CHAPTER 3

Global Configuration Commands

This chapter contains the commands used to configure everything on the router except for specific interfaces and sites. The commands are in alphabetical order. For hardware technical descriptions and global configuration tasks and examples, refer to the *Cisco 1020 User Guide* on UniverCD or a printed copy can be ordered.

access-list (standard)

To define a standard IP access list, use the standard version of the **access-list** global configuration command. To remove a standard access lists, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *source* [*source-mask*]
no access-list *access-list-number*

Syntax Description

access-list-number Number of an access list. This is a decimal number from 1 through 99.

deny Denies access to matching conditions.

permit Permits access for matching conditions.

source Number of the network or host from which the packet is being sent. It is a 32-bit quantity in four-part dotted-decimal format.

source-mask (Optional) Mask to be applied to *source*. It is a 32-bit quantity in four-part dotted-decimal format. Place ones in the low-order bit positions you want to mask.

Default

The access list defaults to an implicit deny statement for everything that has not been permitted.

Command Mode

Global configuration

Usage Guidelines

Plan your access conditions carefully and be aware of the implicit deny.

You can use access lists to control the transmission of packets on an interface to restrict contents of routing updates.

Use the **show access-lists** EXEC command to display the contents of all access lists.

Examples

The following example of a standard access list allows access for only those hosts on the three specified networks. It assumes that subnetting is not used; the masks apply to the host portions of the network addresses. Any host with a source address that does not match the access list statements will be rejected.

```
access-list 1 permit 192.5.34.0  0.0.0.255
access-list 1 permit 128.88.1.0  0.0.255.255
access-list 1 permit 36.0.0.0  0.255.255.255
! (Note: all other access implicitly denied)
```

To specify a large number of individual addresses more easily, you can omit the address mask; that is, all zeros from the **access-list** command. Thus, the following two configuration commands are identical in effect:

```
access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3  0.0.0.0
```

Related Commands

ip access group
show access-lists

access-list (extended)

To define an extended IP access list, use the extended version of the **access-list** global configuration command. To remove the access lists, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *protocol source source-mask destination*
*destination-mask [[[type] operator operand] [type operator operand]] [***established***]*
no access-list *access-list-number*

Syntax Description

access-list-number	Number of an access list. This is a decimal number from 100 through 199.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
protocol	Name or number of an IP protocol. It can be one of the keywords **ip**, **tcp**, **udp**, or **icmp**. To match any TCP, UDP, or ICMP, use the keyword **ip**.
source	Number of the network or host from which the packet is being sent. It is a 32-bit quantity in four-part dotted-decimal format.
source-mask	Mask to be applied to *source*. It is a 32-bit quantity in four-part dotted-decimal format. Place ones in the low-order bit positions you want to mask.
destination	Number of the network or host to which the packet is being sent. It is a 32-bit quantity in four-part dotted-decimal format.
destination-mask	Mask to be applied to *destination*. It is a 32-bit quantity in four-part dotted-decimal format. Place ones in the low-order bit positions you want to mask.
type	**Src** for source port or **dst** for destination port. If not specified, defaults to destination port.
operator	(Optional) Compares destination ports. Possible operands include **lt** (less than), **gt** (greater than), and **eq** (equal). Note that the **ip** and **icmp** protocol keywords do not allow port distinctions.
operand	(Optional) Decimal destination port to compare. Note that the **ip** and **icmp** protocol keywords do not allow port distinctions.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK, FIN or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

Default

An extended access list defaults to an implicit deny statement for everything that has not been permitted.

Command Mode

Global configuration

Usage Guidelines

You can use access lists to control the transmission of packets on an interface. The router stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list.

Note After an access list is created initially, 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.

Example

In the following example, the Ethernet network is a Class B network with the address 128.88.0.0, and the mail host's address is 128.88.1.2. The keyword **established** is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK, FIN or RST bits set, which indicate that the packet belongs to an existing connection.

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255 128.88.1.2 0.0.0.0 eq 25
interface ethernet 0
ip access-group 102 out
```

Related Commands

ip access-group
show access-lists

access-list (standard for ipx)

To define a standard IPX access list, use the standard version of the **access-list** global configuration command. To remove a standard access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *source-network*[**.***source-node*]
[*destination-network*[**.***destination-node*]]
no access-list *access-list-number*

Syntax Description

access-list-number	Number of the access list. This is a decimal number from 800 to 899.
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
source-network	Number of the network from which the packet is being sent. 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. A network number of –1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA.
source-node	(Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers *(xxxx.xxxx.xxxx)*.
destination-network	(Optional) Number of the network to which the packet is being sent. 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. A network number of –1 matches all networks. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA.
destination-node	(Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers *(xxxx.xxxx.xxxx)*.

Default

No access lists are predefined.

Command Mode

Global configuration

Usage Guidelines

Standard IPX access lists filter on the source network. All other parameters are optional.

Use the **ipx access-group** command to assign an access list to an interface. You can apply only one extended or one standard access list to an interface for incoming packets, and another for outgoing packets.

To delete a standard access list, use the **no** form of the command.

no access-list *access-list-number*

Examples

The following example denies access to traffic from all IPX networks (–1) to destination network 2:

```
access-list 800 deny -1 2
```

The following example denies access to all traffic from IPX address 1.0000.0c00.1111:

```
access-list 800 deny 1.0000.0c00.1111
```

The following example denies access from source address 1111.1111.1111 on network 1 to destination address 2222.2222.2222 on network 2:

```
access-list 800 deny 1.1111.1111.1111 2.2222.2222.2222
```

Related Commands

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

access-list (extended for ipx)

To define an extended Novell IPX access list, use the extended version of the **access-list** global configuration command. To remove an extended access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *protocol*
[*source-network*[.*source-node] source-socket*
[*destination-network* [.*destination-node] destination-socket*]]

no access-list *access-list-number*

Syntax Description

access-list-number

Number of the access list. This is a decimal number from 900 to 999.

deny

Denies access if the conditions are matched.

permit

Permits access if the conditions are matched.

protocol

Number of an IPX protocol type, in decimal. This also is sometimes referred to as the packet type. Only -1 is supported on the Cisco 1020.

source-network

Number of the network from which the packet is being sent. 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. A network number of –1 matches all networks.

You do not need to specify leading zeros in the network number, for example, for the network number 000000AA, you can enter just AA.

source-node

(Optional) Node on *source-network* from which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers *(xxxx.xxxx.xxxx)*.

source-socket

Socket number from which the packet is being sent, in hexadecimal.

destination-network

Number of the network to which the packet is being sent. 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. A network number of –1 matches all networks.

You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA.

destination-node

(Optional) Node on *destination-network* to which the packet is being sent. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers *(xxxx.xxxx.xxxx)*.

destination-socket

(Optional) Socket number to which the packet is being sent, in hexadecimal. Table 3-2 in the “Usage Guidelines” section lists some IPX socket numbers.

Default

No access lists are predefined.

Command Mode

Global configuration

Usage Guidelines

Extended IPX access lists filter on protocol type. All other parameters are optional.

Use the **ipx access-group** command to assign an access list to an interface. You can apply only one extended or one standard access list to an interface for incoming IPX traffic, and another for outgoing.

To delete an extended access list, use the **no** form of the command:

no access-list *access-list-number*

Related Commands

access-list (standard for IPX)
ipx access-group
show access-lists

access-list (SAP filtering)

To define an access list for filtering Service Advertisement Protocol (SAP) requests, use the SAP filtering form of the **access-list** global configuration command. To remove the access list, use the **no** form of this command.

access-list *access-list-number* {**deny** | **permit**} *network*[**.***node*]
[*service-type* [*server-name*]]
no access-list *access-list-number* {**deny** | **permit**} *network*[**.***node*]
[*service-type* [*server-name*]]

Syntax Description

access-list-number — Number of the SAP access list. This is a decimal number from 1000 to 1099.

deny — Denies access if the conditions are matched.

permit — Permits access if the conditions are matched.

network — 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. A network number of –1 matches all networks.

You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter just AA.

node — (Optional) Node on *network*. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers *(xxxx.xxxx.xxxx)*.

service-type — (Optional) Service type on which to filter. This is a hexadecimal number. A value of 0 means all services. Table 3-1 in the "Usage Guidelines" section lists examples of service types.

server-name — (Optional) Name of the server providing the specified service type. This can be any contiguous string of printable ASCII characters. Use double quotation marks (" ") to enclose strings containing embedded spaces.

Default

No access lists are predefined.

Command Mode

Global configuration

Usage Guidelines

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 **access-list** command. Do not use the *network.node* address of the particular interface board.

Table 3-1 lists some sample IPX SAP types. For more information about SAP types, contact Novell.

Table 3-1 Sample IPX SAP Services

Service Type (Hexadecimal)	Description
0	All SAP services; IPX defines server type 0 to be an unknown service, which means that you cannot define an access list to permit or deny unknown services
1	User
2	User group
3	Print server queue
4	File server
5	Job server
7	Print server
9	Archive server
A	Queue for job servers
21	NAS SNA gateway
2D	Time Synchronization VAP
2E	Dynamic SAP
47	Advertising print server
4B	Btrieve VAP 5.0
4C	SQL VAP
7A	TES—NetWare for VMS
98	NetWare access server
9A	Named Pipes server
9E	Portable NetWare—UNIX
111	Test server
166	NetWare management (Novell's Network Management Station [NMS])
26A	NetWare management (NMS console)
FFFF	Wildcard (any SAP service)

To delete a SAP access list, specify the minimum number of keywords and arguments needed to delete the proper access list. For example, to delete the entire access list, use the following command:

no access-list *access-list-number*

Example

The following access list blocks all access to a file server (service type 4) on the directly attached network by resources on other Novell networks, but allows access to all other available services on the interface:

```
access-list 1001 deny -1 4
access-list 1001 permit -1
```

Related Commands

ipx output-sap-filter
show access-lists

chat-script

To create a script that will place a call over a modem, use the **chat-script** global configuration command. To disable the specified chat script, use the **no** form of this command.

chat-script *scriptname expect-send*
no chat-script *scriptname*

Syntax Description

scriptname	Name of the chat script
expect-send	Content of the chat script

Default

No chat scripts are configured.

Command Mode

Global configuration

Usage Guidelines

Chat scripts are used in dial-on-demand routing to give commands to dial a modem and commands to log on to remote systems. The defined script will be used to place a call over a modem.

Some characteristics of chat scripts are as follows:

- Chat scripts are case sensitive.
- A string within quotation marks is treated as a single entity.

Escape Sequences

Chat scripts are in the form *expect send*. Each send string is followed by a return unless it ends with \c.

The escape sequences used in chat scripts are listed in Table 3-2.

Table 3-2 Chat Script Escape Sequences

Escape Sequence	Description
“”	Expect a null string.
\c	Suppress newline at the end of the send string.
\r	Send a return.
\\	Send a backslash

Example

```
chat-script hqdial "" “ATDT 5551212” “CONNECT” "" “:” “pr1” “word:”
“what4ever” “>” “ppp 192.168.1.1”
```

Related Commands

system-script

default routing

This command controls whether default routes will be included or listened to in routing updates. Without arguments it will both include and listen for default routes in routing updates. When used in the **no** form it neither includes nor listens for default routes in routing updates.

default routing
default routing {broadcast|listen}
no default routing

Syntax Description

broadcast	Send default route information as part of routing updates but do not accept them in routing updates.
listen	Accept default routes present in routing updates but do not include them in routing updates.

Default

Off

Command Mode

Global Configuration

Usage Guidelines

If **default routing** or **default routing broadcast** is set, the router will send default route information as part of its normal RIP messages. If **default routing** or **default routing listen** is set, the router will accept default route information from other routers connected to any of the interfaces. The default is to not broadcast or listen for default routes. If selected, default routes are broadcast or listened to across all interfaces, including serial interfaces configured for PPP or SLIP.

Related Commands

ip route
routing rip

enable password

To assign a password for the privileged EXEC level, use the **enable password** global configuration command.

enable password *password*

Syntax Description

password	Case-sensitive character string that specifies the line password prompted for in response to the EXEC command enable-password. The string can contain up to 16 characters.

Default

No password is assigned.

Command Mode

Global configuration

Usage Guidelines

When you enter **enable** at the `Username`: prompt, the router will prompt you for this password.

Example

This example sets the password secretword for the privileged command level on all lines, including the console:

```
enable password secretword
```

exit

To exit any command mode or close an active terminal session and terminate the EXEC, use the **exit** command at the system prompt.

exit

Syntax Description

This command has no arguments or keywords.

Command Mode

Available in all command modes

Usage Guidelines

When you enter the **exit** command at the EXEC levels, the EXEC mode is ended. Use the **exit** command at the configuration level to return to privileged EXEC mode. Use the **exit** command in interface and router command modes to return to global configuration mode. You can also press **Ctrl-Z** from any configuration mode to return to privileged EXEC mode.

Example

The following example shows how to exit an active session.

```
Router# exit
```

Related Commands

logout

hostname

To specify or modify the host name for the router, use the **hostname** global configuration command. The host name is used in prompts, default configuration filenames, and as the system ID certifier for CHAP authentication.

hostname *name*

Syntax Description

name	New host name for the router; the name is case sensitive.

Default

No default.

Command Mode

Global configuration.

Example

The following example changes the host name to *sandbox*:

```
hostname sandbox
```

interface

To configure an interface type and enter interface configuration mode, use the **interface** global configuration command.

interface *interface-type interface-number*

Syntax Description

interface-type	Type of interface to be configured. See Table 3-3.
interface-number	Port number. The numbers are assigned at the factory and can be displayed with the **show interfaces** command. On the Cisco 1020 the port number of the interface can be 0, 1, or 2, depending on the type of interface. See Table 3-3.

Table 3-3 Interface Type Keywords

Keyword	Interface Type	Interface Numbers
ethernet	Ethernet IEEE 802.3 interface.	0
async	Asynchronous serial port.	1, 2

Command Mode

Global configuration

Related Commands

show interface

ip domain-lookup

Use the **ip domain-lookup** global configuration command to enable the IP Domain Name System-based host name-to-address translation. Use the **no ip domain-lookup** command to disable the Domain Name System.

ip domain-lookup
no ip domain-lookup

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Global configuration

Example

The following example enables the IP Domain Name System-based host name-to-address translation:

```
ip domain-lookup
```

Related Commands

ip domain-name
ip name-server

ip domain-name

Use the **ip domain-name** global configuration command to define a default domain name that the router uses to complete unqualified host names (names without a dotted-decimal domain name). Use the **no ip domain-name** command to disable host name lookup.

ip domain-name *name*
no ip domain-name

Syntax Description

name	Default domain name used to complete unqualified host names; do not include the initial period that separates an unqualified name from the domain name.

Default

Enabled

Command Mode

Global configuration

Example

The following example defines cisco.com as the default domain name:

```
ip domain-name cisco.com
```

Related Commands

ip domain-lookup
ip name-server

ip host

Use the **ip host** global configuration command to define a static host name-to-address mapping in the host cache. Use the **no ip host** command to remove the name-to-address mapping.

ip host *name address*
no ip host *name address*

Syntax Description

name	Name of the host. The first character can be either a letter or a number, but if you use a number, the operations you can perform are limited.
address	Associated IP address.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

The first character can be either a letter or a number, but if you use a number, the operations you can perform (such as ping) are limited.

Example

The following example uses the **ip host** command to define two static mappings:

```
ip host croff 192.31.7.18
ip host bisso-gw 10.2.0.2
```

ip name-server

Use the **ip name-server** global configuration command to specify the address of one or two name servers to use for name and address resolution. Use the **no ip name-server** command to remove the addresses specified.

ip name-server *server-address1* [*server-address2*]
no ip name-server *server-address1* [*server-address2*]

Syntax Description

server-address1...2	IP addresses of up to two name servers

Default

No name server addresses are specified.

Command Mode

Global configuration

Example

The following example specifies host 131.108.1.111 as the primary name server and host 131.108.1.2 as the secondary server:

```
ip name-server 131.108.1.111 131.108.1.2
```

This command will be reflected in the configuration file as follows:

```
ip name-server 131.108.1.111
ip name-server 131.108.1.2
```

Related Commands

ip domain-lookup
ip domain-name

ip route

Use the **ip route** global configuration command to establish static routes. The **no ip route** command removes the static route.

ip route *network address* [*distance*]
no ip route *network*

Syntax Description

network	Internet address of the target network or subnet
address	Internet address of the next hop that can be used to reach that network
distance	(Optional) An administrative distance from 1 to 14. Distance defaults to 1 if no value is entered.

Default

No static routes are established.

Command Mode

Global configuration

Usage Guidelines

A static route is appropriate when the router cannot dynamically build a route to the destination.

Examples

In the following example, packets for network 131.108.0.0 will be routed to the router at 131.108.6.6:

```
ip route 131.108.0.0 131.108.6.6
```

ipx netbios

The command **ipx netbios** enables broadcasts of type 20 packets (NetBIOS, Network Adapter Basic Input/Output System) across all active interfaces running the IPX protocol. The **no** version of the command disables such broadcasts.

ipx netbios
no ipx netbios

Syntax Description

This command has no arguments or keywords.

Default

Disabled.

Command Mode

Global configuration

Related Commands

option ipx
ipx network

ipx route

To add a static route to the routing table, use the **ipx route** global configuration command. To remove a route from the routing table, use the **no** form of this command.

ipx route *network network.node [distance] [ticks]*
no ipx route *network*

Syntax Description

network	Network to which you want to establish a static route. 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.
network.node	Router to which to forward packets destined for the specified network. The argument *network* 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. The argument *node* is the node number of the target router. This is a 48-bit value represented by a dotted triplet of four-digit hexadecimal numbers *(xxxx.xxxx.xxxx)*.
distance	(Optional) Distance metric for this route. A number from 1 to 15. Distance defaults to 1 if not specified.
ticks	(Optional) Distance tick metric for this route. A number from 1 to 65536.

Default

No static routes are predefined.

Command Mode

Global configuration

Usage Guidelines

The **ipx route** command forwards packets destined for the specified network *(network)* via the specified router *(network.node)*, regardless of whether that router is sending dynamic routing information.

Be careful when assigning static routes. When links associated with static routes are lost, traffic may stop being forwarded, even though alternative paths might be available.

Example

In the following example, the router at address 3abc.0000.0c00.1ac9 handles all traffic destined for network 5e:

```
ipx route 5e 3abc.0000.0c00.1ac9
```

Related Commands

show ipx route

logging

To log messages to a syslog server host use the **logging** global configuration command. The **no logging** command deletes the syslog server.

logging *host*
no logging

Syntax Description

host	Name or IP address of the host to be used as a syslog server

Default

No messages are logged to a syslog server host.

Command Mode

Global configuration

Usage Guidelines

This command identifies a syslog server host to receive logging messages. The auth facility is used.

Example

The following example logs messages to a host named *johnson*:

```
logging johnson
```

modem-def

This command is used to define the optimum speed and initialization string to use for a particular modem.

modem-def *modem* **“***description***”** *bps expect-send*

Syntax Description

modem
A name for the modem to be used by **modem-type**.

description
A longer descriptive name for the modem, which must be enclosed in double-quotes if it contains spaces.

bps
The optimum speed to lock the DTE rate of the port at when using this modem, typically 38400, 57600 or 115200.

expect-send
A series of Expect-Send pairs inside double quotes to be used when initially configuring the modem.

Command Mode

Global configuration

Usage Guidelines

The Expect-Send sequence should configure the modem to raise DCD when carrier is detected, to lock the DTE rate at the specified speed, to reset the modem when DTR is dropped, to use hardware flow control, and to save these values to the modem’s nonvolatile storage. Consult your modem’s manual to determine the proper settings for these. For use with dial-in, set S0=1 to answer the phone.

It is suggested that you differentiate between external modems (for use on async 1) and PCMCIA modems (for use on async 2).

Example

```
modem-def usrv34 “USR V.34 Courier” 115200 ““ “AT&F1S0=1&W” “OK” “”
```

Related Commands

clear interface
modem-type
show modem

option ipx

The **option ipx** global configuration command is used to turn on IPX functionality in the Cisco 1020.

option ipx *key*

Syntax Description

key	Key value is based on your serial number. The key value is provided to you by Cisco when you purchase the IPX option for the Cisco 1020.

Command Mode

Global configuration

Usage Guidelines

None of the IPX commands do anything until a valid ipx key is installed with the **option ipx** command.

Related Commands

access-list (ipx standard)
access-list (ipx extended)
debug ipx packet
ipx access-group
ipx netbios
ipx network
ipx output-sap-filter
ipx route
show ipx route

reverse-telnet-port

This command sets the TCP port number for incoming administrative telnet sessions.

reverse-telnet-port *number*

Syntax Description

number	The TCP port number that the router will listen on for incoming administrative telnet sessions. It must be between 0 and 65535.

Default

23

Command Mode

Global configuration

Usage Guidelines

Note Setting this to 0 turns off the ability to telnet into the router, and will require all further configuration to be done from the console.

site

The **site** command is used to define a remote location that can either dial into the router, be dialed out to, or both.

site *name*

Syntax Description

name	An identifier for the site used for the dial command. It can be up to 12 characters that are alphanumeric or dash, underscore or period. If it contains spaces it must be enclosed in double quotes.

Command Mode

Global Configuration

Related Commands

dial
show sites

snmp-server community

To set up the community access string, use the **snmp-server community** global configuration command. This command enables SNMP server operation on the router. The **no snmp-server community** command removes the specified community string or access list.

snmp-server community [*string* [**RO** | **RW**] [*number*]]
no snmp-server [**community** [*string*]]

Syntax Description

string	(Optional) Community string that acts like a password and permits access to the SNMP protocol.
RO	(Optional) Specifies read-only access.
RW	(Optional) Specifies read-write access.
number	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that may use the community string.

Default

SNMP community string “public” permits read-only access.

Command Mode

Global configuration

Example

The following example assigns the string *comaccess* to the SNMP allowing read-only access and specifies that Internet access list 4 can use the community string.

```
snmp-server community comaccess RO 4
```