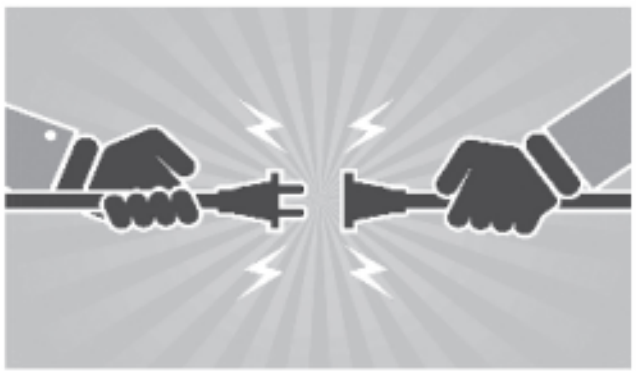
Số 40
11/2015

BẢN TIN dancisco

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



Bạn đang tận hưởng "internet miễn phí" từ hàng tá điểm truy cập Wi-Fi rải rác ở thư viện, quán cà phê / kem, nhà hàng ăn uống hay bar / pub nọ kia, đó là chưa kể một số điểm công cộng lớn, chịu chơi cũng phủ sóng WiFi miễn phí. Mọi thứ trông có vẻ vô hại vì hàng trăm, thậm chí hàng ngàn người cùng dùng chung như bạn kia mà. Vậy nhưng... bạn sẽ không thể ngờ được một điều rằng một người lạ nào đó vẫn có thể biết được nơi sinh của bạn, những ngôi trường mà bạn đã trải qua, kể cả lịch sử duyệt web mới đây nhất trong vòng 20 phút của bạn v.v. Nguy hiểm hơn, những người lạ ấy thậm chí có thể đăng nhập tài khoản Facebook của bạn để xem tin nhắn, đọc những status của bạn bè bạn hoặc... đăng status giùm bạn luôn khi họ cùng kết nối chung một mạng Wi-Fi.

[Trang 02]

Sơ lược về mạng không dây

1. Mạng không dây

Mạng không dây (hay còn gọi là mạng Wi-Fi, mạng Wireless, 802.11) là mạng kết nối các thiết bị có khả năng thu phát sóng (như máy vi tính có gắn Adapter không dây, PDA,...) lại với nhau không sử dụng dây dẫn mà sử dụng song vô tuyến được truyền dẫn trong không gian thông qua các trạm thu/phát sóng.

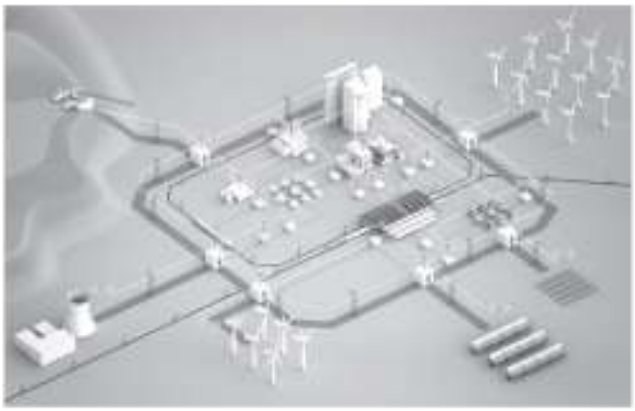
[Trang 11]

VNPRO TRI ÂN GIẢNG VIÊN PHÒNG DA-ĐT NHÂN NGÀY 20/11

Hơn 12 năm nay, VnPro luôn là lựa chọn hàng đầu của những kỹ sư mạng máy tính và các bạn sinh viên trong việc lựa chọn nơi làm bệ phóng cho ước mơ chinh phục đỉnh cao tri thức. Đội ngũ giảng viên chuyên nghiệp và kỹ năng sư phạm tuyệt vời luôn là niềm tự hào của VnPro.

[Trang 07]

TIN TỨC SỰ KIỆN KHÁC



Hiện tại số lượng thiết bị kết nối mạng đang nhiều gấp đôi so với lượng người trên Trái Đất. Từ những bộ điều khiển nhiệt độ, cửa, TV cho đến các máy bơm nước, các hệ thống cảm biến, robot, điện thoại, TV, tất cả đều được gọi chung là Internet of Things (IoT). Nhưng vấn đề nằm ở chỗ chúng không hề nói một "ngôn ngữ" chung nào cả, việc giao tiếp giữa các thiết bị IoT vẫn còn là một vấn đề nan giải. Cái thì dùng Wi-Fi, cái thì xài Bluetooth, một số khác thì dùng sóng radio hay các loại kết nối tầm gần. Vậy làm sao một thiết bị có Wi-Fi kết nối được với thiết bị chỉ có Bluetooth? Gần như không thể nào. Chính vì vậy, không sai khi nói rằng thế giới IoT đang bị thiếu đi một thành phần quan trọng: một giao thức kết nối không dây chung.

Hiện nay các thiết bị IoT thường dùng kết nối gì?

Chúng ta đã khá quen thuộc với Wi-Fi và Bluetooth vì chúng xuất hiện đầy xung quanh mình. Hiện tại rất nhiều thiết bị đã dùng một trong hai hoặc cả hai kết nối này, từ smartphone, tablet, TV, tủ lạnh, lò vi sóng cho đến các bóng đèn thông minh. Bên cạnh đó, những thiết bị mang tính công nghiệp hơn, chẳng hạn như máy bơm, van áp suất, robot... thì hoặc dùng Wi-Fi, hoặc dùng ZigBee. ZigBee còn được gọi là chuẩn 802.15.4, nó là một giao tiếp tầm gần được kỳ vọng sẽ tăng trưởng mạnh trong vòng 5 năm tới, từ con số 425 triệu thiết bị ở hiện tại lên thành 2,1 tỉ vào năm 2019 theo số liệu từ ABI Research. Hiện cũng đã có bóng đèn Philips Hue là dùng ZigBee.

Andrew Zignani, một nhà phân tích của ABI, cho hay: "Khả năng tiêu thụ điện thấp, giá rẻ và kết nối ngang hàng giữa nhiều thiết bị của ZigBee sẽ khiến cho chúng trở thành công nghệ kết nối không dây được chọn dùng cho nhiều loại sản phẩm, từ nhà cửa, tự động hóa trong công nghiệp, đo lường thông minh cho đến giải trí tại gia."

Nhưng không dừng lại ở đây, thị trường IoT còn có một vài kế hoạch khác.

Bluetooth, Wi-Fi, mạng di động hay sóng radio?

Phil Williams, kiến trúc sư trưởng của Rackspace, một công ty chuyên về điện toán đám mây, bình luận: "Các chuẩn chung trong lĩnh vực IoT vẫn còn rất lung tung, nhưng cá nhân tôi thì chọn Wi-Fi bởi vì sự phổ biến của nó trong các hộ gia đình, ngoài ra Bluetooth LE cũng có thể được sử dụng để ghép nối thiết bị IoT với điện thoại di động." Ông còn nghĩ đến việc tận dụng hệ thống điện trong nhà để kết nối nhanh thiết bị IoT với nhau.

Còn mạng di động thì có thể được dùng để theo dõi xem những tài sản, gói hàng đang luân chuyển đến đâu, hoặc để giám sát các phương tiện giao thông công cộng. Ví dụ, nhà mạng AT&T ở Mỹ đã cung cấp một dịch vụ sử dụng thẻ SIM để theo dõi các tác phẩm nghệ thuật khi chúng được chuyển giữa các cuộc triển lãm, hoặc khi đóng thùng để chuyển đi những nơi xa hơn.

Martin Poppelaars, phó chủ tịch mảng bán hàng của công ty công nghệ Lantronix, nói thêm: "Về cơ bản thì những kết nối nói trên không được xem như một giao thức, chúng chỉ là các đường ống để nối những thiết bị lại với nhau". Và thế giới đang cần một "giao thức thứ tư".

Vì sao Wi-Fi, ZigBee không phải là lựa chọn tốt nhất?

Rõ ràng Wi-Fi và ZigBee không thể phủ sóng đi xa. Nếu chỉ dùng trong nhà thì ổn, nhưng khi đưa vào các xưởng sản xuất, các cánh đồng năng lượng gió, hệ phức hợp khai thác dầu mỏ, đèn đường và nông trại thì Wi-Fi không còn là lựa chọn tốt. Nói cách khác, với những món đồ IoT tiêu dùng như bóng đèn, lò vi sóng, cảm biến gắn trong vườn thì có thể xài Wi-Fi hoặc ZigBee, nhưng còn các sản phẩm công nghiệp thì không.

Và mảng công nghiệp mới thật sự lại mảnh đất màu mỡ cho ứng dụng IoT. Đây cũng là nơi mà các tập đoàn lớn như Siemens, GE, Rockwell lẫn các công ty công nghệ như Cisco, Intel, Oracle, Qualcomm nhắm tới. Thị trường thiết bị công nghiệp thường đặt hàng với số lượng lớn, mức độ tái sử dụng cao, lại còn có thể thu được nhiều tiền bảo trì trong nhiều năm sau khi bán sản phẩm nên không lạ khi mà các tập đoàn lớn đều muốn khai thác nó.

Olivier Hersent, CEO, CTO kiêm nhà sáng lập của Actility - công ty giải pháp mạng cho thiết bị IoT - nói thêm rằng IoT hiện tại sẽ tiếp tục dùng Wi-Fi và ZigBee, nhưng vì các hạn chế về thời lượng pin, độ bao phủ và mạng LAN khó quản lý nên đây không phải là những lựa chọn tốt.

còn tiếp ...

Bạn đang tận hưởng "internet miễn phí" từ hàng tá điểm truy cập Wi-Fi rải rác ở thư viện, quán cà phê / kem, nhà hàng ăn uống hay bar / pub nọ kia, đó là chưa kể một số điểm công cộng lớn, chịu chơi cũng phủ sóng WiFi miễn phí. Mọi thứ trông có vẻ vô hại vì hàng trăm, thậm chí hàng ngàn người cũng dùng chung như bạn kia mà. Vậy nhưng... bạn sẽ không thể ngờ được một điều rằng một người lạ nào đó vẫn có thể biết được nơi sinh của bạn, những ngôi trường mà bạn đã trải qua, kể cả lịch sử duyệt web mới đây nhất trong vòng 20 phút của bạn v.v. Nguy hiểm hơn, những người lạ ấy thậm chí có thể đăng nhập tài khoản Facebook của bạn để xem tin nhắn, đọc những status của bạn bè bạn hoặc... đăng status giùm bạn luôn khi họ cùng kết nối chung một mạng Wi-Fi.

À này, đừng vì các thông tin trên mà bạn không bao giờ dám dùng mạng WiFi công cộng nữa nhé, bởi đó không phải lỗi hoàn toàn ở các nơi cung cấp WiFi. Thay vào đó, chúng ta hãy cùng tìm hiểu xem tại sao các mạng Wi-Fi công cộng lại trở thành tổ mật lôi cuốn giới hacker đến thế, và các tay hacker ấy dùng những mánh lới nào để thâm nhập máy tính và đánh cắp thông tin từ bạn.

Vì sao các mạng Wi-Fi công cộng trở thành đích ngắm hấp dẫn? Và các hacker làm cách nào để thâm nhập bất hợp pháp máy tính của người dùng?

Hầu hết các mạng WiFi miễn phí mà chúng ta đang dùng hiện nay hoặc là cùng dùng chung mật khẩu, hoặc nhiều nơi dễ dãi hơn thì để "open" và bất kỳ ai cũng có thể kết nối. Chính vì vậy nên nghiễm nhiên các mạng Wi-Fi công cộng trở thành miếng mồi ngon cho các hacker tìm đến thi thố tài năng.

Các hacker sẽ dùng cách thức đứng giữa người dùng và trang web hay dịch vụ internet mà người dùng đang truy cập để thu thập thông tin. Công việc này tưởng rằng không đơn giản nhưng thật ra với vô số công cụ bẻ khóa, dò quét mạng cộng thêm chút năng khiếu phá phách của chính các hacker thì mọi việc bỗng trở nên đơn giản, nhưng chưa hết, chính bản thân người dùng cũng đã tiếp tay cho các hacker khi hời hợt dùng và chia sẻ các thông tin quan trọng, nhạy cảm bằng chính mạng Wi-Fi công cộng.

Tấn công theo hình thức Man In the Middle

Đây là cách thức tấn công phổ biến và được giới hacker ưa chuộng nhất. Với hình thức tấn công Man In The Middle, các hacker sẽ có thể thấy mọi thông tin được truyền đến và đi từ máy tính của người dùng. Với những gì đã thu thập được thì họ có thể can thiệp và thay đổi tùy thích để phục vụ cho mục đích phá hoại.

Tấn công theo hình thức Evil Twin

Đây là một phiên bản biến tấu của tấn công Man In The Middle. Để tấn công Evil Twin, các hacker sẽ dựng lên các điểm truy cập WiFi giả, và người dùng sẽ ngây thơ kết nối vô một mạng có cái tên trông hoàn toàn vô hại đại loại như "Free Public Wi-Fi". Lắm khi trong khi kết nối còn suýt xoa rằng "người tốt vẫn còn nhiều đấy chứ".

Chỉ có điều là người dùng lúc này đã ngoan ngoãn tự nguyện chui đầu vào bẫy bởi một khi đã kết nối thành công thì tất tần tật những trao đổi qua lại trên mạng đều được các người tốt giấu mặt ngầm nghĩa, thu thập.

Có không ít hacker còn tinh ranh hơn khi đặt một cái tên mạng (SSID) gần giống như tên của các hàng quán quanh đó, chẳng hạn Coffee Bean 1 (giả) có khác gì so với Coffee Bean (thật)? Thế là vô số chú nai vàng ngơ ngác lọt bẫy thôi. Một số hacker cao tay hơn thậm chí còn có thể broadcast các chứng chỉ và credential giả (mà như thật) phù hợp với thông số của các router mà người dùng từng kết nối, và với trình độ này thì đại đa số người dùng phổ thông chỉ có nước từ chết đến bị thương mà vẫn không ngớt cảm kích thầm rằng "đời vẫn nhiều người tốt cho không biếu không lắm".

Tấn công theo hình thức Packet Sniffer

Ngoài tấn công Man In The Middle và Evil Twins ra thì các hacker sẽ còn dùng phần mềm gọi là packet sniffer để thu thập các dữ liệu người dùng giao dịch trên internet. Phần mềm packet sniffer sẽ nghe ngóng và bắt tất cả các gói dữ liệu đang được trao đổi qua lại trên mạng, và công việc còn lại của các hacker là ngồi sàng lọc những gì dùng được cho họ về sau. Thật ra thì phần mềm bắt gói thông tin packer sniffer vẫn được các quản trị viên hệ thống máy tính sử dụng để giám sát và xử lý các trục trặc phát sinh trên đường truyền mạng. Nhưng với mục đích sử dụng bất chính của giới hacker thì hậu quả để lại là khôn lường.

Trên đây là ba hình thức tấn công mạng phổ biến nhất, tiếp theo chúng ta sẽ tìm hiểu xem liệu người dùng có thể làm gì để tự bảo vệ họ.

Những gì người dùng có thể làm

Một số điểm truy cập Wi-Fi công cộng có đòi hỏi người dùng phải đăng nhập, nhưng thực tế là thao tác ấy không giúp bảo vệ người dùng được bao nhiêu mà đó chỉ là một hình thức nhận dạng người dùng để... xuất hóa đơn tính tiền trong trường hợp mạng Wi-Fi đó có tính phí. Các phương pháp sau mới thật sự giúp người dùng bảo vệ chính họ.

còn tiếp ...

LAB CME. Cấu hình CME
cấp số Directory Number cho các IP Phone

Kỳ 4:

Bước 9: Cấu hình tính năng chuyển hướng cuộc gọi Call Forwarding trên CME

Tính năng chuyển hướng cuộc gọi Call Forwarding có thể được thực hiện bằng cách sử dụng giao diện hiển thị phone display trên IP Phone, hoặc có thể chuyển hướng tự động nếu người dùng ở trạng thái bận busy bằng cách cấu hình trên CME.

Cisco IP Phones có một softkey trên giao diện phone display cho phép chuyển hướng cuộc gọi calls tới một số dn number khác. Phone user chỉ cần nhấn vào CFwdAll softkey trên màn hình hiển thị display, dials tới extension mà cuộc gọi calls sẽ được forward tới, nhấn tiếp EndCall softkey để kích hoạt tác vụ chuyển hướng cuộc gọi.

Khi tính năng chuyển hướng cuộc gọi forwarding được kích hoạt (active), tất cả các cuộc gọi tới extension sẽ không phát tín hiệu ring trên phone hiện tại, mà sẽ được chuyển hướng hết tới extension chỉ định trước đó. Để hủy bỏ (cancel) tính năng call forwarding, nhấn nút CFwdAll key thêm lần nữa.

Để chuyển hướng cuộc gọi tự động nếu người dùng ở trạng thái bận busy, hoặc người dùng không bắt máy sau một số lần máy đổ chuông, ta cần cấu hình tính năng call forward trên CME bằng câu lệnh "call-forward command" với nhiều options khác nhau chẳng hạn như forwarding all calls hoặc forwarding calls automatically after hours, trong đó có 2 option phổ biến nhất là chuyển hướng cuộc gọi forwarding calls khi phone ở trạng thái busy và forwarding calls nếu như người dùng không bắt máy sau khoảng thời gian xác định trước (a set amount of time) với tùy chọn (call-forward noan) option sao cho cuộc gọi calls có thể được gửi tới voicemail, tổng đài viên operator, hoặc chuyển sang chế độ trả lời tự động auto- attendant.

Ta sẽ cấu hình để ephone-dn 1 sẽ chuyển hướng cuộc gọi forward calls tới extension x1003 khi ephone-dn ở trạng thái bận busy và khi ephone-dn không trả lời cuộc gọi sau 12 giây.

```
CME(config)# ephone-dn 1
CME(config-ephone-dn)# call-forward ?
all forward all calls
busy forward call on busy
max-length max number of digits allowed for CFwdAll from IP
phone night-service forward call on activated night-service
noan forward call on no-answer
CME(config-ephone-dn)# call-forward busy 1003
CME(config-ephone-dn)# call-forward noan 1003 timeout 12
```

Để test tính năng call forward, từ IP Phone x1002 ta thực hiện cuộc gọi tới x1001, sau 3 lần IP Phone x1001 đổ chuông mà không có người bắt máy, cuộc gọi từ x1002 sẽ được chuyển tới IP Phone x1003.

Nếu có người gọi tới, trên Cisco IP Phones cứ mỗi 4 giây lại đổ chuông một lần, còn trên PSTN phone cứ mỗi 6 giây lại đổ chuông một lần. Nếu như chúng ta muốn chuyển cuộc gọi call forwarding sau 5 lần đổ chuông (ring) ta có thể chỉnh thời gian timeoute là 20 giây.

Thay vì call foward tới x1003, ta có thể thiết lập để chuyển cuộc gọi tới voicemail. Để thực hiện được tính năng forward khi người dùng ở trạng thái bận busy (call-forward busy), ta cần hiệu chỉnh ephone-dn sử dụng đặc tính dual-line để đưa cuộc gọi đến incoming call ở trạng thái call waiting. Cả 2 kênh channels ở chế độ dial-line đều được sử dụng khi sử dụng tùy chọn call-forward busy option.

Nếu ephone-dn 1 chuyển cuộc gọi forward tới ephone-dn 2. Nếu không có ai bắt máy tại ephone-dn2, ephone-dn 2 lại chuyển cuộc gọi cho ephone-dn 1, tại ephone-dn 1 cũng không có ai bắt máy, cuộc gọi đến incoming call chuyển chuyển lại cho ephone-dn 2, tiến trình này cứ lặp liên tục và vĩnh viễn trên hệ thống. Để giải quyết vấn đề này, ta có thể thực hiện câu lệnh "max-redirect command" ở chế độ telephony-service thiết lập số lần chuyển hướng redirect cuộc gọi trước khi cuộc gọi bị ngắt kết nối (disconnected).

```
telephony-service
max-redirect 5
```

Để kiểm tra giá trị "max-redirect", ta có thể thực hiện câu lệnh show telephony-service command.

```
CME# show telephony-service
CONFIG (Version=7.1)
====================
Version 7.1
Cisco Unified Communications Manager Express
<output omitted> max-redirect 5
<output omitted>
```

Bước 10: Thiết lập User cho IP Phone

Để User có thể đăng nhập vào hệ thống system thay đổi các thiết lập setting tương ứng cho IP Phone của người dùng đầu cuối, ta cần phải thực hiện các tác vụ sau:

```
CME(config)#ephone 3
CME(config-ephone)#username Q.Ky password 1003
CME(config-ephone)#pin ?
WORD  A sequence of digits - representing personal identifica-
tion number
```

```
CME(config-ephone)#pin 1003
CME(config-ephone)#exit
CME(config)#
```

Bước 11: Cấu hình Call Detail Records & Accounting

Tính năng Call Detail Records & Accounting có thể được sử dụng để tính phí dịch vụ, kiểm soát các cuộc gọi đường dài, cuộc gọi quốc tế và cũng có thể được sử dụng để khắc phục sự cố.

Có 2 loại logging systems là system event logging và call detail records (CDR). System event logging hỗ trợ khắc phục sự cố liên quan đến hạ tầng mạng network gear, trong khi call detail records được sử dụng để giám sát/thu thập thông tin của mỗi cuộc gọi call gọi ra ngoài khỏi hệ thống system. Các thông tin thống kê có thể được lưu trữ ở bộ nhớ cục bộ local buffer trên thiết bị device hoặc cũng có thể được gửi tới syslog server.

Trong quá trình khắc phục sự cố trên router, ta sẽ quan sát thông tin các logs để thu thập thông tin. Tất cả các thông điệp event messages hiển thị tại giao diện console có thể được gửi tới local logging facility cục bộ tại thiết bị device và tính năng này bị vô hiệu hóa theo mặc didjnh.

Để thuận tiện cho việc khắc phục sự cố được dễ dàng hơn, ta cần chỉnh thời gian của hệ thống sao cho đúng đắn, có thể chỉnh thủ công hoặc để thiết bị tự động điều chỉnh thời gian sử dụng giao thức NTP (Network Tim Protocol). Khi đó, các nhãn thời gian timestamps tương ứng với các sự kiện events sẽ hỗ trợ đắc lực cho tiến trình khắc phục sự cố hệ thống.

Nhãn thời gian timestamps đối với các sự kiện hệ thống system events có thể được thiết lập sử dụng local time zone using bằng câu lệnh "***service timestamps*** command" với từ khóa ***localtime*** keyword.

```
CME(config)# service timestamps log datetime msec localtime
```

Để kích hoạt tiến trình logging, điều chỉnh kích thước size của bộ đệm buffer được sử dụng để lưu trữ các messages (sẽ ảnh hưởng một phần đến bộ nhớ memory sử dụng) bằng câu lệnh "***logging buffered*** command".

```
CME(config)# logging buffered 512000
```

Để phát sinh các log message, ta có thể tiến hành restart lại IP Phone.

```
CME(config)# ephone 1
CME (config-ephone)# restart
restarting 001D.705E.ABF1
Feb 26 18:37:22.779: %IPPHONE-6-UNREGISTER_NORMAL:
ephone-1:SEP001D705EABF1
IP:10.115.0.11 Socket:5 DeviceType:Phone has unregistered
normally.
Feb 26 18:37:24.495: %IPPHONE-6-REG_ALARM: 23:
Name=SEP001D705EABF1 Load= SCCP42.8-4-
2S Last=Reset-Restart
Feb 26 18:37:24.535: %IPPHONE-6-REGISTER:
ephone-1:SEP001D705EABF1 IP:10.115.0.11
Socket:2 DeviceType:Phone has registered.
```

Sử dụng câu lệnh "***show logging*** command" để quan sát ephone unregister và registration messages tại bộ nhớ đệm buffer:

```
CME# show logging
Syslog logging: enabled (0 messages dropped, 4 messages
rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 92 messages logged, xml
disabled, filtering disabled
Monitor logging: level debugging, 0 messages logged, xml
disabled, filtering disabled
filtering disabled Logging Exception size (4096 bytes)
, xml disabled,
Count and timestamp logging messages: disabled Persistent
logging: disabled
No active filter modules.
ESM: 0 messages dropped
Trap logging: level informational, 96 message lines logged
Log Buffer (512000 bytes):
Feb 26 18:36:57.311: %SYS-5-CONFIG_I: Configured from
console by console Feb 26 18:37:22.779: %IPPHONE-6-UN-
REGISTER_NORMAL: ephone-1:SEP001D705EABF1
IP:10.115.0.11 Socket:5 DeviceType:Phone has unregistered
normally.
Feb 26 18:37:24.495: %IPPHONE-6-REG_ALARM: 23:
Name=SEP001D705EABF1 Load= SCCP42.8-4-
2S Last=Reset-Restart
Feb 26 18:37:24.535: %IPPHONE-6-REGISTER:
ephone-1:SEP001D705EABF1 IP:10.115.0.11
Socket:2 DeviceType:Phone has registered.
Feb 26 18:38:10.947: %SYS-5-CONFIG_I: Configured from
console by console
CME#
```

Việc thực hiện cuộc gọi call giữa các IP Phones sẽ không làm các logged messages phát sinh. Lúc này, ta sẽ phải sử dụng tới tính năng CDRs.

Việc xuất các logging messages tới external syslog server cho phép ta sử dụng các scripts để lọc lại các output hiển thị, chúng ta cũng không cần lo lắng về việc mất mát các record nếu như thiết bị khởi động lại hoặc bị mất nguồn đột ngột.

CDRs có thể được gửi tới syslog server (cũng có thể sử dụng RADIUS hoặc FTP) để thu thập thông tin tính phí detailed billing information và call tracing. Để thiết lập CDRs, ta thực hiện câu lệnh "dial-control-mib command", để thiết lập số lượng dòng entry tối đa (maximum number of entries) được sử dụng để lưu trữ các record, ta sử dụng câu lệnh max-size keyword và định nghĩa khoản thời gian lưu giữ các records này bằng câu lệnh retain-timer keyword. Để gửi CDRs tới syslog server, ta thực hiện câu lệnh gw-accounting syslog command, và thực hiện câu lệnh logging command để khai báo địa chỉ IP address của syslog server.

```
CME(config)# dial-control-mib max-size 500
CME(config)# dial-control-mib retain-timer 10080
CME(config)# gw-accounting syslog
CME(config)# logging IP_address_of syslog_server
```

Để kiểm tra, ta tiến hành thực hiện cuộc gọi từ IP Phone 1 tới IP Phone 2. Syslog server sẽ nhận được các CDR.

còn tiếp...

Routing & Switching

Chương trình CCNA R&S

Chương trình CCNP ROUTE

Chương trình CCNP SWITCH

Chương trình CCNP TSHOOT

Chương trình CCIE

Security

Chương trình CCNA Security

Chương trình SECURE

Chương trình FIREWALL

CCNA Voice

Lớp sáng, chiều:

+ Tặng giáo trình, áo thun

Lớp tối:

+ Học 1 tặng 1

+ Ưu đãi 30%

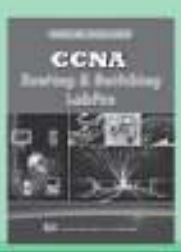
- ***Lớp sáng, chiều:***
  + Tặng *giáo trình, áo thun.*
- ***Lớp tối:***
  + *Học 1 tặng 1 (Tặng khóa Voice căn bản).*
  + *Ưu đãi 30% Học phí giành cho Sinh Viên (kế toán kiểm tra và chụp hình thẻ Sinh viên kẹp chung form khi đăng ký)*

Cam kết lợi ích khi học tại VnPro

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

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

GIẢM* NGAY 20%



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

*** Chương trình ưu đãi sách: Áp dụng chính sách mới là giảm 10% khi đặt sách online**

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

VNPRO TRI ÂN GIẢNG VIÊN PHÒNG DA-ĐT NHÂN NGÀY 20/11

Hơn 12 năm nay, VnPro luôn là lựa chọn hàng đầu của những kỹ sư mạng máy tính và các bạn sinh viên trong việc lựa chọn nơi làm bệ phóng cho ước mơ chinh phục đỉnh cao tri thức. Đội ngũ giảng viên chuyên nghiệp và kỹ năng sư phạm tuyệt vời luôn là niềm tự hào của VnPro.

Với đội ngũ bao gồm 5 giảng viên làm việc toàn thời gian, VnPro là trung tâm duy nhất có đội ngũ nhân sự đông đảo mạnh mẽ cả về chất và lượng. Các giảng viên không chỉ có kiến thức chuyên môn cực kỳ vững chắc kết hợp với kỹ năng sư phạm mà còn hiểu rõ tường tận các kinh nghiệm quản lý dự án thực tế.

Đội ngũ giảng viên chính thức của VnPro (từ trái qua: thầy Đức Phương, thầy Thanh Phong, thầy Hoàng Long, thầy Minh Tiến, thầy Quốc Kỳ)

Đội ngũ giảng viên của VnPro luôn khôngngừng học hỏi với tinh thần cầu thị vì họ biết rằng chỉ có không ngừng tiến lên mới có thể đáp ứng được yêu cầu học hỏi ngày một cao của công nghệ. Chính vì thế tất cả giảng viên của phòng Đào Tạo đều đã đạt được những chứng chỉ quốc tế và kinh nghiệm thực tiễn vô cùng phong phú.

Học phải đi đôi với hành, lý thuyết phải luôn song hành cùng thực tiễn để tạo nên một nền tảng vững chắc. Thấu hiểu được điều đó những giảng viên của VnPro đúc kết hơn 12 năm kinh nghiệm đào tạo cùng kinh nghiệm thực tiễn của mình tạo nên những loạt sách thực hành CCLab-Pro Tiếng Việt. Giáo trình LabPro và những thiết bị thật chính hãng Cisco tạo thành một điểm tựa vững chắc hỗ trợ cho học viên VnPro thực sự biết làm chứ không chỉ có lý thuyết suông.

Năm 2015 phòng Dự án đào tạo cũng tiến hành cải tổ và chuẩn hoá phương pháp dạy và học đồng thời cho ra mắt chương trình đào tạo Collaboration lần đầu tiên được giảng dạy tại Việt Nam. Với chương trình mới này, VnPro trở thành trung tâm duy nhất tại Tp.HCM nói riêng và Việt Nam nói chung, có đầy đủ cơ sở vật chất cùng kinh nghiệm để đáp ứng được những yêu cầu khắc khe của việc đào tạo khoá học này.

Nhân dịp 20/11 VnPro trân trọng gửi lời tri ân đến đội ngũ giảng viên của phòng Đào Tạo. Hy vọng trong tương lai các thầy sẽ nỗ lực và phấn đấu hơn nữa để trở thành điểm tựa vững chắc trong quá trình xây dựng VnPro trở thành "Trung Tâm Đào Tạo Chuyên Gia Quản Trị Mạng Hàng Đầu Việt Nam".

VNPRO RA MẮT DÀN THIẾT BỊ CAO CẤP PHỤC VỤ CHO NGHIÊN CỨU VÀ GIẢNG DẠY

Trong kế hoạch phát triển dài hạn 5 năm từ 2015-2020 của VnPro thì ưu tiên hàng đầu chính là việc nâng cấp trang thiết bị cho giảng viên và học viên của mình. Chính vì lẽ đó mà giữa tháng 10 vừa qua VnPro đã nâng cấp hệ thống LAB của mình theo tiêu chuẩn quốc tế bằng việc trang bị thêm các thiết bị cao cấp của Cisco.

Hình ảnh mới nhất từ các trang thiết bị tại VnPro:

Thầy Quốc Kỳ (chuyên gia Voice) hướng dẫn cách test Ip Phone

IP Phone Cisco chuyên dụng cho khoá học Voice tại VnPro

Hơn 12 năm qua VnPro không ngừng đổi mới để phát triển đồng thời tự nâng cấp mình lên một tầm cao mới. Thông qua việc nâng cấp các thiết bị nghiên cứu và giảng dạy VnPro ngày càng khẳng định vai trò đầu tàu của một trung tâm đào tạo chuyên gia quản trị mạng hàng đầu Việt Nam.

VNPRO BÙNG NỔ CÙNG SINH VIÊN ĐH TÔN ĐỨC THẮNG VỚI CHƯƠNG TRÌNH TƯ VẤN HƯỚNG NGHIỆP

Sáng ngày 04/11/2015 vừa qua, VnPro đã phối hợp cùng với Khoa Điện – Điện Tử trường Đại Học Tôn Đức Thắng tổ chức hội thảo "HƯỚNG NGHIỆP, NHU CẦU TUYỂN DỤNG THỰC TẾ VÀ ỨNG DỤNG CỦA CISCO TỪ LÝ THUYẾT ĐẾN THỰC TIỄN".

Hội thảo được tổ chức với mục đích tạo điều kiện cho các bạn sinh viên Ngành Điện Tử Viễn Thông có cái nhìn rõ ràng và cụ thể hơn về phương thức định hướng nghề nghiệp cho mình trong tương lai.

Các bạn sinh viên có mặt từ rất sớm để tham gia chương trình

Thầy Trần Thanh Phương – Phó Khoa Điện – Điện Tử đại diện phát biểu trong chương trình

Thầy Lê Đức Phương nhiệt tình chia sẻ kinh nghiệm trong việc lựa chọn nghề nghiệp với các bạn sinh viên

Thầy Đặng Ngọc Minh Đức – Trưởng bộ môn Điện Tử Viễn Thông với chương trình bốc thăm may mắn

Đại diện VnPro và Khoa Điện – Điện Tử trao học bổng cho các bạn sinh viên đạt thành tích xuất sắc

Chương trình đã thu hút hơn 100 sinh viên của Ngành Điện Tử Viễn Thông Đại Học Tôn Đức Thắng tham dự. Đến với hội thảo lần này không những các bạn được trang bị thêm kiến thức chuyên môn còn có thêm những kinh nghiệm để chuẩn bị sang một trang mới của cuộc đời khi chính thức ra trường và đi làm. Ngoài ra VnPro còn dành tặng 2 suất học bổng cho 2 bạn sinh viên của khoa đã có những thành tích xuất sắc trong quá trình học tập cùng rất nhiều phần quà dành cho các bạn tham gia hội thảo.

Không khí của buổi hội thảo sôi động ngay từ lúc bắt đầu cho đến tận phút cuối cùng. Với hàng loạt những câu hỏi dành cho diễn giả là thầy Lê Đức Phương về lựa chọn nghề nghiệp cũng như là việc lựa chọn các khoá học phù hợp với mình tại VnPro.

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

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

Challenge LAB - CDP

Giao thức CDP (Cisco Discovery Protocol) là một giao thức lớp 2 trong mô hình OSI thường được sử dụng để kiểm tra kết nối lớp 2 đã thông suốt hay chưa. Đây là một công cụ hỗ trợ đắc lực cho quá trình khắc phục sự cố hệ thống mạng.

CDP được bật mặc định trên các dòng Cisco Switch và Cisco Router, với thông tin thu thập được từ giao thức CDP, ta có thể vẽ nên toàn bộ sơ đồ hệ thống mạng hoàn chỉnh từ cổng đấu nối cho tới sơ đồ IP của hệ thống mạng.

Chẳng hạn như trong sơ đồ hệ thống trên, đứng tại router R1, ta không thể ping được tới router R2 nên lúc này ta có thể xác nhận là kết nối lớp 3 đang có vấn đề. Tiếp đến, ta có thể kiểm tra kết nối lớp 2 đã thông suốt hay chưa bằng cách quan sát thông tin trạng thái "line protocol" đã ở trạng thái "up" hay chưa thông qua nội dung hiển thị của câu lệnh sau:

```
R1# show int f0/0
FastEthernet0/0 is up, line protocol is up (connected)
Hardware is Lance, address is 0001.630d.3901 (bia 0001.630d.3901)
Internet address is 172.16.1.129/26
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

Bên cạnh câu lệnh "show int f0/0" ta cũng có thể kiểm tra thông tin lớp 2 đã thông suốt hay chưa bằng cách sử dụng giao thức CDP:

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID   Local Intrfce  Holdtme  Capability  Platform   Port ID
R2          Fas 0/0        168      R           C2800      Fas 0/1
R1#
```

Ta có thể thấy tại R1 có thể quan sát được các thông tin liên quan đến router R2 thông qua câu lệnh "show cdp neighbors" với các thông tin cụ thể như sau:

- R2: là thông tin hostname của router R2 như minh họa ở sơ đồ bên trên.
- R1 sử dụng cổng f0/0 để kết nối tới f0/1 của R2.
- R2 là dòng router 2800.

Bên cạnh các thông tin trên, tại router R1 ta cũng có thể xác định được IP mà router R2 đang sử dụng là 172.16.1.32 bằng cách thêm từ khóa "details" ở phía sau câu lệnh "show cdp neighbor".

```
R1#show cdp neighbors detail
Device ID: R2
Entry address(es):
IP address : 172.16.1.32
Platform: cisco C2800, Capabilities: Router
Interface: FastEthernet0/0, Port ID (outgoing port): FastEther-
net0/1
Holdtime: 146
Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSER-
VICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
advertisement version: 2
Duplex: full
R1#
```

Với thông tin địa chỉ của router R2 mà ta vừa xác định được là 172.16.1.32, ta có thể xác nhận nguyên nhân mà R1 không thể ping được tới router R2 là do IP giữa router R1 và R2 không cùng lớp mạng với nhau. Đó là chức năng khắc phục sự cố mà CDP đem lại, bên cạnh đó, ta có thể vẽ được sơ đồ hệ thống thông qua nội dung hiển thị của câu lệnh "show cdp neighbors details".

Quan sát thông tin hiển thị sau đây:

```
Switch#show cdp neighbors detail
Device ID: Router
Entry address(es):
 IP address : 172.16.1.199
Platform: cisco C2800, Capabilities: Router
Interface: FastEthernet0/3, Port ID (outgoing port): FastEther-
net0/0
Holdtime: 149

Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSER-
VICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
advertisement version: 2
Duplex: full
-------------------------

Device ID: R1
Entry address(es):
 IP address : 172.16.1.129
Platform: cisco C2800, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEther-
net0/0
Holdtime: 169

Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSER-
VICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
```

Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team
advertisement version: 2
Duplex: full

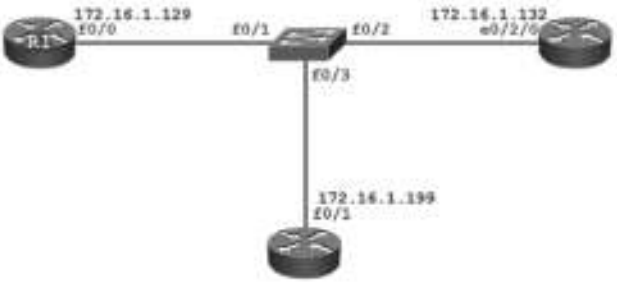
Device ID: Router
Entry address(es):
IP address : 172.16.1.132
Platform: cisco C2800, Capabilities: Router
Interface: FastEthernet0/2, Port ID (outgoing port):
Ethernet0/2/0
Holdtime: 175

Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSER-VICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

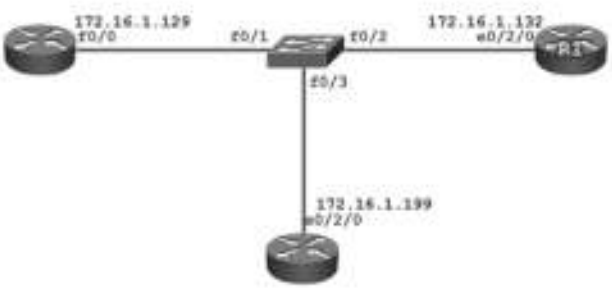
advertisement version: 2
Duplex: full
Switch#

Câu hỏi tình huống?
Question: Với thông tin hiển thị phía trên, ta vẽ được sơ đồ nào sau đây:

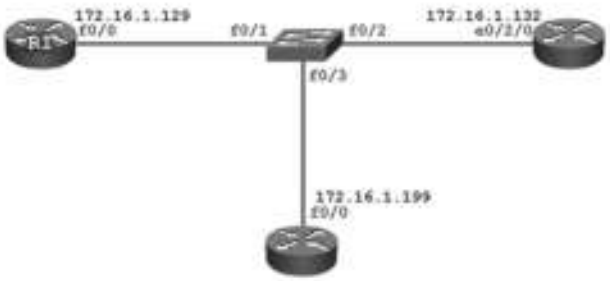
Answer 1:



Answer 2:



Answer 3:



Answer 4: Không phải sơ đồ nào trong số các sơ đồ trên

Sơ lược về mạng không dây

1. Mạng không dây

Mạng không dây (hay còn gọi là mạng Wi-Fi, mạng Wireless, 802.11) là mạng kết nối các thiết bị có khả năng thu phát sóng (như máy vi tính có gắn Adapter không dây, PDA,…) lại với nhau không sử dụng dây dẫn mà sử dụng song vô tuyến được truyền dẫn trong không gian thông qua các trạm thu/phát sóng.

2. Các ứng dụng của Mạng Wireless

Nên thiết lập Wireless ở những nơi có tính chất tạm thời để làm việc hoặc ở những nơi mạng Cable truyền không thể thi công hoặc làm mất thẩm mỹ quan: Như các toà nhà cao tầng, khách sạn, bệnh viện, nhà hang nơi mà khách hang thường sử dụng mạng không dây với cường độ cao và đòi hỏi tính cơ động cao.

Mạng Wireless là kỹ thuật thay thế cho mạng LAN hữu tuyến, nó cung cấp mạng cuối cùng với khoảng cách kết nối tối thiểu giữa một mạng xương sống và mạng trong nhà hoặc người dung di động trong các cơ quan.

3. Nguyên lý hoạt động

Mạng WLAN sử dụng sóng điện từ (vô tuyến và tia hồng ngoại) để truyền thông tin từ điểm này sang điểm khác mà không dựa vào bất kỳ kết nối vật lý nào. Các sóng vô tuyến thường là các sóng mang vô tuyến bởi vì chúng thực hiện chức năng phân phát năng lượng đơn giản tới máy thu ở xa. Dữ liệu truyền được chồng lên trên sóng mang vô tuyến để nó được nhận lại đúng ở máy thu. Đó là sự điều biến sóng mang theo thông tin được truyền. Một khi dữ liệu được chồng (được điều chế) lên trên sóng mang vô tuyến, thì tín hiệu vô tuyến chiếm nhiều hơn một tần số đơn, vì tần số hoặc tốc độ truyền theo bit của thông tin biến điệu được thêm vào sóng mang.

Nhiều sóng mang vô tuyến tồn tại trong cùng không gian tại cùng một thời điểm mà không nhiễu với nhau nếu chúng được truyền trên các tần số vô tuyến khác nhau. Để nhận dữ liệu, máy thu vô tuyến bắt sóng (hoặc chọn) một tần số vô tuyến xác định trong khi loại bỏ tất cả các tín hiệu vô tuyến khác trên các tần số khác.

Trong một cấu hình mạng WLAN tiêu biểu, một thiết bị thu phát, được gọi một điểm truy cập (AP – access point), nối tới mạng nối dây từ một vị trí cố định sử dugj cáp Ethernet chuẩn. Điểm truy cập (access point) nhận, lưu vào bộ nhớ đệm, và truyền dữ liệu giữa mạng WLAN và cơ sở hạn tầng mạng nối dây. Một điểm truy cập đơn hỗ trợ một nhóm nhỏ người sử dụng và vận hành bên trong một phạm vi vài mét tới hàng chục mét. Điểm truy cập(hoặc anten được gắn tới nó) thông thường được gắn trên cao nhưng thực tế được gắn bất cứ nơi đâu miễn là khoảng vô tuyến cần thu được.

Các người dùng đầu cuối truy cập mạng WLAN thông qua các card giao tiếp mạng WLAN mà được thực hiện như các card PC trong các máy tính để bàn, hoặc các thiết bị tích hợp hoàn toàn bên trong các máy tính cầm tay. Các card giao tiếp mạng WLAN cung cấp một giao diện giữa hệ điều hành mạng (NOS) và sóng trời (qua một anten). Bản chất của kết nối không dây là trong suốt với NOS.

4. Ưu và nhược điểm của mạng không dây

4.1. Ưu điểm (lợi ích của mạng Wireless)

– Độ tin tưởng cao trong nối mạng của các doanh nghiệp và sự tăng trưởng mạnh mẽ của mạng Internet và các dịch vụ trực tuyến là bằng chứng mạnh mẽ đối với lợi ích của dữ liệu và tài nguyên dùng chung. Với mạng Wireless, người dùng truy cập thông tin dùng chung mà không tìm kiếm chỗ để cắm vào, và các nhà quản lý mạng thiết lập hoặc bổ sung mạng mà không lắp đặt hoặc di chuyển dây nối. Mạng Wireless cung cấp hiệu suất sau: khả năng phục vụ, tiện nghi, và các lợi thế về chi phí hơn hẳn các mạng nối dây truyền thống.

– Khả năng lưu động cải thiện hiệu suất và dịch vụ: Các hệ thống mạng Wireless cung cấp sự truy cập thông tin thời gian thực tại bất cứ đâu cho người dùng mạng trong tổ chức của họ. Khả năng lưu động này hỗ trợ các cơ hội về hiệu suất và dịch vụ mà mạng nối dây không thể thực hiện được.

– Đơn giản và tốc độ nhanh trong cài đặt: Cài đặt hệ thống mạng Wireless nhanh và dễ dàng và loại trừ nhu cầu kéo dây qua các tường và các trần nhà.

– Linh hoạt trong cài đặt: Công nghệ không dây cho phép mạng đi đến các nơi mà mạng nối dây không thể.

– Giảm bớt giá thành sở hữu: Trong khi đầu tư ban đầu của phần cứng cần cho mạng Wireless có giá thành cao hơn các chi phí phần cứng mạng LAN hữu tuyến, nhưng chi phí cài đặt toàn bộ và giá thành tính theo tuổi thọ thấp hơn đáng kể.

– Tính linh hoạt: Các hệ thống mạng Wireless được định hình theo kiểu topo khác nhau để đáp ứng các nhu cầu của các ứng dụng và cài đặt cụ thể. Cấu hình mạng

dễ thay đổi từ các mạng độc lập phù hợp với số nhỏ người dùng đến các mạng cơ sở hạ tầng với hàng nghìn người sử dụng trong một vùng rộng lớn.

4.2. Nhược điểm

– ***Bảo mật:*** Môi trường kết nối không dây là không khí nên khả năng bị tấn công của người dùng là rất cao.

– ***Phạm vi:*** Một mạng chuẩn 802.11g với các thiết bị chuẩn thì có thể hoạt động tốt trong phạm vi vài chục mét. Nó phù hợp trong một căn nhà, nhưng với một toà nhà lớn thì không đáp ứng được nhu cầu. Để đáp ứng được nhu cầu. Để đáp ứng cần phải mua thêm Repeater hay access point, dẫn đến chi phí gia tăng.

– ***Độ tin cậy:*** Vì sử dụng sóng vô tuyến để truyền thông nên việc bị nhiễu, tín hiệu bị giảm do tác động của các thiết bị khác (lò vi sóng,…) là không tránh khỏi. Làm giảm đáng kể hiệu quả hoạt động của mạng.

– ***Tốc độ:*** Tốc độ của mạng không dây (1 – 125 Mbps) rất chậm so với mạng sử dụng cáp (100 Mbps đến hàng Gbps).

Cấu hình Port Security như thế nào?

Cấu hình mặc định của Port Security:

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC address	1
Violation mode	Shutdown. Port tắt khi maximum number của địa chỉ secure MAC vượt quá, và một thông báo SNMP trap sẽ được gửi.
Aging	Disabled
Aging type	Absolute
Static Aging	Disabled

Cấu hình mặc định trong port security

Một số nguyên tắc khi cấu hình Port Security:

- Một secure port không thể cấu hình trên port trunk.
- Một secure port không phải là một port đích cho SPAN.
- Một secure port không thể thuộc về một interface port-channel. Các câu lệnh cấu hình Port Security:

Câu lệnh	Mục đích
Switch(config)# ***interface*** *interface_id*	Nhập vào chế độ cấu hình và nhập interface vật lý để cấu hình, ví dụ Gigabitethernet 3/1
Switch(config-if)# ***switchport mode access***	Thiết lập chế độ interface như access; một interface ở chế độ mặc định (dynamic desirable) không thể được cấu hình như một secure port.
Switch(config-if)# ***switchport port-security***	Kích hoạt port security trên interface
Switch(config-if)# ***switchport port-security maximum*** *value*	(Optional) Thiết lập số lượng tối đa của địa chỉ MAC secure cho interface. Phạm vi đó là 1-3072; mặc định là 1.
Switch(config-if)# ***switchport port-security violation {restrict| shutdown}***	(Optional) Thiết lập chế độ vi phạm, các hành động được thực hiện khi một sự vi phạm an ninh được phát hiện như: • Restrict – một vi phạm secure port hạn chế dữ liệu và làm tăng bộ đếm SecurityViolation và gửi một thông báo SNMP trap. • Shutdown – Interface là lỗi vô hiệu hóa khi một hành vi vi phạm an ninh xảy ra. Lưu ý: Khi một port an toàn ở trạng thái lỗi , có thể mang nó ra khỏi tình trạng này bằng cách nhập câu lệnh **errdisable recovery cause**
	psecure-violation hoặc có thể tự bật lại nó bằng cách nhập câu lệnh **shutdown** và **no shutdown.**
Switch(config-if)# ***switchport port-security mac-address sticky***	(Optional) Kích hoạt sticky learning trên interface.
Switch(config-if)# ***switchport port-security mac-address*** *mac-address*	(Optional) Vào một địa chỉ MAC an toàn cho interface. Có thể sử dụng lệnh này cho nhập số lượng tối đa về địa chỉ MAC secury. Nếu cấu hình ít địa chỉ secure MAC quá mức tối đa, các địa chỉ MAC còn lại là dynamically learned.
Switch(config-if)# ***switchport port-security mac-address sticky***	(Optional) Kích hoạt sticky learning trên interface
Switch(config-if)# ***end***	Quay lại mode privileged EXEC
Switch(config-if)# ***show port-security address interface*** *interface_id* *Switch(config-if)#* ***show port-security address***	Kiểm tra các entries

Cấu hình Port Security

- Để quay lại interface ở điều kiện mặc định là port không an toàn (tắt port security), sử dụng lệnh cấu hình interface :
  no switchport port-security
- Để xóa một địa chỉ MAC từ bảng địa chỉ, sử dụng câu lệnh:
  no switchport port-security mac-address mac_address
- Để trở về mode violation với tình trạng mặc định (shutdown mode), sử dụng câu lệnh:
  no switchport port-secure violation {restrict | shutdown}
- Để tắt sticky learning trên một interface, sử dụng câu lệnh :
  switchport port-secure mac-address sticky. Interface chuyển đổi địa chỉ sticky MAC secure cho các địa chỉ dynamic secure.
- Để xóa một địa chỉ sticky secure MAC từ bảng địa chỉ, sử dụng câu lệnh :
  switchport port-security sticky mac-address mac_address.
- Để xóa tất cả địa chỉ sticky trên một interface hoặc VLAN, sử dụng câu lệnh:
  no switchport port-security sticky interface interface-id
- Để xóa dynamic learned port security MAC trong bảng CAM, sử dụng câu lệnh :
  clear port-security dynamic. Các từ khóa địa chỉ cho phép xóa một địa chỉ secure MAC. Các từ khóa interface cho phép xóa tất cả các địa chỉ bảo mật trên một interface.

Tiếng Anh thật là "kỳ quặc"

A ship-shipping ship ships shipping-ships

Bức ảnh bên dưới chính là để minh họa cho câu "A ship-shipping ship ships shipping-ships" đấy! Một cách viết lại cho dễ hiểu là "A boat-shipping boat transports shipping-boats", và nghĩa của nó là 'Một con tàu chuyên chở tàu đang chở những con tàu chuyên chở tàu khác'. Trong tiếng Anh còn rất nhiều trường hợp tương tự: câu hoàn toàn đúng ngữ pháp và có nghĩa nhưng đọc lên lại nghe "lùng bùng như thần chú", nguyên nhân là do hiện tượng đồng âm và đa nghĩa của từ. Chúng ta cùng khám phá thêm vài câu cực "kỳ quái" dưới đây nhé!

Buffalo buffalo Buffalo buffalo buffalo buffalo Buffalo buffalo

Bạn đã cảm thấy hoa mắt chưa? Có đến 8 từ "buffalo" đấy! Trong số này, từ "Buffalo" viết hoa là tên một thành phố ở Mỹ. Trong các từ còn lại, ngoài là danh từ quen thuộc chỉ "con trâu", "buffalo" còn đóng vai trò động từ với nghĩa "lấn át, bắt nạt", tương tự như "bully". Câu này có thể viết lại thành "The buffalo from Buffalo who are buffaloed by buffalo from Buffalo, buffalo other buffalo from Buffalo", nghĩa là "Con trâu ở thành phố Buffalo mà bị con trâu khác ở thành phố Buffalo bắt nạt, thì nó cũng đi bắt nạt con trâu khác ở thành phố Buffalo"!

Rose rose to put rose roes on her rows of roses

Câu này khi đọc lên sẽ chứa rất nhiều vần /ou/, do hiện tượng đồng âm. Nghĩa của các từ trong câu bao gồm:

- Rose: tên một người phụ nữ
- Rose: quá khứ của rise (đứng dậy, vươn lên)
- Rose: màu hồng
- Roes: trứng cá (trong trường hợp này là một loại phân bón)
- Rows: luống, hàng
- Roses: hoa hồng

Nghĩa của câu là: "Cô Rose rướn người lên để bón loại phân trứng cá màu hồng vào mấy luống hoa hồng của cô ấy."

Will, will Will will Will Will's will?

Tương tự câu trên, từ "will" trong câu này cũng có rất nhiều chức năng khác nhau, vừa là tên người (ở đây lại có đến 3 bạn trùng tên Will!), vừa là trợ động từ, vừa là động từ chính ("để lại tài sản theo di chúc") vừa là danh từ ("di chúc"). Câu này có thể tạm dịch như sau: "Will à, cậu có nghĩ anh Will kia sẽ để lại di chúc chia tài sản cho anh Will nọ không?"

Những từ Tiếng Anh kỳ lạ nhất trong từ điển

1. Bookkeeper (nhân viên kế toán) là từ duy nhất có ba chữ nhân đôi liền nhau.
2. Hai từ dài nhất thế giới chỉ có duy nhất 1 trong 6 nguyên âm bao gồm cả chữ y là: "defenselessness" (sự phòng thủ) và "respectlessness" (sự thiếu tôn trọng).
3. "Forty" (40) là số duy nhất có các chữ cái theo thứ tự alphabet. Còn "One" (1) là số duy nhất có các chữ cái theo thứ tự ngược lại.
4. Từ dài nhất "honorificabilitudinitatibus" (đất nước có khả năng đạt được nhiều niềm vinh dự) có các nguyên âm và phụ âm xen kẽ nhau.
5. "Antidisestablishmentarianism" (trước đây nó có nghĩa là việc chống lại sự bãi bỏ thiết lập nhà thờ ở Anh, và bây giờ là sự chống lại niềm tin rằng không có sự hiện diện của một nhà thờ chính thống nào trong nước) được liệt kê trong từ điển Oxford đã từng được coi là từ dài nhất nhưng giờ đây ngôi vị ấy đã thuộc về thuật ngữ y học "pneumonoultramicroscopicsilicovolcanoconiosis " (một bệnh phổi do hít phải bụi thạch anh trong các vụ núi lửa phun trào), nhưng có một từ khác là tên của một chất hóa học gồm 267 loại amino axit và enzyme xứng đáng là từ dài nhất, tuy nhiên đấy chỉ là từ ghép từ nhiều từ khác nhau, không được xem là một từ vựng!
6. "The sixth sick sheik's sixth sheep's sick" là cụm từ khiến ta phải líu lưỡi nhiều nhất khi phát âm. Ngoài ra mình còn biết thêm một câu là: "She sells seashells on the seashore"
7. Trong tiếng Anh chỉ có một từ duy nhất có 5 nguyên âm đứng liền nhau là "queueing" (xếp hàng).
8. "Asthma" (hen suyễn) và "isthmi" (kênh đào) là hai từ duy nhất có chữ đầu và chữ cuối đều cùng một nguyên âm còn ở giữa toàn phụ âm.
9. "Rhythms" (nhịp điệu) là từ dài nhất không có nguyên âm bình thường a, e, i, o hay u.


VnPro
7 cardinal rules in LIFE
1 Make PEACE with your PAST so it doesn't spoil your present. Your past does not define your future - your actions and beliefs do.
2 What others THINK of you is none of your business. It's how much you value yourself and how important you think you are.
3 Time HEALS almost everything, give time, time. Pain will be less hurting. Scars make us who we are; they explain our life and why we are the way we are. They challenge us and force us to be stronger.
4 No one is the reason for your own HAPPINESS, except you yourself. Waste no time and effort searching for peace and contentment and joy in the world outside.
5 Don't COMPARE your life with others', you have no idea what their journey is all about. If we all threw our problems in a pile and saw everyone else's, we would grab ours back as fast as we could.
6 Stop THINKING too much, it's alright not to know all the answers. Sometime there is no answer, not going to be any answer, never has been an answer. That's the answer! Just accept it, move on, NEXT!
7 SMILE, you don't own all the problems in the world. A smile can brighten the darkest day and make life more beautiful. It is a potential curve to turn a life around and set everything straight.

VnPro

Sinh viên

ƯU ĐÃI ĐẾN **30%** Học phí

ĐĂNG KÝ TẶNG NGAY KHOÁ HỌC

TẶNG NGAY
VÉ MỜI HỘI THẢO CÙNG CHUYÊN GIA
TỪ SINGAPORE CCIE #21256
TRỊ GIÁ 500.000Đ

LỊCH KHAI GIẢNG THÁNG 11

Mã lớp	Tên Khoá Học	Ngày Khai Giảng	Ngày Học	Giờ Học	Học Phí/Khoá	Thời Gian
CHƯƠNG TRÌNH CCNA						
AK29	CCNAX (200-120)	03/11	3 – 5 - 7	2:00 – 5:00PM	3.360.000	152 giờ
A29				6:30 – 9:30PM	6.720.000	
AK28		16/11	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
A30				6:30 – 9:30PM	6.720.000	
AK31		24/11	3 – 5 - 7	8:30 – 11:30AM	3.360.000	
AK33				2:00 – 5:00PM	3.360.000	
A31				6:30 – 9:30PM	6.720.000	
AK32		25/11	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
AK34				2:00 – 5:00PM	3.360.000	
A32				6:30 – 9:30PM	6.720.000	
AS5	CCNA Security (640-554)	24/11	3 – 5 – 7	6:30 – 9:30PM	6.720.000	100 giờ
AV5	CCNA Voice (640-461)	03/11	3 – 5 – 7	2:00 – 5:00PM	6.720.000	100 giờ
AV7				6:30 – 9:30PM	6.720.000	
CHƯƠNG TRÌNH CCNP						
P1K7	ROUTE (300 - 101)	12/11	3 – 5 – 7	8:30 – 11:30AM	6.600.000	140 giờ
P1-7				2:00 – 5:00PM	6.600.000	
P1-7				6:30 – 9:30PM	9.800.000	
P2-K5	SWITCH (300 - 115)	24/11	3 – 5 – 7	8:30 – 11:30AM	5.880.000	120 giờ
P2-7				2:00 – 5:00PM	5.880.000	
P2-7				6:30 – 9:30PM	8.232.000	
P3-6	TSHOOT (300 - 135)	16/11	2 – 4 – 6	6:30 – 9:30PM	8.232.000	120 giờ
CHƯƠNG TRÌNH CCIE WRITTEN						
EW4	CCIE WRITTEN (Version 5)	26/11	3 – 5 – 7	6:30 – 9:30PM	11.760.000	120 giờ

ĐĂNG KÝ HỌC

Thanh Trâm — Email: thanhtram@vnpro.org — Mobile: 0949 246 829
Mỹ Trang — Email: mytrang@vnpro.org — Mobile: 0964 464 377
Lê Uyên — Email: tranleuyen@vnpro.org — Mobile: 0903 834 636

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

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

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

VnPro®