path

To specify one or more data paths for the IP host backup, use the **path** command in interface configuration mode. To delete a single path, use the **no** form of this command.

path *path*

no path *path*

Syntax Description

path	Hexadecimal value in the range from 0000 to FFFF. This value specifies the logical channel path and consists of two digits for the physical connection (either on the host or on the ESCON director), one digit for the channel logical address, and one digit for the control unit logical address. If the path is not specified in the input/output configuration program (IOCP), the default values for channel logical address and control unit logical address is 0. Up to 16 values for the *path* argument can be specified in the **path** command.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Up to 16 values for the *path* argument can be specified in the **path** command.

The path command places the router in IP host backup configuration mode, where additional commands can be entered to define backup groups for Common Link Access for Workstations (CLAW) and offload connections.

Examples

The following examples show two methods for entering the same IP host backup group information. The first group is the long form, using the **offload** command in interface configuration mode. The second group of commands is the shortcut, using the **path** interface configuration command and an **offload** IP host backup configuration command.

Long form:

```
offload c000 00 198.92.10.5 sysa router1 tcpip tcpip backup
offload c100 00 198.92.10.5 sysa router1 tcpip tcpip backup
offload c200 00 198.92.10.5 sysa router1 tcpip tcpip backup
```

Shortcut form:

```
path c000 c100 c200
  offload 00 198.92.10.5 sysa router1 tcpip tcpip
```

Related Commands

Command	Description
claw (backup)	Configures a CLAW device (read and write subchannel) for communication with a mainframe TCP/IP stack in offload mode and also configures individual members of a CLAW backup group for the IP Host Backup feature.
offload (backup)	Configures a backup group of Offload devices.

ping sna

To initiate an Advanced Program-to-Program Communication (APPC) session with a named destination logical unit (LU) to run the APING transaction program to check network integrity and timing characteristics, use the **ping sna** command in privileged EXEC mode.

ping sna [**-1**] [**-c** *consecutive-packets*] [**-i** *number-iterations*] [**-m** *mode*] [**-n**] [**-r**] [**-s** *size*] [**-t** *tpname*] [**-u** *userid* **-p** *password*] *destination*

Syntax Description

-1	(Optional) Sends data from client to server only (no echo).
-c *consecutive-blocks*	(Optional) Specifies the number of data blocks sent per iteration. The default is 1.
-i *number-iterations*	(Optional) Specifies the number of iterations. The default is 2.
-m *mode*	(Optional) Specifies the APPC mode to use. The default is #INTER.
-n	(Optional) Omits any security (SECURITY=NONE).
-r	(Optional) Displays the route taken by APPC PING.
-s *size*	(Optional) Specifies the size of the data block to be sent. The default is 100 bytes.
-t *tpname*	(Optional) Specifies transaction program (TP) to start on the server. The default is APINGD.
-u *userid*	(Optional) Specifies USERID.
-p *password*	(Optional) Specifies the password associated with the userid specified after **-u**. Required when **-u** is specified. Password must be one to eight characters in length.
destination	Specifies the fully qualified name of the destination logical unit or control point with which an APING transaction should be initiated.

Defaults

If **-1** is not specified, the **ping sna** command will send the quantity of data represented by the **-s** *size*, **-i** *number-iterations,* and **-c** *consecutive blocks* options. It will be first sent in the direction from the **ping sna** requester to the receiver, then in the opposite direction.

If **-c** is not specified, consecutive data blocks per iteration defaults to 1.

If **-i** is not specified, number of iterations defaults to 2.

If **-m** is not specified, the mode defaults to #INTER.

If **-s** is not specified, the size of each block of data transferred defaults to 100 bytes.

If **-t** is not specified, the default transaction program name on the receiver is APINGD.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XN	This command was introduced.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

The **ping sna** command requires the destination to support the APING transaction program for the ping to succeed.

Examples

The following is an example of the **ping sna** command contact the destination NETA.CP001:

```
Router# ping sna NETA.CP001
```

Related Commands

Command	Description
show snasw session	Displays the SNASw session objects.

pool

To define pool names for the TN3270 server and specify the number of screens and printers in each logical cluster, use the **pool** command in TN3270 server configuration mode. To remove a client IP pool, use the **no** form of this command.

pool *poolname* [**cluster layout** *layout-spec-string*]

no pool *poolname*

Syntax Description

poolname	Unique pool name that cannot exceed eight characters in length. Valid characters are (alphabetic characters are not case sensitive): • First character—Alphabetic (A–Z) and national characters "@", "#", and "$" • Second through eighth characters—Alphabetic (A–Z), numeric (0–9), and national characters "@", "#", and "$"
cluster layout *layout-spec-string*	(Optional) Name for the cluster and to indicate a cluster of logical unit (LU)s such as printers. The sum of the numbers must be less than or equal to 255. No spaces are used between the entries in the *layout-spec-string* argument. The default value is 1a.

Defaults

The default value for the *layout-spec-string* argument is 1a.

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.

Usage Guidelines

The **pool** and **allocate lu** commands enable the TN3270 server to know the relationships between screen and printer LUs. These commands are an alternative to the logical unit (LU) nailing feature that allows clients to be nailed to LUs.

The **pool** command is configured in the TN3270 scope. The **pool** command provides the pool names and the definitions of the number of screens and printers in one logical cluster. Each pool statement must have a unique pool name.

The TN3270 server validates pool names when configuring a pool name and when processing the name received on a CONNECT request from the client. The TN3270 server rejects an invalid name and truncates the name received in the CONNECT request from the client to eight characters or at an invalid character (whichever comes first) when processing the CONNECT request.

When using a **pool** command to create a cluster, use a combination of the following values in the *layout-spec-string* argument:

- s (screen)
- p (printer)
- a (any, or wildcard) (refers to a printer or a screen)

Examples

Use the following format to define the *layout-spec-string* argument, where the *decimal-num* argument is a decimal number from 1 to 255:

pool *poolname* **cluster layout** {*decimal-num***s**}{*decimal-num***p**}{*decimal-num***a**}

The total sum of the numbers must be less than or equal to 255. No spaces are used between the entries in the *layout-spec-string* argument. The default is 1a, which defines one screen or one printer. A screen, printer, or a wildcard definition cannot be followed by a definition of the same type. A screen definition can be followed only by a printer or wildcard. Similarly, a printer definition can be followed only by a wildcard or a screen definition.

The following are examples of invalid *layout-spec-string* values, and the corresponding corrected specification:

- A *layout-spec-string* of 3s6s is invalid. The correct specification is 9s.
- A *layout-spec-string* of 3s6p7a8a is invalid. The correct specification is 3s6p15a.
- A *layout-spec-string* of 255s10p is invalid. Although the decimal number for any portion of the *layout-spec-string* can be from 1 to 255, the total number across all parameters cannot exceed 255. To correct this example, you can reduce the screens to 245 as 245s10p.

The combination of a screen, printer, and wildcard constitute a group. The *layout-spec-string* argument can support a maximum of four groups.

Consider the following example:

```
pool CISCO cluster layout 2s3p4a5s6a7s8p9s
```

There are four groups in this definition: 2s3p4a, 5s6a, 7s8p and 9s.

Pools must be defined before any pool references under the listen points are defined. Also, pools must be defined before they are referenced by other statements in the configuration. Failure to define the pool before it is referenced will cause the referencing configuration to be rejected.

Pools that are deleted (using the **no** form of the command) will cause all statements referencing the pool to be deleted.

The following criteria apply to the creation of pool names and local addresses:

- Pool and LU names must be unique; they cannot be identical.
- Local address ranges for pools must not overlap.
- Local address ranges for LU pools must not overlap with the existing client nailing configuration.
- Pool configurations made while LUs are in use do not affect the current LU configuration.

The following example uses the **pool** command to create two pools, pcpool and unixpool:

```
tn3270-server
 pool pcpool cluster layout 4s1p
 pool unixpool cluster layout 49s1p
listen-point 10.20.30.40
 client ip 10.10.10.2 pool pcpool
 pu PU1 91903315 dlur
```

```
  allocate lu 1 pool pcpool clusters 50
pu PU2 91903345 dlur
  allocate lu 1 pool unixpool clusters 5
```

In this example, the pcpool contains a cluster of 4 screens and 1 printer per cluster. The total number of devices in a cluster cannot exceed 255, therefore the pcpool contains a total of 50 clusters with each cluster containing 5 LUs. Note that the remaining 5 LUs automatically go to the generic pool.

The unixpool contains 49 screens and 1 printer per cluster. The total number of devices in a cluster cannot exceed 255, therefore the unixpool contains a total of 5 clusters with each cluster containing 50 LUs. Again, note that the last 5 LUs automatically go to the generic pool.

Related Commands

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

preferred-nnserver

To specify a preferred network node (NN) as server, use the **preferred-nnserver** command in Dependent Logical Unit Requestor (DLUR) configuration mode. To remove the preference, use the **no** form of this command.

preferred-nnserver *name*

no preferred-nnserver

Syntax Description

name	Fully qualified name of an NN.

Defaults

No default behavior or values

Command Modes

DLUR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **preferred-nnserver** command is valid only on the virtual channel interface. Fully qualified names consist of two case-insensitive alphanumeric strings, separated by a period. However, for compatibility with existing Advanced Peer-to-Peer Networking (APPN) products, including virtual telecommunications access method (VTAM), the characters "#" (pound), "@" (at), and "$" (dollar) are allowed in the fully qualified name strings. Each string is from one to 8 characters long; for example, RA12.NODM1PP. The portion of the name before the period is the network entity title (NET) ID and is shared between entities in the same logical network.

When no preferred server is specified, the Dependent Logical Unit Requestor (DLUR) will request NN server support from the first suitable node with which it makes contact. If refused, it will try the next one, and so on.

If a preferred server is specified, then DLUR will wait a short time to allow a link to the preferred server to materialize. If the preferred server is not found in that time, any suitable node can be used.

DLUR will not relinquish the current NN server merely because the preferred server becomes available.

Examples

The following example selects SYD.VMX as the preferred NN server:

```
preferred-nnserver SYD.VMX
```

Related Commands

Command	Description
client pool	Nails clients to pools.

priority-list protocol bstun

To establish block serial tunnel (BSTUN) queueing priorities based on the BSTUN header, use the **priority-list protocol bstun** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

priority-list *list-number* **protocol bstun** *queue* [**gt** | **lt** *packetsize*] [**address** *bstun-group bsc-addr*]

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

Syntax Description

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

Defaults

Prioritize based on BSTUN header.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Examples

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

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

Related Commands

Command	Description
encapsulation bstun	Configures BSTUN on a particular serial interface.

priority-list protocol ip tcp

To establish block serial tunnel (BSTUN) or serial tunnel (STUN) queueing priorities based on the TCP port, use the **priority-list protocol ip tcp** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

priority-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*

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

Syntax Description

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

Defaults

The default *queue* value is **normal**.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **priority-list protocol stun address** command first. Priority settings created with this command are assigned to Synchronous Data Link Control (SDLC) ports.

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

Examples

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

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

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

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

Related Commands

Command	Description
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
encapsulation bstun	Configures BSTUN on a particular serial interface.
encapsulation stun	Enables STUN encapsulation on a specified serial interface.
priority-list protocol bstun	Establishes BSTUN queueing priorities based on the BSTUN header.
priority-list protocol stun address	Establishes STUN queueing priorities based on the address of the serial link.
stun route address tcp	Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for STUN.

priority-list protocol stun address

To establish serial tunnel (STUN) queueing priorities based on the address of the serial link, use the **priority-list protocol stun address** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

priority-list *list-number* **protocol stun** *queue* **address** *group-number address-number*

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

Syntax Description

list-number	Arbitrary integer from 1 to 16 that identifies the priority list selected by the user.
queue	Enables a priority queue type: Valid queue values and their equivalent priority queue type level are: • **high**—Priority queue type is high. • **medium**—Priority queue type is medium. • **normal**—Priority queue type is normal. • **low**—Priority queue type is low. The default *queue* value is **normal**.
group-number	Group number that is used in the **stun group** command.
address-number	Address of the serial link. For an Synchronous Data Link Control (SDLC) link, the format is a 1-byte hexadecimal value (for example, C1). For a non-SDLC link, the address format can be specified by the **stun schema** command.

Defaults

The default *queue* value is **normal**.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
priority-list protocol ip tcp	Establishes BSTUN or STUN queueing priorities based on the TCP port.
stun group	Places each STUN-enabled interface on a router in a previously defined STUN group.
stun route address interface serial	Forwards all HDLC traffic on a serial interface.
stun schema offset length format	Defines a protocol other than SDLC for use with STUN.

profile

To specify a name and a security protocol for a security profile or to modify a profile and enter profile configuration mode, use the **profile** command in security configuration mode. To remove this name and protocol specification, use the **no** form of this command.

profile *profilename* [**ssl** | **none**]

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

Syntax Description

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

Defaults

No default behavior or values

Command Modes

Security configuration

Command History

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

Usage Guidelines

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

Profile names cannot be duplicated.

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

Entering the **profile** command places the router in profile configuration mode. Entering the **no** form of the command places the user into the security configuration mode.

This command has no retroactive effect.

Examples

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

```
tn3270-server
 security
 profile LAM ssl
```

```
  keylen 40
  servercert slot0:lam
  certificate reload
listen-point 10.10.10.1
 sec-profile LAM
 pu DIRECT 012ABCDE tok 0 04
 no profile LAM none
```

Related Commands

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

pu (DLUR)

To create a physical unit (PU) entity that has no direct link to a host or to enter PU configuration mode, use the **pu** command in DLUR configuration mode. To remove the PU entity, use the **no** form of this command.

pu *pu-name idblk-idnum ip-address*

no pu *pu-name*

Syntax Description

pu-name	Name that uniquely identifies this PU.
idblk-idnum	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server enforces uniqueness only within the set of Dependent Logical Unit Requestor (DLUR) PUs.
ip-address	IP address that the clients should use as host IP address to map to logical unit (LU) sessions under this PU.

Defaults

No PU is defined.

Command Modes

DLUR configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

If the PU is already created, the **pu** *pu-name* command with no arguments places the router in PU configuration mode. In this mode you can modify an existing PU DLUR entity.

A typical usage for the IP address is to reserve an IP address per host application. For example, clients wanting to connect to Time Sharing Option (TSO) specify an IP address that will be defined with PUs that have LOGAPPL=TSO.

Examples

The following example defines three PUs. Two of the PUs share the same IP address and the third PU has a separate IP address:

```
pu p0  05D99001 192.195.80.40
pu p1  05D99002 192.195.80.40
pu p2  05D99003 192.195.80.41
```

Related Commands

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

pu (listen-point)

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

pu *pu-name idblk-idnum type adapter-number lsap* [**rmac** *rmac*] [**rsap** *rsap*] [**lu-seed** *lu-name-stem*]

no pu *pu-name*

Syntax Description

pu-name	Name that uniquely identifies this PU.
idblk-idnum	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server enforces uniqueness only within the set of Dependent Logical Unit Requestor (DLUR) PUs.
type	Internal adapter type on the Channel Interface Processor (CIP) card, which corresponds to the value specified in the **lan** internal LAN configuration command. The currently supported type is **token-adapter**.
adapter-number	Internal adapter interface on the CIP card, which is the same value specified in the **adapter** internal LAN configuration command.
lsap	Local service access point (SAP) number in hexadecimal, ranging from 04 to DE. The value must be even, and must be unique within the internal adapter so that no other 802.2 clients of that adapter, in the router or in a host, are allocated the same SAP. Other direct links from TN3270 server direct PUs may use the same value on the internal adapter as long as the remote MAC or SAP is different.
rmac *rmac*	(Optional) Remote MAC address. The remote MAC address in the form *xxxx.xxxx.xxxx* hexadecimal, specifying the MAC address of the remote host. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.
rsap *rsap*	(Optional) Remote SAP address. The remote SAP address is a one- or two-character hexadecimal string, ranging from 04 to FC, that specifies the SAP address of the remote host. The default is 04.
lu-seed *lu-name-stem*	(Optional) logical unit (LU) name that the client uses when a specific LU name request is needed. The format is *x...x*## or *x...x*### where *x...x* is an alphanumeric string. When ## is specified, it is replaced with the LU local address in hexadecimal digits to form the complete LU name. When ### is specified, decimal digits are used, padded with leading zeros to make three characters. The first *x* must be alphabetic and the entire string, including the # symbols, must not exceed eight characters in length.

Defaults

The default remote SAP address is 04 (hexadecimal).

Command Modes

Listen-point configuration

Command History

Release	Modification
11.2	This command was introduced.
11.2(18)BC	Listen-point PU configuration was added.
12.0(5)T	This command was integrated into Cisco IOS Releas12.0(5)T.

Usage Guidelines

The **pu** *pu-name* command is valid only on the virtual channel interface. If the PU is already created, the **pu** *pu-name* command with no arguments puts you in listen-point PU configuration mode, where you can modify an existing PU entity.

The **pu** listen-point command uses values that are defined in two other commands: the **lan** internal LAN configuration command and the **adapter** internal LAN configuration command. The **lan** *type* and **adapter** *adapter-number* values configured on the CIP internal LAN interface are used in the **pu** command.

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

Examples

The following example configures the TN3270 server to be active and has one PU, CAPPU1, trying to connect. An LU seed using hexadecimal digits is defined.

```
tn3270-server
pu CAPPU1 05D18101 token-adapter 3 04 rmac 4000.0501.0001 lu-seed CAP01L##
```

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

```
lan tokenring 0
 adapter 0 4000.0000.0001
 adapter 1 4000.0000.0002
tn3270-server
 listen-point 10.20.30.40
  pu PU1 05d00001 token-adapter 1 8 rmac 4000.0000.0001 rsap 4
```

Related Commands

Command	Description
adapter	Configures internal adapters.
lan	Configures an internal LAN on a CMCC adapter interface and enters internal LAN configuration mode.
listen-point	Defines an IP address for the TN3270 server.
show extended channel tn3270-server	Displays current server configuration parameters and the status of the PUs defined for the TN3270 server.

pu (TN3270)

To create a physical unit (PU) entity that has its own direct link to a host and enter PU configuration mode, use the **pu** command in TN3270 server configuration mode. To remove the PU entity, use the **no** form of this command.

pu *pu-name idblk-idnum ip-address type adapter-number lsap* [**rmac** *rmac*] [**rsap** *rsap*] [**lu-seed** *lu-name-stem*]

no pu *pu-name*

Syntax Description

pu-name	Name that uniquely identifies this PU.
idblk-idnum	Value of this argument must match the IDBLK-IDNUM value defined at the host. The value must be unique within the subarea; however, the TN3270 server generally cannot tell which remote hosts are in which subareas, so the server enforces uniqueness only within the set of Dependent Logical Unit Requestor (DLUR) PUs.
ip-address	IP address that the clients should use as host the IP address to map to logical unit (LU) sessions under this PU.
type	Internal adapter type on the Channel Interface Processor (CIP) card, which corresponds to the value specified in the **lan** internal LAN configuration command. The currently supported type is **token-adapter.**
adapter-number	Internal adapter interface on the CIP card, which is the same value specified in the **adapter** internal LAN configuration command.
lsap	Local service access point (SAP) number in hexadecimal, ranging from 04 to FC. The value must be an even number, and must be unique within the internal adapter so that no other 802.2 clients of that adapter, in the router or in a host, should be allocated the same SAP. Other direct links from TN3270 server direct PUs may use the same value on the internal adapter as long as the remote MAC or SAP is different.
rmac *rmac*	(Optional) Remote MAC address. The remote MAC address of the form *xxxx.xxxx.xxxx* hexadecimal, specifying the MAC address of the remote host. If not specified, a loopback link to another SAP on the same internal LAN adapter is assumed.
rsap *rsap*	(Optional) Remote SAP address. The remote SAP address is a one- or two-character hexadecimal string, ranging from 04 to FC, specifying the SAP address of the remote host. The default is 04.
lu-seed *lu-name-stem*	(Optional) logical unit (LU) name that the client uses when a specific LU name request is needed. The format is *x...x*## or *x...x*### where *x...x* is an alphanumeric string. When ## is specified, it is replaced with the LU local address in hexadecimal digits to form the complete LU name. When ### is specified, decimal digits are used, padded with leading zeros to make three characters. The first *x* must be alphabetic and the entire string, including the # symbols, must not exceed eight characters in length.

Defaults

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

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The **pu** *pu-name* command is valid only on the virtual channel interface. If the PU is already created, the **pu** *pu-name* command with no arguments puts you in PU configuration mode, where you can modify an existing PU entity.

The **pu** (TN3270) command uses values that are defined in two other commands: the **lan** internal LAN configuration command and the **adapter** internal LAN configuration command. The **lan** *type* and **adapter** *adapter-number* values configured on the CIP internal LAN interface are used in the **pu** command.

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

Examples

The following example configures the TN3270 server to be active, and has one PU, CAPPU1, trying to connect in. An LU seed using hexadecimal digits is defined.

```
tn3270-server
pu CAPPU1 05D18101 10.14.20.34 token-adapter 3 04 rmac 4000.0501.0001 lu-seed CAP01L##
```

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

```
lan tokenring 0
 adapter 0 4000.0000.0001
 adapter 1 4000.0000.0002
tn3270-server
 pu PU1 05d00001 10.0.0.1 token-adapter 1 8 rmac 4000.0000.0001 rsap 4
```

Related Commands

Command	Description
adapter	Configures internal adapters.
keylen	Specifies the maximum bit length for the encryption keys for SSL Encryption Support.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

pu dlur (listen-point)

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

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

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

Syntax Description

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

Defaults

No PU is defined.

Command Modes

Listen-point configuration

Command History

Release	Modification
11.2	This command was introduced.
11.2(18)BC	Listen-point PU configuration was added.

Release	Modification
12.0(5)T	This command was integrated in Cisco IOS Release 12.0 T.
12.1(5)T	This command was modified to add the **lu-seed** option and *lu-name-stem* argument. The Luseed naming format was modified.

Usage Guidelines

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

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

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

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

If the explicit LU names conflict, the TN3270 server will reject the PU configuration. If the implicit LU names (that is, the PU names) conflict, the TN3270 server will accept the PU definitions, but the LU names will consist of a modified, truncated version of the PU name and the local address. Valid and invlaid LU seed syntax is shown in Table 5.

Table 5 LU Seed Syntax

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

Examples

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

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

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

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

```
tn3270-server
 pool simple cluster layout 1s
 pool pcpool cluster layout 4s1p
 lu deletion named
 dlur neta.shek neta.mvsd
```

```
 lsap tok 15 04
   link she1 rmac 4000.b0ca.0016
listen-point 172.18.4.18
pu pu1 91903315 tok 16 08 lu-seed abc##pqr
  allocate lu 1 pool simple clusters 50
  allocate lu 100 pool pcpool clusters 10
pu pu2 91913315 dlur lu-seed pqr###
  allocate lu 10 pool pcpool clusters 5
  allocate lu 100 pool simple clusters 100
```

Related Commands

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

qllc accept-all-calls

To enable the router to accept a call from any remote X.25 device, use the **qllc accept-all-calls** command in interface configuration mode. To cancel the request, use the **no** form of this command.

qllc accept-all-calls

no qllc accept-all-calls

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

This command allows Qualified Logical Link Control (QLLC) to accept all inbound X.25 calls, provided that the QLLC Call User Data (CUD) is in the call packet and the destination X.121 address in the call packet matches the serial interface's configured destination X.121 address or subaddress. When this command is used, the source X.121 address need not be configured via an **x25 map qllc** command for the call to be accepted.

This command is applicable to QLLC support for data-link switching plus (DLSw+), Advanced Peer-to-Peer Networking (APPN), and downstream physical unit (DSPU). It is not applicable to QLLC support for source-route bridging (SRB) and remote source-route bridging (RSRB).

Examples

The following example enables QLLC connectivity for DLSw+ and allows QLLC to accept all inbound X.25 calls. Every X.25 connection request for X.121 address 0308 with QLLC CUD is directed to DLSw+. The first switched virtual circuit (SVC) to be established will be mapped to virtual MAC address 4000.0B0B.0001. If a call comes in with an X.121 address of 0308, the call will be forwarded to MAC address 4001.1161.1234.

```
interface serial 0
 encapsulation x25
 x25 address 0308
 qllc accept-all-calls
 qllc dlsw vmac 4000.0B0B.0001 500 partner 4001.1161.1234
```

Related Commands

Command	Description
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.

qllc dlsw

To enable data-link switching plus (DLSw+) over Qualified Logical Link Control (QLLC), use the **qllc dlsw** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

qllc dlsw {**subaddress** *subaddress* | **pvc** *pvc-low* [*pvc-high*]} [**vmac** *vmacaddr poolsize*] [**partner** *partner-macaddr*] [**sap** *ssap dsap*] [**xid** *xidstring*] [**npsi-poll**]

no qllc dlsw {**subaddress** *subaddress* | **pvc** *pvc-low* [*pvc-high*]} [**vmac** *vmacaddr poolsize*] [**partner** *partner-macaddr*] [**sap** *ssap dsap*] [**xid** *xidstring*] [**npsi-poll**]

Syntax Description

subaddress *subaddress*	An X.121 subaddress.
pvc	Map one or more permanent virtual circuits (PVCs) to a particular QLLC service (in this case DLSw+). QLLC will attempt to reach the partner by sending and ID.STN.IND to DLSw+.
pvc-low	Lowest logical channel number (LCN) for a range of X.25 PVCs. Acceptable values for PVCs are decimal numbers from 1 to 4095.
pvc-high	(Optional) Highest LCN. If not specified, the range of PVCs consists of just one PVC.
vmac *vmacaddr*	(Optional) Defines either the only virtual MAC address used for DLSw+ or the lowest virtual MAC address in a pool of virtual MAC addresses.
poolsize	(Optional) Specify the number of contiguous virtual MAC addresses that have been reserved for DLSw+. If the parameter is not present, then only one virtual MAC address is available.
partner *partner-macaddr*	(Optional) Virtual MAC address to which an incoming call wants to connect. The **qllc dlsw** command must be repeated for each different partner. Each partner is identified by a unique subaddress.
sap *ssap dsap*	(Optional) Overrides the default service access point (SAP) values (04) for a Token Ring connection. *dsap* refers to the partner's SAP address; *ssap* applies to the virtual MAC address that corresponds to the X.121 device.
xid *xidstring*	(Optional) Exchange identification (XID) format 0 type 2 string.
npsi-poll	(Optional) Inhibits forwarding a null XID on the X.25 link. Instead the Cisco IOS software will send a null XID response to the device that sent the null XID command.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

Any incoming call whose X.121 destination address matches the router's X.121 address and this subaddress will be dispatched to DLSw+ (with an ID.STN IND). If a router is providing several QLLC services, different subaddresses must be used to discriminate between them. Subaddresses can be used even if a remote X.25 device is not explicitly mapped to a specific virtual MAC address. This is most useful when PU 2.1 devices are connecting to a host because the X.25 device's control point name and network name are used to validate the connection, rather than some virtual MAC address. The subaddress is optional. If no subaddress is provided, any incoming call that matches the router's X.121 address will be dispatched to DLSw+. On outgoing calls the subaddress is concatenated to the interface's X.121 address.

When DLSw+ receives a Can You Reach inquiry about a virtual MAC address in the pool, the QLLC code will attempt to set up a virtual circuit to the X.121 address that maps to the virtual MAC address specified. If an incoming call is received, QLLC sends an ID.STN.IND with a virtual MAC address from the pool to DLSw+. If there is no virtual MAC address, then the **x25 map qllc** or **x25 pvc qllc** command must provide a virtual MAC address.

The **npsi-poll** keyword is needed to support PU 2.0 on the partner side that wants to connect to a front-end processor (FEP) on the X.25 side. In a Token Ring or DLSw+ environment, the PU 2.0 will send a null XID to the FEP. If the software forwards this null XID to an X.25 attached FEP, the FEP will assume that it is connecting to PU2.1, and will break off the connection when the PU 2.0 next sends an XID Format 0 Type 2.

Examples

The following commands assign virtual MAC address 1000.0000.0001 to a remote X.25-attached 3174, which is then mapped to the X.121 address of the 3174 (31104150101) in an X.25-attached router:

```
interface serial 0
 x25 address 3110212011
 x25 map qllc 1000.000.0001 31104150101
 qllc dlsw partner 4000.1161.1234
```

qllc largest-packet

To indicate the maximum size of the Systems Network Architecture (SNA) packet that can be sent or received on an X.25 interface configured for Qualified Logical Link Control (QLLC) conversion, use the **qllc largest-packet** command in interface configuration mode. To restore the default largest packet size, use the **no** form of this command.

qllc largest-packet *virtual-mac-addr max-size*

no qllc largest-packet *virtual-mac-addr max-size*

Syntax Description

virtual-mac-addr	Virtual MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
max-size	Maximum size, in bytes, of the SNA packet that can be sent or received on the X.25 interface configured for QLLC conversion. This value must agree with the value configured in the remote SNA device. The valid range is from 0 to 1024.

Defaults

Maximum size is 265 bytes.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

SNA packets that are larger than the largest value allowed on the X.25 connection and are received on the Logical Link Control, type 2 (LLC2) interface are segmented before being sent on the X.25 interface. When a segmented packet is received on the X.25 interface, it is passed immediately to the LLC2 interface, and no effort is made to wait for the segment to be completed.

When the remote X.25 device has a limit on the maximum total length of recombined X.25 segments it will support, you can use the **qllc largest-packet** command to ensure that the length is not exceeded. For example, a device whose maximum SNA packet size is limited to 265 bytes might not be able to handle a series of X.25 packets that it has to recombine to make a 4, 8, or 17 KM SNA packet, such as one often encounters in an LLC2 environment.

You use the **qllc largest-packet** command in conjunction with the **x25 map qllc** and **qllc srb** commands.

Note Do not configure the maximum SNA packet size on an X.25 interface to be larger than the maximum SNA packet size allowed on the LLC2 interface.

Consult your IBM documentation to set the maximum packet size on the remote X.25 device.

Examples

In the following example, the maximum packet size that has been established for the virtual circuit is used as the maximum packet size that can be sent or received on the X.25 interface:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
!
 qllc partner 0100.0000.0001 4000.0101.0132
 qllc xid 0100.0000.0001 01720001
 qllc largest-packet 0100.0000.0001 521
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc npsi-poll

To enable a connection between a physical unit (PU) 2 on the LAN side and a front-end processor (FEP) running Network Control Program (NCP) Packet Switching Interface (NPSI) on the X.25 side, use the **qllc npsi-poll** command in interface configuration mode. To disable this capability, use the **no** form of this command.

qllc npsi-poll *virtual-mac-addr*

no qllc npsi-poll *virtual-mac-addr*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

The **qllc npsi-poll** command is necessary only when the upstream device is a front-end processor (FEP) running NPSI and the downstream device is a PU 2.

This command is necessary because in a Token Ring or remote source-route bridging (RSRB) environment the LAN attached devices start up by sending a null exchange ID packet upstream. If the Cisco IOS software forwards this null exchange identification (XID) to an X.25-attached FEP, the FEP responds as if it were connecting to a PU2.1 device, and breaks the connection when the PU 2 next sends an XID Format 0 Type 2. The **qllc npsi-poll** command intercepts any null XID packet that the software receives on the LAN interface, and returns a null XID response to the downstream device. It continues to allow XID Format 3 and XID Format 0 packets through the X.25 device.

Examples

The following example facilitates a connection between a FEP running NPSI and a downstream PU 2.0:

```
qllc npsi-poll 0100.0000.0001
```

Related Commands

Command	Description
qllc srb	Enables Qualified Logical Link Control (QLLC) conversion on a serial interface configured for X.25 communication.
sdlc qllc-prtnr	Establishes correspondence between an Synchronous Data Link Control (SDLC) and QLLC connection.

Command	Description
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc partner

To enable a router configured for Qualified Logical Link Control (QLLC) conversion to open a connection to the local Token Ring device on behalf of the remote X.25 device when an incoming call is received, use the **qllc partner** command in interface configuration mode. To disable this capability, use the **no** form of this command.

qllc partner *virtual-mac-addr mac-addr*

no qllc partner *virtual-mac-addr mac-addr*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
mac-addr	48-bit MAC address of the Token Ring host that will communicate with the remote X.25 device.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

When the Cisco IOS software receives an incoming call from the designated X.121 address, it opens a Logical Link Control, type 2 (LLC2) connection with the device at the given MAC address. Both the MAC address of the Token Ring device and the virtual MAC address for the remote X.25 device with which it is to communicate are required in order for the software to initiate connections with the Token Ring device. This allows the Token Ring host to be permanently ready to accept a connection rather than requiring operator action at the host to initiate the connection with the X.25 device.

You must issue the **qllc partner** command for each remote X.25 device that will communicate with the local Token Ring host through this interface.

You use the **qllc partner** command in conjunction with the **x25 map qllc** and **qllc srb** commands.

Examples

In the following example, the **qllc partner** command is used to associate the virtual MAC address 0100.0000.0001, as defined in the previous **x25 map qllc** entry, with the MAC address of the Token Ring host that will communicate with the remote X.25 device:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
```

```
qllc partner 0100.0000.0001 4000.0101.0132
qllc xid 0100.0000.0001 01720001
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
sdlc qllc-prtnr	Establishes correspondence between an SDLC and QLLC connection.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc sap

To associate a service access point (SAP) value other than the default SAP value with a serial interface configured for X.25 communication and Qualified Logical Link Control (QLLC) conversion, use the **qllc sap** command in interface configuration mode. To return this SAP value to its default state, use the **no** form of this command.

qllc sap *virtual-mac-addr ssap dsap*

no qllc sap *virtual-mac-addr ssap dsap*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
ssap	Source SAP value. It can be a decimal number in the range from 2 to 254. The default is 4.
dsap	Destination SAP value. It can be a decimal number in the range from 2 to 254. The default is 4.

Defaults

The default source SAP value is 4.
The default destination SAP value is 4.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

A SAP can be viewed as a port through which a higher-layer application can communicate with its counterpart (peer) operating on another system. Although the standard SAP value for IBM devices is 4, other values are allowed.

You use the **qllc sap** command in conjunction with the **x25 map qllc** and **qllc srb** interface configuration commands.

Examples

In the following example, source SAP and destination SAP values of 2 are specified for the remote X.25 device at the X.121 address 31370054065:

```
interface serial 0
 x25 map qllc 31370054065 4000.0122.0001
 qllc srb 9 100
 qllc sap 4000.0122.0001 02 02
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc srb

To enable Qualified Logical Link Control (QLLC) conversion on a serial interface configured for X.25 communication, use the **qllc srb** command in interface configuration mode. To disable QLLC conversion on the interface, use the **no** form of this command.

qllc srb *virtual-mac-addr srn trn*

no qllc srb *srn trn*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. It must be 1 to 15 digits long.
srn	Source ring number. This value defines a virtual ring for all of the remote X.25 devices attached to the QLLC interface.
trn	Target ring number. It must be a virtual ring group that has been defined with the **source-bridge sdllc-local-ack** global configuration command.

Defaults

QLLC conversion is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Any number of QLLC conversion connections using the same X.25 serial interface can share a source ring. However, this source ring must be a unique hexadecimal ring number within the source-bridged network.

If the router has only one Token Ring interface and is bridging from the remote X.25 devices to this interface, then the *trn* value is the number of the ring on that Token Ring interface. If the router has several Token Ring interfaces and interconnects them by means of the **source-bridge sdllc-local-ack** command, then the *trn* value is the number of that virtual ring group, as assigned using the **source-bridge sdllc-local-ack**

Use the **qllc srb** command to associate the ring number and bridge number that have been assigned to the interface with a virtual ring group of which the interface will be a part. The serial interface appears to be a ring, or source ring number, on a source-route bridge network, and ties in to the virtual ring group, or target ring number. The target ring number provides access to other real rings that have been designated using the **source-bridge** global configuration command. Note that you can configure QLLC conversion on a router containing no Token Ring interface cards, such as a router connecting a serial-attached device to an X.25 public data network (PDN).

The **qllc srb** command automatically turns on the Logical Link Control, type 2 (LLC2) process with default values. To change any of the LLC2 parameters (described in the "LLC2 and Synchronous Data Link Control (SDLC) Commands" chapter in the *Cisco IOS Bridging and IBM Networking*

Configuration Guide.), apply their values to the serial interface that has been configured for QLLC conversion. This is done on the serial interface, even though LLC2 does not run on the serial interface, but on the virtual ring associated with the serial interface.

You use the **qllc srb** command in conjunction with the **x25 map qllc** command.

Examples

In the following example, the **qllc srb** command is used to define a virtual ring number of 201 for the remote X.25 device, and an actual or virtual ring number of 100 for the Token Ring interface:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
```

Related Commands

Command	Description
source-bridge	Configures an interface for source-route bridging (SRB).
source-bridge sdllc-local-ack	Activates local acknowledgment for SDLLC sessions on a particular interface.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

qllc xid

To associate an exchange ID (XID) value with the remote X.25 device that communicates through the Cisco IOS software using Qualified Logical Link Control (QLLC) conversion, use the **qllc xid** command in interface configuration mode. To disable XID processing for this address, use the **no** form of this command.

qllc xid *virtual-mac-addr xid*

no qllc xid *virtual-mac-addr xid*

Syntax Description

virtual-mac-addr	MAC address associated with the remote X.25 device, as defined using the **x25 map qllc** or **x25 pvc qllc** interface configuration command. This address is written as a dotted triple of four-digit hexadecimal numbers.
xid	Combined XID IDBLK and XID IDNUM you are associating with the X.25 device at this X.121 address. This hexadecimal value must be four bytes (eight digits) in length.

Defaults

XID processing is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

Most QLLC installations do not need the **qllc xid** configuration command. It is needed only if the remote X.25 device is not configured to send its own XID. This is only possible for a device that is attached via a permanent virtual circuit (PVC). Even so, most devices that are connected via X.25 will send their own XIDs. Use the **qllc xid** command when the Token Ring host requires login validation for security purposes and the remote X.25 device does not send an XID. The XID value is used to reply to XID requests received on the Token Ring Logical Link Control, type 2 (LLC2) side of the connection. XID requests and responses are usually exchanged before sessions are started. The XID response to the XID request from the Token Ring host will contain the information you configure using the **qllc xid** command. The host will check the XID response it receives with the IDBLK and IDNUM parameters (configured in virtual telecommunications access method [VTAM]). If they match, the Token Ring host will initiate a session with the router. If they do not match, the host will not initiate a session with the router.

You use the **qllc xid** command in conjunction with the **x25 map qllc** and the **qllc srb** commands.

Examples

In the following example, the X.25 device at X.121 address 31104150101 must use an XID IDBLK of 017 and XID IDNUM of 20001 to access the Token Ring host whose MAC address is associated with the remote X.25 device, as applied using the **sdllc partner** command:

```
interface serial 0
 encapsulation x25
 x25 address 31102120100
 x25 map qllc 0100.0000.0001 31104150101
 qllc srb 0100.0000.0001 201 100
!
 qllc partner 0100.0000.0001 4000.0101.0132
 qllc xid 0100.0000.0001 01720001
```

Related Commands

Command	Description
qllc srb	Enables QLLC conversion on a serial interface configured for X.25 communication.
sdllc partner	Enables device-initiated connections for SDLLC. Must be specified for the serial interface that links to the serial line device.
x25 map qllc	Specifies the X.121 address of the remote X.25 device with which communication is planned using QLLC conversion.
x25 pvc qllc	Associates a virtual MAC address with a PVC for communication using QLLC conversion.

queue-list protocol bstun

To customize block serial tunnel (BSTUN) queueing priorities based on the BSTUN header, use the **queue-list protocol bstun** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

queue-list *list-number* **protocol bstun** *queue* [**gt** | **lt** *packetsize*] [**address** *bstun-group bsc-addr*]

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

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the priority list selected by the user.
queue	Enables a priority queue type: Valid **queue** keyword values and their equivalent priority queue type level are: • **high**—Priority queue type is high. • **medium**—Priority queue type is medium. • **normal**—Priority queue type is normal. • **low**—Priority queue type is low.
gt | **lt** *packetsize*	(Optional) Output interface examines header information *and* packet size and places packets with the BSTUN header that match criteria (**gt** or **lt** specified packet size) on specified output.
address *bstun-group bsc-addr*	(Optional) Output interface examines header information and Bisync address and places packets with the BSTUN header that match Bisync address on the specified output queue.

Defaults

Prioritize based on BSTUN header.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Examples

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

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

Related Commands

Command	Description
encapsulation bstun	Configures BSTUN on a particular serial interface.

queue-list protocol ip tcp

To customize block serial tunnel (BSTUN) queueing priorities based on the TCP port, use the **queue-list protocol ip tcp** command in global configuration mode. To revert to normal priorities, use the **no** form of this command.

queue-list *list-number* **protocol ip** *queue* **tcp** *tcp-port-number*

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

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the priority list selected by the user.
queue	Enables a priority queue type: Valid **queue** keyword values and their equivalent priority queue type level are: • **high**—Priority queue type is high. • **medium**—Priority queue type is medium. • **normal**—Priority queue type is normal. • **low**—Priority queue type is low. The default *queue* value is **normal**.
tcp-port-number	BSTUN port and priority settings are as follows: • High—BSTUN port 1976 • Medium—BSTUN port 1977 • Normal—BSTUN port 1978 • Low—BSTUN port 1979 Serial tunnel (STUN) port and priority settings are as follows: • High—STUN port 1994 • Medium—STUN port 1990 • Normal—STUN port 1991 • Low—STUN port 1992

Defaults

The default *queue* value is **normal**.

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Examples

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

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

Related Commands

Command	Description
encapsulation bstun	Configures BSTUN on a particular serial interface.

response-time group

To configure a client subnet group for response-time measurements, use the **response-time group** TN3270 server configuration command. To remove a client subnet group from response-time measurements, use the **no** form of this command.

response-time group *name* [**bucket boundaries** *t1 t2 t3 t4*] [**multiplier** *m*]

no response-time group *name*

Syntax Description

name	Alphanumeric string for the response-time group name. The maximum length of the name is 24 characters. Lower or uppercase letters can be used.
bucket boundaries *t1 t2 t3 t4*	(Optional) Unsigned 32-bit quantity that defines a bucket boundary in tenths of seconds. For other types of client groups, the bucket boundaries and multiplier values are fixed to the following defaults: • Bucket boundaries—10, 20, 50, 100 • Multiplier—30
multiplier *m*	(Optional) Number, in the range from 1 to 5760, which when multiplied by the sample interval of 20 seconds, determines the collection interval.

Defaults

Bucket boundaries and the multiplier value are fixed to the following defaults:

- Bucket boundaries—10, 20, 50, 100
- Multiplier—30

Command Modes

TN3270 server configuration

Command History

Release	Modification
11.2(18)BC	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0 T.

Usage Guidelines

Multiple response-time groups can be configured within the scope of available memory. When this command is used, up to 1024 IP subnets can be defined per response-time group with the **client ip** command. All TN3270 clients belonging to subnets configured within a specific response-time group are added to the response-time group when they connect as clients.

If the IP address and mask combination already exists within any response-time group, the following error message is displayed:

```
Subnet 10.1.1.0 255.255.255.248 already exists in client group MYSUBNET
```

Examples

In the following example, the response-time group MYSUBNET is configured:

```
tn3270-server
response-time group MYSUBNET bucket boundaries 15 25 60 120 multiplier 35
 client ip 10.1.1.0 255.255.255.248
 client ip 10.1.2.0 255.255.255.248
```

Related Commands

Command	Description
client ip	Adds an IP subnet to a client subnet response-time group.
show extended channel tn3270-server response-time application	Displays information about application response-time client groups.
show extended channel tn3270-server response-time global	Displays information about the global response-time client group.
show extended channel tn3270-server response-time link	Displays information about host link response-time client groups.
show extended channel tn3270-server response-time listen-point	Displays information about listen point response-time client groups.
show extended channel tn3270-server response-time subnet	Displays information about Subnet response-time client groups.

rsrb remote-peer lsap-output-list

To define service access point (SAP) filters by local SAP (LSAP) address on the remote source-route bridging WAN interface, use the **rsrb remote-peer lsap-output-list** command in global configuration mode. To remove a SAP filter on the remote source-route bridging (RSRB) WAN interface, use the **no** form of this command.

rsrb remote-peer *ring-group* {**tcp** *ip-address* | **fst** *ip-address* | **interface** *name*} **lsap-output-list** *access-list-number*

no rsrb remote-peer *ring-group* {**tcp** *ip-address* | **fst** *ip-address* | **interface** *name*} **lsap-output-list** *access-list-number*

Syntax Description

ring-group	Virtual ring number of the remote peer.
tcp	TCP encapsulation.
ip-address	IP address.
fst	Fast Sequenced Transport (FST) encapsulation.
ip-address	IP address.
interface	Direct encapsulation.
name	Interface name.
access-list-number	Number of the access list.

Defaults

No filters are assigned.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example specifies SAP filters by LSAP address:

```
rsrb remote-peer 1000 tcp 10.108.2.30 lsap-output-list 201
```

Related Commands

Command	Description
priority-list protocol	Establishes queueing priorities based on the protocol type.
sap-priority	Defines a priority list on an interface.
sap-priority-list	Defines a priority list.

rsrb remote-peer netbios-output-list

To filter packets by NetBIOS station name on a remote source-route bridging WAN interface, use the **rsrb remote-peer netbios-output-list** command in global configuration mode. To remove a filter on an remote source-route bridging (RSRB) WAN interface, use the **no** form of this command.

rsrb remote-peer *ring-group* {**tcp** *ip-address* | **fst** *ip-address* | **interface** *type*} **netbios-output-list host** *name*

no rsrb remote-peer *ring-group* {**tcp** *ip-address* | **fst** *ip-address* | **interface** *type*} **netbios-output-list host** *name*

Syntax Description

ring-group	Virtual ring number of the remote peer.
tcp	TCP encapsulation.
fst	Fast Sequenced Transport (FST) encapsulation.
ip-address	IP address.
interface	Direct encapsulation.
type	Interface name.
name	Name of a NetBIOS access filter previously defined with one or more **netbios access-list host** global configuration commands.

Defaults

No filter is assigned.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example filters packets by NetBIOS station name:

```
rsrb remote-peer 1000 tcp 10.108.2.30 netbios-output-list host engineering
```

Related Commands

Command	Description
netbios access-list host	Assigns the name of the access list to a station or set of stations on the network. The NetBIOS station access list contains the station name to match, along with a permit or deny condition.
priority-list protocol	Establishes queueing priorities based on the protocol type.
sap-priority	Defines a priority list on an interface.
sap-priority-list	Defines a priority list.

sap-priority

To define a priority list on an interface, use the **sap-priority** command in interface configuration mode. To remove a priority list on an interface, use the **no** form of this command.

sap-priority *list-number*

no sap-priority *list number*

Syntax Description

list-number	Priority list number you specified in the **sap-priority-list** command.

Defaults

No priority list is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

The following example specifies priority list number 1:

```
sap-priority 1
```

Related Commands

Command	Description
sap-priority-list	Defines a priority list.
source-bridge	Configures an interface for source-route bridging (SRB).

sap-priority-list

To define a priority list, use the **sap-priority-list** command in global configuration mode. To remove a priority list, use the **no** form of this command.

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

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

Syntax Description

list-number	Arbitrary integer from 1 to 10 that identifies the priority list.
queue-keyword	Priority queue name or a remote source-route bridge TCP port name.
dsap *ds*	(Optional) Destination service access point address. The *ds* argument is a hexadecimal number.
ssap *ss*	(Optional) Source service access point address. The *ss* argument is a hexadecimal number.
dmac *dm*	(Optional) Destination MAC address. The *dm* argument *dm* is written as a dotted triple of four-digit hexadecimal numbers.
smac *sm*	(Optional) Source MAC address. The *sm* argument *sm* is written as a dotted triple of four-digit hexadecimal numbers.

Defaults

No priority list is defined.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

To give precedence to traffic on a particular Logical Link Control, type 2 (LLC2) session, you must specify all four keywords (**dsap**, **ssap**, **dmac**, and **smac**) to uniquely identify the LLC2 session.

Examples

The following example defines priority list 1 and specifies source service access point (SSAP) and destination service access point (DSAP) addresses:

```
sap-priority-list 1 high dsap 04 ssap 04
```

sdlc address

To assign a set of secondary stations attached to the serial link, use the **sdlc address** command in interface configuration mode. To remove an assigned secondary station use the **no** form of this command.

sdlc address *hexbyte* [**echo**] [**ack-mode**] [**xid-poll**] [**switched**] [**seconly**] [**xid-passthru**] [**passive**] [**K** *number*]

no sdlc address *hexbyte* [**echo**] [**ack-mode**] [**xid-poll**] [**switched**] [**seconly**] [**xid-passthru**] [**passive**] [**K** *number*]

Syntax Description

hexbyte	Hexadecimal number (base 16) that indicates the address of the serial link. The range is from 1 to ff. If ff is configured, the **ack-mode** option must be specified.
echo	(Optional) Treats non-echo and echo Synchronous Data Link Control (SDLC) addresses as the same address.
ack-mode	(Optional) Supports applications that require local termination of an SDLC connection with address FF. This option should be used only if you use the SDLC address ff as a regular (not a broadcast) address.
xid-poll	(Optional) Configures the router to send a null exchange identification (XID) to the Token Ring-attached host device. This tells the host device to start the session.
switched	(Optional) Configures the router to send an XID to an SDLC attached device. When the device answers, then a proxy XID is sent to the peer.
seconly	(Optional) Eliminates the need for counting PU4 lines on the Network Control Program (NCP) to determine the correct poll address. Because the router is always secondary, when **seconly** is coded, the polling address will be determined by the router.
xid-passthru	(Optional) Allows the router to pass the XID through the interface in both the host and end device's direction.
passive	(Optional) Causes the router to wait before sending a Set Normal Response (SNRM) until it receives an XID from the host. This keyword is valid only when the role is primary, and it requires the **sdlc partner** command with keyword **inbound** specified.
K number	(Optional) Specifies the maximum number of information frames (I-frames) that a router can send before it expects an acknowledgment from the end device. The minimum window-size is 1 and the maximum size is 7. The default is 7.

Defaults

No secondary stations are assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.0	The SDLC address **ack-mode** option was introduced.
11.3	The command was modified to include the **switched**, **passive**, **xid-poll**, and **xid-passthru** keywords.
11.3(T)	The command was modified to include the **seconly** keyword.
12.1(5)T	The **sdlc address** and **sdlc address ff ack-mode** commands were combined. The **K** keyword was added.

Usage Guidelines

To assign the IBM reserved address ff as a nonbroadcast valid local address, configure the **sdlc address** interface configuration command with a hexbyte value of *ff* and specify the **ack-mode** option. To deactivate, use the **no** form of the command.

Before you can use this command, you must specify the encapsulation on the interface on which you want to enable SDLC; then, establish the router link station role. Next, assign secondary station addresses using the **sdlc address** command. The addresses are given one per line in hexadecimal (base 16).

The **sdlc address ff ack-mode** command is used to support applications that require local termination on an SDLC connection with address ff. This command should be used only if you use the SDLC address ff as a regular (not a broadcast) address.

The optional **echo** keyword is valid only for TG interfaces. When you use the **echo** keyword, the *hexbyte* argument is the non-echo SDLC address.

The optional **passive** keyword is valid only when the role is primary. When you use the **passive** keyword, the **sdlc partner** command is required with keyword **inbound** specified.

Examples

The following example shows how to configure serial interface 0 with two SDLC secondary stations attached to it through a modem-sharing device with addresses C1 and C2:

```
interface serial 0
 encapsulation sdlc
 sdlc role primary
 sdlc address c1
        sdlc address c2
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
encapsulation sdlc-primary	Configures the router as the primary SDLC station if you plan to configure the SDLLC media translation feature.
encapsulation sdlc-secondary	Configures the router as a secondary SDLC station if you plan to configure the SDLLC media translation feature.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

Command	Description
stun route address tcp	Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for serial tunnel (STUN).
sdlc role	Establishes a router to be either a primary or secondary SDLC station.

sdlc dlsw

To attach Synchronous Data Link Control (SDLC) addresses to data-link switching plus (DLSw+), use the **sdlc dlsw** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

sdlc dlsw {*sdlc-address* | **default** | **partner** *mac-address* [**inbound** | **outbound**]}

no sdlc dlsw {*sdlc-address* | **default | partner** *mac-address* [**inbound** | **outbound**]}

Syntax Description

sdlc-address	SDLC addresses are in hexadecimal. Multiple addresses can be assigned. The valid range is from 1 to FE.
default	Allows the user to configure an unlimited number of SDLC addresses to DLSw+.
partner *mac-address*	MAC address for default partner
inbound	(Optional) Partner will initiate connection.
outbound	(Optional) Initiate connection to partner.

Defaults

No correspondence is defined between SDLC addresses and DLSw+.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Examples

The following command attaches SDLC address d2 to DLSw+:

```
sdlc dlsw d2
```

The following command attaches SDLC addresses d2, d5, e3, e4, e6, b1, c3, d4, a1 and a5:

```
sdlc dlsw d2 d5 e3 e4 e6 b1 c3 d4 a1 a5
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
sdlc address	Assigns a set of secondary stations attached to the serial link.
sdlc role	Establishes the router to be either a primary or secondary SDLC station.

sdlc dte-timeout

To adjust the amount of time a DTE interface waits for the DCE to assert a Clear To Send (CTS) signal before dropping a Request To Send (RTS), use the **sdlc dte-timeout** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc dte-timeout *unit*

no sdlc dte-timeout *unit*

Syntax Description

unit	Timeout wait interval in microseconds. The valid range is from 10 to 64000. Each unit is approximately 5 microseconds. The default is 10 units (approximately 50 microseconds).

Defaults

10 units (approximately 50 microseconds)

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use this command on an interface that is in half-duplex mode and that has been configured for DTE.

Examples

The following example sets the amount of time that the DTE waits for the DCE to assert a CTS to 100 units (approximately 500 microseconds):

```
sdlc dte-timeout 100
```

Related Commands

Command	Description
half-duplex	Specifies half-duplex mode on an Synchronous Data Link Control (SDLC) interface or on the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers.
half-duplex timer	Tunes half-duplex timers.

sdlc frmr-disable

To indicate that secondary stations on a particular serial link do not support Frame Rejects (FRMRs) or error indications, use the **sdlc frmr-disable** command in interface configuration mode. To specify that the secondary station does support FRMRs, use the **no** form of this command.

sdlc frmr-disable

no sdlc frmr-disable

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled, which means that secondary stations support FRMRs or error indications.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

FRMRs are error indications that can be sent to a Synchronous Data Link Control (SDLC) station indicating that a protocol error has occurred. Not all SDLC stations support FRMRs. If this command is enabled, when the Cisco IOS software receives an error, it drops the line by sending a disconnect request to the remote station.

Examples

In the following example, the software is set to drop the serial line when it receives a protocol error:

```
interface serial 0
 sdlc frmr-disable
```

Related Commands

Command	Description
show llc2	Displays the LLC2 connections active in the router.

sdlc holdq

To control the maximum number of packets that can be held in a buffer before being sent to a remote Synchronous Data Link Control (SDLC) station, use the **sdlc holdq** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc holdq *address queue-size*

no sdlc holdq *address queue-size*

Syntax Description

address	SDLC address for which you are specifying a queue size.
queue-size	Local send window size. The minimum is 1 packet. No maximum value has been established. The default is 200 packets.

Defaults

200 packets

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is particularly useful with the SDLC Logical Link Control. Cisco (SDLLC) feature that allows a SDLC Logical Link Control. Cisco (SDLLC)-speaking Systems Network Architecture (SNA) station on a Token Ring to communicate with an SDLC-speaking SNA station on a serial link. Frame sizes and window sizes on Token Rings are often much larger than those acceptable for serial links. The fact that serial links are often much slower than Token Rings often makes this problem worse. Therefore, temporary backlogs can exist in periods of high data transfer from the Token Ring station to the serial station. A buffer creates a holding place for backlogged frames waiting to be sent on the serial link. This command is specified for each SDLC address, and therefore, for each SDLC secondary station on the serial link.

Examples

The following example shows how to change the output hold queue length to 30 frames on an SDLC station of address C1 off serial interface 0:

```
interface serial 0
 encapsulation sdlc-primary
 sdlc address c1
 sdlc holdq c1 30
```

Related Commands

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

sdlc k

To set the window size in order to control the maximum number of information frames the Cisco IOS software sends before it must stop sending and wait for an acknowledgment from the receiving router, use the **sdlc k** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc k *window-size*

no sdlc k *window-size*

Syntax Description

window-size	Local send window size. The minimum is one frame. The maximum is seven frames, which is the default.

Defaults

Seven frames

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When the Cisco IOS software is communicating with Synchronous Data Link Control (SDLC), it must have a parameter that controls the maximum number of information frames it will send before it must stop sending and wait for an acknowledgment. The **k** parameter keyword controls this window of acceptable frames. Use this command in conjunction with the **sdlc n1** command to create a balance between frame checking and network performance.

Examples

In the following example, the software can send up to five frames before it must receive an acknowledgment:

```
! enter a global command, if you have not already
interface tokenring 0
!send up to 5 frames, then wait for acknowledgment
 sdlc k 5
```

Related Commands

Command	Description
sdlc n1	Controls the maximum size of an incoming frame.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc line-speed

To enable adaptive Synchronous Data Link Control (SDLC) T1, use the **sdlc line-speed** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

sdlc line-speed *rate*

no sdlc line-speed *rate*

Syntax Description

rate	Clock rate in bits per second.

Defaults

No default rate

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command is used to calculate the adjusted SDLC T1 value. The adjusted T1 is used to compensate for the delay between the time the system software passes a packet to the microcode, and the time the packet is actually sent out on the line. For a DCE device, this should be equal to the clock rate on the interface. For a DTE device, it should be equal to the clock rate on the DCE device to which the DTE is connected.

Examples

In the following example, the SDLC line-speed rate is set to rate:

```
sdlc line-speed rate
```

Related Commands

Command	Description
sdlc n2	Determines the number of times that the Cisco IOS software resends a frame before terminating the SDLC session.
sdlc t1	Controls the amount of time the Cisco IOS software waits for an acknowledgment to a frame or sequence of frames.

sdlc n1

To control the maximum size of an incoming frame, use the **sdlc n1** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc n1 *bit-count*

no sdlc n1 *bit-count*

Syntax Description

bit-count	Number indicating bit size. Frames that exceed this size are rejected. The minimum is 1 bit. The maximum value depends on the configured maximum maximum transmission unit (MTU) value for the interface. The default is 12000 bits.

Defaults

12000 bits

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use with the **sdlc k** command to reduce network overhead while continuing to check the sending of frames.

The formula for determining the maximum allowed value for the *bit-count* argument is the maximum MTU value of the interface + 2 bytes (for the Synchronous Data Link Control [SDLC] header) multiplied by 8 (to convert from bytes to bits). For example, if the maximum MTU of the interface is 1500 bytes, then the largest value for the *bit-count* argument is (1500 + 2) * 8 = 12016 bits. Usually, the default maximum MTU size is 1500 bytes, but it can be configured as high as 18,000 bytes.

Examples

In the following example, the Cisco IOS software rejects frames larger than 10,000 bits:

```
interface serial 0
 sdlc n1 10000
```

Related Commands

Command	Description
sdlc k	Sets the window size in order to control the maximum number of information frames the Cisco IOS software sends before it must stop sending and wait for an acknowledgment from the receiving router
show llc2	Displays the LLC2 connections active in the router.

sdlc n2

To determine the number of times that the Cisco IOS software resends a frame before terminating the Synchronous Data Link Control (SDLC) session, use the **sdlc n2** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc n2 *retry-count*

no sdlc n2 *retry-count*

Syntax Description

retry-count	Number of retry attempts. When this number is exceeded, the SDLC station terminates its session with the other station. The minimum is 1 and the maximum is 255. The default is 20 retries.

Defaults

20 retries

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Use the **sdlc n2** command with the **sdlc t1** command to reduce network overhead while continuing to check the sending of data.

Examples

In the following example, the software is set to drop an SDLC station after five unsuccessful attempts to receive an acknowledgment for a frame:

```
interface serial 0
 sdlc n2 5
```

Related Commands

Command	Description
sdlc t1	Controls the amount of time the Cisco IOS software waits for an acknowledgment to a frame or sequence of frames.
show llc2	Displays the LLC2 connections active in the router.

sdlc partner

To specify the destination address with which a Logical Link Control (LLC) session is established for the Synchronous Data Link Control (SDLC) station, use the **sdlc partner** command in interface configuration mode. To cancel the configuration, use the **no** form of this command.

sdlc partner *mac-address sdlc-address* {**inbound** | **outbound**}

no sdlc partner *mac-address sdlc-address* {**inbound** | **outbound**}

Syntax Description

mac-address	The 48-bit MAC address of the Token Ring host.
sdlc-address	SDLC address of the serial device that will communicate with the Token Ring host. The valid range is from 1 to FE.
inbound	Prevents the router from sending proxy exchange identification (XID)s to the remote end station on behalf of the station specified. The remote end station must initiate the connection. When the router is configured for SDLC role secondary, the default is inbound (the router does not send proxy XIDs until it is polled). The **inbound** keyword is required if you want the router to wait before sending an SNRM until it receives an XID from the host. See the **passive** keyword on the **sdlc address** command for more details.
outbound	Causes the router to send proxy XIDs to the partner end station. If the remote end station responds, then (for physical unit [PU] 2.1 local devices) a NULL XID is sent on the SDLC line. The default behavior for SDLC role primary is outbound, and for SDLC role secondary is inbound.

Defaults

No partner is defined.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
11.2	The following keywords were added: • **inbound** • **outbound**

Usage Guidelines

The **inbound** keyword prevents unwanted messages on the host operator console from inbound XIDs to inactive virtual telecommunications access method (VTAM) Switched Major Nodes. It directs SDLC to not send Test or XID frames to the host, front-end processor (FEP), or 3172 even after the connection to a downstream PU2 is complete. The **inbound** keyword is required for System88 support.

Examples

The following example establishes the correspondence between an SDLC and Qualified Logical Link Control (QLLC) connection:

```
sdlc partner 1000.5aed.1f53 d2 inbound
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
sdlc address	Assigns a set of secondary stations attached to the serial link.
sdlc dlsw	Attaches SDLC addresses to data-link switching plus (DLSw+).
sdlc vmac	Configures a MAC address for the serial interface.

sdlc poll-limit-value

To control how many times a single secondary station can be polled for input before the next station must be polled, use the **sdlc poll-limit-value** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc poll-limit-value *count*

no sdlc poll-limit-value *count*

Syntax Description

count	Number of times the Cisco IOS software can poll one secondary station before proceeding to the next station. The valid range is from 1 through 10. The default is 1.

Defaults

1 time

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

As is typical for the primary station of an Synchronous Data Link Control (SDLC) connection, if a secondary station sends its full possible window of input to the primary router or access server, the Cisco IOS software immediately will re-poll the same secondary for more data in an attempt to capture the complete transaction at one time. The **sdlc poll-limit-value** command indicates how many times this can happen before the next station in the poll loop must be polled.

Increasing the value allows for smoother transaction processing but can delay polling of other stations or giving output to other stations.

Examples

The following example specifies that the router can be polled two times before the next station in the poll list must be polled:

```
! enter a global command, if you have not already
interface serial 4
 no ip address
! use stun encapsulation
encapsulation stun
! establish stun group 4 on interface serial 4
 stun group 4
 stun sdlc-role primary
! poll the router up to two times before polling the next station
 sdlc poll-limit-value 2
```

Related Commands

Command	Description
sdlc poll-pause-timer	Controls how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc poll-pause-timer

To control how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface, use the **sdlc poll-pause-timer** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc poll-pause-timer *milliseconds*

no sdlc poll-pause-timer *milliseconds*

Syntax Description

milliseconds	Number of milliseconds (ms) that the software waits before sending the poll frame to a single serial interface. This is a number in the range from 1 to 10000. The default is 10 ms.

Defaults

10 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

As is typical for the primary station of a Synchronous Data Link Control (SDLC) connection, the software generates polls periodically to each of the secondary stations to solicit their input. After polling each station on a single serial interface, the software will pause before beginning to poll the next station.

Because the secondaries cannot send data until they are polled, increasing this timer value can increase response time to the users. However, making this value too small can flood the serial link with unneeded polls and require the secondary stations to spend wasted CPU time processing them.

Examples

In the following example, the software pauses 2000 ms before sending a series of poll frames through serial interface 4:

```
! enter a global command, if you have not already
interface serial 4
no ip address
! use STUN encapsulation
 encapsulation stun
! establish stun group 4 on interface serial 4
 stun group 4
!
 stun sdlc-role primary
! wait 2000 milliseconds before sending each series of poll frames
 sdlc poll-pause-timer 2000
```

Related Commands

Command	Description
sdlc poll-limit-value	Controls how many times a single secondary station can be polled for input before the next station must be polled.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc poll-wait-timeout

To specify the interval the Cisco IOS software will wait for polls from a primary node before timing out that connection when the router has been configured for local acknowledgment and some form of Synchronous Data Link Control (SDLC) communication (SDLLC or serial tunnel [STUN], for example), use the **sdlc poll-wait-timeout** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc poll-wait-timeout *milliseconds*

no sdlc poll-wait-timeout *milliseconds*

Syntax Description

milliseconds	Number of milliseconds the software will wait for a poll from the primary station before timing out the connection to the primary station. The minimum is 10 ms and the maximum is 64000 ms. The default is 10000 ms.

Defaults

10000 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command can be used on an interface that has been configured as a secondary node, but is not to be used on an interface that has been configured as a primary node.

In a locally acknowledged multidrop environment, the polls the primary node sends to the router can be delayed because the primary node is busy polling other secondary nodes. In such situations, this command can be used to extend the timeout, thus reducing the likelihood the Cisco IOS software times out the connection to the primary node.

Examples

The following example specifies that the local software will wait an interval of 63,000 ms for a poll from a primary station before timing out:

```
! sample stun peer-name global command
stun peer-name 10.136.134.86
! sample protocol-group command
stun protocol-group 4 sdlc
!
interface serial 0
! sample ip address command
 no ip address
! sample encapsulation stun command
 encapsulation stun
! place interface serial0 in previously defined STUN group 4
 stun group 4
```

```
! must enter the next command to use the sdlc poll-wait-timeout command
 stun sdlc-role secondary
! set timeout period for polls from primary station to 63000 milliseconds.
 sdlc poll-wait-timeout 63000
! list the addresses of the sdlc stations on the link
 sdlc address C1
 sdlc address C2
! provide stun route command
 stun route address C2 tcp 10.136.134.58
 stun route address C1 tcp 10.136.134.58
```

Related Commands

Command	Description
sdlc poll-limit-value	Controls how many times a single secondary station can be polled for input before the next station must be polled.
sdlc poll-pause-timer	Controls how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface.

sdlc qllc-prtnr

To establish correspondence between a Synchronous Data Link Control (SDLC) and Qualified Logical Link Control (QLLC) connection, use the **sdlc qllc-prtnr** command in interface configuration mode. To deactivate the command, use the **no** form of this command.

sdlc qllc-prtnr *virtual-mac-address sdlc-address*

no sdlc qllc-prtnr *virtual-mac-address sdlc-address*

Syntax Description

virtual-mac-address	The virtual MAC address in the form *h.h.h.*
sdlc-address	SDLC address in hexadecimal. The valid range is from 1 to FE.

Defaults

No correspondence is defined.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following example establishes the correspondence between an SDLC and QLLC connection:

```
sdlc qllc-prtnr 4000.0122.0001 c1
```

Related Commands

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

sdlc role

To establish the router to be either a primary or secondary Synchronous Data Link Control (SDLC) station, use the **sdlc role** command in interface configuration mode. To cancel the designation, use the **no** form of this command.

sdlc role {**none** | **primary** | **secondary** | **prim-xid-poll**}

no sdlc role {**none** | **primary** | **secondary** | **prim-xid-poll**}

Syntax Description

none	Establishes the router as either a primary or secondary station, depending on the end stations.
primary	Establishes the router as a primary station.
secondary	Establishes the router as a secondary station.
prim-xid-poll	Establishes the router as a primary station when the end station is configured as a secondary NT2.1.

Defaults

No default role is assigned.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If the role is **none**, the router can be either primary or secondary, depending on the end stations. The SDLC end station must be configured as negotiable or primary NT2.1. When the end stations are configured as physical unit type 2 (physical unit [PU] 2), you can set the role of the interface to **primary** or **secondary**. When the end station is configured as secondary NT2.1, you must set the role of the interface to **prim-xid-poll**.

To configure an SDLC multidrop line (downstream), configure the SDLC role as follows:

- **primary** if all SDLC devices are type PU 2.0 or mixed PU 2.0 and 2.1
- **prim-xid-poll** if all devices are type PU 2.1

Examples

The following example configures the router as a primary SDLC station:

```
interface serial 2/6
 no ip address
 encapsulation sdlc
 fras map sdlc c1 serial 2/0 frame-relay 32 4 4
 sdlc role primary
 sdlc address c1
 sdlc xid c1 01700001
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.

sdlc saps

To configure Synchronous Data Link Control (SDLC)-to-Logical Link Control (LLC) sessions with respect to the source service access point (SSAP) and destination service access point (DSAP) on the LLC, use the **sdlc saps** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

sdlc saps *address ssap dsap*

no sdlc saps *address ssap dsap*

Syntax Description

address	Address of the SDLC station that will communicate with the router. Valid range is from 1 to FF.
ssap	SSAP of the partner. Valid range is from 1 to FF. The default is 04.
dsap	DSAP of the partner. Valid range is from 1 to FF. The default is 04.

Defaults

The default value for both the *ssap* and *dsap* arguments is 04.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

The following example configures SDLC address 01, SSAP 08, and DSAP 08.

```
sdlc saps 01 08 08
```

sdlc sdlc-largest-frame

To indicate the largest information frame (I-frame) size that can be sent or received by the designated Synchronous Data Link Control (SDLC) station, use the **sdlc sdlc-largest-frame** command in interface configuration mode. To return to the default value, use the **no** form of this command.

sdlc sdlc-largest-frame *address size*

no sdlc sdlc-largest-frame *address size*

Syntax Description

address	Address of the SDLC station that will communicate with the router.
size	Largest frame size that can be sent or received. The default is 265 bytes.

Defaults

The default size for the largest I-frame is 265 bytes.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

In the following example, the Cisco IOS software can send or receive a frame as large as 265 bytes (the default) from the SDLC station at address C6. Any frames larger will be fragmented by the software.

```
interface serial 4
 sdlc sdlc-largest-frame c6 265
```

sdlc simultaneous

To enable an interface configured as a primary Synchronous Data Link Control (SDLC) station to operate in two-way simultaneous mode, use the **sdlc simultaneous** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc simultaneous [**full-datamode** | **half-datamode**]

no sdlc simultaneous [**full-datamode** | **half-datamode**]

Syntax Description

full-datamode	(Optional) Enables the primary station to send data to and receive data from the polled secondary station.
half-datamode	(Optional) Prohibits the primary station from sending data to the polled secondary station.

Defaults

Two-way simultaneous mode is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

By default, the SDLC driver supports alternative mode. This means that in a multidrop environment, the primary station cannot send data to another secondary station until it receives a response (F bit) from the secondary station with which it is communicating.

In contrast, two-way simultaneous mode enables the interface configured as a primary SDLC station to send data to a second secondary station, even when it is receiving data from another secondary station. This capability improves utilization of a full-duplex serial line.

Examples

The following example enables all primary stations to send and receive data at the same time:

```
sdlc simultaneous full-datamode
```

The following example enables all secondary stations to send or receive data at the same time:

```
sdlc simultaneous half-datamode
```

Related Commands

Command	Description
encapsulation sdlc-primary	Configures the router as the primary SDLC station if you plan to configure the SDLLC media translation feature.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc slow-poll

To enable the slow-poll capability of the router as a primary Synchronous Data Link Control (SDLC) station, use the **sdlc slow-poll** command in interface configuration mode. To disable slow-poll capability, use the **no** form of this command.

sdlc slow-poll *seconds*

no sdlc slow-poll

Syntax Description

seconds	Amount of time in seconds. The default is 10 seconds.

Defaults

10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You can use this command to improve the performance of a multidropped SDLC configuration when one or more of the secondary stations are inactive.

When slow-poll is enabled, if the router acting as a primary station detects that a secondary SDLC station is not responding, it polls that secondary SDLC station less frequently. The router spends less time waiting for the inactive secondary station to respond, thereby minimizing the performance degradation on the active secondary SDLC stations on the multidropped line.

Examples

The following example enables the slow-poll capability:

```
interface serial 0
 sdlc slow-poll
```

Related Commands

Command	Description
sdlc poll-limit-value	Controls how many times a single secondary station can be polled for input before the next station must be polled.
sdlc poll-pause-timer	Controls how long the Cisco IOS software pauses between sending each poll frame to secondary stations on a single serial interface.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc snrm-timer

To specify a Set Normal Response (SNRM) timer that is different from the T1 response time, set the Synchronous Data Link Control (SDLC) SNRM timer using the **sdlc snrm-timer** command in interface configuration mode. To deactivate, use the **no** form of this command.

sdlc snrm-timer *number*

no sdlc snrm-timer *number*

Syntax Description

number	Specifies the time to wait for a reply to a SNRM frame in milliseconds, and is enabled only if the station role is primary. range is from 1 to 64000 ms, and default is the **no** form of the command.

Defaults

No default behavior or values

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use the SNRM timer only if you want to have a unique timeout period to wait for a reply to an SNRM.

The **sdlc snrm-timer** command is used to specify the time to wait for a reply to an SNRM frame in milliseconds. This command is enabled only if the station role is primary.

Examples

The following configuration defines serial interface 0 as the primary SDLC station with two SDLC secondary stations, C1 and C2, attached to it through a modem-sharing device. SDLC simultaneous half-datamode is enabled, and the time to wait for a reply to a SNRM frame is 2500 ms.

```
interface serial 0
 encapsulation sdlc
 sdlc role primary
 sdlc address c1
 sdlc address c2
 sdlc simultaneous half-datamode
 sdlc snrm-timer 2500
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.
sdlc n2	Sets the number of times the Cisco IOS software will retry an operation that has timed out.

Command	Description
sdlc role primary	Establishes the router as a primary SDLC station.
sdlc simultaneous	Enables an interface configured as a primary SDLC station to operate in two-way simultaneous mode.
sdlc t1	Controls the amount of time the Cisco IOS software waits for a reply.

sdlc t1

To control the amount of time the Cisco IOS software waits for an acknowledgment to a frame or sequence of frames, use the **sdlc t1** command in interface configuration mode. To revert to the default setting, use the **no** form of this command.

sdlc t1 *milliseconds*

no sdlc t1 *milliseconds*

Syntax Description

milliseconds	Number of milliseconds that the software waits. The minimum is 1 ms and the maximum is 64000 ms. The default is 3000 ms.

Defaults

3000 ms

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

When an Synchronous Data Link Control (SDLC) station sends a frame, it waits for an acknowledgment from the receiver that the frame has been received. The sending station cannot wait indefinitely for a response. When the frame is sent, a timer is started. To be consistent with the original specification of SDLC, this timer is called the T1 timer and is controlled by this parameter. If this timer reaches its limit before the acknowledgment is received, the software will try again and resend the frame.

Examples

In the following example, the software waits up to 4000 ms for a reply to a frame or sequence of frames:

```
! enter a global command, if you have not already
interface tokenring 0
 sdlc t1 4000
```

Related Commands

Command	Description
sdlc n2	Determines the number of times that the Cisco IOS software resends a frame before terminating the SDLC session.
show llc2	Displays the Logical Link Control, type 2 (LLC2) connections active in the router.

sdlc test serial

To determine the status of end stations, use the **sdlc test serial** command in user EXEC or privileged EXEC mode. To halt the sending of the test frames, use the **sdlc test serial** command with the **stop** keyword.

sdlc test serial *number address* [*iterations* | **continuous** | **stop** | **string** *string*]

Syntax Description

number	Serial interface on which the test frame is to be sent out.
address	Synchronous Data Link Control (SDLC) address (in hexadecimal) of the end station to receive the test frame.
iterations	(Optional) Number of test frames to be sent. The valid range is from 1 to 25 frames. The default is 10 frames.
continuous	(Optional) Sends frames continuously until the **sdlc test serial** command is issued with the **stop** keyword.
stop	(Optional) Halts the sending of test frames.
string *string*	(Optional) Specifies a string of characters as data within the test frame. If this option is not specified, the default test string is ABCDEFGHIJKLMNOPQRSTUVWXYZ.

Defaults

The **sdlc test serial** command is not active.
The default number of test frames sent is 10.
The default test string is ABCDEFGHIJKLMNOPQRSTUVWXYZ.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The command will precheck for correct interface and SDLC address. The results of the test frames sent can be displayed after the frames have been sent or an **sdlc test serial** command with the **stop** keyword has been issued.

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

Examples

The following are variations of the **sdlc test serial** command, followed by the response for each:

```
Router# sdlc test serial 0 c1

SDLC Test for address C1 completed
Frames sent=10 Frames received=10
```

```
Router# sdlc test serial 0 c1 255

SDLC Test for address C1 completed
Frames sent=255 Frames received=255

Router# sdlc test serial 0 C1 stop

SDLC Test for address C1 completed
Frames sent=44 Frames received=44

Router# sdlc test serial 0 c1 string Thestuffofdreams

SDLC Test for address C1 completed
Frames sent=10 Frames received=10
```

Related Commands

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

sdlc virtual-multidrop

To allow Synchronous Data Link Control (SDLC) broadcast address FF to be replicated for each of the serial tunnel (STUN) peers, so that each of the end stations receives the broadcast frame, use the **sdlc virtual-multidrop** command in interface configuration mode. To disable the SDLC broadcast feature, use the **no** form of this command.

sdlc virtual-multidrop

no sdlc virtual-multidrop

Syntax Description

This command has no arguments or keywords.

Defaults

SDLC broadcast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Examples

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

```
sdlc virtual-multidrop
```

Related Commands

Command	Description
stun route address tcp	Specifies TCP encapsulation and optionally establishes SDLC local acknowledgment (SDLC transport) for STUN.

sdlc vmac

To configure a MAC address for the serial interface, use the **sdlc vmac** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

sdlc vmac *mac-address*

no sdlc vmac *mac-address*

Syntax Description

mac-address	48-bit MAC address of the Token Ring host.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

This command must be configured if you will configure data-link switching plus (DLSw+). The last byte of the address must be 00.

Examples

The following example specifies a MAC address for the serial interface:

```
sdlc vmac 1234.3174.0000
```

Related Commands

Command	Description
encapsulation sdlc	Configures an Synchronous Data Link Control (SDLC) interface.
sdlc dlsw	Attaches SDLC addresses to DLSw+.

sdlc xid

To specify an exchange identification (XID) value appropriate for the designated Synchronous Data Link Control (SDLC) station associated with this serial interface, use the **sdlc xid** command in interface configuration mode. To disable XID processing for this address, use the **no** form of this command.

sdlc xid *address xid*

no sdlc xid *address xid*

Syntax Description

address	Address of the SDLC station associated with this interface.
xid	XID the Cisco IOS software will use to respond to XID requests the router receives. This value must be 4 bytes (8 digits) in length and is specified with hexadecimal digits.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

XID requests and responses are usually exchanged before sessions are started. Be sure that the XID value configured in the Cisco IOS software matches the IDBLK and IDNUM parameters configured on the host. The XID response to an XID request will contain the information you configured in the **sdlc xid** command. The host will check the XID response it receives with the IDBLK and IDNUM parameters (that are configured in the virtual telecommunications access method [VTAM]). If they match, the host will initiate a session with the router. If they do not match, the host will not initiate a session.

Examples

The following example specifies an XID value of 01720002 at address C2:

```
interface serial 0
 sdlc xid c2 01720002
```

Related Commands

Command	Description
encapsulation sdlc	Configures an SDLC interface.

sdlc xid-pause-timer

To control the frequency of exchange identification (XID) retries between a router and an upstream virtual telecommunications access method (VTAM), use the **sdlc xid-pause-timer** command in interface configuration mode. To restore the default timer value, use the **no** form of this command.

sdlc xid-pause-timer *time*

no sdlc xid-pause-timer *time*

Syntax Description

time	Length of time the router is to wait, in seconds, before sending the next retry XID. The valid range is from 10 to 300 seconds. The default is 10 seconds.

Defaults

The default XID pause timer value is 10 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

When a router attempts to send an XID upstream to VTAM, and the switched major node is down, the router continues to send retry XIDs at 10-second intervals. If many other routers are also attempting to send retry XIDs to VTAM, the resulting XID flood can cause problems. The **sdlc xid-pause-timer** command enables you to control the interval between router XID retries.

Examples

The following example specifies an XID pause timer value of 60 seconds:

```
interface serial 0
 sdlc xid-pause-timer 60
```

sdllc partner

To enable device-initiated connections for SDLC Logical Link Control. Cisco (SDLLC), use the **sdllc partner** command in interface configuration mode. This command must be specified for the serial interface that links to the serial line device. To cancel the original instruction, use the **no** form of this command.

sdllc partner *mac-address sdlc-address*

no sdllc partner *mac-address sdlc-address*

Syntax Description

mac-address	MAC address of the Token Ring host.
sdlc-address	Synchronous Data Link Control (SDLC) address of the serial device that will communicate with the Token Ring host.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Both the MAC address of the Token Ring host and the SDLC serial line address must be configured to initiate connections with the Token Ring host.

The Token Ring host and the serial device communicate with each other through the Cisco IOS software. Although the device is said to initiate connections, the software actually initiates connections with the Token Ring host on behalf of the serial device. As part of Cisco's SDLLC implementation, the serial device "thinks" that it is communicating with a host also on a serial line. It is actually the software that does all the frame and protocol conversions between serial and Token Ring devices.

There are two conditions under which the Cisco IOS software will attempt to initiate a connection to a host on behalf of a serial device:

- When the serial device attached to the router is powered on. In this case, the router attached to the serial line detects a change in interface signals and initiates a connection with the Token Ring hosts by exchanging explorer and exchange identification (XID) packets.
- When a serial interface previously shut down is brought back online. When the **no shutdown** command is issued, the software will detect a change in the serial line state from down to up and initiate a session with the Token Ring host by exchanging explorer and XID packets.

The Cisco IOS software will continue trying once a minute to initiate a connection whenever one of these two conditions is met, until the host responds to its requests. When you no longer want the software to initiate connections with a host, use the **no sdllc partner** command.

Note For device-initiated sessions, the host will check the IDBLK and IDNUM parameters of the serial device it receives in the XID packet against the information configured on the host. If the information in the XID packet does not match with what is configured on the host, the host will drop the session. Therefore, for device-initiated connections, always specify the correct IDBLK and IDNUM parameters on the router serial interfaces with the **sdllc xid** command.

Examples

In the following example, a serial device at SDLC address C2 wants to initiate a connection with a Token Ring host at MAC address 4000.0122.0001. The router initiates the connection on behalf of a serial device:

```
! sample global command
source-bridge ring-group 100
!
interface serial 0
! router initiates connections with Token Ring host at MAC address
! 4000.0122.0001 on behalf of serial device c2
sdllc partner 4000.0122.0001 c2
```

Related Commands

Command	Description
sdllc xid	Specifies an XID value appropriate for the designated SDLC station associated with this serial interface.

sdllc ring-largest-frame

To indicate the largest I-frame size that can be sent to or received from the Logical Link Control, type 2 (LLC2) primary station, use the **sdllc ring-largest-frame** command in interface configuration mode. To return to the default, use the **no** form of this command.

sdllc ring-largest-frame *bytes*

no sdllc ring-largest-frame *bytes*

Syntax Description

bytes	Frame size in bytes. Values are 516, 1500, 2052, 4472, 8144, 11407, and 17800. The default is 516 bytes.

Defaults

516 bytes

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Values for the *bytes* argument match those for the **lf** *size* of the various **source-bridge remote-peer** commands. You must ensure that your remote peer connection can support this largest frame size. Values for the *bytes* argument are 516, 1500, 2052, 4472, 8144, 11407, and 17800.

Faster screen updates to 3278-style terminals often can be obtained by allowing the Token Ring front-end processor (FEP) to send as large a frame as possible and by allowing the Cisco IOS software to segment the frame into multiple Synchronous Data Link Control (SDLC) I-frames.

Examples

In the following example, the software can send or receive a frame as large as 11407 bytes from the Logical Link Control, type 2 (LLC2) primary station. Any frames larger will be fragmented by the software.

```
! sample global command
source-bridge ring-group 100
!
interface serial 3
! largest frame sent or received on serial 3 is 11407 bytes
sdllc ring-largest-frame 11407
```

Related Commands

Command	Description
source-bridge remote-peer interface	Specifies a point-to-point direct encapsulation connection.
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

sdllc sap

To associate a service access point (SAP) value other than the default SAP value with a serial interface configured for SDLC Logical Link Control. Cisco (SDLLC), use the **sdllc sap** command in interface configuration mode. To return this SAP value to its default state, use the **no** form of this command.

sdllc sap *sdlc-address ssap dsap*

no sdllc sap *sdlc-address ssap dsap*

Syntax Description

sdlc-address	MAC address associated with the remote Synchronous Data Link Control (SDLC) device.
ssap	Source SAP value. It must be in the range from 1 to 254. The default is 4.
dsap	Destination SAP value. It must be in the range from 1 to 254. The default is 4.

Defaults

The default source SAP value for IBM Systems Network Architecture (SNA) devices is 4.
The default destination SAP value for IBM SNA devices is 4.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You use the **sdllc sap** command in conjunction with the **sdllc traddr** command in interface configuration modes. A SAP can be viewed as a port through which a higher-layer application can communicate with its counterpart (peer) operating on another system. Although the standard SAP value for IBM SNA devices is 4, and NetBIOS devices is xF0, other values are allowed.

Examples

In the following example, source SAP and destination SAP values of 2 are specified for the remote SDLC device at the SDLC address C1 02 02:

```
interface serial 0
 sdllc sap c1 02 02
```

Related Commands

Command	Description
sdllc traddr	Enables SDLLC media translation on a serial interface. The address specified is a MAC address to be assigned to the serial station.

sdllc sdlc-largest-frame

To indicate the largest information frame (I-frame) size that can be sent or received by the designated Synchronous Data Link Control (SDLC) station, use the **sdllc sdlc-largest-frame** command in interface configuration mode. To return to the default value, use the **no** form of this command.

sdllc sdlc-largest-frame *address value*

no sdllc sdlc-largest-frame *address value*

Syntax Description

address	Address of the SDLC station that will communicate with the Token Ring host.
value	Largest frame size that can be sent or received by this SDLC station. The default is 265 bytes.

Defaults

265 bytes

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Most SDLC devices are limited to frames of 265 bytes. I-frames received from the Token Ring station that are larger than this size will be properly fragmented.

Examples

In the following example, the Cisco IOS software can send or receive a frame as large as 265 bytes (the default) from the SDLC station at address C6. Any frames larger will be fragmented by the software.

```
! sample global command
source-bridge ring-group 100
!
interface serial 4
! largest frame sent or received on serial 4 is 265 bytes
 sdllc sdlc-largest-frame c6 265
```

sdllc traddr

To enable SDLC Logical Link Control. Cisco (SDLLC) media translation on a serial interface, use the **sdllc traddr** command in interface configuration mode. To disable SDLLC media translation on the interface, use the **no** form of this command.

sdllc traddr *mac-address vrn bn trn*

no sdllc traddr *mac-address vrn bn trn*

Syntax Description

mac-address	MAC address to be assigned to the serial interface.
vrn	SDLLC virtual ring number.
bn	SDLLC bridge number.
trn	SDLLC target ring number.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The address specified is a MAC address to be assigned to the serial station.

Every control unit hooked off the serial line requires a virtual Token Ring address (VTRA). This usually is assigned by the system administrator as a locally administered MAC address (unique across the network).

When you enable SDLLC media translation by specifying the **sdllc traddr** command on a serial interface, you must specify a VTRA for each serial station attached to the serial line. The last two hexadecimal digits (that is, the last byte) of the VTRA *must* be 00. The Cisco IOS software uses this byte to represent the Synchronous Data Link Control (SDLC) address of a station on the serial link.

Note Addresses in the range from *xxxx.xxxx.xx*00 to *xxxx.xxxx.xx*FF are reserved for use by the Cisco IOS software. You must adhere to this addressing requirement. If you do not follow this addressing requirement, there may be a conflict between the VTRA and the addresses reserved by the software for the Synchronous Data Link Control (SDLC) link.

The *vrn*, *bn*, and *trn* arguments represent the SDLLC virtual ring number, bridge number, and target ring number, respectively, that you assign to the interface. In design, the serial interface appears to be a ring, *vrn*, on a source-route bridged network, and ties in through the bridge, *bn*, to the virtual ring group, *trn*. This provides access to other, real rings through remote source-route bridging **source-bridge remote-peer** commands. Note that SDLLC can be configured on a router containing no Token Ring interface cards.

The **sdllc traddr** command automatically turns on the Logical Link Control, type 2 (LLC2) process with default values. To change any of the LLC2 parameters, specify their values on the serial interface that is being enabled for SDLLC. This is done on the serial interface, even though LLC2 does not run on the serial interface, but on the SDLLC virtual ring associated with the serial interface. LLC2 commands can be configured after specifying the **sdllc traddr** command.

Examples

In the following example, SDLLC media translation is enabled off the serial 0 interface to a serial station at MAC address 0110.2222.3300. The SDLLC virtual ring number is 8, the bridge number is 1, and the target ring number is 100.

```
! global command to apply commands to the ring group
source-bridge ring-group 100
! remote peer at IP address 10.108.1.1 belongs to ring group 100 and uses
! tcp as the transport
source-bridge remote-peer 100 tcp 10.108.1.1
source-bridge remote-peer 100 tcp 10.108.2.2
!
interface serial 0
 encapsulation sdlc-primary
! establish address of SDLC station off serial-0 as c1
 sdlc address c1
! enable SDLLC media translation to serial station 0110.2222.3300
! on virtual ring 8, bridge 1, to target ring 100
 sdllc traddr 0110.2222.3300 8 1 100
```

Related Commands

Command	Description
sdllc sap	Associates a SAP value other than the default SAP value with a serial interface configured for SDLLC.
source-bridge remote-peer interface	Specifies a point-to-point direct encapsulation connection.
source-bridge remote-peer tcp	Identifies the IP address of a peer in the ring group with which to exchange source-bridge traffic using TCP.

sdllc xid

To specify an exchange identification (XID) value appropriate for the designated Synchronous Data Link Control (SDLC) station associated with this serial interface, use the **sdllc xid** command in interface configuration mode. To disable XID processing for this address, use the **no** form of this command.

sdllc xid *address xid*

no sdllc xid *address xid*

Syntax Description

address	Address of the SDLC station associated with this interface.
xid	XID the Cisco IOS software will use to respond to XID requests received on the Token Ring Logical Link Control, type 2 (LLC2) side of the connection. This value must be 4 bytes (8 digits) in length and is specified with hexadecimal digits.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Exchange identification (XID) requests and responses are usually exchanged before sessions are started. Be sure that the XID value configured on the router matches the IDBLK and IDNUM parameters configured on the host. The XID response to an XID request from the Token Ring host will contain the information you configured in the **sdllc xid** command. The host will check the XID response it receives with the IDBLK and IDNUM parameters (that are configured in virtual telecommunications access method (VTAM)). If they match, the Token Ring host will initiate a session with the router. If they do not match, the host will not initiate a session.

Examples

The following example specifies an XID value of 01720002 at address C2:

```
! sample global command
source-bridge ring-group 100
!
interface serial 0
! sdllc exchange identification value of 01720002 at address c2
 sdllc xid c2 01720002
```

Related Commands

Command	Description
sdllc partner	Enables device-initiated connections for SDLLC. Must be specified for the serial interface that links to the serial line device.