

CƠ BẢN VỀ MẠNG MÁY TÍNH

Mục tiêu:

- Giải thích được các thành phần mạng
- Biết cách phân loại mạng
- So sánh được mô hình OSI và TCP/IP

Nội dung

- Các thành phần mạng
- Phân loại mạng
 - LAN
 - WAN
 - Internet
 - Peer-to-Peer
 - Client – Server
 - Bus
 - Star
 - Ring
- Mô hình OSI và TCP/IP

Networking Today

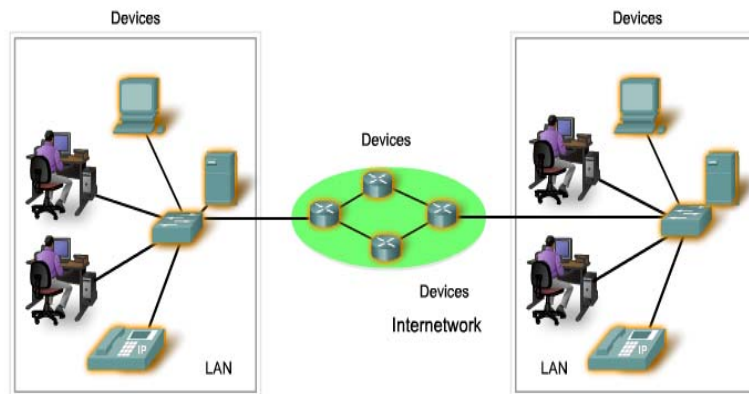


MMT là gì?

- MMT là một tập hợp các host được nối với nhau theo một cấu trúc mạng để chia sẻ và trao đổi thông tin với nhau thông qua môi trường truyền thông



Components of a Network



Network Media

Copper



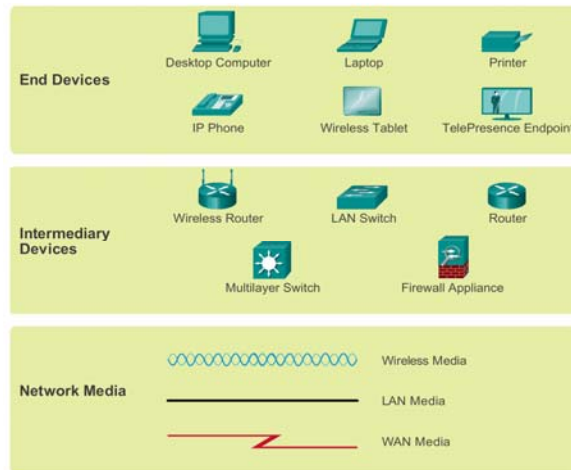
Fiber Optic



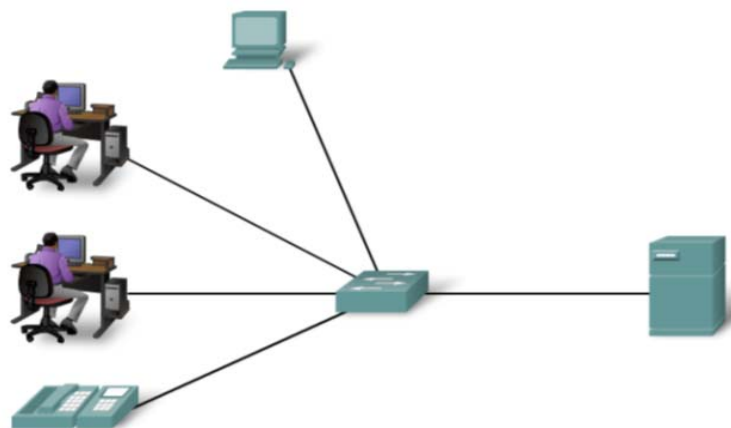
Wireless



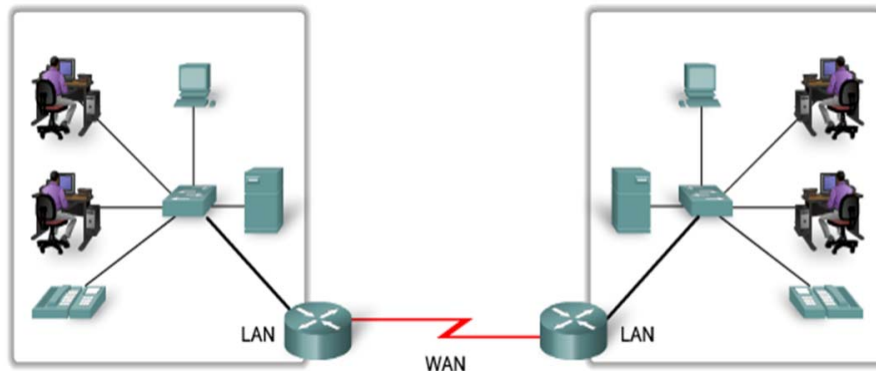
Network Symbols



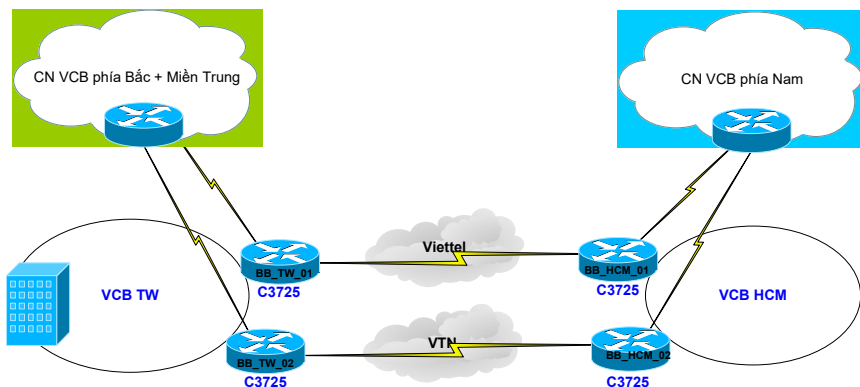
Local Area Networks (LAN)



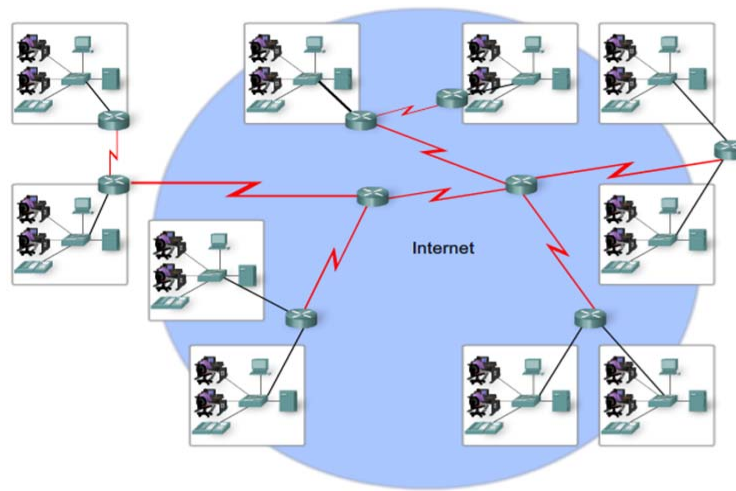
Wide Area Networks (WAN)



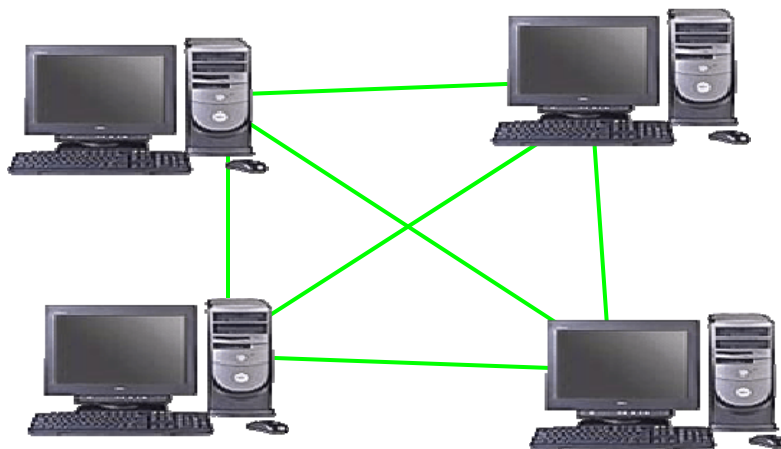
WAN



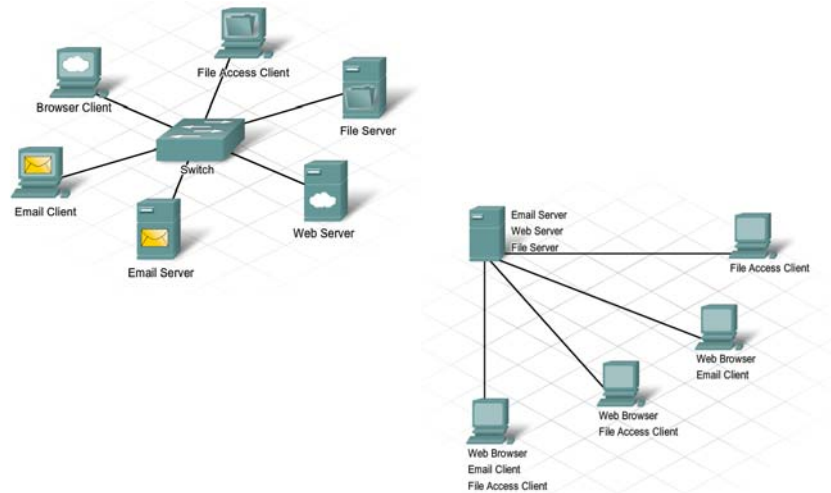
Internet



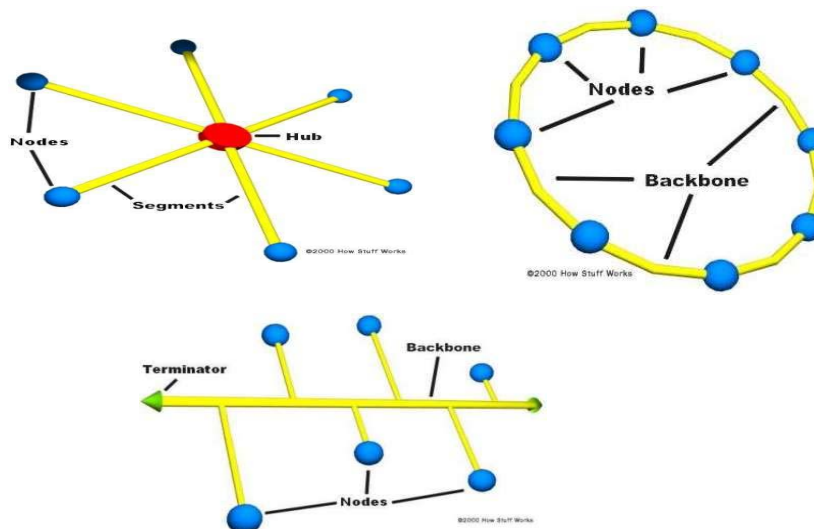
Peer-to-Peer



Client - Server

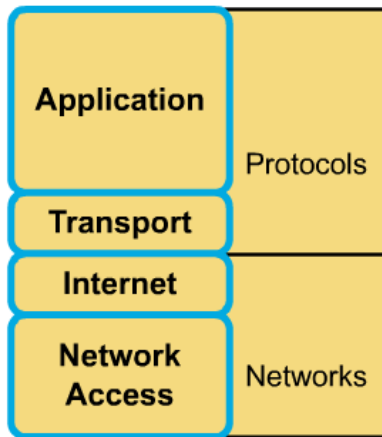


Network topology

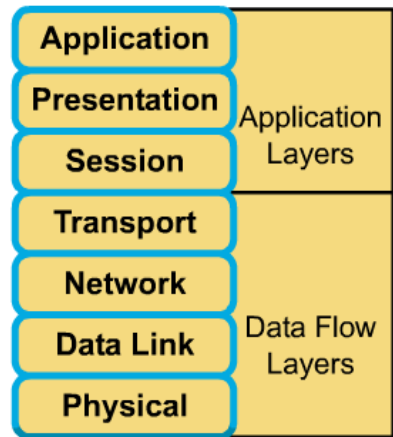


TCP/IP and OSI Model

TCP/IP Model



OSI Model



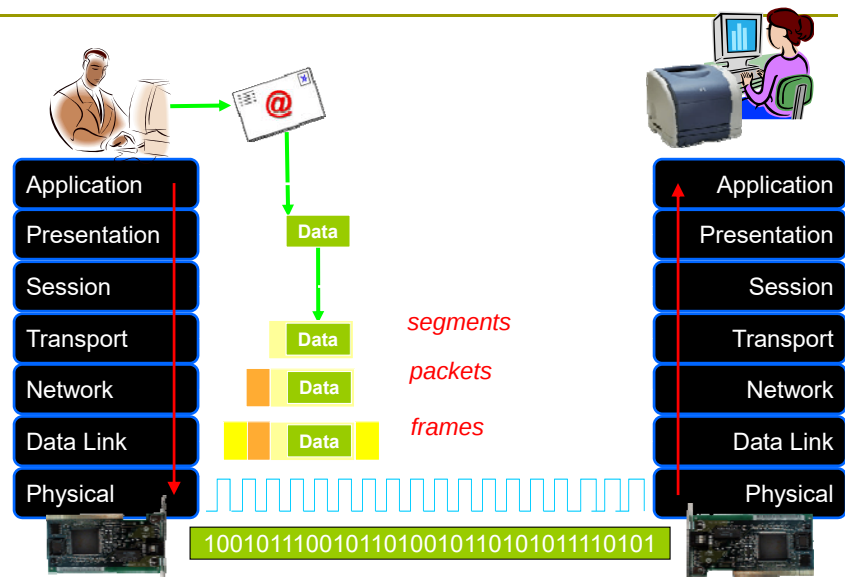
OSI Model



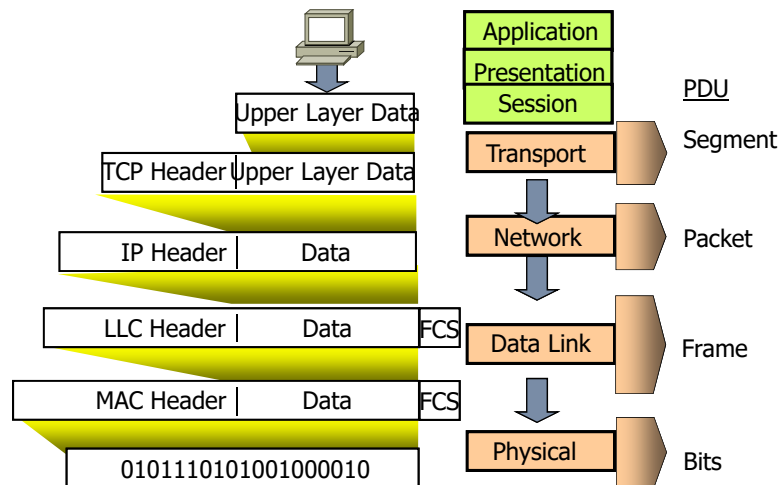
OSI Model

7	Application	Các ứng dụng mạng: email, web, chat,...
6	Presentation	Định dạng dữ liệu, encoding, compression, ...
5	Session	Thiết lập connection
4	Transport	Bảo đảm truyền nhận đúng dữ liệu
3	Network	Routers: Quản lý địa chỉ, chọn đường, truyền nhận các packet .
2	Data Link	Switches: Truyền nhận frame , kiểm tra và sửa lỗi
1	Physical	Cables, hubs: Kết nối vật lý, truyền các bit dữ liệu

OSI Model



Encapsulating



ĐỊA CHỈ IP

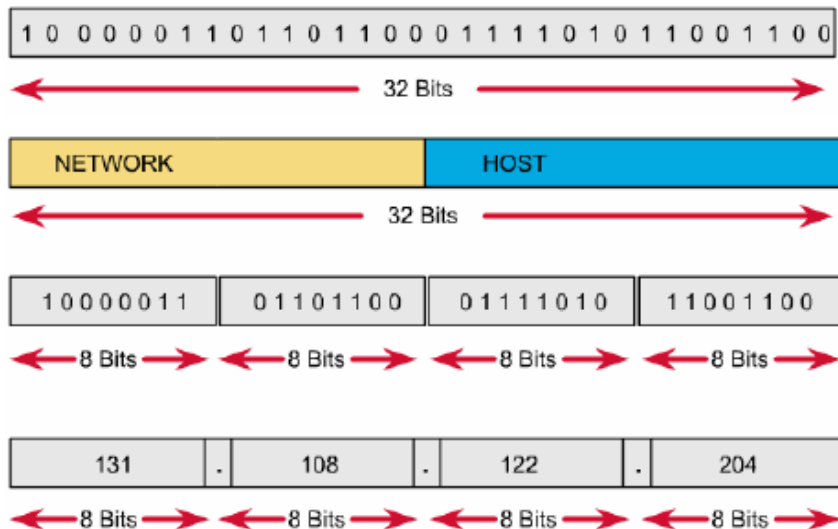
Mục tiêu:

- Giải thích cấu trúc địa chỉ IP
- Phân biệt được các lớp địa chỉ IP
- Xác định được địa chỉ mạng và host

Nội dung

- Cấu trúc địa chỉ IP
- Các lớp địa chỉ IP
- Mặt nạ mạng con (subnet mask)
- Địa chỉ mạng (network address)
- Địa chỉ quảng bá (broadcast address)
- Dải địa chỉ host (host range)

Cấu trúc địa chỉ IPv4



Các lớp địa chỉ IP

Bits:	1	8 9	16 17	24 25	32
Class A:	0NNNNNNN	Host	Host	Host	
	Range (1-126)				
Bits:	1	8 9	16 17	24 25	32
Class B:	10NNNNNN	Network	Host	Host	
	Range (128-191)				
Bits:	1	8 9	16 17	24 25	32
Class C:	110NNNNN	Network	Network	Host	
	Range (192-223)				
Bits:	1	8 9	16 17	24 25	32
Class D:	1110MMMM	Multicast Group	Multicast Group	Multicast Group	
	Range (224-239)				

Mặt nạ con (subnet mask)

Lớp địa chỉ	Các bit sử dụng cho mặt nạ mạng con	Ký pháp thập phân dấu chấm
Lớp A	11111111 00000000 00000000 00000000	255 . 0 . 0 . 0
Lớp B	11111111 11111111 00000000 00000000	255 . 255 . 0 . 0
Lớp C	11111111 11111111 11111111 00000000	255 . 255 . 255 . 0

Địa chỉ IP	131 . 107 . 16 . 200
Mặt nạ mạng con	255 . 255 . 0 . 0
NetID	131 . 107 . Y . Z
HostID	W . Y . 16 . 200

Lớp B

Network ID và host ID

□ Network ID

- Xác định địa chỉ mạng của một thiết bị/host

□ Host ID:

- Xác định địa chỉ của host/thiết bị trong mạng

Bits của IP address

□ Network Bits:

- Xác định network ID
- Xác định class của IP address
- Không cho phép tất cả bit là 0

□ Host Bits:

- Xác định host ID
- Tất cả các bit hosts là 0: địa chỉ mạng
- Tất cả các bit host là 1: địa chỉ broadcast address

Network address

- ❑ Network address là địa chỉ xác định một mạng riêng biệt, là cơ sở để phân biệt với các mạng khác.
- ❑ Hai host khác địa chỉ mạng phải được nối với nhau thông qua một thiết bị định tuyến (Router)
- ❑ Địa chỉ mạng kết thúc với tất cả các bit hosts là bit 0

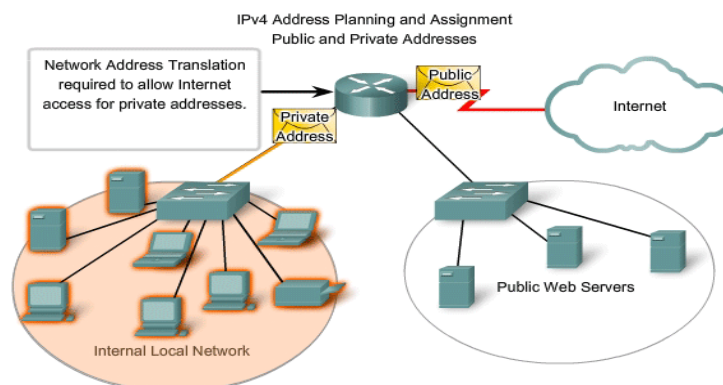
Số networks và số host

Class	Số Networks	Network Address	Số Hosts
Class A	$2^7 - 2 = 126$	1.0.0.0 to 126.0.0.0	$2^{24} - 2$
Class B	2^{14}	128.0.0.0 to 191.255.0.0	$2^{16} - 2$
Class C	2^{21}	192.0.0.0 to 223.255.255.0	$2^8 - 2$

IP private và IP public

Class	Range	Address Range	IP Private range
Class A	1 - 126	1.0.0.1 to 126.255.255.254	10.0.0.1 to 10.255.255.254
Class B	128 - 191	128.0.0.1 to 191.255.255.254	172.16.0.1 to 172.31.255.254
Class C	192 - 223	192.0.0.1 to 223.255.255.254	192.168.0.1 to 192.168.255.254

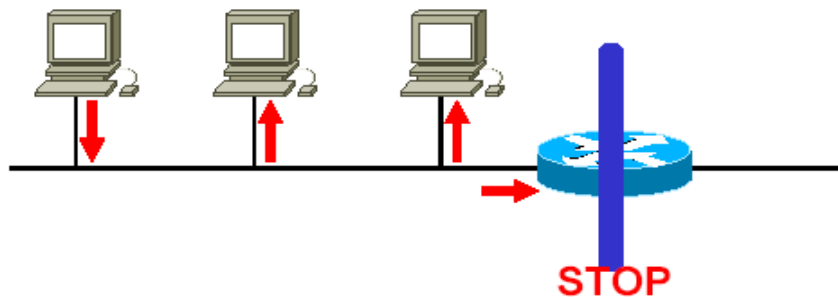
IP private và IP public



Broadcast address

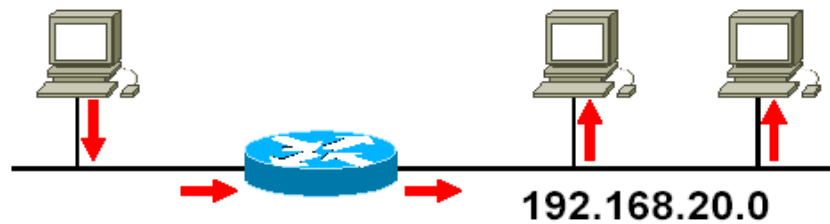
- ❑ Broadcast đi đến tất cả các host có chung một IP mạng.
- ❑ Broadcast address là địa chỉ IP trong đó có tất cả các bit host là 1.
- ❑ Một địa chỉ IP có tất cả các bit host và bit network đều là 1 được gọi là địa chỉ broadcast cục bộ (local broadcast address)

Local broadcast address



Local broadcast address
255.255.255.255

Directed broadcast address



Broadcast address
192.168.20.255

Bài tập lớp địa chỉ IP

Host IP Address	Address Class	Network Address	Host Range	Broadcast Address
216.14.55.137				
123.1.1.15				
150.127.221.224				
194.125.35.199				
175.12.239.244				

Bài tập địa chỉ IP gán cho host

- A. 150.100.255.255
- B. 175.100.255.18
- C. 195.234.253.0
- D. 100.0.0.23
- E. 188.258.221.176
- F. 224.156.217.73

IP SUBNET

Mục tiêu:

- Biết hoạch định và chia IP subnet
- Ứng dụng chia IP subnet trong thực tế
- Biết xác định địa chỉ subnet, host range.

Chia Subnet

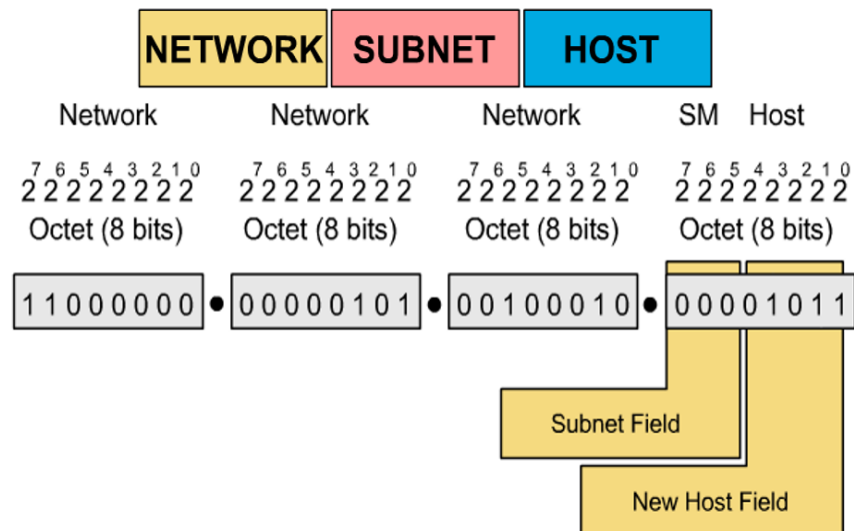
Chia subnet là chia một mạng có số host lớn thành nhiều mạng có số host nhỏ hơn nhằm:

- Có đủ số mạng cần thiết gán cho các site, phòng
- Giảm kích thước broadcast domain
- Thực thi việc quản lý phân cấp
- Tăng tính bảo mật cho các mạng

Ví dụ sử dụng lãng phí IP

Phòng HR Tổng số PC: 50 Network: 192.168.1.0 255.255.255.0	Phòng IT Tổng số PC: 36 Network: 192.168.2.0 255.255.255.0	IP sử dụng P.HR: 50 IP lãng phí: 204 IP sử dụng P.IT: 36 IP lãng phí: 218
Phòng Marketing Tổng số PC: 62 Network: 192.168.3.0 255.255.255.0	Phòng Sales Tổng số PC: 52 Network: 192.168.4.0 255.255.255.0	IP sử dụng P.Marketing: 62 Waste IP: 192 IP sử dụng P.Sales: 52 IP lãng phí: 202

Chia subnet



Các bước chia Subnet

- Xác định cần bao nhiêu host mỗi subnet
- Xác định cần bao nhiêu bit host
- Xác định subnet mask mới
- Xác định Slash value
- Xác định bước nhảy mạng (block size)
- Xác định tổng số subnet
- Xác định Network, Broadcast, First IP, Last IP

Chia subnet có 50 host

Network:
192.168.1.0
255.255.255.0
192.168.1.0 / 24

- Số host cần cho mỗi subnet= 50
- Số bit host cần dùng
 $2^n = 2 * 2 * 2 * 2 * 2 = 64$
 $n=6$
- Subnet Mask mới = 255.255.255.192

128 64 32 16 8 4 2 1

- Slash Value : 192.168.1.0 / 26
- Block size / subnets = 64
- Tổng số subnets = $256 / 64 = 4$

Chia subnet có 50 host

Network:
192.168.1.0
255.255.255.0

Block Size	Network Address	First Useable IP	Last Useable IP	Broadcast Address
0	192.168.1.0	192.168.1.1	192.168.1.62	192.168.1.63
64	192.168.1.64	192.168.1.65	192.168.1.126	192.168.1.127
128	192.168.1.128	192.168.1.129	192.168.1.190	192.168.1.191
192	192.168.1.192	192.168.1.193	192.168.1.253	192.168.1.254
256				

Cách xác định Subnet

Xác định subnet của một host có địa chỉ IP và Subnet mask (hoặc Slash Value)

- Đổi địa chỉ IP ra dạng nhị phân
- Đổi Subnet mask ra dạng nhị phân
- Xác định Network ID và Host ID
- Xác định địa chỉ Subnet, Broadcast
- Xác định địa chỉ First IP và Last IP

Ví dụ xác định subnet

	172	16	2	160	
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
					Subnet
					Broadcast
					First
					Last

Ví dụ xác định subnet

	172	16	2	160	
	3				
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
					Subnet
					Broadcast
					First
					Last

Ví dụ xác định subnet

	172	16	2	160	
	3				
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
					Subnet 4
					Broadcast
					First
					Last

Ví dụ xác định subnet

	172	16	2	160		
					3	
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
				10000000	Subnet	4
				10111111	Broadcast	
					5	
					First	
					Last	

Ví dụ xác định subnet

	172	16	2	160		
					3	
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
				10000000	Subnet	4
				10111111	Broadcast	
					5	
				10000001	First	6
					Last	

Ví dụ xác định subnet

	172	16	2	160		
					3	
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
				10000000	Subnet	4
				10111111	Broadcast	
				10000001	First	5
				10111110	Last	6
						7

Ví dụ xác định subnet

	172	16	2	160		
					3	
172.16.2.160	10101100	00010000	00000010	10100000	Host	1
255.255.255.192	11111111	11111111	11111111	11000000	Mask	2
				10000000	Subnet	4
				10101100	Broadcast	
				10000001	First	5
				10111110	Last	6
						7

Ví dụ xác định subnet

	172	16	2	160	
	3				
172.16.2.160	10101100	00010000	00000010	10100000	Host 1
255.255.255.192	11111111	11111111	11111111	11000000	Mask 2
172.16.2.128	10101100	00010000	00000010	10000000	Subnet 4
172.16.2.191	10101100	00010000	00000010	10111111	Broadcast 5
172.16.2.129	10101100	00010000	00000010	10000001	First 6
172.16.2.190	10101100	00010000	00000010	10111110	Last 7

Bài tập xác định subnet

▣ Xác định địa chỉ subnet của địa chỉ IP sau đây:
192.168.20.180/27?

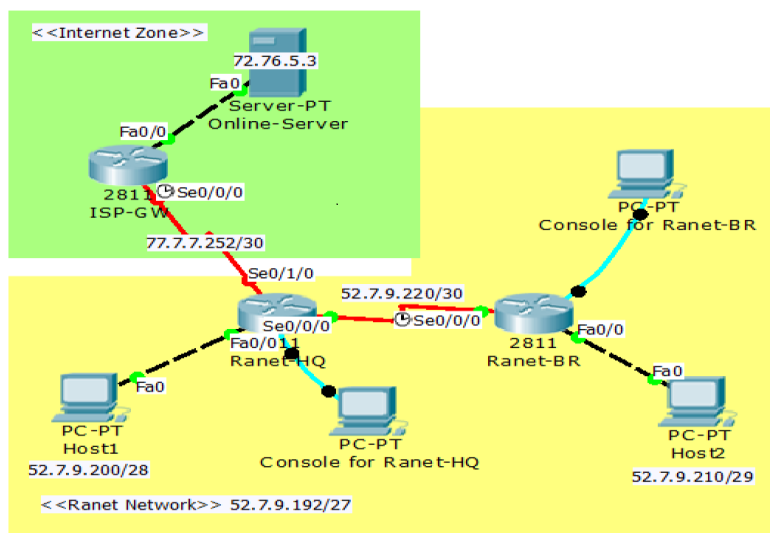
- A. 192.116.20.96/27
- B. 192.116.20.128/27
- C. 192.116.20.160/27
- D. 192.116.20.192/27

Bài tập xác định subnet

▣ Các địa chỉ IP nào sau đây có thể gán được cho các host khi subnet mask là 255.255.255.224

- A. 16.23.118.63
- B. 87.45.16.159
- C. 92.11.178.93
- D. 34.178.18.56
- E. 192.168.16.87
- F. 217.168.166.192

Bài tập xác định subnet



THIẾT BỊ MẠNG ROUTER

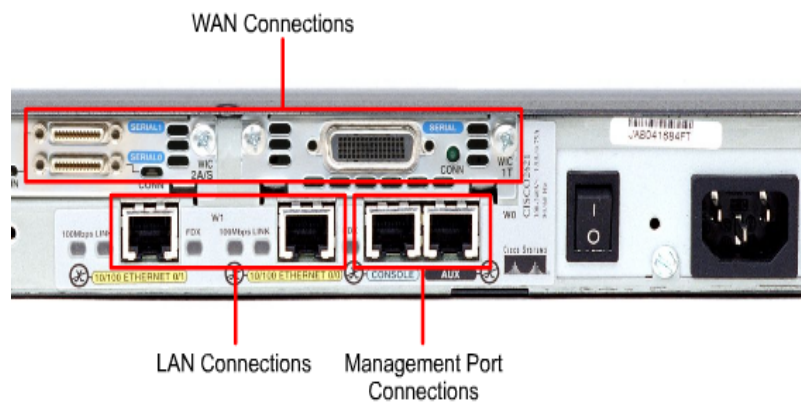
Mục tiêu:

- Hiểu các thành phần của Cisco router
- Biết cách sao lưu cấu hình Cisco router
- Phục hồi password của Cisco router

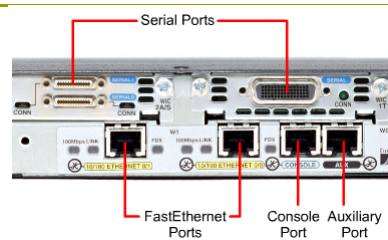
Nội dung

- Các thành phần bên ngoài router
 - WAN interface
 - LAN interface
 - Management ports: Console / AUX (Auxiliary)
- Các thành phần bên trong router
 - CPU
 - ROM
 - RAM
 - NVRAM
 - FLASH
- Hệ điều hành của Cisco router

Thành phần bên ngoài router

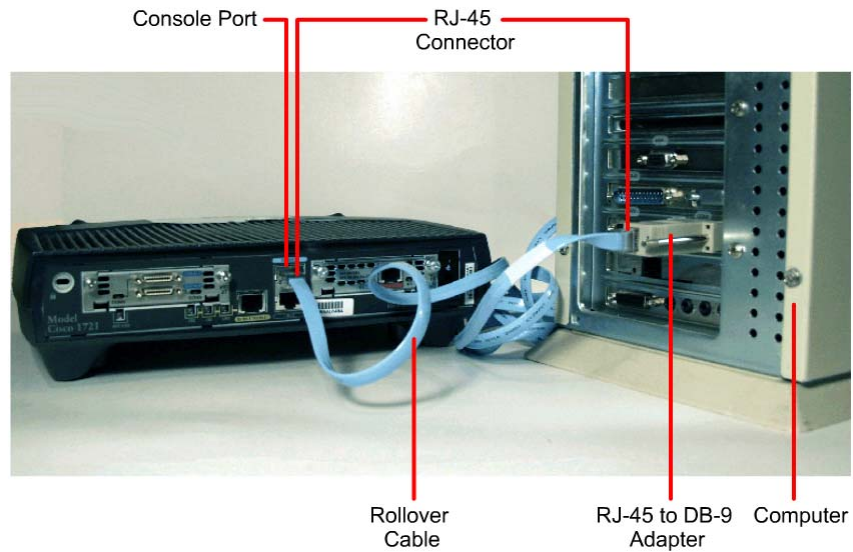


LAN / WAN Interfaces

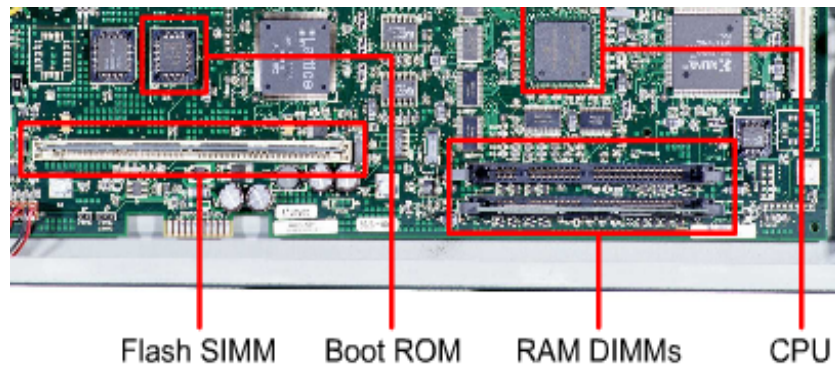


- ❑ Kết nối các router đến mạng để truyền và nhận packet.
- ❑ Interfaces có thể tích hợp trên motherboard cũng có thể ở dạng module rời

Management port: Console



Các thành phần trên Router



CPU

- ❑ CPU (Central Processing Unit) khởi tạo hệ thống
- ❑ CPU thực thi các chỉ thị của HĐH
- ❑ Thực thi chức năng định tuyến
- ❑ Điều khiển network interface
- ❑ Các dòng router lớn có thể có nhiều CPU.

ROM

- ❑ ROM (Read Only Memory) lưu các mã chẩn đoán khởi động power-on diagnostics, chương trình bootstrap và HĐH ROMMON (ROM monitor).
- ❑ Nhiệm vụ chính của ROM là kiểm tra phần cứng của router khi khởi động và load phần mềm IOS từ flash vào RAM.

RAM

- ❑ Cung cấp bộ nhớ tạm cho file cấu hình router trong khi router đang hoạt động (running-config)
- ❑ Lưu trữ các bảng định tuyến (routing tables).
- ❑ Lưu trữ ARP tables (Address Resolution Protocol)
- ❑ Cung cấp vùng nhớ đệm cho các gói dữ liệu đang ở hàng đợi chờ xử lý.
- ❑ RAM có thể được nâng cấp. Nội dung lưu trên RAM sẽ mất khi router bị mất điện hoặc khởi động lại.

NVRAM (Non-volatile RAM)

- ❑ Lưu startup configuration file (startup-config)
- ❑ Nội dung của NVRAM vẫn được lưu giữ khi router bị mất điện hoặc khởi động lại

Flash Memory

- ❑ Lưu HĐH full current version of IOS (Internetworking Operating System) đang chạy trên router
- ❑ Flash là bộ nhớ có thể xóa hoặc ghi đè phiên bản mới của HĐH IOS
- ❑ Nội dung của flash vẫn được lưu giữ khi router bị mất điện hoặc khởi động lại.

Hệ điều hành Cisco router

- ❑ Hỗ trợ các giao thức và chức năng mạng (định tuyến và chuyển mạch)
- ❑ Kết nối chuyển lưu lượng tốc độ cao (high-speed traffic) giữa các thiết bị
- ❑ Đảm bảo tin cậy và bảo mật khi truy xuất các tài nguyên mạng
- ❑ Cung cấp khả năng mở rộng mạng

Hệ điều hành Cisco router

Có 3 dạng HĐH mà router có thể sử dụng:

- ❑ Một hệ điều hành (không phải là IOS) được chứa trong ROM với tên gọi là ROM monitor (viết tắt là ROMMON)
- ❑ HĐH giới hạn limited-function IOS chứa trong ROM
- ❑ HĐH đầy đủ full-function IOS chứa trong flash

Các HĐH của router

Có 3 mode để dùng 3 HĐH tương ứng:

- ❑ ROM monitor: ROMMON>
- ❑ Boot ROM: Router(boot)>
- ❑ Cisco IOS : Router>

ROM monitor: ROMMON>

- ❑ Config-register = 0x2100 là khởi động từ ROM monitor
- ❑ ROM monitor thực hiện quá trình bootstrap kiểm tra phần cứng (bootstrap là 1 tập lệnh để thực hiện kiểm tra phần cứng và khởi động HĐH)
- ❑ Dùng để debug ở cấp thấp hoặc để khôi phục password trong trường hợp bị mất password
- ❑ Chỉ có thể vào mode này từ cổng console trên router

Boot ROM: Router(boot)>

- ❑ Config-register = 0x2101 là khởi động từ ROM với limited-function IOS
- ❑ HĐH này chỉ có các chức năng giới hạn của IOS (Dạng hoạt động này giống như DOS hay Safemode trong Windows).
- ❑ HĐH này sẽ đảm bảo cho Router hoạt động với các thông số cơ bản nhất như các thông số về kết nối IP
- ❑ HĐH này được sử dụng khi bộ nhớ flash bị hỏng và bạn cần copy một hệ điều hành đầy đủ mới vào Router.

Cisco IOS : Router>

- ❑ Config-register = 0x2102 là khởi động từ IOS trong flash
- ❑ Hoạt động bình thường của 1 router yêu cầu sử dụng phần mềm full Cisco IOS lưu trong flash.
- ❑ Ở một số thiết bị, phần mềm IOS được thực thi trực tiếp từ flash.
- ❑ Hầu hết các Cisco router yêu cầu 1 bản copy của IOS được load vào RAM và cũng thực thi từ RAM
- ❑ Lệnh show version xem các thông tin và phiên bản IOS đang chạy. Trong đó có hiển thị giá trị của config-register

Thanh ghi Cisco router

- ❑ Thanh ghi 16-bit trong CPU:
 - The configuration register is a 16-bit register in CPU.



- 0 – 3: Boot field
- 6: Ignore NVRAM contents
- 8: Break disabled
- 11-12: Console line speed
- 13: Boot ROM if network boot fails
- 15: Diagnostic and ignore NVRAM



Thanh ghi Cisco router

Một số giá trị đặc biệt của thanh ghi:

- ❑ 0x2100 là khởi động từ rommon
- ❑ 0x2101 là khởi động từ ROM với limited function IOS.
- ❑ 0x2102 là khởi động từ IOS trong Flash – Full IOS
- ❑ 0x2142: Khởi động bỏ qua NVRAM

Thanh ghi Cisco router

Cisco IOS Software, 2800 Software (C2800NM-IPBASE-M), Version 12.4(3i), RELEASE SOFTWARE (fc2)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 28-Nov-07 21:09 by stshen

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

DHSPKT uptime is 5 weeks, 5 days, 23 hours, 29 minutes

System returned to ROM by power-on

System image file is "flash:c2800nm-ipbase-mz.124-3i.bin"

Cisco 2851 (revision 53.51) with 251904K/10240K bytes of memory.

Processor board ID FHK1150F1M1

2 Gigabit Ethernet interfaces

1 Serial interface

2 Channelized E1/PRI ports

DRAM configuration is 64 bits wide with parity enabled.

239K bytes of non-volatile configuration memory.

62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102

Bài tập

- ▣ Nêu qui trình phục hồi password của Cisco router và đảm bảo không mất cấu hình trước đó?

CẤU HÌNH CISCO ROUTER/SWITCH CƠ BẢN

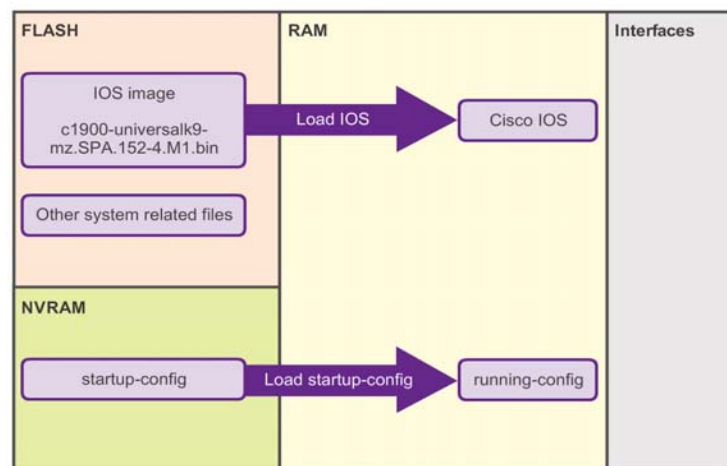
Mục tiêu:

- Biết cách cấu hình cơ bản thiết bị Cisco
- Biết cách bảo mật truy cập thiết bị Cisco

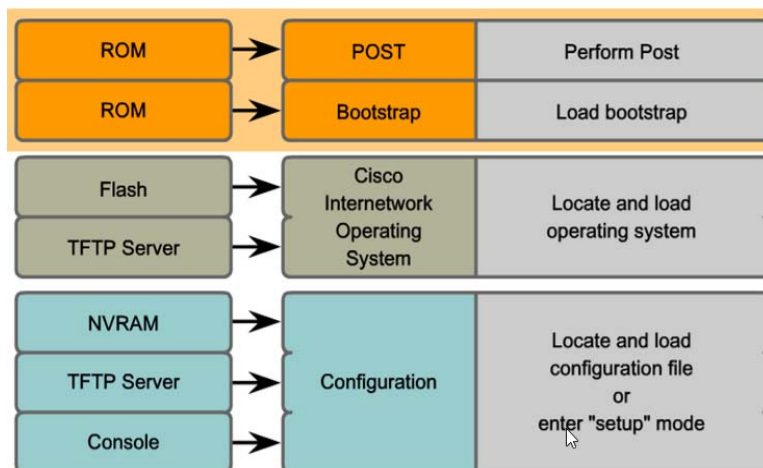
Nội dung

- ❑ Tiến trình khởi động thiết bị
- ❑ Truy cập thiết bị
- ❑ Cấu trúc phân cấp IOS Mode
- ❑ Cấu trúc lệnh IOS
- ❑ Cấu hình các thông số cơ bản
- ❑ Bảo mật truy cập thiết bị
- ❑ Lưu cấu hình

Tiến trình khởi động thiết bị



Tiến trình khởi động thiết bị



Các phương pháp truy cập

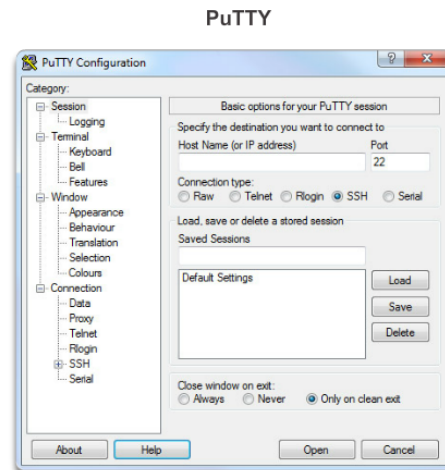
Các phương pháp truy cập Command Line Interface phổ biến

- Console
- Telnet or SSH

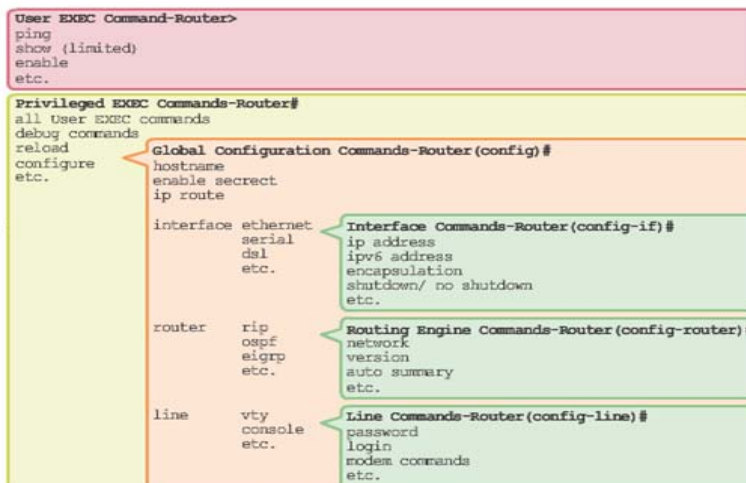


Các phần mềm truy cập

- ▣ PuTTY
- ▣ SecureCRT
- ▣ HyperTerminal
- ▣ ...



Cấu trúc phân cấp IOS Mode



Các Mode chính

User EXEC Mode

Limited examination of router.
Remote access.

```
Switch>  
Router>
```

The **User EXEC** mode allows only a limited number of basic monitoring commands and is often referred to as view-only mode.

Privileged EXEC Mode

The **Privileged EXEC** mode, by default, allows all monitoring commands, as well as execution of configuration and management commands.

Detailed examination of router. Debugging and testing. File manipulation. Remote access.

```
Switch#  
Router#
```

Global Config Mode và Submodes

Privileged EXEC Mode

Detailed examination of router, Debugging and testing.
File manipulation. Remote access.

```
Switch#  
Router#
```

Global Configuration Mode

Global configuration commands.

```
Switch(config)#  
Router(config)#
```

Other Configuration Modes

Specific service or interface configurations.

```
Switch(config-mode)#  
Router(config-mode)#
```

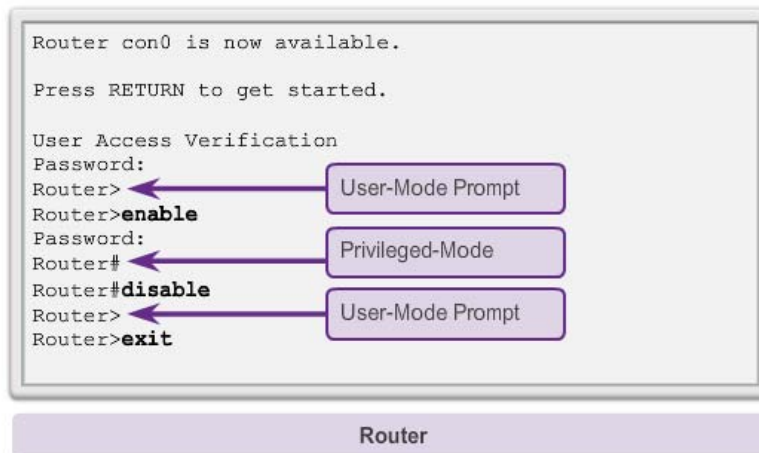
IOS Prompt Structure

```
Router>ping 192.168.10.5  
  
Router#show running-config  
  
Router(config)#Interface FastEthernet 0/0  
  
Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

The prompt changes to denote the current CLI mode.

```
Switch>ping 192.168.10.9  
  
Switch#show running-config  
  
Switch(config)#Interface FastEthernet 0/1  
  
Switch(config-if)#Description connection to WEST LAN4
```

Chuyển đổi IOS Modes



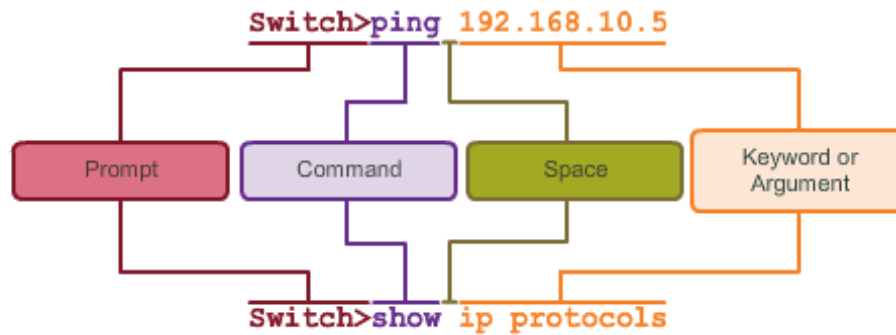
Chuyển đổi IOS Modes

```
Switch>enable  
Switch#configure terminal  
Enter configuration commands, one per line.  
End with CNTL/Z.  
Switch(config)#interface vlan 1  
Switch(config-if)#exit  
Switch(config)#exit  
Switch#
```

```
Switch#configure terminal  
Enter configuration commands, one per line.  
End with CNTL/Z.  
Switch(config)#vlan 1  
Switch(config-vlan)#end  
Switch#
```

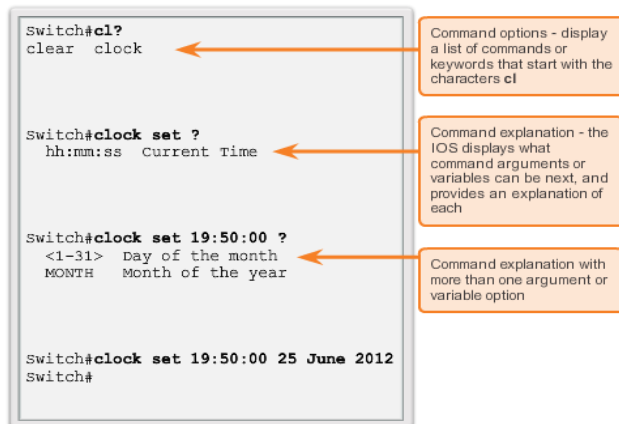
```
Switch#configure terminal  
Enter configuration commands, one per line.  
End with CNTL/Z.  
Switch(config)#line vty 0 4  
Switch(config-line)#interface fastethernet 0/1  
Switch(config-if)#end  
Switch#
```

Cấu trúc lệnh IOS



Context Sensitive Help

Context Sensitive Help



Kiểm tra cú pháp lệnh

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

The IOS returns a help message indicating that required keywords or arguments were left off the end of the command.

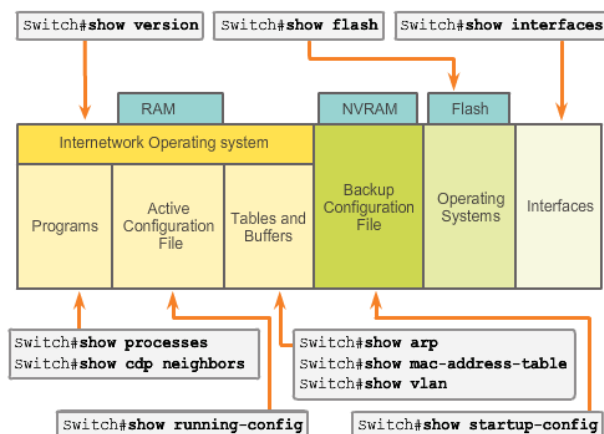
```
Switch#c
% Ambiguous command: 'c'
```

The IOS returns a help message to indicate that there were not enough characters entered for the command interpreter to recognize the command.

```
Switch#clock set 19:50:00 25 6
                        ^
% Invalid input detected at '^'
marker.
```

The IOS returns a "^" to indicate where the command interpreter can not decipher the command.

Các lệnh show kiểm tra



IOS **show** commands can provide information about the configuration, operation and status of parts of a Cisco router.

Ví dụ lệnh show version

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

Router uptime is 10 hours, 9 minutes
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: power-on

<Output omitted>

Cisco CISC01941/K9 (revision 1.0) with 446464K/77824K bytes of memory.
Processor board ID FTX16368482
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of Non-Volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)

<Output omitted>

Technology Package License Information for Module:'c1900'

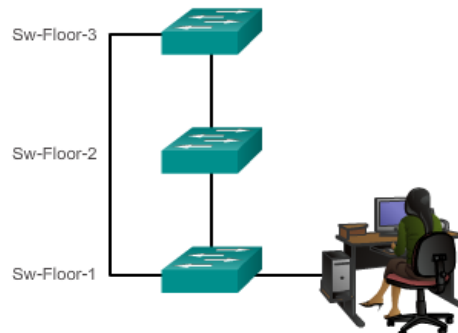
-----
Technology      Technology-package      Technology-package
                  Current          Type              Next reboot
-----
ipbase          ipbasek9              Permanent         ipbasek9
security        None                  None              None
data            None                  None              None

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

Router#
```

Cấu hình Hostname

Configuring Device Names



Cấu hình Hostname

Configure a Hostname

Configure the switch hostname to be 'AtlantaHQSw1'.

```
Switch# configure terminal
```

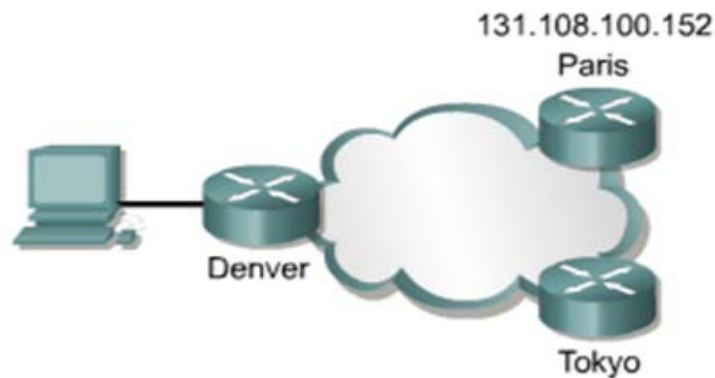
Enter configuration commands, one per line. End with CNTL/Z.

```
Switch(config)# hostname AtlantaHQSw1
```

```
AtlantaHQSw1(config)#
```

You successfully configured the switch hostname.

Bảo mật truy cập thiết bị



Password truy cập Privileged Mode

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Bảo mật truy cập User EXEC

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

Mã hóa Password

Configuring Password Encryption

```
Enter the command to encrypt the plain text passwords.
Switch(config)# service password-encryption
Exit global configuration mode and view the running configuration.
Switch(config)# exit
Switch# show running-config
!
<output omitted>
!
line con 0
 password 7 094F471A1A0A
 login
!
line vty 0 4
 password 7 03095A0F034F38435E49150A1819
 login
!
!
end
```

Banner Messages

Limiting Device Access - MOTD Banner

```
LAB_A(config)#banner motd # This is a secure system. Authorized Access ONLY!!! #
```

This configuration results in this message of the day banner.

Delimiting characters are not included in the message.

```
Sw1-Floor-1 con0 is now available
Press RETURN to get started.
This is a secure system. Authorized
Access ONLY!!!
User Access Verification
password:
Sw1-Floor-1>enable
Password:
Sw1-Floor-1#
```

Lưu file cấu hình

Saving and Erasing the Configuration

```
Switch#show running-config
```

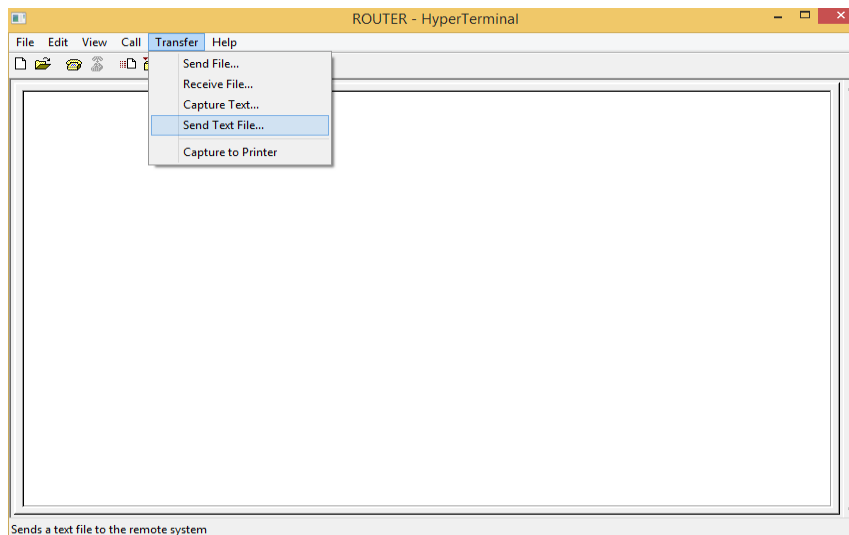
Lists the complete configuration currently active in RAM.

The active configuration can be copied to NVRAM.

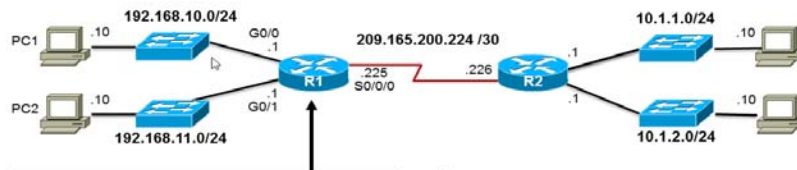
```
Switch#show running-config
Building configuration...
Current configuration : 2904 bytes
!
! Last configuration change at 00:02:32
UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
<output omitted>
!
```

```
Switch#copy running-config startup-config
```

Restore file cấu hình



Ví dụ cấu hình cơ bản



```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# hostname R1
R1(config)#
```

OR

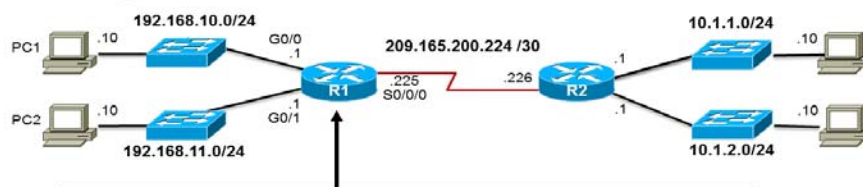
```
Router> en
Router# conf t
Enter configuration commands, one per line.
End with CNTL/Z.
Router(config)# ho R1
R2(config)#
```

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

```
R1(config)# banner motd #
Enter TEXT message. End with the character '#'.
*****
WARNING: Unauthorized access is prohibited!
*****
#
R1(config)#
```

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Cấu hình LAN Interface



```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# description Link to LAN-10
R1(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)# exit
R1(config)#
R1(config)# int g0/1
R1(config-if)# ip add 192.168.11.1 255.255.255.0
R1(config-if)# des Link to LAN-11
R1(config-if)# no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
R1(config-if)# exit
R1(config)#
```

Cấu hình Serial Interface

Enter Global Configuration Mode

```
R1#configure terminal
R1(config)#
```

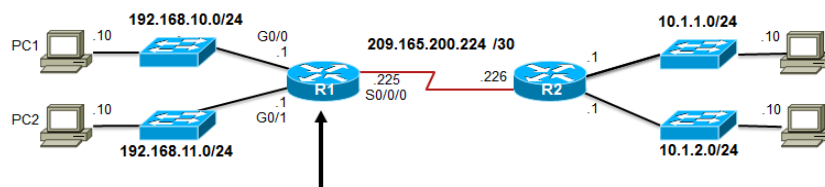
Cấu hình Serial Interface

```
R1(config)#interface serial 0/0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 209.165
.200.225 255.255.255.252
```

Set Clock Rate
(on DCE interfaces only)

```
R1(config-if)#clock rate 64000
R1(config-if)#
```

Kiểm tra cấu hình Interface



```
R1# show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0  192.168.10.1    YES manual up          up
GigabitEthernet0/1  192.168.11.1    YES manual up          up
Serial0/0/0        209.165.200.225 YES manual up          up
Serial0/0/1        unassigned      YES NVRAM  administratively down down
Vlan1              unassigned      YES NVRAM  administratively down down
R1#
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms
R1#
```

Bài tập

- ▣ Cấu hình các thông số cơ bản của thiết bị Router/Switch để có thể telnet từ xa vào thiết bị được?

Bảo mật thiết bị sử dụng SSH

- ▣ SSH (Secure Shell) được sử dụng thay thế cho Telnet để đảm bảo Attacker không thấy được Telnet traffic vì dữ liệu đã được mã hóa khi trao đổi giữa 2 thiết bị mạng
- ▣ SSH là giao thức TCP mặc định sử dụng TCP port là 22, trong khi đó mặc định Telnet sử dụng TCP port là 23

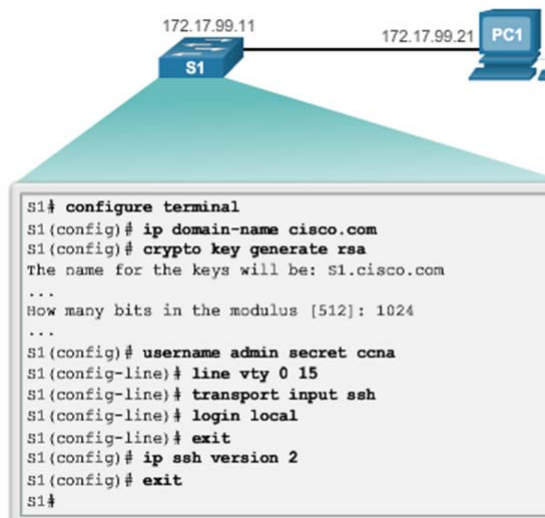


Các yêu cầu để cấu hình SSH

1. Đảm bảo router đang chạy phiên bản Cisco IOS có hỗ trợ SSH:
 - ❑ SSH version 1: Cisco IOS Release 12.1(1)T trở lên
 - ❑ SSH version 2: Cisco IOS Release 12.3(4)T trở lên
2. Đảm bảo mỗi router có một hostname riêng duy nhất.
3. Đảm bảo mỗi router có cấu hình domain name
4. Đảm bảo router được cấu hình local authentication hoặc AAA services để chứng thực username và password

Cấu hình SSH

1. Verify SSH Support –
`show ip ssh`
2. Configure the IP domain.
3. Generate RSA key pairs.
4. Configure user authentication.
5. Configure the vty lines.
6. Enable SSH version 2.



Kiểm tra SSH

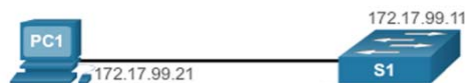
Remote Management SSH Connection



```
172.17.99.11 - PuTTY
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Kiểm tra SSH



```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaClyc2EAAAADAQABAAQgQCdLksVz2QlREscZt2f2scJHbW3aMDM8
/8jq/srGFNL
i+f+qJWwxt26Bwmy694+6ZIQ/j7wUfIVN1QhI8GUOViuKNqVMOMtLg8Ud4qAilbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGM088OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes256-cbc hmac-shal Session started admin
0 2.0 OUT aes256-cbc hmac-shal Session started admin
%No SSHv1 server connections running.
S1#
```

Bài tập cấu hình SSH

- ▣ Cấu hình lab: “Configuring Secure Passwords and SSH”

ĐỊNH TUYẾN TĨNH



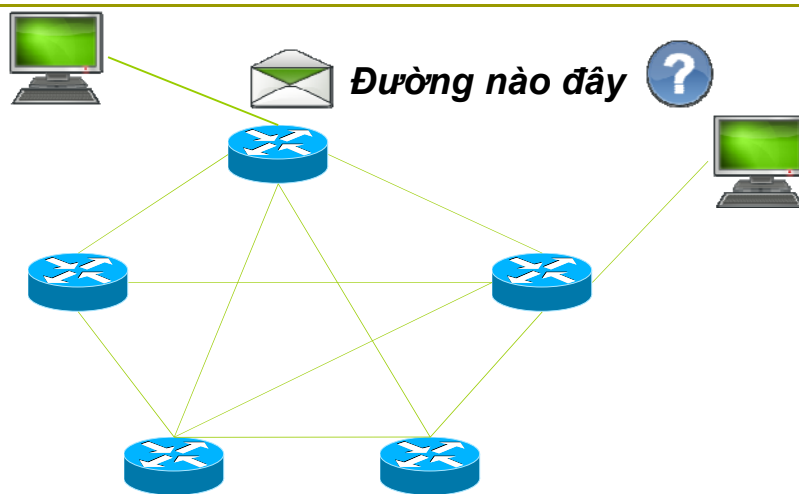
Mục tiêu:

- Hiểu khái niệm định tuyến
- Biết cách cấu hình static route
- Biết cách cấu hình default route

Nội dung

- ▣ Khái niệm định tuyến
- ▣ Phân loại định tuyến
- ▣ Cấu hình static routing
- ▣ Cấu hình default routing

Định tuyến là gì ?



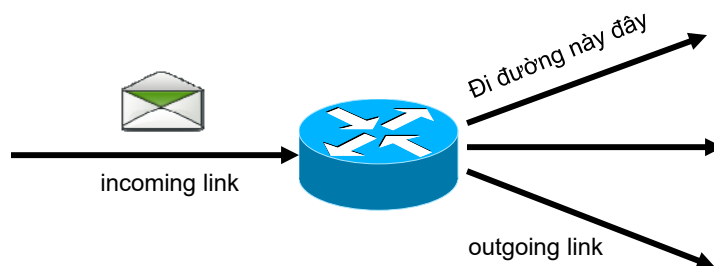
114

Khái niệm về định tuyến

- Định tuyến (routing) là quá trình router lựa chọn tuyến đường để chuyển gói tin đến mạng đích.
- Router đưa ra quyết định dựa trên địa chỉ IP của gói tin.

115

Khái niệm về định tuyến



116

Phân loại định tuyến

- Để chọn được đường đi tối ưu nhất đòi hỏi các Router phải “học” đường đi đến các mạng. Vậy làm sao để “học” đây ?
- Có 2 cách :
 - Cách 1 : Do người quản trị “dạy” gọi là định tuyến tĩnh (Static Routing)
 - Cách 2 : Do Router “tự học” gọi là định tuyến động (Dynamic Routing)

117

Định tuyến tĩnh (static)

- Các thông tin về đường đi do người quản trị mạng cung cấp cho Router.
- Khi mạng có sự thay đổi thì người quản trị phải thay đổi các thông tin này.
- Định tuyến tĩnh áp dụng đối với hệ thống mạng nhỏ, hoặc kết hợp với định tuyến động.

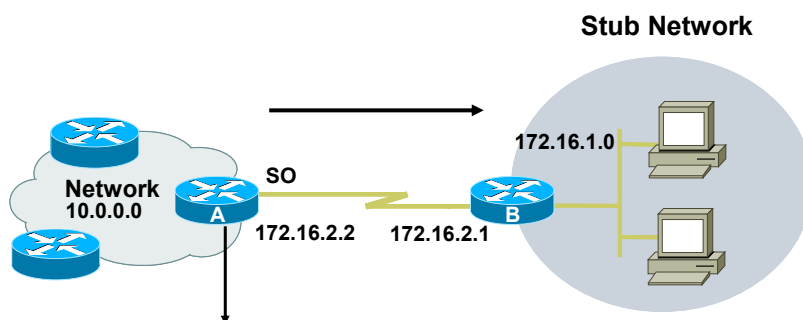
118

Cấu hình Static Routing

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

- Diễn giải lệnh ip route:
 - network—network/subnet đích
 - mask—subnet mask
 - address—IP address của router kế để đến được network/subnet đích
 - Interface—Tên của interface sử dụng để đến network/subnet đích

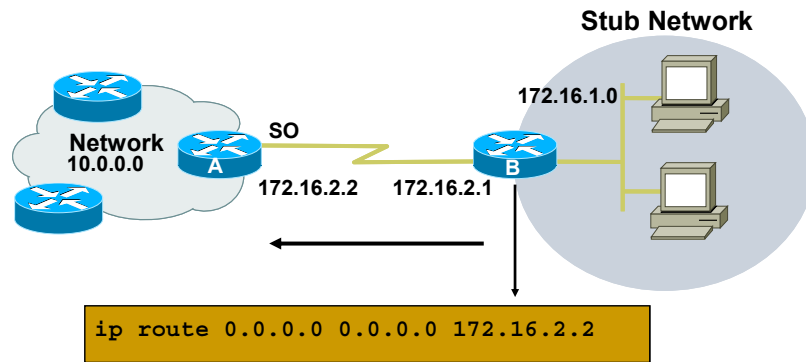
Static Routing



```
ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

```
ip route 172.16.1.0 255.255.255.0 S0
```

Default Routing



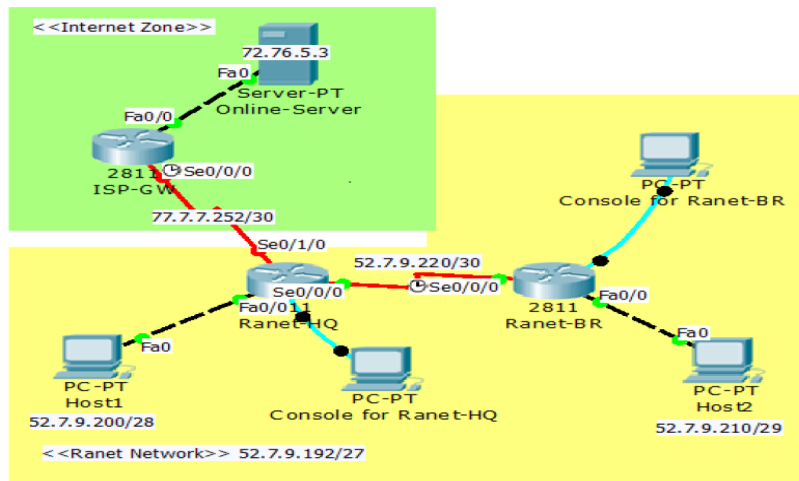
- Tuyến này cho phép stub network đến tất cả các network đã biết từ router A.

Troubleshooting định tuyến

Các lệnh troubleshooting lỗi định tuyến:

- ping
- traceroute
- show ip route
- show ip interface brief
- show cdp neighbors detail

Bài tập static & default route



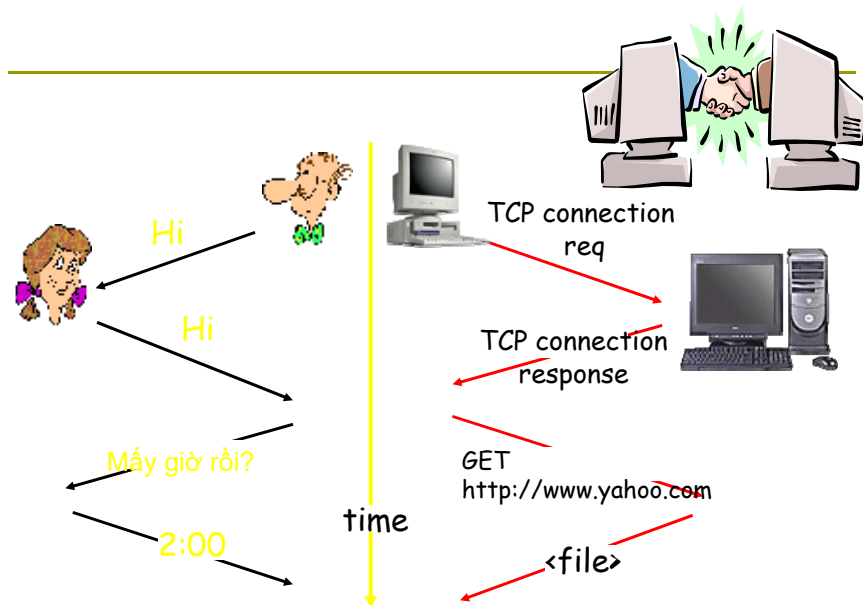
GIAO THỨC



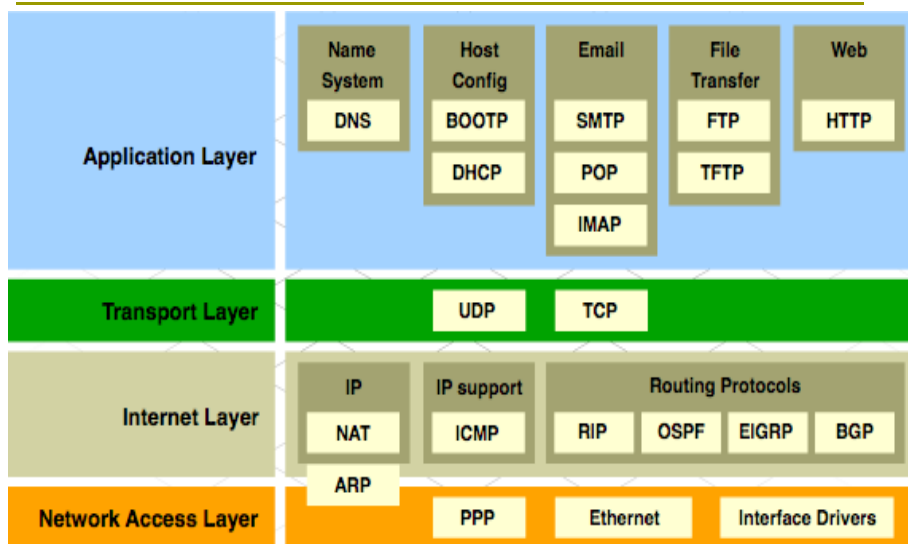
Mục tiêu:

- Hiểu khái niệm giao thức
- Hoạt động của các giao thức trong chồng giao thức TCP/IP

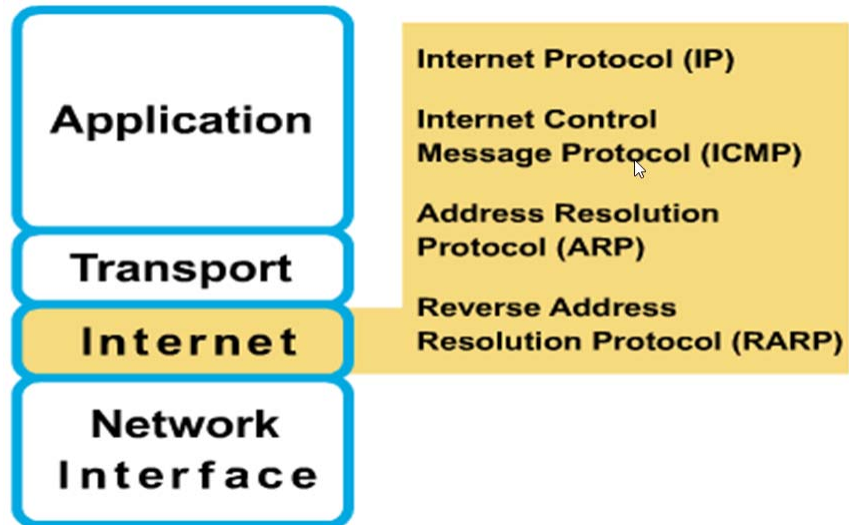
Khái niệm giao thức



Chồng giao thức TCP/IP



Các giao thức ở lớp Internet



ICMP - INTERNET CONTROL MESSAGE PROTOCOL

ICMP

- ❑ Cung cấp cơ chế thông báo lỗi cho giao thức IP
- ❑ Tính năng:
 - Một node phát hiện ra lỗi như gói tin hết TTL, máy đích không tồn tại,... sẽ tạo ra gói ICMP.
 - Cung cấp một số tính năng để chẩn đoán hoạt động của mạng.

Lệnh sử dụng giao thức ICMP

```
Router###ping 10.1.1.10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

```
Router#trace 192.168.101.101
```

```
Type escape sequence to abort.
```

```
Tracing the route to 192.168.101.101
```

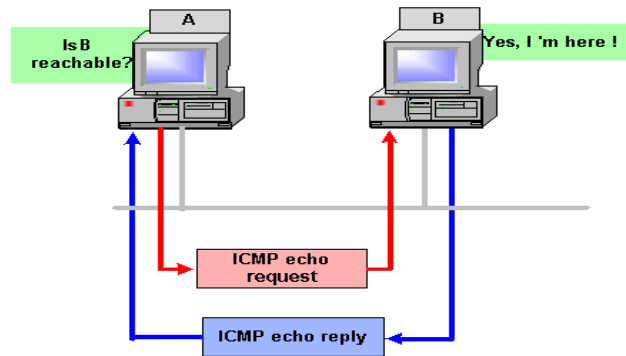
```
  1 p1r1 (192.168.1.49) 20 msec 16 msec 16 msec
```

```
  2 p1r2 (192.168.1.18) 48 msec * 44 msec
```

```
Router#
```

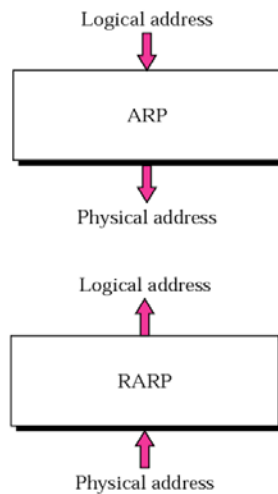
Lệnh Ping

- Lệnh Ping gửi gói “echo request” đến một máy và đợi gói “echo reply”



GIAO THỨC ARP

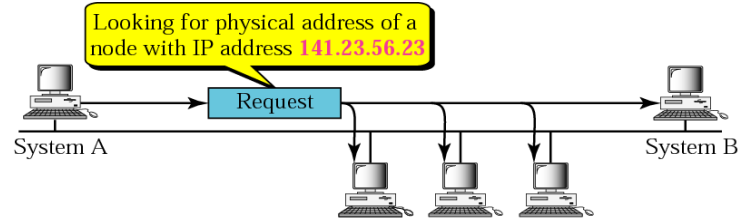
ARP (Addr Resolution Protocol)



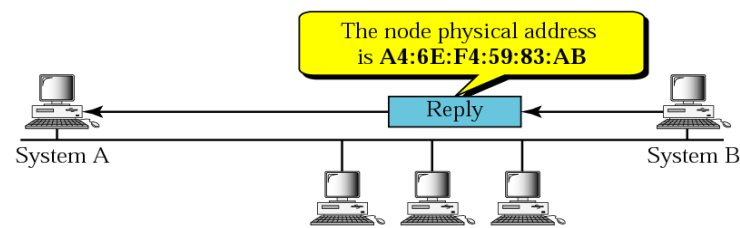
ARP (Addr Resolution Protocol)

- Hoạt động của ARP đơn giản là quá trình “hỏi” (request) và “trả lời” (reply).
 - Request: “Ai có IP là x.y.z.t vui lòng cho biết MAC”
 - Reply: “Địa chỉ x.y.z.t đang ở MAC là ...”
- Gói request được gửi broadcast
- Gói reply được gửi unicast

ARP (Addr Resolution Protocol)



a. ARP request is broadcast



b. ARP reply is unicast

Minh họa lệnh arp

```
C:\Users\PC>arp -a
```

192.168.100.1	00-50-7f-cc-81-f8	dynamic
192.168.100.26	00-26-5e-fc-5e-d9	dynamic
192.168.100.31	00-26-82-ea-ab-1e	dynamic
192.168.100.255	ff-ff-ff-ff-ff-ff	static

DHCP - Dynamic Host Configuration Protocol

Mục tiêu:

- Biết ứng dụng DHCP
- Hiểu hoạt động của DHCP
- Biết cách cấu hình DHCP

Nội dung

- ▣ Khái niệm DHCP
- ▣ Hoạt động của DHCP
- ▣ Cấu hình DHCP

DHCP - Dynamic Host Configuration Protocol

DHCP giúp làm giảm sự phức tạp công việc quản trị hệ thống mạng bằng cách cung cấp thông số TCP/IP tự động.

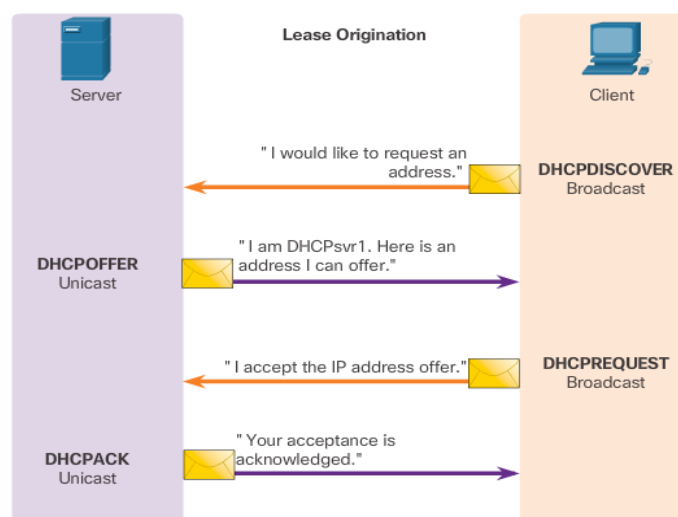
Cấu hình TCP/IP bằng tay

- Địa chỉ IP đặt bằng tay
- Địa chỉ IP có thể không đúng
- Có thể trùng IP dẫn đến hệ mạng bị lỗi.
- Việc di chuyển máy tính làm tăng công việc quản trị

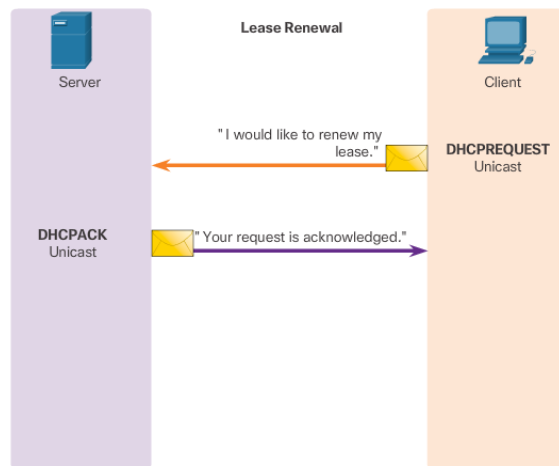
Cấu hình TCP/IP tự động

- Địa chỉ IP được gán tự động
- Thông tin cấu hình chính xác
- Thông số cấu hình của client được thay đổi tự động
- Tránh được các công việc quản trị không cần thiết

HOẠT ĐỘNG CỦA DHCP



HOẠT ĐỘNG CỦA DHCP



Cấu hình DHCP trên Cisco router

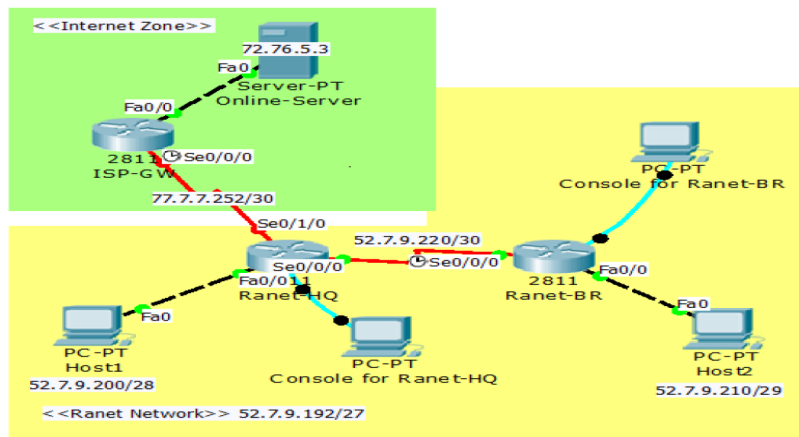
🔧 Các bước cấu hình

- ✦ Xác định dải địa chỉ IP và IP đặt tĩnh để loại trừ
- ✦ Tạo pool name
- ✦ Xác định dải địa chỉ IP cần cấp và subnet mask
- ✦ Chỉ định default gateway, DNS server, domain

```
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) # dns-server 192.168.11.5
R1 (dhcp-config) # domain-name example.com
R1 (dhcp-config) # end
R1 #
```

Bài tập DHCP

Cấu hình DHCP cấp IP động cho các host trong LAN



IP ACCESS CONTROL LIST

Mục tiêu:

- Hiểu khái niệm IP Access Control List
- Biết cách cấu hình Standard ACL
- Biết cách cấu hình Extended ACL

Nội dung

- ▣ Khái niệm IP Access Control List (ACL)
- ▣ Phân loại IP Access Control List
- ▣ Cấu hình Standard ACL
- ▣ Cấu hình Extended ACL

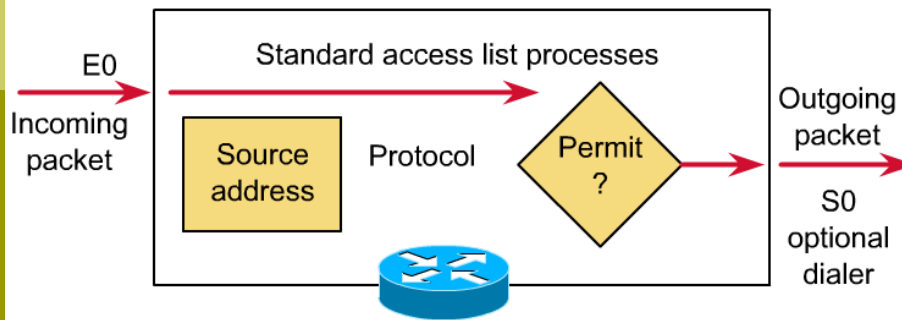
Khái niệm IP ACL

- ✚ ACL là một danh sách các câu lệnh được áp đặt vào các cổng (interface) của router.
- ✚ Danh sách này chỉ ra cho router biết loại packet nào được chấp nhận (permit) và loại packet nào bị hủy bỏ (deny).
- ✚ Sự chấp nhận và hủy bỏ này có thể dựa vào source address, destination address, protocols, port-number.

Khái niệm IP ACL

✦ Áp dụng Access list cho Interface

- ✦ Inbound (in): Lọc các gói dữ liệu đi vào các interface trên Router.
- ✦ Outbound (out): Lọc các gói dữ liệu đi ra từ các interface trên Router.



Phân Loại ACL

✦ Standard ACL

- ✦ Kiểm tra địa chỉ nguồn trong gói tin.
- ✦ Permit hay deny toàn bộ protocol .

✦ Extended ACL

- ✦ Kiểm tra cả địa chỉ nguồn, địa chỉ đích, port.
- ✦ Permit hay deny một giao thức hay ứng dụng cụ thể.

Khái niệm Wildcard Mask

- ✦ Là chỉ số ngược của Subnetmask dùng để xác định một số lượng host cụ thể dựa trên dải địa chỉ IP của các host.
- ✦ Wildcard Mask gồm 32 bit, chia thành 4 octet, mỗi octet có 8 bit.
- ✦ Nó xác định bit nào trong địa chỉ IP sẽ được bỏ qua hay kiểm tra:
 - ✦ Bit '1' trong có nghĩa là bỏ qua (ignore) vị trí bit đó khi so sánh
 - ✦ Bit '0' xác định vị trí bit phải kiểm tra.

Wildcard Masking

128	64	32	16	8	4	2	1		
↓	↓	↓	↓	↓	↓	↓	↓		
0	0	0	0	0	0	0	0	=	Match All Address Bits (Match All)
0	0	1	1	1	1	1	1	=	Ignore Last 6 Address Bits
0	0	0	0	1	1	1	1	=	Ignore Last 4 Address Bits
1	1	1	1	1	1	0	0	=	Ignore First 6 Address Bits
1	1	1	1	1	1	1	1	=	Ignore All Bits in Octet

Tính Wildcard Mask

- Tính wildcard masks khi biết subnet mask

Example 1

	2 5 5 . 2 5 5 . 2 5 5 . 2 5 5
-	2 5 5 . 2 5 5 . 2 5 5 . 0 0 0
	0 0 0 . 0 0 0 . 0 0 0 . 2 5 5

Example 2

	2 5 5 . 2 5 5 . 2 5 5 . 2 5 5
-	2 5 5 . 2 5 5 . 2 5 5 . 2 4 0
	0 0 0 . 0 0 0 . 0 0 0 . 0 1 5

Example 3

	2 5 5 . 2 5 5 . 2 5 5 . 2 5 5
-	2 5 5 . 2 5 5 . 2 5 2 . 0 0 0
	0 0 0 . 0 0 0 . 0 0 3 . 2 5 5

Ví dụ Wildcard Mask

Example 1

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.0	00000000.00000000.00000000.00000000
Result	192.168.1.1	11000000.10101000.00000001.00000001

Example 2

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	255.255.255.255	11111111.11111111.11111111.11111111
Result	0.0.0.0	00000000.00000000.00000000.00000000

Example 3

	Decimal	Binary
IP Address	192.168.1.1	11000000.10101000.00000001.00000001
Wildcard Mask	0.0.0.255	00000000.00000000.00000000.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000

Ví dụ Wildcard Mask

	Decimal	Binary
IP Address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Result Range	192.168.16.0	11000000.10101000.00010000.00000000
	to 192.168.31.255	to 11000000.10101000.00011111.11111111

Cấu hình Standard ACL

Access list number: 1 → 99 hoặc 1300 → 1999

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

Áp ACL:

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

Kiểm tra ACL:

```
Router# show access-lists
```

Cấu hình Extended ACL

Access list number: 100 → 199 hoặc 2000 → 2699

```
Router(config)# access-list access-list-number {permit | deny} protocol  
source source-wildcard destination  
destination-wildcard
```

Áp ACL:

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

Kiểm tra ACL:

```
Router# show access-lists
```

ACL với Wildcard Any và Host

Example 1:

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

Example 2:

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

Bài tập ACL

Bài 1:

```
Router1(config)#access-list 1 deny 172.16.0.0  
0.15.255.255
```

```
Router1(config)#access-list 1 permit any
```

Bài 2:

```
Router2(config)#access-list 2 deny 172.16.32.0  
0.0.15.255
```

```
Router2(config)#access-list 2 permit any
```

NAT - NETWORK ADDRESS TRANSLATION

Mục tiêu:

- Hiểu khái niệm NAT
- Biết cách cấu hình Static NAT
- Biết cách cấu hình Dynamic NAT, PAT

Nội dung

- Khái niệm NAT
- Phân loại NAT
- Static NAT
- Dynamic NAT
- Port Address Translation (PAT)

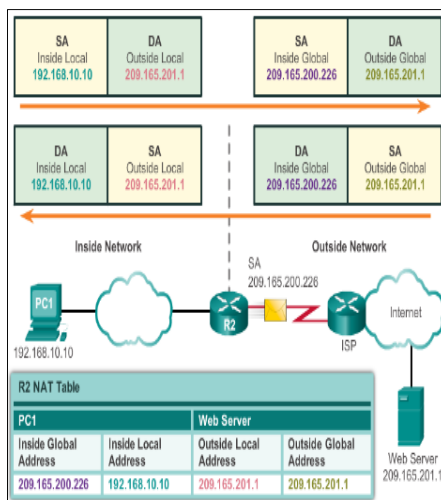
NAT Network Address Translation

□ IPv4 Private Address:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

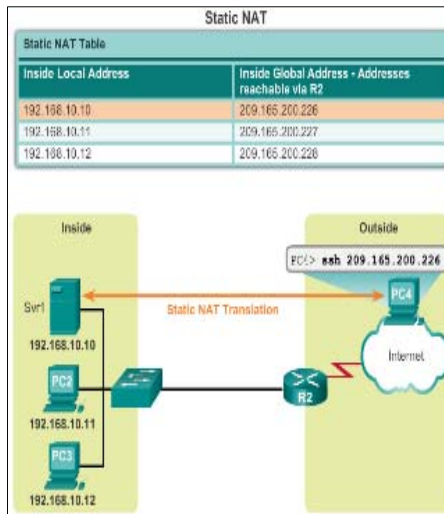
□ NAT là gì?

- NAT là cơ chế chuyển đổi địa chỉ IP private sang địa chỉ IP public để định tuyến ra Internet
- Cấu hình NAT ở router biên.



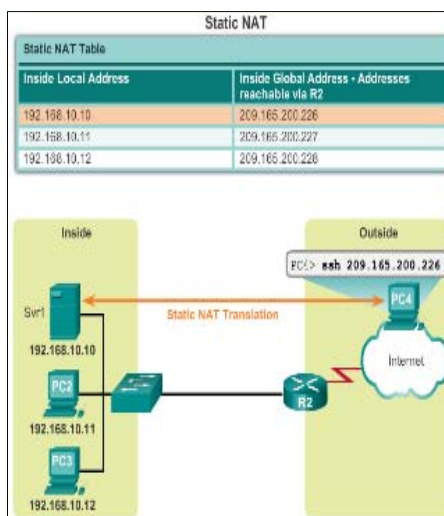
Static NAT

- ❑ Ánh xạ One-to-One giữa 1 địa chỉ private và 1 địa chỉ public
- ❑ Cấu hình bởi network administrator
- ❑ Sử dụng vĩnh viễn



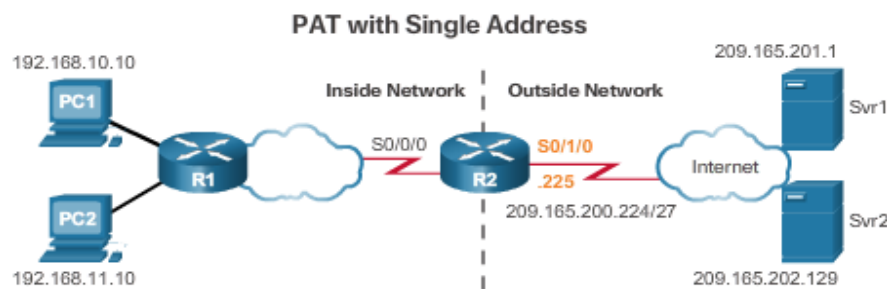
Dynamic NAT

- ❑ Ánh xạ một địa chỉ IP private này sang một địa chỉ public khác một cách tự động
- ❑ Sử dụng 1 dải các địa chỉ public
- ❑ Bất kỳ một địa chỉ IP nào nằm trong dải địa chỉ IP public đều có thể được gán cho một host trong mạng private.



PAT- Port Address Translation

- Ánh xạ nhiều địa chỉ IP private này sang một hoặc một vài địa chỉ public
- Còn được gọi là NAT overload
- Sử dụng port number để chuyển packet.



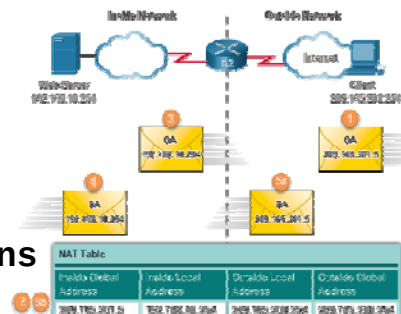
Cấu hình NAT

- Cấu hình NAT
`ip nat inside source static local-ip global-ip`

- Định nghĩa

- ip nat inside
- ip nat outside

- Kiểm tra
`show ip nat translations`



Cấu hình Dynamic NAT

■ Ánh xạ

```
ip nat pool name start-ip end-ip {netmask  
netmask | prefix-length prefix-length}
```

■ Tạo ACL

```
access-list access-list-number permit  
source [source-wildcard]
```

■ Gán ACL tới pool

```
ip nat inside source list access-list-  
number pool name
```

■ Định nghĩa

- **ip nat inside**
- **ip nat outside**

Cấu hình PAT: Single Address

□ Cấu hình PAT: Single Address

■ Định nghĩa standard ACL để permit các địa chỉ sẽ được chuyển đổi

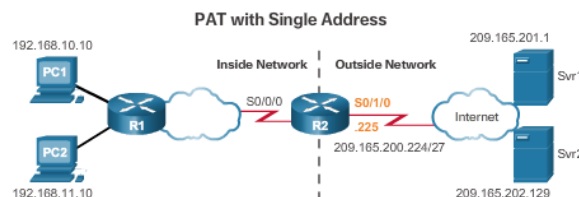
```
access-list access-list-number permit source  
[source-wildcard]
```

■ Thiết lập NAT, chỉ rõ ACL, exit interface, và overload option

```
ip nat inside source list access-list-number  
interface type name overload
```

■ Xác định inside và outside interfaces

- **ip nat inside**
- **ip nat outside**



Bài tập cấu hình NAT

- ▣ Lab1: “Configuring Static NAT”
- ▣ Lab2: “Configuring Dynamic NAT”