CHAPTER 22

STUN and SDLC Local Acknowledgment Commands

Cisco's serial tunneling (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 pass-through of all SDLC traffic (including control frames, such as Receiver Ready) end-to-end between Synchronous Network Architecture (SNA) devices.

Cisco's SDLC Transport, or 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, routers must first be enabled for STUN and 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.

Use the commands in this chapter to configure STUN and SDLC Local Acknowledgment networks. For STUN configuration information and examples, refer to the "Configuring STUN and SDLC Local Acknowledgment" chapter of the *Router Products Configuration Guide*.

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

None

Command Mode

Interface configuration

Usage Guidelines

You must 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 interface serial 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

stun group
stun peer-name
stun protocol-group

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

Syntax Description

list	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

None

Command Mode

Interface configuration

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:

```
! sample stun peer-name global command
stun peer-name 131.108.254.6
! sample protocol-group command telling group 1 to use SDLC
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 4 interface serial 0 direct
! assign priority group 1 to interface serial 0
priority-group 1
! assign a high priority to priority list 1 on serial link identified
! by group 1 and address C1
priority-list 1 stun high address 1 C1
```

Related Command

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*
no priority-group *list*

Syntax Description

list	Priority list number assigned to the interface.

Default

None

Command Mode

Interface configuration

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 list** 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

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

priority-list ip tcp

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

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

Syntax Description

list	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
queue-keyword	Priority queue type: high, medium, normal, or low.
tcp-port-number	STUN port and priority settings are as follows: high (1994), medium (1990), normal (1991), and low (1992).

Default

Normal queue

Command Mode

Global configuration

Usage Guidelines

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.

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 the SDLC port (1994).

```
!
priority list 1 stun high address 1 C1
priority list 1 ip high tcp 1994
!
```

Related Commands

priority group
priority-list stun address

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

Syntax Description

list	Arbitrary integer between 1 and 10 that identifies the priority list selected by the user.
queue-keyword	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

Normal queue

Command Mode

Global configuration

Usage Guidelines

Note SDLC Local Acknowledgment with the priority option must be enabled using the **stun route address serial** command.

The **priority-list** command is described in greater detail in Chapter 5.

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

priority-list ip tcp
stun group
stun schema offset length format

show stun

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

show stun

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

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 enabled for address 7 and that 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 1-1 describes significant fields shown in the output.

Table 1-1 Show STUN 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 (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.
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.

show stun sdlc

Use the **show stun sdlc** EXEC command to display the status of the STUN interfaces using SDLC encapsulation and whether proxy polling is enabled for that interface.

show stun sdlc

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Usage Guidelines

Interfaces with proxy polling enabled are noted with the address followed by an indication of node type.

Sample Display

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

```
router# show stun sdlc

Serial 1 -- 3174 controller
B3: s2 C1: p4 DE: d6
```

The display shows that Serial 1 has three addresses for which proxy polling is enabled. These are B3, for which this end is a secondary link in state 2, and C1, for which this end is a primary link in state 4. Finally, DE is in the primary/secondary/modulus discovery state 6.

Table 1-2 describes significant fields shown in the output.

Table 1-2 Show STUN SDLC Field Descriptions

Field	Description
Serial 1	Name of interface for which STUN is enabled.

Field	Description
3174 controller	IBM device with which this interface communicates.
B3:	First address for which proxy polling is enabled: secondary link in state 2.
s2	First character (s) indicates the node type. Possible values include: • s—secondary • p—primary • d—discovery Second character (2) indicates the node state. Possible values include: • 0—Significant data traveling between the primary and secondary node. No proxy polling occurring. • 1 through 3—Proxy polling in process of being initiated. • 4—Proxy polling is activated for the link at this time. If this is the primary node, the router responds to the primary's poll. If this is the secondary node, the router will periodically generate polls for potential response by the secondary. • 5—The primary router has data from the secondary to send to the primary SDLC machine, but is waiting for a poll from that machine before transmitting the data. • 6 through 7—This router is still trying to determine the primary/secondary character and modulus of the SDLC hosts attached to it. No proxying is done in these states

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 through 255.

Default

None

Command Mode

Interface configuration

Usage Guidelines

Before using this command, complete the following steps: 1) enable STUN on a global basis with the **stun peer-name** command, 2) define the protocol group in which you want to place this interface with the **stun protocol-group** command, and 3) enable STUN on the interface using the **encapsulation stun** command.

Packets will 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 will be 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

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

stun peer-name

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

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

Syntax Description

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

Default

None

Command Mode

Global configuration

Usage Guidelines

You must 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
!
```

Related Commands

encapsulation stun
stun group
stun protocol-group

stun poll-interval

Use the **stun poll-interval** interface configuration command to set the interval between each sequence of proxy polls. Use the **no** form of this command to return to the default of 100 milliseconds.

stun poll-interval *millisecond*s
no stun poll-interval

Syntax Description

milliseconds	An integer. It must be at least 50.

Default

100 milliseconds

Command Mode

Interface configuration

Usage Guidelines

The proxy polling feature is provided for compatibility with Software Release 9.0 or earlier. Proxy polling alleviates loads across the network by allowing the routers to act as proxies for the primary and secondary nodes. This keeps polling traffic off of the shared links.

Note The functions provided by proxy polling have been enhanced and superseded by the SDLC Transport with TCP/IP encapsulation and Local Acknowledgment features. Use of proxy polling is not recommended.

Example

The following example sets the proxy poll interval to 50 milliseconds:

```
!
stun poll-interval 50
!
```

Related Commands

stun primary-pass through
stun proxy-poll address discovery
stun proxy-poll modulus

stun primary-pass through

Use the **stun primary-pass through** global configuration command to change the amount of time the router waits to pass through a poll from a primary SDLC device to a secondary SDLC device. To return to the default value, use the **no** form of this command.

stun primary-pass through *seconds*
no stun primary-pass through

Syntax Description

seconds	Number of seconds between each pass-through of polls.

Default

20 seconds

Command Mode

Global configuration

Usage Guidelines

Periodically, even when proxy polling is enabled, the router on the primary side of an SDLC connection will pass through a poll from the primary SDLC device through the network to the secondary SDLC device. This action causes the secondary device's reply to also traverse the entire network. This periodic pass-through provides an insurance mechanism that makes sure the primary SDLC device maintains an accurate notion of the secondary SDLC device status. The proxy polling feature is provided for compatibility with Software Release 9.0 or earlier. Proxy polling alleviates loads across the network by allowing the routers to act as proxies for the primary and secondary nodes. This keeps polling traffic off of the shared links.

Note The functions provided by proxy polling have been enhanced and superseded by the SDLC Transport with TCP/IP encapsulation and Local Acknowledgment features. Use of proxy polling is not recommended.

Example

The following example changes the amount of time the router waits to pass through a poll to 30 seconds:

```
!
stun primary-pass-through 30
!
```

Related Commands

stun poll-interval
stun proxy-poll

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**]
no stun protocol-group

Syntax Description

group-number	Integer in the range 1 through 255.
basic | **sdlc**	Basic indicates a non-SDLC protocol. SDLC indicates an SDLC group.
sdlc-tg	(Optional.) Identifies the group as part of an SNA Transmission Group.

Default

None

Command Mode

Global configuration

Usage Guidelines

You must use the **sdlc** keyword with this command before you can enable SDLC Local Acknowledgment. SDLC Local Acknowledgment is established with the **stun route address tcp** command.

Use the **basic** keyword when selecting a non-SDLC protocol, such as HDLC, or another protocol you may have defined 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 You cannot use the **stun protocol-group** command in conjunction with the **stun route all** command.

Examples

The following example specifies that group 7 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

encapsulation stun
stun route address tcp
stun route address interface serial
stun schema

stun proxy-poll address discovery

Use the **stun proxy-poll address discovery** interface configuration command to allow the router to discover primary and secondary nodes on the network. Use the **no** form of this command to disable this method of proxy polling.

stun proxy-poll address *address* **discovery**
no stun proxy-poll address *address* **discovery**

Syntax Description

address	Address of the device on which to enable proxy polling.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

Use of the **discovery** keyword is not recommended except where you cannot avoid end hosts that negotiate the status, because proxying will be disabled on the link until session start-up, when the appropriate primary and secondary status, as well as modulus on the link, can be discovered. Until this time, all polls travel through the network.

The proxy polling feature is provided for compatibility with Software Release 9.0 or earlier. Proxy polling alleviates loads across the network by allowing the routers to act as proxies for the primary and secondary nodes. This keeps polling traffic off of the shared links.

Note The functions provided by proxy polling have been enhanced and superseded by the SDLC Transport with TCP/IP encapsulation and Local Acknowledgment features. Use of proxy polling is not recommended.

Example

The following example enables proxy polling for a secondary device at address C1 on interface serial 0 running with modulus 8:

```
! sample stun peer-name global command
stun peer-name 131.108.254.6
! sample protocol-group command for reference
stun protocol-group 4 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 4
stun group 4
! provide stun route subcommand
stun route address 4 interface serial0 direct
!
! enable proxy polling
stun proxy-poll address C1 modulus 8 secondary
```

Related Commands

stun poll-interval
stun primary-pass through
stun proxy-poll address modulus

stun proxy-poll address modulus

Use the **stun proxy-poll address modulus** interface configuration command to alleviate loads across the network by allowing the routers to act as proxies for the primary and secondary nodes. Use the **no** form of this command to disable proxy polling.

stun proxy-poll address *address* **modulus** *modulus* {**primary** | **secondary**}
no stun proxy-poll address *address* **modulus** *modulus* {**primary** | **secondary**}

Syntax Description

address	Address of the device on which to enable proxy polling.
modulus	Modulus of the link as defined by the MODULUS parameter specified in the line descriptions on the SDLC host.
primary | **secondary**	Used with the **modulus** keyword to identify the router as a primary or secondary SDLC device.

Default

Proxy polling is disabled

Command Mode

Interface configuration

Usage Guidelines

Use of the **discovery** keyword is not recommended except where you cannot avoid end hosts that negotiate the status, because proxying will be disabled on the link until session start-up, when the appropriate primary and secondary status, as well as modulus on the link, can be discovered. Until this time, all polls travel through the network.

The proxy polling feature is provided for compatibility with Software Release 9.0 or earlier. Proxy polling alleviates loads across the network by allowing the routers to act as proxies for the primary and secondary nodes. This keeps polling traffic off of the shared links.

Note The functions provided by proxy polling have been enhanced and superseded by the SDLC Transport with TCP/IP encapsulation and Local Acknowledgment features. Use of proxy polling is not recommended.

Example

The following example enables proxy polling for address C1 for a secondary SDLC device at address C1:

```
!
stun proxy-poll address C1 modulus 8 secondary
!
```

Related Commands

stun poll-interval
stun primary-pass through
stun proxy-poll address discovery

stun route address interface serial

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

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

Syntax Description

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

Default

Disabled

Command Mode

Global configuration

Example

In the following example, serial frames with a stun-route address of 4 are forwarded through serial0 using HDLC encapsulation:

```
!
stun route address 4 interface serial0
!
```

In the following example, serial frames with stun-route address 4 are propagated through serial0 using STUN encapsulation:

```
!
stun route address 4 interface serial0 direct
!
```

Related Command

stun route all interface serial

stun route address tcp

Use the **stun route address tcp** global 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**]
no stun route address *address*-number **tcp** *ip-address* [**local-ack**] [**priority**]

Syntax Description

address-number	Number that conforms to TCP addressing conventions.
tcp	Specifies TCP encapsulation.
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.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

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 Command

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 *interface-number* **[direct]**

Syntax Description

interface-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

None

Command Mode

Interface configuration

Usage Guidelines

There must be an appropriately configured router 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.

Example

In the following example, all traffic on serial0 is propagated using STUN encapsulation:

```
!
! propagate serial frames through serial0 using STUN encapsulation
stun route all interface serial0
!
```

In the following example, serial1 is a direct STUN link, not a serial connection to another peer:

```
!
stun route all interface serial1 direct
!
```

Related Command

stun route address interface serial

stun route all tcp

Use the **stun route all tcp** interface configuration command to use TCP encapsulation and 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

None

Command Mode

Interface configuration

Usage Guidelines

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 on the input side of interface serial 0 will be propagated through the bridge:

```
! 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
! 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
! STUN traffic received through serial0 from SDLC address C2
! will be propagated to a device with IP address 131.108.10.1
stun route address C2 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	One of the following address formats and lengths: decimal base 10 (4 bytes), hexadecimal base 16 (8 bytes), or octal base 8 (4 bytes).
format-keyword	Format to be used to specify and display addresses for routes on interfaces that use this STUN protocol. The allowable formats are base 10 addresses (0 through 9), base 16 addresses (0 through F), and base 8 addresses (0 through 7).

Default

None

Command Mode

Global configuration

Usage Guidelines

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/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

A dagger (†) indicates that the command is documented in another chapter.

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

None

Command Mode

Interface configuration

Usage Guidelines

If the router is connected to a cluster controller, for example 3x74, the router should appear as a Front-End Processor (FEP) such as a 37x5, and must be assigned the role of a primary node.

Example

```
interface serial 0
encapsulation stun
stun group 50
stun sdlc-role primary
!
```

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

None

Command Mode

Interface configuration

Usage Guidelines

If the router is connected to a Front-End Processor (FEP) for example 37x5, the router should appear as a cluster controller such as a 3x74, and must be assigned the role of a secondary node.

Example

```
interface serial 0
encapsulation stun
stun group 50
stun sdlc-role secondary
!
```

Related Commands

encapsulation stun
stun sdlc-role primary