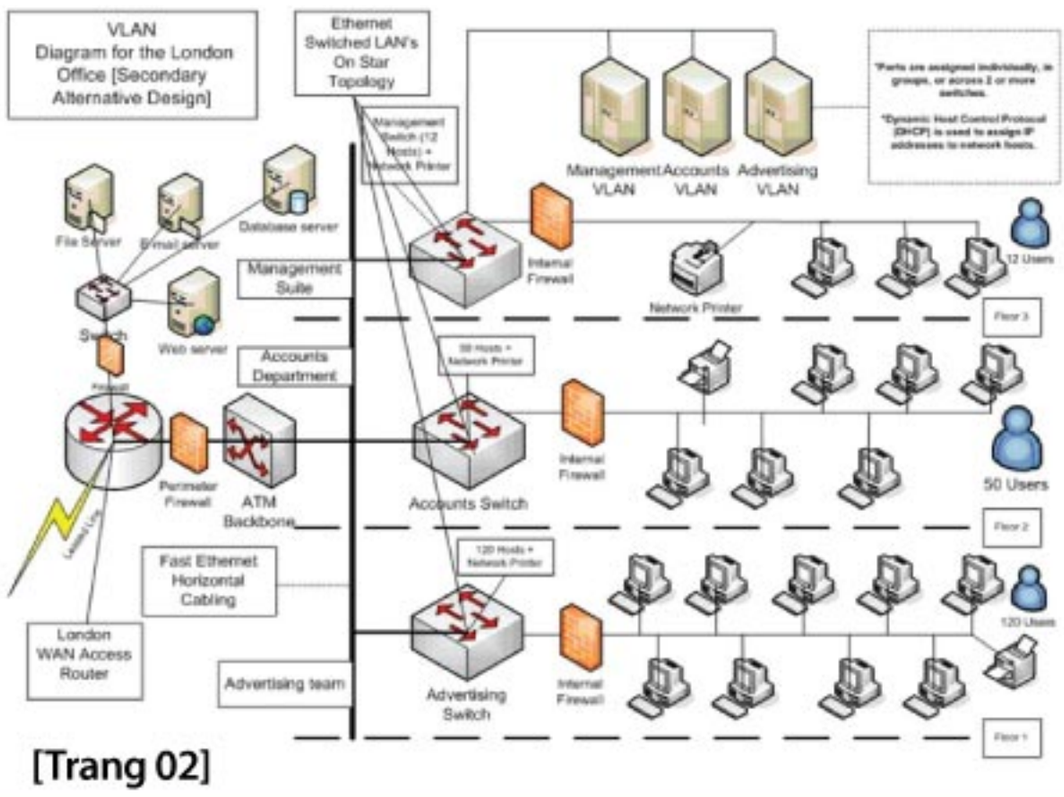
Số 33
11/2014

BẢN TIN dancisco

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

Ứng cử viên có chứng chỉ CCNA có thể làm được những gì?



[Trang 02]

ƯU ĐÃI THÁNG 11

- Tặng ngay áo thun VnPro cực chất
- Tặng bộ sách LabPro cực hay
- Ưu đãi đặc biệt khác: xem thêm tại www.vnpro.vn/khai-giang

MỚI CCNP version 2

Nguyễn Trương Thế Anh

HỌC VIÊN TIÊU BIỂU

Thế Anh vừa thi đậu CCNA Routing& Switching Quốc Tế với số điểm gần như tuyệt đối...

[Trang 07]

Bảo vệ hạ tầng mạng với công nghệ Storm control

Cisco Catalyst switch cung cấp một tính năng khá thú vị là "storm control," cho phép người quản trị giới hạn lưu lượng inbound unicast, multicast, hoặc broadcast traffic ở mức độ cổng giao tiếp layer 2 interface. Tính năng này có thể được sử dụng để .....

[Trang 03]

9 kỹ năng "mềm" quyết định 75% sự thành đạt

[Trang 11]

TIN TỨC SỰ KIỆN KHÁC

10 phần mềm tốt nhất giúp giám sát hạ tầng mạng

Giao diện chương trình Cacti

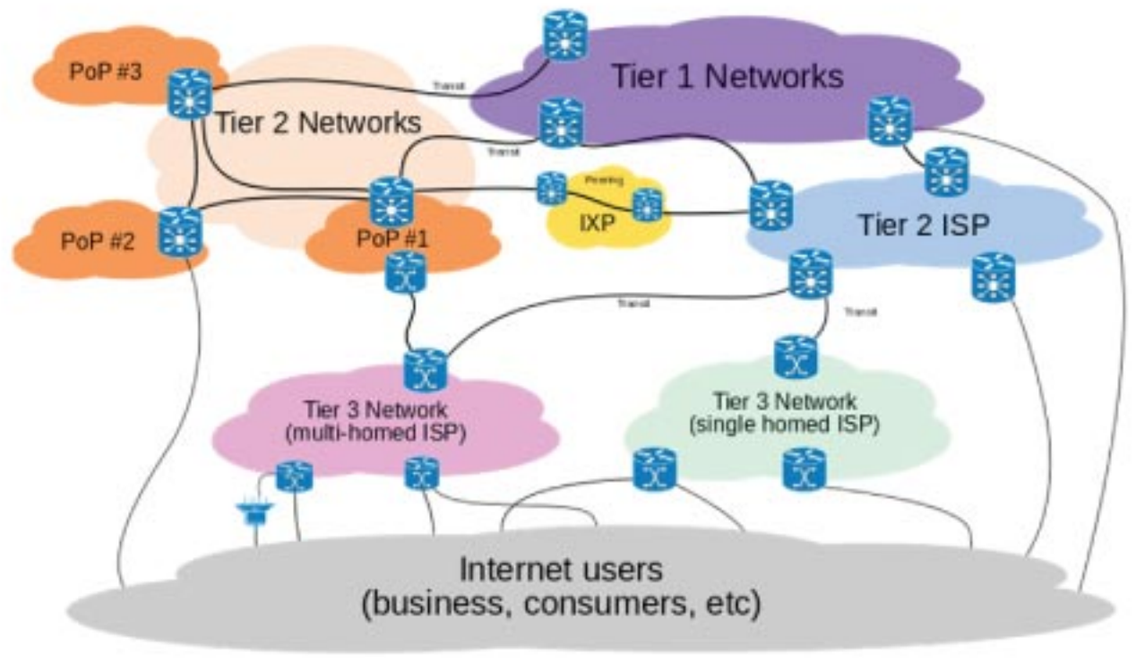
Tại một vị trí tập trung, chúng ta có thể sử dụng một số công cụ để giám sát tất cả các thiết bị mạng cũng như các dịch vụ chẳng hạn như cổng giao tiếp của thiết bị rơi vào trạng thái "down" hoặc mức độ sử dụng dịch vụ quá cao. Sau đây là danh sách các phần mềm cho phép người quả trị có thể giám sát hạ tầng mạng của mình:

- Cacti
- PRTG Network Monitor
- Nagios
- Orion Network Performance Monitor
- Colasoft packet graphing
- Munin
- Zenoss
- Zabbix
- Collectd
- Observium
- Argus
- Ganglia
- Monit
- Splunk
- LogicMonitor

Trong số các chương trình trên, chương trình giám sát hạ tầng mạng Cacti với phiên bản chạy trên nền Linux cho phép doanh nghiệp tiết kiệm khá nhiều chi phí về bản quyền.

Số lượng route trong bảng Internet routing table

Bắt đầu từ năm 1990, số lượng route trong bảng Internet routing table bắt đầu tăng đều. Năm 2008, số lượng route tăng lên 256k route (256 000 route). Cho tới thời điểm này thì số lượng route đã vượt qua ngưỡng 500,000 route, và chuẩn bị đạt mốc 512k. Cisco cung cấp một số dòng thiết bị có thể chứa tới 512k route:



- Cisco Catalyst 6500 Switch
- Cisco 7600 Series Router
- Cisco ASR 9000 Series Aggregation Services Router được trang bị Trident-based line cards
- Cisco ASR 1000 Series Aggregation Services Router trang bị 4GB RAM

Ứng dụng IoE trong cộng đồng người Pháp

Với sự hỗ trợ của Cisco, một nhóm sinh viên công nghệ Handisco đã tận dụng công nghệ Internet of Everything (IoE) để giúp cho người khiếm thị tại Pháp có thể tự mình đi lại trong khu vực thành phố mà không cần người giúp đỡ. Tất cả các thiết bị trong hạ tầng của thành phố đều được trang bị các cảm biến. Với một thiết bị có tên là "smart stick" được kết nối với cơ sở dữ liệu IoE sẽ cung cấp cho người khiếm thị các thông tin từ các bộ cảm biến từ hệ thống chiếu sáng giao thông, vị trí trạm xe buýt, hành lang hai bên đường, các điểm sang đường và thậm chí là tình trạng thời tiết theo thời gian thực. Các cảm biến từ các cửa hàng cũng cung cấp cho người khiếm thị vị trí của các của hàng dọc bên đường, vị trí các đồn cảnh sát trong trường hợp khẩn cấp.

Người biên soạn: Bùi Quốc Kỳ

Ứng cử viên có chứng chỉ CCNA có thể làm được những gì?

CCNA là một trong chứng chỉ của Cisco có uy tín trên thế giới. Ứng cử viên có chứng chỉ CCNA có thể tham gia thiết kế, triển khai hạ tầng mạng doanh nghiệp có tính chất hiện đại bắt kịp với xu hướng thế giới, đảm bảo được yếu tố bảo mật và độ tin cậy cao.

Cisco có 4 xu hướng đào tạo sau đây:

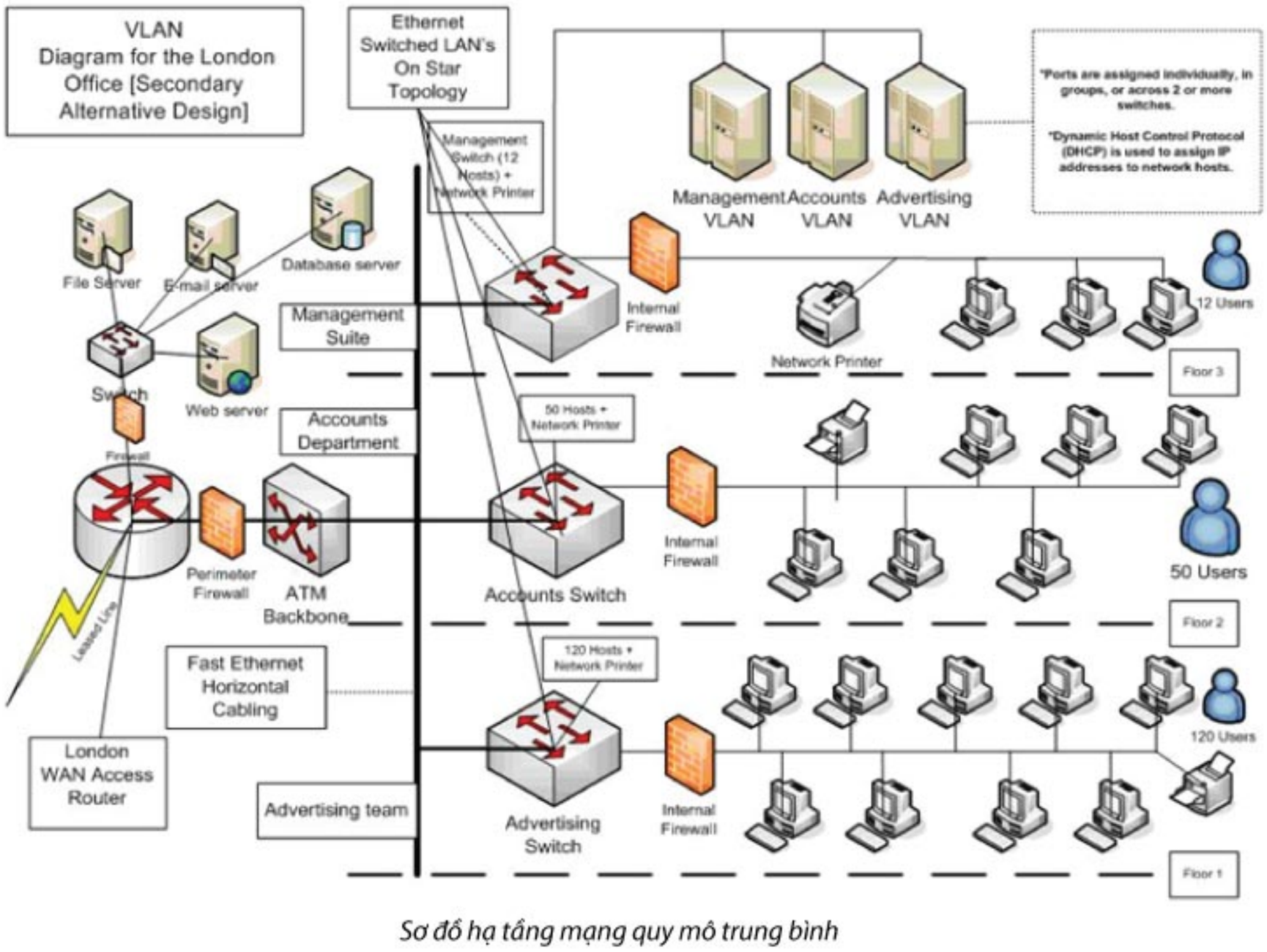
- Networking, Network Design, and Security
- Voice and Collaboration Solutions
- Data Center and Storage Networking
- Service Provider

Trong đó, CCNA thuộc nhóm "Networking, Network Design, and Security", trong nhóm này, ta có thể theo học một trong 4 mảng lĩnh vực cụ thể sau:

- Design
- Routing & Switching
- Network Security
- Wireless

Chứng chỉ CCNA thuộc mảng đào tạo "Routing & Switching" sẽ tập trung phân tích các công nghệ định tuyến trên router và chuyển mạch của switch, đó là 2 công nghệ chủ đạo mà các thiết bị trên hạ tầng mạng hoạt động và với hạ tầng mạng này, các lưu lượng như thoại (voice), video, lưu lượng dữ liệu (data) thông thường cho đến lưu lượng mạng không dây wireless có thể trung chuyển đi. Các thiết bị switch sẽ hình thành nên các mạng "network", và router sẽ đứng ra để kết nối các mạng lại với nhau. Trong mảng lĩnh vực "Routing & Switching" lại chia thành 4 cấp độ khác nhau:

- Entry
- Associate
- Professional
- Expert



Sơ đồ hạ tầng mạng quy mô trung bình

Chứng chỉ CCNA nằm ở cấp độ "Associate" sẽ trang bị cho người học khả năng cài đặt, cấu hình, vận hành và khắc phục các sự cố phát sinh trên hạ tầng mạng quy vừa và nhỏ.

Logo chứng chỉ CCNA Routing & Switching

Theo đó, ứng cử viên có chứng chỉ CCNA có thể nâng cấp lên cấp độ "Professional" với chứng chỉ CCNP, ứng cử viên được công nhận là một chuyên gia trong lĩnh vực mạng (network) có khả năng đánh giá hiệu suất hoạt động của hệ thống cũng như có khả năng đưa ra các giải pháp nhằm tối ưu hóa hệ thống. Ứng cử viên có chứng chỉ CCNP có thể giữ một số vị trí quan trọng trong đội ngũ IT của doanh nghiệp như "Kỹ thuật viên hạ tầng mạng", "Kỹ sư hỗ trợ hạ tầng mạng", "Kỹ sư hạ tầng và hệ thống mạng".

Logo chứng chỉ CCNP Routing & Switching

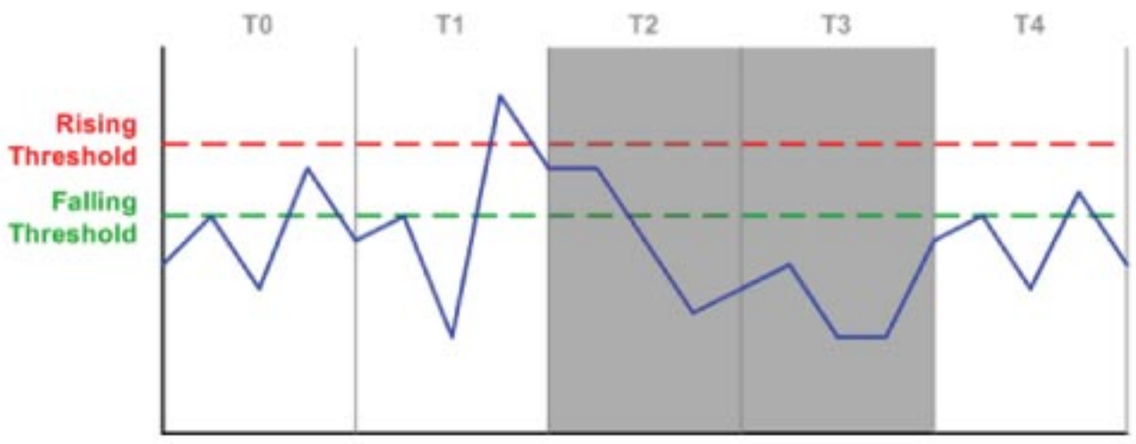
Hệ thống đào tạo theo chứng chỉ CCNP sẽ trang bị cho các ứng cử viên kỹ năng lên kế hoạch, triển khai, kiểm tra, giám sát và khắc phục sự cố trên hạ tầng mạng cục bộ và diện rộng, có khả năng phối hợp với các chuyên gia khác để triển khai hệ thống bảo mật, voice, wireless và giải pháp video.

Người biên soạn: Bùi Quốc Kỳ

Bảo vệ hạ tầng mạng với công nghệ Storm control

Cisco Catalyst switch cung cấp một tính năng khá thú vị là "storm control," cho phép người quản trị giới hạn lưu lượng inbound unicast, multicast, hoặc broadcast traffic ở mức độ cổng giao tiếp layer 2 interface. Tính năng này có thể được sử dụng để hạn chế tình trạng "broadcast storm" do cấu hình lỗi spanning tree, hoặc hạn chế tình trạng "unicast storm" do host NIC lỗi gây nên.

Ở chế độ cổng giao tiếp, maximum threshold có thể được cấu hình sử dụng đơn vị "bits per second" hoặc "packets per second", hoặc thậm chí là phần trăm (%) của interface bandwidth. Nếu "incoming traffic" của loại lưu lượng vượt ngưỡng threshold định trước trong suốt khoảng thời gian thăm dò "polling interval" (mặc định là 1 giây), lưu lượng traffic sẽ bị khóa cho đến khi "incoming rate" rơi xuống ngưỡng threshold trong khoảng thời gian "falling interval".



Trong khoảng thời gian interval T0, lưu lượng đi vào inbound traffic được chấp nhận vì chúng không vượt ngưỡng "rising threshold". Trong khoảng thời gian T1, "rising threshold" bị vi phạm và switch sẽ tiến hành khóa lưu lượng "incoming traffic" cho khoảng interval tiếp theo. Trong khoảng thời gian T2, traffic sẽ bị khóa lại, nhưng switch vẫn tiếp tục giám sát tốc độ đi vào incoming rate. Mặc dù tốc độ rơi xuống ngưỡng rising threshold, nhưng nó vẫn cao hơn ngưỡng "falling threshold", vì thế switch sẽ tiếp tục khóa lưu lượng trong khoảng interval tiếp theo.

Trong suốt khoảng thời gian T3, lưu lượng rơi xuống khoảng "falling interval", vì thế switch sẽ gỡ bỏ chính sách "blocking" lưu lượng trong khoảng thời gian T4. Mặc dù lưu lượng traffic trong khoảng thời gian T4 vượt ngưỡng "falling threshold" nhưng lúc này, lưu lượng không còn bị "blocked" nữa cho khoảng interval tiếp theo vì lưu lượng không vi phạm ngưỡng "rising threshold" nữa.

Để cấu hình tính năng "storm control", chúng ta sẽ chỉ định ra loại lưu lượng traffic type (unicast, multicast, hoặc broadcast) và ngưỡng "rising threshold" như sau:

```
Switch(config-if)# storm-control broadcast level bps 1m 500k
```

Trong ví dụ này, chúng ta sẽ tiến hành cấu hình tính năng "storm control" cho lưu lượng broadcast traffic với 1 Mbps là ngưỡng "rising threshold" và 500 Kbps cho ngưỡng "falling threshold". Trong đó, ngưỡng "falling threshold" là tùy chọn; tức là nếu "falling threshold" không được khai báo thì theo mặc định sẽ bằng giá trị của ngưỡng "rising threshold".

show storm-control giúp hiển thị các cổng giao tiếp interface đang cấu hình tính năng "storm control" và trạng thái của chúng:

```
Switch# show storm-control
Interface Filter State  Upper     Lower     Current
--------- ------------ ---------- ---------- ----------
Fa0/5     Forwarding    1m bps    500k bps   0 bps
```

Nếu ngưỡng upper (rising) threshold bị broadcast traffic vi phạm, ta sẽ quan sát được nội dung hiển thị như bên dưới:

```
Switch# show storm-control
Interface Filter State  Upper     Lower     Current
--------- ------------ ---------- ---------- ----------
Fa0/5     Blocking      1m bps    500k bps   2.08m bps
```

Thêm vào đó, switch sẽ phát sinh thông điệp "log message" để cảnh báo đến người quản trị về tình trạng "storm":

```
%STORM_CONTROL-3-FILTERED: A Broadcast storm
detected on Fa0/5. A packet filter action
has been applied on the interface.
```

Khi "incoming rate" rớt xuống ngưỡng lower (falling) threshold, cổng giao tiếp interface sẽ quay trở về trạng thái "forwarding":

```
Switch# show storm-control
Interface Filter State  Upper     Lower     Current
--------- ------------ ---------- ---------- ----------
Fa0/5     Forwarding    1m bps    500k bps   48.81k bps
```

Ta cũng có thể thực hiện câu lệnh storm-control action trap command ở chế độ interface configuration để gửi đi SNMP trap khi cổng giao tiếp vi phạm chính sách "storm control".

Người biên soạn: Bùi Quốc Kỳ

Phát sinh lưu lượng với tính năng Cisco IOS IP SLA

IP SLA thường được sử dụng để xây dựng các static route tin cậy. Tuy nhiên, chúng ta cũng có thể tận dụng công nghệ này để phát sinh lưu lượng (traffic generator).

Nếu cấu hình hợp lý, chúng ta có thể để IP SLA phát sinh chính xác số lượng packet và payload size, giúp chúng ta thiết lập giả định một luồng lưu lượng nhất định để kiểm tra cấu hình QoS.

Trước khi tiến hành cấu hình, chúng ta thử khảo sát một số công thức tính toán liên quan. Giả sử sử chúng ta muốn gửi đi 16 kbps lưu lượng traffic từ một router tới một router khác trên đường liên kết Ethernet thì số lượng packet chúng ta cần gửi và mức payload size tương ứng trong mỗi packet là bao nhiêu? Các header khác nhau sẽ có kích thước khác nhau:

Chẳng hạn như trong cấu trúc frame trên thì Ethernet header có 14 byte, IP có 20 byte và UDP có 8 byte.

Tính tổng kích thước frame size

Total frame size = L2 header + L3 header + L4 header + payload

Nếu router sử dụng môi trường Ethernet thì L2 header sẽ là 14 byte. IP add sẽ có header 20 byte và UDP header sẽ cần 8 byte. Trong tình huống này, ta sử dụng IP SLA để kiểm tra độ UDP jitter.

14 + 20 + 8 = 42 bytes.

Để giữ cho kết quả tính toán đơn giản, chúng ta sẽ sử dụng payload kích thước 58 byte để tổng kích thước total packet sẽ là 42 + 58 = 100 byte.

Tính toán Bandwidth

Bandwidth = frame size x number of packets

Chúng ta đã tính toán được kích thước frame size là 100 byte. Vì vậy, chúng ta chỉ cần tính toán số lượng packet sẽ được gửi đi trên mỗi giây là bao nhiêu gói mà thôi. Mục đích của chúng ta là phát sinh 16 kbps lưu lượng traffic tương ứng với 16.000 bits per second. Công thức tính toán được thực hiện như sau:

Number of packets = bandwidth / frame size

Trước khi thực hiện công thức tính toán trên, chúng ta cần đổi 16.000 bit sang đơn vị byte:

16.000 bit / 8 = 2000 byte.

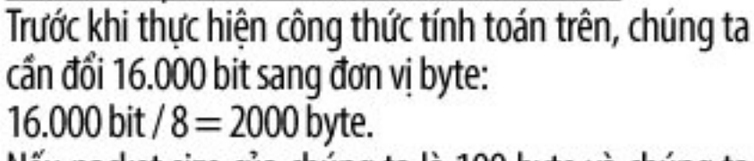
Nếu packet size của chúng ta là 100 byte và chúng ta cần gửi được 2000 bytes per second để đạt tốc độ 16 kbps:

2000 / 100 = 20

Vậy kết quả tính toán cuối cùng là chúng ta cần gửi 20 packets per second với frame size là 100 byte để đạt tốc độ 16 kbps!

Cấu hình

Để minh họa tính năng phát sinh lưu lượng IP SLA chúng ta sử dụng 2 router kết nối trực tiếp với nhau thông qua môi trường Ethernet:



Thực hiện cấu hình tại R1 như sau:

```
ip sla 1
 udp-jitter 192.168.12.2 17002 num-packets 20
 request-data-size 58
 threshold 500
 timeout 500
 frequency 1
ip sla schedule 1 life forever start-time now
```

Theo như kết quả tính toán thì chúng ta cần gửi 20 packets per second với payload size là 58 với destination port 17002.

Sau đây là một ví dụ khác để router phát sinh lưu lượng với bandwidth rate là 32 kbps:

```
ip sla 2
 udp-jitter 192.168.12.2 17002 num-packets 20
 request-data-size 158
 threshold 500
 timeout 500
 frequency 1
ip sla schedule 2 life forever start-time now
```

Tổng mức total frame size là 14 + 20 + 8 + 158 = 200 byte. Chúng ta nhân 200 với 20 packets per second sẽ đạt được tốc độ 4000 bytes per second. 4000 x 8 = 32.000 bps hoặc 32 kbps.

Tương tự như vậy, để phát sinh lưu lượng với tốc độ 64 kbps ta cấu hình như sau:

```
ip sla 3
 udp-jitter 192.168.12.2 17003 num-packets 20
 request-data-size 358
 threshold 500
 timeout 500
 frequency 1
ip sla schedule 3 life forever start-time now
```

Total frame size là 14 + 20 + 8 + 358 = 400 bytes. 400 x 20 = 8.000 bytes per second. 8.000 x 8 = 64.000 bps hoặc 64 kbps. Tương tự như vậy, để phát sinh lưu lượng với tốc độ 128 kbps, ta cấu hình như sau:

```
ip sla 4
 udp-jitter 192.168.12.2 17004 num-packets 20
 request-data-size 758
 threshold 500
 timeout 500
 frequency 1
ip sla schedule 4 life forever start-time now
```

Frame size là 14 + 20 + 8 + 758 = 800 bytes. 800 x 20 = 16.000 bytes per second. 16.000 x 8 = 128.000 bps hoặc 128 kbps.

R1 giờ đây phát sinh các luồng lưu lượng với băng thông tương ứng là 16, 32 ,64 và 128 kbps stream. Tại phía R2, chúng ta tiến hành kiểm tra kết quả vừa triển khai.

Kiểm tra

Một trong những cách thức giúp chúng ta kiểm tra mức incoming bandwidth rate là sử dụng ứng dụng policy-map. Chúng ta sẽ cấu hình access-list tương ứng với mỗi mức bandwidth rate so khớp vơsi định danh port number mà chúng ta sử dụng trong mỗi IP SLA instance. Mỗi access-list liên kết tới class-map trong policy-map không có bất kỳ action nào:

```
ip access-list extended IP_SLA_1
 permit udp any host 192.168.12.2 eq 17001
ip access-list extended IP_SLA_2
 permit udp any host 192.168.12.2 eq 17002
ip access-list extended IP_SLA_3
 permit udp any host 192.168.12.2 eq 17003
ip access-list extended IP_SLA_4
 permit udp any host 192.168.12.2 eq 17004
class-map match-all IP_SLA_1
 match access-group name IP_SLA_1
class-map match-all IP_SLA_2
 match access-group name IP_SLA_2
class-map match-all IP_SLA_3
 match access-group name IP_SLA_3
class-map match-all IP_SLA_4
 match access-group name IP_SLA_4
policy-map TRAFFIC_METER
 class IP_SLA_1
 class IP_SLA_2
 class IP_SLA_3
 class IP_SLA_4
```

Sau đó, ta tiến hành liên kết policy-map lên interface:

```
R2(config)#interface fastEthernet 0/0
R2(config-if)#service-policy input TRAFFIC_METER
R2(config-if)#load-interval 30
```

Câu lệnh load-interval command để chỉ cho router tiến hành cập nhật interface statistic cứ mỗi 30 giây. Giá trị mặc định là 60 giây.

```
R2#show policy-map interface fastEthernet 0/0
 FastEthernet0/0

  Service-policy input: TRAFFIC_METER

    Class-map: IP_SLA_1 (match-all)
      60066 packets, 6006600 bytes
      30 second offered rate 16000 bps
      Match: access-group name IP_SLA_1

    Class-map: IP_SLA_2 (match-all)
      60060 packets, 12012000 bytes
      30 second offered rate 32000 bps
      Match: access-group name IP_SLA_2

    Class-map: IP_SLA_3 (match-all)
      60060 packets, 24024000 bytes
      30 second offered rate 64000 bps
      Match: access-group name IP_SLA_3

    Class-map: IP_SLA_4 (match-all)
      60060 packets, 48048000 bytes
      30 second offered rate 128000 bps
      Match: access-group name IP_SLA_4

    Class-map: class-default (match-any)
      12013 packets, 1129222 bytes
      30 second offered rate 3000 bps, drop rate 0 bps
      Match: any
```

Chúng ta có thể quan sát thấy lưu lượng thống kê được tương ứng với các tốc độ lần lượt 16, 32, 64 và 128 kbps và kết quả được thống kê cứ mỗi 30 giây!

Routing & Switching

Chương trình CCNA R&S

Chương trình CCNP ROUTE

Chương trình CCNP SWITCH

Chương trình CCNP TSHOOT

Chương trình CCIE

Security

Chương trình CCNA Security

Chương trình SECURE

Chương trình FIREWALL

ƯU ĐÃI THÁNG 11

- *Tặng ngay áo thun VnPro cực chất*
- *Tặng bộ sách LabPro cực hay*
- *Ưu đãi đặc biệt khác: xem thêm tại www.vnpro.vn/khai-giang*

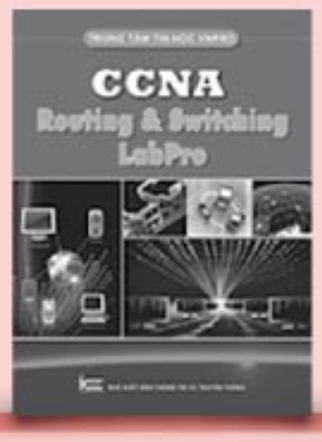
** Áp dụng các lớp buổi tối*

Cam kết lợi ích khi học tại VnPro

- *Vắng học được học bù, không hiểu bài được học lại miễn phí.*
- *Giáo trình giảng dạy chuẩn quốc tế và LabPro tiếng Việt.*
- *Thực hành >70% thời lượng chương trình và trực tiếp 100% trên thiết bị chính hãng, hiện đại. (>100 giờ lab)*
- *Được thực hành miễn phí ngoài giờ.*
- *Chứng chỉ VnPro được công nhận trên toàn quốc.*
- *Thi đậu quốc tế sau khi hoàn tất khóa học.*

Là trung tâm duy nhất trong cả nước phát hành hơn 20 quyển sách mạng LabPro tiếng Việt. Giáo trình VnPro được cập nhật, nâng cấp thường xuyên theo chuẩn giáo trình quốc tế

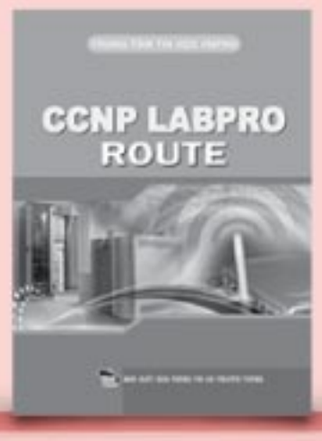
GIẢM* NGAY 10%



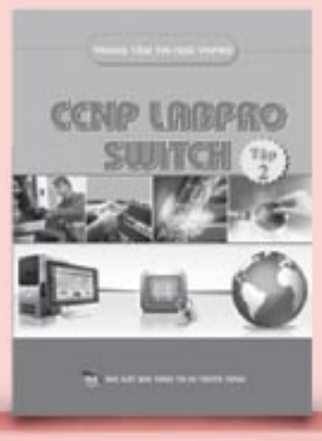
CCNA Routing & Switching
Giá: 220.000 VNĐ

CCDA
Giá: 250.000 VNĐ

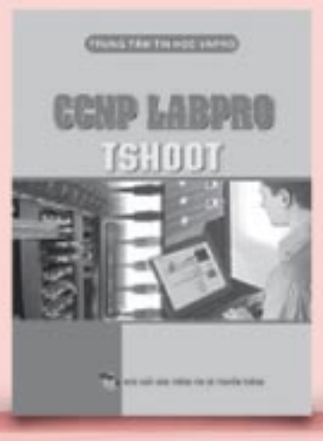
Ôn thi CCNA trong 24h
Giá: 120.000 VNĐ



CCNP LABPRO ROUTE
Giá: 120.000 VNĐ



CCNP LABPRO SWITCH
Giá: 120.000 VNĐ



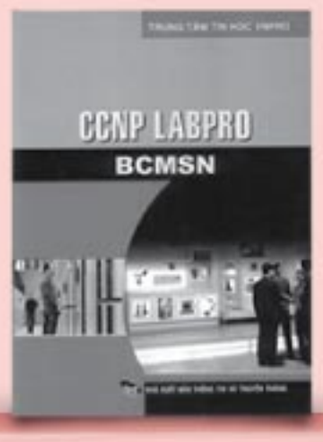
CCNP LABPRO TSHOOT
Giá: 120.000 VNĐ

Ôn thi Route
Giá: 90.000 VNĐ

Ôn thi Switch
Giá: 100.000 VNĐ

Ôn thi Tshoot
Giá: 80.000 VNĐ

CCNP LABPRO BSCI
Giá: 95.000 VNĐ



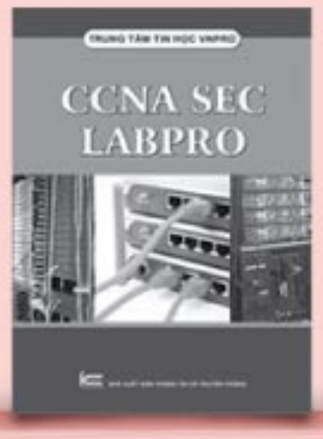
CCNP LABPRO BCMSN
Giá: 70.000 VNĐ

CCNP LABPRO ISCW
Giá: 120.000 VNĐ

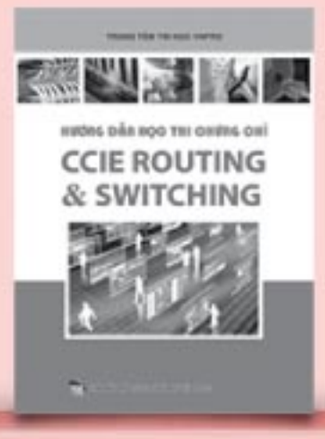
CCSP LABPRO SNAF & SNAA
Giá: 120.000 VNĐ

CCSP LABPRO IPS & CSMARS
Giá: 90.000 VNĐ

CCSP LABPRO SNRS
Giá: 140.000 VNĐ



CCNA SEC LABPRO
Giá: 150.000 VNĐ



CCIE R&S
Giá: 150.000 VNĐ

CWNA
Giá: 90.000 VNĐ

* Khi mua sách LabPro online. Link mua sách online: ***http://www.vnpro.vn/sach-labpro/***

Nguyễn Trương Thế Anh

HỌC VIÊN TIÊU BIỂU

1. Xin chúc mừng Thế Anh vừa thi đậu CCNA Routing& Switching Quốc Tế với số điểm gần như tuyệt đối. Thế Anh có thể chia sẻ một chút về mình được không?

Em tên là Nguyễn Trương Thế Anh, Em đang là sinh viên năm cuối khoa CNTT trường ĐH Khoc Học Tự Nhiên TP.HCM. Khi em bước vào môi trường đại học, ở khoa CNTT có khá nhiều ngành như công nghệ phần mềm, hệ thống thông tin… nhưng em chọn ngành mạng máy tính, em đã xác định con đường của mình là phải đi với từ là "mạng". Ước mơ của em là trở thành một IT Manager quản trị hệ thống mạng của 1 tập đoàn lớn. Trong quá trình học ở đại học em cũng tìm hiểu và cũng tham khảo ý kiến của những đàn anh/chị đi trước, những thầy cô trong trường, rùi em quyết định tham gia những khóa học về chuyên ngàng mạng, em quyết định học chứng chỉ mạng CCNA của Cisco vì nó bổ trợ cho công việc của em sau này rất nhiều.

Nguyễn Trương Thế Anh và thầy Phan Hoàng Gia Liêm – Giảng viên VnPro

2. Thế Anh cảm nhận môi trường học tại VnPro thế nào?

Trước khi trở thành học viên của VnPro, em cũng tìm hiểu thông tin trên mạng, rồi các đàn anh đi trước. Em cũng hiểu rằng dù học ở đâu cũng vậy miễn mình học tốt, chăm chỉ là sẽ tốt hết. Và em quyết định chọn VnPro với nhiều lý do khác nhau (như VnPro được những anh chị học trước đánh giá rất cao về chuyên môn, phong cách giảng dạy và cơ sở vật chất thiết bị đều rất ổn và tốt…và cũng thuận tiện cho việc đi lại của em). Sau 4 tháng học ở VnPro với em là một trãi nghiệm tuyệt diệu, và em cảm nhận rất rõ ràng những lời anh chị từng học ở đây nói là chính xác và em cảm thấy quyết định của em là cực kỳ đúng đắn. Ở đây em không chỉ được các thầy dạy về chuyên môn mà còn được học những kĩ năng mềm, những kĩ năng trong cuộc sống, được làm quen và tiếp xúc với những thiết bị thật như Router, Switch và được triển khai những dịch vụ, học được những giao thức và đặc biệt là được làm những bài lab thực tế với bên ngoài với những thiết bị thật em thấy thích thú vô cùng. Ngoài ra em rất ấn tượng với bộ phân tư vấn, các chị rất vui vẻ và thân thiện, khi gặp vấn đề gì về khóa học hay muốn tham gia những sự kiên do VnPro tổ chức các chị đều hổ trợ hết mình, các chị luôn cập nhật những tin tức cũng như những sự kiện sắp diễn ra tại VnPro cho em và các bạn như ngày hội việc làm, tham gia lớp ôn thi quốc tế, tham gia các lớp phát triển mạng doanh nghiệp. v. v…Tóm lại theo quan điểm của riêng em, VnPro là một môi trường đào tạo rất chuyên nghiệp.

3. Học thi CCNA quốc tế có quá khó hay không? Có kinh nghiệm gì Thế Anh có thể chia sẻ cho các bạn đi sau?

Theo em nghĩ mỗi người mỗi cảm nhận. Nhưng với quan điểm của riêng em, em nghĩ nếu bản thân mình xác định rõ ràng trong tư tưởng là thật sự muốn chinh phục chứng chỉ quốc tế cisco CCNA, vì nghĩ nó cần cho tương lai của mình và thật sự có đam mê và quyết tâm thì em nghĩ cũng không quá khó. Còn về kinh nghiệm, thật sự ra em cũng không có kinh nghiệm gì quá to tát cả. Nhưng ở đây em cũng muốn chia sẽ 1 số điều mà em đã trải qua cho các bạn có ý định thi quốc tế. Đầu tiên đó là tài chính, 1 chi phí không hề nhỏ, nhưng đã gói hành trang thì không suy nghĩ tới nữa, cố gắng đừng nghĩ nhiều thứ khiến cho mình áp lực mà thay vào đó là lên một thời gian biểu phù hợp để ôn và có những phương pháp ôn cụ thể, ví dụ như trong bộ đề sẽ có những câu lý thuyết và các câu sim(câu mà bạn sẽ cấu hình trực tiếp trên đề thi, SIM là câu rất quan trọng vì hệ số điểm rất cao, bạn vào trang http://www. ccnalearn. cf/simulation. html để ôn những câu sim) có thể sáng bạn ôn lý thuyết, chiều bạn ôn SIM, tối bạn ôn cả 2 chẳng hạn. Một bộ đề có từ khoảng 60 câu trở lại và thời gian là 120 phút. Các bạn nhớ rằng khi chọn câu trả lời phải suy nghĩ thật kỹ và nhanh chóng chọn nó vì nếu các bạn lỡ chọn sai đáp án mình mong muốn thì các bạn sẽ không có cơ hội quay lại để sửa vì người ta chỉ cho các bạn 1 nút next thôi. Vì vậy các bạn phải hết sức cẩn thận trong việc chọn câu trả lời.

4. Lời khuyên, chia sẻ kinh nghiệm của Thế Anh cho những bạn muốn học tốt, giỏi hệ thống mạng là gì?

Thật ra nếu các bạn muôn học tốt và giỏi hệ thống mạng thì một điều chắc chắn là các bạn phải có niềm đam mê thật sự với lĩnh vực ngành nghề mà các bạn đang chọn, các bạn phải thật sự thích và hứng thú với nó, muốn tìm hiểu và khám phá nó theo nhiều cách khác nhau. Trong quá trình học thì nên trao đổi những câu hỏi mình thắc mắc từ thầy cô, bạn bè trong lớp hoặc anh chị lớp trước. Vì kiến thức mạng là rất bao la, nếu các bạn không mạnh dạn hỏi thì các bạn sẽ không theo kịp và khi đó các bạn không hiểu vấn đề và bắt đầu các bạn có cảm giác "khó thở" và "chán" đi. Các bạn cũng nên tự học cách tự tìm hiểu, mày mò như đọc sách thêm hay làm lại những bài lab thầy cho trên lớp bằng những chường trình giả lập như Packet Tracer, GNS3 nhiều lần để mình hiểu sâu và nhớ lâu hơn ngoài ra chúng ta còn có thể tìm những mô hình mạng khác để trao dồi thêm.

5. Dự định của Thế Anh trong thời gian sắp tới?

Dạ!Về vấn đề này. Em nghĩ em cũng sắp tốt nghiệp, với những hành trang em có trong tay, em nghĩ em bắt đầu tìm cho mình một công việc thích hợp với đúng chuyên ngành của mình. Em dự định sẽ nộp đơn vào 1 số công ty vừa và nhỏ. Em nghĩ nếu muốn thành công trong tương lai thì em nên bắt đầu ở những nơi vừa và nhỏ trước, sau khi tích lũy được 1 vốn kinh nghiệm đến lúc đó em mới nghĩ tới những tập đoàn hay doanh nghiệp lớn hơn để phát triển sự nghiệp của mình. Và em cũng dự định sắp tới là sẽ sắp xếp thời gian để tham gia những khóa học cao hơn như CCNP, CCNA Security…. tại VnPro để nâng cao kiến thức của mình hơn nữa!!

Chúc Thế Anh sớm tiếp tục gặt hái những thành công tiếp theo trên con đường chinh phục đỉnh cao chuyên gia quản trị mạng quốc tế đẳng cấp!

Ôn tập CCNAX THÁNG 11/2014

Các bạn đã học xong chương trình CCNAX (chứng chỉ CCNA Routing & Switching) nhưng chưa tự tin với kiến thức của mình? Các bạn muốn thi chứng chỉ quốc tế nhưng chưa biết kiến thức mình đã đủ chưa, đề thi CCNA Routing & Switching như thế nào? Giờ đây các bạn không còn phải lo lắng những vấn đề trên nữa, vì trong tháng 11 này VnPro sẽ mở lớp **"Ôn tập CCNAX miễn phí"** dành cho tất cả các bạn cựu học viên VnPro!

Đến với lớp ôn tập CCNAX, các bạn sẽ được ôn luyện lại tất cả các kiến thức cốt lõi nhất của chương trình CCNAX. Từ đó giúp các bạn cũng cố lại thật chắc kiến thức và đồng thời cũng bổ sung những phần cập nhật mới nhất của chứng chỉ CCNAX để giúp các bạn tự tin đi thi quốc tế.

Đặc biệt: ***các học viên tham giá khóa ôn tập còn được phát tài liệu thi miễn phí (được cập nhật thường xuyên và có hướng dẫn giải chi tiết.***

Nội dung chương trình:

Ngày 25/11/2014: Ôn tập kiến thức CCNAX phần 1

Ngày 27/11/2014: Ôn tập kiến thức CCNAX phần 2

Thời gian : từ 18h30 đến 21h30

Địa điểm : Trung tâm tin học VnPro
149/1D Ung Văn Khiêm, P.25, Q. Bình Thạnh, TP.HCM

Đăng ký : http://www.vnpro.vn/on-tap-ccnax/

MIỄN PHÍ

Vì số lượng đăng ký có hạn, Anh/Chị vui lòng đăng ký trước ngày 21/11/2014

Chương trình "BƯỚC CHÂN KỸ SƯ MẠNG"

Trong tháng 11, Trung tâm tin học VnPro sẽ phối hợp cùng câu lạc bộ hội tin học thành phố HCA-TC tổ chức chương trình "Bước chân kỹ sư mạng" & "Kỹ năng mềm - hành trang ra trường"

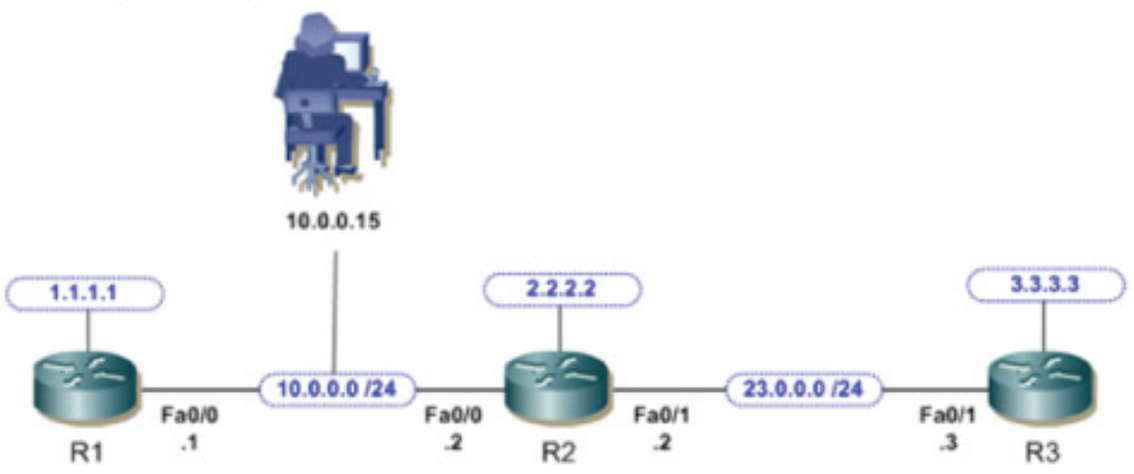
Mục đích chương trình nhằm cung cấp cho sinh viên khoa Điện – Điện Tử Viễn Thông, Khoa công nghệ thông tin các trường đại học một bức tranh tổng thể về thị trường việc làm ngành mạng máy tính và viễn thông hiện tại. Đồng thời cũng giúp định hướng cho sinh viên bổ sung những kiến thức nghề, kỹ năng mềm cần thiết cho quá trình học tập và làm việc sau khi ra trường.

Đăng ký tham gia: **http://www.vnpro.vn/dang-ky-buoc-chan-ky-su-mang/**

Firewal ASA Routed vs. Transparent

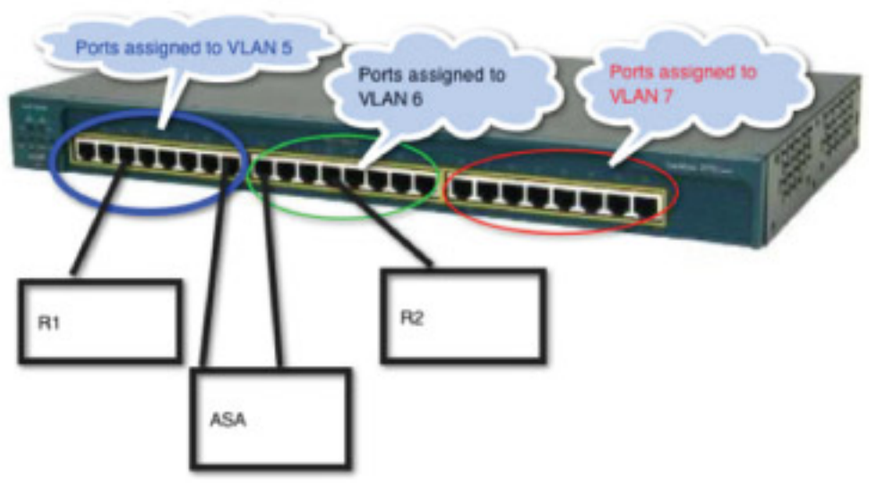
Transparent mode được định nghĩa tại trên cả 2 cổng giao tiếp inside và outside interface tham gia vào cùng lớp mạng subnet, nhưng khác VLAN.

Chẳng hạn như trong trường hợp chúng ta muốn bổ xung thêm firewall như trong hình minh họa bên dưới, để không ảnh hưởng đến kiến trúc IP của hạ tầng mạng sẵn có, lúc này ta có thể gắn firewall giữa R1 và R2 hoạt động ở chế độ "transparent".



Nếu chúng ta thiết lập firewall ở mức L3 giữa R1 và R2, chúng ta sẽ phải quy hoạch lại hệ thống IP của hạ tầng mạng hiện tại vì mỗi cổng giao tiếp L3 interface trên ASA sẽ thuộc các subnet khác nhau, lúc này R1 và R2 sẽ không cùng subnet nữa.

Giải pháp cho tình huống này là thiết lập transparent firewall hoạt động ở mức L2:



Từ switch, VLAN5 và VLAN 6 là 2 VLAN riêng biệt nhau, nhưng nếu ASA hoạt động ở chế độ transparent mode, ASA sẽ kết nối 2 VLAN lại nhưng vẫn thuộc cùng một L2 broadcast domain.

Tất cả các thiết bị thuộc VLAN 5 và 6 sẽ tham gia vào cùng không gian địa chỉ L3 network address, nhưng lưu lượng giữa R1 và R2 sẽ phải đi qua ASA hoạt động ở chế độ transparent mode.

Cách thức nhận diện các dòng switch 3750 dựa vào mã Code?

Thế hệ Switch 3750 có rất nhiều dòng sản phẩm khác nhau như WS-C3750X-48P-L, WS-C3750X-48P-S, WS-C3750X-24T-L, WS-C3750X-24T-S, WS-C3750X-12S-E, WS-C3750G-24PS-S, các mã Code như WS, X/G/E, 24/48/12, T/P/S/PS, -L/-S/-E trong tình huống này đều có ý nghĩa của riêng chúng.

Bài viết này sẽ tiến hành khảo sát ý nghĩa của các mã code được sử dụng để định danh các dòng sản phẩm Cisco 3750 switch, thông tin này sẽ giúp ta xác định chức năng của mỗi dòng model hỗ trợ đắc lực trong việc chọn lựa đúng sản phẩm cho hạ tầng mạng của bạn.

Mã sản phẩm (product code) trên Cisco 3750 switch có thể được viết tổng quát như sau: WS-C3750a-xxbc-dee

WS đại diện cho Switch

C đại diện cho Catalyst series

3750 đại diện cho 3750 product line

a>> blank, G, E

blank=classic 3750 switch, 6.5 hoặc 13.1 mpps forwarding rate

G=tất cả các port đều hoạt động ở chế độ gigabit, 35 hoặc 38 mpps forwarding rate

E=enterprise line, 65.5 hoặc 101.2 mpps forwarding rate

xx>>12, 16, 24, 48

12=12 Ethernet ports

16=16 Ethernet ports

24=24 Ethernet ports

48=48 Ethernet ports

b>>T, P, F, D, W

T=Ethernet ports

P=Power over Ethernet

F=100BASE-FX fiber

D=10 Gigabit Ethernet XENPAK port

W=Wireless

c>>S

S= 2 hoặc 4 Small Form-Factor Pluggable (SFP) uplink

d>>E, S

S= Standard IP Base image (IPB)

E= Enhanced IP Services (IPS)

ee>> 1U, D, 25, 50

1U= 1U Rack Height

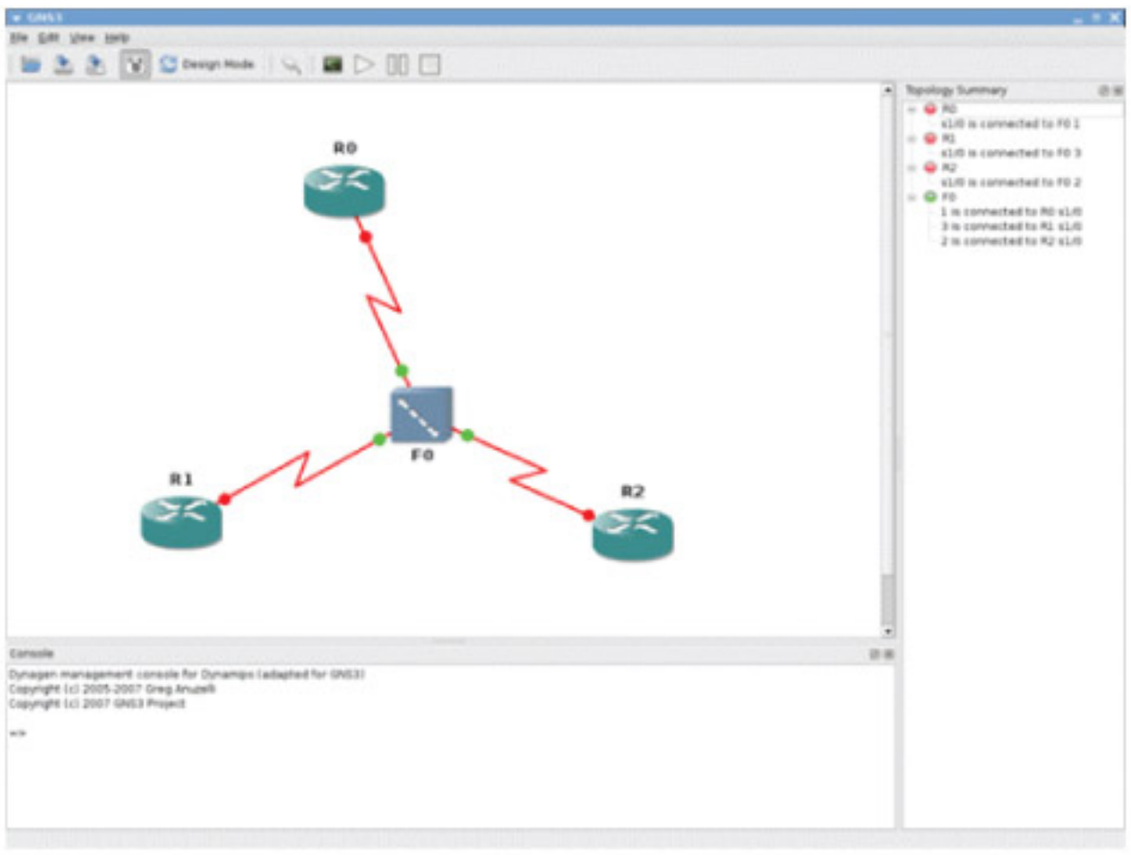
D= DC Power Supply

25= hỗ trợ tối đa 25 Access point

50= hỗ trợ tối đa 50 Access point

Người biên soạn: Bùi Quốc Kỳ

Các phần mềm mô phỏng Router



Giao diện chương trình GNS3

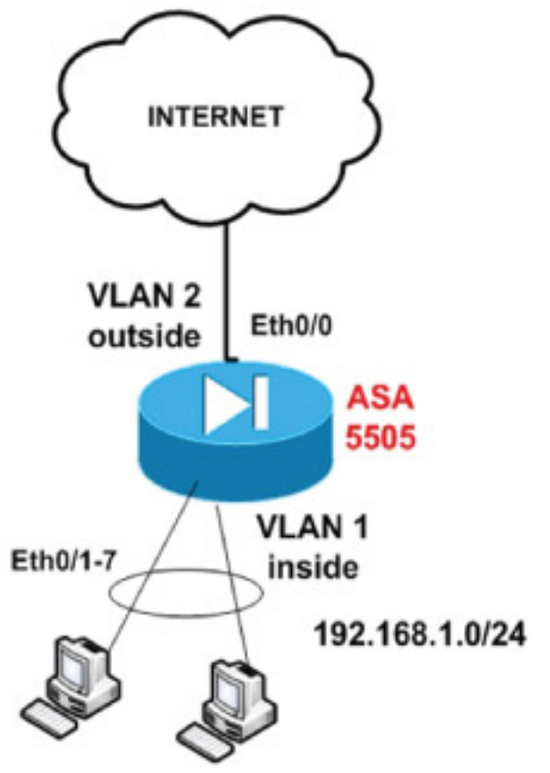
Để hỗ trợ cho quá trình tìm hiểu về mạng, nhiều phần mềm cho phép ta giả lập thiết bị router đã ra đời phục vụ cho quá trình học tập và nghiên cứu. Sau đây là danh sách các phần mềm mà chúng ta có thể sử dụng phục vụ cho quá trình nghiên cứu các công nghệ "network":

- GNS3 (Graphical Network Simulator)
- Cisco Packet Tracer
- SemSim Simulator
- Boson NetSim Simulator
- CertExams Simulator
- RouterSim CCNA Simulator
- MIMIC CCNA Simulator

Trong số các phần mềm trên thì có 2 chương trình thường được sử dụng đó là GNS3 và Cisco Packet Tracer.

Cấu hình Cisco ASA 5505

Cisco ASA 5505 Firewall là dòng model cấp thấp phù hợp cho môi trường mạng doanh nghiệp nhỏ hoặc lắp đặt tại các chi nhánh. Đối với quy mô doanh nghiệp lớn hơn, ta có thể sử dụng các dòng model như 5510, 5520, 5540. Cisco ASA 5505 hỗ trợ thông lượng throughput 150Mbps và 4000 kết nối trên mỗi giây (connections per second).



Sự khác biệt chủ yếu của 5505 model so với các dòng ASA model lớn hơn là nó có 8-port 10/100 switch chỉ có thể hoạt động ở Layer 2. Chúng ta không thể cấu hình các physical port đóng vai trò là Layer 3 port, thay vào đó ta có thể thiết lập các interface Vlan rồi liên kết các Layer 2 interface tương ứng với mỗi VLAN. Theo mặc định thì interface Ethernet0/0 sẽ thuộc thành viên VLAN 2 với vai trò outside interface (kết nối đi Internet), và 7 interface còn lại (Ethernet0/1 tới 0/7) mặc định sẽ tham gia vào VLAN 1 và được sử dụng để kết nối tới internal network.

Bước 1: Cấu hình internal interface vlan

```
ASA5505(config)# interface Vlan 1
ASA5505(config-if)# nameif inside
ASA5505(config-if)# security-level 100
ASA5505(config-if)# ip address 192.168.1.1 255.255.255.0
ASA5505(config-if)# no shut
```

Bước 2: Cấu hình external interface vlan (kết nối tới Internet)

```
ASA5505(config)# interface Vlan 2
ASA5505(config-if)# nameif outside
ASA5505(config-if)# security-level 0
ASA5505(config-if)# ip address 200.200.200.1
255.255.255.0
ASA5505(config-if)# no shut
```

Bước 3: Nhúng Ethernet 0/0 vào Vlan 2

```
ASA5505(config)# interface Ethernet0/0
ASA5505(config-if)# switchport access vlan 2
ASA5505(config-if)# no shut
```

Bước 4: Kích hoạt các interface còn lại với câu lệnh no shut

```
ASA5505(config)# interface Ethernet0/1
ASA5505(config-if)# no shut
```

Thực hiện tương tự trên các cổng giao tiếp Ethernet0/1 tới 0/7.

Bước 5: Cấu hình PAT trên cổng giao tiếp outside interface

```
ASA5505(config)# global (outside) 1 interface
ASA5505(config)# nat (inside) 1 0.0.0.0 0.0.0.0
```

Cấu hình PAT trên ASA Version 8.3

Bắt đầu từ tháng 3 năm 2010, Cisco giới thiệu phiên bản Cisco ASA software version 8.3 với nhiều thay đổi trong cách cấu hình, điển hình nhất là cấu hình NAT/PAT. Câu lệnh "global" command không còn được hỗ trợ nữa. NAT (static và dynamic) và PAT sử dụng thêm khái niệm network object. Cấu hình PAT đối với phiên bản ASA 8.3 và sau này được cấu hình như sau:

```
object network obj_any
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
```

Bước 6: Cấu hình default route trỏ tới ISP (giả sử default gateway là 200.200.200.2)

```
ASA5505(config)# route outside 0.0.0.0 0.0.0.0
200.200.200.2 1
```

Phía trên là những bước cơ bản nhất để cấu hình ASA 5505, bên cạnh đó chúng ta còn phải triển khai thêm một số tính năng khác nữa như Access Control List, Static NAT, DHCP, DMZ zone, authentication, v.v.

Người biên soạn: Bùi Quốc Kỳ

9 kỹ năng "mềm" quyết định 75% sự thành đạt

1. Có một quan điểm lạc quan

Tất cả chúng ta đã từng nghe lời khuyên hãy nhìn cốc nước còn đầy một nửa tốt hơn là nhìn nó đã vơi đi một nửa. Ở nơi làm việc, cách nghĩ lạc quan này có thể giúp bạn phát triển trên một chặng đường dài. Tất cả mọi cái nhìn lạc quan đều dẫn đến một thái độ lạc quan và có thể là một vốn quý trong môi trường làm việc, đánh bại thái độ yếm thế và bi quan.

Chìa khóa để có một thái độ lạc quan là bạn giải quyết một sự trở ngại hay thách thức như thế nào khi gặp phải. Ví dụ, thay vì than phiền về khối lượng công việc gây stress, hãy nghĩ về nó như một cơ hội để thể hiện khả năng làm việc tích cực và hiệu quả của bạn.

2. Hòa đồng với tập thể

Các nhà tuyển dụng rất thích những nhân viên thể hiện được khả năng làm việc tốt trong tập thể. Hòa đồng với tập thể ko chỉ có nghĩa là có tính cộng tác mà còn thể hiện được khả năng lãnh đạo tốt khi có thời điểm thích hợp.

Có thể tới một lúc nào đó, sự xung đột xuất hiện trong tập thể của bạn, hãy tỏ ra chủ động dàn xếp. Khi bạn thấy tập thể của mình đang bị sa lầy trong một dự án, hãy cố gắng xoay chuyển tình thế, đưa cách giải quyết theo một hướng khác. Và bạn làm gì nếu bình thường bạn không làm việc trong một nhóm? Hãy cố gắng tỏ ra sẵn sàng hợp tác trong công việc và thiết lập nên các mối quan hệ công việc với mọi đồng nghiệp nếu có thể. Học cách nói những điều bạn nghĩ như thế nào và thể hiện bằng ngôn ngữ cử chỉ ra sao.

3. Giao tiếp hiệu quả

Kỹ năng giao tiếp tốt là một thế mạnh đối với bất cứ ai trong công việc. Giao tiếp là phương tiện cho phép bạn xây dựng cầu nối với đồng nghiệp, thuyết phục người khác chấp nhận ý kiến của bạn và bày tỏ được nhu cầu của bạn.

Nhiều điều nhỏ nhặt bạn đã từng thực hiện hàng ngày - có thể có những điều bạn không từng nghĩ đến lại có một sự ảnh hưởng rất lớn tới kỹ năng giao tiếp của bạn. Sau đây là những điều bạn nên lưu ý khi giao tiếp với những người khác:

- Nhìn thẳng vào mắt người đối diện

- Đừng tỏ ra bồn chồn

- Tránh những chuyển động cơ thể khiến bạn bị tách ra khỏi họ

- Đừng nói chuyện chỉ để nói, hãy tập trung vào một vấn đề

- Phát âm một cách chính xác

- Sử dụng ngữ pháp chuẩn thông thường

Nói chung, bạn nên để ý tới cách sử dụng từ ngữ của mình để tạo ấn tượng với người đối thoại. Cũng đừng quên rằng một trong những kỹ năng giao tiếp là biết lắng nghe.

4. Tỏ thái độ tự tin

Trong hầu hết các trường hợp, khi bạn muốn gây ấn tượng với một ai đó, sự tự tin là một thái độ rất hiệu quả. Trong khi sự khiêm nhường khi bạn nhận được lời tán dương là rất quan trọng thì sự thừa nhận thế mạnh của mình cũng quan trọng không kém. Hãy tin chắc rằng bạn có sự nhận biết và kỹ năng để có thể bày tỏ được sự tự tin của mình.

5. Luyện kỹ năng sáng tạo

Tính sáng tạo và lối suy nghĩ thông minh được đánh giá cao ở bất cứ công việc nào. Thậm chí công việc mang tính kỹ thuật nhất cũng đòi hỏi khả năng suy nghĩ thoát ra khỏi khuôn khổ. Vì vậy đừng bao giờ đánh giá thấp sức mạnh của việc giải quyết vấn đề theo cách sáng tạo.

Bạn có thể đang phải làm một công việc chán ngắt, buồn tẻ, hãy cố gắng khắc phục nó theo cách hiệu quả hơn. Khi một vấn đề khiến người ta phải miễn cưỡng bắt tay vào làm, hãy nghĩ ra một giải pháp sáng tạo hơn. Nếu không được, ít ra bạn đã từng thử nó.

6. Thừa nhận và học hỏi từ những lời phê bình

Đây là một trong những kỹ năng mang tính thử thách nhất, và cũng chính là kỹ năng gây ấn tượng nhất đối với người tuyển dụng. Khả năng ứng xử trước lời phê bình phản ánh rất nhiều về thái độ sẵn sàng cải thiện của bạn. Đồng thời có khả năng đánh giá, nhận xét mang tính xây dựng đối với công việc của những người khác cũng mang ý nghĩa quan trọng không kém. Hãy nhận thức xem bạn thủ thế như thế nào khi phản ứng trước những lời nhận xét tiêu cực. Đừng bao giờ ném đá vào những lời phê bình mang tính xây dựng mà không nhận thấy rằng ít nhất nó cũng có ích một phần. Khi bạn đưa ra lời nhận xét với người khác, hãy thể hiện sao cho thật khéo léo và chân thành. Cố gắng dự đoán trước phản ứng của người nghe dựa vào tính cách của họ để có cách nói phù hợp nhất.

7. Thúc đẩy chính mình và dẫn dắt người khác

Một điều rất quan trọng đối với nhà tuyển dụng là làm sao để biết được bạn có là người năng động và hay đề ra các sáng kiến hay không? Điều này có nghĩa là bạn liên tục tìm ra những giải pháp mới cho công việc của mình khiến cho nó hấp dẫn hơn thậm chí đối với cả những công việc mang tính lặp đi lặp lại.

Sự sáng tạo có vai trò rất lớn trong việc thúc đẩy, nó khiến bạn đủ dũng cảm để theo đuổi một ý tưởng vốn bị mắc kẹt trong suy nghĩ và cuối cùng là bạn vượt qua được nó. Dẫn dắt những người khác theo cùng một hướng để đạt một mục đích chung, và người lãnh đạo giỏi là người có thể lãnh đạo được người khác bằng chính tấm gương của mình.

8. Đa năng và ưu tiên những việc cần làm trong danh sách của bạn

Ở công sở ngày nay, một nhân viên tốt là một nhân viên có khả năng kiêm nhiệm thêm một số công việc khác, hay nhiều dự án cùng một lúc. Liệu bạn có thể theo dõi được tiến trình của các dự án khác nhau hay không? Bạn có biết lựa chọn để ưu tiên những việc quan trọng nhất không? Nếu có thể, bạn được gọi là người đa năng.

Đừng than phiền rằng bạn phải làm thêm các công việc khác. Hãy thể hiện khả năng đa kỹ năng của bạn. Chắc chắn cái bạn nhận lại sẽ là rất lớn như kinh nghiệm hay các mối quan hệ mới.

9. Có cái nhìn tổng quan

Có cái nhìn tổng quan về công việc có nghĩa là có khả năng xác định được các yếu tố dẫn tới thành công. Điều này cũng có nghĩa là nhận ra các nguy cơ tiềm ẩn và thời điểm nó xảy ra. Ví dụ như bạn làm việc trong lĩnh vực quảng cáo và phải xây dựng một chiến dịch để quảng cáo cho một nhãn hiệu xà bông. Nếu nhìn một cách tổng thể, bạn có thể nhận thấy rằng mục đích không chỉ là bán được hàng, mà còn làm thỏa mãn và thuyết phục khách hàng về chất lượng sản phẩm. Thêm vào đó, bạn còn phải tạo thêm giá trị cho công ty của bạn bằng cách chứng minh rằng tính sáng tạo độc nhất chỉ bạn mới có thể tạo ra.


Chả có gì làm , hay là mỗi người nói một bí mật xấu xa của mình đi , chỉ nhóm mình biết thôi
Ngại quá ,để Chai mở đầu vậy , Chai rất hay .....
Đánh rắm khi đang tắm
Xé thì hay .... đái dầm một cách âm thầm
Haizzz .... Mimi nói Mon sắp có con
Xu luôn phải mếch ắp lúc sắp ra đường
Còn bí mật của Nô là ..... ko bao h giữ được bí mật


Tao có thể ăn một lần 5 quả trứng gà.
Còn tao thì cùng 1 lúc xử đẹp 6 quả trứng vịt.
Bèo! Tao thì một lần xử cả trăm quả.
Vô lý! Mày ăn trứng gì thế?
Trứng... cá. Hehehe
HỰ


AI CỨU TÔI VỚI! TÔI KHÔNG DỪNG XE LẠI ĐƯỢC
TÔNG NÓ ĐI, TÔNG VÀO TƯỜNG LÀ HƯ XE ĐÓ
H3-P27


1 cô gái gặp 1 nhà sư ở chùa, cô ấy hỏi nhà sư:
Ở giữa 2 chân của thầy là gì vậy ạ ?
Nhà sư nghĩ mình đã tu lâu năm nên trả lời : Nó chỉ là 1 cái xác chết ?
"Thế ở giữa 2 chân con là cái gì ?"
Nhà sư hỏi cô gái
Cô gái trả lời: "Là cái quan tài ạ" =)

PHẦN II PHƯƠNG PHÁP GIẢM TẤN CÔNG MẠNG

Tổng quan về các nguy cơ tấn công mạng

Tùy theo quy mô của các hệ thống mạng, các dạng tấn công mạng có thể biến thể theo nhiều kiểu khác nhau. Nếu không có sự bảo vệ đúng đắn, bất kỳ nơi nào trong hệ thống mạng cũng có thể bị tấn công hoặc bị xâm nhập trái phép. Router, switch hoặc các thiết bị máy tính đầu cuối đều có thể bị xâm phạm bởi những hacker chuyên nghiệp, các công ty đối thủ hoặc ngay cả các nhân viên bên trong tổ chức của mình. Thực chất là các thống kê cho thấy rằng phần lớn các cuộc tấn công đều xuất phát từ bên trong mạng nội bộ của công ty.

Các tác nhân đe dọa đến bảo mật mạng:

Tổng quát, các tác nhân có khả năng đe dọa đến bảo mật mạng được chia làm 4 loại:

- Các tác nhân có cấu trúc
- Các tác nhân không có cấu trúc
- Các tác nhân xuất phát từ bên ngoài
- Các tác nhân có nguồn gốc từ bên trong

Các tác nhân không có cấu trúc: (unstructured Attacks)

Các tác nhân này gây ra bởi những hacker sử dụng những công cụ như password cracker, các chương trình sinh số credit card tự động … Mặc dù chủ thể tấn công theo dạng này có thể có chủ ý, nhưng đa số là do muốn biểu diễn khả năng của mình hơn là gây ra phá hoại cho hệ thống mạng.

Các tác nhân có cấu trúc (structured Attacks):

Các tác nhân này gây ra bởi những hacker có trình độ cao. Những hacker này hoạt động một mình hay theo nhóm và dùng / phát triển những công cụ tấn công tinh vi để xâm nhập vào các công ty. Những hacker này thông thường được thuê bởi các tổ chức tội phạm, các công ty đối thủ của nhau….và có khả năng gây phá hoại nặng nề cho các hệ thống mạng.

Các tác nhân xuất phát từ bên ngoài:

Những tác nhân này (bao gồm có cấu trúc hoặc không có cấu trúc) có nguồn gốc xuất phát từ bên ngoài. Những tác nhân này có thể chứa những ý định phá hoại hoặc đơn giản là những lỗi của hệ thống (về phần cứng/ phần mềm) gây ra những tác nhân này.

Các tác nhân có nguồn gốc từ bên trong:

Những tác nhân này gây ra phần lớn từ các nhân viên trong tổ chức, và gây ra nhiều điều đáng ngại hơn so với các tác nhân từ bên ngoài. Tuy nhiên, đã có những công cụ làm giảm ảnh hưởng của các tác nhân này và có thể đáp ứng lại khi có bất kỳ tấn công nào xảy ra.

Các loại tấn công mạng chủ yếu:

Các cuộc tấn công mạng có thể được phân loại thành 4 kiểu sau đây:

- Tấn công theo kiểu do thám
- Tấn công theo kiểu truy xuất
- Tấn công từ chối dịch vụ
- Worms, Viruses và Trojan horses

Tấn công theo kiểu do thám:

Là những hành động dùng các công cụ hoặc những thông tin có sẵn dò tìm các thông tin, các dịch vụ hoặc các lỗ hổng trong hệ thống mạng nào đó. Các hành động này còn được xem là thu thập thông tin và trong nhiều trường hợp đây là những hiện tượng mở đầu cho các tấn công theo kiểu truy nhập hoặc từ chối dịch vụ. Chủ thể tấn công thông thường thực hiện dò tìm các máy nào hiện diện bằng cách ping quét các địa chỉ IP. Sau đó chủ thể này tiếp tục dò tìm các dịch vụ hay các port nào đang mở trên các địa chỉ IP này và sẽ thực hiện yêu cầu (query) trên các port này nhằm xác định loại ứng dụng và version cũng như thông tin về hệ điều hành đang chạy trên máy này.

Tấn công theo kiểu do thám có thể có những dạng sau:

- Bắt gói packet (packet sniffing)
- Dò port (port scan)
- Ping quét (Ping sweep)
- Thực hiện yêu cầu thông tin Internet (Internet Information queries)

a. Bắt gói packet (packet sniffing):

Đây thực chất là một ứng dụng sử dụng NIC mạng cho hoạt động ở mode promicuous nhằm để giữ lại tất cả những gói packet đi qua LAN (cùng collision domain). Cách bắt gói như thế này chỉ tận dụng các thông tin được gửi đi theo dạng text (clear text) (ví dụ các giao thức sau gửi thông tin trong gói ở dạng clear text : Telnet, FTP, SNMP, POP, HTTP …). Các chương trình này có thể được thiết kế theo kiểu tổng quát hay theo kiểu chuyên dùng cho các cuộc tấn công.

Một số cách làm giảm đi khả năng bắt gói trong hệ thống mạng:

- Xác thực người dùng : lựa chọn đầu tiên cho việc chống lại các công cụ bắt gói trong hệ thống mạng là sử dụng cơ chế xác thực người dùng chẳng hạn như mật khẩu chỉ dùng 1 lần (one-time password).
- Hiện thực hệ thống switch trong mạng: hiện thực hệ thống switch trong mạng LAN có thể làm giảm việc bắt gói trong mạng
- Sử dụng những công cụ chống / nhận dạng các phần mềm bắt gói có trong hệ thống của mình.
- Mã hoá dữ liệu: làm cho các công cụ bắt gói trở nên vô hiệu và được xem là hiệu quả nhất để chống lại kiểu tấn công này. Nếu kênh thông tin được bảo mật chặt chẽ, dữ liệu mà các công cụ bắt gói này có được là những dữ liệu đã được mã hóa. Một số công cụ như SSH (Secure Shell Protocol) và SSL (Secure socket Layer) có sử dụng cơ chế mã hóa cho các dữ liệu quản lý của mình để chống lại các tấn công theo kiểu này.

b.Dò port và Ping quét:

Đây là những ứng dụng nhằm kiểm tra thiết bị nào đó với mục đích nhận dạng tất cả các dịch vụ trên thiết bị này. Thông tin có được từ việc thu thập các thông tin về địa chỉ IP và Port từ các port TCP hay UDP.

Cách làm giảm các tấn công kiểu dò port và ping quét :

Tấn công theo kiểu dò port và ping quét rất khó loại bỏ hoàn toàn trong hệ thống mạng ví dụ nếu tắt đi ICMP echo và reply trên router thì ping quét có thể bị loại bỏ nhưng lại gây khó khăn cho người quản trị trong việc chẩn đoán / kiểm tra kết nối khi có sự cố xảy ra. Tuy

nhiên tấn công quét port vẫn có thể hoạt động mà không cần ping quét đi kèm. Một số thiết bị phát hiện xâm nhập (IDS) có thể thông báo cho người quản trị khi phát hiện được đang có các tấn công do thám xảy ra.

c.Thực hiện yêu cầu dò tìm thông tin trên Internet

Các yêu cầu về tên miền (DNS queries) có thể giúp phát hiện một số thông tin chẳng hạn như ai đang sở hữu tên miền và các địa chỉ nào được dùng cho tên miền đó. Ping quét các địa chỉ này sẽ giúp cho chủ thể tấn công có một cái nhìn tổng quát về những thiết bị nào đang "sống" trong môi trường này. Khi đó, các công cụ quét port có thể phát hiện được những dịch vụ nào đang chạy trên các máy này. Cuối cùng, hacker có thể giám sát các đặc tính của các ứng dụng chạy trên máy cụ thể nào đó, bước này có thể dẫn đến việc thu thập một số thông tin để gây tổn hại đến dịch vụ đó.

Việc dò tìm địa chỉ IP như trên có thể biết được những thông tin như ai đang sở hữu những địa chỉ IP nào và tên domain liên kết tới những địa chỉ này.

Tấn công theo kiểu truy xuất và một số phương pháp làm giảm kiểu tấn công này.

Tấn công theo kiểu truy xuất khai thác những lổ hỗng trong các dịch vụ xác thực, FTP, Web ... để lấy các dữ liệu như các tài khoản đăng nhập Web, các cơ sở dữ liệu nội bộ hoặc các thông tin nhạy cảm. Ngoài ra, chủ thể tấn công còn có thể nắm quyền truy nhập và tự làm tăng quyền truy xuất vào hệ thống. Tấn công theo kiểu này bao gồm những dạng sau:

- Tấn công dò tìm mật khẩu
- Khai thác những điểm đáng tin cậy
- Chuyển hướng port ứng dụng
- Tấn công theo kiểu man-in-the-middle attack

a. Tấn công dò tìm mật khẩu

Hacker có thể dò tìm mật khẩu sử dụng một vài cách thức như: tấn công theo kiểu Brute-force, dùng các chương trình Trojan horse, các công cụ bắt gói hay kỹ thuật IP Spoofing. Mặc dù các kỹ thuật bắt gói hay IP Spoofing có thể giúp tìm ra được tài khoản của người sử dụng (username, password), tấn công dò tìm mật khẩu luôn luôn liên hệ tới việc thử-và-sai lặp đi lặp lại thông tin tài khoản, kiểu này còn được gọi là tấn công theo kiểu Brute-force.

Thông thường tấn công theo kiểu brute-force được thực hiện dưới dạng sử dụng chương trình chạy qua mạng và thử truy xuất vào các tài nguyên chia sẻ trên các server. Khi chủ thể tấn công truy nhập vào được các tài nguyên này, chủ thể này có cùng quyền với tài khoản mà mình đang sử dụng. Nếu tài khoản này có đủ quyền hạng, chủ thể tấn công có thể tạo những lỗ hổng truy xuất riêng cho mình vào hệ thống mà không cần thay đổi gì đến tài khoản của người sử dụng. Tấn công Brute-Force có thể xâm nhập và chỉnh sửa các file và các dịch vụ mạng, hoặc bổ sung bảng tìm đường làm cho traffic mạng chuyển hướng đến chủ thể tấn công trước khi chúng đi đến đích đến cuối cùng. Trường hợp này, chủ thể tấn công có thể giám sát tất cả traffic mạng, trở thành một dạng tấn công man-in-the-middle.

Ví dụ:

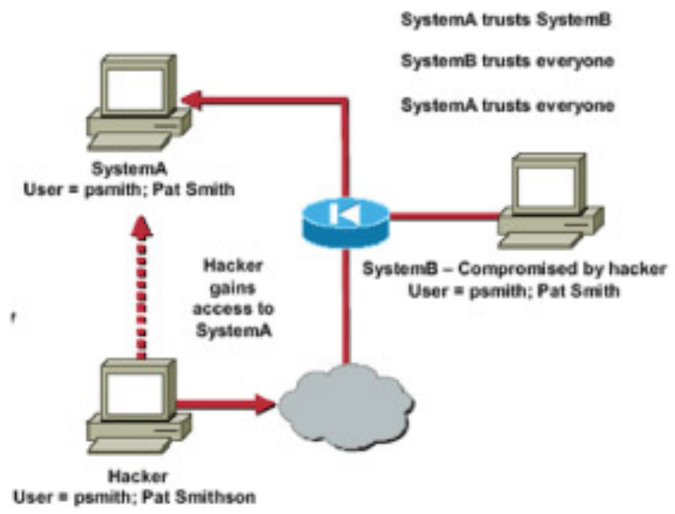
Chương trình L0phtCrack có thể lấy dữ liệu dạng băm (hash) của mật khẩu và khôi phục lại dạng text. Đây là 2 cách tính toán mật khẩu mà chương trình này sử dụng:

- Crack dò tìm theo kiểu từ điển (Dictionary cracking): tất cả các từ trong 1 file từ điển được băm và so sánh với tất cả mật khẩu được băm của người sử dụng. Cách này tương đối nhanh và rất hiệu quả trong việc dò tìm những mật khẩu đơn giản.
- Tính toán theo kiểu Brute-Force: bằng việc sử dụng một tập ký tự đặc biệt, như A-Z hoặc A-Z cùng 0-9, và tính toán ra giá trị băm từ việc kết hợp các ký tự này với nhau. Cách này sẽ luôn tìm ra mật khẩu nếu và chỉ nếu các ký tự có trong mật khẩu nằm trong tập ký tự được chọn. Nhược điểm là tốn rất nhiều thời gian khi sử dụng cách này.

Cách làm giảm tấn công dò tìm mật khẩu:

- Không cho phép người sử dụng dùng cùng mật khẩu trên những hệ thống khác nhau.
- Vô hiệu hóa tài khoản của người sử dụng sau một số lần xác thực không thành công.
- Không sử dụng mật khẩu dạng text. Nên sử dụng các loại mật khẩu chỉ dùng một lần (One-time password OTP) hoặc các mật khẩu đã được mã hóa.
- Đặt mật khẩu có ít nhất 8 ký tự trong đó có chứa ký tự in hoa, ký tự thường, ký tự số và các ký tự đặc biệt. ("strong" password).

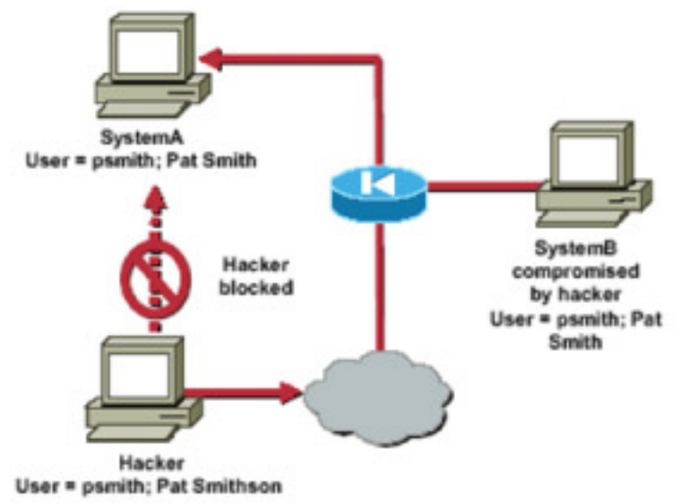
b. Khai thác những điểm được xem là tin cậy trong hệ thống mạng:



Một trong những ví dụ về các điểm được xem là đáng tin cậy đó là một hệ thống mạng có chứa các dịch vụ như DNS, SMTP, và HTTP. Do tất cả các server nằm chung trên một segment mạng nên khi có một máy A bị tấn công cũng có thể dẫn đến các máy khác cũng bị tấn công do các hệ thống này xem A là thiết bị đáng tin cậy (ví dụ như domain hoặc Active Directory trong hệ thống Windows hay NFS và NIS+ trong hệ thống Linux và Unix).

Một ví dụ khác là một máy ở vùng bên ngoài (outside) thiết bị firewall xây dựng được mối liên hệ tin cậy với các thiết bị ở vùng mạng bên trong (inside). Khi máy này bị tấn công thì chủ thể tấn công có thể tận dụng các mối liên hệ tin cậy này để tiếp tục tấn công vào hệ thống bên trong.

Cách làm giảm tấn công :



Cách hay nhất để hạn chế tấn công theo kiểu này đó là các hệ thống ở vùng bên trong của firewall không nên tin / xây dựng các mối quan hệ đáng tin cậy so với các hệ thống bên ngoài của firewall. Và các mối liên hệ đáng tin cậy nếu có xây dựng thì chỉ giới hạn cho những giao thức cụ thể và độ tin cậy nên được đánh giá bởi những yếu tố khác với địa chỉ IP.

ưu đãi

-20%

Ưu đãi lên đến 20% cho học viên cũ*

5%

Ưu đãi ngay 5% cho học viên mới*

Tặng áo thun VnPro

Tặng bộ sách LabPro

LỊCH KHAI GIẢNG THÁNG 11

*Chỉ áp dụng các lớp ban đêm
**Học phí chưa ưu đãi

Mã lớp	Tên khóa học	Ngày khai giảng	Ngày học	Giờ học	Học phí**/khóa	Thời gian
CHƯƠNG TRÌNH CCNA						
AK23	**CCNAX (200-120)**	13/11	3 – 5 - 7	8:30 – 11:30AM	3.360.000	152 giờ
AK25				2:00 – 5:00PM	3.360.000	
A23			3 – 5	6:30 – 9:30PM	6.720.000	
AK22		14/11	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
AK24				2:00 – 5:00PM	3.360.000	
A22				6:30 – 9:30PM	6.720.000	
AK27		18/11	3 – 5 - 7	8:30 – 11:30AM	3.360.000	
A25			3 – 5	6:30 – 9:30PM	6.720.000	
AK26		26/11	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
AK28				2:00 – 5:00PM	3.360.000	
AS3	**CCNA Security** (640-554)	11/11	3 – 5	6:30 – 9:30PM	6.720.000	100 giờ
AV1	**CCNA Voice** (640-461)	18/11	3 – 5	6:30 – 9:30PM	6.720.000	72 giờ
CHƯƠNG TRÌNH CCNP						
P1-K4	**ROUTE** (300 - 101)	14/11	2 – 4 – 6	8:30 – 11:30AM	6.600.000	140 giờ
P1-6				2:00 – 5:00PM	6.600.000	
P1-4				6:30 – 9:30PM	9.800.000	
P1-5		18/11	3 – 5	6:30 – 9:30PM	9.800.000	140 giờ
P2K3	**SWITCH** (300 - 115)	25/11	3 – 5 - 7	8:30 – 11:30AM	5.880.000	120 giờ
P2K5				2:00 – 5:00PM	5.880.000	
P2-5			3 – 5	6:30 – 9:30PM	8.232.000	
P3-4	**TSHOOT** (300 - 135)	27/11	3 – 5	6:30 – 9:30PM	9.800.000	140 giờ
CHƯƠNG TRÌNH CCIE						
EW1	**CCIE WRITTEN** (Version 5)	07/11	2 – 4 – 6	6:30 – 9:30PM	11.760.000	120 giờ
HỌC MẠNG MIỄN PHÍ						
	Thực hành mạng	15/11	Thứ 7	8:30 – 11:30AM	**Miễn phí**	3 giờ
	VoIP căn bản	22/11	Thứ 7	8:30 – 11:30AM	**Miễn phí**	3 giờ
	Ôn tập CCNA	25/11 & 27/11	Thứ 3 - 5	6:30 – 9:30PM	**Miễn phí**	6 giờ

ĐĂNG KÝ HỌC LIÊN HỆ

Bích Diễm Email : bichdiem@vnpro.org Di động: 0909 399 223
Thanh Trâm Email : thanhtram@vnpro.org Di động: 0949 246 829
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) 35 124 257

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: **2.000 cuốn/kỳ**
Kỳ hạn xuất bản: **1 kỳ/tháng**