Số 36
07/2015

BẢN TIN danCISCO

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

BẬT TUNG CẢM XÚC CÙNG SINH VIÊN KHOA ĐÀO TẠO CHẤT LƯỢNG CAO – ĐH SPKT TP.HCM

Ngày 26/06/2015 VnPro đã phối hợp cùng với Khoa đào tạo chất lượng cao trường Đại Học Sư Phạm Kỹ Thuật Tp. Hồ Chí Minh tổ chức hội thảo chuyên đề: ***"MẠNG TRUYỀN THÔNG – XU HƯỚNG TUYỂN DỤNG VÀ KỸ NĂNG TRONG XIN VIỆC".***

Chị Kim Thoa đại diện VnPro tặng hoa và quà lưu niệm cho Trưởng khoa CLC

[Trang 07]

Chứng chỉ CCNP Security có nhiều thay đổi

Hệ thống chứng chỉ CCNP Security có một số thay đổi mới. Cisco loại bỏ các chứng chỉ SECURE, IPS, FIREWALL & VPN và thay vào đó là các module mới:

- *SISAS – Implementing Cisco Secure Access Solutions*
- *SITCS – Implementing Cisco Edge Network Security Solutions*
- *SENSS – Implementing Cisco Security Mobility Solutions*
- *SIMOS – Implementing Cisco Threat Control Solutions*

CISCO CERTIFIED CCNP SECURITY

Các module mới sẽ tương đương với các module như sau:

- *Module SISAS tương đương với module SECURE .*
- *Module SITCS tương đương với module IPS.*
- *Module SENSS tương đương với module FIREWALL.*
- *Module SIMOS tương đương với module VPN.*

Người biên dịch: Phan Thanh Phong.

[Trang 01]

Nội dung của khóa học CCNA Collaboration

[Trang 02]

TIN TỨC SỰ KIỆN KHÁC

Chứng chỉ CCNP Security có nhiều thay đổi

Hệ thống chứng chỉ CCNP Security có một số thay đổi mới. Cisco loại bỏ các chứng chỉ SECURE, IPS, FIREWALL & VPN và thay vào đó là các module mới:

- *SISAS – Implementing Cisco Secure Access Solutions*
- *SITCS – Implementing Cisco Edge Network Security Solutions*
- *SENSS – Implementing Cisco Security Mobility Solutions*
- *SIMOS – Implementing Cisco Threat Control Solutions*

Các module mới sẽ tương đương với các module như sau:

- *Module SISAS tương đương với module SECURE .*
- *Module SITCS tương đương với module IPS.*
- *Module SENSS tương đương với module FIREWALL.*
- *Module SIMOS tương đương với module VPN.*

Người biên dịch: Phan Thanh Phong.

Cisco phát hành bản cập nhật vá lỗ hổng trên khóa SSH hard-coded

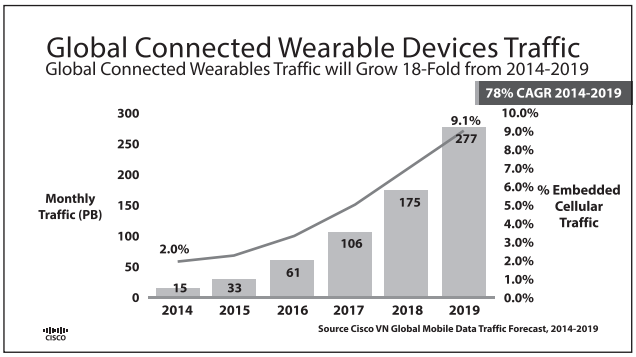
Khóa SSH (Secure Shell) hard-coded mặc định trên 3 ứng dụng phần mềm an ninh từ Cisco có thể bị hacker kết nối tới các sản phẩm của hãng với đặc quyền cao hoặc giải mã lưu lượng dữ liệu qua các sản phẩm này.

3 phần mềm bị ảnh hưởng bao gồm Web Security Virtual Appliance (WSAv), Cisco Email Security Virtual Appliance (ESAv), và Cisco Security Management Virtual Appliance (SMAv). Tất cả đều có chung các khóa SSH hợp lệ và các khóa SSH chủ trong tất cả các cài đặt.

"Một tin tặc có thể khai thác lỗ hổng này bằng cách chiếm lấy một trong những khóa SSH cá nhân và sử dụng để giả mạo hoặc mã hóa các giao dịch giữa WSAv, ESAv, và SMAv," một cố vấn an ninh của Cisco cho biết.

Cisco khắc phục tình trạng này bằng cách phát hành các bản cập nhật phần mềm miễn phí cho tất cả các sản phẩm bị ảnh hưởng của hãng.

Lưu lượng Mobile Traffic bùng nổ cùng với sự tăng trưởng của Internet of Everything



Internet of Everything (IoE) có tầm ảnh hưởng khá mạnh mẽ lên hạ tầng mạng toàn cầu (global network) kể từ lúc Internet of Everything xuất hiện 24 tháng trước đây. Chúng ta có thể nhận thấy tầm ảnh hưởng của IoE thông qua chỉ số thống kê VNI (Visual Networking Index) sau:

- Sẽ có khoảng 8 tỷ thiết bị di động (mobile device) được kết nối vào năm 2019
- 3.2 tỷ trong số 8 tỷ thiết bị – chiếm 40 phần trăm các thiết bị mobile Internet – sẽ được kết nối với nhau dưới hình thức machine-to-machine chẳng hạn như các thiết bị điện tử mang trên người (wearable device) chẳng hạn như thiết bị định vị, theo dõi (fitness tracker), đồng hồ thông minh (smart glass), các thiết bị thể thao (sport accesory), các thiết bị chăm sóc sức khỏe (healthcare device).
- Cisco dự đoán lưu lượng mobile traffic phát sinh từ các thiết bị "wearable device" sẽ tăng gấp 18 lần từ năm 2015 đến 2019.
- Sự gia tăng lưu lượng của các thiết bị "wearable device" khiến cho số lượng các thiết bị "wearable device" tăng lên gấp 5 lần, từ 109 triệu thiết bị vào năm 2014 lên 578 triệu thiết bị vào năm 2019.

Người biên soạn: Bùi Quốc Kỳ

Nội dung của khóa học CCNA Collaboration

Để sở hữu chứng chỉ CCNA Collaboration, thí sinh phải vượt qua 2 kỳ thi 210-060 CICD và 210-065 CIVND. Khóa học CICD ra đời thay thế cho khóa đào tạo CCNA Voice (ICOMM) với mã môn thi mới là 210-060. Khóa học CIVND ra đời thay thế cho khóa đào tạo VIVND với mã môn thi mới là 210-060.

Khóa đào tạo 210-060 CICD sẽ trang bị cho người học các kiến thức về giải pháp truyền thông hợp nhất Cisco Unified Communications (UC) solution với các nội dung cụ thể sau:

- 15% nội dung của chương trình mô tả các đặc điểm của giải pháp truyền thông hợp nhất Cisco Unified Commu nication
  - o Mô tả các thành phần và chức năng của Cisco Unified Communications
  - o Mô tả các luồng tín hiệu call signaling và media flow
  - o Mô tả tiến trình đảm bảo chất lượng dịch vụ cho hạ tầng VoIP network
- 24% nội dung của chương trình trang bị kiến thức về quản trị các "End User" và tương tác với các thiết bị đầu cuối
  - o Mô tả các tùy chọn thiết lập user trên Cisco Unified Communications Manager và Cisco Unified Communications Manager Express
  - o Khởi tạo và tinh chỉnh tài khoản user account trên môi trường Cisco Unified Communications Manager
  - o Khởi tạo và tinh chỉnh tài khoản user account trên môi trường Cisco Unified Communications Manager Express thông qua giao diện đồ họa GUI
  - o Khởi tạo và điều chỉnh các endpoint trên môi trường Cisco Unified Communications Manager
  - o Khởi tạo và điều chỉnh các endpoint trên môi trường Cisco Unified Communications Manager Express thông qua giao diện đồ họa GUI
  - o Mô tả chức năng calling privilege và ảnh hưởng của calling privilege đối với các tính năng của hệ thống system
  - o Khởi tạo và điều chỉnh các directory number
  - o Kích hoạt các tính năng user feature và tương tác giữa calling privilege với extension mobility, call coverage, intercom, native presence, và cấu hình unified mobility remote đầu cuối
  - o Kích hoạt các end user trên môi trường Cisco Unified IM và Presence
  - o Kiểm tra hoạt động của các tính năng tương ứng với user
- 27% nội dung của chương trình trang bị kiến thức về cấu hình "Voice Messaging" và "Presense"
  - o Mô tả các tùy chọn thiết lập user cho voice messaging
  - o Khởi tạo và điều chỉnh user account trên môi trường Cisco Unity Connection
  - o Mô tả Cisco Unified IM và Presence
  - o Cấu hình Cisco Unified IM và Presence
- 10% nội dung của chương trình trang bị kỹ năng bảo trì hệ thống Cisco Unified Communications System
  - o Xuất file CDR và CMR report
  - o Xuất file capacity report
  - o Xuất file usage report
  - o Xuất file RTMT report để giám sát hoạt động của hệ thống
  - o Giám sát việc sử dụng voicemail
  - o Gỡ bỏ các unassigned directory number
  - o Thực hiện backup hệ thống thủ công
- 25% nội dung của chương trình trang bị kỹ năng hỗ trợ người dùng đầu cuối cho các "End User"
  - o Kiểm tra kết nối PSTN connectivity
  - o Xác định các lỗi phát sinh các end user gặp phải
  - o Khắc phục các vấn đề liên quan đến đầu cuối endpoint
  - o Nhận diện các lỗi phát sinh với voicemail và giải quyết các vấn đề liên quan đến user mailbox
  - o Mô tả nguyên nhân và triệu chứng chất lượng cuộc gọi
  - o Reset các thiết bị device
  - o Mô tả cách thức sử dụng các ứng dụng phone application

Khóa đào tạo 210-065 CIVND sẽ trang bị cho người học các kiến thức và kỹ năng triển khai các thiết bị đầu cuối Cisco Video endpoint trên hạ tầng Cisco video infrastructure. Bên cạnh đó, khóa học còn trang bị các kiến thức và kỹ năng triển khai và khắc phục các sự cố liên quan đến Cisco Unified Communication & Collaboration, TelePresence, và Digital Media Player trên kiến trúc hạ tầng giải pháp Cisco business video. Nội dung cụ thể của khóa đào tạo CIVND bao gồm các chủ đề sau:

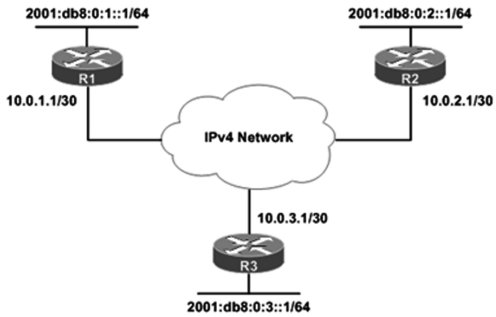
- 21% nội dung của chương trình giới thiệu các khái niệm "Video Concept", mô tả chức năng các thành phần của giải pháp video
  - o Provisioning & scheduling Management
  - o Video compositing
  - o Streaming video
  - o Recording & storage
  - o Media players

Để xem đầy đủ bài lab, mời các bạn truy cập vnpro.org

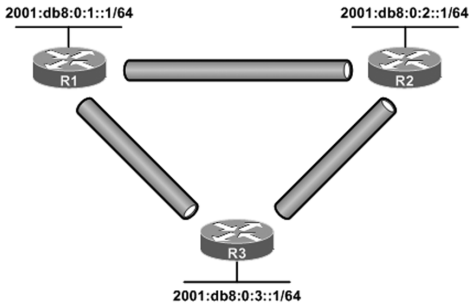
6to4 IPv6 Tunneling

"6to4 tunneling" là một cơ chế chuyển tiếp IPv6 được mô tả trong RFC 3056. Giống như nhiều cơ chế chuyển đổi khác, nó cho phép đóng gói các gói tin IPv6 thành IPv4 để lưu thông trên một mạng IPv4. Nói đơn giản 6to4 là cho phép biên dịch địa chỉ IPv6-to-IPv4 một cách tự động, và đối xử với các mạng IPv4 như một mạng lưới lớn Non-broadcast Multiaccess (NBMA), chứ không phải là một tập hợp các liên kết point-to-point độc lập.

Hãy xem hình bên dưới:



Có ba khu vực, mỗi khu có IPv6 LAN riêng của mình, được kết nối với nhau thông qua một IPv4 backbone. Một cách để kết nối đó là mạng LAN IPv6 sẽ được cấu hình point-to-point IPv6-in-IPv4 tunnels, mỗi khu vực sẽ có một cổng đường hầm cá nhân để đến được tất cả các khu còn lại.



Một giải pháp hiệu quả hơn sẽ tự động đào đường hầm 6to4. 6to4 hoạt động bằng cách tận dụng một IPv6 prefix, 2002 :: / 16. Một cổng 6to4 tunnel sẽ tự động chuyển đổi 32 bit trong địa chỉ IPv6 của nó sau prefix này đến một địa chỉ global unicast IPv4 để lưu thông trên một mạng IPv4 như Internet công cộng.

Cấu hình 6to4

Để cấu hình một đường hầm 6to4, đầu tiên chúng ta cần phải tạo ra một cổng tunnel trên mỗi edge router dual-stack. Có ba thành phần quan trọng có liên quan đến 6to4:

- The tunnel mode (6to4)
- The tunnel source (cổng hoặc địa chỉ IPv4)
- The 6to4 IPv6 address (2002 :: / 16)

Trên R1, mình tạo ra các cổng tunnel, cấu hình là 6to4, và chỉ định cổng IPv4 của nó là tunnel source:

```
R1(config)# interface tunnel0
R1(config-if)# tunnel mode ipv6ip 6to4
R1(config-if)# tunnel source 10.0.1.1
```

Để xác định các địa chỉ IPv6 của cổng tunnel, chúng ta chuyển đổi địa chỉ IPv4 source address sang IPv6 hexa, từ 10.0.1.1 thành 0a00: 0101. Sau đó chúng ta nối nó với các 6to4 prefix (2002 :: / 16), và điền vào phần còn lại của địa chỉ bằng số 0. Host masks (/ 128) được sử dụng cho các địa chỉ 6to4 trong bài này, mặc dù độ dài prefix lengths khác (và các địa chỉ trong / 48) có thể được sử dụng tốt hơn.

```
R1(config-if)# ipv6 address 2002:a00:101::/128
```

Quá trình này được lặp đi lặp lại để tạo ra các cổng tunnel 6to4 cho hai khu vực khác. Chỉ có một cổng tunnel duy nhất cho mỗi router.

```
R2(config)# interface tunnel0
R2(config-if)# tunnel mode ipv6ip 6to4
R2(config-if)# tunnel source 10.0.2.1
R2(config-if)# ipv6 address 2002:a00:201::/128
```

```
R3(config)# interface tunnel0
R3(config-if)# tunnel mode ipv6ip 6to4
R3(config-if)# tunnel source 10.0.3.1
R3(config-if)# ipv6 address 2002:a00:301::/128
```

Lưu ý rằng, không giống như khi cấu hình point-to-point tunnels, chúng ta không chỉ định bất kỳ địa chỉ tunnel destination nào.

Bây giờ địa chỉ 6to4 của mỗi router đã được biết đến, chúng ta có thể quay trở lại và thêm các static routes cần thiết để đạt được kết nối IPv6 giữa cả ba khu. 3 đường static routes phải được thêm vào mỗi router. Việc đầu tiên chỉ ra rằng 2002 :: / 16 là có thể đi ra các cổng Tunnel0. 2 khu còn lại là các đường route cho các /64 prefixes vào một trong các khukhác, để được route qua đường hầm 6to4.

R1

```
ipv6 route 2002::/16 tunnel0
ipv6 route 2001:db8:0:2::/64 2002:a00:201::
ipv6 route 2001:db8:0:3::/64 2002:a00:301::
```

R2

```
ipv6 route 2002::/16 tunnel0
ipv6 route 2001:db8:0:1::/64 2002:a00:101::
ipv6 route 2001:db8:0:3::/64 2002:a00:301::
```

R3

```
ipv6 route 2002::/16 tunnel0
ipv6 route 2001:db8:0:1::/64 2002:a00:101::
ipv6 route 2001:db8:0:2::/64 2002:a00:201::
```

Tại thời điểm này, chúng ta cần phải có kết nối IPv6 trong mạng LAN IPv6 ở tất cả ba địa điểm:

```
R1# ping 2001:db8:0:2::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:2::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/31/56 ms
R1# ping 2001:db8:0:3::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:0:3::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/12/16 ms
```

mời các bạn xem thêm tại vnpro.org

Ethernet VPN - *Khả năng mở rộng Layer 2*

Giới thiệu

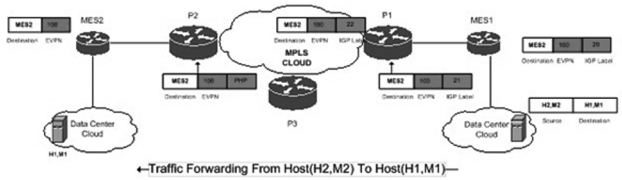
MPLS (Multi-Protocol Label Switching) là công nghệ tiên tiến và đã được chọn rộng rãi bởi hầu hết các nhà cung cấp dịch vụ trên toàn cầu. Ban đầu nó được triển khai cho các switch nhưng do khả năng mở rộng, khả năng phục hồi và giao thức tự nhiên bất khả tri đã làm cho nó thành công hơn trên mạng. VPLS (Virtual Private LAN Services) là một trong những dịch vụ trong MPLS giúp cung cấp các phần mở rộng của tên miền phát sóng từ một đến nhiều trang web trên WAN. VPLS trở nên phổ biến hơn sau khi bùng phát các liên kết nối trung tâm dữ liệu. Lý do hàng đầu đối với các phần mở rộng của lớp layer 2 là khối lượng công việc di chuyển (sự dịch chuyển của các máy ảo tới một trung tâm dữ liệu khác), tính sẵn sàng cao, và khả năng dự phòng địa lý.

Những thách thức hiện tại với VPLS

1. Mở rộng quy mô của hàng ngàn địa chỉ MAC (mỗi một mát ảo yêu cầu địa chỉ mac duy nhất): các ứng dụng ảo hóa đang thúc đẩy nhu cầu của Mac-address trong mạng. Một máy chủ duy nhất mà có thể lưu trữ hàng trăm máy ảo và mỗi máy tiêu thụ một địa chỉ mac cho thấy rõ yêu cầu mở rộng quy mô của bảng Mac-address.
2. Tối ưu forwarding của Multicast: Multicast LSP có thể được hình thành cùng với VPLS nhưng giới hạn từ point to multipoint trong đó tiêu thụ tài nguyên mạng hơn là không có định nghĩa thiết lập các thông số trong VPLS để tạo multipoint to multipoint LSPs multicast.
3. MultiHoming: VPLS hỗ trợ Active / standby BGP mô hình multi homing. MultiHoming với tất cả các mạch kèm theo hoạt động là điều không thể. Trong hợp đồng, khách hàng có thể sử dụng chỉ 50% trong các liên kết thay cho thanh toán 100%.
4. C-Mac (Customer Mac) Transparency: hiện tại giải pháp VPLS không hỗ trợ transparency các địa chỉ mac của khách hàng.
5. Fast Convergence for C-Mac Flushing: Trong trường hợp thất bại của các máy ảo hoặc máy chủ vật lý, mạng hội tụ sẽ xảy ra nhưng có thể dẫn đến các vấn đề làm ngập địa chỉ Mac.

Giải pháp đề xuất

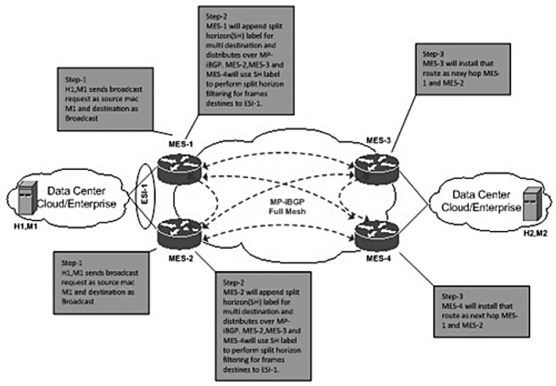
Ethernet Virtual Private Network (E-VPN) là giải pháp được đề xuất để khắc phục những vấn đề nổi bật của VPLS. E-VPN sử dụng các đường backbone MPLS / IP hiện có để vận chuyển các kết nối lớp 2 trong những trung tâm dữ liệu khác nhau cũng là một phần của cùng một VPN. Các giải pháp xử lý các địa chỉ Mac là địa chỉ route và sử dụng giao thức MP-iBGP hiện có để vận chuyển các địa chỉ Mac của khách hàng. Trong E-VPN, việc học Mac tại các router biên (edge routers) không xảy ra trong dữ liệu nhưng trong những kết quả điều khiển kiểm soát nhiều hơn có thể được áp dụng cơ chế này. Quá trình này cũng tương tự như các IPVPN như đã đề cập trong chuẩn RFC 4364. Các thuộc tính chính sách quy định tại E-VPN là gần như tương tự trong MPLS VPN. RD và RT vẫn giữ nguyên, nhưng thay vì chuyển tiếp định tuyến ảo giờ dây chúng ta có Ethernet VPN Instance. Các thông tin về Ethernet TAG của EVI được quảng cáo bởi BGP NLRI đó là E-VPN.



Trong EVPN, việc học Mac có hai loại: 1. Local Mac Learning. 2. Remote Mac Learning. Trong quá trình học Local Mac, MPLS Edge Switch (MES) phải hỗ trợ quá trình học Local Mac thông qua các giao thức chuẩn. Một khi quá trình được hoàn tất, MES có thể quảng bá các nơi học địa chỉ mac tới các nút từ xa MES thông qua MP-iBGP. Quá trình này nhận được địa chỉ mac từ xa của khách hàng thông qua MP-iBGP gọi là quá trình Remote Mac learning.

Giải pháp cho MultiHoming và Tránh Layer 2 Loops trong EVPN

Ethernet Segment ID (ESI) được sử dụng khi thiết bị Customer Edge là multi home tới các MPLS Edge Switches khác nhau như thể hiện trong hình 2. Nó có MPLS BGP Label Extended community được sử dụng cho các thủ tục split horizon trong các tình huống MultiHoming. Như mô tả trong hình 2, host H1 có địa chỉ mac của M1. Nó sẽ gửi các yêu cầu broadcast đến MES-1 và MES2. MES-1 và MES-2 đã xác định rằng các yêu cầu đến từ Extended Segment ID-1, vì vậy trước khi nhân rộng các frames, MESs sẽ nối thêm một nhãn split horizon trên frames. Một khi nó được thực hiện, frames được trao đổi giữa các MESs. Tất cả Mess kiểm tra nhãn SH và nếu tìm thấy cùng ESI-1 được gắn trực tiếp, lưu lượng sẽ âm thầm được lượt bỏ vì một frame có nguồn gốc của một segment sẽ không được nhận bởi cùng một segment. Kỹ thuật này giúp tránh các vòng lặp loops trong các tình huống MultiHoming.



Lưu ý: - nhãn Split horizon chỉ được sử dụng cho unknown unicast, multicast và broadcast

Vai trò của Forwarder Designated

Theo hình 2, MES-3 và MES-4 sẽ nhận được các multi destination frames thông qua MP-iBGP cho segment cụ thể. Chỉ Forwarder Designated sẽ chuyển tiếp các frame tới segment cụ thể và Designated forwarder election được thực hiện bởi mỗi PE quảng bá ESI trong đường route BGP. Tất cả non-Designated Forwarder MES sẽ chặn cổng tương ứng đối với segment đó như thể hiện trong

mời các bạn xem thêm tại vnpro.org

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

CCNA Voice

Ưu đãi:
20% hv cũ
10% hv mới

MÙA HÈ SÔI ĐỘNG

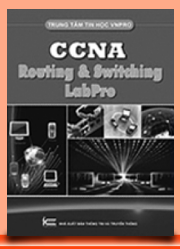
- ✳ *Quà tặng:*
  - *Lớp ngày: áo thun*
  - *Lớp đêm: balo*
- ✳ *Ưu đãi học phí:*
  - *20% học viên cũ, 10% học viên mới*

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

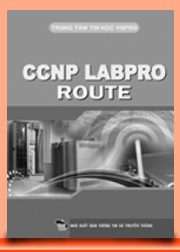
GIẢM* NGAY 10%



CCNA Routing & Switching
Giá: 220.000 VNĐ

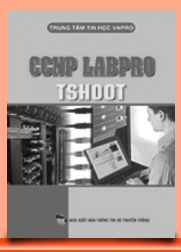
CCDA
Giá: 250.000 VNĐ

Ôn thi CCNA trong 24h
Giá: 120.000 VNĐ



CCNP LABPRO ROUTE
Giá: 120.000 VNĐ

CCNP LABPRO SWITCH
Giá: 120.000 VNĐ

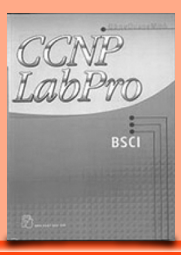


CCNP LABPRO TSHOOT
Giá: 120.000 VNĐ

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

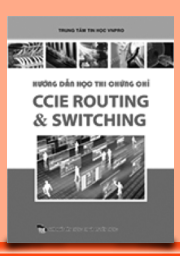
CCNP LABPRO ISCW
Giá: 120.000 VNĐ

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/***

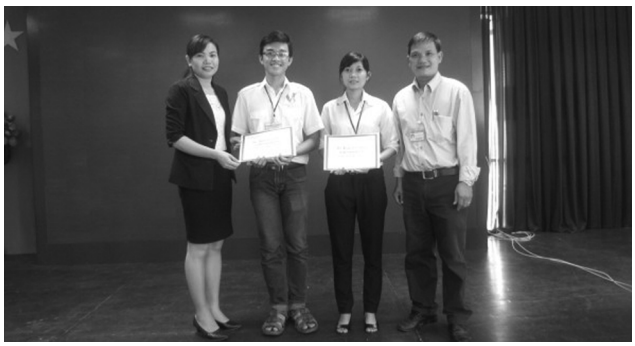
BẬT TUNG CẢM XÚC CÙNG SINH VIÊN KHOA *ĐÀO TẠO CHẤT LƯỢNG CAO – ĐH SPKT TP.HCM*

Ngày 26/06/2015 VnPro đã phối hợp cùng với Khoa đào tạo chất lượng cao trường Đại Học Sư Phạm Kỹ Thuật Tp. Hồ Chí Minh tổ chức hội thảo chuyên đề: ***"MẠNG TRUYỀN THÔNG – XU HƯỚNG TUYỂN DỤNG VÀ KỸ NĂNG TRONG XIN VIỆC".***

Hội thảo được tổ chức nhằm mục đích trang bị thêm cho các bạn sinh viên những kiến thức mới nhất trong lĩnh vực mạng máy tính và những xu hướng tuyển dụng cũng như là kỹ năng trong xin việc.

Chị Kim Thoa đại diện VnPro tặng hoa và quà lưu niệm cho Trưởng khoa CLC

Các bạn sinh viên lắng nghe chia sẻ từ các giảng viên VnPro



Chị Kim Thoa và thầy Ngô Lâm trao học bổng CCNAX cho 2 bạn sinh viên xuất sắc

VnPro chụp hình lưu niệm với thầy Bích và thầy Lâm

Hội thảo thật sự mang lại một giá trị không nhỏ cho hơn 100 bạn sinh viên đến tham dự chương trình. Đến với hội thảo lần này không những các bạn được trang bị thêm kiến thức chuyên môn còn có thêm những kinh nghiệm để chuẩn bị sang một trang mới của cuộc đời khi chính thức ra trường và đi làm. Ngoài ra VnPro còn dành tặng 2 suất học bổng cho 2 bạn sinh viên của khoa đã có những thành tích xuất sắc trong quá trình học tập cùng rất nhiều phần quà dành cho các bạn tham gia hội thảo.

Càng về cuối hội thảo không khí càng thêm sôi động. Với hàng loạt những câu hỏi dành cho các giảng viên của VnPro về kỹ năng trong xin việc và cách thức để chinh phục những nhà tuyển dụng khó tính.

Hội thảo kết thúc nhưng đã để lại những ấn tượng khó phai trong lòng các thầy cô và bạn sinh viên cũng như là ban tổ chức chương trình. Với những kiến thức và chia sẻ kinh nghiệm trong buổi hội thảo VnPro mong rằng đã góp thêm hành trang cho các bạn bước vào ngưỡng cửa mới của cuộc đời.

VnPro xin gửi đến đến Quý Thầy Cô và các bạn sinh viên lời cảm ơn chân thành và sâu sắc, chúc Quý Thầy Cô và các bạn sinh viên thành công hơn nữa trong công việc và trong cuộc sống.

HỌC VIÊN ĐỘI MƯA ĐẾN VNPRO ÔN TẬP ROUTE MIỄN PHÍ

Buổi ôn tập Route hoàn toàn miễn phí do trung tâm tin học VnPro tổ chức vào tối 18/06/2015 đã kết thúc tốt đẹp với số lượng đăng ký và tham gia rất đông.

Ôn tập Route là một trong những hoạt động được VnPro tổ chức hàng tháng nhằm hỗ trợ học viên ôn luyện lại tất cả các kiến thức cốt lõi nhất của chương trình CCNP – Route. Từ đó giúp các bạn học viên củng cố lại thật chắc kiến thức và đồng thời cũng bổ sung những phần cập nhật mới nhất của chứng chỉ CCNP để giúp các bạn tự tin đi thi quốc tế.

Đặc biệt: Các học viên tham gia khóa ôn tập còn được phát Voucher giảm giá 20% khi đăng ký học tại VnPro.

Theo khảo sát của VnPro sau khi kết thúc buổi ôn tập, có đến hơn 95% ý kiến cho rằng nội dung của buổi ôn tập rất thu hút và đúng nhu cầu hiện tại của học viên đang cần, và học viên cảm thấy rất hài lòng về buổi ôn tập này, mong muốn VnPro sẽ duy trì và thường xuyên tổ chức những buổi ôn tập như vậy.

Dưới đây là một số cảm nhận của học viên về buổi ôn tập do VnPro tổ chức:

* Công tác tổ chức chuẩn bị ôn tập rất tốt.

* Thầy giảng rất dễ hiểu, hướng dẫn quá nhiệt tình và trình bày rất chi tiết giúp học viên củng cố lại nền tảng kiến thức đã học.

* Thầy giảng trình bày đầy đủ kiến thức của chương trình, thu hút.

VNPRO ĐỒNG HÀNH SINH VIÊN CNTT "TỰ TIN CHINH PHỤC NHÀ TUYỂN DỤNG"

Sáng ngày 20/06, VnPro đã tổ chức buổi Hội Thảo "Tự Tin Chinh Phục Nhà Tuyển Dụng" với rất đông các bạn sinh viên tham gia.

Nằm trong chuỗi hội thảo "Vì Cộng Đồng Mạng Máy Tính Việt Nam lớn mạnh cả về chất và lượng". VnPro đã tổ chức buổi hội thảo "Tự Tin Chinh Phục Nhà Tuyển Dụng" với mục đích giúp các sinh viên có thêm nhiều kinh nghiệm và tự tin hơn khi đi xin việc. Trước ngưỡng cuộc đời, các sinh viên không tránh khỏi những nỗi lo lắng về tương lai sau khi tốt nghiệp đại học với hàng loạt những câu hỏi và thách thức được đặt ra: Phải bắt đầu từ đâu, cần phải rèn luyện thêm kĩ năng gì, nên xin việc ở công ty nào, làm sao để có được một CV đẹp cho nhà tuyển dụng, cần chuẩn bị gì cho những cuộc phỏng vấn.

Tham dự hội thảo có:

* Bà ***Trần Ngọc Trân*** diễn giả chuyên đề về phỏng vấn tuyển dụng với Jobstreet.com, các trường đại học.

* Ông ***Phạm Hoàng Tuân*** đại diện tuyển dụng nhân sự từ VnPro.

* Cùng hơn 40 sinh viên đến từ các trường đại học cao đẳng.

Diễn giả Trần Ngọc Trân
chia sẻ kinh nghiệm tuyển dụng với sinh viên

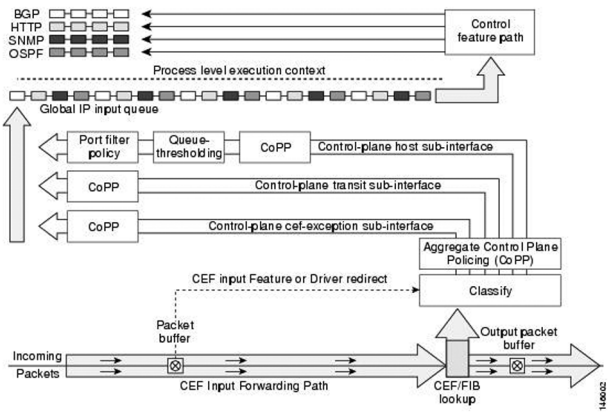
Thầy Phạm Hoàng Tuân
chia sẻ về những kinh nghiệm trong lựa chọn công việc

Rất nhiều các thắc mắc từ các sinh viên đã được các diễn giả giải đáp cặn kẽ: Doanh nghiệp cần gì ở sinh viên tốt nghiệp, làm thế nào để thực tập hiệu quả, cơ hội việc làm cho ngành công nghệ thông tin, cách giải quyết những câu hỏi khó khi phỏng vấn… Bằng cách này, Hội thảo đã xây dựng được mối tương tác từ cả hai phía – diễn giả và thính giả; khiến cho Hội thảo không những trở nên cởi mở hơn với sự hưởng ứng nhiệt tình từ phía các sinh viên mà còn khẳng định những tác động tích cực của phần chia sẻ đối với họ.

Sau hơn 3 giờ, những câu hỏi của các sinh viên đã được các diễn giả chia sẻ và giải đáp một cách thỏa đáng, hi vọng các bạn sinh viên có thêm hành trang để tự tin bước vào xã hội và sẵn sàng ***"Tự Tin Chinh Phục Nhà Tuyển Dụng"!***

Kiểm soát lưu lượng quản lý mạng trên Router như thế nào?

Figure 1 Control-plane Architecture with Control Plane Protection



Như các bạn có thể nhìn thấy từ biểu đồ trên, áp dụng một control-plane policy (Copp) áp dụng một policer tổng hợp cho tất cả traffic truy cập dành cho các CPU. Các bạn có thể nhìn thấy ba sub-interfaces của control-plane:

* Host - host sub-interface xử lý traffic dành cho các router hoặc một trong các interface riêng của mình. IE: Mgmt liên quan đến traffic và một số giao thức định tuyến. (EIGRP iBGP)
* Transit - sub-interface này xử lý switched IP traffic.
* CEF-Exception - sub-interfaces điển hình xử lý non-IP như ARP, LDP, Layer 2 keepalives cùng với một số giao thức định tuyến. (OSPF eBGP).

Đầu tiên chúng ta sẽ tạo ra một vài ACL để phù hợp với traffic:

```
!
ip access-list extended Mgmt_Stuff
 permit udp any any eq snmp
 permit tcp any any eq 22
ip access-list extended Route_Proto
 permit ospf any any
 permit tcp any any eq bgp
 permit tcp any eq bgp any
!
```

Đưa các ACL này vào Class-Map:

```
class-map match-all CM_Mgmt
 match access-group name Mgmt_Stuff
class-map match-all CM_Route_Prot
 match access-group name Route_Proto
!
```

Bây giờ, chúng ta tham khảo các Class-Maps trong Policy-Map:

```
policy-map PM_Mgmt
 class CM_Mgmt
  police 10000 2000 conform-action transmit  exceed-action drop  violate-action drop
policy-map PM_Route_Prot
 class CM_Route_Prot
  police 8000 2000 conform-action transmit  exceed-action transmit  violate-action transmit
!
```

Cuối cùng chúng ta áp dụng một service-policy liên quan đến Policy-Map vừa tạo.

```
policy-map CoPP_Agg
 class CM_Mgmt
  police 10000 2000 conform-action transmit  exceed-action drop  violate-action drop
 class CM_Route_Prot
  police 8000 2000 conform-action transmit  exceed-action transmit  violate-action transmit
```

```
Rack1R2(config)#control-plane
Rack1R2(config-cp)#serv
Rack1R2(config-cp)#service-policy in
Rack1R2(config-cp)#service-policy input  CoPP_Agg
Rack1R2(config-cp)#
Rack1R2(config-cp)#
*Mar 17 05:04:19.951: %CP-5-FEATURE: Control-plane Policing feature enabled on Control plane aggregate path
```

Người biên dịch: Phan Thanh Phong.

Làm thế nào hành xử lưu lượng broadcast trên Cisco router?

Chúng ta có 2 loại địa chỉ IP broadcast address:
- All subnets broadcast IP (255.255.255.255)
- Directed broadcast - specific subnet broadcast IP (e.g. 10.0.12.255 for 10.0.12.0/24 subnet).

1. Directed broadcast:

Ta tiến hành ping từ R1 đến 10.0.23.255. Vì R2 được kết nối trực tiếp đến subnet 10.0.23.0/24, sẽ trả lời đến echo thông qua echo reply nhưng sẽ không chuyển tiếp các gói tin ICMP trên link Fa0/1 hướng tới R3. R3 sẽ không bao giờ có được nó.

Debug IP packet từ R1 sau khi ping:

```
R1# ping 10.0.23.255 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.0.23.255, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 60/60/60 ms
R1#
*Mar 1 00:24:54.467: IP: tableid=0, s=10.0.12.1 (local), d=10.0.23.255 (FastEthernet0/0), routed via FIB
*Mar 1 00:24:54.471: IP: s=10.0.12.1 (local), d=10.0.23.255 (FastEthernet0/0), len 100, sending
*Mar 1 00:24:54.475: ICMP type=8, code=0
*Mar 1 00:24:54.515: IP: tableid=0, s=10.0.12.2 (FastEthernet0/0), d=10.0.12.1 (FastEthernet0/0), routed via RIB
*Mar 1 00:24:54.519: IP: s=10.0.12.2 (FastEthernet0/0), d=10.0.12.1 (FastEthernet0/0), len 100, rcvd 3
*Mar 1 00:24:54.523: ICMP type=0, code=0
```

Như bạn có thể nhìn thấy R1 hồi đáp lại R2.

Thêm câu lệnh no ip directed-broadcast vào Fa0 / 1 trên R2 và xem kết quả:

```
R2(config-if)#int fa0/1
R2(config-if)#no ip directed-broadcast
```

```
R1#ping 10.0.23.255 repeat 1
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.0.23.255, timeout is 2 seconds:
!
Success rate is 100 percent (1/1), round-trip min/avg/max = 36/36/36 ms
R1#
*Mar 1 00:03:56.839: IP: tableid=0, s=10.0.12.1 (local), d=10.0.23.255 (FastEthernet0/0), routed via FIB
*Mar 1 00:03:56.843: IP: s=10.0.12.1 (local), d=10.0.23.255 (FastEthernet0/0), len 100, sending
*Mar 1 00:03:56.847: ICMP type=8, code=0
*Mar 1 00:03:56.863: IP: tableid=0, s=10.0.12.2 (FastEthernet0/0), d=10.0.12.1 (FastEthernet0/0), routed via RIB
*Mar 1 00:03:56.867: IP: s=10.0.12.2 (FastEthernet0/0), d=10.0.12.1 (FastEthernet0/0), len 100, rcvd 3
*Mar 1 00:03:56.871: ICMP type=0, code=0
*Mar 1 00:03:56.931: IP: tableid=0, s=10.0.23.3 (FastEthernet0/0), d=10.0.12.1 (FastEthernet0/0), routed via RIB
R1#
*Mar 1 00:03:56.935: IP: s=10.0.23.3 (FastEthernet0/0), d=10.0.12.1 (FastEthernet0/0), len 100, rcvd 3
*Mar 1 00:03:56.939: ICMP type=0, code=0
```

Như các bạn có thể nhìn thấy, R1 hồi đáp lại từ R2 và R3:

Kiểm tra trên R2 và R3:

```
R2#*Mar 1 00:10:16.995: IP: tableid=0, s=10.0.12.1 (FastEther-
net0/0), d=10.0.23.255 (FastEthernet0/1), routed via RIB
*Mar 1 00:10:16.999: IP: s=10.0.12.1 (FastEthernet0/0),
d=10.0.23.255 (FastEthernet0/1), g=255.255.255.255, len 100,
forward directed broadcast
*Mar 1 00:10:17.007: ICMP type=8, code=0
```

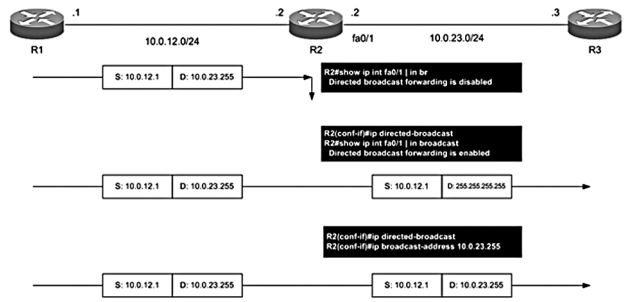
```
R3#*Mar 1 00:07:20.491: IP: s=10.0.12.1 (FastEthernet0/1),
d=255.255.255.255, len 100, rcvd 2
*Mar 1 00:07:20.495: ICMP type=8, code=0
*Mar 1 00:07:20.499: IP: tableid=0, s=10.0.23.3 (local),
d=10.0.12.1 (FastEthernet0/1), routed via FIB
*Mar 1 00:07:20.499: IP: s=10.0.23.3 (local), d=10.0.12.1
```

Các bạn có thể thấy ip directed-broadcast thay đổi destination directed broadcast address (10.1.23.255) cho tất cả subnet broadcast 255.255.255.255.

```
R2#show run int fa0/1
interface FastEthernet0/1
 ip address 10.0.23.2 255.255.255.0
 ip broadcast-address 10.0.23.255
 ip directed-broadcast
```

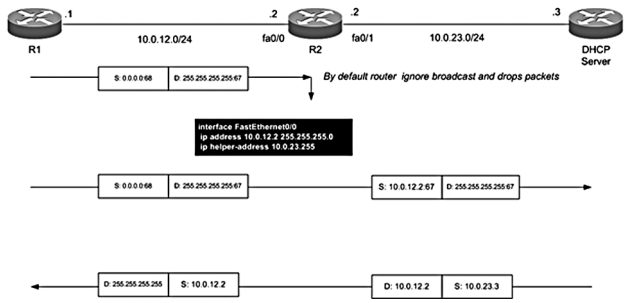
R3 bắt gói ICMP packet directed tới subnet broadcast 10.0.23.255:

```
R3#*Mar 1 00:41:35.391: IP: s=10.0.12.1 (FastEthernet0/1),
d=10.0.23.255 (FastEthernet0/1), len 100, rcvd 3
*Mar 1 00:41:35.395: ICMP type=8, code=0
```



2. Subnets broadcast:

Ví dụ: Thông điệp đầu tiên được gọi là DHCP Discovery được gửi đến địa chỉ broadcast 255.255.255.255. Mặc định router sẽ bỏ qua gói tin này và drop bỏ. Để xử lý được nó và gửi như một unicast IP tới đích cuối cùng, chúng ta phải sử dụng lệnh ip helper-address tại interface Fa0 / 0 trên R2.



Người biên dịch: Phan Thanh Phong.

Ấn định chiều dài tối thiểu của password trên Router?

Lệnh "security passwords min-length <x>" là một lệnh hạn chế sử dụng local password ngắn hơn "<x>". Đây là một nỗ lực rõ ràng để buộc các admin vào việc tạo local password an toàn hơn trên Router và Switch. Lệnh này không giải quyết các yêu cầu phức tạp (trường hợp hỗn hợp, ký tự đặc biệt, vv) mà thường để đáp ứng một tổ chức bảo mật tốt nhất.

```
Router(config)#security passwords min-length ?
Minimum length of all user/enable passwords
Router(config)#security passwords min-length
```

Để kiểm tra, mình sẽ bắt đầu bằng cách kích hoạt "service password-encryption" và tạo mật khẩu "cisco". Như đã thấy dưới đây, IOS yêu cầu sử dụng một mật khẩu thay thế cho "enable password".

```
Router(config)#service password-encryption
Router(config)#enable secret cisco
Router(config)#enable password cisco
The enable password you have chosen is the same as your
enable secret.
This is not recommended.  Re-enter the enable password.
Router(config)#enable password cisco1
Router(config)#username test1 password cisco
Router(config)#username test2 secret cisco
Router(config)#line vty 0 15
Router(config-line)#password cisco

Router(config-line)#do show run
| inc vty|username|enable|password
service password-encryption
enable secret 5 $1$J3j1$kDafwbNSYVLpmYqLXYA/F1
enable password 7 00071A1507545A
username test1 password 7 01100F175804
username test2 secret 5 $1$oP2E$NZWtTscYAIhlZk5KF.I/y.
line vty 0 4
 password 7 104D000A0618
line vty 5 15
 password 7 104D000A0618
```

Cấu hình password có chiều dài tối thiểu là 8 ký tự.

```
Router(config)#security passwords min-length 8
Router(config)#
Router(config)#do telnet 192.0.2.1
Trying 192.0.2.1 ... Open
User Access Verification
Password:
Router>en
Password:
Router#exit
[Connection to 192.0.2.1 closed by foreign host]
Router(config)#
```

Để xem đầy đủ bài lab, mời các bạn truy cập vnpro.org

7 kỹ năng mềm cần có của một người làm CNTT

Hầu hết mọi người nghĩ rằng với nghề công nghệ thông tin (CNTT), các kỹ năng như giải quyết vấn đề, giao tiếp và thuyết trình hiếm khi được xét tới thì trên thực tế đó là những kỹ năng phải có cho một người làm CNTT thành công.

Thuần thục các kỹ năng với máy tính và xử lý lỗi là một phần thiết yếu của một người làm việc trong lĩnh vực CNTT, nhưng nếu nghĩ như vậy là đủ thì bạn khó có thể tiến xa. Dưới đây là những kỹ năng mềm bạn nên luyện tập để trở thành một người chuyên nghiệp:

1. Xử lý sự cố

Khi bạn chịu trách nhiệm về những vấn đề như máy tính, mạng, phần mềm hoặc website, điều tối quan trọng là bạn phải biết cách xử lý các sự cố. Điều này có nghĩa là bạn phải biết cách phát hiện ra vấn đề cũng như phát triển các giải pháp một cách nhanh chóng. Kỹ năng xử lý sự cố không chỉ có nghĩa là "phản ứng lại" mà còn phải là "chủ động". Ví dụ, nếu một nhóm CNTT phát hiện ra một lỗ hổng an ninh trong công ty, họ phải biết cách tiến hành xử lý vấn đề cũng như nâng cấp hệ thống để phòng ngừa các nguy cơ an ninh chứ không chỉ chờ đến lúc công ty bị hack mới hành động.

2. Giao tiếp

Làm việc trong môi trường CNTT yêu cầu sự giao tiếp và tương tác gần như ngay tức thời. Bất cứ khi nào sự cố máy tính xảy ra, hoặc khi bạn quản lý một nhóm, bạn phải biết làm thế nào để tương tác và giao tiếp tốt với những người khác dù ở bất cứ cấp nào. Bạn cần biết cách trình bày và giải thích vấn đề rõ ràng, cùng những người khác tìm ra và thực hiện giải pháp, giao nhiệm vụ cho cả nhóm một cách hiệu quả.

3. Khả năng dịch thuật ngữ chuyên ngành

Khi làm việc trong lĩnh vực công nghệ, bạn sẽ bắt gặp nhiều thuật ngữ chuyên cho lĩnh vực mà bạn làm, thường thì những người ngoài ngành không thể hiểu được. Đó là lý do vì sao các kỹ sư CNTT chuyên nghiệp cần phải có kỹ năng giải thích các vấn đề phức tạp cho những người chỉ có một chút hoặc không hề biết gì về lĩnh vực CNTT. Nếu máy tính của một nhân viên bị lag vì anh này không có đủ RAM, người kỹ sư phải biết cách giải thích các vấn đề này để bất cứ ai cũng có thể hiểu được.

4. Làm việc nhóm

Để có một sự nghiệp thành công trong mảng CNTT, bạn phải biết cách làm việc với nhiều người. Dĩ nhiên, cũng có những dự án mà bạn đóng vai trò duy nhất từ đầu đến cuối, thế nhưng hầu hết các dự án đều cần sự hợp tác chặt chẽ của nhiều kỹ sư. Là một thành viên của nhóm CNTT, bạn cần biết cách lắng nghe người khác, nhận chỉ trích và hướng dẫn cũng như chịu trách nhiệm thực hiện mọi thứ một cách đúng đắn và đúng hẹn.

5. Thuyết trình

Làm việc trong lĩnh vực CNTT yêu cầu bạn phải có khả năng thuyết trình thoải mái và tự tin trước đám đông. Bất cứ khi nào bạn trình bày sản phẩm của nhóm mình cho một cấp cao hơn, giải thích điều gì đó mới cho mọi người trong bộ phận hoặc trình bày trong một buổi đào tạo, kỹ năng thuyết trình là rất quan trọng với những người chuyên nghiệp. Với tư cách là một người làm CNTT chuyên nghiệp, bạn được kỳ vọng có thể thuyết trình độc lập trong một buổi họp quan trọng mà không gặp phải vấp váp nào.

6. Kỹ năng chăm sóc khách hàng

Nghề CNTT yêu cầu bạn phải có khả năng giúp đỡ người khác ở mức cơ bản và đó là lý do vì sao bạn cần có kỹ năng chăm sóc khách hàng. Bạn cần giữ thái độ tích cực khi xử lý một vấn đề nào đó, dù đôi khi nó có kỳ cục và hiển nhiên đến thế nào, phải biết lắng nghe, thể hiện sự quan tâm, thông cảm. Bạn cũng phải biết cách "hạ nhiệt" khi có trục trặc xảy ra trong nhóm của mình.

7. Kiên nhẫn

Một phần quan trọng của nghề này đòi hỏi bạn phải giải thích các ý tưởng phức tạp cho người khác, đào tạo những người mới vào nghề hoặc hỗ trợ công nghệ mới cho những người chỉ biết đôi chút về CNTT. Những thứ này đều đòi hỏi bạn phải hết sức kiên nhẫn và khi bạn đủ kiên nhẫn để luôn bình tĩnh dù trong những trường hợp "ức chế" thế nào, hoặc có thể trả lời đi trả lời lại một câu hỏi mà không nổi cáu thì bạn có hi vọng tiến xa trong ngành.

10 DẤU HIỆU CHO THẤY MÁY TÍNH BỊ NHIỄM VIRUS

Việt hóa bởi: Xuân Dung Phạm

1

Máy hoạt động chậm, ì ạch

2

Không phản hồi khi nhấp chuột vào icon, các phần mềm không hoạt động chính xác

3

Hệ thống tự khởi động lại, đứng máy hoặc bị lỗi không rõ nguyên nhân

4

Phần mềm diệt virus, tường lửa đột nhiên bị vô hiệu hóa

5

Không thể truy cập vào driver và ổ cứng

6

Bỗng nhiên không in được

7

Xuất hiện cửa sổ pop-up báo có virus hoặc dấu hiệu bị nhiễm virus (chương trình lạ, không thể tắt cửa sổ)

8

Bỗng nhiên các cửa sổ pop-up quảng cáo xuất hiện nhiều lần

9

Gặp trục trặc khi cài đặt hoặc tải chương trình chống virus hoặc các phần mềm khác về máy

10

Bỗng nhiên bị mất các icon trên desktop và/hoặc tất cả các tập tin chương trình khác trong các thư mục

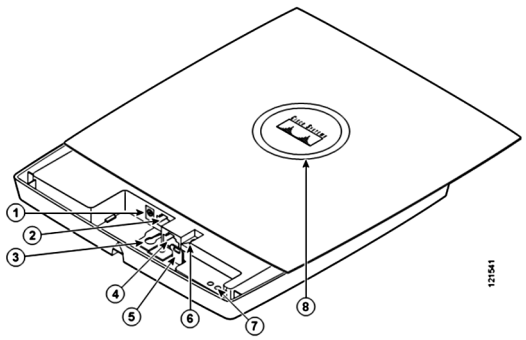
LabPro Wireless: Cấu hình Access Point 1130AG của Cisco

Yêu cầu:

- Giới thiệu sơ lược về Access Point Aironet 1130AG.
- Cấu hình các Access Point tạo ra các SSID. Cho các AP hoạt động cùng kênh ở chuẩn B để kiểm tra nhiễu đồng kênh (co-channel). Kiểm tra chất lượng tín hiệu.

Thực hiện:

1. Giới thiệu sơ lược về AP 1130AG

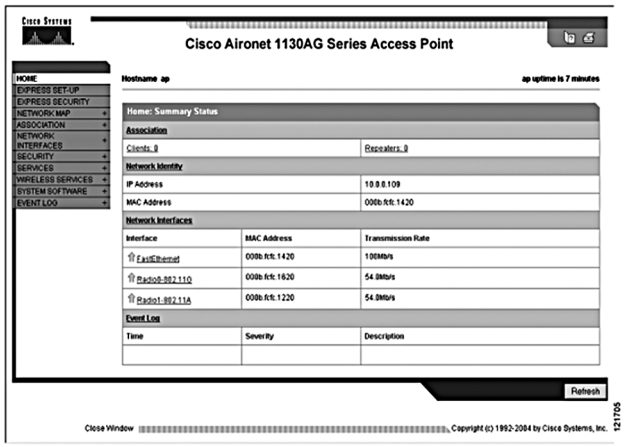


1	Power connector	5	Padlock por
2	Ethernet port	6	Mode button
3	Keyhole port	7	Ethernet (E) and Radio (R) LEDs
4	Console port	8	Status LED

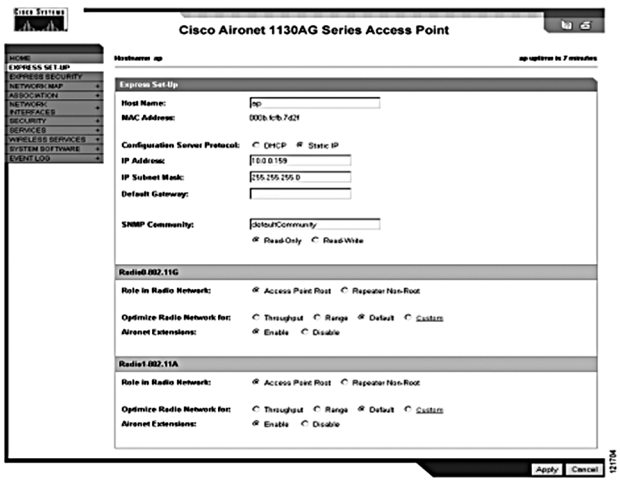
AP 1130AG có 2 anten dipole tích hợp bên trong, một cho chuẩn 802.11b/g (interface dot11 radio 0) và một cho chuẩn 802.11a (interface dot11 radio 1). Lưu ý: kiểu đánh số thứ tự cho các interface radio này giống nhau trên tất cả các AP 802.11a/b/g của Cisco.
AP 1130AG hỗ trợ 2 kiểu cấu hình: CLI (command line) và WEB.

2. Cấu hình basic bằng giao diện WEB

Trước khi có thể cài đặt cấu hình basic, AP và PC phải có địa chỉ IP (để có địa chỉ IP của AP xem phần gán địa chỉ IP sử dụng CLI).
Các bước để cấu hình cơ bản cho AP 1130 sử dụng GUI Express Setup.
Bước 1: Mở trình duyệt và gõ địa chỉ của AP vào thanh tác vụ địa chỉ. Một màn hình username và password xuất hiện.
Bước 2: Gõ username Cisco và password Cisco. Username và password có phân biệt chữ hoa, thường.
Bước 3: Nhấn Enter. Trang Summary Status xuất hiện.



Bước 4: Click Express Setup. Trang Express Setup xuất hiện.



Bước 5: Cấu hình các cài đặt sử dụng những hướng dẫn sau

Host name

- Tên hệ thống là một tên của AP để nhận dạng nó trên mạng
- **Mặc định**: ap

Configuration Server Protocol

- Chỉ ra cách mà AP lấy địa chỉ IP.
- **Tùy chọn**: DHCP và static IP
- **Mặc định**: DHCP

IP Address, IP Subnet Mask

- Gán hoặc thay đổi địa chỉ IP kèm subnet mask của AP. Nếu DHCP được cho phép, AP lấy địa chỉ từ DHCP server. Bạn có thể gán địa chỉ IP tĩnh trong phần này.

Default Gateway

- Xác định địa chỉ AP sử dụng để truy cập vào 1 mạng khác. Gateway này được cung cấp bởi người quản trị mạng. Nếu DHCP được cho phép, để trống phần này.

Web Server

- Cài đặt này chỉ ra kiểu HTTP được sử dụng để truy cập AP thông qua trình duyệt WEB.
- **Tùy chọn**: HTTP chuẩn hoặc HTTPS
- **Mặc định**: HTTP chuẩn

SNMP Community

- Xác định và cài đặt những thuộc tính cho giao thức quản lý mạng đơn giản (SNMP) được dùng để quản lý mạng mà AP trực thuộc.

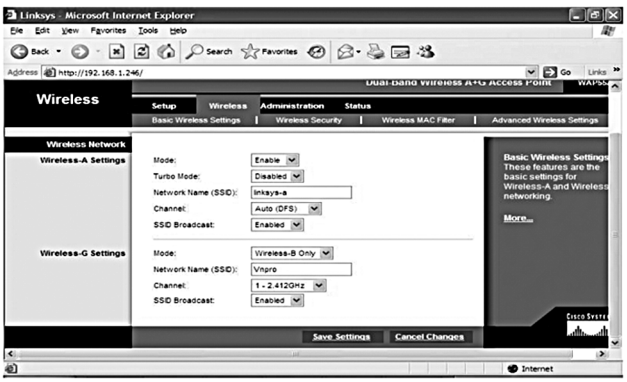
Thuộc tính	Mô tả
Read – Only	AP chỉ cho phép truy cập đọc
Read – Write	AP cho phép truy cập đọc và đọc ghi

Radio 802.11G and 802.11A Setup Sections
Role in Radio Network
- Cài đặt này xác định chức năng của AP trong mạng không dây
- **Tùy chọn**: AP root hoặc Repeater nonroot
- **Mặc định**: AP root

Optimize Radio Network for
- Cài đặt này tối ưu hóa hoạt động của AP trong môi trường không dây bằng cách hiệu chỉnh tốc độ dữ liệu. **Cài đặt này phải giống nhau trên các client.**
- **Tùy chọn**: Throughput, Range, Default, Custom
- **Mặc định**: Default

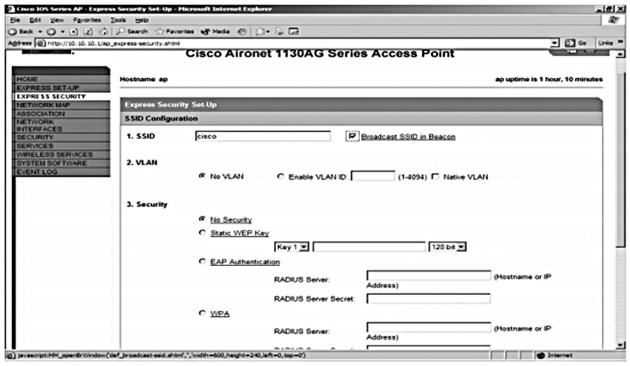
3. Cấu hình basic bằng CLI
Kết nối tới AP bằng cáp console.
Bước 1: Mở nắp đậy AP
Bước 2: Dùng cáp nối tiếp DB-9 to RJ-45 (9 chân, female) nối port nối tiếp RJ-45 trên AP đến cổng COM trên PC.
Bước 3: Dùng Hyper Terminal với các thông số mặc định để giao tiếp với AP: 9600 baud, 8 bit dữ liệu, không dùng parity, 1 bit stop và không có điều khiển luồng. Truy cập vào AP với username Cisco, password Cisco.
Bước 4: Gán địa chỉ IP cho AP sử dụng CLI
ap#conf t ap(config)#interface BVI 1
ap(config-if)#ip address 10.0.0.2 255.0.0.0
Bước 5: Sử dụng CLI, ta có thể cài đặt tất cả các cấu hình cơ bản (và nâng cao) như khi sử dụng giao diện WEB.

4. Kiểm tra chất lượng tín hiệu khi đặt các AP gần nhau và cấu hình cùng kênh truyền hoặc kênh truyền kế cận trong chuẩn B/G.
Cấu hình AP Linksys bằng giao diện WEB, tạo ra SSID VnPro, quảng bá SSID ra ngoài để PC detect thấy, AP hoạt động ở chuẩn B-only, kênh 1. Trên 2 AP Aironet làm tương tự, tạo ra các SSID Cisco và Microsoft, hoạt động ở chuẩn B-only, cũng kênh 1.
a. Cấu hình AP Linksys:

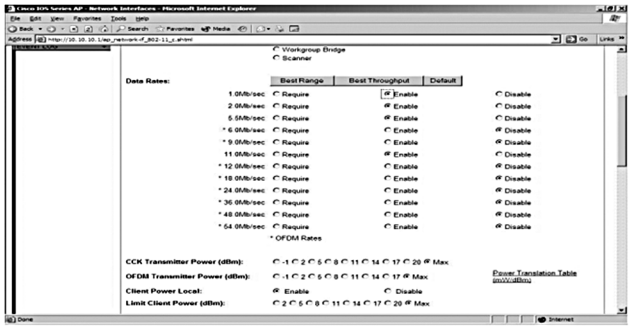


b. Cấu hình AP 1130:
Dùng CLI:
Bước 1: Tạo ra SSID trong configuration mode, chọn kiểu xác thực và quyết định có quảng bá SSID ra ngoài thông qua các beacon hay không:
ap#conf t ap(config)#dot11 ssid cisco
ap(config-ssid)#authentication open/* bật xác thực kiểu Open System */
ap(config-ssid)#guest-mode/ * quảng bá SSID trong các frame beacon */
Bước 2: Chỉ định SSID nào được kết hợp với interface Dot11Radio 0 hoặc 1, sau đó bật interface lên:
ap#conf t
ap(config)#interface dot11radio 0
ap(config-if)#ssid cisco /* cho SSID cisco kết hợp với interface dot11radio 0 */
ap(config-if)#no shut /* bật interface radio 0 lên */
Bước 3: Chọn tốc độ và kênh truyền cho các interface radio
ap(config)interface radio 0
ap(config-if)#speed basic-1.0 2.0 5.5 11.0
Lưu ý:
- Interface BVI (Bridge Virtual Interface) 1 chỉ là interface ảo được sử dụng cho mục đích quản trị AP (giống như vai trò của Interface VLAN 1 trong các switch layer 2 của Cisco).
- Các interface Radio, FastEthernet được cấu hình theo kiểu bridging. AP có chức năng giống như hub trong mạng có dây nên các interface Radio và FastEthernet phải được cấu hình bridge.

Dùng WEB:
Tạo SSID và cho quảng bá SSID trong Beacon.



Chỉ cho AP hoạt động ở chuẩn B (dùng các tốc độ dữ liệu 1, 2, 5.5, và 11 Mbps)



Để xem đầy đủ bài lab, mời các bạn truy cập vnpro.org

LỊCH KHAI GIẢNG THÁNG 7

Mã Lớp	Tên khoá học	Ngày khai giảng	Ngày Học	Giờ Học	Học phí/Khoá	Thời gian
CHƯƠNG TRÌNH CCNA						
AK26	**CCNAX** (200-120)	06/07	2 – 4 – 6	8:30 – 11:30AM	3.360.000	152 giờ
A26				6:30 – 9:30PM	6.720.000	
AK27		09/07	3 – 5 – 7	8:30 – 11:30AM	3.360.000	
AK29				2:00 – 5:00PM	3.360.000	
A27				6:30 – 9:30PM	6.720.000	
AK28		17/07	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
AK30				2:00 – 5:00PM	3.360.000	
A28				6:30 – 9:30PM	6.720.000	
AK31		28/07	3 – 5 – 7	8:30 – 11:30AM	3.360.000	
AK33				2:00 – 5:00PM	3.360.000	
A29				6:30 – 9:30PM	6.720.000	
AK31	**CCNAX Hè**	15/07	2-3-4-5-6	2:00 – 5:00PM	2.900.000	
AS3	**CCNA Security** (640-554)	21/07	3 – 5 – 7	6:30 – 9:30PM	6.720.000	100 giờ
AV4	**CCNA Voice (640-461)**	22/07	2 - 4 - 6	2:00 – 5:00PM	6.720.000	100 giờ
AV6				6:30 – 9:30PM	6.720.000	
CHƯƠNG TRÌNH CCNP						
P1K6	**ROUTE** (300 - 101)	07/07	3 – 5 – 7	8:30 – 11:30AM	~~6.600.000~~ 5.900.000	140 giờ
P1-7				6:30 – 9:30PM	9.800.000	
P1K8		15/07	2 – 4 – 6	2:00 – 5:00PM	6.600.000	
P1-8				6:30 – 9:30PM	9.800.000	
P2K4	**SWITCH** (300 - 115)	22/07	2 – 4 – 6	8:30 – 11:30AM	5.880.000	120 giờ
P2K6				2:00 – 5:00PM	5.880.000	
P2-4				6:30 – 9:30PM	8.232.000	
P3-5	**TSHOOT** (300 - 135)	21/07	3 – 5 – 7	6:30 – 9:30PM	9.800.000	140 giờ
CHƯƠNG TRÌNH CCIE WRITTEN						
EW3	**CCIE WRITTEN** (Version 5)	28/07	3 – 5 – 7	6:30 – 9:30PM	11.760.000	120 giờ

ĐĂNG KÝ NGAY

Lê Uyên — **Email: tranleuyen@vnpro.org** — **Mobile: 0903 834 636**
Thanh Trâm — **Email: thanhtram@vnpro.org** — **Mobile: 0949 246 829**

LIÊN HỆ DỰ ÁN - TƯ VẤN HỆ THỐNG MẠNG - THUÊ THIẾT BỊ PHÒNG HỌC - MUA SÁCH

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

Bản tin Dân Cisco - Được phát hành bởi **Công Ty TNHH Tư Vấn & Dịch Vụ Chuyên Việt**
Chịu trách nhiệm xuất bản: **Nguyễn Cảnh Hoàng**
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**