



Trung Tâm Đào Tạo Quản Trị Mạng & An Ninh Mạng Quốc Tế **ATHENA**

+ 92 Nguyễn Đình Chiểu, P. Đa Kao, Q. 1 Tel: (08) 2210 3801 - 0943 23 00 99

+ 2 Bis Đinh Tiên Hoàng, P. Đa Kao, Q. 1 Tel: (08) 38 244 041 - 0943 20 00 88

Website: www.athena.edu.vn _ Email: training@athenavn.com

TÀI LIỆU CCNA – THỰC HÀNH CẤU HÌNH ROUTING TRÊN GNS3

MỤC LỤC

I.	TỔNG QUAN VỀ PHẦN MỀM MÔ PHỎNG GNS3	5
1.	GIỚI THIỆU	5
2.	CÀI ĐẶT GNS3.....	5
3.	CẤU HÌNH GNS3 & CÀI ĐẶT IOS CHO GNS3.....	11
4.	KẾT NỐI GNS3 VỚI MẠNG THẬT & VMWARE	15
II.	GIỚI THIỆU VỀ ROUTER & MỘT SỐ CẤU HÌNH CƠ BẢN	18
1.	PHẦN MỀM HỆ ĐIỀU HÀNH CISCO IOS	18
1.1.	Mục đích của phần mềm Cisco IOS.....	18
1.2.	Giao diện người dùng của router	18
2.	CÁC CHẾ ĐỘ CẤU HÌNH ROUTER	18
2.1.	Phím trợ giúp trong router CLI.....	21
2.2.	Mở rộng thêm về cách viết câu lệnh.....	22
2.3.	Xử lý lỗi câu lệnh.....	23
3.	CẤU HÌNH ROUTER	24
3.1.	Chế độ giao tiếp dòng lệnh CLI.....	25
3.2.	Đặt tên cho router	25
3.3.	Đặt mật mã cho router.....	26
3.4.	Cấu hình cổng serial.....	28
3.5.	Thực hiện việc thêm bớt, dịch chuyển và thay đổi tập tin cấu hình	29
3.6.	Cấu hình cổng Ethernet.....	30
3.7.	Hoàn chỉnh cấu hình router	31
3.	ĐỊNH TUYẾN VÀ CÁC GIAO THỨC ĐỊNH TUYẾN.....	33
	GIỚI THIỆU	34
1.	TỔNG QUAN VỀ ĐỊNH TUYẾN VÀ ĐỊNH TUYẾN TĨNH.....	34
1.1.	Giới thiệu về giao thức định tuyến tĩnh	34
1.2.	Hoạt động của định tuyến tĩnh.....	34
1.3.	Cấu hình định tuyến tĩnh.....	35
1.4.	Cấu hình đường cố định	36

2.	TỔNG QUAN VỀ ĐỊNH TUYẾN ĐỘNG.....	37
2.1.	Giới thiệu về giao thức định tuyến động.....	37
2.2.	Autonomous system(AS) (Hệ thống tự quản)	37
2.3.	Mục đích của giao thức định tuyến và hệ thống tự quản	38
3.	PHÂN LOẠI CÁC LOẠI ĐỊNH TUYẾN	38
3.1.	Định tuyến theo vectơ khoảng cách	39
3.2.	Tổng quát về giao thức định tuyến.....	45
4.	TỔNG QUAN VỀ GIAO THỨC ĐỊNH TUYẾN RIP.....	46
4.1.	Giới thiệu giao thức RIP	46
4.2.	Tiến trình của RIP	47
4.3.	So sánh RIPv1 và RIPv2.....	47
4.4.	Cấu hình RIPv2.....	48
4.5.	Kiểm tra cấu hình RIP	51
4.6.	Xử lý sự cố về hoạt động cập nhật của RIP	52
4.7.	Ngăn không cho router gửi thông tin định tuyến ra một cổng giao tiếp	53
4.8.	Load Balancing trong RIPv2.....	54
4.9.	Chia tải cho nhiều đường.....	55
5.	TỔNG QUAN VỀ GIAO THỨC ĐỊNH TUYẾN OSPF	56
5.1.	Giới thiệu về giao thức OSPF	56
5.2.	Cơ chế hoạt động của OSPF	57
5.3.	Cấu hình tiến trình định tuyến OSPF.....	58
5.4.	Cấu hình địa chỉ loopback cho OSPF và quyền ưu tiên cho router.....	59
5.5.	Thay đổi giá trị chi phí và Load Balancing trong OSPF.....	61
5.6.	Cấu hình quá trình xác minh cho OSPF.	62
5.7.	Cấu hình các thông số thời gian của OSPF	64
5.8.	OSPF thực hiện quảng bá đường mặc định	65
5.9.	Những lỗi thường gặp trong cấu hình OSPF.....	65
5.10.	Kiểm tra cấu hình OSPF	66
6.	TỔNG QUAN VỀ GIAO THỨC EIGRP	67
6.1.	Giới thiệu	67
6.3.	Cấu hình định tuyến EIGRP	69

6.4.	Cấu hình xác thực EIGRP	71
6.5.	Load Balancing trong EIGRP	72
6.6.	Kiểm tra hoạt động của EIGRP	72
7.	SNIFFER TRONG MẠNG CISCO VÀ CÁCH PHÒNG CHỐNG	75
7.1.	Khái niệm Sniffer	75
7.2.	Mục đích sử dụng	76
7.3.	Các giao thức có thể sử dụng Sniffing	76
7.4.	Phương thức hoạt động Sniffer	76
7.4.1.	Active	77
7.4.2.	Passive	77
7.5.	Các kiểu tấn công	77
7.6.	Phòng chống sniffer	78
1.	SMB/CIFS	78
2.	Keberos:	79
3.	Stanford SRP (Secure Remote Password):	79
4.	OpenSSH	79
5.	VPNs (Virtual Private Network)	79
6.	Static ARP Table	79
7.	Quản lý port console trên Switch	80
8.	Port Security	80



Trung Tâm Đào Tạo Quản Trị Mạng & An Ninh Mạng Quốc Tế **ATHENA**
+ 92 Nguyễn Đình Chiểu, P. Đa Kao, Q. 1 Tel: (08) 2210 3801 - 0943 23 00 99
+ 2 Bis Đinh Tiên Hoàng, P. Đa Kao, Q. 1 Tel: (08) 38 244 041 - 0943 20 00 88
Website: www.athena.edu.vn Email: training@athenavn.com

I. TỔNG QUAN VỀ PHẦN MỀM MÔ PHỎNG GNS3

1. GIỚI THIỆU

GNS3 là 1 chương trình giả lập mạng có giao diện đồ họa cho phép chúng ta có thể giả lập các Cisco router sử dụng IOS thật ,ngoài ra còn có ATM/Frame Relay/Ethernet Switch ,Pix Firewall thậm chí kết nối vào hệ thống mạng thật

GNS3 được phát triển dựa trên Dynamips và Dynagen để mô phỏng các dòng router 1700,2600,3600,3700,7200 có thể sử dụng để triển khai các bài lab của CCNA,CCNP,CCIE nhưng hiện tại vẫn chưa mô phỏng được Catalyst Switch (mặc dù có thể giả lập NM-16ESW trên router 3700 chạy IOS 3725)

2. CÀI ĐẶT GNS3

GNS3 có thể chạy trên Windows,Linux và Mac OSX.Để cài đặt phần mềm trên Window dễ dàng chúng ta có thể sử dụng bộ cài đặt all-in-one cung cấp mọi thứ chúng ta cần để chạy được GNS3.

Chúng ta có thể download GNS3 bản mới nhất tại <http://www.gns3.net/download>

Home News Dynamips Labs Documentation Videos Screenshots Team Forum Switching Appliances Download

Download

Below you can download GNS3, a network simulator for making labs or topologies of routers (IOS, JunOS), firewalls (ASA, PIX) and hosts. It is particularly useful for training to Cisco certifications (CCNA, CCNP, CCIP, CCSP, CCVP or CCIE) or Juniper certifications (JNCIA, JNCIS or JNCIE). Thanks to VirtualBox integration, now even system engineers and administrators can take advantage of GNS3 to study Redhat (RHCE, RHCT), Microsoft (MSCE, MSCA), Novell (CLP) and many other vendor certifications.

Free IPv6 Certification

IPv6.HE.net

Get started in minutes! Become an IPv6 Guru



AdChoices

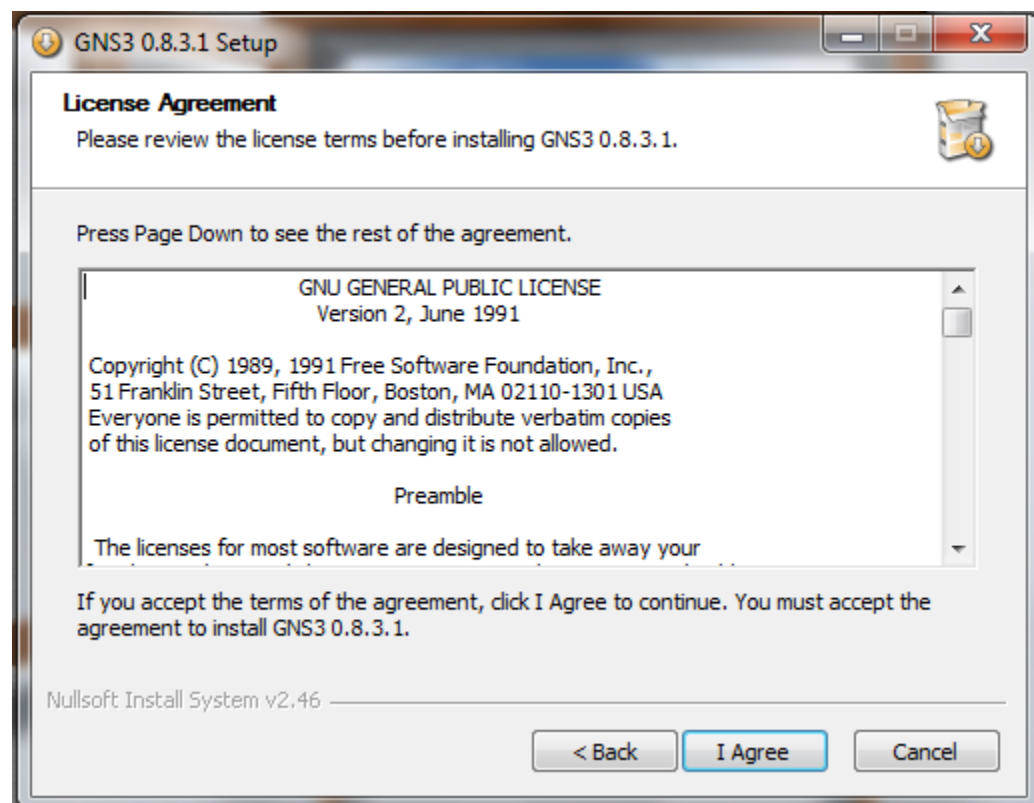
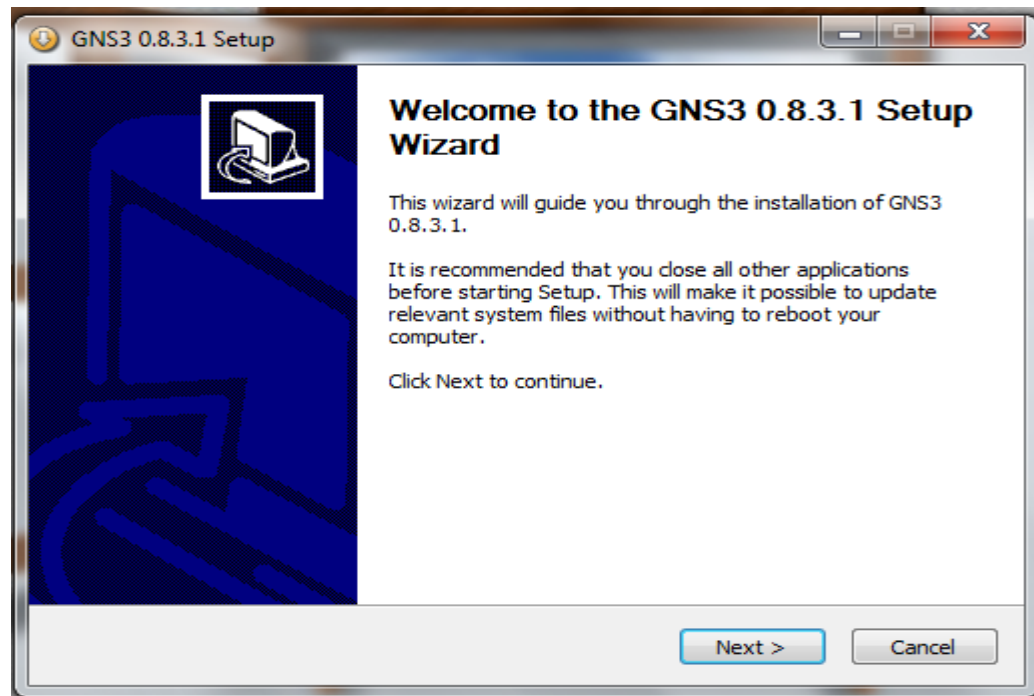
GNS3 0.8.4 Release Candidate 2 is out. Stable version is still 0.8.3.1 (see below).

Windows

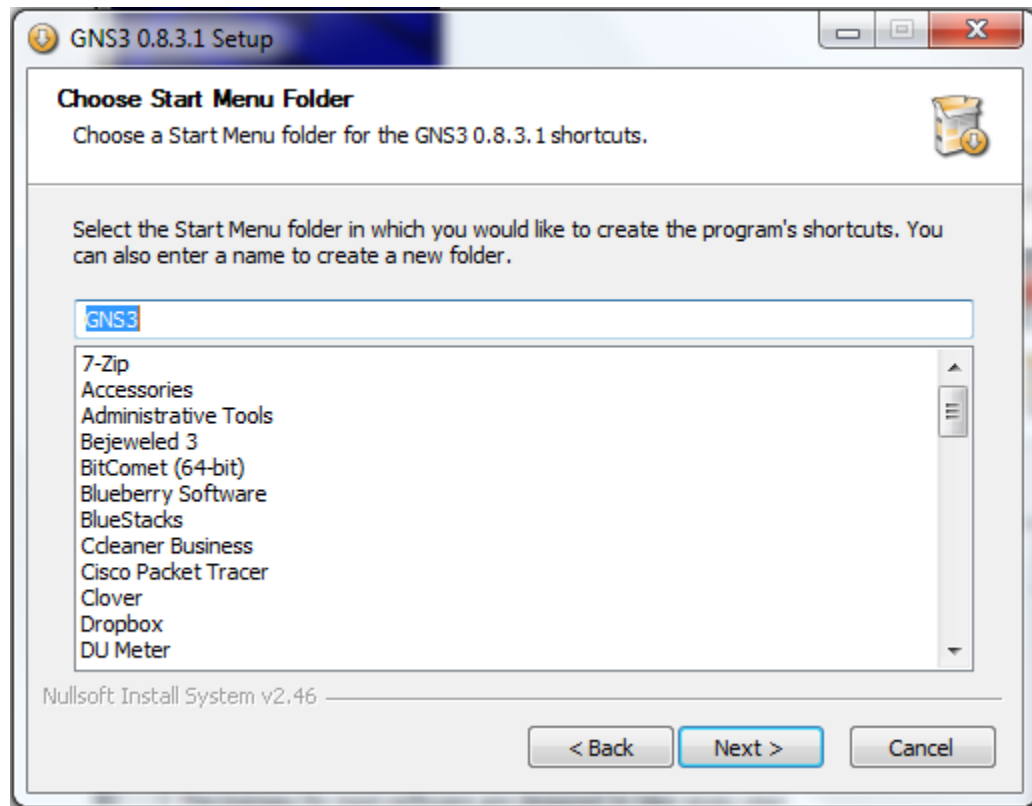
New users to GNS3, it is recommended to download the all-in-one package below.

- [GNS3 v0.8.3.1 all-in-one](#) (installer which includes Dynamips, Qemu/Pemu, Putty, VPCS, WinPCAP and Wireshark)
- [GNS3 v0.8.3.1 standalone 32-bit](#) (archive that includes Dynamips, Qemu/Pemu, Putty, VPCS)
- [GNS3 v0.8.3.1 standalone 64-bit](#) (Windows 64-bit only, archive that includes Dynamips, Qemu/Pemu, Putty, VPCS)

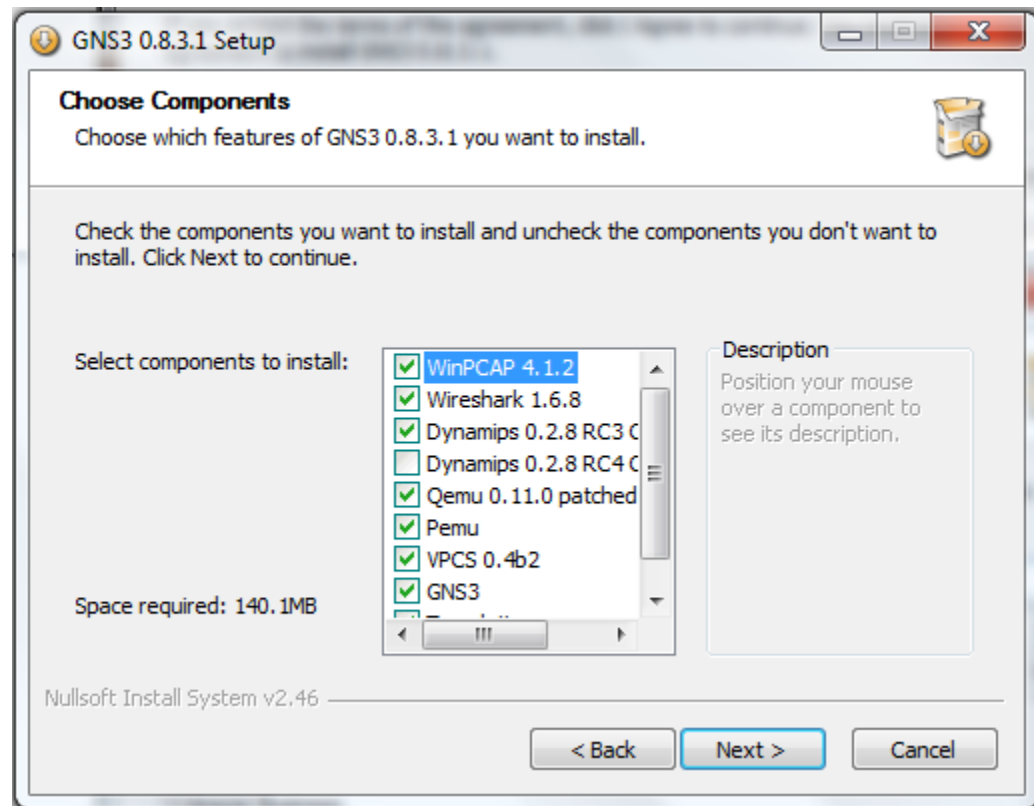
Sau khi tải phần mềm về chúng ta bắt đầu tiến hành cài đặt: Chọn GNS3-0.8.3.1-win32-all-in-one.exe



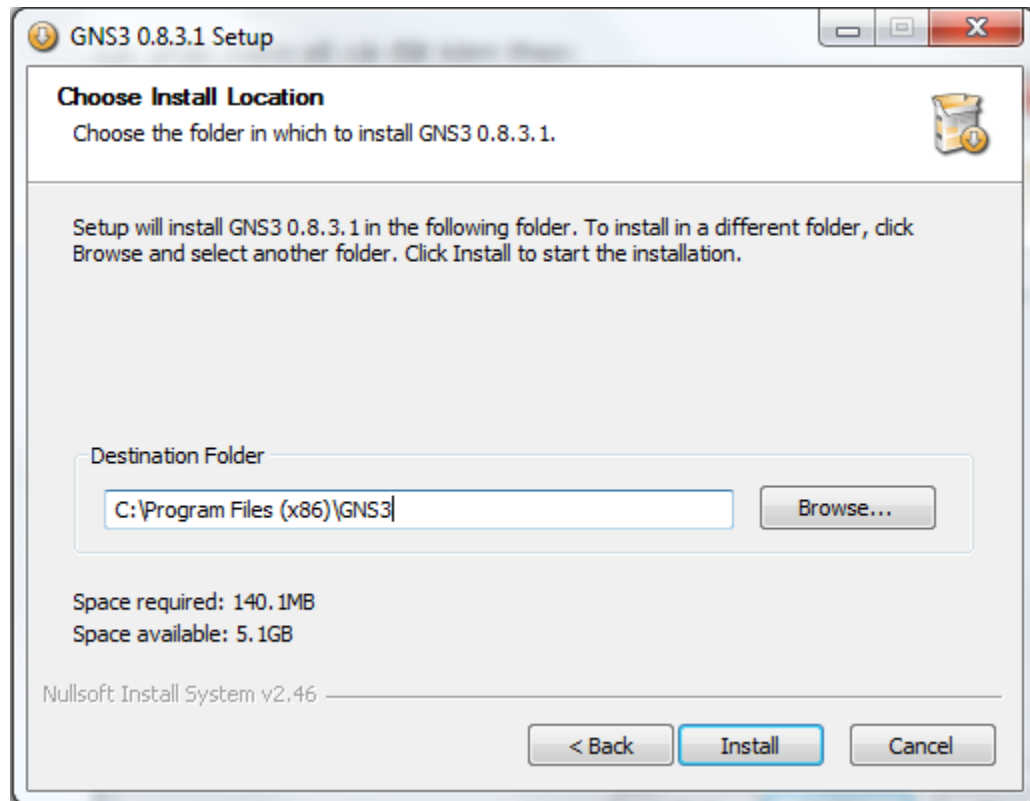
Chọn I Agree để đồng ý với các điều khoản và tiếp tục cài đặt.



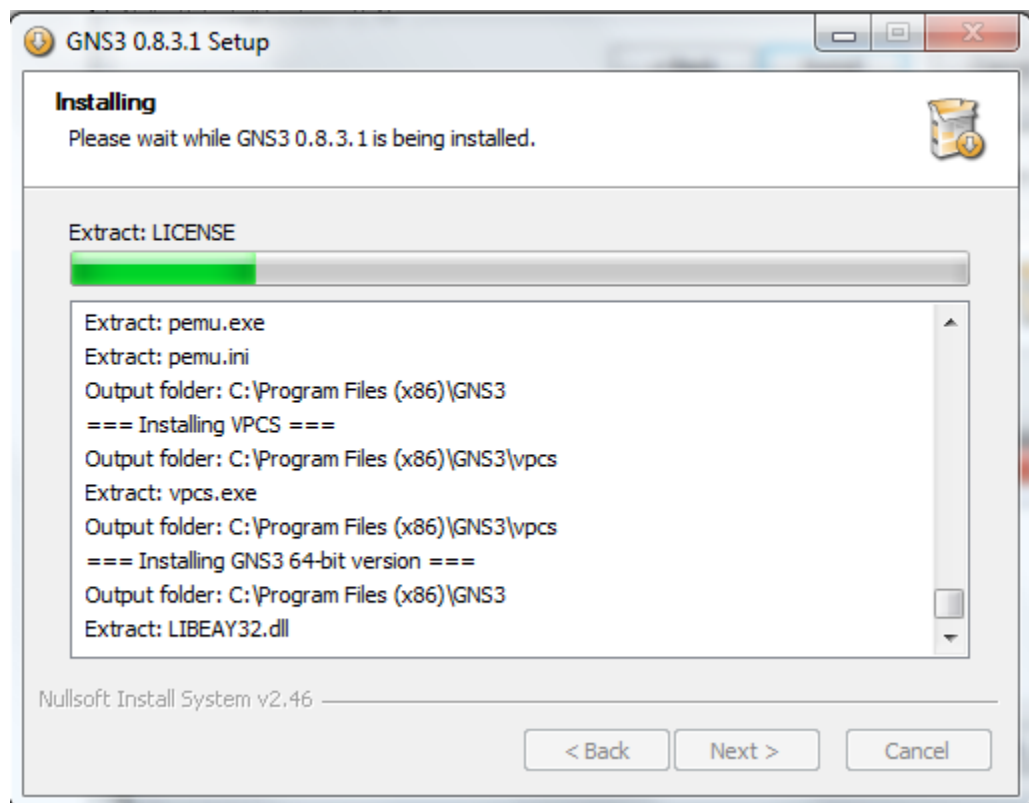
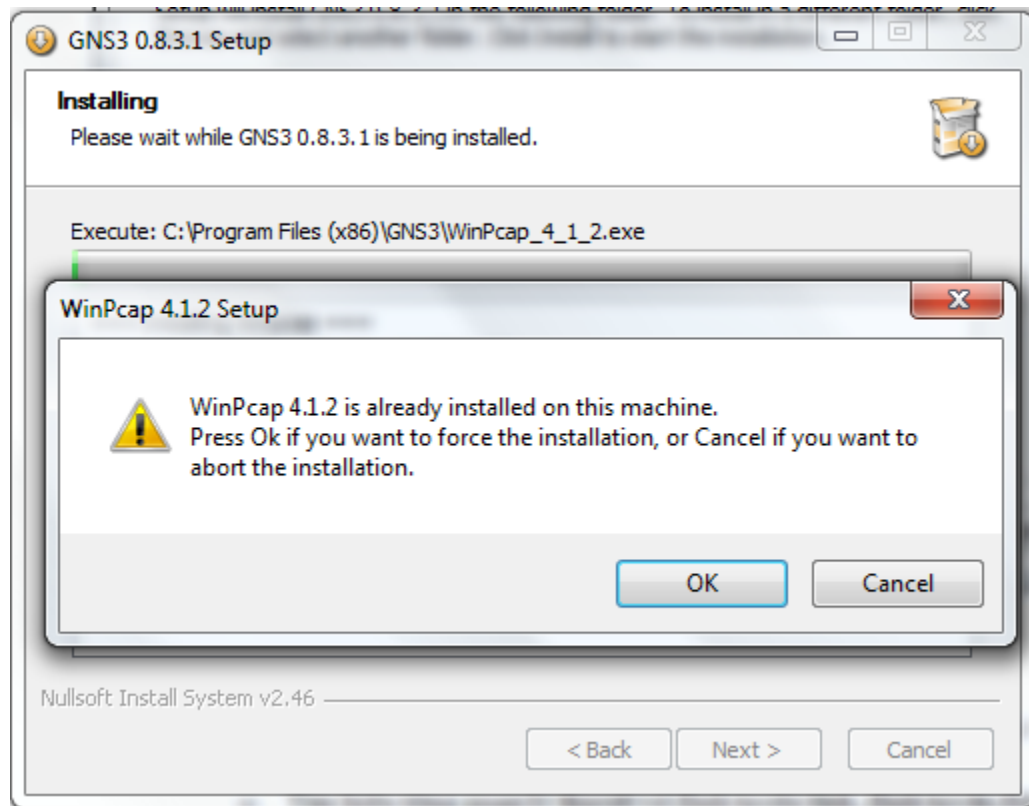
Chọn tên để tạo nên thư mục mới trên program's shortcuts -> nhấn Next >



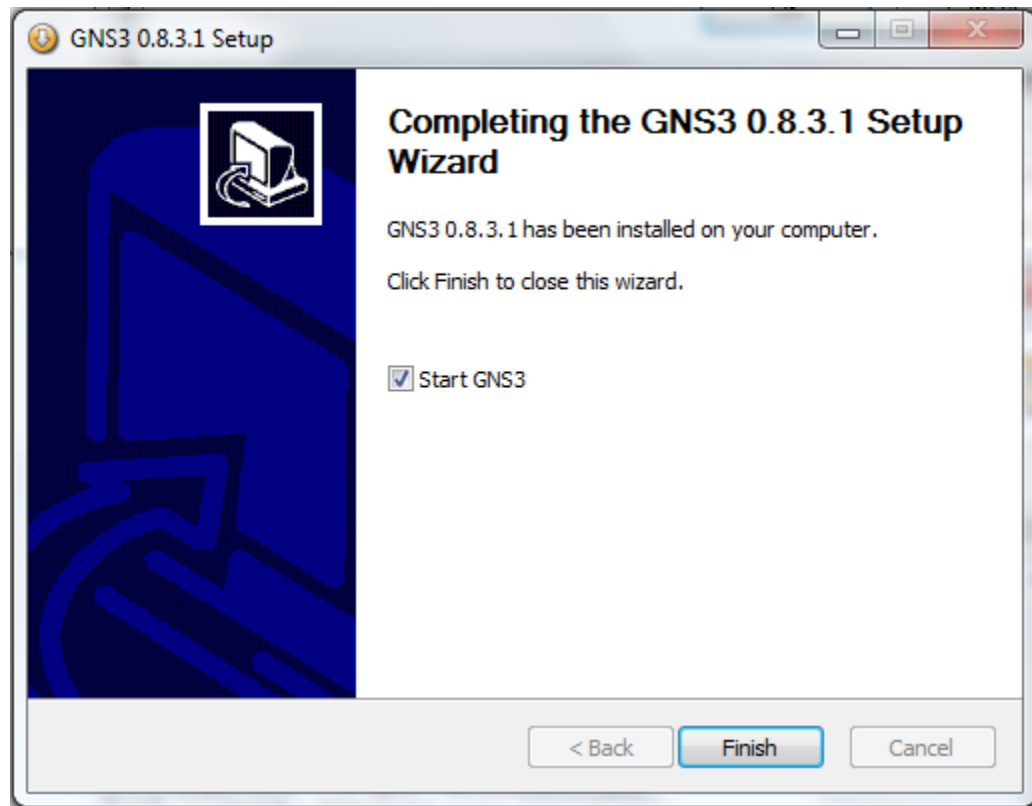
Chọn để cài đặt thêm các phần mềm bổ trợ đi kèm với GNS3 -> nhấn Next >



Chọn đường dẫn phân vùng để cài đặt phần mềm -> nhấn Install để tiến hành cài đặt.



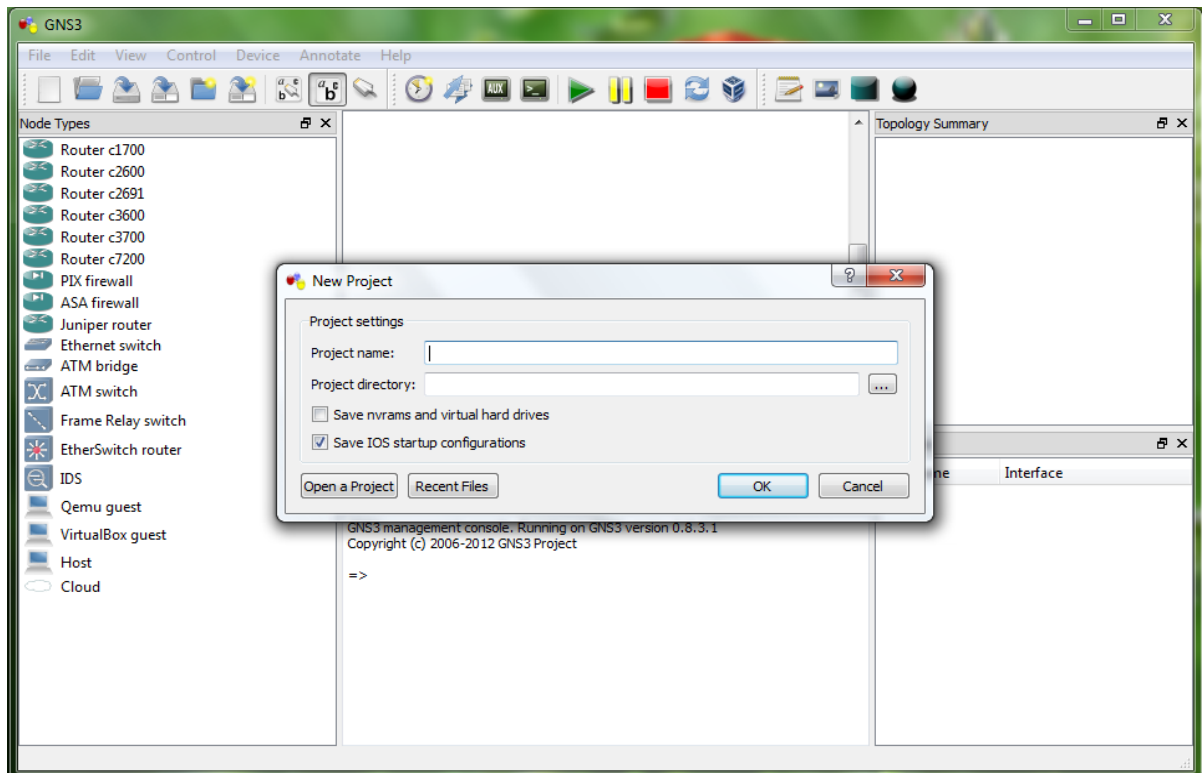
Quá trình cài đặt phần mềm...



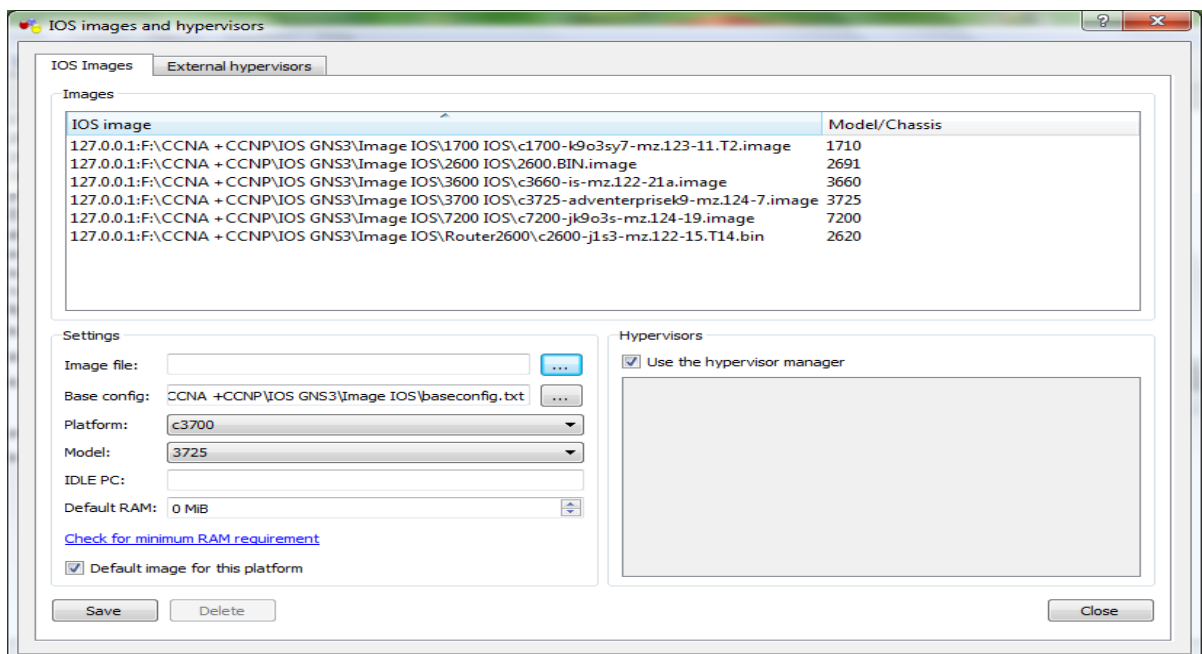
Cài đặt thành công GNS3 trên windows.

3. CẤU HÌNH GNS3 & CÀI ĐẶT IOS CHO GNS3

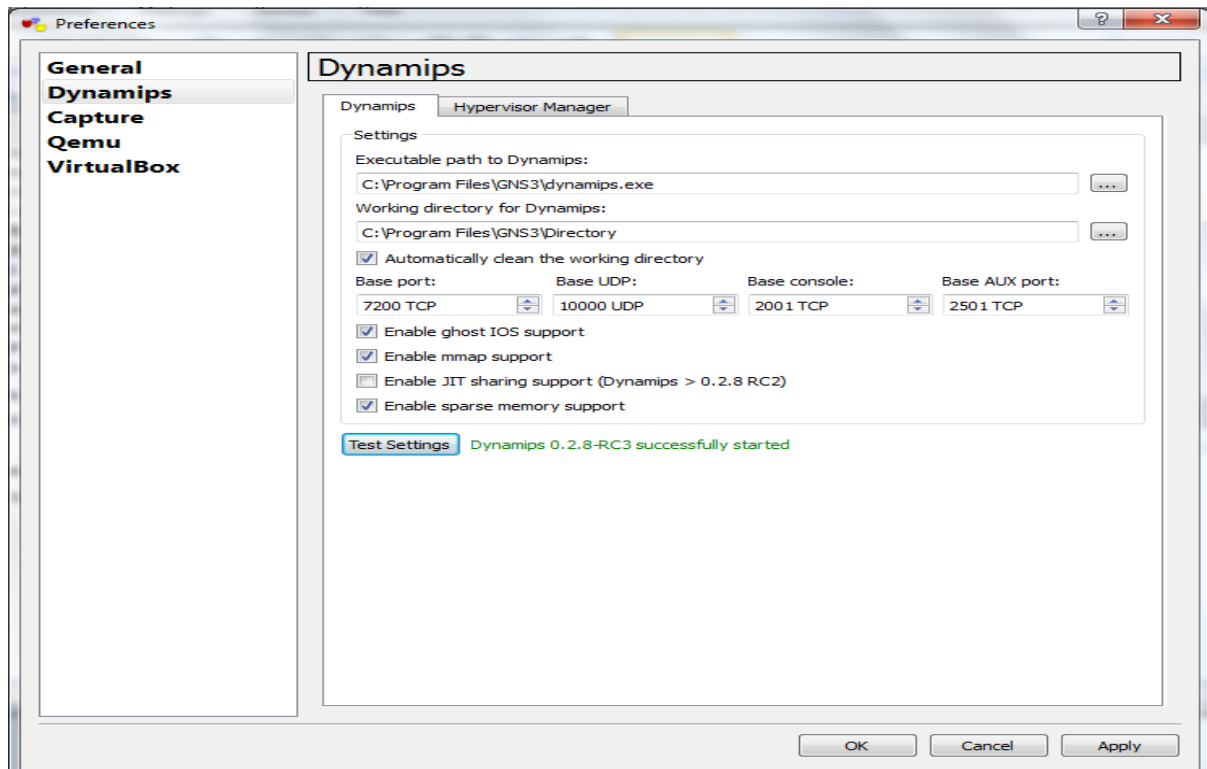
Giao diện sử dụng phần mềm GNS3



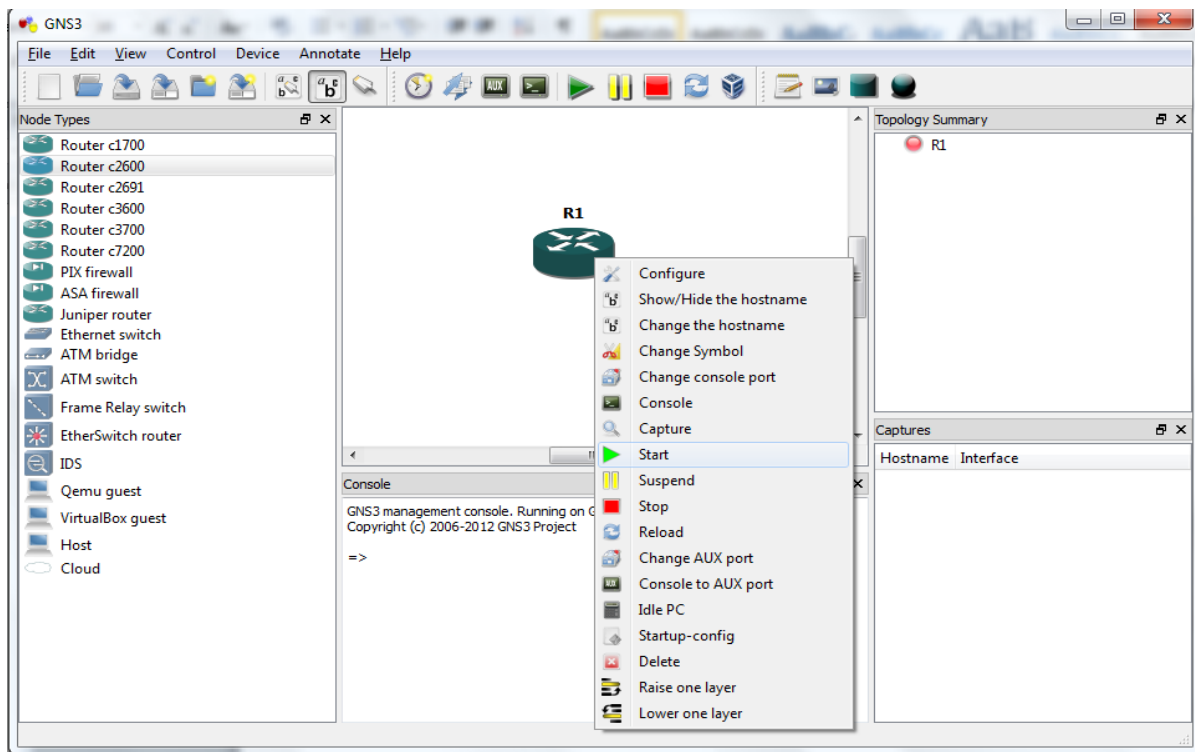
Vào Edit > Add IOS images and hypervisors chỉ đường dẫn đến các file IOS trong mục Setting



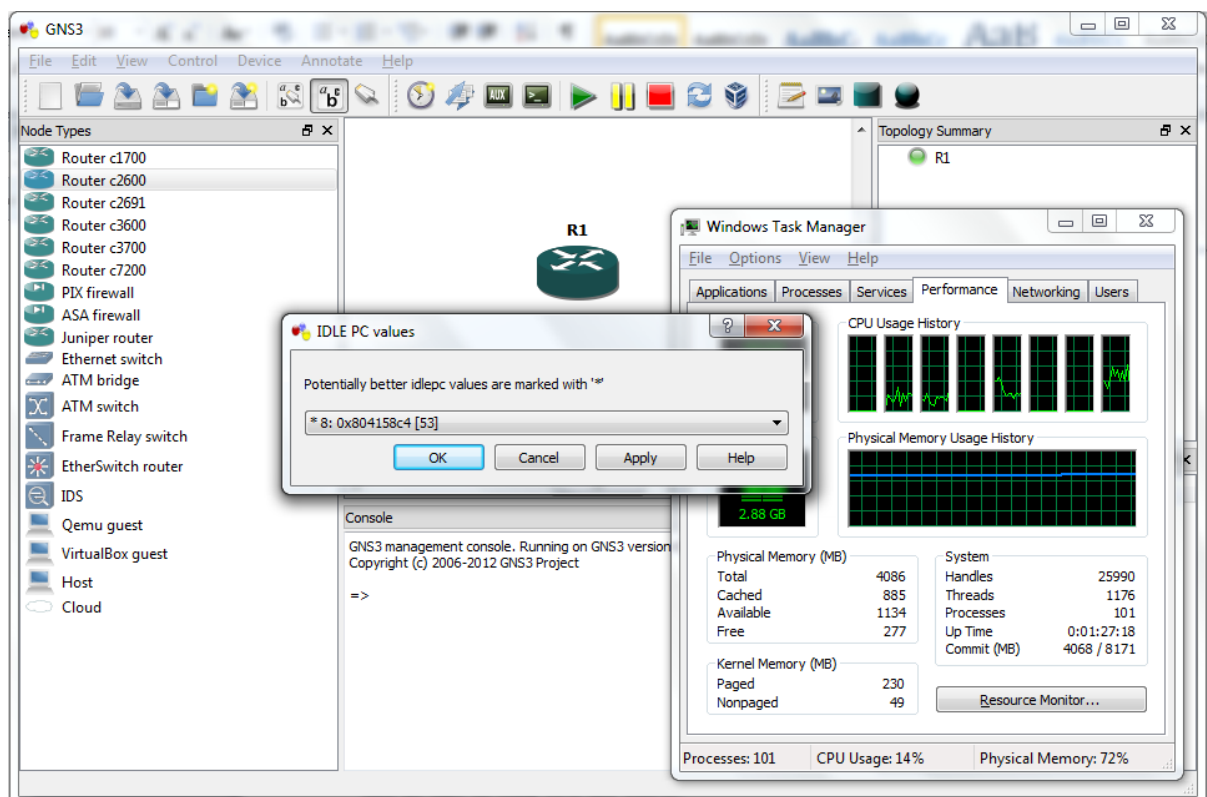
Sau khi chọn xong các IOS theo model các loại router thì nhấn Save để lưu cấu hình lại.



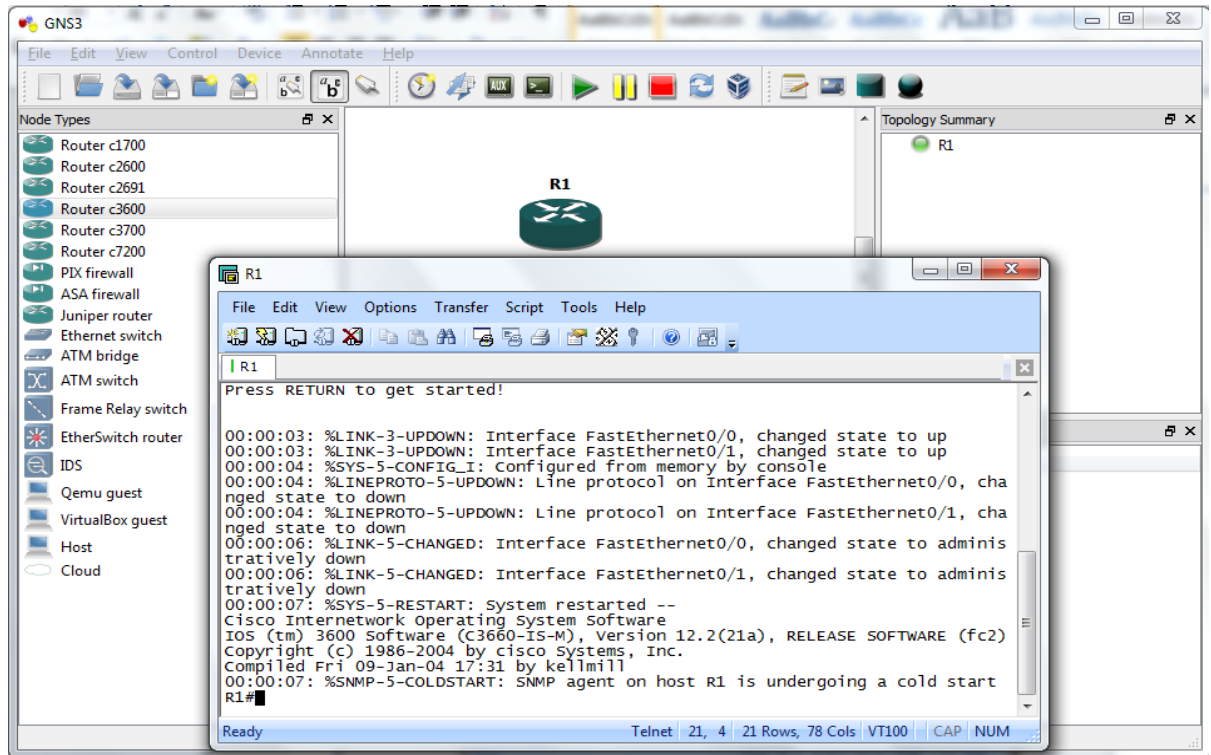
Vào Edit > Preferences > Dynamips > Trong mục Executable Path chọn đường dẫn đến tập tin dynamips.exe trong thư mục cài đặt GNS3 , sau đó bấm vào nút Test để kiểm tra lại hoạt động của Dynamip.



Thử chạy một router 2600 khi cấu hình xong GNS3.



Sau khi khởi chạy router thì chúng ta nhận thấy CPU lên tới 100%, Chúng ta sẽ điều chỉnh trong Idle PC. Chọn dòng có dấu * là tốt nhất.

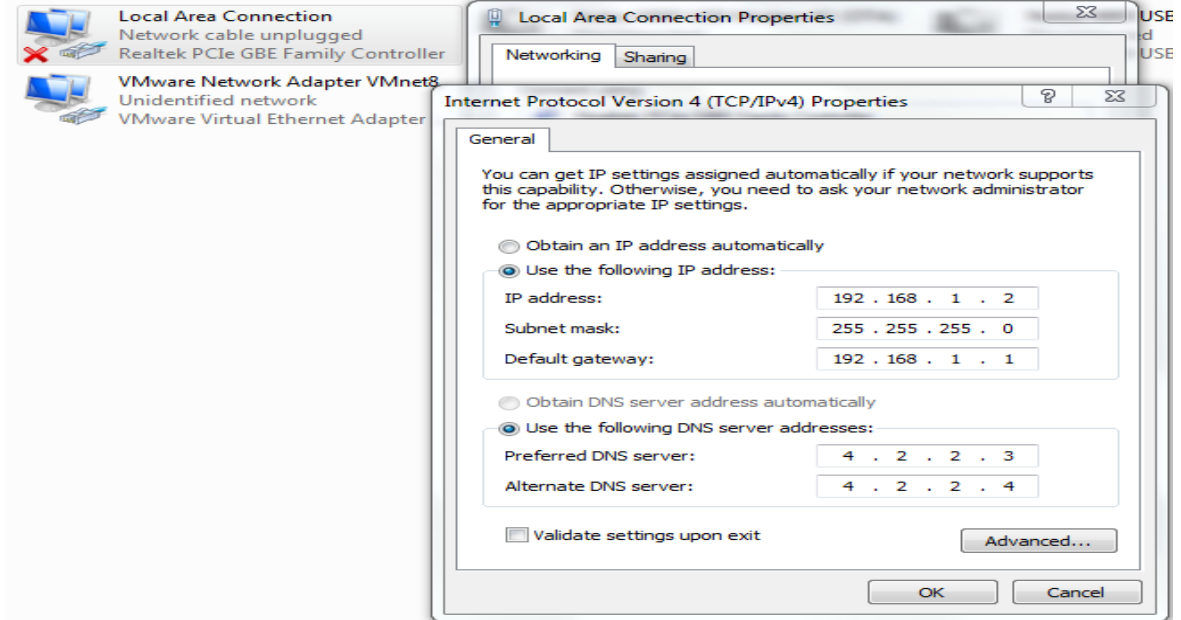


Kết nối router với màn hình CLI để bắt đầu cấu hình.

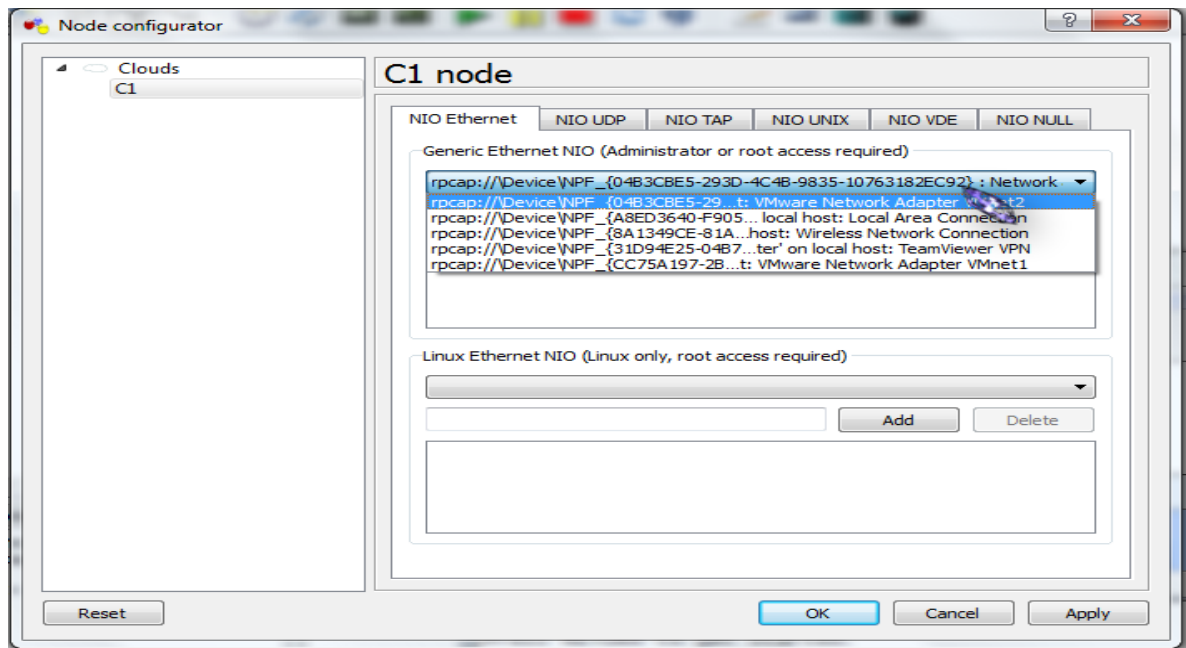
4. KẾT NỐI GNS3 VỚI MẠNG THẬT & VMWARE

GNS3 thông qua việc sử dụng Dynamips có thể tạo cầu nối giữa interface trên router ảo với interface trên máy thật, cho phép mạng ảo giao tiếp được với mạng thật, Trên hệ thống Windows, thư viện Wincap được sử dụng để tạo kết nối này.

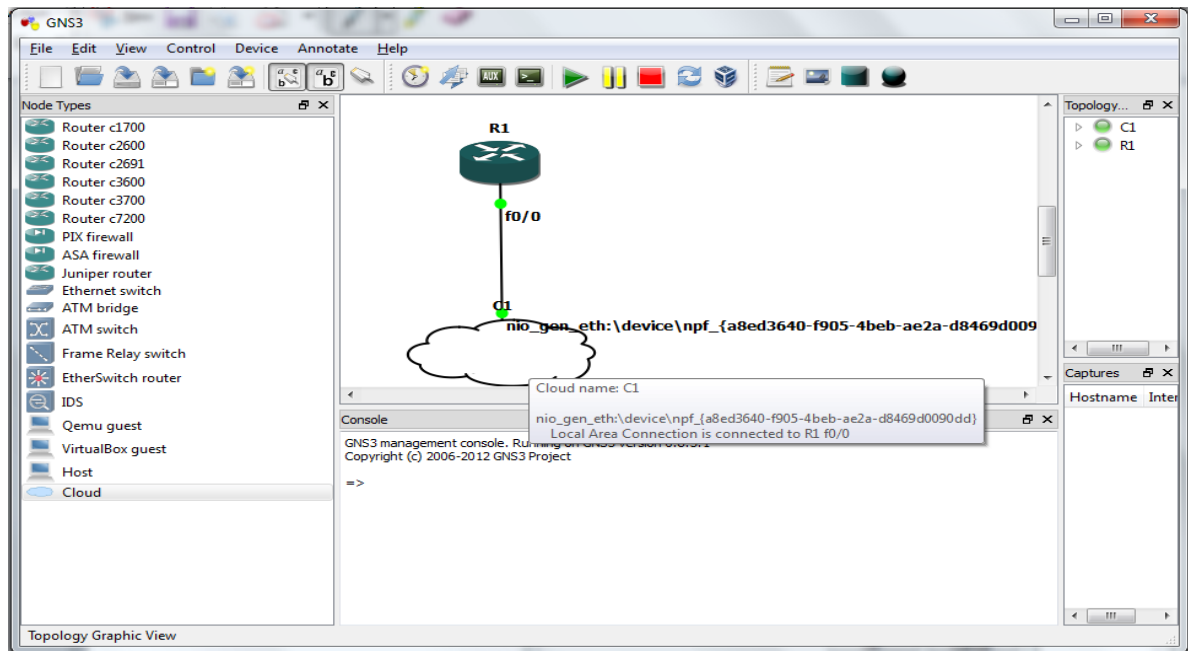
Để kết nối các router ảo trong GNS3 với hệ thống mạng thật ta dùng thiết bị “Cloud”, giả sử ta cần kết nối từ router ảo đến card mạng tên là “Local Area Connection” có địa chỉ là 192.168.1.2



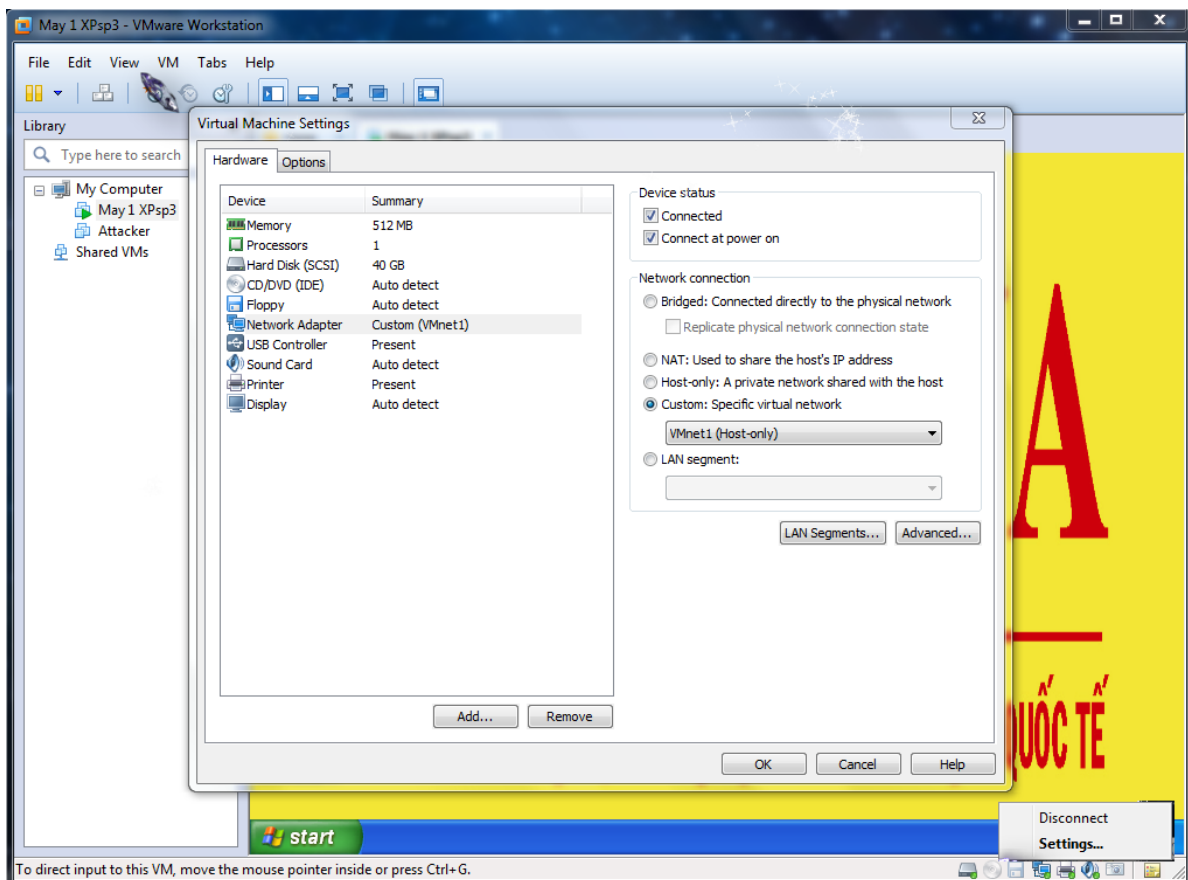
Cấu hình IP trên card máy thật.



Add card mạng thật Local Area Connection vào Cloud hoặc card ảo Vmware



Thực hiện kết nối trên GNS3 giữa router với Cloud.



Cài đặt card mạng tương ứng cho máy ảo trên Vmware.

II. GIỚI THIỆU VỀ ROUTER & MỘT SỐ CẤU HÌNH CƠ BẢN

Các kỹ thuật của Cisco đều được xây dựng dựa trên hệ điều hành mạng Cisco (IOS). Phần mềm IOS điều khiển quá trình định tuyến và chuyển mạch trên các thiết bị kết nối liên mạng. Do đó người quản trị mạng phải nắm vững về IOS.

Trong chương này, em sẽ giới thiệu cơ bản và khảo sát các đặc điểm của IOS. Tất cả các công việc cấu hình mạng từ đơn giản nhất đến phức tạp nhất đều dựa trên một nền tảng cơ bản là cấu hình router. Do đó trong chương này cũng giới thiệu về các kỹ thuật và công cụ cơ bản để cấu hình router mà chúng ta sẽ sử dụng trong hệ thống mạng Cisco.

1. PHẦN MỀM HỆ ĐIỀU HÀNH CISCO IOS

1.1. Mục đích của phần mềm Cisco IOS

Tương tự như máy tính, router và switch không thể hoạt động được nếu không có hệ điều hành. Cisco gọi hệ điều hành của mình là hệ điều hành mạng Cisco hay gọi tắt là Cisco IOS. Hệ điều hành được cài trên các Cisco router và Catalyst Switch. Cisco IOS cung cấp các dịch vụ mạng như sau:

- Định tuyến và chuyển mạch.
- Bảo đảm và bảo mật cho việc truy cập vào tài nguyên mạng.
- Mở rộng hệ thống mạng.

1.2. Giao diện người dùng của router

Phần mềm Cisco sử dụng giao diện dòng lệnh (CLI – Command – line interface) cho môi trường console truyền thống. IOS là một kỹ thuật cơ bản, từ đó được phát triển cho nhiều dòng sản phẩm khác nhau của Cisco. Do đó hoạt động cụ thể của từng IOS sẽ rất khác nhau tùy theo từng loại thiết bị.

Chúng ta có nhiều cách khác nhau để truy cập vào giao diện CLI của router. Cách đầu tiên là kết nối trực tiếp từ máy tính hoặc thiết bị đầu cuối vào cổng console trên router. Cách thứ hai là sử dụng đường quay số qua modem hoặc kết nối null modem vào cổng AUX trên router. Cả hai cách trên đều không cần phải cấu hình trước cho router. Cách thứ ba là telnet vào router. Để thiết lập phiên telnet vào router thì trên router ít nhất phải có một cổng đã được cấu hình địa chỉ IP, các đường vty đã được cấu hình cho phép truy cập và đặt mật mã.

2. CÁC CHẾ ĐỘ CẤU HÌNH ROUTER

Giao diện dòng lệnh của Cisco sử dụng cấu trúc phân cấp. Cấu trúc này đòi hỏi chúng ta muốn cấu hình cái gì thì phải vào chế độ tương ứng. Ví dụ: nếu chúng ta muốn cấu hình cổng giao tiếp nào của router thì chúng ta phải vào chế độ cấu hình cổng giao tiếp đó. Từ chế độ này tất cả các cấu hình được nhập vào chỉ có hiệu lực đối với cổng giao tiếp tương ứng mà thôi. Tương ứng với mỗi chế độ cấu hình có một dấu nhắc đặc trưng riêng và một tập lệnh riêng. IOS có một trình thông dịch gọi là EXEC. Sau khi chúng ta nhập một câu lệnh thì EXEC sẽ thực thi ngay câu lệnh đó.

Vì lý do bảo mật nên Cisco IOS chia phiên bản làm việc của EXEC thành hai chế độ là: chế độ EXEC người dùng và chế độ EXEC đặc quyền. Sau đây là các đặc điểm của chế độ EXEC người dùng và chế độ EXEC đặc quyền:

- Chế độ EXEC người dùng chỉ cho phép thực thi một số câu lệnh hiển thị các thông tin cơ bản của router mà thôi. Chế độ này chỉ để xem chứ không cho phép thực hiện các câu lệnh làm thay đổi cấu hình router. Chế độ EXEC người dùng có dấu nhắc là “>”.
- Chế độ EXEC đặc quyền cho phép thực hiện tất cả các câu lệnh của router.

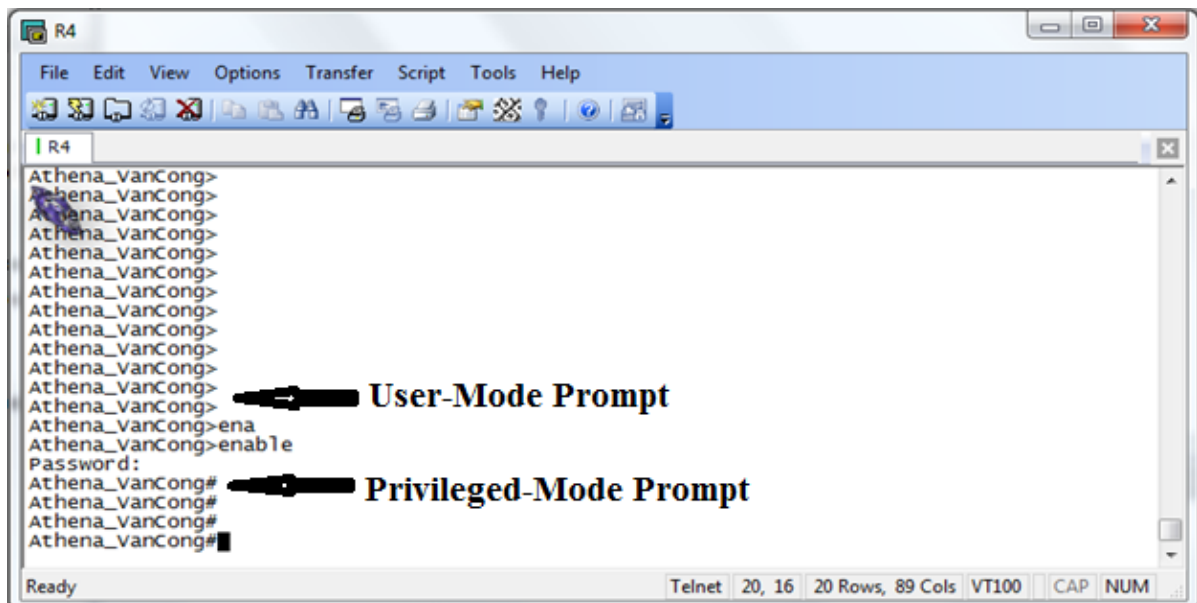
Chúng ta có thể cấu hình để người dùng phải nhập mật mã trước khi truy nhập vào chế độ này. Ngoài ra, để tăng thêm tính bảo mật chúng ta có thể cấu hình thêm userID. Điều này cho phép chỉ những người nào được phép mới có thể truy cập vào router. Người quản trị mạng phải ở chế độ EXEC đặc quyền mới có thể sử dụng các câu lệnh để cấu hình hoặc quản lý router. Từ chế độ EXEC đặc quyền chúng ta có thể chuyển vào các chế độ đặc khác nhau như chế độ cấu hình toàn cục chẳng hạn. Chế độ EXEC đặc quyền được xác định bởi dấu nhắc “#”.

Để chuyển từ chế độ EXEC người dùng sang chế độ EXEC đặc quyền hạn dùng lệnh enable tại dấu nhắc “>”. Nếu mật mã đã được cài đặt thì router sẽ yêu cầu chúng ta nhập mật mã. Vì lý do bảo mật nên các thiết bị mạng Cisco không hiển thị mật mã trong lúc chúng ta nhập chúng. Sau khi mật mã được nhập vào chính xác thì dấu nhắc “>” chuyển thành “#” cho biết chúng ta đang ở chế độ EXEC đặc quyền. Chúng ta gõ dấu chấm hỏi (?) ở dấu nhắc này thì sẽ thấy router hiển thị ra nhiều câu lệnh hơn so với ở chế độ EXEC người dùng.

Ở dấu nhắc password: chúng ta phải nhập mật mã đúng với mật mã đã được cấu hình cho router trước đó bằng lệnh enable secret hoặc enable password. Nếu mật mã của router đã được cấu hình bởi cả 2 lệnh trên thì mật mã của câu lệnh enable secret sẽ được áp dụng. Sau khi hoàn tất các bước trên chúng ta sẽ gặp dấu nhắc “#” cho biết là chúng ta đang ở chế độ EXEC đặc quyền. Từ chế độ này chúng ta mới có thể truy cập vào chế độ cấu hình toàn cục rồi sau đó là các chế độ cấu hình riêng biệt hơn như:

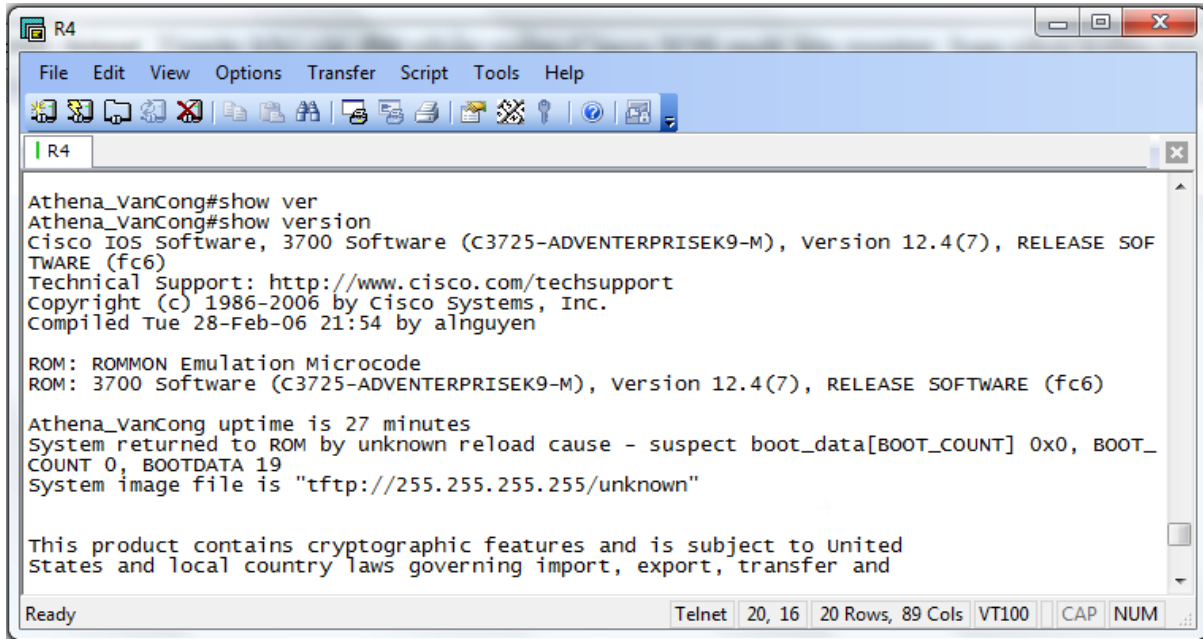
- Chế độ cấu hình cổng giao tiếp.
- Chế độ cấu hình cổng giao tiếp con.
- Chế độ cấu hình đường truy cập.
- Chế độ cấu hình router.
- Chế độ cấu hình route-map.

Từ chế độ EXEC đặc quyền, chúng ta gõ disable hoặc exit để trở về chế độ EXEC người dùng. Để trở về chế độ EXEC đặc quyền từ chế độ cấu hình toàn cục, chúng ta dùng lệnh exit hoặc Ctrl-Z. Lệnh Ctrl-Z có thể sử dụng để trở về ngay chế độ EXEC đặc quyền từ bất kỳ chế độ cấu hình riêng biệt nào.



Để xem dung lượng RAM chúng ta dùng lệnh show version:

...<output omitted>... cisco 1721 (68380) processor (revision c) with 3584k/512K bytes of memory.



```
R4
File Edit View Options Transfer Script Tools Help
R4
Athena_VanCong#show ver
Athena_VanCong#show version
Cisco IOS Software, 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(7), RELEASE SOFTWARE (fc6)
Technical support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Tue 28-Feb-06 21:54 by alnguyen

ROM: ROMMON Emulation Microcode
ROM: 3700 Software (C3725-ADVENTERPRISEK9-M), Version 12.4(7), RELEASE SOFTWARE (fc6)

Athena_VanCong uptime is 27 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0, BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and

Ready Telnet 20, 16 20 Rows, 89 Cols VT100 CAP NUM
```

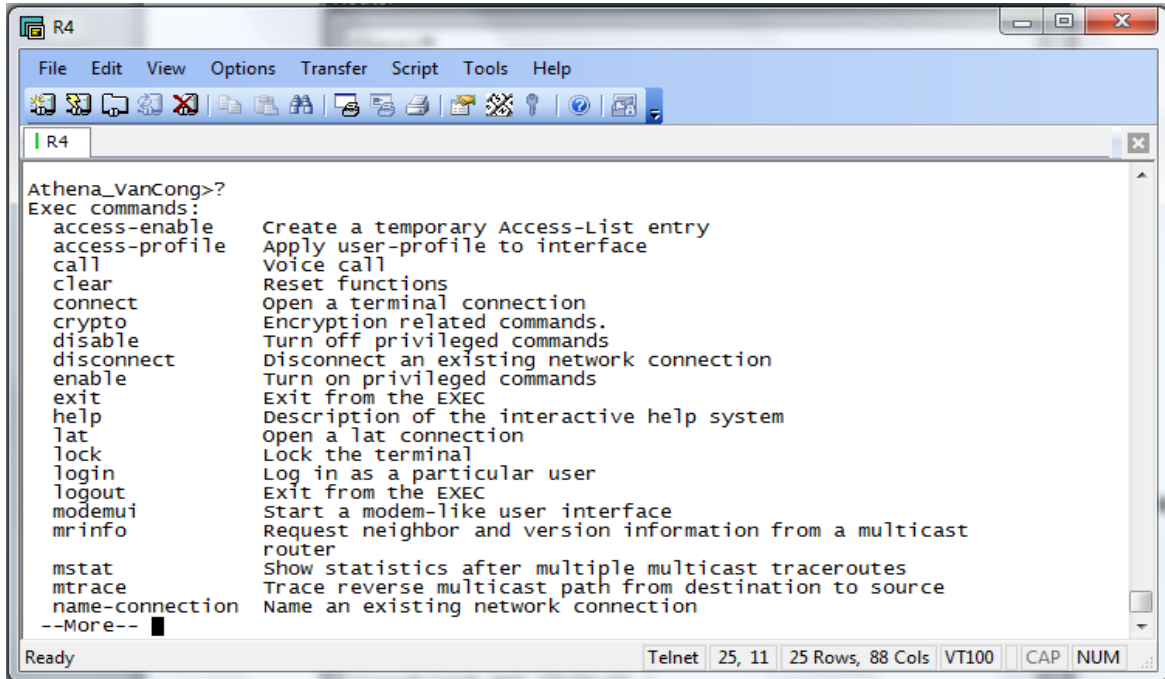
Dòng trên cho biết dung lượng của bộ nhớ chính và bộ nhớ chia sẻ trên router. Có một số thiết bị sử dụng một phần DRAM làm bộ nhớ chia sẻ. Tổng hai dung lượng trên là dung lượng thật sự của DRAM trên router.

Để xem dung lượng của bộ nhớ flash chúng ta dùng lệnh show flash: Athena_VanCong#show flash

...<output omitted>...1599897 bytes total (10889728 bytes free)

2.1. Phím trợ giúp trong router CLI

Khi chúng ta gõ dấu chấm hỏi (?) ở dấu nhắc thì router sẽ hiển thị danh sách các lệnh tương ứng với chế độ cấu hình mà chúng ta đang ở. Chữ "--More--" ở cuối màn hình cho biết là phần hiển thị vẫn còn tiếp. Để xem trang tiếp theo, chúng ta nhấn nhanh Spacebar. Còn nếu chúng ta muốn hiển thị tiếp từng dòng một thì chúng ta nhấn phím Enter hoặc Return. Chúng ta có thể nhấn từng dòng một thì chúng ta nhấn phím bất kỳ nào khác để quay trở về dấu nhắc.



```
R4
File Edit View Options Transfer Script Tools Help
R4
Athena_VanCong>?
Exec commands:
access-enable      Create a temporary Access-List entry
access-profile     Apply user-profile to interface
call               Voice call
clear              Reset functions
connect            Open a terminal connection
crypto             Encryption related commands.
disable            Turn off privileged commands
disconnect         Disconnect an existing network connection
enable             Turn on privileged commands
exit              Exit from the EXEC
help              Description of the interactive help system
lat               Open a lat connection
lock              Lock the terminal
login             Log in as a particular user
logout            Exit from the EXEC
modemui           Start a modem-like user interface
mrinfo            Request neighbor and version information from a multicast
                  router
mstat             Show statistics after multiple multicast traceroutes
mtrace            Trace reverse multicast path from destination to source
name-connection   Name an existing network connection
--More--
```

Sau khi chúng ta đã vào được chế độ EXEC đặc quyền rồi thì chúng ta gõ dấu chấm hỏi (?), chúng ta sẽ thấy là danh sách các câu lệnh dùng cho chế độ EXEC đặc quyền nhiều hơn hẳn danh sách các câu lệnh mà chúng ta thấy trong chế độ EXEC người dùng. Tuy nhiên các tập lệnh này sẽ khác nhau tùy theo cấu hình của router và tùy theo từng phiên bản phần mềm Cisco IOS.

2.2. Mở rộng thêm về cách viết câu lệnh

Trong giao diện người dùng của router, router có thể có chế độ hỗ trợ soạn thảo câu lệnh. Chúng ta có thể sử dụng các tổ hợp phím để di chuyển con trỏ trên dòng lệnh mà chúng ta đang viết khi chúng ta cần phải chỉnh sửa câu lệnh đó. Trong các phiên bản phần mềm hiện nay, chế độ hỗ trợ soạn thảo câu lệnh là hoàn toàn tự động. Tuy nhiên nếu chế độ này lên ảnh hưởng khi chúng ta biết các script thì chúng ta có thể tắt bằng lệnh `terminal no editing` trong chế độ EXEC đặc quyền.

Khi soạn thảo câu lệnh, màn hình sẽ cuộn ngang khi câu lệnh dài quá một hàng. Khi con trỏ đến hết lề phải thì dòng lệnh sẽ dịch sang trái 10 khoảng trắng. Khi đó 10 ký tự đầu tiên của câu lệnh sẽ không nhìn thấy được trên màn hình nữa. Chúng ta có thể cuộn lại để xem bằng cách nhấn `Ctrl-B` hoặc nhấn phím mũi tên (`←`) cho tới khi màn hình cuộn tới đầu câu lệnh. Hoặc chúng ta có thể nhấn `Ctrl-A` để chuyển ngay về đầu dòng lệnh.

Phím `Ctrl-Z` được sử dụng để quay trở về chế độ EXEC đặc quyền từ bất kỳ chế độ cấu hình riêng biệt nào.

Khi cấu hình router, router có lưu lại một số các lệnh chúng ta đã sử dụng. Điều này đặc biệt có ích khi chúng ta muốn lặp lại các câu lệnh dài và phức tạp. Với cơ chế này chúng ta có thể thực hiện các việc sau:

- Cài đặt kích thước vùng bộ đệm để lưu các câu lệnh đã sử dụng.
- Gọi lại các câu lệnh đã sử dụng.
- Tắt chức năng này đi.

Mặc định là router sẽ lưu lại 10 câu lệnh trong bộ đệm. Chúng ta có thể thay đổi số lượng câu lệnh mà router lưu lại bằng lệnh `terminal history size` hoặc `historysize`. Tối đa là 255 câu lệnh có thể lưu lại được.

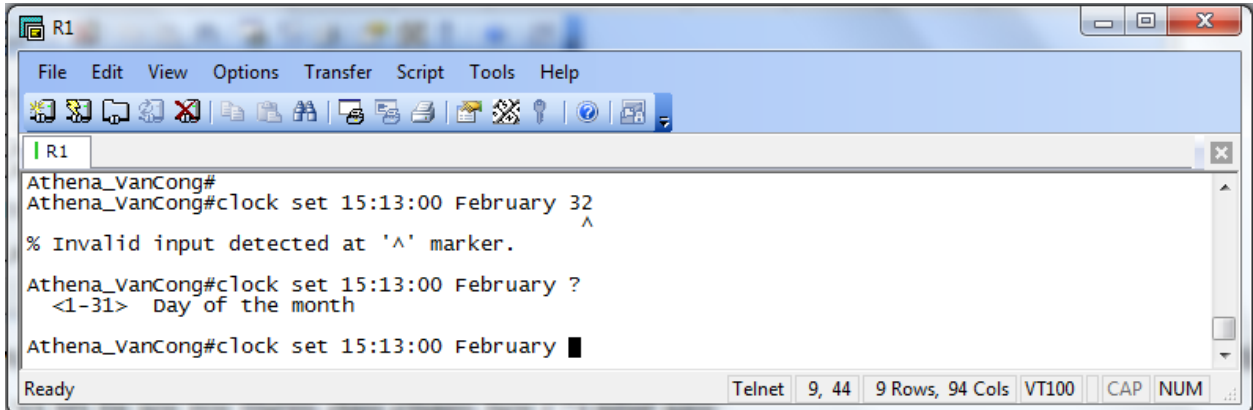
Nếu chúng ta muốn gọi lại câu lệnh vừa mới sử dụng gần nhất thì chúng ta nhấn Ctrl-P hoặc phím mũi tên (↑). Nếu chúng ta tiếp tục nhấn thì mỗi lần nhấn như vậy chúng ta sẽ gọi lại tuần tự các câu lệnh trước đó nữa. Nếu chúng ta muốn gọi lại một câu lệnh sau đó thì chúng ta nhấn Ctrl-N hoặc nhấn phím mũi tên (↓). Tương tự, nếu chúng ta tiếp tục nhấn như vậy thì mỗi lần nhấn chúng ta sẽ gọi lại một lệnh đó.

Khi gõ lệnh, chúng ta chỉ cần gõ các ký tự đủ để router phân biệt với mọi câu lệnh khác rồi nhấn phím Tab thì router sẽ tự động hoàn tất câu lệnh cho chúng ta. Khi chúng ta dùng phím Tab mà router hiển thị được đủ câu lệnh thì có nghĩa là router đã nhận biết được câu lệnh mà chúng ta muốn nhập.

Ngoài ra, hầu hết các router đều có thêm chức năng cho chúng ta đánh dấu khối và copy. Nhờ đó chúng ta có thể copy câu lệnh trước đó rồi dán hoặc chèn vào câu lệnh hiện tại.

2.3. Xử lý lỗi câu lệnh

Lỗi câu lệnh thường là do chúng ta gõ sai. Sau khi chúng ta gõ một câu lệnh bị sai thì chúng ta sẽ gặp dấu báo lỗi (^). Dấu báo lỗi (^) đặt ở vị trí mà câu lệnh bắt đầu bị sai. Dựa vào đó và vận dụng chức năng trợ giúp của hệ thống chúng ta sẽ tìm ra và chỉnh sửa lại lỗi cú pháp của câu lệnh.



```
R1
File Edit View Options Transfer Script Tools Help
Athena_VanCong#
Athena_VanCong#clock set 15:13:00 February 32
% Invalid input detected at '^' marker.
Athena_VanCong#clock set 15:13:00 February ?
<1-31> Day of the month
Athena_VanCong#clock set 15:13:00 February █
Ready Telnet 9, 44 9 Rows, 94 Cols VT100 CAP NUM
```

Trong ví dụ trên, dấu báo lỗi cho biết câu lệnh bị sai ở số 32. Chúng ta gỡ lại câu lệnh từ đầu tới vị trí bị lỗi rồi thêm dấu chấm hỏi (?) như sau:

- Athena_VanCong# clock set 13:32:00 February ?

<1-31> Day of the month

Sau đó chúng ta nhập lại câu lệnh với số năm đúng như cú pháp ở trên:

- Athena_VanCong#clock set 13:32:00 February 31

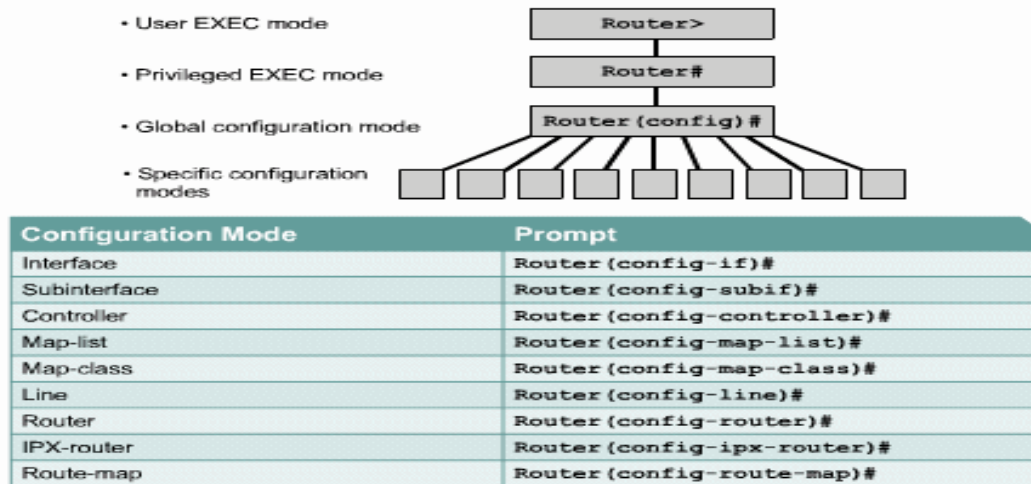
Sau khi chúng ta gõ xong câu lệnh rồi nhấn phím Enter mà câu lệnh đó bị sai thì chúng ta có thể dùng phím mũi tên (↑) để gọi câu lệnh vừa mới nhập. Sau đó chúng ta dùng các phím mũi tên sang phải, sang trái di chuyển con trỏ tới vị trí bị sai để sửa lại. Nếu cần xóa các ký tự thì chúng ta có thể dùng phím <backspace>.

3. CẤU HÌNH ROUTER

Cấu hình router để cho router thực hiện nhiều chức năng mạng phức tạp là một công việc đầy thử thách. Tuy nhiên bước bắt đầu cấu hình router thì không khó lắm. Nếu ngay từ bước này chúng ta cố gắng thực hành nhiều để làm quen và nắm vững được các bước di chuyển giữa các chế độ cấu hình của router thì công việc cấu hình phức tạp về sau sẽ trở nên đơn giản hơn rất nhiều. Trong phần này sẽ giới thiệu về các chế độ cấu hình cơ bản của router và một số lệnh cấu hình đơn giản.

Kỹ năng đọc và hiểu một cách rõ ràng các tập tin cấu hình là một kỹ năng rất quan trọng của người quản trị mạng. Cisco IOS có cung cấp một số công cụ cho người quản trị mạng để thêm một số thông tin cần thiết vào tập tin cấu hình. Cũng giống như những người lập trình phải có tài liệu của từng bước lập trình thì người quản trị mạng cũng cần được cung cấp thông tin càng nhiều càng tốt khi mà hệ thống mạng do người khác quản trị.

3.1. Chế độ giao tiếp dòng lệnh CLI



Tất cả các câu lệnh làm thay đổi cấu hình router đều xuất phát từ chế độ cấu hình toàn cục. Tùy theo ý chúng ta muốn thay đổi phần cấu hình đặc biệt nào của router thì chúng ta chuyển vào chế độ chuyên biệt tương ứng. Các chế độ cấu hình chuyên biệtnày đều là chế độ con của chế độ cấu hình toàn cục.

Các câu lệnh được sử dụng trong chế độ cấu hình toàn cục là những câu lệnh có tác động lên toàn bộ hệ thống. Chúng ta sử dụng câu lệnh sau để di chuyển vào chế độ cấu hình toàn cục:

Chú ý: Sự thay đổi của dấu nhắc cho biết chúng ta đang ở chế độ cấu hình toàn cục

- Router # configure terminal
- Router(config)#

Chế độ cấu hình toàn cục là chế độ cấu hình chính. Từ chế độ này chúng ta có thể chuyển vào các chế độ chuyên biệt. Khi chúng ta chuyển vào chế độ cấu hình chuyên biệt nào thì dấu nhắc sẽ thay đổi tương ứng. Các câu lệnh trong đó chỉ có tác động đối với các cổng hay các tiến trình nào liên quan đến chế độ cấu hình đó thôi.

Chúng ta dùng lệnh exit để trở về chế độ cấu hình toàn cục hoặc chúng ta dùng phím Ctrl-Z để quay về thẳng chế độ EXEC đặc quyền.

3.2. Đặt tên cho router

Công việc đầu tiên khi cấu hình router là đặt tên cho router. Trong chế độ cấu hình toàn cục, chúng ta dùng lệnh sau:

- Router(config)#hostname Athena_VanCong
- Athena_VanCong(config)#

Ngay sau khi chúng ta nhấn phím Enter để thực thi câu lệnh chúng ta sẽ thấy dấu nhắc đổi từ tên mặc định (Router) sang tên mà chúng ta vừa mới đặt (Athena_VanCong).

3.3. Đặt mật mã cho router

Mật mã được sử dụng để hạn chế việc truy cập vào router. Thông thường ta luôn đặt mật mã cho đường vty và console trên router. Ngoài ra mật mã còn được sử dụng để kiểm soát sự truy cập vào chế độ EXEC đặc quyền trên router. Khi đó, chỉ những người nào được phép mới có thể thực hiện việc thay đổi tập tin cấu hình trên router. Sau đây là các lệnh mà chúng ta cần sử dụng để thực hiện việc đặt mật mã cho đường console:

- Athena_VanCong(config)#line console 0
- Athena_VanCong(config-line)#password <password>
- Athena_VanCong(config-line)#login

Chúng ta cũng cần đặt mật mã cho một hoặc nhiều đường vty để kiểm soát các user truy nhập từ xa vào router và Telnet. Thông thường Cisco router có 5 đường vty với thứ tự từ 0 đến 4. Chúng ta thường sử dụng một mật mã cho tất cả các đường vty, nhưng đôi khi chúng ta nên đặt thêm mật mã riêng cho một đường để dự phòng khi cả 4 đường kia đều đang được sử dụng. Sau đây là các lệnh cần sử dụng để đặt mật mã cho đường vty:

- Athena_VanCong(config)#line vty 0 4
- Athena_VanCong(config-line)#password <password>
- Athena_VanCong(config-line)#login

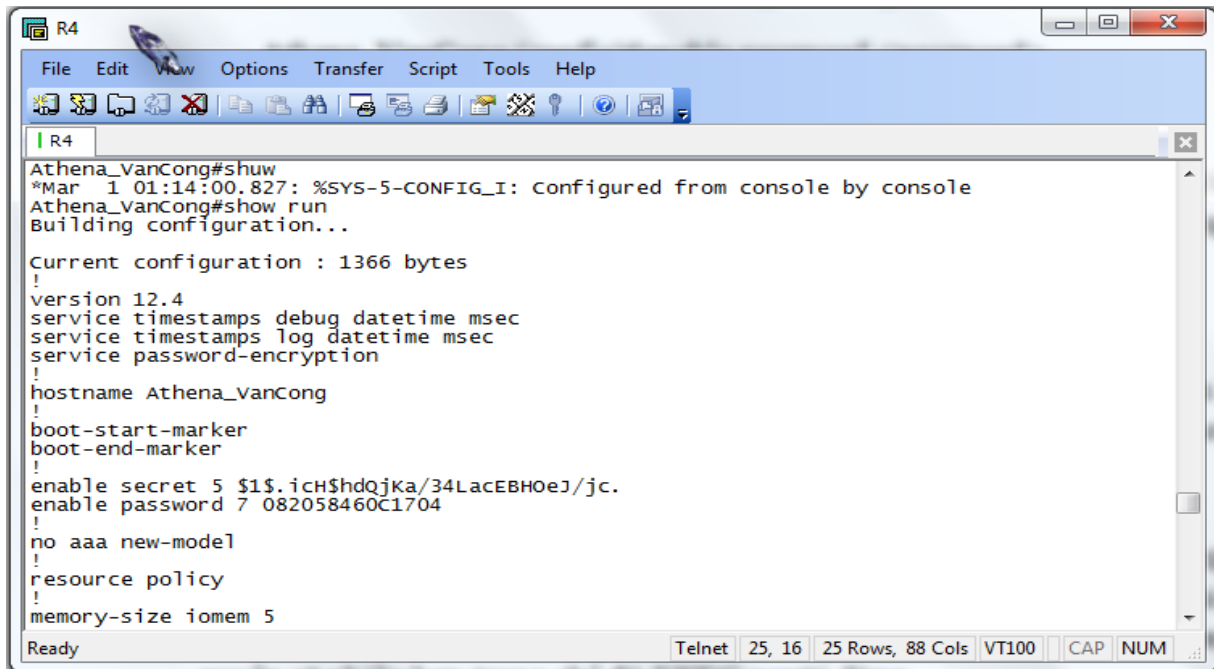
Mật mã enable và enable secret được sử dụng để hạn chế việc truy cập vào chế độ EXEC đặc quyền. Mật mã enable chỉ được sử dụng khi chúng ta cài đặt mật mã enable secret vì mật mã này được mã hoá còn mật mã enable thì không. Sau đây là các lệnh dùng để đặt mật mã enable secret:

- Athena_VanCong(config)#enable password <password>
- Athena_VanCong(config)#enable secret <password>

Đôi khi chúng ta sẽ thấy là rất không an toàn khi mật mã được hiển thị rõ ràng khi sử dụng lệnh show running-config hoặc show startup-config. Để tránh điều này chúng ta nên dùng lệnh sau để mã hoá tất cả các mật mã hiển thị trên tập tin cấu hình của router:

- Athena_VanCong(config)#service password-encryption

Lệnh service password-encryption sẽ áp dụng một cơ chế mã hoá đơn giản lên tất cả các mật mã chưa được mã hoá. Riêng mật mã enable secret thì sử dụng một thuật toán mã hoá rất mạnh là MD5.



```
R4
Athena_VanCong#shu
*Mar 1 01:14:00.827: %SYS-5-CONFIG_I: Configured from console by console
Athena_VanCong#show run
Building configuration...

Current configuration : 1366 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Athena_VanCong
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$.ich$hdQjKa/34LacEBHoeJ/jc.
enable password 7 082058460C1704
!
no aaa new-model
!
resource policy
!
memory-size iomem 5
Ready
```

Chúng ta có rất nhiều lệnh show được dùng để kiểm tra nội dung các tập tin trên router và để tìm ra sự cố. Trong cả hai chế độ EXEC đặc quyền và EXEC người dùng, khi chúng ta gõ show? Thì chúng ta sẽ xem được danh sách các lệnh show. Đương nhiên là số lệnh show được trong chế độ EXEC đặc quyền sẽ nhiều hơn trong chế độ EXEC người dùng.

Một số lệnh show như :

- Athena_VanCong#Show interface <interface>- hiển thị trạng thái của tất cả các cổng giao tiếp trên router.
- Athena_VanCong#Show controllers serial - hiển thị các thông tin chuyên biệt về phần cứng của các cổng serial.
- Athena_VanCong#Show clock - hiển thị đồng hồ được cài đặt trên router.
- Athena_VanCong#Show hosts - hiển thị danh sách tên và địa chỉ tương ứng.
- Athena_VanCong#Show users - hiển thị tất cả các user đang kết nối vào router.
- Athena_VanCong#Show history - hiển thị danh sách các câu lệnh vừa mới được sử dụng.

- Athena_VanCong#Show flash – hiển thị thông tin bộ nhớ flash và tập tin IOS chứa trong đó.
- Athena_VanCong#Show version - hiển thị thông tin về router và IOS đang chạy trên RAM.
- Athena_VanCong#Show ARP - hiển thị bảng ARP trên router.
- Athena_VanCong#Show protocol - hiển thị trạng thái toàn cục và trạng thái của các cổng giao tiếp đã được cấu hình giao thức lớp 3.
- Athena_VanCong#Show startup-configuration - hiển thị tập tin cấu hình đang chạy trên RAM.

3.4. Cấu hình cổng serial

Chúng ta có thể cấu hình cổng serial bằng đường console hoặc vty. Sau đây là các bước cần thực hiện khi cấu hình cổng serial:

1. Vào chế độ cấu hình toàn cục.
2. Vào chế độ cấu hình cổng serial.
3. Khai báo địa chỉ và subnet mask.
4. Đặt tốc độ clock nếu đầu cáp cắm vào cổng serial là DCE. Nếu đầu cáp là DTE thì chúng ta có thể bỏ qua này.
5. Khởi động serial.

Mỗi một cổng serial đều phải có một địa chỉ IP và subnet mask để chúng có thể định tuyến các gói IP. Để cấu hình địa chỉ IP chúng ta dùng lệnh sau:

- Athena_VanCong(config)#interface <serial interface>
- Athena_VanCong(config)#ip address <ip address><netmask>

Cổng serial cần phải có tín hiệu clock để điều khiển thời gian thực hiện thông tin liên lạc. Trong hầu hết các trường hợp, thiết bị DCE, ví dụ như CSU, sẽ là thiết bị cung cấp tín hiệu clock. Mặc định thì Cisco router là thiết bị DTE nhưng chúng ta có thể cấu hình chúng thành thiết bị DCE.

Trong môi trường làm lab thì các đường liên kết serial được kết nối trực tiếp với nhau. Do đó phải có một đầu là DCE để cấp tín hiệu clock. Chúng ta dùng lệnh clockrate để cài đặt tốc độ clock. Sau đây là các tốc độ clock mà chúng ta có thể đặt cho router (đơn vị của tốc độ clock là bit/s): 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, 4000000. Tuy nhiên sẽ có một số tốc độ chúng ta không sử dụng được tùy theo khả năng vật lý của từng cổng serial.

Mặc định thì các cổng giao tiếp trên router đều đóng. Nếu chúng ta muốn mở hay khởi động các cổng này thì chúng ta phải dùng lệnh `no shutdown`. Nếu chúng ta muốn đóng cổng lại để bảo trì hoặc xử lý sự cố thì chúng ta dùng lệnh `shutdown`.

Trong môi trường làm lab, tốc độ clock thường được sử dụng là 56000. Sau đây là các lệnh được sử dụng để cài đặt tốc độ clock và khởi động cổng serial:

- `Athena_VanCong(config)#interface serial 0/0`
- `Athena_VanCong(config-if)#clock rate 56000`
- `Athena_VanCong(config-if)#no shutdown`

3.5. Thực hiện việc thêm bớt, dịch chuyển và thay đổi tập tin cấu hình

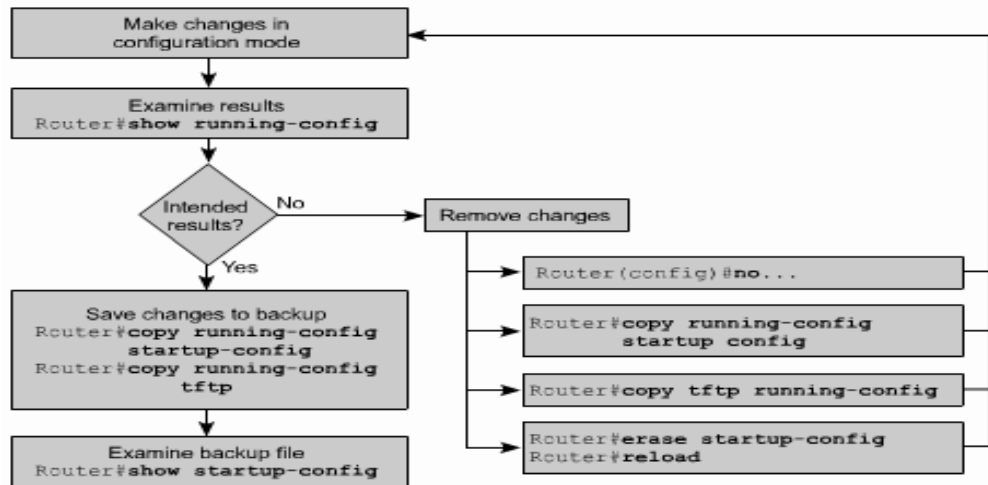
Nếu chúng ta cần chỉnh sửa tập tin cấu hình thì chúng ta phải di chuyển vào đúng chế độ cấu hình và thực hiện cần thiết. Ví dụ: nếu chúng ta cần mở một cổng nào đó trên router thì trước hết chúng ta phải vào chế độ cấu hình toàn cục, sau đó vào chế độ cấu của cổng đó rồi dùng lệnh `no shutdown`.

Để kiểm tra những gì mà chúng ta vừa mới thay đổi, chúng ta dùng lệnh `show running-config`. Lệnh này sẽ hiển thị nội dung của tập tin cấu hình hiện tại. Nếu kết quả hiển thị có những gì không đúng thì chúng ta có thể chỉnh sửa lại bằng cách thực hiện một hoặc nhiều cách sau:

- Dùng dạng `no` của các lệnh cấu hình.
- Khởi động lại router với tập tin cấu hình nguyên thủy trong NVRAM.
- Chép tập tin cấu hình dự phòng từ TFTP server.
- Xóa tập tin cấu hình khởi động bằng lệnh `erase startup-config`, sau đó khởi động lại router và vào chế độ cài đặt.

Để lưu tập tin, cấu hình hiện tại thành tập tin cấu hình khởi động lưu trong NVRAM, chúng ta dùng lệnh như sau:

- `Athena_VanCong#copy running-config startup-config` hoặc
- `Athena_VanCong#wr`



3.6. Cấu hình cổng Ethernet

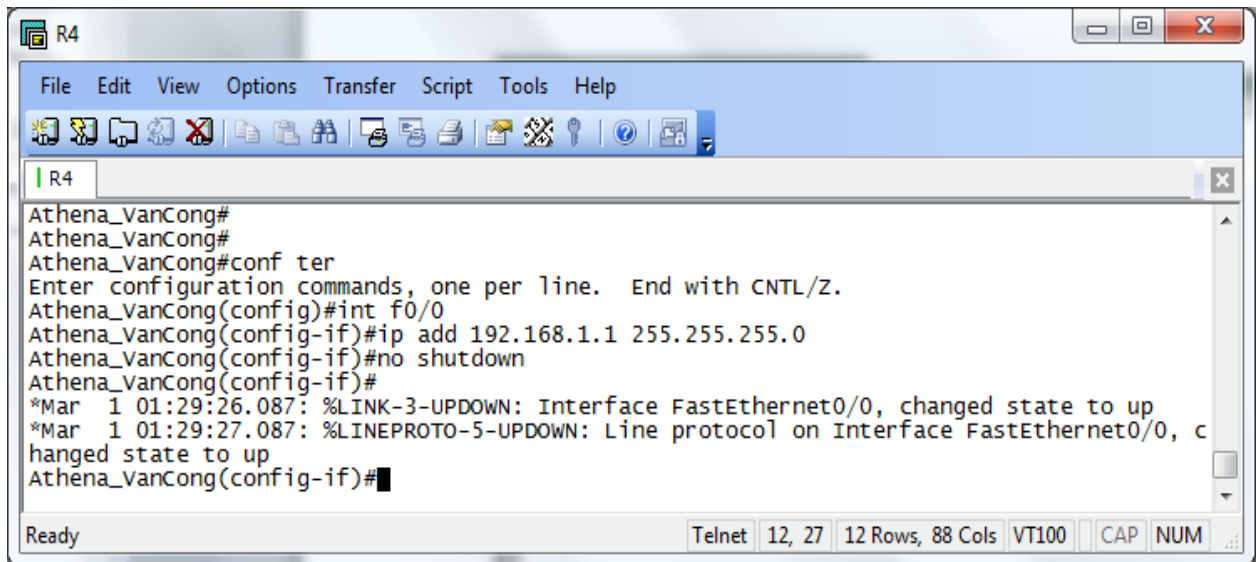
Tương tự như cổng serial, chúng ta có thể cấu hình cổng Ethernet bằng đường console hoặc vty.

Mỗi cổng Ethernet cũng cần phải có một địa chỉ IP và subnet mask để có thể thực hiện định tuyến các gói IP qua cổng đó.

Sau đây là các bước thực hiện cấu hình Ethernet:

- Vào chế độ cấu hình toàn cục.
- Vào chế độ cấu hình cổng Ethernet.
- Khai báo địa chỉ và subnet mask.
- Khởi động cổng Ethernet.

Mặc định là các cổng trên router đều đóng. Do đó, chúng ta phải dùng lệnh `no shutdown` để mở hay khởi động cổng. Nếu chúng ta cần đóng cổng lại để bảo trì hay xử lý sự cố thì chúng ta dùng lệnh `shutdown`.



```
R4
File Edit View Options Transfer Script Tools Help
Athena_VanCong#
Athena_VanCong#
Athena_VanCong#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Athena_VanCong(config)#int f0/0
Athena_VanCong(config-if)#ip add 192.168.1.1 255.255.255.0
Athena_VanCong(config-if)#no shutdown
Athena_VanCong(config-if)#
*Mar 1 01:29:26.087: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:29:27.087: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, c
hanged state to up
Athena_VanCong(config-if)#
```

3.7. Hoàn chỉnh cấu hình router

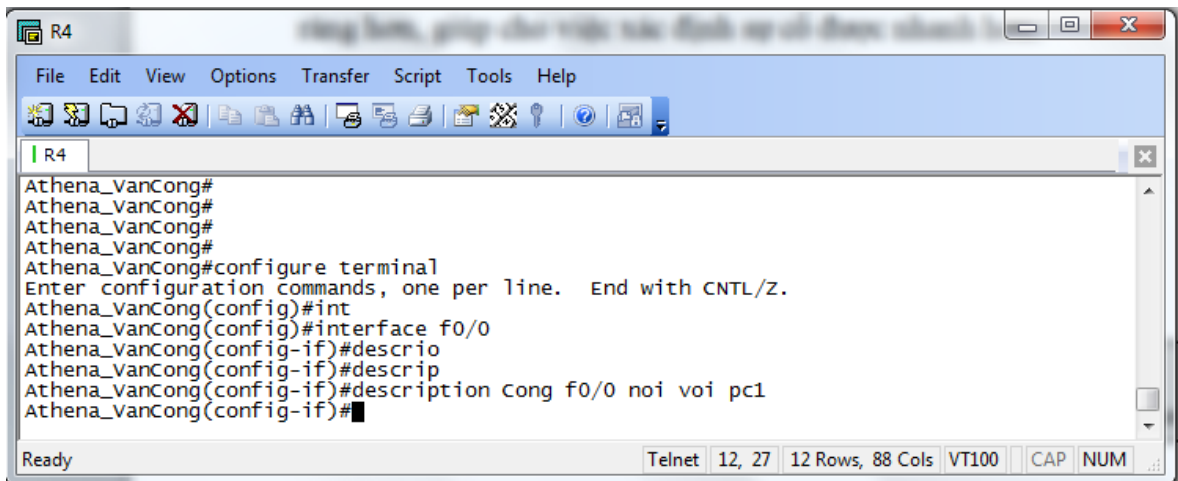
3.7.1. Tầm quan trọng của việc chuẩn hoá tập tin cấu hình

Trong một tổ chức việc phát các quy định dành cho các tập tin cấu hình là rất cần thiết. Từ đó ta có thể kiểm soát được các tập tin nào cần bảo trì, lưu các tập tin ở đâu và như thế nào.

3.7.2. Câu chú thích cho các cổng giao tiếp

Trên các cổng giao tiếp chúng ta nên ghi chú lại một số thông tin quan trọng, ví dụ như chỉ số mạch mà cổng này kết nối vào, hay thông tin vào router khác, về phân đoạn mạng mà cổng này kết nối đến. Dựa vào các câu chú thích này, người quản trị mạng có thể biết được là cổng giao tiếp này kết nối vào đâu.

Câu chú thích chỉ đơn giản là ghi chú thêm cho các cổng giao tiếp, ngoài ra nó hoàn toàn không có tác động gì đối với hoạt động của router nhưng lại giúp cho tập tin cấu hình được rõ ràng hơn, giúp cho việc xác định sự cố được nhanh hơn.



```

R4
File Edit View Options Transfer Script Tools Help
Athena_VanCong#
Athena_VanCong#
Athena_VanCong#
Athena_VanCong#
Athena_VanCong#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Athena_VanCong(config)#int
Athena_VanCong(config)#interface f0/0
Athena_VanCong(config-if)#descrio
Athena_VanCong(config-if)#descrip
Athena_VanCong(config-if)#description Cong f0/0 noi voi pc1
Athena_VanCong(config-if)#

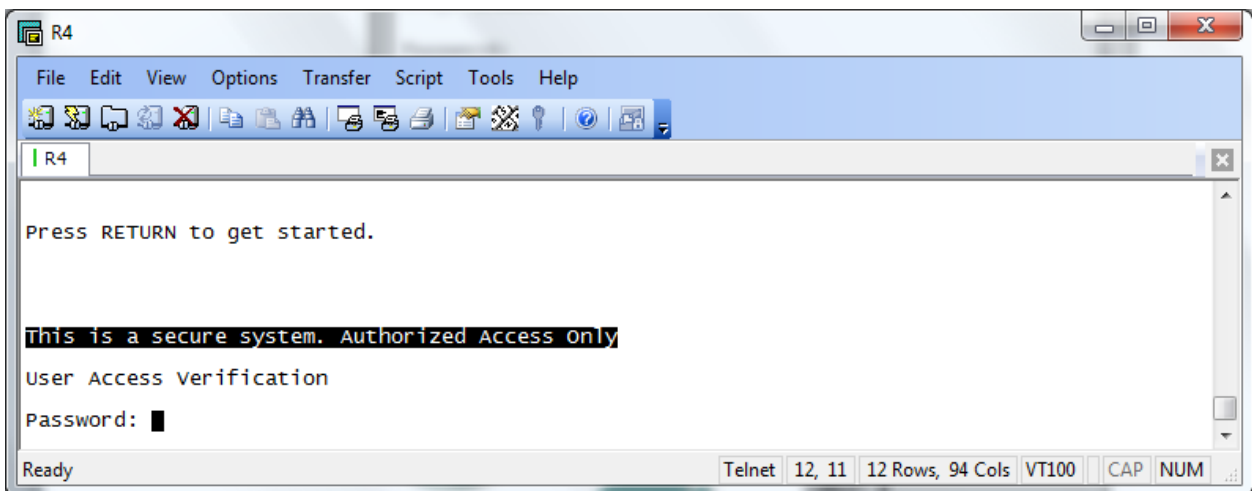
```

- Athena_VanCong#configure terminal
- Athena_VanCong(config)#interface <interface>
- Athena_VanCong(config-if)# description <Chú thích>

3.7.3. Thông điệp đăng nhập

Thông điệp đăng nhập được hiển thị khi chúng ta đăng nhập vào hệ thống. Loại thông điệp này rất hữu dụng khi chúng ta cần cảnh báo trước khi đến giờ tắt hệ thống mạng.

Ví dụ một thông điệp như sau: “This is a secure system, Authorized Access Only!” (Đây là hệ thống được bảo mật, chỉ dành cho những người có thẩm quyền!) được sử dụng để cảnh báo những vị khách viếng thăm bất hợp pháp.



```

R4
File Edit View Options Transfer Script Tools Help
Press RETURN to get started.

This is a secure system. Authorized Access Only
User Access Verification
Password:

```

3.7.4. Cấu hình thông điệp đăng nhập (MOTD)

Thông điệp MOTD có thể hiển thị trên tất cả các thiết bị đầu cuối kết nối vào router.



Trung Tâm Đào Tạo Quản Trị Mạng & An Ninh Mạng Quốc Tế **ATHENA**
+ 92 Nguyễn Đình Chiểu, P. Đa Kao, Q. 1 Tel: (08) 2210 3801 - 0943 23 00 99
+ 2 Bis Đinh Tiên Hoàng, P. Đa Kao, Q. 1 Tel: (08) 38 244 041 - 0943 20 00 88
Website: www.athena.edu.vn Email: training@athenavn.com

Để cấu hình thông điệp MOTD chúng ta vào chế độ cấu hình toàn cục. Tại đây chúng ta dùng lệnh `banner motd`, cách một khoảng trắng, nhập ký tự phân cách ví dụ như ký tự `#`, rồi viết câu thông báo, kết thúc bằng cách nhập ký tự phân cách một lần nữa.

Sau đây là các bước thực hiện để cấu hình thông điệp MOTD:

1. Vào chế độ cấu hình toàn cục bằng lệnh `configure terminal`
2. Nhập lệnh như sau: `banner motd # The message of the day goes here #`.
3. Lưu cấu hình vừa rồi bằng lệnh `copy running-config startup-config`.

3. ĐỊNH TUYẾN VÀ CÁC GIAO THỨC ĐỊNH TUYẾN

GIỚI THIỆU

Định tuyến đơn giản chỉ là tìm đường đi từ mạng này đến mạng khác. Thông tin về những con đường này có thể là được cập nhật tự động từ các router khác hoặc là do người quản trị mạng chỉ định cho router. Chúng ta sẽ đi tìm hiểu về định tuyến động, các loại giao thức định tuyến động và phân tích mỗi loại một giao thức tiêu biểu.

Người quản trị mạng khi chọn lựa một giao thức định tuyến động cần cân nhắc một số yếu tố như: độ lớn của hệ thống mạng, băng thông các đường truyền, khả năng của router. Loại router và phiên bản router, các giao thức đang chạy trong hệ thống mạng. Chương này mô tả chi tiết về sự khác nhau giữa các giao thức định tuyến để giúp cho nhà quản trị mạng trong việc chọn lựa một giao thức định tuyến.

1. TỔNG QUAN VỀ ĐỊNH TUYẾN VÀ ĐỊNH TUYẾN TĨNH

Định tuyến là quá trình mà router thực hiện để chuyển gói dữ liệu tới mạng đích. Tất cả các router dọc theo đường đi đều dựa vào địa chỉ IP đích của gói dữ liệu để chuyển gói theo đúng hướng đến đích cuối cùng. Để thực hiện được điều này, router phải học thông tin về đường đi tới các mạng khác. Nếu router chạy định tuyến động thì router tự động học những thông tin này từ các router khác. Còn nếu router chạy định tuyến tĩnh thì người quản trị mạng phải cấu hình các thông tin đến các mạng khác cho router.

1.1. Giới thiệu về giao thức định tuyến tĩnh

Đối với định tuyến tĩnh, các thông tin về đường đi phải do người quản trị mạng nhập cho router. Khi cấu trúc mạng có bất kỳ thay đổi nào thì chính người quản trị mạng phải xóa hoặc thêm các thông tin về đường đi cho router. Những loại đường đi như vậy gọi là đường đi cố định. Đối với hệ thống mạng lớn thì công việc bảo trì mạng định tuyến cho router như trên tốn rất nhiều thời gian. Còn đối với hệ thống mạng nhỏ, ít có thay đổi thì công việc này đỡ mất công hơn. Chính vì định tuyến tĩnh đòi hỏi người quản trị mạng phải cấu hình mọi thông tin về đường đi cho router nên nó không có được tính linh hoạt như định tuyến động. Trong những hệ thống mạng lớn, định tuyến tĩnh thường được sử dụng kết hợp với giao thức định tuyến động cho một số mục đích đặc biệt.

1.2. Hoạt động của định tuyến tĩnh.

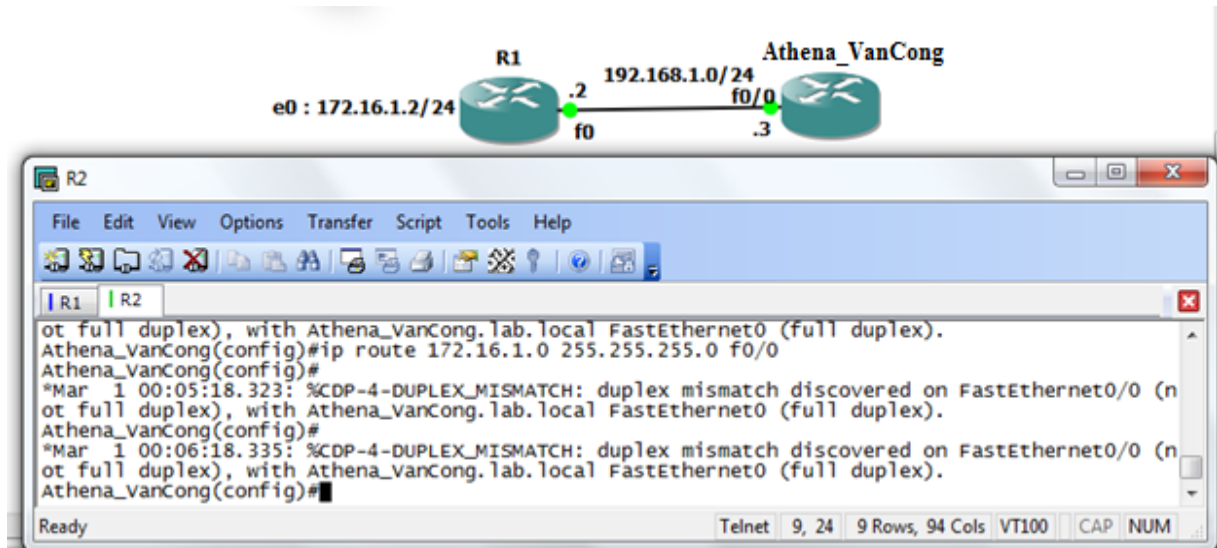
Hoạt động của định tuyến tĩnh có thể chia ra làm 3 bước như sau:

- Đầu tiên, người quản trị mạng cấu hình các đường cố định cho router
- Router cài đặt các đường đi này vào bảng định tuyến.

- Gói dữ liệu được định tuyến theo các đường cố định này .

1.3. Cấu hình định tuyến tĩnh

Người quản trị mạng cấu hình đường cố định cho router bằng lệnh iproute. Cú pháp của lệnh iproute.



- Athena_VanCong(config)# ip router network subnet-mask outgoinginterface| ip next hop

Câu lệnh mà người quản trị của router Athena_VanCong cấu hình đường cố định cho router đến mạng 172.16.1.0/24 . Câu lệnh này chỉ cho router biết đường đến mạng đích đi ra bằng cổng giao tiếp nào . Chúng ta còn có thể chỉ cho router biết địa chỉ IP của router kế tiếp là gì để đến được mạng đích. Cả 2 câu lệnh đều cài đặt đường cố định vào bảng định tuyến của router Athena_VanCong. Điểm khác nhau duy nhất giữa 2 câu lệnh này là chỉ số tin cậy của 2 đường cố định tương ứng trên bảng định tuyến của router sẽ khác nhau.

Chỉ số tin cậy là một thông số đo lường độ tin cậy của một đường đi .Chỉ số này càng thấp thì độ tin cậy càng cao .Do đó ,nếu đến cùng một đích thì con đường nào có chỉ số tin cậy thấp hơn thì đường đó được vào bảng định tuyến của router trước .Trong ví dụ trên,đường cố định sử dụng địa chỉ IP của trạm kế tiếp sẽ có chỉ số tin cậy mặc định là 1,còn đường cố định sử dụng cổng ra thì có chỉ số tin cậy mặc định là 0 .Nếu chúng ta muốn chỉ định chỉ số tin cậy thay vì sử dụng giá trị mặc định thì chúng ta thêm thông số này vào sau thông số về cổng ra/địa chỉ IP trạm kế của câu lệnh .Giá trị của chỉ số này nằm trong khoảng từ 0 đến 255.

- Athena_VanCong(config)# ip router 172.16.1.0 255.255.255.0 192.168.1.2

Nếu router không chuyển được gói ra cổng giao tiếp đã được cấu hình thì có nghĩa là cổng giao tiếp đang bị đóng, đường đi tương ứng cũng sẽ không được đặt vào bảng định tuyến.

Đôi khi chúng ta sử dụng đường cố định làm đường dự phòng cho đường định tuyến động. Router sẽ chỉ sử dụng đường cố định khi đường định tuyến động bị đứt. Để thực hiện điều này, chúng ta chỉ cần đặt giá trị chỉ số tin cậy của đường cố định cao hơn chỉ số tin cậy của giao thức định tuyến động đang sử dụng là được.

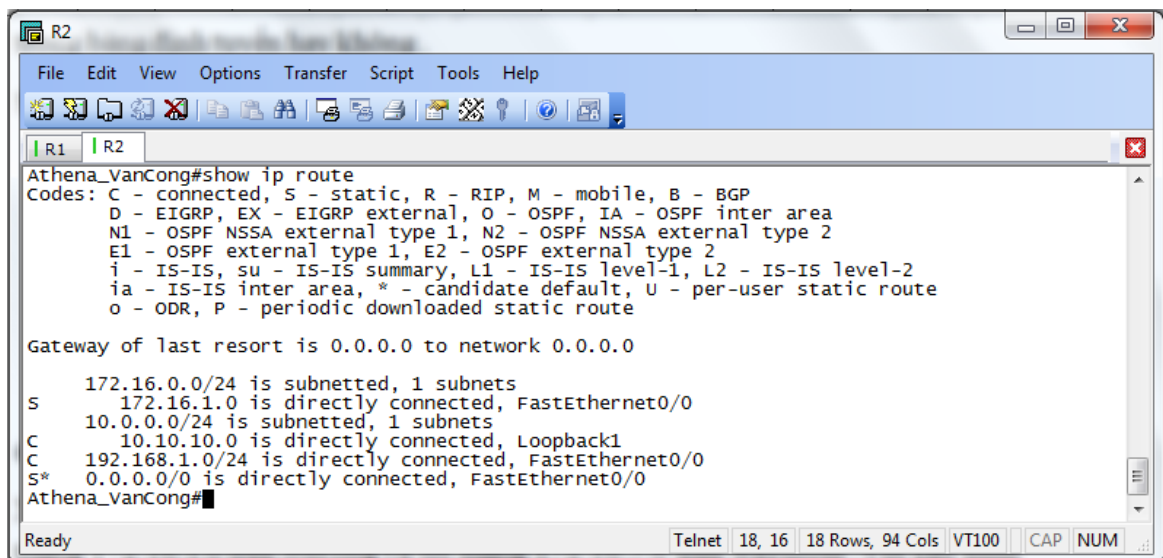
1.4. Cấu hình đường cố định

Cấu hình đường mặc định cho router chuyển gói đi là đường mà router sẽ sử dụng trong trường hợp router không tìm thấy đường đi nào phù hợp trong bảng định tuyến để tới đích của gói dữ liệu. Chúng ta thường cấu hình đường mặc định cho đường ra Internet của router vì router không cần phải lưu thông tin định tuyến tới từng mạng trên Internet. Lệnh cấu hình đường mặc định thực chất cũng là lệnh cấu hình đường cố định, cụ thể là câu lệnh như sau:

- Athena_VanCong(config)#ip route 0.0.0.0 0.0.0.0 [next-hop-address/outgoing interface]

Subnet 0.0.0.0 khi được thực hiện phép toán AND logic với bất kỳ địa chỉ IP đích nào cũng có kết quả là mạng 0.0.0.0. Do đó, nếu gói dữ liệu có địa chỉ đích mà router không tìm được đường nào phù hợp thì gói dữ liệu đó sẽ được định tuyến tới mạng 0.0.0.0.

Sau khi cấu hình đường cố định chúng ta dùng lệnh show ip route để xem có đường cố định trong bảng định tuyến hay không.



```
R2
Athena_VanCong#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

    172.16.0.0/24 is subnetted, 1 subnets
S       172.16.1.0 is directly connected, FastEthernet0/0
    10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Loopback1
C       192.168.1.0/24 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 is directly connected, FastEthernet0/0
Athena_VanCong#
```


Bây giờ trên router Athena_VanCong ,chúng ta thực hiện lệnh ping tới một node trong mạng 172.16.1.0. Ví dụ lệnh ping không thành công .Sau đó chúng ta dùng lệnh traceroute đến node mà chúng ta vừa mới ping để xem lệnh traceroute bị rớt ở đâu .

2. TỔNG QUAN VỀ ĐỊNH TUYẾN ĐỘNG

2.1. Giới thiệu về giao thức định tuyến động

Giao thức định tuyến khác với giao thức được định tuyến cả về chức năng và nhiệm vụ .Giao thức định tuyến được sử dụng để giao tiếp giữa các router với nhau.Giao thức định tuyến cho phép router này chia sẻ các thông tin định tuyến mà nó biết cho các router khác .Từ đó ,các router có thể xây dựng và bảo trì bảng định tuyến của nó.

Sau đây là một số giao thức định tuyến :RIP, IGRP, EIGRP, OSPF...

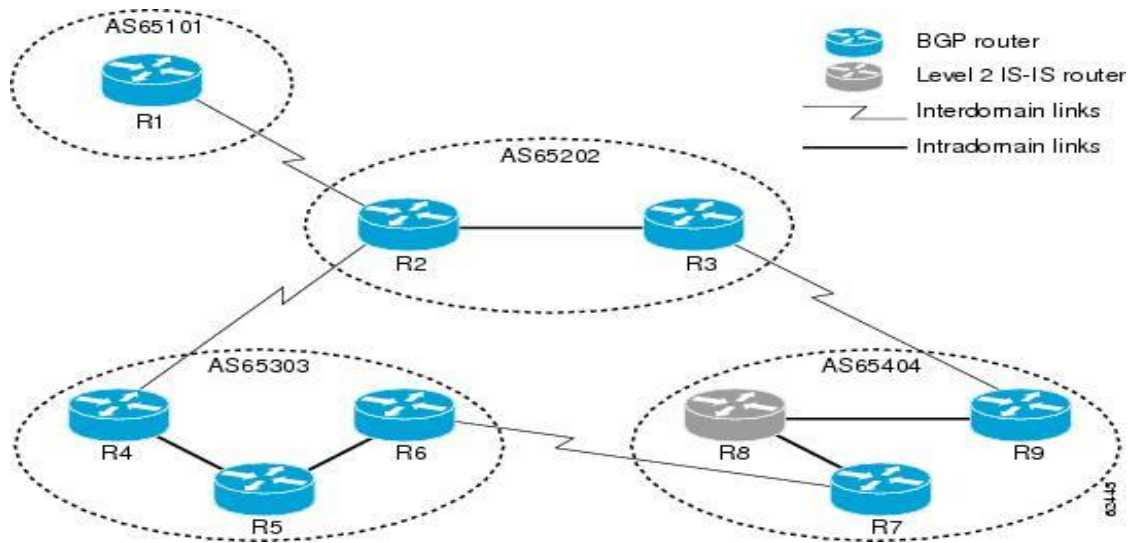
Còn giao thức được định tuyến thì được sử dụng để định hướng cho dữ liệu của người dùng. Một giao thức được định tuyến sẽ cung cấp đầy đủ thông tin về địa chỉ lớp mạng để gói dữ liệu có thể truyền đi từ host này đến host khác dựa trên cấu trúc địa chỉ đó .

Sau đây là các giao thức được định tuyến:

- Internet Protocol (IP)
- Internetwork Packet Exchange(IPX)

2.2. Autonmous sytem(AS) (Hệ thống tự quản)

Hệ tự quản (AS) là một tập hợp các mạng hoạt động dưới cùng một cơ chế quản trị về định tuyến .Từ bên ngoài nhìn vào ,một AS được xem như một đơn vị .Tổ chức Đăng ký số Internet của Mỹ (ARIN-American Registry of Internet Numbers) là nơi quản lý việc cấp số cho mỗi AS .Chỉ số này dài 16 bit .Một số giao thức định tuyến ,ví dụ như giao thức IRGP của Cisco,đòi hỏi phải có số AS xác định khi hoạt động .



2.3. Mục đích của giao thức định tuyến và hệ thống tự quản

Mục đích của giao thức định tuyến là xây dựng và bảo trì bảng định tuyến. Bảng định tuyến này mang thông tin về các mạng khác và các cổng giao tiếp trên router đến các mạng này. Router sử dụng giao thức định tuyến để quản lý thông tin nhận được từ các router khác, thông tin từ cấu hình của các cổng giao tiếp và thông tin cấu hình các đường cố định.

Giao thức định tuyến cập nhật về tất cả các đường, chọn đường tốt nhất đặt vào bảng định tuyến và xóa đi khi đường đó không sử dụng được nữa. Còn router thì sử dụng thông tin trên bảng định tuyến để chuyển gói dữ liệu của các giao thức được định tuyến.

Định tuyến động hoạt động trên cơ sở các thuật toán định tuyến. Khi cấu trúc mạng có bất kỳ thay đổi nào như mở rộng thêm, cấu hình lại, hay bị trục trặc thì khi đó ta nói hệ thống mạng đã được hội tụ. Thời gian để các router đồng bộ với nhau càng ngắn càng tốt vì khi các router chưa đồng bộ với nhau về các thông tin trên mạng thì sẽ định tuyến sai.

Với hệ thống tự quản (AS), toàn bộ hệ thống mạng toàn cầu được chia ra thành nhiều mạng nhỏ, dễ quản lý hơn. Mỗi AS có một số AS riêng, không trùng lặp với bất kỳ AS khác, và mỗi AS có cơ chế quản trị riêng của mình.

3. PHÂN LOẠI CÁC LOẠI ĐỊNH TUYẾN

Đa số các thuật toán định tuyến được xếp vào 2 loại sau:

- Vector khoảng cách.
- Trạng thái đường liên kết.

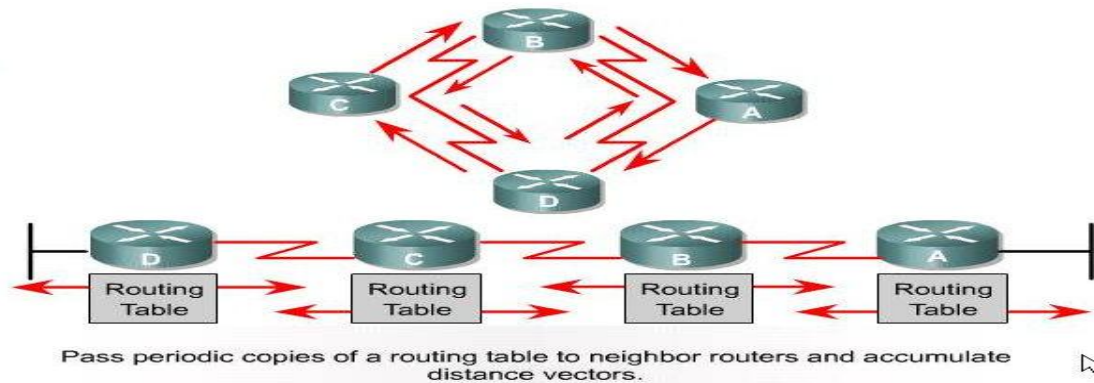
3.1. Định tuyến theo vectơ khoảng cách

3.1.1. Cơ chế định tuyến

Định tuyến theo vectơ khoảng cách thực hiện truyền bản sao của bảng định tuyến từ router này sang router khác theo định kỳ. Việc cập nhật định kỳ giữa các router giúp trao đổi thông tin khi cấu trúc mạng thay đổi. Thuật toán định tuyến theo vectơ khoảng cách còn được gọi là thuật toán Bellman-Ford.

Mỗi router nhận được bảng định tuyến của những router láng giềng kết nối trực tiếp với nó. Ví dụ router B nhận được thông tin từ router A. Sau đó router B sẽ cộng thêm khoảng cách từ router B đến router (ví dụ như tăng số hop lên) vào các thông tin định tuyến nhận được từ A. Khi đó router B sẽ có bảng định tuyến mới và truyền bảng định tuyến này cho router láng giềng khác là router C. Quá trình này xảy ra tương tự cho tất cả các router láng giềng khác.

Chuyển bảng định tuyến cho router láng giềng theo định kỳ và tính lại vectơ khoảng cách.



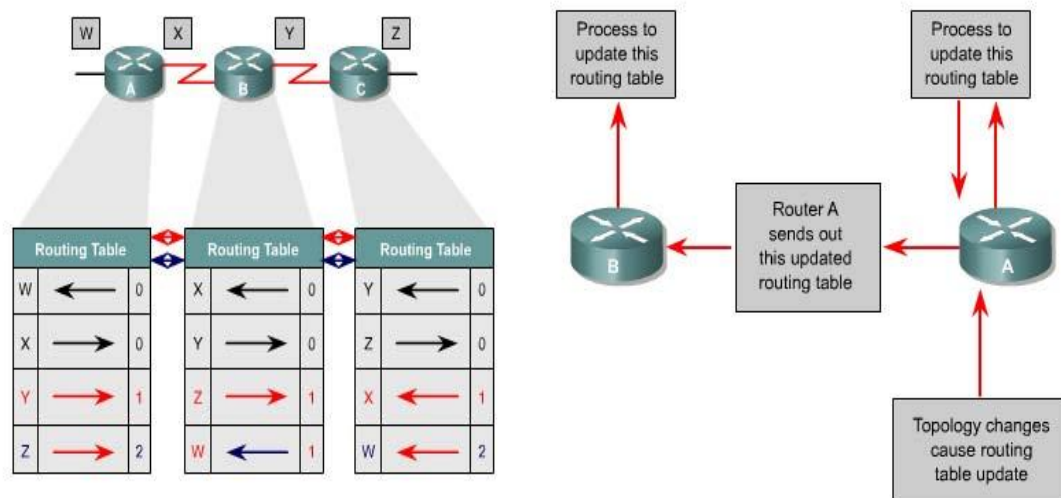
Router thu thập thông tin về khoảng cách đến các mạng khác, từ đó nó xây dựng và bảo trì một cơ sở dữ liệu về thông tin định tuyến trong mạng. động theo thuật toán vectơ khoảng cách chính xác cấu trúc của toàn bộ hệ thống giềng kết nối trực tiếp với nó mà thôi.

Tu nhiên, hoạt cách như vậy thì routers sẽ không biết được mạng mà chỉ biết được các router láng

Khi sử dụng định tuyến theo vectơ khoảng cách, bước đầu tiên là router phải xác định các router láng giềng với nó. Các mạng kết nối trực tiếp vào cổng giao tiếp của routers sẽ có khoảng cách là 0. Còn đường đi tới các mạng không kết nối trực tiếp vào router thì routers sẽ chọn đường tốt nhất dựa trên thông tin mà nó nhận được từ các router láng giềng. Ví dụ Router A nhận được thông tin về các mạng khác từ router B. Các thông tin này được đặt trong bảng định tuyến với vectơ khoảng cách đã được tính toán lại chi phí từ router A đến mạng đích thì đi theo hướng nào, khoảng cách bao nhiêu.

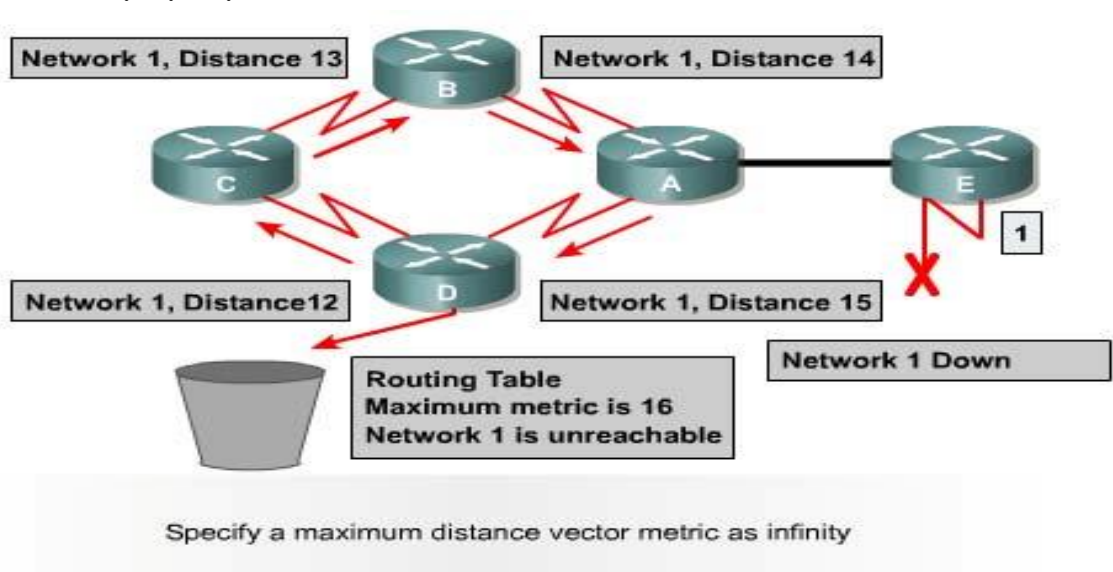
3.1.2. Cơ chế cập nhật định tuyến

Bảng định tuyến được cập nhật khi cấu trúc mạng có sự thay đổi. Quá trình cập nhật này cũng diễn ra từng bước một từ router này đến router khác. Khi cập nhật, mỗi router gửi đi toàn bộ bảng định tuyến của nó cho các router láng giềng. Trong bảng định tuyến có thông tin về đường đi tới từng mạng đích: tổng chi phí cho đường đi, địa chỉ của router kết tiếp.



3.1.3. Lỗi định tuyến lặp và giá trị tối đa

Định tuyến lặp có thể xảy ra khi bảng định tuyến trên các router chưa được cập nhật hội tụ do quá trình hội tụ chậm.



Nguyên nhân là do cập nhật sai về Mạng 1 của router B, C, D khi cập nhật sai bảng định tuyến của nhau trong khi router A chưa cập nhật cho các router còn lại về mạng 1. Điều này sẽ bị lặp vòng như vậy hoài cho đến khi nào có một tiến trình khác cắt đứt được quá trình này.

Tình trạng như vậy gọi là đếm vô hạn, gói dữ liệu sẽ bị lặp vòng trên mạng trong khi thực tế là Mạng 1 đã bị ngắt.

Với vector khoảng cách sử dụng thông số là số lượng hop thì mỗi khi router chuyển thông tin cập nhật cho router khác, chỉ số hop sẽ tăng lên 1. Nếu không có biện pháp khắc phục tình trạng đếm vô hạn, thì cứ như vậy chỉ số hop sẽ tăng lên đến vô hạn.

Bản thân thuật toán định tuyến theo vector khoảng cách có thể tự sửa lỗi được nhưng quá trình lặp vòng này có thể kéo dài đến khi nào đếm đến vô hạn. Do đó để tránh tình trạng lỗi này kéo dài, giao thức định tuyến theo vector khoảng cách đã định nghĩa giá trị tối đa.

Bằng cách này, giao thức định tuyến cho phép vòng lặp kéo dài đến khi thông số định tuyến vượt qua giá trị tối đa. Ví dụ như hình vẽ dưới, khi thông số định tuyến là 16 hop lớn hơn giá trị tối đa là 15 thì thông tin cập nhật đó sẽ bị router hủy bỏ. Trong bất kỳ trường hợp nào, khi giá trị của thông số định tuyến vượt qua giá trị tối đa thì xem như mạng đó là không đến được.

3.1.4. Các cách phòng chống lỗi định tuyến lặp

3.1.4.1. Tránh định tuyến lặp vòng bằng split horizon

Một nguyên nhân khác gây ra lặp vòng là router gửi lại những thông tin định tuyến mà nó vừa nhận được cho chính router đã gửi những thông tin đó.

Sử dụng bằng câu lệnh Router(config-if)#no ip split- horizon

3.1.4.2. Tránh định tuyến lặp vòng bằng Route poisoning

Route poisoning được sử dụng để tránh xảy ra các vòng lặp lớn và giúp cho router thông báo thẳng là mạng đã không truy cập được nữa bằng cách đặt giá trị cho thông số định tuyến (số lượng hop chẳng hạn) lớn hơn giá trị tối đa.

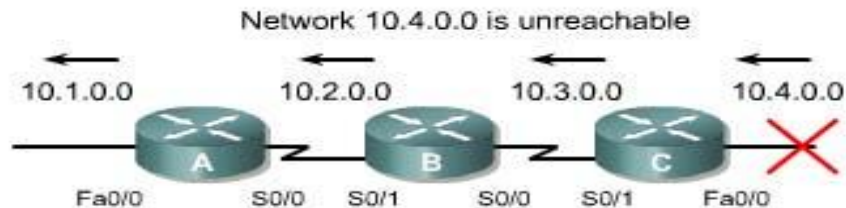
Route poisoning có nghĩa là khi có một con đường nào đó bị ngắt thì router sẽ thông báo về con đường đó với thông số định tuyến lớn hơn giá trị tối đa. Cơ chế route poisoning không hề gây mâu thuẫn với cơ chế split horizon. Split horizon có nghĩa là khi router gửi thông tin cập nhật ra một đường liên kết thì router không được gửi lại những thông tin nào mà nó vừa nhận vào từ đường liên kết đó. Bây giờ, router vẫn gửi lại những thông tin đó nhưng với thông số định tuyến lớn hơn giá trị tối đa thì kết quả vẫn như vậy. Cơ chế này gọi là split horizon kết hợp với poison reverse.

Khi mạng x bị ngắt, Router sẽ sử dụng route poisoning bằng cách đặt giá trị 16 trên bảng định tuyến để cho biết mạng này không đến được nữa.

3.1.4.3. Tránh định tuyến lặp vòng bằng cơ chế cập nhật tức thời

Hoạt động cập nhật bảng định tuyến giữa các router láng giềng được thực hiện theo chu kỳ. Ví dụ: cứ sau 30 giây RIP thực hiện cập nhật một lần. Ngoài ra còn có cơ chế cập nhật tức thời để thông báo về một thay đổi nào đó trong bảng định tuyến. Khi router phát hiện ra có một thay đổi nào đó trong cấu trúc thì nó lập tức gửi thông điệp cập nhật cho các router láng giềng để thông báo về sự thay đổi đó. Nhất là khi có một đường nào đó bị lỗi không truy cập được nữa thì router phải cập nhật tức thời thay vì đợi đến hết chu kỳ. Cơ chế cập nhật tức thời kết hợp với route poisoning sẽ đảm bảo cho tất cả các router nhận được thông tin khi có một đường nào đó bị ngắt trước khi thời gian holddown kết thúc.

Cơ chế cập nhật tức thời cho toàn bộ mạng khi có sự thay đổi trong cấu trúc mạng giúp cho các router được cập nhật kịp thời và khởi động thời gian holddown nhanh hơn.



Ví dụ như router C cập nhật tức thời ngay khi mạng 10.4.0.0 không truy cập được nữa. Khi nhận được thông tin này, router B cũng phát thông báo về mạng 10.4.0.0 ra cổng S0/1. Đến lượt router A cũng sẽ phát thông báo ra cổng Fa0/0. Network 10.4.0.0 is unreachable

Với cập nhật tức thời, router sẽ gửi thông điệp ngay để thông báo sự thay đổi trong bảng định tuyến của mình.

3.1.4.4. Tránh lặp vòng bằng thời gian holddown

Khi router nhận được từ router láng giềng một thông tin cho biết là một mạng X nào đó bây giờ không truy cập được nữa thì router sẽ đánh dấu vào con đường tới mạng X đó là không truy cập được nữa và khởi động thời gian holddown. Trong khoảng thời gian holddown này, nếu router nhận được thông tin cập nhật từ chính router láng giềng lúc này thông báo là mạng X đã truy cập lại được thì router mới cập nhật thông tin đó và kết thúc thời gian holddown.

Trong suốt thời gian holddown nếu router nhận được thông tin cập nhật từ một router láng giềng khác (không phải là router láng giềng đã phát thông tin cập nhật về mạng X lúc này) nhưng thông tin này cho biết có đường đến mạng X với thông số định tuyến tốt hơn con đường mà router trước đó thì nó sẽ bỏ qua, không cập nhật thông tin này. Cơ chế này giúp cho router

tránh được việc cập nhật nhầm những thông tin cũ do các router lảng giềng chưa hay biết gì về việc mạng X đã không truy cập được nữa. Không thời gian holddown bảo đảm cho tất cả các router trong hệ thống mạng đã được cập nhật xong về thông tin mới. Sau khi thời gian hold-down hết thời hạn, tất cả các router trong hệ thống đều đã được cập nhật là mạng X không truy cập được nữa, khi đó các router đều có thể nhận biết chính xác về cấu trúc mạng. Do đó, sau khi thời gian holddown kết thúc thì các router lại cập nhật thông tin như bình thường.

Sử dụng câu lệnh để thay đổi thời gian holddown:

- Router(config- router)#timers basic update invalid holddown flush[sleeptime]

3.1.5. Đặc điểm của giao thức định tuyến theo trạng thái đường liên kết

Thuật toán định tuyến theo trạng thái đường liên kết là thuật toán Dijkstras hay còn gọi là thuật toán SPF (Shortest Path First tìm đường ngắn nhất). Thuật toán định tuyến theo trạng thái đường liên kết thực hiện việc xây dựng và bảo trì một cơ sở dữ liệu đầy đủ về cấu trúc của toàn bộ hệ thống mạng.

Định tuyến theo trạng thái đường liên kết sử dụng những công cụ sau:

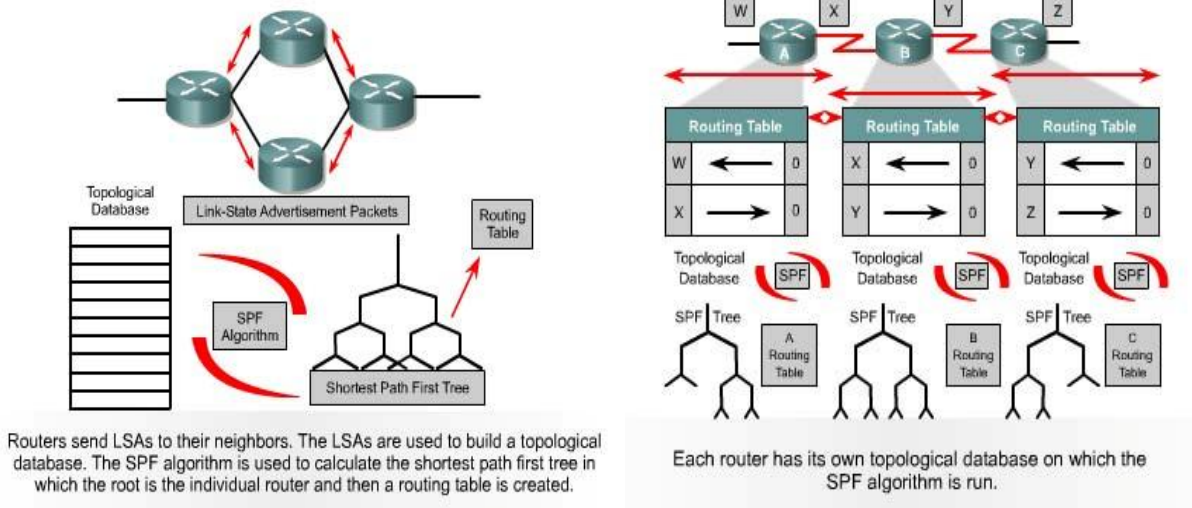
- Thông điệp thông báo trạng thái đường liên kết (LSA-Link-state Advertisement): LSA là một gói dữ liệu nhỏ mang thông tin định tuyến được truyền đi giữa các router .
- Cơ sở dữ liệu về cấu trúc mạng :được xây dựng từ thông tin thu thập được từ các LSA .
- Thuật toán SPF :dựa trên cơ sở dữ liệu về cấu trúc mạng ,thuật toán SPF sẽ tính toán để tìm đường ngắn nhất .
- Bảng định tuyến :chứa danh sách các đường đi đã được chọn lựa .

Quá trình thu thập thông tin mạng để thực hiện định tuyến theo trạng thái đường liên kết:

Mỗi router bắt đầu trao đổi LSA với tất cả các router khác, trong đó LSA mang cơ sở dữ liệu dựa trên thông tin của các LSA.

Mỗi router tiến hành xây dựng lại cấu trúc mạng theo dạng hình cây với bản thân nó là gốc ,từ đó router vẽ ra tất cả các đường đi tới tất cả các mạng trong hệ thống. Sau đó thuật toán SPF chọn đường ngắn nhất để đưa vào bảng định tuyến. Trên bảng định tuyến sẽ chứa thông tin về các đường đi đã được chọn với cổng ra tương ứng. Bên cạnh đó, router vẫn tiếp tục duy trì cơ sở dữ liệu về cấu trúc hệ thống mạng và trạng thái của các đường liên kết. Router nào phát hiện cấu trúc mạng thay đổi đầu tiên sẽ phát thông tin cập nhật cho tất cả các router

khác. Router phát gói LSA, trong đó có thông tin về router mới, các thay đổi về trạng thái đường liên kết. Gói LSA này được phát đi cho tất cả các router khác.

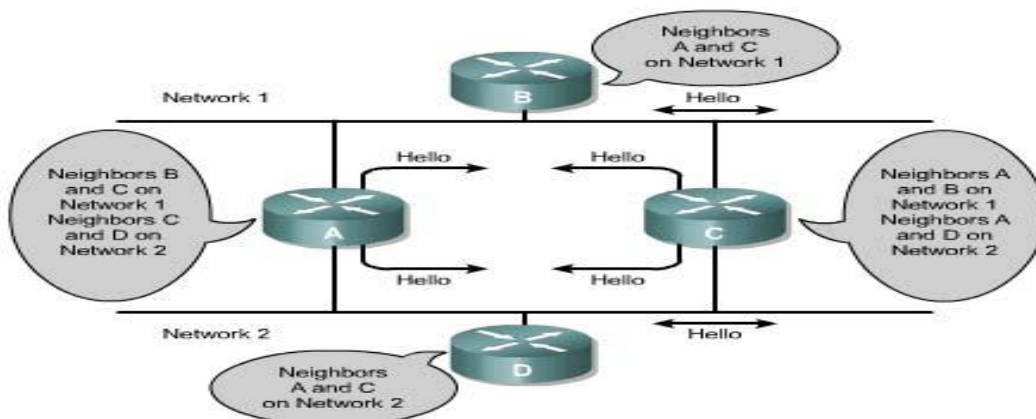


Mỗi router có cơ sở dữ liệu riêng về cấu trúc mạng và thuật toán SPF thực hiện tính toán dựa trên cơ sở dữ liệu này.

Khi router nhận được gói LSA thì nó sẽ cập nhật lại cơ sở dữ liệu của nó với thông tin mới vừa nhận được. Sau đó SPF sẽ tính lại để chọn đường lại và cập nhật lại cho bảng định tuyến.

Định tuyến theo trạng thái đường liên kết có một số nhược điểm sau:

- Bộ xử lý trung tâm của router phải tính toán nhiều
- Đòi hỏi dung lượng bộ nhớ phải lớn
- Chiếm dụng băng thông đường truyền



Router sử dụng định tuyến theo trạng thái đường liên kết sẽ phải cần nhiều bộ nhớ hơn và hoạt động xử lý nhiều hơn là sử dụng định tuyến theo vectơ khoảng cách. Router phải có đủ bộ nhớ để lưu cơ sở dữ liệu về cấu trúc mạng ,bảng định tuyến. Khi khởi động việc định tuyến ,tất cả các router phải gửi gói LSA cho tất cả các router khác, khi đó băng thông đường truyền sẽ bị chiếm dụng làm cho băng thông dành cho đường truyền dữ liệu của người dùng bị giảm xuống. Nhưng sau khi các router đã thu thập đủ thông tin để xây dựng cơ sở dữ liệu về cấu trúc mạng thì băng thông đường truyền không bị chiếm dụng nữa .Chỉ khi nào cấu trúc mạng thay đổi thì router mới phát gói LSA để cập nhật và những gói LSA này chiếm một phần băng thông rộng rất nhỏ.

3.2. Tổng quát về giao thức định tuyến

3.2.1. Quyết định chọn đường đi

Router có 2 chức năng chính là :

- Quyết định chọn đường đi
- Chuyển mạch

Quá trình chọn đường đi được thực hiện ở lớp Mạng.Router dựa vào bảng định tuyến để chọn đường cho gói dữ liệu ,sau khi quyết định đường ra thì router thực hiện việc chuyển mạch để phát gói dữ liệu .

Chuyển mạch là quá trình mà router thực hiện để chuyển gói từ cổng nhận vào ra cổng phát đi .Điểm quan trọng của quá trình này là router phải đóng gói dữ liệu cho phù hợp với đường truyền mà gói chuẩn bị đi ra

3.2.2. Cấu hình định tuyến

Để cấu hình giao thức định tuyến ,chúng ta cần cấu hình trong chế độ cấu hình toàn cục và cài đặt các đặc điểm định tuyến .Bước đầu tiên ,ở chế độ cấu hình toàn cục,chúng ta cần khởi động giao thức định tuyến mà chúng ta muốn ,ví dụ nhưRIP,IRGP,EIGRP hay OSPF. Sau đó ,trong chế độ cấu hình định tuyến ,công việc chính là chúng ta khai báo địa chỉ IP .Định tuyến động thường sử dụng broadcast và multicast để trao đổi thông tin giữa các router .Router sẽ dựa vào thông số định tuyến để chọn đường tốt nhất tới từng mạng đích.

Lệnh router dùng để khởi động giao thức định tuyến .Lệnh network dùng để khai báo các cổng giao tiếp trên router mà ta muốn giao thức định tuyến gửi và nhận các thông tin cập nhật về định tuyến .

Sau đây là các ví dụ về cấu hình định tuyến:

- Athena_VanCong(config)#router rip
- Athena_VanCong(config-router)#network 172.16.1.0

Địa chỉ mạng khai báo trong câu lệnh network là địa chỉ mạng theo lớp A, B hoặc C chứ không phải là địa chỉ mạng con (subnet) hay địa chỉ host riêng lẻ .

3.2.3. Các giao thức định tuyến

Ở lớp Internet của bộ giao thức TCP/IP , router sử dụng một giao thức định tuyến IP để thực hiện việc định tuyến .Sau đây là một số giao thức định tuyến IP:

- RIP – giao thức định tuyến nội theo vector khoảng cách
- IGRP- giao thức định tuyến nội theo vector khoảng cách Cisco.
- OSPF – giao thức định tuyến nội theo trạng thái đường liên kết
- EIGRP- giao thức mở rộng của IGRP
- BGP- giao thức định tuyến ngoại theo vector khoảng cách

4. TỔNG QUAN VỀ GIAO THỨC ĐỊNH TUYẾN RIP

4.1. Giới thiệu giao thức RIP

RIP (Routing Information Protocol) là một giao thức định tuyến theo vector khoảng cách được sử dụng rộng rãi trên thế giới .Mặc dù RIP không có những khả năng và đặc điểm như những giao thức định tuyến khác nhưng RIP dựa trên những chuẩn mở và sử dụng đơn giản nên vẫn được các nhà quản trị mạng ưa dùng .Do đó RIP là một giao thức tốt để người học về mạng bước đầu làm quen, sau đây là các đặc điểm chính của RIP :

- Là giao thức định tuyến theo vector khoảng cách
- Sử dụng số lượng hop để làm thông số chọn đường đi
- Nếu số lượng hop để tới đích lớn hơn 15 thì gói dữ liệu sẽ bị huỷ bỏ
- Cập nhật theo định kỳ mặc định là 30 giây

4.2. Tiến trình của RIP

RIP được phát triển trong nhiều năm bắt đầu từ phiên bản 1 (RIPv1). RIP chỉ là giao thức định tuyến theo lớp địa chỉ cho đến phiên bản 2(RIPv2)

RIP trở thành giao thức định tuyến không theo lớp địa chỉ. RIPv2 có những ưu điểm hơn như sau:

- Cung cấp thêm nhiều thông tin định tuyến hơn.
- Có cơ chế xác minh giữa các router khi cập nhật để bảo mật cho bảng định tuyến.
- Có hỗ trợ VLSM(variable Length Subnet Masking-Subnet mask có chiều dài khác nhau).

RIP tránh định tuyến lặp vòng đếm đến vô hạn bằng cách giới hạn số lượng hop tối đa cho phép từ máy gửi đến máy nhận, số lượng hop tối đa cho mỗi con đường là 15. Đối với các con đường mà router nhận được từ thông tin cập nhật của router láng giềng, router sẽ tăng chỉ số hop lên 1 vì router xem bản thân nó cũng là 1 hop trên đường đi. Nếu sau khi tăng chỉ số hop lên 1 mà chỉ số này lớn hơn 15 thì router sẽ xem như mạng đích không tương ứng với con đường này không đến được. Ngoài ra, RIP cũng có những đặc tính tương tự như các giao thức định tuyến khác. Ví dụ như : RIP cũng có horizon và thời gian holddown để tránh cập nhật thông tin định tuyến không chính xác.

4.3. So sánh RIPv1 và RIPv2

RIP sử dụng thuật toán định tuyến theo vector khoảng cách. Nếu có nhiều đường đến cùng một đích thì RIP sẽ chọn đường có số hop ít nhất. Chính vì chỉ dựa vào số lượng hop để chọn đường nên đôi khi con đường mà RIP chọn không phải là đường nhanh nhất đến đích.

RIPv1 cho phép các router cập nhật bảng định tuyến của chúng theo chu kỳ mặc định là 30 giây. Việc gửi thông tin định tuyến cập nhật liên tục như vậy giúp cho topo mạng được xây dựng nhanh chóng. Để tránh bị lặp vòng vô tận, RIP giới hạn số hop tối đa để chuyển gói là 15 hop. Nếu một mạng đích xa hơn 15 router thì xem như mạng đích đó không thể tới được và gói dữ liệu đó sẽ bị huỷ bỏ. Điều này làm giới hạn khả năng mở rộng của RIP, RIPv1 sử dụng cơ chế split horizon để chống lặp vòng. Với cơ chế này khi gửi thông tin định tuyến ra một cổng giao tiếp, RIPv1 router không gửi ngược trở lại các thông tin định tuyến mà nó học được từ

chính công đó, RIPv1 còn sử dụng thời gian holddown để chống lặp vòng. Khi nhận được một thông báo về một mạng đích bị sự cố, router sẽ khởi động thời gian holddown. Trong suốt khoảng thời gian holddown router sẽ không cập nhật tất cả các thông tin có thông số định tuyến xấu hơn về mạng đích đó.

RIPv2 được phát triển từ RIPv1 nên nó cũng có các đặc tính như trên RIPv2 cũng là giao thức định tuyến theo vectơ khoảng cách sử dụng số lượng hop làm thông số định tuyến duy nhất. RIPv2 cũng sử dụng thời gian holddown và cơ chế split horizon để tránh lặp vòng. Sau đây là các điểm khác nhau giữa RIPv1 và RIPv2:

RIPv1	RIPv2
Cấu hình đơn giản	Cấu hình đơn giản
Định tuyến theo lớp địa chỉ	Định tuyến không theo lớp địa chỉ
Không gửi thông tin về subnet mask trong thông tin định tuyến.	Có gửi thông tin về subnet mask trong thông tin định tuyến.
Không hỗ trợ VLSM. Do đó tất cả các mạng trong hệ thống RIPv1 phải có cùng subnet mask.	Hỗ trợ VLSM. Các mạng trong hệ thống IPv2 có thể có chiều dài subnet mask khác nhau.
Không có cơ chế xác minh thông tin định tuyến.	Có cơ chế xác minh thông tin định tuyến.
Gửi quảng bá theo địa chỉ 255.255.255.255.	Gửi multicast theo địa chỉ 224.0.0.9 nên hiệu quả hơn.

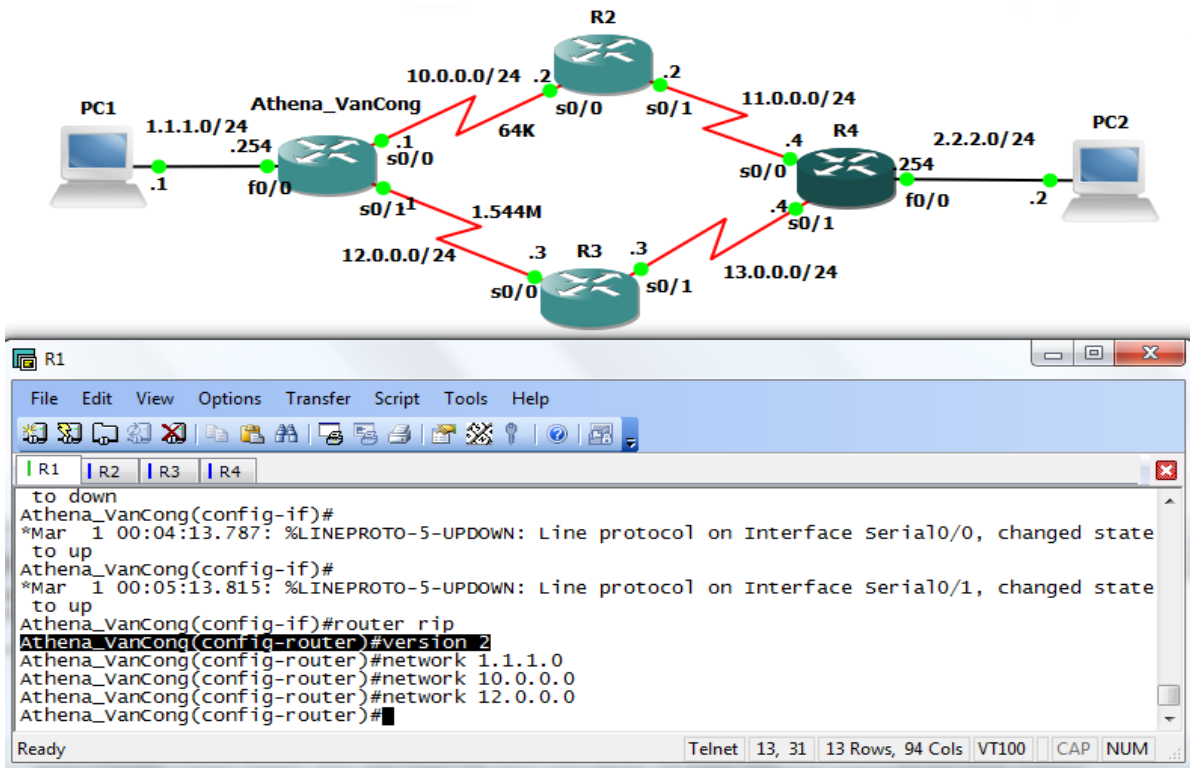
4.4. Cấu hình RIPv2

Lệnh router rip dùng để khởi động RIP. Lệnh network khai báo địa chỉ mạng IP tham gia và tiến trình định tuyến. Cổng nào của router có địa chỉ IP rơi vào trong địa chỉ mạng được khai báo ở lệnh network thì cổng đó sẽ tham gia vào quá trình gửi và nhận thông tin định tuyến cập nhật. Mặt khác lệnh network cũng khai báo những địa chỉ mạng mà router sẽ thực hiện quảng cáo về mạng đó.

Lệnh router rip version 2 xác định RIPv2 được chọn làm giao thức định tuyến chạy trên router.

Chúng ta có thể cấu hình cho RIP thực hiện cập nhật tức thời khi cấu trúc mạng thay đổi bằng lệnh ip rip triggered. Lệnh này chỉ áp dụng cho cổng serial của router. Khi cấu trúc mạng thay đổi, router nào nhận biết được sự thay đổi đầu tiên sẽ cập nhật vào bảng định tuyến của nó

trước, sau đó nó lập tức gửi thông tin cập nhật cho các router khác để thông báo về sự thay đổi đó. Hoạt động này là cập nhật tức thời và nó xảy ra hoàn toàn độc lập với cập nhật định kỳ.



- Athena_VanCong(config)# router rip – khởi động giao thức định tuyến RIP.
- Athena_VanCong(config- router)# version 2 – chạy phiên bản RIPv2
- Athena_VanCong(config- router)#network network- number -khai báo các mạng kết nối với router để quảng bá.

RIP là giao thức broadcast. Do đó, khi muốn chạy RIP trong mạng non-broadcast như Frame Relay thì ta cần phải khai báo các router RIP lắng giềng bằng lệnh sau:

Router(config- router) # neighbor ip address

Phần mềm Cisco IOS mặc nhiên nhận gói thông tin của cả RIP phiên bản 1 và 2 nhưng chỉ gửi đi gói thông tin bằng RIP phiên bản 1. Nhà quản trị mạng có thể cấu hình cho router chỉ gửi và nhận gói phiên bản 1 hoặc là chỉ gửi gói phiên bản 2...bằng các lệnh sau:

- Router(config- router) # version {1/2}
- Router(config- if) # ip rip send version 1
- Router(config- if) # ip rip send version 2
- Router(config- if) # ip rip send version 1 2

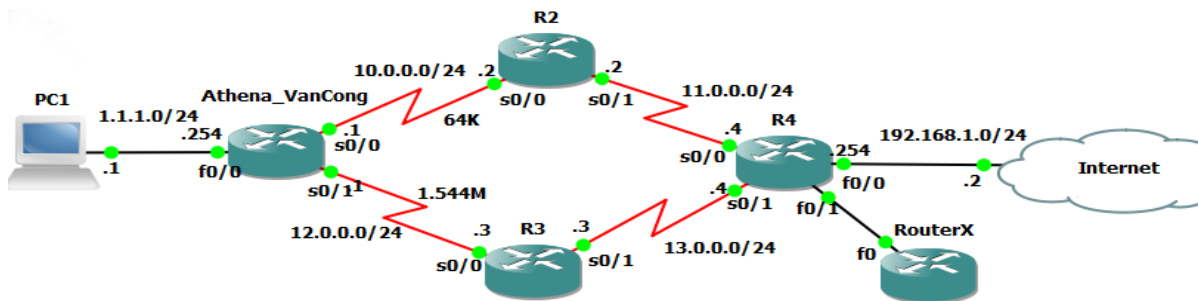
- Router(config- if) # ip rip receive version 1
- Router(config- if) # ip rip receive version 2
- Router(config- if) # ip rip receive version 1 2

Mặc định router học thông tin về đường đến mạng đích bằng 3 cách sau:

Đường cố định – là đường do người quản trị mạng cấu hình bằng tay cho router trong đó chỉ định rõ router kế tiếp để tới mạng đích. Đường cố định có khả năng bảo mật cao vì không có hoạt động gửi thông tin cập nhật như đường định tuyến động. Đường cố định rất hữu dụng khi chỉ có một đường duy nhất đến đích không còn đường nào khác phải chọn lựa.

Đường mặc định cũng do người quản trị mạng cấu hình bằng tay cho router. Trong đó khai báo đường mặc định để sử dụng khi router không biết đường đến đích. Với đường mặc định định tuyến router sẽ được ngắn gọn hơn. Khi gói dữ liệu có địa chỉ mạng đích mà router sẽ gửi nó ra đường mặc định.

Đường định tuyến động là những đường do router học được từ các router khác nhờ giao thức định tuyến động.



Giả sử hệ thống mạng này sử dụng giao thức định tuyến động. Router R4 có kết nối ra internet, kết nối này là đường mặc định của toàn bộ hệ thống mạng bên trong. Những gói nào không gửi đến các mạng bên trong nội bộ mà gửi ra ngoài thì mặc nhiên sẽ được gửi lên đường mặc định ra internet. Để khai báo đường mặc định cho router R4 chúng ta dùng lệnh sau :

```
R4(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2
```

Lệnh trên là lệnh cấu hình đường cố định đặc biệt đại diện cho bất kì mạng đích nào với bất kì subnetmask nào. Xin nhấn mạnh một lần nữa, lệnh trên được sử dụng để khai báo đường mặc định cho router nào có kết nối đường mặc định vào nó. Các router còn lại trong hệ thống, ta dùng lệnh `ip default-network` để khai báo mạng mặc định này cho các router:

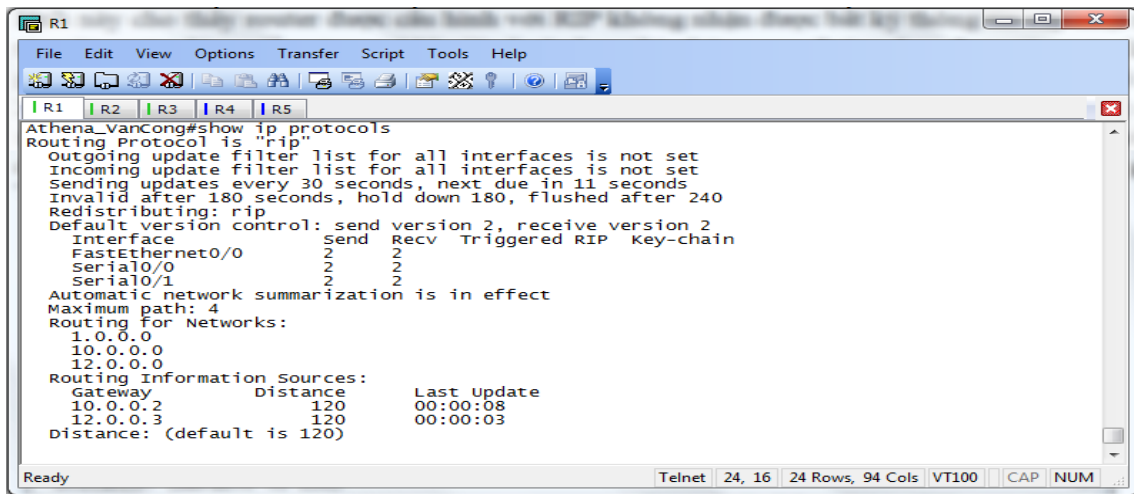
```
Router(config)#ip default-network 192.168.1.0
```

Các router R1, R2, R3, R5 sẽ sử dụng mạng 192.168.1.0 làm mạng đích mặc định. Những gói dữ liệu nào có địa chỉ đích mà các router nào không tìm thấy trên bảng định tuyến của chúng thì chúng sẽ gửi về mạng mặc định 192.168.1.0. Kết quả là các gói dữ liệu này được chuyển tới router R4. Trên router R4, với khai báo mặc định là iproute 0.0.0.0 0.0.0.0 192.168.1.2, các gói dữ liệu sẽ được truyền ra đường kết nối với Internet.

4.5. Kiểm tra cấu hình RIP

Có nhiều lệnh có thể sử dụng để kiểm tra cấu hình RIP có đúng hay không. Trong đó hai lệnh thường được sử dụng nhiều nhất là show ip route và show ip protocols.

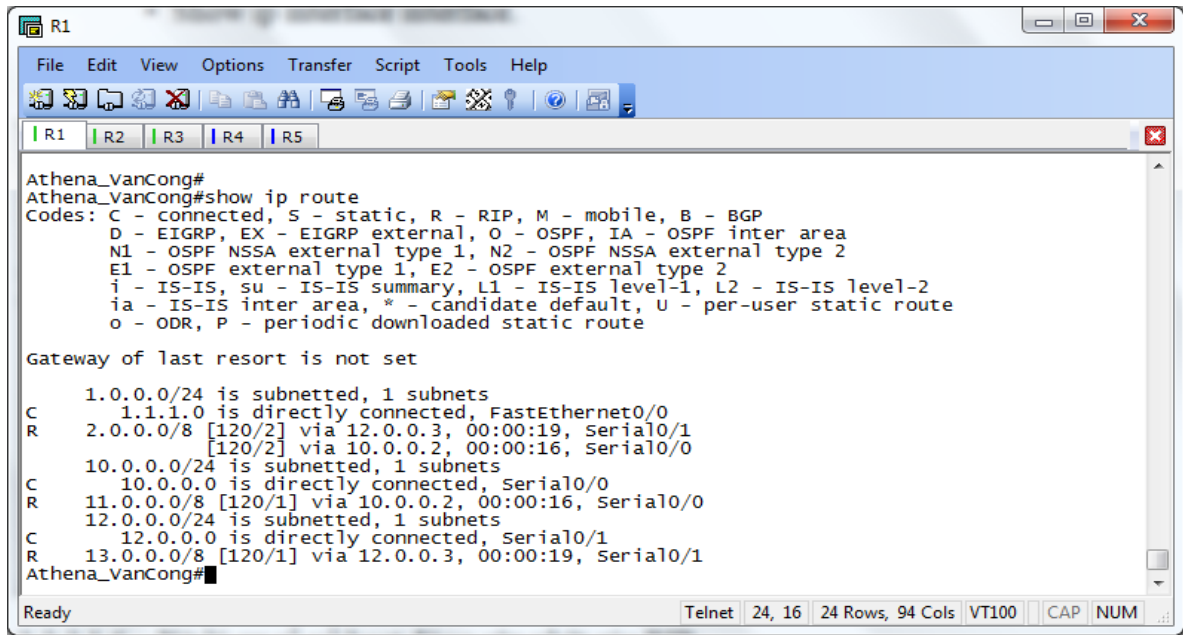
Lệnh show ip protocols sẽ hiển thị các giao thức định tuyến IP đang được chạy trên router. Lệnh này cho thấy router được cấu hình với RIP không nhận được bất kỳ thông tin cập nhật nào từ một router láng giềng trong 180 giây hoặc hơn thì những con đường học được từ router láng giềng đó sẽ được xem là không còn giá trị. Nếu vẫn không nhận thông tin cập nhật gì cả thì sau 240 giây, các con đường này sẽ bị xóa khỏi bảng định tuyến. Trong hình router Athena_VanCong nhận được cập nhật mới nhất từ router 2 cách đây 8 giây. Thời gian holddown 180 giây. Khi có một con đường được thông báo là đã bị ngắt con đường đó sẽ được đặt vào trạng thái holddown trong 180 giây.



```
Athena_VanCong#show ip protocols
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 11 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface        Send Recv Triggered RIP Key-chain
  FastEthernet0/0    2     2
  Serial0/0          2     2
  Serial0/1          2     2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    1.0.0.0
    10.0.0.0
    12.0.0.0
  Routing Information Sources:
    Gateway         Distance    Last Update
    10.0.0.2         120         00:00:08
    12.0.0.3         120         00:00:03
  Distance: (default is 120)
```

Lệnh show ip route được sử dụng để kiểm tra xem những đường đi mà router học được từ các router RIP láng giềng có được cài đặt vào bảng định tuyến không trên. Trên kết quả hiển thị bảng định tuyến, chúng ta kiểm tra các đường có đánh dấu bằng chữ “R” ở đầu dòng là những đường mà router học được từ các router RIP láng giềng. Chúng ta cũng nên nhớ rằng các router luôn có một khoảng thời gian để hội tụ với nhau, do đó các thông tin mới có thể chưa được hiển thị ngay trên bảng định tuyến được. Ngoài ra còn có một số lệnh khác mà chúng ta có thể sử dụng để kiểm tra cấu hình RIP :

- Show interface interface.
- Show ip interface interface.
- Show running –config



```

R1
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 R5
Athena_vanCong#
Athena_vanCong#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

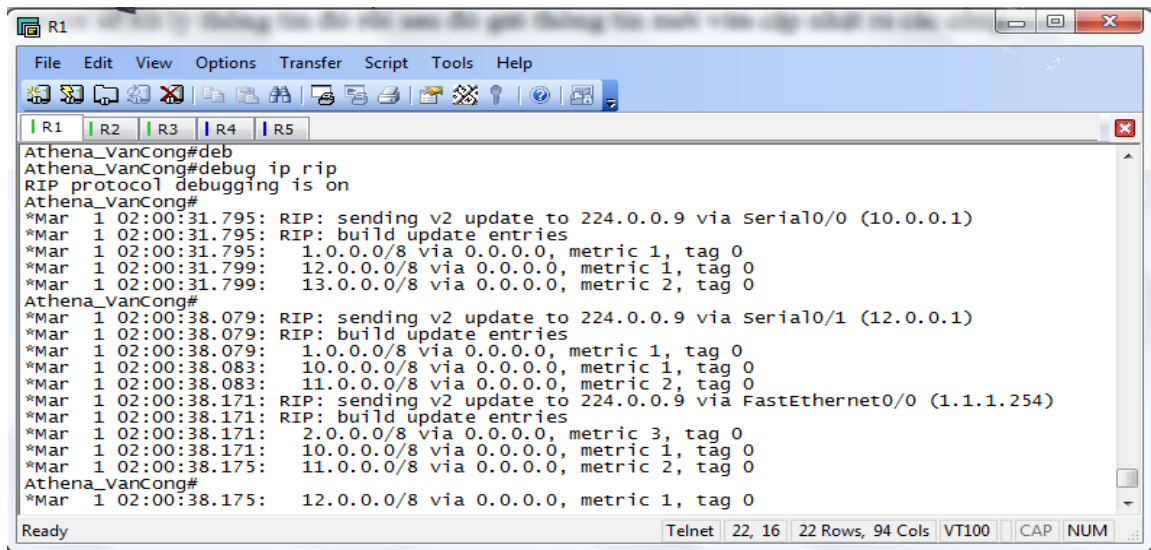
  1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, FastEthernet0/0
R    2.0.0.0/8 [120/2] via 12.0.0.3, 00:00:19, Serial0/1
      [120/2] via 10.0.0.2, 00:00:16, Serial0/0
 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Serial0/0
R    11.0.0.0/8 [120/1] via 10.0.0.2, 00:00:16, Serial0/0
 12.0.0.0/24 is subnetted, 1 subnets
C    12.0.0.0 is directly connected, Serial0/1
R    13.0.0.0/8 [120/1] via 12.0.0.3, 00:00:19, Serial0/1
Athena_vanCong#
Ready Telnet 24, 16 24 Rows, 94 Cols VT100 CAP NUM

```

4.6. Xử lý sự cố về hoạt động cập nhật của RIP

Hầu hết các lỗi cấu hình RIP đều do khai báo câu lệnh network sai, subnet không liên tục hoặc là do split horizon. Lệnh có tác dụng nhất trong việc tìm lỗi của RIP trong hoạt động cập nhật là lệnh debug ip rip

Lệnh debug ip rip sẽ hiển thị tất cả các thông tin định tuyến mà RIP gửi và nhận. Ví dụ hình dưới cho thấy kết quả hiển thị của lệnh debug ip rip. Sau khi nhận được thông tin cập nhật, router sẽ xử lý thông tin đó rồi sau đó gửi thông tin mới vừa cập nhật ra các cổng.



```
R1
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 R5
Athena_vanCong#deb
Athena_vanCong#debug ip rip
RIP protocol debugging is on
Athena_vanCong#
*Mar 1 02:00:31.795: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (10.0.0.1)
*Mar 1 02:00:31.795: RIP: build update entries
*Mar 1 02:00:31.795: 1.0.0.0/8 via 0.0.0.0, metric 1, tag 0
*Mar 1 02:00:31.799: 12.0.0.0/8 via 0.0.0.0, metric 1, tag 0
*Mar 1 02:00:31.799: 13.0.0.0/8 via 0.0.0.0, metric 2, tag 0
Athena_vanCong#
*Mar 1 02:00:38.079: RIP: sending v2 update to 224.0.0.9 via Serial0/1 (12.0.0.1)
*Mar 1 02:00:38.079: RIP: build update entries
*Mar 1 02:00:38.079: 1.0.0.0/8 via 0.0.0.0, metric 1, tag 0
*Mar 1 02:00:38.083: 10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
*Mar 1 02:00:38.083: 11.0.0.0/8 via 0.0.0.0, metric 2, tag 0
*Mar 1 02:00:38.171: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0 (1.1.1.254)
*Mar 1 02:00:38.171: RIP: build update entries
*Mar 1 02:00:38.171: 2.0.0.0/8 via 0.0.0.0, metric 3, tag 0
*Mar 1 02:00:38.171: 10.0.0.0/8 via 0.0.0.0, metric 1, tag 0
*Mar 1 02:00:38.175: 11.0.0.0/8 via 0.0.0.0, metric 2, tag 0
Athena_vanCong#
*Mar 1 02:00:38.175: 12.0.0.0/8 via 0.0.0.0, metric 1, tag 0
Ready Telnet 22, 16 22 Rows, 94 Cols VT100 CAP NUM
```

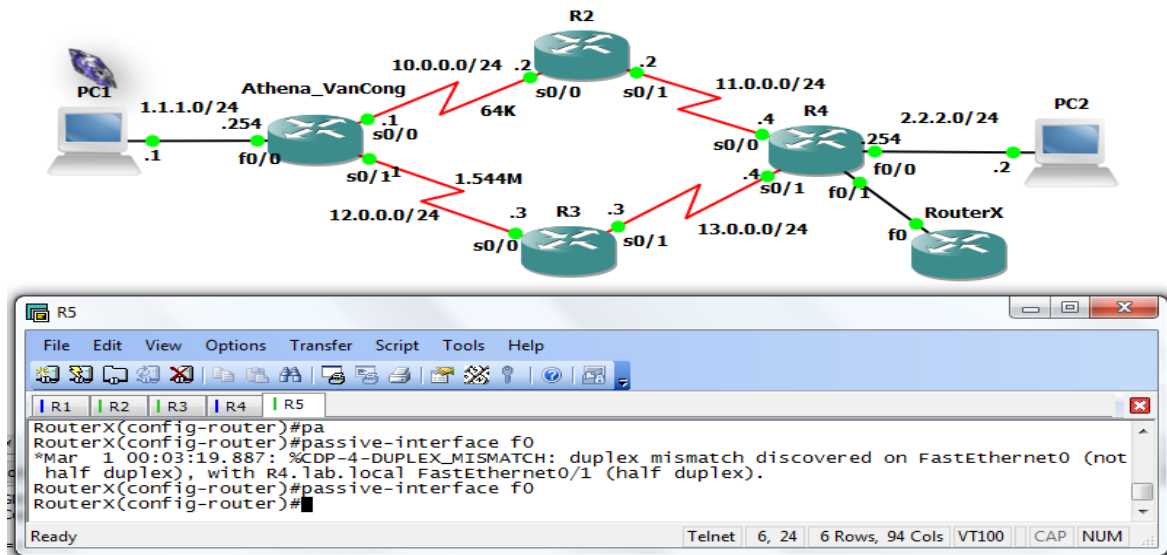
Có rất nhiều điểm quan trọng mà chúng ta cần chú ý trong kết quả hiển thị của lệnh debug ip rip. Một số vấn đề phải ví dụ như subnet không liên tục hay trùng subnet, có thể phát hiện được nhờ lệnh này. Trong những trường hợp như vậy chúng ta sẽ thấy là cùng một mạng đích nhưng router gửi thông tin đi thì mạng đích đó lại có thông số định tuyến thấp hơn so với khi router nhận vào trước đó.

- Ngoài ra còn một số lệnh có thể sử dụng để xử lý sự cố của RIP:
- Show ip database.
- Show ip protocols(summary).
- Show ip route.
- Debug ip rip{ events}.
- Show ip interface brief.

4.7. Ngăn không cho router gửi thông tin định tuyến ra một cổng giao tiếp

Router có thể thực hiện chọn lọc thông tin định tuyến khi cập nhật hoặc khi gửi thông tin cập nhật. Đối với router sử dụng giao thức định tuyến theo vector khoảng cách, cơ chế này có tác dụng vì router định tuyến dựa trên các thông tin định tuyến nhận được từ các router láng giềng. Tuy nhiên, đối với các router sử dụng giao thức định tuyến theo trạng thái đường liên kết thì cơ chế trên không hiệu quả vì các giao thức định tuyến này quyết định chọn đường đi dựa trên cơ sở dữ liệu về trạng thái các đường liên kết chứ không dựa vào thông tin định tuyến nhận được. Chính vì vậy mà cách thực hiện để ngăn không cho router gửi thông tin định tuyến ra một cổng giao tiếp được đề cập dưới đây chỉ sử dụng cho các giao thức định tuyến theo vector khoảng cách như RIP, IGRP thôi.

Chúng ta có thể sử dụng lệnh `passive interface` để ngăn không cho router gửi thông tin cập nhật về định tuyến ra một cổng nào đó. Làm như vậy thì chúng ta sẽ ngăn được hệ thống mạng khác học được các thông tin định tuyến trong hệ thống của mình.

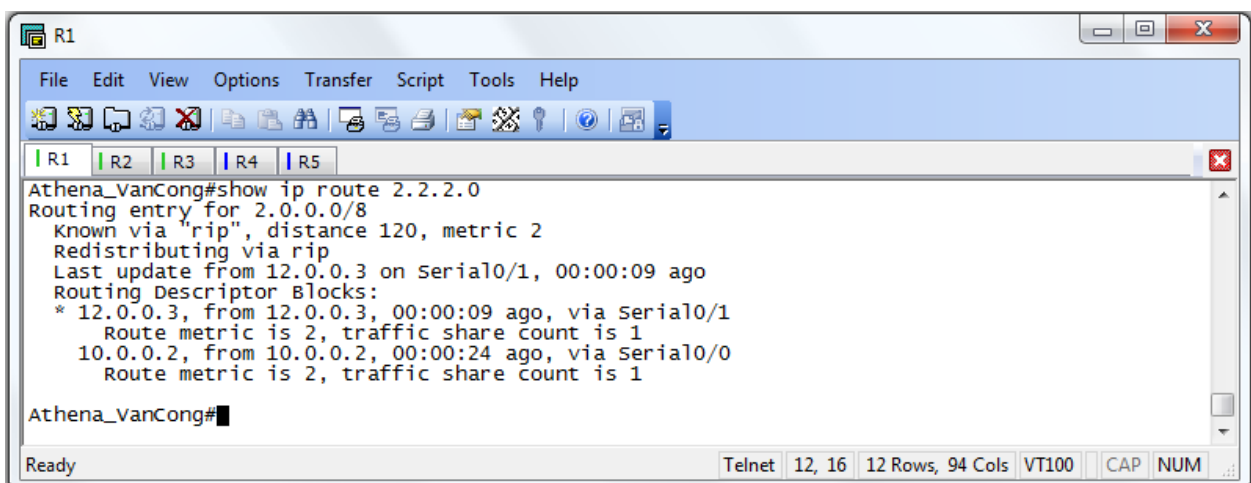


Router(config- router)#passive- interface Fa0/0.

4.8. Loadbalancing RIPv2

Router có thể chia tải ra nhiều đường khi có nhiều đường tốt đến cùng một đích. Chúng ta có thể cấu hình bằng tay cho router chia tải ra các đường hoặc là các giao thức định tuyến động có thể tự tính toán để chia tải.

RIP có khả năng chia tải ra tối đa là sáu đường có chi phí bằng nhau, còn mặc định thì RIP chỉ chia ra làm 4 đường. RIP thực hiện chia tải bằng cách sử dụng lần lượt và luân phiên từng đường.



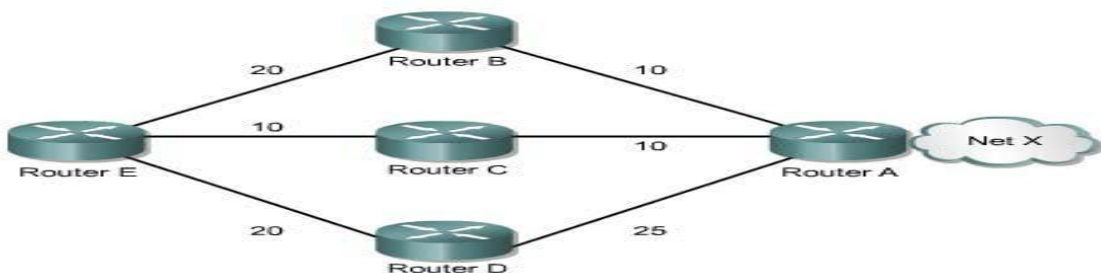
Ví dụ về kết quả hiển thị của lệnh show ip route. Trong đó, chúng ta thấy có hai phần, mỗi phần mô tả về một đường. Trong phần mô tả về đường thứ hai có dấu(*) ở đầu dòng. Dấu (*) này cho biết con đường này là con đường kế tiếp sẽ được sử dụng.

4.9. Chia tải cho nhiều đường

Router có khả năng chia tải ra nhiều đường để chuyển các gói dữ liệu đến cùng mục đích. Chúng ta có thể cấu hình bằng tay cho router thực hiện chia tải hoặc là các giao thức định tuyến động như RIP, IGRP, EIGRP và OSPF sẽ tự động tính toán. Khi router nhận được thông tin cập nhật về nhiều đường khác nhau đến cùng một đích thì router sẽ chọn đường nào có chỉ số tin cậy (Administrative distance) nhỏ nhất để đặt vào bảng định tuyến. Trong trường hợp các đường này có cùng chỉ số tin cậy thì router sẽ chọn đường nào có chi phí thấp nhất hoặc là đường nào có thông số định tuyến nhỏ nhất. Mỗi giao thức định tuyến sẽ có cách tính chi phí khác nhau và chúng ta cần phải cấu hình các chi phí này để router thực hiện chia tải.

Khi router có nhiều đường có cùng chỉ số tin cậy và cùng chi phí đến cùng một đích thì router sẽ thực hiện việc chia tải. Thông thường thì router có khả năng chia tải đến 6 đường có cùng chi phí (giới hạn tối đa số đường chia tải là phụ thuộc vào bảng định tuyến của Cisco IOS), tuy nhiên một số giao thức định tuyến nội (IGP) có thể có giới hạn riêng. Ví dụ như EIGRP chỉ cho phép tối đa là 4 đường.

Mặc định thì hầu hết các giao thức định tuyến IP đều chia tải ra 4 đường. Đường cố định thì chia tải ra 6 đường. Chỉ riêng BGP là ngoại lệ, mặc định của BGP là chỉ cho phép định tuyến 1 đường đến 1 đích.



Số đường tối đa mà router có thể chia tải là từ 1 đến 6 đường. Để thay đổi số đường tối đa cho phép chúng ta sử dụng lệnh sau:

- Router(config-router) #maximum-paths[number]

Khi định tuyến IP, Cisco IOS có hai cơ chế chia tải là: chia tải theo gói dữ liệu và chia tải theo địa chỉ đích. Nếu router chuyển mạch theo tiến trình thì router sẽ chia gói dữ liệu ra các

đường. Còn nếu router chuyển mạch nhanh thì router sẽ chuyển tất cả gói dữ liệu đến cùng một mạng đích thì sẽ tải ra đường kế tiếp. Cách này gọi là chia tải theo địa chỉ đích.

Administrative Distance	Route Source	Default Distance
Connected interface		0
Static route		1
Enhanced IGRP summary route		5
External BGP		20
Internal Enhanced IGRP		90
IGRP		100
OSPF		110
IS-IS		115
RIP		120
EIGRP external route		170
Internal BGP		200
Unknown		255

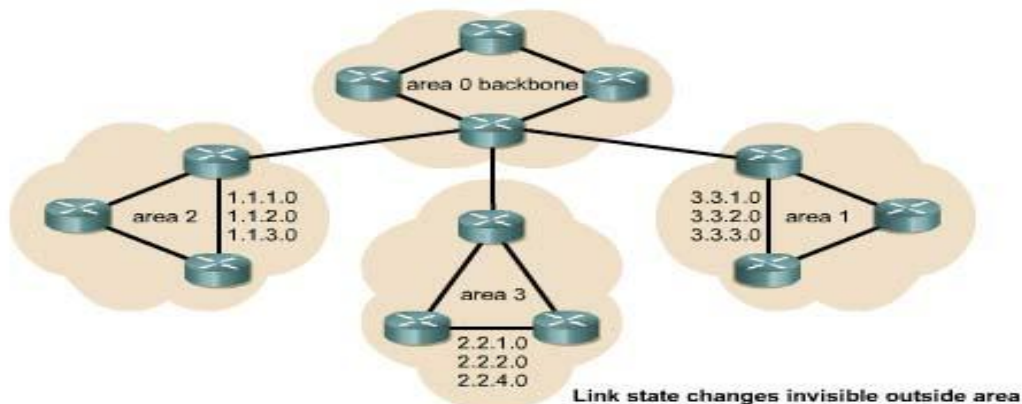
Đường cố định là đường do người quản trị cấu hình cho router chuyển gói tới mạng đích theo đường mà mình muốn. Mặt khác, lệnh để cấu hình đường cố định cũng được sử dụng để khai báo cho đường mặc định. Trong trường hợp router không tìm thấy đường nào trên bảng định tuyến để chuyển gói đến mạng đích thì router sẽ sử dụng đường mặc định.

Giao thức định tuyến có số AD nhỏ hơn lên luôn luôn được router chọn lựa trước. Khi đường định tuyến động bị sự cố không sử dụng được nữa thì router sẽ sử dụng tới đường định tuyến cố định để chuyển gói đến mạng đích.

5. TỔNG QUAN VỀ GIAO THỨC ĐỊNH TUYẾN OSPF

5.1. Giới thiệu về giao thức OSPF

OSPF là giao thức định tuyến theo trạng thái đường liên được triển khai dựa trên các chuẩn mở. OSPF được mô tả trong nhiều chuẩn của IETF (Internet Engineering Task Force). Chuẩn mở ở đây có nghĩa là OSPF hoàn toàn mở đối với công cộng, không có tính độc quyền.



Large OSPF networks are hierarchical and divided into multiple areas.

Nếu so sánh với RIPv1 và v2 thì OSPF là một giao thức định tuyến nội vi IGP tốt hơn vì khả năng mở rộng của nó. RIP chỉ giới hạn trong 15 hop, hội tụ chậm và đôi khi chọn đường có tốc độ chậm vì khi quyết định chọn đường nó không quan tâm đến các yếu tố quan trọng khác như băng thông chẳng hạn. OSPF khắc phục được các nhược điểm của RIP và nó là một giao thức định tuyến mạnh, có khả năng mở rộng, phù hợp với các hệ thống mạng hiện đại. OSPF có thể được cấu hình đơn vùng để sử dụng cho các mạng nhỏ.

Mạng OSPF lớn cần sử dụng thiết kế phân cấp và chia thành nhiều vùng. Các vùng này đều được kết nối vào cùng phân phối là vùng 0 hay còn gọi là vùng xương sống (backbone). Kiểu thiết kế này cho phép kiểm soát hoạt động cập nhật định tuyến. Việc phân vùng như vậy làm giảm tải của hoạt động định tuyến, tăng tốc độ hội tụ, giới hạn sự thay đổi của hệ thống mạng vào từng vùng và tăng hiệu suất hoạt động

Sau đây là các đặc điểm chính của OSPF:

- Là giao thức định tuyến theo trạng thái đường liên kết.
- Được định nghĩa trong RFC 2328.
- Sử dụng thuật toán SPF để tính toán chọn đường đi tốt nhất.
- Chỉ cập nhật khi cấu trúc mạng có sự thay đổi.

5.2. Cơ chế hoạt động của OSPF

OSPF thực hiện thu thập thông tin về trạng thái các đường liên kết từ các router láng giềng. Mỗi router OSPF quảng cáo trạng thái các đường liên kết của nó và chuyển tiếp các thông tin mà nó nhận được cho tất cả các láng giềng khác.

Router xử lý các thông tin nhận được để xây dựng một cơ sở dữ liệu về trạng thái các đường liên kết trong một vùng. Mọi router trong cùng một vùng OSPF sẽ có cùng một cơ sở dữ liệu này. Do đó mọi router sẽ có thông tin giống nhau về trạng thái của các đường liên kết và láng giềng của các router khác. Mỗi router áp dụng thuật toán SPF và cơ sở dữ liệu của nó để tính toán chọn đường tốt nhất đến từng mạng đích. Thuật toán SPF tính toán chi phí dựa trên băng thông của đường truyền. Đường nào có chi phí nhỏ nhất sẽ được chọn để đưa vào bảng định tuyến.

Mỗi router giữ một danh sách các láng giềng thân mật, danh sách này gọi là cơ sở dữ liệu các láng giềng thân mật. Các láng giềng được gọi là thân mật là những láng giềng mà router có thiết lập mối quan hệ hai chiều. Một router có thể có nhiều láng giềng nhưng không phải láng giềng nào cũng có mối quan hệ thân mật. Do đó chúng ta cần lưu ý mối quan hệ láng giềng khác với mối quan hệ láng giềng thân mật, hay gọi tắt là mối quan hệ thân mật. Đối với mỗi router danh sách láng giềng thân mật sẽ khác nhau.

Để giảm bớt số lượng trao đổi thông tin định tuyến với nhiều router láng giềng trong cùng một mạng, các router OSPF bầu ra một router đại diện gọi là Designated router (DR) và một router đại diện dự phòng gọi là Backup Designated (BDR) làm điểm tập trung các thông tin định tuyến.

5.3. Cấu hình tiến trình định tuyến OSPF

Định tuyến OSPF sử dụng khái niệm về vùng. Mỗi router xây dựng một cơ sở dữ liệu đầy đủ về trạng thái các đường liên kết trong một vùng. Một vùng trong mạng OSPF được cấp số từ 0 đến 65.535. Nếu OSPF đơn vùng thì đó là vùng 0. Trong mạng OSPF đa vùng, tất cả các vùng đều phải kết nối vào vùng 0. Do đó vùng 0 được gọi là vùng xương sống.

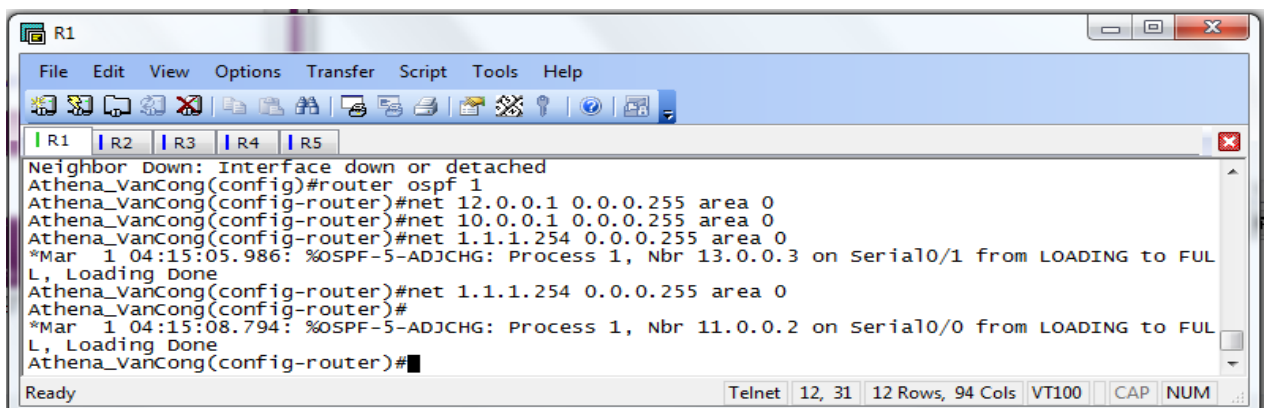
Trước tiên, chúng ta cần khởi động tiến trình định tuyến OSPF trên router, khai báo địa chỉ mạng và chỉ số vùng. Địa chỉ mạng được khai báo kèm theo wildcard mask chứ không phải là subnet mask. Chỉ số danh định (ID) của vùng được viết dưới dạng số hoặc dưới dạng số thập phân có dấu chấm tượng tự như IP.

Để khởi động định tuyến OSPF chúng ta dùng lệnh sau trong chế độ cấu hình toàn cục:

- Router (config)#router ospf process-id

Process-id là chỉ số xác định tiến trình định tuyến OSPF trên router. Chúng ta có thể khởi động nhiều tiến trình OSPF trên cùng một router. Chỉ số này có thể là bất kỳ giá trị nào trong khoảng từ 1 đến 65.535. Đa số các nhà quản trị mạng thường giữ chỉ số process-id này giống nhau trong cùng một hệ tự quản, nhưng điều này là không bắt buộc. Rất hiếm khi nào chúng ta cần chạy nhiều hơn một tiến trình OSPF trên một router. Chúng ta khai báo địa chỉ mạng cho OSPF như sau:

- Router(config-router)#network address wildcard-mask area area-id



```
R1
File Edit View Options Transfer Script Tools Help
R1 | R2 | R3 | R4 | R5
Neighbor Down: Interface down or detached
Athena_VanCong(config)#router ospf 1
Athena_VanCong(config-router)#net 12.0.0.1 0.0.0.255 area 0
Athena_VanCong(config-router)#net 10.0.0.1 0.0.0.255 area 0
Athena_VanCong(config-router)#net 1.1.1.254 0.0.0.255 area 0
*Mar 1 04:15:05.986: %OSPF-5-ADJCHG: Process 1, Nbr 13.0.0.3 on Serial0/1 from LOADING to FULL, Loading Done
Athena_VanCong(config-router)#net 1.1.1.254 0.0.0.255 area 0
Athena_VanCong(config-router)#
*Mar 1 04:15:08.794: %OSPF-5-ADJCHG: Process 1, Nbr 11.0.0.2 on Serial0/0 from LOADING to FULL, Loading Done
Athena_VanCong(config-router)#
Ready Telnet 12, 31 12 Rows, 94 Cols VT100 CAP NUM
```


Mỗi mạng được quy ước thuộc về một vùng. Address có thể là địa chỉ của toàn mạng, hoặc là một subnet hoặc là địa chỉ của một cổng giao tiếp. Wildcard-mask sẽ xác định chuỗi địa chỉ host nằm trong mạng mà chúng ta cần khai báo.

5.4. Cấu hình địa chỉ loopback cho OSPF và quyền ưu tiên cho router

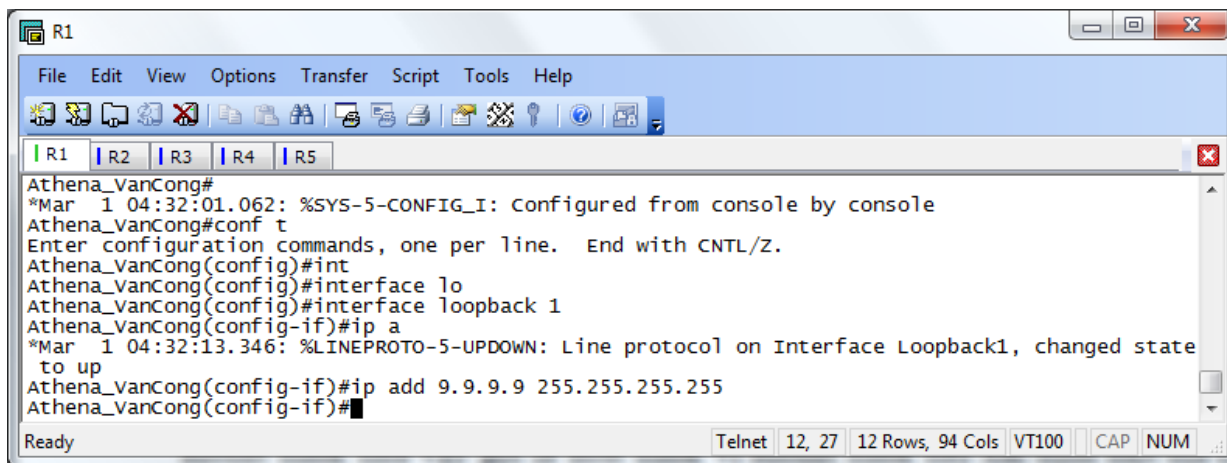
Khi tiến trình OSPF bắt đầu hoạt động, Cisco IOS sử dụng địa chỉ IP lớn nhất đang hoạt động trên router làm router ID. Nếu không có cổng nào đang hoạt động thì tiến trình OSPF không thể bắt đầu được. Khi router đã chọn địa chỉ IP của một cổng làm router ID và sau đó cổng này bị sự cố thì tiến trình sẽ bị mất router ID. Khi đó tiến trình OSPF sẽ bị ngưng hoạt động cho đến khi cổng đó hoạt động trở lại.

Để đảm bảo cho OSPF hoạt động ổn định chúng ta cần phải có một cổng luôn luôn tồn tại cho tiến trình OSPF. Chính vì vậy cần cấu hình một cổng loopback là một cổng luận lý chứ không phải cổng vật lý. Nếu có một cổng loopback được cấu hình thì OSPF sẽ sử dụng địa chỉ của cổng loopback làm router ID mà không quan tâm đến giá trị của địa chỉ này.

Nếu trên router có nhiều hơn một cổng loopback thì OSPF sẽ chọn địa chỉ IP lớn nhất trong các địa chỉ IP của các cổng loopback làm router ID. Để tạo cổng loopback và đặt địa chỉ IP cho nó chúng ta sử dụng các lệnh sau:

- Router (config)#interface loopback number
- Router (config-if)#ip address ip-address subnet-mask

Chúng ta nên sử dụng cổng loopback cho mọi router chạy OSPF. Cổng loopback này nên được cấu hình với địa chỉ có subnet mask là 255.255.255.255. Địa chỉ 32-bit subnet mask như vậy gọi là host mask vì subnet mask này xác định một địa chỉ mạng chỉ có một host. Khi OSPF phát quảng cáo về mạng loopback, OSPF sẽ luôn luôn quảng cáo loopback như là một host với 32-bit mask.



```
Athena_VanCong#
*Mar  1 04:32:01.062: %SYS-5-CONFIG_I: Configured from console by console
Athena_VanCong#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Athena_VanCong(config)#int
Athena_VanCong(config)#interface lo
Athena_VanCong(config)#interface loopback 1
Athena_VanCong(config-if)#ip a
*Mar  1 04:32:13.346: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state
to up
Athena_VanCong(config-if)#ip add 9.9.9.9 255.255.255.255
Athena_VanCong(config-if)#
```

Trong mạng quảng bá đa truy cập có thể có nhiều hơn hai router. Do đó, OSPF bầu ra một router đại diện (DR – Designated Router) làm điểm tập trung tất cả các thông tin quảng cáo và cập nhật về trạng thái của các đường liên kết. Vì vai trò của DR rất quan trọng nên một router đại diện dự phòng (BDR – Backup Designated Router) cũng được bầu ra để thay thế khi DR bị sự cố.

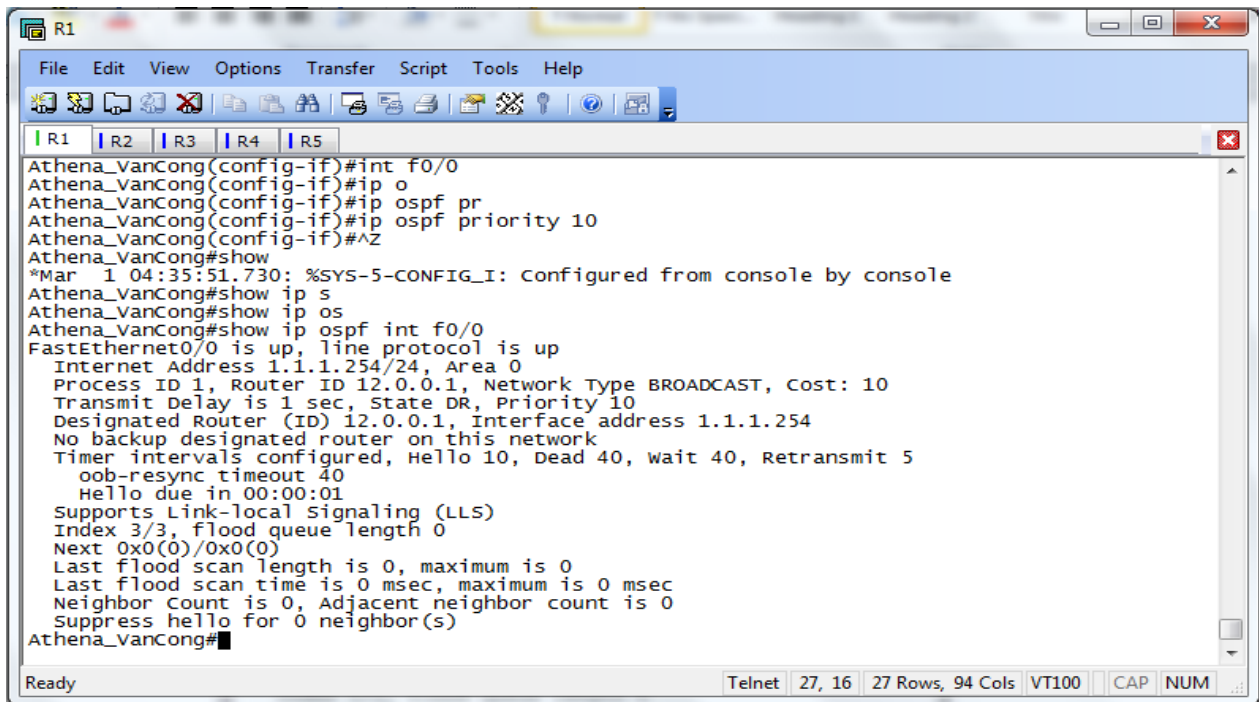
Đối với cổng kết nối vào mạng quảng bá, giá trị ưu tiên mặc định của OSPF trên cổng đó là 1. Khi giá trị OSPF ưu tiên của các router đều bằng nhau thì OSPF sẽ bầu DR dựa trên router ID. Router ID nào lớn nhất sẽ được chọn.

Chúng ta có thể quyết định kết quả bầu chọn DR bằng cách đặt giá trị ưu tiên cho cổng của router kết nối vào mạng đó. Cổng của router nào có giá trị ưu tiên cao nhất thì router đó chắc chắn là DR.

Giá trị ưu tiên có thể đặt bất kỳ giá trị nào nằm trong khoảng từ 0 đến 255. Giá trị 0 sẽ làm cho router đó không bao giờ được bầu chọn. Router nào có giá trị ưu tiên OSPF cao nhất sẽ được chọn làm DR. Router nào có vị trí ưu tiên thứ 2 sẽ là BDR. Sau khi bầu chọn xong, DR và BDR sẽ giữ luôn vai trò của nó cho dù chúng ta có đặt thêm router mới vào mạng với giá trị ưu tiên OSPF cao hơn.

Để thay đổi giá trị ưu tiên OSPF, chúng ta dùng lệnh `ip ospf priority` trên cổng nào cần thay đổi. Chúng ta dùng lệnh `show ip ospf interface` có thể xem được giá trị ưu tiên của cổng và nhiều thông tin quan trọng khác.

- Router(config-if)#ip ospf priority number
- Router#show ip ospf interface type number



```

R1
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 R5
Athena_VanCong(config-if)#int f0/0
Athena_VanCong(config-if)#ip 0
Athena_VanCong(config-if)#ip ospf pr
Athena_VanCong(config-if)#ip ospf priority 10
Athena_VanCong(config-if)#^Z
Athena_VanCong#show
*Mar 1 04:35:51.730: %SYS-5-CONFIG-I: Configured from console by console
Athena_VanCong#show ip s
Athena_VanCong#show ip os
Athena_VanCong#show ip ospf int f0/0
FastEthernet0/0 is up, line protocol is up
Internet Address 1.1.1.254/24, Area 0
Process ID 1, Router ID 12.0.0.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State DR, Priority 10
Designated Router (ID) 12.0.0.1, Interface address 1.1.1.254
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, wait 40, Retransmit 5
  oob-resync timeout 40
  Hello due in 00:00:01
Supports Link-local Signaling (LLS)
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 0, maximum is 0
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Athena_VanCong#
Ready Telnet 27, 16 27 Rows, 94 Cols VT100 CAP NUM

```

5.5. Thay đổi giá trị chi phí và chia tải của OSPF.

OSPF sử dụng chi phí làm thông số chọn đường tốt nhất. Giá trị chi phí này liên quan đến đường truyền và dữ liệu nhận vào của một cổng trên router. Nói tóm lại, chi phí của một kết nối được tính theo công thức $108/\text{băng thông}$, trong đó băng thông được tính theo đơn vị bit/s. Người quản trị mạng có thể cấu hình giá trị chi phí bằng nhiều cách. Cổng nào có chi phí thấp thì cổng đó sẽ được chọn để chuyển dữ liệu. Cisco IOS tự động tính chi phí dựa trên băng thông của cổng tương ứng. Do đó, để OSPF hoạt động đúng chúng ta cần cấu hình băng thông đúng cho cổng của router.

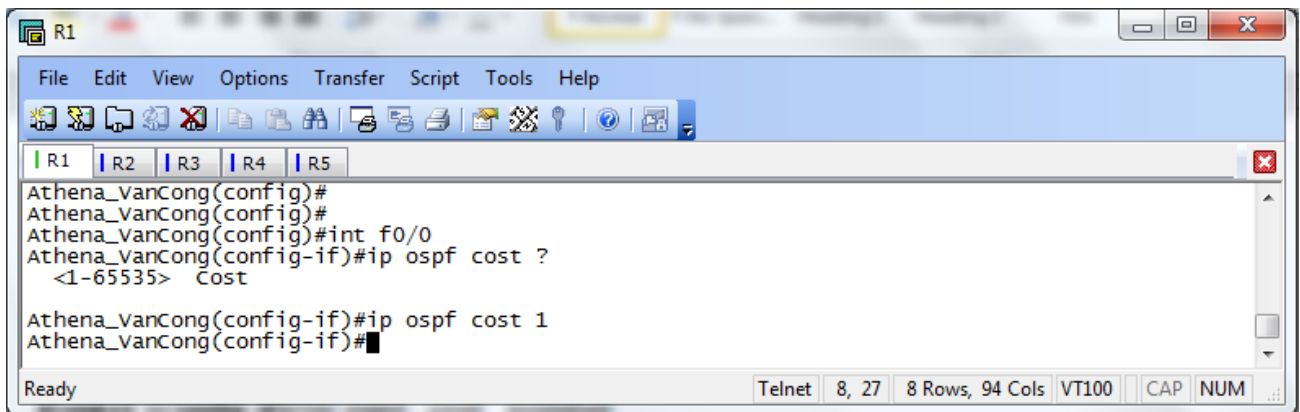
- Router (config)#interface <interface>
- Router(config-if)#bandwidth <băng thông>

Giá trị băng thông mặc định của cổng Serial Cisco là 1,544Mbps hay 1544kbs.

Medium	Cost
56 kbps serial link	1785
T1 (1.544 Mbps serial link)	64
E1 (2.048 Mbps serial link)	48
4 Mbps Token Ring	25
Ethernet	10
16 Mbps Token Ring	6
100 Mbps Fast Ethernet, FDDI	1

Giá trị chi phí thay đổi sẽ ảnh hưởng đến kết quả tính toán của OSPF. Trong môi trường định tuyến có nhiều hãng khác nhau, chúng ta sẽ phải thay đổi giá trị chi phí để giá trị chi phí của hãng này tương thích với giá trị chi phí của hãng kia. Một trường hợp khác chúng ta cần thay đổi giá trị chi phí khi sử dụng Gigabit Ethernet. Giá trị chi phí mặc định thấp nhất, giá trị 1, là tương ứng với kết nối 100Mbps. Do đó, khi trong mạng vừa có 100Mbps và Gigabit Ethernet thì giá trị chi phí mặc định sẽ làm cho việc định tuyến có thể không tối ưu. Giá trị chi phí nằm trong khoảng từ 1 đến 65.535. Chúng ta sử dụng câu lệnh sau trong chế độ cấu hình cổng tương ứng để cài đặt giá trị chi phí cho cổng đó:

- Router (config-if)#ip ospf cost number



Khi có nhiều đường để đi đến đích với cùng chi phí trong cùng một quá trình định tuyến, chúng ta sẽ có hiện tượng cân bằng tải, và các đường này cũng sẽ được đưa vào bảng định tuyến. Ta có thể chỉnh số lượng tối đa các đường đi đến cùng một đích bằng lệnh `maximum-paths` ở mode router. Khoảng giá trị của nó là từ 1 đến 64, mặc định cho OSPF là 16.

5.6. Cấu hình quá trình xác minh cho OSPF.

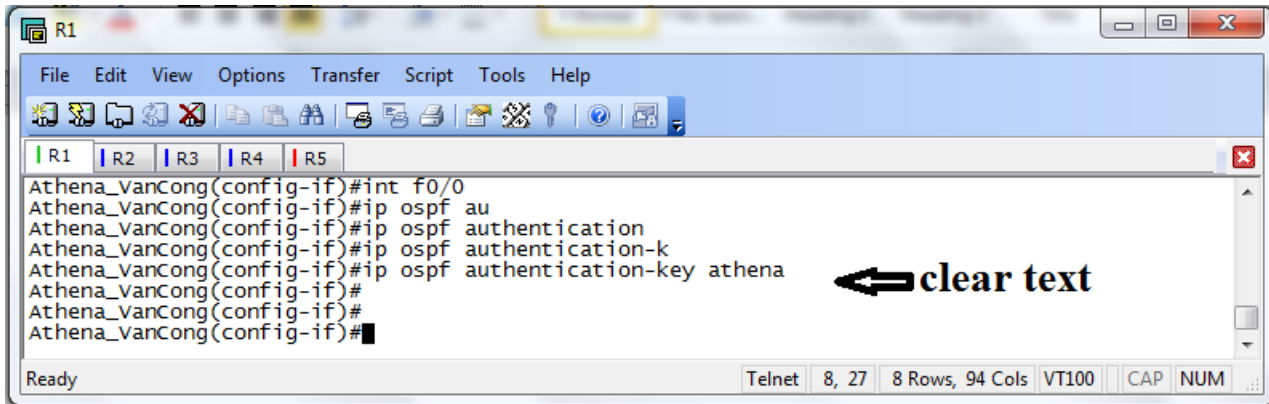
Các router mặc nhiên tin rằng những thông tin định tuyến mà nó nhận được là do đúng router tin cậy phát ra và những thông tin này không bị can thiệp dọc đường đi. Để đảm bảo điều này, các router trong một vùng cần được cấu hình để thực hiện xác minh với nhau.

Mỗi một cổng OSPF trên router cần có một chìa khoá xác minh để sử dụng khi gửi các thông tin OSPF cho các router khác cùng kết nối với cổng đó. Chìa khoá xác minh, hay còn gọi là mật mã, được chia sẻ giữa hai router. Chìa khoá này sử dụng để tạo ra dữ liệu xác minh (trường Authentication data) đặt trong phần header của gói OSPF. Mật mã này có thể dài đến 8 ký tự. Chúng ta sử dụng câu lệnh sau để cấu hình mật mã xác minh cho một cổng OSPF:

- Router (config-if)#ip ospf authentication-key password

Sau khi cấu hình mật mã xong, chúng ta cần bật chế độ xác minh cho OSPF:

- Router(config-router)#areaarea-number authentication



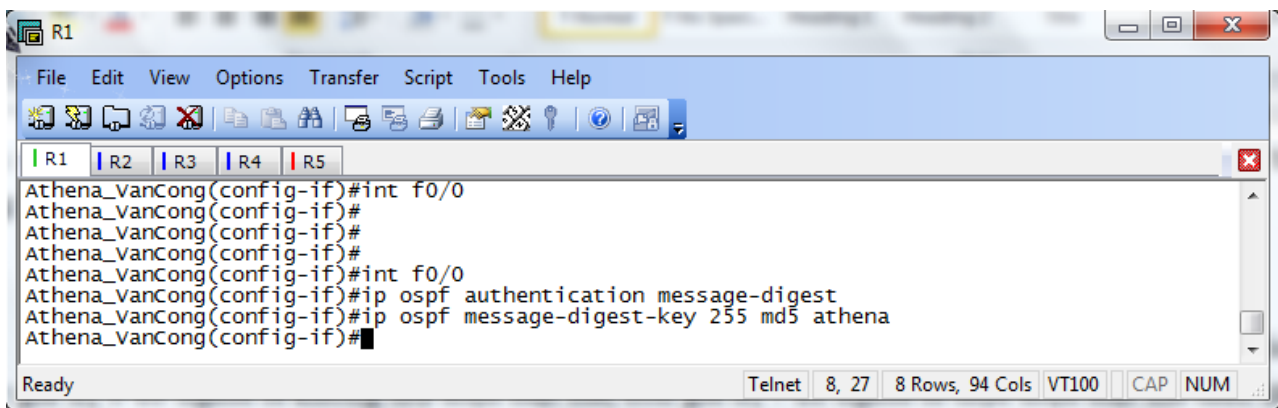
```
Athena_vanCong(config-if)#int f0/0
Athena_vanCong(config-if)#ip ospf au
Athena_vanCong(config-if)#ip ospf authentication
Athena_vanCong(config-if)#ip ospf authentication-k
Athena_vanCong(config-if)#ip ospf authentication-key athena
Athena_vanCong(config-if)#
Athena_vanCong(config-if)#
```

← clear text

Với cơ chế xác minh đơn giản trên, mật mã được gửi đi dưới dạng văn bản. Do đó nó dễ dàng được giải mã nếu gói OSPF bị những kẻ tấn công bắt được.

Chính vì vậy các thông tin xác minh nên được mật mã lại. Để đảm bảo an toàn hơn và thực hiện mật mã thông tin xác minh, chúng ta nên cấu hình mật mã message-digest bằng câu lệnh sau trên cổng tương ứng của router:

- Router(config-if)#ip ospf message-digest-key key-id encryption-type md5 key

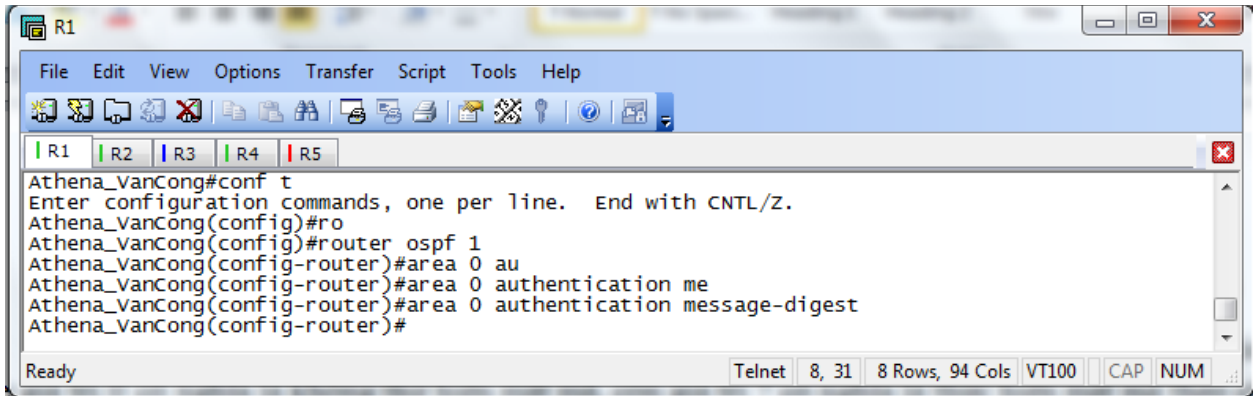


```
Athena_vanCong(config-if)#int f0/0
Athena_vanCong(config-if)#
Athena_vanCong(config-if)#
Athena_vanCong(config-if)#
Athena_vanCong(config-if)#int f0/0
Athena_vanCong(config-if)#ip ospf authentication message-digest
Athena_vanCong(config-if)#ip ospf message-digest-key 255 md5 athena
Athena_vanCong(config-if)#
```

MD5 là một thuật toán mật mã thông điệp message-digest. Nếu chúng ta đặt tham số encryption-type giá trị 0 có nghĩa là không thực hiện mật mã, còn giá trị 7 có nghĩa là thực hiện mật mã theo cách độc quyền của Cisco. Tham số key-id là một con số danh định có giá trị từ 1 đến 255. Tham số key là phần cho chúng ta khai báo mật mã, có thể dài đến 16 ký tự. Các router láng giềng bắt buộc phải có cùng số key-id và cùng giá trị key.

Sau khi cấu hình mật mã MD5 xong chúng ta cần bật chế độ xác minh message-digest trong OSPF:

- Router (config-router)#area area-id authentication message-digest



```
R1
File Edit View Options Transfer Script Tools Help
R1 R2 R3 R4 R5
Athena_VanCong#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Athena_VanCong(config)#ro
Athena_VanCong(config)#router ospf 1
Athena_VanCong(config-router)#area 0 au
Athena_VanCong(config-router)#area 0 authentication me
Athena_VanCong(config-router)#area 0 authentication message-digest
Athena_VanCong(config-router)#
Ready Telnet 8, 31 8 Rows, 94 Cols VT100 CAP NUM
```

Từ mật mã và nội dung của gói dữ liệu, thuật toán mật mã MD5 sẽ tạo ra một thông điệp gắn thêm vào gói dữ liệu. Router nhận gói dữ liệu sẽ dùng mật mã mà bản thân router có kết hợp với gói dữ liệu nhận được để tạo ra một thông điệp. Nếu kết quả hai thông điệp này giống nhau thì có nghĩa là router đã nhận được gói dữ liệu từ đúng nguồn và nội dung gói dữ liệu đã không bị can thiệp. Nếu cơ chế xác minh là message-digest thì trường authentication data sẽ có chứa key-id và thông số cho biết chiều dài của phần thông điệp gắn thêm vào gói dữ liệu. Phần thông điệp này giống như một con dấu không thể làm giả được.

5.7. Cấu hình các thông số thời gian của OSPF

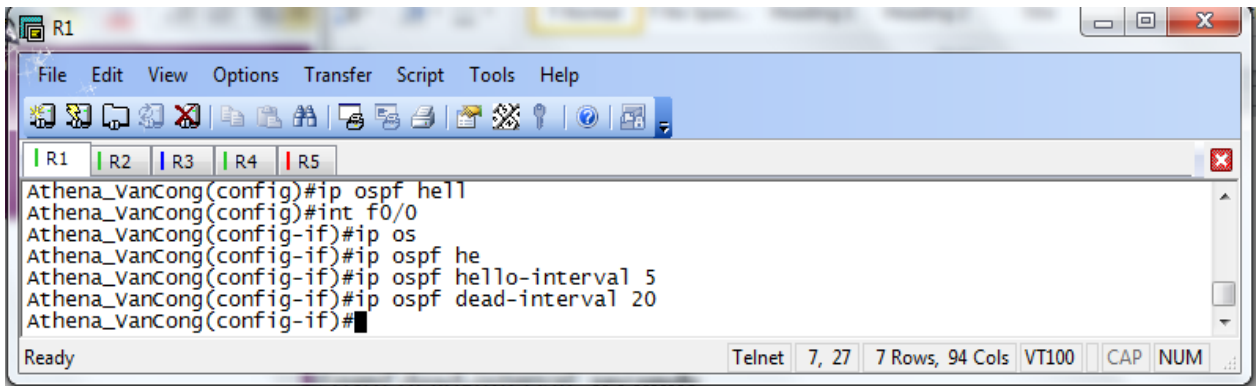
Các router OSPF bắt buộc phải có khoảng thời gian hello và khoảng thời gian bất động với nhau mới có thể thực hiện trao đổi thông tin với nhau. Mặc định, khoảng thời gian bất động bằng bốn lần khoảng thời gian hello. Điều này có nghĩa là một router có đến 4 cơ hội để gửi gói hello trước khi nó xác định là đã chết.

Trong mạng OSPF quảng bá, khoảng thời gian hello mặc định là 10 giây, khoảng thời gian bất động mặc định là 40 giây. Trong mạng không quảng bá, khoảng thời gian hello mặc định là 30 giây và khoảng thời gian bất động mặc định là 120 giây. Các giá trị mặc định này có ảnh hưởng đến hiệu quả hoạt động của OSPF và đôi khi chúng ta cần phải thay đổi chúng.

Người quản trị mạng được phép lựa chọn giá trị cho hai khoảng thời gian này. Để tăng hiệu quả hoạt động của mạng chúng ta cần ưu tiên thay đổi giá trị của hai khoảng thời gian này. Tuy nhiên, các giá trị này phải được cấu hình giống nhau cho mọi router láng giềng kết nối với nhau.

Để cấu hình khoảng thời gian hello và khoảng thời gian bất động trên một cổng của router, chúng ta sử dụng câu lệnh sau:

- Router (config-if)#ip ospf hello-interval seconds
- Router (config-if)#ip ospf dead-interval seconds



```
Athena_VanCong(config)#ip ospf hell
Athena_VanCong(config)#int f0/0
Athena_VanCong(config-if)#ip os
Athena_VanCong(config-if)#ip ospf he
Athena_VanCong(config-if)#ip ospf hello-interval 5
Athena_VanCong(config-if)#ip ospf dead-interval 20
Athena_VanCong(config-if)#
```

5.8. OSPF thực hiện quảng bá đường mặc định

Định tuyến OSPF đảm bảo các con đường đến tất cả các mạng đích trong hệ thống không bị lặp vòng. Để đến được các mạng nằm ngoài hệ thống thì OSPF cần phải biết về mạng đó hoặc là phải có đường mặc định. Tốt nhất là sử dụng đường mặc định vì nếu router phải lưu lại từng đường đi cho mọi mạng đích trên thế giới thì sẽ tốn một lượng tài nguyên khổng lồ.

Trên thực tế, chúng ta khai báo đường mặc định cho router OSPF nào kết nối ra ngoài. Sau đó thông tin về đường mặc định này được phân phối vào cho các router khác trong hệ tự quản (AS – autonomous system) thông qua hoạt động cập nhật bình thường của OSPF.

Trên router có cổng kết nối ra ngoài, chúng ta cấu hình mặc định bằng câu lệnh sau:

- Router (config)#ip route 0.0.0.0 0.0.0.0 [interface | next-hop address]

Mạng tám số 0 như vậy tương ứng với bất kỳ địa chỉ mạng nào. Sau khi cấu hình đường mặc định xong, chúng ta cấu hình cho OSPF chuyển thông tin về đường mặc định cho mọi router khác trong vùng OSPF:

- Router (config-router) #default – information originate

Mọi router trong hệ thống OSPF sẽ nhận biết được là có đường mặc định trên router biên giới kết nối ra ngoài.

5.9. Những lỗi thường gặp trong cấu hình OSPF

OSPF router phải thiết lập mối quan hệ láng giềng hoặc thân mật với OSPF router khác để trao đổi thông tin định tuyến. Mối quan hệ này không thiết lập được có thể do những nguyên nhân sau:

- Cả hai bên láng giềng với nhau đều không gửi Hello.
- Khoảng thời gian Hello và khoảng thời gian bất động không giống nhau giữa các router láng giềng.
- Loại cổng giao tiếp khác nhau giữa các router láng giềng.
- Mật mã xác minh và chìa khoá khác nhau giữa các router láng giềng.

Trong cấu hình định tuyến OSPF việc đảm bảo tính chính xác của các thông tin sau cũng vô cùng quan trọng:

- Tất cả các cổng giao tiếp phải có địa chỉ và subnet mask chính xác.
- Câu lệnh network area phải có wildcard mask chính xác.
- Câu lệnh network area phải khai báo đúng area mà network đó thuộc về.

5.10. Kiểm tra cấu hình OSPF

Để kiểm tra cấu hình OSPF chúng ta có thể dùng các lệnh show được liệt kê các lệnh show hữu dụng cho chúng ta khi tìm sự cố của OSPF như sau:

- Show ip protocol - Hiện thị các thông tin về thông số thời gian, thông số định tuyến, mạng định tuyến và nhiều thông tin khác của tất cả các giao thức định tuyến đang hoạt động trên router.
- Show ip ospf interface - Lệnh này cho biết cổng của router đã được cấu hình đúng với vùng mà nó thuộc về hay không. Nếu cổng loopback không được cấu hình thì ghi địa chỉ IP của cổng vật lý nào có giá trị lớn nhất sẽ được chọn làm router ID. Lệnh này cũng hiện thị các thông số của khoảng thời gian hello và khoảng thời gian bất động trên cổng đó, đồng thời cho biết các router láng giềng thân mật kết nối vào cổng.
- Show ip ospf - Lệnh này cho biết số lần đã sử dụng thuật toán SPF, đồng thời cho biết khoảng thời gian cập nhật khi mạng không có gì thay đổi.
- Show ip ospfneighbor detail - Liệt kê chi tiết các láng giềng, giá trị ưu tiên của chúng và trạng thái của chúng.
- Show ip ospf database - Hiện thị nội dung của cơ sở dữ liệu về cấu trúc hệ thống mạng trên router, đồng thời cho biết router ID, ID của tiến trình OSPF.

Các lệnh clear và debug dùng để kiểm tra hoạt động OSPF.

- Clear ip route * - Xoá toàn bộ bảng định tuyến.

- Clear ip route a.b.c.d - Xoá đường a.b.c.d trong bảng định tuyến.
- Debug ip ospf events- Báo cáo mọi sự kiện của OSPF.
- Debug ip ospf adj - Báo cáo mọi sự kiện về hoạt động quan hệ thân mật của OSPF.

6. TỔNG QUAN VỀ GIAO THỨC EIGRP

6.1. Giới thiệu

Enhanced Interior Gateway Routing Protocol (EIGRP) là một giao thức định tuyến độc quyền của Cisco được phát triển từ Interior Gateway Routing Protocol (IGRP). Không giống như IGRP là một giao thức định tuyến theo lớp địa chỉ, EIGRP có hỗ trợ định tuyến liên miền không theo lớp địa chỉ (CIDR – Classless Interdomain Routing) và cho phép người thiết kế mạng tối ưu không gian sử dụng địa chỉ bằng VLSM. So với IGRP, EIGRP có thời gian hội tụ nhanh hơn, khả năng mở rộng tốt hơn và khả năng chống lặp vòng cao hơn.

Hơn nữa, EIGRP còn thay thế được cho giao thức Novell Routing Information Protocol (Novell RIP) và Apple Talk Routing Table Maintenance Protocol (RTMP) để phục vụ hiệu quả cho cả hai mạng IPX và Apple Talk.

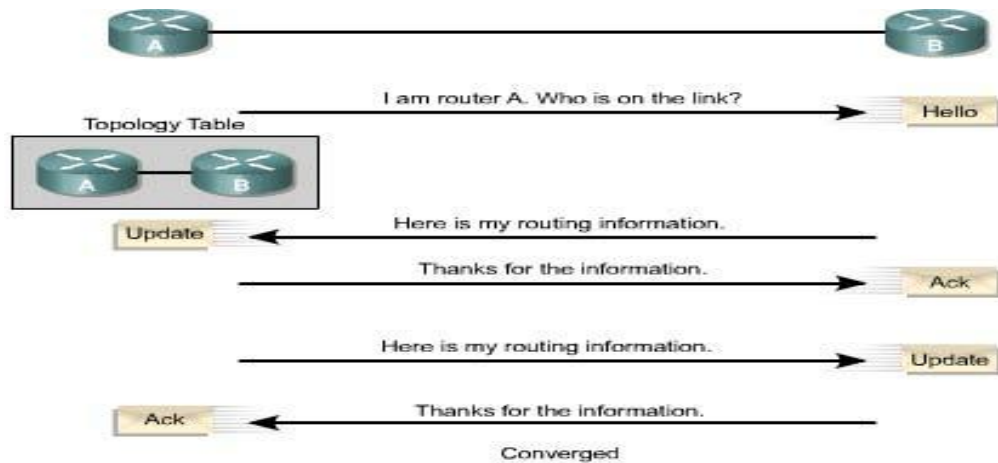
EIGRP thường được xem là giao thức lai vì nó kết hợp các ưu điểm của cả giao thức định tuyến theo vector khoảng cách và giao thức định tuyến theo trạng thái đường liên kết.

EIGRP là một giao thức định tuyến nâng cao hơn dựa trên các đặc điểm cả giao thức định tuyến theo trạng thái đường liên kết. Những ưu điểm tốt nhất của OSPF như thông tin cập nhật một phần, phát hiện router láng giềng...được đưa vào EIGRP. Tuy nhiên, cấu hình EIGRP dễ hơn cấu hình OSPF.

EIGRP là một lựa chọn lý tưởng cho các mạng lớn, đa giao thức được xây dựng dựa trên các Cisco router.

6.2. Các đặc điểm của EIGRP

EIGRP hoạt động khác với IGRP. Về bản chất EIGRP là một giao thức định tuyến theo vector khoảng cách nâng cao nhưng khi cập nhật và bảo trì thông tin láng giềng và thông tin định tuyến thì nó làm việc giống như một giao thức định tuyến theo trạng thái đường liên kết.



Sau đây là các ưu điểm của EIGRP so với giao thức định tuyến theo vector khoảng cách thông thường:

- Tốc độ hội tụ nhanh.
- Sử dụng băng thông hiệu quả.
- Có hỗ trợ VLSM (Variable – Length Subnet Mask) và CIDR (Classless Interdomain Routing). Không giống như IGRP, EIGRP có trao đổi thông tin về subnet mask nên nó hỗ trợ được cho hệ thống IP không theo lớp.
- Hỗ trợ nhiều giao thức mạng khác nhau.
- Không phụ thuộc vào giao thức định tuyến. Nhờ cấu trúc từng phần riêng biệt tương ứng với từng giao thức mà EIGRP không cần phải chỉnh sửa lâu. Ví dụ như khi phát triển để hỗ trợ một giao thức mới như IP chẳng hạn, EIGRP cần phải có thêm phần mới tương ứng cho IP nhưng hoàn toàn không cần phải viết lại EIGRP.

EIGRP router hội tụ nhanh vì chúng sử dụng DUAL. DUAL bảo đảm hoạt động không bị lặp vòng khi tính toán đường đi, cho phép mọi router trong hệ thống mạng thực hiện đồng bộ cùng lúc khi có sự thay đổi xảy ra.

EIGRP sử dụng băng thông hiệu quả vì nó chỉ gửi thông tin cập nhật một phần và giới hạn chứ không gửi toàn bộ bảng định tuyến. Nhờ vậy nó chỉ tốn một lượng băng thông tối thiểu khi hệ thống mạng đã ổn định. Điều này tương tự như hoạt động cập nhật của OSPF, nhưng không giống như router OSPF, router EIGRP chỉ gửi thông tin cập nhật một phần cho router nào cần thông tin đó mà thôi, chứ không gửi cho mọi router khác trong vùng như OSPF. Chính vì vậy mà hoạt động cập nhật của EIGRP gọi là cập nhật giới hạn. Thay vì hoạt động cập nhật theo chu kỳ, các router EIGRP giữ liên lạc với nhau bằng các gói hello rất nhỏ. Việc trao đổi các gói hello theo định kỳ không chiếm nhiều băng thông đường truyền.

EIGRP có thể hỗ trợ cho IP, IPX và Apple Talk nhờ có cấu trúc từng phần theo giao thức (PDMs – Protocol-dependent modules). EIGRP có thể phân phối thông tin của IPX RIP và SAP để cải tiến hoạt động toàn diện. Trên thực tế, EIGRP có thể điều khiển hai giao thức này. Router EIGRP nhận thông tin định tuyến và dịch vụ, chỉ cập nhật cho các router khác khi thông tin trong bảng định tuyến hay bảng SAP thay đổi.

EIGRP còn có thể điều khiển giao thức Apple Talk Routing Table Maintenance Protocol (RTMP). RTMP sử dụng số lượng hop để chọn đường nên khả năng chọn đường không được tốt lắm. Do đó, EIGRP sử dụng thông số định tuyến tổng hợp cấu hình được để chọn đường tốt nhất cho mạng Apple Talk. Là một giao thức định tuyến theo vectơ khoảng cách, RTMP thực hiện trao đổi toàn bộ thông tin định tuyến theo chu kỳ. Để giảm bớt sự quá tải này, EIGRP thực hiện phân phối thông tin định tuyến Apple Talk khi có sự kiện thay đổi mà thôi. Tuy nhiên, Apple Talk client cũng muốn nhận thông tin RTMP từ các router nội bộ, do đó EIGRP dùng cho Apple Talk chỉ nên chạy trong mạng không có client, ví dụ như các liên kết WAN chẳng hạn.

6.3. Cấu hình định tuyến EIGRP

Sử dụng lệnh sau để khởi động EIGRP và xác định con số của hệ tự quản:

- Router(config)#router eigrp autonomous-system-number

Thông số autonomous-system-number xác định các router trong một hệ tự quản. Những router nào trong cùng một hệ thống mạng thì phải có con số này giống nhau.

Khai báo những mạng nào của router mà chúng ta đang cấu hình thuộc về hệ tự quản EIGRP:

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

Thông số network-number là địa chỉ mạng của các cổng giao tiếp trên router thuộc về hệ thống mạng EIGRP. Router sẽ thực hiện quảng cáo thông tin về những mạng được khai báo trong câu lệnh network này. Network là những mạng nào kết nối trực tiếp vào router.

Khi cấu hình cổng serial để sử dụng trong EIGRP, việc quan trọng là cần đặt băng thông cho cổng này. Nếu chúng ta không thay đổi băng thông của cổng, EIGRP sẽ sử dụng băng thông mặc định của cổng thay vì băng thông thực sự. Nếu đường kết nối thực sự chậm hơn, router có thể không hội tụ được, thông tin định tuyến cập nhật có thể bị mất hoặc là kết quả chọn đường không tối ưu. Để đặt băng thông cho một cổng serial trên router, chúng ta dùng câu lệnh sau trong chế độ cấu hình của cổng đó:

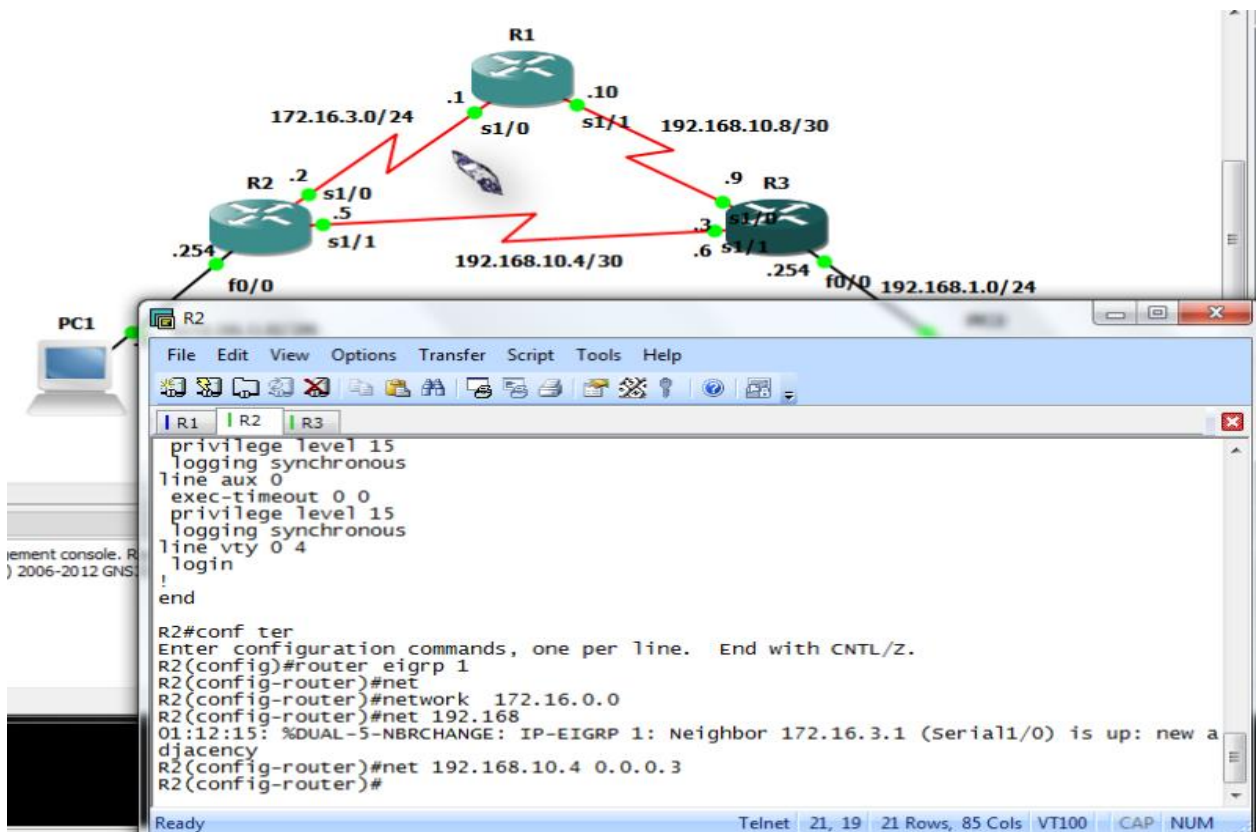
- Router(config-if)#bandwidth kilobits

Giá trị băng thông khai trong lệnh bandwidth chỉ được sử dụng tính toán cho tiến trình định tuyến, giá trị này nên khai đúng với tốc độ của cổng.

Cisco còn khuyến cáo nên thêm câu lệnh sau trong cấu hình EIGRP:

- Router(config-if)#eigrp log-neighbor-changes

Câu lệnh này sẽ làm cho router xuất ra các câu thông báo mỗi khi có sự thay đổi của các router láng giềng thân mật giúp chúng ta theo dõi sự ổn định của hệ thống định tuyến và phát hiện được sự cố nếu có.



Với EIGRP, việc tổng hợp đường đi có thể được cấu hình bằng tay trên từng cổng của router với giới hạn tổng hợp mà chúng ta muốn chứ không tự động tổng hợp theo lớp của địa chỉ IP. Sau khi khai báo địa chỉ tổng hợp cho một cổng của router, router sẽ phát quảng cáo ra cổng đó các địa chỉ được tổng hợp như một câu lệnh đó cài đặt.

Địa chỉ tổng hợp được khai báo bằng lệnh ip summary-address eigrp như sau:

- Router(config-if)# ip summary-address eigrp autonomous-system-number ip-addressmask administrative-distance

Đường tổng hợp của EIGRP có chỉ số mặc định của độ tin cậy (administrative- distance) là 5. Tuy nhiên, chúng ta có thể khai báo giá trị cho chỉ số này trong khoảng từ 1 đến 255. Trong đa số các trường hợp, khi chúng ta muốn cấu hình tổng hợp địa chỉ bằng tay thì chúng ta nên tắt chế độ tự động tổng hợp bằng lệnh `no auto-summary`.

6.4. Cấu hình xác thực EIGRP

EIGRP hỗ trợ kiểu xác thực MD5.

- Router(config)# interface <interface>

Vào chế độ cấu hình interface

- Router(config-if)# ip authenticationmode eigrp as-number md5

Cho phép thuật toán MD5 sẽ được sử dụng để xác thực đối với các gói tin của EIGRP trên các interface.

- Router(config-if)# ip authenticaitonkey-chain eigrp as-number athena

Cho phép xác thực các gói tin của EIGRP. athena là tên của key chain.

- Router(config-if)# exit Trở về chế độ cấu hình Privileged.
- Router(config)# key chain athena

Tạo ra một key chain. Tên của key chain đó phải tương ứng với tên đã được cấu hình trong mode interface.

- Router(config-keychain)# key 1

Xác định chỉ số của key.

* Chú ý: Chỉ số của key có thể nằm trong khoảng từ 0 đến 2147483647. Chỉ số key đó không cần phải liên tiếp nhau. Cần phải tạo ít nhất một key trong một key chain.

- Router(config-keychain-key)# keystring vancong

Xác định key string.

* Chú ý: một key string có thể chứa từ 1 đến 80 ký tự và trong đó bao gồm cả các ký tự thường, hoa, đặc biệt, số.

- Router(config-keychainkey)# accept-lifetime start-time {infinite | end-time | durationseconds}

Tùy chọn này sẽ chỉ ra khoảng thời gian mà key sẽ được nhận.

- Router(config-keychain-key)# sendlifetime start-time {infinite | endtime | duration seconds}

Tùy chọn này chỉ ra khoảng thời gian mà key sẽ được gửi.

6.5. Chia tải trong EIGRP

Một đặc điểm nổi trội của EIGRP là giao thức này cho phép cân bằng tải ngay cả trên những đường không đều nhau. Điều này giúp tận dụng tốt hơn các đường truyền nối đến router. Nếu một đường đi đến đích của một router mà không có Feasibel Successor, thì nó sẽ không được sử dụng để thực hiện cơ chế cân bằng tải. Giao thức định tuyến EIGRP hỗ trợ cân bằng tải tối đa là 6 đường có cost không bằng nhau.

- Router(config)# router eigrp as-number

Cho phép router hoạt động với giao thức định tuyến EIGRP với số AS

- Router(config-router)# network network-address

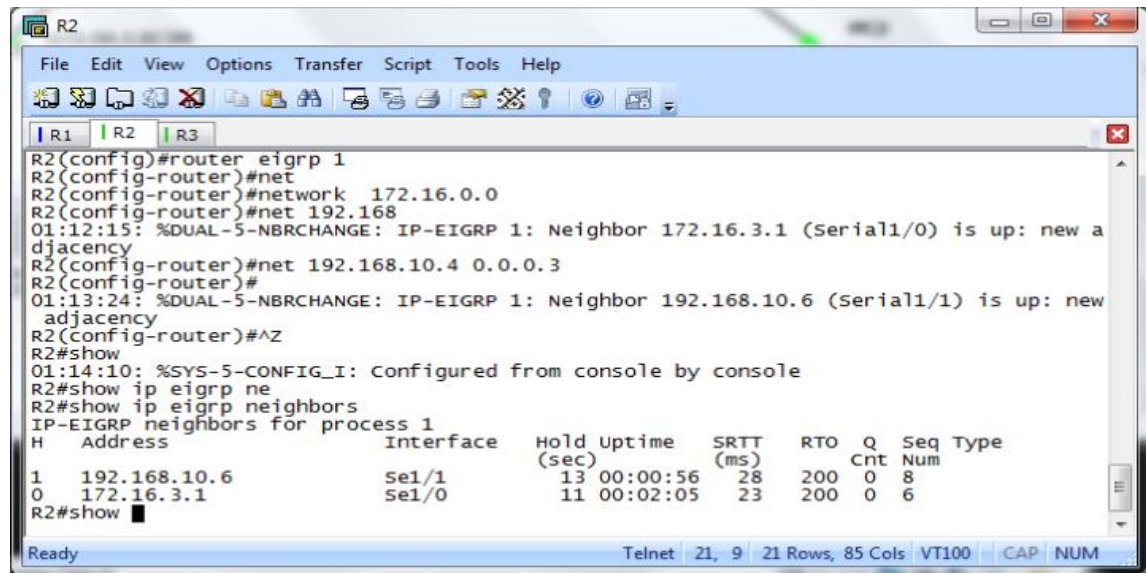
Chỉ ra những mạng sẽ được quảng bá bởi EIGRP.

- Router(config-router)# variance <n>

Router sẽ chọn những đường đi có metric nhỏ hơn hoặc bằng $n \times \text{metric}$ thấp nhất của router đó đến mạng đích. Trong đó n là chỉ số được chỉ ra bởi câu lệnh variance

6.6. Kiểm tra hoạt động của EIGRP

Chúng ta sử dụng các lệnh show như sau để kiểm tra các hoạt động của EIGRP. Ngoài ra, các lệnh debug là những lệnh giúp chúng ta theo dõi hoạt động EIGRP khi cần thiết.



```

R2
File Edit View Options Transfer Script Tools Help
R1 R2 R3
R2(config)#router eigrp 1
R2(config-router)#net
R2(config-router)#network 172.16.0.0
R2(config-router)#net 192.168
01:12:15: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial1/0) is up: new a
djacency
R2(config-router)#net 192.168.10.4 0.0.0.3
R2(config-router)#
01:13:24: %DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.6 (Serial1/1) is up: new
adjacency
R2(config-router)#^Z
R2#show
01:14:10: %SYS-5-CONFIG_I: Configured from console by console
R2#show ip eigrp ne
R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H Address Interface Hold Uptime SRTT RTO Q Seq Type
1 192.168.10.6 Se1/1 13 00:00:56 28 200 0 8
0 172.16.3.1 Se1/0 11 00:02:05 23 200 0 6
R2#show
Ready Telnet 21, 9 21 Rows, 85 Cols VT100 CAP NUM

```

Show ip eigrpneighbors [type number] [details]

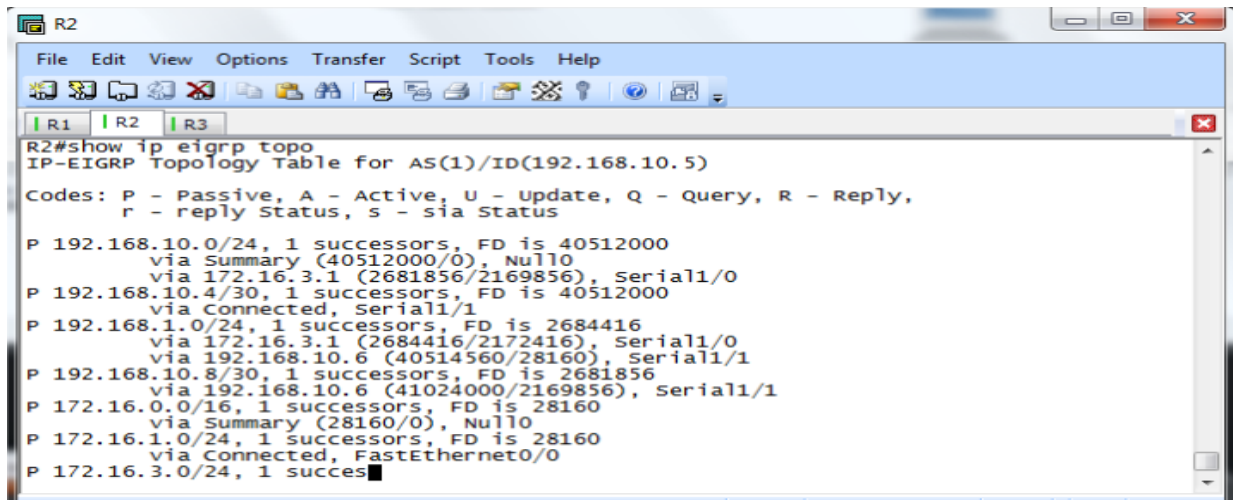
Hiển thị bảng láng giềng của EIGRP. Sử dụng tham số type number để xác định cụ thể công cần xem. Từ khoá details cho phép hiển thị thông tin chi tiết hơn.

Show ip eigrpinterfaces [type number] [as- number] [details]

Hiển thị thông tin EIGRP của các cổng. Sử dụng các tham số in nghiêng cho phép giới hạn phần thông tin hiển thị cho từng cổng hoặc trong từng AS. Từ khoá details cho phép hiển thị thông tin chi tiết hơn.

Show ip eigrptopology [as- number] [[ip- address] mask]

Hiển thị tất cả các feasible successor trong bảng cấu trúc mạng của EIGRP. Sử dụng các tham số in nghiêng để giới hạn thông tin hiển thị theo số AS hay theo địa chỉ mạng cụ thể.



```

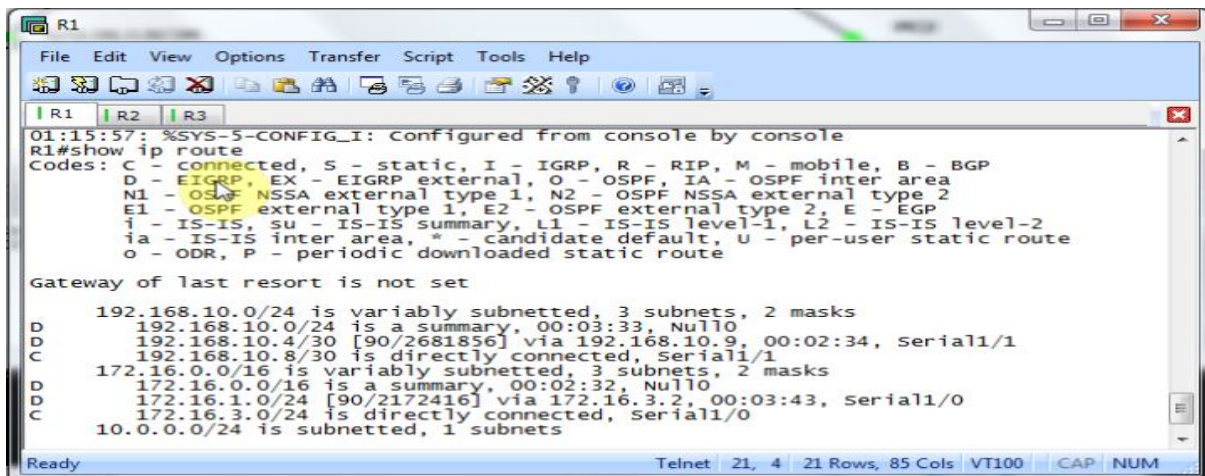
R2
File Edit View Options Transfer Script Tools Help
R1 R2 R3
R2#show ip eigrp topo
IP-EIGRP Topology Table for AS(1)/ID(192.168.10.5)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 192.168.10.0/24, 1 successors, FD is 40512000
   via Summary (40512000/0), Null0
   via 172.16.3.1 (2681856/2169856), Serial1/0
P 192.168.10.4/30, 1 successors, FD is 40512000
   via Connected, Serial1/1
P 192.168.1.0/24, 1 successors, FD is 2684416
   via 172.16.3.1 (2684416/2172416), Serial1/0
   via 192.168.10.6 (40514560/28160), Serial1/1
P 192.168.10.8/30, 1 successors, FD is 2681856
   via 192.168.10.6 (41024000/2169856), Serial1/1
P 172.16.0.0/16, 1 successors, FD is 28160
   via Summary (28160/0), Null0
P 172.16.1.0/24, 1 successors, FD is 28160
   via Connected, FastEthernet0/0
P 172.16.3.0/24, 1 succes
  
```

Show ip eigrptopology [active | pending | zero- successors]

Tùy theo chúng ta sử dụng từ khoá nào, router sẽ hiển thị thông tin về các đường đi đang hoạt động, đang chờ xử lý hay không có successor.

Show ip eigrp topology all-links - Hiển thị thông tin về mọi đường đi chứ không chỉ cófeasible successor trong bảng cấu trúc EIGRP.

Show ip eigrp traffic [as-number] - Hiển thị số gói EIGRP đó gửi đi và nhận được.Chúng ta sử dụng tham số as-number để giới hạn thưng tin hiển thịtrong một AS cụ thể.



```

R1
File Edit View Options Transfer Script Tools Help
R1 R2 R3
01:15:57: %SYS-5-CONFIG-I: Configured from console by console
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D   192.168.10.0/24 is a summary, 00:03:33, Null0
D   192.168.10.4/30 [90/2681856] via 192.168.10.9, 00:02:34, Serial1/1
C   192.168.10.8/30 is directly connected, Serial1/1
D   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D   172.16.0.0/16 is a summary, 00:02:32, Null0
D   172.16.1.0/24 [90/2172416] via 172.16.3.2, 00:03:43, Serial1/0
C   172.16.3.0/24 is directly connected, Serial1/0
10.0.0.0/24 is subnetted, 1 subnets
  
```

Các lệnh debug:

Debug eigrp fsm -Hiển thị hoạt động của các EIGRP feasible successor giúp chúng ta xác định khi nào tiến trình định tuyến cài đặt và xóa thông tin cập nhật về đường đi.

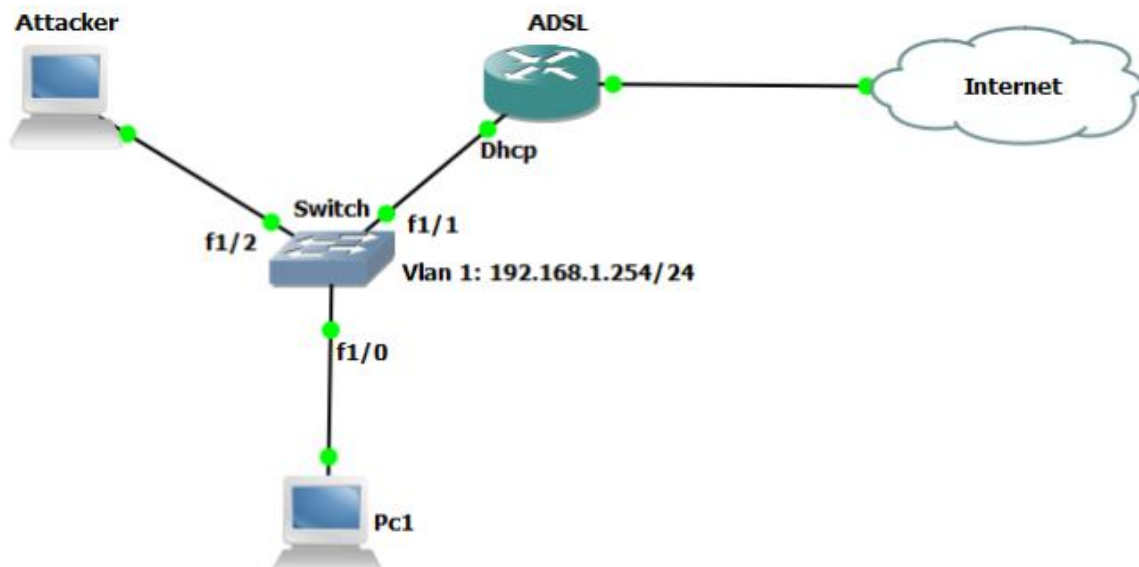
Debug eigrp packet - Hiện thị các gói EIGRP gửi đi và nhận được. Các gói này có thể là gói hello, cập nhật, báo nhận, yêu cầu hoặc hồi đáp. Số thứ tự của gói và chỉ số báo nhận được sử dụng để gửi bảo đảm các gói EIGRP cũng được hiển thị.

7. SNIFFER TRONG MẠNG CISCO VÀ CÁCH PHÒNG CHỐNG

7.1. Khái niệm Sniffer

Khởi đầu Sniffer là tên một sản phẩm của Network Associates có tên là Sniffer Network Analyzer. Sniffer được hiểu đơn giản như là một chương trình cố gắng nghe ngóng các lưu lượng thông tin trên (trong một hệ thống mạng). Tương tự như là thiết bị cho phép nghe lén trên đường dây điện thoại. Chỉ khác nhau ở môi trường là các chương trình Sniffer thực hiện nghe lén trong môi trường mạng máy tính.

Tuy nhiên những giao dịch giữa các hệ thống mạng máy tính thường là những dữ liệu ở dạng nhị phân (Binary). Bởi vậy để nghe lén và hiểu được những dữ liệu ở dạng nhị phân này, các chương trình Sniffer phải có tính năng được biết như là sự phân tích các giao thức (Protocol Analysis), cũng như tính năng giải mã (Decode) các dữ liệu ở dạng nhị phân sang dạng khác để hiểu được chúng. Trong một hệ thống mạng sử dụng những giao thức kết nối chung và đồng bộ. Chúng ta có thể sử dụng Sniffer ở bất cứ Host nào trong hệ thống mạng của chúng ta. Chế độ này được gọi là chế độ hỗn tạp (promiscuous mode).



Đối tượng Sniffing là :

- Password (từ Email, Web, SMB, FTP, SQL hoặc Telnet)
- Các thông tin về thẻ tín dụng

- Văn bản của Email
- Các tập tin đang di động trên mạng (tập tin Email, FTP hoặc SMB)

7.2. Mục đích sử dụng

Sniffer thường được sử dụng vào 2 mục đích khác biệt nhau. Nó có thể là một công cụ giúp cho các quản trị mạng theo dõi và bảo trì hệ thống mạng của mình. Cũng như theo hướng tiêu cực nó có thể là một chương trình được cài vào một hệ thống mạng máy tính với mục đích đánh hơi, nghe lén các thông tin trên đoạn mạng này...

Dưới đây là một số tính năng của Sniffer được sử dụng theo cả hướng tích cực và tiêu cực :

- Tự động chụp các tên người sử dụng (Username) và mật khẩu không được mã hoá (Clear Text Password). Tính năng này thường được các Hacker sử dụng để tấn công hệ thống của chúng ta.
- Chuyển đổi dữ liệu trên đường truyền để những quản trị viên có thể đọc và hiểu được ý nghĩa của những dữ liệu đó.
- Bằng cách nhìn vào lưu lượng của hệ thống cho phép các quản trị viên có thể phân tích những lỗi đang mắc phải trên hệ thống lưu lượng của mạng. Ví dụ như : Tại sao gói tin từ máy A không thể gửi được sang máy B...
- Một số Sniffer tân tiến còn có thêm tính năng tự động phát hiện và cảnh báo các cuộc tấn công đang được thực hiện vào hệ thống mạng mà nó đang hoạt động (Intrusion Detecte Service).
- Ghi lại thông tin về các gói dữ liệu, các phiên truyền... Tương tự như hộp đen của máy bay, giúp các quản trị viên có thể xem lại thông tin về các gói dữ liệu, các phiên truyền sau sự cố... Phục vụ cho công việc phân tích, khắc phục các sự cố trên hệ thống mạng.

7.3. Các giao thức có thể sử dụng Sniffing

- Telnet và Rlogin : ghi lại các thông tin như Password, usernames
- HTTP: Các dữ liệu gửi đi mà không mã hóa
- SMTP : Password và dữ liệu gửi đi không mã hóa
- NNTP : Password và dữ liệu gửi đi không mã hóa
- POP : Password và dữ liệu gửi đi không mã hóa
- FTP : Password và dữ liệu gửi đi không mã hóa
- IMAP : Password và dữ liệu gửi đi không mã hóa

7.4. Phương thức hoạt động Sniffer

Công nghệ Ethernet được xây dựng trên một nguyên lý chia sẻ. Theo một khái niệm này thì tất cả các máy tính trên một hệ thống mạng cục bộ đều có thể chia sẻ đường truyền của hệ thống mạng đó. Hiểu một cách khác tất cả các máy tính đó đều có khả năng nhìn thấy lưu lượng dữ liệu được truyền trên đường truyền chung đó. Như vậy phần cứng Ethernet được xây dựng với tính năng lọc và bỏ qua tất cả những dữ liệu không thuộc đường truyền chung với nó.

Nó thực hiện được điều này trên nguyên lý bỏ qua tất cả những Frame có địa chỉ MAC không hợp lệ đối với nó. Khi Sniffer được tắt tính năng lọc này và sử dụng chế độ hỗn tạp (promiscuous mode). Nó có thể nhìn thấy tất cả lưu lượng thông tin từ máy B đến máy C, hay bất cứ lưu lượng thông tin giữa bất kỳ máy nào trên hệ thống mạng. Miễn là chúng cùng nằm trên một hệ thống mạng.

7.4.1. Active

Là Sniffing qua Switch, nó rất khó thực hiện và dễ bị phát hiện. Attacker thực hiện loại tấn công này như sau:

- Attacker kết nối đến Switch bằng cách gởi địa chỉ MAC nặc danh
- Switch xem địa chỉ kết hợp với mỗi khung (frame)
- Máy tính trong LAN gởi dữ liệu đến cổng kết nối

7.4.2. Passive

Đây là loại Sniffing lấy dữ liệu chủ yếu qua Hub. Nó được gọi là Sniffing thụ động vì rất khó có thể phát hiện ra loại Sniffing này. Attacker sử dụng máy tính của mình kết nối đến Hub và bắt đầu Sniffing

7.5. Các kiểu tấn công

7.5.1. Man in the Middle

Một trong những tấn công mạng thường thấy nhất được sử dụng để chống lại những cá nhân và các tổ chức lớn chính là các tấn công MITM (Man in the Middle). Có thể hiểu nôm na về kiểu tấn công này thì nó như một kẻ nghe trộm. MITM hoạt động bằng cách thiết lập các kết nối đến máy tính nạn nhân và relay các message giữa chúng. Trong trường hợp bị tấn công, nạn nhân cứ tin tưởng là họ đang truyền thông một cách trực tiếp với nạn nhân kia, trong khi đó sự thực thì các luồng truyền thông lại bị thông qua host của kẻ tấn công. Và kết quả là các host này không chỉ có thể thông dịch dữ liệu nhạy cảm mà nó còn có thể gửi xen vào cũng như thay đổi luồng dữ liệu để kiểm soát sâu hơn những nạn nhân của nó.

Giả sử hacker muốn theo dõi hostA gởi thông tin gì cho hostB. Đầu tiên hacker sẽ gởi gói Arp reply đến hostA với nội dung là địa chỉ MAC của hacker và địa chỉ IP của hostB. Tiếp theo

hacker sẽ gửi gói Arp reply tới hostB với nội dung là MAC của máy hacker và IP của hostA. Như vậy cả hai hostA và hostB đều tiếp nhận gói Arp reply đó và lưu vào trong Arp table của mình. Đến lúc này khi hostA muốn gửi thông tin cho hostB nó liền tra vào Arp table thấy đã có sẵn thông tin về địa chỉ MAC của hostB nên hostA sẽ lấy thông tin đó ra sử dụng, nhưng thực chất địa chỉ MAC đó là của hacker. Đồng thời máy tính của hacker sẽ mở chức năng gọi là IP Forwarding giúp chuyển tải nội dung mà hostA gửi qua hostB. HostA và hostB giao tiếp bình thường và không có cảm giác bị qua máy trung gian là máy của hacker.

Trong trường hợp khác, hacker sẽ nghe lén thông tin từ máy chúng ta đến Gateway. Như vậy mọi hàng động ra internet của chúng ta đều bị hacker ghi lại hết, dẫn đến việc mất mát các thông tin nhạy cảm.

7.5.2. MAC Flooding

Kiểu tấn công làm tràn bảng CAM dựa vào điểm yếu của thiết bị chuyển mạch: bảng CAM chỉ chứa được một số hữu hạn các ánh xạ

(ví dụ như switch Catalyst 6000 có thể chứa được tối đa 128000 ánh xạ) và các ánh xạ này không phải tồn tại mãi mãi trong bảng CAM. Sau một khoảng thời gian nào đó, thường là 300 s, nếu địa chỉ này không được dùng trong việc trao đổi thông tin thì nó sẽ bị gỡ bỏ khỏi bảng.

Khi bảng CAM được điền đầy, tất cả thông tin đến sẽ được gửi đến tất cả các cổng của nó trừ cổng nó nhận được. Lúc này chức năng của switch không khác gì chức năng của một hub.

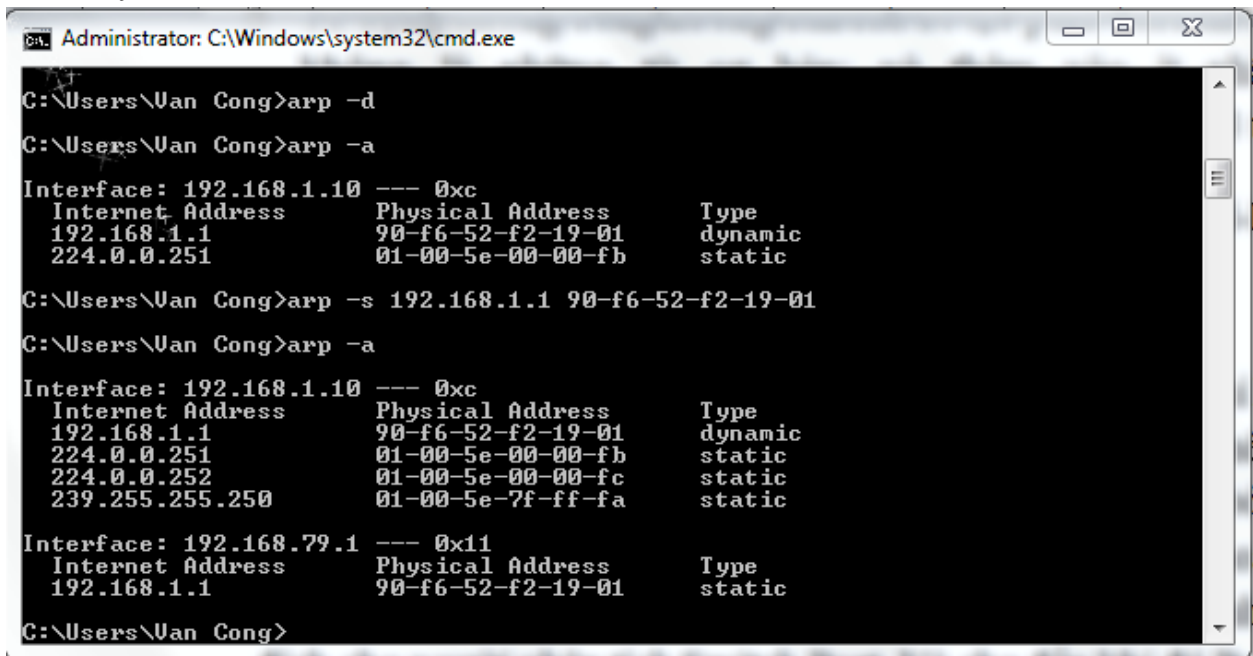
Cách tấn công này cũng dùng kỹ thuật Arp poisoning mà đối tượng nhắm đến là Switch. Hacker sẽ gửi những gói Arp reply giả tạo với số lượng khổng lồ nhằm làm Switch xử lý không kịp và trở nên quá tải. Khi đó Switch sẽ không đủ sức thể hiện bản chất Layer2 của mình nữa mà broadcast gói tin ra toàn bộ các port của mình. Hacker dễ dàng bắt được toàn bộ thông tin trong mạng của chúng ta.

7.6. Phòng chống sniffer

Để ngăn chặn những kẻ tấn công muốn Sniffer Password. Chúng ta đồng thời sử dụng các giao thức, phương pháp để mã hoá password cũng như sử dụng một giải pháp chứng thực an toàn (Authentication):

1. **SMB/CIFS:** Trong môi trường Windows/SAMBA chúng ta cần kích hoạt tính năng LANmanager Authentication.

2. **Kerberos**: Một giải pháp chứng thực dữ liệu an toàn được sử dụng trên Unix cũng như Windows: Kerberos Users' Frequently Asked Questions 1.14.
3. **Stanford SRP (Secure Remote Password)**: Khắc phục được nhược điểm không mã hoá Password khi truyền thông của 2 giao thức FTP và Telnet trên Unix: The SRP Project.
4. **OpenSSH**: Khi chúng ta sử dụng Telnet, FTP... 2 giao thức chuẩn này không cung cấp khả năng mã hoá dữ liệu trên đường truyền. Đặc biệt nguy hiểm là không mã hoá Password, chúng chỉ gửi Password qua đường truyền dưới dạng Clear Text. Điều gì sẽ xảy ra nếu những dữ liệu nhạy cảm này bị Sniffer. OpenSSH là một bộ giao thức được ra đời để khắc phục nhược điểm này: ssh (sử dụng thay thế Telnet), sftp (sử dụng thay thế FTP)...
5. **VPNs (Virtual Private Network)**: Được sử dụng để mã hoá dữ liệu khi truyền thông trên Internet. Tuy nhiên nếu một Hacker có thể tấn công và thỏa hiệp được những Node của của kết nối VPN đó, thì chúng vẫn có thể tiến hành Sniffer được.
6. **Static ARP Table**: Rất nhiều những điều xấu có thể xảy ra nếu có ai đó thành công thuộm độc bảng ARP của một máy tính trên mạng của chúng ta. nhưng làm thế nào để chúng ta ngăn chặn một ai đó cố gắng để đầu độc bảng ARP. Một cách để ngăn chặn những tác động xấu của hành vi này là để tạo mục bảng ARP tĩnh cho tất cả các thiết bị trên đoạn mạng địa phương của chúng ta. Khi điều này được thực hiện, hạt nhân sẽ bỏ qua tất cả các câu trả lời ARP cho địa chỉ IP cụ thể được sử dụng trong các mục nhập và sử dụng địa chỉ MAC chỉ định thay thế.



```
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Van Cong>arp -d
C:\Users\Van Cong>arp -a

Interface: 192.168.1.10 --- 0xc
Internet Address      Physical Address      Type
192.168.1.1           90-f6-52-f2-19-01    dynamic
224.0.0.251           01-00-5e-00-00-fb    static

C:\Users\Van Cong>arp -s 192.168.1.1 90-f6-52-f2-19-01
C:\Users\Van Cong>arp -a

Interface: 192.168.1.10 --- 0xc
Internet Address      Physical Address      Type
192.168.1.1           90-f6-52-f2-19-01    dynamic
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

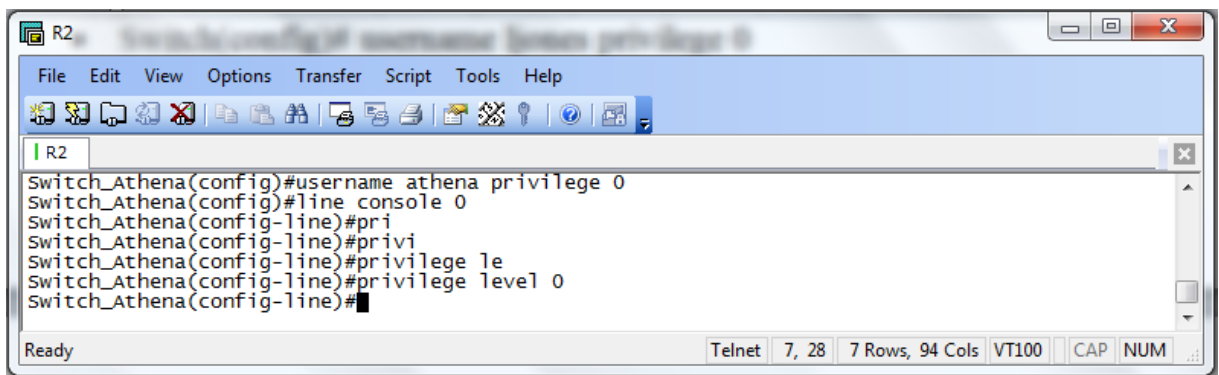
Interface: 192.168.79.1 --- 0x11
Internet Address      Physical Address      Type
192.168.1.1           90-f6-52-f2-19-01    static

C:\Users\Van Cong>
```

Sử dụng câu lệnh arp -a để xem bảng ARP. Câu lệnh arp -s <IP><MAC> để gán tĩnh địa chỉ MAC với địa chỉ IP tương ứng. Câu lệnh arp -d để xóa bảng ARP và các địa chỉ MAC tự nhận động các địa chỉ IP.

7. **Quản lý port console trên Switch:** Một hệ điều hành của Switch Cisco có quản lý port, dây Console(line con 0) mà nó cung cấp sự truy xuất trực tiếp đến Switch cho sự quản trị. Nếu sự quản lý port được cài đặt quá lỏng lẻo thì Switch có thể bị ảnh hưởng bởi các cuộc tấn công. Giải pháp là cài đặt một tài khoản duy nhất cho mỗi nhà quản trị khi truy xuất bằng dây Console. Lệnh sau chỉ ra 1 ví dụ về việc tạo 1 tài khoản ở cấp privileged và cài đặt cấp privilege thành mặc định(0) cho dây Console . Ở cấp privileged 0 là cấp thấp nhất của Switch Cisco và cho phép cài đặt rất ít lệnh. Người quản trị có thể làm tăng cấp privileged lên 15 bằng câu lệnh enable. Cũng vậy, tài khoản này cũng có thể được truy xuất từ dây virtual terminal.

- Switch(config)# username athena privilege 0
- Switch(config)# line con 0
- Switch(config-line)# privilege level 0



```
R2
Switch_Athena(config)#username athena privilege 0
Switch_Athena(config)#line console 0
Switch_Athena(config-line)#pri
Switch_Athena(config-line)#privi
Switch_Athena(config-line)#privilege le
Switch_Athena(config-line)#privilege level 0
Switch_Athena(config-line)#
```

Sử dụng những dòng hướng dẫn sau để tạo password an toàn: password ít nhất là 8 ký tự; không là những từ cơ bản; và thêm vào ít nhất 1 ký tự đặc biệt hay số như: !@#\$%^&*()|+_...; thay đổi password ít nhất là 3 tháng 1 lần. Sử dụng:

- Switch(config)# username ljones secret g00d-P5WD
- Switch(config)# line con 0
- Switch(config-line)# login local

8. **Port Security:** Port Security giới hạn số lượng của địa chỉ MAC hợp lệ được cho phép trên Port. Tất cả những port trên Switch hoặc những interface nên được đảm bảo trước khi triển khai. Theo cách này, những đặt tính được cài đặt hoặc gỡ bỏ như là những yêu cầu để thêm vào hoặc làm dài thêm những đặt tính 1 cách ngẫu nhiên hoặc là những kết quả bảo mật vốn đã có sẵn. Nên nhớ rằng Port Security không sử dụng cho những Port access động hoặc port đích cho người phân tích Switch Port. Và cho đến khi đó Port security để bật tính năng Port trên Switch nhiều nhất có thể. Ví dụ sau cho thấy dòng lệnh shutdown một interface hoặc một mảng các interface:

Single interface:

- Switch(config)# interface <interface>
- Switch(config-if)# shutdown

Range of interfaces:

- Switch(config)# interface range fastethernet 0/2 – 8
- Switch(config-if-range)# shutdown

Port Security có khả năng làm thay đổi sự phụ thuộc trên chế độ Switch và phiên bản IOS. Mỗi Port hoạt động có thể bị hạn chế bởi số lượng tối đa địa chỉ MAC với hành động lựa chọn cho bất kì sự vi phạm nào. Những vi phạm này có thể làm drop gói tin (violation protect) hoặc drop và gửi thông điệp (restrict or action trap) hoặc shutdown port hoàn toàn (violation shutdown or action shutdown). Shutdown là trạng thái mặc định , đảm bảo hầu hết protect và restrict cả hai đều yêu cầu theo dõi địa chỉ MAC mà nó đã được quan sát và phá huỷ tài nguyên xử lí hơn là shutdown. Địa chỉ MAC được thu thập một cách tự động với vài Switch hỗ trợ Entry tĩnh và Sticky Entry.

Entry tĩnh thì được cấu hình bằng tay để thêm vào trên mỗi port (e.g., switchport port-security mac- address mac- address) và được lưu lại trong file cấu hình.. Sticky Entry được xem như là Entry tĩnh, ngoại nó được học một cách tự động . Những Entry động tồn tại được chuyển sang Sticky Entry sau khi sử dụng câu lệnh (switchport port-security mac- address Sticky). Những Entry động cũ được lưu lại trong file cấu hình (switchport port-security mac- address Sticky mac- address) nếu file cấu hình được lưu và chạy thì địa chỉ MAC không cần học lại lần nữa cho việc restart lần sau. Và cũng vậy một số lượng tối đa địa chỉ MAC có thể được cài đặt bằng câu lệnh sau(e.g.,switchport port-security maximum value) .

Người quản trị có thể bật tính năng cấu hình địa chỉ MAC tĩnh trên các port bằng cách sử dụng câu lệnh switchport port-security aging static. Lệnh aging time (e.g., switchport port-security aging time time) có thể đặt dưới dạng phút. Đồng thời dòng lệnh aging có thể đặt cho sự không hoạt động (e.g., switchport port-security aging type inactivity), điều này có nghĩa là độ tuổi các địa chỉ đó được cấu hình trên port ở ngoài nếu không có dữ liệu lưu thông từ những địa chỉ này cho khai báo từng phần bằng dòng lệnh aging time. Đặt tính này cho phép tiếp tục truy cập đến số lượng những địa chỉ giới hạn đó.

Ví dụ:

+ Những dòng lệnh sau dùng để giới hạn tĩnh một cổng trên CatalystSwitch 3550.

- Switch(config-if)# switchport port-security
- Switch(config-if)# switchport port-security violation shutdown
- Switch(config-if)# switchport port-security maximum 1
- Switch(config-if)# switchport port-security mac-address 0011.2233.4455
- Switch(config-if)# switchport port-security aging time 10
- Switch(config-if)# switchport port-security aging type inactivity

+ Những dòng lệnh sau để giới hạn động một cổng trên Catalyst Switch 3550. Chú ý những dòng lệnh aging không được sử dụng với những địa chỉ sticky MAC.

- Switch(config-if)# switchport port-security
- Switch(config-if)# switchport port-security violation shutdown
- Switch(config-if)# switchport port-security maximum 1
- Switch(config-if)# switchport port-security mac-address sticky

Chú ý khi có sự vi phạm port security xảy ra thì ngay lập tức nó sẽ trở thành trạng thái error-disable và đèn LED sẽ tắt. Switch cũng sẽ gửi một thông điệp SNMP trap, logs (sys-log) và làm tăng lên sự phản đối của xâm nhập. Khi một port ở trạng thái error-disable, người quản trị có thể đưa nó ra khỏi trạng thái này bằng cách sử dụng dòng lệnh ở chế độ toàn cục errdisable recovery cause psecure-violation hoặc dòng lệnh shutdown và no shutdown trên cổng được cấu hình.

Có một số vấn đề quan trọng phát sinh khi cấu hình port security trên port kết nối đến một IP phone. Mặc dù port security không được sử dụng trên Trunk port, địa chỉ MAC phản đối việc xem xét việc gán VLAN của gói tin đến. Cùng IP phone gửi gói tin ra 2 Vlan sẽ có 2 bảng entries được chia ra trong bảng MAC vì thế nó sẽ đếm 2 lần lên đến maximum MAC.

Khi IP Phone có thể sử dụng 2 gói tin không được gán vào (untagged, e.g., Layer 2 CDP protocol) và gói tin Voice Vlan có gán(tagged); địa chỉ MAC của IP Phone sẽ được thấy trên cả 2 native VLAN và Voice VLAN. Vì vậy nó sẽ được đếm 2 lần. Việc đặt tối đa địa chỉ MAC cho 1 port kết nối đến 1 IP Phone cho trường hợp nhiều máy tính tấn công vào IP Phone. Những máy tính truyền hợp lệ sử dụng nhiều địa chỉ MAC phải được cấu hình để tính toán.

Một khả năng mới để bảo đảm cho những port của Switch nhanh hơn và thích hợp hơn đó là macros. Macros cho phép nhóm những port sẵn sàng để mà những lệnh đó được chấp nhận bằng cấu hình tay. Bất kỳ dòng lệnh nào được thêm vào bằng việc sử dụng ký tự “#” tại đầu mỗi dòng lệnh và kết thúc bởi ký tự “@”.

Ví dụ sau đây tạo ra sự ngăn cản security macro gọi là unused để bảo đảm trên những port hoặc trên những interface trên Switch 3550.

- Switch(config)# macro name unused

Sau khi tạo sự gắn cấm security macro, unused, áp đặt macro trên tất cả các port của Switch như sự bảo đảm ranh giới với các dòng lệnh sau.

- Switch(config)# interface range fasteth0/1 – 24 , giga0/1 – 2
- Switch(config-if-range)# macro apply unused

Sau khi macros được xây dựng tính bảo đảm dựa trên unused macro được thiết lập để bật tính năng bảo mật đủ để hỗ trợ tất cả các hệ thống theo mong đợi..

- Switch(config)# macro name host

Việc chấp nhận những macros sẽ chỉ làm thay đổi đến tính bảo đảm ở những biên được yêu cầu cho những port hỗ trợ hoàn toàn những hệ thống thích hợp.

Người quản trị có thể sử dụng câu lệnh macro trace để thay thế cho câu lệnh macro apply bởi vì câu lệnh macro trace có thể xác định debugging của macros. Thường xuyên sử dụng show parser macro description để biết macro cuối cùng được áp lên mỗi port. Cuối cùng địa chỉ MAC tĩnh và port security áp trên mỗi port của Switch có thể trở thành gánh nặng cho người quản trị. Port Access Control List (PACLs) có thể cung cấp khả năng bảo mật tương tự như địa chỉ MAC tĩnh và port security và PACLs cũng cung cấp nhiều tính năng linh động và điều khiển. Việc cho phép địa chỉ MAC và địa chỉ IP có thể được chia và được xem xét từ phía của một Switch mở rộng.

Một số công cụ giúp sniffer và phát hiện các gói Sniffer:

- Cain & Able : Một công cụ sniffer toàn diện với nhiều cách thức scan bắt gói tin, giải mã dữ liệu...
- AntiSniff: công cụ phát hiện các gói Sniffer toàn diện hiệu quả..
- CPM (Check Promiscuous Mode): Công cụ được phát triển bởi Carnegie-Mellon nhằm giúp kiểm tra Sniffer trên các hệ thống UNIX.