Số 62
11/2017

# BẢN TIN dancisco

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



## VNPRO TRAO HỌC BỔNG KHUYẾN HỌC CHO HỌC VIÊN XUẤT SẮC TRONG THÁNG 10/2017


*Thầy Đức Phương* trao học bổng cho anh *Nguyễn Phước Huy Hoàng lớp 17A100*

[Trang 07]

## Lỗ hổng Wi-Fi lớn nhất từ trước đến nay nguy hiểm ra sao?

*Lỗ hổng trong giao thức WPA2 khiến hacker có thể chen ngang kết nối giữa thiết bị và điểm truy cập Wi-Fi, ảnh hưởng đến mạng Wi-Fi toàn cầu.*

Một báo cáo mới đây chỉ ra lỗ hổng của mạng Wi-Fi, có thể gây nguy hại cho toàn bộ các thiết bị kết nối, từ máy tính, điện thoại cho đến những thiết bị IoT.

Phương thức khai thác lỗ hổng, tên gọi KRACK, có thể chen ngang kết nối giữa thiết bị và giao thức bảo mật của điểm truy cập Wi-Fi.

Dưới đây là những thông tin quan trọng bạn cần biết:

**Điều gì xảy ra?**

Một nhà nghiên cứu người Bỉ tên là Mathy Vanhoef phát hiện ra vấn đề trong các đoạn code của WPA2, giao thức giúp kết nối mạng Wi-Fi và các thiết bị thông dụng.

Lỗ hổng này có thể giúp hacker xâm nhập mọi đường truyền kết nối Internet vào và ra khỏi laptop, điện thoại, thiết bị thông minh và bất cứ thứ gì có kết nối Wi-Fi.

[Trang 03]

## TIN TỨC SỰ KIỆN KHÁC

# Cảnh báo biến thể mới của mã độc Mirai nhắm đến thiết bị IoT tại Việt Nam

***Những thiết bị IoT như Router Wifi, Camera IP… trong các gia đình Việt Nam đang nằm trong "tầm ngắm" của mã độc Mirai, 15 triệu máy tính bị nhiễm virus trong 3 tháng gần đây là những điểm nhấn về an ninh mạng trong quý III năm 2017.***

```
.data:00000000005147E0                    public passwords
.data:00000000005147E0 passwords          dq offset a1234567890    ; DATA XREF: Star
.data:00000000005147E0                                             ; StartTheLelz+AB
.data:00000000005147E0                                             ; "1234567890"
.data:00000000005147E8                    dq offset aTelnet        ; "telnet"
.data:00000000005147F0                    dq offset aVnpt          ; "vnpt"
.data:00000000005147F8                    dq offset aAntslq        ; "antslq"
.data:0000000000514800                    dq offset aSupport       ; "support"
.data:0000000000514808                    dq offset unk_410A64
.data:0000000000514810                    dq offset aRoot          ; "root"
.data:0000000000514818                    dq offset aZyad1234      ; "zyad1234"
.data:0000000000514820                    dq offset unk_410A64
```

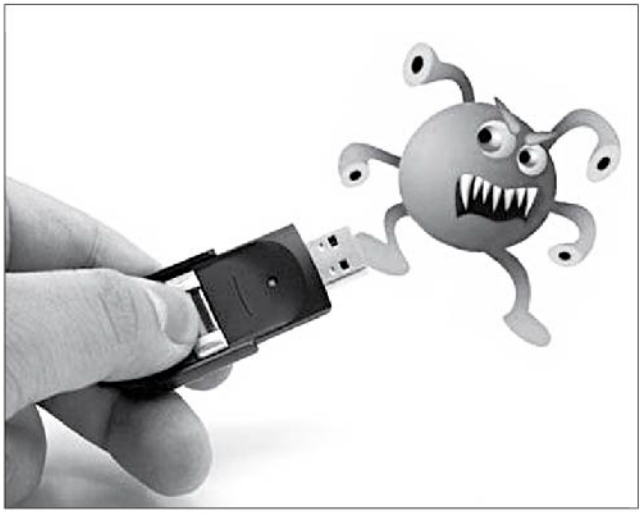
***Biến thể của mã độc Mirai đến Việt Nam***

Phân tích một biến thể mới của Mirai các chuyên gia Bkav phát hiện hacker đang nhắm mục tiêu đến Việt Nam. Mirai là dòng mã độc đã tấn công hàng loạt thiết bị IoT trên thế giới, thông qua việc dò mật khẩu mặc định từ nhà sản xuất để lây nhiễm. Trong biến thể mới Bkav phân tích, danh sách mật khẩu được mã độc sử dụng để tấn công xuất hiện thông tin tài khoản mặc định của nhà mạng tại Việt Nam.

Sự bùng nổ của IoT khiến vấn đề an ninh trên các thiết bị như Router Wifi, Camera IP… trở thành chủ đề nóng trong thời gian gần đây. Kết quả nghiên cứu của Bkav năm 2016 cũng cho thấy có hơn 5,6 triệu router trên khắp thế giới có lỗ hổng, riêng tại Việt Nam con số này là 300 nghìn, tương đương với 300 nghìn hệ thống mạng đang trong tình trạng bỏ ngỏ. Sau khi tấn công, kiểm soát thiết bị IoT, hacker có thể huy động các thiết bị này trở thành botnet trong các cuộc tấn công từ chối dịch vụ DDoS hoặc kiểm soát toàn bộ truy cập của người dùng trong mạng, thực hiện các hình thức tấn công MitM, Phishing để ăn cắp tài khoản ngân hàng, mạng xã hội, email...

Ông Ngô Tuấn Anh, Phó Chủ tịch phụ trách An ninh mạng của Bkav, khuyến cáo:"Để phòng tránh nguy cơ bị truy cập trái phép, người sử dụng cần phải kiểm tra, thay đổi mật khẩu quản trị các thiết bị IoT đồng thời tắt tính năng cho phép truy cập thiết bị từ mạng Internet bên ngoài khi không sử dụng. Về phía nhà cung cấp dịch vụ, thiết bị cũng cần thông báo việc phải thay đổi mật khẩu mặc định cho khách hàng sau khi lắp đặt và đưa thiết bị vào sử dụng".

Ngoài ra, theo thống kê từ hệ thống giám sát virus của Bkav, số lượng máy tính bị nhiễm virus tại Việt Nam trong quý III/2017 vẫn ở mức rất cao, lên tới 15 triệu lượt máy. Trong đó, con đường lây nhiễm virus chính vẫn là qua USB, chiếm tới hơn 50%.



Lý giải cho việc USB vẫn đang là nguồn lây nhiễm virus nhiều nhất, các chuyên gia Bkav phân tích, mặc dù USB là phương tiện phổ biến để sao lưu, trao đổi dữ liệu giữa các máy tính, nhưng ý thức về sử dụng USB an toàn vẫn chưa được cải thiện nhiều. Cũng theo thống kê của Bkav trong năm 2016, có tới 83% USB từng bị nhiễm virus trong năm.

Để hạn chế việc lây nhiễm của virus lây lan qua USB cũng như tự bảo vệ dữ liệu của bản thân, người dùng cá nhân cần trang bị phần mềm diệt virus thường trực để quét USB trước khi sử dụng, hạn chế sử dụng USB trên các máy lạ. Với các cơ quan doanh nghiệp, cần trang bị giải pháp kiểm soát chính sách an ninh đồng bộ, trong đó có kiểm soát, phân quyền sử dụng USB theo nhu cầu và độ quan trọng của từng máy.

*Theo VnReview*

# Lỗ hổng Wi-Fi lớn nhất từ trước đến nay nguy hiểm ra sao?

***Lỗ hổng trong giao thức WPA2 khiến hacker có thể chen ngang kết nối giữa thiết bị và điểm truy cập Wi-Fi, ảnh hưởng đến mạng Wi-Fi toàn cầu.***

Một báo cáo mới đây chỉ ra lỗ hổng của mạng Wi-Fi, có thể gây nguy hại cho toàn bộ các thiết bị kết nối, từ máy tính, điện thoại cho đến những thiết bị IoT.

Phương thức khai thác lỗ hổng, tên gọi KRACK, có thể chen ngang kết nối giữa thiết bị và giao thức bảo mật của điểm truy cập Wi-Fi.

Dưới đây là những thông tin quan trọng bạn cần biết:

**Điều gì xảy ra?**

Một nhà nghiên cứu người Bỉ tên là Mathy Vanhoef phát hiện ra vấn đề trong các đoạn code của WPA2, giao thức giúp kết nối mạng Wi-Fi và các thiết bị thông dụng.

Lỗ hổng này có thể giúp hacker xâm nhập mọi đường truyền kết nối Internet vào và ra khỏi laptop, điện thoại, thiết bị thông minh và bất cứ thứ gì có kết nối Wi-Fi.

**KRACK có nghĩa là gì?**

*Nó là viết tắt của "Key Reinstallation Attack", liên quan đến thủ thuật giúp mở ra đường truyền Internet cho hacker, buộc thiết bị phải liên tục gửi thông tin nhạy cảm để định danh bản thân trước khi thiết lập kết nối Internet.*

**Nó tồi tệ đến đâu?**

Tin vui cho người dùng hacker cần phải ở gần thiết bị để thực hiện tấn công bằng phương pháp này. Điều này làm giảm nguy cơ về việc một người có thể tấn công nhiều thiết bị cùng lúc tại nhiều địa điểm. Tuy nhiên, điểm tệ hại là mọi thiết bị sử dụng Wi-Fi đều có nguy cơ bị tấn công.

**Cách tốt nhất để bảo vệ mình là gì?**

Điều quan trọng nhất là bạn cần nâng cấp phần mềm thiết bị khi có bản vá.

**Đổi mật khẩu Wi-Fi có tác dùng gì không?**

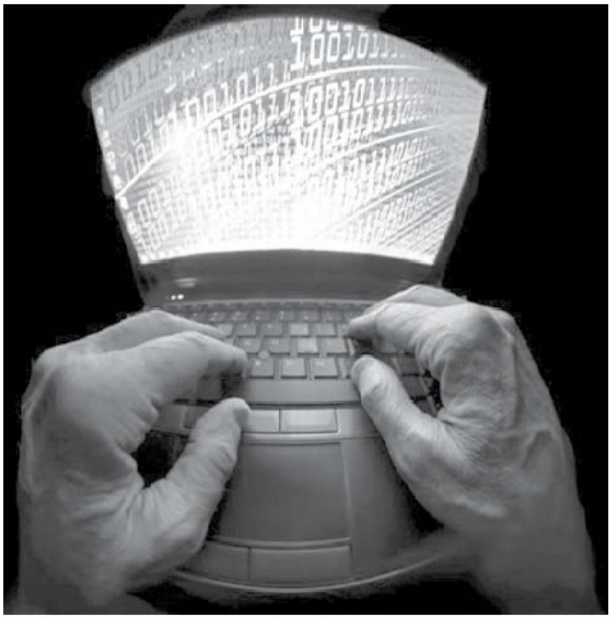
Đổi mật khẩu chỉ là một trong những phương pháp tăng cường bảo mật nhưng đây được xem là bước kém quan trọng nhất chống lại KRACK. Ngay cả khi đổi mật khẩu, hacker vẫn có thể sử dụng KRACK để xâm nhập.

**Khi nào có bản vá?**

Người dùng Windows đã được bảo vệ nếu họ cài đặt phiên bản cập nhật hôm thứ 3 tuần trước (10/10). Apple nói đang tạo bản vá cho iOS, MacOS, WatchOS và TVOS, có thể phát hành trong vài tuần tới.

Google thì khẳng định họ đã phát hiện ra vấn đề và ra mắt bất cứ bản vá cần thiết nào trong vài tuần. Các nhà sản xuất router như Linksys hay Netgear đều đã nhận thức được vấn đề và bắt đầu làm việc.

**Có nên mua router mới?**



*Chưa cần thiết. Nếu bạn sử dụng router cũ và không nghĩ nhà sản xuất sẽ cung cấp bản vá cho nó, bạn có thể lên kế hoạch mua router mới.*

Liên minh Wi-Fi cho biết họ sẽ yêu cầu nhà sản xuất phải công bố việc router mới không bị ảnh hưởng bởi KRACK nhưng những chiếc router đang bán ra hiện tại chưa được kiểm định. Điều quan trọng nhất vẫn là cập nhật phần mềm cho điện thoại, máy tính và các thiết bị kết nối Internet khác.

**Những thiết bị chưa nâng cấp của người khác có ảnh hưởng đến tôi?**

Ngay cả khi đã cài bản vá cho điện thoại và router của mình, bạn vẫn có thể bị ảnh hưởng nếu kết nối điện thoại với một chiếc router chưa được nâng cấp phần mềm khác.

Vanhoef cho hay router khó bị tấn công hơn so với điện thoại hay thiết bị khác. Cách an toàn nhất vẫn là hạn chế sử dụng Wi-Fi từ lúc này.

**Mạng Wi-Fi công cộng thì sao?**

Wi-Fi công cộng chưa bao giờ an toàn. Thông thường, dữ liệu truy cập trên mạng Wi-Fi ở các quán cafe không bao giờ được mã hóa, đồng nghĩa hacker có thể sử dụng một thiết bị rẻ tiền để "câu" dữ liệu truy cập của bạn. Điều mà KRACK thực hiện chính là biến mọi mạng Wi-Fi trở nên kém an toàn như Wi-Fi công cộng.

**Tắt Wi-Fi, dùng mạng 3G/4G có an toàn?**

Mạng di động (3G/4G) không bị ảnh hưởng bởi KRACK. Do đó, việc tắt Wi-Fi sẽ bảo vệ bạn.

**HTTPS có gặp nguy hiểm?**

Nhiều website – bắt đầu với HTTPS – cung cấp thêm một lớp mã hóa cho kết nối Internet của bạn. KRACK không phá bỏ được lớp mã hóa này.

Tuy nhiên, Vanhoef nói chỉ HTTPS không đủ an toàn để bảo vệ dữ liệu của bạn nếu hacker sử dụng KRACK để đọc dữ liệu luân chuyển. Sau nhiều lần thực hiện, hacker có thể tìm ra cách phá vỡ lớp mã hóa này.

**Tôi có thể dùng VPN để bảo vệ mình không?**

Có, mạng riêng ảo (VPN) mã hóa toàn bộ dữ liệu kết nối từ thiết bị đến mạng Internet. Nó là dịch vụ hầu hết người dùng sử dụng khi cần kết nối tới mạng máy tính ở nơi làm việc khi không có mặt tại đó. Nó tạo ra một đường hầm an toàn cho dữ liệu của bạn mà không ai theo dõi được. Tuy nhiên, không phải mọi mạng VPN đều có khả năng bảo mật như nhau.

## 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*

## CCNA Voice

CISCO CERTIFIED CCNA VOICE

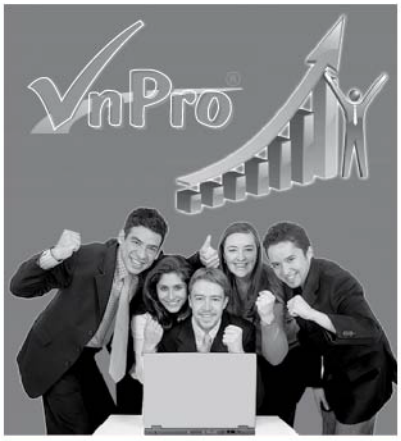
## *Chương trình ưu đãi các khóa học:*

### *Lớp sáng, chiều:*

** Tặng Giáo Trình.*
** Ưu đãi 5% khi đăng ký nhóm 2 học viên.*
** Tặng Áo Thun.*

### *Lớp tối:*

** Ưu đãi 30% HP dành cho Sinh Viên.*
** Ưu đãi lên đến 20% HP dành cho Học viên cũ.*
** Ưu đãi dành cho khách hàng doanh nghiệp.*
** Tặng Balo, giáo trình.*

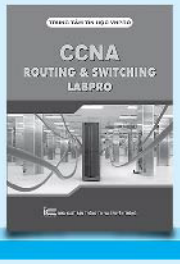



## *Cam kết lợi ích khi học tại VnPro*

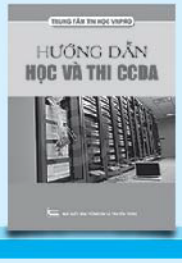
- *Giáo trình giảng dạy chuẩn quốc tế và LabPro tiếng Việt.*
- *Thực hành >70% thời lượng chương trình và trực tiếp 100% trên thiết bị chính hãng, hiện đại. (>100 giờ lab)*
- *Được thực hành miễn phí ngoài giờ.*
- *Chứng chỉ VnPro được công nhận trên toàn quốc.*
- *Thi đậu quốc tế sau khi hoàn tất khóa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

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

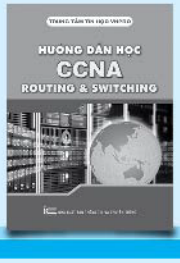
**GIẢM* NGAY 10%**



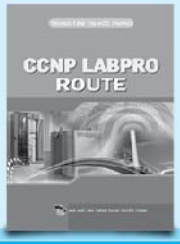

**CCNA Routing & Switching**
Giá: 150.000 VNĐ




**CCDA**
Giá: 250.000 VNĐ

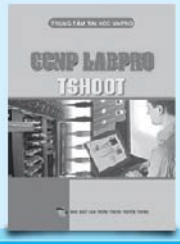



**Hướng dẫn học CCNA Routing & Switching**
Giá: 180.000 VNĐ




**CCNP LABPRO ROUTE**
Giá: 120.000 VNĐ


**CCNP LABPRO SWITCH**
Giá: 120.000 VNĐ



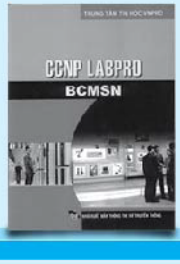

**CCNP LABPRO TSHOOT**
Giá: 120.000 VNĐ


**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



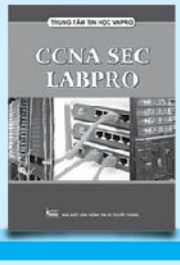

**CCNP LABPRO BCMSN**
Giá: 70.000 VNĐ


**CCNP LABPRO ISCW**
Giá: 120.000 VNĐ

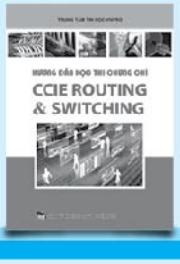

**CCSP LABPRO SNAF & SNAA**
Giá: 120.000 VNĐ


**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 là giảm 10% khi đặt sách online**

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

# VNPRO TRAO HỌC BỔNG KHUYẾN HỌC CHO HỌC VIÊN XUẤT SẮC TRONG THÁNG 10/2017


*Thầy Đức Phương* trao học bổng cho anh *Nguyễn Phước Huy Hoàng lớp 17A100*


*Thầy Trung Hiếu* trao học bổng học viên xuất sắc *lớp 17P235* cho bạn *Hà Quang Nhơn*

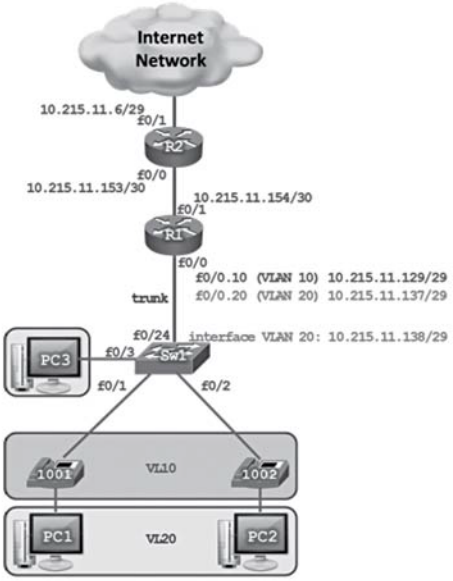

*VnPro* trao học bổng cho anh *Tạ Ngọc Hưng* *lớp 17P234*


*Thầy Thanh Phong* trao học bổng học viên xuất sắc *lớp A98* cho bạn *Võ Duy Hiếu*


*Thầy Đông Khê* trao học bổng học viên xuất sắc *lớp AK100* cho bạn *Lê Bình Nguyên*

***Phòng Pr-Marketing VnPro***

# Giám sát các thiết bị kết nối vào hạ tầng mạng bằng công cụ IP Device Tracking và EPIC EM




Danh sách IP các thiết bị:

- R1: 10.215.11.154
- R2: 10.215.11.153
- Sw1: 10.215.11.138
- APIC EM Server: được cài đặt trên PC3 có thể giao tiếp tới các thiết bị trên hệ thống

**Các bước thực hiện:**

- Bước 1. Cấu hình cơ bản trên các thiết bị.
- Bước 2. Kích hoạt tính năng IPDT (IP Device Tracking) trên Sw1.
- Bước 3. Sử dụng APIC EM giám sát các thiết bị trên hạ tầng mạng.

o Bước 3.1. Khai báo thông tin telnet/ssh, SNMP phục vụ cho quá trình "Discovery" các Network Device trên hạ tầng mạng.

o Bước 3.2. Tính năng "Discovery" cho phép tự động dò tìm các thiết bị thông qua thông tin Telnet, SNMP và đưa vào chương trình quản lý APIC EM.

o Bước 3.3. Tính năng Device Inventory thống kê danh sách các thiết bị mà APIC EM quét được.

o Bước 3.4. Tính năng Host Inventory cho phép thu thập thông tin các thiết bị đầu cuối kết nối tới Switch.

o Bước 3.5. Tính năng Topology cho phép APIC tự động vẽ sơ đồ hệ thống mạng.

o Bước 3.6. Hỗ trợ khắc phục sự cố bằng tính năng "Path Trace".

**Thực hiện:**

**Bước 1.** Cấu hình cơ bản trên các thiết bị.

Cấu hình cơ bản trên Router R1.

```
hostname R1
interface f0/0
 no shutdown
 exit
interface f0/0.10
 encapsulation dot1q 10
 ip address 10.215.11.129 255.255.255.248
 no shutdown
 exit
interface f0/0.20
 encapsulation dot1q 20
 ip address 10.215.11.137 255.255.255.248
 no shutdown
 exit
interface f0/1
 ip address 10.215.11.154 255.255.255.252
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 10.215.11.153
enable password bqk
username bqk privilege 15 password bqk
line vty 0 4
 privilege level 15
 login local
 exit
line console 0
 logging synchronous
 exec-timeout 0 0
 exit
cdp run
no ip domain-lookup
no service timestamps debug
no service timestamps log
snmp-server community bqk rw
snmp-server community bqk ro
```

```
ip dhcp excluded-address 10.215.11.129
ip dhcp excluded-address 10.215.11.137 10.215.11.138
ip dhcp pool VOICE
 network 10.215.11.128 255.255.255.248
 default-router 10.215.11.129
 option 150 ip 10.215.11.129
 exit
ip dhcp pool DATA
 network 10.215.11.136 255.255.255.248
 default-router 10.215.11.137
 exit
```

```
exit
clock set 12:00:00 20 Sept 2017
configure terminal
```

```
telephony-service
 ip source-address 10.215.11.129 port 2000
 max-dn 144
 max-ephones 42
 no auto-reg-ephone
 cnf-file perphone
 exit
ephone-dn 1 dual-line
 number 1001
 exit
ephone-dn 2 dual-line
 number 1002
 exit
ephone-dn 3 dual-line
 number 1003
 exit
ephone 1
 mac-address fcfb.fbcb.5919
 type 7942
 button 1:1
 restart
 exit
ephone 2
 mac-address 001d.a23e.a48f
 type 7942
 button 1:2
 restart
 exit
ephone 3
 mac-address 0000.aaaa.1003
 type CIPC
 button 1:3
 restart
 exit
telephony-service
 create cnf-files
 exit
```

Cấu hình cơ bản trên Router R2.

```
hostname R2
interface f0/0
 ip address 10.215.11.153 255.255.255.252
 no shutdown
 exit
interface f0/1
 ip address 10.215.11.6 255.255.255.248
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 10.215.11.1
ip route 10.215.11.128 255.255.255.248 10.215.11.154
ip route 10.215.11.136 255.255.255.248 10.215.11.154
enable password bqk
username bqk privilege 15 password bqk
line vty 0 4
 privilege level 15
 login local
 exit
line console 0
 logging synchronous
 exec-timeout 0 0
 exit
cdp run
no ip domain-lookup
no service timestamps debug
no service timestamps log
snmp-server community bqk rw
snmp-server community bqk ro
```

Cấu hình cơ bản trên Router Sw1.

```
hostname Sw1
vlan 10
vlan 20
 exit
interface vlan 20
 ip address 10.215.11.138 255.255.255.248
 no shutdown
 exit
interface range f1/0/1, f1/0/2
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 10
 spanning-tree portfast
 no shutdown
 exit
interface range f1/0/3
 switchport mode access
 switchport access vlan 20
 spanning-tree portfast
 no shutdown
 exit
interface range f1/0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
 no shutdown
 exit
ip default-gateway 10.215.11.137
no ip routing
enable password bqk
username bqk privilege 15 password bqk
line vty 0 4
 privilege level 15
 login local
 exit
line console 0
 logging synchronous
 exec-timeout 0 0
 exit
cdp run
no ip domain-lookup
no service timestamps debug
no service timestamps log
snmp-server community bqk rw
snmp-server community bqk ro
```

**Bước 2.** Kích hoạt tính năng IPDT (IP Device Tracking) trên Sw1.

- ip device tracking: kích hoạt tính năng IPDT trên switch.
- ip device tracking maximum 2: cho phép interface cập nhật tối đa 2 entry thông tin của thiết bị kết nối trên interface được kích hoạt.

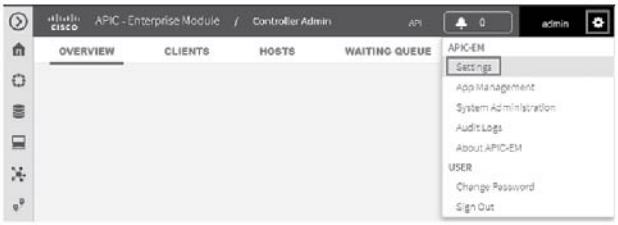
```
Sw1(config)# ip device tracking
```

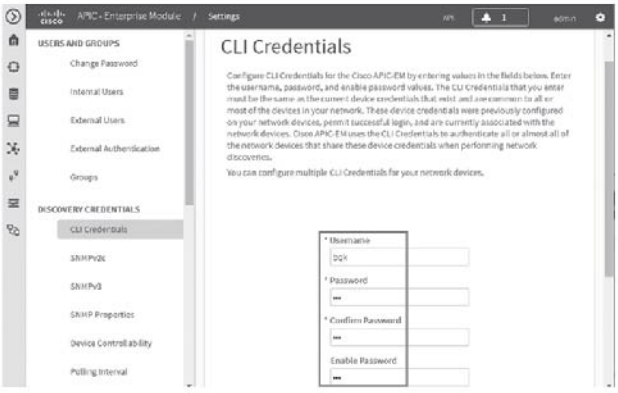
```
Sw1(config)#
interface f1/0/24
 ip device tracking maximum 3
 exit
interface range f1/0/1, f1/0/2, f1/0/3
 ip device tracking maximum 2
 exit
```

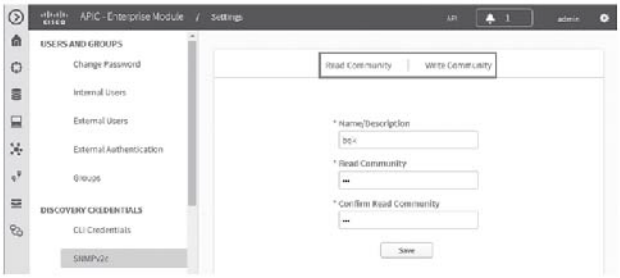
```
Sw1# show ip device tracking all
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
--------------------------------------------------------------------
  IP Address      MAC Address    Vlan  Interface                STATE
--------------------------------------------------------------------
10.215.11.130    001d.a23e.a48f  10    FastEthernet1/0/2        ACTIVE
10.215.11.131    fcfb.fbcb.5919  10    FastEthernet1/0/1        ACTIVE
10.215.11.139    24b6.fd08.19e4  20    FastEthernet1/0/3        ACTIVE
10.215.11.137    0017.95bc.6e10  20    FastEthernet1/0/24       ACTIVE
Total number interfaces enabled: 4
Enabled interfaces:
  Fa1/0/1, Fa1/0/2, Fa1/0/3, Fa1/0/24
Sw1#
```

**Bước 3.** Sử dụng APIC EM giám sát các thiết bị trên hạ tầng mạng.

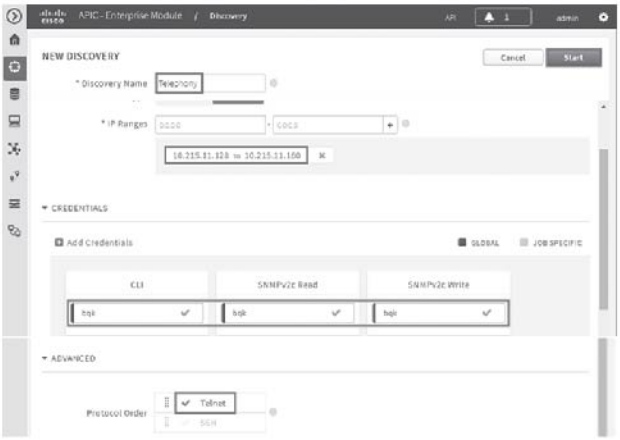
**Bước 3.1.** Khai báo thông tin telnet/ssh, SNMP phục vụ cho quá trình "Discovery" các Network Device trên hạ tầng mạng.

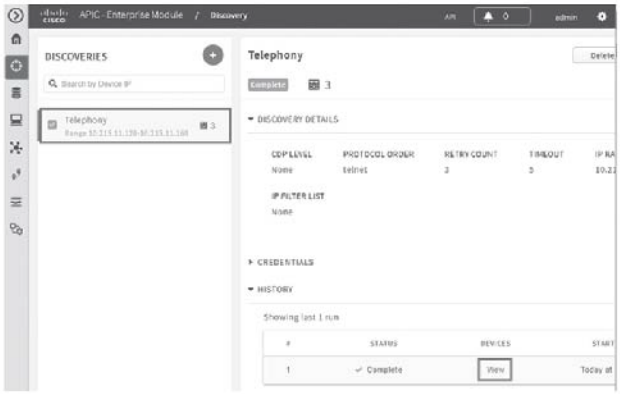


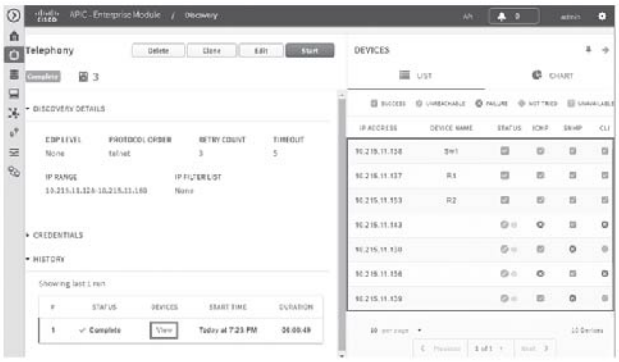




**Bước 3.2.** Tính năng "Discovery" cho phép tự động dò tìm các thiết bị thông qua thông tin Telnet, SNMP và đưa vào chương trình quản lý APIC EM.

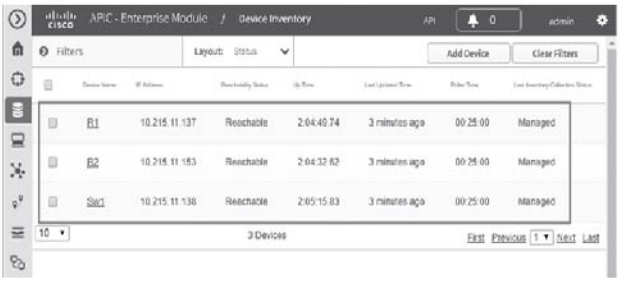


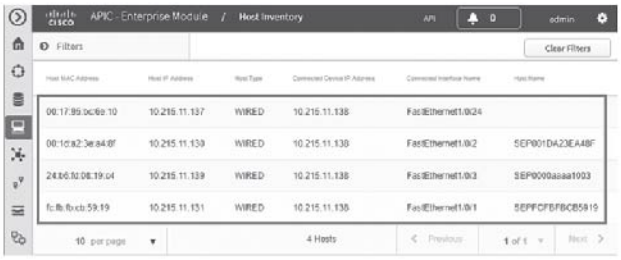

**Bước 3.3.** Tính năng Device Inventory thống kê danh sách các thiết bị mà APIC EM quét được.

Bằng cách tùy biến Layout của Device Inventory, ta có thể xem được cấu hình running-config của các thiết bị thông qua giao diện APIC EM.



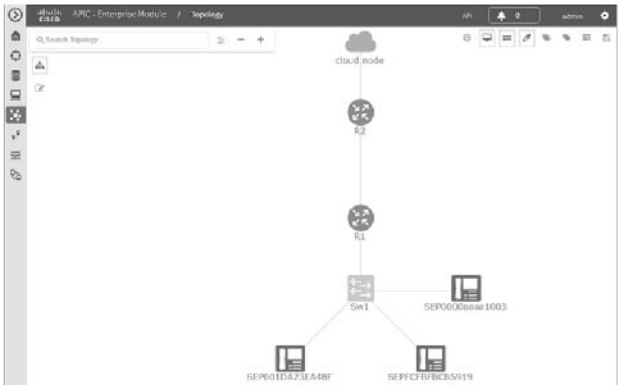
**Bước 3.4.** Tính năng Host Inventory cho phép thu thập thông tin các thiết bị đầu cuối kết nối tới Switch.

Tính năng Host Inventory thu thập thông tin tất cả các thiết bị kết nối tới Sw1 (10.215.11.138), trên Sw1 ta cần kích hoạt tính năng IP Device Tracking.

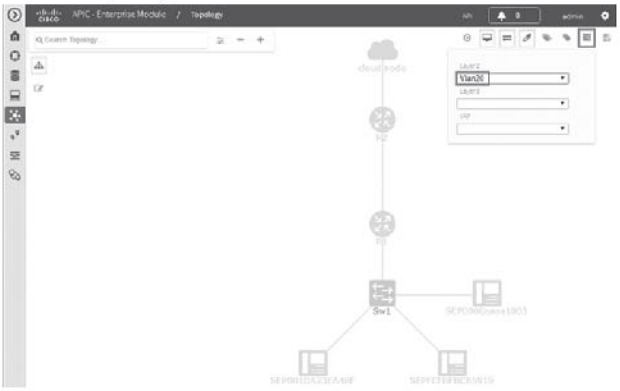



**Bước 3.5.** Tính năng Topology cho phép APIC tự động vẽ sơ đồ hệ thống mạng.

Tính năng tự động phác họa Topology hệ thống mạng dựa trên thông tin CDP, SNMP thu thập được từ các thiết bị.



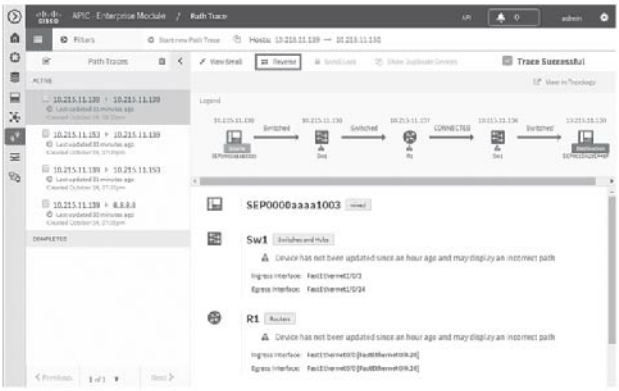

Tính năng Layers cho phép quan sát Topology dưới dạng Layer 2 hoặc Layer 3.




**Bước 3.6.** Hỗ trợ khắc phục sự cố bằng tính năng "Path Trace".

Thực hiện Path Trace từ PC3 (10.215.11.139) tới Internet (8.8.8.8).


Từ PC3 (10.215.11.139) thuộc VLAN 20 tiến hành "Path Trace" tới Phone 1002 (10.215.11.130) thuộc VLAN 10.

# Top 3 phương pháp học tiếng Anh tốt nhất

**1. Phương pháp Eng Breaking**

Bằng cách thức tiếp cận tiếng Anh giao tiếp mới, Eng Breaking mang lại một khối lượng kiến thức nền tảng, đi kèm các từ vựng thiết thực (từ lóng, thành ngữ) mà người bản ngữ thực sự sử dụng trong giao tiếp hàng ngày.

Eng Breaking sử dụng 3 kỹ thuật: nghe ngấm, nói đuổi, phản xạ đa chiều. Mỗi một kỹ thuật sẽ giúp bạn giải quyết một vấn đề riêng:

- Kỹ thuật nghe ngấm giúp tiết kiệm 71% thời gian luyện nghe tiếng Anh. Bạn sẽ nhận ra được phát âm chuẩn các từ thông qua kỹ thuật này.
- Kỹ thuật nói đuổi giúp luyện tai nhạy, miệng dẻo và nói tiếng Anh trôi chảy chỉ sau 1 tháng. Sau khi nghe ngấm kỹ thuật này sẽ giúp bạn có được phát âm chuẩn Anh-Mỹ như người bản ngữ.
- Kỹ thuật phản xạ 3 chiều cho phép bạn luyện giao tiếp cùng trợ lý ảo người Mỹ hàng ngày.

Sau này, bạn vẫn có thể áp dụng 3 phương pháp này vào việc học tiếng Anh của mình. Đây là những phương pháp học tập khoa học và rất dễ áp dụng đối với bạn cũng như những người học tiếng Anh khác.

Eng Breaking có đầy đủ bộ đĩa kèm giáo trình, kế hoạch hành động, mục tiêu, phiếu bảo hành. Với các giọng nói tự nhiên, đầy cuốn hút cùng các email hỗ trợ hàng ngày sẽ tạo động lực, hứng thú học tập cho bạn.

Nội dung các bài học của Eng Breaking rất thiết thực và gần gũi với đời sống hàng ngày của chúng ta. Bạn sẽ học được cách nói những câu tưởng chừng như rất đơn giản nhưng bạn lại không biết cách diễn đạt sao cho vừa đúng vừa tự nhiên.

Mỗi bài học của Eng Breaking không chỉ có hội thoại, mà bạn còn được nghe các đoạn Story được kể lại dưới 3 thời thì: quá khứ đơn, hiện tại đơn, tương lai đơn. Bên cạnh đó, bạn còn được luyện trả lời các câu hỏi sau mỗi bài Story để tập phản xạ giao tiếp trôi chảy.

Phương pháp học tiếng Anh Eng Breaking phù hợp cho mọi đối tượng từ người mới học tiếng Anh cho đến người kém khoản giao tiếp.

**2. Phương pháp Effortless English**

Effortless English là phương pháp tự học tiếng anh lấy ý tưởng từ cách tiếp cận ngôn ngữ của một đứa trẻ do tiến sĩ A.J. Hoge (người Mỹ) sáng lập ra, được áp dụng rất phổ biến ở 25 quốc gia với hàng triệu người theo học. Effortless English dạy học viên cách sử dụng cơ thể, đầu óc và phương pháp học tiếng Anh.

Bản chất của phương pháp này nằm ở 7 quy tắc quan trọng. 7 quy tắc này được A.J. Hoge đúc kết được sau nhiều năm nghiên cứu và đã được nhiều người kiểm chứng thành công:

- Quy tắc 1: Don't Study Indivisual Word – Học cụm từ, không học từng từ đơn lẻ.
- Quy tắc 2: Don't study Grammar Rules – Không học các quy tắc ngữ pháp.
- Quy tắc 3: Learn with your ears, not your eyes – Học bằng tai, không phải bằng mắt.
- Quy tắc 4: Deeply learning – Học sâu, nhớ lâu.
- Quy tắc 5: Learn with Point Of View mini Story – Học ngữ pháp qua những câu hỏi ở các thì khác nhau sử dụng những đoạn hỏi đáp ngắn.
- Quy tắc 6: Learn Real English – Học tiếng Anh thực tế.
- Quy tắc 7: Listen and Answer – Nghe và trả lời.

Phương pháp này tập trung vào kỹ năng nghe là chính. Khi giỏi kỹ năng nghe thì đó là nền tảng giúp người học vươn xa và học tiếng Anh giao tiếp một cách toàn diện. Bạn không cần phải ghi nhớ bất cứ thứ gì, chỉ cần nghe, thư giãn, trả lời các câu hỏi khi được nhắc nhở.

Mục tiêu của Effortless là giúp đỡ người học tiến bộ nhanh và nói ra một cách dễ dàng mà không cần phải dịch, hoặc cảm thấy gượng ép, căng thẳng khi nói.

Ngoài ra, Effortless English không chỉ giúp bạn cải thiện khả năng giao tiếp tiếng Anh, mà còn dạy bạn cách thành công hơn trong cuộc sống cá nhân.

Nhược điểm lớn nhất của effortless English là không dễ cho người mới bắt đầu tiếp cận với Tiếng Anh. Bạn phải có nền tảng và khả năng tự học tốt mới có thể thành công.

**3. Phương pháp Pimsleur**

Phương pháp Pimsleur là khóa học ngôn ngữ giao tiếp phổ biến nhất trên thế giới. Bạn có thể học 40 ngôn ngữ khác khau thông qua phương pháp Pimsleur. Có đến 14 phiên bản với các khóa học ngôn ngữ khác nhau cho chương trình học tiếng Anh. Trong vòng 30 năm qua đã có hơn 25 triệu người sử dụng phương pháp Pimsleur.

Với phương pháp Pimsleur, bạn sẽ học ngôn ngữ mới giống như trẻ em học tiếng mẹ đẻ. Bạn học bằng cách nghe và nói những từ phổ thông nhất, những cụm từ và câu được sử dụng trong giao tiếp hàng ngày, không cần dùng sách giáo khoa. Phương pháp Pimsleur sử dụng kỹ thuật nhớ lại theo khoảng thời gian nhất định để giúp bạn có thể nhớ được lâu hơn. Phương pháp này đặc biệt thích hợp cho những người mới học Tiếng Anh.

Tuy nhiên, phương pháp Pimsleur cũng có nhược điểm: vì các từ lặp lại như vậy rất dễ gây nhàm chán. Ngoài ra, theo như các nhà phê bình đánh giá thì phương pháp này cũng không giúp người học tiếp thu một vốn từ vựng phong phú. Giống như Effortless English, người học phải có nỗ lực và quyết tâm rất lớn mới có thể hoàn thành bài mỗi ngày.

**Kết luận**

Trên đây là top 3 phương pháp học tiếng Anh có thể xem là tốt nhất hiện nay. Mỗi phương pháp đều có ưu, nhược điểm riêng, bạn hãy tham khảo và chọn phương pháp mà bạn thấy là phù hợp nhất với mình. Học tiếng Anh là một việc lâu dài, đòi hỏi một sự quyết tâm cao. Dù chọn cách học nào thì bạn cũng cần phải kiên trì theo đuổi đến cùng.

# Vì sao hacker thích mặc áo trùm đầu, ngồi trong bóng tối???

***Thời trang của hacker thường giống nhau và hầu hết bị ảnh hưởng bởi phim ảnh hay các phương tiện truyền thông.***

Hacker được phân ra thành 2 nhóm dựa theo cách thức hoạt động của họ: hacker "mũ trắng" chuyên phát hiện lỗ hổng bảo mật để bảo vệ người dùng và hacker "mũ đen" chuyên sử dụng khả năng tấn công mạng của mình vào mục đích xấu. Có một nhóm hacker khác được gọi là "mũ xám" nằm giữa ranh giới của "mũ đen" và "mũ trắng", tức thường có xu hướng vừa bảo vệ người dùng, vừa đánh cắp dữ liệu cho mục đích không chính đáng. Tuy nhiên, tất cả khi xuất hiện đều có điểm chung: mặc áo đen có mũ trùm đầu và ngồi trong bóng tối cùng với máy vi tính, ít nhất là theo những bức ảnh từng được đăng tải trên Internet.

***Hình tượng hacker thường thấy***

Tuy nhiên, hình ảnh này không phải đến bây giờ mới xuất hiện. Theo chuyên gia an ninh mạng Marc Rogers - Giám đốc bộ phận an ninh thông tin của Cloudflare và là người đứng đầu hội nghị hacker lớn nhất thế giới Defcon - phong cách này từng có mặt từ đầu những năm 90 của thế kỷ trước.

Theo Rogers, trong thập niên 80 và đầu những năm 90, hacker trông giống như một "cyberpunks". Trong một ấn bản năm 1993 của tạp chí Mondo 2000, "cyberpunks" là những người mang giày cao gót, mặc áo khóa da và găng tay trùm kín các ngón tay.

Đến năm 1995, khi bộ phim "Hackers" được trình chiếu, khuôn mẫu thời trang của tin tặc dần thay đổi. "Cyberpunks không phải là hình tượng thời trang xấu xí trong mắt hacker, nhưng bộ phim đã khiến họ bắt chước nhiều thứ, từ đó khiến chúng trở nên tươi mới hơn", Rogers nhận định.

Defcon đã tồn tại trong khoảng hơn 2 thập kỷ (từ tháng 6-1993) và Rogers đã chứng kiến nhiều sự thay đổi về thời trang của hacker. "Vẫn còn đó áo khoác da, giày dép, ủng... Nhưng sau đó, một số người còn xuất hiện với mái tóc nhuộm, ván trượt. Họ là tuýp người đã xem bộ phim Hackers, muốn trở thành hacker, lấy hình ảnh từ đó và một số làm chúng trở nên tươi mới hơn", Rogers cho biết.

Trong những năm gần đây, khi xu hướng hacker "mũ đen" nhiều hơn, đặc biệt là những tội phạm mạng chuyên đánh cắp tài khoản ngân hàng, áo choàng có mũ trùm đầu bắt đầu được sử dụng do muốn "có nhiều hình tượng hơn". Theo CNN, nguyên nhân đến từ các phương tiện thông tin đại chúng và cả mạng xã hội.

"Mặc dù hacker thường nhạo báng các phương tiện truyền thông, nhưng chính họ lại bị tác động bởi phong cách thời trang được hiển thị trên đó. Đôi khi, áo đen trùm đầu lại trở thành 'đồng phục' của một nhóm hacker", Brian Bartholomew, nhà nghiên cứu bảo mật cao cấp của Kaspersky Lab, cho biết.

Bartholomew cho rằng, bộ phim Mr.Robot minh họa rõ nhất phong cách này. Trong phim, Elliot - nhân vật chính, một hacker 29 tuổi - thường xuyên mặc áo choàng đen.

Ngoài ra, còn một phong cách nữa, đó là sống trong bóng tối và đội mặt nạ đen kín mặt. Rogers cho rằng, phong cách này nhằm tăng thêm "sự bí hiểm", làm cho hacker "có vẻ đáng sợ" hơn.

Rogers dự đoán những khuôn mẫu trên có thể sẽ tiếp tục thay đổi trong tương lai và các phương tiện thông tin, mạng xã hội là yếu tố tác động nhiều nhất.

# Chúc Mừng Ngày Nhà Giáo Việt Nam 20-11

VnPro

Ưu Đãi -30% Sinh Viên

Ưu Đãi -10% Doanh Nghiệp

Ưu Đãi -5% Nhóm từ 2 HV

## Lịch khai giảng tháng 11/2017

| Tên khóa học | Ngày khai giảng | Ngày học | Giờ học | Học phí/khóa | Thời gian |
|---|---|---|---|---|---|
| **CHƯƠNG TRÌNH CCNA** | | | | | |
| **CCNAX (200–125)** | 02/11 | 3 – 5 – 7 | 8:30 – 11:30AM | 3.700.000 | 152 giờ |
| | | | 2:00 – 5:00PM | 3.700.000 | |
| | | | 6:30 – 9:30PM | 7.400.000 | |
| | 10/11 | 2 – 4 – 6 | 8:30 – 11:30AM | 3.700.000 | |
| | | | 2:00 – 5:00PM | 3.700.000 | |
| | | | 6:30 – 9:30PM | 7.400.000 | |
| | 16/11 | 3 – 5 – 7 | 8:30 – 11:30AM | 3.700.000 | |
| | | | 6:30 – 9:30PM | 7.400.000 | |
| | 22/11 | 2 – 4 – 6 | 8:30 – 11:30AM | 3.700.000 | |
| | | | 6:30 – 9:30PM | 7.400.000 | |
| | 28/11 | 3 – 5 – 7 | 8:30 – 11:30AM | 3.700.000 | |
| | | | 6:30 – 9:30PM | 7.400.000 | |
| **CCNAX Online** | 16/11 | 3 – 5 – 7 | 6:30 – 9:30PM | 2.900.000 | 72 giờ |
| | 27/11 | 2 – 4 – 6 | 6:30 – 9:30PM | 2.900.000 | |
| **CCNA Security (210–260)** | 28/11 | 3 – 5 – 7 | 6:30 – 9:30PM | 5.900.000 | 72 giờ |
| **CCNA Collaboration** | 28/11 | 3 – 5 – 7 | 6:30 – 9:30PM | 7.400.000 | 100 giờ |
| **CHƯƠNG TRÌNH CCNP** | | | | | |
| **ROUTE (300–101)** | 01/11 | 2 – 4 – 6 | 6:30 – 9:30PM | 8.900.000 | 120 giờ |
| | 14/11 | 3 – 5 – 7 | 8:30 – 11:30AM | 5.900.000 | |
| | | | 6:30 – 9:30PM | 8.900.000 | |
| | 25/11 | Thứ 7 | Sáng + Chiều | 8.900.000 | |
| **SWITCH (300–115)** | 01/11 | 2 – 4 – 6 | 6:30 – 9:30PM | 8.900.000 | 120 giờ |
| | 21/11 | 3 – 5 – 7 | 2:00 – 5:00PM | 5.900.000 | |
| | | | 6:30 – 9:30PM | 8.900.000 | |
| **TSHOOT (300 135)** | 27/11 | 2 – 4 – 6 | 6:30 – 9:30PM | 8.900.000 | 120 giờ |
| **CHƯƠNG TRÌNH CCIE WRITTEN** | | | | | |
| **CCIE WRITTEN** | 27/11 | 2 – 4 – 6 | 6:30 – 9:30PM | 12.500.000 | 120 giờ |
| **KHÓA HỌC CHUYÊN ĐỀ** | | | | | |
| **FIREWALL** | 25/11 | Thứ 7 | Sáng + Chiều | 5.900.000 | 54 giờ |

>>> ĐĂNG KÝ NGAY <<<

HOTLINE 0933.427.079

## TRUNG TÂM TIN HỌC VNPRO

149/1D Ung Văn Khiêm, phường 25, quận Bình Thạnh, TP. Hồ Chí Minh

Điện Thoại: (028). 35124257 | Email: vnpro@vnpro.org | Website: www.vnpro.vn

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®