Guide to Network Defense and Countermeasures Third Edition

Chapter 4
Routing Fundamentals

Objectives

- Describe the routing process
- Configure a Cisco router
- Describe the router security controls
- Create access control lists

Examining the Routing Process

- **Routing**: the process of transporting packets of information across a network from source to destination
  - Takes place at the Network layer of the OSI model
- **Routers**: determine the best path for packets to take and then send them toward their destination
  - Use metrics such as hop count, bandwidth, or link state
  - Administrators can also configure predetermined paths for packets based on protocols and other variables

The Address Resolution Protocol Processes

- Address Resolution Protocol (ARP) – resolves IP addresses to MAC addresses
  - A packet cannot reach its destination until the MAC address is determined
- ARP tables – list the MAC and IP address resolutions of other devices
  - Dynamic entries have a limited time to live (2 minutes in Windows workstations)
  - If computer does not find an entry for destination IP address, it sends an ARP broadcast to subnet in an attempt to discover it

Accessing a Router

- The back of a Cisco router contains several interfaces (network connections), a power switch, and other devices specific to the router model
  - Auxiliary (AUX) port and console (CON) port are important for configuration, troubleshooting, and maintenance
  - Must use a rollover cable to connect from the CON port to a laptop or other workstation
    - Rollover cable: pins 1-8 on one end of the cable connect to pins 8-1 on the other end of the cable

Routing Tables, Part 1

- Routing tables: lists of networks that contain information for reaching the networks
  - Also contain indicators (metrics) such as hop count and link-state that help determine the most efficient route
- Routing tables have three types of entries:
  - Static routes: entered manually by an administrator
  - Dynamic routes: populated automatically by routing protocols and routing algorithms
  - Default routes: manually configured routes that direct all packets not specifically configured in routing table

Routing Tables, Part 2

- Cisco routers use three main processes to build and maintain routing tables:
  - Routing protocol
  - Forwarding process – requests information from the routing table for making forwarding decisions
  - Routing tables from other routers that are sent in response to request for information or are sent automatically as default updates

Static Routing, Part 1

- Routing protocols use network bandwidth, consume resources, and are a security concern
- If the network can be run efficiently using only static routes, dynamic routes should be eliminated
  - Stub network: router with only one route
    - Generally found at the network's edge and are considered dead-end segments
    - Example of when to use static routing

Stub Network

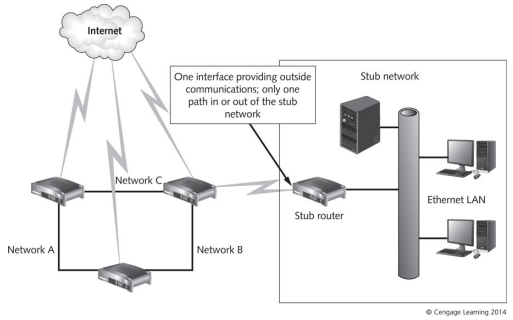


Figure 4-1 Stub network

Static Routing, Part 2

- Administrator might need to specify certain routes or adjust traffic flow to maximize efficiency, improve efficiency, improve security or performance, and conserve bandwidth
- Static routes are configured on Cisco routers using the **ip route** command:
  - ip route [*destination network*] [*destination network subnet mask*] [*IP address of the next hop interface*] [*administrative distance*]
- Disadvantage: time required to configure routes and the effort needed to maintain

Dynamic Routing, Part 1

- Routing protocols: enable routers to communicate with each other and map the network (routing tables)
  - Routing tables are updated at regular intervals or when a route changes
- Convergence: state in which all network routers have up-to-date information about the network topology

Dynamic Routing, Part 2

- Distance-Vector Routing Protocols
  - Uses mathematical calculations to compare routes based on measurement of distance, such as hops
- Link-State Routing Protocols
  - Requires each router to maintain at least a partial network map
  - Routers monitor link status and when the topology changes, updates are sent to neighboring routers
    - Use a notification called a link-state advertisement to broadcast changes

Routing Metrics

- Metrics: cost values that help routers assess the durability of a link
  - Examples include: hop count, load, bandwidth, delay, and reliability
  - "Cost" is a method of assigning preference ratings to a route
- Distance-vector protocols use only hop count
  - Assessment process is prone to errors
- Link-state protocols use multiple metrics, such as reliability and bandwidth

Choosing a Routing Protocol

- Most common routing protocols are RIP, EIGRP, OSPF, and IS-IS
- Factors when determining which protocol is best:
  - Administrative cost of management
  - Administrative cost of configuration
  - Bandwidth usage
  - Frequency of network failures
  - Network recovery time
  - Convergence time
  - Network topology

Route Summarization, Part 1

- Route summarization (supernetting): allows service providers to assign addresses in a classless fashion
  - More efficient use of available Internet addresses
  - A single entry in a routing table for 194.28.0.0/21 summarizes all network addresses below

Class C network	Binary representation (common network bits in bold)
194.28.0.x	11000010.00011100.00000000.x
194.28.1.x	11000010.00011100.00000001.x
194.28.2.x	11000010.00011100.00000010.x
194.28.3.x	11000010.00011100.00000011.x
194.28.4.x	11000010.00011100.00000100.x
194.28.5.x	11000010.00011100.00000101.x
194.28.6.x	11000010.00011100.00000110.x
194.28.7.x	11000010.00011100.00000111.x

Table 4-2 Determination of matching network bits in each Class C network

Route Summarization, Part 2

- Variable length subnet masking (VLSM)
  - Uses subnet masks of different lengths on the same network to assign network addresses based on need
  - Divide the network into subnets of varying sizes
  - Can be useful when setting the endpoint addresses for links between branch offices
    - A subnet in which only two addresses are needed

IPv6 Routing

- IPv6 is gradually replacing IPv4
  - Rip has upgraded to IPv6-compliant RIPng
  - OSPFv3, EIGRP for IPv6, and IS-IS for IPv6 are all IPv6 compliant
  - All US government agencies must deploy IPv6 on their public Web sites by September 30, 2012
    - Entire internal infrastructure must be upgraded by September 30, 2014

IPv6 Addressing in Branch Networks

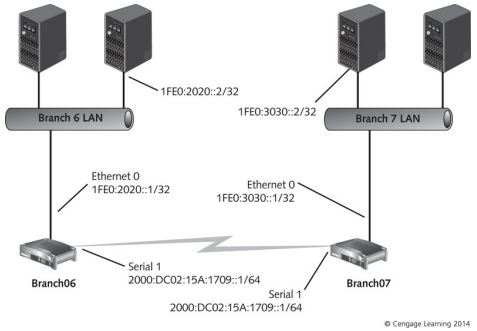


Figure 4-2 IPv6 addressing in branch networks

Router Security Fundamentals

- Routers contain detailed information about network topology
  - Are a target for malicious attacks
- Router security is crucial to network defense
- Routers work in conjunction with IDPS to block packets from a threat

Creating and Using Access Control Lists

- Router access control lists (ACLs)
  - Permit and deny statements that filter traffic based on:
    - Source and destination address
    - Source or destination port number
    - Protocol
  - Provide traffic-flow control and enhance network security
  - Can also be used to fine-tune performance and control access to sensitive network segments

Use and Rules

- Consider two factors when configuring ACLs:
  - ACLs end with an implicit “deny any” statement
    - Means any packet that does not match requirements for passage is blocked
  - ACLs are processed in sequential order
    - To conserve router processing resources, rules that match common network traffic should be placed higher on the list

ACLs: Common Problems and Solutions

Problem	Solution
Lack of planning results in simple logic mistakes	Plan carefully what needs to be filtered and what needs access.
Sequential processing results in filtering errors.	Use the IP Access List Entry Sequence Numbering feature in Cisco IOS versions 12.2 and above, which allows you to move and insert rules in an existing ACL.
Applying ACLs via Telnet can result in lost connectivity for the administrator applying the list.	Use the reload command to restore access as long as the running configuration was not copied to the startup configuration.

Table 4-3 ACLs: Common problems and solutions

Use and Rules, Part 1

- General rules for ACLs:
  - Routers apply lists sequentially
  - Packets are processed only until a match is made
    - Then they are allowed or denied
  - Lists always end with an implicit “deny any” statement
  - ACLs must be applied to an interface as inbound or outbound filters
  - The terms inbound and outbound refer to the perspective of the router
    - Packet entering the router is considered inbound
    - Packet exiting the router is considered outbound

Use and Rules, Part 2

- General rules for ACLs (cont’d):
  - ACLs are not active until they are applied to an interface
  - Only one ACL per protocol and per direction can be applied to an interface
  - ACLs take effect immediately
    - If you want the list to be permanent, you must copy the running configuration to the startup configuration
- Test ACLs thoroughly before applying
  - Should have a baseline so you know what “normal” traffic looks like

Standard ACLs, Part 1

- Standard ACLs have minimal configuration options
  - Filter only on source IP address information
  - Applied to inbound or outbound packets
  - Only one ACL direction can be applied to an interface at a time
- Standard IP ACLs
  - Use an inverse mask that tells the router which bits in the address to be filtered are significant
    - 0 bit means to check the corresponding bit value
    - 1 bit means to ignore the corresponding bit value

Standard ACLs, Part 2

- Standard ACLs have the following characteristics:
  - They can filter based on source address
  - They can filter by host, subnet, or network address using an inverse mask
  - They should be placed on the router interface as close to the destination as possible
  - They have a default inverse mask of 0.0.0.0

Standard ACLs, Part 3

- Standard ACLs use the following syntax:
  - access-list [*list#*] [*permit*|*deny*] [*source IP address*] [*source wildcard mask*]
    - *list#* - Standard ACLs are represented by a number from 1-99
    - *permit*|*deny* – specifies action to be taken
    - *source IP address* – indicates source to be identified for filtering
    - *source wildcard mask* – determines which bits of the source address mask must match for the packets to be identified for filtering

Extended ACLs, Part 1

- Extended ACLs offer many more filtering options
  - Provide control over source and destination addresses, ports, and protocols that you want to filter
  - Increased complexity means more chances to make a mistake
    - Take great care when creating and using extended ACLs

Extended ACLs, Part 2

- Extended IP ACLs use the following syntax:
  - access-list [*list#*] [*permit*|*deny*] [*protocol*] [*source IP address*] [*source wildcard mask*] [*operator*] [*port*] [*destination IP address*] [*destination wildcard mask*] [*operator*] [*port*] [*log*]
    - *list#* - Extended IP ACLs are represented by a number from 100-199
    - *protocol* – IP protocol to be filtered
    - *operator* – less than (lt), greater than (gt), or equal (eq)
    - *port* – source or destination port number of protocol
    - *log* – turns logging of ACL activity

Extended ACLs, Part 3

- Important points about extended IP ACLs:
  - Do not have a default inverse mask of 0.0.0.0
  - Should be applied to an interface as close to the traffic source as possible
  - The "established" parameter can be used to allow incoming traffic that responds to an internal request
  - Must be applied to an interface to be active
  - Must be at least one permit access control entry in every ACL

Named ACLs

- Starting with IOS version 11.2, Cisco has supported name ACLS
  - Referring to an ACL with a name instead of a number
    - Easier to identify
    - Support more advanced features such as filtering traffic based on IP options, TCP flags, and TTL (time to live), and non-initial fragments of packets
- Use the following syntax
  - ip access-list [*type*] [*name*]
    - *type* – specify extended or standard

Examining Cisco Router Logging

- Logging – provides information for troubleshooting, monitoring traffic patterns, and discovering and tracking down possible security incidents
- Cisco routers use the following types of logging:
  - AAA logging – Authentication, authorization, and accounting (AAA) logging collects information about remote user connections, commands issued, logons, logoffs, HTTP access, and similar events
  - SNMP trap logging – Simple Network Management Protocol (SNMP) sends notification of system status changes to SNMP management stations
  - System logging – reports system logs to different locations

Logging Levels

- Events are tagged with an urgency level from 0-7
  - 0 indicates the highest urgency and 7 the lowest
  - Routers can be set to only record a certain level or higher
  - Can view logging messages by using the show logging command at the privileged exec mode prompt
    - Buffered logging is limited by the amount of memory in the router
    - Large log files may cause performance problems

Cisco Router Logging Severity Levels

Level	Urgency
0	Emergency—system is unusable
1	Alert—requires immediate action
2	Critical—indicates a critical condition
3	Error—indicates an error condition
4	Warning—specifies a warning condition
5	Notification—indicates a normal but possibly significant condition
6	Informational—displays an informational message
7	Debugging—displays a debugging message

Table 4-4 Cisco router logging severity levels

Options for the Logging Command

```
Branch03(config)#logging ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  buginf               Enable buginf logging for debugging
  cns-events           Set CNS Event logging level
  console              Set console logging parameters
  count                Count every log message and timestamp last occurrence
  esm                  Set ESM filter restrictions
  exception            Limit size of exception flush output
  facility             Facility parameter for syslog messages
  filter               Specify logging filter
  history              Configure syslog history table
  host                 Set syslog server IP address and parameters
  monitor              Set terminal line (monitor) logging parameters
  on                   Enable logging to all enabled destinations
  origin-id            Add origin ID to syslog messages
  queue-limit          Set logger message queue size
  rate-limit           Set messages per second limit
  reload               Set reload logging level
  server-arp           Enable sending ARP requests for syslog servers when
                       first configured
  source-interface     Specify interface for source address in logging
                       transactions
  trap                 Set syslog server logging level
  userinfo             Enable logging of user info on privileged mode enabling
```

Source: Cisco ASA firewall

Figure 4-3 Options for the logging command

Buffered Logging

- Buffered logging – stores log out files in the router's memory (RAM)

```
Branch03(config)#logging buffered ?
  <0-7>              Logging severity level
  <4096-2147483647>  Logging buffer size
  alerts             Immediate action needed           (severity=1)
  critical           Critical conditions               (severity=2)
  debugging          Debugging messages                (severity=7)
  emergencies        System is unusable                (severity=0)
  errors             Error conditions                  (severity=3)
  filtered           Enable filtered logging
  informational      Informational messages            (severity=6)
  notifications      Normal but significant conditions (severity=5)
  warnings           Warning conditions                (severity=4)
  xml                Enable logging in XML to XML logging buffer
  <cr>
```

Source: Cisco ASA firewall

Figure 4-4 Options for the logging buffered command

Antispoofing Logging, Part 1

- Antispoofing – a way to prevent spoofing and ensure that no packets arrive at your security perimeter with suspicious addresses
  - Accomplished by using ACLs
- Adding the log keyword to the end of an extended ACL, tells router to send information about matching packets to the router's log
  - deny any 172.16.0.0 0.0.255.255 any log
- Use the logging command to specify the IP address of a computer that will host the log file
  - logging 180.50.0.12

Antispoofing Logging, Part 2

- Once an ACL is created and applied to an interface:
  - Use the **show ip access-lists** command from privileged exec mode to review ACLs

```
Branch03#show ip access-lists
Extended IP access list ResearchLAN
    10 deny icmp any any redirect
    20 deny ip 180.50.0.0 0.0.255.255 any log
    30 deny igmp 224.0.0.0 31.255.255.255 any
    40 permit ip any any log
```

Source: Cisco ASA firewall

Figure 4-5 Output of the show ip access-lists command

Cisco Authentication and Authorization, Part 1

- Authentication – process of determining that users are who they say they are
- Authorization – specifies what users are allowed to do after they have access the system
- Two types of authentication on a Cisco router:
  - AAA (Authentication, authorization, and accounting)
  - Non-AAA
    - Any method that does not use Cisco AAA Security Services is considered non-AAA

Cisco Authentication and Authorization, Part 2

- Cisco's AAA uses one or more of three security protocols:
  - TACACS+: proprietary Cisco protocol that uses TCP for transport and encrypts all data
  - RADIUS: open standard that uses UDP ports and encrypts only passwords
  - Kerberos

Router Passwords, Part 1

- Cisco routers have five types of passwords:
  - Enable
  - Enable secret
  - AUX
  - VTY
  - Console
- Password requirements:
  - Must be 1 to 25 characters long
  - Leading spaces are ignored but other spaces in it are considered part of the password
  - First character cannot be a number

Router Passwords, Part 2

- Cisco passwords have three levels of encryption:
  - Type 0 – provides no encryption
  - Type 7 – encrypted but can be decrypted by router-password-cracking tools
  - Type 5 – strongest level, which is a Message Digest 5 (MD5)
    - MD5 is a one-way hash and cannot be decrypted

Router Passwords, Part 3

- Enable Password
  - Main purpose is to prevent casual or accidental access to privileged exec mode (uses weak encryption)
- Enable Secret Password
  - Uses type 5 encryption and overrides an enable password
- AUX, VTY, and Console Passwords
  - Set passwords on each port

Router Passwords, Part 4

- Encrypting passwords
  - Enable secret password is the only encrypted password type by default
  - Use the **service password-encryption** command in global configuration mode to encrypt all passwords on router

```
line con 0
 password 7 03345A4F42182E5E4A
 login
line aux 0
 password 7 08114D0A4D0E0A0516
line vty 0 4
 password 7 08114D0A4D0E0A0516
```

Source: Cisco ASA firewall

Figure 4-7 Encrypted passwords in the show running-configuration command output

Banners

- Banners: messages displayed to greet users who log on to a router
  - Provide information or warnings during logon
  - Most common banners display legal disclaimers
    - Should clearly state the company's policy on unauthorized access
  - Should never include wording that could give attackers information about system or network
    - Such as names, IP addresses and software versions

Remote Access with Secure Shell

- Secure Shell (SSH): a remote shell program that is more secure than Telnet or FTP
  - An alternative to SSH is OpenSSH
    - OpenSSH includes several tools: secure copy, secure FTP, and SSH daemon
- Support for SSH-2 was added beginning with Cisco IOS 12.1.(19)E

Enabling SSH on the Router, Part 1

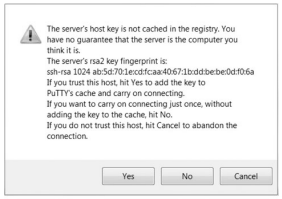
- Before enabling SSH:
  - Router must be configured with a hostname, domain name, and one interface must have a static IP address
- Enable SSH server by using the command:
  - **crypto key generate rsa**
- Next, choose a key size (range from 360 to 2048)
  - Use a key larger than default size of 512 to ensure strong encryption
  - Key size of 1024 should work for most applications

Enabling SSH on the Router, Part 2

- After SSH is enabled, configure the authentication timeout interval (time in seconds the server waits for a client to respond with a password)
  - Maximum and default setting is 120 seconds
  - **ip ssh time-out 60** (sets timeout interval at 60)
- To configure the number of logon attempts allowed before router drops the connection:
  - **ip ssh authentication-retries 3** (maximum is 5)
- To create a user account:
  - username [*username*] [priv] [*priv level*] [pass] [*password*]

Enabling SSH on the Router, Part 3

- To connect to a router using SSH
  - Connecting systems need to have SSH client software installed
  - PuTTY is a popular choice



Source: PuTTY

Figure 4-8 PuTTY security alert

Packet Capture of an SSH Connection

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.201	192.168.1.200	TCP	66	49855 > ssh [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.004869	192.168.1.200	192.168.1.201	TCP	60	ssh > 49855 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
3	0.005158	192.168.1.201	192.168.1.200	TCP	54	49855 > ssh [ACK] Seq=1 Ack=1 Win=64240 Len=0
4	0.010868	192.168.1.200	192.168.1.201	SSHv2	74	Server Protocol: SSH-1.99-Cisco-1.25
5	0.011150	192.168.1.201	192.168.1.200	SSHv2	82	Client Protocol: SSH-2.0-PuTTY_Release_0.62\r
6	0.011229	192.168.1.201	192.168.1.200	TCP	566	[TCP segment of a reassembled PDU]
7	0.011263	192.168.1.201	192.168.1.200	SSHv2	182	Client: Key Exchange Init
8	0.015512	192.168.1.200	192.168.1.201	SSHv2	334	Server: Key Exchange Init
9	0.021802	192.168.1.201	192.168.1.200	SSHv2	198	Client: Diffie-Hellman Key Exchange Init
10	0.330018	192.168.1.201	192.168.1.200	SSHv2	198	[TCP Retransmission] Client: Diffie-Hellman Key Exchange Init
11	0.377552	192.168.1.200	192.168.1.201	TCP	60	ssh > 49855 [ACK] Seq=301 Ack=813 Win=3316 Len=0
12	0.763002	192.168.1.200	192.168.1.201	SSHv2	502	Server: Diffie-Hellman Key Exchange Reply
13	0.765272	192.168.1.200	192.168.1.201	SSHv2	70	Server: New Keys
14	0.765345	192.168.1.201	192.168.1.200	TCP	54	49855 > ssh [ACK] Seq=813 Ack=765 Win=63476 Len=0
15	0.787297	192.168.1.201	192.168.1.200	SSHv2	70	Encrypted request packet len=16
16	0.787538	192.168.1.201	192.168.1.200	SSHv2	142	Encrypted request packet len=88
17	0.792022	192.168.1.200	192.168.1.201	SSHv2	106	Encrypted response packet len=52
18	1.000042	192.168.1.201	192.168.1.200	TCP	54	49855 > ssh [ACK] Seq=917 Ack=817 Win=63424 Len=0
19	3.224022	192.168.1.201	192.168.1.200	SSHv2	158	Encrypted request packet len=104
20	3.227413	192.168.1.200	192.168.1.201	SSHv2	106	Encrypted response packet len=52
21	3.423134	192.168.1.201	192.168.1.200	TCP	54	49855 > ssh [ACK] Seq=1021 Ack=869 Win=63372 Len=0

Source: Wireshark

Figure 4-9 Packet capture of an SSH connection

Verifying SSH

- Use the show **ip ssh** command to verify SSH
- If SSH is not enabled, you see this output:
  SSH Disabled – version 1.99
  Please create RSA keys to enable SSH
- Verify connections to the SSH server by using the **show ssh** command
- You should set a session timeout on VTY interfaces to reduce risk of administrators leaving computer unattended while logged on:
  - **exec-timeout 10 0** (sets timeout to 10 minutes)

Hardening a Router

- Hardening: securing a router
  - Disable any unnecessary service or protocol
  - Check your router security policy
    - Specifies what traffic is allowed and whether traffic is incoming or outgoing
  - Check router's vendor Web site for new patches and security notices
  - Enable logging
  - Configuration management: process of formally proposing, approving, and implementing router configuration changes

Summary, Part 1

- Routers direct transportation of packets across networks
- Routers process OSI Network layer headers to determine source and destination addresses
- Ways to access a router for administrative purposes: AUX port, CON port, and VTY ports
- Routing tables contain information about the network topology and are stored in router's memory
- Static routing saves network bandwidth and gives administrators control over small networks

Summary, Part 2

- Routing protocols: RIP, OSPF, EIGRP, and IS-IS
- Routes can be summarized through the process of supernetting
- Access control lists are created to allow routers to perform packet filtering
- Logging packet filtering and configuration activity is an important part of router and network security
- Authentication, authorization, and accounting must be managed carefully to ensure router security

Summary, Part 3

- Password security is not particularly strong on Cisco routers
- Older router access methods such as Telnet are not secure because data is transferred in clear text
  - SSH uses encrypted access methods
- Routers should be hardened in the same way as servers and other computers