Số 30
07/2014

BẢN TIN dancisco

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

GIỚI THIỆU CHỨNG CHỈ CCDA

Chứng chỉ CCDA (Cisco Certified Design Associate) nằm trong hệ thống chứng chỉ đào tạo của Cisco trang bị cho các kiến trúc sư hạ tầng mạng các kiến thức liên quan để có thể thiết kế, xây dựng hạ tầng mạng với ...

[Trang 02]

ƯU ĐÃI LỚN

[Trang 05]

CẤU HÌNH PRIVATE VLAN TRÊN CISCO 3560 SWITCH

Private-VLAN đem đến cho nhà cung cấp dịch vụ (service provider) hai lợi ích chủ yếu khi sử dụng VLAN:

1. Tính mở rộng (Scalability)
2. Cho phép cấu hình định tuyến IP routing ...

[Trang 03]

Nguy cơ bảo mật VLAN HOPPING

VLan hopping mô phỏng 1 kiểu tấn công mà các traffic bình thường không thể đi qua được các VLAN khác trong hệ thống...

[Trang 07]

10 QUY TẮC GIÚP BẠN ĐỌC SÁCH HIỆU QUẢ

Ngày nay, khi mà kiến thức được đăng tải rộng rãi khắp các kênh phương tiện thông tin đại chúng trên internet thì văn hoá ...

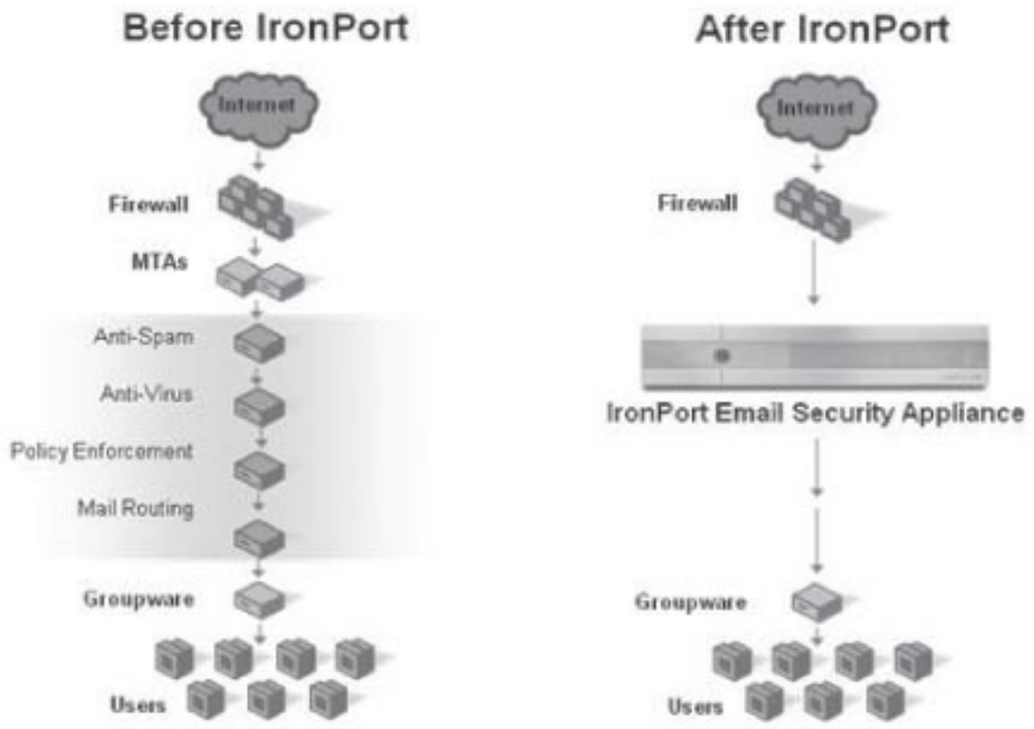
[Trang 08]

TIN TỨC SỰ KIỆN KHÁC

Giải pháp hội họp trực tuyến của Cisco

Cisco cung cấp giải pháp hội họp trực tuyến là Cisco TelePresence. Đối với giải pháp Cisco TelePresence, một máy chủ Cisco UCS server sẽ được triển khai trên hạ tầng mạng doanh nghiệp. Người dùng đầu cuối có thể tham gia cuộc họp bằng thiết bị đầu cuối là PC, máy tính bảng, smartphone cài chương trình Cisco Jabber hoặc thiết bị chuyên dụng của Cisco như Cisco TelePresence System 500, 1000, 1100, 3000, 3200 (được trang bị camera, màn hình, microphone) kết nối vào hạ tầng mạng doanh nghiệp.

Giải pháp bảo mật Cisco IronPort



Cisco IronPort là giải pháp chống thư rác (spam, spyware, phishing), chống virus, mã hóa email và hỗ trợ công cụ quản lý mạng. Cisco đã mua lại công ty IronPort System với giá là 830 triệu USD vào năm 2007. Hiện nay, Cisco IronPort tại Việt nam có các dòng sản phẩm sau:

- Ironport C160: Tích hợp đầy đủ các tính năng và dễ dàng sử dụng cho các doanh nghiệp vừa và nhỏ
- Ironport C360D: Dành cho các doanh nghiệp vừa với tính năng kiểm soát thư nâng cao
- Ironport C370: Dành cho các doanh nghiệp có quy mô từ vừa đến lớn
- Ironport C670: Được thiết kế cho các doanh nghiệp lớn và các nhà cung cấp dịch vụ
- Ironport X1070: Được xây dựng nhằm đáp ứng nhu cầu các mạng của nhà cung cấp lớn trên thế giới.

Cisco hợp tác với Copenhagen phát triển Internet of Thing

Trong tháng 6 vừa qua, Cisco đã tiến hành hợp tác với Copenhagen (Thủ đô của Đan Mạch) cùng các vùng lân cận Albertslund, Frederikssund để phát triển các giải pháp công nghệ Internet of Thing cho phép vận hành từ xa hệ thống thống chiếu sáng, bãi đậu xe và hệ thống năng lượng (điện, khí đốt) cho thành phố. Các nhà lãnh đạo cấp cao của thành phố Copenhagen đã lên kế hoạch Smart City project trong vài năm tới nhằm hiện đại hóa và giúp nâng cao chất lượng cuộc sống của cư dân thành thị. Nếu thành công, kế hoạch này sẽ được nhân bản sang các thành phố khác của Đan Mạch tương tự như sự thành công của các thành phố khác như Barcelona, Amsterdam, Hamburg, Chicago, Dallas, San Francisco, Songdo, Nice, Kansas.

Internet of Thing là xu hướng tất yếu của một thành phố hiện đại

Internet of thing (IoT) cho phép kết nối con người, dữ liệu và mọi thứ xung quanh chúng ta lại với nhau giúp xây dựng một xã hội tiện nghi hơn, đem lại nhiều lợi ích kinh tế cho doanh nghiệp và cộng đồng.

Nhờ IoT, hệ thống chiếu sáng ở Albertslund (một thành phố ở Đan Mạch) có thể được bật lên từ một vị trí tập trung hoặc tắt đi toàn bộ hệ thống, giúp sử dụng hiệu quả tối đa năng lượng chiếu sáng. IoT còn được sử dụng để vận hành hệ giống bãi đậu xe, hệ thống tưới nước công cộng, kiểm soát hệ thống lưới điện của các thành phố.

Kết hợp với các bộ cảm biến, IoT có thể được sử dụng để thu thập thông tin nhiệt độ, tiếng ồn, độ ẩm hay những nơi tập trung đông người ở như sân bay, trung tâm mua sắm giúp các nhân viên an ninh phân bố lực lượng túc trực hợp lý hơn.

Theo dự đoán, năm 2020 sẽ có đến 50 tỉ kết nối Internet để phục vụ cho xu hướng IoT.

Người dịch: Bùi Quốc Kỳ

Giới thiệu chứng chỉ CCDA

Chứng chỉ CCDA (Cisco Certified Design Associate) nằm trong hệ thống chứng chỉ đào tạo của Cisco trang bị cho các kiến trúc sư hạ tầng mạng các kiến thức liên quan để có thể thiết kế, xây dựng hạ tầng mạng với hiệu suất vận hành hệ thống tối ưu nhất. Đây là chứng chỉ mà rất nhiều công ty giải pháp hạ tầng mạng tại Việt Nam yêu cầu các ứng cử viên phải có. Nội dung kiến thức trong chương trình CCDA sẽ trang bị các kiến thức và kỹ năng lập kế hoạch và triển khai hạ tầng mạng trục campus, data center, security, voice, và hạ tầng mạng không dây (wireless network). Hiện nay, VnPro là trung tâm duy nhất tại thành phố Hồ Chí Minh xuất bản đầu sách "Hướng dẫn học và thi CCDA" liên quan đến chứng chỉ này.

Nội dung sách CCDA

Chương 1: PHƯƠNG PHÁP THIẾT KẾ HỆ THỐNG MẠNG

1.1. Những mô hình kiến trúc hạ tầng mạng doanh nghiệp

1.3. Thu thập thông tin về những yêu cầu phía doanh nghiệp đối với hạ tầng mạng

1.4. Phân tích, thu thập những đặc điểm hạ tầng mạng doanh nghiệp sẵn có

1.5. Thiết kế mô hình hạ tầng mạng, xây dựng giải pháp dựa trên những thông tin đã thu thập được.

Chương 2: MÔ HÌNH KIẾN TRÚC HẠ TẦNG MẠNG

2.1. Mô hình hệ thống mạng phân cấp

2.2. Mô hình kiến trúc mạng doanh nghiệp

2.3. Những dịch vụ hạ tầng mạng có tính sẵn sàng cao HA (High Availability)

Chương 3: THIẾT KẾ HỆ THỐNG MẠNG LAN TRONG DOANH NGHIỆP

3.1. Phương tiện truyền dẫn trong hệ thống mạng LAN sử dụng công nghệ Ethernet

3.2. Các nguyên tắc thiết kế mạng LAN 100-Mbps Fast Ethernet, 1000-Mbps Gigabit Ethernet, LAN 10-Gbps Ethernet

3.6. Thiết kế hệ thống mạng trục trong môi trường mạng LAN và các mô hình thực tiễn

3.7. Large-building LAN

3.8. Enterprise Campus LAN

3.9. Edge Distribution

3.10. Medium-Size LAN

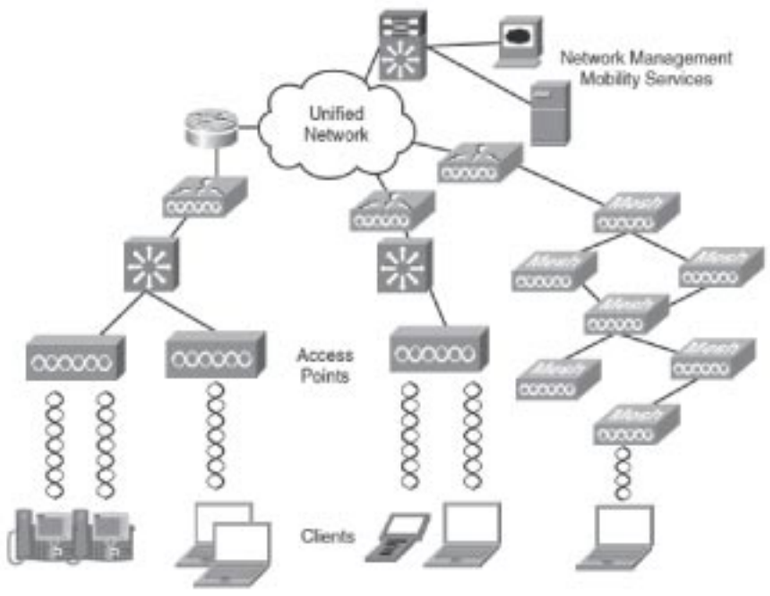
3.11. Small and Remote Site LAN

3.12. Server Farm Module

3.13. Enterprise Data Center Infrastructure

Chương 4: THIẾT KẾ HỆ THỐNG CƠ SỞ DỮ LIỆU TẬP TRUNG

4.1. Mô hình, các thành phần kiến trúc, topology hệ thống cơ sở dữ liệu tập trung



4.4. Những thách thức của hệ thống Data Center

4.5. Các thành phần và một số vấn đề cần quan tâm khi triển khai hệ thống Data Center

4.7. Cấp nguồn cho hệ thống Data Center

4.8. Làm mát hệ thống Data Center

4.9. Nhiệt lượng phát sinh từ hệ thống Data Center

4.10. Hệ thống cáp đấu nối của Data Center

4.11. Hạ tầng hệ thống Data Center doanh nghiệp

4.12. Tổng quan về công nghệ ảo hóa

4.13. Công nghệ ảo hóa server

4.14. Một số tiêu chí cần quan tâm khi thiết kế hệ thống mạng sử dụng công nghệ ảo hóa

Chương 5: THIẾT KẾ HỆ THỐNG MẠNG KHÔNG DÂY WIRELESS LAN

5.1. Các công nghệ mạng không dây Wireless LAN

5.2. Phương thức bảo mật WLAN

5.3. Kiểm soát truy cập kết nối từ hệ thống mạng không dây WLAN đến hệ thống các máy chủ

5.4. Hệ thống mạng không dây hợp nhất Cisco Unified Wireless Network

5.6. Các chế độ của AP.

5.7. Quá trình khám phá WLC thông qua giao thức LWAPP

5.8. Xác thực trong hệ thống mạng không dây WLAN

5.9. Các tùy chọn xác thực

5.10. Các thành phần điều khiển trong hệ thống mạng không dây WLAN.

5.13. Roaming và nhóm di động

5.14. Thiết kế hệ thống WLAN

5.16. Sử dụng đường hầm EoIP dành cho các dịch vụ khách Guest Service

5.17. Hệ thống mạng lưới mạng không dây triển khai ngoài trời

5.18. Thiết kế hệ thống mạng không dây tại chi nhánh

5.19. Tóm tắt các vấn đề cần lưu ý khi thiết kế mạng không dây WLAN

Chương 6: TỔNG QUAN VỀ HẠ TẦNG WAN

6.3. Các công nghệ vận chuyển trong WAN

6.4. WAN Design Methodology

Chương 7: CÁC CÔNG NGHỆ MẠNG WAN TRUYỀN THỐNG

7.1. Mô hình Hub-and-Spoke, Full-Mesh, Partial-Mesh

7.4. Thiết kế mạng truy cập từ xa, mạng VPN

7.6. So sánh VPN của doanh nghiệp và VPN của nhà cung cấp dịch vụ

7.10. Thiết kế dự phòng cho mạng WAN

7.11. Hướng dẫn cân bằng tải

7.12. Dự phòng WAN trong Internet

7.13. Kiến trúc mạng WAN cho doanh nghiệp

7.14. Thiết kế mạng chi nhánh.

7.15. Thiết kế chi nhánh nhỏ, vừa, lớn

7.18. Thiết kế mạng từ xa cho doanh nghiệp

Chương 8: INTERNET PROTOCOL VERSION 4

Chương 9: INTERNET PROTOCOL VERSION 6

Chương 10: ĐẶC ĐIỂM CỦA CÁC GIAO THỨC ĐỊNH TUYẾN RIP VÀ EIGRP

Chương 11: OSPF, ROUTE MANIPULATION VÀO IP MULTICAST

Chương 12: QUẢN LÝ BẢO MẬT HẠ TẦNG MẠNG

Chương 13: GIẢI PHÁP BẢO MẬT

13.1. Giải pháp bảo mật mạng nền tảng và Kiến trúc SAFE của Cisco

13.11. Tích hợp và Quản lý bảo mật mạng vào thiết bị mạng

13.15. Bảo vệ mạng doanh nghiệp

13.16. Triển khai bảo mật trong cơ sở và trong biên giới doanh nghiệp và WAN

Chương 14: THIẾT KẾ VOICE VÀ VIDEO

14.1. Kiến trúc truyền thống của mạng voice

14.2. Đánh số trong PSTN

14.3. Các dịch vụ PSTN khác

14.4. Các thuật ngữ trong kỹ thuật voice

14.5. Thiết kế mạng hội tụ đa dịch vụ

14.6. Triển khai video

14.7. Thiết kế mạng IPT

Chương 15: CÁC GIAO THỨC QUẢN LÝ HỆ THỐNG MẠNG

Cấu hình Private VLAN trên Cisco 3560 Switch

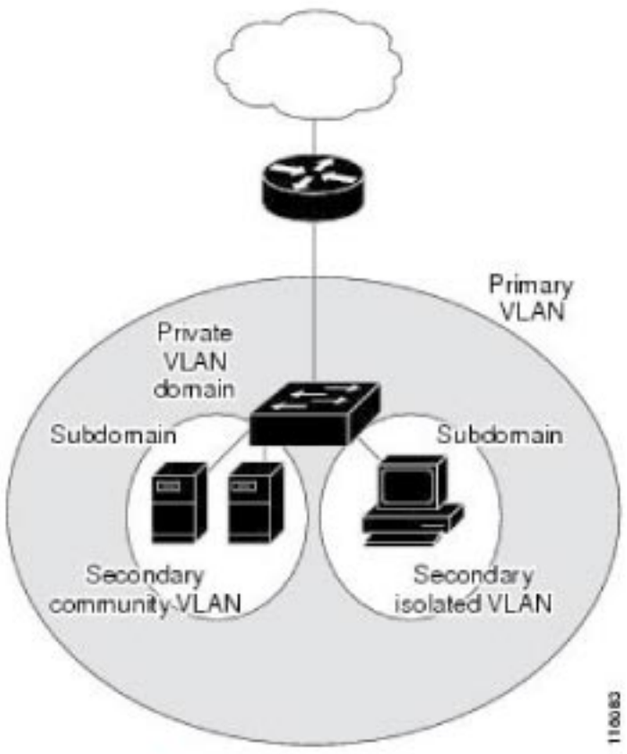
Private-VLAN đem đến cho nhà cung cấp dịch vụ (service provider) hai lợi ích chủ yếu khi sử dụng VLAN:

1. Tính mở rộng (Scalability): Thiết bị switch có thể hỗ trợ lên đến 1005 active VLAN. Nếu nhà cung cấp dịch vụ service provider quy hoạch mỗi một VLAN tương ứng với một khách hàng customer thì số lượng khách hàng mà nhà cung cấp dịch vụ có thể hỗ trợ sẽ rất hạn chế.

2. Cho phép cấu hình định tuyến IP routing: Mỗi VLAN thông thường sẽ được gom vào cùng một không gian địa chỉ mạng, điều này có thể gây ra tình trạng lãng phí đối với các địa chỉ IP không được sử dụng tới, đặc biệt là trong quá trình quản lý các IP.

Private VLAN giúp nhà cung cấp dịch vụ linh hoạt hơn khi mở rộng hệ thống mạng cũng như việc quản lý các địa chỉ IP được dễ dàng và thuận tiện hơn, và đồng thời cung cấp tính năng bảo mật tại lớp 2 đối với các khách hàng.

***Lưu ý**: Private VLAN giúp chia VLAN domain truyền thống thành các subdomain và có thể có nhiều cặp VLAN pair bên trong mỗi subdomain. Một subdomain thông thường sẽ bao gồm một primary VLAN và một secondary VLAN. Tất cả các VLAN pair trong private VLAN chia sẻ cùng một primary VLAN. Secondary VLAN ID trong mỗi subdomain sẽ khác biệt trong các subdomain khác.*



Có hai loại secondary VLAN:

Isolated VLAN—Các Port tham gia vào isolated VLAN không thể giao tiếp với các port khác vì chúng bị ngăn cách nhau ở Layer 2.

Community VLAN—Các Port bên trong một community VLAN có thể giao tiếp với nhau nhưng không thể giao tiếp với các port thuộc các community khác tạiLayer 2.

Private VLAN cung cấp khả năng cách lý ở mức độ Layer 2 đối với các port thuộc cùng private VLAN.

Các Private-VLAN port hoạt động ở chế độ access port bao gồm 3 loại sau:

Isolated port: là một host port tham gia vào isolated secondary VLAN. Port này hoàn toàn bị cách ly ở mức Layer 2 so với các port khác cùng private VLAN, ngoại trừ các promiscuous port. Private VLAN sẽ tiến hành khóa mọi lưu lượng tới isolated port ngoại trừ lưu lượng đến từ promiscuous port. Lưu lượng nhận được từ isolated port chỉ được forward tới promiscuous port.

Command: switchport mode private-vlan host

Community port: là một host port tham gia vào community secondary VLAN. Community port có thể truyền thông với các port khác trong cùng một community VLAN và giao tiếp với promiscuous port. Các interface này được cách ly ở mức độ Layer 2 với các interface thuộc các community khác và cách ly với các isolated port bên trong private VLAN.

Command: switchport mode private-vlan host

Promiscuous port: là port tham gia vào primary VLAN và có thể truyền thông với tất cả các loại interface còn lại, bao gồm cả community và isolated host port thuộc secondary VLAN liên kết tới primary VLAN.

Command: switchport mode private-vlan promiscuous

Các bước cấu hình Private VLAN

Bước 1 Thiết lập VTP mode ở chế độ transparent.

```
vtp mode transparent
```

Bước 2 Khởi tạo primary và secondary VLAN và liên kết chúng lại

```
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-502
```

Bước 3 Cấu hình các interface ở chế độ isolated hoặc community host port và gán vào VLAN tương ứng

```
Switch(config)# interface fastethernet0/22
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
```

Bước 4 Cấu hình các interface ở chế độ promiscuous port và liên kết promiscuous port tới primary-secondary VLAN pair

```
Switch# configure terminal
Switch(config)# interface fastethernet0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-502
Switch(config-if)# end
```

Các Cisco Switch hỗ trợ Private VLAN — Đầy đủ các tính năng (Community & Isolated VLAN):

1) Catalyst 6500/6000 – CatOS on Supervisor and Cisco IOS on MSFC 5.4(1) on Supervisor and 12.0(7)XE1 on MSFC
2) Catalyst 6500/6000 – Cisco IOS System software +12.1(8a)EX, 12.1(11b)E1
3) Catalyst 4500/4000 – CatOS + 6.2(1)
4) Catalyst 4500/4000 – Cisco IOS +12.1(8a)EW 12.2(20)EW(Community VLAN)
5) Catalyst 3560 + 12.2(20)SE – EMI
6) Catalyst 3750 + 12.2(20)SE – EMI
7) Catalyst 2948G/2980G + 6.2

Các Cisco Catalyst Switch hỗ trợ PVLAN Edge (Protected Port)

1) Catalyst 3550 + 12.1(4)EA1
2) Catalyst 2950 + 12.0(5.2)WC1, 12.1(4)EA1
3) Catalyst 2900XL/3500XL + 12.0(5)XU (on 8MB switches only)
4) Catalyst 3560 + 12.1(19)EA1
5) Catalyst 3750 + 12.1(11)AX
6) Catalyst 3750 Metro + 12.1(14)AX
7) Catalyst 2940 + 12.1(13)AY
8) Catalyst 2955
9) Catalyst 297

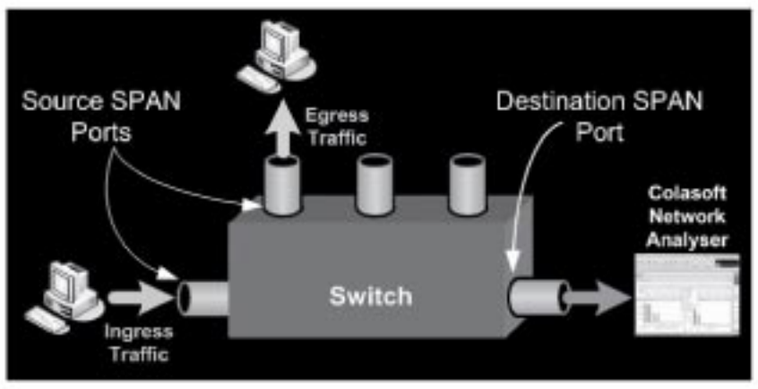
Người dịch: Bùi Quốc Kỳ

Giám sát hạ tầng mạng với công nghệ SPAN trên Cisco Catalyst Switch

Việc giám sát lưu lượng mạng hỗ trợ đắc lực cho quá trình khác phục sự cố, giám sát các sự cố liên quan đến bảo mật (security audit).
Trước đây, để giám sát hoặc bắt lưu lượng, ta thường sử dụng thiết bị hub. Theo nguyên lý hoạt động, khi hub nhận được bất kỳ gói tin trên port nào, nó sẽ tiến hành "forward" gói tin đó ra tất
Tuy nhiên, thiết bị hub giờ đây đã được thay thế bởi dòng thiết bị thông minh hơn, đó là switch. Không giống như hub, khi switch nhận được một unicast packet, nó chỉ forward ra đúng port chỉ định. Mặc dù vậy, ta vẫn có thể tiến hành giám sát được lưu lượng hạ tầng mạng trên Cisco Catalyst switch nhờ tính năng **Switched Port Analyser (SPAN).**

Một số thuật ngữ trong SPAN

- Ingress Traffic: lưu lượng dữ liệu đi vào switch
- Egress Traffic: lưu lượng dữ liệu đi ra khỏi switch
- Source (SPAN) port: port được giám sát
- Source (SPAN) VLAN: VLAN mà lưu lượng traffic của VLAN được giám sát
- Destination (SPAN) port: port phụ trách việc giám sát source port, đây là port thường được đấu nối tới hệ thống phân tích mạng network analyser.
- Remote SPAN (RSPAN): khi Source port không nằm trên cùng một switch với Destination port. RSPAN là một tính năng được cải tiến cần đến một VLAN đặc biệt để vận chuyển lưu lượng được giám sát.



Source SPAN port là port được giám sát đối với lưu lượng nhận received (RX), lưu lượng truyền đi transmitted (TX) hoặc cả hai chiều truyền và nhận bidirectional (both). Lưu lượng đi vào hoặc gửi ra Source SPAN port sẽ được sao chép sang Destination SPAN port. Thông thường, chúng ta sẽ kết nối PC cài đặt chương trình phân tích dữ liệu network analyser với Destination SPAN port.
Chương trình Network Analyser không những có thể thống kê các loại lưu lượng nhận được mà còn có khả năng tự động phân tích các sự cố liên quan đến quá trình truyền lại dữ liệu của phiên kết nối TCP, các sự cố phân giải tên miền DNS, tiến trình hồi đáp TCP bị chậm trễ, cảnh báo các thong điệp ICMP redirect message và nhiều tính năng hỗ trợ khác. Những thông tin hữu dụng trên giúp người quản trị nhanh chóng phát hiện được sự cố một cách dễ dàng.

Một số đặc điểm cần lưu ý trên Source Port

- Source port có thể được giám sát bởi nhiều phiên SPAN session khác nhau.
- Mỗi source port có thể được cấu hình giám sát theo một hướng nhất định (ingress, egress, hoặc cả hai).
- Source port có thể cùng hoặc khác VLAN với Destination port.
- Đối với VLAN SPAN source, tất cả các active port thuộc source VLAN đều đóng vai trò là source port.

Một số đặc điểm cần lưu ý trên Destination Port

Mỗi phiên SPAN session phải có ít nhất một destination port để nhận các bản sao lưu lượng từ source port và VLAN. Destination port có một số đặc điểm cần lưu ý sau:

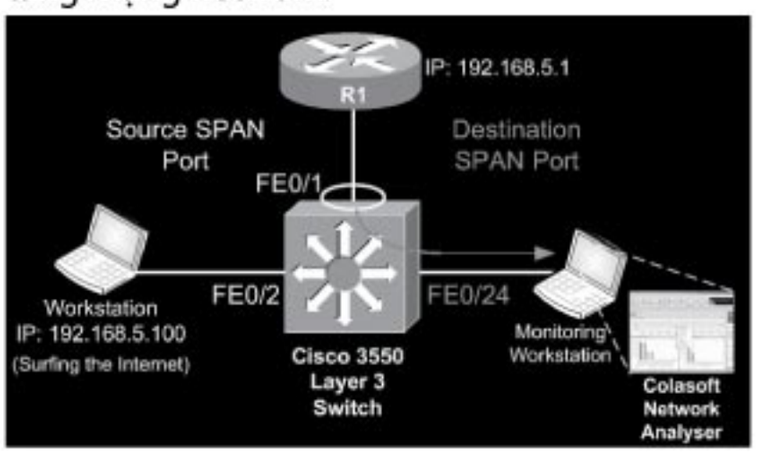
- Một destination port phải nằm trên cùng một switch với source port (đối với phiên SPAN session cục bộ).
- Một destination port chỉ có thể tham gia vào một phiên SPAN session tại một thời điểm.
- Destination port không thể đóng vai trò của một source port.

Lưu ý

- Cisco Catalyst 2950 switch chỉ có thể kích hoạt một phiên SPAN session tại một thời điểm và không thể giám sát VLAN source.
- Cisco Catalyst 3550, 3560 và 3750 switch có thể hỗ trợ hai phiên SPAN session tại cùng một thời điểm và có khả năng hỗ trợ giám sát cả VLAN source.
- Chỉ có duy nhất một destination port tương ứng với mỗi SPAN session và một destination port không thể tham gia vào hai phiên SPAN session cùng lúc. Do đó, hai phiên SPAN session không thể có cùng một destination port.

Cấu hình SPAN trên Cisco Catalyst Switch

Cấu hình sau đây được thực hiện Cisco Catalyst 3550 Layer 3 switch, tuy nhiên, các câu lệnh này cũng tương tự và được hỗ trợ trên các dòng Cisco Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560–E, 3750, 3750–E và 4507R Series Switch.
Chúng ta sẽ tiến hành cấu hình SPAN để giám sát lưu lượng đi vào traffic entering (Ingress) và đi ra exiting (Egress) trên port của switch đấu nối tới router (FE0/1). Cấu hình này sẽ giúp chúng ta giám sát toàn bộ lưu lượng vào ra hạ tầng mạng network.



Do router R1 kết nối tới 3550 Catalyst switch thông qua port FE0/1, nên port này sẽ được cấu hình với vai trò là Source SPAN port. Lưu lượng từ cổng FE0/1 sẽ được sao chép ra FE0/24 nơi máy trạm được cài đặt chương trình bắt lưu lượng.

```
Catalyst-3550(config)# monitor session 1 source interface fastethernet 0/1
Catalyst-3550(config)# monitor session 1 destination interface fastethernet 0/24
```

Sau khi cấu hình hoàn tất, chúng ta sẽ nhận thấy đèn LED trên FE0/24 bắt đầu nháy tương tự như đèn LED của port FE0/1.
Chúng ta có thể kiểm tra lại phiên monitoring session bằng câu lệnh sau::

```
Catalyst-3550# show monitor session 1
Session 1
---------
Type          : Local Session
Source Ports  :
   Both       : Fa0/1
Destination Ports: Fa0/24
   Encapsulation : Native
       Ingress: Disabled
```

Để hiển thị thông tin chi tiết cấu hình phiên giám sát, ta thực hiện câu lệnh sau:

```
Catalyst-3550# show monitor session 1 detail
Session 1
---------
Type          : Local Session
Source Ports  :
   RX Only    : None
   TX Only    : None
   Both       : Fa0/1
Source VLANs  :
   RX Only    : None
   TX Only    : None
   Both       : None
Source RSPAN VLAN : None
Destination Ports  : Fa0/24
   Encapsulation   : Native
       Ingress:    Disabled
Reflector Port     : None
Filter VLANs       : None
Dest RSPAN VLAN    : None
```

Tại máy trạm có cài đặt chương trình bắt gói tin, ta có thể tiến hành các thao tác phân tích, thống kê như hình minh họa sau:

Routing & Switching

CISCO CERTIFIED CCNA ROUTING & SWITCHING

Chương trình CCNA R&S

CISCO CERTIFIED CCNP

Chương trình CCNP ROUTE

CISCO CERTIFIED CCNP

Chương trình CCNP SWITCH

CISCO CERTIFIED CCNP

Chương trình CCNP TSHOOT

CISCO CERTIFIED CCIE ROUTING AND SWITCHING

Chương trình CCIE

Security

CISCO CERTIFIED CCNA SECURITY

Chương trình CCNA Security

CISCO CERTIFIED CCNP SECURITY

Chương trình SECURE

CISCO CERTIFIED CCNP SECURITY

Chương trình FIREWALL

CISCO CERTIFIED CCNP SECURITY

CISCO CERTIFIED CCNP SECURITY

ƯU ĐÃI LỚN

Tháng 7 mùa ưu đãi

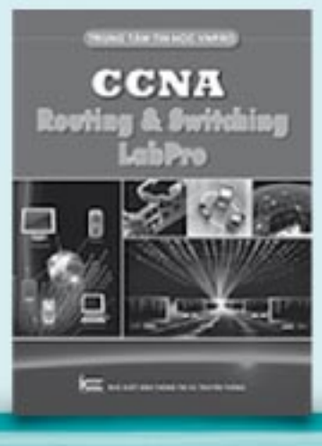
- ***Ưu đãi hấp dẫn khi tham gia đóng nhóm & đóng cặp***
- ***Ưu đãi 10% cho học viên cũ***
- ***Tặng ngay áo thun VnPro***
- ***Tham gia dự đoán kết quả World Cup 2014 với tổng giải thưởng lên đến 50 triệu đồng***

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

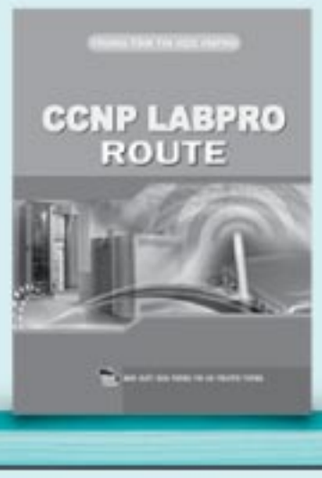
GIẢM* NGAY 10%



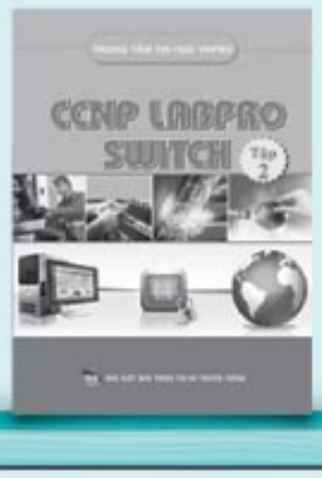
CCNA Routing & Switching
Giá: 220.000 VNĐ

CCDA
Giá: 250.000 VNĐ

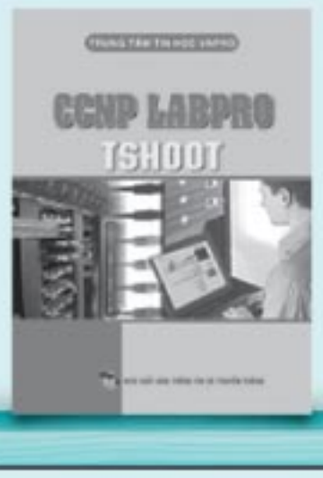
Ôn thi CCNA trong 24h
Giá: 120.000 VNĐ



CCNP LABPRO ROUTE
Giá: 120.000 VNĐ



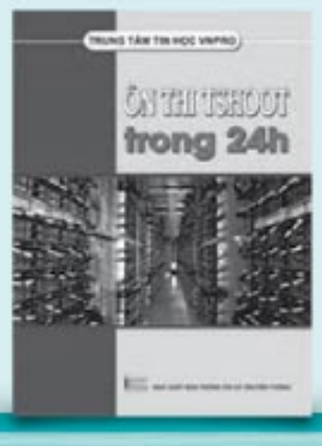
CCNP LABPRO SWITCH
Giá: 120.000 VNĐ



CCNP LABPRO TSHOOT
Giá: 120.000 VNĐ

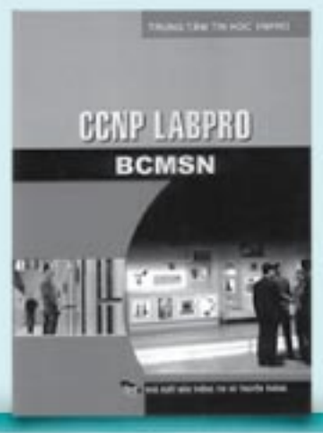
Ôn thi Route
Giá: 90.000 VNĐ

Ôn thi Switch
Giá: 100.000 VNĐ

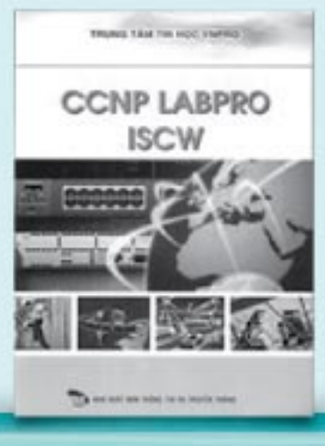


Ôn thi Tshoot
Giá: 80.000 VNĐ

CCNP LABPRO BSCI
Giá: 95.000 VNĐ

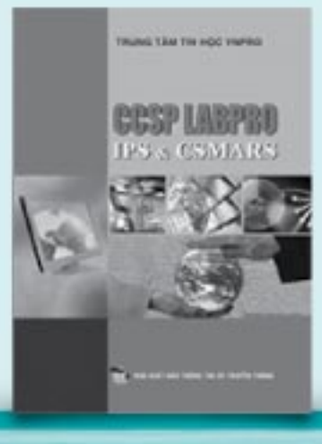


CCNP LABPRO BCMSN
Giá: 70.000 VNĐ

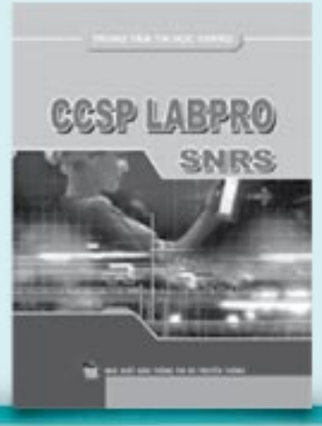


CCNP LABPRO ISCW
Giá: 120.000 VNĐ

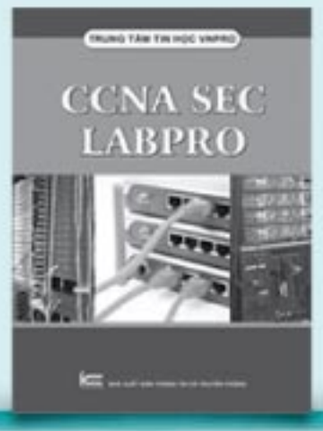
CCSP LABPRO SNAF & SNAA
Giá: 120.000 VNĐ



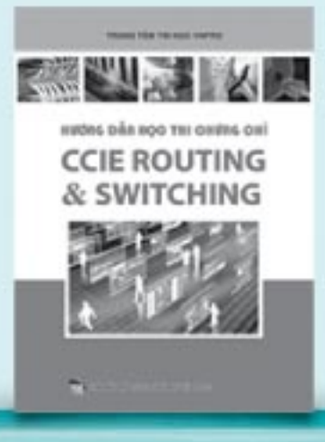
CCSP LABPRO IPS & CSMARS
Giá: 90.000 VNĐ



CCSP LABPRO SNRS
Giá: 140.000 VNĐ



CCNA SEC LABPRO
Giá: 150.000 VNĐ

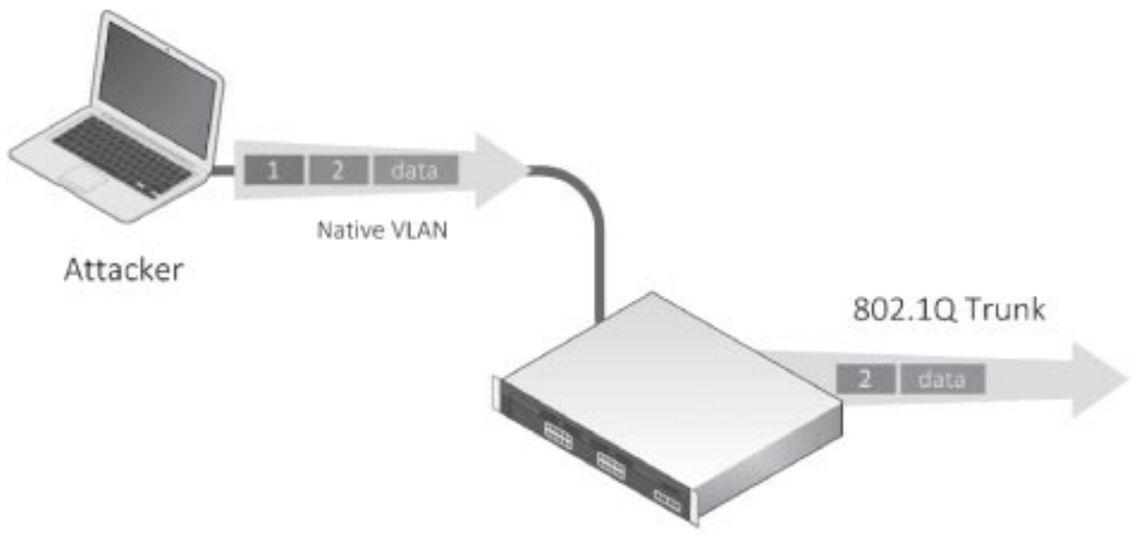


CCIE R&S
Giá: 150.000 VNĐ

CWNA
Giá: 90.000 VNĐ

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

NGUY CƠ BẢO MẬT **VLAN HOPPING**



VLan hopping mô phỏng 1 kiểu tấn công mà các traffic bình thường không thể đi qua được các VLAN khác trong hệ thống. VLAN hopping sẽ lợi dụng 2 bước: giả mạo Switch, và tag hai thông tin vlan đi qua trunk port.

- **Giả mạo Switch (Switch Snoofing)**

  Switch Spoofing có thể xảy ra khi 1 attacker kết nối vào 1 cổng của switch ở chế độ trunking hoặc sử dụng DTP để thiết lập đường trunk. Lúc này, 2 thiết bị sẽ cho phép sử dụng kiểu đóng gói frame 802.1q và tag vào gói tin nhưng thông tin VLAN khác nhau để xác định. Attacker sẽ thêm header 802.1q và tag thông tin VLAN với mục đích đẩy gói tin ra đến các VLAN ở xa. Khi nhận được switch sẽ hiểu frame đó như 1 nguồn từ 802.1q và đẩy frame đó đến VLAN tương ứng.

- **Cơ chế chống lại kiểu tấn công Switch Spoofing**

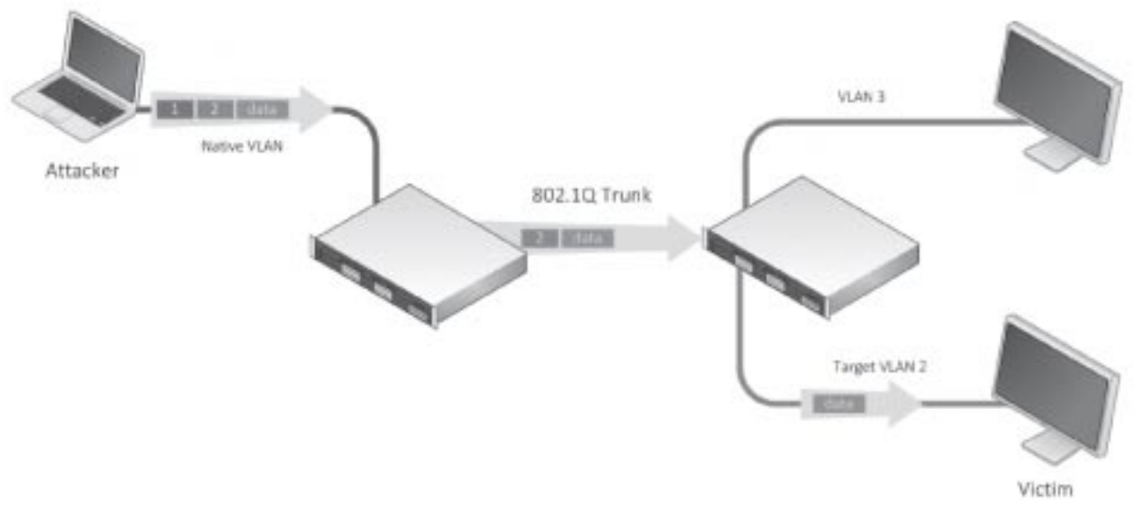
  Để ngăn chặn tình trạng tấn công giả mạo switch này thì cần phải bật tất cả các port trên switch là mode access hoặc là tắt chế độ tự động thỏa thuận DTP. Lệnh switchport mode access buộc các cổng hoạt động như một cổng để truy cập, vô hiệu hóa bất kỳ cơ hội mà nó có thể trở thành một cổng trunk và gửi lưu lượng truy cập cho nhiều VLAN. Tắt DTP bằng tay để ngăn chặn truy cập giả mạo tự động lên trunk của những kẻ tấn công.

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport nonegotiate
```

- **Cơ chế tấn công Double Tagging**

+ Khi tấn công thì kẻ tấn công sẽ gửi frame và tag 2 thông tin VLAN vào header. Nếu kẻ tấn công kết nối vào 1 cổng access thì sẽ tag thông tin VLAN phù hợp với port đó. Nếu kẻ tấn công đang kết nối vào cổng trunk hoặc là cổng đang để DTP thì tag thông tin đầu tiên sẽ là native VLAN (thường là vlan 1) và thông tin VLAN thứ 2 sẽ là thông tin của vlan mà kẻ tấn công muốn gửi tới.

+ Khi Switch nhận được frame của kẻ tấn cống, switch sẽ gỡ tag đầu tiên và sau đó đẩy ra các cổng trunk đến các switch láng giềng (Các switch đều sử dụng Native VLAN giống nhau). Vì vậy, tag VLAN thứ 2 sẽ không bị gỡ bỏ và các switch sẽ đẩy nó đến VLAN tương ứng.



- **Phương thức chống lại kiểu tấn công Double Tagging**

+ Chìa khóa để tấn công theo kiểu VLAN hopping chính là native VLAN, do các switch mặc định đều lấy VLAN 1 làm native VLAN cho các đường trunk vì thế rất dễ để xác định mục tiêu. Bước đầu tiên để ngăn chặn ra chuyển hết các port access thuộc native VLAN đi sang các VLAN khác.

```
Switch(config-if)# switchport access vlan 10
Switch(config-if)# description access_port
```

+ Bước 2 đổi native VLAN thành 1 VLAN khác với VLAN 1.

```
Switch(config-if)# switchport trunk native vlan 99
```

+ Bước 3 tắt chế độ tự động không tag native VLAN sang lựa chọn tag thông tin VLAN native trên các port trunk.

```
Switch(config-if)# switchport trunk native vlan tag
```

Người dịch: Phạm Minh Nguyên

10 QUY TẮC GIÚP BẠN ĐỌC SÁCH HIỆU QUẢ

Ngày nay, khi mà kiến thức được đăng tải rộng rãi khắp các kênh phương tiện thông tin đại chúng trên internet thì văn hoá đọc sách và kỹ năng đọc sách cần phải đặc biệt chú trọng hơn. Giới trẻ ngày nay rất ít khi chịu bỏ tiền ra mua sách. Số bỏ tiền ra mua sách thì lại biết cách đọc sách hiệu quả. Hãy xem 10 bí quyết sau đây của DeltaViet có thể giúp bạn cải thiện kỹ năng đọc sách- 1 trong những kỹ năng mềm quan trọng cho bất cứ ai:

▪ **Quy tắc 1**: Không đọc lùi lại. Dù là bài viết về khoa học kỹ thuật khó đến đâu cũng chỉ đọc một lần. Không được chuyển động mắt trở lại những dòng, trang đã đọc. Chỉ khi đã đọc xong và suy nghĩ về những điều đã đọc nếu có khúc mắc gì, mới có thể đọc lại bài nếu như thật sự cần thiết nhé.

▪ **Quy tắc 2**: Đọc và hiểu theo khối thuật toán tích hợp. Phải thường xuyên nhớ lại nội dung của từng khối kiến thức. Trong quá trình đọc, hãy tìm cách trả lời những câu hỏi tiêu chuẩn để ra cho mỗi khối của thuật toán thường là đầu khối hay cuối khối.

▪ **Quy tắc 3**: Không đọc phát thành tiếng. Đọc mà phát âm chính là kẻ thù độc nhất vô nhị của việc đọc nhanh. Hãy thực hiện các bài tập và gõ nhịp để nhịn phát âm thành tiếng, đừng để âm thanh vụt ra khỏi cổ họng nhé. Khi thấy tốc độ đọc bị giảm cần phải luyện lại để có thể cải thiện tốc độ đọc.

▪ **Quy tắc 4**: Chuyển động mắt theo chiều thẳng đứng khi đọc tránh chuyển động theo chiều ziczac. Khi đọc, mắt di chuyển theo chiều thẳng đứng từ trên xuống dưới, theo dòng tưởng tượng ở ngay giữa trang giấy. Hãy tập phát triển thói quen nhìn ngoại vi. Hãy đọc báo có cột hẹp trước, rồi đọc sách sau đó, sơ bộ vạch đường ở giữa trang bằng bút chì sau đó là bút hết mực. Phấn đấu đọc một trang chỉ trong 10 – 15 giây, cố hiểu được nội dung chung chung. Tuỳ mức độ thành thục trong việc di chuyển mắt mà chuyển sang đọc hiểu cả trang sách chỉ trong 30 giây.

▪ **Quy tắc 5**: Tập trung tư tưởng cao độ khi đọc sách. Tập trung chính là chất xúc tác của quá trình đọc sách. Đọc nhanh lại càng đòi hỏi tập trung trí não với cường độ cực cao hơn để tư duy và nắm bắt vấn đề nhanh hơn.

▪ **Quy tắc 6**: Hiểu những điều mình đã đọc trong quá trình đọc sách. Khi đọc sách cần làm rõ các từ khoá, các điểm tựa suy luận, tức là các điểm tựa để hiểu bài và nhận thức vấn đề nhanh nhất có thể.

▪ **Quy tắc 7**: Áp dụng các cách nhớ chủ yếu mà bạn biết trong khi đọc. Mục đích của việc đọc sách để nhớ thông tin. Nhớ cái gì là tuỳ theo mục đích đọc cần thiết của mình và chỉ nên nhớ những gì hiểu được chứ đừng nhớ những thứ linh tinh, vô bổ không cần thiết. Không cần nhớ từng câu, từng chữ nhưng phải nhớ đại ý và thông điệp của tác giả cuốn sách.

▪ **Quy tắc 8**: Đọc với tốc độ biến đổi theo mức độ. Biết đọc với các tốc độ khác nhau cũng rất quan trọng cho việc đọc hiểu và chọn lọc xử lý thông tin. Có chỗ chỉ cần đọc lướt qua nhanh, song có trang thì nên đọc chậm lại để hiểu được thực chất vấn đề là gì. Hãy biết chọn cách đọc cần thiết, đúng lúc và đúng chỗ cho từng đoạn nội dung.

▪ **Quy tắc 9**: Phải thường xuyên luyện tập, củng cố không ngừng thói quen đọc sách mỗi ngày.

▪ **Quy tắc 10**: Đặt tiêu chuẩn đọc mỗi ngày 2 tờ báo, 1 tờ tạp chí và khoảng 50 đến 70 trang sách sau đó nâng lên nhiều hơn.

Làm được 10 điều như vậy, sau một thời gian ngắn chắc chắn bạn sẽ là người đọc sách báo nhanh hơn và hiệu quả hơn rất nhiều người và kiến thức bạn tiếp nhận được cũng sẽ nhiều hơn. Chúc bạn thành công!

Các loại Network: LAN, WAN, PAN, MAN

Chúng ta sẽ có một cái nhìn sâu sắc hơn về hạ tầng mạng internet nếu nắm bắt và phân biệt được các loại network khác nhau. Bài viết này sẽ giới thiệu ngắn gọn, đặc điểm của từng loại mạng khác nhau: LAN, WAN, PAN và MAN.

LAN

LAN *(Local Area Network)* đại diện cho một hạ tầng mạng cục bộ thường triển khai trong một văn phòng, một tòa nhà và có thể mở rộng bằng hệ thống mạng không dây Wi-Fi.

Hệ thống mạng LAN có thể sử dụng môi trường truyền dẫn có dây (twisted-pair cable) hoặc không dây nhưng vẫn dựa trên nền tảng Ethernet.

WAN

WAN *(Wide Area Network)* trái ngược với mạng LAN có thể nới rộng ra phạm vi vật lý rộng hơn cho phép kết nối các tòa nhà lại với nhau, các quận huyện hoặc thậm chí là xuyên quốc gia. Các hệ thống mạng WAN sẽ được kết nối với nhau và kết nối nhiều hệ thống mạng LAN để hình thành nên hạ tầng mạng Internet.

Hệ thống mạng WAN có thể được kết nối bằng các loại cáp quang (fiber-optic cable), hay thậm chí có thể sử dụng môi trường mạng không dây (wireless) để truyền dẫn. Wireless WAN thường sử dụng sóng microwave hoặc sóng hồng ngoại infrared (IR) để truyền dẫn, thậm chí có thể sử dụng vệ tinh (satellite) để phục vụ cho việc truyền dẫn. Tuy nhiên, cáp quang thường được sử dụng cho hạ tầng mạng lõi campus vì nó phù hợp cho khoảng cách xa với chi phí hợp lý.

Personal Area Network (PAN)

Mạng PAN đại điện cho hạ tầng mạng cá nhân trong phạm vi không quá lớn như không gian của một phòng nhỏ. Công nghệ mạng wireless PAN điển hình mà chúng ta thường thấy là Bluetooth. Các thiết bị như tai nghe không dây (wireless headset), máy in printer không dây hoặc smart-phone thường sử dụng công nghệ mạng PAN để truyền dữ liệu. Công nghệ mạng Wi-Fi cũng có thể được xem là công nghệ mạng PAN nếu như được sử dụng trong một khoảng không gian chật hẹp.

MAN

Mạng MAN *(Metropolitan Area Network)* thường được sử dụng để kết nối các chi nhánh của một công ty rải rác giữa các quận lại với nhau.

Hạ tầng mạng MAN có thể sử dụng môi trường phát sóng microwave antenna tương tự như hệ thống antenna của TV hoặc có thể sử dụng cáp quang (fiber-optic cable) tương tự nhưng trong mạng WAN. Thường thì công ty có nhu cầu triển khai hạ tầng mạng MAN sẽ thuê nhà cung cấp dịch vụ ISP triển khai vì chi phí tự mình triển khai là quá lớn.

Trước đây, hạ tầng mạng MAN thường sử dụng các công nghệ asynchronous transfer mode (ATM), FDDI hoặc SMDS.

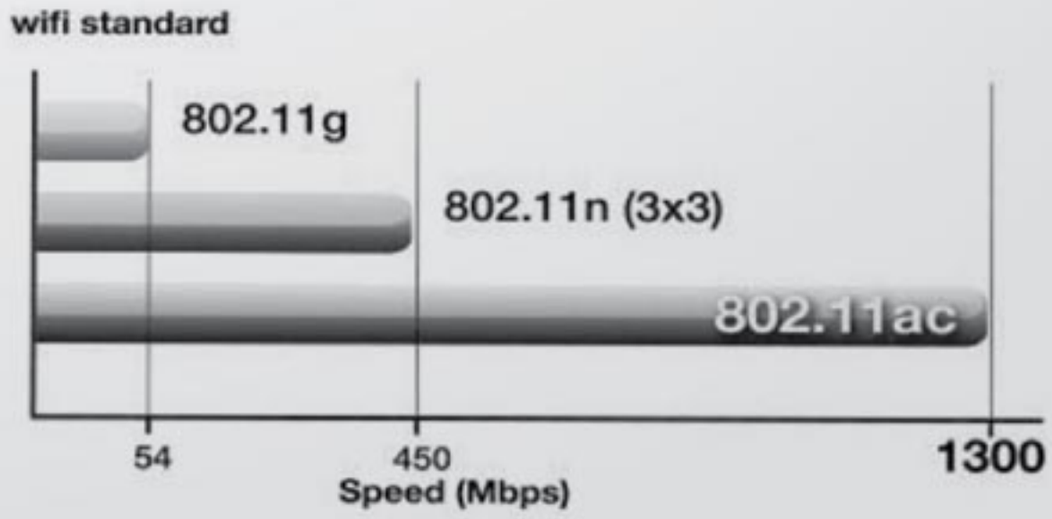
Sự khác biệt giữa **802.11ac** và **802.11n** là gì?

Một số chuẩn wireless thường gặp là 802.11a/b/g/n. Laptop và smartphone thường hỗ trợ các chuẩn wireless cơ bản là B hoặc G, và trong tương lai, các thiết bị này sẽ bắt buộc phải hỗ trợ chuẩn wireless N. 802.11n để bắt kịp với xu hướng tương lai **(chuẩn 802.11n đã xuất hiện từ năm 2009)** cho phép truyền dữ liệu với tốc độ nhanh hơn. 802.11ac là một giao thức Wi-Fi protocol mới kế thừa sự thành công của chuẩn 802.11n. Chuẩn này thường được gọi là **"5G Wi-Fi"** hoặc **"Gigabit Wi-Fi"**

Logo tương thích với chuẩn 802.11ac

Chuẩn Wi-Fi 802.11ac có khả năng tương thích ngược với các chuẩn 802.11b, g và n. Vì vậy, các thiết bị tuân theo chuẩn 802.11ac có thể tương tác tốt với các thiết bị hạ tầng cũ hiện tại. Tuy nhiên, nếu có thể thì chúng ta nên nâng cấp hết tất cả các thiết bị trong hệ thống mạng thành 802.11ac để tận hưởng tốc độ vượt trội của chuẩn này.

802.11ac Speed

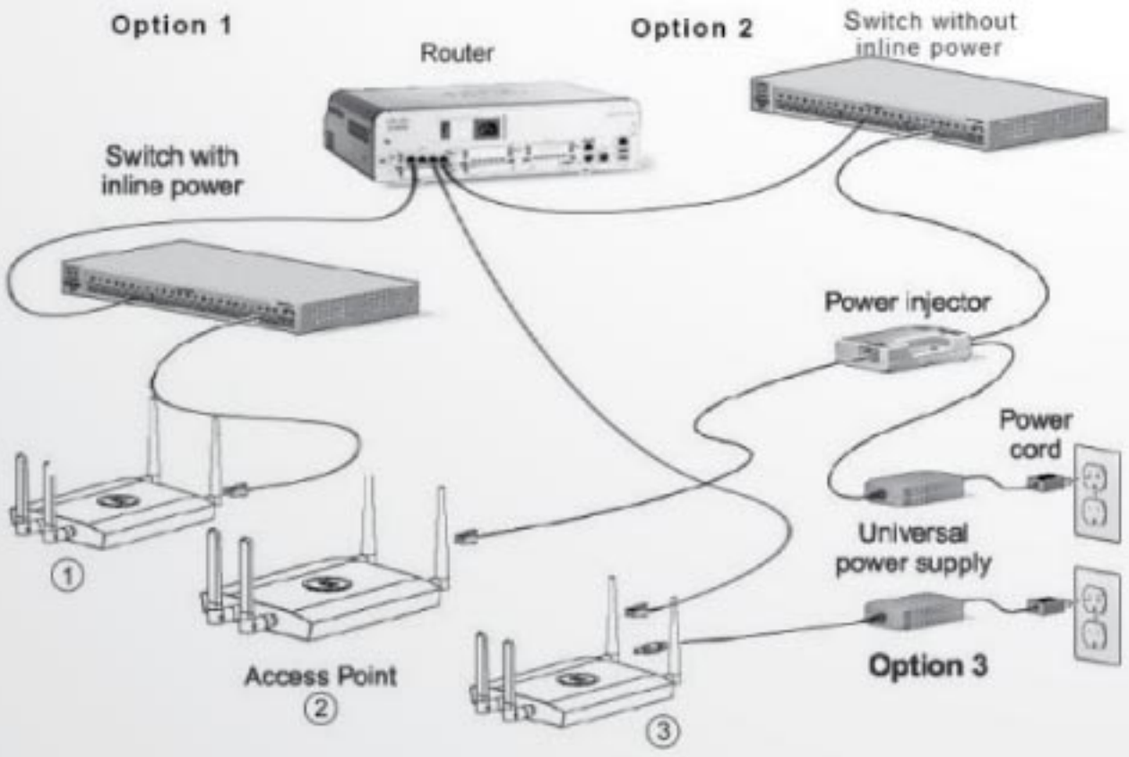


1.3 Gbps là tốc độ của chuẩn 802.11ac còn chuẩn 802.11n thì hỗ trợ tốc độ 0.45Gbps. Tuy nhiên, do nhiều yếu tố khác nhau có thể ảnh hưởng đến tốc độ của môi trường mạng không dây như nhiễu, số lượng antenna trên Access Point, khoảng cách giữa thiết bị truyền tới thiết bị nhận mà hiệu suất thực sự của chuẩn wireless n chỉ dao động từ 50-150Mbit và đối với chuẩn 802.11ac là 250-300Mbit.

Wireless 802.11n hỗ trợ tối đa 4 antenna cho phép truyền 100Mbit trên mỗi antenna, 802.11ac hỗ trợ tối đa 8 antenna cho phép truyền 400Mbit trên mỗi antenna.

Để hỗ trợ tốc độ cao hơn, thiết bị không dây có thể được trang bị nhiều antenna. Các thiết bị nhỏ như smartphones thường thì chỉ hỗ trợ 1 antenna, các thiết bị lớn hơn như máy tính bảng tablet có thể hỗ trợ đến 4 antenna và máy tính laptop và television có thể hỗ trợ từ 4 cho tới 8 antenna. Tuy nhiên, thông thường thì các 802.11ac router sẽ rất ít khi nào hỗ trợ vượt quá 6 antenna.

Thiết bị **Access Point Wireless** có những tùy chọn cấp nguồn nào



Thiết bị Cisco Wireless Access Point có hỗ trợ 3 tùy chọn cấp nguồn:

- **Tùy chọn 1**

(Cisco Router → Cisco POE switch → Cisco AP): cấp nguồn cho AP (Access Point) thông qua qua switch hỗ trợ PoE.

- **Tùy chọn 2**

(Router → Switch *(without POE)* → Power injector → AP): cấp nguồn cho AP thông qua Power injector.

- **Tùy chọn 3**

(Router → AP → Power supply): cấp nguồn cho AP thông qua Power supply.

Phân biệt cáp **Cat5, Cat5e, Cat6**

Nếu nhìn diện mạo bên ngoài, các loại cáp Ethernet trông có vẻ giống nhau, và tất cả chúng đều được cắm vào Ethernet port, nhưng chất liệu kim loại bên trong các loại cáp sẽ khác biệt nhau tùy theo từng loại. Tuy nhiên, chúng ta có thể quan sát các ký tự trên vỏ cáp để nhận biết loại cáp: Cat5, Cat5e và Cat6.

- **Cat5:**

Category 5 gọi tắt là Cat5, hỗ trợ tốc độ 10Mbps và 100Mbps. Chúng ta có thể sử dụng cáp Cat5 để truyền với tốc độ gigabit nhưng sẽ bị giới hạn chiều dài cáp và cũng không đảm bảo về mặt tốc độ.

- **Cat5e: Faster with Less Interference**

Category 5e hay còn gọi là Cat5e có tốc độ và khả năng chống nhiễu tốt hơn so với Cat5. Cáp Cat5e hỗ trợ tốc độ truyền dẫn 1000 Mbps "gigabit".

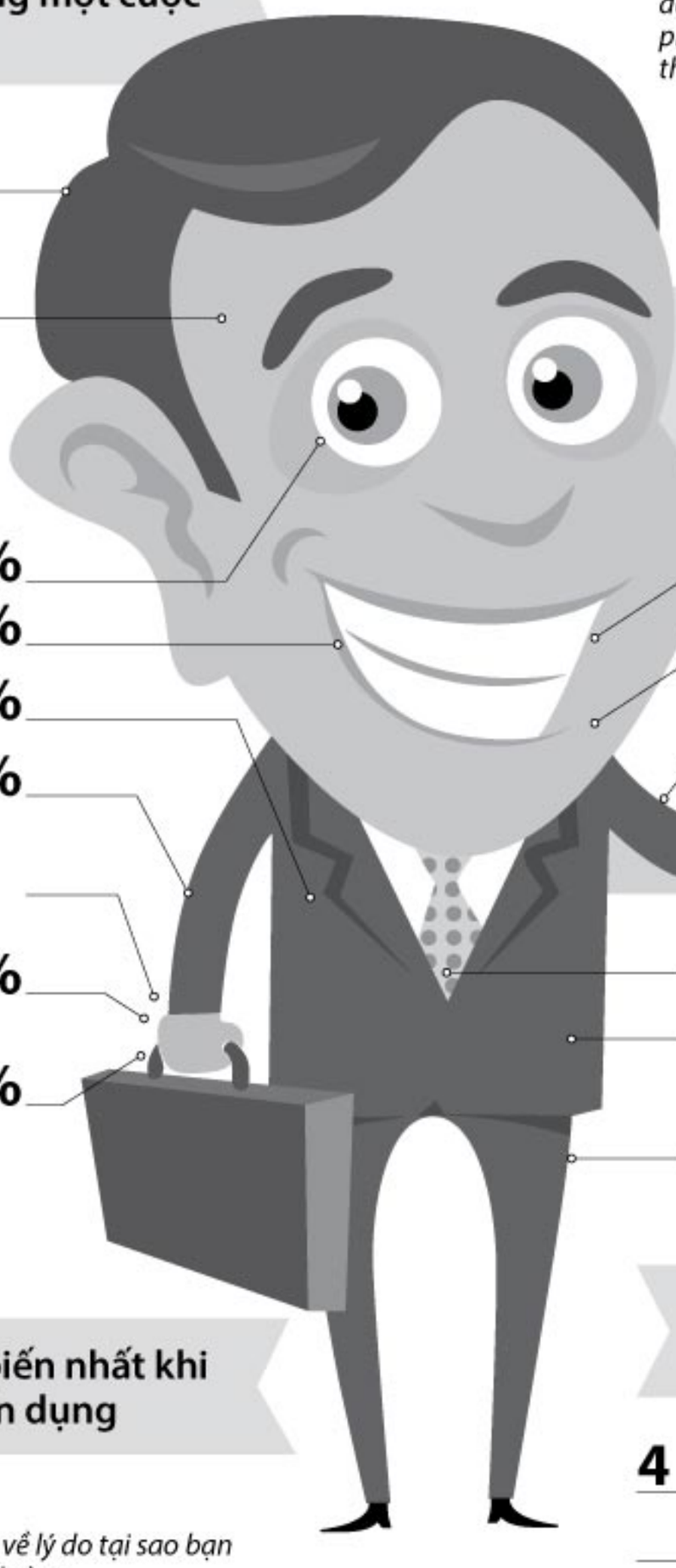
- **Cat6:**

Category 6 là thế hệ tiếp theo của Cat5e được cải tiến lên và có khả năng truyền với tốc độ 10-Gigabit. Với tốc độ này thì đây là loại cáp ít được sử dụng ở hộ gia đình vì chúng ta sẽ không bao giờ tận dụng hết băng thông của loại cáp này.

Có một đặc điểm cần lưu ý đó là tốc độ của hạ tầng mạng khác với tốc độ truy cập internet. Việc nâng cấp tốc độ hạ tầng mạng LAN cục bộ không có nghĩa là tốc độ truy cập Facebook hướng ra ngoài internet sẽ nhanh hơn. Tuy nhiên, nếu chúng ta có nhu cầu truyền file giữa các máy tính cục bộ với nhau và các máy tính này hỗ trợ phần cứng tương thích tốc độ gigabit thì tốc độ sẽ nhanh hơn rất nhiều. Nếu chúng ta trang bị cổng gigabit trên router thì PC cũng cần phải trang bị gigabit network card. Hầu hết các thiết bị router và card mạng sau này đều hỗ trợ tốc độ gigabit nhưng các thiết bị PC và router cũng vẫn còn được sử dụng thì chắc hẳn chúng ta sẽ khó có thể tận dụng tốc độ gigabit trên các thiết bị mới này.

NHỮNG ĐIỀU BẠN NÊN BIẾT KHI
PHỎNG VẤN TUYỂN DỤNG

Những lỗi phi ngôn ngữ thường gặp trong một cuộc phỏng vấn



21% *nghịch **tóc** hoặc sờ vào mặt*

47% *có ít hoặc **không có** kiến thức về công ty. Đây là sai lầm phổ biến của các ứng viên trong các cuộc phỏng vấn*

*Thất bại trong việc **giao tiếp bằng mắt*** **67%**

*Thiếu **nụ cười*** **38%**

Tư thế xấu **33%**

***Khoanh tay** trước ngực* **21%**

*Sử dụng quá nhiều **cử chỉ tay*** **9%**

***Bắt tay** quá yếu ớt* **26%**

*Quá **lo lắng*** **33%**

Trong một cuộc khảo sát với 2000 quản lý,

33% *trong số họ cho rằng chỉ cần **90 giây** đầu của một cuộc phỏng vấn học đã có thể biết họ **nên thuê ai**.*

*Thời gian trung bình của một cuộc phỏng vấn là **40 phút***

Thống kê cho thấy những người mới sẽ có ấn tượng với những hành vi sau

7% *từ những gì chúng ta **chia sẻ***

38% *từ **cách nói** và **sự tự tin** của ứng viên*

55% *từ cách **ăn mặc, hành động** và cách ứng viên **bước vào** phòng*

Trang phục

***Màu sắc chói** không được ưa thích*

70% *những nhà tuyển dụng phàn nàn rằng họ không muốn các ứng viên ăn mặc **thời trang** hay **chạy theo xu hướng***

65% *các quản lý lại cho biết **trang phục** có thể là yếu tố **quyết định** giữa hai ứng cử viên tương đương nhau*

10 sai lầm phổ biến nhất khi phỏng vấn tuyển dụng

10 ***Giải thích quá nhiều** về lý do tại sao bạn lại mất công việc cuối cùng*

*Thể hiện rằng bạn **không có gì vượt trội*** **9**

8 *Thiếu **hài hước, ấm áp** hoặc **cá tính***

*Không thể hiện đủ **sự quan tâm** hoặc **nhiệt tình*** **7**

6 ***Nghiên cứu** chưa đầy đủ về nhà tuyển dụng tiềm năng*

Chú trọng** quá nhiều vào những gì bạn **muốn **5**

4 ***Cố gắng thỏa mãn** tất cả mọi người*

***Quá bay bổng** trong cuộc phỏng vấn* **3**

2 ***Không tạo sự khác biệt** giữa bản thân và các ứng viên khác*

Không đưa ra những đòi hỏi về công việc **1**

Các mẹo chuẩn bị cho một cuộc phỏng vấn

4 ***Tìm hiểu** về tổ chức*

*Có một **công việc cụ thể** trong tâm trí* **3**

2 *Xem xét **trình độ** của bạn trong công việc*

*Sẵn sàng mô tả ngắn gọn **kinh nghiệm của bạn*** **1**

5 câu hỏi phỏng vấn được sử dụng nhiều nhất

*Cho tôi biết **kinh nghiệm** của bạn về .....* **5**

4 *Lý do tại sao bạn **muốn làm việc cho chúng tôi?***

*Bạn biết gì về **công ty của chúng tôi?*** **3**

2 *Lý do tại sao bạn lại **bỏ công việc trước?***

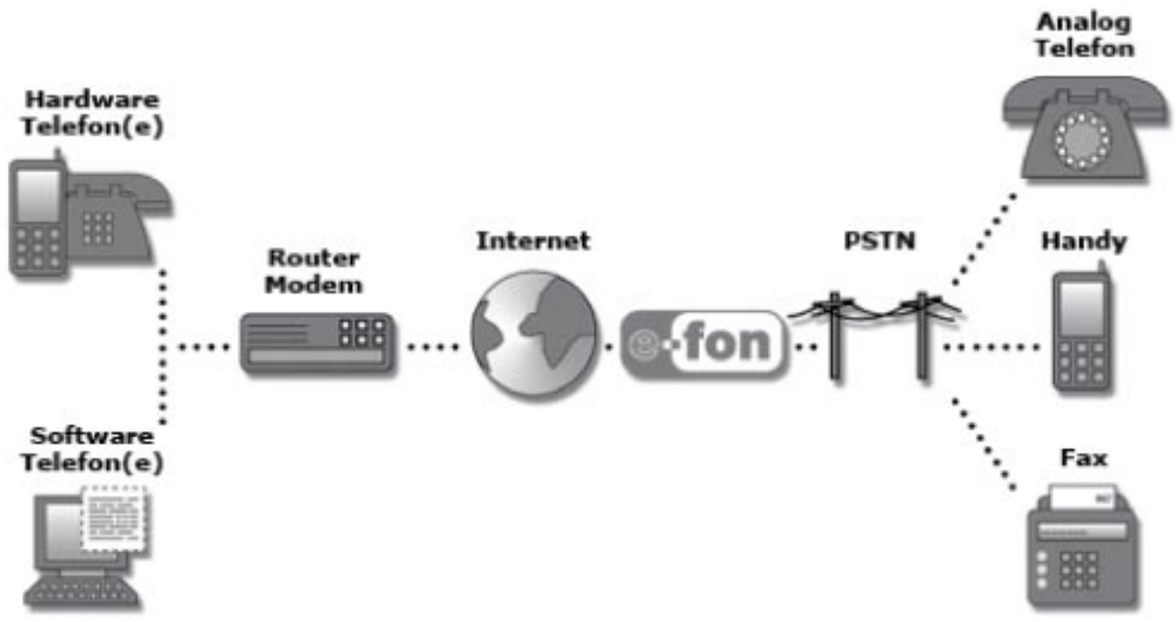
Nói cho tôi biết về bản thân bạn **1**

THÁNG **08** CHỦ ĐỀ

CÔNG NGHỆ VOIP THẾ KỶ 21

Giới thiệu:

Tín hiệu thoại được truyền đi trên hạ tầng cáp thoại, riêng biệt với lưu lượng dữ liệu thường được gửi đi trên hạ tầng cáp mạng LAN, WAN. Với cuộc công nghệ cách mạng VoIP, tín hiệu thoại và dữ liệu người dùng có thể trung chuyển trên cùng một hạ tầng mạng hợp nhất. Các doanh nghiệp có sẵn hạ tầng mạng Internet có thể ứng dụng giải pháp VoIP để tiết kiệm đáng kể chi phí. Chính vì vậy, VoIP dần trở thành một xu hướng tất yếu và nhu cầu tìm hiểu về công nghệ VoIP cũng ngày càng cao.



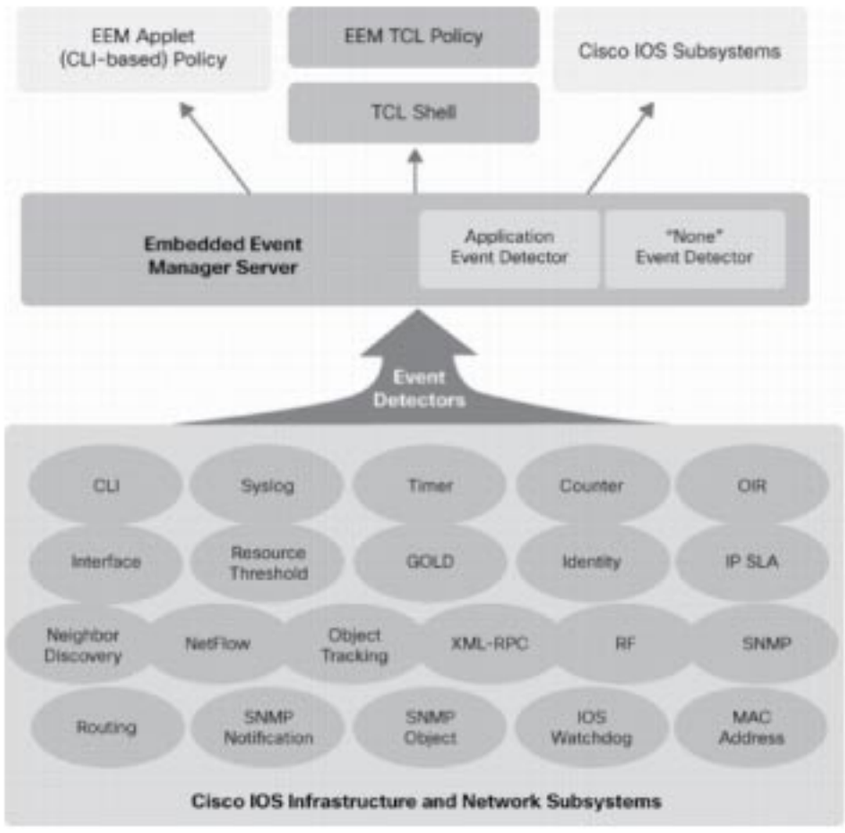
THÁNG **09** CHỦ ĐỀ

TRIỂN KHAI EEM TRÊN HẠ TẦNG MẠNG DOANH NGHIỆP

Giới thiệu:

EEM (Embedded Event Manager) là một công cụ tích hợp sẵn trên các Cisco IOS, cho phép hỗ trợ giám sát và điều khiển linh hoạt các thiết bị trên hạ tầng mạng một cách tự động tùy theo các sự kiện phát sinh chẳng hạn tự động giới hạn lưu lượng không cần thiết trên một cổng khi băng thông sử dụng vượt ngưỡng cho phép, thu thập thông tin về thiết bị (mức sử dụng tài nguyên CPU, RAM) ở những khoảng thời gian xác định trước, giám sát các phiên kết nối từ xa của các phụ tá quản trị đến hạ tầng mạng, cho phép tự động "ping" kiểm tra độ tin cậy của đường truyền tại những khoảng thời định nghĩa trước trong ngày.

*Hãy cùng truy cập web: **vnpro.vn** để cập nhật tin tức và đăng ký tham dự hội thảo bạn nhé!*



(Trích dẫn từ sách VnPro)

CHƯƠNG 6: CÁC TỔ CHỨC VÀ CHUẨN WLAN

4. Các quy tắc về công suất phát

FCC ép buộc những quy tắc nhất định liên quan đến công suất phát ra của anten tùy thuộc vào môi trường là điểm-điểm hay điểm-đa điểm. Thuật ngữ được sử dụng cho công suất phát bởi anten là "công suất bức xạ đẳng hướng hiệu dụng" EIRP (Effective Isotropically Radiated Power).

Kết nối điểm-đa điểm

Kết nối điểm-đa điểm PtMP (Point-to-MultiPoint) có một điểm trung tâm của các kết nối và 2 hay nhiều điểm khác. Kết nối PtMP thường được cấu hình theo mô hình hub-n-spoke. Điểm kết nối trung tâm có thể sử dụng anten đẳng hướng hoặc không. Điều quan trọng cần lưu ý là khi sử dụng anten đẳng hướng thì FCC sẽ tự động xem như kết nối đó là kết nối PtMP. FCC giới hạn EIRP là 4 W cho cả 2,4 GHz ISM và 5 GHz UNII. Hơn nữa, công suất giới hạn cho bộ bức xạ định hướng (thiết bị truyền tín hiệu vô tuyến) cho mỗi băng tần này là 1 W. Nếu như thiết bị WLAN có thể điều chỉnh công suất phát được thì hệ thống có thể tùy biến công suất theo nhu cầu sử dụng.

Giả sử bộ phát sóng truyền tín hiệu 1 W (+30 dBm) được kết nối trực tiếp vào một anten đẳng hướng có độ khuếch đại 12 dBi thì tổng công suất phát của anten là khoảng 16 W, mức này là quá lớn so với giới hạn là 4 W. FCC quy định rằng: *"mỗi khi tăng 3 dBi trên độ khuếch đại ban đầu của anten (6 dBi) thì công suất tại bộ bức xạ định hướng phải giảm 3 dB dưới mức ban đầu là +30 dBm"*. Ví dụ, vì độ khuếch đại của anten là 12 dBi (cao hơn 6 dBi so với mức quy định 6 dBi) nên công suất tại bộ bức xạ định hướng phải giảm đi 6 dB. Lúc này, công suất tại bộ bức xạ định hướng là +24 dBm (30 dBm – 6 dB) hay 250 mW và EIRP là 36 dBm (24 dBm + 12 dBi) hay 4 W. Rõ ràng là nguyên tắc này có thể gây nhầm lẫn nhưng kết quả cuối cùng phải có được là công suất tại bộ bức xạ định hướng không bao giờ lớn hơn 1 W và EIRP không bao giờ lớn hơn 4 W cho kết nối PtMP.

Khi sử dụng anten đẳng hướng thì các quy tắc về công suất cho kết nối điểm-đa điểm phải được tuân thủ cho dù thật sự bạn đang triển khai kết nối điểm-điểm hay điểm-đa điểm.

Bảng 6.1:
Bảng bù công suất trong kết nối điểm-đa điểm

Công suất tại anten (dBm)	Độ khuyếch đại anten (dBi)	EIRP (dBm)	EIRP (W)
30	6	36	4
27	9	36	4
24	12	36	4
21	15	36	4
18	18	36	4
15	21	36	4
12	24	36	4

Kết nối điểm-điểm

Kết nối điểm-điểm PtP (Point-to-Point) bao gồm một anten truyền định hướng duy nhất và một anten nhận định hướng duy nhất. Kết nối này thường là trong liên kết giữa các tòa nhà hay những kết nối tương tự và phải tuân theo các quy tắc đặc biệt. Đối với kết nối PtP, FCC quy định rằng: "Cứ mỗi khi tăng 3 dBi trên mức độ khuếch đại ban đầu của anten (6 dBi), thì công suất tại bộ bức xạ định hướng phải bị giảm đi 1 dB dưới mức ban đầu là +30 dBm"

Hãy xem xét ví dụ trước: vì độ khuếch đại của anten là 12 dBi nên công suất tại bộ bức xạ định hướng phải bị giảm đi 2 dB (thay vì 6 dB như ví dụ trên). Lúc này công suất tại bộ bức xạ định hướng là 28 dBm (30 dBm - 2 dBm) hay khoảng 630 mW và EIRP là 40 dBm (28 dBm + 12 dBi) hay 10 W. Trong trường hợp này, công suất tại bộ bức xạ định hướng vẫn bị giới hạn là 1 W nhưng giới hạn của EIRP đã được tăng lên cùng với độ khuếch đại của anten. Điều này là rất quan trọng để phân biệt rõ ràng giữa 2 quy tắc dành cho kết nối PtMP và PtP.

Bảng 6.2:
Bảng bù công suất trong kết nối điểm-điểm

Công suất tại anten (dBm)	Độ khuyếch đại anten tối đa (dBi)	EIRP (dBm)	EIRP (W)
30	6	36	4
29	9	38	6,3
28	12	40	10
27	15	42	16
26	18	44	25
25	21	46	39,8
24	24	48	63
23	27	50	100
22	30	52	158

II. VIỆN KỸ SƯ ĐIỆN VÀ ĐIỆN TỬ - IEEE

Viện Kỹ sư Điện và Điện tử IEEE (Institute of Electrical and Electronic Engineers) là tổ chức chuyên tạo ra các chuẩn liên quan đến công nghệ thông tin trong nước Mỹ. IEEE tạo ra các chuẩn tuân thủ theo luật của FCC. IEEE đã đưa ra nhiều chuẩn công nghệ như mã hóa khóa công cộng PKC (Public Key Crytography – IEEE 1363), FireWire (IEEE 1394), Ethernet (IEEE 802.3), WLAN (802.11),…

Một phần nhiệm vụ của IEEE là phát triển các chuẩn cho hoạt động của WLAN trong khuôn khổ các quy tắc của FCC. Dưới đây là 4 chuẩn IEEE chính cho mạng WLAN:

- 802.11
- 802.11a
- 802.11b
- 802.11g

1. IEEE 802.11

Chuẩn 802.11 là chuẩn đầu tiên mô tả hoạt động của WLAN. Chuẩn này bao gồm tất cả các công nghệ truyền dẫn sẵn có như trải phổ chuỗi trực tiếp DSSS (Direct Sequence Spread Spectrum), trải phổ nhảy tần FHSS (Frequency Hopping Spread Spectrum) và hồng ngoại (Infrared).

Chuẩn 802.11 mô tả hệ thống DSSS chỉ hoạt động tại tốc độ 1 Mbps và 2 Mbps. Nếu hệ thống DSSS hoạt động ở các tốc độ khác như 1 Mbps, 2 Mbps và 11 Mbps thì nó vẫn được gọi là hệ thống tương thích chuẩn 802.11. Tuy nhiên, nếu như hệ thống hoạt động ở tốc độ nào khác ngoài 1 Mbps và 2 Mbps thì mặc dù hệ thống đó là tương thích chuẩn 802.11 bởi vì nó có thể hoạt động ở 1 và 2 Mbps thì nó vẫn không hoạt động trong chế độ tương thích 802.11 và không thể mong chờ nó giao tiếp được với các thiết bị tương thích 802.11 khác.

IEEE 802.11 là một trong 2 chuẩn mô tả hoạt động của hệ thống WLAN nhảy tần (Frequency hopping). Nếu như người quản trị mạng gặp phải một hệ thống nhảy tần thì nó có thể là hệ thống tương thích 802.11 hay hệ thống tương thích OpenAir. Chuẩn 802.11 mô tả việc sử dụng hệ thống FHSS tại 1 Mbps và 2 Mbps. Có nhiều hệ thống FHSS mở rộng tốc độ hoạt động lên đến 3-10 Mbps sử dụng các công nghệ độc quyền nhưng chỉ với DSSS, nếu hệ thống đang hoạt động ở tốc độ 1 và 2 Mbps thì cũng không thể mong chờ nó sẽ giao tiếp được với các thiết bị tương thích 802.11.

Các sản phẩm 802.11 hoạt động trong băng tần 2,4 GHz ISM giữa 2,4000 GHz và

2,4835 GHz. Hồng ngoại cũng được mô tả trong 802.11, nó là một công nghê dựa trên ánh sáng và không sử dụng băng tần 2,4 GHz ISM.

2. IEEE 802.11b

Mặc dù chuẩn 802.11 đã thành công trong việc cho phép hệ thống DSSS và FHSS giao tiếp được với nhau, tuy nhiên, công nghệ này cũng đã trở nên lỗi thời. Không lâu sau khi phê chuẩn và cài đặt 802.11 thì hệ thống WLAN DSSS đã có thể hoạt động với tốc độ lên đến 11 Mbps. Nhưng không có một chuẩn nào để hướng dẫn cách hoạt động của các thiết bị như vậy, vì thế nảy sinh vấn đề tương thích và cài đặt. Các nhà sản xuất đã giải quyết được hầu hết các vấn đề về cài đặt nên công việc của IEEE khá là đơn giản: tạo ra chuẩn tuân theo cách hoạt động chung của các hệ thiết bị WLAN trên thị trường. Đây là điều không thường xảy ra khi tạo ra một chuẩn mới, đặc biệt là khi công nghệ phát triển một cách nhanh chóng.

IEEE 802.11b còn được gọi là "tốc độ cao" (High-rate) hay "Wi-fi " chỉ định hệ thống DSSS hoạt động ở tốc độ 1; 2; 5,5 và 11 Mbps. Chuẩn 802.11b không mô tả hệ thống FHSS. Các thiết bị tương thích chuẩn 802.11b thì mặc định cũng tương thích với chuẩn 802.11, có nghĩa là chúng tương thích ngược và hỗ trợ cả hai tốc độ dữ liệu là 1 và 2 Mbps. Việc tương thích ngược là rất quan trọng bởi vì nó cho phép WLAN được nâng cấp mà không tốn chi phí thay thế thiết bị mới. Đặc điểm này cùng với tốc độ cao làm cho các phần cứng 802.11b rất phổ biến.

Tốc độ cao của các thiết bị 802.11b là kết quả của việc sử dụng những công nghệ mã hóa (coding) khác nhau. Mặc dù hệ thống là một hệ thống chuỗi trực tiếp (direct sequencing system) nhưng cách mà chip được mã hóa (sử dụng CCK thay vì Barker Code) cùng với cách mà thông tin được điều chế (QPSK cho tốc độ 2; 5,5 và 11 Mbps và BPSK – Binary Phased Shift Keying – cho 1 Mbps) cho phép một lượng lớn dữ liệu được truyền đi trong cùng một khung thời gian. Các sản phẩm 802.11b hoạt động chỉ trong băng tần 2,4 GHz giữa 2,4000 GHz và 2,4835 GHz.

3.IEEE 802.11a

Chuẩn 802.11a mô tả các thiết bị WLAN hoạt động trong băng tần 5 GHz UNII. Việc hoạt động trong băng tần UNII làm cho các thiết bị 802.11a không thể tương tác được với các thiết bị theo chuẩn 802.11 khác. Lý do của sự không tương thích này chính là một hệ thống 5 GHz sẽ không giao tiếp được với một hệ thống 2,4 GHz.

Sử dụng băng tần UNII nên hầu hết các thiết bị có thể đạt được tốc độ 6, 9, 12, 18, 24, 36, 48 và 54 Mbps. Một số thiết bị có thể đạt được tốc độ lên đến 108 Mbps sử dụng những công nghệ độc quyền. Tốc độ cao này là kết quả của các công nghệ mới không nằm trong chuẩn 802.11a. IEEE 802.11a chỉ yêu cầu các tốc độ 6, 12 và 24 Mbps. Một thiết bị WLAN phải hỗ trợ ít nhất các tốc độ này trong băng tần UNII để có thể được gọi là tương thích chuẩn 802.11a. Tốc độ tối đa được chỉ định trong chuẩn 802.11a là 54 Mbps.

4. IEEE 802.11g

802.11g cung cấp cùng một tốc độ tối đa như 802.11a tuy nhiên nó tương thích ngược với các thiết bị 802.11b. Tính tương thích ngược này sẽ làm cho việc nâng cấp mạng WLAN trở nên đơn giản và ít chi phí hơn.

802.11g hoạt động trong băng tần 2,4 GHz ISM. Để đạt được tốc độ cao hơn như 802.11a thì các thiết bị 802.11g sử dụng công nghệ điều chế ghép kênh phân chia theo tần số trực giao OFDM (Orthogonal Frequency Division Multiplexing). Các thiết bị này có thể tự động chuyển sang kiểu điều chế khóa dịch pha cầu phương QPSK (Quadrature Phased Shift Keying) để giao tiếp với thiết bị 802.11b hay 802.11 có tốc độ thấp hơn.

III. CÁC TỔ CHỨC KHÁC

FCC và IEEE chịu trách nhiệm đưa ra các chuẩn và luật cho WLAN ở Mỹ. Ngoài FCC và IEEE thì còn có nhiều tổ chức khác cả ở Mỹ và các nước khác đóng góp vào sự phát triển và giáo dục của mạng WLAN. Ở đây chúng ta khảo sát 3 tổ chức sau:

- Liên minh tương thích ethernet không dây WECA (Wireless Ethernet Compatibility Alliance).
- Viện chuẩn Viễn thông Châu Âu ETSI (European Telecommunications Standards Institute).
- Liên minh LAN không dây WLANA (Wireless LAN Association).

1. Liên minh tương thích Ethernet không dây – WECA

WECA đưa ra và kiểm tra tính tương thích WLAN của các thiết bị 802.11b và 802.11a. Nhiệm vụ của WECA là chứng nhận tính tương thích của các sản phẩm Wi-fi (802.11) và làm cho wi-fi trở thành một chuẩn WLAN toàn cầu. Với tư cách là một người quản trị mạng, bạn phải giải quyết được các vấn đề mâu thuẩn giữa các thiết bị WLAN như nhiễu, tương thích,…

Khi một sản phẩm đáp ứng được các yêu cầu về tính tương thích do WECA kiểm tra thì WECA sẽ gán cho sản phẩm đó một chứng nhận về tính tương thích và cho phép nhà sản xuất sử dụng logo wi-fi trong việc quảng cáo và đóng gói các sản phẩm đã được chứng nhận.

Một trong số các kiểm tra về tính tương thích của WECA là việc sử dụng khóa WEP 40 bit (lưu ý là 40 bit và 64 bit đều giống nhau). Một khóa mật 40 bit được nối với 24 bit vector khởi tạo IV (Initialization Vector) để có được khóa 64 bit. WECA không kiểm tra tính tương thích của khóa 128 bit vì thế không có gì đảm bảo cho tính tương thích giữa các sản phẩm có nhãn wi-fi khi sử dụng khóa 128 bit.

Có nhiều yếu tố khác ngoài khóa WEP 40 bit được yêu cầu trong tiêu chuẩn wi-fi. Những yếu tố này bao gồm việc hỗ trợ phân mảnh, chế độ tiết kiệm điện năng PSP (Power Save Polling), yêu cầu dò tìm định danh tập dịch vụ mở rộng ESSID (Extended Service Set IDentifier),,…

2. Viện chuẩn Viễn thông Châu Âu – ETSI

ETSI có nhiệm vụ đưa ra các chuẩn truyền thông ở Châu Âu giống với IEEE ở Mỹ. Các chuẩn mà ETSI đã thiết lập như HiPerLAN/2 là một chuẩn cạnh tranh trực tiếp với chuẩn 802.11 của IEEE. Sau đó IEEE đã đưa ra chuẩn 802.11h để có thể tương tác được với chuẩn HiPerLAN/2 của ETSI.

Trước đó, chuẩn HiPerLAN/1 đã hỗ trợ tốc độ lên đến 24 Mbps sử dụng công nghệ DSSS trong phạm vi 45 m. HiPerLAN/1 sử dụng băng tần UNII thấp và UNII trung giống như HiPerLAN/2, 802.11a và 802.11h.

Chuẩn HiPerLAN/2 hỗ trợ tốc độ lên đến 54 Mbps và sử dụng tất cả 3 băng tần của UNII. HiPerLAN/2 còn hỗ trợ chất lượng dịch vụ QoS (802.1p, RSVP – Resource Reservation Protocol, DiffServ-FC), DES (Data Encryption Standard), 3DES, ATM (Asynchronous Tranfer Mode), Ethernet, PPP (Point-to-Point Protocol), FireWire và 3G (Third Generation).

3. Tổ chức LAN không dây – WLANA

Nhiệm vụ của WLANA là giáo dục và làm tăng sự nhận thức của khách hàng về việc sử dụng WLAN cũng như đưa WLAN thành một chuẩn chung. WLANA có nhiều đối tác trong ngành công nghiệp đã đóng góp vào nội dung danh mục thông tin của WLANA. Trong danh mục này có rất nhiều nguồn tài nguyên thông tin phong phú về WLAN.

[... còn tiếp]

Tháng mùa 7

ưu đãi

Từ 1/7 đến 31/7/14

VnPro

Ưu đãi lên đến 20% cho học viên cũ*

Ưu đãi ngay 10% cho học viên mới*

Ưu đãi đặc biệt khi đăng ký đóng cặp các lớp ban ngày

LỊCH KHAI GIẢNG THÁNG 7

*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						
A8	CCNAX (200-120)	02/07/2014	2-3-4-5-6-7	08:30 – 11:30	3.360.000	152 giờ
AK12			2 – 4 – 6	18:30 – 21:30	6.720.000	
AK11		08/07/2014	3 – 5 - 7	08:30 – 11:30	3.360.000	
A7				18:30 – 21:30	6.720.000	
AK14		18/07/2014	2 – 4 – 6	08:30 – 11:30	3.360.000	
AK16				14:00 – 17:00	3.360.000	
A10				18:30 – 21:30	6.720.000	
AK18		21/07/2014	2-3-4-5-6-7	14:00 – 17:00	3.360.000	
AK13		24/07/2014	3 – 5 - 7	08:30 – 11:30	3.360.000	
AK15				14:00 – 17:00	3.360.000	
A9				18:30 – 21:30	6.720.000	
AK20		30/07/2014	2 – 4 – 6	08:30 – 11:30	3.360.000	
A12				18:30 – 21:30	6.720.000	
AV1	CCNA Voice (640-461)	22/07/2014	3 – 5 - 7	18:30 – 21:30	6.720.000	100 giờ
CHƯƠNG TRÌNH CCNP						
P1-K2	ROUTE (642-902)	16/07/2014	2 – 4 – 6	08:30 – 11:30	5.880.000	120 giờ
P1-4				18:30 – 21:30	8.232.000	
P1-3		24/07/2014	3 – 5 - 7	18:30 – 21:30	8.232.000	
P2K2	SWITCH (642-813)	10/07/2014	3 – 5 - 7	08:30 – 11:30	5.880.000	120 giờ
P2K4				14:00 – 17:00	5.880.000	
P2-3				18:30 – 21:30	8.232.000	
P3-3	TSHOOT (642-832)	15/07/2014	3 – 5 – 7	18:30 – 21:30	8.232.000	120 giờ
CHƯƠNG TRÌNH CCIE						
EW1	CCIE WRITTEN (Version 5)	30/07/2014	2 – 4 – 6	18:30 – 21:30	11.760.000	120 giờ

ĐĂNG KÝ HỌC LIÊN HỆ

THANH TRÂM Email: thanhtram@vnpro.org Di động: 0949 246 829
KIM LOAN Email: kimloan@vnpro.org Di động: 0936 393 167
LIÊN HỆ DỰ ÁN ĐÀO TẠO, TƯ VẤN HỆ THỐNG MẠNG, THUÊ THIẾT BỊ, PHÒNG HỌC, MUA SÁCH
Website: www.vnpro.vn Email: vnpro@vnpro.org Điện thoại: (08) 35124257

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**

VnPro®