IBM Networking Commands

access-expression

To define an access expression, use the **access-expression** command in interface configuration mode. To remove the access expression from the given interface, use the **no** form of this command.

access-expression {**in** | **out**} *expression*

no access-expression {**in** | **out**} *expression*

Syntax Description

in | **out**	Either **in** or **out** is specified to indicate whether the access expression is applied to packets entering or leaving this interface. You can specify both an input and an output access expression for an interface, but only one of each.
expression	Boolean access list expression, built as explained in the "Usage Guidelines" section.

Command Default

No access expression is defined.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

Use this command in conjunction with the **access-list** command in interface configuration mode.

An access expression consists of a list of terms, separated by Boolean operators, and optionally grouped in parentheses.

An access expression term specifies a type of access list, followed by its name or number. The result of the term is either true or false, depending on whether the access list specified in the term permits or denies the frame.

Table 1 describes the terms that can be used.

Table 6 Access Expression Terms

Access Expression Term	Definition
lsap(2nn)	Subnetwork Access Protocol access list to be evaluated for this frame (Cisco 200 series).
type(2nn)	Subnetwork Access Protocol (SNAP) type access list to be evaluated for this frame (Cisco 200 series).
smac(7nn)	Access list to match the source MAC address of the frame (Cisco 700 series).
dmac(7nn)	Access list to match the destination MAC address of the frame (Cisco 700 series).
netbios-host(name)	NetBIOS-host access list to be applied on NetBIOS frames traversing the interface.
netbios-bytes(name)	NetBIOS-bytes access list to be applied on NetBIOS frames traversing the interface.

Access expression terms are separated by Boolean operators, as listed in Table 2.

Table 7 Boolean Operators for Access Expression Terms

Boolean Operators	Definitions
~ (called “not”)	Negates, or reverses, the result of the term or group of terms immediately to the right of the ~. Example: “~lsap (201)” returns FALSE if “lsap (201)” itself were TRUE.
& (called “and”)	Returns TRUE if the terms or parenthetical expressions to the left and right of the & both return TRUE. Example: “lsap (201) & dmac (701)” returns TRUE if both the lsap (201) and dmac (701) terms return TRUE.
| (called “or”)	Returns TRUE if the terms or parenthetical expressions either to the left or to the right of the | or both return TRUE. Example: “lsap (201) | dmac (701)” returns TRUE if either the lsap (201) or dmac (701) terms return TRUE, or if both return TRUE.

Terms can be grouped in parenthetical expressions. Any of the terms and operators can be placed in parentheses, similar to what is done in arithmetic expressions, to affect order of evaluation.

An “access-expression” type filter cannot exist with a “source-bridge” type filter on the same interface. The two types of filters are mutually exclusive.

Note The incorrect use of parentheses can drastically affect the result of an operation because the expression is read from left to right.

Related Commands

Command	Description
access-list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

access-list

To configure the access list mechanism for filtering frames by protocol type or vendor code, use the **access-list** command in global configuration mode. To remove the single specified entry from the access list, use the **no** form of this command.

access-list *access-list-number* {**permit** | **deny**} {*type-code wild-mask* | *address mask*}

no access-list *access-list-number* {**permit** | **deny**} {*type-code wild-mask* | *address mask*}

Syntax Description

access-list-number	Integer that identifies the access list. If the *type-code* and *wild-mask* arguments are included, this integer ranges from 200 to 299, indicating that filtering is by protocol type. If the *address* and *mask* arguments are included, this integer ranges from 700 to 799, indicating that filtering is by vendor code.
permit	Permits the frame.
deny	Denies the frame.
type-code	16-bit hexadecimal number written with a leading 0x; for example, 0x6000. Specify either a Link Service Access Point (LSAP) type code for 802-encapsulated packets or a Subnetwork Access Protocol (SNAP) type code for SNAP-encapsulated packets. (LSAP, sometimes called SAP, refers to the type codes found in the DSAP and SSAP fields of the 802 header.)
wild-mask	16-bit hexadecimal number whose ones bits correspond to bits in the *type-code* argument. The *wild-mask* argument indicates which bits in the *type-code* argument should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be 0x0101 because these two bits are used for purposes other than identifying the SAP code.)
address	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. This field is used for filtering by vendor code.
mask	48-bit Token Ring address written as a dotted triple of four-digit hexadecimal numbers. The ones bits in *mask* are the bits to be ignored in *address*. This field is used for filtering by vendor code. For source address filtering, the mask always should have the high-order bit set. This is because the IEEE 802 standard uses this bit to indicate whether a Routing Information Field (RIF) is present, not as part of the source address.

Command Default

No access list is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.

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

Usage Guidelines

For a list of type codes, refer to Appendix: Ethernet Type Codes.

Examples

In the following example, the access list permits only Novell frames (LSAP 0xE0E0) and filters out all other frame types. This set of access lists would be applied to an interface via the **source-bridge input-lsap list** or **source-bridge input-lsap list** command (described later in this chapter).

```
access-list 201 permit 0xE0E0 0x0101
access-list 201 deny 0x0000 0xFFFF
```

Combine the DSAP/LSAP fields into one number to do LSAP filtering; for example, 0xE0E0—not 0xE0. Note that the deny condition specified in the preceding example is not required; access lists have an implicit deny as the last statement. Adding this statement can serve as a useful reminder, however.

The following access list filters out only SNAP type codes assigned to Digital Equipment Corporation (DEC) (0x6000 to 0x6007) and lets all other types pass. This set of access lists would be applied to an interface using the **source-bridge input-type-list** or **source-bridge output-type-list** command (described later in this chapter).

```
access-list 202 deny 0x6000 0x0007
access-list 202 permit 0x0000 0xFFFF
```

Note Use the last item of an access list to specify a default action; for example, to permit everything else or to deny everything else. If nothing else in the access list matches, the default action is to deny access; that is, filter out all other type codes.

Type code access lists will negatively affect system performance by greater than 30 percent. Therefore, we recommend that you keep the lists as short as possible and use wildcard bit masks whenever possible.

Related Commands

Command	Description
access-expression	Defines an access expression.
source-bridge input-address-list	Applies an access list to an interface configured for source-route bridging, and filters source-routed packets received from the device interface based on the source MAC address.
source-bridge input-lsap-list	Filters, on input, FDDI and IEEE 802-encapsulated packets that include the DSAP and SSAP fields in their frame formats.
source-bridge input-type-list	Filters SNAP-encapsulated packets on input.

Command	Description
source-bridge output-address-list	Applies an access list to an interface configured for SRB, and filters source-routed packets sent to the device interface based on the destination MAC address.
source-bridge output-lsap-list	Filters, on output, FDDI and IEEE 802-encapsulated packets that have DSAP and SSAP fields in their frame formats.
source-bridge output-type-list	Filters SNAP-encapsulated frames by type code on output.

access-list (extended-ibm)

To provide extended access lists that allow more detailed access lists, use the **access-list** command in global configuration mode. These lists allow you to specify both source and destination addresses and arbitrary bytes in the packet.

access-list *access-list-number* {**permit** | **deny**} *source source-mask destination destination-mask offset size operator operand*

Syntax Description

access-list-number	Integer from 1100 to 1199 that you assign to identify one or more **permit/deny** conditions as an extended access list. Note that a list number in the range from 1100 to 1199 distinguishes an extended access list from other access lists.
permit	Allows a connection when a packet matches an access condition. The Cisco IOS software stops checking the extended access list after a match occurs. All conditions must be met to make a match.
deny	Disallows a connection when a packet matches an access condition. The software stops checking the extended access list after a match occurs. All conditions must be met to make a match.
source	MAC Ethernet address in the form *xxxx.xxxx.xxxx.*
source-mask	Mask of MAC Ethernet source address bits to be ignored. The software uses the *source* and *source-mask* arguments to match the source address of a packet.
destination	MAC Ethernet value used for matching the destination address of a packet.
destination-mask	Mask of MAC Ethernet destination address bits to be ignored. The software uses the *destination* and *destination mask* arguments to match the destination address of a packet.
offset	Range of values that must be satisfied in the access list. Specified in decimal or in hexadecimal format in the form 0x*nn*. The offset is the number of bytes from the destination address field; it is not an offset from the start of the packet. The number of bytes you need to offset from the destination address varies depending on the media encapsulation type you are using.
size	Range of values that must be satisfied in the access list. Must be an integer from 1 to 4.

operator	Compares arbitrary bytes within the packet. Can be one of the following keywords: **lt**—less than **gt**—greater than **eq**—equal **neq**—not equal **and**—bitwise and **xor**—bitwise exclusive or **nop**—address match only
operand	Compares arbitrary bytes within the packet. The value to be compared to or masked against.

Command Default

No extended access lists are established.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

After an access list is initially created, any subsequent additions (possibly entered from the terminal) are placed at the *end* of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

An extended access list should not be used on FDDI interfaces that provide transit bridging.

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

Note Due to their complexity, extended access lists should only be used by those who are very familiar with the Cisco IOS software. For example, to use extended access lists, it is important to understand how different encapsulations on different media would generally require different offset values to access particular fields.

Caution Do not specify offsets into a packet that are greater than the size of the packet.

Examples

The following example shows an extended access list. The first **access-list** command permits packets from MAC addresses 000c.1b*xx.xxxx* to any MAC address if the packet contains a value less than 0x55AA in the 2 bytes that begin 0x1e bytes into the packet. The seconds **access-list** command permits an NOP operation:

```
access-list 1102 permit 000c.1b00.0000 0000.00ff.ffff 0000.0000.0000
    ffff.ffff.ffff 0x1e 2 lt 0x55aa
access-list 1101 permit 0000.0000.0000 ffff.ffff.ffff 0000.0000.0000
    ffff.ffff.ffff
!
interface ethernet 0
 bridge-group 3 output-pattern 1102
```

The following is sample output from the **show interfaces crb** command for the access list configured above:

```
Device# show interfaces crb

Bridged protocols on Ethernet0/3:
clns  decnet  vines  apollo
novell  xns

Software MAC address filter on Ethernet0/3
Hash Len   Address         Matches   Act   Type
0x00: 0    ffff.ffff.ffff  0         RCV   Physical broadcast
0x00: 1    ffff.ffff.ffff  0         RCV   Appletalk zone
0x2A: 0    0900.2b01.0001  0         RCV   DEC spanning tree
0x49: 0    0000.0c36.7a45  0         RCV   Interface MAC address
0xc0: 0    0100.0ccc.cccc  48        RCV   CDP
0xc2: 0    0180.c200.0000  0         RCV   IEEE spanning tree
0xF8: 0    0900.07ff.ffff  0         RCV   Appletalk broadcast
```

Table 3 describes significant fields shown in the display.

Table 8 show interfaces crb Field Descriptions

Field	Description
Bridged protocols on…	List of the bridged protocols configured for the specified interface.
Software MAC address filter on…	Table of software MAC address filter information for the specified interface.
Hash	Hash key/relative position in the keyed list for this MAC-address entry.
Len	Length of this entry to the beginning element of this hash chain.
Address	Canonical (Ethernet ordered) MAC address.
Matches	Number of received packets matched to this MAC address.
Act	Action to be taken when that address is looked up; choices are to receive or discard the packet.
Type	MAC address type.

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.
access-list (type-code-ibm)	Builds type-code access lists.
bridge-group output-pattern-list	Associates an extended access list with a particular interface.

access-list (standard-ibm)

To establish a MAC address access list, use the **access-list** command in global configuration mode. To remove access list, use the **no** form of this command.

access-list *access-list-number* {**permit** | **deny**} *address mask*

no access-list *access-list-number*

Syntax Description

access-list-number	Integer from 700 to 799 that you select for the list.
permit	Permits the frame.
deny	Denies the frame.
address mask	48-bit MAC addresses written as a dotted triple of four-digit hexadecimal numbers. The ones bits in the *mask* argument are the bits to be ignored in *address*.

Command Default

No MAC address access lists are established.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Configuring bridging access lists of type 700 may cause a momentary interruption of traffic flow.

Examples

The following example assumes that you want to disallow the bridging of Ethernet packets of all Sun workstations on Ethernet interface 1. Software assumes that all such hosts have Ethernet addresses with the vendor code 0800.2000.0000. The first line of the access list denies access to all Sun workstations, and the second line permits everything else. You then assign the access list to the input side of Ethernet interface 1.

```
access-list 700 deny 0800.2000.0000 0000.00FF.FFFF
access-list 700 permit 0000.0000.0000 FFFF.FFFF.FFFF
!
interface ethernet 1
 bridge-group 1 input-address-list 700
```

Related Commands

Command	Description
access-list (type-code-ibm)	Builds type-code access lists.

access-list (type-code-ibm)

To build type-code access lists, use the **access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

access-list *access-list-number* {**permit** | **deny**} *type-code wild-mask*

no access-list *access-list-number*

Syntax Description

access-list-number	User-selectable number from 200 to 299 that identifies the list.
permit	Permits the frame.
deny	Denies the frame.
type-code	16-bit hexadecimal number written with a leading "0x"; for example, 0x6000. You can specify either an Ethernet type code for Ethernet-encapsulated packets, or a destination service access point (DSAP)/source service access point (SSAP) pair for 802.3 or 802.5-encapsulated packets. Ethernet type codes are listed in the appendix "Ethernet Type Codes."
wild-mask	16-bit hexadecimal number whose ones bits correspond to bits in the *type-code* argument that should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be at least 0x0101 because these two bits are used for purposes other than identifying the SAP codes.)

Command Default

No type-code access lists are built.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Type-code access lists can have negatively affect system performance; therefore, keep the lists as short as possible and use wildcard bit masks whenever possible.

Access lists are evaluated according to the following algorithm:

- If the packet is Ethernet Type II or SNAP, the type-code field is used.
- If the packet is another type, then the LSAP is used.

Packets are treated according to the following algorithm:

- If the length/type field is greater than 1500, the packet is treated as an Advanced Research Projects Agency (ARPA) packet.
- If the length/type field is less than or equal to 1500, and the DSAP and SSAP fields are AAAA, the packet is treated using type-code filtering.
- If the length/type field is less than or equal to 1500, and the DSAP and SSAP fields are *not* AAAA, the packet is treated using Link Service Access Point (LSAP) filtering.

If the LSAP-code filtering is used, all SNAP and Ethernet Type II packets are bridged without obstruction. If type-code filtering is used, all LSAP packets are bridged without obstruction.

If you have both Ethernet Type II and LSAP packets on your network, you should set up access lists for both.

Examples

The following example shows how to permit only local-area transport (LAT) frames (type 0x6004) and filters out all other frame types:

```
access-list 201 permit 0x6004 0x0000
```

The following example shows how to filter out only type codes assigned to Digital Equipment Corporation (DEC) (0x6000 to 0x600F) and lets all other types pass:

```
access-list 202 deny 0x6000 0x000F
access-list 202 permit 0x0000 0xFFFF
```

Use the last item of an access list to specify a default action; for example, permit everything else or deny everything else. If nothing else in the access list matches, the default action is normally to deny access; that is, filter out all other type codes.

Related Commands

Command	Description
access-list (standard-ibm)	Establishes MAC address access lists.

adapter

To configure internal adapters, use the **adapter** command in internal LAN interface configuration submode. To remove an internal adapter, use the **no** form of this command.

adapter *adapter-number* [*mac-address*] [**hsma-partner** *hsma-mac-address*]

no adapter *adapter-number* [*mac-address*]

Syntax Description

adapter-number	Number in the range from 0 to 31 that uniquely identifies the internal adapter (relative adapter number) for all internal LANs of the same type on the Cisco Mainframe Channel Connection (CMCC) adapter. In Cisco Systems Network Architecture (CSNA), this value corresponds to the adapter number (ADAPNO) parameter defined in the Virtual Telecommunications Access Method (VTAM) Extended Communications Adapter (XCA) Major Node.
mac-address	(Optional) MAC address for this internal adapter. This is a hexadecimal value in the form *xxxx.xxxx.xxxx*.
hsma-partner	(Optional) Specifies a hot standby MAC address (HSMA) partner.
hsma-mac-address	(Optional) MAC address of the HSMA partner control adapter.

Command Default

No default behavior or values.

Command Modes

Internal LAN interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.3(3)	The **hsma-partner** keyword and *hsma-mac-address* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is valid only on the virtual channel interface. Internal adapters are used to provide LAN gateway MAC addresses for the following CMCC adapter features: CSNA, Cisco Multipath Channel (CMPC), and TN3270 Server.

Up to 18 internal adapters can be configured on a CMCC adapter. Internal adapters are configured on internal LANs. The only limit to the number of internal adapters that you can configure on a single internal LAN is the limit of up to 18 total internal adapters per CMCC.

When an internal adapter configuration command is removed or an existing internal adapter is modified, the *mac-address* parameter is not required. In internal adapter configuration mode, the device prompt appears as follows:

```
Device(cfg-adap-type n-m)#
```

In this syntax, *type* is the internal LAN type, *n* is the LAN ID, and *m* is the adapter number.

HSMA is designed to allow redundant CMCC internal adapter MAC addresses in an Ethernet environment. Communication between the HSMA control adapters is used to ensure that only one of the adapters is active at a time.

Examples

The following example shows how to configure internal adapters 3 and 4 (with their corresponding MAC addresses) on the internal Token Ring LAN number 20, and internal adapter 1 on the internal Token Ring LAN number 10:

```
interface channel 1/2
 lan tokenring 20
  adapter 3 4000.7500.0003
  adapter 4 4000.7500.0004
 lan tokenring 10
  source-bridge 100 1 100
  adapter 1 4000.7500.1111
```

The following example shows how to configure internal adapter 9 to communicate with the HSMA partner at the MAC address 4043.3333.001a:

```
interface Channel1/2
 lan TokenRing 20
  source-bridge 310 3 100
  adapter 9 4043.1313.9009 hsma-partner 4043.3333.001a
 lan TokenRing 20
  source-bridge 319 9 100
  adapter 26 4043.1111.001a
   hsma enable
```

Related Commands

Command	Description
lan	Configures an internal LAN on a CMCC adapter interface and enters the internal LAN configuration mode.
name	Assigns a name to an internal adapter.
show extended channel hsma	Displays hot standby MAC address (HSMA) information
show extended channel lan	Displays the internal LANs and adapters configured on a CMCC adapter.
show extended channel llc2	Displays information about the LLC2 sessions running on CMCC adapter interfaces.
show extended channel connection-map llc2	Displays the number of active LLC2 connections for each SAP and the mapping of the internal MAC adapter and the SAP to the resource that activated the SAP.
source-bridge	Configures an interface for SRB.

allocate lu

To assign logical unit (LU)s to a pool, use the **allocate lu** command in listen-point physical unit (PU) configuration submode. To remove LUs assigned to a pool, use the **no** form of this command.

allocate lu *lu-address* **pool** *poolname* **clusters** *count*

no allocate lu *lu-address* **pool** *poolname* **clusters** *count*

Syntax Description

lu-address	Starting number of the LOCADDR to which a cluster of LUs are to be allocated.
pool *poolname*	Pool name to which you want to allocate LUs. The pool name cannot exceed eight characters in length.
clusters *count*	Range of LUs in a cluster that are allocated to the specified pool. For example, if the **lu** keyword specifies the beginning of the LOCADDR number, the **cluster** keyword specifies the number of clusters to be included in the pool.

Command Default

No LUs are assigned to a pool.

Command Modes

Listen-point PU configuration

Command History

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

Usage Guidelines

The following guidelines apply to the **allocate lu** command:

- The LUs assigned to a pool constitute a cluster. When multiple pools are configured, the LU ranges for different pools on the same PU must not overlap.
- A maximum of 255 LOCADDRs can be allocated to a pool. Configurations with invalid LOCADDRs are deleted. Overlapping LU ranges between different pools are invalid.
- The LOCADDR ranges must not overlap for multiple allocation statements and with existing ranges specified for client nailing statements.
- When LUs are allocated while LUs are in use, existing clients are allowed to complete their sessions unaffected.

Examples

In the following example, the starting LOCADDR is 10. Each cluster has 10 LOCADDRs, therefore 50 LOCADDRs are allocated to the pool name LOT1.

```
interface channel 0/2
 tn3270-server
 pool LOT1 cluster layout 4s1p
  listen-point 10.20.30.40
   pu PU1
    allocate lu 10 pool LOT1 clusters 5
```

As a result of this configuration, the following LOCADDRs are created in each cluster:

- Cluster 1
  - LOCADDR 10—Screen
  - LOCADDR 11—Screen
  - LOCADDR 12—Screen
  - LOCADDR 13—Screen
  - LOCADDR 14—Printer
- Cluster 2
  - LOCADDR 15—Screen
  - LOCADDR 16—Screen
  - LOCADDR 17—Screen
  - LOCADDR 18—Screen
  - LOCADDR 19—Printer

All of the LUs in these clusters are allocated to pool LOT1.

Related Commands

Command	Description
pool	Defines pool names for the TN3270 server and specifies the number of screens and printers in each logical cluster.
pu (TN3270)	Creates a PU entity that has its own direct link to a host and enters PU configuration mode.
pu dlur (listen-point)	Creates a PU entity that has no direct link to a host and enters listen-point PU configuration mode.
tn3270-server	Starts the TN3270 server on a CMCC adapter and enters TN3270 server configuration mode.

alps a1-map a2-map

To specify the A1 and A2 logical agent-set control unit (ASCU) identification information, use the **alps a1-map a2-map** command in Airline Product Set (ALPS) ASCU configuration submode. To remove the specification of the A1 and A2 logical ASCU identification information, use the **no** form of this command.

alps a1-map *a1-value* **a2-map** *a2-value*

no alps a1-map *a1-value* **a2-map** *a2-value*

Syntax Description

a1-value	A1 logical ASCU identification: • airline link control (ALC) range—Hexadecimal number in the range from 0 to 0xFF. • Unisys Terminal System (UTS) range—Hexadecimal number in the range from 0 to 0xFF.
a2-value	A2 logical ASCU identification: • ALC range—Hexadecimal number in the range from 0 to 0xFF. • UTS range—Hexadecimal number in the range from 0 to 0xFF.

Command Default

No A1 and A2 logical ASCU identification information is specified.

Command Modes

ALPS ASCU submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(2)T	The range values were modified.
12.0(5)T	The range values were modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies the A1 identification as 0x4C and the A2 identification as 0x20:

```
alps a1-map 4C a2-map 20
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps alias

To specify that an airline link control (ALC) agent-set control unit (ASCU) is to operate in nonpolling mode, and to specify the parent ASCU interchange address to which this ASCU is aliased, use the **alps alias** command in Airline Product Set (ALPS) ASCU configuration submode. To return the ASCU to polled mode, use the **no** form of this command.

alps alias *alias-interchange-address*

no alps alias *alias-interchange-address*

Syntax Description

alias-interchange-address	Specifies the interchange address of the polled (alias) ASCU with which to associate this non-polled ASCU. Valid range is between 41 and 7E, except 43, 44, 50 to 53, and 60.

Command Default

If you do not specify the **alps alias** command, the ASCU functions in normal polled mode. You must specify the **alps alias** command to enable non-polled handling.

Command Modes

ALPS ASCU configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to ALC ASCUs.

By default, an ALC ASCU cannot send data to a remote device until it is polled by that device. However, you can use this command to configure *non-polled* ALC ASCUs.

A non-polled ASCU must be associated with another, polled ASCU, known as the alias ASCU. When a remote device polls the alias ASCU, the device accepts data from that ASCU and from all non-polled ASCUs associated with that ASCU. The non-polled ASCUs present the same characteristics to the host as the alias ASCU, so the current ASCU configuration is maintained.

This command does not impact the ALC send path or the circuit management code.

Examples

The following example sets the ALC ASCU with interchange address 4B to operate in nonpolling mode and sets 42 as the alias interchange address:

```
alps ascu 4B
alps alias 42
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
show alps ascu	Displays the status of the ALPS ASCU.

alps ascu

To specify a physical agent-set control unit (ASCU) identity, use the **alps ascu** command in Airline Product Set (ALPS) ASCU configuration submode. To remove the ASCU from the interface and delete any messages queued for transmission to the ASCU or the network, use the **no** form of this command.

alps ascu *id*

no alps ascu *id*

Syntax Description

id	ASCU identification. Valid range is from 41 to 7E, except 43, 44, 50 to 53, and 60. The Unisys Terminal System (UTS) valid range is from 21 to 4F.

Command Default

No physical ASCU identity is specified.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(2)T	This command was modified for UTS support.
12.1(2)T	The valid range values were modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If an ASCU already exists on the interface, the **alps ascu** command initiates the ALPS ASCU configuration submode for that ASCU. If the ASCU does not exist, an ASCU is created and the ALPS ASCU configuration submode is initiated.

Examples

The following example specifies the interchange address as 4B:

```
alps ascu 4B
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol is used on the serial interface.
encapsulation alc	Specifies that the P1024B airline link control (ALC) protocol is used on the serial interface.

alps auto-reset

To automatically reset a nonresponsive airline link control (ALC) agent-set control unit (ASCU) in the DOWN state, use the **alps auto-reset** command in Airline Product Set (ALPS) ASCU configuration submode. To disable the automatic reset, use the **no** form of this command.

alps auto-reset

no alps auto-reset

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic ASCU reset is disabled by default.

Command Modes

ALPS ASCU configuration submode

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to ALC ASCUs.

Examples

The following example shows how to configure automatic reset for all nonresponsive ASCUs in the DOWN state:

```
alps auto-reset
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
encapsulation alc	Specifies that the P1024B ALC protocol is used on the serial interface.

alps circuit

To specify an Airline Product Set (ALPS) circuit at the remote customer premises equipment (CPE) across a TCP/IP connection, use the **alps circuit** command in ALPS circuit configuration submode. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

alps circuit *name*

no alps circuit *name*

Syntax Description

name	Name given to identify an ALPS circuit.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Entering this command causes a circuit control block to be created. The command also initiates the ALPS circuit configuration submode. If the circuit already exists, the only action is the initiation of the ALPS circuit configuration submode.

Note that this command is used to statically create an ALPS circuit at the remote CPE. ALPS X.25 circuits (at the central CPE) are always dynamically created and are never created using this command.

Examples

The following example specifies the name of the ALPS circuit at the remote CPE as CKT1:

```
alps circuit CKT1
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps connection-type permanent

To specify that this circuit should be established when the circuit is enabled, use the **alps connection-type permanent** command in Airline Product Set (ALPS) circuit configuration submode. To remove the permanent activation behavior and return the behavior to the default dynamic activation, use the **no** form of this command.

alps connection-type permanent [*retry-timer*]

no alps connection-type permanent [*retry-timer*]

Syntax Description

retry-timer	(Optional) Specifies the maximum interval between consecutive attempts to establish a circuit in the event of a failure. The default for the retry timer is 30 seconds and the range is from 1 to 180 seconds.

Command Default

The default is 30 seconds.

Command Modes

ALPS circuit submode

Command History

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

Examples

The following example specifies that the circuit is established when enabled and that the customer premises equipment (CPE) will retry the connection every 30 seconds in the event of a failure:

```
alps connection-type permanent 30
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps default-circuit

To specify the Airline Product Set (ALPS) circuit that this agent-set control unit (ASCU) uses, use the **alps default-circuit** command in ALPS ASCU submode. To remove the default circuit specification, use the **no** form of this command.

alps default-circuit *name*

no alps default-circuit *name*

Syntax Description

name	Name given to identify an ALPS circuit on the remote customer premises equipment (CPE).

Command Default

No default behavior or values.

Command Modes

ALPS ASCU submode

Command History

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

Examples

The following example shows how to specify that ALPS circuit to be used is CKT1:

```
alps default-circuit CKT1
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps enable-alarms ascu

To enable alarms for the Airline Product Set (ALPS) agent-set control unit (ASCU)s, use the **alps enable-alarms ascu** command in global configuration mode at the remote customer premises equipment (CPE). To disable alarms for the ALPS ASCUs, use the **no** form of this command.

alps enable-alarms ascu [*interface id*]

no alps enable-alarms ascu

Syntax Description

interface id	(Optional) ASCU identifier. Enable alarms for the specified ASCU.

Command Default

If no interface and interchange address combination is specified, then alarms (Syslog messages and SNMP traps) are enabled for all ALPS ASCUs.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If an interface and interchange address combination is specified, then the alarms are enabled only for the ASCU matching that combination. Up to eight **alps enable-alarms ascu** commands can be entered to allow a set of ALPS ASCUs to be monitored. ALPS ASCU alarms are generated only at the remote CPE.

Examples

The following example enables alarms for ALPS ASCU 42 on serial interface 1:

```
alps enable-alarms ascu Serial1 42
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps enable-alarms circuit

To enable alarms for the Airline Product Set (ALPS) circuits, use the **alps enable-alarms circuit** command in global configuration mode. To remove the circuit definition from the configuration, use the **no** form of this command.

alps enable-alarms circuit [*name*]

no alps enable-alarms circuit [*name*]

Syntax Description

name	(Optional) Name given to identify an ALPS circuit on the remote customer premises equipment (CPE).

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If a valid circuit name is specified, then the alarms are enabled only for the circuit matching the name. Up to eight **alps enable-alarms circuit** commands can be entered to allow a subset of ALPS circuits to be monitored. ALPS circuit alarms are generated at both the remote airline link control (ALC) CPE and the central (X.25) CPE.

Examples

The following example enables alarms for the ALPS circuit named CKT1:

```
alps enable alarms circuit CKT1
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps enable-alarms peer

To enable alarms for the Airline Product Set (ALPS) peers, use the **alps enable-alarms peer** command in global configuration mode. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

alps enable-alarms peer [*ip-address*]

no alps enable-alarms peer [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the remote peer for which alarms are enabled.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If an IP address is specified, then the alarms are enabled only for the remote peer matching the IP address. Up to eight **alps enable-alarms peer** commands can be entered to allow a set of ALPS peers to be monitored. ALPS peer alarms are generated at both the remote and the central customer premises equipment (CPE).

Examples

The following example enables alarms for the ALPS peer at IP address 172.22.0.91:

```
alps enable alarms peer 172.22.0.91
```

Related Commands

Command	Description
show alps peers	Displays the status of the ALPS partner peers.

alps enable-ascu

To move the previously defined agent-set control unit (ASCU) from the inactive poll list to the active poll list, use the **alps enable-ascu** command in Airline Product Set (ALPS) ASCU configuration submode. This move results in the protocol handler polling the ASCU and rendering it ready for handling terminal traffic. To remove the ASCU from the active poll list to the inactive poll list, use the **no** form of this command. This action prevents the ASCU from being polled, rendering it not ready for handling terminal traffic.

alps enable-ascu

no alps enable-ascu

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

ALPS ASCU submode

Command History

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

Examples

The following example moves the ASCU to the active poll list:

```
alps enable-ascu
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps enable-circuit

To enable the circuit to be activated when data is received from an agent-set control unit (ASCU), use the **alps enable-circuit** command in Airline Product Set (ALPS) circuit configuration submode. To disable the circuit, use the **no** form of this command.

alps enable-circuit

no alps enable-circuit

Syntax Description

This command has no arguments or keywords.

Command Default

The circuit is disabled by default.

Command Modes

ALPS circuit submode

Command History

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

Examples

The following example specifies the circuit to be activated when data is received from an ASCU:

```
alps enable-circuit
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps error-display

To specify where error messages about service availability or network problems are displayed, use the **alps error-display** command in Airline Product Set (ALPS) agent-set control unit (ASCU) configuration submode. To return to the default values, use the **no** form of this command.

alps error-display *number1 number2*

no alps error-display *number1 number2*

Syntax Description

number1	For P1024B airline link control (ALC), specifies the terminal address where these service messages are sent. Valid numbers are hexadecimal numbers in the range from 0x40 to 0x7F. The default address is 0x72. For P1024C Unisys Terminal System (UTS), specifies the screen line number where service messages are displayed. Valid numbers are hexadecimal numbers in the range from 0x00 to 0x7F. The default line number is 0x37.
number2	For P1024B ALC, specifies the screen line number where service messages are displayed. Valid numbers are hexadecimal numbers in the range from 0x40 to 0x7F. The default screen line number is 0x66. For P1024C UTS, specifies the column number where service messages are displayed. Valid numbers are hexadecimal numbers in the range from 0x00 to 0x7F. The default column number is 0x20.

Command Default

The default terminal address for P1024B ALC is 0x72.
The default screen line for P1024B ALC is 0x20.
The default line number for P1024C UTS is 0x37.
The default column number for P1024C UTS is 0x20.

Command Modes

ALPS ASCU submode

Command History

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

Examples

The following example specifies that error messages are displayed at terminal address 6d, on screen line number 78:

```
alps error-display 6d 78
```

Related Commands

Command	Description
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps host-hld host-link

To enable Airline Product Set (ALPS) on the X.25 interface, use the **alps host-hld host-link** command in interface configuration mode. To disable ALPS on the X.25 interface, use the **no** form of this command.

alps host-hld *hld* **host-link** *number* {**ax25** [**damp-tmr** *value*] | **emtox** *x.121* [*pseudo-conv*]} [**life-tmr** *value*] [**reply-tmr** *value*]

no alps host-hld *hld* **host-link** *number* {{**ax25** [**damp-tmr** *value*]} | {**emtox** *x.121* [*pseudo-conv*]}} [**life-tmr** *value*] [**reply-tmr** *value*]

Syntax Description

hld	Host high-level designator. A hexadecimal number in the range from 1 to 7f7f.
number	Host-link identifier. A number in the range from 1 to 255.
ax25	Specifies airline X.25 implementation of X.25.
damp-tmr *value*	(Optional) Specifies the AX.25 permanent virtual circuit (PVC) damping timer. The *value* argument is the length of time that a PVC can be inactive before it is destroyed and the corresponding ALPS circuits are closed. The default is 10 seconds.
emtox	Specifies EMTOX implementation of X.25.
x.121	X.121 address of the EMTOX host (called address on calls to the EMTOX host).
pseudo-conv	(Optional) Specifies the pseudo-conversational format of EMTOX packets.
life-tmr *value*	(Optional) Specifies the maximum amount of time (in seconds) that a message may be queued for sending to the host X.25 system before it is discarded. The *value* argument is time (in seconds).
reply-tmr *value*	(Optional) Specifies the duration of the no-reply timer. If the X.2 line is idle for this duration, and the X.25 transmit window is full, then ALPS sends an X.25 reset message on the virtual circuit to reset the transmit/receive windows. The no-reply timer can be configured for 10 to 600 seconds.

Command Default

The default damping timer value is 10 seconds.
The default no-reply timer value is 60 seconds.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example shows how to enable ALPS on the X.25 interface:

```
alps host-hld 1 host-link 1 emtox
```

alps hostlink

To specify information required to establish an X.25 virtual circuit at the central customer premises equipment (CPE), use the **alps hostlink** command in Airline Product Set (ALPS) circuit configuration submode. To remove the circuit definition from the configuration, send a close message on the ALPS circuit, and delete any queued messages for the circuit, use the **no** form of this command.

alps hostlink *number* {**ax25** *lcn* | **emtox** *x121-address*} [**winout** *val1*] [**winin** *val2*] [**ops** *val3*] [**ips** *val4*]

no alps hostlink *number* {**ax25** *lcn* | **emtox** *x121-address*} [**winout** *val1*] [**winin** *val2*] [**ops** *val3*] [**ips** *val4*]

Syntax Description

number	Interface at the host CPE. Decimal number in the range from 1 to 255.
ax25	Specifies airline X.25 implementation of X.25.
lcn	Local channel number for AX.25 connections.
emtox	Specifies EMTOX implementation of X.25.
x121-address	X.121 address for EMTOX connections. This is the X.121 calling address for X.25 call packets sent from the central CPE to the EMTOX host. This address is the source address in a call to the host.
winout *val1*	(Optional) Specifies the X.25 send window The *val1* argument is a decimal number in the range from 1 to 7.
winin *val2*	(Optional) Specifies the X.25 receive window. The *val2* argument is a decimal number in the range from 1 to 7.
ops *val3*	(Optional) Specifies the maximum output packet size. The *val3* argument is one of the following numbers: 128, 240, 256, 512, 1024, 2048, or 4096.
ips *val4*	(Optional) Specifies the maximum input packet size. The *val4* argument is one of the following numbers: 128, 240, 256, 512, 1024, 2048, or 4096.

Command Default

If no values are specified, the default values at the X.25-attached central CPE are used.

Command Modes

ALPS circuit submode

Command History

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

Examples

The following example establishes an X.25 virtual circuit at the central CPE. The configuration specifies airline X.25 implementation. The host CPE interface is 3, the local channel number for airline X.25 connections is 120, and the X.25 send window is 3.

```
alps hostlink 3 ax25 120 winout 3 winin 3
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

alps idle-timer

To specify (for dynamic circuits) the length of time that can elapse before an idle circuit is disabled, use the **alps idle-timer** command in Airline Product Set (ALPS) circuit configuration submode. To return to the default idle-timer value, use the **no** form of this command.

alps idle-timer *timer*

no alps idle-timer *timer*

Syntax Description

timer	Length of time that can elapse before an idle circuit is brought down. The range is from 10 to 600 seconds. The default is 60 seconds.

Command Default

The default length of time that can elapse before an idle circuit is brought down is 60 seconds.

Command Modes

ALPS circuit submode

Command History

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

Examples

The following example specifies that an idle circuit is maintained for 90 seconds before it is disabled:

```
alps idle-timer 90
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

alps keepalive

To enable TCP keepalives for Airline Product Set (ALPS) TCP peer connections, use the **alps keepalive** command in global configuration mode. A TCP keepalive request will be sent to the remote peer if the TCP connection to the remote peer is silent for a time period larger than the interval specified. The TCP connection to the ALPS host will be closed when a count equal to the retry count specified is missed consecutively. To disable keepalives for ALPS, use the **no** form of this command.

alps keepalive [**interval** *time*] [**retry** *count*]

no alps keepalive [**interval** *time*] [**retry** *count*]

Syntax Description

interval *time*	(Optional) Interval for keepalive requests. The *time* argument is the keepalive interval, in the range from 10 to 300 seconds. The default is 30 seconds.
retry *count*	(Optional) Indicates how many times keepalive requests will be sent before the connection is closed. The *count* argument is the retry count, in the range from 1 to 10. The default is three retries.

Command Default

The default keepalive interval is 30 seconds.
The default retry count is 3.

Command Modes

Global configuration (config)

Command History

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

Examples

The following example specifies that a TCP keepalive request will be sent to the remote peer if the TCP peer connection is idle for 60 seconds. The connection will be closed after three consecutive keepalive requests are sent.

```
alps keepalive interval 60 retry 8
```

Related Commands

Command	Description
alps local-peer	Specifies the IP address of the local peer.

alps lifetime-timer

To specify how long messages can be queued in the Airline Product Set (ALPS) circuit queue awaiting transmission to the central customer premises equipment (CPE), use the **alps lifetime-timer** command in ALPS circuit configuration submode. To return to the default lifetime-timer value, use the **no** form of this command.

alps lifetime-timer *timer*

no alps lifetime-timer *timer*

Syntax Description

timer	Length of time, in seconds, that a message can be queued. The range is from 1 to 20 seconds. The default is 4 seconds.

Command Default

The default length of time that a message can be queued in the ALPS circuit queue is 4 seconds.

Command Modes

ALPS circuit submode

Command History

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

Usage Guidelines

Messages that exceed the timer limit are discarded.

Examples

The following example specifies that a message remains in the ALPS circuit queue for no longer than 3 seconds:

```
alps lifetime-timer 3
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

alps local-hld remote-hld

To specify the local and remote high-level designator (HLD)s to use for this Airline Product Set (ALPS) circuit, use the **alps local-hld remote-hld** command in ALPS circuit configuration submode. To remove the definition from the configuration, use the **no** form of this command.

alps local-hld *loc-hld* **remote-hld** *rem-hld*

no alps local-hld *loc-hld* **remote-hld** *rem-hld*

Syntax Description

loc-hld	Local HLD to use for ALPS circuit. Hexadecimal number in the range from 1 to FFFF.
rem-hld	Remote HLD to use for ALPS circuit. Hexadecimal number in the range from 1 to FFFF.

Command Default

No default behavior or values.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(5)T	This command was modified and the **remote-hld** keyword was not applicable for mapping of airline traffic over IP (MATIP).
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **remote-hld** keyword is not applicable for ALPS with MATIP.

Examples

The following example specifies the local HLD as 4B10:

```
alps local-hld 4B10
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive airline link control (ALC) ASCU in the DOWN state.
show alps circuits	Displays the status of the ALPS circuits.

alps local-peer

To specify the IP address of the local peer, use the **alps local-peer** command in global configuration mode. To remove all subsequent Airline Product Set (ALPS) configuration commands from the device, use the **no** form of this command.

alps local-peer *ip-address* [**promiscuous**]

no alps local-peer *ip-address* [**promiscuous**]

Syntax Description

ip-address	IP address of the local peer.
promiscuous	(Optional) Keyword specified at the central customer premises equipment (CPE) to accept incoming TCP connections from any remote customer premises equipment (CPE).

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

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

Examples

The following example specifies the local peer IP address as 172.22.0.91 and specifies that the CPE accepts incoming TCP connections from any CPE:

```
alps local-peer 172.22.0.91 promiscuous
```

Related Commands

Command	Description
show alps peers	Displays the status of the ALPS partner peers.

alps matip-close-delay

To specify the interval between the closing and reopening of mapping of airline traffic over IP (MATIP) circuit connections, use the **alps matip-close-delay** command in Airline Product Set (ALPS) circuit configuration submode circuit submode command. To restore the definition to the default value, use the **no** form of this command.

alps matip-close-delay *time*

no alps matip-close-delay *time*

Syntax Description

time	Minimum number of seconds between the closing and reopening of an ALPS MATIP circuit. The range is from 1 to 90 seconds. The default is 10 seconds.

Command Default

The default value is 10 seconds.

Command Modes

ALPS circuit submode

Command History

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

Examples

The following example specifies a close delay time of 20 seconds:

```
alps matip-close-delay 20
```

Related Commands

Command	Description
show alps circuits	Displays the status of the ALPS circuits.

alps max-msg-length

To specify maximum input message length, use the **alps max-msg-length** command in Airline Product Set (ALPS) agent-set control unit (ASCU) configuration submode. To return to the default maximum input message length, use the **no** form of this command.

alps max-msg-length *value*

no alps max-msg-length *value*

Syntax Description

value	Maximum input message length. The range is from 1 to 3840. The default is 962 characters.

Command Default

The default maximum input message length is 962 characters.

Command Modes

ALPS ASCU submode

Command History

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

Examples

The following example specifies that the maximum length of a message is 1000 characters:

```
alps max-msg-length 1000
```

alps mpx

To specify the multiplexing and the agent-set control unit (ASCU) identification header for this circuit, use the **alps mpx** command in Airline Product Set (ALPS) ASCU configuration submode. To remove the definition from the configuration, use the **no** form of this command.

alps mpx {**group** | **single**} **hdr** {**a1a2** | **none**}

no alps mpx {**group** | **single**} **hdr** {**a1a2** | **none**}

Syntax Description

group	Specifies that multiple ASCUs will be multiplexed on the ALPS circuit. This setting is the default.
single	Specifies that only one ASCU will use this circuit.
hdr	Specifies the ASCU identification header for the circuit. The default is a1a2.
a1a2	ASCU identification via A1, A2.
none	No ASCU identification.

Command Default

The default for multiplexing is **group**.

The default header is a1a2.

Command Modes

ALPS circuit submode

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(1)	This command was available for general release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **alps mpx group** command is specified, multiple ASCUs will be multiplexed on this ALPS circuit and the **none** option is not applicable. If the **alps mpx single** command is specified, then only one ASCU uses this ALPS circuit. If **alps mpx single hdr none** command is specified, the A1 and A2 ASCU identification information is not added to the front of data frames sent across this circuit, and it is assumed that it does not exist in frames received on this circuit. The exclusion of ASCU identification should be specified only when the EMTOX protocol is used.

Examples

The following example shows how to specify the multiplexing and the ASCU identification header:

```
alps mpx group hdr a1a2
```

alps n1

To specify the threshold of consecutive errors logged before an agent-set control unit (ASCU) is declared down, use the **alps n1** command in interface configuration mode. To reassert the default number of consecutive errors before declaring an ASCU down, use the **no** form of this command.

alps n1 *errors*

no alps n1 *errors*

Syntax Description

errors	Error count limit. The valid range is from 1 to 30 errors. The default for airline link control (ALC) is 30 errors. The default for Unisys Terminal System (UTS) is 10 errors.

Command Default

The default ALC error count is 30 errors.

The default UTS error count is 10 errors.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(2)T	The error ranges were modified.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The error count limit is a threshold value. If the ASCU state is UP and the error count threshold is exceeded, the ASCU state changes to DOWN and it is moved to the inactive poll. If alarms are enabled for the ASCU, a Syslog message is displayed and an Simple Network Management Protocol (SNMP) notification is sent to the SNMP network management station.

Examples

The following example specifies that an ASCU is declared down when the error count exceeds one:

```
alps n1 1
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps n2

To specify the number of polls that must be correctly replied to before an agent-set control unit (ASCU) is declared up, use the **alps n2** command in interface configuration mode. To reassert the default number of polls that must be correctly replied to before an ASCU is declared up, use the **no** form of this command.

alps n2 *polls*

no alps n2 *polls*

Syntax Description

polls	Number of polls that must be correctly replied to. The valid range is from 1 to 30 polls. The default is 1 poll.

Command Default

The default number of polls that must be correctly replied to is one.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

If the ASCU state is DOWN and the reply threshold is exceeded, the ASCU state changes to UP and the ASCU is moved to the active poll list. If alarms are enabled for the ASCU, a Syslog message is displayed and an Simple Network Management Protocol (SNMP) notification is sent to the SNMP management station.

Examples

The following example specifies that two polls must be correctly replied to before the ASCU is declared up:

```
alps n2 2
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
encapsulation uts	Specifies that the P1024C Universal Terminal Support (UTS) protocol will be used on the serial interface.

alps n3

To specify the maximum number of retransmissions of an unacknowledged output data message to an agent-set control unit (ASCU), use the **alps n3** command in interface configuration mode. To reassert the default, use the **no** form of this command.

alps n3 *value*

no alps n3 *value*

Syntax Description

value	Maximum number of times an unacknowledged output data message can be re-sent. When the number is exceeded, the output data message is dropped. The valid range is from 1 to 10 resends. The default is 3 resends.

Command Default

The default number of resends is three.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

This command is valid only on 1026C interfaces.

Examples

The following example specifies that 6 is the maximum number of resends of an unacknowledged output data message to an ASCU:

```
alps n3 6
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
show alps ascu	Displays the status of the ALPS ASCU.

alps poll-pause

To set the minimum interval, in milliseconds, between two polls to the same agent-set control unit (ASCU), use the **alps poll-pause** command in interface configuration mode. To the default interval, use the **no** form of this command to revert.

alps poll-pause *milliseconds*

no alps poll-pause

Syntax Description

milliseconds	Minimum interval between polls, in milliseconds (ms). The valid range is from 10 to 1000 ms. The default interval is 50 ms.

Command Default

The default minimum interval is 50 ms.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example sets a 200-ms minimum interval between polls:

```
alps poll-pause 200
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.

alps primary-peer

To specify the primary TCP peer and, optionally, a backup TCP peer for an Airline Product Set (ALPS) circuit, use the **alps primary-peer** command in ALPS circuit configuration submode. To remove the definition from the configuration, use the **no** form of this command.

alps primary-peer *ip-address* [**backup-peer** *ip-address*]

no alps primary-peer *ip-address* [**backup-peer** *ip-address*]

Syntax Description

ip-address	IP address specified in the **alps remote-peer** command.
backup-peer	(Optional) Backup TCP peer for the ALPS circuit.
ip-address	(Optional) IP address specified in the **alps remote-peer** command.

Command Default

No default behavior or values.

Command Modes

ALPS circuit submode

Command History

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

Examples

The following example specifies a primary peer at IP address 172.22.0.91 and a backup peer at IP address 172.22.0.92:

```
alps primary-peer 172.22.0.91 backup-peer 172.22.0.92
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive airline link control (ALC) ASCU in the DOWN state.
show alps peers	Displays the status of the ALPS partner peers.

alps remote-peer

To specify the partner IP address for an Airline Product Set (ALPS) circuit, use the **alps remote-peer** command in global configuration mode. To remove the definition from the configuration, use the **no** form of this command.

alps remote-peer *ip-address* [**protocol** {**atp** | **matip-a**}] [**status-interval** *interval*] [**status-retry** *retries*] [**dynamic** [*inact-timer*] [**no-circuit** *no-circ-timer*]] [**tcp-qlen** [*number*]]

no alps remote-peer *ip-address* [**protocol** {*atp* | *matip-a*}] [**status-interval** *interval*] [**status-retry** *retries*] [**dynamic** [*inact-timer*] [**no-circuit** *no-circ-timer*]] [**tcp-qlen** [*number*]]

Syntax Description

ip-address	IP address of the peer.
protocol {**atp** | **matip-a**}	(Optional) Specifies the type of encapsulation for the connection. The following options are available: • ALPS Tunneling Protocol encapsulation. This encapsulation is the default. • mapping of airline traffic over IP (MATIP) Type A (conversational) encapsulation.
status-interval *interval*	(Optional) Specifies amount of time, in seconds, between sending of MATIP status messages. The messages verify the integrity of the TCP connection. Number of seconds between status messages. The range is from 0 to 300 seconds. The default value is 0 (off).
status-retry *retries*	(Optional) Specifies number of times to retry sending a MATIP status message before the peer connection is closed. Number of retries. The range is from 0 to 100 retries. The default value is 2.
dynamic *inact-timer*	(Optional) Allows the TCP connection to the host peer to be opened only when there is data to be transferred to the host reservation system. Length of inactivity, in seconds, after which the connection is closed. The range is from 0 to 300 seconds. The default is 30 seconds. A value of zero indicates that the timer is disabled.
no-circuit *no-circ-timer*	(Optional) Specifies amount of time, in seconds, that a peer will stay connected while no circuits are using the peer connection. This parameter is valid only if the dynamic parameter is first configured. Number of seconds before which the timer will expire. The range is from 0 to 3600 seconds. The default is 90 seconds.
tcp-qlen *number*	(Optional) Specifies the maximum length of a TCP queue for peer connections. Number of packets allowed in the TCP queue. The range is from 26 to 100 packets. The default is 50 packets.

Command Default

The default for the **status-interval** argument is 0 (off).
The default for the **status-retry** argument is 2.
The default for the **dynamic** argument is 30 seconds.
The default for the **no-circuit** argument is 90 seconds.
The default for the **tcp-qlen** argument is 50 packets.

Command Modes Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.0(5)T	The **protocol**, **status-interval**, **status-retry** and the **no-circuit** keyword options were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the protocol option is configured for MATIP, the peer connection is dynamic.

When the protocol option is configured for ALPS Tunneling Protocol (ATP), the peer connection is permanent.

The **no-circuit** option within the dynamic keyword does not apply to permanent airline link control (ALC)/Universal Terminal Support (UTS) connections.

The **status-interval** and **status-retry** options apply only to the MATIP protocol.

Issuing the **no alps remote-peer** command does the following:

- Closes TCP connection.
- Notifies the partner TCP peer that this connection is closed.

Notifies the ALPS circuits using this TCP peer that the connection is closed.

Examples

The following example specifies a MATIP peer connection at IP address 10.22.0.92. Status messages will be sent every 9 seconds and will be resent twice before the connection is closed. The maximum TCP length is 30:

```
alps remote-peer 10.22.0.92 protocol matip-a status-interval 9 status-retry 2 tcp-qlen 30
```

Related Commands

Command	Description
alps local-peer	Specifies the IP address of the local peer.
show alps peers	Displays the status of the ALPS partner peers.

alps retry-option

To configure the customer premises equipment (CPE) to signal the agent-set control unit (ASCU) whenever an error is detected, use the **alps retry-option** command in Airline Product Set (ALPS) ASCU configuration submode. To reassert the default action of no retry, use the **no** form of this command.

alps retry-option {**resend** | **reenter**}

no alps retry-option

Syntax Description

resend	Specifies the retry option as resend. This option causes an indicator LED to signal the operator at the ASCU to resend data.
reenter	Specifies the retry option as reenter. This option causes a service message to signal the operator at the ASCU to reenter data.

Command Default

The default retry option is no retry.

Command Modes

ALPS ASCU submode

Command History

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

Usage Guidelines

This command is applicable only for P1024B automatic level control (ALC) interfaces; it is invalid on P1024C Unisys Terminal System (UTS) interfaces.

Examples

The following example specifies that an indicator LED signals the ASCU to resend data:

```
alps retry-option resend
```

Related Commands

Command	Description
alps ascu	Specifies a physical ASCU identity.
encapsulation uts	Specifies that the P1024C UTS protocol will be used on the serial interface.

alps service-msg data-drop

To specify where to retrieve the terminal address to be used when a service message is sent to an agent-set control unit (ASCU) as the result of a dropped data message, use the **alps service-msg data-drop** command in interface configuration mode. To remove the terminal address specification, use the **no** form of this command.

alps service-msg data-drop {**msg-term** | **config-term**}

no alps service-msg data-drop {**msg-term** | **config-term**}

Syntax Description

msg-term	Specifies that the service message will be sent to the terminal address of the dropped message.
config-term	Specifies that the service message terminal address is the same address configured in the **alps-error display** command.

Command Default

The **config-term option** is the default.
If this command is not configured and a data message is dropped from a terminal, the resulting service message is sent to the terminal specified in the **alps error-display** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to serial interfaces configured with airline link control (ALC) encapsulation only.

Examples

The following example specifies that service messages resulting from dropped data messages are sent to the terminal address of the dropped message:

```
alps service-msg data-drop msg-term
```

Related Commands

Command	Description
alps error-display	Specifies where error messages about service availability or network problems are displayed.
encapsulation alc	Specifies that the P1024B ALC protocol is used on the serial interface.

alps service-msg format

To specify the protocol format of service messages sent from the device to an agent-set control unit (ASCU), use the **alps service-msg format** command in interface configuration mode. To remove the protocol format specification, use the **no** form of this command.

alps service-msg format {**sita** | **apollo**}

no alps service-msg format {**sita** | **apollo**}

Syntax Description

sita	Specifies the sita protocol format.
apollo	Specifies the apollo protocol format.

Command Default

The default protocol format is **sita**.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to serial interfaces configured with automatic level control (ALC) encapsulation only.

Examples

The following example specifies the apollo protocol format:

```
alps service-msg format apollo
```

Related Commands

Command	Description
encapsulation alc	Specifies that the P1024B airline link control (ALC) protocol is used on the serial interface.

alps service-msg status-change

To specify that service messages for Airline Product Set (ALPS) circuit status changes be sent to agent-set control unit (ASCU)s on the serial interface, use the **alps service-msg status-change** command in interface configuration mode. To send service messages for ALPS circuit status changes only when airline link control (ALC) data messages are dropped, use the **no** form of this command.

alps service-msg status-change

no alps service-msg status-change

Syntax Description

This command has no arguments or keywords.

Command Default

The default is on. Unless the **no** form of this command is configured, unsolicited service messages are sent to all ASCUs multiplexed on the mapping of airline traffic over IP (MATIP) session when the following ALPS circuit events occur:

- MATIP session status change
- ASCU status change

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to serial interfaces configured with ALC encapsulation only.

If the **no** form of this command is configured, service messages for ALPS circuit status changes are sent only when airline link control (ALC) data messages are dropped.

Examples

The following example specifies that unsolicited service messages resulting from ALPS circuit status changes be sent to ASCUs on the serial interface:

```
alps service-msg status-change
```

Related Commands

Command	Description
encapsulation alc	Specifies that the P1024B ALC protocol is used on the serial interface.

alps service-msg-interval

To specify the interval between consecutive transmissions of service messages from the remote customer premises equipment (CPE) to the agent-set control unit (ASCU), use the **alps service-msg-interval** command in Airline Product Set (ALPS) circuit configuration submode. To remove the definition from the configuration, use the **no** form of this command.

alps service-msg-interval *seconds*

no alps service-msg-interval *seconds*

Syntax Description

seconds	Interval, in seconds, between consecutive sendings of service messages from the remote CPE to the ASCU. The range is from 1 to 20 seconds. The default interval is 4 seconds.

Command Default

The default interval between consecutive sendings of service messages from the remote CPE to the ASCU is 4 seconds.

Command Modes

ALPS circuit submode

Command History

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

Usage Guidelines

The “PLEASE RETRY” message is sent only to ASCUs that use circuits with a dynamic connection type.

Examples

The following example specifies an interval of 3 seconds between sending service messages from the CPE to the ASCU:

```
alps service-msg-interval 3
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive ALC ASCU in the DOWN state.
alps service-msg-list	Defines the service message list to be used for this circuit.

alps service-msg-list

To define the service message list to be used for this circuit, use the **alps service-msg-list** command in Airline Product Set (ALPS) circuit configuration submode. To remove the list from the circuit configuration, thus issuing no service messages until another list is configured, use the **no** form of this command.

alps service-msg-list *list*

no alps service-msg-list *list*

Syntax Description

list	The service message list to be used for this circuit. The valid numbers are from 1 to 8.

Command Default

No default behavior or values.

Command Modes

ALPS circuit submode

Command History

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

Examples

The following example specifies that message list 1 is used for this circuit:

```
alps service-msg-list 1
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive airline link control (ALC) ASCU in the DOWN state.
alps service-msg-interval	Specifies the interval between consecutive transmissions of service messages from the remote CPE to the agent-set control unit (ASCU).

alps service-msg-list number

To define the service message identity and its contents for a service message list, use the **alps service-msg-list number** command in global configuration mode. To remove a service message number from the service message list configuration, use the **no** form of this command.

alps service-msg-list *list* **number** *number message*

no alps service-msg-list *list* **number** *number message*

Syntax Description

list	Service message list to be used for this circuit. Valid numbers are from 1 to 8.
number	List number. Valid numbers are from 1 to 8.
message	Contents of a service message. Maximum number of characters allowed in a service message is 32. **Note** Configuring the *message* argument with a value of OFF disables this particular service message.

Command Default

The default service message is used if no service message list number is specified.

Table 9 shows the default service message text strings.

Table 9 Service Message Default Text Strings

Message Number	Event	Text String
1	ALPS circuit to host is opened.	CONNECTION UP
2	X.25 virtual circuit at the host is cleared.	DISC BY THE HOST
3	X.25 interface at the host is down.	HOST ISOLATED
4	No response from the host device when trying to establish a connection.	NETWORK PROBLEM
5	Connection to host was disconnected because of inactivity.	READY TO CONNECT
6	Network is congested.	CONGESTION
7	Network congestion has cleared.	PLEASE PROCEED
8	Network operator has disabled the path to the host.	DISC BY NET OPERAT

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.1(2)T	The OFF option was added to the *message* argument and the maximum service message length was increased to 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To disable a particular service message, configure the *message* argument with a value of OFF.

Examples

The following example specifies the text of message list 1, message number 2:

```
alps service-msg-list 1 number 2 "Turn off the terminal NOW."
```

The following example disables service message 3 from list 1:

```
alps service-msg-list 1 number 3 $OFF$
```

Related Commands

Command	Description
alps service-msg list	Defines the service message list to be used for this circuit.

alps servlim

To specify the number of polls of the agent-set control unit (ASCU) UP list allowed between two successive polls of the ASCU DOWN list, use the **alps servlim** command in interface configuration mode. To reassert the default number of cycles through the normal (active) poll list allowed before the slow poll list is processed, use the **no** form of this command.

alps servlim *polls*

no alps servlim *polls*

Syntax Description

polls	Number of polls of the ASCU UP list. The valid range is from 1 to 512 polls. The default is 30 polls.

Command Default

The default number of polls of the ASCU UP list allowed between two successive polls of the ASCU DOWN list is 30 polls.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example specifies that five polls of the ASCU UP list are allowed between two successive polls of the ASCU DOWN list.

```
alps servlim 5
```

Related Commands

Command	Description
alps n1	Specifies the threshold of consecutive errors logged before an ASCU is declared down.
alps n2	Specifies the number of polls that must be correctly replied to before an ASCU is declared up.
alps t1	Specifies the timeout delay between polling and response.
alps t2	Specifies the timeout delay between receipt of the first character of an IP sequence solicited by a poll and receipt of a GA sequence.

alps t1

To specify the timeout delay between polling and response, use the **alps t1** command in interface configuration mode. To reassert the default poll timeout value of 0.5 seconds, use the **no** form of this command.

alps t1 *delay*

no alps t1 *delay*

Syntax Description

delay	Timeout delay, in seconds, between polling and response. The valid range is from 1 to 20-tenths of a second (0.1 to 2 seconds). The default is 5-tenths of a second (0.5 second).

Command Default

The default timeout delay between polling and response is 5-tenths of a second (0.5 second).

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3(6)T	This command was introduced.
12.1(2)T	The range for the timeout delay was extended.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example specifies a 0.5-second timeout delay between polling and response:

```
alps t1 5
```

Related Commands

Command	Description
alps n1	Specifies the threshold of consecutive errors logged before an agent-set control unit (ASCU) is declared down.
alps n2	Specifies the number of polls that must be correctly replied to before an ASCU is declared up.
alps servlim	Specifies the number of polls of the ASCU UP list allowed between two successive polls of the ASCU DOWN list.
alps t2	Specifies the timeout delay between receipt of the first character of an IP sequence solicited by a poll and receipt of a Go Ahead (GA) sequence.

Command	Description
encapsulation alc	Specifies that the P1024B airline link control (ALC) protocol is used on the serial interface.
encapsulation uts	Specifies that the P1024C UTS protocol is used on the serial interface.

alps t2

To specify the timeout delay between receipt of the first character of an I/P sequence solicited by a poll and receipt of a Go Ahead (GA) sequence, use the **alps t2** command in interface configuration mode. To reassert the default timeout value of 6 seconds, use the **no** form of this command.

alps t2 *delay*

no alps t2 *delay*

Syntax Description

delay	Timeout delay, in seconds, between receipt of first character of an I/P sequence solicited by a poll and receipt of GA sequence. The valid range is from 1 to 10 seconds. The default is 6 seconds.

Command Default

The default timeout delay between receipt of first character of an I/P sequence solicited by a poll and receipt of GA sequence is 6 seconds.

Command Modes

Interface configuration (config-if)

Command History

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

Examples

The following example specifies a timeout delay of 8 seconds between receipt of the first character of an I/P sequence solicited by a poll and receipt of a GA sequence:

```
alps t2 8
```

Related Commands

Command	Description
alps n1	Specifies the threshold of consecutive errors logged before an agent-set control unit (ASCU) is declared down.
alps n2	Specifies the number of polls that must be correctly replied to before an ASCU is declared up.
alps servlim	Specifies the number of polls of the ASCU UP list allowed between two successive polls of the ASCU DOWN list.
alps t1	Specifies the timeout delay between polling and response.

alps translate

To map an X.121 address to an IP address of a remote peer, use the **alps translate** command in interface configuration mode. To remove mapping from the configuration, use the **no** form of this command.

alps translate *x.121-address ip-address*

no alps translate *x.121-address ip-address*

Syntax Description

x.121-address	X.121 address to be mapped to an IP address of a remote peer.
ip-address	IP address of the remote peer.

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

The X.121 address is compared to the Called Address on inbound X.25 call packets to determine if the call should be accepted. The X.121 address may have an asterisk (*) at the end to indicate “all X.121 addresses prefixed with the address before the *.”

Examples

The following example maps all X.121 addresses prefixed with the address 88845 to the remote peer IP address 172.22.0.90:

```
alps translate 88845* 172.22.0.90
```

Related Commands

Command	Description
encapsulation x25	Specifies operation of a serial interface as an X.25 device.

alps update-circuit

To update one or more Airline Product Set (ALPS) circuits, use the **alps update-circuit** command in user EXEC or privileged EXEC mode. If a circuit name is specified, then only that circuit will be updated; otherwise, all circuits will be updated.

alps update-circuit [*name*]

Syntax Description

name	(Optional) Specifies name of the circuit to update.

Command Default

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Usage Guidelines

If the **alps update-circuit** command is issued for a circuit that is using the ALPS Tunneling Protocol (ATP) protocol, the circuit will be closed and reopened.

If the **alps update-circuit** command is issued for a circuit that is using the mapping of airline traffic over IP (MATIP) protocol, a configuration update will be sent in the form of a MATIP Session Open command.

The **alps update-circuit** command is effective only for ALPS circuits that are enabled and active (opening or opened state).

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

Examples

The following example specifies that circuit 1 has been updated:

```
Device# alps update-circuit CKT-1
```

Related Commands

Command	Description
alps auto-reset	Automatically resets a nonresponsive airline link control (ALC) agent-set control unit (ASCU) in the DOWN state.

Command	Description
alps enable-circuit	Enables the circuit to be activated when data is received from an ASCU.
show alps circuits	Displays the status of the ALPS circuits.

asp addr-offset

To configure an asynchronous port to send and receive polled asynchronous traffic through a block serial tunnel (BSTUN), use the **asp addr-offset** command in interface configuration mode. To disable the traffic flow through a BSTUN, use the **no** form of this command.

asp addr-offset *address-offset*

no asp addr-offset

Syntax Description

address-offset	Location of the address byte within the polled asynchronous frame being received. The range is from 0 to 255. The default value is 0.

Command Default

No polled asynhronous protocol group is defined within the frame of the address byte.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **asp addr-offset** *address-offset* command to specify the offset from the start of the frame where the address byte is located. This command is applicable only when the asynchronous-generic protocol is specified on an interface using a combination of the **bstun protocol-group** command in global configuration mode and the **bstun group** command in interface configuration mode.

Interfaces configured to run the asynchronous-generic protocol have the following configuration:

- baud rate set to 9600 bps
- 8 data bits
- no parity
- 1 start bit
- 1 stop bit

If different line configurations are required, use the **rxspeed** command, **txspeed** command, **databits** command, **stopbits** command, and **parity line** command in the global configuration mode to change the line attributes. The addresses of the alarm panels must be used in the address field of the **bstun route address** command in the interface configuration mode

Examples

The following example shows that the fifth byte in the polled asynchronous frame contains the device address:

```
Device(config)# interface Serial 3/0
Device(config-if)# physical-layer async
Device(config-if)# encapsulation bstun
Device(config-if)# asp addr-offset 5
Device(config-if)# end
```

Related Commands

Command	Description
asp role	Specifies whether the device is acting as the primary end of the polled asynchronous link or the secondary end of the polled asynchronous link connected to the serial interface, and whether the attached remote device is a security alarm control station.
asp rx-ift	Specifies a time period that, by expiring, signals the end of one frame being received and the start of the next.
bstun group	Specifies the BSTUN group to which the interface belongs.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

asp broadcast-addr

To specify the address byte that asynchronous serial protocols (ASP) use to broadcast packets from their remote stations, use the **asp broadcast-addr** command in interface configuration mode. To disable asynchronous broadcast, use the **no** form of this command.

asp broadcast-addr *address*

no asp broadcast-addr

Syntax Description

address	Broadcast address in hexadecimal format. The range is from 0 to 0xff.

Command Default

No broadcast address is defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.2(3)T	This command was modified. Support was extended to enable the ASP broadcast mask to transmit packets as broadcasts.

Usage Guidelines

Use the **asp broadcast-addr** command to specify the address byte that Asynchronous Serial Protocols (ASP) use to broadcast packets. All packets that are to be broadcast are copied and sent to all peers defined on the serial interface. The broadcast addresses identify the packets transmitted to all remote devices in the same Block Serial Tunnel (BSTUN) group.

For example, the address values configured using the **bstun route** command can be 01, 02, 03, and so on. If the address value is configured using the **asp broadcast-addr ff** command, the packets received are considered as a broadcast. These packets are transmitted to all remote devices in that BSTUN group.

Note A broadcast-mask value of ff identifies all packets as broadcasts. Therefore, all address bytes in the range 0x00 to 0xff are classified as broadcasts.

Examples

The following example shows how to configure an asynchronous broadcast address using the address ff:

```
Device(config)# interface Serial 3/0
Device(config-if)# asp broadcast-addr ff
Device(config-if)# end
```

Related Commands

Command	Description
asp eof-char	Specifies an EOF character for the asynchronous generic application that is used to end ASP transmissions.
asp ignore-sequence-number	Instructs a device to ignore the ASP sequence numbers that are used to synchronize ASP traffic between head-end and tail-end devices.
asp sof-char	Specifies an SOF character for the asynchronous generic application.
brdcast-address-mask	Allows the configuration of multiple address masks.

asp brdcast-address-mask

To specify the bit or bits in the address byte that the asynchronous serial protocols (ASP) use to broadcast packets from their remote stations, use the **asp brdcast-address-mask** command in interface configuration mode. To disable the bit or bits in the address byte that the ASP uses to broadcast packets, use the **no** form of this command.

asp brdcast-address-mask *address*

no asp brdcast-address-mask

Syntax Description

address	Broadcast address in hexadecimal format. The range is from 0 to 0xff.

Command Default

No address masks are configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(3)T	This command was modified. Support was extended to enable the ASP broadcast mask to transmit packets as broadcasts.

Usage Guidelines

This command will force the ASP to take an ASP asynchronous character and mask it to check if it is a valid broadcast address mask. The broadcast address mask is predetermined; for example, you can set up your network such that any address above 0x7f is a broadcast address mask. Broadcast addresses identify packets that are transmitted to all remote devices in the same block serial tunnel (BSTUN) group.

For example, use the **asp brdcast-address-mask 80** command to set up the network such that any address beyond 0x7f is a broadcast address. The broadcast address is logically anded with the address byte. If the resulting value is not zero, the address is considered as a broadcast.

Note A broadcast-mask value of 0xff identifies all packets as broadcasts. Therefore, all address bytes in the range 0x00 to 0xff are classified as broadcasts.

Examples

The following example shows the configuration of ASP address broadcast mask 30 on the Serial interface:

```
Device(config)# interface Serial 0/0
Device(config-if)# asp brdcast-address-mask 30
Device(config-if)# end
```

Related Commands

Command	Description
asp addr-offset	Configures an asynchronous port to send and receive polled asynchronous traffic through a BSTUN.
asp broadcast-addr	Specifies the address that an asynchronous generic application uses to broadcast packets from its remote stations.
asp role	Allows configuration of multiple address masks.

asp dcd always

To specify that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when the serial interface starts, use the **asp dcd always** command in interface configuration mode. To specify that DSR and DCD are to be asserted when the HAYES AT connect message is sent to the point of sale (POS) device, use the **no** form of this command.

asp dcd always

no asp dcd always

Syntax Description

This command has no arguments or keywords.

Command Default

The **asp dcd always** command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For APOS, the device always functions as the DCE. If the **asp dcd always** command is enabled, then both DSR and DCD will be asserted when the serial interface is started.

If the **asp dcd always** command is disabled, then DSR and DCD are asserted when the HAYES AT connect message is sent to the POS device. When the connection to the POS device is terminated, DSR and DCD are de-asserted.

Some POS devices require that the DSR and DCD work independently, and that DSR be asserted when the serial interface starts and DCD be asserted when the connect message is sent. This requires a modified cable to disconnect the DTR and DSR connection in both directions, and on the DB25 side of the connector tying the DTE's output DTR to the DTE's input DSR.

If the **asp dcd always** command is disabled, then DSR and DCD are asserted when the HAYES AT connect message is sent to the POS device. When the connection to the POS device is terminated, DSR and DCD are de-asserted. For devices using modified cables that require that DCD be asserted only where there is a connection to the host, the **asp dcd always** command should be disabled.

Examples

The following example configures the **asp dcd always** command:

```
asp dcd always
```

Related Commands

Command	Description
asp direct	Disables dial mode and automatically activate the peer connection.
asp enq	Configures how the device sends ENQ(0x05) messages to the terminal.
asp retries	Specifies the number of times a packet will be resent before the connection with the terminal is disconnected.
asp send ack	Enables the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests.
asp timer	Customizes the ASP timers.

asp direct

To disable dial mode and automatically activate the peer connection, use the **asp direct** command in interface configuration mode. To enable dial mode, use the **no** form of this command.

asp direct

no asp direct

Syntax Description

This command has no arguments or keywords.

Command Default

The **asp direct** command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **asp direct** command is enabled, the connect timer is used to reactivate the connection if the peer connection goes down.

Examples

The following example configures the **asp direct** command:

```
asp direct
```

Related Commands

Command	Description
asp dcd always	Specifies that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when traffic starts to the serial interface.
asp enq	Configures how the device sends ENQ(0x05) messages to the terminal.
asp retries	Specifies the number of times a packet will be resent before the connection with the terminal is disconnected.
asp send ack	Enables the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests.
asp timer	Customizes the ASP timers.

asp enq

To configure how the device sends ENQ(0x05) messages to the terminal, use the **asp enq** command in interface configuration mode. To restore the default method of sending of ENQ messages to the terminal to initiate sessions, use the **no** form of this command.

asp enq {**disable** | **delay** *milliseconds*}

no asp enq {**disable** | **delay**}

Syntax Description

disable	Disables the device from sending ENQ messages to the terminal to initiate sessions.
delay	Configures a delay between the sending of a connect message and the ENQ message.
milliseconds	Duration of the delay in milliseconds. Allowed values are from 1 to 1000.

Command Default

By default, ENQ messages are sent to the terminal.
milliseconds: 10 milliseconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **asp enq disable** command should be enabled only if the terminal the device is connecting to does not require ENQ messages as part of the session flow.

The **delay** keyword can be used to slow responses in dialed networks.

Examples

The following example specifies that ENQ messages be sent 500 milliseconds after the connect message is sent:

```
asp enq delay 500
```

Related Commands

Command	Description
asp dcd always	Specifies that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when traffic starts to the serial interface.
asp direct	Disables dial mode and automatically activate the peer connection.
asp retries	Specifies the number of times a packet will be resent before the connection with the terminal is disconnected.
asp send ack	Enables the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests.
asp timer	Customizes the ASP timers.

asp eof-char

To specify an end-of-frame (EOF) character for asynchronous serial protocols (ASP) to use to end ASP transmissions, use the **asp eof-char** command in interface configuration mode. To remove a previously configured EOF character, use the **no** form of this command.

asp eof-char *eof-character*

no asp eof-char

Syntax Description

eof-character	EOF character in hexadecimal format. The range is from 0 to ff.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **asp eof-char** command is enabled, asynchronous serial protocols (ASP) stops receiving characters when it receives the specified EOF character. When the **asp eof-char** command is disabled, ASP continues to receive characters until the RX-IFT timer expires.

Examples

The following example sets 3e as the EOF character:

```
asp eof-char 3e
```

Related Commands

Command	Description
asp broadcast-addr	Specifies the address that an asynchronous generic application uses to broadcast packets from its remote stations.
asp ignore-sequence-number	Instructs a device to ignore the ASP sequence numbers that are used to synchronize ASP traffic between head-end and tail-end devices.
asp sof-char	Specifies an SOF character for the asynchronous generic application.

asp ignore-sequence-number

To instruct a device to ignore the asynchronous serial protocols (ASP) sequence numbers that are used to synchronize ASP traffic between head-end and tail-end devices, use the **asp ignore-sequence-number** command in interface configuration mode. To instruct a device to use the ASP sequence numbers to validate ASP traffic, use the **no** form of this command.

asp ignore-sequence-number

no asp ignore-sequence-number

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled. The ASP sequence numbers are used to validate ASP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **asp ignore-sequence-number** command should be enabled when there is not a one-to-one correspondence between commands from the head-end device and commands from the tail-end device.

When the **asp ignore-sequence-number** command is disabled, ASP validates the sequence numbers.

Examples

The following example instructs the device to ignore ASP sequence numbers:

```
asp ignore-sequence-number
```

Related Commands

Command	Description
asp broadcast-addr	Specifies the address that an asynchronous application uses to broadcast packets from its remote stations.
asp eof-char	Specifies an EOF character for the asynchronous generic application to use to end ASP transmissions.
asp sof-char	Specifies an SOF character for the asynchronous generic application.

asp retries

To specify the number of times a packet will be resent before the connection with the terminal is disconnected, use the **asp retries** command in interface configuration mode. To reset the number of asynchronous serial protocols (ASP) retries to its default value, use the **no** form of this command.

asp retries *number*

no asp retries

Syntax Description

number	Number of times a packet will be resent before the connection with the terminal is disconnected. Allowed values are from 1 to 10.

Command Default

number: 4

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures ten ASP retries:

```
Device(config-if)# asp retries 10
```

Related Commands

Command	Description
asp dcd always	Specifies that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when traffic starts to the serial interface.
asp direct	Disables dial mode and automatically activate the peer connection.
asp enq	Configures how the device sends ENQ(0x05) messages to the terminal.
asp send ack	Enables the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests.
asp timer	Customizes the ASP timers.

asp role

To specify that the device is the primary end or the secondary end of the polled asynchronous link that is connected to a serial interface and that the attached remote device is a security alarm control station, use the **asp role** command in interface configuration mode. To remove the specification, use the **no** form of this command.

asp role {**primary** | **secondary**}

no asp role

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

This command configures the interface as primary or secondary to the device on which asynchronous serial protocol (ASP) is configured. Configure the interface connected to the alarm console as the secondary device and the interface connected to the alarm panel as the primary device. The addresses of the alarm panels must be used in the address field of the **bstun route address** command in the interface configuration mode.

Examples

The following example shows how to specify the device as the primary end of the link:

```
Device(config)# interface Serial 3/0
Device(config-if)# asp role primary
Device(config-if)# end
```

Related Commands

Command	Description
asp brdcast-address-mask	Allows the configuration of multiple address masks.
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

asp rx-ift

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

asp rx-ift *interframe-timeout*

no asp rx-ift

Syntax Description

interframe-timeout	Number of milliseconds between the end of one frame being received and the start of the next frame. The default timeout value is 40 milliseconds.

Command Default

The default timeout value is 40 ms.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

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

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

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

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

Examples

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

```
asp rx-ift 6
```

Related Commands

Command	Description
asp addr-offset	Configures an asynchronous port to send and receive polled asynchronous traffic through a BSTUN tunnel.
asp role	Specifies whether the device is acting as the primary end of the polled asynchronous link or as the secondary end of the polled asynchronous link connected to the serial interface, and whether the attached remote device is a security alarm control station.
bstun protocol-group	Defines a BSTUN group and the protocol it uses.
bstun route	Defines how frames will be forwarded from a BSTUN interface to a remote BSTUN peer.

asp send ack

To enable the sending of ACK(0x06) messages to the terminal to acknowledge terminal requests, use the **asp send ack** command in interface configuration mode. To disable the sending of ACK messages, use the **no** form of this command.

asp send ack

no asp send ack

Syntax Description

This command has no arguments or keywords.

Command Default

The **asp send ack** command is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the **asp send ack** command is enabled, an acknowledgement is immediately sent when the device receives a packet. If the **asp send ack** command is disabled, an acknowledgement is not sent until the device receives a response from the host.

Examples

The following example configures the **asp send ack** command:

```
asp send ack
```

Related Commands

Command	Description
asp dcd always	Specifies that both data set ready (DSR) and data carrier detect (DCD) are to be asserted when traffic starts to the serial interface.
asp direct	Disables dial mode and automatically activate the peer connection.
asp enq	Configures how the device sends ENQ(0x05) messages to the terminal.
asp retries	Specifies the number of times a packet will be resent before the connection with the terminal is disconnected.
asp timer	Customizes the ASP timers.

asp sof-char

To specify a start-of-frame (SOF) character, use the **asp sof-char** command in interface configuration mode. To remove a previously configured SOF character, use the **no** form of this command.

asp sof-char *address*

no asp sof-char

Syntax Description

address	SOF character in hexadecimal format. The range is from 0 to ff.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the **asp sof-char** command is enabled, asynchronous serial protocols (ASP) ignores any characters received prior to the specified SOF character. When the **asp sof-char** command is disabled, ASP receives all characters.

Examples

The following example sets d9 as the SOF character:

```
asp sof-char d9
```

Related Commands

Command	Description
asp broadcast-addr	Specifies the address that an asynchronous generic application uses to broadcast packets from its remote stations.
asp eof-char	Specifies an EOF character for the asynchronous generic application to use to end ASP transmissions.
asp ignore-sequence-number	Instructs a device to ignore the ASP sequence numbers that are used to synchronize ASP traffic between head-end and tail-end devices.

asp timer

To customize the asynchronous serial protocols (ASP) timers, use the **asp timer** command in interface configuration mode. To reset the ASP timers to their default values, use the **no** form of this command.

asp timer {**rsp** *rsp-time* | **rx** *rx-time* | **host** *host-time* | **connect** *connect-time*}

no asp timer {**rsp** | **rx** | **host** | **connect**}

Syntax Description

rsp	Duration the device will wait for a response to a packet before resending.
rsp-time	Allowed values are from 1 to 30 seconds.
rx	Duration the device will wait for the entire packet to be received, beginning when the STX(0x02) character is received.
rx-time	Allowed values are from 10 to 60 seconds.
host	Duration the device will wait for a response packet from the host, beginning when the terminal request is forwarded to APIP
host-time	Allowed values are from 10 to 120 seconds.
connect	Duration the device will wait for the peer connection to activate when in dial mode, beginning when the device receives a dial string.
connect-time	Allowed values are from 1 to 30 seconds.

Command Default

rsp-time: 7 seconds
rx-time: 15 seconds
host-time: 60 seconds
connect-time: 8 seconds

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the RSP timer to 30 seconds, the RX timer to 60 seconds, the host timer to 120 seconds and the connect timer to 30 seconds:

```
asp timer rsp 30
asp timer rx 60
asp timer host 120
asp timer connect 30
```