VnPro Lịch Khai Giảng Tháng 11

- Ưu đãi đặc biệt cho học viên đóng nhóm
- Ưu đãi 10% học phí cho học viên cũ
- Tặng áo thun khi đăng ký học

Mã lớp	Tên khóa học	Ngày khai giảng	Ngày học	Giờ học	Học phí/khóa	Thời gian
CHƯƠNG TRÌNH CCNA & CCNA SECURITY						
AK30	CCNAX	01/11/2013	2 – 4 – 6	8:30 – 11:30AM	3.360.000 vnđ	152 giờ
A28				6:30 – 9:30PM	6.720.000 vnđ	
AK29		07/11/2013	3 – 5 - 7	8:30 – 11:30AM	3.360.000 vnđ	
AK31				2:00 – 5:00PM	3.360.000 vnđ	
A29				6:30 – 9:30PM	6.720.000 vnđ	
AK32		15/11/2013	2 – 4 – 6	8:30 – 11:30AM	3.360.000 vnđ	
AK34				2:00 – 5:00PM	3.360.000 vnđ	
AK34		18/11/2013	2-3-4-5-6-7	2:00 – 5:00PM	3.360.000 vnđ	
AK33		21/11/2013	3 – 5 - 7	8:30 – 11:30AM	3.360.000 vnđ	
A31				6:30 – 9:30PM	6.720.000 vnđ	
AS2	CCNA Security	18/11/2013	2 – 4 – 6	6:30 – 9:30PM	6.720.000 vnđ	100 giờ
CHƯƠNG TRÌNH CCNP & CCNP SECURITY						
P1K4	ROUTE (642-902)	08/11/2013	2 – 4 – 6	8:30 – 11:30AM	5.880.000vnđ	120 giờ
P1K6				2:00 – 5:00PM	5.880.000vnđ	
P1-6				6:30 – 9:30PM	8.232.000vnđ	
P2K2	SWITCH (642-813)	04/11/2013	2 – 4 – 6	8:30 – 11:30AM	5.880.000vnđ	120 giờ
				6:30 – 9:30PM	8.232.000vnđ	
P2K3		19/11/2013	3 – 5 - 7	2:00 – 5:00PM	5.880.000vnđ	
P2-3				6:30 – 9:30PM	8.232.000vnđ	
P3K1	TSHOOT (642-832)	07/11/2013	3 – 5 – 7	8:30 – 11:30AM	5.880.000vnđ	120 giờ
P3-3				6:30 – 9:30PM	8.232.000vnđ	
PS13	FIREWALL	26/11/2013	3 – 5 – 7	6:30 – 9:30PM	8.232.000vnđ	100 giờ
CHƯƠNG TRÌNH CCIE WRITTEN						
EW2	CCIE Written	11/11/2013	2 – 4 – 6	6:30 – 9:30PM	11.760.000vnđ	120 giờ

Đăng ký học liên hệ :

THANH TRÂM — EMAIL : THANHTRAM@VNPRO.ORG — MOBILE : 0949.246.829 - 0906.61.63.22
KIM LOAN — EMAIL : KIMLOAN@VNPRO.ORG — MOBILE : 0936.39.31.67
LIÊN HỆ DỰ ÁN ĐÀO TẠO HOẶC DỊCH VỤ KHÁC:
MINH TUẤN — EMAIL : PHAMMINHTUAN@VNPRO.ORG — MOBILE : 0986.900.869

CCNAX v2.0

Trung Tâm Tin Học VnPro - 149/1D Ung Văn Khiêm, P.25, Q.BT, TP.HCM - (84.8)35124257 - Email: vnpro@vnpro.org

Bản tin Dân Cisco - Được phát hành bởi **Công Ty TNHH Tư Vấn & Dịch Vụ Chuyên Việt**
Chịu trách nhiệm xuất bản: **Phạm Minh Tuấn**
Giấy phép xuất bản số: **69/QĐ - STTTT** Ngày ĐK: **26/10/2011**
Công ty in: **Sao Băng Design**
Số lượng in: **2.000 cuốn/kỳ**
Kỳ hạn xuất bản: **1 kỳ/tháng**

Số 23
11/2013

BẢN TIN dan CISCO

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

Thiết lập Site to Site VPN giữa ASA Firewall và Cisco Router

Trong sơ đồ bên dưới, site (Remote1) được trang bị Cisco ASA firewall (sử dụng bất kỳ model nào) và site (Remote2) được trang bị Cisco Router. Thiết bị Cisco ASA firewall theo mặc định hỗ trợ IPSEC VPN như trên Cisco Router chúng ta cần ...

(Trang 03)

CCNA MỞ RỘNG CƠ HỘI NGHỀ NGHIỆP

Theo thống kê indeed.com (trang web kiếm việc hàng top thế giới) thì mức lương CCNA trung bình 83.000 USD/ năm (~ 7.000USD/ tháng) và ...

(Trang 07)

Chúc Mừng Ngày Nhà Giáo Việt Nam

VnPro gửi lời tri ân sâu sắc đến Thầy Cô nhân ngày 20/11

KỸ NĂNG GIAO TIẾP ỨNG XỬ

Giao tiếp ứng xử là một hoạt động thường ngày của mỗi chúng ta, thế nhưng không phải cứ thực hiện nhiều là bạn đã "thành thạo". Trên thực tế, có ...

(Trang 08)

THẦY VÒNG CHẤN NGUYÊN đạt chứng chỉ cao cấp hàng đầu của Cisco CCIE VOICE # 40970

(Trang 05)

TIN TỨC SỰ KIỆN KHÁC

Cisco IOS cập nhật tám lỗ hổng bảo mật từ chối dịch vụ Denial of Service (ưu điểm: tốt, khuyết: cisco yếu)

Trong tháng 9, Cisco đã tiến hành cập nhật 8 lỗ hổng bảo mật ảnh hưởng đến tính sẵn sàng của các thiết bị trên nhiều version của các IOS software khác nhau.

IOS là một hệ điều hành đa tác vụ kết hợp chức năng giữa "networking" và "telecommunication" và được sử dụng trên nhiều thiết bị mạng của nhiều doanh nghiệp hiện nay.

Tất cả các lỗ hổng bảo mật được vá lỗi có thể ảnh hưởng đến tính hoạt động liên tục của thiết bị nếu chúng được khai thác bởi các đối tượng tấn công. Chúng ta có thể ảnh hưởng đến quá trình hoạt động trên Cisco IOS khi triển khai các công nghệ, giao thức như Network Time Protocol (NTP), Internet Key Exchange protocol, the Dynamic Host Configuration Protocol (DHCP), Resource Reservation Protocol(RSVP), tính năng virtual fragmentation reassembly (VFR) dành cho IP version 6 (IPv6), Zone-Based Firewall (ZBFW) , T1/E1 driver queue và chức năng Network Address Translation (NAT) dành cho DNS (Domain Name System) và PPTP (Point-to-Point Tunneling Protocol).

Các lỗ hổng bảo mật có thể được phát hiện và khai thác bởi các đối tượng tấn công bằng cách gửi đi các "crafted packet" tới các thiết bị mạng sử dụng IOS được kích hoạt các tính năng như đã đề cập trên.

Tùy thuộc vào lỗ hổng bảo mật nhất định được khai thác, các đối tượng tấn công có thể khiến cho các thiết bị này bị treo, khởi động lại hoặc mất kết nối các phiên làm việc tại thiết bị, các kết nối định tuyến hoặc tạo điều kiện cho các cuộc tấn công từ chối dịch vụ denial-of-service (DoS) khác được thực hiện.

Để hạn chế các nguy cơ bảo mật trên, người sử dụng sẽ phải cài đặt các bản vá "patched version" của IOS software tương ứng với phiên bản "version" hiện tại mà họ đang sử dụng.

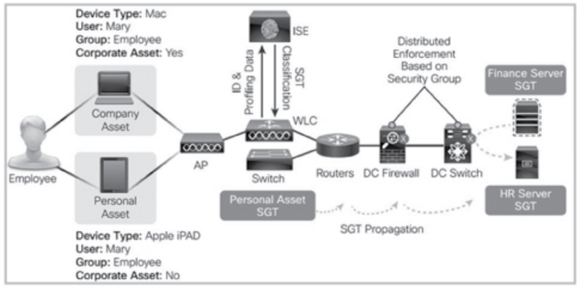
Phía doanh nghiệp sẽ không nhận biết bất kỳ lỗ hổng bảo mật nào cho đến khi họ quan sát các thông báo giám sát hệ thống mạng.

Tất cả các cập nhật bảo mật có thể tìm thấy tại liên kết http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130925-ntp

[Người dịch: Bùi Quốc Kỳ]

Liên kết tham khảo:
http://blog.router-switch.com/2013/09/cisco-ios-updates-fix-eight-denial-of-service-vulnerabilities/

Công nghệ Cisco TrustSec



Cisco TrustSec giúp đơn giản hóa việc cung cấp và quản lý việc truy cập một cách an toàn đến các ứng dụng và dịch vụ mạng. So với cơ chế kiểm soát truy cập dựa trên network topology, Cisco TrustSec xác định các chính sách bằng cách sử dụng các nhóm chính sách luận lý, thế nên việc truy cập một cách bảo mật luôn luôn được duy trì kể cả khi các tài nguyên mạng được chuyển từ nơi này đến nơi khác hoặc đi chuyển trong môi trường ảo hóa. Việc cách ly quyền truy cập giữa các địa chỉ IP và các VLAN giúp đơn giản hóa công việc duy trì chính sách bảo mật, giảm chi phí hoạt động của hệ thống, cho phép các chính sách truy cập phổ biến được áp dụng cho các dạng truy cập như truy cập có dây, không dây và VPN.

Các chức năng chính sách của Cisco TrustSec được nhúng vào các thiết bị của Cisco như thiết bị chuyển mạch, định tuyến, mạng không dây và tường lửa. Nhờ việc phân loại traffic dựa vào đặc trưng ngữ cảnh của từng endpoint với các địa chỉ IP của chúng, Cisco TrustSec cho phép việc kiểm soát truy cập linh hoạt hơn trong nhiều môi trường mạng cũng như các data center.

Về vấn đề truy cập mạng, 1 nhóm chính sách Cisco TrustSec được gọi là 1 Security Group Tag(SGT), nó được gán cho 1 endpoint dựa vào user, thiết bị và vị trí của endpoint đó. SGT bao hàm các quyền truy cập của endpoint và tất cả traffic mang thông tin SGT xuất phát từ SGT. Các switch, router và các firewall dùng SGT để quyết định việc forward traffic.

Với Cisco TrustSec, người quản trị mạng có thể triển khai các phân đoạn mạng lớn và kiểm soát truy cập mà không cần thay đổi kiến trúc mạng (như việc thêm VLAN) cũng như các quy định về quản trị, điều này giúp đơn giản hóa cho việc quản trị và vận hành mạng. Các chính sách Cisco TrustSec được quản lý tập trung bởi Cisco Identity Services Engine (ISE) với các chức năng sẵn có trong các switch mạng campus, data center, tường lửa và các router.

[Người dịch: Phạm Quốc Bảo]

Liên kết tham khảo:
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11640/at_a_glance_c45-726831.pdf

10 "tử huyệt" chôn vùi bạn khi thuyết trình trước đám đông

Phát biểu trước nhiều người là việc tương đối khó khăn đối với hầu hết mọi người, vì vậy chúng ta thường hay bối rối không biết xử lý tình huống này như thế nào. Nếu bạn đã có sự chuẩn bị, bạn sẽ tránh khỏi việc trở thành "anh hề" trước mọi người. Một khi bạn đã vượt qua những nỗi sợ hãi khi nói trước đám đông, bạn có thể bắt đầu học những kỹ năng giúp bạn trở thành một nhà hùng biện. Tuy nhiên, trước đó, bạn nên "thuộc lòng" 10 điều cần tránh khi phát biểu trước đám đông, và trong bài viết này, NLL xin chia sẻ với các bạn về những điều đó

1. Ăn mặc luộm thuộm

Cái nhìn đầu tiên của mọi người nhìn vào bạn chính là bạn ăn mặc quần áo như thế nào. Một người ăn mặc lịch sự luôn thể hiện được đẳng cấp của mình trước đám đông. Còn ăn mặc luộm thuộm sẽ nói lên đẳng cấp và địa vị thấp kém của mình. Nếu bạn không biết cách ăn mặc đúng mực, bạn nên nhờ người khác giúp đỡ

2. Tác phong, tư thế không đàng hoàng

Đây là điều bắt buộc phải tránh. Dù là đứng hay ngồi thì bạn cũng phải chắc chắn rằng, chân bạn đứng vững trên sàn. Tránh tối đa dồn hết cả trọng lượng lên một bên chân, hoặc đứng vắt chéo chân. Hình ảnh này sẽ tạo ấn tượng về một con người bấp bênh và mọi người sẽ cho rằng, bạn không được tự tin lắm trong lần phát biểu này.Nếu bạn phát biểu trước bục, không nên dựa người vào đó, cũng đừng giữ khư khư bản bảo cáo. Hãy nhớ rằng dưới ghế khán giả có rất nhiều cặp mắt đang dõi theo bạn, hãy tạo cho mình một tác phong thật đĩnh đạc

3. Phát biểu như đọc từ văn bản viết sẵn

Viết bài phát biểu ra chưa đủ; bạn phải nói được như đang đứng trước mọi người. Nếu quên những điểm mấu chốt, hãy ghi chú vào tờ giấy nhỏ và xem lại khi cần thiết. Tuy nhiên diễn thuyết không phải đơn giản là cầm tờ giấy được vạch sẵn và đọc to, rõ ràng. Nếu bạn chỉ cầm giấy và đọc thì không khác gì đang học môn "Tập đọc" ở trường và dám chắc mọi người ở dưới không ai muốn trở thành "giáo viên dự giờ bất đắc dĩ"

4. Lẩn tránh tiếp xúc mắt với khán giả

Ánh mắt là một trong những cách chủ yếu để thu hút sự chú ý của khán giả. Để thu hút sự tập chung bạn phải làm cho mọi người cảm thấy rằng bạn đang nói với họ chứ không phải nói với cái trần nhà hay cái phòng mà họ đang ngồi đó. Nhìn trực tiếp là một trong những cách quan trọng để thu hút sự tập chung.Đừng nhìn ra ngoài, hãy nhìn tất cả các khán giả từ từ bởi vì liếc mắt nhanh làm bạn trông có vẻ mang tâm trạng không tự tin. Khi bạn chú ý đến một khán giả hãy giữ ánh mắt của bạn trong vài giây nhưng không được quá lâu vì điều này khiến khán giả mất tự nhiên và sợ hãi (làm người nghe lo lắng không phải là quy tắc nói trước công chúng).

5. Không tập dượt trước những gì sẽ phát biểu

Đây sẽ là điều hết sức nguy hiểm, đặc biệt khi bài phát biểu của bạn mang tính chất quan trọng. Hãy tập bài thuyết trình ở nhà hoặc bất cứ nơi đâu bạn cảm thấy dễ chịu và thoải mái, trước gương, gia đình mình, bạn bè hay đồng nghiệp. Sử dụng một máy ghi âm và lắng nghe chính mình. Ngoài ra có thể quay phim phần trình bày và phân tích kỹ lưỡng để thấy được điểm mạnh điểm yếu của bản thân . Cố gắng phát huy ưu điểm trong suốt thời gian trình bày.

6. Đứng yên như pho tượng

Những nhà diễn thuyết xuất chúng không đứng yên như lính chào vì làm như vậy bài phát biểu của họ sẽ trở nên nhạt nhẽo. Thay vào đó họ di chuyển qua lại, sử dụng cử chỉ đôi tay một cách chừng mực, không lạm dụng, quá đà giọng nói và cử chỉ của họ rất linh hoạt.

7. Lạm dụng slide

Những nhà diễn thuyết xuất chúng luôn đánh giá cao khả năng tiếp thu của khán giả. Họ không đọc từng chữ trên slide và hiểu slide chỉ là công cụ hỗ trợ cho lời nói chứ không thể thay lời nói. Đừng viết quá nhiều từ trên slide mà chỉ tối đa 6 hàng với mỗi hàng 4 từ là đủ. Nếu cần tô thêm màu để nhấn mạnh, phần còn lại để cho khán giả.

8. Nói dông dài

Những nhà diễn thuyết xuất chúng hiểu sức mạnh của 1 bài phát biểu ngắn gọn, rõ ràng và cô đọng. Nhiều nghiên cứu chỉ ra rằng, khán giả mất dần sự tập trung khi bài nói dài quá 18 phút. Tiếc thay, nhiều doanh nhân cứ tưởng rằng, nói càng dài khán giả càng tiếp thu tốt. Lời khuyên là bạn không nên bỏ ra 5 phút để nói những điều có thể nói gọn trong 30s. Ngay cả nói chuyện điện thoại, chat và email cũng nên ngắn gọn.

9. Không tạo được không khí phấn khích

Những nhà diễn thuyết xuất chúng luôn biết cách huy động sự chú ý của khán giả từ lúc mới bước vào cửa và khán giả thường nhớ những gì họ phát biểu từ đầu đến cuối. Hãy giao lưu với khán giả mỗi khi có triệu chứng gà gật xuất hiện. Đây là cách cho khán giả tham gia vào bài phát biểu của mình để tạo không khí.

10. Kết thúc bài phát biểu 1 cách nhạt nhẽo

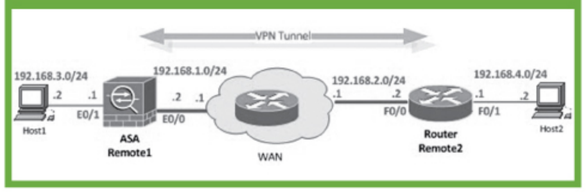
Những nhà diễn thuyết xuất chúng luôn dành cho phần kết bài phát biểu một ý mới thú vị chưa đề cập trong bài. Nghiên cứu cho thấy, không phải phần giữa bài phát biểu giữa bài phát biểu thường dùng để chuyển tải những ý quan trọng mới lưu lại cho người nghe mà chính phần kết thúc mới được họ lưu giữ nhiều nhất. Tính bất ngờ của phần kết thúc chính là bản lĩnh của diễn giả.

Thuyết trình trước đám đông là một việc khó khăn nhưng không có nghĩa là bạn không có thể làm được. Hi vọng những chia sẻ trên của NLL có thể giúp các bạn tránh các "tử huyệt" để không tự chôn vùi hình ảnh của mình khi thuyết trình trước đám đông. Chúc các bạn thành công !

[Sưu tầm]

Thiết lập Site to Site VPN giữa ASA Firewall và Cisco Router

Trong sơ đồ bên dưới, site (Remote1) được trang bị Cisco ASA firewall (sử dụng bất kỳ model nào) và site (Remote2) được trang bị Cisco Router. Thiết bị Cisco ASA firewall theo mặc định hỗ trợ IPSEC VPN như trên Cisco Router chúng ta cần kiểm tra xem liệu IOS software có hỗ trợ VPN tunnel được mã hóa hay không.



Các thiết bị được sử dụng trong bài LAB:

- ASA 5510–Cisco Adaptive Security Appliance Software Version 8.0(3)
- Cisco Router 2801–C2801-ADVIPSERVICESK9-M Version 12.4(9)T4

Kịch bản giả định:

Hệ thống LAN tại Remote1 có nhu cầu kết nối tới hệ thống LAN đặt tại Remote2 thông qua đường VPN Tunnel. Hạ tầng mạng WAN trong trường hợp này là hệ thống Internet, vì thế cần phải thiết lập kết nối an toàn giữa hai hệ thống mạng LAN lại với nhau trên hạ tầng mạng Internet.

Thao tác đầu tiên chúng ta cần thực hiện là đảm bảo các kết nối outside interface của ASA và router có thể giao tiếp được với nhau trên hạ tầng mạng WAN. Sau đó, chúng ta sẽ tiến hành thiết lập cấu hình IPSEC VPN như sau.

Cấu hình tại Cisco ASA

Đầu tiên, chúng ta sẽ tiến hành định nghĩa một Access list chỉ định loại lưu lượng nào sẽ được mã hóa. Nếu lưu lượng khớp với điều kiện IP nguồn là 192.168.3.0/24 và IP đích là 192.168.4.0/24, lưu lượng đó sẽ được mã hóa và gửi đi trên đường tunnel.

```
ASA(config)# access-list vpn extended permit ip 192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0

!IKE PHASE #1
! I've created a phase1 policy. This policy provides secured process of exchanging Keys.
ASA(config)# crypto isakmp policy 1

! For authentication I used Pre-shared. This method is most frequently used today.
ASA(config)# authentication pre-share

!For encryption I used 3des.
ASA(config)# encryption 3des

! Hashing md5.
ASA(config)# hash md5

! I used second group of diffie-hellman. Group1 is used by default. The most secured is Group5.
ASA(config)# group 2

! configure crypto key. The keys must match to each other between peers. Otherwise Phase1 will not be completed.
ASA(config)# crypto isakmp secretsharedkey address 192.168.2.2
```

Lưu ý: Crypto key sẽ được ẩn đi trong cấu hình của ASA. Nếu chúng ta quan sát phần cấu hình, nội dung mà chúng ta quan sát được tương tự như minh họa bên dưới.

```
tunnel-group 192.168.2.2 ipsec-attributes
pre-shared-key *

! Activate policy on Outside interface.
ASA(config)# crypto isakmp enable outside

! IKE PHASE #2- VPN Tunnel is established during this phase and the traffic between VPN Peers is encrypted according to the security parameters of this phase.
! I created Transform-set, by which the traffic will be encrypted and hashed between VPN peers.
ASA(config)# crypto ipsec transform-set ts esp-3des esp-md5-hmac

! Apply the access list created earlier for matching the interesting traffic.
ASA(config)# crypto map vpn 10 match address vpn

! I indicated address of Remote2 peer public outside interface.
ASA(config)# crypto map vpn 10 set peer 192.168.2.2

! Apply also the transform-set.
ASA(config)# crypto map vpn 10 set transform-set ts

! Attach the already created Crypto-map and VPN to outside interface.
ASA(config)# crypto map vpn interface outside
```

Tiếp theo, ta sẽ tiến hành cấu hình tại Router.

Cấu hình tại Cisco Router

```
ISAKMP Phase 1

! Enter crypto-isakmp policy configuration mode for configuring crypto isakmp policy.
Router(config)# crypto isakmp policy 10

! Turn on 3des as an encryption type.
Router(config)# encr 3des

! I indicated MD5 as a hashing type.
Router(config)# hash md5

! I indicated pre-share authentication.
Router(config)# authentication pre-share

! I used second group of diffie-hellman. group1 is used by default.
Router(config)# group 2

! I defined peer key same as ASA site.
Router(config)# crypto isakmp secretsharedkey address 192.168.1.2
```

Thông tin chỉ số policy number không cần phải khớp nhau, điều quan trọng là các tham số trong chính sách policy phải giống nhau giữa hai bên. Nếu các tham số này không khớp nhau, phiên Phase1 sẽ không bao giờ được thiết lập thành công.

```
! Access list for matching interesting traffic.
Router(config)# ip access-list extended vpn
Router(config)# permit ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255

ISAKMP PHASE 2
!
! Create IPSEC transform-set, by which the mechanism of hashing and encryption is determined, by which the traffic will be hashed/encrypted in VPN tunnel later.
Router(config)# crypto ipsec transform-set ts esp-3des esp-md5-hmac

! Enter into crypto-map configuration mode.
Router(config)# crypto map vpn 10 ipsec-isakmp

! Indicate IP address of peer.
Router(config)# set peer 192.168.1.2

! Indicate IPsec transform-set created above.
Router(config)# set transform-set ts

! Apply access list created above.
Router(config)# match address vpn

! Apply crypto-map to interface.
Router(config)# interface FastEthernet0/0
Router(config)# crypto map vpn
```

Với câu lệnh trên, các thông tin cấu hình VPN bắt đầu có hiệu lực.

```
! In the output below it is shown that ISAKMP PHASE1 is active, which means that negotiation of PHASE1 is completed successfully.
ASA# show crypto isakmp sa

Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 192.168.2.2
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE

Router# show crypto isakmp sa
dst src state conn-id slot
192.168.1.2 192.168.2.2 MM_ACTIVE 1 0
```

! Checking ISAKMP PHASE2. Here we see that IPSec is working and the interesting traffic flows in VPN Tunnel.

```
ASA# show crypto ipsec sa
interface: outside
Crypto map tag: vpn, seq num: 10, local addr: 192.168.1.2

access-list vpn permit ip 192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
current_peer: 192.168.2.2

#pkts encaps: 344, #pkts encrypt: 344, #pkts digest: 344
#pkts decaps: 344, #pkts decrypt: 344, #pkts verify: 344
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 344, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #framents created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#send errors: 0, #recv errors: 0

Router# show crypto ipsec sa
interface: FastEthernet0/0
Crypto map tag: vpn, local addr 192.168.2.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer 192.168.1.2 port 500
PERMIT, flags={origin_is_acl,}

#pkts encaps: 344, #pkts encrypt: 344, #pkts digest: 344
#pkts decaps: 344, #pkts decrypt: 344, #pkts verify: 344
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

Với thông tin hiển thị trên, ta có thể xác nhận đường VPN Tunnel đã được thiết lập thành công

[Người dịch: Bùi Quốc Kỳ]

Liên kết tham khảo:
http://blog.router-switch.com/2013/05/site-to-site-vpn-between-asa-firewall-cisco-router/

THẦY VÒNG CHẤN NGUYÊN

đạt chứng chỉ cao cấp hàng đầu của Cisco CCIE VOICE # 40970

Sáng ngày 21/10/2013 VnPro hân hoan chúc mừng khi nhận được tin vui từ Thầy Vòng Chấn Nguyên - Giảng viên VnPro, anh đã đem vinh dự đến cho cộng đồng Networker Việt Nam, CCIE (Cisco Certified Internetwork Expert) đầu tiên của Việt Nam về mảng Voice với Magic Number # 40970 sau khi vượt qua kì thi cam go vào ngày 19/10/2013 tại Hồng Kong trong suốt 8h đồng hồ.

Giờ đây, VnPro đã có thêm 1 CCIE Lab – người thứ 10 trong hơn 10 năm hoạt động, điều này cũng góp phần nâng số CCIE tại Việt Nam hiện tại lên vượt ngưỡng 40.

CCIE Voice là một trong những chứng chỉ mạng thuộc hàng danh giá nhất thế giới, theo thống kê Cisco mới nhất của Cisco live, hiện tại số lượng CCIE Voice trên toàn thế giới vào khoảng gần 2400

Để đạt được chứng chỉ Cisco cao cấp này, thí sinh bắt buộc phải có kinh nghiệm thực tế, tiếp cận với rất nhiều mô hình lớn, thực tế bên ngoài. Một CCIE Voice là một chuyên gia trong việc xây dựng, thiết kế giải pháp, khắc phục sự cố về VoIP, cấu hình một mạng điện thoại nhiều thành phần từ đầu đến cuối (end-to-end).

CCIE Information Worldwide

Total of Worldwide CCIEs:	38,005*
Total of Routing and Switching CCIEs:	27,552
Total of Security CCIEs:	4,264
Total of Service Provider CCIEs:	3,142
Total of Voice CCIEs:	2,341
Total of Wireless CCIEs:	64

Multiple Certifications

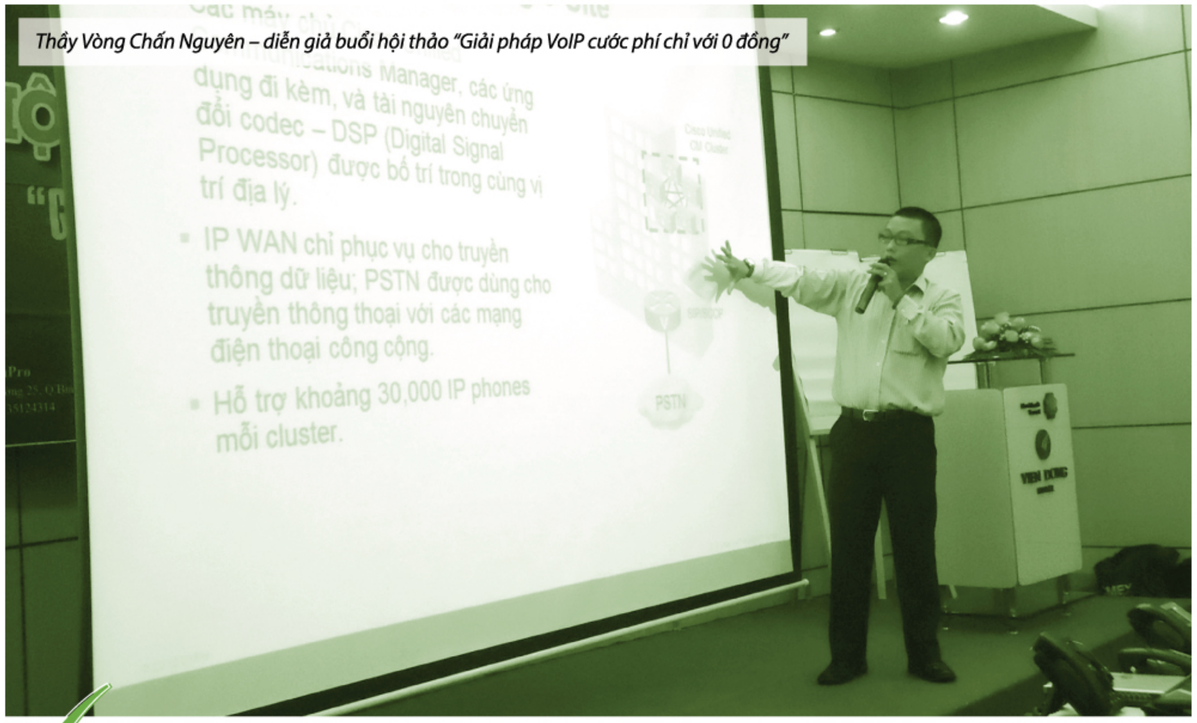
Many CCIEs Have Gone on to Pass the Certification Exams In Additional Tracks, Becoming a "Multiple CCIE." Below Are Selected Statistics on CCIEs Who Are Certified in More Than One Track

Total with Multiple Certifications Worldwide:	3,547*
Total of Routing and Switching and Security CCIEs:	1026
Total of Routing and Switching and Service Provider CCIEs:	1053
Total of Routing and Switching and Voice CCIEs:	502
Total with 3 Certifications	511
Total with 4 Certifications	110
Total with 5 or More Certifications	25

VoIP là ngành đang có rất nhiều triển vọng, xu hướng VoIP trong tương lai hứa hẹn sẽ phát triển rất mạnh mẽ. Hiện tại có rất nhiều tập đoàn đã và đang ứng dụng các giải pháp VoIP để giảm chi phí cước thoại tối đa cho doanh nghiệp mình. Ngoài ra, việc chạy thoại (Voice) trên nền IP sẽ tạo ra sự hợp nhất, do dễ dàng kết hợp các ứng dụng đang chạy trên nền IP tích hợp thoại, sẽ tạo lợi thế rất lớn trong việc triển khai các chiến lược chăm sóc khách hàng cho doanh nghiệp lớn tới doanh nghiệp vừa và nhỏ.

Hy vọng trong tương lai trong tương lai gần, VnPro sẽ có nhiều học viên đạt chứng chỉ CCIE Voice danh giá này.

[P. Giảng Viên VnPro]



Thầy Vòng Chấn Nguyên – diễn giả buổi hội thảo "Giải pháp VoIP cước phí chỉ với 0 đồng"

VnPro gửi lời tri ân sâu sắc đến Thầy Cô nhân ngày 20/11

- Nếu hỏi: *"Thành công bắt nguồn từ đâu?"*

Tôi sẽ trả lời rằng *"Là Thầy – người đã mang đến cho chúng tôi kiến thức, hành trang bước vào đời".*

Anh Lê Võ Thanh Tân, học viên VnPro tâm sự: "Sau khi tốt nghiệp trung học phổ thông mình theo học ngành quản trị kinh doanh được 1 năm thì gia đình mở dịch vụ Internet. Khi bắt đầu hoạt động, mình có theo 1 anh IT phụ giúp cho nhanh và học lõm tin học, cũng từ đó mình đam mê công nghệ thông tin hơn nên quyết định chuyển ngành sang network. Sau đó, có thể là do duyên may, được sự giới thiệu của một người anh thuộc hàng gạo cội trong giới CNTT, mình có dịp tiếp xúc và theo học các khóa đào tạo chuyên gia quản trị mạng quốc tế tại VnPro.

Hơn nữa, tại VnPro "nhờ các thầy tận tình hướng dẫn và tư vấn, con đường network của *mình trở nên rõ ràng hơn bao giờ hết*, giúp cho niềm đam mê về công nghệ trong mình càng sâu sắc hơn và đặc biệt là công nghệ mạng hàng đầu Cisco

[…]

Và hiện tại mình đang làm ở vị trí *chuyên gia tư vấn giải pháp VoIP, hạ tầng mạng*"

- Nghề giáo bao đời nay luôn được xem là nghề cao quý, nghề *"trồng người"*. Người thầy, dù ở đâu cũng là những người được kính trọng nhất. Và tại VnPro, trong hơn *10 năm hoạt động*, VnPro càng thấm nhuần hai chữ ấy.

Bên cạnh niềm tự hào xây dựng được một hệ thống đào tạo mạng chuyên nghiệp, hiện đại với khả năng cung cấp các *khóa học toàn diện và chất lượng* hàng đầu tại Việt Nam.

- **VnPro còn là trung tâm duy nhất khắp cả nước phát hành và xuất bản hơn 20 đầu sách mạng tiếng Việt ở mọi cấp độ**
- **Đào tạo hơn 11000 học viên**
- **Là trung tâm duy nhất đã có 10 CCIE Lab hàng đầu Việt Nam, góp phần nâng số CCIE tại Việt Nam hiện tại lên vượt ngưỡng 40**

Đó cũng chính nhờ vào sự đóng góp to lớn ngày đêm của hơn 40 thầy cô, giảng viên hiện là các chuyên gia hàng đầu trong các công ty lớn trên toàn quốc.

- Nhân ngày Nhà giáo Việt Nam, VnPro xin chúc tất cả các thầy cô luôn luôn mạnh khoẻ, trẻ trung, vui tính, chúc cho mọi lời chúc của tất cả học trò dành cho các thầy các cô đều trở thành hiện thực. Và các Thầy Cô sẽ đào tạo ra nhiều, nhiều hơn nữa các chuyên gia quản trị mạng hàng đầu Việt Nam.

VnPro

Trân trọng!

THẦY VÒNG CHẤN NGUYÊN

đạt chứng chỉ cao cấp hàng đầu của Cisco CCIE VOICE # 40970

Sáng ngày 21/10/2013 VnPro hân hoan chúc mừng khi nhận được tin vui từ Thầy Vòng Chấn Nguyên - Giảng viên VnPro, anh đã đem vinh dự đến cho cộng đồng Networker Việt Nam, CCIE (Cisco Certified Internetwork Expert) đầu tiên của Việt Nam về mảng Voice với Magic Number # 40970 sau khi vượt qua kì thi cam go vào ngày 19/10/2013 tại Hồng Kong trong suốt 8h đồng hồ.

Giờ đây, VnPro đã có thêm 1 CCIE Lab – người thứ 10 trong hơn 10 năm hoạt động, điều này cũng góp phần nâng số CCIE tại Việt Nam hiện tại lên vượt ngưỡng 40.

CCIE Voice là một trong những chứng chỉ mạng thuộc hàng danh giá nhất thế giới, theo thống kê Cisco mới nhất của Cisco live, hiện tại số lượng CCIE Voice trên toàn thế giới vào khoảng gần 2400

Để đạt được chứng chỉ Cisco cao cấp này, thí sinh bắt buộc phải có kinh nghiệm thực tế, tiếp cận với rất nhiều mô hình lớn, thực tế bên ngoài. Một CCIE Voice là một chuyên gia trong việc xây dựng, thiết kế giải pháp, khắc phục sự cố về VoIP, cấu hình một mạng điện thoại nhiều thành phần từ đầu đến cuối (end-to-end).

CCIE Information Worldwide

Total of Worldwide CCIEs:	38,005*
Total of Routing and Switching CCIEs:	27,552
Total of Security CCIEs:	4,264
Total of Service Provider CCIEs:	3,142
Total of Voice CCIEs:	2,341
Total of Wireless CCIEs:	64

Multiple Certifications

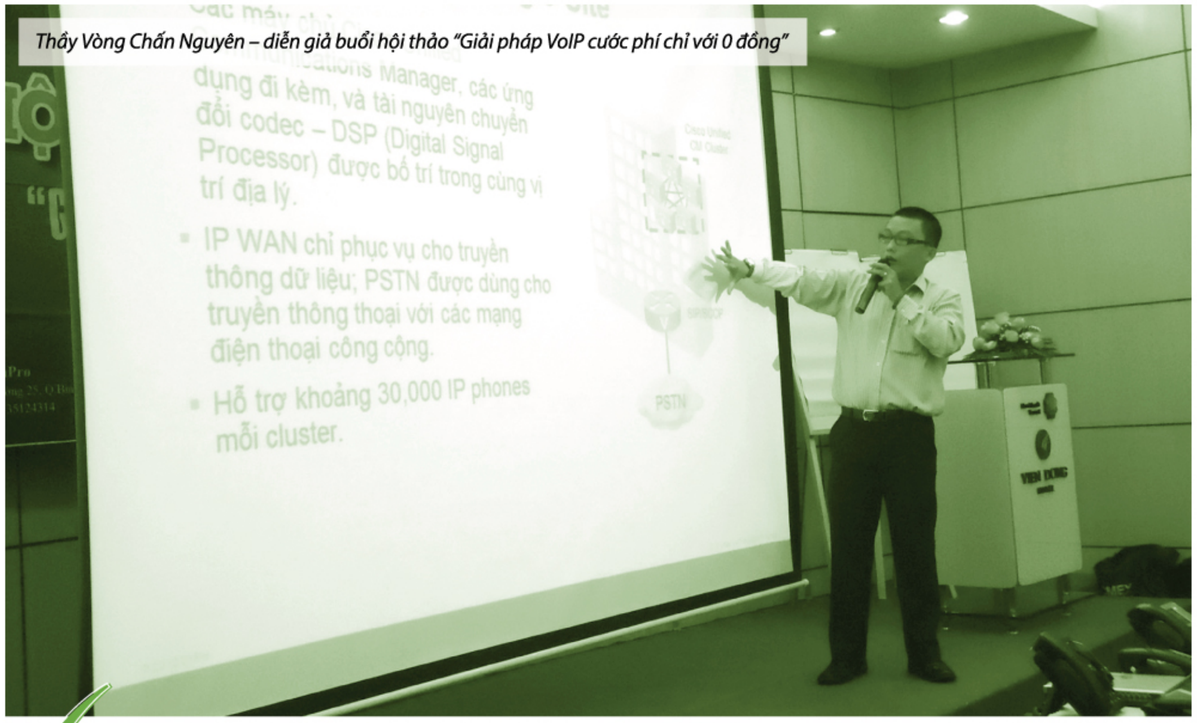
Many CCIEs Have Gone on to Pass the Certification Exams In Additional Tracks, Becoming a "Multiple CCIE." Below Are Selected Statistics on CCIEs Who Are Certified in More Than One Track

Total with Multiple Certifications Worldwide:	3,547*
Total of Routing and Switching and Security CCIEs:	1026
Total of Routing and Switching and Service Provider CCIEs:	1053
Total of Routing and Switching and Voice CCIEs:	502
Total with 3 Certifications	511
Total with 4 Certifications	110
Total with 5 or More Certifications	25

VoIP là ngành đang có rất nhiều triển vọng, xu hướng VoIP trong tương lai hứa hẹn sẽ phát triển rất mạnh mẽ. Hiện tại có rất nhiều tập đoàn đã và đang ứng dụng các giải pháp VoIP để giảm chi phí cước thoại tối đa cho doanh nghiệp mình. Ngoài ra, việc chạy thoại (Voice) trên nền IP sẽ tạo ra sự hợp nhất, do dễ dàng kết hợp các ứng dụng đang chạy trên nền IP tích hợp thoại, sẽ tạo lợi thế rất lớn trong việc triển khai các chiến lược chăm sóc khách hàng cho doanh nghiệp lớn tới doanh nghiệp vừa và nhỏ.

Hy vọng trong tương lai trong tương lai gần, VnPro sẽ có nhiều học viên đạt chứng chỉ CCIE Voice danh giá này.

[P. Giảng Viên VnPro]



Thầy Vòng Chấn Nguyên – diễn giả buổi hội thảo "Giải pháp VoIP cước phí chỉ với 0 đồng"

VnPro gửi lời tri ân sâu sắc đến Thầy Cô nhân ngày 20/11

- Nếu hỏi: *"Thành công bắt nguồn từ đâu?"*

Tôi sẽ trả lời rằng *"Là Thầy – người đã mang đến cho chúng tôi kiến thức, hành trang bước vào đời".*

Anh Lê Võ Thanh Tân, học viên VnPro tâm sự: "Sau khi tốt nghiệp trung học phổ thông mình theo học ngành quản trị kinh doanh được 1 năm thì gia đình mở dịch vụ Internet. Khi bắt đầu hoạt động, mình có theo 1 anh IT phụ giúp cho nhanh và học lõm tin học, cũng từ đó mình đam mê công nghệ thông tin hơn nên quyết định chuyển ngành sang network. Sau đó, có thể là do duyên may, được sự giới thiệu của một người anh thuộc hàng gạo cội trong giới CNTT, mình có dịp tiếp xúc và theo học các khóa đào tạo chuyên gia quản trị mạng quốc tế tại VnPro.

Hơn nữa, tại VnPro "nhờ các thầy tận tình hướng dẫn và tư vấn, con đường network của *mình trở nên rõ ràng hơn bao giờ hết*, giúp cho niềm đam mê về công nghệ trong mình càng sâu sắc hơn và đặc biệt là công nghệ mạng hàng đầu Cisco

[…]

Và hiện tại mình đang làm ở vị trí *chuyên gia tư vấn giải pháp VoIP, hạ tầng mạng*"

- Nghề giáo bao đời nay luôn được xem là nghề cao quý, nghề *"trồng người"*. Người thầy, dù ở đâu cũng là những người được kính trọng nhất. Và tại VnPro, trong hơn *10 năm hoạt động*, VnPro càng thấm nhuần hai chữ ấy.

Bên cạnh niềm tự hào xây dựng được một hệ thống đào tạo mạng chuyên nghiệp, hiện đại với khả năng cung cấp các *khóa học toàn diện và chất lượng* hàng đầu tại Việt Nam.

- **VnPro còn là trung tâm duy nhất khắp cả nước phát hành và xuất bản hơn 20 đầu sách mạng tiếng Việt ở mọi cấp độ**
- **Đào tạo hơn 11000 học viên**
- **Là trung tâm duy nhất đã có 10 CCIE Lab hàng đầu Việt Nam, góp phần nâng số CCIE tại Việt Nam hiện tại lên vượt ngưỡng 40**

Đó cũng chính nhờ vào sự đóng góp to lớn ngày đêm của hơn 40 thầy cô, giảng viên hiện là các chuyên gia hàng đầu trong các công ty lớn trên toàn quốc.

- Nhân ngày Nhà giáo Việt Nam, VnPro xin chúc tất cả các thầy cô luôn luôn mạnh khoẻ, trẻ trung, vui tính, chúc cho mọi lời chúc của tất cả học trò dành cho các thầy các cô đều trở thành hiện thực. Và các Thầy Cô sẽ đào tạo ra nhiều, nhiều hơn nữa các chuyên gia quản trị mạng hàng đầu Việt Nam.

VnPro

Trân trọng!

Khôi phục mật khẩu trên FIREWALL ASA 5500 Series Adaptive Security Appliance

Thực hiện các bước sau đây:

Bước 1 Kết nối thiết PC tới cổng console của thiết bị thông qua terminal (HyperTerminal) với các tham số 9600 baud, 8 data bits, no parity, 1 stop bit, no flow control.

Bước 2 Tắt nguồn sau đó bật nguồn trở lại.

Bước 3 Trong suốt tiến trình thiết bị khởi động, ta nhấn phím Escape để truy cập vào chế độ ROMMON.

Bước 4 Để thiết lập cho thiết bị lờ đi file cấu hình "startup configuration" trong tiến trình khởi động, ta tiến hành cấu hình các tham số sau:

```
rommon #1> confreg
```

Thiết bị sẽ hiển thị giá trị "configuration register" hiện tại và hỏi xem liệu chúng ta có muốn thay đổi lại giá trị này hay không:

```
Current Configuration Register: 0x00000011
Configuration Summary:
  boot TFTP image, boot default image from Flash on
netboot failure
Do you wish to change this configuration? y/n [n]:
```

Bước 5 Với giá trị "configuration register" hiện tại, chúng ta sẽ phải thiết lập lại sau đó.

Bước 6 Tại chế độ nhắc nhở hiện tại, chúng ta chọn tùy chọn Y để thay đổi giá trị "configuration register". Thiết bị sẽ yêu cầu chúng ta khai báo một giá trị mới.

Bước 7 Nếu chấp nhận các giá trị mặc định ngoại trừ tham số "disable system configuration?", sau đó ta tiếp tục lựa chọn tùy chọn Y.

Bước 8 Khởi động lại thiết bị với câu lệnh sau:

```
rommon #2> boot
```

Lúc này thiết bị sẽ khởi động lại với cấu hình mặc định thay vì sử dụng file cấu hình "startup configuration".

Bước 9 Để truy cập chế độ đặc quyền privileged EXEC mode ta thực hiện câu lệnh sau:

```
hostname> enable
```

Bước 10 Khi được hỏi thông tin password, ta nhấn Return. Thông tin password lúc này sẽ để trống.

Bước 11 Tải file cấu hình "startup configuration" bằng câu lếnh sau:

```
hostname# copy startup-config running-config
```

Bước 12 Truy cập vào chế độ cấu hình toàn cục "global configuration" thông qua câu lệnh:

```
hostname# configure terminal
```

Bước 13 Thay đổi thông tin các password thông qua các câu lệnh tương ứng sau:

```
hostname(config)# password password
hostname(config)# enable password password
hostname(config)# username name password password
```

Bước 14 Thay đổi giá trị "configuration register" về giá trị mặc định ban đầu 0x1 cho lần khởi động tiếp theo:

```
hostname(config)# config-register value
```

Bước 15 Lưu thông tin các password mới vào file "startup configuration" bằng câu lệnh sau:

```
hostname(config)# copy running-config startup-config
```

[P. Giảng Viên VnPro]

Gói dịch vụ Cisco SMARTnet Service

Cisco® SMARTnet® Service là 1 dịch vụ hỗ trợ kỹ thuật cho phép nhân viên IT có thể trao trực tiếp bất kỳ lúc nào với các chuyên gia Cisco và những nguồn tự giúp đỡ trực tuyến để yêu cầu giải quyết những vấn đề phát sinh với hầu hết những dòng sản phẩm của Cisco. Với Cisco SMARTnet Service, bạn có thể lựa chọn nhiều gói dịch vụ cho các sản phẩm Cisco

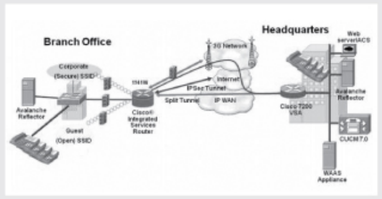
Các gói dịch vụ Cisco SMARTnet Service: Cisco SMARTnet Service cung cấp các gói hỗ trợ ở các cấp độ sau:

- Hỗ trợ trực tiếp thông qua phương thức truy cập từ xa bất kỳ thời điểm nào trong nào trong ngày, 365 ngày/năm với các chuyên gia Trung tâm hỗ trợ kỹ thuật của Cisco (Cisco Technical Assistance Center - TAC).
- Hỗ trợ trực tuyến thông qua phương tiện trực tuyến, cộng đồng, tài nguyên và các công cụ của Cisco.
- Gói hỗ trợ thông minh giúp chuẩn đoán tự động và cảnh báo tức thì trên những thiết bị nhất định với tính năng Cisco Smart Call Home.
- Gói hỗ trợ cập nhật hệ điều hành, cập nhật phần mềm, bao gồm cả những bản phát hành nhỏ và chính thức trong tập tính năng được cấp phép của bạn.
- Gói hỗ trợ các lựa chọn thay thế phần cứng với thời lượng hỗ trợ trong 2 giờ hoặc 4 giờ
- Gói dịch vụ tùy chọn tại chỗ: được hỗ trợ trực tiếp bởi 1 kỹ sư có chuyên môn nhất định giúp cài đặt, hoặc thay thế các thiết bị.

[Người dịch: Trương Xuân Quang (ứng viên lớp GV AI10)]

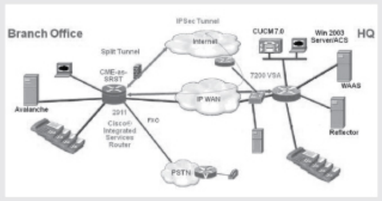
Giới thiệu một số dòng Cisco Router sử dụng tại chi nhánh

1. Dòng Cisco ISR 1941 cho hạ tầng mạng quy mô nhỏ



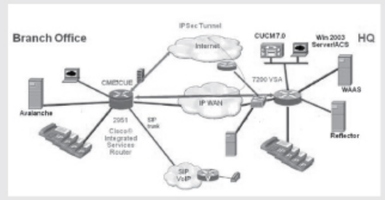
Để xây dựng một văn phòng chi nhánh nhỏ, Cisco ISR 1941W đã được cấu hình như một router chi nhánh. Kết nối mạng chính được thiết lập thông qua một kết nối internet công cộng với DMVPN (Dynamic Multi-point Virtual Private Network) được mã hóa đến trụ sở của công ty. Một kết nối dữ liệu không dây 3G đã được thiết lập dự phòng cho chi nhánh trong trường hợp liên kết WAN chính lỗi. Cisco ISR 1941W cũng đã được cấu hình để hỗ trợ cho mạng không dây chuẩn 802.11n sử dụng sóng vô tuyến để mở rộng mạng lưới không dây của công ty. Tính năng khu vực an ninh dựa trên Firewall, Cisco IPS IOS và lọc nội dung đã được kích hoạt. Các dịch vụ thoại được cung cấp bởi CUCM (Cisco Unified Communications).

2. Dòng Cisco ISR 2911 cho hạ tầng mạng trung bình.



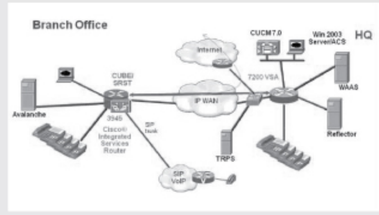
Khi triển khai chi nhánh quy mô trung bình có thể sử dụng Cisco ISR 2911. Trường hợp chi nhánh này hỗ trợ khoảng 25 người dùng, các mạng kết nối chính và backup được cung cấp bởi 2 đường Ethernet WAN riêng biệt. Một địa chỉ IP WAN cung cấp kết nối mạng chính với một kết nối an toàn DMVPN phục vụ như backup vào trụ sở công ty. Tính năng khu vực an ninh dựa trên Firewall, Cisco IOS IPS được kích hoạt. Dịch vụ thoại được cung cấp bởi CUCM với local POTS (Plain Old Telephone Service) truy cập từ Cisco ISR 2911.

3. Dòng Cisco ISR 2911 cũng có thể sử dụng cho quy mô hạ tầng mạng lớn



Một chi nhánh lớn với 40 đến 60 users được tạo nên bằng cách sử dụng Cisco ISR 2951. Trong trường hợp này, 2951 đã được cấu hình để cung cấp cho đường truy cập chính và backup thông qua một kết nối nối IP WAN kết nối chính đến trụ sở chính và một kết nối Interner public an toàn DMVPN để dự phòng. Trong trường hợp này tất cả các chức năng voice sẽ được thực hiện bởi Cisco Unified Communications Manager Express (CUCME) để kiểm soát cuộc gọi và cung cấp dịch vụ voice-email với Cisco Unity Express. Truy cập local PSTN được cung cấp bởi đường SIP trunk từ 2951 với mạng điện thoại địa phương. Vùng dựa vào Firewall, Cisco IOS IPS và Cisco WAAS cũng được kích hoạt tại các router.

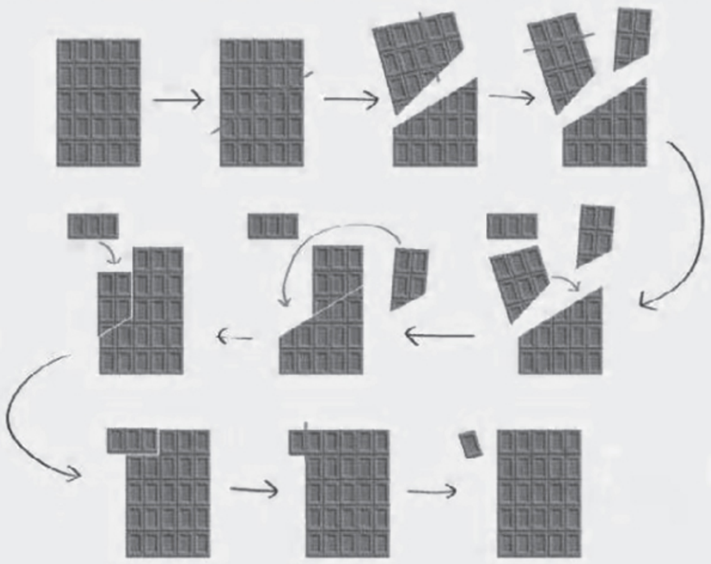
4. Dòng Cisco ISR 3945 cho quy mô hạ tầng mạng lớn



Một văn phòng lớn với 150 nhân viên trở lên có thể triển khai Cisco 3945. Kết nối chính và backup đến trụ sở chính được cung cấp với các kết nối IP WAN và đường Internet dự phòng. Cisco 3945 series được cấu hình để hỗ trợ CUBE (Cisco Unified Border Element) cung cấp chức năng điều khiển cuộc gọi cùng với một CUCM tại trụ sở công ty. Chức năng SRST cũng đã được kích hoạt tại Cisco 3945 trong trường hợp kết nối với trung tâm CUCM bị sự cố. Truy cập local PSTN được cung cấp bởi đường SIP trunk với mạng điện thoại địa phương. Vùng dựa vào Firewall, Cisco IOS IP và Cisco WAAS cũng được kích hoạt tại router.

Liên kết tham khảo: http://ciscorouter-switch.over-blog.com/article-cisco-branch-routers-series-platform-116732627.html

[Người dịch: Nguyễn Hoàng Nhơn (ứng viên lớp GV AI10)]



Theo bạn có thể dư 1 thỏi chocolate như hình không?

Ôi Thầy

Vậy là ngày 20/11 nữa lại về, đang nghĩ ngợi bâng quơ tôi chợt nghe bài hát "Người thầy", lời bài hát như tiếng lòng của ai đó từ một nơi nào xa lắm vọng về. Tôi đã lắng nghe bài hát đó với một cảm xúc lạ, một nỗi niềm. Sau những giờ bươn trải với cuộc sống bộn bề lo toan, giai điệu bài hát và tâm hồn tôi như hòa làm một. Trong một phút nào đó tôi quên đi thực tại và trở về với những ngày xa xưa ấy. Cái ngày bên mái trường với thầy cô bạn bè. Kí ức như một cuộn phim quay ngược, kỉ niệm cũng giống như những phím đàn – khi chạm tay vào, âm thanh sẽ ngân lên, nhưng không phải lúc nào cũng tuyệt vời, mà có cái hay cái dở, cái muốn nhớ, cái lại muốn xóa đi. Nhưng dù hay dù dở còn tùy thuộc vào cảm nghĩ của mỗi người.

Ngày ấy, thầy cô bảo tôi hiền, bạn bè bảo tôi ngố nhưng dù là gì thì tôi cũng vui với những cái tên, biệt danh mà bạn bè gắn cho. Với tư cách là phó học tập, tuy không gây bất mãn cho bạn bè nhưng cũng có vài tên cá biệt trong lớp không thích mỗi khi tôi ghi tên vào sổ theo dõi. Có lần mấy tên ấy canh lúc tôi thường đi vệ sinh đã gài một thùng nước với cánh cửa nhà vệ sinh. Nhưng không may hôm ấy, thầy chủ nhiệm gặp tôi bàn một số việc học tập của lớp, rồi thầy cùng tôi đi vệ sinh, tôi nhường thầy vào trước và cuối cùng cả thùng nước đã đổ lên người thầy. Tôi mắt chữ "o", miệng chữ "a" nhìn cả người thầy ước nhem. Tội nghiệp thầy không biết làm sao mà lên văn phòng, thầy lại là giáo viên mới ra trường vừa nhận công tác chủ nhiệm lớp tôi vậy mà xảy ra chuyện thật khó xử. Nhìn mặt thầy mà tôi thấy thương và giận trò nghịch ấy của bạn bè. Tôi cứ nghĩ hôm sau sẽ có chuyện, còn đám bạn sau trò ấy tuy có sợ và thất vọng vì tôi không bị nạn nhưng thích thú vì người ấy là thầy chủ nhiệm. Buổi sinh hoạt lớp, mỗi người một tâm trạng vì hầu như cả lớp đều biết chuyện, nữ thì liếc đám bạn phá phách trách "vô ý thức", nam thì có người thương thầy, có người bình thản, riêng nhóm phá phách kia lại tỏ ra như không có gì. Thầy vào, vẫn sinh hoạt bình thường và tiết sinh hoạt qua đi trong hồi hộp chờ đợi của mọi người nhưng tất cả không như mọi người nghĩ, thầy vẫn bình thường. Sau này tôi mới biết, tối đó thầy đã gặp riêng các bạn ấy nhưng tôi cũng không biết thầy đã nói gì mà trở về sau các bạn ấy đã giảm và hầu như không còn những trò nghịch phá với thầy cô và cả tôi nữa. Sau này, mỗi lần về thăm thầy tôi đều hỏi nhưng thầy chỉ cười cười và nhìn tấm ảnh tập thể lớp mà ánh mắt thầy ánh lên một niềm vui khó tả.

Có ai nhớ chăng bao kỉ niệm êm đềm thấm đượm tình thầy trò? (Ảnh minh họa)

Chẳng bù cho cuộc sống ngày nay, từ những chuyện bán mua cả tình cảm, trí tuệ thầy không ra thầy, trò không ra trò. Tôi chợt nhớ đến những người thầy của mình, những người nghiêm khắc nhưng đầy tình người đã hướng chúng tôi – những đứa học trò đến bến bờ tri thức. Không phải tự nhiên mà người ta có câu "nhất quỷ, nhì ma, thứ ba học trò". Học trò là lứa tuổi hồn nhiên, trong sang nhất và có thể nói phá phách nhất. Ai đã từng đi qua tuổi học trò mà không "ghi dấu" vài trò nghịch với thầy cô, và muôn vàn những trò tinh quái khác mà chỉ có học trò mới nghĩ ra được. Những trò nghịch ngợm và tuổi học trò tươi đẹp sẽ là một kỉ niệm của mỗi người mang theo trong suốt cuộc đời.

Thế đấy các bạn ạ. Thầy cô chúng ta như những người đưa đò đưa chúng ta đến bến bờ của tri thức, đến đỉnh cao của sự thành đạt nhưng đâu phải ai cũng nhớ. Thầy cô vẫn thức trắng đêm để có được những trang giáo án, những kiến thức để truyền thụ cho chúng ta. Mái tóc thầy cô đã điểm bạc theo thời gian. Như một nghịch lí của đời người, tuổi đời của thầy cô ngắn lại theo từng viên phấn trắng để tri thức của học trò càng dày lên thêm.Thầy cô đã chắp cánh cho ước mơ của chúng ta bay cao. Thế mà, có ai lần về thăm lớp cũ trường xưa để thăm lại những người đã hy sinh tâm huyết giúp chúng ta thành người hữu ích? Có ai nhớ chăng bao kỉ niệm êm đềm thấm đượm tình thầy trò?

Mặc cho cuộc sống bôn ba, thầy cô vẫn một đời chèo đò đưa từng lớp học sinh qua bến bờ tri thức. Ngày lại ngày, người thầy vẫn cặm cụi nắm vững tay chèo, chỉ sợ học sinh của mình lạc lối trên đường đời có lắm bão táp, chông gai. Ánh nắng mặt trời cuối ngày rồi sẽ tắt, dòng sông đến con đò rồi cũng sẽ rẽ sang một hướng khác. Nhưng việc dạy người làm sau rẽ được, gắn bó đời người bằng một lối đi chung. Cao cả thay tấm lòng người thầy, lặn lội chở người qua bão táp phong ba cập bờ hạnh phúc. Đến nơi rồi một nụ cười đọng mãi rồi lặng lẽ quay về lái tiếp những chuyến đò sau. Câu chuyện năm xưa nhưng mãi đến bây giờ tôi mới hiểu, thầy ơi – người đưa đò vĩ đại. Con đến với cuộc đời từ sự hy sinh thầm lặng ấy trên chuyến đò của thầy chở nặng yêu thương.

[sưu tầm]

HOA HỒNG SỐNG BẰNG GÌ?

Cô giáo hôm nay mặc áo mới, trên ngực thêu hoa hồng. Thấy các học sinh chăm chú nhìn, cô giáo rất vui, hỏi: *Thế các em có biết hoa hồng sống bằng gì ko?*

Vôva trả lời: *Thưa cô bằng sữa ạ!*

Cô giáo đỏ mặt đuổi Vôva ra đứng hành lang. Thấy hiệu trưởng đi ngang thấy Vôva vật vờ ở ấy, hỏi đầu đuôi sự tình rồi nói: *Vôva em nhầm rồi, hoa hồng sống bằng phân và nước tiểu!*

Vôva lầm bầm: *Em đâu biết rễ nó dài đến thế*

[... tiếp theo trang 8]

hoặc đưa ra một cách trả lời khéo léo: "hình như tôi không hợp với phong cách này, tôi thấy không thích lắm…"

Sử dụng ánh mắt khi giao tiếp:

- Khi nói chuyện, hãy nhìn thẳng vào người đối diện, song đừng nhìn chằm chằm. Thỉnh thoảng hãy đưa mắt nhìn phạm vi xung quanh họ để giảm tải căng thẳng cho cả hai.
- Không đảo mắt liên hồi, nhìn xéo sang một người trong khi nói chuyện với người khác nữa.
- Không đá lông nheo với người khác giới, trừ khi đó chỉ là cử chỉ hài hước bạn tạo ra cho mọi người vui vẻ.
- Không hướng mắt nhìn xuống chân: người bi quan, thiếu tự tin, kẻ phạm tội thường có cử chỉ này, do đó nó gây ra những cảm giác không hay ở người đối diện.
- Dù nói chuyện với một người lớn tuổi hay nhỏ tuổi, bạn cũng đừng nên nhìn vào khuyết điểm trên thân thể của họ. Dù bạn không cố ý nhưng đôi khi ánh mắt của bạn lại gợi lên những ý nghĩ tiêu cực đầu họ.
- Khi nhờ vả ai đó, trong khi chờ họ ra quyết định, không nên nhìn chằm chằm vào họ. Vô tình ánh mắt của bạn lại tạo áp lực bắt họ phải đồng ý giúp đỡ bạn. Khi ăn cơm, không nhìn người khác gắp thức ăn vì bạn sẽ khiến họ lúng túng.
- Tránh để cho người đối diện thấy bạn khóc, bởi bạn sẽ khiến họ rất khó xử, dù họ có phải là người khiến cho bạn khóc hay không.

Xem ra đây chưa phải là tất cả các nguyên tắc giao tiếp ứng xử bạn cần nắm, nhưng ít nhất, bạn cũng sẽ học được cách giao tiếp tốt hơn bằng việc tuân thủ các nguyên tắc này đấy. Chúc bạn thành công nhé!

[sưu tầm]

(Trích dẫn từ sách VnPro)

CHƯƠNG 5: ANTEN VÀ CÁC THIẾT BỊ PHỤ TRỢ

Anten thường được sử dụng để làm tăng vùng phủ sóng của mạng WLAN, nhưng việc chọn lựa anten thích hợp cũng có thể làm tăng tính an toàn cho mạng không dây. Chọn lựa anten một cách đúng đắn, cài đặt anten ở những vị trí thích hợp có thể làm giảm việc rò rỉ tín hiệu ra khỏi vùng làm việc và làm cho việc ngăn chặn tín hiệu cũng cực kỳ khó khăn. Vì thế chúng ta sẽ thảo luận về dạng phát sóng của các loại anten khác nhau và ảnh hưởng của vị trí anten đến mức độ nhận tín hiệu.

Anten có 3 loại chính được sử dụng trong WLAN gồm: Đẳng hướng (Omni-directional), bán định hướng (semi-directional) và định hướng cao (highly-directional). Chúng ta sẽ thảo luận các thuộc tính của các loại anten trên cũng như những phương thức thích hợp để cài đặt mỗi loại anten. Chúng ta cũng sẽ thảo luận về sự phân cực, hình dạng vùng phủ sóng, cách sử dụng và chỉ ra nhiều thành phần khác nhau được sử dụng để kết nối anten với các phần cứng WLAN khác.

Nguồn điện qua Ethernet PoE (Power over Ethernet) đã trở thành một tính năng quan trọng trong các sản phẩm WLAN hiện nay. Vì thế chúng ta cũng sẽ thảo luận về nó cũng như những kiểu thiết bị khác nhau được sử dụng để phân phối nguồn điện đến các thiết bị có khả năng PoE.

I. ANTEN VÔ TUYẾN

Anten vô tuyến là một thiết bị được sử dụng để chuyển đổi tín hiệu tần số cao (RF) trên đường truyền dẫn (cáp) sang dạng sóng để phát vào không khí. Trường điện từ phát ra từ anten được gọi là chùm (beams) hay búp (lobes). Có 3 loại anten chính:

- Đẳng hướng – Omni-directional.
- Bán định hướng – Semi-directional.
- Định hướng cao – Highly-directional.

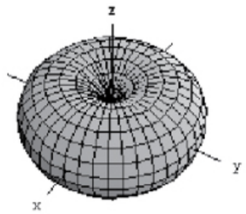
Mỗi loại có nhiều kiểu anten khác nhau, mỗi kiểu có đặc điểm về sóng vô tuyến và cách sử dụng khác nhau. Khi độ khuếch đại (gain) của anten tăng lên thì vùng bao phủ của anten sẽ rộng lớn hơn.

1. Anten đẳng hướng - Dipole

Loại anten WLAN phổ biến nhất là Dipole. Có thiết kế đơn giản, anten Dipole là một thiết bị chuẩn trên hầu hết các AP. Dipole chính là anten đẳng hướng bởi vì chúng phát ra năng lượng một cách đều nhau theo mọi hướng xung quanh trục của nó. Anten định hướng (directional) tập trung năng lượng của chúng tạo thành một hình nón được gọi là chùm (beam). Dipole có thành phần phát sóng chỉ dài 2,54 cm thực hiện chức năng tương tự như anten tai thỏ ở TV.

Anten dipole được sử dụng trong WLAN có kích thước nhỏ hơn nhiều bởi vì phổ tần số của WLAN là 2,4 GHz thay vì 100 MHz như của TV. Khi tần số cao hơn thì bước sóng và anten trở nên nhỏ hơn.

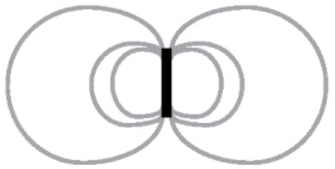
Hình 5.1 cho thấy năng lượng phát ra của dipole được tập trung tạo thành một vùng trông như một chiếc bánh rán. Tín hiệu từ anten đẳng hướng phát ra 360 độ theo chiều ngang. Nếu như một anten phát ra theo mọi hướng bằng nhau (tạo thành một hình cầu) thì nó được gọi là anten bức xạ đẳng hướng (isotropic). Mặt trời chính là một ví dụ điển hình của bức xạ đẳng hướng. Chúng ta không thể tạo ra một anten bức xạ đẳng hướng, nó chỉ là một lý thuyết tham khảo cho anten. Trên thực tế thì tất cả các loại anten có một độ khuếch đại nào đó so với bức xạ đẳng hướng. Độ khuếch đại càng lớn thì hình dạng bánh rán sẽ càng bị ép lại cho đến lúc nó giống như là một chiếc bánh dẹp. Đây chính là trường hợp của anten có độ khuếch đại cực kỳ cao.



Hình 5.1: Dạng bức xạ hình bánh rán của anten Dipole

Dipole bức xạ một cách đồng đều theo mọi hướng xung quanh trục của nó, nhưng lại không bức xạ dọc theo chiều dài của chính nó, vì thế đã tạo nên hình bánh rán. Nếu chúng ta nhìn từ bên cạnh hình dạng phát sóng của dipole như trong hình 5.2 thì chúng ta sẽ thấy một hình số 8.

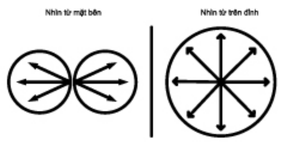
Hình 5.2: Anten Dipole nhìn từ bên cạnh



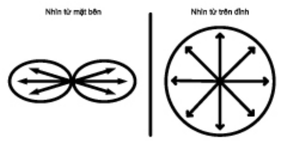
Nếu anten dipole được đặt ở trung tâm của một tầng (trong nhà có nhiều tầng) thì năng lượng của chúng sẽ được phát ra dọc theo chiều dài của tầng đó và một phần đáng kể sẽ phát lên tầng ở trên và tầng bên dưới.

Hình 5.3: Anten đẳng hướng

Hình 5.4: Vùng phủ sóng của anten đẳng hướng



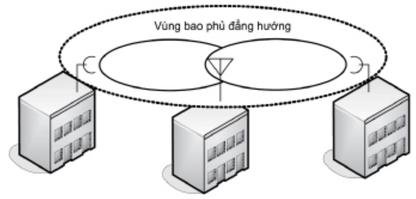
Hình 5.4: Vùng phủ sóng của anten đẳng hướng có độ khuếch đại cao



Anten đẳng hướng có độ khuếch đại cao thì sẽ có vùng phủ sóng theo chiều ngang nhiều hơn nhưng vùng bao phủ theo chiều dọc thì lại bị giảm. Đặc điểm này có thể được xem như là một yếu tố quan trọng khi cài đặt một anten có độ khuếch đại cao ở trong nhà (trên trần nhà). Nếu như trần nhà quá cao thì vùng bao phủ có thể không thể phủ đến nền nhà, nơi mà người dùng thường hay làm việc.

Cách sử dụng

Hình 5.6: Kết nối điểm-đa điểm



Anten đẳng hướng được sử dụng khi có nhu cầu bao phủ xung quanh theo mọi hướng của trục ngang của anten. Anten đẳng hướng là hiệu quả nhất trong môi trường cần vùng bao phủ rộng lớn xung quanh điểm trung tâm. Ví dụ, đặt một anten đẳng hướng ở giữa một phòng rộng sẽ cho vùng bao phủ tốt nhất. Anten đẳng hướng thường được sử dụng trong thiết kế điểm-đa điểm với mô hình mạng hub-n-spoke[1]. Khi sử dụng ngoài trời, anten đẳng hướng nên được đặt trên đỉnh của một tòa nhà nằm ở giữa vùng bao phủ. Ví dụ, trong khuôn viên của một trường đại học thì anten có thể được đặt ở trung tâm của trường để có vùng bao phủ lớn nhất. Khi sử dụng trong nhà, anten nên được đặt ở giữa nhà (ở trần nhà) hay giữa vùng bao phủ mong muốn để có vùng bao phủ tối ưu. Anten đẳng hướng phát ra một vùng bao phủ rộng lớn theo dạng hình tròn và rất thích hợp cho các môi trường như nhà kho, trung tâm triển lãm,… nơi thường có vùng bao phủ từ góc này sang góc khác của tòa nhà.

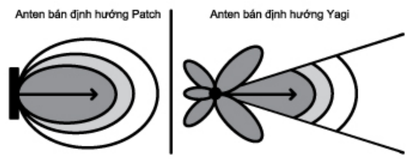
2. Anten bán định hướng

Anten bán định hướng có nhiều kiểu và hình dạng khác nhau. Một số kiểu anten bán định hướng thường được sử dụng trong WLAN gồm: Patch, Panel và Yagi. Tất cả các loại anten này thường có dạng phẳng và được thiết kế để treo lên tường. Mỗi kiểu có đặc điểm bao phủ khác nhau.

Hình 5.7: Anten bán định hướng

Các kiểu anten này tập trung năng lượng từ bộ phát sóng của chúng theo một hướng nào đó thay vì phát đều theo mọi hướng như trong anten đẳng hướng. Anten bán định hướng thường có vùng bao phủ hình bán cầu hay hình trụ.

Hình 5.8: Vùng phủ sóng của anten bán định hướng

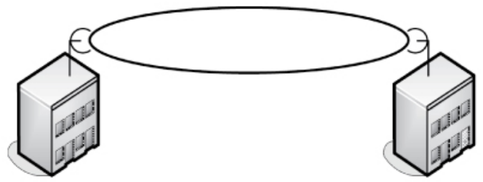


Cách sử dụng

Anten bán định hướng rất lý tưởng cho việc kết nối ở khoảng cách ngắn và trung bình. Ví dụ, hai tòa nhà nằm cách nhau 1 con đường cần chia sẻ kết nối mạng với nhau chính là một trường hợp tốt để sử dụng anten bán định hướng. Ở môi trường trong nhà có không gian rộng lớn, nếu như bộ phát tín hiệu phải đặt ở góc nhà, ở cuối tòa nhà, ở hành lang hay ở một phòng rộng lớn thì anten semi-directional chính là một sự lựa chọn tốt để cung cấp vùng bao phủ thích hợp.

Nhiều khi, trong suốt quá trình khảo sát trong nhà, các kỹ sư thường nghĩ đến việc làm thế nào để xác định vị trí đặt anten đẳng hướng tốt nhất. Trong một số trường hợp, anten bán định hướng cung cấp cùng một vùng bao phủ như đẳng hướng nên chúng có thể loại bỏ nhu cầu cần phải có nhiều AP trong tòa nhà. Ví dụ, ở một hành lang dài, nhiều AP với anten đẳng hướng có thể được sử dụng, nhưng thay vào đó, ta chỉ cần 1 hay 2 AP với anten bán định hướng được bố trí thích hợp sẽ tiết kiệm được cho khách hàng một khoảng tiền khá lớn. Đôi khi anten bán định hướng có các búp sóng (lobe) phát ra phía sau và bên cạnh nên nếu sử dụng một cách hiệu quả sẽ giảm việc phải mua thêm AP mới.

Hình 5.9: Kết nối điểm-điểm sử dụng anten bán định hướng



[P. Giảng Viên VnPro]