

Configuring STUN and BSTUN

Cisco's serial tunnel (STUN) implementation allows Synchronous Data Link Control (SDLC) devices and High-Level Data Link Control (HDLC) devices to connect to one another through a multiprotocol internetwork.

Our block serial tunnel (BSTUN) implementation enhances Cisco 2500 series, Cisco 4000 series, and Cisco 4500 series routers to support devices that use the Binary Synchronous Communication (BSC) data link protocol.

This chapter describes both STUN and BSTUN configurations. The first part of the chapter, beginning with the section "Cisco's Implementation of Serial Tunneling," describes the STUN features and lists the tasks you must perform to configure a STUN network in either passthrough or local acknowledgment mode. The last part of the chapter, beginning with the section "Cisco's Implementation of Block Serial Tunneling (BSTUN)," describes the BSTUN features, and lists the tasks you must perform to configure a BSC network in either passthrough or local acknowledgment mode.

For a complete description of the commands mentioned in this chapter, refer to the "STUN and BSTUN Commands" chapter in the *Router Products Command Reference* publication.

Cisco's Implementation of Serial Tunneling

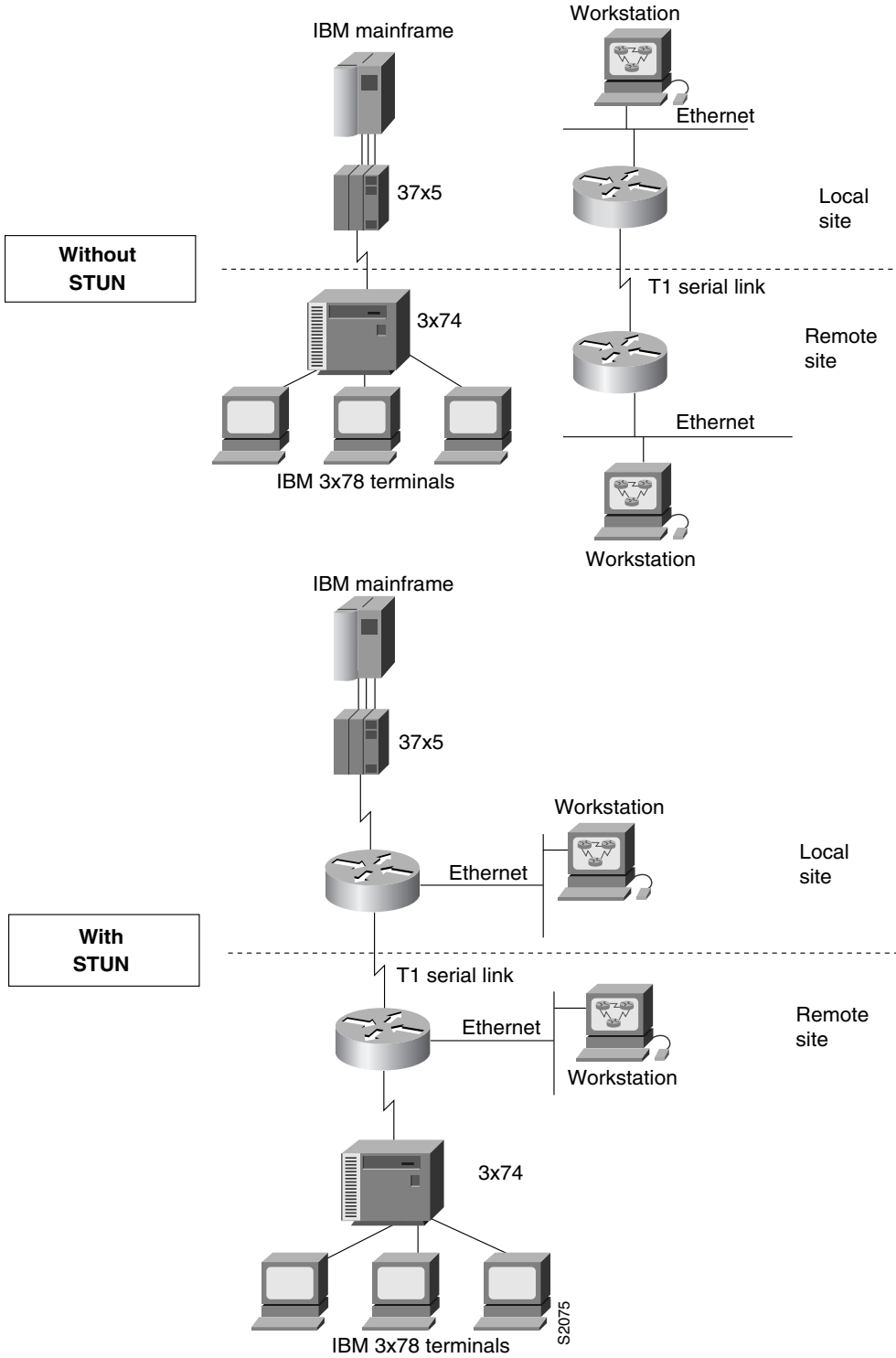
Our STUN implementation provides the following features:

- Encapsulates SDLC frames in either the Transmission Control Protocol/Internet Protocol (TCP/IP) or the HDLC protocol.
- Allows two devices using SDLC- or HDLC-compliant protocols that are normally connected by a direct serial link to be connected through one or more Cisco routers, reducing leased-line costs.

When you replace direct serial links with routers, serial frames can be propagated over arbitrary media and topologies to another router with a STUN link to an appropriate end point. The intervening network is not restricted to STUN traffic, but rather, is multiprotocol. For example, instead of running parallel backbones for DECnet and SNA/SDLC traffic, this traffic now can be integrated into an enterprise backbone network.

- Supports local acknowledgment for direct Frame Relay connectivity between routers, without TCP/IP required.
- Allows networks with IBM mainframes and communications controllers to share data using Cisco routers and existing network links. As an SDLC function, STUN fully supports the IBM Systems Network Architecture (SNA), and allows IBM SDLC frames to be transmitted across the network media and and/or shared serial links. Figure 27-1 illustrates a typical network configuration with and without STUN.
- Encapsulates SDLC frame traffic packets and routes them over any of the supported network media—serial, Fiber Distributed Data Interface (FDDI), Ethernet, and Token Ring, X.25, Switched Multimegabit Data Service (SMDS), and T1/T3—using TCP/IP encapsulation. Because TCP/IP encapsulation is used, you can use any of the Cisco routing protocols to route the packets.
- Copies frames to destinations based on address. STUN in passthrough mode does not modify the frames in any way or participate in SDLC windowing or retransmission; these functions are left to the communicating hosts. However, STUN in local acknowledgment mode does participate in SDLC windowing and retransmission through local termination of the SDLC session.
- Ensures reliable data transmission across serial media having minimal or predictable time delays. With the advent of STUN and wide-area network (WAN) backbones, serial links now can be separated by wide, geographic distances spanning countries and continents. As a result, these serial links have time delays that are longer than SDLC allows for bidirectional communication between hosts. The STUN local acknowledgment feature addresses the problems of unpredictable time delays, multiple retransmissions, or loss of sessions.
- Allows for configuration of redundant links to provide transport paths in the event part of the network goes down.

Figure 27-1 IBM Network Configuration with and without STUN



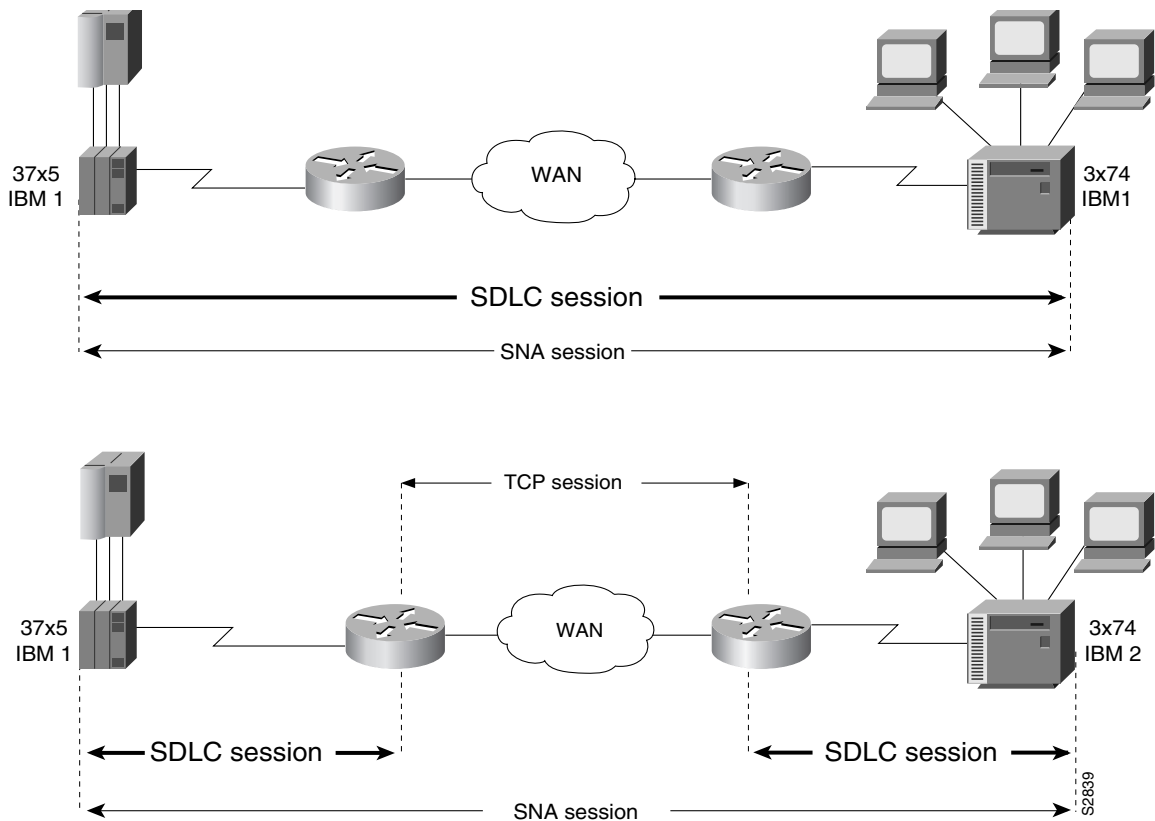
The STUN Network

STUN operates in two modes: passthrough and local acknowledgment. Figure 27-2 shows the difference between passthrough mode and local acknowledgment mode.

The upper half of Figure 27-2 shows STUN configured in passthrough mode. In passthrough mode, the routers act as a wire and the SDLC session remains between the end stations. In this mode, STUN provides a straight pass-through of all SDLC traffic, including control frames.

The lower half of Figure 27-2 shows STUN configured in local acknowledgment mode. In local acknowledgment mode, the routers terminate the SDLC sessions and send only data across the WAN. Control frames no longer travel the WAN backbone networks.

Figure 27-2 Comparison of STUN in Passthrough Mode and Local Acknowledgment Mode



Note To enable STUN local acknowledgment, you first enable routers for STUN and configure them to appear on the network as primary or secondary SDLC nodes. TCP/IP encapsulation must be enabled. Our STUN local acknowledgment feature also provides priority queuing for TCP-encapsulated frames.

STUN Configuration Task List

To configure and monitor STUN, or STUN Local Acknowledgment, complete the tasks in the following sections:

- Enable STUN
- Enable STUN Quick-Response
- Configure SDLC Broadcast
- Specify a STUN Protocol Group
- Enable STUN Interfaces and Place Them in STUN Group
- Establish the Frame Encapsulation Method
- Configure STUN with Multilink Transmission Groups
- Set Up STUN Traffic Priorities
- Monitor STUN Network Activity

The “STUN Configuration Examples” section follows these configuration tasks.

Enable STUN

To enable STUN perform the following task in global configuration mode:

Task	Command
Enable STUN for a particular IP address.	<code>stun peer-name ip-address</code>

When configuring redundant links, ensure that the STUN peer names you choose on each router are the IP addresses of the most stable interfaces on each router, such as a loopback or Ethernet interface. See “STUN Configuration Examples” later in this chapter.

Enable STUN Quick-Response

You can enable STUN quick-response, which improves network performance when used with local acknowledgment. When STUN quick-response is used with local acknowledgment, 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 STUN 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.

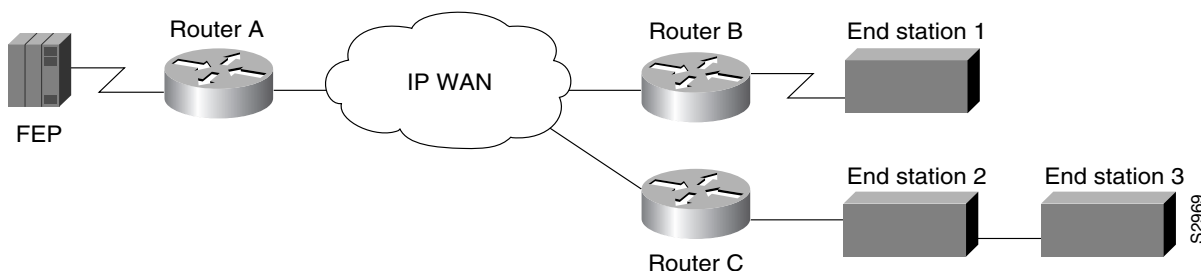
To enable STUN quick-response, perform the following task in global configuration mode:

Task	Command
Enable STUN quick-response.	stun quick-response

Configure SDLC Broadcast

The SDLC broadcast feature allows SDLC broadcast address FF to be replicated for each of the STUN peers, so each of the end stations receives the broadcast frame. For example, in Figure 27-3, the FEP views the end stations 1, 2 and 3 as if they are on an SDLC multidrop link. Any broadcast frame sent from FEP to Router A is duplicated and sent to each of the downstream routers (B and C).

Figure 27-3 SDLC Broadcast across Virtual Multidrop Lines



To enable SDLC broadcast, perform the following task in interface configuration mode:

Task	Command
Enable SDLC broadcast.	sdlc virtual-multidrop

Only enable SDLC broadcast on the router that is configured to be the secondary station on the SDLC link (Router A in Figure 27-3).

You must also configure SDLC address FF on Router A for each of the STUN peers. To do so, perform the following task in interface configuration mode:

Task	Command
Configure SDLC address FF on Router A for each STUN peer.	stun route address address-number tcp ip-address [local-ack] [priority] [tcp-queue-max]

Specify a STUN Protocol Group

Place each STUN interface in a group that defines the ISO 3309-compliant framed protocol running on that link. Packets will only travel between STUN interfaces that are in the same protocol group.

There are three predefined STUN protocols:

- Basic
- SDLC
- SDLC transmission group

You also can specify a custom STUN protocol.

You must specify either the SDLC protocol or the SDLC transmission group protocol if you want to use the STUN Local Acknowledgment feature.

Note Before you can specify a custom protocol, you must first define the protocol; see the section “Create and Specify a Custom STUN Protocol” later in this chapter for the procedure.

Specify a Basic STUN Group

The basic STUN protocol is not dependent on the details of serial protocol addressing and is used when addressing is unimportant. Use this when your goal is to replace one or more sets of point-to-point (not multidrop) serial links by using a protocol other than SDLC. Perform the following task in global configuration mode:

Task	Command
Specify a basic protocol group and assign a group number.	stun protocol-group <i>group-number</i> basic

Specify an SDLC Group

You can specify SDLC protocol groups to associate interfaces with the SDLC protocol. Use the SDLC STUN protocol to place the routers in the midst of either point-to-point or multipoint (multidrop) SDLC links. To define an SDLC protocol group, perform the following task in global configuration mode:

Task	Command
Specify an SDLC protocol group and assign a group number.	stun protocol-group <i>group-number</i> sdlc

If you specify an SDLC protocol group, you cannot specify the **stun route all** command on any interface of that group.

For an example of how to configure an SDLC protocol group, see the “Configuring Serial Link Address Prioritization Using STUN TCP/IP Encapsulation Example” later in this chapter.

Specify an SDLC Transmission Group

An SNA transmission group is a set of lines providing parallel links to the same pair of SNA front-end-processor (FEP) devices. This provides redundancy of paths for fault tolerance and load sharing. To define an SDLC transmission group, perform the following task in global configuration mode:

Task	Command
Specify an SDLC protocol group, assign a group number, and create an SNA transmission group.	stun protocol-group <i>group-number</i> sdlc-tg

All STUN connections in a transmission group must connect to the same IP address and use the SDLC local acknowledgment feature.

Create and Specify a Custom STUN Protocol

To define a custom protocol and tie STUN groups to the new protocol, perform the following tasks in global configuration mode:

Task	Command
Step 1 Create a custom protocol.	stun schema <i>name</i> offset <i>constant-offset</i> length <i>address-length</i> format <i>format-keyword</i>
Step 2 Specify the custom protocol group and assign a group number.	stun protocol-group <i>group-number</i> schema

Enable STUN Interfaces and Place Them in STUN Group

You must enable STUN on serial interfaces and place these interfaces in the protocol groups you have defined. To enable STUN on an interface and to place the interface in a STUN group, perform the following tasks in interface configuration mode:

Task	Command
Step 1 Enable STUN function on a serial interface.	encapsulation stun
Step 2 Place the interface in a previously defined STUN group.	stun group <i>group-number</i>

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.

Establish the Frame Encapsulation Method

To allow SDLC frames to travel across a multimedia, multiprotocol network, you must encapsulate them using one of the methods in the following sections:

- Configure HDLC Encapsulation without Local Acknowledgment
- Configure TCP Encapsulation without Local Acknowledgment
- Configure TCP Encapsulation with SDLC Local Acknowledgment and Priority Queuing
- Configure Local Acknowledgment for Direct Frame Relay Connectivity between Routers

Configure HDLC Encapsulation without Local Acknowledgment

You can encapsulate SDLC or HDLC frames using the HDLC protocol. The outgoing serial link still can be used for other kinds of traffic. The frame is not TCP encapsulated. To configure HDLC encapsulation, perform one of the following tasks in interface configuration mode:

Task	Command
Forward all HDLC or SDLC traffic of the identified interface number.	stun route all interface serial <i>interface-number</i>
Forward all HDLC or SDLC traffic on a direct STUN link.	stun route all interface serial <i>interface-number</i> direct

Task	Command
Forward HDLC or SDLC traffic of the identified address.	stun route address <i>address-number</i> interface serial <i>interface-number</i>
Forward HDLC or SDLC traffic of the identified address across a direct STUN link.	stun route address <i>address-number</i> interface serial <i>interface-number</i> direct

Use the **no** forms of these commands to disable HDLC encapsulation.

Note You can only forward all traffic if you are using basic STUN protocol groups.

Configure TCP Encapsulation without Local Acknowledgment

If you do not want to use SDLC local acknowledgment and only need to forward all SDLC frames encapsulated in TCP, complete the following tasks in interface configuration mode:

Task	Command
Forward all TCP traffic for this IP address.	stun route all tcp <i>ip-address</i>
Specify TCP encapsulation.	stun route address <i>address-number</i> tcp <i>ip-address</i> [priority] [tcp-queue-max]

Use the **no** form of these commands to disable forwarding of all TCP traffic.

This configuration is typically used when the two routers can be connected via an IP network as opposed to a point-to-point link. Otherwise, always use HDLC.

Configure TCP Encapsulation with SDLC Local Acknowledgment and Priority Queuing

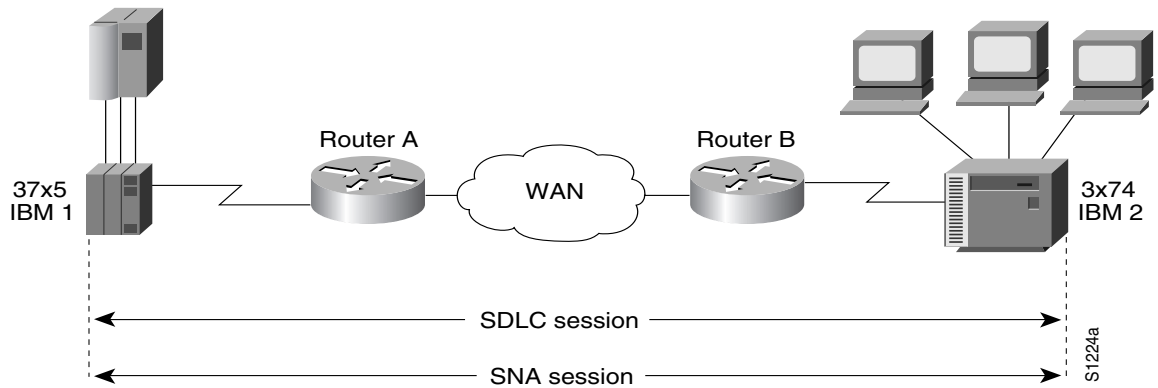
You can only configure SDLC local acknowledgment using TCP encapsulation. When you configure SDLC local acknowledgment, you also have the option to enable support for priority queuing.

Note To enable SDLC local acknowledgment, you must have specified an SDLC or SDLC transmission group.

SDLC local acknowledgment provides local termination of the SDLC session so that control frames no longer travel the WAN backbone networks. This means that time-outs are less likely to occur.

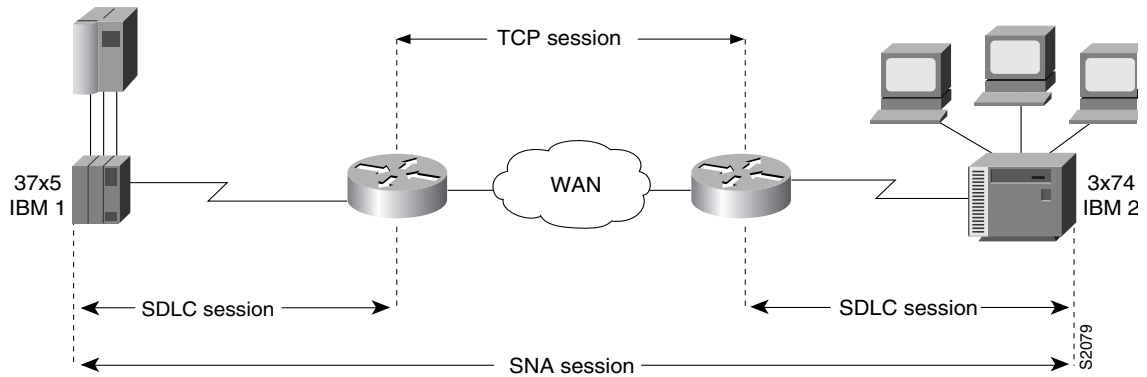
Figure 27-4 illustrates an SDLC session. IBM 1, using a serial link, can communicate with IBM 2 on a different serial link separated by a wide-area backbone network. Frames are transported between Router A and Router B using STUN. However, the SDLC session between IBM 1 and IBM 2 is still end-to-end. Every frame generated by IBM 1 traverses the backbone network to IBM 2, which, upon receipt of the frame, acknowledges it.

Figure 27-4 SDLC Session without Local Acknowledgment



With SDLC local acknowledgment, the SDLC session between the two end nodes is not end-to-end but instead terminates at the two local routers, as shown in Figure 27-5. The SDLC session with IBM 1 ends at Router A, and the SDLC session with IBM 2 ends at Router B. Both Router A and Router B execute the full SDLC protocol as part of SDLC Local Acknowledgment. Router A acknowledges frames received from IBM 1. The node IBM 1 treats the acknowledgments it receives as if they are from IBM 2. Similarly, Router B acknowledges frames received from IBM 2. The node IBM 2 treats the acknowledgments it receives as if they are from IBM 1.

Figure 27-5 SDLC Session with Local Acknowledgment



To configure TCP encapsulation with SDLC local acknowledgment and priority queuing, perform the tasks in the following sections:

- Assign the Router an SDLC Primary or Secondary Role
- Enable the SDLC Local Acknowledgment Feature
- Establish Priority Queuing Levels

Assign the Router an SDLC Primary or Secondary Role

To establish local acknowledgment, the router must play the role of an SDLC primary or secondary node. Primary nodes poll secondary nodes in a predetermined order. Secondaries then transmit if they have outgoing data.

For example, in the IBM environment, an FEP is the primary station and cluster controllers are secondary stations. If the router is connected to a cluster controller, it should appear as an FEP and must therefore be assigned the role of a primary SDLC node. If the router is connected to an FEP, it should appear as a cluster controller and must therefore be assigned the role of a secondary SDLC node. Routers connected to SDLC primary end-stations must play the role of an SDLC secondary and routers attached to SDLC secondary end stations must play the role of an SDLC primary station.

To assign the router a primary or secondary role, perform one of the following tasks in interface configuration mode:

Task	Command
Assign the STUN-enabled router an SDLC primary role.	stun sdlc-role primary
Assign the STUN-enabled router an SDLC secondary role.	stun sdlc-role secondary

Enable the SDLC Local Acknowledgment Feature

To enable SDLC local acknowledgment, complete the following task in interface configuration mode:

Task	Command
Establish SDLC local acknowledgment using TCP encapsulation.	stun route address address-number tcp ip-address [local-ack] [priority] [tcp-queue-max]

The **stun route address 1 tcp local-ack priority tcp-queue-max** interface configuration command enables local acknowledgment and TCP encapsulation. Both these options are required to use transmission groups. You should specify the SDLC address with the echo bit turned off for transmission group interfaces. The SDLC broadcast address 0xFF is routed automatically for transmission group interfaces. The **priority** keyword creates multiple TCP sessions for this route. The **tcp-queue-max** keyword sets the maximum size of the outbound TCP queue for the SDLC. The default TCP queue size is 100. The value for **hold-queue in** should be greater than the value for **tcp-queue-max**.

You can use the **priority** keyword (to set up the four levels of priorities to be used for TCP encapsulated frames) at the same time you enable local acknowledgment. The **priority** keyword is described in the following section. Use the **no** form of this command to disable SDLC Local Acknowledgment. For an example of how to enable local acknowledgment, see “Configuring Serial Link Address Prioritization Using STUN TCP/IP Encapsulation Example” later in this chapter.

Establish Priority Queuing Levels

With SDLC local acknowledgment enabled, you can establish priority levels used in priority queuing for serial interfaces. The priority levels are as follows:

- Low
- Medium
- Normal
- High

To set the priority queuing level, perform the following task in interface configuration mode:

Task	Command
Establish the four levels of priorities to be used in priority queuing.	stun route address address-number tcp ip-address [local-ack] priority [tcp-queue-max]

Use the **no** form of this command to disable priority settings. For an example of how to establish priority queuing levels, see “Configuring Serial Link Address Prioritization Using STUN TCP/IP Encapsulation Example” later in this chapter.

Configure Local Acknowledgment for Direct Frame Relay Connectivity between Routers

To implement STUN with local acknowledgment using direct Frame Relay encapsulation, perform the following task in interface configuration mode:

Task	Command
Configure Frame Relay encapsulation between STUN peers with local acknowledgment.	stun route address sdhc-addr interface frame-relay-port dlci number localsap local-ack cls

Configure STUN with Multilink Transmission Groups

You can configure multilink SDLC transmission groups across STUN connections between IBM communications controllers such as IBM 37x5s. Multilink transmission group allow you to collapse multiple WAN leased lines into one leased line.

SDLC multilink transmission groups provide the following features:

- Network Control Program (NCP) SDLC address allowances, including echo and broadcast addressing.
- Remote NCP load sequence. After a SIM/RIM exchange but before a SNRM/UA exchange, NCPs send numbered I-frames. During this period, I-frames are not locally acknowledged but instead are passed through. After the SNRM/UA exchange, local acknowledgment occurs.
- Rerouting of I-frames sent from the router to the NCP if a link is lost in a multilink transmission group.
- Flow control rate tuning causes a sending NCP to “feel” WAN congestion and hold frames that would otherwise be held in the router waiting to be transmitted on the WAN. This allows the NCP to perform its class-of-service algorithm more efficiently based on a greater knowledge of network congestion.

STUN connections that are part of a transmission group must have local acknowledgment enabled. Local acknowledgment keeps SDLC poll traffic off the WAN and reduces store-and-forward delays through the router. It also might minimize the number of NCP timers that expire due to network delay. Also, these STUN connections must go to the same IP address. This is because SNA transmission groups are parallel links between the same pair of IBM communications controllers.

Design Recommendations

This section provides some recommendations that are useful in configuring SDLC multilink transmission groups.

The bandwidth of the WAN should be larger than or equal to the aggregate bandwidth of all serial lines to avoid excessive flow control and ensure no degradation in response time. If other protocols also are using the WAN, ensure that the WAN bandwidth is significantly greater than the aggregate SNA serial line bandwidth to ensure that the SNA traffic does not monopolize the WAN.

When you use a combination of routed transmission groups and directly connected NCP transmission groups, you need to plan the configuration carefully to ensure that SNA sessions do not stop unexpectedly. Assuming that hardware reliability is not an issue, from a software point of view, single-link routed transmission group are as reliable as direct NCP-to-NCP single-link transmission groups. This is true because neither the NCP nor the router can reroute I-frames when a transmission group has only one link. Additionally, a multilink transmission group directed between NCPs and a multilink transmission group through router are equally reliable. Both can perform rerouting.

However, you might run into problems if you have a configuration in which two NCPs are directly connected (via one or more transmission group links) and one link in the transmission group is routed. The NCPs will treat this as a multilink transmission group. However, the router views the transmission group as a single-link transmission group.

A problem can arise in the following situation: Assume that an I-frame is being transmitted from NCP A (connected to router A) to NCP B (connected to router B) and that all SDLC links are currently active. Router A acknowledges the I-frame sent from NCP A and sends it over the WAN. If, before the I-frame reaches Router B, the SDLC link between router B and NCP B goes down, Router B attempts to reroute the I-frame on another link in the transmission group when it receives the I-frame. However, because this is a single-link transmission group, there are no other routes, and router B drops the I-frame. NCP B will never receive this I-frame because router A acknowledged its receipt, and NCP A marked it as transmitted and deleted it. NCP B detects a gap in the transmission group sequence numbers and waits to receive the missing I-frame. It will wait forever for this I-frame, and in the meantime will not send or receive any other frames. This means that NCP B is technically inoperational and that all SNA sessions through NCP B will be lost.

One final design recommendation note concerns a configuration in which one or more lines of an NCP transmission group are connected to a router and one or more lines are directly connected between NCPs. If the network delay associated with one line of an NCP transmission group is different from the delay of another line in the same NCP transmission group, the receiving NCP will spend additional time resequencing PIUs.

Set Up STUN Traffic Priorities

Use the methods described in the following sections to determine the order in which traffic should be handled on the network:

- Assign Queuing Priorities
- Prioritize STUN Traffic over All Other Traffic

Assign Queuing Priorities

You can assign queuing priorities by one of the following:

- Serial interface address or TCP port
- Logical unit (LU) address

Prioritize by Serial Interface Address or TCP Port

You can prioritize traffic on a per-serial-interface address or TCP port basis. You might want to do this so that traffic between one source-destination pair will always be sent before traffic between another source-destination pair.

Note You must first enable local acknowledgment and priority levels as described earlier in this chapter.

To prioritize traffic, perform one of the following tasks in global configuration mode:

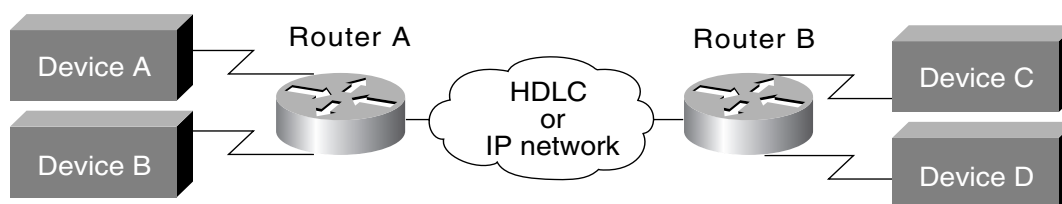
Task	Command
Assign a queuing priority to the address of the STUN serial interface.	priority-list <i>list-number</i> stun <i>queue-keyword</i> address <i>group-number</i> <i>address-number</i>
Assign a queuing priority to a TCP port.	priority-list <i>list-number</i> protocol ip <i>queue-keyword</i> tcp <i>tcp-port-number</i>

You must also perform the following task in interface configuration mode:

Task	Command
Assign a priority list to a priority group.	priority-group <i>list-number</i>

Figure 27-6 illustrates serial link address prioritization. Device A communicates with Device C, and Device B communicates with Device D. With the serial link address prioritization, you can choose to give A-C a higher priority over B-D across the serial tunnel.

Figure 27-6 Serial Link Address Prioritization



S1221a

To disable priorities, use the **no** forms of these commands.

For an example of how to prioritize traffic according to serial link address, see “Configuring Serial Link Address Prioritization Using STUN TCP/IP Encapsulation Example” later in this chapter.

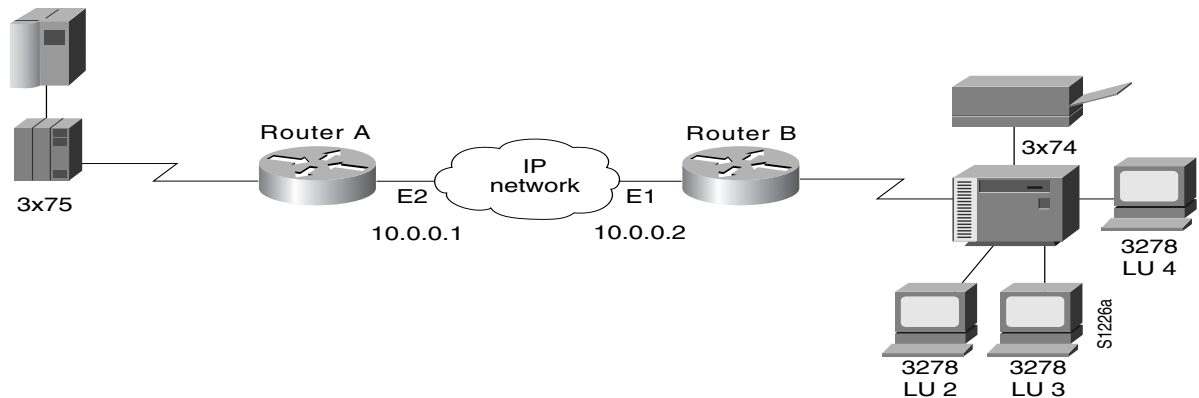
Prioritize by Logical Unit Address

SNA local logical unit (LU) address prioritization is specific to IBM SNA connectivity and is used to prioritize SNA traffic on either STUN or remote source-route bridging (RSRB). To set the queuing priority by LU address, perform the following task in interface configuration mode:

Task	Command
Assign a queuing priority based on the logical unit address.	locaddr-priority-list <i>list-number</i> <i>address-number</i> <i>queue-keyword</i>

In Figure 27-7, LU address prioritization can be set so that particular LUs receive data in preference to others or so that LUs have priority over the printer, for example.

Figure 27-7 SNA LU Address Prioritization



To disable this priority, use the **no** form of this command.

For an example of how to prioritize traffic according to logical unit address, see “Configuring LOCADDR Priority Groups for STUN Example” later in this chapter.

Prioritize STUN Traffic over All Other Traffic

You can prioritize STUN traffic to be routed first before all other traffic on the network. To give STUN traffic this priority, perform the following task in global configuration mode:

Task	Command
Prioritize STUN traffic in your network over that of other protocols.	priority-list <i>list-number</i> stun <i>queue-keyword</i> address <i>group-number</i> <i>address-number</i>

To disable this priority, use the **no** form of this command.

For an example of how to prioritize STUN traffic over all other traffic, see “Configuring Serial Link Address Prioritization Using STUN TCP/IP Encapsulation Example” later in this chapter.

Monitor STUN Network Activity

You can list statistics regarding STUN interfaces, protocol groups, number of packets sent and received, local acknowledgment states, and more. To get activity information, perform the following task in EXEC mode:

Task	Command
List the status display fields for STUN interfaces.	show stun

STUN Configuration Examples

The following sections provide STUN configuration examples:

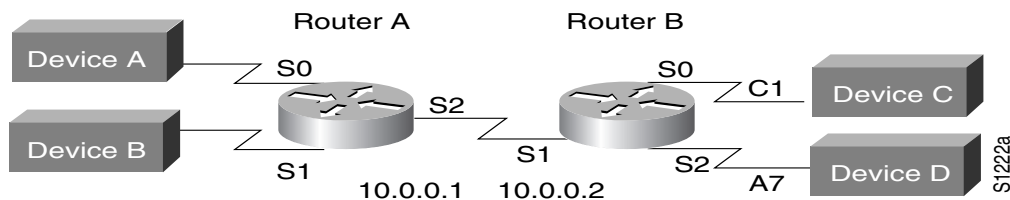
- Configuring STUN Priorities Using HDLC Encapsulation Example

- Configuring SDLC Broadcast Example
- Configuring Serial Link Address Prioritization Using STUN TCP/IP Encapsulation Example
- Configuring STUN Multipoint Implementation Using a Line-Sharing Device Example
- Configuring STUN Local Acknowledgment for SDLC Example
- Configuring STUN Local Acknowledgment for Frame Relay Example
- Configuring LOCADDR Priority Groups—Simple Example
- Configuring LOCADDR Priority Groups for STUN Example

Configuring STUN Priorities Using HDLC Encapsulation Example

Assume that the link between Router A and Router B in Figure 27-8 is a serial tunnel that uses the simple serial transport mechanism. Device A communicates with Device C (SDLC address C1) with a high priority. Device B communicates with Device D (SDLC address A7) with a normal priority.

Figure 27-8 STUN Simple Serial Transport



The following configurations set the priority of STUN hosts A, B, C, and D.

Configuration for Router A

```

stun peer-name 1.0.0.1
stun protocol-group 1 sdlc
stun protocol-group 2 sdlc
!
interface serial 0
no ip address
encapsulation stun
stun group 1
stun route address C1 interface serial 2
!
interface serial 1
no ip address
encapsulation stun
stun group 2
stun route address A7 interface serial 2
!
interface serial 2
ip address 1.0.0.1 255.0.0.0
priority-group 1
!
priority-list 1 stun high address 1 C1
priority-list 1 stun low address 2 A7

```

Configuration for Router B

```

stun peer-name 1.0.0.2

```

```

stun protocol-group 1 sdlc
stun protocol-group 2 sdlc
!
interface serial 0
no ip address
encapsulation stun
stun group 1
stun route address C1 interface serial 1
!
interface serial 1
ip address 1.0.0.2 255.0.0.0
priority-group 1
!
interface serial 2
no ip address
encapsulation stun
stun group 2
stun route address A7 interface serial 1
!
priority-list 1 stun high address 1 C1
priority-list 1 stun low address 2 A7

```

Configuring SDLC Broadcast Example

In the following example, an FEP views end stations 1, 2, and 3 as if they were on an SDLC multidrop link. Any broadcast frame sent from the FEP to Router A is duplicated and sent to each of the downstream routers (B and C):

```

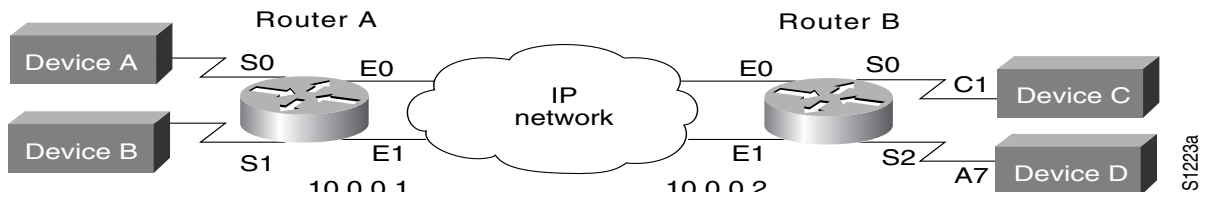
stun peer-name xxx.xxx.xxx.xxx
stun protocol-group 1 sdlc
interface serial 1
encapsulation stun
stun group 1
stun sdlc-role secondary
sdlc virtual-multidrop
sdlc address 1
sdlc address 2
sdlc address 3
stun route address 1 tcp yyy.yyy.yyy.yyy local-ack
stun route address 2 tcp zzz.zzz.zzz.zzz local-ack
stun route address 3 tcp zzz.zzz.zzz.zzz local-ack
stun route address FF tcp yyy.yyy.yyy.yyy
stun route address FF tcp zzz.zzz.zzz.zzz

```

Configuring Serial Link Address Prioritization Using STUN TCP/IP Encapsulation Example

Assume that the link between Router A and Router B is a serial tunnel that uses the TCP/IP encapsulation as shown in Figure 27-9. Device A communicates with Device C (SDLC address C1) with a high priority. Device B communicates with Device D (SDLC address A7) with a normal priority. The configuration file for each router follows the figure.

Figure 27-9 STUN TCP/IP Encapsulation



Configuration for Router A

```

stun peer-name 1.0.0.1
stun protocol-group 1 sdlc
stun protocol-group 2 sdlc
!
interface serial 0
no ip address
encapsulation stun
stun group 1
stun route address C1 tcp 1.0.0.2 local-ack priority
priority-group 1
!
interface serial 1
no ip address
encapsulation stun
stun group 2
stun route address A7 tcp 1.0.0.2 local-ack priority
priority-group 2
!
interface ethernet 0
ip address 1.0.0.1 255.0.0.0
!
interface ethernet 1
ip address 1.0.0.3 255.0.0.0
!
priority-list 1 protocol ip high tcp 1994
priority-list 1 protocol ip medium tcp 1990
priority-list 1 protocol ip normal tcp 1991
priority-list 1 protocol ip low tcp 1992
priority-list 1 stun high address 1 C1
!
priority-list 2 protocol ip high tcp 1994
priority-list 2 protocol ip medium tcp 1990
priority-list 2 protocol ip normal tcp 1991
priority-list 2 protocol ip low tcp 1992
priority-list 2 stun normal address 2 A7
!
hostname routerA
router igrp
network 1.0.0.0
    
```

Configuration for Router B

```

stun peer-name 1.0.0.2
stun protocol-group 1 sdlc
stun protocol-group 2 sdlc
!
interface serial 0
no ip address
encapsulation stun
stun group 1
stun route address C1 tcp 1.0.0.1 local-ack priority
    
```

```

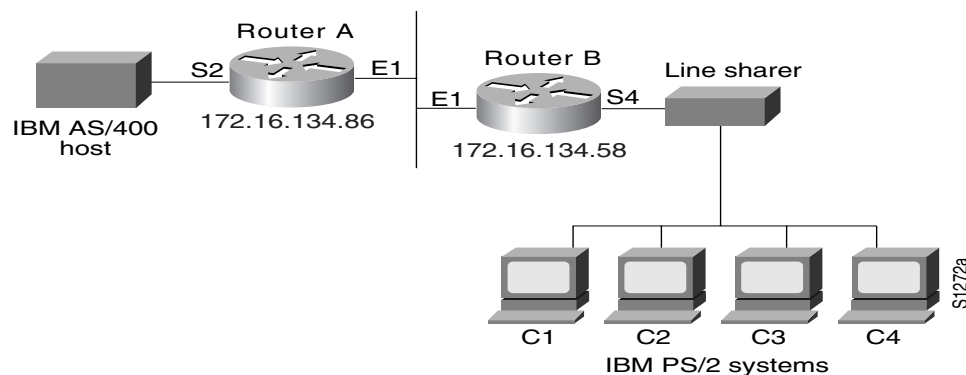
priority-group 1
!
interface serial 2
no ip address
encapsulation stun
stun group 2
stun route address A7 tcp 1.0.0.1 local-ack priority
priority-group 2
!
interface ethernet 0
ip address 1.0.0.2 255.0.0.0
!
interface ethernet 1
ip address 1.0.0.4 255.0.0.0
!
priority-list 1 protocol ip high tcp 1994
priority-list 1 protocol ip medium tcp 1990
priority-list 1 protocol ip normal tcp 1991
priority-list 1 protocol ip low tcp 1992
priority-list 1 stun high address 1 C1
!
priority-list 2 protocol ip high tcp 1994
priority-list 2 protocol ip medium tcp 1990
priority-list 2 protocol ip normal tcp 1991
priority-list 2 protocol ip low tcp 1992
priority-list 2 stun normal address 2 A7
!
hostname routerB
router igrp 109
network 1.0.0.0

```

Configuring STUN Multipoint Implementation Using a Line-Sharing Device Example

In Figure 27-10, four separate PS/2 computers are connected to a line-sharing device off of Router B. Each PS/2 computer has four sessions open on an AS/400 device attached to Router A. Router B functions as the primary station, while Router A functions as the secondary station. Both routers locally acknowledge packets from the IBM PS/2 systems.

Figure 27-10 STUN Communication Involving a Line-Sharing Device



The configuration file for the routers shown in Figure 27-10 follows.

Configuration for Router A

```
! enter the address of the stun peer
```

STUN Configuration Examples

```
stun peer-name 150.136.134.86
! specify that group 4 uses the SDLC protocol
stun protocol-group 4 sdlc
stun remote-peer-keepalive

interface ethernet 1
! enter the IP address for the Ethernet interface
ip address 150.136.134.86 255.255.255.0
!
! description of IBM AS/400 link
interface serial 2
! description of IBM AS/400 link; disable the IP address on a serial interface
no ip address
! enable STUN encapsulation on this interface
encapsulation stun
! apply previously defined stun group 4 to serial interface 2
stun group 4
! establish this router as a secondary station
stun sdlc-role secondary
! wait up to 63000 msec for a poll from the primary before timing out
sdlc poll-wait-timeout 63000
! list addresses of secondary stations (PS/2 systems) attached to link
sdlc address C1
sdlc address C2
sdlc address C3
sdlc address C4
! use tcp encapsulation to send frames to SDLC stations C1, C2, C3, or
! C4 and locally terminate sessions with these stations
stun route address C1 tcp 150.136.134.58 local-ack
stun route address C2 tcp 150.136.134.58 local-ack
stun route address C3 tcp 150.136.134.58 local-ack
stun route address C4 tcp 150.136.134.58 local-ack
```

Configuration for Router B

```
! enter the address of the stun peer
stun peer-name 150.136.134.58
! this router is part of SDLC group 4
stun protocol-group 4 sdlc
stun remote-peer-keepalive
!
interface ethernet 1
! enter the IP address for the Ethernet interface
ip address 150.136.134.58 255.255.255.0
!
! description of PS/2 link
interface serial 4
! disable the IP address on a serial interface
no ip address
! enable STUN encapsulation on this interface
encapsulation stun
! apply previously defined stun group 4 to serial interface 2
stun group 4
! establish this router as a primary station
stun sdlc-role primary
sdlc line-speed 9600
! wait 2000 milliseconds for a reply to a frame before resending it
sdlc t1 2000
! resend a frame up to four times if not acknowledged
sdlc n2 4
! list addresses of secondary stations (PS/2 systems) attached to link
sdlc address C1
sdlc address C2
sdlc address C3
```

```

sdlc address C4
! use tcp encapsulation to send frames to SDLC stations C1, C2, C3, or
! C4 and locally terminate sessions with these stations
stun route address C3 tcp 150.136.134.86 local-ack
stun route address C1 tcp 150.136.134.86 local-ack
stun route address C4 tcp 150.136.134.86 local-ack
stun route address C2 tcp 150.136.134.86 local-ack
! set the clockrate on this interface to 9600 bits per second
clockrate 9600

```

Configuring STUN Local Acknowledgment for SDLC Example

The following example shows a sample configuration for a pair of routers performing SDLC local acknowledgment.

Configuration for Router A

```

stun peer-name 150.136.64.92
stun protocol-group 1 sdlc
stun remote-peer-keepalive
!
interface Serial 0
no ip address
encapsulation stun
stun group 1
stun sdlc-role secondary
sdlc address C1
stun route address C1 tcp 150.136.64.93 local-ack
clockrate 19200

```

Configuration for Router B

```

stun peer-name 150.136.64.93
stun protocol-group 1 sdlc
stun remote-peer-keepalive
!
interface Serial 0
no ip address
encapsulation stun
stun group 1
stun sdlc-role primary
sdlc line-speed 19200
sdlc address C1
stun route address C1 tcp 150.136.64.92 local-ack
clockrate 19200

```

Configuring STUN Local Acknowledgment for Frame Relay Example

The following example describes an interface configuration for Frame Relay STUN with local acknowledgment:

```

stun peer-name 10.1.21.1 cls 4
stun protocol-group 120 sdlc
!
interface Serial1
no ip address
encapsulation frame-relay
frame-relay lmi-type ansi
frame-relay map 11c2 22
!

```

```
interface Serial4
  no ip address
  encapsulation stun
  clockrate 9600
  stun group 120
  stun sdlc-role secondary
  sdlc address C1
  sdlc address C2
  stun route address C1 interface Serial11 dlci 22 04 local-ack
  stun route address C2 interface Serial11 dlci 22 08 local-ack
!
```

Configuring LOCADDR Priority Groups—Simple Example

The following example shows how to establish queuing priorities on a STUN interface based on an LU address:

```
! 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
locaddr-priority 1
priority-group 1
interface Ethernet 0
! give locaddr-priority-list 1 a high priority for LU 02
locaddr-priority-list 1 02 high
! give locaddr-priority-list 1 a low priority for LU 05
locaddr-priority-list 1 05 low
```

Configuring LOCADDR Priority Groups for STUN Example

The following configuration example shows how to assign a priority group to an input interface:

Configuration for Router A

```
stun peer-name 1.0.0.1
stun protocol-group 1 sdlc
!
interface serial 0
no ip address
encapsulation stun
stun group 1
stun route address C1 tcp 1.0.0.2 local-ack priority
clockrate 19200
locaddr-priority 1
priority-group 1
!
interface Ethernet 0
ip address 1.0.0.1 255.255.255.0
```

```

!
locaddr-priority-list 1 02 high
locaddr-priority-list 1 03 high
locaddr-priority-list 1 04 medium
locaddr-priority-list 1 05 low
!
priority-list 1 protocol ip high tcp 1994
priority-list 1 protocol ip medium tcp 1990
priority-list 1 protocol ip normal tcp 1991
priority-list 1 protocol ip low tcp 1992

```

Configuration for Router B

```

stun peer-name 1.0.0.2
stun protocol-group 1 sdlc
!
interface serial 0
no ip address
encapsulation stun
stun group 1
stun route address C1 tcp 1.0.0.1 local-ack priority
clockrate 19200
locaddr-priority 1
priority-group 1
!
interface Ethernet 0
ip address 1.0.0.2 255.255.255.0
!
locaddr-priority-list 1 02 high
locaddr-priority-list 1 03 high
locaddr-priority-list 1 04 medium
locaddr-priority-list 1 05 low
!
priority-list 1 protocol ip high tcp 1994
priority-list 1 protocol ip medium tcp 1990
priority-list 1 protocol ip normal tcp 1991
priority-list 1 protocol ip low tcp 1992

```

Cisco's Implementation of Block Serial Tunneling (BSTUN)

Our implementation of BSTUN provides the following features:

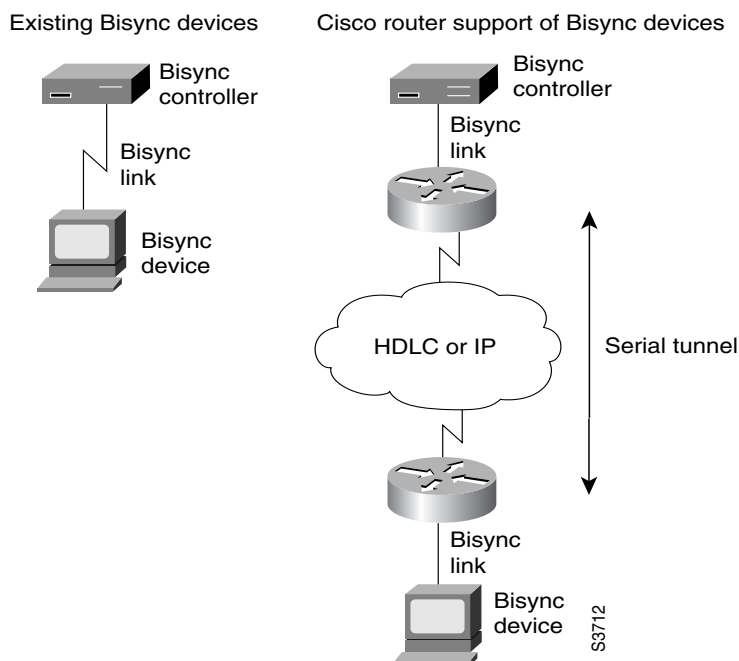
- Encapsulates BSC traffic for transfer over router links
- Supports legacy BSC devices and host applications without modification
- Uses standard synchronous serial interfaces on Cisco 2500 series and the 4T network interface module (NIM) on the Cisco 4000 series and Cisco 4500 series
- Supports point-to-point, multidrop, and virtual multidrop configurations

BSC Network Overview

The BSC feature enables your Cisco 2500 series, Cisco 4000 series, or Cisco 4500 series router to support devices that use the Binary Synchronous Communication (BSC) data link protocol. This protocol enables enterprises to transport BSC traffic over the same network that supports their SNA and multiprotocol traffic, eliminating the need for separate bisync facilities.

At the access router, traffic from the attached BSC device is encapsulated in IP. The BSC traffic can then be routed across arbitrary media to the host site where another router supporting BSC will remove the IP encapsulation headers and present the BSC traffic to the BSC host or controller over a serial connection. HDLC can be used as an alternative encapsulation method for point-to-point links. Figure 27-11 shows how you can reconfigure an existing BSC link between two devices and provide the same logical link without any changes to the existing BSC devices.

Figure 27-11 Routers Consolidate BSC Traffic by Encapsulation in IP or HDLC



The routers transport all BSC blocks between the two devices in passthrough mode using BSTUN as encapsulation. BSTUN uses the same encapsulation architecture as STUN, but is implemented on an independent tunnel.

Point-to-Point and Multidrop Support

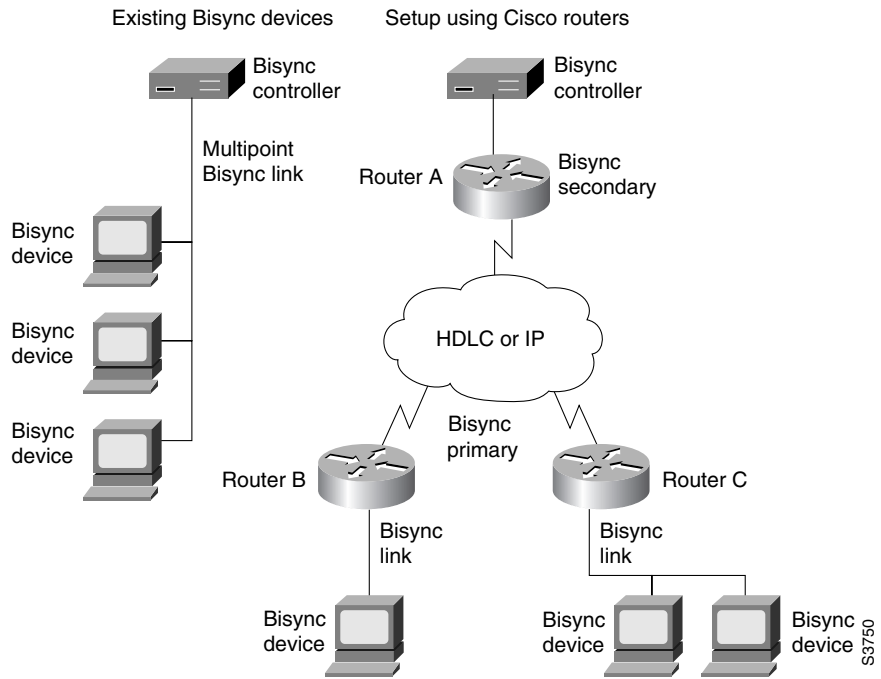
The BSC feature supports point-to-point, multidrop, and virtual multidrop BSC configurations.

Point-to-Point Operation

In point-to-point operation the BSC blocks between the two point-to-point devices are received and forwarded transparently by the routers. The contention to acquire the line for transmission is handled by the devices themselves.

Cisco’s BSC multipoint operation is provided as a logical multipoint configuration. Figure 27-12 shows how a multipoint BSC link is reconfigured using Cisco routers. Router A is configured as BSC Secondary. It monitors the address field of the polling or selection block and uses this address information to put into the BSTUN frame for BSTUN to deliver to the correct destination router. To simulate the BSC multidrop, an EOT block is sent by the BSC Primary router before a poll or selection block. This ensures that BSC tributary stations are in control mode before being polled or selected.

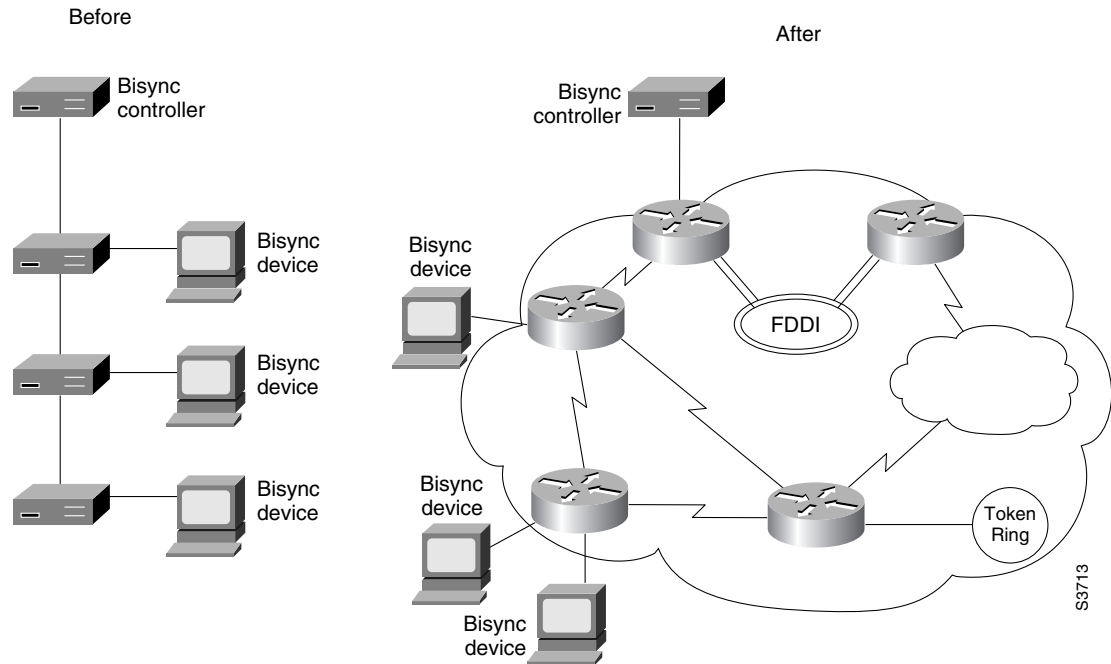
Figure 27-12 Multipoint BSC Link Reconfigured Using Routers



Multidrop Configuration

Multidrop configurations are common in BSC networks where up to eight or ten BSC devices are frequently connected to a BSC controller port over a single low-speed link. Our virtual multidrop support allows BSC devices from different physical locations in the network to appear as a single multidrop line to the BSC host or controller. Figure 27-13 illustrates a multidrop BSC configuration before and after implementing routers.

Figure 27-13 Integrating BSC Devices over a Multiprotocol Network



Frame Sequencing

BSC is a half-duplex protocol. Each block of transmission is acknowledged explicitly. To avoid the problem associated with simultaneous transmission, there is an implicit role of primary and secondary station. The primary resends the last block if there is no response from the secondary within the period of block receive timeout. In the multidrop setup, the BSC control station is the primary and the tributary stations are secondary. In a point-to-point configuration, the primary role is assumed by the BSC device that has successfully acquired the line for transmission through the ENQ bidding sequence. The primary role stays with this station until it sends EOT.

To protect against occasional network latency, which causes the primary station to time out and resend the block before the BSC block sent by the secondary is received, the control byte of the encapsulating frame is used as a sequence number. This sequence number is controlled and monitored by the primary BSC router. This allows the primary BSC router to detect and discard "late" BSC blocks sent by the secondary router and ensure integrity of the BSC link.

Note Frame sequencing is implemented in passthrough mode only.

BSTUN Configuration Task List

The BSC feature is configured similar to SDLC STUN, but it is configured as a protocol within a BSTUN feature. To configure and monitor BSTUN, complete the tasks in the following sections:

- Enable Block Serial Tunneling
- Define the BSC Protocol Group
- Configure BSTUN on the Serial Interface
- Place a Serial Interface in a BSTUN Group
- Define How Frames Are Forwarded
- Set Up BSTUN Traffic Priorities
- Configure BSC Options on a Serial Interface
- Monitor the Status of BSTUN

The “BSTUN Configuration Examples” section follows these tasks.

Enable Block Serial Tunneling

To enable BSTUN, perform the following task in global configuration mode:

Task	Command
Enable BSTUN.	bstun peer-name <i>ip-address</i>

Define the BSC Protocol Group

Define a BSTUN group and specify the protocol it uses. Currently the only block serial protocol supported is BSC. To define the BSC protocol group, perform the following task in global configuration mode:

Task	Command
Define the BSC protocol group.	bstun protocol-group <i>group-number protocol</i> [bsc bsc-local-ack]

Configure BSTUN on the Serial Interface

Configure BSTUN on the serial interface before issuing any further BSTUN or BSC configuration commands for the interface. To configure the BSTUN function on a specified interface, perform the following command in interface configuration mode:

Task	Command
Configure BSTUN on an interface.	encapsulation bstun

Place a Serial Interface in a BSTUN Group

Each BSTUN-enabled interface on a router must be placed in a previously defined BSTUN group. Packets will only travel between BSTUN-enabled interfaces that are in the same group. To assign a serial interface to a BSTUN group, perform the following task in interface configuration mode:

Task	Command
Assign a serial interface to a BSTUN group.	bstun group <i>group-number</i>

Define How Frames Are Forwarded

To specify how frames are forwarded when received on a BSTUN interface, perform one of the following tasks in interface configuration mode:

Task	Command
Propagate all BSTUN traffic received on the input interface, regardless of the address contained in the serial frame. TCP encapsulation is used to propagate frames that match the entry.	bstun route all tcp <i>ip-address</i> ¹
Propagate all BSTUN traffic received on the input interface, regardless of the address contained in the serial frame. HDLC encapsulation is used to propagate the serial frames.	bstun route all interface serial <i>interface-number</i>
Use HDLC encapsulation to propagate the serial frames. The specified interface is also a direct BSTUN link, rather than a serial connection to another peer.	bstun route interface serial <i>interface-number</i> direct
Propagate the serial frame that contains a specific address. TCP encapsulation is used to propagate frames that match the entry.	bstun route address <i>address-number</i> tcp <i>ip-address</i>
Propagate the serial frame that contains a specific address. HDLC encapsulation is used to propagate the serial frames.	bstun route address <i>address-number</i> interface serial <i>interface-number</i>
Propagate the serial frame that contains a specific address. HDLC encapsulation is used to propagate the serial frames. The specified interface is also a direct BSTUN link, rather than a serial connection to another peer.	bstun route address <i>address-number</i> interface serial <i>interface-number</i> direct

1. This command functions in either passthrough or local acknowledgment mode.

Note We recommend that for BSC local acknowledgment you use the **bstun route all tcp** command. This command reduces the amount of duplicate configuration detail that would otherwise be needed to specify routers at each end of the tunnel.

Set Up BSTUN Traffic Priorities

You can assign BSTUN traffic priorities based on either the BSTUN header or the TCP port. To prioritize traffic, perform one of the following tasks in global configuration mode:

Task	Command
Establish BSTUN queuing priorities based on the BSTUN header.	priority-list <i>list-number</i> protocol bstun queue [gt <i>packet-size</i>] [lt <i>packet-size</i>] address <i>bstun-group bsc-addr</i>
Assign a queuing priority to TCP port.	priority-list <i>list-number</i> protocol ip queue tcp <i>tcp-port-number</i>

You can customize BSTUN queuing priorities based on either the BSTUN header or TCP port. To customize priorities, perform one of the following tasks in global configuration mode:

Task	Command
Customize BSTUN queuing priorities based on the BSTUN header.	queue-list <i>list-number</i> protocol bstun queue [gt <i>packet-size</i>] [lt <i>packet-size</i>] address <i>bstun-group bsc-addr</i>
Customize BSTUN queuing priorities based on the TCP port.	queue-list <i>list-number</i> protocol ip queue tcp <i>tcp-port-number</i>

Configure BSC Options on a Serial Interface

To configure BSC options on a serial interface, perform one of the following tasks in interface configuration mode:

Task	Command
Specify the character set used by the BSC support feature.	bsc char-set [<i>ascii</i> <i>ebcdic</i>]
Specify that the BSC link connected to the serial interface is a point-to-point BSC station.	bsc contention
Specify that the interface can run BSC in full-duplex mode using non-switched RTS signals.	full-duplex ¹
Specify the amount of time between the start of one polling cycle and the next.	bsc pause <i>time</i>
Specify the timeout for a poll or a select sequence.	bsc poll-timeout <i>time</i>
Specify that the router is acting as the primary end of the BSC link.	bsc primary
Specify the number of retries before a device is considered to have failed.	bsc retries <i>retry-count</i>
Specify that the router is acting as the secondary end of the BSC link.	bsc secondary
Specify specific polls, rather than general polls, used on the host-to-router connection.	bsc spec-poll
Specify the number of cycles of the active poll list that are performed between polls to control units in the inactive poll list.	bsc servlim <i>servlim-count</i>

1. This command is documented in the “Interface Commands” chapter of the *Router Products Command Reference*.

Monitor the Status of BSTUN

To list statistics regarding BSTUN interfaces, protocol groups, number of packets sent and received, local acknowledgment states, and other activity information, perform the following task in EXEC mode:

Task	Command
List the status display fields for BSTUN interfaces.	show bstun
Display status of the interfaces on which BSC is configured.	show bsc

BSTUN Configuration Examples

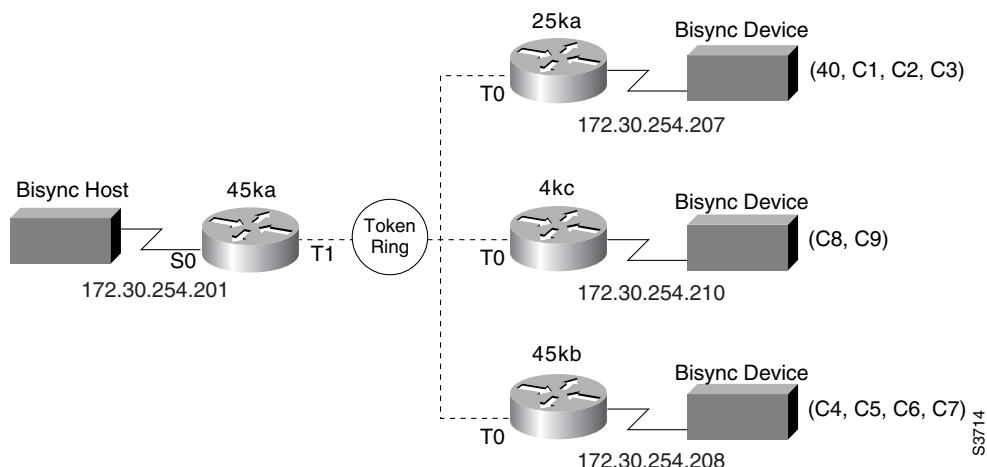
The following sections provide BSTUN configuration examples:

- Simple BSC Configuration Example
- Priority Queueing: Prioritization Based on BSTUN Header Example
- Priority Queueing: Prioritization Based on BSTUN Header and Packet Sizes Example
- Priority Queueing: Prioritization Based on BSTUN Header and BSC Address Example
- Priority Queueing: Prioritization Based on BSTUN TCP Ports Example
- Priority Queueing: Prioritization Based on BSTUN TCP Ports and BSC Address Example
- Custom Queueing: Prioritization based on BSTUN Header Example
- Custom Queueing: Prioritization Based on BSTUN Header and Packet Size Example
- Custom Queueing: Prioritization Based on BSTUN Header and BSC Address Example
- Custom Queueing: Prioritization Based on BSTUN TCP Ports Example
- Custom Queueing: Prioritization Based on BSTUN TCP Ports and BSC Address Example

Simple BSC Configuration Example

Figure 27-14 shows a simple BSTUN configuration example.

Figure 27-14 Simple BSC Configuration



S3714

The configuration files for the routers shown in Figure 27-14 follow.

Configuration for Router 45ka

```
!  
version 10.2  
!  
hostname 45ka  
!  
!  
no ip domain-lookup  
!  
bstun peer-name 150.10.254.201  
bstun protocol-group 1 bsc  
!  
interface Ethernet0  
ip address 198.92.0.201 255.255.255.0  
media-type 10BaseT  
!  
interface Ethernet1  
no ip address  
shutdown  
media-type 10BaseT  
!  
interface Serial0  
no ip address  
encapsulation bstun  
clockrate 19200  
bstun group 1  
bsc char-set ebcdic  
bsc secondary  
bstun route address C9 tcp 150.10.254.210  
bstun route address C8 tcp 150.10.254.210  
bstun route address C7 tcp 150.10.254.208  
bstun route address C6 tcp 150.10.254.208  
bstun route address C5 tcp 150.10.254.208  
bstun route address C4 tcp 150.10.254.208  
bstun route address C3 tcp 150.10.254.207  
bstun route address C2 tcp 150.10.254.207  
bstun route address C1 tcp 150.10.254.207  
bstun route address 40 tcp 150.10.254.207  
!  
interface Serial1  
no ip address  
shutdown  
!  
interface Serial2  
no ip address  
shutdown  
!  
interface Serial3  
no ip address  
shutdown  
!  
interface TokenRing0  
no ip address  
shutdown  
!  
interface TokenRing1  
ip address 150.10.254.201 255.255.255.0  
ring-speed 16  
!  
!
```

```
line con 0
line aux 0
line vty 0 4
login
!
end
```

Configuration for Router 25ka

```
!
version 10.2
!
hostname 25ka
!
!
no ip domain-lookup
!
bstun peer-name 150.10.254.207
bstun protocol-group 1 bsc
!
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
encapsulation bstun
clockrate 19200
bstun group 1
bsc char-set ebedic
bsc primary
bstun route address C3 tcp 150.10.254.201
bstun route address C2 tcp 150.10.254.201
bstun route address C1 tcp 150.10.254.201
bstun route address 40 tcp 150.10.254.201
!
interface TokenRing0
ip address 150.10.254.207 255.255.255.0
ring-speed 16
!
interface BRI0
no ip address
shutdown
!
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Configuration for Router 4kc

```
!
version 10.2
!
hostname 4kc
!
!
no ip domain-lookup
!
```

```

bstun peer-name 150.10.254.210
bstun protocol-group 1 bsc
!
interface Ethernet0
ip address 198.92.0.210 255.255.255.0
media-type 10BaseT
!
interface Serial0
no ip address
encapsulation bstun
clockrate 19200
bstun group 1
bsc char-set ebcddic
bsc primary
bstun route address C9 tcp 150.10.254.201
bstun route address C8 tcp 150.10.254.201
!
interface Serial1
no ip address
shutdown
!
interface Serial2
no ip address
shutdown
!
interface Serial3
no ip address
shutdown
!
interface TokenRing0
ip address 150.10.254.210 255.255.255.0
ring-speed 16
!
interface TokenRing1
no ip address
shutdown
!
|
line con 0
line aux 0
line vty 0 4
login
!
end

```

Configuration for Router 25kb

```

!
version 10.2
!
hostname 25kb
!
!
no ip domain-lookup
!
bstun peer-name 150.10.254.208
bstun protocol-group 1 bsc
!
interface Serial0
no ip address
encapsulation bstun
no keepalive
clockrate 19200

```

```
bstun group 1
bsc char-set ebcdic
bsc primary
bstun route address C7 tcp 150.10.254.201
bstun route address C6 tcp 150.10.254.201
bstun route address C5 tcp 150.10.254.201
bstun route address C4 tcp 150.10.254.201
!
interface Serial1
no ip address
shutdown
!
interface TokenRing0
ip address 150.10.254.208 255.255.255.0
ring-speed 16
!
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

Priority Queueing: Prioritization Based on BSTUN Header Example

In this example, the output interface examines header info and places packets with the BSTUN header on specified output queue.

```
priority-list <list> protocol bstun <outputQ>
int Serial0
priority-group <list>
int Serial1
encap bstun
bstun group 1
bstun route all interface serial 0
...or...
bstun route address <bsc-addr> interface serial 0
```

Priority Queueing: Prioritization Based on BSTUN Header and Packet Sizes Example

In this example, the 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 queue.

```
priority-list <list> protocol bstun <outputQ> gt <pak-size>
priority-list <list> protocol bstun <outputQ> lt <pak-size>
int Serial0
priority-group <list>
int Serial1
encap bstun
bstun group 1
bstun route all interface serial 0
...or...
bstun route address <bsc-addr> interface serial 0
```

Priority Queueing: Prioritization Based on BSTUN Header and BSC Address Example

In this example, the output interface examines header information and BSC address and places packets with the BSTUN header that match BSC address on specified output queue.

```
priority-list <list> protocol bstun <outputQ>
address <bstun-group> <bsc-addr>
int Serial0
priority-group <list>
int Serial1
encap bstun
bstun group 1
bstun route address <bsc-addr> interface serial 0
```

Priority Queueing: Prioritization Based on BSTUN TCP Ports Example

In this example, the output interface examines TCP port number and places packets with the BSTUN port number (1976) on specified output queue.

```
priority-list <list> protocol ip <outputQ> tcp 1976
int Serial0
priority-group <list>
int Serial1
encap bstun
bstun group 1
bstun route all tcp <bstun-peer-ip-addr>
```

Priority Queueing: Prioritization Based on BSTUN TCP Ports and BSC Address Example

In this example, four TCP/IP sessions (high, medium, normal, & low) are established with BSTUN peers using BSTUN port numbers. The input interface examines the BSC address and uses the specified output queue definition to determine which BSTUN TCP session (high, medium, normal, or low) to use for sending the packet to the BSTUN peer.

The output interface examines TCP port number and places packets with the BSTUN port numbers on specified output queue.

```
priority-list <list> protocol ip high tcp 1976
priority-list <list> protocol ip medium tcp 1977
priority-list <list> protocol ip normal tcp 1978
priority-list <list> protocol ip low tcp 1979

priority-list <list> protocol bstun <outputQ>
address <bstun-group> <bsc-addr>

int Serial0
priority-group <list>

int Serial1
encap bstun
bstun group 1
bstun route address <bsc-addr> tcp <bstun-peer-ip-addr> priority
priority-group <list>
```

Custom Queueing: Prioritization based on BSTUN Header Example

In this example, the output interface examines header info and places packets with the BSTUN header on specified output queue.

```
queue-list <list> protocol bstun <outputQ>
```

```
int Serial0
custom-queue-list <list>

int Serial1
encap bstun
bstun group 1
bstun route all interface serial 0
```

Custom Queueing: Prioritization Based on BSTUN Header and Packet Size Example

In this example, the 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 queue.

```
queue-list <list> protocol bstun <outputQ> gt <pak-size>
queue-list <list> protocol bstun <outputQ> lt <pak-size>

int Serial0
custom-queue-list <list>

int Serial1
encap bstun
bstun group 1
bstun route all interface serial 0
```

Custom Queueing: Prioritization Based on BSTUN Header and BSC Address Example

In this example the output interface examines header info _and_ BSC address and places packets with the BSTUN header that match BSC address on specified output queue.

```
queue-list <list> protocol bstun <outputQ>
address <bstun-group> <bsc-addr>

int Serial0
custom-queue-list <list>

int Serial1
encap bstun
bstun group 1
bstun route address <bsc-addr> interface serial 0
```

Custom Queueing: Prioritization Based on BSTUN TCP Ports Example

In this example, the output interface examines TCP port number and places packets with the BSTUN port number (1976) on specified output queue.

```
queue-list <list> protocol ip <outputQ> tcp 1976

int Serial0
custom-queue-list <list>

int Serial1
encap bstun
bstun group 1
bstun route all tcp <bstun-peer-ip-addr>
```

Custom Queueing: Prioritization Based on BSTUN TCP Ports and BSC Address Example

In this example, four TCP/IP sessions (high, medium, normal, & low) are established with BSTUN peers using BSTUN port numbers.

Input interface examines the BSC address and uses the specified output queue definition to determine which BSTUN TCP session (high, medium, normal, or low) to use.

Output interface examines TCP port number and places packets with the BSTUN port numbers on specified output queue.

For BSC addressing, output queues map as follows:

outputQ 1	Maps to medium BSTUN port (1977)
outputQ 2	Maps to normal BSTUN port (1978)
outputQ 3	Maps to low BSTUN port (1979)
outputQ 4-10	Maps to high BSTUN port (1976)

```

queue-list <list> protocol ip <outputQ> tcp 1976
queue-list <list> protocol ip <outputQ> tcp 1977
queue-list <list> protocol ip <outputQ> tcp 1978
queue-list <list> protocol ip <outputQ> tcp 1979

priority-list <list> protocol bstun <outputQ>
address <bstun-group> <bsc-addr>

int Serial0
custom-queue-list <list>

int Serial1
encap bstun
bstun group 1
bstun route address <bsc-addr> tcp <bstun-peer-ip-addr> priority
custom-queue-list <list>

```

