Cisco Certified Network Associate
CCNA 640-802
Access the WAN

Assist.Prof.lt-arun Pitimon
ltarun.p@cpe.rmutt.ac.th

DAY 4

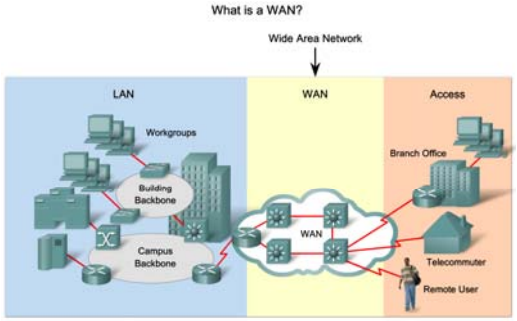
Agenda

- Services in a Converged WAN
- Point-to-Point Protocol
- Frame Relay
- Enterprise Network Security
- Access Control Lists
- Providing Teleworker Services
- Implementing IP Addressing Services

SERVICES IN A CONVERGED WAN

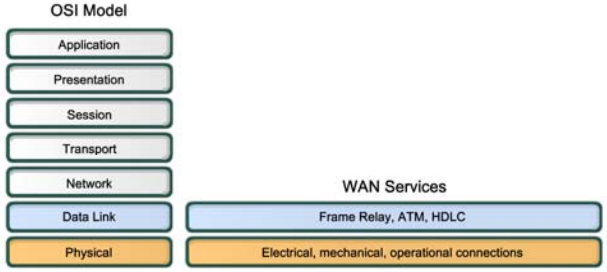
Describe How ECNM Provides Integrated Services over an Enterprise Network

- Explain the purpose and function of WANs



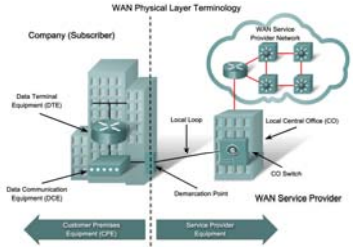
Describe the Key WAN Technology Concepts

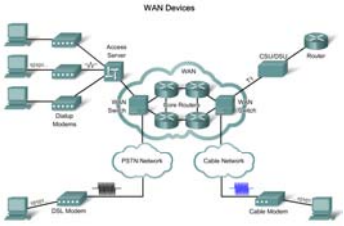
- Describe WAN functions in terms of the OSI Reference Model



Describe the Key WAN Technology Concepts

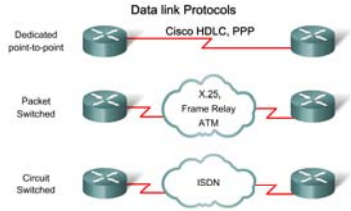
- Describe the key WAN physical layer concepts for network and Internet communications





Describe the Key WAN Technology Concepts

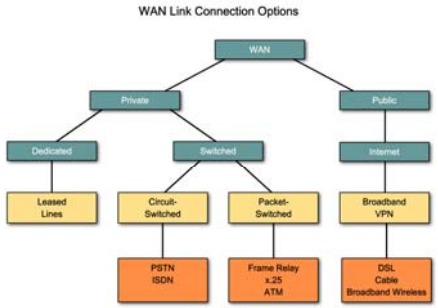
- Describe the key WAN data link layer protocols used in today's Enterprise WAN networks



Protocol	Usage
Link Access Procedure Balanced (LAPB)	X.25
Link Access Procedure D Channel (LAPD)	ISDN D channel
Link Access Procedure Frame (LAPF)	Frame Relay
High-Level Data Link Control (HDLC)	Cisco default
Point-to-Point Protocol (PPP)	Serial WAN switched connections

Select the Appropriate WAN Technology to meet ECNM Requirements

- List the various options for connecting subscribers to the WAN



Select the Appropriate WAN Technology to meet ECNM Requirements

- List factors to consider when selecting a WAN connection

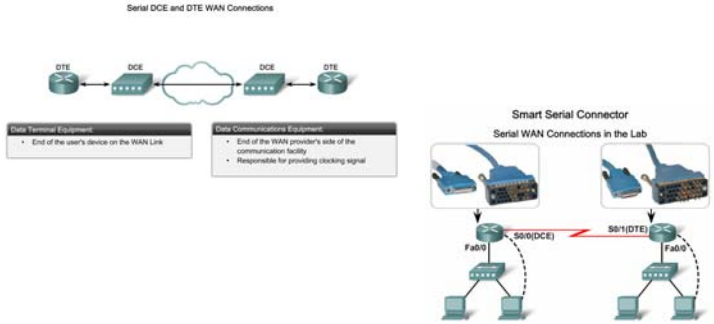
Choosing a WAN Link Connection

Option	Description	Advantages	Disadvantages	Sample protocols used
Leased line	Point-to-Point connection between two computers or Local Area Networks (LANs).	Most secure	Expensive	PPP, HDLC, SDLC, HNAS
Circuit switching	A dedicated circuit path is created between endpoints. Best example is dialup connections.	Less expensive	Call setup	PPP, ISDN
Packet switching	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier interwork. Variable length packets are transmitted over permanent virtual circuits (PVCs) or switched virtual circuits.(SVCs)		Shared media across link	X.25, Frame Relay

POINT-TO-POINT PROTOCOL (PPP)

Describe the Fundamental Concepts of Point-to-Point Serial Communication

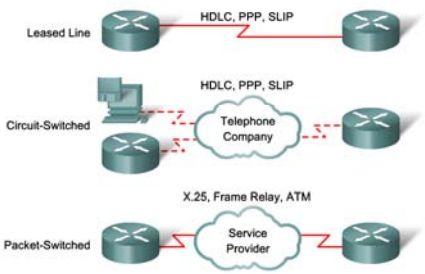
- Explain the terms DTE and DCE with relative to the location of devices in a network



Describe the Fundamental Concepts of Point-to-Point Serial Communication

- Describe how high-level data link control (HDLC) uses one of three frame types to encapsulate data

WAN Encapsulation Protocols



Describe the Fundamental Concepts of Point-to-Point Serial Communication

- Explain when and how to configure HDLC encapsulation on a router

Configuring HLDC Encapsulation

```
Router(config-if)#encapsulation hdlc
```

- Enable HDLC encapsulation
- HDLC is the default encapsulation on synchronous serial interfaces

Describe the Fundamental Concepts of Point-to-Point Serial Communication

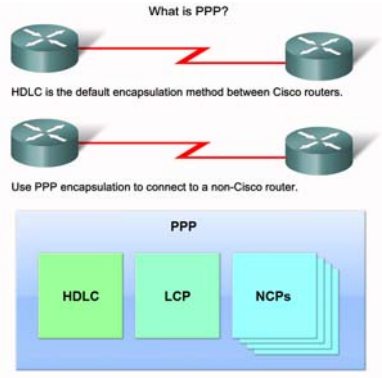
- Describe the procedure to follow when troubleshooting a serial connection

Troubleshooting a Serial Interface

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is up	This is the proper status line condition.	No action is required.
Serial x is down, line protocol is down (DTE mode)	The router is not sensing a CD signal, which means the CD is not active. A WAN carrier service provider problem has occurred, which means the line is down or is not connected to CSU/DSU. Cabling is faulty or incorrect. Hardware failure has occurred (CSU/DSU).	1. Check the LEDs on the CSU/DSU to see whether the CD is active, or insert a breakout box on the line to check for the CD signal. 2. Verify that the proper cable and interface are being used by looking at the hardware installation documentation. 3. Insert a breakout box and check all control leads. 4. Contact the leased-line or other carrier service to see whether there is a problem. 5. Swap faulty parts. 6. If faulty router hardware is suspected, change the serial line to another port. If the connection comes up, the previously connected interface has a problem.
Serial x is up, line protocol is down (DTE mode)	A local or remote router is misconfigured. Keepalives are not being sent by the remote router. A leased-line or other carrier service problem has occurred, which means a noisy line or misconfigured or failed switch. A timing problem has occurred on	1. Put the modem, CSU, or DSU in local loopback mode and use the **show interfaces serial** command to determine whether the line protocol comes up. If the line protocol comes up, a WAN carrier service provider problem or a failed remote router is the likely problem. 2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU. 3. Verify all cabling. Make certain that the cable is attached to the correct interface, the correct CSU/DSU, and the correct

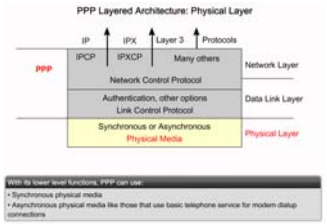
Describe Point-to-Point Concepts

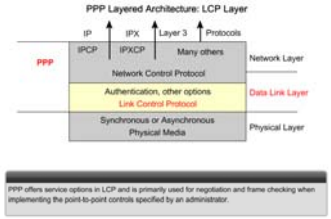
- Describe PPP in terms of its use in WAN links



Describe Point-to-Point Concepts

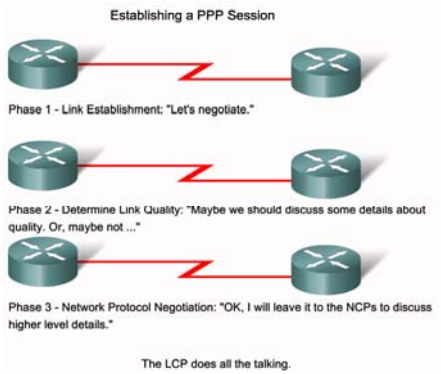
- Describe the general function of each layer of PPP architecture





Describe Point-to-Point Concepts

- Define the three phases of PPP session establishment

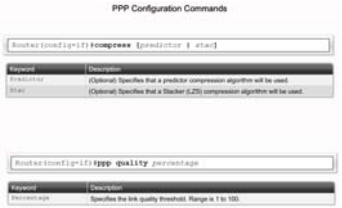


Describe Point-to-Point Concepts

- Explain the role of the LCP in PPP

Configure PPP on a Serial Interface

- Explain the purpose of the commands used to configure and verify PPP connections



Configure PPP on a Serial Interface

- Explain the output of the show interfaces serial command

Practice: Verifying and Debugging Commands

Command	Description
`show interfaces`	Displays statistics for all interfaces configured on the router or access server
`show interfaces serial`	Displays information about a serial interface
`debug ppp`	Debugs PPP
`undebug all`	Turns off all debugging displays

Configure PPP on a Serial Interface

- Explain the output of the debug ppp command

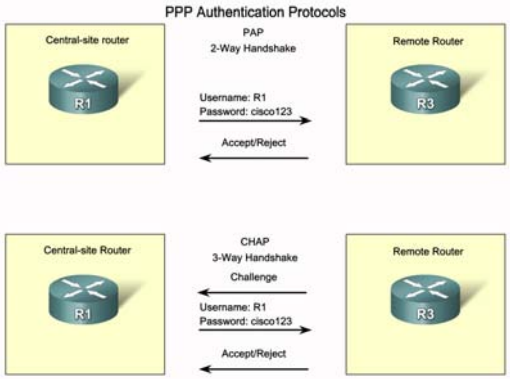
`debug ppp` Command Parameters

```
debug ppp {packet | negotiation | error | authentication | compression |
          cbcp}
```

Parameter	Usage
`packet`	Displays PPP packets being sent and received. (This command displays low-level packet dumps.)
`negotiation`	Displays PPP packets transmitted during PPP startup, where PPP options are negotiated.
`error`	Displays protocol errors and error statistics associated with PPP connection negotiation and operation.
`authentication`	Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.
`compression`	Displays information specific to the exchange of PPP connections using MPPC. This command is useful for obtaining incorrect packet sequence number information where MPPC compression is enabled.
`cbcp`	Displays protocol errors and statistics associated with PPP connection negotiations using MSCB.

Configuring PPP with Authentication

- Differentiate between PAP and CHAP



Configuring PPP with Authentication

- Explain how to configure a PPP connection with authentication

The `ppp authentication` Command

```
ppp authentication {chap | chap pap | pap chap | pap} [if-needed]
[list-name | default] [callin]
```

The ppp authentication Command	
`chap`	Enables CHAP on a serial interface.
`pap`	Enables PAP on a serial interface.
`chap pap`	Enables both CHAP and PAP, and performs CHAP authentication before PAP.
`pap chap`	Enables both CHAP and PAP, and performs PAP authentication before CHAP.
`if-needed` (Optional)	Used with TACACS and XTACACS. Do not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
`list-name` (Optional)	Used with AAA/TACACS+. Specifies the name of a list of TACACS+ methods of authentic list name is specified, the system uses the default. Lists are created with the **`aaa authentication ppp`** command.
`default` (Optional)	Used with AAA/TACACS+. Created with the **`aaa authentication ppp`** command.
`callin`	Specifies authentication on incoming (received) calls only.

Configuring PPP with Authentication

- Explain the output of the debug ppp authentication command

Troubleshooting a PPP Configuration with Authentication

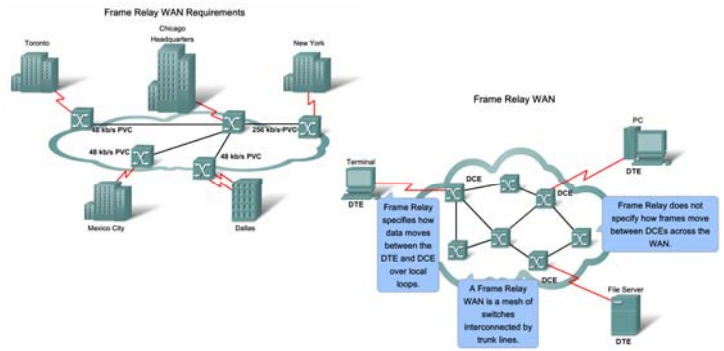
```
R2# debug ppp authentication

Serial0: Unable to authenticate. No name received from peer
Serial0: Unable to validate CHAP response. USERNAME pioneer not found.
Serial0: Unable to validate CHAP response. No password defined for USERNAME pioneer
Serial0: Failed CHAP authentication with remote.
Remote message is Unknown name
Serial0: remote passed CHAP authentication.
Serial0: Passed CHAP authentication with remote.
Serial0: CHAP input code = 4 id = 3 len = 48
```


FRAME RELAY

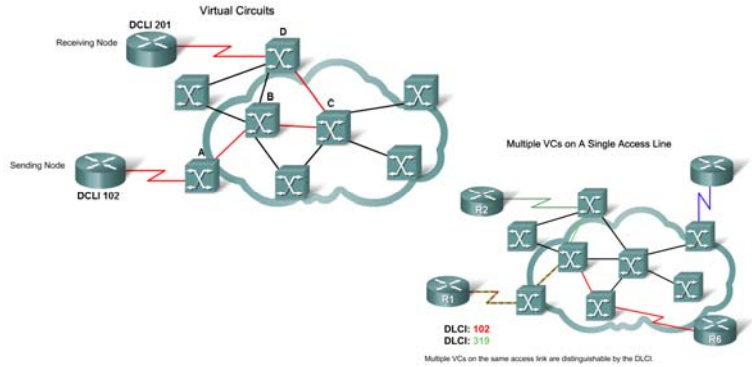
Describe the Fundamental Concepts of Frame Relay Technology

- Describe how Frame Relay is used to provide WAN services to the Enterprise



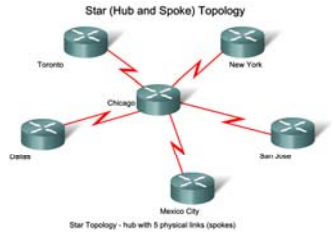
Describe the Fundamental Concepts of Frame Relay Technology

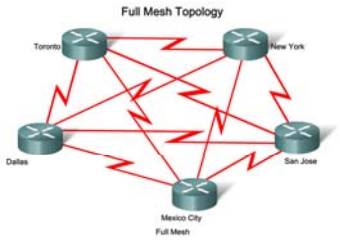
- Describe how Frame Relay uses virtual circuits to carry packets from one DTE to another



Describe the Fundamental Concepts of Frame Relay Technology

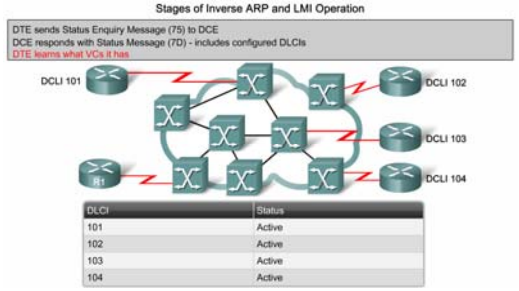
- Describe the types of topologies that are used for implementing Frame Relay in different environments





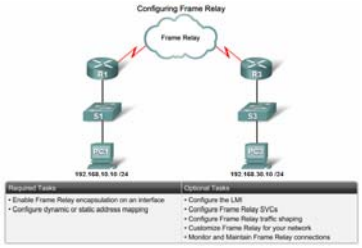
Describe the Fundamental Concepts of Frame Relay Technology

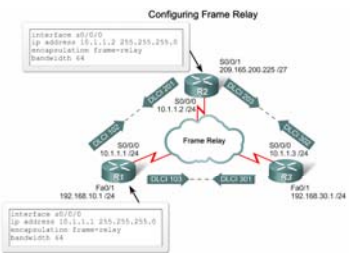
- Describe how a router attached to a Frame Relay network uses LMI status messages and inverse ARP queries to map VCs to layer 3 network IP Addresses



Configure a Basic Frame Relay PVC

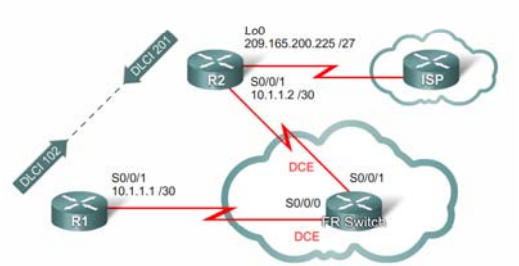
- Configure a basic Frame Relay PVC on a router serial interface





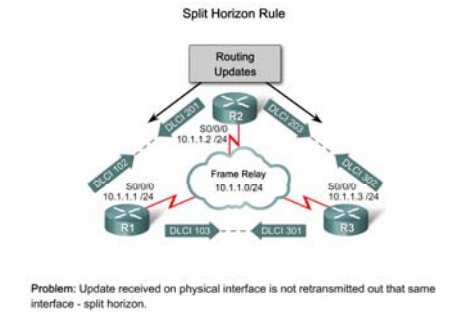
Configure a Basic Frame Relay PVC

- Configure a static Frame Relay map



Describe Advanced Concepts of Frame Relay Technology

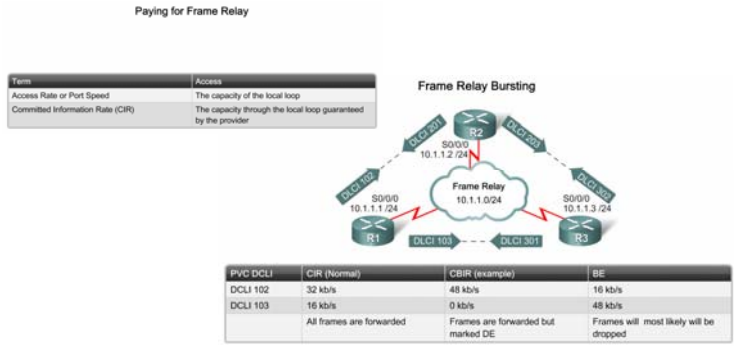
- Explain the reachability issues associated with the Frame Relay NBMA topology



Problem: Update received on physical interface is not retransmitted out that same interface - split horizon.

Describe Advanced Concepts of Frame Relay Technology

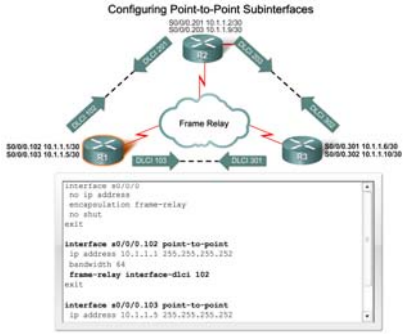
- Describe how to implement bandwidth control in the Frame Relay technology



PVC DCLI	CIR (Normal)	CBIR (example)	BE
DCLI 102	32 kb/s	48 kb/s	16 kb/s
DCLI 103	16 kb/s	0 kb/s	48 kb/s
	All frames are forwarded	Frames are forwarded but marked DE	Frames will most likely will be dropped

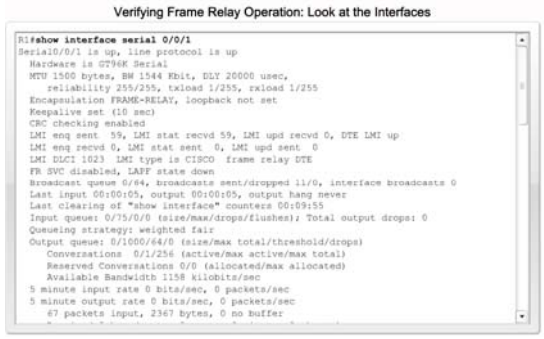
Configure an Advanced Frame Relay PVC

- Explain the steps to configure point-to-point subinterfaces on a physical interface



Configure an Advanced Frame Relay PVC

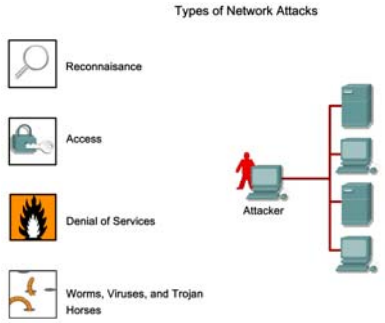
- Describe the commands used for verifying Frame Relay operation



ENTERPRISE NETWORK SECURITY

Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

- Describe the most common types of network attacks and how they impact enterprises

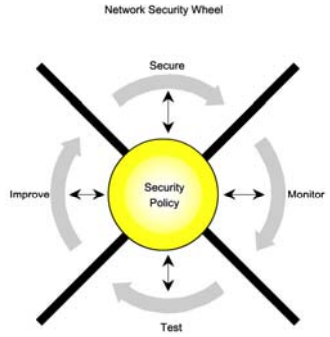


Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

- Describe the common mitigation techniques that enterprises use to protect themselves against threats

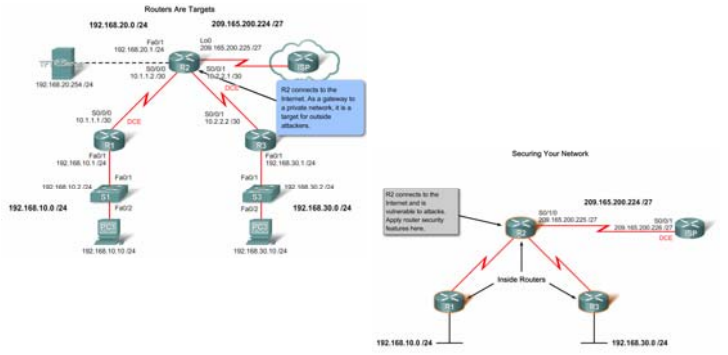
Describe the General Methods used to Mitigate Security Threats to Enterprise Networks

- Explain the concept of the Network Security Wheel



Configure Basic Router Security

- Explain why the security of routers and their configuration settings is vital to network operation



Configure Basic Router Security

- Describe the recommended approach to applying Cisco IOS security features on network routers

Applying Cisco IOS Security Features to Routers

Steps to safeguard a router:
Step 1. Manage router security
Step 2. Secure remote administrative access to routers
Step 3. Logging router activity
Step 4. Secure vulnerable router services and interfaces
Step 5. Secure routing protocols
Step 6. Control and filter network traffic

Configure Basic Router Security

- Describe the basic security measures needed to secure Cisco routers

Passphrase Examples

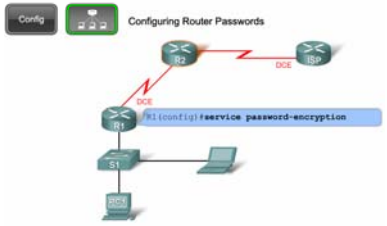
"All people seem to need data processing" would translate to Apstndp
"My favourite spy is James Bond 007" would translate to MfsiJB007
"It was the best of time, it was the worst of times" would translate to Iwtbotiwtwot
"Fly me to the moon. And let me play among the stars" would translate to Fmttm.Almpats

Step 2: Encrypt Passwords

```
R1(config)#service password-encryption
R1(config)#end

R1#show running-config
!
Line con 0
Password 7 0956F57A109A
-----Output Omitted----
```

Configuring Router Passwords



Administrator encrypts all passwords in the configuration file.

Explain How to Disable Unused Cisco Router Network Services and Interfaces

- Describe the router services and interfaces that are vulnerable to network attack

Vulnerable Router Services

Feature	Description	Default	Recommendation
Cisco Discovery Protocol (CDP)	Proprietary Layer 2 protocol between Cisco devices.	Enabled	CDP is almost never needed; disable it.
TCP small servers	Standard TCP network services: echo, chargen, and so on.	>=11.3: disabled 11.2: enabled	This is a legacy feature; disable it explicitly.
UDP small servers	Standard UDP network services: echo, discard, and so on.	>=11.3: disabled 11.2: enabled	This is a legacy feature; disable it explicitly.
Finger	UNIX user lookup service, allows remote listing of users.	Enabled	Unauthorized persons do not need to know this; disable it.
HTTP server	Some Cisco IOS devices offer web-based configuration.	Varies by device	If not in use, explicitly disable; otherwise, restrict access.
BOOTP server	Service to allow other routers to boot from this one.	Enabled	This is rarely needed and may open a security hole; disable it.
Configuration auto-loading	Router will attempt to load its configuration via TFTP.	Disabled	This is rarely used; disable it if it is not in use.
IP source routing	IP feature that allows packets to specify their own routes.	Enabled	This rarely-used feature can be helpful in attacks; disable it.
Proxy ARP	Router will act as a proxy for Layer 2 address resolution.	Enabled	Disable this service unless the router is serving as a LAN bridge.
IP directed broadcast	Packets can identify a target LAN for broadcasts.	>=11.3: enabled	Directed broadcast can be used for attacks; disable it.
Classless routing	Router will forward packets with	Enabled	Certain attacks can benefit from

Explain How to Use Cisco SDM

- Provide an overview of Cisco SDM

What Is Cisco SDM?

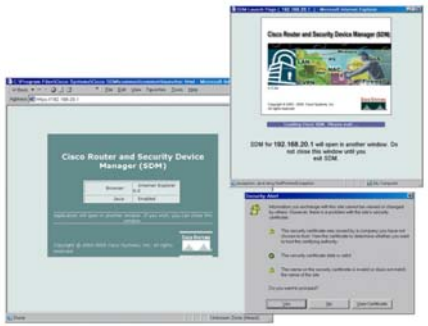
Cisco SDM Features

- Embedded web-based management tool
- Intelligent wizards
- Tools for more advanced users
  - ACL
  - VPN crypto map editor
  - Cisco IOS CLI preview

Explain How to Use Cisco SDM

- Explain the steps you follow to start SDM

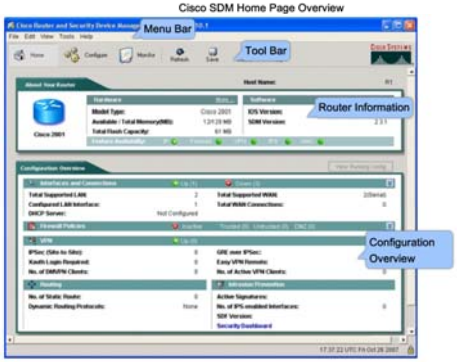
Starting Cisco SDM



Explain How to Use Cisco SDM

- Describe the Cisco SDM Interface

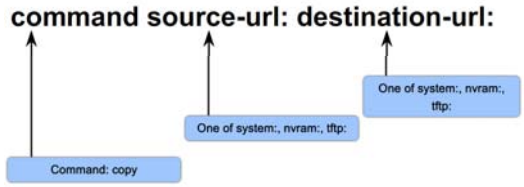
Cisco SDM Home Page Overview



Manage Cisco IOS Devices

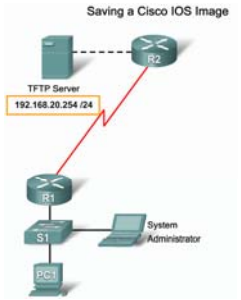
- Describe how to backup and upgrade a Cisco IOS image

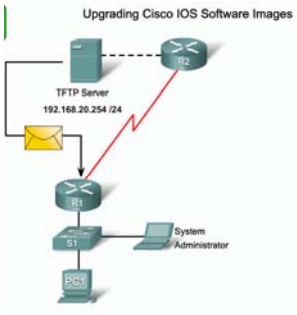
Commands for Managing Configuration Files



Manage Cisco IOS Devices

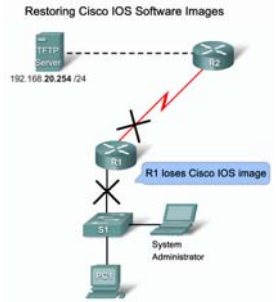
- Explain how to back up and upgrade Cisco IOS software images using a network server

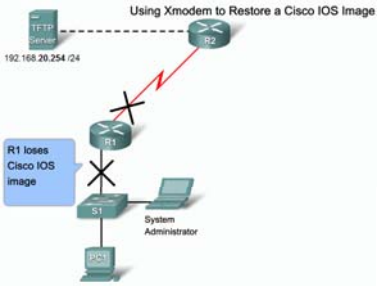




Manage Cisco IOS Devices

- Explain how to recover a Cisco IOS software image

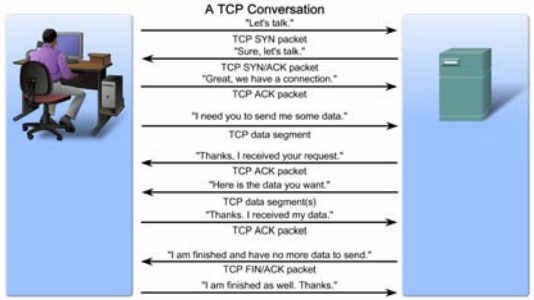




ACCESS CONTROL LISTS

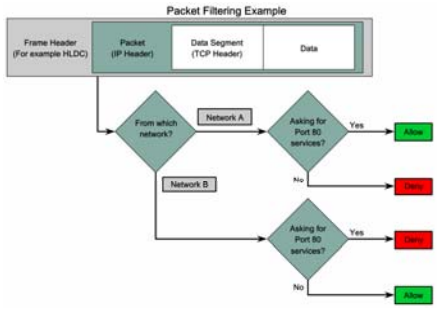
Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Describe the steps that occur in a complete TCP conversation



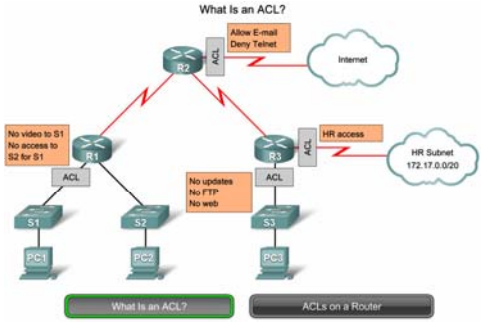
Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Explain how a packet filter allows or blocks traffic



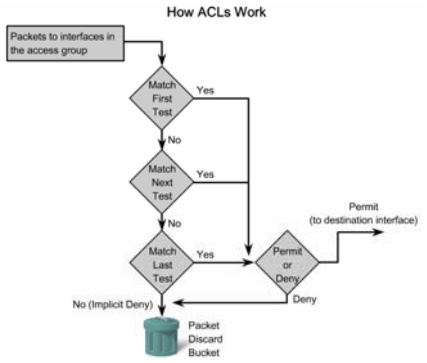
Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Describe how ACLs control access to networks



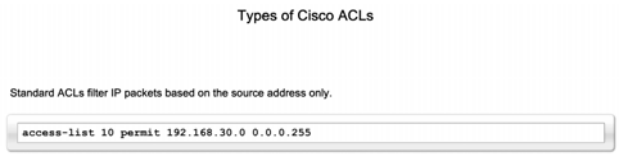
Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Use a flow chart to show how ACLs operate



Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Describe the types and formats of ACLs



Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

- Explain how Cisco ACLs can be identified using standardized numbering or names

Numbering and Naming ACLs

Numbered ACL:

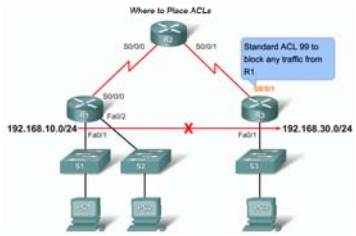
You assign a number based on which protocol you want filtered:
- (1 to 99) and (1300 to 1999): Standard IP ACL
- (100 to 199) and (2000 to 2699): Extended IP ACL

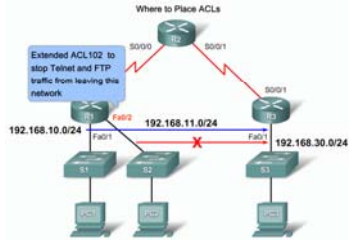
Named ACL:

You assign a name by providing the name of the ACL:
- Names can contain alphanumeric characters.
- It is suggested that the name be written in CAPITAL LETTERS.
- Names cannot contain spaces or punctuation and must begin with a letter.
- You can add or delete entries within the ACL.

Explain How ACLs are Used to Secure a Medium-Size Enterprise Branch Office Network

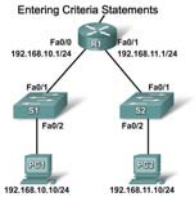
- Describe where ACLs should be placed in a network





Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain why the order in which criteria statements are entered into an ACL is important



ACL 101

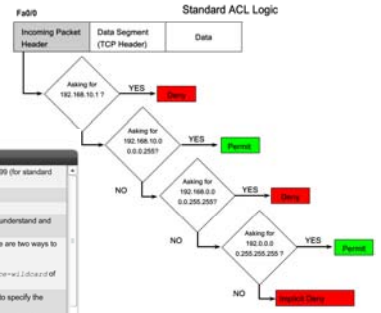
```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

ACL 102

```
access-list 102 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 102 deny ip any any
```


Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain how to configure a standard ACL



Standard ACL `access-list` Command Syntax

Parameter	Description
access-list-number	Number of an ACL. This is a decimal number from 1 to 99, or 1300 to 1999 (for standard ACL).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Add a remark about entries in an IP access list to make the list easier to understand and scan.
source	Number of the network or host from which the packet is being sent. There are two ways to specify the source: • Use a 32-bit quantity in four-part, dotted- decimal format. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.55.
source-wildcard	(Optional) Wildcard bits to be applied to the source. There are two ways to specify the source-wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore. • Use the keyword **any** as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.55.
log	(Optional) Causes an informational logging message about the packet that matches the

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to use wildcard masks with ACLs

Wildcard Mask Example

	Decimal Address	Binary Address
IP address to be processed	192.168.10.0	11000000.10101000.00001010.00000000
Wildcard mask	0.0.255.255	00000000.00000000.11111111.11111111
Resulting IP address	192.168.0.0	11000000.10101000.00000000.00000000

Wildcard Mask Calculation - 1

255.255.255.255
- 255.255.255.000
000.000.000.255

Wildcard Mask Calculation - 2

255.255.255.255
- 255.255.255.240
000.000.000.015

The `any` and `host` Keywords

Example 1:

```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

Example 2:

```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

This is the format of the host and any optional keywords in an ACL statement.

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to apply a standard ACL to an interface

Procedure for Configuring Standard ACLs

Step 1 Use the `access-list` global configuration command to create an entry in a standard IPv4 ACL.

```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
```

Enter the global `no access-list` command to remove the entire ACL. The example statement matches any address that starts with 192.168.10.x. Use the `remark` option to add a description to your ACL.

Step 2 Use the interface configuration command to select an interface to which to apply the ACL

```
R1(config)# interface FastEthernet 0/0
```

Step 3 Use the `ip access-group` interface configuration command to activate the existing ACL on an interface.

```
R1(config-if)# ip access-group 1 out
```

To remove an IP ACL from an interface, enter the `no ip access-group` command on the interface. This example activates the standard IPv4 ACL 1 on the interface as an outbound filter.

Standard ACL to Permit My Network Only


```
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface S0/0/0
R1(config-if)# ip access-group 1 out
```


Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain the process for editing numbered ACLs

Editing Numbered ACLs

Step 1	`R1#show running-config | include access-list`
	`access-list 20 permit 192.168.10.100`
	`access-list 20 deny 192.168.10.0 0.0.0.255`

Step 2	`access-list 20 permit 192.168.10.11` `access-list 20 deny 192.168.10.0 0.0.0.255`

Step 3	`R1#conf t`
	`Enter configuration commands, one per line. End with CTRL/Z.`
	`R1(config)#no access-list 20`
	`R1(config)#access-list 20 permit 192.168.10.100`
	`R1(config)#access-list 20 deny 192.168.10.0 0.0.0.255`

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain how to create a named ACL

Named ACL Example

```
Router(config)# ip access-list [standard | extended] name
```

- Alphanumeric name string must be unique and cannot begin with a number

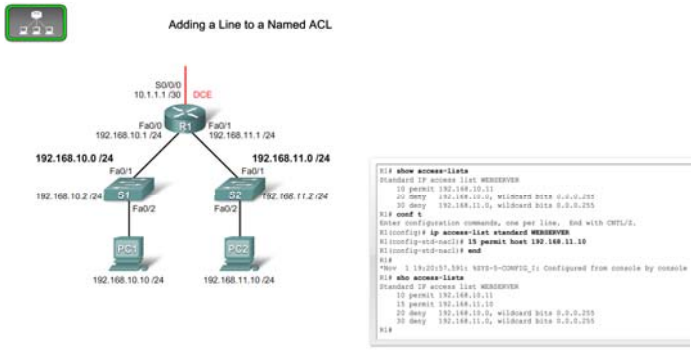
```
Router(config-std-nacl)# [permit | deny | remark] {source [source-wildcard]} [log]
```

```
Router(config-if)#ip access-group name [in | out]
```

- Activates the named IP ACL on an interface

Configure Standard ACLs in a Medium-Size Enterprise Branch Office Network

- Explain the process for editing named ACLs



Configure Extended ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to configure extended ACLs

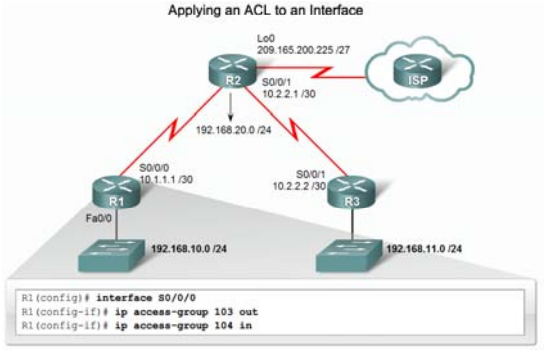
Configuring Extended ACLs

```
access-list access-list-number {deny | permit | remark} protocol source [source-wildcard]
[operator operand] [port port-number or name] destination [destination-wildcard] [operator
operand] [port port-number or name] [established]
```

Parameter	Description
access-list-number	Identifies the access list using a number in the range 100 to 199 (for an extended IP ACL) and 2000 to 2699 (expanded IP ACLs).
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.
remark	Indicates whether this entry allows or blocks the specified address. Could also be used to enter a remark.
protocol	Name or number of an Internet protocol. Common keywords include icmp, ip, tcp, or udp. To match any Internet protocol (including ICMP, TCP, and UDP) use the ip keyword.
source	Number of the network or host from which the packet is being sent.
source-wildcard	Wildcard bits to be applied to source.
destination	Number of the network or host to which the packet is being sent.
destination-wildcard	Wildcard bits to be applied to the destination.

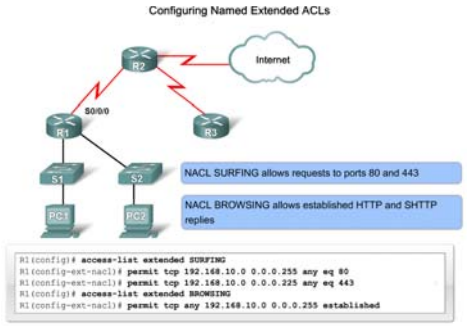
Configure Extended ACLs in a Medium-Size Enterprise Branch Office Network

- Describe how to apply an extended ACL to an interface



Configure Extended ACLs in a Medium-Size Enterprise Branch Office Network

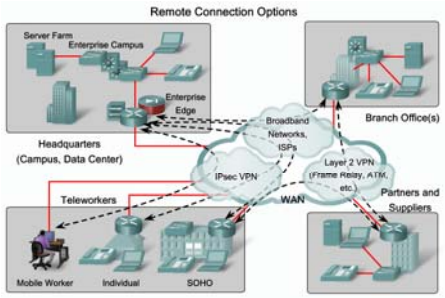
- Describe how to create named extended ACLs



PROVIDING TELEWORKER SERVICES

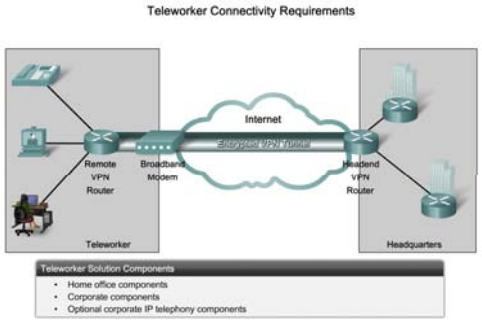
Describe the Enterprise Requirements for Providing Teleworker Services

- List remote connection technologies and describe scenarios in which each would be implemented.



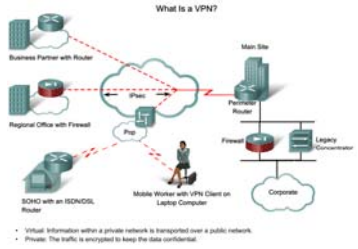
Describe the Enterprise Requirements for Providing Teleworker Services

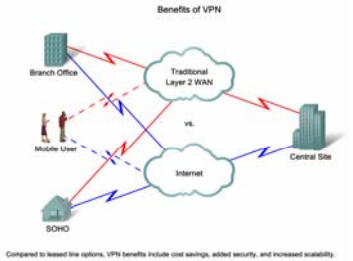
- Describe the key differences between private and public network infrastructures



Describe How VPN Technology Provides Secure Teleworker Services in an Enterprise Setting

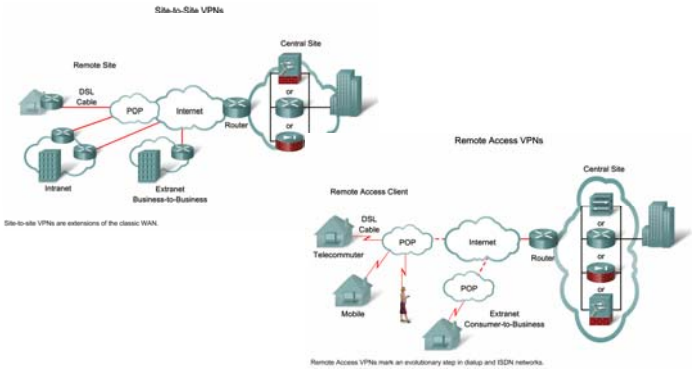
- Explain the importance and benefits of VPN technology





Describe How VPN Technology Provides Secure Teleworker Services in an Enterprise Setting

- Compare site-to-site VPNs to remote-access VPNs



Describe How VPN Technology Provides Secure Teleworker Services in an Enterprise Setting

- Describe the characteristics of secure VPNs

Characteristics of Secure VPNs

Characteristic	Purpose
Data Confidentiality	Protects data from eavesdroppers (spoofing).
Data Integrity	Guarantees that no tampering or alterations occur.
Authentication	Ensures that only authorized senders and devices enter the network.

Describe How VPN Technology Provides Secure Teleworker Services in an Enterprise Setting

- Describe the concept of VPN tunneling

VPN Security

Tunneling Protocols

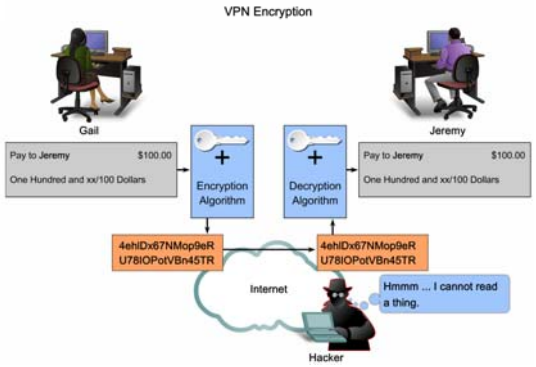
Carrier protocol:
- The protocol over which the information is traveling (Frame Relay, ATM, MPLS).

Encapsulating protocol:
- The protocol that is wrapped around the original data (GRE, IPSec, L2F, PPTP, L2TP).

Passenger protocol:
- The protocol over which the original data was being carried (IPX, AppleTalk, IPv4, IPv6).

Describe How VPN Technology Provides Secure Teleworker Services in an Enterprise Setting

- Describe the concept of VPN encryption



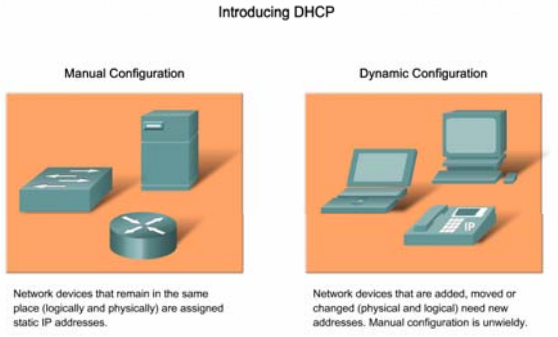
Describe How VPN Technology Provides Secure Teleworker Services in an Enterprise Setting

- Describe the concept of IPsec Protocols

IMPLEMENTING IP ADDRESSING SERVICES

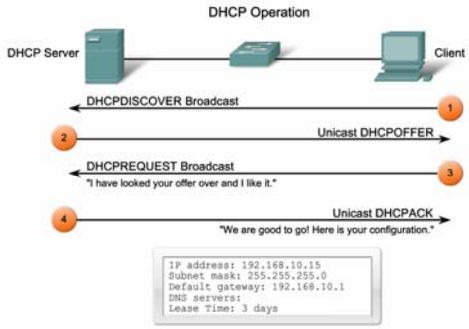
Configure DHCP in an Enterprise Branch Network

- Describe the function of DHCP in a network



Configure DHCP in an Enterprise Branch Network

- Describe how DHCP dynamically assigns an IP address to a client



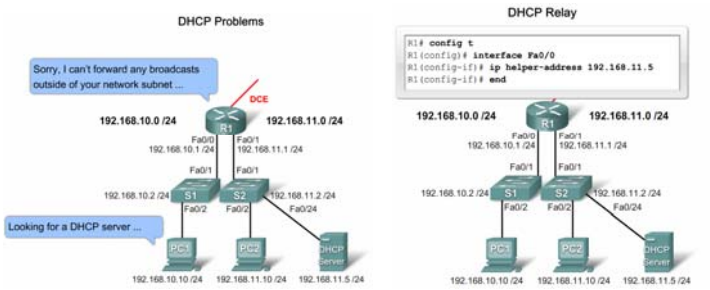
Configure DHCP in an Enterprise Branch Network

- Describe how to configure a DHCP server

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# domain-name span.com
R1(dhcp-config)# end
```


Configure DHCP in an Enterprise Branch Network

- Explain how DHCP Relay can be used to configure a router to relay DHCP messages when the server and the client are not on the same segment



Configure NAT on a Cisco Router

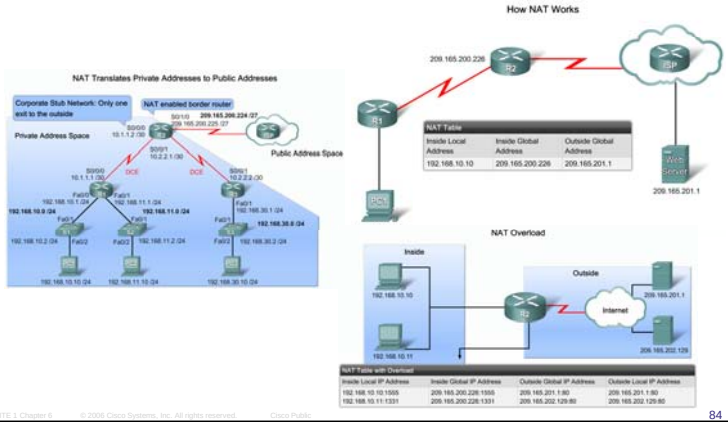
- Describe the operation and benefits of using private and public IP addressing

Private Internet addresses are defined in RFC 1918:

Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Configure NAT on a Cisco Router

- Explain the key features of NAT and NAT overload



Configure NAT on a Cisco Router

- Explain the advantages and disadvantages of NAT

NAT Benefits and Drawbacks

NAT Benefits
- Conserves the legally registered addressing scheme
- Increases the flexibility of connections to the public network
- Provides consistency for internal network addressing schemes.
- Provides network security

NAT Drawbacks
- Performance is degraded
- End-to-end functionality is degraded
- End-to-end IP traceability is lost
- Tunneling is more complicated
- Initiating TCP connections can be disrupted
- Architectures need to be rebuilt to accommodate changes

Configure NAT on a Cisco Router

- Describe how to configure static NAT to conserve IP address space in a network

Configuring Static NAT

Step	Action	Notes
1	Establish static translation between an inside local address and an inside global address. `Router(config)#ip nat inside source static local-ip global-ip`	Enter the global command `no ip nat inside source static` to remove the static source translation.
2	Specify the inside interface. `Router(config)#interface type number`	Enter the `interface` command. The CLI prompt will change from `(config)#` to `(config-if)#`.
3	Mark the interface as connected to the inside. `Router(config-if)#ip nat inside`	
4	Exit interface configuration mode. `Router(config-if)# exit`	
5	Specify the outside interface. `Router(config)#interface type number`	
6	Mark the interface as connected to the outside. `Router(config-if)#ip nat outside`	

Configure NAT on a Cisco Router

- Describe how to configure dynamic NAT to conserve IP address space in a network

Configuring Dynamic NAT

Step	Action	Notes
1	Define a pool of global addresses to be allocated as needed. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask|prefix-length prefix-length}`	Enter the global command `no ip nat pool name` to remove the pool of global addresses.
2	Define a standard access list permitting those addresses that are to be translated. `Router(config)#access-list access-list-number permit source [ source-wildcard]`	Enter the global command `no access-list access-list-number` to remove the access list.
3	Establish dynamic source translation, specifying the access list defined in the prior step. `Router(config)#ip nat inside source list access-list-number pool name`	Enter the global command `no ip nat inside source` to remove the dynamic source translation.
4	Specify the inside interface. `Router(config)#interface type number`	Enter the `interface` command. The CLI prompt will change from `(config)#` to `(config-if)#`.
5	Mark the interface as connected to the inside. `Router(config-if)#ip nat inside`	
6	Specify the outside interface. `Router(config)#interface type number`	
7	Mark the interface as connected to the outside. `Router(config-if)#ip nat outside`	
8	Exit interface configuration mode. `Router(config-if)# exit`	

Configure NAT on a Cisco Router

- Describe how to configure NAT Overload to conserve IP address space in a network

NAT Overload Configuration Example

Step	Action	Notes
1	Define a standard access list permitting those addresses that are to be translated. `Router(config)#access-list acl-number permit source [source-wildcard]`	Enter the global command `no access-list access-list-number` to remove the access list.
2	Establish dynamic source translation, specifying the access list defined in the prior step. `Router(config)#ip nat inside source list acl-number interface interface overload`	Enter the global command `no ip nat inside source` to remove the dynamic source translation. The overload keyword enables PAT.

3	Specify the inside interface.
	`Router(config)#interface type number`
	`Router(config-if)#ip nat inside`
		Enter the `interface` command. The CLI prompt will change from `(config)#` to `(config-if)#`.

4	Specify the outside interface.
	`Router(config-if)#interface type number`
	`Router(config-if)#ip nat outside`	

NAT Overload Configuration Using a Pool of Public Addresses

Step	Action	Notes
1	Define a standard access list permitting those addresses that are to be translated. `Router(config)#access-list acl-number permit source [source-wildcard]`	Enter the global command `no access-list access-list-number` to remove the access list.
2	Specify the global address, as a pool, to be used for overloading. `Router(config)#ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}`	
3	Establish overload translation. `Router (config)#ip nat inside source list acl-number pool name overload`	

4	Specify the inside interface.
	`Router(config)#interface type number`
	`Router(config-if)#ip nat inside`
		Enter the `interface` command. The CLI prompt will change from `(config)#` to `(config-if)#`.

5	Specify the outside interface.
	`Router(config-if)#interface type number`
	`Router(config-if)#ip nat outside`	

Configure New Generation RIP (RIPng) to use IPv6

- Describe the format of the IPv6 addresses and the appropriate methods for abbreviating them

IPv6 Address Representation

IPv6 Formats

Format:
- x:x:x:x:x:x:x:x, where x is a 16-bit hexadecimal field
  - Case-insensitive for hexadecimal A, B, C, D, E, and F
- Leading zeros in a field are optional
- Successive fields of zeros can be represented as :: only once per address

Examples:
- 2031:0000:130F:0000:0000:09C0:876A:130B
  - Can be represented as 2031:0:130f::9c0:876a:130b
  - Cannot be represented as 2031::130f::9c0:876a:130b
- FF01:0:0:0:0:0:0:1 FF01::1
- 0:0:0:0:0:0:0:1 ::1
- 0:0:0:0:0:0:0:0 ::

Configure New Generation RIP (RIPng) to use IPv6

- Explain the various methods of assigning IPv6 addresses to a device

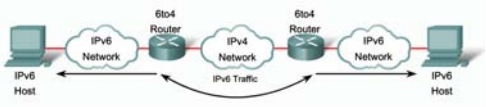
Assigning IPv6 Addresses

Static assignment	Dynamic assignment
• Manual interface ID assignment • EUI-64 interface ID assignment	• Stateless autoconfiguration • DHCPv6 (stateful)

Configure New Generation RIP (RIPng) to use IPv6

- Describe the transition strategies for implementing IPv6

IPv6 Transition Strategies



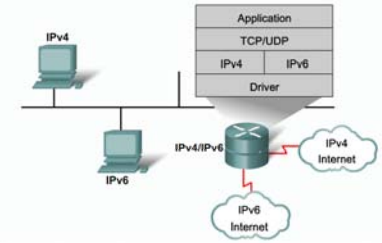
Different transition mechanisms are available:
- Dual stack
- Manual tunnel
- 6to4 tunnel
- ISATAP tunnel
- Teredo tunnel

Different compatibility mechanisms:
- Proxying and translation (NAT-PT)

Configure New Generation RIP (RIPng) to use IPv6

- Describe how Cisco IOS dual stack enables IPv6 to run concurrently with IPv4 in a network

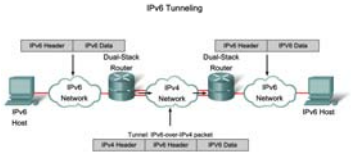
Cisco IOS Dual Stack



Dual stack is an integration method in which a node has implementation and connectivity to both an IPv4 and IPv6 network.

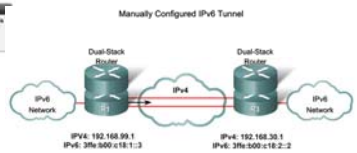
Configure New Generation RIP (RIPng) to use IPv6

- Describe the concept of IPv6 tunneling



Tunneling is an integration method in which an IPv6 packet is encapsulated within another protocol, such as IPv4. This method of encapsulation is IPv4:

- Includes a 20-byte IPv4 header with no options and an IPv6 header and payload
- Requires dual-stack routers



Configured tunnels require:

- Dual-stack endpoints
- IPv4 and IPv6 addresses configured at each end

Configure New Generation RIP (RIPng) to use IPv6

- Describe how IPv6 affects common routing protocols, and how these protocols are modified to support IPv6

RIPng Routing Protocol

Similar IPv4 features:

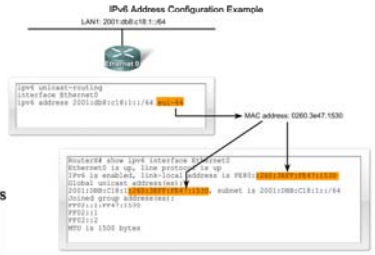
- Distance vector, radius of 15 hops, split horizon, and poison reverse
- Based on RIPv2

Updated features for IPv6:

- IPv6 prefix, next-hop IPv6 address
- Uses the multicast group FF02::9, the all-rip-routers multicast group, as the destination address for RIP updates
- Uses IPv6 for transport
- Named RIPng

Configure New Generation RIP (RIPng) to use IPv6

- Explain how to configure a router to use IPv6



Enabling IPv6 on Cisco Routers

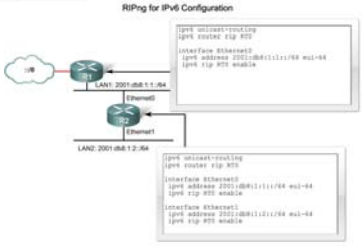
Command	Purpose
`RouterX(config)# ipv6 unicast-routing`	Enables IPv6 traffic forwarding
`RouterX(config-if)# ipv6 address ipv6prefix/prefix-length eui-64`	Configures the interface IPv6 addresses

Configure New Generation RIP (RIPng) to use IPv6

- Explain how to configure and verify RIPng for IPv6

Configuring RIPng for IPv6

Command	Purpose
`RouterX(config)#ipv6 router rip name`	Creates and enters RIP router configuration mode.
`RouterX(config-if)#ipv6 rip name enable`	Configures RIP on an interface.



Configure New Generation RIP (RIPng) to use IPv6

- Explain how to verify and troubleshoot IPv6

Commands

Command	Purpose
`show ipv6 interface`	Displays the status of interfaces configured for IPv6.
`show ipv6 interface brief`	Displays a summarized status of interfaces configured for IPv6.
`show ipv6 neighbors`	Displays IPv6 neighbor discovery cache information.
`show ipv6 protocols`	Displays the parameters and current state of the active IPv6 routing protocol processes.
`show ipv6 rip`	Displays information about the current
`show ipv6 route`	Displays the current IPv6 routing table.
`show ipv6 route summary`	Displays a summarized form of the current IPv6 routing table.
`show ipv6 routers`	Displays IPv6 router advertisement information received from other routers.
`show ipv6 static`	Displays only static IPv6 routes installed in the routing table.
`show ipv6 static 2001:db8:5555:0/16`	Displays only static route information about the specific address given.
`show ipv6 static interface serial 0/0`	Displays only static route information with the specified interface as the outgoing interface.
`show ipv6 static detail`	Displays a more detailed entry for IPv6 static routes.
`show ipv6 traffic`	Displays statistics about IPv6 traffic.