Số 28
05/2014

BẢN TIN danCISCO

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

Cấu hình Port Security

Bảng "mac address-table" trên các switch chỉ có thể lưu được một số lượng giới hạn các địa chỉ MAC (khoảng hơn 4000 địa chỉ MAC đối với dòng Catalyst 3750-X). Theo nguyên tắc hoạt động của Switch thì một "port" có thể học được rất nhiều địa chỉ MAC khác nhau. Do vậy một đối tượng tấn công có thể đứng tại một "port" sử dụng tool công cụ ....

[Trang 02]

ƯU ĐÃI 10% CHÀO HÈ

- *Ưu đãi hấp dẫn khi tham gia đóng nhóm*
- *Ưu đãi 10% cho học viên cũ*
- *Tặng ngay áo thun VnPro + Lịch thi đấu World Cup 2014*

Cấu hình địa chỉ IPv6 trên Router Cisco

IPv4 được dùng để truyền thông cho Internet khá tốt nhưng nó bị giới hạn ở không gian địa chỉ và phát sinh vấn đề khi có quá nhiều máy tính kết nối vào Internet. Để giải quyết vấn đề đó, kỹ thuật CIDR (Classless Interdomain Routing) được ...

[Trang 04]

Thiết kế và triển khai hệ thống mạng Campus Wireless Network

Một hệ thống mạng không dây WLAN (Wireless LAN) cần phải được thiết kế hợp lý để đáp ứng được nhu cầu thực tế của người sử dụng. Chính vì thế, chúng ta cần phải thu thập ...

[Trang 07]

TIN TỨC SỰ KIỆN KHÁC

01. Tin tức công nghệ thông tin
03. Tủ sách LabPro
05. Cấu hình PPP với xác thực CHAP
06. Tin tức VnPro
08. Cisco triển khai một trong những hệ thống Wi-Fi Network lớn nhất thế giới
09. Dịch vụ thi công hệ thống mạng
10. Hệ thống chứng chỉ của Cisco
11. Thư giãn
12. Trích dẫn từ sách VnPro

Internet of Things

Cisco dự đoán sẽ có trên 50 tỷ thiết bị sẽ được kết nối Internet vào năm 2020. Khi các thiết bị được kết nối một cách dễ dàng hơn sẽ làm thay đổi phương thức sản xuất của các ngành công nghiệp, giao thông vận tải, các hình thức dịch vụ vui chơi và giải trí, tổ chức chính phủ, tổ chức giáo dục và thị trường bán lẻ cũng sẽ có những thay đổi đáng kể.

Xu hướng IoT (Internet of Things) trong tương lai là tất yếu cho phép con người, máy móc, dữ liệu đều được kết nối và tương tác với nhau. IoT giúp giải quyết các vấn đề nhằm cải thiện cuộc sống của người dân trong các lãnh vực như y tế, giáo dục, giao thông vận tải, việc làm và an ninh.

IoT có thể gọi là tập hợp các kết nối thông minh (smart connect) trên các thiết bị ngoại vi mà ta vẫn hay dùng (wifi, NFC, mã QR , bluetooth...) qua Internet để thực hiện một công việc nhất định. Chẳng hạn như chiếc tủ lạnh thông thường của bạn không được kết nối với thiết bị nào khác. Nếu chúng ta muốn ghi lại nhiệt độ ở từng thời điểm của tủ, chúng ta chỉ có cách ghi lại thủ công rồi nhập vào một máy tính hay thiết bị lưu trữ. Hay như bóng đèn neon ở nhà chẳng hạn, chúng ta muốn thu thập, điều chỉnh độ sáng của nó thì phải đo thủ công rồi ghi lại.

Còn nếu như máy tính có khả năng giúp con người thu thập tất cả những dữ liệu về mọi thứ xung quanh, chúng ta có thể "theo dõi và đếm mọi thứ, giúp giảm hao phí tổn. Chúng ta sẽ biết chính xác khi nào các vật dụng cần phải sửa chữa, thay thế, khi nào chúng còn mới và khi nào thì chúng hết hạn sử dụng. Chưa kể đến việc chúng ta có thể kiểm soát chúng mọi lúc mọi nơi. IoT có tiềm năng thay đổi thế giới, giống như cách mà Internet đã thay đổi cuộc sống của chúng ta. Ngôi nhà thông minh với các bóng đèn thông minh, máy giặt thông minh, tủ lạnh thông minh,... có thể xem là bước đầu của IoT bởi chúng đều được liên kết với nhau và kết nối tới Internet.

Một trong những vấn đề thách thức đặt ra đối với IoT đó là khả năng tạo ra một ứng dụng IoT nhanh chóng. Để khắc phục, hiện nay nhiều hãng, công ty, tổ chức trên thế giới đang nghiên cứu các nền tảng giúp xây dựng nhanh ứng dụng dành cho IoT. Đại học British Columbia ở Canada hiện đang tập trung vào một bộ toolkit cho phép phát triển phần mềm IoT chỉ bằng các công nghệ Web, sử dụng các giao thức phổ biến. Công ty ioBridge thì cung cấp giải pháp kết nối và điều khiển hầu như bất kì thiết bị nào có khả năng kết nối Internet, kể cả đèn bàn, quạt máy. IoT hứa hẹn sẽ tạo ra một chu kỳ đổi mới mạnh mẽ trải dài trên các mảng lĩnh vực trong tương lai.

Catalyst Switch 2960-X

Catalyst access switch 2960-S /SF có khả năng cung cấp tốc độ truyền dẫn 40Gbs trong khi dòng Catalyst 2960-X hứa hẹn sẽ tăng gấp đôi tốc độ chuẩn của dòng 2960-S. 2960-X hỗ trợ 4MB bộ nhớ đệm, cung cấp đến 8 hàng đợi cho phép QoS một cách linh hoạt hơn, hỗ trợ số lượng port 24 hoặc 48 cổng 10/100/1000 Mbps Ethernet và có thể hỗ trợ thêm 4 cổng 1GbE hoặc 2 cổng 10GbE Uplink port.

Bên cạnh đó, 2906-X còn được bổ xung thêm một loạt các tính năng mới và một số tính năng hữu dụng khác như Cisco NetFlow-Lite cho phép kiểm soát lưu lượng các ứng dụng luân chuyển trên hạ tầng mạng tại các access switch, hỗ trợ cơ chế tiết kiệm điện EnergyWise, hỗ trợ chuẩn PoE và PoE+.

Switch 2960-X cũng hỗ trợ định tuyến lớp 3 như định tuyến tĩnh static route, RIPv2, OSPF, EIGRP và hỗ trợ Independent Multicast PIM (giao thức định tuyến Multicast), hỗ trợ giao thức dự phòng HSRP (Hot Standby Router Protocol).

(tiếp theo trang 02)

```
00:07:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
00:07:43: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
```

Ta thấy cổng f0/1 đã bị đưa vào trạng thái *err-disable* và bị shutdown.

Muốn cho cổng hoạt động trở lại, ta phải cắm lại đúng máy PC A vào cổng f0/1, vào cổng f0/1 shutdown rồi no shutdown lại:

```
Switch(config)interface f0/1
Switch(config-if)#shutdown
Switch(config-if)#no shutdown
```

Ta cũng có thể cho cổng tự động ra khỏi trạng thái *err-disable* 30 giây sau khi đã khắc phục nguyên nhân gây ra lỗi bằng câu lệnh:

```
Switch(config)# errdisable recovery cause psecurity-violation
Switch(config)# errdisable recovery interval 30
```

Ta có thể chỉnh thời gian chờ phục hồi trong dải giá trị từ 30 giây đến 86400 giây (24 giờ).

Cấu hình Port Security

Mô tả:

Bảng "mac address-table" trên các switch chỉ có thể lưu được một số lượng giới hạn các địa chỉ MAC (khoảng hơn 4000 địa chỉ MAC đối với dòng Catalyst 3750-X). Theo nguyên tắc hoạt động của Switch thì một "port" có thể học được rất nhiều địa chỉ MAC khác nhau. Do vậy một đối tượng tấn công có thể đứng tại một "port" sử dụng tool công cụ để đánh tràn bảng "mac address-table" nhằm phá hoại hoặc đánh cắp dữ liệu (tool công cụ sẽ liên tục gửi đi các cấu trúc frame với MAC nguồn và MAC đích ngẫu nhiên). Tính năng Port Security khi được cấu hình trên một cổng của Switch có thể giới hạn số lượng địa chỉ MAC được đi vào cổng này.

Trong bài lab này, chúng ta sẽ thực hiện cấu hình tính năng Port – security trên cổng F0/1 của Switch để cổng này chỉ chấp nhận các Ethernet frame xuất phát từ máy PC A.

Thực hiện:

Bước 1: Chuyển cổng f0/1 về mode access và bật tính năng port – security.

```
Switch(config)#interface f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

Nếu cổng chưa ở chế độ access, switch sẽ phát ra một thông báo lỗi từ chối bật tính năng port – security:

```
Switch(config-if)#switchport port-security
Command rejected: Fa0/1 is not an access port
```

Bước 2: Quy định số địa chỉ MAC tối đa được phép đi vào cổng f0/1:

```
Switch(config-if)#switchport port-security maximum 1
```

Ta có thể quy định được số lượng địa chỉ MAC được quyền đi vào một cổng port – security bằng câu lệnh "switchport port-security maximum number_of_MAC_address". Số lượng địa chỉ này có thể khác nhau tùy dòng switch, thông thường dải giá trị sẽ là từ 1 đến 132 địa chỉ. Mặc định nếu ta không cấu hình câu lệnh này, số lượng địa chỉ được phép đi vào cổng sẽ là 1 địa chỉ.

Bước 3: Chỉ rõ ra địa chỉ nào được phép đi vào cổng.

```
Switch(config-if)#switchport port-security mac-address 0009.b7ed.a9a0
```

Trong câu lệnh, địa chỉ được chỉ ra chính là địa chỉ MAC của card mạng PC A. Như vậy, chỉ PC A được phép truy nhập vào cổng f0/1 của Switch. Ta có thể cho switch học tự động địa chỉ được phép truy nhập bằng cách thay địa chỉ trong câu lệnh bằng từ khóa "sticky". Khi đó, khi PC A truyền một frame vào cổng, switch sẽ tự động ghi nhớ và đưa địa chỉ MAC của PC A vào chế độ port – security:

```
Switch(config-if)#switchport port-security mac-address sticky
```

Nếu ở bước 2, ta chỉ ra số lượng địa chỉ MAC lớn hơn 1 thì ta phải khai báo cho đủ số hoặc cho học tự động đủ số lượng địa chỉ đã khai báo.

Bước 4: Quy định hình thức phản ứng trên cổng khi có một frame lạ xâm nhập.

```
Switch(config-if)#switchport port-security violation {shutdown | restrict | protect}
```

Có 3 tùy chọn trong câu lệnh này:

- ***Shutdown:*** nếu một frame lạ (có Source MAC không nằm trong dãy địa chỉ được cho phép), cổng sẽ đi vào trạng thái *err – disabled*. Ở trạng thái này, cổng sẽ bị shutdown, kết nối bị ngắt. Muốn đưa cổng hoạt động trở lại, ta phải khắc phục nguyên nhân gây lỗi (frame đi vào cổng phải có Source MAC được cho phép), vào mode cấu hình cổng, shutdown cổng rồi no shutdown cổng trở lại.
- ***Restrict và Protect:*** cổng sẽ không bị đưa vào trạng thái *err – disabled* nhưng các frame lạ đi vào sẽ bị loại bỏ. Điểm khác biệt giữa hai tùy chọn này là: với Restrict, một thông báo về sự vi phạm sẽ được phát ra trên màn hình cấu hình, còn với Protect, switch sẽ chỉ đơn giản loại bỏ frame mà không phát ra một thông báo lỗi nào cả.
- ***Tùy chọn mặc định*** được sử dụng nếu ta không đánh lệnh này là *shutdown*.

Ta sử dụng tùy chọn ***shutdown*** trong bài lab này:

```
Switch(config-if)#switchport port-security violation shutdown
```

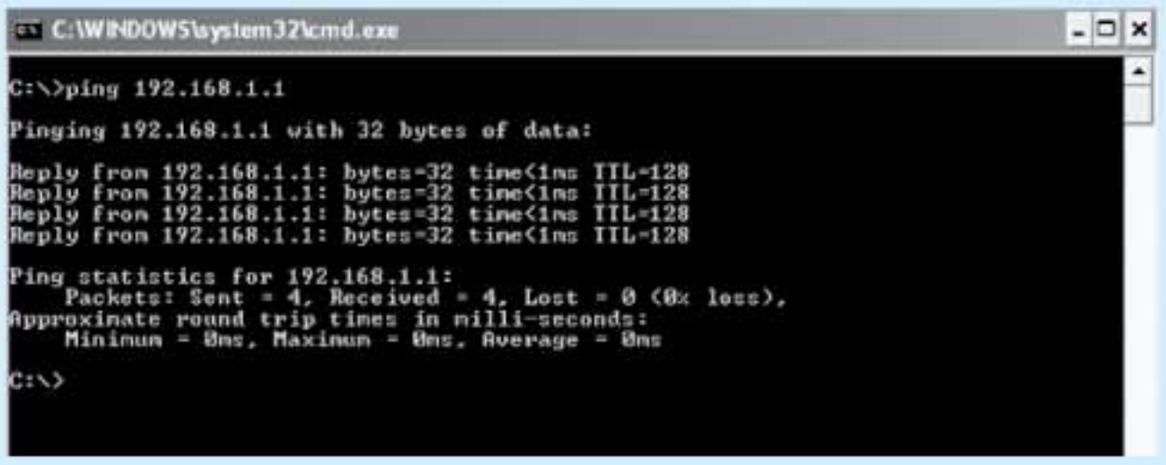
Bước 5: Thực hiện đặt địa chỉ IP cho switch và PC A để ping kiểm tra.

Trên switch, ta đặt địa chỉ trên interface vlan 1:

```
Switch(config)interface vlan 1
Switch(config-if)#no shutdown
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
```

Trên PC đặt một địa chỉ cùng mạng với địa chỉ IP của Switch, ta chọn địa chỉ là 192.168.1.2/24.

Bước 6: Ping kiểm tra giữa PC A và Switch.



Frame chứa gói IP ICMP ping giữa PC A và Switch có source MAC được phép đi vào cổng F0/1 do đó không bị chặn. Ping thành công.

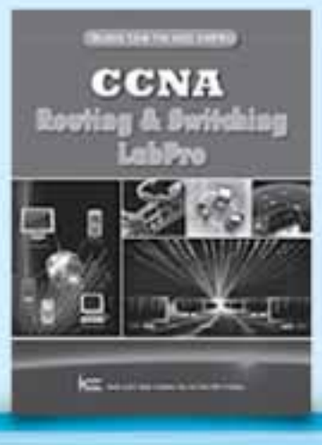
Bước 7: Thay PC A bằng PC B có MAC là 0023.4e08.0233– là MAC không được phép đi vào cổng và thực hiện ping lại thử. Trên màn hình console, phát ra một thông báo lỗi:

```
00:07:41: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in err-disable state
00:07:41: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0023.4e08.0233 on port FastEthernet0/1.
```

(xem tiếp trang 01)

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

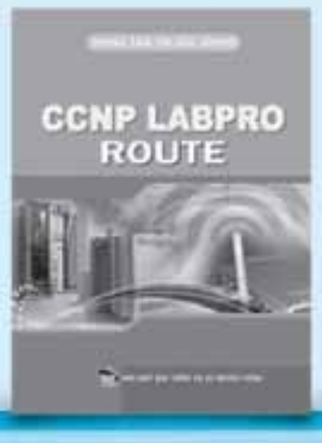
GIẢM* NGAY 10%



CCNA Routing & Switching
Giá: 220.000 VNĐ

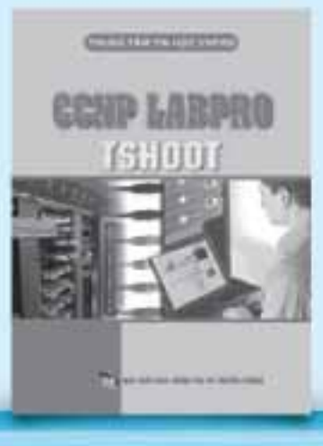
CCDA
Giá: 250.000 VNĐ

Ôn thi CCNA trong 24h
Giá: 120.000 VNĐ



CCNP LABPRO ROUTE
Giá: 120.000 VNĐ

CCNP LABPRO SWITCH
Giá: 120.000 VNĐ



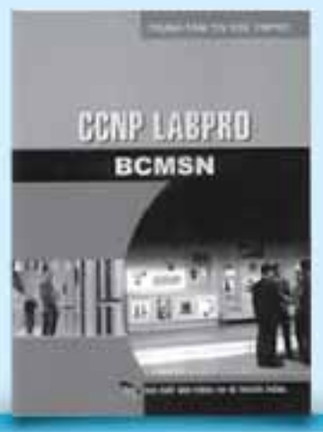
CCNP LABPRO TSHOOT
Giá: 120.000 VNĐ

Ôn thi Route
Giá: 90.000 VNĐ

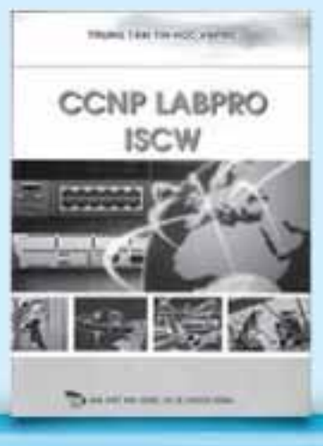
Ôn thi Switch
Giá: 100.000 VNĐ

Ôn thi Tshoot
Giá: 80.000 VNĐ

CCNP LABPRO BSCI
Giá: 95.000 VNĐ



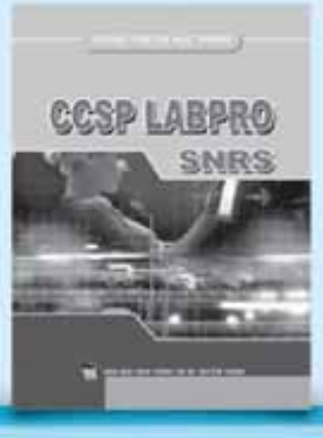
CCNP LABPRO BCMSN
Giá: 70.000 VNĐ



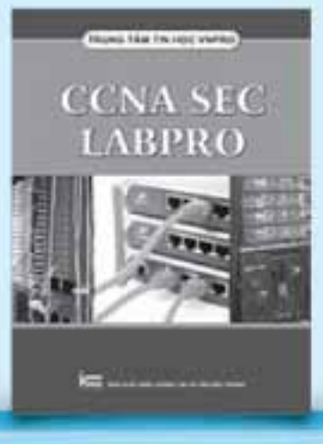
CCNP LABPRO ISCW
Giá: 120.000 VNĐ

CCSP LABPRO SNAF & SNAA
Giá: 120.000 VNĐ

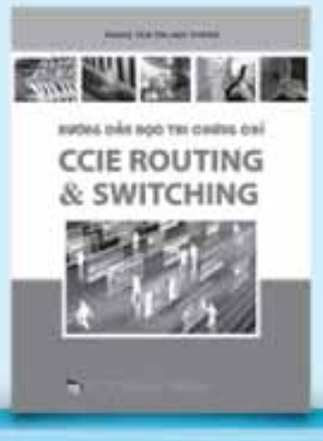
CCSP LABPRO IPS & CSMARS
Giá: 90.000 VNĐ



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/***

Cấu hình địa chỉ IPv6 trên Router Cisco

Giới thiệu tổng quan về địa chỉ IPv6

IPv4 được dùng để truyền thông cho Internet khá tốt nhưng nó bị giới hạn ở không gian địa chỉ và phát sinh vấn đề khi có quá nhiều máy tính kết nối vào Internet. Để giải quyết vấn đề đó, kỹ thuật CIDR (Classless Interdomain Routing) được phát triển, cho phép cấp phát các địa chỉ theo từng lô phù hợp với quy mô hạ tầng mạng của các tổ chức. Bên cạnh đó, công nghệ NAT cho phép nhiều PC (hơn 10.000 PC) sử dụng IP Private có thể chia sẻ cùng một IP Public để truy cập Internet cũng giúp tiết kiệm đáng kể không gian địa chỉ IPv4. Tuy nhiên, để giải quyết triệt để vấn đề thiếu hụt địa chỉ IPv4, chúng ta cần một loại địa chỉ mới với không gian địa chỉ IP nhiều hơn. Đó chính là lý do có sự ra đời của một loại địa chỉ mới, địa chỉ IPv6.

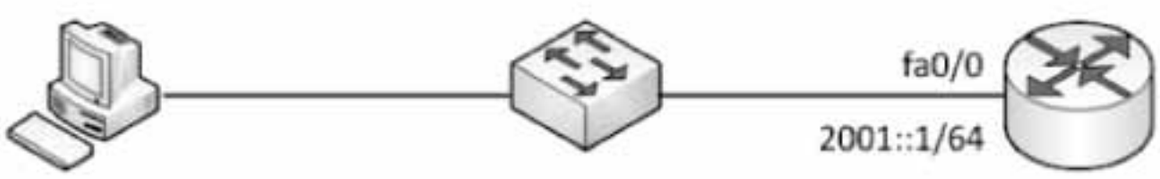
IPv6 ra đời vào những năm 1990, IPv6 còn gọi là IPng (IP next generation). Đặc điểm nổi bật nhất của IPv6 là không gian địa chỉ của nó. IPv6 dài 16 byte (128bit), nhiều hơn IPv4 (có 32 bit). Nhờ vậy nó sẽ cung cấp đủ địa chỉ để gán đia chỉ IP cho bất kỳ người dùng nào và bất kỳ thiết bị nào.

IPv6 có 3 kiểu địa chỉ:

- **Unicast** - Địa chỉ định nghĩa cho một host.
- **Anycast** - Sử dụng một địa chỉ Unicast để gán cho một nhóm các host, chẳng hạn như một tập các server chạy cùng ứng dụng. Một Packet gửi đến địa chỉ Anycast sẽ chuyển đến một trong các host gần nhất được gán địa chỉ Anycast đó.
- **Multicast** - Địa chỉ định nghĩa một tập hợp các host. Một Packet gửi đến địa chỉ Multicast sẽ chuyển đến tất cả các host trong cùng nhóm. IPv6 không có địa chỉ broadcast như IPv4. Trong IPv6, chức năng broadcast được thay thế bởi hình thức multicast.

Địa chỉ IPv4 được viết dưới dạng số thập phân gồm 4 phần, mỗi phần gồm 4 byte phân cách nhau bằng dấu chấm (.). Ví dụ như 198.133.219.25 là một địa chỉ IPv4. Với IPv6, địa chỉ thể hiện dưới dạng giá trị thập lục phân gồm 8 khối 16-bit, phân cách bởi dấu 2 chấm (:). Ví dụ như FF04:19:5:ABD4:187:2C:754:2B1. Để rút gọn địa chỉ IPv6 ta có thể sử dụng dấu 2 chấm kép (::) để biểu thị cho nhiều khối 16-bit số zero; một ví dụ, địa chỉ FF01:0:0:0:0:0:0:5A có thể viết FF01::5A. Theo nguyên tắc, chỉ có thể chỉ xuất hiện một dấu :: trong địa chỉ IPv6.

Sơ đồ mạng



Yêu cầu:

Cấu hình địa chỉ aggregatable global 2001::1/64 trên cổng fa0/0 của router, tại PC tiến hành cài đặt chồng giao thức IPv6, PC tự động phát sinh địa chỉ IPv6 theo phương thức "autoconfiguration", tiến hành "ping" kiểm tra từ PC tới router và ngược lại.

Các bước triển khai:

Bước 1: Bật chức năng định tuyến IPv6 trên router

```
Router# configure terminal
Router(config)# ipv6 unicast-routing
```

Bước 2: Cấu hình địa chỉ aggregatable global 2001::1/64 trên cổng fa0/0 của router

```
Router(config)# interface f0/0
! Kích hoạt IPv6 trên cổng giao tiếp
Router(config-if)# ipv6 enable
! Khai báo địa chỉ 2001::1/64 cho cổng giao tiếp
Router(config-if)# ipv6 address 2001::1/64
Router(config-if)# no shutdown
```

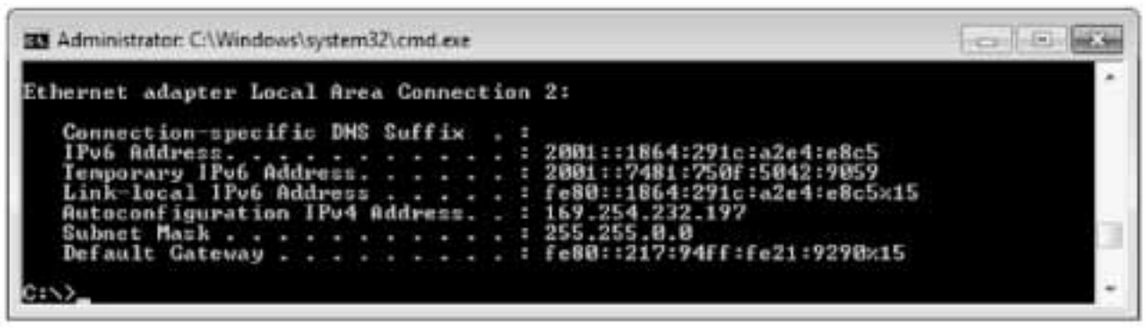
Lưu ý: Để cơ chế tự động phát sinh địa chỉ autoconfiguration trên PC hoạt động, phía router cần phải sử dụng địa chỉ IPv6 với prefix-length là /64.

Bước 3: Kiểm tra thông tin địa IPv6 trên router

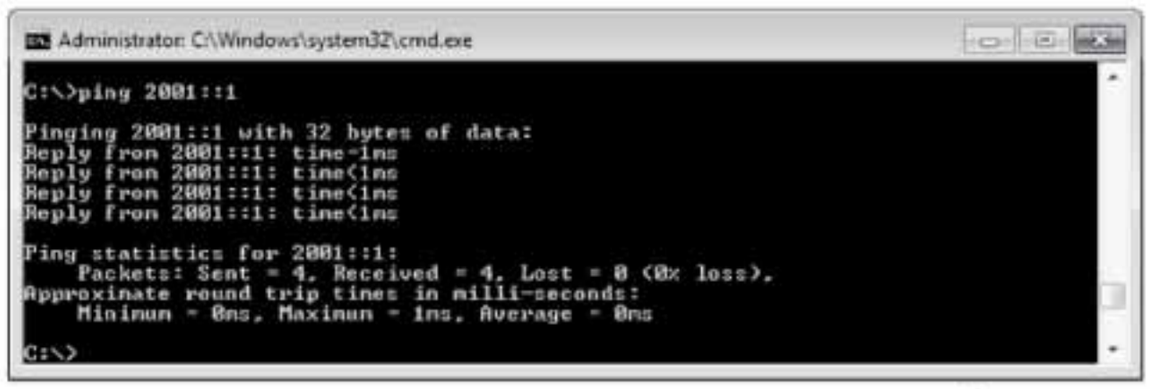
```
Router#show ipv6 interface brief
FastEthernet0/0        [up/up]
    FE80::C000:1CFF:FE30:0
    2001::1
FastEthernet0/1        [administratively down/down]
Router#
```

Bước 4: Cài đặt IPv6 trên PC thông qua giao diện cửa sổ cmd

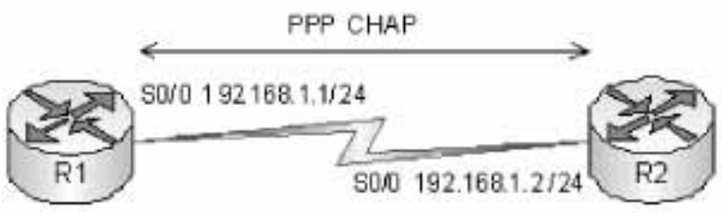
Bước 5: Kiểm tra địa chỉ IPv6 trên PC đã được cấu hình theo cơ chế autoconfiguration, tại cửa sổ cmd thực hiện câu lệnh ipconfig hoặc ipconfig /all



Bước 6: Tiến hành "ping" kiểm tra đến router



Cấu hình PPP với xác thực CHAP



Hình 7.2.1

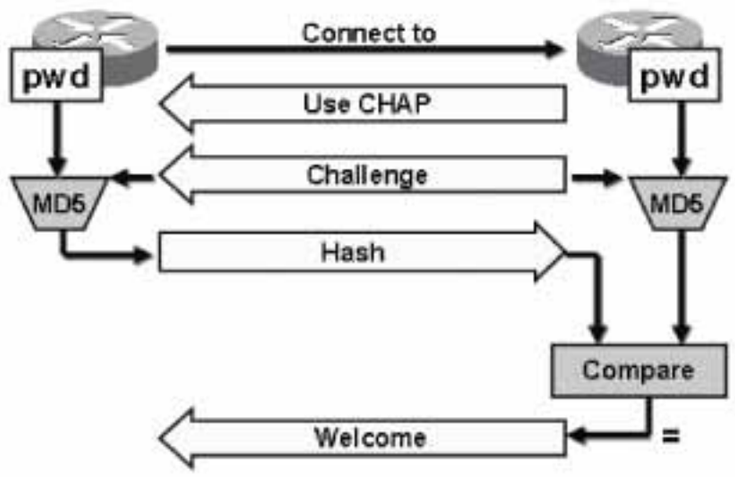
Mô tả

CHAP là giao thức xác thực được xem là bảo mật hơn PAP vì không gởi Password clear text trên đường truyền.

CHAP dùng thuật toán Hash MD5 để bảo vệ quá trình xác thực.

Trong bài tập này dùng CHAP để xác thực giữa hai thiết bị.

Lưu ý : Khác với PAP, password được sử dụng cuả thiết bị xác thực phải giống nhau (hình 7.2.2).



Hình 7.2.2

Cấu hình:

```
R1#sh run
Building configuration...

Current configuration : 727 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
ip subnet-zero
ip cef
!
ip audit po max-events 100
!
username vnpro password 0 123 // Database local
dùng để xác thực neighbor
!
!
interface Ethernet0/0
 no ip address
 half-duplex
 no keepalive
!
interface Serial0/0
 ip address 192.168.1.1 255.255.255.0
 encapsulation ppp
 ppp authentication chap
 ppp chap hostname cisco
 ppp chap password 0 123
!
ip http server
no ip http secure-server
ip classless
!
end
```

```
R2#sh run
Building configuration...

Current configuration : 779 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!

ip subnet-zero
ip cef
!
username cisco password 0 123 // Database local
dùng để xác thực neighbor
!
interface Serial0/0
 ip address 192.168.1.2 255.255.255.0
 encapsulation ppp
 clock rate 64000
 ppp authentication chap
 ppp chap hostname vnpro
 ppp chap password 0 123
!
ip http server
no ip http secure-server
ip classless
!
end
```

Kiểm tra

Nếu cả hai thiết bị xác thực thành công trạng thái line protocol trên cổng sẽ UP

Kiểm tra trường hợp xác thực sai, bằng việc thay đổi database nội bộ:

```
R2(config)#username cisco password 456
```

Mặc dù CHAP sẽ định kì trao đổi thông tin xác thực, nhưng để kiểm tra ta sẽ cần thiết bị tham gia xác thực lại:

```
R2(config)#interface s0/0
R2(config-if)#shut
R2(config-if)#
R2(config-if)#no shut
*Mar 1 01:57:09.819: %LINK-5-CHANGED:
Interface Serial0/0, changed state to administra-
tively down
*Mar 1 01:57:10.821: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Serial0/0, changed
state to down
```

```
R2#
*Mar 1 01:57:14.158: %SYS-5-CONFIG_I:
Configured from console by console
*Mar 1 01:57:15.015: %LINK-3-UPDOWN: Interface
Serial0/0, changed state to up
*Mar 1 01:57:15.015: Se0/0 PPP: Using default call
direction
*Mar 1 01:57:15.015: Se0/0 PPP: Treating connec-
tion as a dedicated line
*Mar 1 01:57:15.015: Se0/0 PPP: Session
handle[3100008B] Session id[145]
*Mar 1 01:57:15.015: Se0/0 PPP: Authorization
required
*Mar 1 01:57:15.028: Se0/0 CHAP: O CHALLENGE id
107 len 26 from "vnpro"
*Mar 1 01:57:15.032: Se0/0 CHAP: I CHALLENGE id
105 len 26 from "cisco"
*Mar 1 01:57:15.036: Se0/0 CHAP: Using hostname
from interface CHAP
*Mar 1 01:57:15.036: Se0/0 CHAP: Using password
from AAA
*Mar 1 01:57:15.036: Se0/0 CHAP: O RESPONSE id
105 len 26 from "vnpro"
*Mar 1 01:57:15.040: Se0/0 CHAP: I RESPONSE id
107 len 26 from "cisco"
*Mar 1 01:57:15.044: Se0/0 PPP: Sent CHAP LOGIN
Request
*Mar 1 01:57:15.044: Se0/0 PPP: Received LOGIN
Response FAIL
*Mar 1 01:57:15.048: Se0/0 CHAP: O FAILURE id
107 len 25 msg is "Authentication failed"
R2#sh interfaces s0/0
Serial0/0 is up, line protocol is down
 Hardware is PowerQUICC Serial
 Internet address is 192.168.1.2/24
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 253/255, txload 1/255, rxload 1/255
 Encapsulation PPP, LCP Listen, loopback not set
```

Bây giờ thay đổi lại thông tin xác thực như ban đầu:

```
R2(config)#username cisco password 123
*Mar 1 01:58:42.819: %LINEPROTO-5-UPDOWN:
Line protocol on Interface Serial0/0, changed
state to up
```

```
R2#sh interfaces s0/0
Serial0/0 is up, line protocol is up
 Hardware is PowerQUICC Serial
 Internet address is 192.168.1.2/24
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation PPP, LCP Open
 Open: IPCP, CDPCP, loopback not set
```

```
R2#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 28/29/32 ms
```

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 **10%**

CHÀO HÈ

- *Ưu đãi hấp dẫn khi tham gia đóng nhóm*
- *Ưu đãi 10% cho học viên cũ*
- *Tặng ngay áo thun VnPro + Lịch World Cup 2014*

LÝ DO KHÁCH HÀNG CHỌN VnPro

- ***Hơn 11 năm*** *đào tạo và phát triển*
- ***Hơn 11.000 học viên*** *đã theo học tại VnPro.*
- ***Đào tạo hơn 400 doanh nghiệp lớn*** *trên toàn quốc và các tập đoàn đa quốc gia.*
- ***Có 10 CCIE Lab*** *(hiện Việt Nam có khoảng 40 CCIE Lab)*
- ***300 trang thiết bị*** *đủ các chủng loại*
- ***Tạo cơ hội việc làm cho học viên.***
- ***Miễn phí cho học viên cũ****: các buổi cập nhật công nghệ, hội thảo, chuyên đề, kỹ năng mềm hàng tháng.*
- ***Đội ngũ giảng viên chuyên nghiệp****: là chuyên gia cấp cao đầu ngành trong các công ty và tập đoàn lớn trên cả nước, được trang bị kỹ năng sư phạm chuyên nghiệp, trải qua nhiều kỳ sát hạch để đạt tiêu chuẩn giảng dạy tại VnPro.*

Thiết kế và triển khai hệ thống mạng Campus Wireless Network

Một hệ thống mạng không dây WLAN (Wireless LAN) cần phải được thiết kế hợp lý để đáp ứng được nhu cầu thực tế của người sử dụng. Chính vì thế, chúng ta cần phải thu thập một số thông tin sau:

- WHO Kết nối wireless được sử dụng cho đối tượng nào? Nhân viên, học viên hoặc khách hàng viếng thăm của công ty?
- WHAT Các thiết bị tham gia kết nối là những thiết bị nào (Laptop, Desktop, Point-Of-Sale, cell phones/PDA, IP phone)? Các loại ứng dụng nào sẽ được hỗ trợ (dữ liệu Internet, streaming video, IP multicast, voice)?
- WHERE Vị trí người sử dụng tiến hành kết nối wireless connectivity? Phòng học, văn phòng, ngoài trời?
- HOW MANY Số lượng thiết bị truy cập wireless không dây ở mỗi vị trí kết nối? Phòng học, quán ăn, thư viện, văn phòng? Mức băng thông hỗ trợ cho từng loại ứng dụng như thế nào?
- WHEN Thời điểm người dùng sử dụng kết nối không dây? Số lượng kết nối đồng thời là bao nhiêu?

Bên cạnh các yêu tố trên, chúng ta còn cần quan tâm đến các nguyên tắc chẳng hạn như phạm vi bao phủ, khả năng sẵn có của hạ tầng mạng và vấn đề bảo mật.

Kiến trúc hạ tầng WLAN

Hạ tầng mạng WLAN bao gồm các thiết bị như Access Point (AP) cho phép chuyển đổi từ môi trường Ethernet frame có dây sang môi trường tín hiệu không dây wireless RF signal. Các thiết bị khách Client tiến hành kết nối tới AP thông qua tín hiệu RF signal. Ở mức độ cơ bản, có hai phương thức để triển khai hạ tầng mạng WLAN

(1) Sử dụng autonomous AP ("fat" AP).
(2) Sử dụng lightweight AP ("thin" AP).

Autonomous Access Point

Autonomous AP có khả năng tự vận hành và thường được triển khai độc lập (stand-alone) cho phép nhiều client kết nối được tới hạ tầng mạng có dây wired network truyền thống. Các tính năng của autonomous AP có thể được cấu hình một cách độc lập. Đây là mô hình triển khai cơ bản. Figure 1 minh họa mô hình kiến trúc autonomous AP.

Lightweight Access Point (LAP)

Lightweight Access Points (LAP) được kiểm soát và cấu hình tập trung bởi "cloud controller" hoặc Wireless LAN Controller (WLC) cho phép khả năng mở rộng linh hoạt và dễ dàng quản trị.

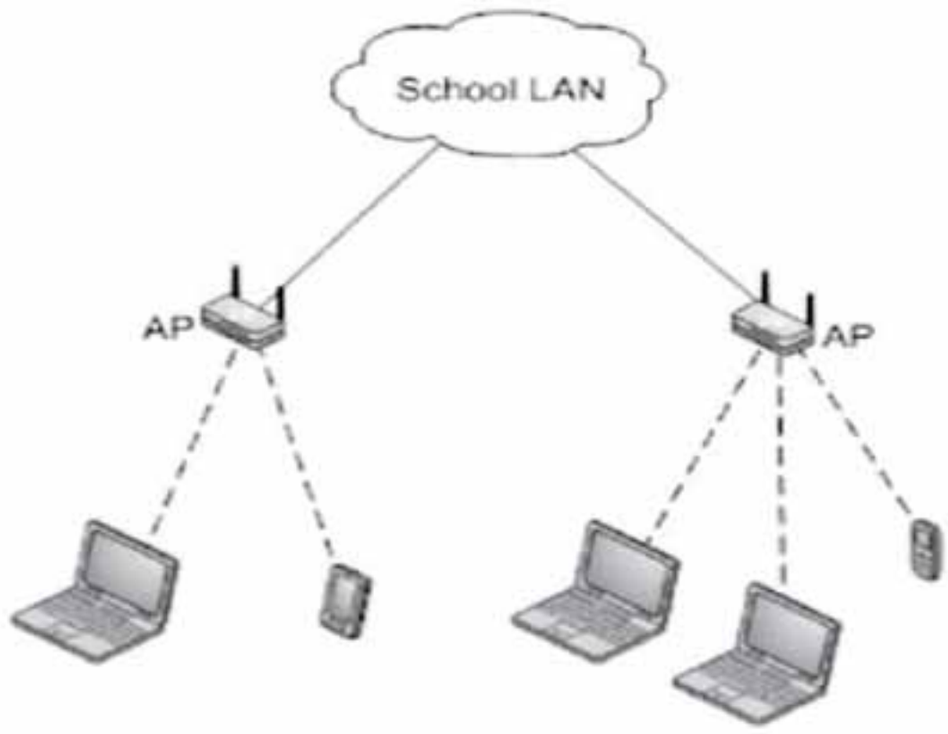


Figure 1: AUTONOMOUS/"FAT" AP ARCHITECTURE

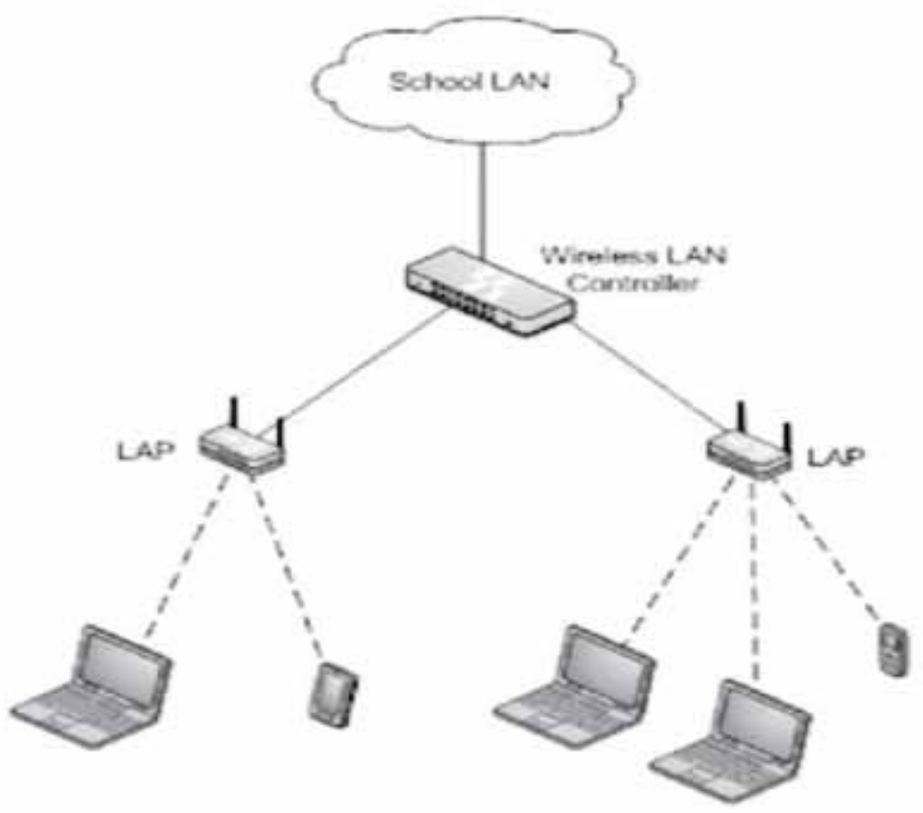


Figure 2: LIGHTWEIGHT/"THIN" AP ARCHITECTURE

Cisco triển khai một trong những hệ thống mạng Wi-Fi Network lớn nhất thế giới

Cisco đã tiến hành hợp tác với Fira de Barcelona và GSMA để xây dựng một trong những hệ thống mạng Wi-Fi network lớn nhất thế giới được giới thiệu tại hội chợ triển lãm Mobile World Congress 2014 của GSMA. Trong suốt tiến trình diễn ra sự kiện, hơn 80,000 người tham dự truy cập miễn phí đến hệ thống mạng Wi-Fi và chỉ trong 4 ngày đã có gần 81,000 thiết bị kết nối đi Internet phát sinh tới 19.1 terabyte lưu lượng dữ liệu.

Theo thống kê sơ bộ thì những người tham dự truy cập hệ thống mạng Wi-Fi network để phục vụ cho công việc, tham gia các mạng xã hội; 33 phần trăm lưu lượng là sử dụng các kết nối bảo mật để truy cập các dịch vụ phục vụ công việc chẳng hạn như email, các kết nối truy cập web, Skype, Google Service và Facebook. Tổng số lượng thiết bị kết nối đi Internet là 80,880 thiết bị, gấp đôi số lượng kết nối so với hội chợ triển lãm Mobile World Congress 2013. Tốc độ lưu lượng truy cập Internet đỉnh điểm là 1.2 gigabyte mỗi giây.

Cisco đã phối hợp với Fira de Barcelona để tiến hành cài đặt hạ tầng mạng Wi-Fi network lên đến diện tích 240,000 m2 tại hội chợ triển lãm Mobile World Congress.

Ta có thể triển khai các chính sách quản trị tại controller như chính sách bảo mật security, RF threshold, QoS, quản lý phần mềm, và xác thực client. Trong khi đó, nhiệm vụ chính của các AP lúc này là vận chuyển các Ethernet frame trên hạ tầng mạng có dây truyền thống sang môi trường mạng không dây thông qua tín hiệu wireless RF signal, lưu lượng data traffic có thể được xử lý tại AP hoặc AP sẽ trung chuyển lên controller. Trái ngược với LAP, AP autonomy có thể tự vận hành mà không cần có sự can thiệp của controller.

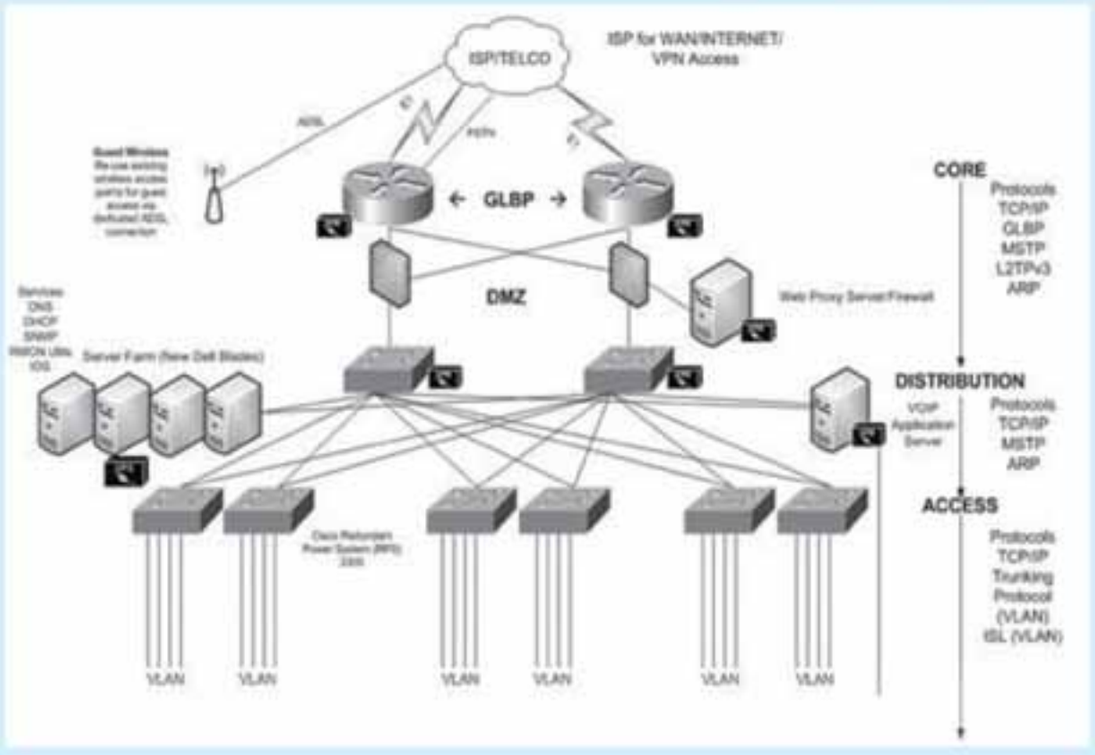
Thông tin thống kê các công nghệ không dây Wireless

Technology	Frequency (GHz)	Channels (US)		Data Rates (Mbps)		Throughput (typical, Mbps)	Standard Ratified	Typical indoor Range (m)*
		Total	Non-overlapping	Max/ channel	Supported			
802.11b	2.4	11	3 (1, 6, 11)	11M	1, 2, 5.5, 11	5	1999	35
802.11g	2.4	11	3 (1, 6, 11)	54M	1, 2, 5.5, 11, 6 ,9, 12, 18, 24, 36, 48, 54	23	2003	25+
802.11a	5	24	24	54M	6, 9 ,12, 18, 24, 36, 48, 54	23	1999	25
802.11n	2.4 or 5	Uses a/b/g bands	Uses a/b/g bands	300M	6, 9, 12, 18, 24, 36, 48, 54, others	100	2009	50
802.11ac	5	Uses 'a' (5GHz) band	Uses 'a' (5GHz) band	500M	6, 9, 12, 18, 24, 36, 48, 54, others	N/A	In progress	N/A

DỊCH VỤ THI CÔNG HỆ THỐNG MẠNG

Với các chuyên gia thiết kế hệ thống mạng có nhiều kinh nghiệm trong việc thiết kế và triển khai hệ thống mạng, trung tâm tích hợp dữ liệu, chúng tôi cung cấp các dịch vụ sau:

- Dịch vụ tư vấn thiết kế, thi công mạng nội bộ (LAN)
- Dịch vụ tư vấn thiết kế, thi công mạng diện rộng (WAN)
- Dịch vụ tư vấn thiết kế, thi công mạng Internet / Intranet
- Dịch vụ tư vấn thiết kế, thi công các lớp bảo mật cho hệ thống mạng



Lợi ích của Khách hàng:

- Tiết kiệm thời gian và chi phí, công sức khi phải tự mình thiết kế hoặc phải thu thiết kế riêng biệt cho từng phần của toàn bộ mô hình hệ thống
- Với tư cách là một chuyên gia hoạt động trong lĩnh vực CNTT, chúng tôi có những quan hệ và cũng là đối tác trực tiếp với nhiều nhà phân phối của các hãng CNTT nổi tiếng của thế giới, chúng tôi có thể tích hợp các công nghệ tiên tiến và phù hợp nhất cho hệ thống của Quý khách hàng.
- Quý khách hàng sẽ được hỗ trợ tư vấn chuyên nghiệp bởi đội ngũ các chuyên viên có kinh nghiệm tư vấn và thiết kế dự án, hệ thống thông tin.
- Quý khách hàng không những được tư vấn các giải pháp và mô hình hệ thống đáp ứng với các nhu cầu hiện tại, chúng tôi còn hỗ trợ tư vấn cho Quý khách hàng khi có nhu cầu mở rộng hệ thống trong tương lai.

QUY TRÌNH TRIỂN KHAI DỊCH VỤ:

I. KHẢO SÁT & THIẾT KẾ HỆ THỐNG

1. Khảo sát & ghi nhận thông tin khách hàng
- Mục đích sử dụng của khách hàng và yêu cầu sử dụng thiết bị
- Khảo sát mặt bằng, kết cấu toà nhà và vị trí lắp đặt thiết bị
- Điều kiện thi công và chất lượng vật liệu thi công (cable, ống, nẹp….) Các điều kiện có thể ảnh hưởng đến hệ thống (điện, môi trường…)

2. Thiết kế chi tiết
- Vẽ kỹ thuật chi tiết hệ thống loại thiết bị được dùng (biểu giá, tính năng kỹ thuật, thời hạn bảo hành) bao gồm: Sơ đồ logic, sơ đồ lắp đặt...
- Số lượng vật tư và các linh kiện đi kèm
- Thời gian thi công

II. LẮP ĐẶT HỆ THỐNG

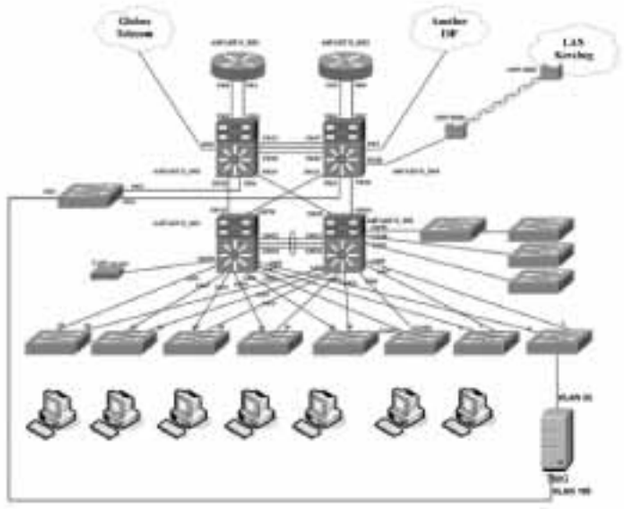
1. Thi công hệ thống cáp mạng
- Triển khai thiết bị dẫn (ống nhựa, nẹp, dây dẫn …)
- Triển khai hệ thống cáp mạng theo đúng sơ đồ thiết kế
- Đánh dấu dây cáp và kết nối vào bộ tập trung (Swich, Router, Firewall...)
- Gắn máy tính vào hệ thống mạng
- Gắn các thiết bị ngoại vi vào hệ thống mạng

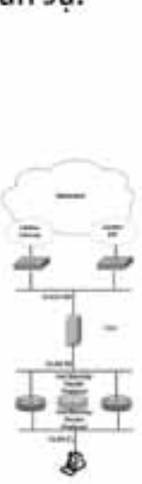
2. Cài đặt hệ thống mạng
- Phân chia nhóm người dùng theo VLAN (chia hệ thống ra thành các mạng con)
- Cấu hình Router, các giao thức định tuyến, load-balancing...
- Cấu hình tường lửa, tạo DMZ cho Server
- Cài đặt hệ điều hành cho server
- Cài đặt giao thức và các dịch vụ mạng
- Tạo nhóm người dùng
- Thiết lập tài khoản của người dùng
- Phân quyền người dùng
- Cài đặt chương trình ứng dụng mạng
- Cài đặt giao thức các máy Client
- Tạo tài khoản máy Client
- Chia sẻ tài nguyên máy Client

III. CHUYỂN GIAO HỆ THỐNG

1. Nghiệm thu hệ thống và chuyển giao
- Kiểm tra sự tương thích và tính ổn định của hệ thống
- Nghiệm thu hệ thống chuyển giao hồ sơ thiết bị (phiếu bảo hành, hoá đơn thanh toán…)
- Chuyển giao hợp đồng thiết kế và lắp đặt, sơ đồ mạng

2. Hướng dẫn sử dụng hệ thống và đào tạo nhân sự.





Hệ thống chứng chỉ của Cisco

Certification Tracks	Entry	Associate	Professional	Expert	Architect
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center	
Design	CCENT	CCDA	CCDP	CCDE	CCAr
Routing & Switching	CCENT	CCNA	CCNP	CCIE Routing & Switching	
Security	CCENT	CCNA Security	CCNP Security	CCIE Security	
Service Provider		CCNA Service Provider	CCNP Service Provider	CCIE Service Provider	
Service Provider Operations	CCENT	CCNA Service Provider Operations	CCNP Service Provider Operations	CCIE Service Provider Operations	
Storage Networking	CCENT			CCIE Storage Networking	
Video		CCNA Video			
Voice	CCENT	CCNA Voice	CCNP Voice	CCIE Voice	
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless	

Cisco Systems là tập đoàn cung cấp giải pháp công nghệ mạng và sản xuất thiết bị mạng lớn nhất trên thế giới. Các nhà tuyển dụng tại Việt Nam hiện nay coi chứng chỉ Cisco như một lợi thế tuyển dụng.

Hệ thống chứng chỉ của Cisco có 9 phân ngành kỹ thuật chính trong lĩnh vực mạng và được phân thành 3 cấp: Associate, Professional, Expert.

Cấp độ chuyên viên (Associate)

- CCNA R&S (Cisco Certified Network Associate Routing and Switching)
- CCDA (Cisco Certified Design Associate)
- CCNA Data Center
- CCNA Security
- CCNA Service Provider
- CCNA Service Provider Operations
- CCNA Video
- CCNA Voice
- CCNA Wireless

Cấp độ chuyên gia (Professional)

- CCNP (Cisco Certified Network Professional)
- CCDP (Cisco Certified Design Professional)
- CCNP Data Center
- CCNP Security
- CCNP Service Provider
- CCNP Service Provider Operations
- CCNP Voice
- CCNP Wireless

Chuyên gia cao cấp (Expert)

Chứng chỉ thuộc cấp độ này gọi là CCIE (Cisco Certified Internetwork Expert), đây được coi là một trong những chứng chỉ nghề CNTT có giá trị và cũng là chứng chỉ khó đạt nhất trong hệ thống chứng chỉ của Cisco:

- CCDE
- CCIE Collaboration
- CCIE Data Center
- CCIE Routing & Switching
- CCIE Security
- CCIE Service Provider
- CCIE Service Provider Operations
- CCIE Storage
- CCIE Wireless

Đây là con đường học tập để trở thành chuyên gia cao cấp Cisco:

Certification Paths	Associate	Professional	Expert
Routing & Switching	CCNA Routing and Switching	CCNP	CCIE Routing & Switching
Design	CCDA	CCDP	CCDE
Data Center	CCNA Data Center	CCNP Data Center	CCIE Data Center
Network Security	CCNA Security	CCNP Security	CCIE Security
Service Provider	CCNA Service Provider	CCNP Service Provider	CCIE Service Provider
Service Provider Operations	CCNA Service Provider Operations	CCNP Service Provider Operations	CCIE Service Provider Operations
Video	CCNA Video		
Voice	CCNA Voice	CCNP Voice	CCIE Collaboration
Wireless	CCNA Wireless	CCNP Wireless	CCIE Wireless

Người biên soạn: Bùi Quốc Kỳ

CẮT TÓC

CON GÁI	CON TRAI
TRƯỚC	TRƯỚC
SAU	SAU
HẾT 300K	HẾT 50K

Nếu:2 = 5
3 = 10
4 = 17
Thì: 5 = ? ? ?

Có 10s thôi nhé :3

Đáp án: 2+ 5 + 3=10, 3+10+4=17, còn lại tự cộng nhé

Khi tôi nói dẫn người yêu về nhà

Bố mẹ nghĩ

Người thân nghĩ

Hàng xóm nghĩ

Bạn bè cũ nghĩ

Bạn đại học nghĩ

Một số người khác nghĩ

Sự thật là

www.nhincuoi.com

HÃY XEM PHIM ONLINE CÙNG PHIM.BIZ

Phim.biz *xin chào bạn!*

Nhằm mong muốn bạn và bạn bè, người thân của mình được thưởng thức những tác phẩm điện ảnh xuất sắc miễn phí và không bị làm phiền bởi quảng cáo, website ***http://phim.biz*** *đã được ra đời.*

Tại trang web ***http://phim.biz****, bạn có cơ hội thưởng thức hơn 6000 tựa phim độ nét cao, hấp dẫn, đa dạng với nhiều thể loại, được tổng hợp và cập nhật liên tục từ nhiều nguồn miễn phí. Từ những bộ phim điện ảnh trong và ngoài nước mới nhất (những bộ phim đang ra rạp trên toàn thế giới) với chất lượng cao, thuyết minh hoặc phụ đề chuẩn hoàn toàn bằng tiếng Việt (đối với phim nước ngoài) mà không làm mất đi bản sắc gốc của phim. Cùng với đó là những bộ phim truyền hình dài tập, phim bộ đang được trình chiếu trên các đài truyền hình Việt Nam và các quốc gia Hàn Quốc, Hồng Công, Đài Loan, Trung Quốc,… Bạn sẽ được thả hồn vào những đoạn phim tình cảm lãng mạn, ngạt thở với những pha hành động ngoạn mục, phiêu lưu cùng những nhân vật huyền thoại, hồi hộp, sợ hãi với những thước phim kinh dị, cười vui đầy sảng khoái với những tình tiết hài hước từ những bộ phim hài… Tất cả đều có tại* ***http://phim.biz***

Ngay bây giờ, bạn có thể sử dụng điện thoại, máy tính bảng hoặc máy tính cá nhân của mình truy cập vào trang ***http://phim.biz*** *để thưởng thức những bộ phim mới và hấp dẫn nhất.*

Phim.biz *chúc bạn có những giây phút thư giãn thoải mái!*

Thân mến,

Phim.biz – Xem phim Online miễn phí

(Trích dẫn từ sách VnPro)

CHƯƠNG 5: ANTEN VÀ CÁC THIẾT BỊ PHỤ TRỢ

2. Bộ giảm tín hiệu

Bộ giảm tín hiệu vô tuyến là một thiết bị làm giảm biên độ của tín hiệu vô tuyến nhưng không làm méo dạng sóng, ngược lại với bộ khuếch đại. Tại sao bạn lại cần phải giảm tín hiệu RF? Hãy xem xét trường hợp một AP có công suất phát cố định là 100 mW và chỉ sử dụng anten đẳng hướng có độ khuếch đại 20 dBi. Nếu bạn sử dụng bộ thiết bị như trên thì sẽ vi phạm các quy tắc của FCC dành cho công suất phát. Vì thế, bạn cần phải sử dụng một bộ giảm tín hiệu để làm giảm tín hiệu vô tuyến xuống còn 30 mW trước khi đưa chúng vào anten. Cách này sẽ đảm bảo cho bạn vẫn tuân thủ theo các quy tắc của FCC.

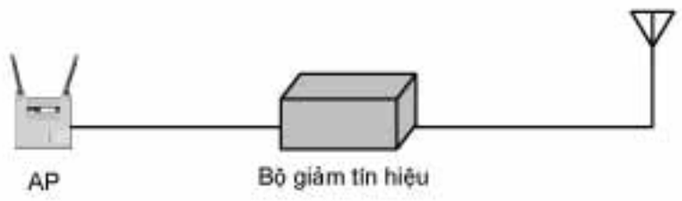
Các tùy chọn phổ biến

Bộ giảm tín hiệu vô tuyến có 2 loại là suy giảm cố định và suy giảm biến thiên. Cũng tương tự như bộ khuếch đại thì bộ giảm tín hiệu biến thiên sẽ cho phép người quản trị mạng cấu hình lượng suy giảm mong muốn.

Hình 5.22: Bộ giảm tín hiệu cố định

Hình 5.23 Bộ giảm tín hiệu biến thiên

Hình 5.24: Vị trí đặt bộ giảm tín hiệu trong WLAN



Để chọn được bộ giảm tín hiệu loại nào thì bạn hãy xem xét ví dụ tương tự như khi chọn loại khuếch đại ở trên. Kiểu giảm tín hiệu (cố định hay biến thiên), trở kháng, công suất đầu vào, suy hao, tần số đáp ứng và kiểu đầu nối là tất cả những điều mà bạn cần quan tâm khi quyết định chọn bộ giảm loại nào.

Cấu hình và quản trị

Tương tự như bộ khuếch đại, bộ giảm tín hiệu cũng được cài đặt trực tiếp trên đường tín hiệu chính. Bộ giảm tín hiệu cố định đồng trục được kết nối trực tiếp giữa bất kỳ 2 điểm kết nối nào nằm giữa bộ phát sóng và anten. Ví dụ, một bộ giảm tín hiệu cố định đồng trục có thể được kết nối trực tiếp vào bất kỳ điểm nào giữa AP và anten.

Việc cấu hình là không cần thiết trừ khi bạn sử dụng bộ giảm tín hiệu biến thiên. Các chỉ dẫn cấu hình của nhà sản xuất thường được kèm theo khi mua thiết bị.

3. Bộ thu lôi

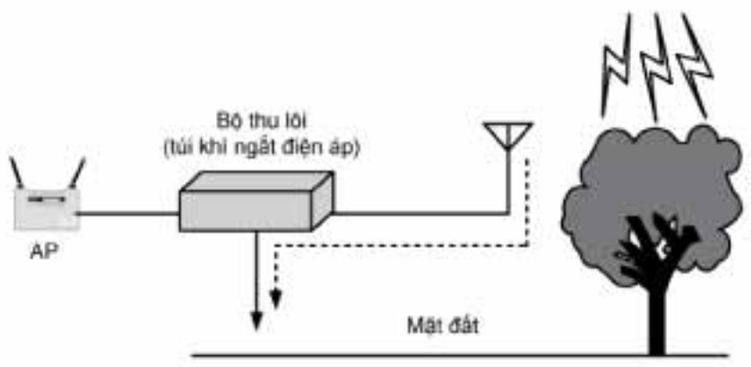
Bộ thu lôi được sử dụng để chuyển hướng dòng điện gây ra bởi sét xuống mặt đất. Nó cũng được sử dụng để bảo vệ phần cứng WLAN như AP, cầu nối hay cầu nối nhóm được kết nối vào đường truyền đồng trục. Đường truyền đồng trục rất dễ bị ảnh hưởng bởi sét đánh ở các vùng lân cận.

Một sự hiểu nhầm phổ biến về bộ thu lôi là nó được lắp đặt để bảo vệ chống lại sét đánh trực tiếp. Nếu như anten bị sét đánh trực tiếp thì cho dù bộ thu lôi có tốt đến đâu thì anten của bạn vẫn bị phá hủy và các thiết bị WLAN khác vẫn có thể bị hư hỏng. Hãy nhớ là bộ thu lôi không phải dùng để bảo vệ sét đánh trực tiếp mà chỉ bảo vệ khi sét đánh ở vùng lân cận gây ra sự tăng dòng điện đột ngột trong dây dẫn.

Một bộ thu lôi có thể chuyển hướng một dòng điện lên đến 5000 A và 50 V. Bộ thu lôi hoạt động như sau:

- Sét đánh ở những vật lân cận.
- Dòng điện sẽ tăng đột ngột trên đường truyền RF.
- Bộ thu lôi cảm nhận được dòng điện này và ngay lập tức ion hóa khí được lưu giữ bên trong gây ra ngắn mạch (một đường dẫn hầu như không có trở kháng) trực tiếp xuống mặt đất.

Hình 5.25: Cài đặt bộ thu lôi trong mạng



Khi một vật thể bị sét đánh thì điện trường sẽ được hình thành xung quanh vật đó chỉ trong chốc lát. Khi sét đánh xong (ngừng cấp điện vào vật thể) thì điện trường cũng mất dần. Khi điện trường biến mất thì nó cũng sinh ra một lượng dòng điện lớn vào bên trong vật thể (trong trường hợp này là anten hay đường truyền đồng trục).

Các tùy chọn phổ biến

Có một số ít tùy chọn cho bộ thu lôi và chi phí khoảng từ 50 đến 150 $ cho mỗi dòng sản phẩm. Tuy nhiên, có một số thuộc tính nên được xem xét khi mua bất kỳ bộ thu lôi nào:

- Tuân theo chuẩn IEEE (tốc độ phản ứng < 8 µs).
- Sử dụng lại được.
- Túi khí ngắt điện áp.
- Kiểu đầu nối.
- Tần số đáp ứng.
- Trở kháng.
- Suy hao chèn (cài đặt thêm thiết bị vào).
- Tỷ lệ điện áp sóng đứng VSWR.
- Bảo hành.

<u>*Chuẩn IEEE:*</u> Hầu hết các bộ thu lôi đều có thể gây ra ngắn mạch xuống mặt đất chỉ chưa tới 2 µs nhưng IEEE quy định rằng tiến trình này nên xảy ra không quá 8 µs. Vì thế bạn cần bảo đảm rằng thiết bị bạn chọn ít nhất cũng tuân theo chuẩn IEEE.

<u>*Có thể sử dụng lại:*</u> Một số bộ thu lôi có thể sử dụng lại được sau khi sét đánh. Sẽ rất là hiệu quả về mặt chi phí nếu bạn sử dụng một bộ thu lôi có thể sử dụng lại nhiều lần. Các model sử dụng lại được có túi khí có thể thay thế, nó sẽ rẻ hơn so với việc phải thay mới bộ thu lôi. Việc mua một bộ thu lôi có túi khí thay thế được và có khả năng thay thế trong khi vẫn được cấp nguồn hoạt động sẽ là một tính năng rất hữu ích cho phép bạn thay thế các thành phần của bộ thu lôi mà không cần phải tạm thời ngắt mạng WLAN.

<u>*Điện áp ngắt:*</u> Một số bộ thu lôi hỗ trợ việc chuyển điện áp 1 chiều DC để sử dụng trong việc cấp nguồn cho bộ khuếch đại vô tuyến. Bạn nên sử dụng bộ thu lôi có tính năng này nếu như bạn dự định sử dụng bộ khuếch đại gần anten hơn là gần bộ thu lôi. Túi khí ngắt điện áp (mức điện áp mà bộ thu lôi bắt đầu ngắn mạch dòng điện xuống mặt đất) nên cao hơn mức điện áp yêu cầu cho sự hoạt động của bộ khuếch đại. Có một khuyến cáo là bạn nên đặt bộ thu lôi là thành phần cuối cùng trên đường truyền vô tuyến trước khi đến anten để cho bộ thu lôi có thể bảo vệ bộ khuếch đại và bộ suy hao cũng như cầu nối hay AP.

<u>*Kiểu đầu nối:*</u> Hãy đảm bảo rằng kiểu đầu nối của bộ thu lôi mà bạn đã chọn phải tương xứng với cáp mà bạn dự định sử dụng trong mạng WLAN. Nếu như chúng không tương xứng với nhau thì một bộ tiếp hợp đầu nối (adapter connector) phải được sử dụng, điều này gây ra sự mất mát trong mạch vô tuyến nhiều hơn mức cần thiết.

<u>*Tần số đáp ứng:*</u> Tần số đáp ứng của bộ thu lôi phải ít nhất là cao bằng mức tần số cao nhất được sử dụng trong WLAN. Ví dụ, nếu bạn chỉ sử dụng mạng WLAN 2,4 GHz thì bộ thu lôi nên 3 GHz là tốt nhất.

<u>*Trở kháng:*</u> Trở kháng của bộ thu lôi nên tương xứng với tất cả các thiết bị khác trong mạch giữa bộ phát sóng và anten. Trở kháng thường là 50 Ohm trong hầu hết các thiết bị WLAN.

Suy hao chèn: Suy hao chèn càng thấp càng tốt (khoảng 0,1 dB) để cho nó không gây ra sự mất mát biên độ tín hiệu vô tuyến khi tín hiệu được truyền qua bộ thu lôi.

Tỷ số điện áp sóng đứng VSWR: Tỷ số VSWR của một bộ thu lôi có chất lượng tốt là khoảng 1,1:1, nhưng một số có thể lên đến 1,5:1. Tỷ số này của thiết bị càng thấp thì tín hiệu vô tuyến sẽ càng tốt hơn.

Bảo hành: Cho dù chất lượng của bộ thu lôi có tốt đến đâu thì nó cũng có thể gặp trục trặc. Hãy tìm những nhà sản xuất cung cấp chế độ bảo hành tốt nhất.

Cấu hình và quản trị

Việc cấu hình là không cần thiết đối với bộ thu lôi. Nó được cài đặt trên đường tín hiệu vô tuyến chính và nối đất nên có trở kháng thấp hơn 5 Ohm. Bạn nên kiểm tra nối đất với thiết bị kiểm tra trở kháng thích hợp trước khi quyết định cài đặt bộ thu lôi. Bạn cũng nên thường xuyên kiểm tra định kỳ các thành phần khác của bộ thu lôi như túi khí,…

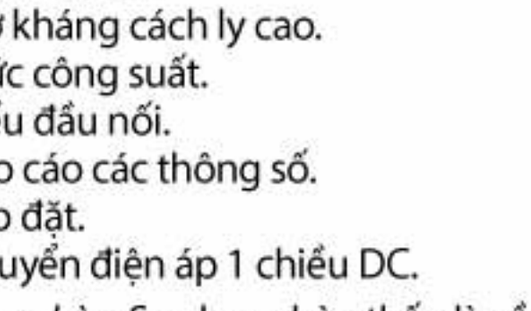
4. Bộ tách

Bộ tách là một thiết bị có một đầu vào và nhiều đầu ra. Nó được sử dụng nhằm mục đích chia một tín hiệu thành nhiều tín hiệu độc lập. Việc sử dụng bộ tách thường xuyên trong mạng WLAN là không được khuyến khích. Đôi khi, 2 anten Panel 1200 hay 2 anten Panel 900 có thể được kết hợp với một bộ tách khi anten chỉa ra 2 hướng ngược nhau. Cấu hình này sẽ sinh ra một vùng phủ sóng theo 2 hướng có thể là lý tưởng để phủ sóng những vùng dọc theo sông hay đường cao tốc. Hai anten Panel 900 quay lưng với nhau có thể được tách biệt khoảng 25 cm hay 101 cm ở cả 2 phía của cột thay tháp. Mỗi anten Panel trong cấu hình này có thể có một độ nghiêng nào đó. Kết quả là độ khuếch đại theo mỗi hướng phát sóng sẽ bị giảm đi 3-4 dB.

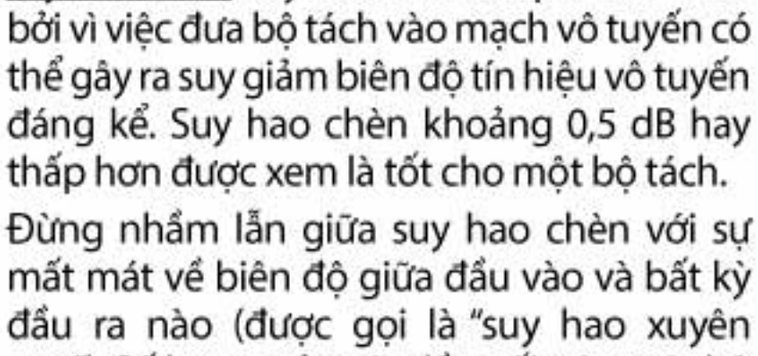
Khi cài đặt một bộ tách, thì đầu vào nên luôn luôn quay mặt vào nguồn của tín hiệu vô tuyến. Các đầu ra (đôi khi được gọi là "tap") được kết nối hướng về đích của tín hiệu vô tuyến.

Bộ tách có thể được sử dụng để theo dõi công suất phát trên một đường kết nối WLAN. Bằng cách mắc một máy đo công suất vào một đầu ra và một anten ở đầu ra kia thì người quản trị mạng có thể chủ động giám sát công suất phát ở bất cứ thời điểm nào. Trong trường hợp này, máy đo công suất, anten và bộ tách tất cả phải có trở kháng bằng nhau. Việc thay thế máy đo công suất ở một đầu ra của bộ tách bằng một thiết bị tải 50 Ohm sẽ cho phép người quản trị mạng di chuyển máy đo công suất từ một điểm kết nối này đến điểm kết nối khác trong mạng WLAN để đo công suất phát.

Hình 5.26: Bộ tách sóng vô tuyến



Hình 5.27: Cài đặt bộ tách trong mạng



Chọn lựa bộ tách

Dưới đây là danh sách các thứ cần xem xét khi chọn lựa một bộ tách:

- Suy hao chèn.
- Tần số đáp ứng.
- Trở kháng.
- Tỷ số VSWR.
- Trở kháng cách ly cao.
- Mức công suất.
- Kiểu đầu nối.
- Báo cáo các thông số.
- Lắp đặt.
- Chuyển điện áp 1 chiều DC.

Suy hao chèn: Suy hao chèn thấp là cần thiết bởi vì việc đưa bộ tách vào mạch vô tuyến có thể gây ra suy giảm biên độ tín hiệu vô tuyến đáng kể. Suy hao chèn khoảng 0,5 dB hay thấp hơn được xem là tốt cho một bộ tách.

Đừng nhầm lẫn giữa suy hao chèn với sự mất mát về biên độ giữa đầu vào và bất kỳ đầu ra nào (được gọi là "suy hao xuyên qua"). Số lượng của các đầu nối trên một bộ tách sẽ quyết định số đường (gọi theo thuật ngữ của công suất) mà biên độ của sóng vô tuyến sẽ bị chia. Một bộ tách 2 đường nên có suy hao khoảng 3 dB giữa đầu vào và bất kỳ đầu ra nào. Suy hao lớn hơn mức này có thể được cho là do suy hao chèn (sẽ được cộng thêm vào suy hao xuyên qua khi tính toán) hay do sự không chính xác trong khả năng phân chia công suất giữa các đầu ra.

Tần số đáp ứng: Tần số đáp ứng của bộ tách nên cao ít nhất là bằng tần số cao nhất được sử dụng trong mạng WLAN. Ví dụ, nếu bạn đang sử dụng mạng WLAN 2,4 GHz thì bộ tách nên khoảng 3 GHz là tốt nhất.

Trở kháng: Trở kháng thường là 50 Ohm trong hầu hết các mạng WLAN. Trở kháng của bộ tách nên tương xứng với tất cả các thiết bị khác trong mạch giữa bộ phát sóng và anten.

Tỷ số VSWR: Cũng giống như nhiều thiết bị vô tuyến khác, tỷ số VSWR nên càng gần 1:1 càng tốt. Thông thường thì tỷ số VSWR cho bộ tách là nhỏ hơn 1,5:1. Tỷ số VSWR thấp đối với bộ tách là quan trọng hơn so với các thiết bị khác bởi vì công suất vô tuyến phản xạ trong bộ tách có thể được phản xạ theo nhiều hướng bên trong bộ tách làm ảnh hưởng đến cả đầu vào và đầu ra.

Trở kháng cách ly cao: Trở kháng cách ly cao giữa các cổng trên bộ tách là rất quan trọng vì nhiều lý do khác nhau. Thứ nhất, tải trên một cổng ra không nên gây ảnh hưởng lên công suất phát của các cổng ra khác trên bộ tách. Thứ hai, một tín hiệu đến từ cổng ra của bộ tách (như tín hiệu vô tuyến nhận được) nên được hướng trực tiếp vào cổng vào hơn là vào một cổng ra khác. Các yêu cầu này có thể đạt được bằng trở kháng cao giữa các đầu ra. Trở kháng cách ly thường là ⊠ 20 dB giữa các cổng ra. Một số bộ tách có một tính năng được gọi là cách ly đảo cổng cho phép cổng ra được sử dụng như là cổng vào. Sử dụng bộ tách theo kiểu này cho phép người quản trị mạng kết nối 2 hay 3 AP hay cầu nối vào bộ tách, các AP này sau đó sẽ cung cấp tín hiệu cho 1 anten duy nhất. Cấu hình này có thể tiết kiệm chi phí phải mua và cài đặt nhiều anten.

Mức công suất: Các bộ tách đã được ước tính công suất đầu vào lớn nhất, có nghĩa là lượng công suất giới hạn mà bạn có thể đưa vào bộ tách. Nếu bạn đưa vào mức công suất cao hơn mức cho phép của nhà sản suất thì sẽ gây hư hỏng bộ tách.

Kiểu đầu nối: Bộ tách thường có các kiểu đầu nối như N-Type hay SMA. Bạn phải sử dụng bộ tách có cùng kiểu đầu nối với cáp. Như thế sẽ tiết kiệm được chi phí phải mua thêm bộ tiếp hợp đầu nối. Điều này là rất quan trọng vì bộ tách đã làm giảm biên độ tín hiệu nên nếu dùng thêm bộ tiếp hợp đầu nối sẽ làm giảm hơn nữa biên độ tín hiệu.

Báo cáo các thông số: Tất cả các bộ tách nên đi kèm với một báo cáo về thông số trong đó cho biết suy hao chèn, tần số đáp ứng, suy hao xuyên qua của mỗi đầu nối,… Bạn nên làm các báo cáo này 1 năm 1 lần để cho người quản trị mạng có thể biết được bộ tách có gây ra một sự sụt giảm về hiệu năng nào không. Lúc thực hiện báo cáo này đòi hỏi phải tạm thời ngắt mạng WLAN trong một thời gian ngắn và dường như là không thực tế nhưng nó rất cần thiết để duy trì sự tối ưu về thông lượng cho mạng.

Lắp đặt: Việc lắp đặt bộ tách cũng giống như lắp đặt các thiết bị khác. Một số model có các phần cứng kèm theo để lắp đặt theo dạng cột sử dụng chốt hình chữ U. Tùy vào nhà sản suất, bộ tách có thể chịu đựng được thời tiết, có nghĩa là nó có thể cài đặt ngoài trời trên một cái cột mà không cần lo lắng đến thời tiết (nước, mưa, gió,…) gây ảnh hưởng. Khi cài đặt ngoài trời thì bạn nên bọc cáp lại và sử dụng một rãnh thoát nước.

Chuyển điện áp DC: Một số bộ tách có khả năng chuyển điện áp DC ra tất cả các cổng ra một cách đồng thời. Tính năng này rất hữu ích khi bạn có sử dụng một bộ khuếch đại cần cấp nguồn DC bằng một bộ cấp điện áp DC (thông qua PoE) nằm trong phòng thiết bị, mà bộ khuếch đại này nằm ở cổng ra của bộ tách.

[... còn tiếp]

CHÀO HÈ

Ưu đãi hấp dẫn khi tham gia đóng nhóm
Ưu đãi 10% cho học viên cũ
Tặng ngay áo thun VnPro + Lịch World Cup 2014

LỊCH KHAI GIẢNG THÁNG 6

Mã lớp	Tên khóa học	Ngày khai giảng	Ngày học	Giờ học	Học phí/khóa	Thời gian
CHƯƠNG TRÌNH CCNAX & CCNA SECURITY						
AK9	**CCNAX** (200-120)	05/06/2014	3 – 5 – 7	8:30 – 11:30	3.360.000	152 giờ
A7				18:30 – 21:30	6.720.000	
AK12		11/06/2014	2 – 4 – 6	8:30 – 11:30	3.360.000	
AK14				14:00 – 17:00	3.360.000	
A8				18:30 – 21:30	6.720.000	
AK11		19/06/2014	3 – 5 - 7	8:30 – 11:30	3.360.000	
AK13				14:00 – 17:00	3.360.000	
A9				18:30 – 21:30	6.720.000	
AK16		25/06/2014	2 – 4 – 6	14:00 – 17:00	3.360.000	
A10				18:30 – 21:30	6.720.000	
	CCNAX Hè	16/06/2014	2-3-4-5-6-7	8:30 – 11:30	3.360.000	
		26/06/2014		14:00 – 17:00	3.360.000	
	Ôn CCNAX	24&26/6/2014	3 -5	18:30 – 21:30	Miễn phí	6 giờ
AS1	**CCNA Security** (640-554)	04/06/2014	2 – 4 – 6	18:30 – 21:30	6.720.000	100 giờ
AV1	**CCNA Voice** (640-461)	19/06/2014	3 – 5 - 7	18:30 – 21:30	6.720.000	
CHƯƠNG TRÌNH CCNP						
P1-K2	**ROUTE** (642-902)	19/06/2014	3 – 5 - 7	8:30 – 11:30	5.880.000	120 giờ
P1-4				14:00 – 17:00	5.880.000	
P1-K3				18:30 – 21:30	8.232.000	
P2K2	**SWITCH** (642-813)	12/06/2014	3 – 5 - 7	8:30 – 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)	17/06/2014	3 – 5 – 7	18:30 – 21:30	8.232.000	120 giờ
CHƯƠNG TRÌNH CCIE						
EW1	**CCIE WRITTEN** (Version 5)	27/06/2014	2 – 4 – 6	18:30 – 21:30	11.760.000	120 giờ

ĐĂNG KÝ HỌC LIÊN HỆ

KIM LOAN Email: kimloan@vnpro.org Di động: 0936 393 167
THANH TRÂM Email: thanhtram@vnpro.org Di động: 0949 246 829 – 0906 616322
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**