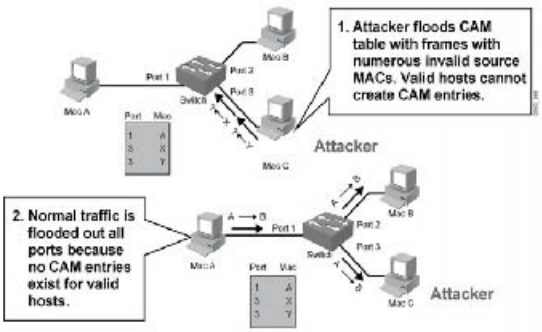
Số 46
06/2016

BẢN TIN dancisco

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

Chống MAC Layer Attack trên Switch



Bảng CAM (Content Addressable Memory) lưu trữ các địa chỉ MAC của các port, và các tham số VLAN trong switch. Không gian nhớ trong bảng CAM là hạn chế nên có nguy cơ tràn bảng CAM. Kiểu tấn công làm tràn MAC sẽ cố gắng làm tràn bảng CAM của các switch, khi đó switch sẽ cư xử như các hub. Một cuộc tấn công kiểu này trông giống như lưu lượng từ hàng ngàn máy tính được chuyển đến một port, nhưng thực tế là nó chỉ đến từ một máy giả mạo địa chỉ MAC của hàng ngàn host giả mạo.

[Trang 11]

NHỮNG VỊ TRÍ CÔNG VIỆC BẠN CÓ THỂ ĐẢM NHẬN KHI THEO NGHỀ NETWORK

VnPro thường xuyên nhận được câu hỏi từ rất nhiều bạn từ khắp nơi ở Việt Nam là: "Sau khi học Network xong mình sẽ làm gì? Làm việc ở đâu và làm những cái gì?". Để giải đáp những thắc mắc đó của tất cả các bạn, VnPro sẽ tổng hợp tất cả những vị trí mà các bạn có thể đảm nhận khi theo học quản trị mạng.

[Trang 07]

HỌC KỸ THUẬT HAY KINH TẾ ?

[Trang 08]

TIN TỨC SỰ KIỆN KHÁC

01. Tin tức công nghệ
03. Tin tức công nghệ
06. Tủ sách LabPro
09. Challenge LAB
12. Bài viết chuyên đề
13. Cùng học tiếng Anh

Cisco Certified Network Associate (200-125)

Chứng chỉ CCNA Routing and Switching ver 2.0 (200-120) đã được cập nhật lên version 3.0. Chứng chỉ CCNA Routing and Switching (200-125) ver 3.0 sẽ đánh giá, kiểm tra kiến thức và kỹ năng của người dự thi tập trung vào các phần như:

- Mô hình mạng cơ bản.
- Công nghệ chuyển mạch trong mạng LAN
- Kỹ thuật định tuyến IPv4 và IPv6.
- Các dịch vụ hạ tầng và bảo mật trong công nghệ mạng WAN.

Thời gian thi sẽ kéo dài trong vòng 90 phút bao gồm 50 – 60 câu hỏi trắc nghiệm. Cisco vẫn cho phép các thí sinh thi version 2.0 đến hết ngày 20/08/2016.

Về phần đào tạo, Cisco đã bổ sung thêm một vài phần như sau:

- Nâng cao kiến thức, hiểu biết về kiến trúc hạ tầng mạng.
- Chủ đề VPN được bổ sung thêm các kỹ thuật về Dynamic Multipoint VPN (DMVPN), site-to-site VPN và VPN client.
- Tăng cường tập trung vào kiến thức và cấu hình giao thức định tuyến IPv6.
- Tìm hiểu về triển khai tài nguyên điện toán đám mây (Cloud) trong hạ tầng mạng doanh nghiệp.
- Tìm hiểu về các khái niệm và ứng dụng của QoS (Quality of Service) trong hạ tầng mạng doanh nghiệp.

Các chủ đề của chương trình CCNA Routing and Switching (200-125) ver 3.0 đã được cập nhật như sau:

15% 1.0 Network Fundamentals

1.1 Compare and contrast OSI and TCP/IP models
1.2 Compare and contrast TCP and UDP protocols
1.3 Describe the impact of infrastructure components in an enterprise network
1.3.a Firewalls
1.3.b Access points
1.3.c Wireless controllers
1.4 Describe the effects of cloud resources on ente prise network architecture
1.4.a Traffic path to internal and external cloud services
1.4.b Virtual services
1.4.c Basic virtual network infrastructure
1.5 Compare and contrast collapsed core and three-tier architectures
1.6 Compare and contrast network topologies
1.6.a Star
1.6.b Mesh
1.6.c Hybrid
1.7 Select the appropriate cabling type based on implementation requirements
1.8 Apply troubleshooting methodologies to resolve problems
1.8.a Perform and document fault isolation
1.8.b Resolve or escalate
1.8.c Verify and monitor resolution
1.9 Configure, verify, and troubleshoot IPv4 addressing and subnetting
1.10 Compare and contrast IPv4 address types
1.10.a Unicast
1.10.b Broadcast
1.10.c Multicast
1.11 Describe the need for private IPv4 addressing
1.12 Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment
1.13 Configure, verify, and troubleshoot IPv6 addressing
1.14 Configure and verify IPv6 Stateless Address Auto Configuration
1.15 Compare and contrast IPv6 address types
1.15.a Global unicast
1.15.b Unique local
1.15.c Link local
1.15.d Multicast
1.15.e Modified EUI 64
1.15.f Autoconfiguration
1.15.g Anycast

21% 2.0 LAN Switching Technologies

2.1 Describe and verify switching concepts
2.1.a MAC learning and aging
2.1.b Frame switching
2.1.c Frame flooding
2.1.d MAC address table
2.2 Interpret Ethernet frame format
2.3 Troubleshoot interface and cable issues (collisions, errors, duplex, speed)
2.4 Configure, verify, and troubleshoot VLANs (normal/extended range) spanning multiple switches
2.4.a Access ports (data and voice)
2.4.b Default VLAN
2.5 Configure, verify, and troubleshoot interswitch connectivity
2.5.a Trunk ports
2.5.b Add and remove VLANs on a trunk
2.5.c DTP, VTP (v1&v2), and 802.1Q 2.5.d Native VLAN
2.6 Configure, verify, and troubleshoot STP protocols
2.6.a STP mode (PVST+ and RPVST+)
2.6.b STP root bridge selection
2.7 Configure, verify and troubleshoot STP related optional features
2.7.a PortFast
2.7.b BPDU guard
2.8 Configure and verify Layer 2 protocols
2.8.a Cisco Discovery Protocol
2.8.b LLDP
2.9 Configure, verify, and troubleshoot (Layer 2/Layer 3) EtherChannel
2.9.a Static
2.9.b PAGP
2.9.c LACP
2.10 Describe the benefits of switch stacking and chassis aggregation

23% 3.0 Routing Technologies

3.1 Describe the routing concepts
3.1.a Packet handling along the path through a network
3.1.b Forwarding decision based on route lookup
3.1.c Frame rewrite
3.2 Interpret the components of a routing table
3.2.a Prefix 3.2.b Network mask
3.2.c Next hop
3.2.d Routing protocol code
3.2.e Administrative distance
3.2.f Metric
3.2.g Gateway of last resort
3.3 Describe how a routing table is populated by different routing information sources
3.3.a Admin distance
3.4 Configure, verify, and troubleshoot inter-VLAN routing
3.4.a Router on a stick
3.4.b SVI
3.5 Compare and contrast static routing and dynamic routing
3.6 Compare and contrast distance vector and link state routing protocols
3.7 Compare and contrast interior and exterior routing protocols

3.10 Configure, verify, and troubleshoot single area and multi-area OSPFv3 for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub, virtuallink, and LSAs)
3.11 Configure, verify, and troubleshoot EIGRP for IPv4 (excluding authentication, filtering, manual summarization, redistribution, stub)
3.12 Configure, verify, and troubleshoot EIGRP for IPv6 (excluding authentication, filtering, manual summarization, redistribution, stub)
3.13 Configure, verify, and troubleshoot RIPv2 for IPv4 (excluding authentication, filtering, manual summarization, redistribution)
3.14 Troubleshoot basic Layer 3 end-to-end connectivity issues

10% 4.0 WAN Technologies
4.1 Configure and verify PPP and MLPPP on WAN interfaces using local authentication
4.2 Configure, verify, and troubleshoot PPPoE client-side interfaces using local authentication
4.3 Configure, verify, and troubleshoot GRE tunnel connectivity
4.4 Describe WAN topology options
4.4.a Point-to-point
4.4.b Hub and spoke
4.4.c Full mesh
4.4.d Single vs dual-homed
4.5 Describe WAN access connectivity options
4.5.a MPLS
4.5.b Metro Ethernet
4.5.c Broadband PPPoE
4.5.d Internet VPN (DMVPN, site-to-site VPN, client VPN)
4.6 Configure and verify single-homed branch connectivity using eBGP IPv4 (limited to peering and route advertisement using Network command only)
4.7 Describe basic QoS concepts
4.7.a Marking
4.7.b Device trust
4.7.c Prioritization
4.7.c. (i) Voice
4.7.c. (ii) Video
4.7.c. (iii) Data
4.7.d Shaping
4.7.e Policing
4.7.f Congestion management

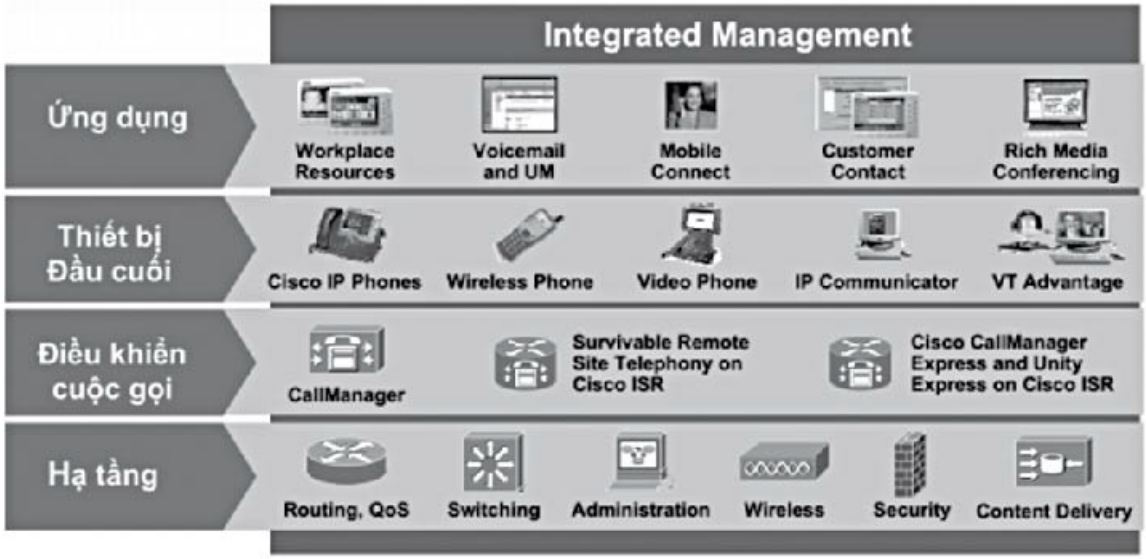
10% 5.0 Infrastructure Services
5.1 Describe DNS lookup operation
5.2 Troubleshoot client connectivity issues involving DNS
5.3 Configure and verify DHCP on a router (excluding static reservations)
5.3.a Server
5.3.b Relay
5.3.c Client
5.3.d TFTP, DNS, and gateway options
5.4 Troubleshoot client- and router-based DHCP connectivity issues
5.5 Configure, verify, and troubleshoot basic HSRP
5.5.a Priority 5.5.b Preemption
5.5.c Version
5.6 Configure, verify, and troubleshoot inside source NAT
5.6.a Static
5.6.b Pool
5.6.c PAT
5.7 Configure and verify NTP operating in a client/server mode

11% 6.0 Infrastructure Security
6.1 Configure, verify, and troubleshoot port security
6.1.a Static
6.1.b Dynamic
6.1.c Sticky
6.1.d Max MAC addresses
6.1.e Violation actions
6.1.f Err-disable recovery
6.2 Describe common access layer threat mitigation techniques
6.2.a 802.1x
6.2.b DHCP snooping
6.2.c Nondefault native VLAN
6.3 Configure, verify, and troubleshoot IPv4 and IPv6 access list for traffic filtering
6.3.a Standard
6.3.b Extended
6.3.c Named
6.4 Verify ACLs using the APIC-EM Path Trace ACL Analysis tool
6.5 Configure, verify, and troubleshoot basic device hardening
6.5.a Local authentication
6.5.b Secure password
6.5.c Access to device
6.5.c. (i) Source address
6.5.c. (ii) Telnet/SSH
6.5.d Login banner
6.6 Describe device security using AAA with TACACS+ and RADIUS

10% 7.0 Infrastructure Management
7.1 Configure and verify device-monitoring protocols
7.1.a SNMPv2
7.1.b SNMPv3
7.1.c Syslog
7.2 Troubleshoot network connectivity issues using ICMP echo-based IP SLA
7.3 Configure and verify device management
7.3.a Backup and restore device configuration
7.3.b Using Cisco Discovery Protocol or LLDP for device discovery
7.3.c Licensing
7.3.d Logging
7.3.e Timezone
7.3.f Loopback
7.4 Configure and verify initial device configuration
7.5 Perform device maintenance
7.5.a Cisco IOS upgrades and recovery (SCP, FTP, TFTP, and MD5 verify)
7.5.b Password recovery and configuration register
7.5.c File system management
7.6 Use Cisco IOS tools to troubleshoot and resolve problems
7.6.a Ping and traceroute with extended option
7.6.b Terminal monitor
7.6.c Log events
7.6.d Local SPAN
7.7 Describe network programmability in enterprise network architecture
7.7.a Function of a controller
7.7.b Separation of control plane and data plane
7.7.c Northbound and southbound APIs

CCNA VOICE – ĐÀO TẠO KỸ NĂNG TRIỂN KHAI VoIP TRONG HẠ TẦNG MẠNG DOANH NGHIỆP

VoIP (Voice over Internet Protocol) chính là bước tiến lớn trong viễn thông nói riêng và công nghệ thông tin nói chung. Với giải pháp áp dụng công nghệ VoIP giúp tiết kiệm được chi phí hơn so với vận hành mạng PSTN truyền thống, từ đó triển khai thêm các dịch vụ gia tăng nhằm tối ưu hóa lợi nhuận cho doanh nghiệp.



Một số ưu điểm của giải pháp VoIP khi áp dụng vào doanh nghiệp:

- Gọi điện miễn phí giữa các chi nhánh trên cùng một quốc gia hoặc các quốc gia khác nhau.
- Hỗ trợ cuộc gọi audio lẫn video trên các thiết bị dầu cuối.
- Hỗ trợ thực hiện cuộc gọi nhóm (conference) giữa nhiều người dùng khác nhau.
- Có thể kết nối với các nhà cung cấp dịch vụ Internet Phone để gọi quốc tế mà không cần nâng cấp thiết bị.
- Nhân viên từ xa có thể đăng nhập vào hệ thống để thực hiện các cuộc gọi nội bộ và nhận bất kỳ cuộc gọi từ bên ngoài ở bất kỳ đâu trên thế giới.
- Nhiều tính năng nổi trội như âm thoại tương tác (cơ chế trả lời tự động đa cấp) với người dùng, cuộc gọi hội nghị, tích hợp khả năng ghi âm cuộc gọi, gửi tin nhắn Voice Mail.
- Có thể dùng điện thoại bàn, điện thoại di động để gọi quốc tế giá rẻ thông qua tổng đài IP.
- Dễ dàng nâng cấp, có thể tích hợp nhiều ứng dụng khác.
- Dễ dàng di chuyển điện thoại giữa các phòng ban, chi nhánh mà không cần phải đi dây lại.

- Khóa học CCNA Voice là chứng chỉ ở cấp độ cơ bản về việc quản lý, triển khai các công nghệ thoại trên nền IP như tổng đài IP PBX, diện thoại IP, thiết bị cầm tay, điều khiển cuộc gọi và giải pháp hộp thư thoại.

Sau khi hoàn tất khóa học CCNA Voice tại VnPro bạn sẽ được trang bị kiến thức nền tảng và những tính năng dựa trên cấu trúc Cisco Unified Communication Callmanger Express với quy mô doanh nghiệp vừa và nhỏ (~450 users). Và những khái niệm và cấu hình cơ bản dựa trên kiến trúc Cisco Unified Communication Callmanger Server với quy mô doanh nghiệp lớn (~80000 users). Với Những kiến thức và thực hành lab thực tế giúp học viên có đủ tự tin triển khai giải pháp IP Telephony cho doanh nghiệp vừa và nhỏ.

Tìm hiểu thêm về lợi ích mà khóa học CCNA Voice mang lại, vui lòng liên hệ:

TRUNG TÂM TIN HỌC VNPRO

149/1D Ung Văn Khiêm, Phường 25, Quận Bình Thạnh, Tp. Hồ Chí Minh.

ĐT: 083 5124257 | Email: vnpro@vnpro.org

Hoặc:

Ms. Thanh Trâm: thanhtram@vnpro.org | 0949 246 829

Ms. Mỹ Trang: mytrang@vnpro.org | 0964 464 377

Ms. Lê Uyên: tranleuyen@vnpro.org | 0903 834 636

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:

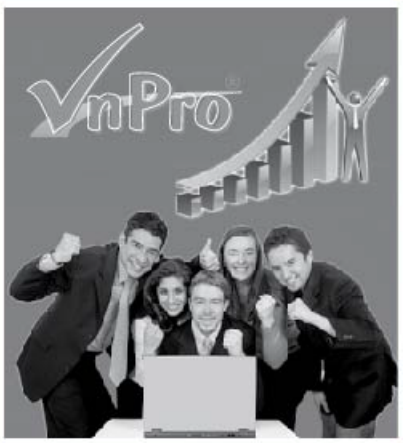
+ Tặng áo thun
+ Sách LabPro

Lớp chiều:

+ Lớp CCNAX thường: 2.900.000
+ Lớp CCNAX Hè: 3.360.000 – Tặng sách LabPro.

Lớp tối:

+ Ưu đãi 30% Học phí dành cho Sinh Viên
+ Ưu đãi 10% Học phí dành cho Học viên cũ.
+ Ưu đãi dành cho khách hàng doanh nghiệp.
+ Tặng Balo, giáo trình khi đăng ký học

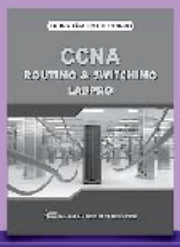


Cam kết lợi ích khi học tại VnPro

- 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.

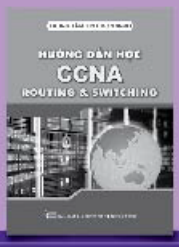
Là trung tâm duy nhất trong cả nước phát hành hơn 20 quyển sách mạng LabPro tiếng Việt. Giáo trình VnPro dược cập nhật, nâng cấp thường xuyên theo chuẩn giáo trình quốc tế

GIẢM* NGAY 10%

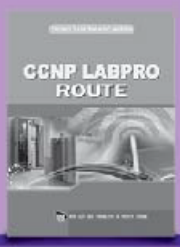


CCNA Routing & Switching
Giá: 150.000 VNĐ

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

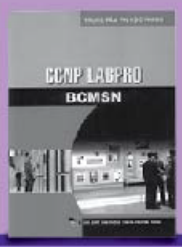
CCNP LABPRO TSHOOT
Giá: 120.000 VNĐ

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

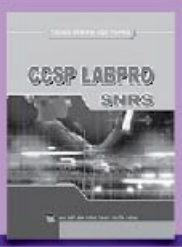


CCNP LABPRO BCMSN
Giá: 70.000 VNĐ

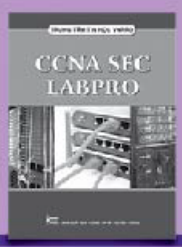
CCNP LABPRO ISCW
Giá: 120.000 VNĐ

CCSP LABPRO SNAF & SNAA
Giá: 120.000 VNĐ

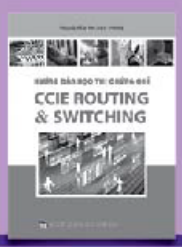
CCSP LABPRO IPS & CSMARS
Giá: 90.000 VNĐ



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/***

NHỮNG VỊ TRÍ CÔNG VIỆC BẠN CÓ THỂ ĐẢM NHẬN KHI THEO NGHỀ NETWORK

VnPro thường xuyên nhận được câu hỏi từ rất nhiều bạn từ khắp nơi ở Việt Nam là: "Sau khi học Network xong mình sẽ làm gì? Làm việc ở đâu và làm những cái gì?". Để giải đáp những thắc mắc đó của tất cả các bạn, VnPro sẽ tổng hợp tất cả những vị trí mà các bạn có thể đảm nhận khi theo học quản trị mạng.

Quản trị mạng (IT Admin)

Vị trí này là quản trị một hệ thống mạng đã có sẵn trong doanh nghiệp. Đối với các doanh nghiệp lớn thì đã có sự phân công công việc một cách rất rõ ràng, nhưng đối với các doanh nghiệp vừa và nhỏ đôi khi vị trí này có thể kiêm rất nhiều công việc thậm chí kiêm luôn vai trò IT Helpdesk.

Vị trí làm việc này rất phù hợp với các bạn sinh viên mới ra trường, cần tích lũy thêm kinh nghiệm.

Các công ty SI (System Integrated)

Các công ty SI cung cấp cho khách hàng các gói dịch vụ về giải pháp, triển khai, hỗ trợ kỹ thuật và phân phối thiết bị. Các công ty SI tiêu biểu ở Việt Nam như: FPT, CMC, Sao Bắc Đẩu, …

Những vị trí khi làm việc tại một công ty SI người kỹ sư mạng có thể đảm nhận như:

- *Sales: Vị trí này đòi hỏi người kỹ sư mạng ngoài chuyên môn về kỹ thuật ở mức độ cơ bản cần có thêm các yếu tố khác như: kỹ năng giao tiếp, kỹ năng bán hàng, năng động và đặc biệt là phải có khiếu nói chuyện.*
- *Pre-Sales: Vị trí này được coi là rất quan trọng trong quy trình tư vấn giải pháp của một công ty SI. Các Pre-Sales phải là những người có kinh nghiệm lâu năm với vốn kiến thức chuyên môn cực tốt. Từ đó đưa ra giải pháp phù hợp với từng đối tượng khách hàng khác nhau. Phù hợp với những người đã có kinh nghiệm làm việc chuyên môn từ 3-5 năm.*
- *Port-Sales: Vị trí này hay còn gọi là nhân viên triển khai. Khi làm việc ở vị trí này tại các công ty SI bạn sẽ có cơ hội được làm việc trực tiếp tại môi trường thực tế, đòi hỏi bạn phải chịu đi công tác xa dài ngày. Vị trí này rất thích hợp với các bạn sinh viên mới ra trường muốn trải nghiệm công việc và không ngại khó khăn.*

Các công ty Dịch Vụ

Các công ty cung cấp dịch vụ công nghệ thông tin cho các doanh nghiệp: bảo trì, quản trị, triển khai… Những công ty dịch vụ khá nổi tiếng ở Việt Nam như: KDDI, NTT, CSC,… Làm việc tại môi trường này người kỹ sư mạng sẽ có cơ hội học tập để nâng cao kinh nghiệm của mình. Vị trí này phù hợp với sinh viên mới ra trường cần môi trường học tập tích lũy kinh nghiệm.

Kỹ sư sản phẩm cho các Distributor hoặc Vendor

Đây được coi là vị trí được rất nhiều người kỹ sư mạng đặt cho mình mục tiêu. Bởi lẽ vị trí này bạn sẽ được làm việc cho các Vendor rất nổi tiếng như: Cisco, Microsoft, Juniper, HP, … Hoặc các Distributor như FPT, Sao Bắc Đẩu, … Những người làm việc ở vị trí này phải cập nhật thông tin về các dòng sản phẩm mới của hãng hoặc phải nghiên cứu và nắm vững, sử dụng thành thạo các thiết bị của hãng.

Vị trí này đòi hỏi bạn phải có kiến thức chuyên môn cực tốt, nắm vững các nguyên lý hoạt động cũng như là thông số kỹ thuật của các dòng sản phẩm. Vị trí này thường đòi hỏi kinh nghiệm phải từ 3-5 năm.

Các công ty ISP (Internet Service Provider)

Nếu bạn có khao khát được làm việc trong một hệ thống mạng lớn chuyên cung cấp dịch vụ hạ tầng mạng như: truy cập Internet, kênh thuê riêng, … thì các ISP là điểm đến rất lý tưởng. Các ISP nổi tiếng ở Việt Nam như: FPT, VNPT, Viettel, …

Các ISP cũng là những điểm đến lý tưởng cho các bạn sinh viên mới ra trường muốn tích lũy thêm kinh nghiệm.

Trên đây chỉ là một vài vị trí bạn có thể đảm nhận khi theo đổi nghề Network. Ngoài ra còn rất nhiều vị trí chuyên môn cho đến quản lý khác mà bạn có thể đảm nhận khác nữa. Tuy vậy dù là công việc nào thì cũng cần phải có cái TÂM và ĐAM MÊ nếu không bạn sẽ rất khó để theo đuổi.

Bộ phận Marketing – Phòng Kinh Doanh

HỌC KỸ THUẬT HAY KINH TẾ ?

Giống như tiêu đề bài viết, VnPro muốn gửi gắm đến những bạn đang chuẩn bị lựa chọn cho mình một ngành nghề mà biết đâu mình sẽ gắn bó suốt cả cuộc đời.

CEO của Word Link Japan INC ông Ito Junichi cho biết: "Nếu bắt đầu với công việc nhỏ, lao động chân tay, làm những việc kỹ thuật, thì khi làm trên mức độ quản lý, hay kinh doanh, có thể nắm bắt và hiểu rõ cốt lõi của vấn đề đồng thời xử lý tốt hơn những người chỉ học lý thuyết, tưởng tượng".

Hiện nay, hầu hết các học sinh cấp 3 ở Việt Nam đều thiếu mất đi định hướng nghề nghiệp, điều đó dẫn đến khi bước chân vào Đại Học vẫn không biết rằng sau này ra trường sẽ làm gì và làm như thế nào. Song song với việc đó là lựa chọn nghề nghiệp tương lai theo xu thế, thú vui mà quên mất đi một điều rất quan trọng là đam mê và sở thích. Kinh tế, ngân hàng, kế toán, … năm nào cũng đông, ra trường cũng rất nhiều, mà tỷ lệ thất nghiệp (hoặc làm trái nghề) theo như thống kê thì lên đến 63% theo thống kê của Bộ Giáo Dục.

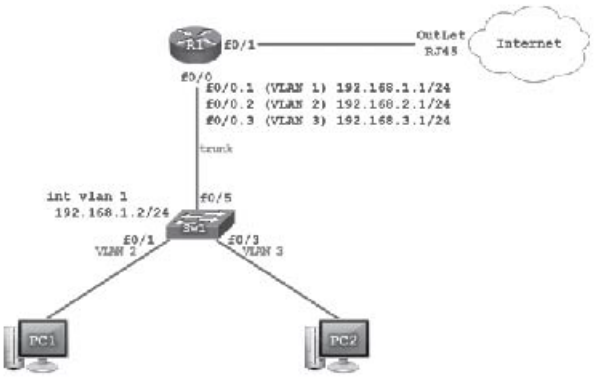
Một thống kê khác ở Bắc Mỹ cho thấy rằng từ năm 2004 đến 2014, việc làm về khoa học và kỹ thuật STEM tăng 26%, tức là gấp 2 lần so với tốc độ tăng trưởng trung bình của các ngành nghề khác (điều này thật sự rất khác biệt khi ở Việt Nam).

Việt Nam hiện nay nhận được sự đầu tư rất lớn từ các nước trên thế giới, bởi đây là thị trường hết sức tiềm năng. Đồng thời với nguồn nhân lực dồi dào thật sự là điểm đến tiềm năng của các tập đoàn lớn trên thế giới. Để có thể làm việc tại các công ty đa quốc gia này, ngoài vốn tiếng Anh cực tốt thì bạn cần phải giỏi trong chuyên môn của chính mình. Về các lĩnh vực kinh tế lại thiếu đi một sự minh chứng cần thiết, trong khi nếu bạn là một người kỹ thuật thì bằng cấp và các chứng chỉ Quốc Tế sẽ là điểm tựa vững chắc của bạn khi đối diện với nhà tuyển dụng.

Chốt lại, dù là bạn lựa chọn ngành nghề nào, kỹ thuật hay kinh tế điều quan trọng hơn cả chính là đam mê, yêu nghề và phù hợp với xu thế toàn cầu.

LAB DHCP over VLAN, DNS, ACL cấm truy cập facebook

KỲ 1



Cổng f0/1 của R1 sẽ tiến hành đấu nối tới OutLet trên tường (sử dụng cáp thẳng) để truy cập được đi Internet.

OutLet RJ45

Yêu cầu:

1. Cấu hình cơ bản trên các thiết bị.
2. VLAN:
   a. Tạo VLAN 2 trên Sw1, đặt tên cho VLAN 2 là PhongKinh Doanh, gom các port f0/1 tới f0/2 vào VLAN 2.
   b. Tạo VLAN 3 trên Sw1, đặt trên cho VLAN 3 là PhongKeToan, gom các port f0/3 tới f0/4 vào VLAN 3.
3. Trunk: Trên Sw1, cấu hình f0/5 thành đường trunk sử dụng kiểu đóng gói dot1q.
4. InterVLAN: Trên R1 tạo các sub-interface rồi liên kết các sub-interface vào VLAN tương ứng.
5. DHCP:
   a. Cấu hình DHCP Server trên R1 cấp IP xuống cho các PC và thiết bị thuộc mạng VLAN 2 dải IP thuộc lớp mạng 192.168.2.0/24.
   b. Cấu hình DHCP Server trên R1 cấp IP xuống cho các PC và thiết bị thuộc mạng VLAN 3 dải IP thuộc lớp mạng 192.168.3.0/24.
   c. Cấu hình DHCP Client trên cổng f0/1 xin IP từ Router tại VnPro.
6. NAT: Cấu hình NAT Overload trên R1 đảm bảo các PC thuộc VLAN 1 và VLAN 2 có thể truy cập Internet.
7. HTTP: Cấu hình R1 trở thành HTTP Server.
8. DNS: Cấu hình R1 trở thành DNS Server phân giải tên miền www.facebook.com thành IP 192.168.2.1 để chuyển hướng lưu lượng của người dùng từ trang www.facebook.com sang website của R1 là 192.168.2.1.
9. ACL: Cấu hình ACL trên R1 cấm các PC thuộc VLAN 2 truy cập www.facebook.com, VLAN 3 vẫn có thể truy cập www.facebook.com bình thường.

Thực hiện:

Yêu cầu 1: Cấu hình cơ bản trên các thiết bị (đặt IP trên các cổng giao tiếp, cấu hình cơ chế chống trôi dòng lệnh "logging synchronous", cấu hình bỏ qua cơ chế phân giải tên miền "no ip domain-lookup").

Ý nghĩa của câu lệnh "exec-timeout 0 0": Khi đang cấu hình tại giao diện console (Hyperterminal, Putty hoặc SecureCRT), nếu sau một khoảng thời gian nhất định mà người quản trị không gõ lệnh nào cũng như không thực hiện bất kỳ thao tác nào thì phiên truy cập console sẽ tự động bị "logout", người quản trị sẽ phải đăng nhập lại để tiến hành cấu hình. Câu lệnh "exec-timeout 0 0" dùng để tắt cơ chế tự động "logout".

Mặc định các Cisco Switch sử dụng giao thức STP (PVST+), để tăng thời gian hội tụ của hệ thống mạng, ta có thể chỉnh giao thức RSTP (PVRST+) trên các Switch bằng câu lệnh "spanning-tree mode rapid-pvst". RSTP sẽ được tìm hiểu trong những bài học sau.

Trong bài LAB này, ta nên tiến hành cấu hình tính năng "spanning-tree portfast" cho các Port từ f0/1 tới f0/6 của Sw1.

Câu lệnh "spanning-tree portfast" dùng để tăng thời gian hội tụ của hệ thống lên. Thông thường, khi PC kết nối vào một port của Switch, đèn tín hiệu trên port lập tức chuyển thành màu cam. Port sẽ ở trạng thái màu cam trong vòng khoảng 30 giây để tính toán chống "loop" bằng giao thức STP trước khi chuyển sang màu xanh lá. Trong suốt khoảng thời gian 30 giây ở trạng thái màu cam, port không thể gửi hoặc nhận dữ liệu được nên người dùng PC cần phải đợi ít nhất là 30 giây thì mới bắt đầu truy cập vào hệ thống mạng được. Câu lệnh "spanning-tree portfast" sau khi được cấu hình trên cổng sẽ bỏ qua 30 giây ở trạng thái màu cam và lập tức chuyển sang màu xanh lá nên người dùng mạng user có thể gửi nhận dữ liệu liền mà không cần phải chờ đợi. Tính năng "spanning-tree portfast" chỉ nên cấu hình trên các port đấu nối xuống PC, không nên cấu hình tính năng "spanning-tree portfast" trên các port đóng vai trò là đường trunk. Công nghệ Trunk, STP sẽ được tìm hiểu trong những bài học sau.

```
Sw1(config)# interface range f0/1 - 4
Sw1(config-if-range)# switchport mode access
Sw1(config-if-range)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast will be configured in 4 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
Sw1(config-if-range)# exit
Sw1(config)#
```

Cấu hình cơ bản trên Switch Sw1.

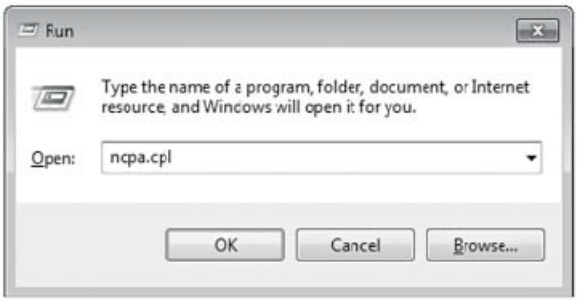
```
hostname Sw1
interface vlan 1
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.1.1
spanning-tree mode rapid-pvst
interface range f0/1 - 4
switchport mode access
spanning-tree portfast
exit
line vty 0 4
privilege level 15
no login
exit
line console 0
logging synchronous
exec-timeout 0 0
exit
no ip domain-lookup
```

Cấu hình cơ bản trên R1.

```
hostname R1
interface f0/0
no shutdown
exit
line vty 0 4
privilege level 15
no login
exit
line console 0
logging synchronous
exec-timeout 0 0
exit
no ip domain-lookup
```

Thiết lập PC trở thành DHCP Client xin IP động bằng câu lệnh thông qua chương trình cmd như sau.

Kiểm tra tên của card mạng bằng cách vào giao diện "Network Connections". Thực hiện nhấn tổ hợp phím Window + R rồi gõ tiếp command line "ncpa.cpl".



Tại giao diện "Network Connections", quan sát tên của card mạng hiện tại là "Local Area Connection".

Thiết lập PC trở thành DHCP Client xin IP động bằng câu lệnh thông qua chương trình cmd. Phải đảm bảo kết nối cáp và tín hiệu đèn đã sáng mới tiến hành gõ lệnh.

Cách 1: Thiết lập PC trở thành DHCP Client xin IP động từ DHCP Server.

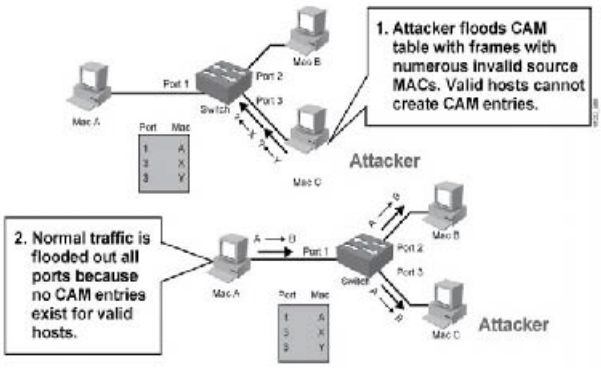
```
C:\PC> netsh
netsh> interface ip
netsh interface ipv4> set address name= "Local Area Connection" source=dhcp

netsh interface ipv4> exit
C:\PC>
```

Cách 2: Thiết lập PC trở thành DHCP Client xin IP và DNS động từ DHCP Server.

```
C:\PC> netsh interface ip set address name="Local Area Connection" dhcp
C:\PC> netsh interface ip set dns name="Local Area Connection" dhcp
```

Chống MAC Layer Attack trên Switch



Bảng CAM (Content Addressable Memory) lưu trữ các địa chỉ MAC của các port, và các tham số VLAN trong switch. Không gian nhớ trong bảng CAM là hạn chế nên có nguy cơ tràn bảng CAM. Kiểu tấn công làm tràn MAC sẽ cố gắng làm tràn bảng CAM của các switch, khi đó switch sẽ cư xử như các hub. Một cuộc tấn công kiểu này trông giống như lưu lượng từ hàng ngàn máy tính được chuyển đến một port, nhưng thực tế là nó chỉ đến từ một máy giả mạo địa chỉ MAC của hàng ngàn host giả mạo.

VD: Macof là một công cụ thông dụng để thực hiện các cuộc tấn công kiểu này, có thể tạo ra hàng chục ngàn MAC entry gửi đến port mỗi phút. Khi đó, switch nhìn thấy lưu lượng và nghĩ rằng các địa chỉ MAC từ các gói mà kẻ tấn công gửi đi là các cổng hợp lệ và nó sẽ thêm entry vào bảng CAM. Khi tràn bảng CAM, switch sẽ broadcast lưu lượng trên VLAN mà ko cần thông qua bảng CAM nữa.

Tấn công làm ngập lụt bảng MAC là 1 trong những kĩ thuật tấn công phổ biến nhất ở Layer 2. Trong kiểu tấn công này thì Switch đã bị lụt với các gói tin của các địa chỉ MAC khác nhau, do đó làm tiêu hao bộ nhớ trong Switch, lúc này Switch sẽ trở thành Hub. Do đó người dùng bất hợp pháp có thể sử dụng 1 công cụ Packet Sniffer để thâu tóm các dữ liệu nhạy cảm. Sau đây sẽ là mô hình mô phỏng cuộc tấn công MAC Flooding.

Nguyên tắc phòng chống: Nguyên lí chung của các phương pháp phòng chống là không để các gói tin có địa chỉ MAC lạ đi qua switch. Phương pháp phòng chống hiệu quả nhất là cấu hình port security trên switch. Đây là một đặc trưng cấu hình cho phép điều khiển việc truy cập vào cổng switch thông qua địa chỉ MAC của thiết bị gắn vào.

Khi switch nhận được một gói tin chuyển đến, nó sẽ kiểm tra địa chỉ MAC nguồn của gói tin với danh sách các địa chỉ đã được cấu hình trước đó. Nếu hai địa chỉ này khác nhau thì tuỳ theo sự cấu hình của người quản trị mà switch sẽ xử lí gói tin đến với các mức độ khác nhau.

Cấu hình Port Security

Các lệnh cấu hình port security:

• Switch(config-if)# switchport mode access

• Switch(config-if)# switchport port-security: cho phép cổng được hoạt động trong chế độ port-security.

• Switch(config-if)# switchport port-security maximum value (tuỳ chọn): câu lệnh cho phép cấu hình số địa chỉ MAC tối đa mà cổng có thể học tự động và cho phép các thiết bị này truyền dữ liệu qua. Mặc định thì cổng chỉ cho phép một địa chỉ MAC (một thiết bị) được gán vào và số địa chỉ có thể nằm trong khoảng từ 1 đến 1024.

• Switch(config-if)# switchport port-security mac-address mac_address (tuỳ chọn) : bên cạnh cách cấu hình cho phép switch học tự động địa chỉ MAC; có thể gán tĩnh một số địa chỉ MAC có thể truy cập vào một port. Nếu số lượng địa chỉ gán tĩnh mà nhỏ hơn số địa chỉ MAC switch có thể học tự động thì số địa chỉ MAC còn lại sẽ được học tự động.

• Switch(config-if)# switchport port-security violation {protect | restrict | shutdown} (tuỳ chọn) : Đây là các biện pháp mà người quản trị có thể tiến hành khi một gói tin đến không phù hợp với yêu cầu của port-security (khi có nhiều hơn số địa chỉ MAC tối đa được học hoặc khi gói tin đến có địa chỉ MAC khác so với các địa chỉ MAC đã được cấu hình tĩnh). Các biện pháp xử lí có thể là :

1. shutdown: cổng sẽ bị ngừng hoạt động; không nhận và chuyển gói tin.
2. restrict: cổng chỉ cho phép các gói tin có địa chỉ MAC hợp lệ đi qua; các gói tin vi phạm sẽ bị huỷ. Đồng thời số lượng các bản tin vi phạm sẽ được thống kê và báo cho người quản trị biết.
3. protect: cũng giống như trong trường hợp restrict, tuy nhiên việc vi phạm sẽ không được ghi lại.

Phương pháp này tuy có yêu cầu công việc của người quản trị tăng lên đôi chút tuy nhiên nó là phương pháp rất hiệu quả để khoá các gói tin không rõ nguồn gốc có ý định tấn công vào switch.

Đào Lê Hoàng – VnPro

VLAN Attack và Spoofing Attack trên Switch

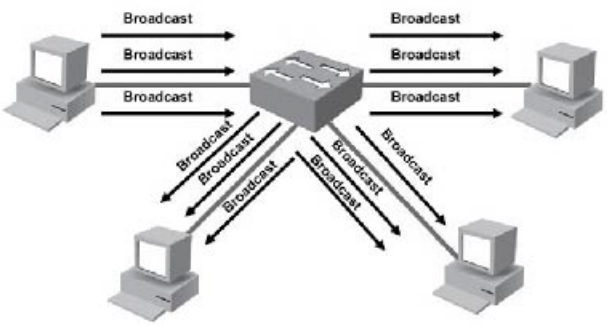
1. VLAN Attack

Đầu tiên ta nghiên cứu về khái niệm địa chỉ MAC. Địa chỉ MAC (Media Access Control) là kiểu địa chỉ vật lí, đặc trưng cho một thiết bị hoặc một nhóm các thiết bị trong mạng LAN. Địa chỉ này được dùng để nhận diện các thiết bị giúp cho các gói tin lớp 2 có thể đến đúng đích.

Một địa chỉ MAC bao gồm 6 byte và thường được viết dưới dạng hexa, với các thiết bị của Cisco, địa chỉ này được viết dưới dạng số hexa, ví dụ: 0000.0C12.FFFF là một địa chỉ MAC hợp lệ. Để đảm bảo địa chỉ MAC của một thiết bị là duy nhất, các nhà sản xuất cần phải ghi địa chỉ đó lên ROM của thiết bị phần cứng và định danh của nhà sản xuất sẽ được xác định bởi 3 byte đầu OUI (Organizationally Unique Identifier).

Địa chỉ MAC được phân làm 3 loại

+ Unicast: đây là loại địa chỉ dùng để đại diện cho một thiết bị duy nhất.
+ Multicast: đây là loại địa chỉ đại diện cho một nhóm các thiết bị trong mạng LAN. Địa chỉ được dùng trong trường hợp một ứng dụng có thể muốn trao đổi với một nhóm các thiết bị. Bằng cách gửi đi một bản tin có địa chỉ multicast; tất cả các thiết bị trong nhóm đều nhận và xử lí gói tin trong khi các thiết bị còn lại trong mạng sẽ bỏ qua. Giao thức IP cũng hỗ trợ truyền multicast. Khi một gói tin IP multicast được truyền qua một mạng LAN, địa chỉ MAC multicast tương ứng với địa chỉ IP sẽ là 0100.5exxx.xxxx.
+ Broadcast: địa chỉ này đại diện cho tất cả các thiết bị trong cùng một mạng LAN. Điều đó cũng có nghĩa là nếu một gói tin có địa chỉ MAC là FFFF.FFFF.FFFF được gửi đi thì tất cả các thiết bị trong mạng LAN đều phải thu nhận và xử lí. Khi mà các địa chỉ MAC này,nhất là các địa chỉ broadcast được gửi đi ngập khắp các port trong mạng (cả kể trên các Vlan) dẫn đến đẩy hiệu suất của CPU lên gần đến 100%, làm giảm đi hiệu năng sử dụng của CPU trên Switch



Để kiểm soát "Storm" ta có thể sử dụng các chức năng được cấu hình sẵn trên các dòng Switch của Cisco bằng các dòng lệnh với cú pháp như sau:

+ Switch(config-if)#storm-control{{broadcast|multicast-|unicast} level {level [level low] |bps bps [bps-low]|pps pps [pps-low]}}|{action {shutdown|trap}}
+ Switch(config-if)#storm-control broadcast level 75.5
+ Switch(config-if)#storm-control multicast level pps 2k 1k
+ Switch(config-if)#storm-control action shutdown

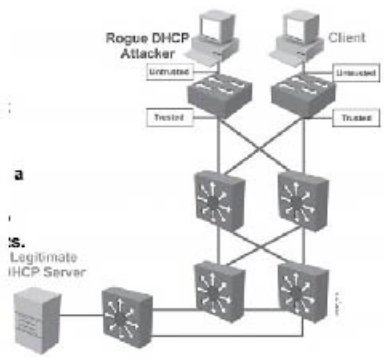
2. Spoofing Attack

Ngày nay, phần lớn user thực hiện request ip qua dhcp server. DHCP server nhận được request của client và response request bao gồm (ip, subnet mac, getway, dns) gửi tới client.

Tuy nhiên, nếu hacker kết nối 1 dhcp server giả vào mạng, và thực hiện response dhcp request cho client. Nếu trong mô hình mạng có 2 con dhcp, thì con nào gần client hơn sẽ response gói tin dhcp request của client trước. ở đây dhcp server sẽ trả lời gói tin request của người dùng trc vì nó gần client hơn.

Mục đích của tấn công dhcp snoofing là làm thay đổi cấu trúc của gói dhcp respon của dhcp server thật. DHCP giả sẽ trả lời các thông số ip và gateway có thể là gateway của attacker để khi người dùng request dhcp thành công, mọi traffic đều đi qua máy của hacker ,hacker có thể bắt tất cả các traffic qua nó, ngoài ra còn gây hỗn loạn mạng.

Tính năng DHCP snooping trên switch cisco có thể được sử dụng để chống lại tấn công dhcp server spoofing. Với giải pháp này, SW Cisco được cấu hình trên 2 trạng thái port, là trusted và untrusted. Nếu port ở trạng thái trusted, nó cho phép nhận dhcp response, còn nếu ở trạng thái untrust thì nó ko cho phép nhận dhcp response. Và nếu port ở trạng thái untrusted nó ko cho phép nhận dhcp response, và nếu 1 dhcp response được thực hiệnv và untrusted port thì port sẽ bị disable.



Cấu hình DHCP Snooping

+ Switch(config)#ip dhcp snooping
+ Switch(config)#ip dhcp snooping information option
+ Switch(config)#ip dhcp snooping trust
+ Switch(config)#ip dhcp snooping limit rate [rate]
+ Switch(config)#ip dhcp snooping vlan number [number]

Đào Lê Hoàng – VnPro

TẤT TẦN TẬT VỀ GIỚI TỪ TIẾNG ANH

1. Định nghĩa

Giới từ là từ loại chỉ sự liên quan giữa các từ loại trong cụm từ, trong câu. Những từ thường đi sau giới từ là tân ngữ (Object), Verb + ing, Cụm danh từ ... Ví dụ:

• I went into the room.

• I was sitting in the room at that time.

Ta thấy rõ, ở ví dụ a., "the room" là tân ngữ của giới từ "into". Ở ví dụ b., "the room" là tân ngữ của giới từ "in".Chú ý: Các bạn phải luôn phân biệt trạng từ và giới từ, vì thường khi một từ có hai chức năng đó (vừa là trạng từ và giới từ). Điều khác nhau cơ bản là Trạng từ thì không có tân ngữ theo sau.

2. Cách sử dụng giới từ trong tiếng Anh

Có thể nói việc dùng các giới từ không phải dễ, vì mỗi nước có cách dùng giới từ đặc biệt; vậy ta phải rất chú ý đến nó ngay từ lúc mới học môn ngoại ngữ đó nói chung và tiếng Anh nói riêng. Trong tiếng Anh, người ta không thể đặt ra các quy luật về các phép dùng giới từ mang tính cố định cho mỗi giới từ đó - cùng một giới từ, khi đi với từ loại khác nhau thì tạo ra nghĩa khác nhau. Vậy chúng ta nên học thuộc mỗi khi gặp phải và học ngay từ lúc ban đầu.

3. Vị trí của giới từ

a) Sau TO BE, trước danh từ

+ THE BOOK IS ON THE TABLE. = Quyển sách ở trên bàn.

+ I WILL STUDY IN AUSTRALIA FOR 2 YEARS. = Tôi sẽ học ở Úc trong 2 năm.

b) Sau động từ: Có thể liền sau động từ, có thể bị 1 từ khác chen giữa động từ và giới từ.

+ I LIVE IN HO CHI MINH CITY = Tôi sống ở thành phố Hồ Chí Minh.

+ TAKE OFF YOUR HAT! Cởi nón của bạn ra!

+ I HAVE AN AIR-CONDITIONER, BUT I ONLY TURN IT ON IN SUMMER. = Tôi có máy lạnh, nhưng tôi chỉ bật nó lên vào mùa hè.

c) Sau tính từ:

+ I'M NOT WORRIED ABOUT LIVING IN A FOREIGN COUNTRY. = Tôi không lo lắng về việc sốngở nước ngoài.

+ HE IS NOT ANGRY WITH YOU. = Anh ấy không giận bạn.

4. Một số sai lầm thường gặp khi sử dụng giới từ

a) Suy luận từ cách dùng đã gặp trước đó.

Ví dụ: Trước đó ta gặp: worry about: lo lắng về Lần sau gặp chữ: disscuss _____ (thảo luận về) thế là ta suy ra từ câu trên mà điền about vào, thế là sai.

b) Không nhận ra là giới từ thay đổi vì thấy cùng một danh từ:

Ví dụ:Trước đó ta gặp: in the morning Thế là khi gặp: ___ a cold winter morning, thấy morning nên chọn ngay in => sai (đúng ra phải dùng on)

c) Bị tiếng Việt ảnh hưởng: Tiếng Việt nói: lịch sự với ai nên khi gặp: polite (lịch sự) liền dùng ngay with (với) => sai (đúng ra phải dùng to)

5. Hình thức của giới từ

a) Giới từ đơn (simple prepositions): Là giới từ có một chữ: in, at, on, for, from, to, under, over, with …

b) Giới từ đôi (doubleprepositions): Là giới từ được tạo ra bằng cách hợp 2 giới từ đơn lại: Into, onto, upon, without, within, underneath, throughout, from among…

- Ex: The boy runs into the room (thằng bé chạy vào trong phòng)

- Ex: He fell onto the road (anh ta té xuống đường)

- Ex: I chose her from among the girls (tôi chọn cô ấy từ trong số các cô gái)

c) Giới từ kép (compound prepositions): Là giới từ được tạo thành bằng tiếp đầu ngữ a hoặc be: About, among, across , amidst, above, against, Before, behind, beside, beyond, beneath, between, below…

d) Giới từ do phân từ (participle prepositions): According to (tùy theo), during (trong khoảng), owing to (do ở), pending (trong khi) , saving = save = except (ngoại trừ), notwithstanding (mặc dù) , past (hơn, qua) considering (xét theo) concerning/ regarding /touching (về vấn đề, về), excepting = except (ngoại trừ)

- Ex: She is very intelligent, considering her age. (xét theo tuổi thì cô ấy rất thông minh)

e) Cụm từ được dùng như giới từ: Giới từ loại này bao gồm cả một cụm từ:

- Because of (bởi vì)

- By means of (do, bằng cách)

- In spite of (mặc dù)

- In opposition to (đối nghịch với)

- On account of (bởi vì)

- In the place of (thay vì)

- In the event of (nếu mà)

Ex: In the event of my not coming, you can come home.(nếu mà tôi không đến thì anh cứ về)

- With a view to (với ý định để)

Ex: I learn English with the view of going abroad.(tôi học TA với ý định đi nước ngoài)- For the shake of (vì)_Ex: I write this lesson for the shake of your progress. (tôi viết bài này vì sự tiến bộ của các bạn)

- On behalf of (thay mặt cho)

Ex: On behalf of the students in the class, I wish you good health (thay mặt cho tất cả học sinh của lớp, em xin chúc cô được dồi dào sức khỏe)

- In view of (xét về)

Ex: In view of age, I am not very old. (xét về mặt tuổi tác, tôi chưa già lắm)

- With reference to (về vấn đề, liên hệ tới)_Ex: I send this book to you with reference to my study.(tôi đưa bạn quyển sách này có liên hệ đến việc học của tôi.) 6) Giới từ trá hình: Đây là nhóm giới từ được ẩn trong hình thức khác: At 7 o'clock (o' = of): Lúc 7 giờ

6. Các loại giới từ thường gặp

1) Giới từ chỉ thời gian:

- At: vào lúc (thường đi với giờ)
- On: vào (thường đi với ngày)
- In: vào (thường đi với tháng, năm, mùa, thế kỷ)
- Before: trước - After: sau
- During: (trong khoảng) (đi với danh từ chỉ thời gian)

2) Giới từ chỉ nơi chốn:

- At: tại (dùng cho nơi chốn nhỏ như trường học, sân bay...)
- In: trong (chỉ ở bên trong) , ở (nơi chốn lớn thành phố, tỉnh ,quốc gia, châu lục...)
- On,above,over: trên
- On: ở trên nhưng chỉ tiếp xúc bề mặt.

3) Giới từ chỉ sự chuyển dịch:

- To, into, onto: đến
+ to: chỉ hướng tiếp cận tới người,vật,địa điểm.
+ into: tiếp cận và vào bên trong vật,địa điểm đó
+ onto: tiếp cận và tiếp xúc bề mặt,ở phía ngoài cùng của vật,địa điểm
- From: chỉ nguồn gốc xuất xứ Ex: i come from vietnamese
- Across: ngang qua Ex: He swims across the river. (anh ta bơi ngang qua sông)
- Along: dọc theo- Round,around,about: quanh

4) Giới từ chỉ thể cách:

- With: với
- Without: không, không có
- According to: theo
- In spite of: mặc dù
- Instead of: thay vì

5) Giới từ chỉ mục đích:

- To: để
- In order to: để
- For: dùm, dùm cho- Ex: Let me do it for you: để tôi làm nó dùm cho bạn.
- So as to: để

6) Giới từ chỉ nguyên do:

- Thanks to: nhờ ở - Ex: Thanks to your help, I passed the exam (nhờ sự giúp đỡ của bạn mà tôi thi đậu).
- Through: do, vì- Ex: Don't die through ignorance (đừng chết vì thiếu hiểu biết).
- Because of: bởi vì - Owing to: nhờ ở, do ở- Ex: Owing to the drought,crops are short (vì hạn hán nên mùa màng thất bát)
- By means of: nhờ, bằng phương tiện

12 ĐẶC ĐIỂM CỦA MỘT NGƯỜI SẾP TUYỆT VỜI

1. Suy nghĩ tích cực
Hiểu được sức mạnh của tâm lý tích cực, luôn nhìn thấy cơ hội ở mọi tình huống.

2. Trung thực
Hãy trung thực và luôn nói với nhân viên của mình sự thật, cho dù có thể khiến họ tổn thương.

3. Uỷ thác
Biết khi nào nên để cho nhân viên tự xử lý công việc, không độc đoán kiểm soát từng ly từng tý một.

4. Giao tiếp
Ở nhiều đơn vị và tổ chức, có quá nhiều rắc rối xảy ra chỉ vì thiếu sự giao tiếp giữa sếp và nhân viên.

5. Tạo cảm hứng
Tạo cảm hứng cho các nhân viên của mình, khiến họ có thêm nhiệt huyết và đam mê với công việc và công ty.

6. Chỉnh đốn đội ngũ
Giữ cho tất cả mọi người đoàn kết, đồng lòng vì một mục tiêu dài hạn.

7. Giữ cân bằng
Con người làm việc hiệu quả nhất khi họ biết cân bằng giữa công việc và cuộc sống riêng tư.

8. Tin tưởng
Thể hiện sự tin tưởng đối với nhân viên sẽ khiến các nhân viên cảm thấy tự tin hơn.

9. Khuyến khích p.triển
Khuyến khích nhân viên phát triển bản thân, họ sẽ trở nên hiệu quả hơn.

10. Khen ngợi
Thể hiện sự biết ơn của bạn, cho dù những việc làm của nhân viên là rất nhỏ.

11. Cố vấn
Thay vì ra lệnh cho nhân viên phải làm gì, hãy làm mẫu hoặc hướng dẫn cho nhân viên cách làm việc đó.

12. Công bằng
Việc thiên vị cho 1 cá nhân nào đó sẽ khiến cho những người khác mất tinh thần, thậm chí cảm thấy ganh tị.

BONUS

MỘT NGƯỜI SẾP TUYỆT VỜI CŨNG

13. THƯỜNG XUYÊN CHIA SẺ NHỮNG ĐIỀU TUYỆT VỜI

Luôn chia sẻ những điều tuyệt vời bạn biết cho nhân viên của bạn, như infographic này chẳng hạn, điều đó giúp cho sếp và nhân viên hiểu nhau hơn và làm việc đạt kết quả cao hơn, khiến các nhân viên luôn yêu và gắn bó với công ty.

SINH VIÊN -30%

HỌC VIÊN CŨ -20%

KHÁCH HÀNG DN

LỊCH KHAI GIẢNG
THÁNG 6

Mã lớp	Tên khóa học	Ngày khai giảng	Ngày học	Giờ học	Học phí/khóa	Thời gian
CHƯƠNG TRÌNH CCNA						
A5	CCNAX	02/06	3 – 5 - 7	6:30 – 9:30PM	6.720.000	152 giờ
AK5		09/06	3 – 5 - 7	8:30 – 11:30AM	3.360.000	
A7				6:30 – 9:30PM	6.720.000	
AK8		17/06	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
AK10				6:30 – 9:30PM	6.720.000	
AK9		21/06	3 – 5 - 7	2:00 – 5:00PM	2.900.000	
A9				6:30 9:30PM	6.720.000	
AK12		29/06	2 – 4 – 6	8:30 – 11:30AM	3.360.000	
AK14				2:00 – 5:00PM	2.900.000	
A6				6:30 – 9:30PM	6.720.000	
AK11	CCNAX HÈ	09/06	3 – 5 - 7	Sáng + Chiều	3.360.000	
AK13		20/06	2-3-4-5-6-7	Chiều	3.360.000	
AS5	CCNA Security (640-554)	16/06	3 – 5 – 7	6:30 – 9:30PM	5.500.000	72 giờ
AV5	CCNA Voice (640-461)	16/06	3 – 5 – 7	6:30 – 9:30PM	6.720.000	100 giờ
CHƯƠNG TRÌNH CCNP						
P1K1	ROUTE (300 - 101)	09/06	3 – 5 – 7	8:30 – 11:30AM	5.880.000	120 giờ
P1-3				6:30 – 9:30PM	8.232.000	
P2-K3	SWITCH (300 115)	17/06	2 – 4 – 6	8:30 – 11:30AM	5.880.000	120 giờ
P2-5				6:30 – 9:30PM	8.232.000	
P3 2	TSHOOT (300 - 135)	01/06	2 – 4 – 6	6:30 – 9:30PM	8.232.000	120 giờ
CHƯƠNG TRÌNH CCIE WRITTEN						
EW2	CCIE WRITTEN (Version 5)	01/06	2 – 4 – 6	6:30 – 9:30PM	11.760.000	120 giờ
KHÓA HỌC CHUYÊN ĐỀ						
PS1-1	FIREWALL	18/06	Thứ 7	Sáng + Chiều	5.500.000	54 giờ
PS1-3	VPN	21/06	3 – 5 – 7	6:30 – 9:30PM	5.500.000	54 giờ
PS1-5	MPLS Nguyên Lý & Ứng Dụng	16/06	3 – 5 – 7	2:00 – 5:00PM	5.500.000	54 giờ
PS1-7		28/06	3 – 5 – 7	6:30 – 9:30PM	5.500.000	

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 Tell: (08) 3 5124 257

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**