which can be used with local acknowledgment. Use the **no** form of this command to disable STUN quick-response.

stun quick-response
no stun quick-response

Syntax Description

This command has no arguments or keywords.

Default

STUN quick-response is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3(5).

This command is used with local acknowledgment (local ack).

When STUN quick-response is enabled, the router responds to an exchange identification (XID) or a Set Normal Response Mode (SNRM) request with a Disconnect Mode (DM) response when the device is not in the CONNECT state. The request is then passed to the remote router and, if the device responds, the reply is cached. The next time the device is sent an XID or SNRM, the router replies with the cached DM response.

Note Using STUN quick-response avoids an AS/400 line reset problem by eliminating the Non-Productive Receive Timer (NPR) expiration in the AS/400. With quick-response enabled, the AS/400 receives a response from the polled device, even when the device is down. If the device does not respond to the forwarded request, the router continues to respond with the cached DM response.

Example

The following example enables STUN quick-response:

```
stun quick-response
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

stun route address interface dlci
stun route address interface serial
stun route address tcp
stun route all interface serial
stun route all tcp

stun remote-peer-keepalive

Use the **stun remote-peer-keepalive** global configuration command to enable detection of the loss of a peer. Use the **no** form of this command to disable detection.

stun remote-peer-keepalive *seconds*
no stun remote-peer-keepalive

Syntax Description

seconds	Keepalive interval, in seconds. The range is 1 to 300 seconds. The default is 30 seconds.

Default

30 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

In the following example, the remote-peer-keepalive interval is set to 60 seconds:

```
stun remote-peer-keepalive 60
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

stun keepalive-count

stun route address interface dlci

Use the **stun route address interface dlci** interface configuration command to configure direct Frame Relay encapsulation between STUN peers with SDLC local acknowledgment. Use the **no** form of this command to disable the configuration.

stun route address *sdlc-addr* **interface** *frame-relay-port* **dlci** *number localsap* **local-ack cls**
no stun route address *sdlc-addr* **interface** *frame-relay-port* **dlci** *number localsap* **local-ack cls**

Syntax Description

sdlc-addr	Address of the serial interface.
frame-relay-port	Port number.
number	Data-link connection identifier (DLCI) number.
localsap	Local connecting SAP.
local-ack	Enable local acknowledgment.
cls	Use Cisco Link Services (CLS) to access the frame relay network.

Default

The configuration is disabled.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following command enables Frame Relay encapsulation between STUN peers with SDLC local acknowledgment:

```
stun route address c1 interface serial1 dlci 22 04 local-ack
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

stun route all interface serial

stun route address interface serial

Use the **stun route address interface serial** interface configuration command to forward all HDLC traffic on a serial interface. Use the **no** form of this command to disable this method of HDLC encapsulation.

stun route address *address-number* **interface serial** *number* [**direct**]
no stun route address *address-number* **interface serial** *number*

Syntax Description

address-number	Address of the serial interface.
number	Number assigned to the serial interface.
direct	(Optional) Forwards all HDLC traffic on a direct STUN link.

Default

The configuration is disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Examples

In the following example, serial frames with a STUN route address of 4 are forwarded through serial interface 0 using HDLC encapsulation:

```
stun route address 4 interface serial 0
```

In the following example, serial frames with STUN route address 4 are propagated through serial interface 0 using STUN encapsulation:

```
stun route address 4 interface serial 0 direct
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

stun route all interface serial

stun route address tcp

Use the **stun route address tcp** interface configuration command to specify TCP encapsulation and optionally establish SDLC local acknowledgment (SDLC transport) for STUN. Use the **no** form of this command to disable this method of TCP encapsulation.

stun route address *address-number* **tcp** *ip-address* [**local-ack**] [**priority**] [**tcp-queue-max**]
no stun route address *address-number* **tcp** *ip-address* [**local-ack**] [**priority**][**tcp-queue-max**]

Syntax Description

address-number	Number that conforms to SDLC addressing conventions.
ip-address	IP address by which this STUN peer is known to other STUN peers that are using the TCP as the STUN encapsulation.
local-ack	(Optional) Enables local acknowledgment for STUN.
priority	(Optional) Establishes the four levels used in priority queuing: low, medium, normal, and high.
tcp-queue-max	(Optional) Sets the maximum size of the outbound TCP queue for the SDLC link.

Defaults

TCP encapsulation is not established; TCP queue size default is 100.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **tcp-queue-max** keyword first appeared in Cisco IOS Release 11.1.

SDLC transport participates in SDLC windowing and retransmission through support of local acknowledgment. SDLC sessions require that end nodes send acknowledgments for a set amount of data frames received before allowing further data to be transmitted. Local acknowledgment provides local termination of the SDLC session, so that control frames no longer travel the WAN backbone networks. This means end nodes do not time out, and a loss of sessions does not occur.

Example

In the following example, a frame with a source-route address of 10 is propagated using TCP encapsulation to a device with an IP address of 131.108.8.1:

```
stun route address 10 tcp 131.108.8.1
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

sdlc address ff ack-mode
stun route all tcp

stun route all interface serial

Use the **stun route all interface serial** interface configuration command to encapsulate and forward all STUN traffic using HDLC encapsulation on a serial interface.

stun route all interface serial *number* [**direct**]

Syntax Description

number	Number assigned to the serial interface.
direct	(Optional) Indicates that the specified interface is also a direct STUN link, rather than a serial connection to another peer.

Default

No default is specified.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

An appropriately configured router must exist on the other end of the designated serial line. The outgoing serial link still can be used for other kinds of traffic (the frame is not TCP encapsulated). This mode is used when TCP/IP encapsulation is not needed or when higher performance is required. Enter the serial line number connected to the router for the *interface-number* argument.

Examples

In the following example, all traffic on serial interface 0 is propagated using STUN encapsulation:

```
stun route all interface serial 0
```

In the following example, serial interface 1 is a direct STUN link, not a serial connection to another peer:

```
stun route all interface serial 1 direct
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

stun route address interface serial

stun route all tcp

Use the **stun route all tcp** interface configuration command with TCP encapsulation to forward all STUN traffic on an interface regardless of what address is contained in the serial frame.

stun route all tcp *ip-address*

Syntax Description

ip-address	IP address by which this remote STUN peer is known to other STUN peers. Use the address that identifies the remote STUN peer that is connected to the far serial link.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

TCP/IP encapsulation allows movement of serial frames across arbitrary media types and topologies. This is particularly useful for building shared, multiprotocol enterprise network backbones.

Example

In the following example, all STUN traffic received will be propagated through the bridge:

```
stun route all tcp 131.108.10.1
```

stun schema offset length format

Use the **stun schema offset length format** global configuration command to define a protocol other than SDLC for use with STUN. Use the **no** form of this command to disable the new protocol.

stun schema *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*
no stun schema *name* **offset** *constant-offset* **length** *address-length* **format** *format-keyword*

Syntax Description

name	Name that defines your protocol. It can be up to 20 characters in length.
constant-offset	Constant offset, in bytes, for the address to be found in the frame.
address-length	Length in one of the following formats: decimal (4 bytes), hexadecimal (8 bytes), or octal (4 bytes).
format-keyword	Format to be used to specify and display addresses for routes on interfaces that use this STUN protocol. The allowable format keywords are **decimal** (0 to 9), **hexadecimal** (0 to F), and **octal** (0 to 7).

Default

No protocol is defined.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Use this command before defining the protocol group (**stun protocol-group** command). The serial protocol you define must meet the following criteria:

- The protocol uses full-duplex conventions (RTS/CTS always high).
- The protocol uses standard HDLC checksum and framing (beginning and end of frames, data between frames).
- Addresses are contained in a constant location (offset) within the frame.
- Addresses are found on a byte boundary.

Example

In the following example, a protocol named *new-sdlc* is created. In the protocol frame structure, the constant offset is 0, the address length is 1 byte, and the address format is hexadecimal:

```
stun schema new-sdlc offset 0 length 1 format hexadecimal
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

priority-list stun
stun protocol-group

stun sdlc-role primary

Use the **stun sdlc-role primary** interface configuration command to assign the router the role of SDLC primary node. Primary nodes poll secondary nodes in a predetermined order.

stun sdlc-role primary

Syntax Description

This command has no arguments or keywords.

Default

No role is assigned.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If the router is connected to a cluster controller, for example a 3x74, it should appear as a front-end processor such as a 37x5, and must be assigned the role of a primary node.

Example

The following example assigns the router the role of SDLC primary node:

```
stun sdlc-role primary
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

encapsulation stun
stun sdlc-role secondary

stun sdlc-role secondary

Use the **stun sdlc-role secondary** interface configuration command to assign the router the role of SDLC secondary node. Secondary nodes respond to polls sent by the SDLC primary by transmitting any outgoing data they may have.

stun sdlc-role secondary

Syntax Description

This command has no arguments or keywords.

Default

No secondary role is assigned.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If the router is connected to a front-end processor, for example a 37x5, it should appear as a cluster controller such as a 3x74, and must be assigned the role of a secondary node.

Example

The following example assigns the router the role of SDLC secondary node:

```
stun sdlc-role secondary
```

Related Commands

You can use the master indexes or search online for documentation of related commands.

encapsulation stun
stun sdlc-role primary