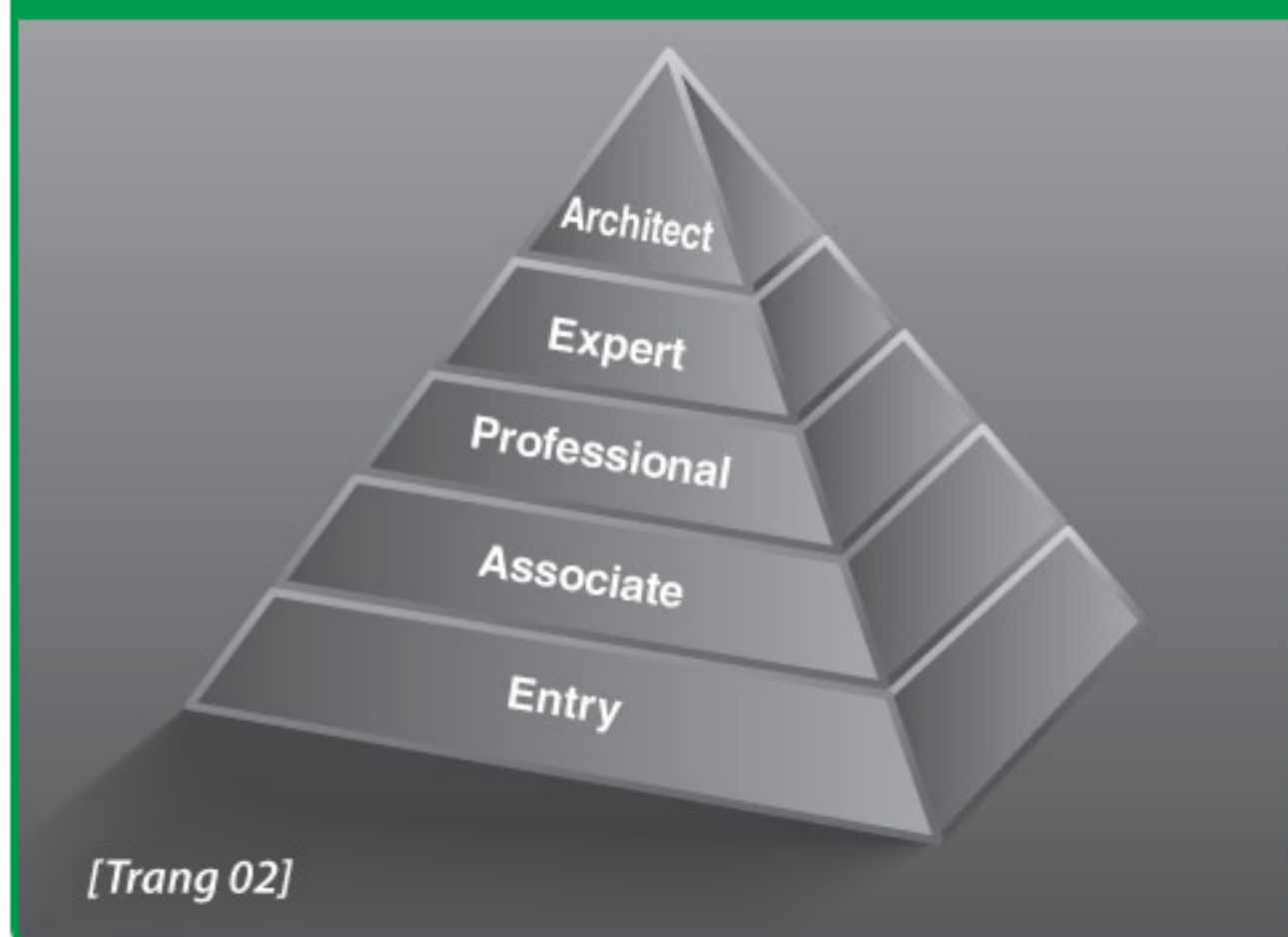


CCNP code mới (version 2) được VnPro triển khai đào tạo từ cuối tháng 7/2014



Giải pháp công nghệ Web Cache WCCPv2 của Cisco

Web Cache Communication Protocol (WCCP) được Cisco phát triển hơn 10 năm nay, cho phép can thiệp vào lưu lượng web một cách trong suốt rồi chuyển hướng chúng tới thiết bị caching device ...

[Trang 03]

từ 1/8 đến 31/8/14

VUI TỬU TRƯỞNG

HOÀN HẠC PHÍ LÊN ĐẾN

1.000.000đ

9 KỸ NĂNG CNTT mà nhà tuyển dụng không thể từ chối

Tám chuyên gia – gồm các nhà tuyển dụng, nhà biên soạn chương trình dạy nghề, giáo sư khoa học máy tính, nhà quản trị doanh nghiệp – đã tóm tắt trên báo Computerworld12 kỹ năng CNTT cần thiết nhất mà người tìm việc cần có ...

[Trang 08]

Chương trình VnPro

KẾT NỐI NHÀ TUYỂN DỤNG CAREER 2014

[Trang 12]

TIN TỨC SỰ KIỆN KHÁC

- 01. Tin tức công nghệ
- 04. Cấu hình QoS cho lưu lượng VOIP trên Cisco Router
- 06. Tủ sách LabPro
- 07. Tiêu chuẩn kiến trúc hạ tầng mạng

- 09. Giải đáp công nghệ thông tin
- 11. Thư giãn
- 12. Chủ đề hội thảo
- 13. Tìm hiểu cơ chế phân mảnh gói tin

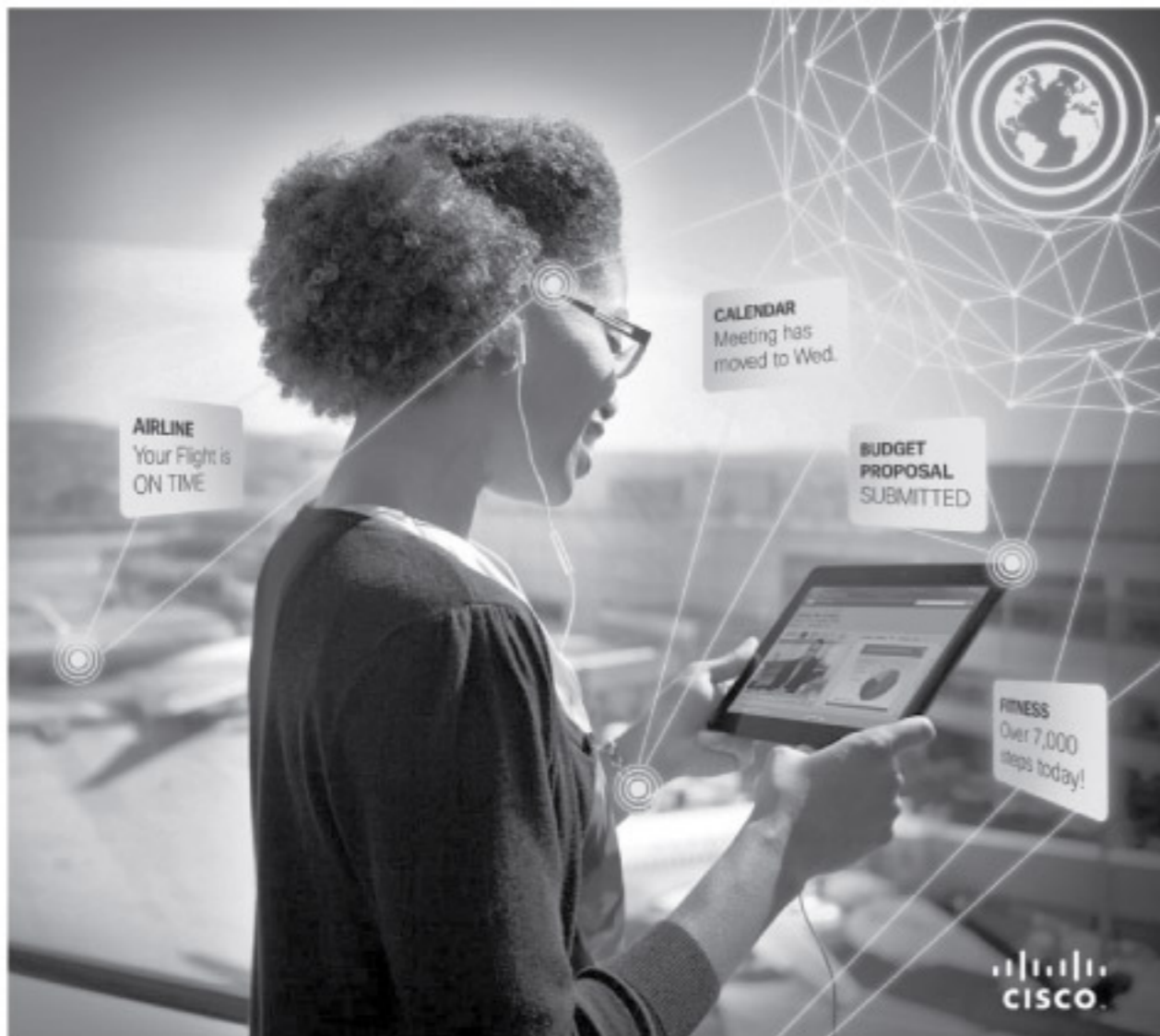
Cisco phát triển công nghệ Jabber

Truyền thông hợp nhất UC (Unified Communication) hứa hẹn sẽ tăng trưởng mạnh vào thế kỷ 21, bằng việc tiết kiệm kinh phí di chuyển nhưng vẫn đảm bảo khả năng cộng tác linh hoạt của công nghệ, nó sẽ giúp doanh nghiệp tiết kiệm đáng kể về chi phí và tăng năng suất làm việc



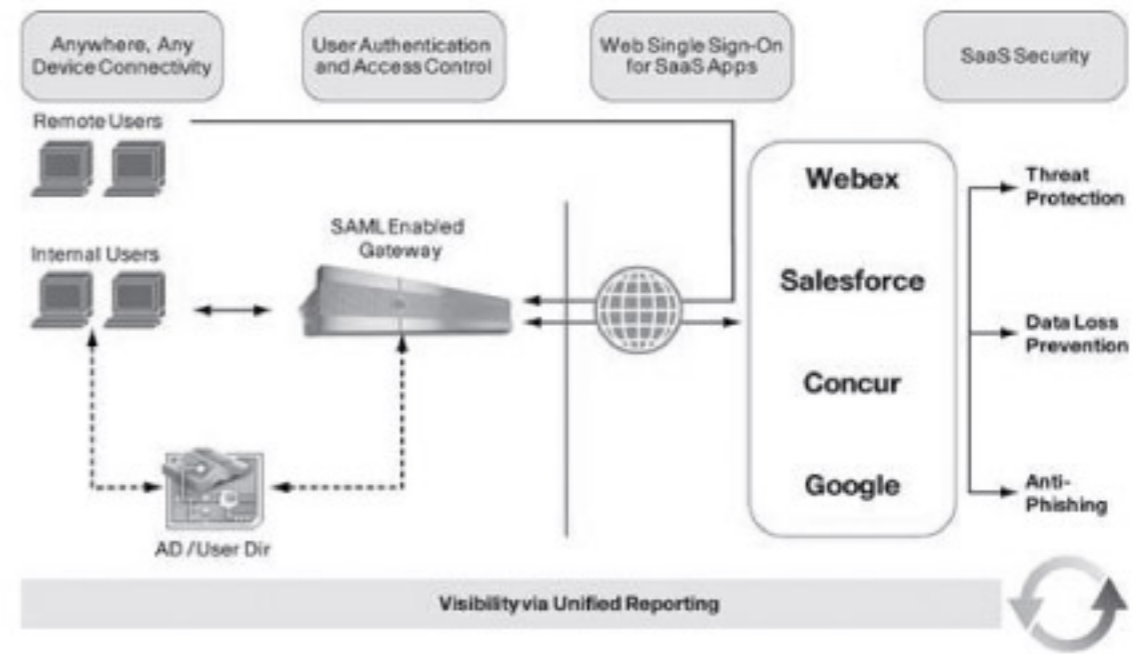
Theo dự đoán từ nhiều chuyên gia, công nghệ UC do Cisco đề xướng sẽ được nhiều doanh nghiệp triển khai trong vòng 2 năm tới đây. Công nghệ Jabber của Cisco có khả năng hỗ trợ các ứng dụng thời gian thực như "chat" trực tuyến bằng văn bản, hình ảnh và âm thanh trực tiếp trên các điện thoại thông minh smartphone iPhone hoặc iPad.

Mobile Cloud sẽ trở thành xu hướng làm việc trong tương lai



Cùng với sự phát triển mãnh liệt của công nghệ điện toán đám mây, sự phổ biến của Internet of Thing, trong bối cảnh các phương tiện di động mobile ngày càng trở nên phổ biến (dự kiến sẽ có 10 tỷ thiết bị được kết nối tới năm 2018), đa dạng về chức năng và có thể phục vụ đầy đủ cho công việc thì các công ty có thể sẽ lên kế hoạch để các nhân viên có thể làm việc ở bất kỳ địa điểm nào nhưng vẫn có thể kết nối thời gian thực tới hạ tầng mạng của công ty để truy cập các tài nguyên cần thiết.

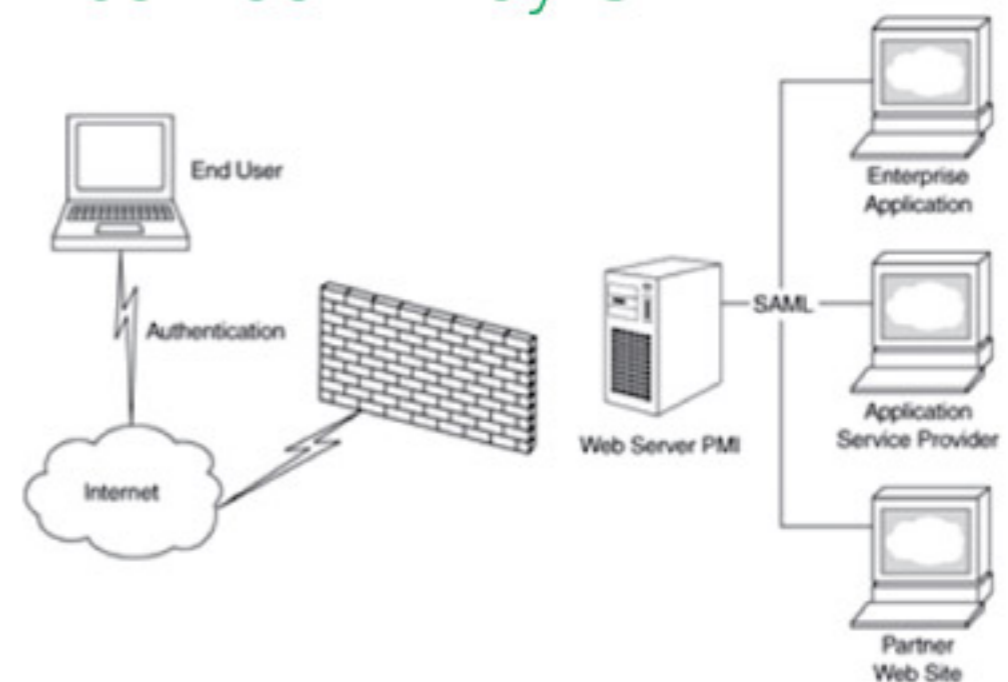
Giải pháp công nghệ giúp doanh nghiệp tiết kiệm chi phí SaaS



Giải pháp phần mềm Software-as-a-Service (SaaS) được triển khai trên hạ tầng điện toán đám mây cloud-computing model hứa hẹn sẽ đem đến cho doanh nghiệp nhiều lợi ích như tiết kiệm chi phí, nâng cao hiệu suất làm việc. Tuy nhiên, nó cũng đặt ra nhiều thách thức trong vấn đề quản trị các dịch vụ (managing access control) về mặt xác thực, định danh và cấp quyền cho người dùng trên môi trường điện toán vì người dùng có thể truy cập dữ liệu nhạy cảm của doanh nghiệp trên các thiết bị di động ở vị trí bất kỳ và thời điểm bất kỳ.

Hiện nay có khoảng 300 ứng dụng SaaS được sử dụng phổ biến, trong đó có một số phần mềm SaaS điển hình có thể kể đến như giải pháp hội họp trực tuyến Cisco WebEX, Google Apps, Zoho. Theo các chuyên gia, các ứng dụng SaaS sẽ trở nên phổ biến trong bốn năm tới.

Giải pháp xác thực trên môi trường điện toán đám mây SAML



Khi các doanh nghiệp triển khai các ứng dụng, dịch vụ trên môi trường điện toán đám mây, phương thức xác thực và cấp quyền cho người dùng user truyền thống không còn phù hợp nữa. Lúc này, giải pháp kiểm soát truy cập Security Assertion Markup Language (SAML) sẽ là sự lựa chọn lý tưởng khi triển khai các ứng dụng điện toán. SAML sử dụng các chuẩn XML để trao đổi thông tin xác thực (authentication) và cấp quyền (authorization) giữa nhà cung cấp định danh xác thực và phía người dùng thông qua giao diện website.

Người dịch: Bùi Quốc Kỳ

CCNP code mới (version 2)

được VnPro triển khai đào tạo từ cuối tháng 7/2014

Theo thông tin mới nhất từ trang chủ của Cisco www.cisco.com, vào cuối tháng 7/2014, Cisco sẽ chính thức áp dụng code CCNP mới vào chương trình giảng dạy của mình. Không lấy làm ngạc nhiên từ sự thay đổi code của Cisco lần này, Trung tâm tin học VnPro sẽ bắt đầu đưa vào giảng dạy chương trình CCNP code mới từ cuối tháng 7/2014 với 3 khóa học ROUTE, SWITCH, TSHOOT có mở rộng thêm Ipv6, Cisco StackWise, VSS và DMVPN .v.v... (loại bỏ Wireless, VOIP, Video).

Để giúp học viên của mình tiếp cận và làm quen hơn với code mới, VnPro sẽ tổ chức cập nhật nội dung code mới hoàn toàn miễn phí cho những bạn đang theo học CCNP code cũ. Không những thế, Trung tâm tin học VnPro cũng sẽ tổ chức các buổi ôn thi CCNP quốc tế miễn phí từ nay đến hết tháng 1/2015. Do số lượng hạn chế nên hãy luôn truy cập vnpro.vn để là người đầu tiên tham dự.

- Thông tin mới nhất Cisco cho biết :

- + Thời gian hết hạn thi code cũ là 29/01/2015, nếu bạn vẫn chưa thi thì hãy đăng ký thi sớm các module còn lại để hoàn tất chứng chỉ CCNP quốc tế.
- + Thời hạn của chứng chỉ CCNP là 3 năm, sau đó bạn có thể thi bất kỳ module CCNP hoặc cao hơn để gia hạn chứng chỉ CCNP Quốc tế.

Chi tiết so sánh code CCNP cũ và mới được thể hiện đầy đủ bảng dưới đây:

ROUTE		SWITCH		TSHOOT	
Removed	Added	Removed	Added	Removed	Added
Complex enterprise network requirements (Cisco Network Models, SONA Framework)	Overview of Basic Network and Routing Concepts	Cisco Service-Oriented Architecture (SONA)	Cisco SDM Templates	FCAPS Model	Troubleshooting IPv6 Address Assignment on Clients
Implementation Planning and Documentation	Implementing RIPng	Cisco Lifecycle Services and Network Implementation	DHCP for IPv6	Troubleshooting TCAM Problems	Troubleshooting DHCP Snooping
Advertising an IP Default Network in EIGRP	Configuring EIGRP for IPv6	Syslog	NTP for IPv4 and IPv6, SNTP	Understanding Cisco IOS Switching Paths (Process Switching, Fast Switching, CEF)	Cisco TAC
EIGRP over Multipoint Subinterfaces	Configuring Named EIGRP Configuration	SNMP Version 2 Configuration	SNMP Version 3 Configuration	Cisco IOS Firewall Security Feature	EIGRP Named Configuration
EIGRP Bandwidth Use Across WAN Links	Configuring OSPFv3	Voice and Video in Campus Networks	SPAN		Troubleshooting FHRP Tracking
Details in OSPF over Different Frame Relay Implementations	Cisco Express Forwarding Switching	Integrating Wireless LAN	Switch Virtualization (StackWise, VSS)		Troubleshooting GRE Tunnels
OSPF Virtual Links	Implementing Nat Virtual Interface		First Hop Redundancy for IPv6	Troubleshooting Policy Based Routing	
Implementation of NSSA and Totally NSSA OSPF Areas	Implementing IPv6 Internet Connectivity		Storm Control		Troubleshooting EIGRP for IPv6
	Implementing BGP for IPv6				Troubleshooting BGP for IPv6
	Securing Cisco Routers				Troubleshooting OSPFv3 Address Families Feature

Giải pháp công nghệ Web Cache WCCPv2 của Cisco

Web Cache Communication Protocol (WCCP) được Cisco phát triển hơn 10 năm nay, cho phép can thiệp vào lưu lượng web một cách trong suốt rồi chuyển hướng chúng tới thiết bị caching device cục bộ. Được phát triển qua nhiều giai đoạn, giờ đây WCCP có thể can thiệp cả các giao thức IP-based protocol. Công nghệ WCCPv2 thường được sử dụng nhằm tối ưu hóa đường liên kết WAN chẳng hạn như giải pháp Cisco Wide Area Application Services (WAAS).

WCCPv2 hoạt động trên môi trường server và client. WCCP server chịu trách nhiệm chuyển hướng các lưu lượng chỉ định tới một hoặc nhiều WCCP client. Chức năng của WCCP server được thực hiện bởi Cisco IOS và được hỗ trợ trên nhiều dòng router và switch platform:

- Catalyst 3560/3750 Series Switch
- Catalyst 4500/4948 Series Switch
- Catalyst 6500 Series Switches
- Cisco 1800/2800/3800 Series Integrated Services Routers (ISR)
- Cisco 7600 Series Router

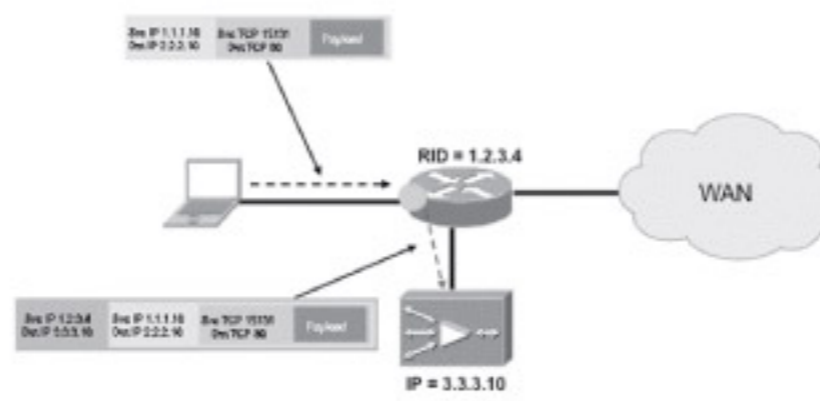
WCCP client chịu trách nhiệm định nghĩa ra loại lưu lượng nào dựa trên các thông tin như IP protocol và có thể tùy chọn dựa thêm thông số Layer 4 transport protocol port. Cisco WCCP client được thực hiện trên nhiều dòng sản phẩm, trong đó có giải pháp Cisco Wide Area Application Services (WAAS). WCCP client cũng có thể thực thi tác vụ chuyển hướng lưu lượng giữa các thiết bị, chia tải đều ra nhiều WCCP client trong một cluster.

Service Group (Nhóm dịch vụ)

Các WCCP server và client tham gia thực hiện cùng một dịch vụ được gọi chung là một service group. Một service group định nghĩa ra các đặc điểm về lưu lượng nào sẽ được chuyển hướng và cache lại (lưu trữ lại). Service group có thể được định nghĩa theo hai cách thức: well-known hoặc dynamic. Well-known service (static service) thì cần phải thiết lập các tham số tĩnh trên cả WCCP server (IOS) và client. Còn dynamic service thì được thực hiện bởi WCCP client. Các tiêu chí được triển khai dựa trên dynamic service được trao đổi giữa WCCP server (IOS) khi client tham gia vào service group. Mỗi service group được nhận diện bởi một service ID duy nhất dao động từ 0 tới 255. Service ID từ 0 đến 50 được dành riêng cho các dịch vụ well-known service.

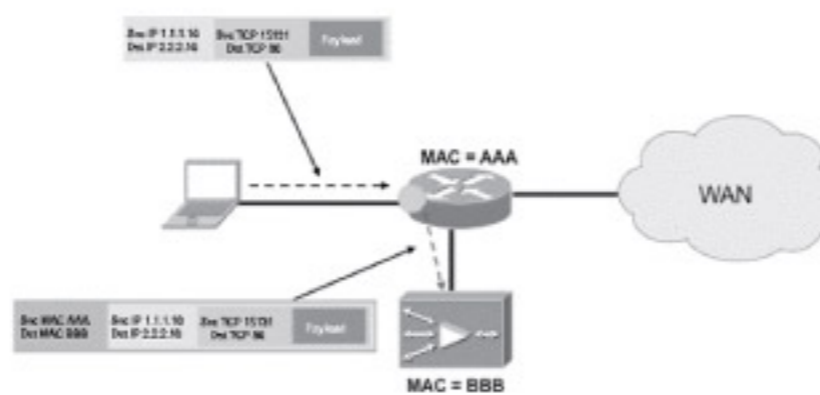
Forwarding Method (Phương thức chuyển hướng)

WCCP forwarding method xác định cách thức can thiệp vào lưu lượng sẽ được gửi từ WCCP server (IOS) tới WCCP client (WAE chạy trên Cisco WAAS). Có 2 phương thức chuyển hướng (forwarding method) như sau:



WCCP interception với GRE forwarding

- Generic Routing Encapsulation (GRE) – GRE forwarding là phương thức chuyển hướng forwarding method mặc định bằng cách đóng gói các "intercepted packet" và bổ sung IP GRE header với source IP của WCCP server (IOS) và destination IP của target WCCP client thông qua một tunnel, cho phép WCCP server (IOS) có thể có nhiều Layer 3 hop tới WCCP client.
- Layer 2 (L2) – L2 forwarding cần phải được triển khai trên một số dòng hardware-based platform chẳng hạn như Catalyst series switch, giải pháp này đơn giản là thay đổi thông tin destination MAC của "intercepted packet" sang địa chỉ MAC của "target WCCP client". L2 forwarding đòi hỏi WCCP server (IOS) phải thiết lập Layer 2 adjacent tới WCCP client.



WCCP interception với L2 forwarding.

Return Method (Phương thức hồi đáp)

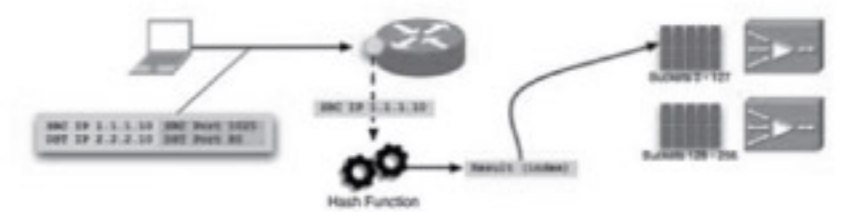
WCCP return method định nghĩa cơ chế WCCP client hồi đáp "intercepted traffic" ngược trở lại cho WCCP server (IOS). Phương thức hồi đáp "return method" cung cấp cách thức cho các WCCP client lấy dữ liệu hồi đáp cho hệ thống mạng. Một vài WCCP client được triển khai hiện nay (bao gồm cả Cisco WAAS) cho phép lưu lượng "intercepted traffic" được chuyển hướng thông suốt về WCCP server (IOS) ngay cả khi WCCP client có thể thực hiện trực tiếp tác vụ của WCCP server.

Tương tự như WCCP forwarding method, WCCP return method cũng có 2 tùy chọn:

- Generic Routing Encapsulation (GRE) – Các packet được đóng gói và bổ sung IP GRE header với source IP của WCCP client và destination IP của WCCP server (IOS).
- Layer 2 (L2) – Các packet được thay đổi destination MAC là MAC address của WCCP server. Để tránh việc nhầm lẫn với lưu lượng "re-intercepting L2 return traffic", WCCP client sẽ gửi lưu lượng hồi đáp trên một VLAN khác với VLAN trước đó phục vụ cho dịch vụ.

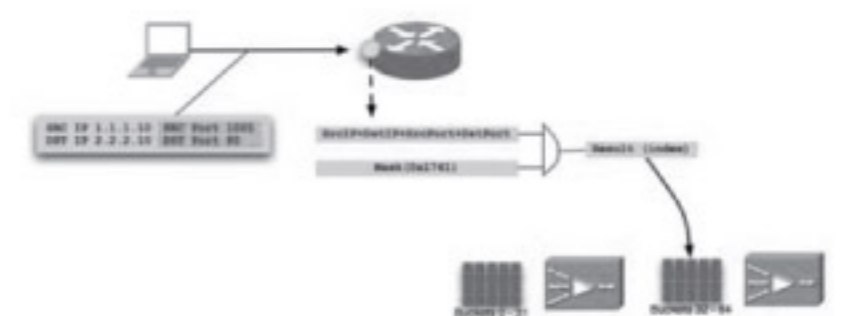
Assignment Method (Phương thức phân phối)

Khi nhiều WCCP client tham gia vào cùng một service group, WCCP sẽ tự động phân phối lưu lượng "intercepted traffic" tới tất cả các WCCP client trong service group. Cơ chế phân phối lưu lượng "intercepted traffic" tới các WCCP client trong service group được gọi là assignment method. WCCPv2 sử dụng 2 phương thức "assignment method": hash assignment và mask assignment.



Cơ chế hash và phân phối bucket

Phương thức "assignment method" mặc định là hash assignment sử dụng một bảng 256-bucket redirection hash table để phân phối lưu lượng tới các WCCP client trong một service group. Lưu lượng WCCP server (IOS) intercepts traffic dựa vào các thông tin như source/destination IP hoặc source/destination port (tùy theo service group được cấu hình như thế nào) để thực hiện chức năng hash function tính toán các giá trị index value. Index value sẽ được liên kết tới một trong số 256 bucket trong bảng hash table. Mỗi bucket trong bảng hash table được gán tương ứng cho mỗi WCCP client trong service group.



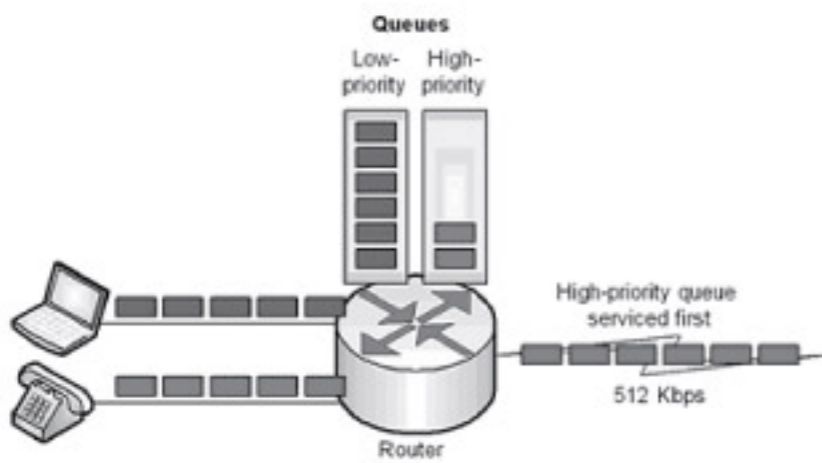
Giá trị mask và tiến trình phân phối value assignment

Mask assignment được thực hiện trên các hardware-based routers/switch sử dụng mask và bảng giá trị để phân phối lưu lượng tới các WCCP client trong một service group. Mask assignment được phát triển trên các dòng Cisco Catalyst series switch cho phép cơ chế WCCP interception được thực hiện hoàn toàn bằng phần cứng. Lưu lượng WCCP server (IOS) intercepts traffic dựa vào thuật toán bitwise AND giữa mỗi giá trị mask value và nội dung của packet (tham số source/destination IP và port). Kết quả tính toán sẽ được so sánh với danh sách các giá trị tương ứng với mỗi mask. Mỗi giá trị value được phân phối cho từng WCCP client chỉ định trong service group.

Interception Direction (Hướng can thiệp)

Cấu hình WCCP server (IOS) bao gồm các thiết lập ở chế độ global và interface configuration mode. Chế độ global configuration định nghĩa

Cấu hình QoS cho lưu lượng VOIP trên Cisco Router



Chất lượng dịch vụ quality of service (QoS) trên hạ tầng mạng nên được triển khai để đảm bảo băng thông (bandwidth) và mức ưu tiên (priority) tương ứng với từng loại lưu lượng trên hệ thống. It's important to understand the difference between bandwidth and priority.

Cấu hình QoS tương đối phức tạp và có nhiều cách thức để đạt được kết quả cuối cùng, sau đây là các bước cơ bản nhất mà chúng ta có thể thực hiện để triển khai QoS trên Cisco router.

Bước 1: Định nghĩa lưu lượng VOIP traffic thông qua ACL

Chúng ta có thể định nghĩa lưu lượng VoIP thông qua ACL để định mức Priority hoặc Bandwidth cho lưu lượng này, hoặc cũng có thể sử dụng tính năng tự động nhận diện lưu lượng Network Based Application Recognition (NBAR) để tiến trình cấu hình sẽ trở nên dễ dàng hơn. Với ACL thì chúng ta có thể tùy chỉnh các tiêu chí để phân loại lưu lượng. Còn với NBAR, cho phép router tự động nhận diện lưu lượng thoại loại nào, chẳng hạn như nhận diện các lưu lượng đi qua nó là lưu lượng HTTP, nhưng hạn chế của cơ chế này là không phải router có thể nhận diện tất cả các loại lưu lượng hiện nay.

Nếu sử dụng ACL để phân loại lưu lượng VoIP thì chúng ta sẽ triển khai các câu lệnh sau:

```
Router(config)#access-list 105 remark access list for voip traffic for QoS
Router(config)#access-list 105 permit udp any any eq 5060
Router(config)#access-list 105 permit udp any any eq 5061
Router(config)#access-list 105 permit udp any any range 5000 10000
```

các service group ID mà WCCP server (IOS) sẽ hỗ trợ. Tiếp đến, WCCP sẽ được kích hoạt trên mỗi interface mà lưu lượng traffic sẽ được thực hiện tiến trình interception. WCCP interface configuration được áp dụng theo chiều inbound hoặc outbound.

```
!
hostname INBOUND
!
```

```
Router(config)#access-list 105 permit udp any any range 10000 20000
Router(config)#access-list 105 permit ip host 127.0.0.1 any
Router(config)#access-list 105 permit ip any host 127.0.0.1
Router(config)#access-list 105 permit ip host VOIP-host-here any
Router(config)#access-list 105 permit ip any host VOIP-host-any
```

Lưu lượng VOIP traffic trong access list 105 có lưu lượng SIP server traffic (5060, 5061), RTP traffic, VOIP host tới any và any tới VOIP host được sử dụng trong class-map.

Bước 2: Thiết lập class-map tương ứng với lưu lượng VOIP traffic:

Một class-map định nghĩa các nhóm lưu lượng thành các group. Trong ví dụ này, ta sẽ thiết lập class-map với tên gọi là voice.

```
Router(config)#class-map match-all voice
Router(config-cmap)#?
QoS class-map configuration commands:
description Class-Map description
exit Exit from QoS class-map configuration mode
match classification criteria
no Negate or set default values of a command
rename Rename this class-map
Router(config-cmap)#match access-group 105
```

Bước 3: Thiết lập policy-map cho lưu lượng VOIP traffic:

Một policy-map sẽ tiến hành phân phối băng thông (bandwidth) và priority tương ứng với các class được định nghĩa trong các class-map như sau:

```
Router(config)#policy-map voice-policy
Router(config-pmap)#?
QoS policy-map configuration commands:
class policy criteria
description Policy-Map description
exit Exit from QoS policy-map configuration mode
no Negate or set default values of a command
```

```
rename Rename this policy-map
Router(config-pmap)#class voice
Router(config-pmap-c)#?
QoS policy-map class configuration commands:
bandwidth Bandwidth
compression Activate Compression
drop Drop all packets
exit Exit from QoS class action configuration mode
netflow-sampler NetFlow action
no Negate or set default values of a command
police Police
priority Strict Scheduling Priority for this Class
queue-limit Queue Max Threshold for Tail Drop
random-detect Enable Random Early Detection as drop policy
service-policy Configure Flow Next
set Set QoS values
shape Traffic Shaping
Router(config-pmap-c)#priority 1024
Router(config-pmap)#class class-default
Router(config-pmap-c)#fair-queue
```

Bước 4: Áp dụng policy-map tương ứng với VOIP traffic lên cổng giao tiếp Router interface

Tương tự như ACL, chúng ta sẽ tiến hành liên kết policy-map lên cổng giao tiếp chỉ định theo hướng output hoặc input:

```
service-policy output|input {name of policy-map}
```

Nếu chúng ta sử dụng tính năng NBAR để nhận diện lưu lượng, ta phải cấu hình câu lệnh sau tại chế độ cổng ip nbar protocol-discovery command.

```
Router(config)#interface FastEthernet0/0
Router(config-if)service-policy output voice-policy
Router(config)#interface Serial0/2/1
Router(config-if)service-policy output voice-policy
```

Người biên soạn: Bùi Quốc Kỳ

```
ipwccp 99
!
interface GigabitEthernet0/0
ip address 10.10.10.1 255.255.255.0
ipwccp 99 redirect in
!
!
hostname OUTBOUND
!
```

```
ipwccp 99
!
interface Serial0/0
ip address 11.11.11.2 255.255.255.252
ipwccp 99 redirect out
!
```

Người biên soạn: Bùi Quốc Kỳ

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



HOÀN
HỌC PHÍ
LÊN ĐẾN
1.000.000đ

từ 1/8 đến 31/8/14

VUI TỰU TRƯỜNG

- ▲ Bốc là trúng 100% - Hoàn học phí lên đến 1.000.000đ
- ▲ Giảm thêm 10% cho học viên cũ.
- ▲ Ưu đãi đặc biệt khi đóng cặp.

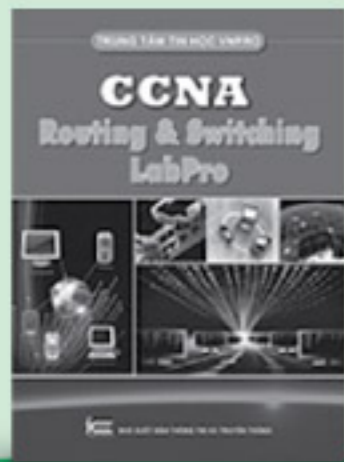
Cam kết lợi ích khi học tại VnPro

- 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 đấu 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%



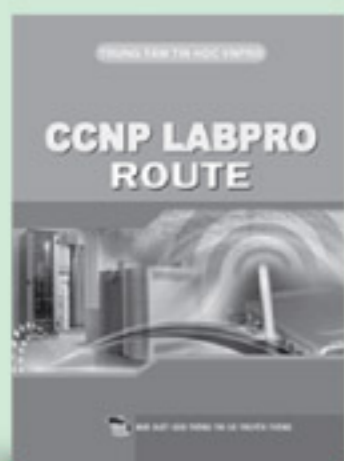
CCNA Routing & Switching
Giá: 220.000 VNĐ



CCDA
Giá: 250.000 VNĐ



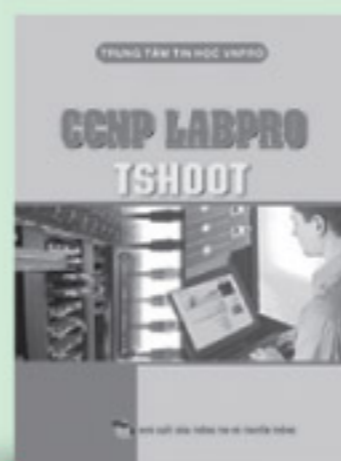
Ôn thi CCNA trong 24h
Giá: 120.000 VNĐ



CCNP LABPRO ROUTE
Giá: 120.000 VNĐ



CCNP LABPRO SWITCH
Giá: 120.000 VNĐ



CCNP LABPRO TSHOOT
Giá: 120.000 VNĐ



Ôn thi Route
Giá: 90.000 VNĐ



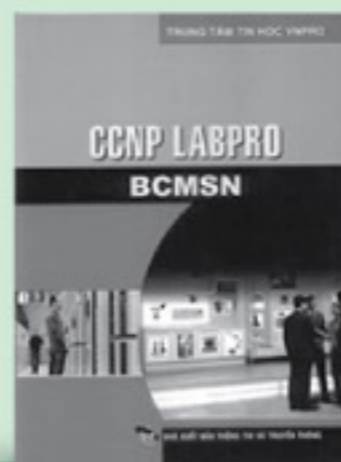
Ôn thi Switch
Giá: 100.000 VNĐ



Ôn thi Tshoot
Giá: 80.000 VNĐ



CCNP LABPRO BSCI
Giá: 95.000 VNĐ



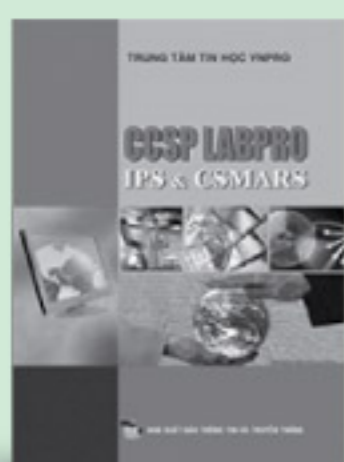
CCNP LABPRO BCMSN
Giá: 70.000 VNĐ



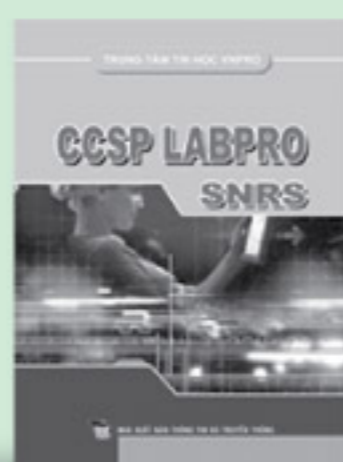
CCNP LABPRO ISCW
Giá: 120.000 VNĐ



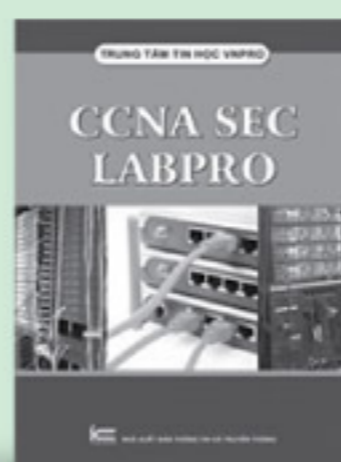
CCSP LABPRO SNAF & SNAA
Giá: 120.000 VNĐ



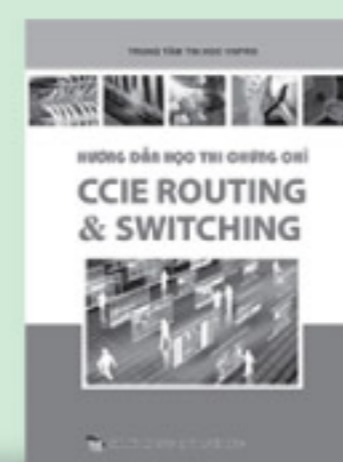
CCSP LABPRO IPS & CSMARS
Giá: 90.000 VNĐ



CCSP LABPRO SNRS
Giá: 140.000 VNĐ



CCNA SEC LABPRO
Giá: 150.000 VNĐ



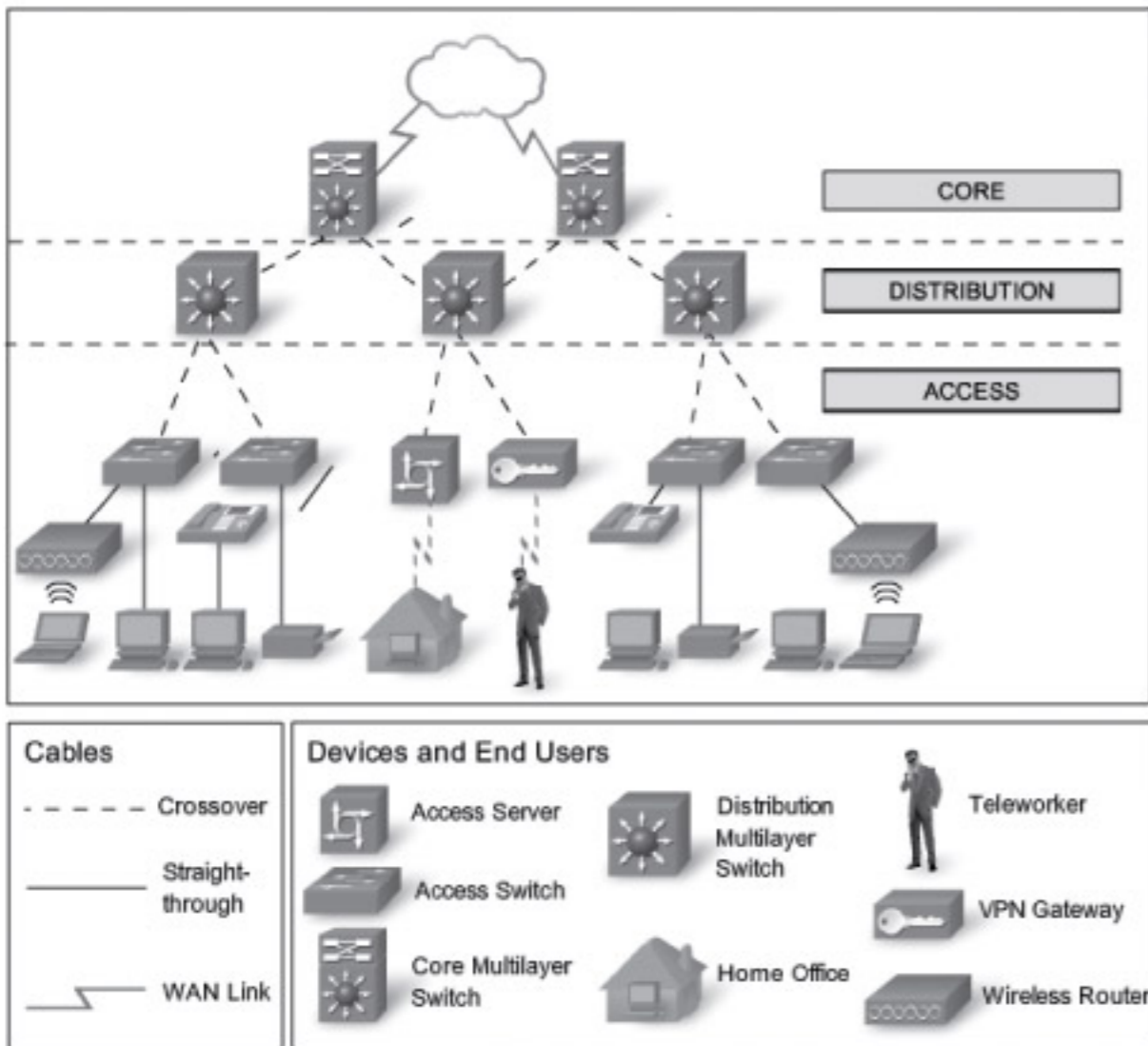
CCIE R&S
Giá: 150.000 VNĐ



CWNA
Giá: 90.000 VNĐ

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

TIÊU CHUẨN KIẾN TRÚC HẠ TẦNG MẠNG



Kiến trúc hạ tầng mạng 3 phân lớp

Kiến trúc hạ tầng mạng lý tưởng thường được chia thành 3 lớp: **Access, Distribution và Core**.

Access Layer - cung cấp kết nối vào hệ thống mạng cho các thiết bị đầu cuối và kiểm soát các thiết bị này được giao tiếp được tới các thiết bị khác hay không như PC, printer, IP phone, router, switch, bridge, hub, và wireless access points (AP).

Distribution Layer - tập kết dữ liệu từ access layer rồi định tuyến tới core layer. Distribution layer có vai trò kiểm soát luồng lưu lượng giữa các broadcast domain, các VLAN được phân chia tại tầng access layer thông qua các chính sách policy dựa trên nền tảng định tuyến. Các thiết bị được triển khai tại tầng này thường là switch lớp 3 (có thể lọc lưu lượng dựa trên thông tin lớp 2 (địa chỉ MAC) và thông tin lớp 3 (địa chỉ IP)) có hiệu suất hoạt động cao để đảm bảo độ tin cậy.

Core Layer - đây là hệ thống mạng lõi với các thiết bị switch hoặc router có tốc độ truyền dẫn cao cho phép truyền tải một khối lượng lớn dữ liệu với.

Lợi ích của mô hình mạng phân cấp

- Dễ dàng mở rộng hệ thống mạng
- Hạ tầng mạng distribution và core có tính dự phòng cao, hiệu suất chuyển mạch tối ưu giúp đảm bảo lưu lượng trao đổi giữa tất cả các thiết bị
- Các chính sách bảo mật có thể được triển khai linh hoạt ở tầng access, hoặc tầng distribution
- Dễ quản lý, dễ triển khai và khắc phục sự cố phát sinh
- Mô hình phân cấp đảm bảo đường kính tối đa giữa các thiết bị là ít nhất giúp giảm độ trễ trên hệ thống mạng, phù hợp cho việc triển khai voice và data trên cùng một hạ tầng mạng

Bảng tổng kết đặc điểm của các switch tại các tầng

	Access	Distribution	Core
Bandwidth aggregation	✓	✓	✓
Fast Ethernet/Gigabit Ethernet	✓		
Gigabit Ethernet/10 Gigabit Ethernet		✓	✓
High forwarding rate		✓	✓
Layer-3 Support		✓	✓
Port security	✓		
Power over Ethernet (PoE)	✓		
Quality of Service (QoS)	✓	✓	✓
Redundant components		✓	✓
Security Policies/Access Control Lists		✓	
Very High forwarding rate			✓
VLANs	✓		

Người dịch: Phạm Minh Nguyên

GIỚI THIỆU CHỨNG CHỈ CCNA



Chứng chỉ CCNA

CCNA là chứng chỉ khởi đầu cho thế giới hạ tầng mạng của Cisco nói riêng và hạ tầng mạng trên toàn thế giới nói chung. Nó là điểm khởi đầu tốt và thuận lợi nhất để đạt được thành công trong sự nghiệp sau này. CCNA công nhận bạn là một chuyên viên triển khai hạ tầng mạng lành nghề, có đầy đủ các kiến thức và kỹ năng để vận hành được một hệ thống vừa và nhỏ trong các doanh nghiệp. Bên cạnh đó, nội dung của CCNA cũng giúp bạn rèn luyện cách tư duy hiệu quả và xử lý nhanh các vấn đề xảy ra trong hệ thống. Và điều quan trọng cuối cùng là CCNA trang bị cho bạn có một nền tảng thật vững chắc để tiếp tục rèn luyện và phát triển chuyên môn cao hơn.

Khả năng làm việc

Chương trình CCNA mang đến cho bạn khối lượng kiến thức đầy đủ để bạn tự tin làm việc trong những môi trường chuyên nghiệp nhất. Cụ thể hơn bạn sẽ thiết kế được một hệ thống mạng với số lượng user lên đến 150 người và số lượng hoạt động từ 3 đến 5 chi nhánh. Phân tích được các yêu cầu hiện tại của doanh nghiệp và tiến hành nghiên cứu triển khai. Xây dựng hệ thống mạng Wan liên kết các chi nhánh lại với nhau. Vận hành tốt hệ thống định tuyến cũng như chuyển mạch giúp tốc độ xử lý đạt mức tốt nhất. Xây dựng các dịch vụ quan trọng nhằm tăng cường sự tiện lợi cho người dùng để đạt hiệu quả cao trong kinh doanh.



9 KỸ NĂNG CNTT mà nhà tuyển dụng không thể từ chối

1. Hiểu biết máy tính

Khi các công ty xây dựng các phần mềm lọc thư rác và phát hiện sự lừa đảo, làm sinh ra những núi dữ liệu khổng lồ, thì nhu cầu tuyển chuyên viên CNTT có kiến thức sâu về máy tính bỗng dưng tăng vọt. Người có kiến thức về máy tính không chỉ hiểu biết cơ chế vận hành của máy mà phải có khả năng thiết kế, phát triển các thuật toán (algorithm) và kỹ thuật cải thiện hoạt động của hệ thống. Kevin Scott, nhà quản trị cao cấp về công nghệ của Tập đoàn Google, cho rằng vấn đề cơ bản là bạn sẽ tổ chức dữ liệu và trình bày chúng như thế nào. Kỹ năng này liên quan đến việc khai thác dữ liệu, mô hình hóa hoạt động thống kê và cấu trúc cơ sở dữ liệu. Scott nói: "Cách thức bạn tổ chức dữ liệu và các thuật toán bạn sử dụng sẽ quyết định việc bạn có được giải pháp hợp lý hay không."

Kiến thức về máy tính có thể được tích lũy qua công việc hoặc qua học tập ở nhà trường, song cho dù thế nào, nắm vững những kiến thức này nhanh là một lợi thế.

2. Các ứng dụng di động

Theo Sean Ebner, Phó chủ tịch phụ trách các dịch vụ chuyên nghiệp của Spherion Pacific Enterprises ở Florida, cuộc đua sáng tạo nội dung cho các loại thiết bị di động đang diễn ra sôi nổi giống như những ngày đầu của Internet vào thập niên 1990, cùng với sự phổ dụng các loại điện thoại di động thông minh như Blackberry, Treo, O2... Vì vậy, các công ty đang cần những chuyên viên CNTT có khả năng đưa các ứng dụng về quản lý nguồn lực doanh nghiệp (ERP), kế toán... vào thiết bị di động.

3. Mạng không dây

Các giao thức truyền dữ liệu không dây như Wi-Fi, WiMAX, Bluetooth... đã trở thành những công cụ không thể thiếu của cộng đồng cư dân mạng. Từ đó, nỗi lo hàng đầu của nhà quản trị là làm sao tuyển được chuyên viên CNTT có khả năng bảo đảm an toàn dữ liệu và bảo đảm sự hoạt động thông suốt của mạng. Theo Neil Hopkins, Phó chủ tịch về phát triển kỹ năng của Hiệp hội Công nghệ Tính toán (CompTIA), nỗi lo của nhà quản trị doanh nghiệp là làm sao kết nối các giao thức mạng không dây với nhau và nắm bắt những rủi ro về an ninh đang tăng lên rất nhanh do việc sử dụng mạng không dây. "Nếu tôi tuyển một chuyên viên mạng không dây, tôi muốn anh ta phải hiểu biết những rủi ro tiềm ẩn về an ninh và xây dựng các biện pháp kiểm soát ngay từ đầu", đó là ý kiến của Howard Schmidt, Chủ tịch Hiệp hội An toàn Hệ thống thông tin và là nhà chiến lược chính về an ninh

mạng của Tập đoàn eBay. Tuy nhiên Hopkins khuyên rằng, đừng nên bước ra thị trường lao động chỉ với tấm giấy chứng nhận về công nghệ không dây vì sẽ không ai thuê mướn một chuyên viên "không dây" thuần túy. Cái mà thị trường cần là kỹ năng quản trị mạng cộng thêm sự hiểu biết sâu về công nghệ không dây, nghĩa là biết rõ mạng không dây sẽ hoạt động thế nào khi kết nối với mạng máy tính nói chung.

4. Giao diện con người-máy tính

Nhu cầu về thiết kế giao diện con người-máy tính (human-computer interaction) hay nói gọn là giao diện người dùng (user interface) cho tất cả các ứng dụng web đang rất cấp bách. "Nhờ những công ty như Apple Inc., người tiêu dùng ngày càng có ý thức về sản phẩm đẹp, thiết kế ấn tượng nên chuyên viên CNTT không thể chỉ biết có kỹ thuật", Scott nói.

5. Quản lý dự án

Chuyên viên quản lý dự án CNTT thì bao giờ và ở đâu cũng cần, nhưng bây giờ yêu cầu của nhà tuyển dụng đối với vị trí này đã khắt khe hơn nhiều. Theo ông Grant Gordon, Giám đốc điều hành Công ty cung ứng nhân lực Intrinsic Solutions Group ở Kansas, thị trường cần những chuyên viên quản lý dự án "thứ thiệt" chứ không phải những người có bằng cấp, nghĩa là có kỹ năng và kinh nghiệm trong việc xử lý những tình huống khác nhau, chẳng hạn sự mâu thuẫn trong nội bộ nhóm làm việc chung quanh những vấn đề công nghệ. "Các công ty cần những người có khả năng lãnh đạo một tập thể chuyên viên, tận dụng hiệu quả vòng đời của dự án và kỹ năng quản lý dự án thật sự", Gordon nói.

6. Kỹ năng mạng nói chung

Theo Scott, cho dù bạn làm việc ở đâu trong lĩnh vực CNTT bạn cũng không thể đứng bên ngoài "mạng". Vì thế, điều cấp thiết là các chuyên viên làm việc "ngoài mạng" như kỹ sư phần mềm cũng phải có những hiểu biết căn bản về mạng máy tính, chẳng hạn như về TCP/IP, Ethernet, cáp quang... và có kiến thức khả dụng (working knowledge) về phương thức phân phối và tính toán trên mạng.

7. Kỹ thuật viên hội tụ mạng

Theo Hopkins, việc các công ty sử dụng ngày càng nhiều điện thoại trên giao thức Internet (VoIP) đã làm phát sinh nhu cầu cần có các nhà quản trị mạng hiểu biết tất cả các kiểu mạng - mạng LAN, WAN, Voice, Internet... - và cách thức hội tụ chúng. Hopkins nói: "Cuộc nghiên

cứu của chúng tôi cho thấy nhu cầu đang tăng nhanh đối với những chuyên viên điện thoại có hiểu biết sâu về mạng CNTT, cũng như những chuyên viên quản trị mạng CNTT hiểu biết về mạng điện thoại và cách thức kết nối chúng."

8. Hệ thống thông tin doanh nghiệp

Dù muốn hay không, trong thời cạnh tranh quyết liệt này các doanh nghiệp đều có ý hướng xây dựng hệ thống thông tin kinh doanh (business intelligence - BI). Theo Ebner, nhu cầu tuyển dụng đang tăng đối với những người có khả năng về công nghệ BI như Cognos, Business Object và Hyperion và khả năng áp dụng các công nghệ đó vào hoạt động doanh nghiệp. "Các công ty đang đầu tư lớn vào BI. Nhưng họ không cần những chuyên viên kỹ thuật thuần túy chỉ biết soạn câu hỏi (query) hoặc viết mã (script). Để trở thành người khai thác dữ liệu có tài năng, bạn cần kiến thức chuyên sâu về loại hình kinh doanh bạn sẽ làm việc", Ebner nói.

9. An ninh mọi lúc mọi nơi

Chuyên viên an ninh máy tính thì bao giờ cũng cần nhưng ngày nay, theo ông Schmidt, các doanh nghiệp cần chuyên viên có kỹ năng bảo mật và an ninh ở tất cả các lĩnh vực CNTT chứ không chỉ là những chuyên viên chỉ chăm chăm lo bảo đảm an toàn hệ thống mạng. "Doanh nghiệp tìm người có khả năng xây dựng một môi trường an toàn, cho dù đó là người quản lý hệ thống thư điện tử hay là người phát triển phần mềm", Schmidt nói. Theo ông, xu thế này phản ánh hiện tượng tích hợp công tác an ninh và bảo mật vào mọi hoạt động hằng ngày của doanh nghiệp hơn là xem an ninh là một bộ phận cộng thêm do một chuyên viên an ninh đảm trách. Vì vậy, mọi chuyên viên CNTT muốn tìm được việc làm nhất thiết phải có sự hiểu biết về công tác an ninh và bảo mật trong phạm vi chuyên ngành của mình. Hopkins nhận xét: "Phản hồi từ các công ty nghiên cứu thị trường cho thấy kỹ năng bảo mật và an ninh là cần thiết ở mọi người, mọi việc; ngay cả nhân viên kỹ thuật tập sự cũng phải biết về an ninh". Còn theo Saunders của Đại học DeVry, để đáp ứng nhu cầu của doanh nghiệp, trường DeVry đã xây dựng giáo trình về an ninh CNTT đưa ra giảng dạy ở tất cả các chi nhánh của trường trên đất Mỹ. Ông nói: "Các công ty ngày càng quan tâm bảo vệ tài sản của mình trước sự tấn công của bọn khủng bố trên mạng (cyberterrorism) và những mối đe dọa ngay trong nội bộ."

Theo: quantrimang.com.vn

Nâng cấp IOS cho Cisco Router thông qua USB

Để nâng cấp IOS cho router, chúng ta thường sử dụng TFTP server, bên cạnh đó ta cũng có thể nâng cấp IOS cho router bằng cách sử dụng cổng giao tiếp USB trên router. Để tiến hành "copy" IOS từ USB sang bộ nhớ flash của router, ta thực hiện câu lệnh sau:

```
Router# copy usbflash0:c880data-universalk9-mz.152-1.T1.bin flash:
```

Sau khi thực hiện câu lệnh trên, ta có thể quan sát tiến trình "copy" như sau:

```
Router#copy usbflash0:c880data-universalk9-mz.152-1.T1.bin f1
Router#copy usbflash0:c880data-universalk9-mz.152-1.T1.bin flash:
Destination Filename [c880data-universalk9-mz.152-1.T1.bin]?
Copy in progress...
Ready
```

Tiếp theo, chúng ta chỉ định cho router sử dụng IOS mới trong suốt tiến trình khởi động bằng câu lệnh sau:

```
Router#conf t
Router(config)#boot system flash
c880data-universalk9-mz.152-1.T1.bin
```

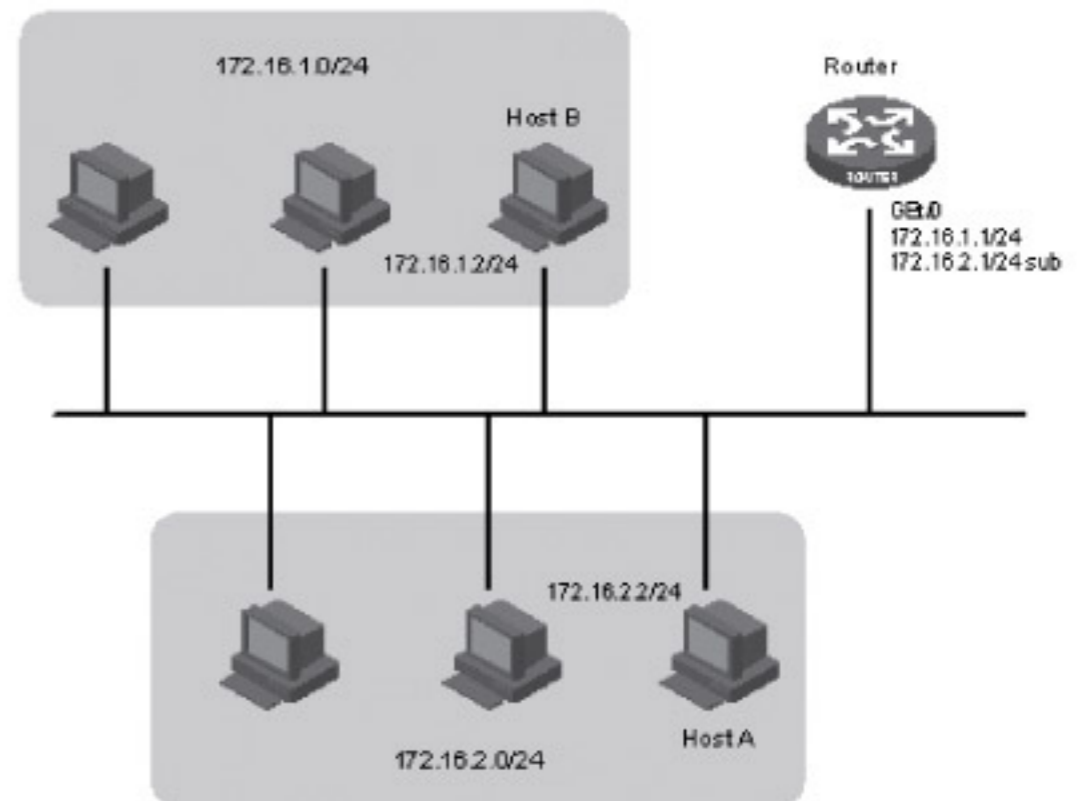
```
33273984 bytes copied in 99.436 secs (334627 bytes/sec)
Router#sh
Router#show f1
Router#show fla
Router#show flash:
#- --length-- --date/time----- path
1 30552244 Mar 1 1984 00:01:00 +00:00 c880data-universalk9-mz.151-2.T1.bin
2 1001 Aug 25 2011 18:51:24 +00:00 ccpbackup2011-08-25_09_50_11
3 96395 Aug 27 2011 17:37:58 +00:00 vds1log.bin
4 33273984 Oct 10 2011 22:04:26 +00:00 c880data-universalk9-mz.152-1.T1.bin
5 33273984 Oct 16 2011 16:22:52 +00:00 c880data-universalk9-mz.152-1.T1.bin
31633408 bytes available (97210368 bytes used)
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system flash
Router(config)#boot system flash c880data-universalk9-mz.152-1.T1.bin
Router(config)#
```

Cuối cùng, chúng ta lưu lại các cấu hình và tiến hành khởi động lại router.

- Lưu ý:
- Một số dòng router hỗ trợ cổng giao tiếp USB 2.0 (định dạng FAT32) bao gồm các dòng 800, 1800, 2800, 3800.
 - Chúng ta có thể sử dụng một số câu lệnh sau để kiểm tra giao tiếp USB trên router:

```
dir usbflash0:
show usb device
show usb controllers
show usb driver
show usb port
```

Cấu hình nhiều địa chỉ IP trên Cisco Router Interface



Cisco IOS cho phép cấu hình nhiều IP trên cùng một cổng giao tiếp interface. Chúng ta có thể cấu hình 1 địa chỉ Primary IP và nhiều địa chỉ Secondary IP (không giới hạn) trên Router interface. Chúng ta có thể cấu hình nhiều địa chỉ IP trên cisco router khi muốn sử dụng nhiều subnet trên cùng một cổng physical interface.

Secondary IP có thể được sử dụng trong nhiều tình huống không đủ số lượng địa chỉ host address trên phân đoạn mạng network segment. Chẳng hạn như giả sử ban đầu chúng ta thiết kế cho phép 254 host tương ứng với mỗi logical subnet, nhưng sau này trên phân đoạn mạng physical subnet lại cần đến 300 host address. Lúc này, chúng ta có thể sử dụng secondary IP trên các routers hoặc access server để sử dụng cùng lúc 2 logical subnet trên cùng một physical subnet.

Cấu hình nhiều địa chỉ IP trên Cisco Router Interface:

Chúng ta có thể cấu hình nhiều địa chỉ IP thuộc nhiều subnet khác nhau. Tại chế độ cổng RouterInterface configuration mode, cấu hình primary IP và secondary IP:

Cấu hình primary IP trên Router Interface:

```
Router# config t
Router(config)# int g0/1
Router(config-if)# ip address 172.16.1.1 255.255.255.0
```

Cấu hình Secondary IP trên Router Interface:

Tại cổng fa0/1, ta tiếp tục khai báo secondary IP.

```
Router(config-if)# ip address 172.16.2.1 255.255.255.0 secondary
```

Chúng ta có thể thực hiện được nhiều câu lệnh IP addresses command với từ khóa "secondary".

So sánh các giao thức HSRP, VRRP & GLBP Protocol

Các giao thức hỗ trợ xây dựng mạng dự phòng first hop redundancy protocol bao gồm các giao thức HSRP, VRRP và GLBP. Chúng ta cần nhận biết sự khác biệt giữa các giao thức này để đưa ra quyết định lựa chọn giao thức nào sẽ được triển khai trên hạ tầng mạng.

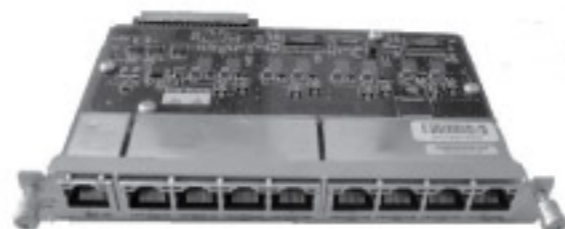
Bảng so sánh các giao thức HSRP, VRRP và GLBP Protocol

Đặc tính giao thức	HSRP	VRRP	GLBP
Tiêu chuẩn	Độc quyền của Cisco	Chuẩn IEEE	Độc quyền của Cisco
OSI Layer	Layer-3	Layer-3	Layer-2
Load Balancing	Không	Không	Có
Multicast Group IP address	224.0.0.2 trong version 1 và 224.0.0.102 trong version 2	224.0.0.18	224.0.0.102
Transport Port Number	UDP 1985	UDP 112	UDP 3222
Timers	Hello – 3 giây	Advertisement – 1 giây	Hello – 3 giây
	Hold – 10 giây	Master down time = 3*Advertisement Time + Skew TimeSkew Time = (256-Priority)/256	Hold – 10 giây
Tiến trình bầu chọn	Active Router: 1. Priority cao nhất 2. IP cao nhất	Master Router: (*) 1. Priority cao nhất 2. IP cao nhất	Active Virtual Gateway: 1. Priority cao nhất 2. IP cao nhất
Vai trò của Router	- Một Active Router, một Standby Router- một hoặc nhiều listening Router	- Một Active Router- Một hoặc nhiều Backup Router	- Một AVG (Active Virtual Gateway)- có thể có đến 4 AVF Router trong một group (Active Virtual Forwarder).- hỗ trợ tối đa 1024 virtual Router (GLBP group) trên mỗi physical interface.
Preempt	Vô hiệu hóa theo mặc định	Được kích hoạt theo mặc định	Vô hiệu hóa theo mặc định
Group VirtualMac Address	0000.0c07.acxx	0000.5e00.01xx	0007.b4xx.xxxx
Hỗ trợ IPv6	Có	Không	Có

Lưu ý: Trong môi trường VRRP group, Router có thể sử dụng IP thật đóng vai trò IP ảo cho group để trở thành Active Router bằng cách tự động tăng giá trị priority lên giá trị tối đa là 255, vì thế ta chỉ có thể cấu hình giá trị priority dao động [1-254].

Cấu hình HWIC-4ESW và HWIC-D-9ESW Switch module trên Cisco Router

4-port HWIC-4ESW và **9-port HWIC-D-9ESW** EtherSwitch HWIC (high speed WAN interface card) được hỗ trợ trên các dòng router Cisco 1800 (modular), Cisco 2800, và Cisco 3800 ISR (integrated services Routers). **HWIC-4ESW / HWIC-D-9ESW** được trang bị các cổng giao tiếp 10/100BaseT Layer 2 Ethernet có khả năng thực hiện chức năng Layer 3 Routing.



Một số hạn chế của EtherSwitch HWIC:

- Không thể cài đặt nhiều hơn 2 Ethernet Switch HWIC (network module) trên Router nhưng chúng lại không có khả năng tương tác trực tiếp với nhau.
- Các port trên HWIC-D-9ESW card không có khả năng cấp nguồn inline power.
- Tính năng Auto MDIX sẽ không được hỗ trợ trên các port của HWIC-D-9ESW card nếu ta tinh chỉnh thủ công speed hoặc duplex chứ không phải tùy chọn auto.
- Không hỗ trợ tiến trình cài đặt nóng online insertion/removal (OIR) EtherSwitch HWIC khi router đang hoạt động.
- Không hỗ trợ tính năng VTP pruning.
- Chỉ có thể cấu hình tối đa 200 secure MAC address trên mỗi module EtherSwitch HWIC.

Các bước cấu hình HWIC-4ESW / HWIC-D-9ESW:

Thiết lập VLAN instance:

Mỗi EtherSwitch HWIC hỗ trợ tối đa 15 VLAN, thực hiện các bước sau để cấu hình Fast Ethernet interface với vai trò Layer 2 access:

```
Router# vlan database
Router# vlan vlan_id
Router# exit
```

Cấu hình VTP:

```
Router# vlan database
Router(vlan)# vtp server
Router(vlan)# vtp domain domain_name
Router(vlan)# vtp password password_value
Router(vlan)# exit
```

Cấu hình Fast Ethernet Interface đóng vai trò Layer 2 Trunk:

```
Router(config)# interface fastethernet interface-id
Router(config-if)# switchport mode trunk
Router(config-if)# switchport trunk native vlan vlan-num
Router(config-if)# switchport trunk allowed vlan {add | except | none | remove} vlan 1 [,vlan[,vlan[,...]]
```

Cấu hình Fast Ethernet Interface với vai trò Layer 2 Access.

```
Router(config)# interface fastethernet interface-id
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan vlan_num
Router(config-if)# no shutdown
Router(config-if)# end
```

Một số loại HWIC etherswitch module khác có thể sử dụng được liệt kê trong bảng mô tả sau:

Product Number	Description
HWIC-4ESW	4-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC
HWIC-4ESW-POE*	4-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC với power daughter card có khả năng cấp nguồn PoE
HWIC-D-9ESW	9-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC
HWIC-D-9ESW-POE*	9-port Cisco EtherSwitch 10BASE-T/100BASE-TX autosensing HWIC với power daughter card có khả năng cấp nguồn PoE

Người biên soạn: Bùi Quốc Kỳ

Mặc dù đặc thù của ngành CNTT chuyên nghiệp là yêu cầu cao và công việc căng thẳng
Nhưng phần lớn dân IT đều tự hào và hài lòng với lựa chọn nghề nghiệp của mình

200 kĩ sư CNTT đã chia sẻ những trải nghiệm về

Stress & Tự hào

2 nguyên nhân chính dẫn đến stress cho dân IT



Phải tiếp tục bắt kịp công nghệ (31%)



Mất cân bằng giữa cuộc sống và công việc (28%)



95%

Tự hào vì đã chọn nghề IT

Sự kỳ vọng cao

Trong thời gian hành chính

57%

thời gian làm việc, các kĩ sư CNTT có kinh nghiệm được kỳ vọng sẵn sàng làm việc 24x7



CNTT luôn luôn có nhu cầu tăng trưởng

81%

được tuyển dụng ngay sau khi tốt nghiệp



Trong kỳ nghỉ

71%

thời gian làm việc, các kĩ sư CNTT mức trung bình KHÔNG được kỳ vọng làm việc 24x7



81% sẽ vẫn dẫn thân vào nghề IT, mặc dù có cơ hội chọn lại nghề nghiệp

81 phần trăm hứa hẹn với công ty rằng những thành viên còn lại trong dự án sẽ hoàn thành công việc trong khi họ đi nghỉ mát,

81%

Ngoài công việc, 72 phần trăm sẽ tự nguyện giúp đỡ gia đình, bạn bè, người thân về các vấn đề liên quan đến CNTT

72%

CHƯƠNG TRÌNH

VnPro

Tại: Trung tâm tin học VnPro
 Lúc: 08:30 - 11:30
 Thứ bảy, ngày 09/08/2014

KẾT NỐI NHÀ TUYỂN DỤNG CAREER 2014

Chương trình "VnPro kết nối nhà tuyển dụng - Career 2014" nằm trong chuỗi sự kiện miễn phí do VnPro tổ chức hàng tháng sẽ mang đến cho bạn bí quyết thành công trong học - ứng tuyển - làm việc chuyên nghiệp tại môi trường quốc tế. Đồng thời còn được trò chuyện cùng các chuyên gia IT để tìm hiểu và định hướng nghề nghiệp phù hợp, đào tạo về kỹ năng làm việc theo nhóm. Đặc biệt, tại chương trình "VnPro kết nối nhà tuyển dụng - Career 2014" sẽ mang lại cho bạn cơ hội ứng tuyển trực tiếp vào các công ty công nghệ hàng đầu Việt Nam.



CƠ HỘI NHẬN QUÀ HẤP DẪN TỪ BTC & DOANH NGHIỆP KHI THAM GIA CHƯƠNG TRÌNH MIỄN PHÍ THAM GIA 100%

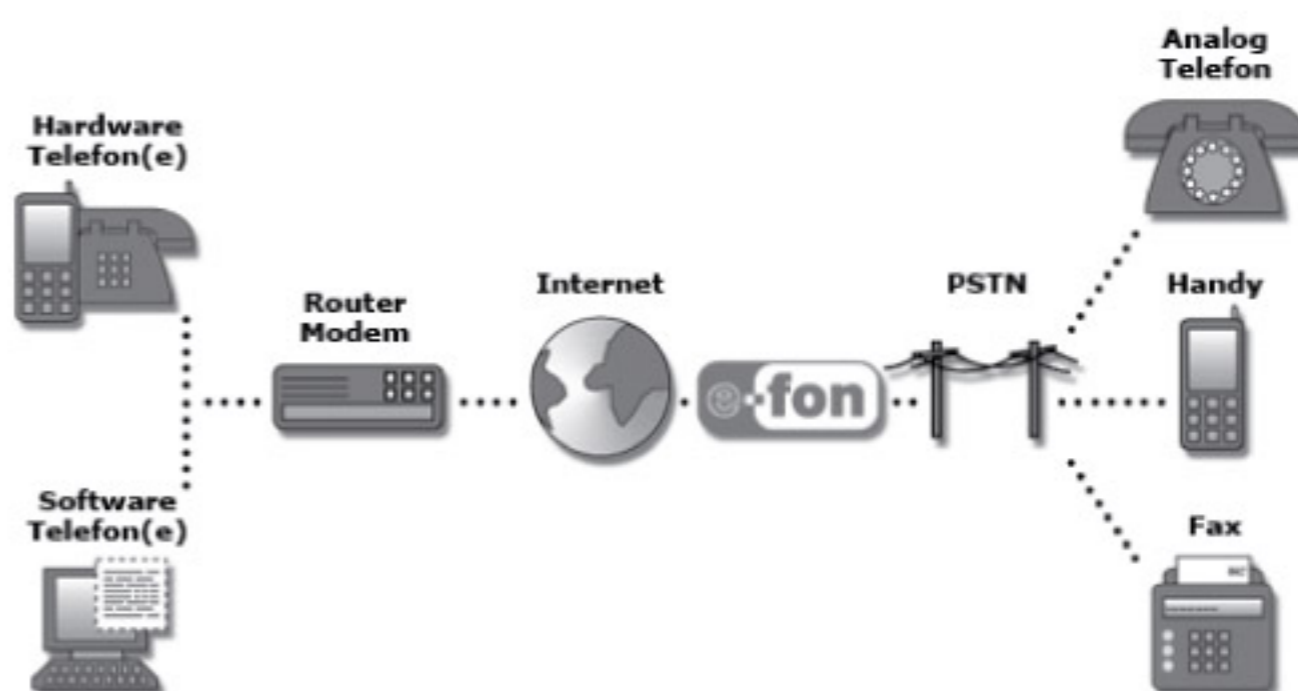


THÁNG 09 CHỦ ĐỀ

CÔNG NGHỆ VOIP THẾ KỶ 21

Giới thiệu:

Tín hiệu thoại được truyền đi trên hạ tầng cáp thoại, riêng biệt với lưu lượng dữ liệu thường được gửi đi trên hạ tầng cáp mạng LAN, WAN. Với cuộc công nghệ cách mạng VoIP, tín hiệu thoại và dữ liệu người dùng có thể trung chuyển trên cùng một hạ tầng mạng hợp nhất. Các doanh nghiệp có sẵn hạ tầng mạng Internet có thể ứng dụng giải pháp VoIP để tiết kiệm đáng kể chi phí. Chính vì vậy, VoIP dần trở thành một xu hướng tất yếu và nhu cầu tìm hiểu về công nghệ VoIP cũng ngày càng cao.



TÌM HIỂU CƠ CHẾ PHÂN MẢNH GÓI TIN

Giới thiệu

Mục đích của tài liệu này là trình bày cách thức hoạt động của tiến trình phân mảnh gói tin IP Fragmentation và cơ chế Path Maximum Transmission Unit Discovery (PMTUD), thảo luận một số tình huống liên quan đến hành vi của PMTUD khi kết hợp với các loại IP tunnel.

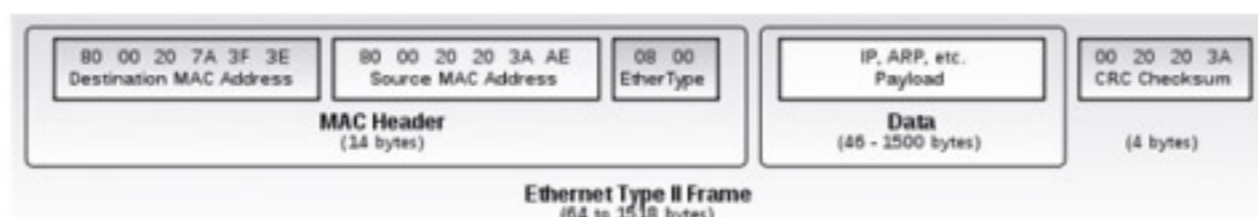
IP Fragmentation và tái phân mảnh Reassembly (Sự chia nhỏ hay sự phân mảnh gói tin IP và cách thức ghép nối lại).

Giao thức IP được thiết kế để sử dụng trên nhiều loại môi trường truyền dẫn transmission link như ethernet, serial, Mặc dù chiều dài tối đa của một IP datagram (dữ liệu) là 64K nhưng hầu hết việc truyền tải trên các kết nối đều giới hạn chiều dài tối đa của một packet (gói tin), còn được gọi là MTU. Giá trị của MTU phụ thuộc vào loại kết nối. Giao thức IP được thiết kế để chứa những giá trị MTU khác nhau, nó cho phép Routers chia nhỏ dữ liệu khi cần thiết. Các thiết bị mạng (Router, PC, ..) tiếp nhận có trách nhiệm ghép nối lại các phân mảnh trở lại kích thước đầy đủ như gói tin IP gốc.

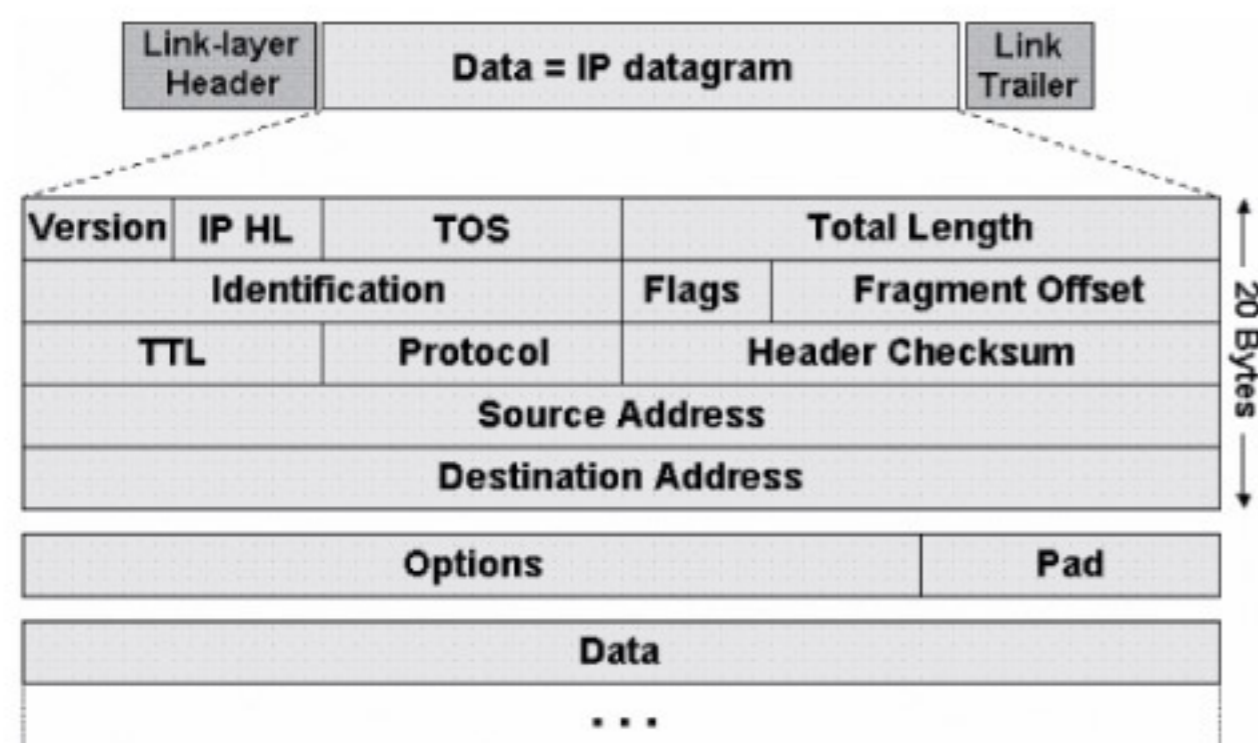
MTU trên một số môi trường mạng

Interface Type	Default MTU
Ethernet	1500
Serial	1500
ATM	4470
POS	4470

Vậy MTU chính là phần Data của Ethernet Frame.



Hình mô tả vị trí các (field) trường trong IP header.



IP Fragmentation là bẻ dữ liệu thành những phần nhỏ hơn và những phần này có thể được ghép lại sau đó.

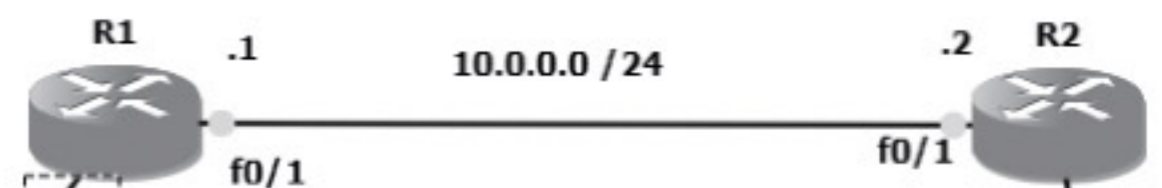
IP source, destination, identification, total length, and fragment offset fields, cùng với các bit "more fragments" và "don't fragment" trong trường flags của IP header thì được sử dụng cho IP fragmentation và reassembly.

- Trường Identification (16 bits): là một giá trị được gán bởi người gửi gói tin IP nhằm hỗ trợ trong việc ghép nối lại những gói tin đã bị chia nhỏ.
- Trường fragment offset (13 bits): chỉ ra nơi một gói tin đã bị chia nhỏ thuộc về gói tin IP gốc.
- Trường flags (3 bits):
 - Bit 0 được dành riêng (chưa sử dụng).
 - Bit 1 là DF bit (0 = "may fragment", 1 = "don't fragment").
 - Bit 2 là MF bit (0 = "last fragment," 1 = "more fragments")

Value	Bit 0 Reserved	Bit 1 DF	Bit 2 MF
0	0	May	Last
1	0	Do not	More

Ví dụ:

Lab 1: Identification, Fragment offset, flags.



Bài lab dùng GNS3 để giả lập. Đặt ip như hình vẽ. Dùng Wireshark bắt gói tại f0/1 của R1.

```
R1#sh int f0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Gt96k FE, address is c200.0494.0001 (bia c200.0494.0001)
Internet address is 10.0.0.1/24
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
R1#ping 10.0.0.2 size 5120 repeat 2
!!
"size 5120" = 20 bytes (IP header) + 5100 bytes (Data của gói IP).
"repeat 2" : gửi 2 gói tin
```

Để phân biệt 2 gói tin này thì R1 sẽ dùng trường Identification.

- Gói thứ nhất trong bài lab này có Identification là 0x000a
- Gói thứ hai có Identification là 0x000b

Nhưng khi gửi gói tin thứ nhất có Identification là 0x000a đi thì R1 sẽ tiến hành "Fragment" nó thành những gói nhỏ hơn cho phù hợp với giá trị MTU (Maximum Transmission Unit) của cổng fast-ethernet f0/1 là 1500 bytes. (Chú ý: nếu gói tin mà ta gửi đi có giá trị Data + ip header <= 1500 bytes thì sẽ không có những gói Fragment).

Vậy ta có gói tin thứ nhất là 5100 byte là Data (xét ở Layer 4) được chia nhỏ ra thành 4 Fragment packets là 1480 + 1480 + 1480 + 660. Sau đó tiếp tục đóng xuống Layer 3 thì ta sẽ có 4 gói tin (packets) lần lượt có MTU là 1500 + 1500 + 1500 + 680.

```

Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
  Total Length: 1500
  Identification: 0x000a (10)
  Flags: 0x01 (More Fragments)
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    ..1. ... = More fragments: Set
  Fragment offset: 0
  
```

Hình Fragment packet số 1

```

Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
  Total Length: 1500
  Identification: 0x000a (10)
  Flags: 0x01 (More Fragments)
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    ..1. ... = More fragments: Set
  Fragment offset: 1480
  
```

Hình Fragment packet số 2

```

Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
  Total Length: 1500
  Identification: 0x000a (10)
  Flags: 0x01 (More Fragments)
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    ..1. ... = More fragments: Set
  Fragment offset: 2960
  
```

Hình Fragment packet số 3

```

Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.2 (10.0.0.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-capable Transport))
  Total Length: 680
  Identification: 0x000a (10)
  Flags: 0x00
    0... .. = Reserved bit: Not set
    .0.. .. = Don't fragment: Not set
    ..0. .... = More fragments: Not set
  Fragment offset: 4440

[4 IPv4 Fragments (5100 bytes): #272(1480), #273(1480), #274(1480), #275(660)]
  [Frame: 272, payload: 0-1479 (1480 bytes)]
  [Frame: 273, payload: 1480-2959 (1480 bytes)]
  [Frame: 274, payload: 2960-4439 (1480 bytes)]
  [Frame: 275, payload: 4440-5099 (660 bytes)]
  [Fragment count: 4]
  [Reassembled IPv4 length: 5100]
  [Reassembled IPv4 data: 08006ce50002000000000000001896c0ababcdababcdabcd...]
Internet Control Message Protocol
  
```

Hình Fragment packet số 4, gói fragment cuối cùng chứa thông tin về những gói fragment trước đồng thời có cả ICMP header.

Original IP Datagram

Identification	Total length	DF May / Don't	MF Last / More	Fragment Offset
0x000a	5120	0	0	0

IP Fragments (Ethernet)

Identification	Total length	DF May / Don't	MF Last / More	Fragment Offset
0x000a	1500	0	1	0
0x000a	1500	0	1	1480
0x000a	1500	0	1	2960
0x000a	680	0	0	4440

R1 cũng làm tương tự với gói thứ hai có Identification là 0x000b.

Lab 2: Ping with df-bit = 1

```

"size 1501" = 20 bytes (IP header) + 1481 bytes (Data của gói IP).
R1#ping 10.0.0.2 size 1501 df-bit repeat 2
Packet sent with the DF bit set
..
Success rate is 0 percent (0/2)
  
```

Lý do packet có MTU 1501 > default MTU trên interface f0/1 nên bắt buộc packet này phải được fragment. Nhưng do ta ping có bật df-bit =1 (có nghĩa là không cho fragment gói tin này) nên kết quả ping không thành công.

Bây giờ ta thử ping với MTU <= 1500.

```

R1#ping 10.0.0.2 size 1500 df-bit repeat 2
Packet sent with the DF bit set
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 28/30/32 ms
R1#ping 10.0.0.2 size 1499 df-bit repeat 2
Packet sent with the DF bit set
!!
Success rate is 100 percent (2/2), round-trip min/avg/max = 16/28/40 ms
  
```

Do gói tin có MTU <= default MTU nên packet này không cần thiết phải fragment. Nên df-bit có bật hay tắt cũng không quan trọng. Ping vẫn thành công.

Người biên soạn: Nguyễn Đình Hiến

Welcome
Back to SCHOOL

VUI TỬ TRƯỞNG

từ 1/8 đến 31/8/14

MỚI
CCNP
version 2

VnPro



Bốc là trúng 100%
HOÀN HỌC PHÍ
lên đến **1.000.000 đ**

giảm thêm 10% cho học viên cũ

LỊCH KHAI GIẢNG THÁNG 8

Mã lớp	Tên khóa học	Ngày khai giảng	Ngày học	Giờ học	Thời gian
CHƯƠNG TRÌNH CCNA & CCNA SECURITY					
AK11	CCNAX (200-120)	02-08-2014	3 - 5 - 7	14:00 - 17:00	152 giờ
AK13		07-08-2014		08:30 - 11:30	
A9				18:30 - 21:30	
AK12		15-08-2014	2 - 4 - 6	08:30 - 11:30	
AK14				14:00 - 17:00	
A10			18:30 - 21:30		
AK15			21-08-2014	3 - 5 - 7	
A11		18:30 - 21:30			
AK16		29-08-2014		2 - 4 - 6	
A16			18:30 - 21:30		
AS3	CCNA Security	21-08-2014	3 - 5 - 7	18:30 - 21:30	100 giờ
AV1	CCNA Voice (640-461)	14-08-2014	3 - 5 - 7	18:30 - 21:30	
CHƯƠNG TRÌNH CCNP (version 2)					
P1-K2	ROUTE (300-101)	06-08-2014	2 - 4 - 6	08:30 - 11:30	140 giờ
P1-4				18:30 - 21:30	
P1-3		14-08-2014	3 - 5 - 7	18:30 - 21:30	
P2K2	SWITCH (300-115)	19-08-2014	3 - 5 - 7	08:30 - 11:30	120 giờ
P2K4				14:00 - 17:00	
P2-3				18:30 - 21:30	
P3-3	TSHOOT (300-135)	18-08-2014	2 - 4 - 6	18:30 - 21:30	140 giờ
CHƯƠNG TRÌNH CCIE					
EW1	CCIE WRITTEN (Version 5)	25-08-2014	2 - 4 - 6	18:30 - 21:30	120 giờ

ĐĂNG KÝ HỌC LIÊN HỆ

KIM LOAN

Email: kimloan@vnpro.org

Di động: 0936 393 167

THANH TRÂM

Email: thanhtram@vnpro.org

Di động: 0949 246 829

LIÊN HỆ DỰ ÁN ĐÀO TẠO, TƯ VẤN HỆ THỐNG MẠNG, THUÊ THIẾT BỊ, PHÒNG HỌC, MUA SÁCH

Website: www.vnpro.vn

Email: vnpro@vnpro.org

Điện thoại: (08) 35124257

Bản tin Dân Cisco - Được phát hành bởi Công Ty TNHH Tư Vấn & Dịch Vụ Chuyên Việt

Chịu trách nhiệm xuất bản: **Phạm Minh Tuấn**

Giấy phép xuất bản số: **69/QĐ - STTTT** Ngày ĐK: **26/10/2011**

Công ty in: **Sao Bàng Design**

Số lượng in: **2.000 cuốn/kỳ**

Kỳ hạn xuất bản: **1 kỳ/tháng**

VnPro[®]