CHAPTER 5

Site Configuration Commands

This chapter defines the commands used to configure a site table entry that contains information about the other end of your dialup network connection, whether dialing in or out, or both. The order of site commands is unimportant *except* that **max-ports** must be the last command for **continuous** or **on-demand** sites.

For examples using site commands see the chapter “Configuring the Cisco 1020” in the *Cisco 1020 User Guide*.

dial-on

This command determines when dial out to a site occurs.

dial-on {continuous|demand|manual}

Syntax Description

continuous	The router always keeps the dial-up connection to the site active. If the connection is lost the router will re-dial to the site.
demand	The router will dial and establish a connection to the site only when packets are queued for that site. The router creates a network interface and the appropriate routing information to notify the attached local area network of the available connectivity of the remote site.
manual	The router will dial to the site only if the Privileged EXEC **dial** command is used.

Command Mode

Site Configuration

Usage Guidelines

When switching a location from **manual** to **demand** make sure the dial-out connection has been closed before making the change to the site entry. This can be done with the **clear interface** Privileged EXEC command used on whichever interface(s) are currently in use for that site.

Related Commands

dial

dialgroup

This command identifies the dial group to use when establishing a dial out connection to this site.

dialgroup *number*

Syntax Description

number The number of the dial group to use, between 0 and 99.

Command Mode

Site Configuration

Usage Guidelines

Use the **dialer rotary-group** interface configuration command with the same *number* to indicate interface(s) which may be used when dialing out to this site.

Related Commands

dialer rotary-group

encapsulation

To configure Serial Line Internet Protocol (SL/IP) encapsulation, use the **encapsulation slip** site configuration command. To configure Point-to-Point Protocol (PPP) encapsulation, use the **encapsulation ppp** site configuration command.

encapsulation slip
encapsulation ppp

Syntax Description

This command has no arguments or keywords.

Command Mode

Site configuration

Usage Guidelines

SLIP is designed to encapsulate Internet Protocol (IP) datagrams over point-to-point links. PPP can encapsulate IP, IPX, or both over point-to-point links.

ip access-group

Use the **ip access-group** site configuration command to control access to an interface. Use the **no ip access-group** command to remove the specified access group.

ip access-group *access-list-number* {**in | out**}
no ip access-group *access-list-number* {**in | out**}

Syntax Description

access-list-number	Access list number from 1 through 199
in	Filters on inbound packets
out	Filters on outbound packets

Default

Entering a keyword is strongly recommended, but if a keyword is not specified, **out** is the default.

Command Mode

Site configuration

Usage Guidelines

For inbound access lists, after receiving a packet, the router checks the packet against the access list. If the access list permits the packet, the router continues to process the packet. If the access list rejects the packet, the router discards the packet and returns an *ICMP Host Unreachable* message.

For outbound access lists, after receiving and routing a packet to a controlled interface, the router checks the packet against the access list. If the access list permits the packet, the router transmits the packet. If the access list rejects the packet, the router discards the packet and returns an *ICMP Host Unreachable* message.

Access lists are applied on either outbound or inbound interfaces, or both.

If the specified access list does not exist, all packets are passed.

Related Commands

access-list (standard)
access-list (extended)
show access-lists

ip address

Use the **ip address** site configuration command to set an IP address for the remote site's IP address. Use the **no ip address** command to remove the specified address.

ip address *ip-address mask*
no ip address

Syntax Description

ip-address	IP address
mask	Mask for the associated IP subnet

Default

No IP address is defined for an interface.

Command Mode

Site configuration

ip tcp header-compression

Use the **ip tcp header-compression** site configuration command to enable TCP header compression. Use the **no ip tcp header-compression** command to disable compression.

ip tcp header-compression
no ip tcp header-compression

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Site configuration

Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using SLIP or PPP encapsulation. You must enable compression on both ends of a serial connection. RFC 1144 specifies the compression process. Compressing the TCP header can speed up Telnet connections dramatically. In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets while file transfers use large packets. This feature only compresses the TCP header, so it has no effect on UDP packets or other protocol headers.

When using SLIP, both ends must agree on whether TCP header compression is to be used. PPP will negotiate for header compression and turn it off if either end is unwilling to support it.

ipx access-group

To apply a generic output filter to an interface, use the **ipx access-group** site configuration command. To remove the access list, use the **no** form of this command.

ipx access-group *access-list-number [in|out]*
no ipx access-group *access-list-number*

Syntax Description

access-list-number	Number of the access list. All outgoing packets defined with either standard or extended access lists and forwarded through the interface are filtered by the entries in this access list. For standard access lists, *access-list-number* is a decimal number from 800 to 899. For extended access lists, *access-list-number* is a decimal number from 900 to 999.
in	Apply to IPX packets coming in on the interface.
out	Apply to IPX packets before they go out on the interface.

Default

No filters are predefined.

Command Mode

Site configuration

Usage Guidelines

Generic filters control which packets are sent in or out on an interface based on the packet's source and destination addresses, IPX protocol type, and source and destination socket numbers. You use the standard **access-list** and extended **access-list** commands to specify the filtering conditions.

You can apply only one generic filter to an interface for each of **in** and **out**.

Example

In the following example, access list 801 is applied to interface Ethernet 0 for outgoing packets.

```
interface ethernet 0
ipx access-group 801 out
```

Related Commands

access-list (standard for ipx)
access-list (extended for ipx)

ipx network

To enable IPX routing to a particular site, use the **ipx network** site configuration command. To disable IPX routing, use the **no** form of this command.

ipx network *number*
no ipx network *number*

Syntax Description

number	Network number. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFE. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter just AA.

Default

IPX routing is disabled.

Command Mode

Site configuration

Usage Guidelines

Each point-to-point link requires a unique IPX network number, not duplicated by any IPX networks used for Ethernets or servers.

Related Commands

option ipx
routing rip

ipx output-sap-filter

To control which services are included in Service Advertisement Protocol (SAP) updates sent by the communication server, use the **ipx output-network-filter** site configuration command. To remove the filter, use the **no** form of this command.

ipx output-sap-filter *access-list-number*
no ipx output-sap-filter *access-list-number*

Syntax Description

access-list-number	Number of the SAP access list. All outgoing service advertisements are filtered by the entries in this access list. The argument access-list-number is a decimal number from 1000 to 1099.

Default

No filters are predefined.

Command Mode

Site configuration

Usage Guidelines

The communication server applies output SAP filters prior to sending SAP packets.

You can issue only one **ipx output-sap-filter** command on each interface.

When configuring SAP filters for NetWare 3.11 and later servers, use the server's internal network and node number (the node number is always 0000.0000.0001) as its address in the SAP **access-list** command. Do not use the *network.node* address of the particular interface board.

Related Commands

access list (SAP filtering)

load-threshold

This sets the number of bytes of queued traffic required to open an additional dial out line to the remote site.

load-threshold *number*

Syntax Description

number The number of bytes that can be queued before an additional line is used.

Command Mode

Site Configuration

Usage Guidelines

This is only used for multiline load-balancing when there are available modems, and requires **max-ports** to be set higher than 1 and more than one async interface to be configured in the same **dialer rotary-group** as this site's **dialgroup**.

Generally interactive terminal traffic will rarely have more than a hundred bytes queued, but file transfers (e.g., FTP) will queue several thousand bytes. These size differences should be used when deciding on a value for **load-threshold**.

Related Commands

dialer rotary-group
dialgroup
max-ports

max-ports

This command sets the maximum number of ports to use when dialing out to a site.

max-ports *number*

Syntax Description

number	If set to 0, this site will not be dialed out to. If set to 1, one line will be used. If set higher than one, multiline load-balancing will be done if modems are available.

Default

0

Command Mode

Site configuration

Usage Guidelines

For sites which are set to **dial-on demand** or **dial-on continuous** setting **max-ports** to a value of 1 or 2 should be the last configuration entry done for that site, since a non-zero value of max-ports indicates that the site is available for dialing to.

Related Commands

dial-on
dialgroup
load-threshold

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** site configuration command. Use the **no mtu** command to restore the MTU value to its original default value.

mtu *bytes*
no mtu

Syntax Description

bytes	Desired size in bytes

Command Mode

Site configuration

password

To specify a password for a site that will be dialing in, use the **password** site configuration command. Use the **no** form of this command to remove the password.

password *password*
no password

Syntax Description

password	Character string that specifies the site password. The first character cannot be a number. The string can contain any alphanumeric characters, up to 16 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different than the password secret. If spaces are included, the password must be enclosed in double quotes.

Default

No password is specified.

Command Mode

Site configuration

Usage Guidelines

The password is used to authenticate the remote site when it dials in.

Example

The following example sets the password for dial-in site mars to ezzgess4na:

```
site mars
password ezgess4na
```

routing rip

When used within a site entry this command controls whether routing updates will be sent or listened to on an interface that site is using. Without arguments it will both broadcast and listen for updates. When used in the **no** form it neither broadcasts nor listens for routing updates.

routing rip
routing rip {broadcast|listen}
no routing rip

Syntax Description

listen	Listen for routing updates on the interface but do not broadcast them.
broadcasting	Send routing updates on the interface but do not listen for them.

Command Mode

Site Configuration

Usage Guidelines

Caution This command controls both IP and IPX routing updates for this interface. Caution should be used when passing routing packets unidirectionally.

session-timeout

To set the interval for closing a dial-out connection when there is no input or output traffic, use the **session-timeout** site configuration command. The **no session-timeout** command removes the timeout definition.

session-timeout *minutes*
no session-timeout

Syntax Description

minutes	Specifies the time interval in minutes, for 0 to 255.

Default

The default interval is zero, indicating the router maintains the connection indefinitely.

Command Mode

Site configuration

Usage Guidelines

This command sets the interval that the router waits for traffic before closing the connection to a remote computer and returning the port to an idle state. Routing updates are not counted as traffic. The session-timeout is only applied if the router dials out.

system-script

This command identifies the chat-script which will be used to dial out to this site.

system-script *scriptname*

Syntax Description

scriptname A script identifier also used in chat-script.

Command Mode

Site configuration

Related Commands

chat-script
dial