Mã lớp	Tên khóa học	Ngày khai giảng	Ngày học	Giờ học	Học phí/khóa	Thời gian
CHƯƠNG TRÌNH CCNA						
AK25	CCNAX (200-120)	05/03	3 – 5 - 7	8:30 – 11:30AM	3.360.000	152 giờ
AK27				2:00 – 5:00PM	3.360.000	
A25				6:30 – 9:30PM	6.720.000	
AK24		11/03	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
AK26				2:00 – 5:00PM	3.360.000	
A24				6:30 – 9:30PM	6.720.000	
AK29		19/03	3 – 5 - 7	8:30 – 11:30AM	3.360.000	
A27				6:30 – 9:30PM	6.720.000	
AK28		27/03	2 – 4 – 6	2:00 – 5:00PM	3.360.000	
A26				6:30 – 9:30PM	6.720.000	
AS3	CCNA Security (640-554)	19/03	3 – 5 – 7	6:30 – 9:30PM	6.720.000	100 giờ
AV1	CCNA Voice (640-461)	04/03	2 – 4 – 6	6:30 – 9:30PM	6.720.000	100 giờ
CHƯƠNG TRÌNH CCNP						
P1-K5	ROUTE (300 - 101)	11/03	2 – 4 – 6	8:30 – 11:30AM	6.600.000	140 giờ
P1K7				2:00 – 5:00PM	6.600.000	
P1-5				6:30 – 9:30PM	9.800.000	
P1-6		26/03	3 – 5 – 7	6:30 – 9:30PM	9.800.000	
P2K3	SWITCH (300 - 115)	18/03	2 – 4 – 6	8:30 – 11:30AM	5.880.000	120 giờ
P2K5				2:00 – 5:00PM	5.880.000	
P2-5				6:30 – 9:30PM	8.232.000	
P3-4	TSHOOT (300 - 135)	17/03	3 – 5 – 7	6:30 – 9:30PM	9.800.000	140 giờ
CHƯƠNG TRÌNH CCIE						
EW2	CCIE WRITTEN (Version 5)	24/03	3 – 5 – 7	6:30 – 9:30PM	11.760.000	120 giờ

Ngày Xuân Hạnh Phúc Bình An Đến

Năm Mới Vinh Hoa Phú Quý Về

Đăng ký học liên hệ :

Thanh Trâm Email : thanhtram@vnpro.org Mobile : 0949 246 829
Bích Diễm Email : bichdiem@vnpro.org Mobile : 0909 399 223
Lê Uyên Email : tranleuyen@vnpro.org Mobile : 0903 834 636
Ngọc Nữ Email : ngocnu@vnpro.org Mobile : 0933 850 356

Liên hệ dự án đào tạo - tư vấn hệ thống mạng - thuê thiết bị phòng học - mua sách

Website: www.vnpro.vn Email : vnpro@vnpro.org Điện thoại: (08) 35124257

Trung Tâm Tin Học VnPro - 149/1D Ung Văn Khiêm, P.25, Q.BT, TP.HCM - (08) 35124257 - Email: vnpro@vnpro.org

Bản tin Dân Cisco – Được phát hành bởi **Công Ty TNHH Tư Vấn & Dịch Vụ Chuyên Việt**
Chịu trách nhiệm xuất bản: **Phạm Minh Tuấn**
Giấy phép xuất bản số: **69/QĐ – STTTT** Ngày ĐK: **26/10/2011**
Công ty in: **Sao Băng Design**
Số lượng in: **2000 cuốn/kỳ**
Kỳ hạn xuất bản: **1 kỳ/tháng**

Số 35
02/2015

BẢN TIN dancisco

Được phát hành bởi Công Ty TNHH Tư Vấn và Dịch Vụ Chuyên Việt

2015 Xuân Ất Mùi

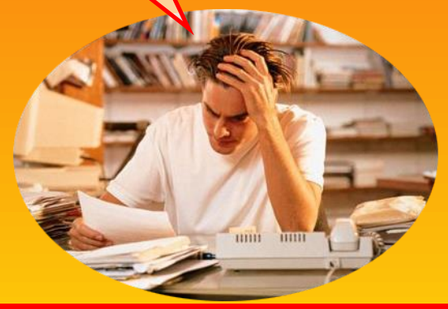
VnPro - 12 năm hình thành và phát triển

12 năm, VnPro đã đi qua một chặn đường dài và đạt được những thành tựu đáng tự hào trong sự nghiệp đào tạo...

[Trang 07]

Kĩ năng làm chủ cảm xúc – hóa giải áp lực

[Trang 15]



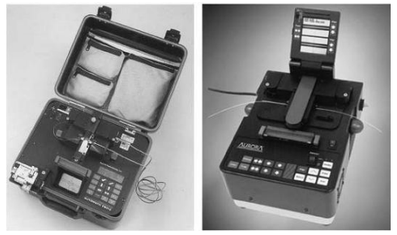
Bảo mật mạng vlan một cách tốt nhất

Bài viết này tập trung vào vấn đề đảm bảo sự an toàn cho VLAN và cách thực hiện nó trong môi trường mạng doanh nghiệp. ...

[Trang 12]

TIN TỨC SỰ KIỆN KHÁC

Các dạng nối dây cáp quang



Điều gì sẽ xảy ra khi sợi cáp quang bị đứt? Cần một người để định vị chỗ đứt và khôi phục lại. Kỹ thuật phục hồi các sợi cáp hay sáp nhập hai sợi cáp lại để tăng chiều dài của nó được gọi là nối dây. Nó được thực hiện theo hai cách:

1. Mechanical Splicing
2. Fusion Splicing

Mỗi chỗ nối cần được tính toán nhất định. Fusion Splicing sẽ mất đi 0.02 dB, Mechanical Splicing sẽ mất đi 0.75 dB. Nếu không được thực hiện theo cách tốt nhất, nó có thể tăng hậu quả thiệt hại trong tốc độ truyền dữ liệu. Cách tốt nhất để kiểm tra tổng số chỗ nối cuối cùng để kết thúc mạch là để xem các báo cáo OTDR (Optical Time Domain Reflector) giúp để tìm ra vấn đề trong sợi cáp.

Người biên dịch: Phan Thanh Phong.

Các bộ cảm biến "sensor" thay đổi cuộc sống ở các nước đang phát triển

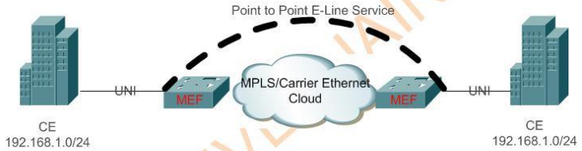
Công nghệ IoE technology có thể được sử dụng ở tất cả mọi lĩnh vực từ nông nghiệp cho đến chất lượng nước ở những quốc gia đang phát triển. Các bộ cảm biến có thể được lắp đặt ở những giếng bơm nước tại vị trí cần bơm nước và định kỳ báo cho các kỹ thuật viên dưới dạng biểu đồ "dashboard" hoặc dưới hình thức email hoặc tin nhắn "message" biết được vị trí, chất lượng nước các giếng tới hệ thống mạng "cell phone" để các kỹ thuật viên từ đó kịp thời sửa chữa khi cần thiết.

Công nghệ IoE cũng có thể được áp dụng cho hệ thống nông nghiệp. Các bộ cảm biến có thể được thiết lập rải rác trên các cánh đồng trồng trọt cứ mỗi 6 đến 8 inch. Thông qua các bộ cảm biến, các kỹ sư nông nghiệp có thể thu thập được thông tin về lượng nước và phân bón được sử dụng, trạng thái tơi xốp và mức độ màu mỡ của đất, nhiệt độ môi trường xung quanh, độ ẩm và cường độ chiếu sáng. Thông tin có thể được gửi lên môi trường điện toán đám mây của máy tính hoặc smartphone để xử lý, hệ thống sẽ tính toán để đưa ra những tham số về lượng nước và phân bón tốt nhất cho từng khu vực và đối với từng loại đất cho từng loại cây trồng. Các thông tin thu thập được có thể biển diễn dưới dạng sơ đồ, đồ thị theo ngày, tuần hoặc tháng.

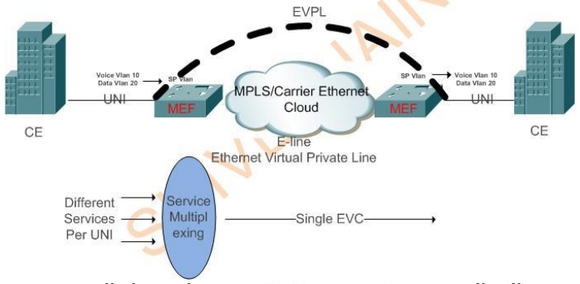
Người biên soạn: Bùi Quốc Kỳ.

Dịch vụ E-Line Carrier Ethernet

E-Line Carrier Ethernet Service được chia thành hai phần:



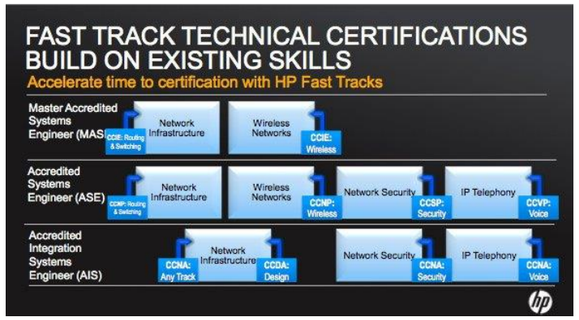
Ethernet Private Line aka EPL: Ethernet Private Line là sự thay thế dành riêng cho TDM private line cho kết nối point to point, giúp tiết kiệm cap-ex cũng như op-ex. Đây là port chuyên dụng và kết nối Ethernet ảo cho mỗi UNI.



Ethernet Virtual Private Line aka EVPL: Ethernet Virtual Private Line là sự thay thế của frame relay và mạch atm. Nhiều dịch vụ có thể được gộp trong mỗi UNI.

Người biên dịch: Phan Thanh Phong.

Chuyển đổi chứng chỉ Cisco (Certs) sang chứng chỉ HP



HP vừa đưa ra một số thay đổi trong hệ thống chứng chỉ của hãng. Với một số chứng chỉ của Cisco (Cisco certification), chúng ta đã hoàn tất tới 77% yêu cầu để có được chứng chỉ của HP (HP cert).

Tổng quan hệ thống chứng chỉ ExpertOne của HP

Một trong những điểm mới của hệ thống chứng chỉ HP cũng tương tự như mỗi tương quan giữa chứng chỉ CCDE và Cisco Certified Architect. Chứng chỉ Cisco CCDE là chứng chỉ liên quan đến thiết kế tương tự với thách thức để vượt qua được kỳ sát hạch CCIE lab. Cisco Certified Architect đòi hỏi ứng cử viên phải đạt được một số các chứng chỉ nhất định, có kiến thức rộng và chuyên sâu về công nghệ network liên quan đến hạ tầng mạng Cisco; chứng chỉ này tương đương với trình độ Tiến Sĩ.

Hệ thống chứng chỉ ExpertOne của HP còn được gọi là Master Accredited Systems Engineer (Master ASE) có tính chất tương tự như chứng chỉ CCDE – có kiến thức rộng và chuyên sâu về vấn đề thiết kế hạ tầng mạng – với các bài kiểm tra tương tự như mức độ chứng chỉ Cisco Architect. Theo HP cho biết, chứng chỉ này tập trung trang bị cho ứng cử viên khả năng lên kế hoạch xây dựng hạ tầng mạng, khả năng dự toán tài chính và lựa chọn các công nghệ sẽ sử dụng, các công nghệ có thể rất đa dạng và có thể tương tác được giữa nhiều hãng thiết bị lẫn nhau thay vì tập trung vào công nghệ của Cisco như trong chứng chỉ Cisco cert.

Tổng quan về việc chuyển đổi chứng chỉ Cisco (Certs) sang chứng chỉ HP

Những kiến thức tìm hiểu trong chứng chỉ CCNA như ARP, DHCP, RIP, STP cũng được nhắc lại trong kỳ thi chứng chỉ HP cert. Để tránh hỏi lại những điều tương tự, HP đã đưa ra kỳ thi sát hạch "delta" exam tập trung vào sự khác biệt giữa phần kiến thức giữa chứng chỉ của HP và Cisco.

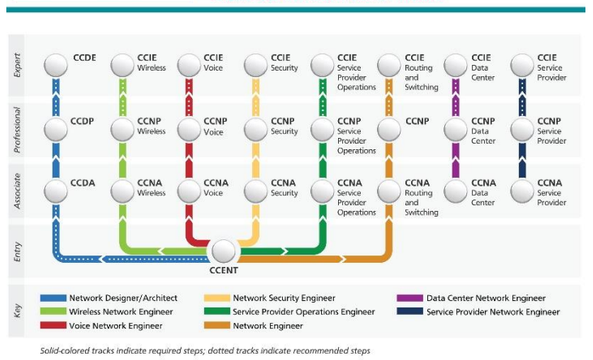
HP đưa ra một số chứng chỉ như AIS - Network Infrastructure và ASE Network Infrastructure.

HP AIS - Network Infrastructure

Nếu ứng cử viên đã có chứng chỉ CCDA hoặc CCNA Security thì có thể thi nâng cấp lên chứng chỉ AIS Infrastructure. AIS infrastructure bao gồm những kiến thức được đề cập trong chương trình CCNA và một số kiến thức khác. Tuy nhiên, để nâng cấp lên chứng chỉ AIS Infrastructure, ta phải có chứng chỉ CCDA hoặc CCNA Security và vượt qua kỳ thi delta exam mã môn thi HP2-Z18 với chi phí thi vào khoảng $75. Kỳ thi delta exam tương tự như kỳ thi CCNA (ICND1, ICND2) với thời gian làm bài 90 phút, số lượng câu hỏi 55 câu và điểm đậu "passing score" là 73%.

HP ASE - Network Infrastructure

Chứng chỉ ***ASE - Network Infrastructure*** thì tương đương với chứng chỉ CCNP (R/S), và ứng cử viên có thể sử dụng chứng chỉ CCNP để thi nâng cấp thành chứng chỉ ASE – Networrk Infrastructure.



Hệ thống chứng chỉ của Cisco

Static NAT trên Cisco ASA

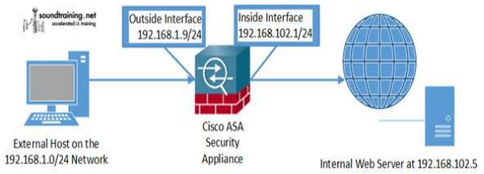
Có hai phương thức network address translation (NAT) phổ biến là dynamic port address translation (PAT) và static NAT.

PAT là phương thức many-to-one thường được sử dụng trên hạ tầng mạng nhỏ cho phép nhiều host nội bộ sử dụng địa chỉ RFC 1918 chẳng hạn như 192.168.0.0/24 chia sẻ cùng một địa chỉ IP public mặt ngoài để kết nối đi Internet.

Static NAT là phương thức one-to-one được sử dụng để "public" một host nội bộ, cho phép hệ thống mạng ngoài Internet có thể truy cập dịch vụ bên trong host nội bộ.

Bài viết này sẽ giới thiệu cách thức cấu hình Static NAT để "public" internal Web server ra ngoài Internet. Quá trình "public" một mail server, FTP server, hay các loại server khác cũng tương tự.

Trong bài viết này, ta sử dụng **ASA software Version 9.0** (1) và áp dụng cho **Version 8.3** hoặc các phiên bản sau này.



Thực hiện 4 bước sau để triển khai static NAT:

1. Thiết lập network object và định nghĩa static NAT.

Một network object sẽ được thiết lập để nhận diện các internal host (host nội bộ). Bên trong network object, chúng ta sẽ thiết lập static NAT để nhận diện outside interface, địa chỉ IP và loại lưu lượng sẽ được forward đi:

```
object network InternalHost
  host 192.168.102.5
  nat (inside,outside) static interface service tcp 80 80
```

2. Định nghĩa NAT statement nhận diện cổng giao tiếp outside interface

Trong định nghĩa static NAT như trên, ta sử dụng từ khóa "*interface*" để NAT sử dụng bất kỳ địa chỉ nào trên cổng giao tiếp outside interface. Định danh port *80* đầu tiên là "originating port number". Định danh port *80* thứ 2 là "destination port number".

3. Định nghĩa Access-Control List Danh sách Access-Control List định nghĩa luồng lưu lượng nào sẽ được phép đi qua:

```
access-list OutsideToWebServer permit tcp any host
192.168.102.5 eq www
```

4. Áp ACL lên cổng giao tiếp outside interface thông qua câu lệnh Access-Group command:

```
access-group OutsideToWebServer in interface outside
```

Toàn bộ thông tin cấu hình được thực hiện như sau:

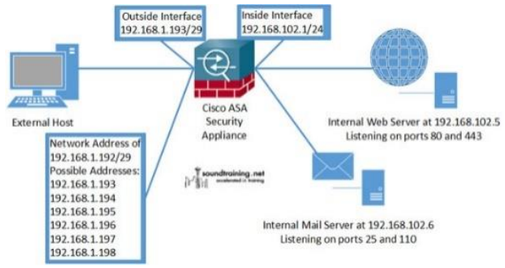
```
asa02#
asa02# configure terminal
asa02(config)# object network Outside_to_Inside_Web_Server
asa02(config-network-object)# host 192.168.102.5
asa02(config-network-object)# nat (inside,outside) static interface service tcp 80 80
asa02(config-network-object)# access-list OutsideToWebServer permit tcp any host 192.168.102.5 eq www
asa02(config)# access-group OutsideToWebServer in interface outside
asa02(config)#
```

Khi triển khai thành công, các host ngoài mạng (outside network) có thể truy cập dịch vụ tới internal Web server thông qua địa chỉ IP mặt ngoài của ASA (outside interface).

Cấu hình ASA với nhiều địa chỉ Outside Interface

Chúng ta không thể gán nhiều địa chỉ IP lên cổng giao tiếp outside interface của Cisco ASA nhưng chúng ta vẫn có thể cấu hình để ASA tiến hành forward nhiều địa chỉ outside tới nhiều host bên trong inside network.

Chẳng hạn như ISP cấp cho chúng ta dải IP thuộc lớp mạng /29. Giả sử chúng ta có thêm mail server sử dụng POP3 và SMTP và Web server sử dụng HTTP và HTTPS bên trong inside network. Chúng ta sẽ tiến hành thiết lập sao cho mỗi server sẽ được liên kết tới một địa chỉ IP outside khác biệt nhau thông qua phương thức static NAT.



Các bước triển khai cũng tương tự như quá trình cấu hình single-address static NAT:

1. Cấu hình network object. Cấu hình một network object tương ứng cho mỗi internal host trong định nghĩa static NAT static và chỉ định địa chỉ outside kèm với service type (port number) sẽ được forward.

```
object network WebServer-HTTP
  host 192.168.102.5
  nat (inside,outside) static 192.168.1.194 service tcp 80 80
!
object network WebServer-HTTPS
  host 192.168.102.5
  nat (inside,outside) static 192.168.1.194 service tcp 443
443
!
object network MailServer-SMTP
  host 192.168.102.6
  nat (inside,outside) static 192.168.1.195 service tcp 25 25
!
object network MailServer-POP3
  host 192.168.102.6
  nat (inside,outside) static 192.168.1.195 service tcp 110
110
```

2. Cấu hình Access-Control List cho phép lưu lượng đi vào.

```
access-list OutsideToInside permit tcp any host
192.168.102.5 eq 80
access-list OutsideToInside permit tcp any host
192.168.102.5 eq 443
access-list OutsideToInside permit tcp any host
192.168.102.6 eq 25
access-list OutsideToInside permit tcp any host
192.168.102.6 eq 110
```

3. Áp dụng Access-Control List lên cổng giao tiếp outside interface.

```
access-group OutsideToInside in interface outside
```

Toàn bộ thông tin cấu hình được triển khai như sau:

```
asa02#
asa02# configure terminal
asa02(config)# object network WebServer-HTTP
asa02(config-network-object)# host 192.168.102.5
asa02(config-network-object)# nat (inside,outside) static 192.168.1.194 service tcp 80 80
asa02(config-network-object)# !
asa02(config-network-object)# object network WebServer-HTTPS
asa02(config-network-object)# host 192.168.102.5
asa02(config-network-object)# nat (inside,outside) static 192.168.1.194 service tcp 443 443
asa02(config-network-object)# !
asa02(config-network-object)# object network MailServer-SMTP
asa02(config-network-object)# host 192.168.102.6
asa02(config-network-object)# nat (inside,outside) static 192.168.1.195 service tcp 25 25
asa02(config-network-object)# !
asa02(config-network-object)# object network MailServer-POP3
asa02(config-network-object)# host 192.168.102.6
asa02(config-network-object)# nat (inside,outside) static 192.168.1.195 service tcp 110 110
asa02(config-network-object)# !
asa02(config-network-object)# access-list OutsideToInside permit tcp any host 192.168.102.5 eq 80
asa02(config)# access-list OutsideToInside permit tcp any host 192.168.102.5 eq 443
asa02(config)# access-list OutsideToInside permit tcp any host 192.168.102.6 eq 25
asa02(config)# access-list OutsideToInside permit tcp any host 192.168.102.6 eq 110
asa02(config)# !
asa02(config)# access-group OutsideToInside in interface outside
asa02(config)#
```

Người biên soạn: Bùi Quốc Kỳ.

Kiểm tra MTU với công cụ Ping

Công cụ "ping" thường được sử dụng bởi các nhà quản trị mạng, cho phép kiểm tra kết nối thông suốt giữa các thiết bị mạng. Trước khi kiểm tra được giá trị MTU, chúng ta cần xác định kích thước của một packet:

Datagram/Packet size (IP Total Length field) = IP Header + Payload
Kích thước của packet tương ứng với datagram/packet size sẽ bằng IP Header + Payload.

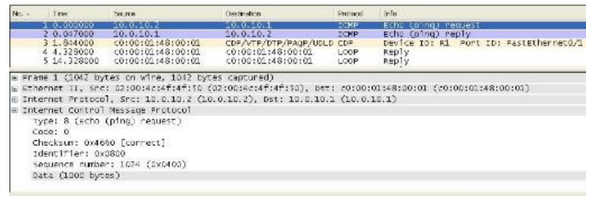
Trên router của Cisco, nếu kích thước packet size là 1000 byte như minh họa bên dưới, thì ICMP Echo ping message sẽ bao gồm **20 byte IP Header + 980 byte ICMP Payload** (ICMP type field: 1B, code: 1B, checksum: 2B, identifier: 2B, sequence number: 2B, data: 972B).

```
R1#ping 10.0.23.3 repeat 1 size 1000
Type escape sequence to abort.
Sending 1, 1000-byte ICMP Echos to 10.0.23.3, timeout is
2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max
= 80/80/80 ms
```

Đối với hệ điều hành Windows OS thì nếu chúng ta khai báo data size là 1000B thì đó lại là kích thước của ICMP data trong payload + các trường "field" trong ICMP + IP Header. Trong trường hợp đó thì IP packet size sẽ bao gồm **20 byte IP Header + 1008 byte ICMP Payload** (ICMP type field: 1B, code: 1B, checksum: 2B, identifier: 2B, sequence number: 2B, **data: 1000B**). Trong trường hợp đó là Ethernet network frame thì kích thước sẽ là 1042B (cộng thêm 14B Ethernet II Header).

```
C:\>ping 10.0.10.1 -l 1000 -n 1
```

Chúng ta có thể sử dụng chương trình bắt gói để quan sát kích thước gói tin ICMP echo request khi sử dụng công cụ Windows ping tool.



Tổng kết lại: Cisco ping size = toàn bộ chiều dài IP packet.
Windows ping size = chỉ có ICMP data và chưa bao gồm các trường ICMP 8B field như trường type, code, checksum, identifier và sequence.

Phân mảnh Fragmentation và Maximum Transmission Unit (MTU)

IP protocol MTU định nghĩa kích thước của IP packet (tương ứng với tham số trong trường IP Total Length field) có thể gửi đi trên network device interface. Các packet sau đó tiếp tục được đóng gói thành frame tại lớp data link layer với kích thước đủ nhỏ thì mới có thể được truyền đi tùy thuộc vào công nghệ truyền dẫn physical transmission technology. Trong trường hợp packet lớn hơn kích thước tối đa maximum size so với công nghệ network technology đang sử dụng thì IP packet cần phải phân mảnh thành các phân khúc IP chunk nhỏ hơn. Tiến trình này được gọi là tiến trình phân mảnh IP fragmentation, các phân khúc chunk sẽ được tập hợp trở lại tại phía đầu xa của quá trình truyền dẫn được gọi là tiến trình reassemble, tiến trình reassemble các IP packet được thực hiện tại đầu cuối IP destination.

Các vấn đề bất cập liên quan đến tiến trình phân mảnh Fragmentation.

Fragmentation làm tăng khối lượng tác vụ cần xử lý (overhead) trên cả receiver lẫn sender. Các thiết bị đứng ra thực hiện tác vụ phân mảnh fragmentation cần phải xây dựng header mới cho mỗi phân mảnh fragment. Tại phía thiết bị nhận receiver sẽ phải tiêu tốn tài nguyên bộ nhớ để phục vụ cho việc tái phân mảnh các fragment thành một packet hoàn chỉnh. Điều này có thể không ảnh hưởng nhiều đến các host đầu cuối nhưng sẽ ảnh hưởng rất nhiều nếu thiết bị đầu cuối là một router.

Một số bất cập thường thấy nếu tiến trình fragmentation diễn ra:

- Nếu tiến trình phân mảnh diễn ra thì router sẽ phải xử lý các packet bằng CPU (process switched) thay vì chuyển mạch dựa trên phần cứng (CEF switched), điều này ảnh hưởng nhiều đến hiệu năng hoạt động của hệ thống.
- Trong trường hợp router phải đứng ra để thực hiện tiến trình tái phân mảnh reassemble, tiến trình này sẽ tiêu tối khá nhiều tài nguyên bộ đệm buffer vì router có thể không biết gì về thông tin kích thước của IP packet nguyên thủy.
- Nếu một phân mảnh fragment của một IP packet bị drop bỏ thì toàn bộ IP packet sẽ phải gửi lại và tiến trình phân mảnh lại diễn ra thêm một lần nữa.

Fragmentation trên môi trường GRE và IPsec tunnel

Tiến trình IP fragmentation ảnh hưởng rất nhiều trên cổng giao tiếp ảo GRE tunnel. Chẳng hạn như nếu Router A nhận được 1476B packet rồi sau đó bổ xung thêm phần GRE header rồi gửi đi trên đường tunnel. Giả sử router tham gia vào môi trường MPLS cloud với link MTU 1400B. Router này sẽ tiến hành phân mảnh GRE packet (thông tin GRE IP header, inner origanl IP và TCP header sẽ nằm trong fragment đầu tiên), trong tình huống này thì GRE tunnel destination router sẽ phải đứng ra để tái phân mảnh reassemble các fragmented packet.

Để tránh tiến trình IP fragmentation, cách tốt nhất là chúng ta tùy chỉnh tăng MTU trên các hướng di chuyển của packet, trong trường hợp môi trường mạng nhà cung cấp MPLS provider thì vấn đề phân mảnh ít khi xảy ra vì nhiều nhà cung cấp đều hỗ trợ tùy chỉnh MTU lên tới giá trị 1600B để hỗ trợ IPsec hoặc GRE. Trong trường hợp nhà cung cấp dịch vụ provider không hỗ trợ MTU cao hơn mức cần thiết thì chúng ta có thể giảm IP MTU trên cổng giao tiếp tunnel interface, tùy chỉnh giá trị MSS value hoặc sử dụng PMTUD. Để tùy chỉnh giá trị MTU sao cho hợp lý, chúng ta có thể thực hiện tiến trình "ping" mở rộng để xác định giá trị MTU hợp lý.

Tình huống giả định

Giả sử hạ tầng mạng có 2 CE router, một ở chi nhánh branch A và một ở chi nhánh đầu xa remote branch B, chúng ta sẽ xác định lại giá trị MTU trên mỗi hướng (path) trên hạ tầng mạng nhà cung cấp provider MPLS cloud với giá trị xác định là 1500B.

Để kiểm tra giá trị MTU trên mỗi chặng đường đi (path), cách thức tốt nhất là gửi đi các packet với kích thước tăng dần. Tính năng "extended ping" với tùy chọn sweep option là tùy chọn lý tưởng giúp chúng ta thực hiện điều này. Như trong ví dụ bên dưới, chúng ta sẽ thiết lập quá trình "ping" gửi đi các gói "ICMP echo request" với tổng kích thước dao động từ 1490B cho tới 1510B với kích thước gói tin mỗi lần tăng là 1B. Một trong những tùy chọn quan trọng trong tình huống này là giá trị Don't Fragment bit cần phải được thiết lập .

```
R1#ping
Protocol [ip]:
Target IP address: 10.0.23.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]: y
Sweep min size [36]: 1490
Sweep max size [18024]: 1510
Sweep interval [1]:
Type escape sequence to abort.
Sending 105, [1490..1510]-byte ICMP Echos to 10.0.23.3,
timeout is 2 seconds:
Packet sent with the DF bit set
!!!!.........!!!!!!.
Success rate is 54 percent (50/91), round-trip min/avg/max
= 40/99/224 ms
```

Chúng ta tiến hành gửi đi 10 ICMP echo request với kích thước bắt đầu là 1490B và nhận được 10 response tương ứng, nhưng 10 packet tiếp theo gửi đi thì không thấy hồi đáp, điều đó có nghĩa là các packet không để đến được đích với giá trị MTU lớn hơn ngưỡng 1500B. Router được kiểm tra đã cấu hình MTU là 1500B trên các cổng giao tiếp nên tiến trình debug cho phép chúng ta quan sát thấy các packet lớn hơn 1500B sẽ không bao giờ được "route" bởi bảng FIB lẫn bảng RIB.

```
*Mar 1 00:16:42.179: IP: tableid=0, s=10.0.12.1 (local),
d=10.0.23.3 (FastEthernet0/0), routed via FIB
*Mar 1 00:16:42.183: IP: s=10.0.12.1 (local), d=10.0.23.3
(FastEthernet0/0), len 1499, sending
*Mar 1 00:16:42.183: ICMP type=8, code=0
*Mar 1 00:16:42.219: IP: tableid=0, s=10.0.23.3
(FastEthernet0/0), d=10.0.12.1 (FastEthernet0/0), routed
via RIB
*Mar 1 00:16:42.223: IP: s=10.0.23.3 (FastEthernet0/0),
d=10.0.12.1 (FastEthernet0/0), len 1499, rcvd 3
*Mar 1 00:16:42.227: ICMP type=0, code=0
*Mar 1 00:16:42.231: IP: tableid=0, s=10.0.12.1 (local),
d=10.0.23.3 (FastEthernet0/0), routed via FIB
*Mar 1 00:16:42.231: IP: s=10.0.12.1 (local), d=10.0.23.3
(FastEthernet0/0), len 1500, sending
*Mar 1 00:16:42.231: ICMP type=8, code=0
*Mar 1 00:16:42.283: IP: tableid=0, s=10.0.23.3
(FastEthernet0/0), d=10.0.12.1 (FastEthernet0/0), routed
via RIB
*Mar 1 00:16:42.287: IP: s=10.0.23.3 (FastEthernet0/0),
d=10.0.12.1 (FastEthernet0/0), len 1500, rcvd 3
*Mar 1 00:16:42.291: ICMP type=0, code=0
*Mar 1 00:16:42.299: IP: tableid=0, s=10.0.12.1 (local),
d=10.0.23.3 (FastEthernet0/0), routed via FIB
*Mar 1 00:16:42.299: IP: s=10.0.12.1 (local), d=10.0.23.3
(FastEthernet0/0), len 1501, sending
*Mar 1 00:16:42.303: ICMP type=8, code=0
*Mar 1 00:16:44.295: IP: tableid=0, s=10.0.12.1 (local),
d=10.0.23.3 (FastEthernet0/0), routed via FIB
*Mar 1 00:16.:44.299: IP: s=10.0.12.1 (local), d=10.0.23.3
(FastEthernet0/0), len 1502, sending
```

Router gửi đi 20 packet (với kích thước bắt đầu từ 1490B cho tới 1510B). Trong đó, chúng ta đã gửi đi 10 packet với 1490 + 10 với kích thước lớn nhất là 1500B và vì router cấu hình 1500B MTU nên các packet với kích thước lớn hơn sẽ bị "drop" bỏ bởi vì các packet được nhúng vào DF bit set.

Ví dụ – GRE over IPsec

Fragmentation sẽ ảnh hưởng nhiều đến hoạt động của router nếu chúng ta sử dụng GRE over IPsec khi thiết bị đầu cuối cấu hình IPsec tunnel cho phép nhúng vào GRE Header rồi thực hiện tiến trình mã hóa. GRE header sẽ bổ xung thêm 24B vào packet, IPsec với ESP 56B sẽ làm tăng thêm kích thước packet 80B overhead. Giải pháp cho tình huống này có thể là sử dụng cơ chế phát hiện MTU là PMTUD, tuy nhiên nếu như các router "drop" bỏ các ICMP message do chính sách bảo mật thì cơ chế PMTUD sẽ không thể hoạt động được để xác định được kích thước MTU size phù hợp trên cổng giao tiếp tunnel GRE interface. GRE source router sẽ đứng ra thực hiện tiến trình IP fragmentation trước khi bổ sung thêm GRE và IPsec header. Để tính toán giá trị MTU tương ứng cho đường tunnel thì tùy chọn tốt nhất là tận dụng công nghệ "sweep ping" như đề cập ở trên.

Nếu chúng ta thiết lập GRE/IPsec giữa R1 và R3 thì R3 router sẽ tiêu tốn khá nhiều tài nguyên CPU để xử lý và tốc độ truyền tải cũng chịu ảnh hưởng theo nếu tiến trình fragment diễn ra. Vì thế, chúng ta cần phải xác định được giá trị MTU nhỏ nhất có thể gửi đi trên đường tunnel để tránh tiến trình IP fragmentation có thể xảy ra.

Chúng ta không thể ping với DF bit được thiết lập để giả lập lưu lượng GRE/IPsec bởi vì router sẽ không sao chép DF bit sang IPsec header (GRE tunnel sẽ gỡ bỏ mọi giá trị DF bit trừ phi chúng ta sử dụng tunnel path-mtu discovery under tunnel GRE), thay vào đó, chúng ta có thể ping với gói tin IP thuần túy để xác định giá trị MTU trước khi triển khai IPsec tunnel.

Xác định giá trị MTU nhỏ nhất trên chặng đường đi đến đích:

```
R1#ping
Protocol [ip]:
Target IP address: 10.0.23.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]: y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]: y
Sweep min size [36]: 1300
Sweep max size [18024]: 1500
Sweep interval [1]:
Type escape sequence to abort.
Sending 1005, [1300..1500]-byte ICMP Echos to 10.0.23.3,
timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!M.M.M.M.M.M.M.M.M.M.M.M.M.M
.M.M.M.M.M
.M.M.M.
Success rate is 68 percent (101/147), round-trip
min/avg/max = 4/19/60 ms
```

Sau 101 lần gửi đi gói tin request thành công với kích thước gói tin ICMP là 1300B tới 1400B từ đó ta xác định giá trị MTU nhỏ nhất là 1400B. M cho thấy gói tin không thể bị phân mảnh fragment. Sau đó, ta có thể lấy giá trị 1400B tương ứng với tham số IP MTU nhỏ nhất trừ đi cho 80B (24B GRE và 56B ESP tunnel IPsec).

Người biên soạn: Bùi Quốc Kỳ

VNPRO - 12 NĂM HÌNH THÀNH VÀ PHÁT TRIỂN

12 năm, VnPro đã đi qua một chặn đường dài và đạt được những thành tựu đáng tự hào trong sự nghiệp đào tạo: Đi đầu trong lĩnh vực đào tạo công nghệ mạng Cisco tại Việt Nam; Chất lượng đào tạo tại VnPro được đánh giá cao; Cơ sở vật chất trang bị đáp ứng đầy đủ cho từng Học viên; Đội ngũ nhân sự, Giảng viên cao cấp trong ngành; Cung cấp nguồn lực chất lượng cao cho thị trường; Các chương trình ưu đãi hỗ trợ sinh viên; Các chương trình hoạt động từ thiện xã hội.

VnPro đi đầu trong lĩnh vực đào tạo công nghệ mạng Cisco

Ảnh tổng hợp hoạt động đào tạo

VnPro chất lượng đào tạo luôn được đặt lên hàng đầu

Đào tạo các kỹ sư mạng đạt tiêu chuẩn quốc tế đó là tiêu chí được đặt lên hàng đầu trong công tác đào tạo nhân lực cho thị trường tuyển dụng của VnPro, xét theo thời điểm hiện nay thì Việt Nam có khoảng gần 50 CCIE trong số đó được đào tạo tại VnPro chiếm 10 CCIE, ngoài ra còn có hàng ngàn CCNP đang làm cho các doanh nghiệp trong và ngoài nước. Với tiêu chí đặt chất lượng lên hàng đầu, VnPro cam kết tất cả các học viên theo học nếu thi trượt các chứng chỉ Quốc Tế đều được đào tạo lại hoàn toàn miễn phí, ngoài ra VnPro còn có chính sách tư vấn hỗ trợ học viên trong suốt quá trình học và làm việc, hỗ trợ giải quyết những khó khăn những thách thức trong công việc. Hàng tháng VnPro thường xuyên tổ chức các lớp ôn tập miễn phí, các lớp upgrade công nghệ, hội thảo chuyên ngành..

Với 12 năm đào tạo, VnPro luôn mong muốn tất cả các học viên có một kiến thức thật vững chắc và tự tin bước vào lĩnh vực công nghệ mạng và luôn thành công.

VnPro cơ sở vật chất luôn được đầu tư mới theo nhu cầu thị trường

Trong 12 năm hoạt động, VnPro luôn luôn đổi mới phòng học và thiết bị phù hợp với công nghệ hiện tại. Tính từ thời điểm mới thành lập các Router 2500 đã được đưa vào sử dụng, thời điểm đó thiết bị này được xem là hàng top trong lĩnh vực mạng, cho tới nay toàn bộ đã được thay thế bằng các thiết bị Router 2800, Switch đa lớp 3560, PIX thì được nâng cấp lên ASA 5520.. các PC đều được trang bị từ core 2 duo trở lên. Hàng năm VnPro luôn nâng cao chất lượng thiết bị, và mới đây nhất là hệ thống Lab Voice được đưa vào sử dụng với các thiết bị mới như Cisco IP Phone 7960G, Voice Gateway ...

Trong tương lai gần, VnPro sẽ nâng cấp các thiết bị lên thành Router 2900, Switch 3700 ... nhằm đáp ứng nhu cầu cho các khóa học mời, giúp học viên tự tin hơn sau khi học xong.

VnPro đội ngũ nhân sự, giảng viên cao cấp trong ngành

Với khoảng 70 giảng viên fulltime và parttime là thạc sỹ, kỹ sư, và chuyên viên cao cấp đang làm việc cho các công ty, tập đoàn lớn trong nước. Áp dụng các phương pháp đào tạo giảng viên chuyên nghiệp, trải qua nhiều kỳ sát hạch để đạt tiêu chuẩn giảng dạy tại VnPro. Ngoài ra các giảng viên đều có các chứng chỉ quốc tế phù hợp với chương trình giảng dạy từ cấp độ CCNA đến CCIE. Tham gia các khóa học, học viên được truyền đạt các kiến thức thực tế, các mô hình doanh nghiệp đang áp dụng giúp học viên có cái nhìn nhận thực tế sau khi học và áp dụng được ngay trong công việc hiện tại.

VnPro đi đầu trong lĩnh vực đào tạo công nghệ mạng Cisco

VnPro thành lập từ tháng 3/2003, thời điểm này cũng là lúc công nghệ Cisco được đưa vào đào tạo tại Việt Nam (VN) phổ biến. Các khóa học đầu tiên được tổ chức cùng sự dẫn dắt của CCIE đầu tiên là Thầy Đặng Quang Minh (CCIE#11897), tiếp bước thành công này VnPro đã đào tạo thành công 10 CCIE lab và hàng ngàn CCNA và CCNP R&S. Bên cạnh đó, VnPro cũng là trung tâm đi đầu về sự thích ứng trong công nghệ với chu kỳ khoảng 3-4 năm lại cập nhật thay đổi các môn học 1 lần theo tiêu chuẩn Quốc tế và lần cập nhật mới đây là CCNP Version 2 với 3 môn học Route (300-101), Switch (300-115), Tshoot (300-135) đã đưa vào đào tạo từ tháng 9 năm 2014.

Đối với những lĩnh vực đào tạo khác ngoài Routing & Switching truyền thống như Security, Voice, Data center, ... VnPro cũng là trung tâm đi đầu trong phát triển đào tạo các công nghệ này, cụ thể hơn đó là CCIE Security đầu tiên tại VN - Thầy Bùi Nguyễn Hoàng Long cũng được ra đời tại "lò luyện" này. Nhận thấy sự phức tạp và khó khăn trong công việc nghiên cứu và triển khai tích hợp truyền thông hợp nhất vào hệ thống, VnPro cũng đã cung cấp cho giới IT doanh nghiệp các khóa đào tạo CCNA Voice (640-461) và CCNP Voice giúp cho doanh nghiệp hiện thực được các dịch vụ gia tăng một cách hoàn thiện hơn. Với sự tín nhiệm của sinh viên, IT doanh nghiệp và các doanh nghiệp lớn như ISP, Ngân hàng, IDC, công ty tài chính, DN nước ngoài... cũng chứng tỏ được năng lực đào tạo và chất lượng đào tạo uy tín của VnPro trong suốt 12 năm hoạt động.

VnPro cung cấp nguồn lực chất lượng cao cho thị trường lao động

Ảnh tổng hợp các hoạt động cộng đồng

VnPro thường xuyên tổ chức các hoạt động "vì cộng đồng"

Một số hoạt động từ thiện

Cung cấp nguồn lực chất lượng cao cho thị trường lao động

Gần 12 năm hoạt động, cũng ngần ấy thời gian VnPro cung cấp cho thị trường lao động hàng ngàn IT có trình độ chuyên môn chất lượng cao sau đào tạo. Theo đó là các chương trình Roadshow, kết nối doanh nghiệp, kết nối nhà tuyển dụng, chỉnh sửa hồ sơ, chuyển tiếp hồ sơ cho nhà tuyển dụng. Với sự tin tưởng của các nhà tuyển dụng lớn như FPT, HPT, HiPT, VNPT, Viettel, SPT.. khối ngân hàng như ACB, HDBank, HSBC, Sacombank, VietinBank, SHB...và hàng ngàn doanh nghiệp khác trong và ngoài nước. Hàng tháng VnPro đều nhận được thông tin tuyển dụng và giới thiệu cung cấp nguồn lực chất lượng cao. Chương trình kết nối đều được VnPro tài trợ và thực hiện trong suốt quá trình hoạt động.

Chương trình hỗ trợ sinh viên, từ thiện xã hội

Nhóm sinh viên thực tập tại VnPro

Đối với sinh viên, VnPro là nơi đào tạo nền tảng ban đầu để hội tụ những kỹ năng nhất định trong bước tiến sự nghiệp của mỗi sinh viên, hàng năm VnPro tổ chức 4 đợt tiếp nhận sinh viên thực tập từ các trường, thông qua các giáo trình thực tập khắt khe, hầu hết tất cả các luận văn đều được bảo vệ thành công và nhận được đánh giá cao từ hội đồng nhà trường. Quá trình thực tập, sinh viên sẽ được hướng dẫn cụ thể từng chi tiết nhỏ, được hỗ trợ tối đa về thiết bị, phòng lab, được hướng dẫn nhiệt tình qua các tình huống thực tế... đây cũng là hành trang giúp các bạn ra đời có thêm nhiều thành công hơn.

Với tinh thần vì cộng đồng nên trong suốt 12 năm hoạt động, VnPro luôn chia sẽ bớt những khó khăn của xã hội từ những chương trình thiết thực như phát gạo từ thiện, phát động ủng hộ hộ nghèo, quyên góp đồng bào bị lũ lụt thiên tai, tặng vé xe buýt cho sinh viên, chương trình hiến máu nhân đạo và hàng trăm học bổng khuyến học Cisco do VnPro tài trợ.

Hàng năm, Ban giám đốc VnPro cũng trích ra 1 phần từ kinh doanh để tham gia các chương trình từ thiện xã hội do phường, quận, hay các đoàn thể hiệp hội cùng tổ chức, với mong muốn san sẽ những khó khăn của mọi người trong cuộc sống.

Tiếp bước 2015, VnPro tiếp tục khẳng định vị trí của mình trên thị trường: Đi đầu trong lĩnh vực đào tạo Cisco, chất lượng đào tạo, ... Trong thời gian tới VnPro đặt mục tiêu phát triển trung tâm lớn mạnh hơn nữa, có nhiều chương trình thiết thực hơn nữa và công tác cộng đồng sôi động hơn nữa.

(VnPro News).

Phỏng vấn thầy Trần Quảng Thanh

Thầy Trần Quảng Thanh – Trưởng phòng Dự án đào tạo, Giảng viên CCIE của VnPro và cũng là chuyên gia network với hơn 10 năm kinh nghiệm trong ngành, thực hiện nhiều dự án lớn cho các tập đoàn đa quốc gia, các công ty lớn trong nước và quốc tế. Thêm vào đó thầy cũng thường xuyên tích lũy kinh nghiệm, nâng cao kiến thức với nhiều chứng chỉ như CCIE WR, CCNP VoIP (Voice over IP), Security, Datacenter…

Để giúp các bạn học viên có thể hiểu rõ hơn về chuyên ngành network, VnPro đã có cuộc trao đổi ngắn với thầy Thanh về những xu hướng hệ thống mạng trong tương lai, kèm theo đó những lời khuyên của thầy dành cho các bạn học viên, giúp các bạn có thêm những định hướng về ngành network.

Chào thầy Thanh, VnPro muốn hỏi thầy là tính đến thời điểm hiện tại thầy đã gắn bó với lĩnh vực công nghệ thông tin được bao lâu rồi ? Và kế hoạch sắp tới của thầy sẽ có những dự án mới cho công tác giảng dạy tại VnPro hay không ?

Hơn 10 năm gắn bó với công nghệ thông tin, với trải nghiệm của tôi trong ngành tại các doanh nghiệp lớn trong và ngoài nước thì các kỹ sư công nghệ thông tin hiện nay cần trang bị cho mình những kiến thức cơ bản như Routing & Switching, Security. Ngoài ra, để theo kịp với công nghệ thì những mảng như VoIP, Datacenter cũng đang là những làn gió mới trong mạng doanh nghiệp mang lại lợi ích lớn về kinh tế. Vì thế, kế hoạch của tôi trong công tác đào tạo tại VnPro ngoài việc tập trung update version R&S, Security sẽ còn đẩy mạnh thêm các mảng VoIP và Datacenter.

Vậy theo thầy, với số lượng lớn kiến thức như vậy chúng ta sẽ phải có bí quyết nào để giúp thầy học tốt, và trở thành 1 networker giỏi ?

Phương châm học của tôi " học đi đôi với hành" khi chúng ta nghiên cứu kiến thức gì thì phải kiểm chứng tính chính xác của kiến thức đó qua lab hoặc là bạn bè đồng nghiệp rồi sau đó viết document lại để lưu giữ những kiến thức, hệ thống lại để có nền tảng vững chắc về chuyên môn.

Với tầm nhìn của thầy về chuyên ngành mạng, theo thầy mảng nào của Cisco sẽ là mảng phát triển trong tương lai ở nước ta ?

Theo tôi, nền tảng vẫn là Routing và Switching, tuy nhiên trong tương lai sẽ có thêm các mảng Voice base over IP (VoIP) và Datacenter. Hiện tại ở nước ta VoIP đang là luồng gió mới trong lĩnh vực công nghệ, tích hợp hệ thống thoại dựa trên nền tảng IP tạo nhiều thuận lợi trong công tác quản trị (**Management**), khả năng mở rộng (**Scalability)** dễ dàng tận dụng tối đa năng suất sản phẩm (**Productivity**) và giảm chi phí dịch (**Cost**) vụ về hội thoại, mang lại nhiều tiện lợi và lợi ích kinh tế cho doanh nghiệp. Còn với các doanh nghiệp từ xưa đến nay thì quan trọng nhất vẫn là cơ sở dữ liệu, khi doanh nghiệp phát triển càng mạnh thì cơ sở dữ liệu càng phình ra nhưng vẫn đảm bảo truy xuất giữ liệu phải có kết quả nhanh. Muốn được như vậy thì các doanh nghiệp phải triển khai, xây dựng hệ thống Datacenter đảm bảo tính security, backup dữ liệu và sự mở rộng của cơ sở dữ liệu khi quy mô doanh nghiệp ngày càng phát triển.

Thầy có thể cho các bạn học viên VnPro biết thêm các dự án lớn mà thầy đã thực hiện triển khai thành công trong công việc của mình từ lúc thầy theo ngành ?

Với hơn 10 năm theo nghề thì những dự án tôi triển khai rất nhiều vd như : HSBC, BP Oil & Gas, AIG/AIA, Nestle, Colgate, Pepsi, Coca cola, QTSC, Adidas, Citi Bank, Fubon Bank, Dai-chi-life, VINCOM, VTI+FPT+Cisco System VN (Telepresence System), HoTram Resort Casino 5 star plus….

Cảm ơn thầy Thanh rất nhiều !

Cuộc trò chuyện ngắn với thầy đã giúp cho các bạn học viên VnPro định hướng và hiểu biết thêm rất nhiều về công việc trong tương lai của các bạn.

Chúc Thầy nhiều sức khỏe và tiếp tục gặt hái được nhiều thành công!

Sinh viên thực tập được trải nghiệm và làm việc thực tế tại VnPro

Nhằm tạo điều kiện để các bạn sinh viên tại các trường Đại Học, Cao Đẳng, Trung Cấp được thực tập và trải nghiệm trong môi trường làm việc chuyên nghiệp, giúp các bạn tích lũy kinh nghiệm thực tế. Hằng năm, Trung Tâm VnPro tổ chức đều đặn các đợt tiếp nhận sinh viên thực tập.

Thực tập tại Trung tâm tin học VnPro, các bạn sẽ được hướng dẫn từ lý thuyết đến thực hành, các kỹ năng mềm cần thiết cho công việc từ trưởng bộ phận, các chuyên viên và đội ngũ giảng viên nhiệt tình và giàu kinh nghiệm.

Trong đợt thực tập này, bên cạnh việc nghiên cứu, thực hiện đề tài của mình, các bạn sinh viên sẽ được tiếp xúc và triển khai thực tế:

- Xây dựng thực tế hệ thống mạng VoIP từ A-Z phục vụ doanh nghiệp.
- Xây dựng cơ chế quản lý, đánh nhãn thiết bị theo tiêu chuẩn quốc tế.
- Triển khai nâng cấp hệ thống mạng, switch Cisco của doanh nghiệp lên tối thiểu 1Gbps.
- Thực hiện dự án vụ di chuyển hệ thống mạng doanh nghiệp lên môi trường ảo hóa.

Và đây là những chia sẻ, cảm nhận của các bạn sinh viên đang thực tập tại VnPro trong đợt này:

Cảm nhận từ bạn Lê Hoàng Khánh:

VnPro sở hữu riêng cho mình hệ thống mạng doanh nghiệp với quy mô hơn một trăm nhân viên. Thực tập tại đây mình được làm quen với mô hình mạng thực tế, trực tiếp cấu hình, xử lý các sự cố. Ngoài ra, mình còn được tham gia vào dự án xây dựng mới hệ thống tổng đài VoIP với sự hướng dẫn nhiệt tình từ các giảng viên giàu kinh nghiệm của trung tâm. Thêm vào đó, các công hằng ngày tại trung tâm như quản lý website, diễn đàn, hỗ trợ học viên, quản lý thiết bị… giúp mình rèn luyện sự tỉ mỉ, cẩn thận, tính kỉ luật, thái độ đối với công việc. Ba tháng thực tập tại VnPro đã giúp mình bước đầu tích lũy được những kinh nghiệm thực tế phục vụ cho công việc sau này.

Cảm nhận từ bạn Cao Trần Hữu Lộc:

Ban đầu, mình đến với chương trình thực tập VnPro với mong ước được trao dồi kiến thức của mình về lĩnh vực mạng máy tính. Sau hơn một tháng thực tập, mình nhận ra được nhiều điều hơn thế. Tuy những ý định và dự án ban đầu vẫn chưa có thời gian thực hiện, nhưng bù lại mình được tiếp xúc rất nhiều với những công việc mang tính thực tế hơn, từ những việc nhẹ nhưng nhiều như kiểm tra thiết bị, sửa chữa máy tính, dán nhãn… đến những dự án mang tầm vóc vĩ mô như triển khai hệ thống VoIP cho công ty. Các anh chị trong trung tâm cũng rất thân thiện, môi trường làm việc rất thoải mái. Tuy khối lượng thời gian và công sức bỏ ra ở VnPro, cộng với chương trình học ở trường, có thể nói là khá vất vả với mình trong thời gian đầu, tuy nhiên giờ đây mình đã quen dần với mạch làm việc và thật sự rất vui vì quyết định thực tập của mình.

Cảm nhận từ bạn Phạm Thanh Đông Khê:

Hiện tại mình đã hoàn thành chương trình đại học. Trong thời gian chờ nhận bằng tốt nghiệp, mình quyết định xin thực tập tại VnPro để học hỏi, tích lũy kinh nghiệm, tìm hiểu môi trường làm việc thực tế.

Mình đã thực tập đây được 2 tuần. Ngay ngày đầu tiên vào thực tập mình đã được tham gia dự án về VoIP, từ nghiên cứu sơ đồ mạng đến mua sắm thiết bị, lắp đặt cho các phòng học vì sắp tới VnPro sẽ là trung tâm đầu tiên tại Việt Nam tổ chức khóa học CCNA Voice. Đây là lần đầu tiên mình tham gia vào các công việc như thế này nên hơi vất vả nhưng ngược lại mình nhận được sự hướng dẫn tận tình của các thầy, các anh kỹ thuật cùng các anh chị khác tại trung tâm và các bạn cùng thực tập cũng rất nhiệt tình, vui vẻ. Ngoài ra mình còn được tham gia vào các công việc khác như đăng bài, quản trị các website của VnPro, được sử dụng các thiết bị mạng thật của Cisco, biết được các thông tin tuyển dụng của các doanh nghiệp gửi đến trung tâm,… đây đều là các hoạt động thực tế rất có ích với người sắp ra trường như mình.

Cảm nhận từ bạn Nguyễn Hoài Nam:

VnPro là trung tâm nghiên cứu và đào tạo mạng Cisco với đội ngũ giảng viên đầy kinh nghiệm, đã có nhiều học viên đạt chứng chỉ CCIE-chứng chỉ cao nhất của Cisco. VnPro có đội ngũ giảng viên đầy kinh nghiệm, giảng dạy và hướng dẫn học viên một cách tường tận, bám sát với thực tế…Khi được thực tập thực tế tại VnPro em cảm thấy rất thoải mái và vui vẻ.

Chúc VnPro càng ngày càng phát triển trên những bước tiến sau này.

Cảm nhận từ bạn Lương Ngọc Đức:

Đến với VnPro chỉ là dịp tình cờ. Nhưng sau thời gian học CCNA ở đây, tôi cảm thấy nơi đây có một thứ "tình" gì đó khác lạ. Vừa vui vẻ, hòa đồng, thân thiện lại có chút quan tâm, lo lắng của mọi người. Quay lại VnPro lần này, với vai trò là thực tập sinh, tôi càng tin tưởng hơn về khả năng quyết định lựa chọn công ty thực tập của mình, được các anh hướng dẫn tận tình từ những việc đầu tiên, từ những thứ nhỏ nhất. Nói về VnPro, chắc có lẽ còn nhiều lắm, mỗi người rồi sẽ có những cảm nhận và kỉ niệm riêng khi gắn kết với nơi này. Cảm ơn VnPro đã cho tôi thêm nhiều kiến thức, hành trang để bước vào đời. Hứa hẹn một ngày không xa, tôi lại quay về VnPro lần nữa. Chúc VnPro ngày càng phát triển lớn mạnh, vững bền.

Cảm nhận từ bạn Đinh Đại Đồng:

Đến với VnPro, được học tập và thực tập đó là một điều vô cùng may mắn đối với mình. Ở đây, mình nhận được rất nhiều sự giúp đỡ và hướng dẫn tận tình của các thầy, anh chị và các bạn ngoài ra còn có cả cô lao công, chú bảo vệ nữa. Những kiến thức và kinh nghiệm mình nhận được không những giúp ích rất nhiều trong quá trình hoàn thiện kiến thức, năng lực bản thân mà còn cả sau này khi mình đi làm… Một lần nữa mình xin cám ơn VnPro - luôn tận tâm và sẻ chia!

Cảm nhận từ bạn Trương Quang Lân:

Mình là Trương Quang Lân, sinh viên khoa Công Nghệ Thông Tin, trường đại học Khoa Học Tự Nhiên Thành Phố Hồ Chí Minh. Mình rất cảm ơn trung tâm VnPro đã tạo cơ hội được thực tập tại trung tâm trong 3 tháng dưới sự hướng dẫn của anh Tuấn. Trong thời gian này mình đã nhận được nhiều sự giúp đỡ từ trung tâm như được hỗ trợ miễn phí thiết bị để thực hiện các đề tài thực tập, được sự chỉ dẫn tận tình từ các thầy… Chính những điều này đã giúp mình học hỏi được thêm nhiều kiến thức và kinh nghiệm nâng cao trình độ chuyên môn về chuyên ngành mạng.

Bằng chính những chia sẻ này VnPro hy vọng sẽ cho bạn sinh viên thực tập mùa sắp tới những cái nhìn thực tế về môi trường thực tập tại VnPro.

VnPro xin chúc các bạn sinh viên thực tập tiếp tục gặt hái được nhiều thành công, thu được nhiều kinh nghiệm triển khai hệ thống mạng thực tế sau khi kết thúc đợt thực tập. Chúc các bạn hoàn thành và đạt kết quả tốt trong học tập.

VnPro – Đào tạo chuyên gia mạng Quốc Tế!

Cấu hình theo dõi đường static route sử dụng tính năng ip sla

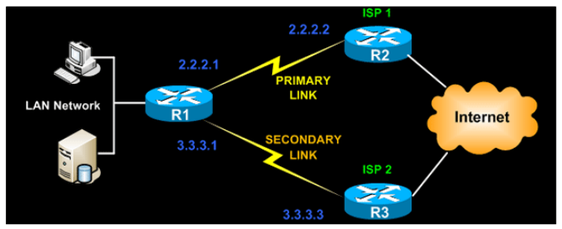
Trong môi trường mạng hiện nay, yếu tố dự phòng (***redundancy***) là một trong những khía cạnh quan trọng nhất, bất kể ở mạng LAN hoặc mạng WAN. Trong chủ đề này mình sẽ sử dụng tính năng dự phòng trong mạng WAN với nhiều kết nối WAN trên một router duy nhất.

Cách tốt nhất và đơn giản nhất để thực hiện tính năng dự phòng mạng WAN trên các thiết bị Cisco là sử dụng sao lưu các tuyến đường tĩnh đáng tin cậy (***Reliable Static backup routes***) với công nghệ IP SLA tracking.

IP SLA là một tính năng có trong phần mềm Cisco IOS cho phép các quản trị viên có khả năng phân tích các cấp độ dịch vụ IP cho các ứng dụng và dịch vụ IP. IP SLA sử dụng công nghệ traffic-monitoring để giám sát hoạt động giao thông liên tục trên hệ thống mạng. Đây là một phương pháp đáng tin cậy và hàng đầu trong việc đo lường hiệu suất mạng. Các Router của Cisco cung cấp tính năng IP SLA Responders, nó cho biết tính chính xác của dữ liệu đo được qua hệ thống mạng.

Với IP SLA, thiết bị Router và Switch thực hiện phép đo định kỳ. Số lượng và loại của các phép đo có sẵn là rất lớn và trong bài viết này mình sẽ nói về tính năng ICMP ECHO.

Chúng ta hãy lấy một ví dụ về các đường liên kết dự phòng trong một mạng WAN cơ bản như hình dưới đây:



Trong hình trên các thiết bị của Cisco được kết nối với ISP1 và ISP2. Các thiết lập phổ biến nhất mà chúng ta sử dụng trong cuộc sống hằng ngày là phải có cấu hình ***default routes*** trên router Cisco với ***next-hop IPs*** tương ứng như hình dưới đây:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 3.3.3.3 10
```

Nếu bạn chú ý tới số AD (***Administrative Distance***) của đường secondary route trỏ tới ISP2 sẽ được tăng lên 10 để nó trở thành các đường liên kết dự phòng (***backup link***).

Cấu hình trên chỉ với hai tuyến đường định tuyến tĩnh là một phần hoàn thành yêu cầu vì nó sẽ chỉ làm việc trong trường hợp mà các cổng router kết nối với các liên kết WAN đang ở trạng thái up/ down hoặc down/ down. Nhưng trong rất nhiều tình huống, chúng ta thấy rằng mặc dù các liên kết vẫn ở trạng thái up nhưng chúng ta không thể tiếp cận tới cổng gateway, vấn đề này thường xảy ra và lỗi là ở phía ISP.

Trong tình huống như vậy, IP SLA trở thành người bạn tốt nhất của một kỹ sư mạng. Với khoảng 6 câu lệnh được thêm vào, chúng ta có thể có một môi trường tự động chuyển đổi dự phòng đáng tin cậy hơn.

Sử dụng IP SLA bản Cisco IOS có khả năng sử dụng Internet Control Message Protocol (ICMP) dung lệnh ***ping*** để xác định khi một liên kết WAN bị tắt khi quá trình truy cập kết thúc và khi đó nó sẽ cho phép bắt đầu một kết nối sao lưu từ một port thay thế. Lệnh Reliable Static Routing Backup sử dụng tính năng theo dõi đối tượng để có thể đảm bảo đường dự phòng đó đáng tin cậy trong trường hợp của một vài trường hợp xấu nhất có thể xảy ra, như đứt mạch Internet hay các thiết bị ngang hàng bị lỗi.

IP SLA được cấu hình để ping một mục tiêu, chẳng hạn như một địa chỉ IP công khai hoặc một mục tiêu bên trong mạng công ty hoặc một next-hop IP trên router của ISP. Lệnh ping sẽ được chuyển tới một cổng duy nhất.

Sau đây là một ví dụ về cấu hình của IP SLA để tạo ra lệnh ping icmp nhằm mục tiêu vào các ISP1 next-hop IP:

```
R1(config)# ip sla 1
R1(config)# icmp-echo 2.2.2.2 source-interface FastEthernet0/0
R1(config)# timeout 1000
R1(config)# threshold 2
R1(config)# frequency 3
R1(config)# ip sla schedule 1 life forever start-time now
```

Xin lưu ý rằng các câu lệnh Cisco IP SLA đã thay đổi qua các bản IOS khác nhau. Để biết lệnh chính xác phù hợp với bản IOS, các bạn nên kiểm tra tài liệu của Cisco. Các lệnh trên là dành cho IOS 12,4(4)T, 15(0)1M và các bản IOS sau này.

Cấu hình trên đã tạo và bắt đầu một cuộc dò xét IP SLA.

- Lệnh ICMP Echo cứ mỗi 3 giây sẽ gửi một gói tin ICMP Echo tới next-hop 2.2.2.2 IP.
- Thời gian chờ timeouts được thiết lập (tính bằng mili giây) cho mỗi hoạt động của Cisco IOS IP SLA đề chờ đợi một phản ứng từ gói theo yêu cầu của nó.
- Ngưỡng này tạo ra một sự kiện phản ứng và lưu trữ thông tin lịch sử cho sự vận hành Cisco IOS IP SLA.
- Sau khi xác định các hoạt động IP SLA, bước tiếp theo của chúng ta là xác định một đối tượng theo dõi thăm dò SLA. Điều này có thể được thực hiện bằng cách sử dụng lệnh IOS Track Object như hình dưới đây:

```
R1(config)# track 1 ip sla 1 reachability
```

- Lệnh trên sẽ theo dõi tình trạng hoạt động IP SLA. Nếu không có lệnh ping phản hồi từ IP next-ho, quá trình theo dõi sẽ bị tắt đi và nó sẽ mở lại khi hoạt động IP SLA bắt đầu nhận được lệnh ping phản hồi.
- Để kiểm tra, theo dõi tình trạng, ta sử dụng lệnh "show track" như hình dưới đây:

```
R1# show track

Track 1
IP SLA 1 reachability
Reachability is Down
1 change, last change 00:03:19
Latest operation return code: Unknown
```

- Kết quả trên cho thấy quá trình bị tắt. Mọi hoạt động IP SLA duy trì một giá trị mã trả về (return-code). Mã trở về này được giải thích bởi quá trình theo dõi. Mã trả lại có thể trả lời OK, mặt khác, một số mã trả lại sẽ cho giá trị khác.
- Các hoạt động khác nhau có thể có giá trị mã trả lại khác nhau, vì vậy chỉ có vài giá trị phổ biến cho tất cả các loại hoạt động được sử dụng. Bảng dưới đây cho thấy các quá trình theo dõi một mã IP SLA trả lại:

Tracking	Return Code	Track State
Reachability	OK or over threshold	Up
	(all other return codes)	Down

Bước cuối trong cấu hình IP SLA Reliable Static Route là thêm "track" các tuyến đường default routes trỏ đến các router ISP như hình dưới đây:

```
R1(config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2 track 1
R1(config)# ip route 0.0.0.0 0.0.0.0 3.3.3.3 10
```

Sự kết hợp từ khóa số theo dõi và lập luận xác định rằng các đường định tuyến tĩnh (static route) chỉ được cài đặt nếu trạng thái của đối tượng theo dõi là ***Up***. Do đó nếu trạng thái của đối tượng theo dõi là ***Down,*** đường định tuyến dự phòng (secondary route) sẽ được sử dụng để chuyển tiếp tất cả các lưu lượng truy cập.

Người biên soạn: Phan Thanh Phong.

Liên kết tham khảo:
http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/813-cisco-router-ipsla-basic.html

Bảo mật mạng vlan một cách tốt nhất

Bài viết này tập trung vào vấn đề đảm bảo sự an toàn cho VLAN và cách thực hiện nó trong môi trường mạng doanh nghiệp. Mình sẽ đưa ra những mẹo và câu lệnh của Cisco để giúp các bạn nâng cấp độ an toàn cho mạng VLAN.

Mặc dù nhiều quản trị viên và người quản lý CNTT đều nhận biết được khái niệm và công nghệ của VLAN. Nhưng không may thay, thực tế đã chứng minh rằng chúng ta không thể áp dụng nó cho việc bảo mật mạng VLAN. Trong phần này, chúng ta chủ yếu tập trung vào việc thực hiện trên switch Cisco, nhiều khái niệm có thể được áp dụng trên các thiết bị Switch của nhà cung cấp khác.

Nguyên tắc đầu tiên trong việc đảm bảo một mạng VLAN an toàn là bảo mật vật lý (***physical security***). Nếu bạn không muốn thiết bị của mình bị giả mạo, truy cập vật lý (***physical access***) đến các thiết bị phải được kiểm soát chặt chẽ. Các Core switch thường được đặt một cách an toàn trong một trung tâm dữ liệu (***datacenter***) với truy cập hạn chế, tuy nhiên các Switch vùng biên (***edge switches***) không được may mắn như vậy và thường được đặt ở những nơi mà có thể dễ dàng tiếp xúc được.

Cũng như hướng dẫn của việc bảo mật vật lý (***physical security***) yêu cầu các thiết bị phải được đặt trong một không gian kiểm soát, bảo mật mạng VLAN dựa trên đòi hỏi việc sử dụng các công cụ đặc biệt và vài "hoạt động bảo mật tốt nhất"để cung cấp các kết quả như mong muốn.

Chúng ta hãy xem xét một vài bước quan trọng mà một quản trị viên (***Administrator***) hay một IT Manager dùng để xử lý các vấn đề an ninh hầu hết các mạng mắc phải trong thời buổi hiện nay:

1. **Loại bỏ các loại cáp CONSOLE-PORT, giới thiệu về việc sử dụng truy cập bằng CONSOLE/VTY có password với quy định về timeouts và giới hạn truy cập.**

Cổng Console ở mặt sau thiết bị Switch của Cisco giúp chúng ta truy cập trực tiếp vào hệ thống. Nếu các bạn không chú ý đảm bảo an toàn cho phương pháp truy cập này, khi đó thiết bị Switch có thể được truy cập vào bởi bất cứ ai, chỉ bằng một sợi cáp console màu xanh dương khá phổ biến hiện nay. Thông tin người sử dung thiết bị sẽ được hiển thị trên dây console và các cổng telnet/ ssh sẽ đảm bảo ngăn chặn bất cứ người lạ nào khi cố gắng truy cập vào thiết bị. Sử dụng các lệnh đặc biệt như lệnh "***exec-timeout***", khi người quản trị Administrator vô tình quên đăng xuất khỏi phiên truy cập, thiết bị có 1 khoảng thời gian chờ (timeout) được cấu hình tuỳ chỉnh và sẽ tự động logout sau khi hết khoảng thời gian chờ đó

Sau đây là một tập hợp các lệnh sẽ giúp các bạn thực hiện các biện pháp hạn chế truy cập vào Switch:

```
Switch# configure terminal
Switch(config)# username admin privilege 15 secret *Firewall.cx*
Switch(config)# line console 0
Switch(config-line)# login local
Switch(config-line)# password cisco
Switch(config-line)# exec-timeout 60 0
```

Mình cũng áp dụng các lệnh này tương tự vào phần VTY (telnet/ ssh) và tạo ra access-list 115 để hạn chế truy cập telnet/ ssh từ một số các mạng và host nhất định:

```
Switch (config)# line vty 0 15
Switch (config-line)# password cisco
Switch (config-line)# login local
Switch (config-line)# exec-timeout 60 0
Switch (config-line)# transport preferred ssh
Switch (config-line)# access-class 115 in
```

Dưới đây là access-list 115 mà mình đã tạo ra:

```
Switch (config)# access-list 115 remark -=[Restrict VTY Access]=-
Switch (config)# access-list 115 permit ip host 74.200.84.4 any
Switch (config)# access-list 115 permit ip host 69.65.126.42 any
Switch (config)# access-list 115 permit ip 192.168.50.0 0.0.0.255 any
Switch (config)# access-list 115 remark
```

Luôn luôn đảm bảo việc sử dụng các thông số "***Secret***" hơn là thông số "***Password***" trong cú pháp tên đăng nhập của bạn. Khi xác định tên người dùng (usernames) và mật khẩu (passwords) của họ, thông số "***Password***" sử dụng một thuật toán mã hóa yếu hơn nhiều mà nó có thể mã hóa một cách dễ dàng.

2. Tránh sử dụng VLAN1 (DEFAULT VLAN) cho hệ thống dữ liệu mạng của bạn.

VLAN 1 là VLAN đặc biệt được lựa chọn để chứa các thông tin cụ thể cho các giao thức như CDP (Cisco Discovery Protocol), VTP, PAgP và nhiều hơn nữa. VLAN 1 chưa bao giờ được dự định sẽ được sử dụng như một VLAN tiêu chuẩn để chứa các dữ liệu mạng.

Bởi vì cấu hình mặc định, bất kỳ liên kết truy cập (Access Link) trên một switch Cisco đều được đặt vàoVLAN 1, điều này gây ra một vấn đề an ninh quan trọng như việc truy cập trực tiếp đến các mạng backbone. Và kết quả là, VLAN 1 có thể kết thúc việc mở rộng hệ thống mạng một cách không kiểm soát nếu không loại bỏ một số tính năng nhất định.

Việc sử dụng một VLAN như vậy cho mục đích quản lý sẽ làm các thiết bị đáng tin cậy có nguy cơ bị tấn công an ninh từ các thiết bị không tin cậy rằng bằng cách cấu hình sai hoặc khai thác những lỗi cơ bản để truy cập vào VLAN 1 và cố gắng khai thác lỗ hổng bảo mật bất ngờ này.

Như một quy luật chung, người quản trị mạng nên lượt bỏ bớt VLAN, và đặc biệt là VLAN 1 từ tất cả các cổng nơi mà VLAN đó không cần thiết sử dụng đến.

Ví dụ sau đây mình đã lượt bỏ VLAN 1-5 và 7-8, chỉ cho phép truy cập vào VLAN 6 khi ở chế độ ***trunking mode***. Hơn nữa, mình cũng chỉ gán các cổng vào VLAN 6 mà thôi:

```
Switch(config)# interface fastethernet0/24
Switch(config-if)# switchport trunk allowed vlan remove ? (help)
WORD  VLAN IDs of disallowed VLANS when this port is in trunking mode

Switch(config-if)# switchport trunk allowed vlan remove 1,2,3,4,5,7,8
Switch(config-if)# switchport access vlan 6
```

3. Tắt các giao thức mà có nguy cơ bị tấn công cao trên các cổng không được sử dụng

Nếu một cổng được kết nối với một thiết bị bên ngoài, không nên cố gắng hồi đáp lại nó – Bởi vì nó có thể được chuyển sang lợi thế cho người khác và sử dụng chống lại mạng của bạn. Hãy đảm bảo rằng các bạn đã tắt các giao thức như CDP, DTP, PAgP, UDLD (Unidirectional Link Detection Protocol) và luôn luôn bật chức năng ***portfast spanning-tree bpduguard*** trên cổng.

Dưới đây mình sẽ đữa ra một ví dụ về cách để tắt các giao thức nêu trên và ***cho phép spanning-tree portfast bpduguard***:

```
Switch(config)# interface fastethernet0/24
Switch(config-if)# no cdp enable
Switch(config-if)# no udld port
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# spanning-tree guard root
```

Cuối cùng, nếu các cổng không được sử dụng, hãy sử dụng lệnh "***Shutdown***" để đảm bảo nó sẽ không thể được truy cập bởi bất cứ ai mà không được cho phép.

4. VTP DOMAIN, VTP PRUNING và PASSWORD PROTECTION

Có hai sự lựa chọn ở đây - một là cấu hình VTP domain thích hợp hoặc là tắt VTP hoàn toàn! VTP là một công cụ tuyệt vời để đảm bảo tất cả các thông tin VLAN được chứa đựng trên các Switch trong hệ thống mạng của bạn. Nếu các biện pháp an ninh cần thiết không được thực hiện, việc lan truyền cấu hình VLAN trong hệ thống mạng của bạn là dễ dàng như kết nối với một Switch được cấu hình một cách tồi tệ nhất.

Một Switch giả mạo được cấu hình với cùng 'VTP domain', với vai trò là "Server" và có số "VTP revision" cao hơn so với số "VTP revision" của VTP server thật sự (thường là Core Switch), là tất cả những gì cần thiết để gây ra sự gián đoạn lớn và rối loạn trên bất kỳ quy mô mạng nào. Tất cả các switch khác sẽ tự động "lắng nghe" VTP Server giả mạo và xóa tất cả thông tin VLAN hiện có.

Sau đây mình sẽ đưa ra vài lệnh cơ bản để giúp Core Switch của các bạn tránh trường hợp như trên:

```
CoreSwitch(config)# vtp domain firewall.cx
CoreSwitch(config)# vtp password fedmag secret
CoreSwitch(config)# vtp mode server
CoreSwitch(config)# vtp version 2
CoreSwitch(config)# vtp pruning
```

Các Switch ở vùng biên (***edge switches***), sẽ cấu hình theo yêu cầu: "VTP mode client" và "VTP password", sau khi cấu hình lệnh trên, các switch này sẽ tự động tiếp nhận tất cả các thông tin của VLAN từ Core Switch của bạn.

Các bạn có thể kiểm tra cấu hình bằng cách sử dụng lệnh: ***show vtp status***

5. Kiểm soát Inter-Vlan Routing bằng IP Access lists

Inter-VLAN routing là một tính năng tuyệt vời và cần thiết. Bởi vì trong nhiều trường hợp có nhu cầu để cô lập VLAN hoặc hạn chế truy cập giữa chúng, việc sử dụng IP Access lists là bắt buộc.

IP Access lists được tạo ra bằng cách vẫn cho phép luồng dữ liệu giữa các VLAN thông suốt, nhưng không tiếp xúc với các mạng cần được bảo vệ. Sau khi Access Lists được tạo ra, chúng được gán trực tiếp trên cổng VLAN của Swicth Core layer 3. Tất cả lưu lượng truy cập từ các VLAN được gán nếu cố gắng để vượt qua các VLAN khác sẽ bị từ chối theo Access Lists, đảm bảo mạng Core không được tiếp xúc.

Chúng ta hãy lấy một ví dụ phổ biến để thực hiện thủ thuật này thực tế hơn.

Các bạn tạo một VLAN guest (VLAN 6 – mạng 192.168.141.0/24) để cung cấp truy cập Internet miễn phí cho khách hàng đến công ty của bạn. Yêu cầu là cho phép truy cập Internet đầy đủ, nhưng hạn chế quyền truy cập vào các VLAN khác. Ngoài ra, cấu hình một DHCP Server cũng được coi là cần thiết, để làm cho cuộc sống của bạn dễ dàng hơn và ít phiền hà.

Đây là cấu hình sử dụng cho DHCP Server phục vụ VLAN này:

```
CoreSwitch(config)# ip dhcp pool vlan6-Guest-Internet
CoreSwitch(dhcp-config)# network 192.168.141.0 255.255.255.0
CoreSwitch(dhcp-config)# dns-server 192.168.130.5
CoreSwitch(dhcp-config)#  default-router 192.168.141.1
```

Lưu ý rằng 192.168.141.1 là địa chỉ IP của VLAN 6 trên Core Switch và 192.168.130.5 là địa chỉ DNS Server nằm trên các VLAN khác nhau.

Tiếp theo, chúng ta tạo ra một Access Lists cần thiết.

```
CoreSwitch(config)# access-list 100 remark --[Allow Guest DNS requests to DNS Server]--
CoreSwitch(config)# access-list 100 permit udp 192.168.141.0 0.0.0.255 host 192.168.130.5 eq 53
CoreSwitch(config)# access-list 100 remark [Necessary for DHCP Server to receive Client requests]
CoreSwitch(config)# access-list 100 permit udp any any eq bootps
CoreSwitch(config)# access-list 100 permit udp any any eq bootpc
CoreSwitch(config)# access-list 100 remark --[Deny Guest Access to other VLANs]--
CoreSwitch(config)# access-list 100 deny   ip 192.168.141.0 0.0.0.255 192.168.50.0 0.0.0.255 log
CoreSwitch(config)# access-list 100 deny   ip 192.168.141.0 0.0.0.255 192.168.130.0 0.0.0.255 log
CoreSwitch(config)# access-list 100 deny   ip 192.168.141.0 0.0.0.255 192.168.135.0 0.0.0.255 log
CoreSwitch(config)# access-list 100 deny   ip 192.168.141.0 0.0.0.255 192.168.160.0 0.0.0.255 log
CoreSwitch(config)# access-list 100 deny   ip 192.168.141.0 0.0.0.255 192.168.131.0 0.0.0.255 log
CoreSwitch(config)# access-list 100 deny   ip 192.168.141.0 0.0.0.255 192.168.170.0 0.0.0.255 log
CoreSwitch(config)# access-list 100 deny   ip 192.168.141.0 0.0.0.255 192.168.180.0 0.0.0.255 log
CoreSwitch(config)# access-list 100 remark --[Permit Guest Access to everywhere else --Internet ]--
CoreSwitch(config)# access-list 100 permit ip 192.168.141.0 0.0.0.255 any
CoreSwitch(config)# access-list 100 remark
```

Chú ý rằng chúng ta cho phép DNS và DHCP theo yêu cầu ban đầu, và sau đó từ chối truy cập đến tất cả các VLAN. Cuối cùng chúng ta cho phép truy cập ở khắp mọi nơi khác. Cấu trúc hợp lý này của Access Lists được xây dựng để phù hợp với việc thực hiện kiểm tra Top-Down Access List trên các Core Switch.

Nếu chúng ta đặt DNS hoặc BOOTP cuối cùng trong Access Lists, Dù nó sẽ không rõ ràng nhưng việc từ chối truy cập vẫn được áp dụng. Cuối cùng, các thông số "log" sẽ được báo cáo và gửi về cho Core Switch, cho phép chúng ta theo dõi và phát hiện ra bất kỳ khách hàng nào đang cố gắng để truy cập VLAN khác trong công ty.

Bước cuối cùng, các bạn sẽ gán Access Lists vào cổng VLAN mới được tạo ra:

```
CoreSwitch(config)# interface vlan 6
CoreSwitch (config-if)# ip access-group 100 in
```

Tóm lại

Công nghệ VLAN là tuyệt vời - nó cung cấp những cải tiến rất tốt cho hệ thống mạng và cung cấp đường dẫn để chạy nhiều dịch vụ trong môi trường bị cô lập mà không bị mất tốc độ, chất lượng và hiệu năng của hệ thống mạng. Nếu các nguyên tắc bảo mật cơ bản cần thiết được đưa vào xem xét trong quá trình thực hiện ban đầu, nó có thể thực hiện điều kỳ diệu và làm giảm đáng kể chi phí hành chính từ quản trị viên IT (Administrators) hoặc quản lý (Managers). Mặt khác, nếu các nguyên tắc bảo mật bị bỏ qua, hệ thống mạng của bạn sẽ có nguy cơ bị tấn công và chỉ vấn đề chỉ là thời gian mà thôi.

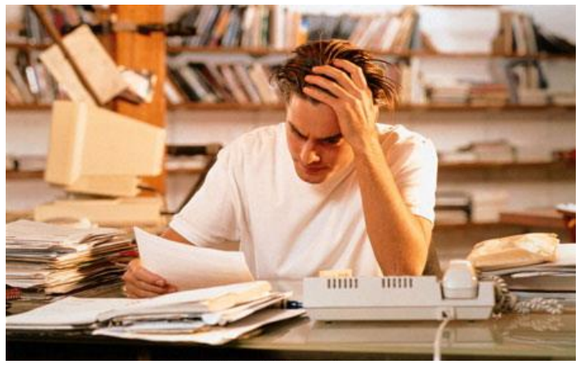
Có lẽ sai lầm nghiêm trọng nhất mà một quản trị viên IT (Administrators) hoặc quản lý (Managers) là đánh giá thấp tầm quan trọng của tầng Data Link layer, và các VLAN đặc biệt trong kiến trúc của hệ thống mạng.

Người biên soạn: Phan Thanh Phong.

Kỹ năng làm chủ cảm xúc – Hóa giải áp lực

"Mỗi ngày chọn một niềm vui" để hướng tới giá trị sống tích cực.

Trong đời ai cũng có thể đối diện với những bất ngờ gây sốc, lúc đó kỹ năng ứng phó và bản lĩnh của từng người sẽ được bộc lộ và được xã hội thẩm định một cách rõ nét nhất. Tại sao người ta lại khủng hoảng, có khi khủng hoảng nặng nề đến vậy? Làm sao để có thể vượt qua khủng hoảng và ứng xử phù hợp với những bất ngờ không muốn có đó...?



Sự căng thẳng có thể đến với chúng ta bất kỳ lúc nào khi người ta không nhìn nhận vấn đề một cách bình thường, không xem xét vấn đề một cách thông thường. Mọi vấn đề đều có thể lý giải trên nhiều góc độ, nhưng nếu chủ thể nhìn nhận sự việc một cách bi kịch thì vấn đề sẽ trở nên nghiêm trọng, thậm chí hết sức trầm trọng. Điều đó sẽ làm cho các chủ thể trở nên lo lắng thái quá, mất phương hướng và nảy sinh những phản ứng tiêu cực. Ở một khía cạnh khác, một khi chủ thể ngộ nhận về giá trị thật của mình, không nhận biết chính xác thái độ tiềm ẩn của người khác đối với mình hoặc có những dự báo quá chủ quan về phản ứng từ cộng đồng, chủ thể cũng sẽ hoang mang, mất tự chủ và nảy sinh phản ứng tiêu cực...

Mặt khác, khi sự kiện nào đó xảy ra, những phản ứng của cộng đồng có khuynh hướng thái quá, vượt khỏi sức chịu đựng của cá nhân có liên quan đến sự kiện ấy thì họ cũng sẽ "đùng đùng nổi giận" và... điên tiết với những phản ứng bất thường. Để trút bỏ căng thẳng và có những phản ứng phù hợp, người ta có nhiều cách thức hết sức đa dạng và tùy thuộc vào tình huống, tùy thuộc vào nguồn gốc vấn đề cũng như môi trường tác động. Tuy nhiên trước hết cần chú ý một số nguyên tắc, những yêu cầu cơ bản giúp chúng ta hạn chế nguy cơ đối diện với căng thẳng, stress ,phòng ngừa và hạn chế những phản ứng thái quá.

- **Làm chủ cảm xúc, điều khiển bản thân** để thích ứng với những biến đổi của môi trường. Để làm được điều này, chúng ta hãy**cố gắng sống thật với cảm xúc**.

- **Sống thật đơn giản với một quan niệm rất đơn giản "điều gì cũng có thể xảy ra, điều gì cũng có thể giải quyết".** Cuộc sống luôn xuất hiện nhiều sự kiện, cả tích cực lẫn tiêu cực, nhưng nếu chúng ta nhận thức các sự kiện trong đời sống xã hội với một thái độ hết sức thiện chí và với niềm tin của chính mình thì hẳn chúng ta sẽ cảm thấy an toàn và chẳng bao giờ căng thẳng. Nhiều người vì quá đặt nặng chuyện thắng thua trong cuộc chơi, quá quan trọng hóa thành tích đã trở nên hụt hẫng và căng thẳng.

- "Mỗi ngày tôi chọn một niềm vui" là một cách có thể giúp chúng ta trút bỏ mệt nhọc để hướng tới những giá trị tích cực của vấn đề. Điều này phản ánh một nguyên tắc hết sức quan trọng là "lấy niềm vui lấn át muộn phiền", một khi chúng ta tự tìm được niềm vui, chúng ta đã thật sự chủ động giải phóng được những áp lực từ môi trường và sẽ cảm thấy thanh thản một cách tự nhiên...

- **Chấp nhận vấn đề như chính nó đang diễn ra** để không có cảm giác thất bại vì nếu cố gắng chối bỏ sự thật thì vấn đề cũng sẽ không được cải thiện. Chấp nhận sự thật như là một phương pháp tự mình cân bằng được cảm xúc, không tự mình dằn vặt bản thân, không tự mình làm mình cảm thấy mất giá trị, điều đó cũng làm chính bản thân không cảm thấy hoài nghi mình. Hãy là chính mình, đừng cố gắng trở thành một ai đó không phải như bản chất của mình. Một khi biết được bản thân mình là ai, chính mình sẽ trở nên dễ chịu với người khác, trở nên cân bằng khi cạnh tranh với người khác.

- **Hãy cố gắng hợp tác với mọi người** để được chia sẻ cảm xúc và tiếp sức trong hoạt động. Môi trường hoạt động thân thiện với người xung quanh làm mọi người ít có cảm giác bất an, sự tự vệ không phải là nỗi lo ám ảnh, điều đó làm tinh thần trở nên phấn chấn và sẽ sẵn sàng "quẳng gánh lo đi để vui sống".

- Điều quan trọng cuối cùng, hãy thật **bình tĩnh xem sự việc xảy đến như một bài học** để mỗi người có cơ hội tự điều chỉnh mình và rút kinh nghiệm để những "rủi ro" không còn xảy ra và sẵn sàng thích ứng một cách chủ động và tự chủ. Dù không thật đơn giản nhưng nếu mỗi người có thiện chí và có kỹ thuật làm chủ bản thân, hành vi của chúng ta có thể sẽ được kiểm soát.

Chuyện vui ngày tết

Điệp khúc mùa xuân

Hai vợ chồng nọ cùng làm một cơ quan, chồng thường hay đi công tác xa, gần Tết chồng điện về hỏi vợ:

- "Em đã thấy mùa xuân chưa?".

Hiểu ý chồng muốn hỏi: "Đã có tiền thưởng Tết chưa?", vợ liền trả lời:

- "Xuân đã về" rồi, nhưng mà "Anh cho em mùa xuân" nghe...

Chồng cụt hứng thở dài:

- Như vậy là đối với anh "Mùa xuân không còn nữa" ư?

- Đương nhiên rồi, đó là "Điệp khúc mùa xuân" mà anh!

Tìm đồ thất lạc

Đêm Giao thừa, một bợm nhậu loay hoay quanh cột đèn đường, cảnh sát hỏi:

- Anh đang làm gì ở đây?

- Tôi đang tìm cái ví bị mất.

- Anh có chắc anh đánh rơi ở đây?

- Không! Nhưng chỉ có chỗ này có ánh sáng để tìm!!!

Tiền lì xì

Cu Tý nhận được rất nhiều tiền lì xì nhân dịp năm mới. Cậu bé dùng số tiền đó để mua sô-cô-la, người bán hàng nói:

- Cháu nên dùng số tiền này để làm từ thiện thì hơn.

- Không. Cháu sẽ mua sô-cô-la và bác sẽ dùng số tiền đó để làm từ thiện.

Thầy đồ làm biếng

Có một thầy đồ rất lười biếng, thường kiếm cớ để không phải dạy dỗ gì cả.

Một hôm ông vào lớp hỏi học trò:

- Tụi bây biết hôm nay học cái gì không?

Cả lớp trả lời:

- Thưa thầy không!

Thầy đồ tỏ vẻ giận dữ:

- Không biết? Vậy tụi mày tới trường để làm cái gì? Cút về hết đi!

Đám học trò khúm núm kéo về hết và bàn với nhau là lần sau thầy có hỏi thì sẽ có cách trả lời xem thầy tính sao.

Hôm sau, thầy giáo lại hỏi:

- Hôm nay tụi bây biết sẽ học cái gì không?

Cả lớp đồng thanh trả lời:

- Dạ biết!

- Đã biết hết rồi thì tụi bây còn ở đây làm cái gì vậy? Về hết đi!

Tụi học trò tức lắm, cho nên bàn rằng kì sau thầy có hỏi thì nửa lớp sẽ trả lời "có" và nửa lớp sẽ trả lời "không" coi thầy tính sao.

Ngày kế tiếp thầy hỏi:

- Bây biết hôm nay học cái gì không?

Nửa lớp trả lời:

- Thưa biết!

Nửa lớp trả lời:

- Thưa không!

- Vậy thì đứa nào biết ở lại dạy mấy đứa không biết, còn tao về!

Bài vè chúc Tết

Nghe vẻ nghe ve, nghe vè chúc Tết

30 mùng Một, năm mới cận kề

Bao nỗi bộn bề qua năm là hết

Chờ ăn bánh Tết bao đỏ liền tay

Tài lộc vận may không mong cũng đến

Tình duyên cặp bến hạnh phúc đáo gia

Chúc khắp mọi nhà quanh năm no đủ

Tiền vô đầy tủ, sự nghiệp vinh quang

Vui vẻ họ hàng người người phấn khởi

Học hành tấn tới khởi sự thành công.

Chuyển đổi địa chỉ MAC Multicast thành địa chỉ IP Multicast

Trong bài viết này, chúng ta sẽ cùng bàn luận về khái niệm chuyển đổi địa chỉ IP thành địa chỉ MAC.

- Để thực hiện việc chuyển đổi địa chỉ IP Multicast ở layer 3 và địa chỉ MAC multicast ở layer 2, dãy 23 bit bậc thấp (low-order) của địa chỉ IP (layer 3) sẽ được chuyển về dãy 23 bit bậc thấp (low-order) của địa chỉ MAC (layer2).
- Dãy 4 bit bậc cao của địa chỉ IP layer 3 được chuyển thành **1110** để chỉ ra không gian địa chỉ lớp D (class D) từ **224.0.0.0** đến **239.255.255.255**
- Địa chỉ MAC Ethernet bắt đầu từ dãy **01:00:5E**, cho phép cho một phạm vi từ **01:00:5E:00:00:00** đến **01:00:5E:7F:FF:FF**.
- Với tổng số 32 bit hiện diện trong một địa chỉ IP và 4 bit bậc cao của nó chuyển thành **1110**. Mình sẽ chừa lại 28 bit của địa chỉ IP đó mà chúng ta có thể sử dụng được (32-4 = 28).
- Nhưng hãy nhớ rằng, 23 bit bậc thấp trong số 28 bit có sẵn được ánh xạ tới địa chỉ MAC, chỉ còn chừa lại cho chúng ta 5 bit.
- Với 5 bit thêm được chồng lên nhau, có 32 địa chỉ IP multicast (2^5 = 32) được chuyển thành một địa chỉ multicast MAC.

Ví dụ sau đây sẽ chỉ cho các bạn thấy cách chuyển 32 bit của địa chỉ IP thành một địa chỉ MAC

Để tham khảo, mình sẽ sử dụng biểu đồ sau đây để chuyển đổi mã thập lục phân thành nhị phân và ngược lại:

DECIMAL	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
HEX	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
BINARY	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111

Hãy bắt đầu bằng cách sử dụng địa chỉ MAC đưa ra trong sách: **01:00:5e:0a:00:01**

1. ***Chuyển đổi địa chỉ MAC hệ thập lục phân 01:00:5e:0a:00:01 để nhị phân***

0000 0001:0000 0000:0101 1110:0000 1010:0000 0000:0000 001

01	00	5E	0A	00	01
0000 0001	0000 0000	0101 1110	0000 1010	0000 0000	0000 0001

2. ***Cô lập dãy 23 bit bậc thấp của hệ nhị phân từ địa chỉ MAC đã chuyển đổi:***

0000 0001 : 0000 0000 : 0101 1110 : 0000 1010 : 0000 0000 : 0000 0001

3. ***Lấy dãy 23 bit từ bước 2 và gán nó vào dãy 23 bit của địa chỉ IP (làm điều này trong hệ nhị phân):***

1110 *xxxx* : *x*000 1010 : 0000 0000 : 0000 0000

+ **1110 –** Dãy 4 bit bậc cao của địa chỉ IP cho không gian địa chỉ multicast (224.xxx).

+ **xxxx x -** 5 bit còn lại sau khi 23 bit của địa chỉ IP được ánh xạ tới địa chỉ MAC cộng với dãy 4 bit bậc cao (1110). tổng cộng 32 địa chỉ IP.

4. ***Chuyển đổi dãy nhị phân của địa chỉ IP về hệ thập phân, thay thế các biến x với tất cả các giá trị để có được tất cả 32 địa chỉ IP có thể:***

- **1110***0000* : *0*000 1010 : 0000 0000 : 0000 0001= **224.10.0.1**
- **1110***0001* : *0*000 1010 : 0000 0000 : 0000 0001= **225.10.0.1**
- **1110***0010* : *0*000 1010 : 0000 0000 : 0000 0001= **226.10.0.1**
- **1110***0011* : *0*000 1010 : 0000 0000 : 0000 0001= **227.10.0.1**
- **1110***0100* : *0*000 1010 : 0000 0000 : 0000 0001= **228.10.0.1**
- **1110***0101* : *0*000 1010 : 0000 0000 : 0000 0001= **229.10.0.1**
- **1110***0110* : *0*000 1010 : 0000 0000 : 0000 0001= **230.10.0.1**
- **1110** *0111* : *0*000 1010 : 0000 0000 : 0000 0001= **231.10.0.1**
- **1110***1000* : *0*000 1010 : 0000 0000 : 0000 0001= **232.10.0.1**
- **1110***1001* : *0*000 1010 : 0000 0000 : 0000 0001= **233.10.0.1**
- **1110***1010* : *0*000 1010 : 0000 0000 : 0000 0001= **234.10.0.1**
- **1110***1011* : *0*000 1010 : 0000 0000 : 0000 0001= **235.10.0.1**
- **1110***1100* : *0*000 1010 : 0000 0000 : 0000 0001= **236.10.0.1**
- **1110***1101* : *0*000 1010 : 0000 0000 : 0000 0001= **237.10.0.1**
- **1110***1110* : *0*000 1010 : 0000 0000 : 0000 0001= **238.10.0.1**
- **1110***1111* : *0*000 1010 : 0000 0000 : 0000 0001= **239.10.0.1**
- **1110***0000* : *1*000 1010 : 0000 0000 : 0000 0001= **224.138.0.1**
- **1110***0001* : *1*000 1010 : 0000 0000 : 0000 0001= **225.138.0.1**
- **1110***0010* : *1*000 1010 : 0000 0000 : 0000 0001= **226.138.0.1**
- **1110***0011* : *1*000 1010 : 0000 0000 : 0000 0001= **227.138.0.1**
- **1110***0100* : *1*000 1010 : 0000 0000 : 0000 0001= **228.138.0.1**
- **1110***0101* : *1*000 1010 : 0000 0000 : 0000 0001= **229.138.0.1**
- **1110***0110* : *1*000 1010 : 0000 0000 : 0000 0001= **230.138.0.1**
- **1110***0111* : *1*000 1010 : 0000 0000 : 0000 0001= **231.138.0.1**
- **1110***1000* : *1*000 1010 : 0000 0000 : 0000 0001= **232.138.0.1**
- **1110***1001* : *1*000 1010 : 0000 0000 : 0000 0001= **233.138.0.1**
- **1110***1010* : *1*000 1010 : 0000 0000 : 0000 0001= **234.138.0.1**
- **1110***1011* : *1*000 1010 : 0000 0000 : 0000 0001= **235.138.0.1**
- **1110***1100* : *1*000 1010 : 0000 0000 : 0000 0001= **236.138.0.1**
- **1110***1101* : *1*000 1010 : 0000 0000 : 0000 0001= **237.138.0.1**
- **1110***1110* : *1*000 1010 : 0000 0000 : 0000 0001= **238.138.0.1**
- **1110***1111* : *1*000 1010 : 0000 0000 : 0000 0001= **239.138.0.1**

5. ***Tất cả 32 địa chỉ IP ở bước 4 được ánh xạ thành địa chỉ MAC: 01:00:5e:0a:00:01.***

(*)Chuyển đổi địa chỉ MAC Multicast thành địa chỉ IP Multicast

Tương đương, một địa chỉ IP multicast có thể được chuyển đổi sang địa chỉ MAC. Một khi bạn đã tìm ra cách để chuyển đổi địa chỉ MAC ở layer 2 thành địa chỉ IP ở layer 3, thực hiện nó rất dễ dàng.

Để bắt đầu, chúng ta có thể chọn bất kỳ địa chỉ từ 32 địa chỉ IP mà mình đã chuyển đổi ở trên. Hãy chọn một địa chỉ ngẫu nhiên như **227.138.0.1**

- Đầu tiên chuyển đổi địa chỉ 227.138.0.1 thành nhị phân:

+11100011: 10001010: 00000000: 00000001

+Chúng ta chỉ quan tâm đến phần màu đỏ đại diện cho 23 bits bậc thấp của địa chỉ IP.

+Chú ý rằng chúng ta bỏ bit bậc cao của octet thứ hai.

- Chuyển đổi dãy 23 bit về hệ thập lục phân: **0A:00:01**
- Chúng ta đã biết rằng 3-byte đầu tiên (24 bit) của địa chỉ MAC là **01:00:5E**. Điều này đã được nói ở phần trên. Đơn giản chỉ cần thêm kết quả bước 2 đến 3 byte đầu tiên và bạn có địa chỉ MAC: **01:00:5E:0A:00:01**

+Các bạn có thể chọn bất kỳ trong số 32 địa chỉ IP có trong danh sách ở trên và bạn sẽ luôn có được địa chỉ MAC là **01:00:5E:0A:00:01** nếu làm theo các bước ở trên.

Tóm tắt

- Octet 1 - Chú ý rằng octet đầu tiên luôn đứng một mình.
- Octet 2 - Bạn chỉ cần chuyển đổi 7 bit cuối thành hệ thập lục phân. Octet thứ hai trong hệ thập phân là **138**. Nhưng nếu bạn lượt bỏ bit cao nhất, nó sẽ trở thành một số thập phân **10** hoặc số thập lục phân **0A**.
- Octet thứ 3 - Chuyển đổi trực tiếp cho thành hệ thập lục phân.
- Octet thứ 4 - Chuyển đổi trực tiếp cho thành hệ thập lục phân.

Người biên soạn: Phan Thanh Phong

Liên kết tham khảo:
http://routemyworld.com/2009/03/04/ip-multicast-to-mac-address-mapping/

Thiết lập lệnh tắt "alias command" trên thiết bị Cisco

Chúng ta liên tục sử dụng các câu lệnh như ***show ip interface brief, copy run start, configure terminal, show running-config***.....Để tiết kiệm thời gian và sự lặp lại của lệnh nhập nhiều lần, bạn có thể sử dụng những lệnh gõ tắt. Cisco IOS cho phép bạn cấu hình một lệnh tắt hoặc một lệnh phức tạp. Một lệnh tắt có thể được cấu hình để làm bất cứ điều gì có thể trên một dòng lệnh, nhưng lệnh gõ tắt không thể di chuyển giữa các chế độ, gõ mật khẩu, hoặc thực hiện bất kỳ chức năng tương tác.

Dưới đây Bảng chứa lệnh tắt cho lệnh gốc Cisco.

h	help
lo	Logout
p	ping
s	show
U or un	undebug
w	where

Sử dụng lệnh ***show aliases*** trên Cisco Router để show ra bảng:

```
Cisco-Router#sh aliases
Exec mode aliases:
h                    help
lo                   logout
p                    ping
r                    resume
s                    show
u                    undebug
un                   undebug
w                    where
Cisco-Router#
```

Các lệnh gõ tắt được cấu mình ở chế độ modes exec: Privilege #, global configuration: (config)#, interface configuration: (config-if)#, router configuration: (config-router)#. Bạn có thể thực hiện lệnh ***show aliases ?*** để xem có bao nhiêu chế độ đang có

```
Cisco-Router#sh alias ?
Buffer                          config-owner-buffer
RITE-profile                    Router IP traffic export profile
command mode
RMI-Node-Config                 Resource Policy Node Config mode
RMI-Resource-Group              Resource Group Config mode
RMI-Resource-Manager            Resource Manager Config mode
RMI-Resource-Policy             Resource Policy Config mode
SASL-profile                    SASL profile configuration mode
aaa-attr-list                   AAA attribute list config mode
aaa-user                        AAA user definition
accept-dialin                   VPDN group accept dialin
configuration mode
accept-dialout                  VPDN group accept dialout
configuration mode
acct_mlist                      AAA accounting methodlist
definitions
address-family                  Address Family configuration mode
aic                             Alarm Interface Card
configuration mode
appfw-application-aim           Appfw for AIM Configuration Mode
appfw-application-msnmsgr       Appfw for MSN Messenger
Configuration Mode
appfw-application-ymsgr         Appfw for Yahoo! Messenger
Configuration Mode
appfw-policy                    Application FW Policy
Configuration Mode
application-http                Appfw for HTTP Configuration Mode
archive                         Archive the router configuration
mode
.........     output removed
config                          Global Configuration mode
.........     output removed
exec                            Exec mode
.........     output  removed
```

Câu lệnh để thực hiện chức năng gõ tắt ở global configuration mode là ***alias mode <command-alias> <original-command>***

Cisco-Router(config)# ***alias exec prt partition—privileged EXEC mode***
Cisco-Router(config)# ***alias configure sb source-bridge—global configuration mode***
Cisco-Router(config)# ***alias interface rl rate-limit—interface configuration mode***
Cisco-Router(config)# ***alias exec scn show cdp neighbor – Privileged Exec Mode***
Cisco-Router(config)# ***alias interface ns no shutdown***

Nếu các bạn thực hiện lệnh gõ tắt ở 'interface mode' và 'privileged mode' thì sử dụng lệnh:

Cisco-Router(config)# ***alias configure sir do show ip route***
Cisco-Router(config)# ***alias interface sir do show ip route***

Để xem các lệnh tắt do mặc định hoặc do người dung tạo ra, sử dụng lệnh ***show alias command***.

Người biên soạn: Phan Thanh Phong.

Liên kết tham khảo:

http://www.ciscoconsole.com/wan/cisco-general/how-to-configure-cisco-alias-commands-on-cisco-router.html/

Quá trình khởi động mặc định của router cisco

Router Cisco có thể khởi động IOS từ các nơi sau đây:

- Flash memory.
- TFTP server.
- ROM (một số IOS không hỗ trợ).

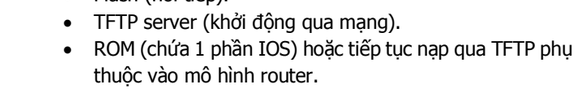
Quá trình khởi động mạc định của Router để xác định các IOS:

- NVRAM.
- Flash (nối tiếp).
- TFTP server (khởi động qua mạng).
- ROM (chứa 1 phần IOS).

Lưu ý: các lệnh hệ thống khởi động của Cisco có thể được sử dụng để xác định nguồn IOS chính và IOS dự phòng.

Toàn bộ quán trình khởi động Router của Cisco và định vị các IOS Cisco:

1. POST (Power On Self Test) và mã Bootstrap được thực hiện:



POST là một quá trình được sử dụng để kiểm tra phần cứng Router. Sau khi POST được chạy, chương trình bootstrap sẽ được nạp.

2. Xác định vị trí phần mềm Cisco IOS và tải nó vào bộ nhớ RAM của Router.

Các chương trình bootstrap xác định vị trí của Cisco IOS và tải nó vào bộ nhớ RAM. Các tập tin Cisco IOS có thể được đặt tại một trong ba địa điểm: bộ nhớ flash, TFTP server, hoặc một vị trí khác được chỉ ra trong tập tin cấu hình khởi động. Theo mặc định, Cisco IOS được tải lên từ bộ nhớ flash. Các thiết lập cấu hình phải được thay đổi để tải IOS từ một trong những nơi khác.

I. Kiểm tra giá trị cấu hình Configuration Register (NVRAM) mà nó có thể được sửa đổi bằng cách sử dụng lệnh **config- register** từ chế độ **Global mode** trên Router của Cisco.

0 = chế độ ROM Monitor.
1 = ROM IOS.
2-15 = startup-config trong NVRAM.

II. Kiểm tra tập tin Startup-config cho các lệnh khởi động hệ thống (NVRAM).

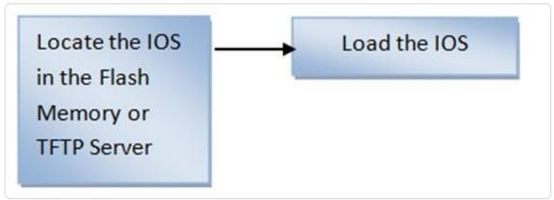
a) Nếu hệ thống khởi động lệnh trong ***startup-config***

Hệ thống khởi động chạy lệnh theo thứ tự mà chúng xuất hiện trong startup-config để xác định vị trí IOS

[Nếu lệnh hệ thống khởi động không thành công, quá trình khởi động mặc định sẽ xác định vị trí IOS ở đâu? (Flash, TFTP, ROM)]

b) Nếu không có lệnh khởi động hệ thống trong ***startup-config***, nó sẽ sử dụng các trình tự khởi động mặc định trong việc xác định vị trí các IOS Cisco:

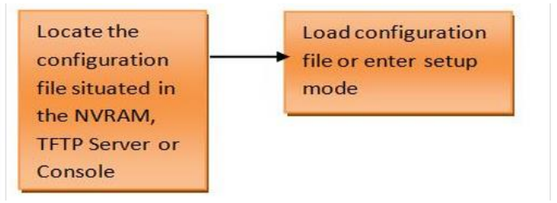
- Flash (nối tiếp).
- TFTP server (khởi động qua mạng).
- ROM (chứa 1 phần IOS) hoặc tiếp tục nạp qua TFTP phụ thuộc vào mô hình router.



Lưu ý: Nếu Cisco IOS không được xác định hoặc bị gián đoạn từ lệnh khởi động hệ thống và trình tự khởi động mặc định, Router sẽ nhập vào chế độ màn hình ROM hoặc chế độ rommon.

3. Xác định vị trí và thực hiện các tập tin cấu hình khởi động.

Nếu IOS được nạp, chương trình bootstrap tìm kiếm các tập tin cấu hình khởi động trong NVRAM. Tập tin này chứa các lệnh cấu hình đã lưu trước đó và các thông số, bao gồm cả địa chỉ các cổng, thông tin định tuyến, mật khẩu và các thông số cấu hình khác. Nếu tập tin cấu hình khởi động nằm trong NVRAM, nó sẽ tải vào bộ nhớ RAM khi chạy cấu hình.



Nếu không có tập tin ***startup-config***, Router Cisco sẽ sử dụng dự phòng mặc định hoặc chế độ tự khởi động để xác định tập tin ***startup-config*** và sau đó nó sẽ vào chế độ setup mode hoặc setup dialogue.

- NVRAM
- TFTP server
- Setup Mode

Các lệnh khởi động hệ thống của Cisco:

Cisco-Router(config)# boot system flash IOS filename - khởi động từ bộ nhớ FLASH.

Cisco-Router(config)# boot system tftp IOS filename tftp server ip address - khởi động từ một máy chủ TFTP server

Cisco-Router(config)# boot system rom - khởi động từ hệ thống ROM.

Câu lệnh cấu hình Configuration Register trên Router của Cisco:

Cisco-Router(config)# config-register 0x10x (chữ x cuối cùng thường là 0-F trong hệ thập lục phân).

Khi chữ x cuối cùng thường là:

0 = khởi động vào chế độ ROM Monitor

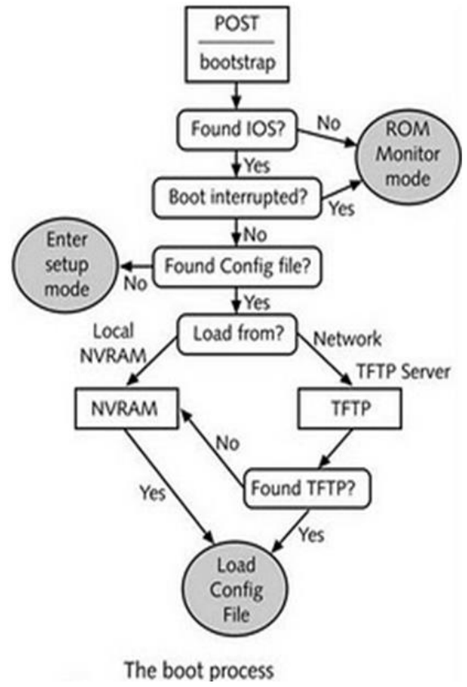
1 = khởi động ROM IOS

2-15 = dựa vào tập tin cấu hình ***startup-config*** trong NVRAM.

Bảng dưới đây mô tả các thao tác tiến trình khởi động Router với giá trị Configuration register và các lệnh khởi động hệ thống:

Giá trị Boot	***Chức năng***
0x0	Vào chế độ rommon và bỏ qua các lệnh khởi động hệ thống
0x1	Nạp IOS từ ROM và bỏ qua các lệnh khởi động hệ thống. Điều còn được gọi là chế độ RXBoot mode.
0x2-0xF	Nếu sử dụng lệnh không khởi động cấu hình, đầu tiên các tập tin IOS trong Flashmemory được tải; nếu thất bại, router sẽ tìm kiếm một IOS trên máy chủ TFTP. Nếu thất bại, IOS từ ROM được nạp.
0x2-0xF	Nếu sử dụng với lệnh khởi động hệ thống ROM, IOS từ ROM sẽ được nạp.
0x2-0xF	Nếu sử dụng với lệnh khởi động hệ thống từ Flash, tập tin đầu tiên trong Bộ nhớ flash sẽ được tải.
0x2-0xF	Nếu sử dụng lệnh khởi động hệ thống flash file_name, IOS với file_name quy định được nạp từ bộ nhớ Flash.
0x2-0xF	Nếu sử dụng lệnh khởi động hệ thống tftp file_name 10.1.1.1, IOS với file_name quy định được tải từ máy chủ TFTP server.
0x2-0xF	Nếu sử dụng nhiều lệnh khởi động hệ thống, một quá trình xảy ra để tải IOS dựa trên lệnh khởi động đầu tiên trong cấu hình. Nếu thất bại, lệnh khởi động thứ hai được sử dụng, vv., Cho đến khi một IOS được nạp thành công.

Biểu đồ Trình tự khởi động của Router:



The boot process

Người biên soạn: Phan Thanh Phong.

Website: http://vnpro.vn; **Forum**: http://vnpro.org; **Network channel:** http://www.dancisco.com