

Cisco Router Command Quick Reference

Two basic levels of login:

Standard Read Mode (prompt looks like “router-name>”)

Enable Mode (Prompt looks like “router-name#”)

You only ever need to type enough of the command to distinguish from other commands

You can always press tab to finish the command you start typing

If you are locked up by router output enter:

“<ctrl><shift><6><x>”

“?” is the universal help command

To see what commands are available beyond an initial command enter:

“Initial command ?” (example “show ?”)

To save configuration changes:

“copy running-config startup-config”

To save configuration to a TFTP Server enter:

“copy running-config tftp” then follow the prompts

Some good show commands to utilize:

Show Dial
Show IP Route
Show IP Protocol
Show version

To see debug output from a telnet session you must first enter:

“Terminal monitor “

To reboot the router enter:

“reload”

Always remember where you are by the router prompt

Cisco Router Command Quick Reference

```
router>
|
router#
|
router(config)#
/ | \
router(config-if) # router(config-line)# router(config-router)#
```

Using Cisco Wildcard Mask

Cisco wildcard mask for an entire subnet

```
255.255.255.255
- 255.255.192.0
```

0. 0. 63.255

Cisco wildcard mask to match range

100.1.16.0 - 100.1.31.255

```
100.1.31.255
- 100.1.16.0
```

0.0.15.255

Take the broadcast and subtract from the network

Packet filtering on CISCO routers

Many routers offer some degree of packet filtering capabilities. Since CISCO routers are common place in WAN connectivity, and they offer such extended capabilities we have chosen to address them directly.

This topic is not meant to be an introduction to the CISCO IOS but a discussion of packet filter implementation using CISCO IOS. For detailed information on CISCO IOS see appendix "A" References and Recommended Reading.

CISCO routers implement packet filters as Access Control List (ACL) *not to be confused with Windows NT ACL's*. Basically put you create sets of ACL's and then apply them to the desired router interface as Access Groups.

Here is a sample configuration:

The first set of access list created describes the connections allowed into the network from the outside.

Cisco Router Command Quick Reference

List 101

```
access-list 101 deny ip 192.168.100.0 0.0.0.255 any
```

Anti Spoofing - This statement will not allow any connections from IP address within the internal network number.

```
access-list 101 permit tcp any any established
```

#Allow any tcp connections to ports that were established from the inside.

```
access-list 101 permit tcp 192.168.200.0 0.0.0.255 any eq telnet
```

#Allow telnet connections from the specific class C network 192.168.200.0

```
access-list 101 permit tcp any any eq ftp
```

#Allow FTP connections

```
access-list 101 permit tcp any any eq ftp-data
```

#Allow FTP-Data connections

```
access-list 101 permit tcp any any eq domain
```

```
access-list 101 permit udp any any eq domain
```

#Allow DNS connections

```
access-list 101 permit tcp any any eq pop3
```

#Allow POP3 connections for retrieving mail

```
access-list 101 permit tcp any any eq smtp
```

#Allow SMTP for mail servers to transfer mail

```
access-list 101 permit tcp any any eq www
```

#Allow connections to Web Servers

```
access-list 101 permit tcp any any eq 443
```

```
access-list 101 permit udp any any eq 443
```

#Allow connections to SSL for HTTPS

```
access-list 101 permit udp any any eq 1723
```

```
access-list 101 permit tcp any any eq 1723
```

#Allow Connections to port 1723 for Point to Point Tunneling Protocol

```
access-list 101 permit icmp any any
```

#Allow All ICMP messages for Flow Control, Ping, Error messages and such.

#Note: to protect from Smurf attacks and Ping Flooding you may need to deny ICMP Echo and Echo-

#Request

```
access-list 101 permit 47 any any
```

#Allow all General Encapsulation Protocol number 47 for VPN's and PPTP

#You don't see it, or need to enter it, but there is always an implicit Deny all Else as the last statement

#in each ACL.

Cisco Router Command Quick Reference

List 102

```
access-list 102 permit ip any any  
#Allow all IP connections
```

```
access-list 102 permit icmp any any  
#Allow all ICMP connections
```

```
access-list 102 permit 47 any any  
#Allow all General Encapsulation Protocol number 47 for VPN's and PPTP
```

#You don't see it, or need to enter it, but there is always an implicit Deny all Else as the last statement in #each ACL.

Once these access list are entered they can be applied to the desired interfaces to provide protection. This is a point of confusion for many people. The best rule to remember the proper assignment of ACL's to router interfaces is OUT means out of the router interface and IN means into the router interface. Keeping this in mind consider the following configuration.

A T-1 connection to the Internet, which is connected to the router Serial 0 interface, and the internal network is connected to router Ethernet 0 Interface.

To apply the most restrictive ACL's described you could assign access list 101 to Ethernet interface 0 out by

```
Interface ethernet 0  
ip access-group 101 out
```

These directives invoke access list 101 directives for all packets leaving the router destined for the network on interface ethernet 0.

To apply the least restrictive ACL's described you could assign access list 102 to Ethernet interface 0 in for connections leaving your internal network.

```
Interface ethernet 0  
ip access-group 101 in
```

These directives invoke access list 102 directives for all packets entering the router destined for anywhere.

Access list can be tricky. Some key points to remember are:

- Access lists are evaluated from the top down, and once a rule is met the packet is dealt with accordingly.
- There is always an implicit deny all else at the end of each ACL.
- It is best to construct and invoke access list from the terminal rather than a telnet session since you could quite easily implement an access list that would terminate your connection.
- Test your access list completely.