Cisco Router Configuration and Management
• Router Management
• Introduction to Routing Protocols
• Access-list
• Network Address Translation
• Troubleshooting Tools
Router Management
• Configurations can come from many sources
• Configurations will act in device memory
Creating a HyperTerminal Session

Step 1: Verify cabling

Step 2: Power on PC

Step 3: Open HyperTerminal Folder

Step 4: Open HyperTerminal

Step 5: Describe Connection
Creating a HyperTerminal Session (cont.)

Step 6: Select COM port to be used

![COM port selection dialog]

Step 7: Select properties

![Properties selection dialog]

www.netstarnetworks.com
Creating a HyperTerminal Session (cont.)

Step 8: Access Device

Connect Disconnect

Router> Router> en Router# Router# Router# Router#
Connecting to the Modem

Forward connection to a router to login

Reverse connection to a modem to configure it
### Sample Output for `show line`

<table>
<thead>
<tr>
<th>Tty Typ</th>
<th>Tx/Rx</th>
<th>A Modem</th>
<th>Ratey</th>
<th>AccD</th>
<th>AccI</th>
<th>Uses</th>
<th>Noise</th>
<th>Overruns</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 0 CTY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>* 1 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td>4</td>
<td>31</td>
<td>26</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>* 2 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td>30</td>
<td>37</td>
<td>23</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>A 3 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td>.5</td>
<td>10</td>
<td>24</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>* 4 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td>4</td>
<td>20</td>
<td>63</td>
<td>1</td>
<td>0/0</td>
</tr>
<tr>
<td>* 5 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td>.45</td>
<td>18</td>
<td>325</td>
<td>22</td>
<td>0/0</td>
</tr>
<tr>
<td>A 6 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td>.5</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>I 7 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td></td>
<td>6</td>
<td>36</td>
<td>1</td>
<td>0/0</td>
</tr>
<tr>
<td>I 8 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td></td>
<td>3</td>
<td>25</td>
<td>3</td>
<td>0/0</td>
</tr>
<tr>
<td>* 9 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>-</td>
<td></td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>A 10 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td>56</td>
<td></td>
<td>2</td>
<td>470</td>
<td>216</td>
<td>0/0</td>
</tr>
<tr>
<td>* 11 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>I 12 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>I 13 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td></td>
<td></td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>I 14 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>I 15 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>I 16 TTY</td>
<td>115200/115200</td>
<td>in/out</td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
</tr>
<tr>
<td>17 AUX</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>1</td>
<td>2/104800</td>
<td></td>
</tr>
<tr>
<td>18 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>103</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>19 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>6</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>20 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>21 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>22 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>23 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>24 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>25 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>26 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>27 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>28 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>29 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>30 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>31 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>32 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>33 VTY</td>
<td>9600/9600</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td></td>
</tr>
</tbody>
</table>
EXEC Connection Commands

Router>telnet [host] [2000+aux_tty#]
- Makes a connection with the Telnet protocol

Router>disconnect [session-number]
- Disconnects the specified session or all sessions

Router>ctrl-shift-6 x
- Suspends a session
Interface AUX and Line Configuration

Physical configuration

```
Router(config)#line 17
Router(config-line)#modem inout
Router(config-line)#transport input all
Router(config-line)#flowcontrol hardware
```
# Standard Modem Commands

<table>
<thead>
<tr>
<th>Action intended</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loads factory default settings</td>
<td>AT&amp;F</td>
</tr>
<tr>
<td>Auto answer</td>
<td>ATS0=n</td>
</tr>
<tr>
<td>CD truly reflects line state</td>
<td>AT&amp;C1</td>
</tr>
<tr>
<td>Hangs up at DTR low</td>
<td>AT&amp;D3</td>
</tr>
<tr>
<td>Ignore “+++” (in-band signaling)</td>
<td>ATS2=255</td>
</tr>
<tr>
<td>Echo off</td>
<td>ATE0</td>
</tr>
<tr>
<td>Turn off speaker</td>
<td>ATM0</td>
</tr>
<tr>
<td>Save modem config</td>
<td>AT&amp;W</td>
</tr>
</tbody>
</table>
Cisco’s IOS software delivers network services and enables networked applications.
There are two main EXEC modes for entering commands.

First mode:

**User Mode**

- Limited examination of switch or router
- Command Prompt is `hostname>`
Second mode (and most commonly used):

**Privileged (or enabled) Mode**
- Detailed examination of switch or router
- Enables configuration and debugging
- Prerequisite for other configuration modes
- Command prompts on the device
  > hostname#

---

www.netstarnetworks.com
Initial Start Up of the Cisco Router

- System startup routines initiate router software
- Router falls back to startup alternatives if needed

1. Before you start the router, verify the power, cabling, and console connection
2. Push the power switch to on
3. Observe the boot sequence
   - Cisco IOS software output text on the console
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[ ]'.

wg_ro con0 is now available
Press RETURN to get started.

wg_ro>

Unconfigured versus configured router
Router#setup

--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: n
First, would you like to see the current interface summary? [yes]:

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRI0</td>
<td>unassigned</td>
<td>YES unset administratively</td>
<td>down down</td>
</tr>
<tr>
<td>BRI0:1</td>
<td>unassigned</td>
<td>YES unset administratively</td>
<td>down down</td>
</tr>
<tr>
<td>BRI0:2</td>
<td>unassigned</td>
<td>YES unset administratively</td>
<td>down down</td>
</tr>
<tr>
<td>Ethernet0</td>
<td>unassigned</td>
<td>YES unset administratively</td>
<td>down down</td>
</tr>
<tr>
<td>Serial0</td>
<td>unassigned</td>
<td>YES unset administratively</td>
<td>down down</td>
</tr>
</tbody>
</table>

Interfaces found during startup
Configuring global parameters:

Enter host name [Router]: wg_ro

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.
Enter enable secret: cisco

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.
Enter enable password: sanfran

The virtual terminal password is used to protect access to the router over a network interface.
Enter virtual terminal password: sanjose
Configure SNMP Network Management? [no]:

Initial global parameters
Logging into the Router

wg_ro con0 is now available
Press RETURN to get started.

wg_ro>
wg_ro>enable
wg_ro#
wg_ro#disable
wg_ro>
wg_ro>logout

User mode prompt
Privileged mode prompt
wg_ro>?
Exec commands:
- `access-enable` Create a temporary Access-List entry
- `atmsig` Execute Atm Signalling Commands
- `cd` Change current device
- `clear` Reset functions
- `connect` Open a terminal connection
- `dir` List files on given device
- `disable` Turn off privileged commands
- `disconnect` Disconnect an existing network connection
- `enable` Turn on privileged commands
- `exit` Exit from the EXEC
- `help` Description of the interactive help system
- `lat` Open a lat connection
- `lock` Lock the terminal
- `login` Log in as a particular user
- `logout` Exit from the EXEC

You can abbreviate a command to the fewest characters that make a unique character string
Router Privileged Mode
Command List

wg_ro#?

Exec commands:
access-enable    Create a temporary Access-List entry
access-profile   Apply user-profile to interface
access-template  Create a temporary Access-List entry
bfe              For manual emergency modes setting
cd               Change current directory
clear            Reset functions
clock            Manage the system clock
configure        Enter configuration mode
connect          Open a terminal connection
copy             Copy from one file to another
debug            Debugging functions (see also 'undebug')
delete           Delete a file
dir              List files on a filesystem
disable          Turn off privileged commands
disconnect       Disconnect an existing network connection
enable           Turn on privileged commands
erase            Erase a filesystem
exit             Exit from the EXEC
help             Description of the interactive help system

-- More --

You can complete a command string by typing the unique character string then pressing the tab key.
**show version Command**

```plaintext
wg_ro# show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-IK9O3S-M), Version 12.2(21), RELEASE SOFTWARE (fc3)
Copyright (c) 1986-2003 by cisco Systems, Inc
...
ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

wg_ro uptime is 6 weeks, 2 days, 10 hours, 1 minute
System returned to ROM by reload
System restarted at 23:57:58 TPE Fri Jan 9 2004
System image file is "flash:c3640-ik9o3s-mz.122-21.bin"
...
cisco 3640 (R4700) processor (revision 0x00) with 126976K/4096K bytes of memory.
Processor board ID 16186480
R4700 CPU at 100Mhz, Implementation 33, Rev 1.0
2 Ethernet/IEEE 802.3 interface(s)
...
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```
Viewing the Configuration

Setup saves the configuration to NVRAM.
show running and show startup Commands

In RAM

```
wg_ro#show running-config
Building configuration...

Current configuration:
!
version 12.0
!
  -- More --
```

In NVRAM

```
wg_ro#show startup-config
Using 1359 out of 32762 bytes
!
version 12.0
!
  -- More --
```

Display current and saved configuration
Overview of Router Modes

User EXEC mode
Privileged EXEC mode
Global configuration mode

<table>
<thead>
<tr>
<th>Configuration Mode</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Router(config-if)#</td>
</tr>
<tr>
<td>Subinterface</td>
<td>Router(config-subif)#</td>
</tr>
<tr>
<td>Line</td>
<td>Router(config-line)#</td>
</tr>
<tr>
<td>Router</td>
<td>Router(config-router)#</td>
</tr>
</tbody>
</table>

Diagram:
- User EXEC mode: `Router>enable`
- Privileged EXEC mode: `Router#config term`
- Global configuration mode: `Router(config)#`
- Ctrl-Z (end)
- Exit
Saving Configurations

wg_ro#
wg_ro#copy running-config startup-config
Destination filename [startup-config]?
Building configuration…

wg_ro#write memory

Copy the current configuration to NVRAM
Configuring Router Identification

Router Name

```
Router(config)#hostname wg_ro
wg_ro(config)#
```

Message of the Day Banner

```
wg_ro(config)#banner motd  
   Accounting Department
   You have entered a secured
   system. Authorized access
   only! 
```

Interface Description

```
wg_ro(config)#interface ethernet 0
wg_ro(config-if)#description Engineering LAN, Bldg. 18
```

- Sets local identity or message for the accessed router or interface
Router Password Configuration

Console Password

Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password cisco

Virtual Terminal Password

Router(config)#line vty 0 4
Router(config-line)#login
Router(config-line)#password sanjose

Enable Password

Router(config)#enable password cisco

Secret Password

Router(config)#enable secret sanfran
Configuring an Interface

Router(config)#interface type number
Router(config-if)#

- **type** includes serial, ethernet, token ring, fddi, hssi, loopback, dialer, null, async, atm, bri, and tunnel
- **number** is used to identify individual interfaces

Router(config)#interface type slot/port
Router(config-if)#

- For modular routers

Router(config-if)#exit

- Quit from current interface configuration mode
Disabling or Enabling an Interface

Router#configure term
Router(config)#interface serial 0
Router(config-if)#shutdown
%LINK-5-CHANGED: Interface Serial0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed state to down

Administratively turns off an interface

Router#configure term
Router(config)#interface serial 0
Router(config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line Protocol on Interface Serial0, changed state to up

Enables an interface that is administratively shutdown
Router# `show interfaces`  
Ethernet0 is **up**, line protocol is **up**  
  Hardware is Lance, address is 00e0.1e5d.ae2f (bia 00e0.1e5d.ae2f)  
  Internet address is 10.1.1.11/24  
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255  
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)  
  ARP type: ARPA, ARP Timeout 04:00:00  
  Last input 00:00:07, output 00:00:08, output hang never  
  Last clearing of "show interface" counters never  
  Queueing strategy: fifo  
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops  
  5 minute **input rate** 0 bits/sec, 0 packets/sec  
  5 minute **output rate** 0 bits/sec, 0 packets/sec  
  81833 packets input, 27556491 bytes, 0 no buffer  
  Received 42308 broadcasts, 0 runts, 0 giants, 0 throttles  
  1 input errors, 0 CRC, 0 frame, 0 overrun, 1 ignored, 0 abort  
  0 input packets with dribble condition detected  
  55794 packets output, 3929696 bytes, 0 underruns  
  0 output errors, 0 collisions, 1 interface resets  
  0 babbles, 0 late collision, 4 deferred  
  0 lost carrier, 0 no carrier  
  0 output buffer failures, 0 output buffers swapped out
Interpreting Interface Status

Router#show interfaces serial 1

Serial1 is up, line protocol is up

Hardware is HD64570
Description: 64Kb Line to San Jose
:: :: :: :: :: :: :: :: ::

Operational................. Serial1 is up, line protocol is up
Connection problem... Serial1 is up, line protocol is down
Interface problem........... Serial1 is down, line protocol is down
Disabled ....................... Serial1 is administratively down, line protocol is down
Configuring SNMP

Router# configure term
Router(config)# snmp-server community string [view view-name] [ro | rw] [acl_number]

Defines the community access string

Router# configure term
Router(config)# snmp-server host host-id [traps | informs][version {1 | 2c | 3 [auth | noauth | priv]} ] community-string [udp-port port-number] [notification-type]

Specifies the recipient (host) of the notifications
show snmp Command

Router#sh snmp
337739 SNMP packets input
   0 Bad SNMP version errors
   10 Unknown community name
   0 Illegal operation for community name supplied
   0 Encoding errors
   1283846 Number of requested variables
   0 Number of altered variables
   332559 Get-request PDUs
   5170 Get-next PDUs
   0 Set-request PDUs
341921 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   1685 No such name errors
   0 Bad values errors
   0 General errors
   337729 Response PDUs
   4192 Trap PDUs

SNMP logging: enabled
Logging to 10.10.19.241.162, 0/10, 3995 sent, 197 dropped.
Introduction to Routing Protocol
Introduction to Routing Protocol

- Type of Routing Protocol
- Routing Information Protocol
- Enhanced IGRP
- OSPF
What Is Routing?

• Routing is the process of forwarding an item from one location to another
• Routers forward traffic to a logical destination in a computer network
• Routers perform two major functions:
  – Routing
    • Learning the logical topology of the network
  – Switching
    • Forwarding packets from an inbound interface to an outbound interface
What is Routing? (cont.)

- Routers must learn destinations that are not directly connected
To route a router need to know:

- Destination addresses
- Sources it can learn from
- Possible routes
- Best route
- Maintain and verify routing information
Identifying Static and Dynamic Routes

**Static Route**

Uses a route that a network administrator enters into the router *manually*

**Dynamic Route**

Uses a route that a network *routing protocol* adjusts *automatically* for topology or traffic changes
Configure unidirectional static routes to and from a stub network to allow communications to occur.
Static Route Configuration

Router(config)#ip route network  mask  {address | interface} [distance] [permanent]

Defines a path to an IP destination network or subnet
Static Route Example

This is a unidirectional route. You must have a route configured in the opposite direction.
Default Routes

Router(config)#
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2

This route allows the stub network to reach all known networks beyond router A.
Routing protocols are used between routers to determine paths and maintain routing tables.

Once the path is determined a router can route a **routed** protocol.

<table>
<thead>
<tr>
<th>Network Protocol</th>
<th>Destination Network</th>
<th>Exit Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>10.120.2.0</td>
<td>E0</td>
</tr>
<tr>
<td>RIP</td>
<td>172.16.2.0</td>
<td>S0</td>
</tr>
<tr>
<td>IGRP</td>
<td>172.17.3.0</td>
<td>S1</td>
</tr>
</tbody>
</table>

Routed Protocol: IP/IPX
Routing protocol: RIP, IGRP, OSPF
I need to send a packet to Network E. Both router B and C will get it there. Which route is best?
Administrative Distance

- Administrative distance is a selection method for IP routing protocols
- The lower the administrative distance, the more trusted the learning mechanism
  - Manually entered routes are preferred to dynamically learned routes
  - Routing protocols with sophisticated metrics are preferred over protocols with simple metric structures
## Administrative Distance Comparison Chart

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route out an interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route to a next hop</td>
<td>1</td>
</tr>
<tr>
<td>EIGRP summary route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>Internal EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>IGRP</td>
<td>100</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>IS-IS</td>
<td>115</td>
</tr>
<tr>
<td>RIP v1, v2</td>
<td>120</td>
</tr>
<tr>
<td>EGP</td>
<td>140</td>
</tr>
<tr>
<td>External EIGRP</td>
<td>170</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
<tr>
<td>Unknown</td>
<td>255</td>
</tr>
</tbody>
</table>
Classful Routing Overview

• Classful routing protocols are a consequence of the distance vector method of route calculation
  – RIPv1
  – IGRP

• Routing masks are not carried within the periodic routing updates
  – Within a network, consistency of masks is assumed
Classful Routes

- Subnetwork routes are shared by devices within the same network
- Summary routes are exchanged between foreign networks
  - Summary routes are automatically created at Class A, B, and C network boundaries
Classless Routing Overview

- Classless routing protocols include the routing mask with the route advertisement
  - OSPF
  - EIGRP
  - RIPv2
  - IS-IS
  - BGP

- Summary routes can be manually controlled within the network
• Subnetwork routes are shared by devices within the same network

• Summary routes are exchanged between foreign networks
  – Summary routes are automatically created at Class A, B, and C network boundaries
Classes of Routing Protocols

Distance Vector

Hybrid Routing

Link State
Distance Vector Routing Protocols

- In a distance vector environment, routing updates are propagated only to directly connected neighbors.
- Pass periodic copies of full routing table to neighbor routers and accumulate distance vectors.
Distance Vector—Sources of Information and Discovering Routes

Routers discover the best path to destinations from each neighbor.
In a link-state environment, link-state announcements are propagated to all devices in the routing domain.

- Hierarchical design can limit the requirement to notify all devices.
After initial flood, pass small event-triggered link-state updates to all other routers.
Hybrid Routing

Choose a routing path based on distance vectors

Balanced Hybrid Routing

Converge rapidly using change-based updates

Share attributes of both distance-vector and link-state routing
Router configuration

- Select routing protocols
- Specify networks or interfaces

Networks:
- 160.89.0.0
- 172.30.0.0
- 172.16.0.0

Routing Protocols:
- IGRP
- RIP
Dynamic Routing Configuration

Router(config)#router protocol [keyword]

- Defines an IP routing protocol

Router(config-router)#network network-number

- Mandatory configuration command for each IP routing process
- Identifies the physically connected network that routing updates are forwarded to
RIP Overview
RIP Overview

- Hop count metric selects the path
- Routes update every 30 seconds
- Hop count to infinity = 16
**RIP Routing Metrics**

- Routing metric used by RIP is hop count
  - Using a neighboring router interface is a hop
- Routing process arbitrarily selects a path from several possible equal metric paths
  - IP load balancing is enabled by default

These Addresses Are All Part of the 192.168.0.0 Network

C  5.0 dir conn Eth0
C  4.0 dir conn Ser0
R  10.0 [120/4] via 5.2, Eth0
R  10.0 [120/4] via 5.3, Eth0
R  10.0 [120/4] via 5.4, Eth0
RIP Configuration

Router(config)#**route rip**

- Starts the RIP routing process

Router(config-router)#**network network-number**

- Selects participating attached networks
- The network number must be a major classful network number
RIP1/2 Configuration Example

```
router rip
network 172.16.0.0
network 10.0.0.0
version 2
no auto-summary
```

```
router rip
network 192.168.1.0
network 10.0.0.0
```

```
router rip
network 10.0.0.0
```
Verifying the Routing Protocol—RIP

RouterA#sh ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 0 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: rip
  Default version control: send version 1, receive any version

<table>
<thead>
<tr>
<th>Interface</th>
<th>Send</th>
<th>Recv</th>
<th>Key-chain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Serial2</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

Routing for Networks:
  10.0.0.0
  172.16.0.0

Routing Information Sources:
  Gateway  Distance  Last Update
  10.1.1.2  120      00:00:10

Distance: (default is 120)
Displaying the IP Routing Table

RouterA

#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o - ODR
T - traffic engineered route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets
C  172.16.1.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 2 subnets
R  10.2.2.0 [120/1] via 10.1.1.2, 00:00:07, Serial2
C  10.1.1.0 is directly connected, Serial2
R  192.168.1.0/24 [120/2] via 10.1.1.2, 00:00:07, Serial2

172.16.1.0/24 is subnetted, 1 subnets
S2  172.16.1.1 is connected, Ethernet0
  10.1.1.1
S2  10.1.1.2
S3  10.2.2.2
S3  10.2.2.3
E0  192.168.1.1
EIGRP Overview
What Is Enhanced IGRP (EIGRP)?

- EIGRP supports:
  - Hybrid Routing Protocol
  - Rapid convergence
  - Reduced bandwidth usage
  - Cisco proprietary
EIGRP Features

- Advanced distance vector
- 100% loop free
- Fast convergence
- Easy configuration
- Less network design constraints than OSPF
- Incremental updates
- Supports VLSM and discontiguous networks
- Classless routing
- Compatible with existing IGRP networks
Advantages of EIGRP

• Uses multicast instead of broadcast
• Unequal cost path load balancing
• Easy configuration
• More flexible than OSPF
  – Manual summarization can be done in any interface at any router within the network
EIGRP Support for Different Topologies

- EIGRP supports
  - Multiaccess (LANs)
  - Point-to-point (HDLC)
  - NBMA (Frame Relay)
EIGRP Support for IP Addresses

- EIGRP supports:
  - Variable-length subnet masks (VLSMs)
  - Hierarchical designs
EIGRP Support for Route Summarization

- **EIGRP performs route summarization**
  - Classful network boundaries (default)
  - Arbitrary network boundaries (manual)
EIGRP Operations

- Hello: Establish neighbor relationships
- Update: Send routing updates
- Query: Ask neighbors about routing information
- Reply: Response to query about routing information
- ACK: Acknowledgement of a reliable packet
Two routers become neighbors when they see each other’s hello packet

- Hello address = 224.0.0.10

Hellos sent periodically (5 or 30 seconds)

Neighbor declared dead when no EIGRP packets are received within hold interval

- Not only hello can reset the hold timer

Hold time by default is three times the hello time
What Is in a Neighbor Table?

```
p2r2# show ip eigrp neighbors
IP-EIGRP neighbors for process 400
H Address  Interface  Hold Uptime  SRTT  RTO Q  Seq
          (sec)           (ms)     Cnt Num
1 172.68.2.2  To0    13 02:15:30  8     200  0   9
0 172.68.16.2 Se1    10 02:38:29 29     200  0   6
```
### Initial Route Discovery

1. **Hello**
   - I am router A, who is on the link?

2. **Update**
   - Here is my complete routing information.

3. **Ack**
   - Thanks for the information!

4. **Topology Table**

5. **Update**
   - Here is my complete route information.

6. **Ack**
   - Thanks for the information!

**Converged!**
EIGRP Route Selection

- EIGRP uses a composite metric to pick the best path
Configuring EIGRP

- Network 192.168.0.0 is not configured on Router A because it is not directly connected to Router A

```plaintext
router eigrp 109
network 10.0.0.0
network 172.16.0.0
```

---

www.netstarnetworks.com
EIGRP Summarization—Automatic

- **Purpose**: Smaller routing tables, smaller updates, query boundary

- **Autosummarization**:
  - On major network boundaries, subnetworks are summarized to a single classful (major) network
  - Autosummarization is turned on by default

Diagram:

```
172.16.X.X 172.17.X.X
172.16.0.0/16
```
EIGRP Summarization—Manual

- Manual summarization
  - Configurable on a per-interface basis in any router within network
  - When summarization is configured on an interface, the router immediately creates a route pointing to null zero
    - Loop prevention mechanism
      - When the last specific route of the summary goes away, the summary is deleted
      - The minimum metric of the specific routes is used as the metric of the summary route
Configuring Summarization

(config-router)#

no auto-summary

• Turns off autosummarization for the EIGRP process

(config-if)#

ip summary-address eigrp <as-number> <address> <mask>

• Creates a summary address to be generated by this interface
Summarizing EIGRP Routes

```
router eigrp 1
network 10.0.0.0
network 172.16.0.0
!
int s0
ip address 192.168.4.2 255.255.255.0
!
ip summary-address eigrp 1 172.16.0.0 255.255.0.0
```
Verifying EIGRP Operation

- Displays the neighbors discovered by IP EIGRP
- Displays the IP EIGRP topology table
- Displays current EIGRP entries in the routing table
- Displays the parameters and current state of the active routing protocol process
- Displays the number of IP EIGRP packets sent and received

Router# show ip eigrp neighbors

Router# show ip eigrp topology

Router# show ip route eigrp

Router# show ip protocols

Router# show ip eigrp traffic
OSPF Overview
What Is OSPF?

- Open Shortest Path First
- Has fast convergence
- Hierarchical Routing
- Supports VLSM
- Processes updates efficiently
- Selects paths based on bandwidth
- Supports equal-cost multipath
OSPF Terminology

Autonomous System

Area 1

Cost = 1785

Interfaces

Cost = 10

Neighborhood Database
Lists Neighbors

Token Ring

Area 0

Neighbors

Routing Table
Lists Best Routes

Topography Database
Lists All Routes

Cost = 6
OSPF Topologies

- Broadcast Multiaccess
- Point-to-Point
- NBMA

X.25 Frame Relay
Neighborship

Router ID
Hello/dead intervals *
Neighbors
Area-ID *
Router priority
DR IP address
BDR IP address
Authentication password*
Stub area flag *

* Entry must match on neighboring routers
DR and BDR

- Hellos elect DR and BDR to represent segment
- Each router then forms adjacency with DR and BDR
Choosing Routes

Topology Table

<table>
<thead>
<tr>
<th>Net</th>
<th>Cost</th>
<th>Out Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.2.0</td>
<td>6</td>
<td>To0</td>
</tr>
<tr>
<td>10.3.3.0</td>
<td>7</td>
<td>To0</td>
</tr>
<tr>
<td>10.3.3.0</td>
<td>10</td>
<td>E0</td>
</tr>
</tbody>
</table>

This is the best route to 10.3.3.0.
Link-State Change

- Router A tells all OSPF DRs on 224.0.0.6
- DR tells others on 224.0.0.5

I need to update my routing table.
Configuring OSPF on Internal Routers

Can Assign Network or Interface Address.

Broadcast Network

A

E0

10.64.0.1

B

E0

10.64.0.2

Point-to-Point Network

S0

10.2.1.2

S1

10.2.1.1

Router A:

interface Ethernet0
ip address 10.64.0.1 255.255.255.0

Router B:

interface Ethernet0
ip address 10.64.0.2 255.255.255.0

Router C:

interface Serial0
ip address 10.2.1.2 255.255.255.0

Router C:

router ospf 1
network 10.0.0.0 0.255.255.255 area 0

Router B:

router ospf 50
network 10.2.1.2 0.0.0.0 area 0
network 10.64.0.2 0.0.0.0 area 0

<Output Omitted>
Configuring Optional Commands

Router ID:
- Number by which the router is known to OSPF
- Default: The highest IP address on an active interface at the moment of OSPF process startup
- Can be overridden by a loopback interface: Highest IP address of any active loopback interface

Unadvertised Loopback Address
Ex: 192.168.255.254
- Not in OSPF table
- Saves address space
- Cannot use ping

Advertised Loopback Address
Ex: 172.16.17.5
- In OSPF table
- Uses address space
- Can use ping

Network 172.16.0.0
Configuring Optional Commands (cont.)

Router(config-if)#

```
ip ospf cost cost
```

- Assigns a cost to an outgoing interface
- May be required for interoperability
- Use default cost between Cisco devices
Issues with Maintaining a Large OSPF Network

The SPF is running too often for me to route.

I am only receiving LSAs, no data.

My routing table is too big, I am running low on memory.
OSPF Hierarchical Routing

- Consists of areas and autonomous systems
- Minimizes routing update traffic
Types of OSPF Routers

- **Area 1**
  - Internal Routers
  - ASBR and Backbone Router

- **Backbone Area 0**
  - Backbone/Internal Routers
  - ABR and Backbone Router
  - External AS

- **Area 2**
  - Internal Routers
  - ABR and Backbone Router
Types of Link-State Advertisements

- Type 1: Router link entry
- Type 2: Network link entry
- Type 3 and 4: Summary link entry
- Type 5: AS external link entry
LSAs in OSPF Database

Router Link States (Area 1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Link count</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.2.1</td>
<td>10.1.2.1</td>
<td>651</td>
<td>0x80000005</td>
<td>0xD482</td>
<td>4</td>
</tr>
</tbody>
</table>

Net Link States (Area 1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.64.0.1</td>
<td>10.64.0.1</td>
<td>538</td>
<td>0x80000002</td>
<td>0xAD9A</td>
</tr>
</tbody>
</table>

Summary Net Link States (Area 1)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.1.0</td>
<td>10.2.1.2</td>
<td>439</td>
<td>0x80000002</td>
<td>0xE6F8</td>
</tr>
</tbody>
</table>

p1r3# `show ip ospf database`

OSPF Router with ID (10.64.0.1) (Process ID 1)
Types of Areas

- **Stub Area**: Does not accept external LSAs.
- **Backbone Area 0**: Interconnects areas; accepts all LSAs.
- **Totally Stubby Area**: Does not accept external or summary LSAs.
Configuring OSPF ABRs

Area 0

ABR

Area 1

A

B

C

interface Ethernet0
ip address 10.64.0.1 255.255.255.0
!
router ospf 77
network 10.0.0.0 0.255.255.255 area 0

interface Ethernet0
ip address 10.64.0.2 255.255.255.0
!
interface Serial0
ip address 10.2.1.2 255.255.255.0
router ospf 50
network 10.2.1.2 0.0.0.0 area 1
network 10.64.0.2 0.0.0.0 area 0
Configuring Route Summarization

Router(config-router)#

```
area area-id range address mask
```

- Consolidates intra-area (IA) routes on an ABR

Router(config-router)#

```
summary-address address mask [not-advertise] [tag tag]
```

- Consolidates external routes on an ASBR
Route Summarization Configuration Example

R1#
router ospf 100
network 172.16.32.1 0.0.0.0 area 1
network 172.16.96.1 0.0.0.0 area 0
area 0 range 172.16.96.0 255.255.224.0
area 1 range 172.16.32.0 255.255.224.0

R2#
router ospf 100
network 172.16.64.1 0.0.0.0 area 2
network 172.16.127.1 0.0.0.0 area 0
area 0 range 172.16.96.0 255.255.224.0
area 1 range 172.16.32.0 255.255.224.0
Verifying OSPF Operation

Router#

- `show ip protocols`
  - Verifies that OSPF is configured

Router#

- `show ip route`
  - Displays all the routes learned by the router

Router#

- `show ip ospf interface`
  - Displays area ID and adjacency information
Verifying OSPF Operation (cont.)

Router#

```
show ip ospf
```

- Displays OSPF timers and statistics

Router#

```
show ip ospf neighbor detail
```

- Displays information about DR, BDR and neighbors

Router#

```
show ip ospf database
```

- Displays the link-state database
Verifying OSPF Operation (cont.)

Router#

`clear ip route *`

- Allows you to clear the IP routing table (for all routing protocol)
R2#show ip ospf int e0
Ethernet0 is up, line protocol is up
   Internet Address 192.168.0.12/24, Area 0
   Process ID 1, Router ID 192.168.0.12, Network Type BROADCAST, Cost: 10
   Transmit Delay is 1 sec, State DROTHER, Priority 1
   Designated Router (ID) 192.168.0.11, Interface address 192.168.0.11
   Backup Designated router (ID) 192.168.0.13, Interface address 192.168.0.13
   Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:04
   Neighbor Count is 3, Adjacent neighbor count is 2
      Adjacent with neighbor 192.168.0.13 (Backup Designated Router)
      Adjacent with neighbor 192.168.0.11 (Designated Router)
   Suppress hello for 0 neighbor(s)
R2#show ip ospf database

OSPF Router with ID (192.168.0.12) (Process ID 1)

Router Link States (Area 0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
<th>Link count</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.10</td>
<td>192.168.0.10</td>
<td>817</td>
<td>0x80000003</td>
<td>0xFF56</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.11</td>
<td>192.168.0.11</td>
<td>817</td>
<td>0x80000003</td>
<td>0xFD55</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.12</td>
<td>192.168.0.12</td>
<td>816</td>
<td>0x80000003</td>
<td>0xFB54</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.13</td>
<td>192.168.0.13</td>
<td>816</td>
<td>0x80000003</td>
<td>0xF953</td>
<td>1</td>
</tr>
<tr>
<td>192.168.0.14</td>
<td>192.168.0.14</td>
<td>817</td>
<td>0x80000003</td>
<td>0xD990</td>
<td>1</td>
</tr>
</tbody>
</table>

Net Link States (Area 0)

<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.14</td>
<td>192.168.0.14</td>
<td>812</td>
<td>0x80000002</td>
<td>0x4AC8</td>
</tr>
</tbody>
</table>
R2# show ip route ospf

163.24.0.0/16 is variably subnetted, 16 subnets, 3 masks
O E2  163.24.0.0/16 [110/20] via 163.24.165.254, 1w5d, Vlan1
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O E2  10.163.96.0/19 [110/20] via 163.24.165.254, 1w5d, Vlan1
O E2  210.60.38.0/24 [110/20] via 163.24.165.254, 1w5d, Vlan1
O E2  203.71.77.0/24 [110/20] via 163.24.165.254, 1w5d, Vlan1
ip classless Command

To get to 10.7.1.1:
- With `ip classless` → Default
- With `no ip classless` → Drop
Configuring IP Access Lists
Managing IP Traffic Overview

- Limit traffic and restrict network use
- Enable directed forwarding of broadcasts
Access List Applications

Transmission of Packets on an Interface

Virtual Terminal Line Access (IP)

- Access lists control packet movement through a network
IP Standard Access Lists Overview

• Use source address only
• Access list range: 1 to 99
Inbound Access List Processing

For Standard IP Access Lists

- Incoming packet
  - Access list on interface?
    - No
    - Yes
      - Does source address match?
        - No
          - More entries?
            - Yes
              - Next entry in list
            - No
              - Deny
        - Yes
          - Apply condition
            - Permit
            - Deny
      - More entries?
        - Yes
          - Next entry in list
        - No
          - ICMP Message

- Do route table lookup
  - Route to interface
For Standard IP Access Lists

1. Outgoing packet
2. Do route table lookup
3. Access list on interface?
   - Yes
     1. Next entry in list
     2. Does source address match?
        - Yes
         1. Apply condition
         2. Permit
        - No
         1. Deny
         2. ICMP Message
   - No
     1. Next entry in list
     2. More entries?
        - Yes
         1. Go to step 2
        - No
         1. Go to step 3
### Access Lists Use Wildcard Mask

<table>
<thead>
<tr>
<th>Address</th>
<th>Mask</th>
<th>Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
<td>any address</td>
</tr>
<tr>
<td>131.108.0.0/16</td>
<td>0.0.255.255</td>
<td>network 131.108.0.0</td>
</tr>
<tr>
<td>131.104.7.11/16</td>
<td>0.0.0.0</td>
<td>host or subnet address</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>0.0.0.0</td>
<td>local broadcast</td>
</tr>
<tr>
<td>131.111.8.0</td>
<td>0.0.7.255</td>
<td>only subnet 131.111.8.0 *</td>
</tr>
</tbody>
</table>

- **0 bit = must match bits in addresses**
- **1 bit = no need to match bits in addresses**

* Assuming subnet mask of 255.255.248.0
**Wildcard Bits: How to Check the Corresponding Address Bits**

<table>
<thead>
<tr>
<th>Octet bit position and address value for bit</th>
<th>128</th>
<th>64</th>
<th>32</th>
<th>16</th>
<th>8</th>
<th>4</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0 0 0 0 0 0 0 0 0 =</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 0 0 1 1 1 1 1 1 1 =</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0 0 0 0 0 0 1 1 1 1 1 =</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 1 1 1 1 1 0 0 0 =</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 1 1 1 1 1 1 1 1 1 =</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Examples**
- check all address bits (match all)
- ignore last 6 address bits
- ignore last 4 address bits
- check last 2 address bits
- do not check address (ignore bits in octet)

- 0 means check corresponding address bit value
- 1 means ignore value of corresponding address bit
Wildcard Bits to Match a Specific IP Host Address

Test conditions: Check all the address bits (match all)

An IP host address, for example:

172.30.16.29

Wildcard mask: 0.0.0.0

(checks all bits)

- Example 172.30.16.29 0.0.0.0 checks all the address bits

- Abbreviate this wildcard mask using the IP address preceded by the keyword host (host 172.30.16.29)
Test conditions: Ignore all the address bits (match any)

Any IP address
0.0.0.0

Wildcard mask: 255.255.255.255
(ignore all)

- Accept any address: 0.0.0.0 255.255.255.255
- Abbreviate the expression using the keyword *any*
Check for IP subnets 172.30.16.0/24 to 172.30.31.0/24
Address and wildcard mask:

172.30.16.0  0.0.15.255

Network  .host
172.30.16.0

Wildcard mask:
0 0 0 1 0 0 0 0
0 0 0 0 1 1 1 1

|<---- match ---->|<----- don’t care ----->|
0 0 0 1 0 0 0 0 = 16
0 0 0 1 0 0 0 1 = 17
0 0 0 1 0 1 0 0 = 18
: 
0 0 0 1 1 1 1 1 = 31
To create an access list, perform the following tasks:

- Define an access list
- Apply the list to an interface
Standard Access List Commands

Router(config)#
```text
access-list access-list-number { permit | deny }
{ source [ source-wildcard ] | any }
```

• Defines a standard access list (numbered 1-99)

Router(config-if)#
```text
ip access-group access-list-number { in | out }
```

• Applies an access list to a specific interface
Implicit Masks

For Standard IP Access Lists

<table>
<thead>
<tr>
<th>Correct</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list 1</td>
<td>permit 131.108.5.17</td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Common Errors</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list 1</td>
<td>permit 0.0.0.0</td>
</tr>
<tr>
<td>access-list 1</td>
<td>permit 131.108.0.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Not Needed</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list 1</td>
<td>deny any</td>
</tr>
<tr>
<td>access-list 1</td>
<td>deny 0.0.0.0 255.255.255.255</td>
</tr>
</tbody>
</table>

- Omitted mask assumed to be 0.0.0.0
- Last two lines unnecessary (implicit deny any)
Configuration Principles

• Top-down processing
  – Place more specific references first

• Implicit deny any
  – Unless access list ends with explicit permit any

• New lines added to the end
  – Cannot selectively add/remove lines

• Undefined access list = permit any
  – Need to create access list lines for implicit deny any
Standard IP Access List
Example 1

Router(config)#access-list 2 permit 10.48.0.3
Router(config)#access-list 2 deny 10.48.0.0 0.0.255.255
Router(config)#access-list 2 permit 10.0.0.0 0.255.255.255
Router(config)#!(Note: all other access implicitly denied)
Router(config)#interface ethernet 0
Router(config-if)#ip access-group 2 in

• Who can connect to A?
Standard IP Access List
Example 2

access-list 1 permit 172.16.0.0 0.0.255.255
(implicit deny all - not visible in the list)
(access-list 1 deny 0.0.0.0 255.255.255.255)

interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out

• Permit my network only
Standard IP Access List

Example 3

```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0 255.255.255.255)
interface ethernet 0
ip access-group 1 out

• Deny a specific host
```
Standard IP Access List Example 4

- Deny a specific subnet

access-list 1 deny 172.16.4.0 0.0.0.255
access-list 1 permit any
(implicit deny all)
(access-list 1 deny 0.0.0.0 255.255.255.255)

interface ethernet 0
ip access-group 1 out
On which router should the access list be configured to deny host Z access to network 10.20.0.0?

How does location of a standard access list change the policy implemented?
IP Extended Access List
Overview

• Control traffic by application, not just address
### Standard versus External Access List

<table>
<thead>
<tr>
<th>Standard</th>
<th>Extended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters Based on Source.</td>
<td>Filters Based on Source and destination.</td>
</tr>
<tr>
<td>Permit or deny entire TCP/IP protocol suite.</td>
<td>Specifies a specific IP protocol and port number.</td>
</tr>
<tr>
<td>Range is 1 through 99</td>
<td>Range is 100 through 199.</td>
</tr>
</tbody>
</table>
Extended Access List Processing

- Access list?
  - Yes: Match
    - Source address
      - Match
        - Destination address
          - Match
            - Protocol? *
              - Match
                - Protocol options? *
                  - Match
                    - Apply condition
                        - Deny
                          - Does Not Match
                        - Permit
                          - Forward Packet
                    - Does Not Match
                      - Next entry in list
                  - Does Not Match
                    - Next entry in list
                - Does Not Match
                  - Next entry in list
            - Does Not Match
              - Next entry in list
        - Does Not Match
          - Next entry in list
    - Does Not Match
      - Next entry in list
  - No

* If present in access list
Extended IP Access List Command

Router(config)#

access-list  access-list-number { permit | deny }

{ protocol | protocol-keyword }

{ source source-wildcard | any }

{ destination destination-wildcard | any }

[ protocol-specific options ] [ log ]

- Defines an extended access list (numbered 100 to 199)
- Protocol keywords icmp, tcp, and udp define alternate syntax with protocol-specific options
Extended Mask Keywords

- The keyword *any* can be used in place of the address 0.0.0.0 with mask 255.255.255.255

- The keyword *host* preceding an *ip-address* can be used in place of the mask 0.0.0.0
ICMP Command Syntax

Router(config)#

access-list access-list-number { permit | deny } icmp
{ source source-wildcard | any }
{ destination destination-wildcard | any }
[ icmp-type [ icmp-code ] | icmp-message ]

• Filters based on ICMP messages
### ICMP Message and Type Names

- administratively-prohibited
- alternate-address
- conversion-error
- dod-host-prohibited
- dod-net-prohibited
- echo
- echo-reply
- general-parameter-problem
- host-isolated
- host-tos-redirect
- host-tos-unreachable
- host-unknown
- host-unreachable
- information reply
- mask-reply
- mask-request
- mobile-redirect
- net-redirect
- net-tos-redirect
- net-tos-unreachable
- net-unreachable
- network-unknown
- no-room-for-option
- option-missing
- packet-too-big
- parameter-problem
- port unreachable
- reassembly-timeout
- redirect
- router-advertisement
- router-solicitation
- source-quench
- source-route-failed
- source-route-failed
- traceroute
- ttl-exceeded
- unreachable

- **Names simplify configuration**
TCP Syntax

Router(config)#

access-list access-list-number { permit | deny } tcp

{ source source-wildcard | any }

[ operator source-port | source-port ]

{ destination destination-wildcard | any }

[ operator destination-port | destination-port ]

[ established ]

- Filters based on tcp/tcp port number or name
### TCP Port Names

<table>
<thead>
<tr>
<th>bgp</th>
<th>gopher</th>
<th>sunrpc</th>
</tr>
</thead>
<tbody>
<tr>
<td>chargen</td>
<td>hostname</td>
<td>syslog</td>
</tr>
<tr>
<td>daytime</td>
<td>irc</td>
<td>tacacs-ds</td>
</tr>
<tr>
<td>discard</td>
<td>klogin</td>
<td>talk</td>
</tr>
<tr>
<td>domain</td>
<td>kshell</td>
<td>telnet</td>
</tr>
<tr>
<td>echo</td>
<td>lpd</td>
<td>time</td>
</tr>
<tr>
<td>finger</td>
<td>nntp</td>
<td>uucp</td>
</tr>
<tr>
<td>ftp control</td>
<td>pop2</td>
<td>whois</td>
</tr>
<tr>
<td>ftp-data</td>
<td>pop3</td>
<td>www</td>
</tr>
</tbody>
</table>

- Enter `?` to get port numbers corresponding to names
- Other port numbers found in the Assigned Numbers RFC
Router(config)#

```
access-list access-list-number { permit | deny } udp
  { source source-wildcard | any }
  [ operator source-port | source-port ]
{ destination destination-wildcard | any }
  [ operator destination-port | destination-port ]
```

- Filters based on UDP protocol or UDP port number or name
### UDP Port Names

<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>biff</td>
<td>nameserver</td>
<td>syslog</td>
</tr>
<tr>
<td>bootpc</td>
<td>netbios-dgm</td>
<td>tacasds-ds</td>
</tr>
<tr>
<td>bootps</td>
<td>netbios-ns</td>
<td>talk</td>
</tr>
<tr>
<td>discard</td>
<td>ntp</td>
<td>tftp</td>
</tr>
<tr>
<td>dns</td>
<td>rip</td>
<td>time</td>
</tr>
<tr>
<td>dnsix</td>
<td>snmp</td>
<td>whois</td>
</tr>
<tr>
<td>echo</td>
<td>snmptrap</td>
<td>xdmcp</td>
</tr>
<tr>
<td>mobile-ip</td>
<td>sunrpc</td>
<td></td>
</tr>
</tbody>
</table>

- Enter `?` to get port numbers corresponding to the name
- Other port numbers found in the Assigned Numbers RFC

www.netstarnetworks.com
Extended Access List
Example 1

Providing Internet Mail

```
172.22.1.2

access-list 103 permit tcp any 172.22.0.0 0.0.255.255 established
access-list 103 permit tcp any host 172.22.1.2 eq smtp

! interface ethernet 1
ip access-group 103 in
```
access-list 104 permit tcp any 172.22.0.0 0.0.255.255 established  
access-list 104 permit tcp any host 172.22.1.2 eq smtp  
access-list 104 permit udp any any eq dns  
access-list 104 permit icmp any any echo  
access-list 104 permit icmp any any echo-reply  
!  
interface serial 0  
ip access-group 104 in
access-list 118 permit tcp any 172.22.0.0 0.0.255.255 eq www established
access-list 118 permit tcp any host 172.22.1.2 eq smtp
access-list 118 permit udp any any eq dns
access-list 118 permit udp 172.22.3.0 0.0.0.255 172.22.1.0 0.0.0.255 eq snmp
access-list 118 deny icmp any 172.22.0.0 0.0.255.255 echo
access-list 118 permit icmp any any echo-reply
!
interface ethernet 0
ip access-group 118 out
Extended Access List Example 4

access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
access-list 101 permit ip any any
(implicit deny all)
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

interface ethernet 0
ip access-group 101 out

- Deny FTP from subnet 172.16.4.0 to subnet 172.16.3.0 out of E0
- Permit all other traffic
Extended Access List Example 5

access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23
access-list 101 permit ip any any
(implicit deny all)

interface ethernet 0
ip access-group 101 out

- Deny only Telnet from subnet 172.16.4.0 out of E0
- Permit all other traffic
Virtual Terminal Access Overview

- Standard and extended access lists will not block access from the router
- For security, virtual terminal (vty) access can be blocked to or from the router
How to Control vty Access

- Five virtual terminal lines (0 through 4)
- Set identical restrictions on all the virtual terminal lines
Virtual Terminal Line Commands

Router(config)#

```bash
line vty { vty-number | vty-range }
```

- Enters configuration mode for a terminal line or a range of lines

Router(config-line)#

```bash
access-class access-list-number { in | out }
```

- Restricts incoming and outgoing connections between a particular virtual terminal line (into a device) and the addresses in an access list
Virtual Terminal Access Example

Controlling Inbound Access

access-list 12 permit 192.89.55.0 0.0.0.255
!
line vty 0 4
access-class 12 in

• Permits only hosts in network 192.89.55.0 to connect to the virtual terminal ports on the router
Access List show Commands

- Displays access lists from all protocols
  Router#
  show access-list

- Displays a specific IP access list
  Router#
  show ip access-list [ access-list-number ]

- Clears packet counts
  Router#
  clear access-list counters [ access-list-number ]

- Displays line configuration
  Router#
  show line
show ip access-lists
Command

p1r1#show access-lists
Extended IP access list 100
  deny tcp host 10.1.1.2 host 10.1.1.1 eq telnet (3 matches)
  deny tcp host 10.1.2.2 host 10.1.2.1 eq telnet
  permit ip any any (629 matches)

• Matches are shown for extended access lists
Network Address Translation
Why Use NAT?

Use NAT if:

- You need to connect to the Internet and your hosts do not have globally unique IP addresses
- You change over to a new ISP that requires you to renumber your network
- Two intranets with duplicate addresses merge
- You want to support basic load sharing
NAT Overview and Terminology

Inside

10.1.1.2
10.1.1.1

Internet

NAT table

<table>
<thead>
<tr>
<th>Inside Local IP Address</th>
<th>Inside Global IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>A 10.1.1.1</td>
<td>B 192.168.2.2</td>
</tr>
</tbody>
</table>

Host B 172.20.7.3

SA 10.1.1.1
DA 192.168.2.2

SA 192.168.2.2
DA 10.1.1.1
• **Inside local address**
  —The IP address that is assigned to a host on the inside network. The address is probably not a legitimate IP address assigned by the Network Information Center (NIC) or service provider.

• **Inside global address**
  —A legitimate IP address (assigned by the NIC or service provider) that represents one or more inside local IP addresses to the outside world.

• **Outside local address**
  —The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it was allocated from address space routable on the inside.

• **Outside global address**
  —The IP address assigned to a host on the outside network by the host's owner. The address was allocated from globally routable address or network space.
NAT functions:

- Translation inside local addresses
- Overloading inside global addresses
Translating Inside Local Addresses

<table>
<thead>
<tr>
<th>Inside Local IP Address</th>
<th>Inside Global IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.3</td>
<td>192.168.2.4</td>
</tr>
<tr>
<td>10.1.1.2</td>
<td>192.168.2.3</td>
</tr>
<tr>
<td>10.1.1.1</td>
<td>192.168.2.2</td>
</tr>
</tbody>
</table>
Overloading Inside Global Addresses

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Inside Local IP Address: Port</th>
<th>Inside Global IP Address: Port</th>
<th>Outside Global IP Address: Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>10.1.1.3:1723</td>
<td>192.168.2.2:1492</td>
<td>172.21.7.3:23</td>
</tr>
<tr>
<td>TCP</td>
<td>10.1.1.2:1723</td>
<td>192.168.2.2:1723</td>
<td>172.21.7.3:23</td>
</tr>
<tr>
<td>TCP</td>
<td>10.1.1.1:1024</td>
<td>192.168.2.2:1024</td>
<td>172.20.7.3:23</td>
</tr>
</tbody>
</table>
Static NAT Configuration Example

```
interface Ethernet0
  ip address 10.1.1.10 255.255.255.0
  ip nat inside

interface Serial0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside

ip nat inside source static 10.1.1.1 192.168.2.2
```

This interface connected to the inside network.

This interface connected to the outside world.

Maps the inside local address to the inside global address.
Translate between inside hosts addressed from 10.1.1.0/24 to the globally unique 192.168.2.0/24 network.

This interface connected to the inside network.

This interface connected to the outside world.
ip nat pool ovrd-nat 192.168.2.1 192.168.2.2
    netmask 255.255.255.0
ip nat inside source list 1 pool ovrd-nat overload
!
interface Ethernet0/0
 ip address 10.1.1.10 255.255.255.0
 ip nat inside
!
interface Serial0/0
 ip address 172.16.2.1 255.255.255.0
 ip nat outside
!
access-list 1 permit 10.1.1.0 0.0.0.255
Verifying NAT

Basic IP address translation

```
Router# show ip nat trans
Pro Inside global  Inside local  Outside local Outside global
--- 192.2.2.1      10.1.1.1     --- ---
--- 192.2.2.2      10.1.1.2     --- ---
```

```
Router# show ip nat trans
Pro Inside global  Inside local  Outside local Outside global
--- 192.2.2.1      10.1.1.1     --- ---
--- 192.2.2.2      10.1.1.2     --- ---
```

IP address translation with overloading

```
Router# sh ip nat trans
Pro Inside global  Inside local  Outside local Outside global
tcp 192.168.2.1:11003 10.1.1.1:11003 172.16.2.2:23 172.16.2.2:23
tcp 192.168.2.1:1067 10.1.1.1:1067 172.16.2.3:23 172.16.2.3:23
```

Unique TCP port numbers are used to distinguish between hosts.

A translation for a Telnet is still active.
Two different inside hosts appear on the outside with a single IP address.
Clearing NAT Translation Entries

All entries are cleared.

192.168.2.2 is cleared.
Troubleshooting Tools
Troubleshooting Tools

- Cisco IOS tools and commands in the router
- Password recovery
- Router IOS Backup & Upgrade
Use Built-In Tools for Troubleshooting

- Cisco IOS tools and commands in the router
- TCP/IP tools included with Windows
Cisco IOS Software Tools and Commands

- show ip interface
- clear counter
- show ip route
- show ip traffic
- show cdp neighbor
- show ip arp (and clear arp-cache)
- ping ip (privileged)
- Tracerotue (privileged)
- show process
- Show ip accounting
- Show ip
- show logging
- show ip account
show interfaces ethernet

Router> `show interfaces ethernet 0`

Ethernet 0 is **up**, line protocol is **up**
   Hardware is MCI Ethernet, address is **aa00.0400.0134** (bia **0000.0c00.4369**)
   Internet address is **131.108.1.1**, subnet mask is **255.255.255.0**
   MTU 1500 bytes, **BW 10000 Kbit**, DLY 1000 usec, **rely 255/255**, **load 1/255**
   Encapsulation ARPA, loopback not set, keepalive set (10 sec)
   ARP type: ARPA, PROBE, ARP Timeout 4:00:00
   Last input 0:00:00, output 0:00:00, output hang never
   Last clearing of “show interface” counters 0:56:40
   Output queue 0/40, 0 drops; input queue 0/75, 2 drops
   Five minute **input rate** 6100 bits/sec, 4 packets/sec
   Five minute **output rate** 1000 bits/sec, 2 packets/sec
   2295197 **packets input**, 305539992 bytes, 0 no buffer
   Received 1925500 broadcasts, 0 runts, 0 giants
   3 **input errors**, 3 **CRC**, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 input packets with dribble condition detected
   3594664 **packets output**, 436549843 bytes, 0 underruns
   8 output errors, 1790 collisions, 10 interface resets, 0 restarts
clear counters Command

Router> show int s 1
Serial1 is up, line protocol is up

Hardware is cxBus Serial
Description: 56Kb Line San Jose - MP
Internet address is 150.136.190.203, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 56 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:07, output 0:00:00, output hang never
Last clearing of "show interface" counters 2w4d
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
16263 packets input, 1347238 bytes, 0 no buffer
Received 13983 broadcasts, 0 runts, 0 giants
2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
0 input packets with dribble condition detected
22146 packets output, 2383680 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets, 0 restarts
1 carrier transitions

Router#clear counters
show cdp neighbors

```
Capability Codes: R - Router, T - Trans Bridge,
                 B - Source Route Bridge,
                 S - Switch, H - Host, I - IGMP

Device ID     Local Intrfce Holdtme Capability Platform  Port ID
routerB.cisco.com Eth 0       151       R T       AGS       Eth 0
routerB.cisco.com Ser 0       165       R T       AGS       Ser 3
```

detail

```
Device ID: routerB.cisco.com
Entry address(es):
  IP address: 198.92.68.18
  CLNS address: 490001.1111.1111.1111.00
  Appletalk address: 10.1
Platform: AGS, Capabilities: Router Trans-Bridge
Interface: Ethernet0, Port ID (outgoing port): Ethernet0
Holdtime : 143 sec
```
show ip arp Command

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age(min)</th>
<th>Hardware Addr</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>171.69.233.22</td>
<td>9</td>
<td>0000.0c59.f892</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>171.69.233.21</td>
<td>8</td>
<td>0000.0c07.ac00</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>171.69.233.19</td>
<td>-</td>
<td>0000.0c63.1300</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>171.69.233.30</td>
<td>9</td>
<td>0000.0c36.6965</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.19.168.11</td>
<td>-</td>
<td>0000.0c63.1300</td>
<td>SNAP</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.19.168.254</td>
<td>9</td>
<td>0000.0c36.6965</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.19.168.17</td>
<td>0</td>
<td>Incomplete</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
</tbody>
</table>
Clear arp-cache Command

Router# **clear arp-cache**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age(min)</th>
<th>Hardware Addr</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>171.69.233.22</td>
<td>0</td>
<td>0000.0c59.f892</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>171.69.233.21</td>
<td>0</td>
<td>0000.0c07.ac00</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>171.69.233.19</td>
<td>-</td>
<td>0000.0c63.1300</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>171.69.233.30</td>
<td>0</td>
<td>0000.0c36.6965</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.19.168.11</td>
<td>-</td>
<td>0000.0c63.1300</td>
<td>SNAP</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.19.168.254</td>
<td>0</td>
<td>0000.0c36.6965</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
</tbody>
</table>
Reachability and Step-by-Step Path Tests

Test reachability:
• ping ip

Test step-by-step path:
• trace

These tests operate in two levels: user mode and privileged mode
R4#ping 10.36.195.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.36.195.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
R4#ping 10.36.195.95
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.36.195.95, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#  ping
Protocol [ip]:
Target IP address: fred
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]
Extended commands [n]: y
Source address: 10.36.195.148
Type of service [0]:
Set DF bit in IP header? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Number of hops [9]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 131.108.1.115, timeout is 2 seconds:
!!!!!
Router# trace ip ABA.NYC.mil
Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
1 DEBRIS.CISCO.COM (131.108.1.6) 1000 msec 8 msec 4 msec
2 BARRNET-GW.CISCO.COM (131.108.16.2) 8 msec 8 msec 8 msec
3 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
4 BB2.SU.BARRNET.NET (131.119.254.6) 8 msec 8 msec 8 msec
5 SU.ARC.BARRNET.NET (131.119.3.8) 12 msec 12 msec 8 msec
6 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
7 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
Router# trace
Protocol [ip]:
Target IP address: mit.edu
Source address:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port number[33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to MIT.EDU (18.72.2.1)
  1 ICM-DC-2-V1.ICP.NET (192.108.209.17) 72 msec 72 msec 88 msec
  2 ICM-FIX-E-H0-T3.ICP.NET (192.157.65.122) 80 msec 128 msec 80 msec
  3 192.203.229.246 540 msec 88 msec 84 msec
  4 T3-2.WASHINGTON-DC-CNSS58.T3.ANS.NET (140.222.58.3) 84 msec 116 msec 88 msec
  5 T3-3.WASHINGTON-DC-CNSS56.T3.ANS.NET (140.222.56.4) 80 msec 132 msec 88 msec
  6 T3-0.NEW-YORK-CNSS32.T3.ANS.NET (140.222.32.1) 92 msec 132 msec 88 msec
  7 T3-0.HARTFORD-CNSS48.T3.ANS.NET (140.222.48.1) 88 msec 88 msec 88 msec
show processes command

Router# `show processes`

- Add argument `cpu` to show detailed CPU utilization
- Add argument `memory` to show memory usage

<table>
<thead>
<tr>
<th>PID</th>
<th>Q</th>
<th>T</th>
<th>PC</th>
<th>Runtime (ms)</th>
<th>Invoked</th>
<th>uSecs</th>
<th>Stacks</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 M</td>
<td>E</td>
<td>122DE</td>
<td>62812</td>
<td>4897</td>
<td>12826</td>
<td>780/1000</td>
<td>0</td>
<td>Net Background</td>
<td></td>
</tr>
<tr>
<td>2 M</td>
<td>E</td>
<td>22842</td>
<td>8</td>
<td>19</td>
<td>421</td>
<td>804/1000</td>
<td>0</td>
<td>Logger</td>
<td></td>
</tr>
<tr>
<td>809 M</td>
<td>E</td>
<td>74AF0</td>
<td>272808</td>
<td>489888</td>
<td>556</td>
<td>1504/2000</td>
<td>36</td>
<td>Exec</td>
<td></td>
</tr>
<tr>
<td>4 H</td>
<td>E</td>
<td>67C0</td>
<td>373540</td>
<td>630248</td>
<td>592</td>
<td>628/900</td>
<td>0</td>
<td>IP Input</td>
<td></td>
</tr>
<tr>
<td>5 M</td>
<td>E</td>
<td>3E124</td>
<td>26044</td>
<td>630201</td>
<td>41</td>
<td>824/1000</td>
<td>0</td>
<td>IP Protocols</td>
<td></td>
</tr>
<tr>
<td>6 M</td>
<td>E</td>
<td>46BA2</td>
<td>592</td>
<td>255178</td>
<td>2</td>
<td>794/1000</td>
<td>0</td>
<td>TCP Timer</td>
<td></td>
</tr>
<tr>
<td>7 L</td>
<td>E</td>
<td>47CE6</td>
<td>1736</td>
<td>1635</td>
<td>1061</td>
<td>776/1000</td>
<td>0</td>
<td>TCP Protocols</td>
<td></td>
</tr>
<tr>
<td>8 L</td>
<td>E</td>
<td>67C0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>958/1000</td>
<td>0</td>
<td>ARP Input</td>
<td></td>
</tr>
<tr>
<td>813 M *</td>
<td>768</td>
<td>384</td>
<td>93</td>
<td>4129</td>
<td>1456/2000</td>
<td>42</td>
<td>Virtual Exec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 M</td>
<td>E</td>
<td>3F51E</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>894/1000</td>
<td>0</td>
<td>BOOTP Server</td>
<td></td>
</tr>
<tr>
<td>11 H</td>
<td>E</td>
<td>67C0</td>
<td>25096</td>
<td>194823</td>
<td>128</td>
<td>426/500</td>
<td>0</td>
<td>Net Input</td>
<td></td>
</tr>
<tr>
<td>12 M</td>
<td>T</td>
<td>36FA</td>
<td>5420</td>
<td>277303</td>
<td>19</td>
<td>850/1000</td>
<td>0</td>
<td>TTY Background</td>
<td></td>
</tr>
<tr>
<td>13 L</td>
<td>E</td>
<td>5444E</td>
<td>65996</td>
<td>24907</td>
<td>2649</td>
<td>686/1000</td>
<td>0</td>
<td>SNMP Server</td>
<td></td>
</tr>
<tr>
<td>14 M</td>
<td>E</td>
<td>6E842</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>966/1000</td>
<td>0</td>
<td>Serial Line IP</td>
<td></td>
</tr>
</tbody>
</table>
show ip accounting command

Router(config)# interface int_id
Router(config-int)# ip accounting output-packets

Router# sh ip accounting

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.206.26</td>
<td>218.145.30.108</td>
<td>4005</td>
<td>256571</td>
</tr>
<tr>
<td>192.168.206.25</td>
<td>134.208.10.102</td>
<td>1020</td>
<td>1164464</td>
</tr>
<tr>
<td>192.168.206.25</td>
<td>207.157.91.50</td>
<td>1</td>
<td>92</td>
</tr>
<tr>
<td>192.168.206.1</td>
<td>210.242.194.193</td>
<td>35978</td>
<td>45950896</td>
</tr>
<tr>
<td>192.168.206.26</td>
<td>63.241.199.50</td>
<td>4594</td>
<td>325046</td>
</tr>
<tr>
<td>192.168.206.30</td>
<td>64.4.15.117</td>
<td>29</td>
<td>1419</td>
</tr>
<tr>
<td>192.168.206.30</td>
<td>67.128.31.226</td>
<td>15</td>
<td>875</td>
</tr>
<tr>
<td>192.168.206.26</td>
<td>203.66.227.80</td>
<td>706</td>
<td>49264</td>
</tr>
<tr>
<td>192.168.206.26</td>
<td>209.69.32.137</td>
<td>4629</td>
<td>280846</td>
</tr>
</tbody>
</table>

- Output packets accounting with source and destination address
**show ip cache flow command**

Router(config)# `interface int_id`
Router(config-int)# `ip route-cache flow`

Router# `sh ip cache flow`

... (omitted)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Total Flows</th>
<th>Flows /Sec</th>
<th>Packets Bytes</th>
<th>Packets /Pkt</th>
<th>Active(Sec)</th>
<th>Idle(Sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-WWW</td>
<td>4489203</td>
<td>1.1</td>
<td>28</td>
<td>752</td>
<td>33.4</td>
<td>7.2</td>
</tr>
<tr>
<td>TCP-SMTP</td>
<td>6851085</td>
<td>1.7</td>
<td>34</td>
<td>737</td>
<td>61.4</td>
<td>6.9</td>
</tr>
<tr>
<td>UDP-DNS</td>
<td>4687104</td>
<td>1.2</td>
<td>6</td>
<td>62</td>
<td>7.9</td>
<td>2.6</td>
</tr>
<tr>
<td>ICMP</td>
<td>7076822</td>
<td>1.8</td>
<td>1</td>
<td>191</td>
<td>2.7</td>
<td>0.7</td>
</tr>
<tr>
<td>IP-other</td>
<td>2519</td>
<td>0.0</td>
<td>22</td>
<td>494</td>
<td>0.0</td>
<td>13.5</td>
</tr>
<tr>
<td>Total:</td>
<td>395612036</td>
<td>103.4</td>
<td>6</td>
<td>552</td>
<td>716.1</td>
<td>3.6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SrcIf</th>
<th>SrcIPaddress</th>
<th>DstIf</th>
<th>DstIPaddress</th>
<th>Pr</th>
<th>SrcP</th>
<th>DstP</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Se0/0</td>
<td>210.71.184.250</td>
<td>Et0/0</td>
<td>202.39.206.201</td>
<td>06</td>
<td>1201</td>
<td>01BB</td>
<td>571</td>
</tr>
<tr>
<td>Et0/0</td>
<td>10.10.32.9</td>
<td>Null</td>
<td>10.10.255.255</td>
<td>11</td>
<td>008A</td>
<td>008A</td>
<td>8</td>
</tr>
<tr>
<td>Et1/0</td>
<td>219.137.120.198</td>
<td>Et0/0</td>
<td>61.67.10.21</td>
<td>06</td>
<td>1AE1</td>
<td>1341</td>
<td>2262</td>
</tr>
</tbody>
</table>

- Flow records with detailed information.
Error Message Loggin

- **Console**
  - logging on (default)
  - logging console

- **Syslog Server**
  - logging ip-address
  - logging trap

- **PC**
  - logging monitor
  - logging buffered (default)
Router#show logging
Syslog logging: enabled
  Console logging: disabled
  Monitor logging: level debugging, 18 messages logged.
  Trap logging: level informational, 18 messages logged.
  Logging to 192.31.7.19
SNMP logging: enabled, retransmission after 30 seconds
  741 messages logged
  Logging to 131.108.1.27, 0/10
Feb 18 19:49:50 %SYS-5-CONFIG_I: Configured from console by vty0 (10.36.195.154)
Feb 18 20:05:13 %SYS-5-CONFIG_I: Configured from console by vty0 (10.36.195.154)
...
Password Recovery
Internal Configuration Components

RAM  NVRAM  Flash  ROM
Router Status Commands

Router#show version
Router#show flash
Router#show interface

RAM
- Internetwork Operating System
- Programs
- Dynamic Configuration Information
- Table and Buffers

NVRAM
- Backup Configuration File
- Operation System

Flash
- Interfaces

Router#show processes CPU
Router#show protocols
Router#show mem
Router#show ip route
Router#show startup-config
Router#show running-config
Break Boot Procedure

- Attach a terminal to the console port of the router.
- Power off/on router
- Press **Break-key** on the terminal keyboard after power-up to put the router into ROMMON.
## Break Key Map

<table>
<thead>
<tr>
<th>Software</th>
<th>Operating System</th>
<th>Try This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypertermina l</td>
<td>Windows</td>
<td>Ctrl-Break</td>
</tr>
<tr>
<td>Netterm</td>
<td>Windows</td>
<td>Edit/ Send short break</td>
</tr>
<tr>
<td>SecureCRT</td>
<td>Windows</td>
<td>Ctrl-Break</td>
</tr>
<tr>
<td>Telix</td>
<td>DOS</td>
<td>Ctrl-End</td>
</tr>
</tbody>
</table>

**Configuration Register Values**

```plaintext
rommon> confreg 0x2142
rommon> reset
```

<table>
<thead>
<tr>
<th>Configuration Register Boot Field Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2142</td>
<td>Boot from flush <em>without</em> loading configuration</td>
</tr>
<tr>
<td>0x2102</td>
<td>Boot from flush <em>with</em> loading configuration</td>
</tr>
</tbody>
</table>
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: y

At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: n
Loading the Configuration

Roter>en
Router#`config memory`
or
Router#`copy startup-config running-config`

- Load and execute config from NVRAM
In RAM

wg_ro# show running-config

Building configuration...

Current configuration:
!
version 12.0
!
   -- More --

Configuration is restored!
Enable Password

`wg_ro(config) #enable secret cisco`

- Old password cannot get back.
- Set a new enable password.
Enabling the Interfaces

Router# show ip interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0</td>
<td>10.200.40.37</td>
<td>YES</td>
<td>TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/0</td>
<td>unassigned</td>
<td>YES</td>
<td>TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Ethernet0/1</td>
<td>unassigned</td>
<td>YES</td>
<td>TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Serial0/1</td>
<td>unassigned</td>
<td>YES</td>
<td>TFTP</td>
<td>administratively down</td>
<td>down</td>
</tr>
</tbody>
</table>

wg_ro #configure term
wg_ro (config)#interface serial 0/0
wg_ro (config-if)#no shutdown
%LINK-3-UPDOWN: Interface Serial0, changed state to up
%LINEPROTO-5-UPDOWN: Line Protocol on Interface Serial0, changed state to up

Enables an interface that are administratively shutdown
**Configuration Register Values**

wg_ro(config)# config-reg 0x2102
wg_ro(config)# end

<table>
<thead>
<tr>
<th>Configuration Register Boot Field Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x2142</td>
<td>Boot from flush <em>without</em> loading configuration</td>
</tr>
<tr>
<td>0x2102</td>
<td>Boot from flush <em>with</em> loading configuration</td>
</tr>
</tbody>
</table>
wg_ro# `show version`
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 08-Feb-99 18:18 by phanguye
Image text-base: 0x03050C84, data-base: 0x00001000

ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c), ..... 

wg_ro_a uptime is 20 minutes
System restarted by reload
System image file is "flash:c2500-js-l_120-3.bin"
(output omitted)
-- More --

Configuration register is 0x2142 (will be 0x2102 at next reload)
Saving Configurations

wg_ro#telnet ……
wg_ro#write memory
Building configuration…
wg_ro#reload

• Telnet to itself to double confirm.
• Copy the current configuration to NVRAM
Summary

- More password recovery procedure:
  http://www.cisco.com/warp/customer/474/
IOS Backup & Upgrade
Cisco IOS File Systems and Devices

- RAM
- NVRAM (config)
- Flash (IOS)
- ROM
- TFTP server
Managing IOS Images

Backup:
- Router
- Network server
  - c2500-js-l_120-3.bin

Upgrade:
- Router
- Network server
  - FLASH
Preparing for a Network Transmission

- Check connectivity between router and tftp server
- Check flash/space available on the router/server
- Check file naming convention
- Create file on server if required
- TFTP utility

http://support.3com.com/software/utilities_for_windows_32_bit.htm
TFTP server

File directory
wg_ro# `sh flash`

System flash directory:
File  Length   Name/status
1  10084696  c2500-js-l_120-3.bin
[10084760 bytes used, 6692456 available, 16777216 total]
16384K bytes of processor board System flash (Read ONLY)

• Check the current IOS in flash memory.

• Verify Flash memory has room for the IOS image
show version Command

Wg_ro>show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.1(20), RELEASE SOFTWARE (fc2)
...
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
...
System image file is "flash:c2600-is-mz.121-20.bin"

cisco 2611 (MPC860) processor (revision 0x202) with 26624K/6144K bytes of memory.
...
2 Serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

• Make sure flash and DRAM sizes meet the minimal requirement for IOS
Upgrading the Image from the Net

wg_ro#copy tftp flash
Address or name of remote host []? 10.1.1.1
Source filename []? c2500-js-l_120-3.bin
Destination filename [c2500-js-l_120-3.bin]?
Accessing tftp://10.1.1.1/c2500-js-l_120-3.bin...

Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeee (output omitted) ...erased
Erase of flash: complete
Loading c2500-js-l_120-3.bin from 10.1.1.1 (via Ethernet0): !!!!!!!!!!!!!!!!!!
(output omitted)
[OK - 10084696/20168704 bytes]
Verifying checksum... OK (0x9AA0)
10084696 bytes copied in 309.108 secs (32636 bytes/sec)
wg_ro#reload
Define a Booting IOS file

`wg_ro#sh flash:

System flash directory:
File  Length   Name/status
 1  7724588   c2600-i-mz.121-20.bin
 2  9923856   c2600-is-mz.121-20.bin`

`wg_ro#config t
wg_ro(config)#boot system flash c2600-is-mz.121-20.bin`

• New IOS will take effect after reload.
Creating a Software Image Backup

Back up current files prior to updating Flash

wg_ro# `copy flash tftp`
Source filename []? c2500-js-l_120-3.bin
Address or name of remote host []? 10.1.1.1
Destination filename [c2500-js-l_120-3.bin]?

10084696 bytes copied in 709.228 secs (14223 bytes/sec)
wg_ro#
wg_ro_a#copy running-config tftp
Address or name of remote host []? 10.1.1.1
Destination filename [running-config]? wgroa.cfg
.!!
1684 bytes copied in 13.300 secs (129 bytes/sec)

wg_ro_a#copy tftp running-config
Address or name of remote host []? 10.1.1.1
Source filename []? wgroa.cfg
Destination filename [running-config]?
Accessing tftp://10.1.1.1/wgroa.cfg...
Loading wgroa.cfg from 10.1.1.1 (via Ethernet0): !
[OK - 1684/3072 bytes]

1684 bytes copied in 17.692 secs (99 bytes/sec)
Thanks you !