

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC & KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH (CO3093)

THIẾT KẾ MẠNG MÁY TÍNH CHO MỘT DOANH NGHIỆP NHỎ

GVHD: Phạm Trần Vũ
Bùi Xuân Giang
Lớp: L05
SV thực hiện: Trần Bảo Kha 1913678
Duy Mạnh 1914121
Trần Lê Viết Khánh 1913758
Lương Đoàn Việt Hoàng 1913430

Tp. Hồ Chí Minh, Tháng 10/2021

Mục lục

1	Phân tích yêu cầu hệ thống mạng Trụ sở và Chi nhánh	3
1.1	Giới thiệu về B Bank Building	3
1.2	Phân tích yêu cầu của hệ thống mạng ngân hàng	3
2	Tổng quan kiến trúc mạng của hệ thống	3
2.1	Kiến trúc mạng bảo mật giữa Trụ sở và các chi nhánh	3
2.2	Kiến trúc mạng bảo mật cho các tòa nhà	4
3	Xác định các vùng có tải trọng lớn	5
4	Phân tích cấu trúc mạng được áp dụng	5
4.1	Phân chia sever trên các phân vùng	5
4.2	Kiến trúc mạng của Trụ sở ở Thành phố Hồ Chí Minh	5
4.3	Kiến trúc mạng của Chi nhánh ở Đà Nẵng và Nha Trang	6
5	Danh sách các trang thiết bị	6
5.1	Các thiết bị kết nối mạng	6
5.1.1	Switch: Cisco Catalyst WS-C2960-24TC-S, Cisco Catalyst 3560	6
5.1.2	Router: Cisco ISR4321/K9	7
5.1.3	Cable: AMP Cat 5e UTP	7
5.1.4	Access Point: Access Point PT	7
5.2	Các thiết bị workstation và sever	7
5.2.1	Workstations	7
5.2.2	DNS server	7
5.2.3	WEB server	7
5.2.4	DHCP server	7
6	Sơ đồ đi dây của hệ thống	8
6.1	Sơ đồ đi dây kết nối Trụ sở và Chi nhánh	8
6.2	Sơ đồ đi dây của Trụ sở ở Thành phố Hồ Chí Minh	8
6.3	Sơ đồ đi dây của Chi nhánh ở Đà Nẵng và Nha Trang	8
7	Tính toán throughput, banwitch và các thông số an toàn cho mạng máy tính	9
7.1	Các thông số mạng tại Trụ sở tại Thành phố Hồ Chí Minh	9
7.1.1	Đối với hệ thống mạng có dây	9
7.1.2	Đối với hệ thống mạng không dây	9
7.2	Các thông số mạng tại Chi nhánh tại Đà Nẵng và Nha Trang	10
7.2.1	Đối với hệ thống mạng có dây	10
7.2.2	Đối với hệ thống mạng không dây	10
8	Thiết kế sơ đồ mạng sử dụng Cisco Packet Tracer	11
8.1	Tổng quan	11
8.2	Trụ sở	11
8.3	Chi nhánh 1	12
8.4	Chi nhánh 2	12
9	Kiểm tra hệ thống mạng mô phỏng	13
9.1	Kiểm tra định tuyến giữa các Router	13
9.2	Kiểm tra kết nối giữa các VLAN với router	13
9.3	Kiểm tra InterVlan	13
9.4	Kiểm tra kết nối tới DMZ	13
9.5	Kiểm tra DNS server và Web server	13

10	Đánh giá hệ thống mạng đã thiết kế	14
10.1	Yêu cầu đối với hệ thống	14
10.2	Xác định các tài nguyên cần được bảo vệ, các mối đe dọa và biện pháp	14
10.3	Xử lý an toàn khi xảy ra sự cố	15
10.4	Nâng cấp hệ thống	15
10.5	Những hạn chế còn tồn tại	15
10.6	Định hướng phát triển hệ thống trong tương lai	15
11	Tài liệu tham khảo	16

Danh sách hình vẽ

1	Sơ đồ hệ thống	8
2	Sơ đồ của trụ sở	8
3	Sơ đồ của chi nhánh	9
4	Tổng quan	11
5	Trụ sở	11
6	Chi nhánh 1	12
7	Chi nhánh 2	12
8	Các router có thể ping được nhau	13
9	Các thiết bị trong Vlan sẽ ping được tới router	13
10	Vì cấu hình intervlan, các vlan khác nhau sẽ ping được với nhau thông qua router	13
11	Ping tới vùng DMZ	13
12	Kiểm tra DNS server và Web server	14

1 Phân tích yêu cầu hệ thống mạng Trụ sở và Chi nhánh

1.1 Giới thiệu về B Bank Building

Ngân hàng BBB(B Bank Building) gồm một Trụ sở chính được đặt tại Thành phố Hồ Chí Minh và 2 chi nhánh khác tại Đà Nẵng và Nha Trang. Trụ sở chính là một tòa building cao khoảng 7 tầng, tầng 1 là phòng kỹ thuật mạng và phòng tập trung dây mạng.

Chi nhánh có thiết kế tương tự như Trụ sở nhưng với quy mô nhỏ hơn. Gồm một tòa building 2 tầng, với phòng kỹ thuật mạng và phòng tập trung dây mạng nằm ở tầng 1.

BBB được xem như là một doanh nghiệp nh:.

- Với trụ sở: 100 workstations, 5 servers và 10 network equipments.
- Với chi nhánh: 50 workstations, 3 servers và 5 network equipments.

1.2 Phân tích yêu cầu của hệ thống mạng ngân hàng

Trụ sở ở Thành phố Hồ Chí Minh phải có kết nối với 2 chi nhánh ở Nha Trang và Đà Nẵng thông qua đường links WAN (Wide Area Network).

Hệ thống phải sử dụng công nghệ mới về hạ tầng mạng, với tốc độ upload/download là 100/1000 Mbps, cho phép kết nối không dây (Wireless).

Hệ thống mạng được tổ chức theo VLAN (Virtual Local Area Network).

Dùng kết hợp giữa Licensed and Open Source Softwares.

Kết nối với bên ngoài bằng 2 Leased line và 1 ADSL, sử dụng Load-balancing.

Hệ thống mạng được sử dụng với các ứng dụng văn phòng, client-server, đa phương tiện, database,...

Hệ thống được phải có tính bảo mật cao, an toàn khi xảy ra sự cố, dễ dàng nâng cấp hệ thống.

Đặc biệt, hệ thống có các thông số về lưu lượng và tải, dùng chung cho cả trụ sở và chi nhánh như sau:

- Lưu lượng và tải hệ thống tập trung khoảng 80% vào 2 khung giờ cao điểm là 9g-11g và 15g-16g.
- Server được sử dụng cho việc truy cập vào web, database, các thao tác cập nhật database, ... Tổng dung lượng upload và download vào khoảng 500MB/ngày.
- Mỗi workstation dùng để duyệt web, tải tài liệu, giao dịch với khách hàng, ... Tổng dung lượng upload và download vào khoảng 100MB/ngày.
- Máy laptop kết nối wifi dùng cho khách hàng truy xuất khoảng 50MB/ngày.

Hệ thống Mạng máy tính của ngân hàng BBB được dự toán cho mức độ phát triển 20% trong 5 năm (về số lượng người sử dụng, tải trọng mạng, mở rộng nhiều chi nhánh,...)

2 Tổng quan kiến trúc mạng của hệ thống

2.1 Kiến trúc mạng bảo mật giữa Trụ sở và các chi nhánh

Việc kết nối giữa trụ sở và chi nhánh sẽ thông qua đường link WAN (Wide area network)

- Wide Area Networks – WAN, là mạng được thiết lập để liên kết các máy tính của hai hay nhiều khu vực khác nhau, ở khoảng cách xa về mặt địa lý.
- Sử dụng mạng WAN và truy cập từ xa sẽ giúp ngân hàng BBB gia tăng hiệu quả công việc nhờ việc chia sẻ và trao đổi thông tin giữa trụ sở và các chi nhánh thực hiện một cách dễ dàng. Bên cạnh đó thông tin được chia sẻ và xử lý bởi nhiều máy tính dưới sự giám sát của nhiều người, đảm bảo tính chính xác và hiệu quả cao.
- Ta sẽ sử dụng 2 đường Leased Line (kênh thuê riêng) để kết nối giữa Trụ sở và 2 chi nhánh. Tuy giá thành của đường Leased line khá cao, nhưng việc sử dụng đường dây này mang lại những lợi ích như:

- Kết nối Internet chuyên dụng, tốc độ cao: Trong quá trình kết nối, Leased line không chia sẻ băng thông với các doanh nghiệp hoặc người dùng khác. Dịch vụ đảm bảo băng thông cố định, hạn chế xảy ra sự cố tắc nghẽn trong giờ cao điểm. Phạm vi tốc độ của kênh thuê riêng có thể lên đến 2Mbps – 10Gbps.
 - Tốc độ upload và download cân bằng: Leased line đóng vai trò là cổng kết nối quốc tế nên có tốc độ tải lên và tải xuống đảm bảo cân bằng trong mọi thời điểm hoạt động. Theo đó, tốc độ tải càng cao thì kết nối tổng càng vận hành nhanh chóng và hiệu quả hơn. Đối với doanh nghiệp, điều này sẽ tạo điều kiện thuận lợi cho việc gửi email, truy cập dữ liệu trên các máy chủ hay thực hiện cuộc gọi VoIP.
 - Đảm bảo tính riêng tư và bảo mật cao: Leased line là đường truyền kết nối chuyên dụng dành riêng cho doanh nghiệp, công ty nên có thể đảm bảo tính riêng tư và bảo mật cao. Bên cạnh đó, hệ thống kết nối còn được quản lý và bảo vệ từ nhà cung cấp dịch vụ, tránh sự xâm nhập của các đối tượng xấu.
- Sử dụng giao thức định tuyến OSPF (Open Shortest Path First): Mỗi router khi chạy giao thức sẽ gửi các trạng thái đường link của nó cho tất cả các router trong vùng (area). Sau một thời gian trao đổi, các router sẽ đồng nhất được bảng cơ sở dữ liệu trạng thái đường link (Link State Database – LSDB) với nhau, mỗi router đều có được bản đồ mạng của cả vùng. Từ đó mỗi router sẽ chạy giải thuật Dijkstra tính toán ra một cây đường đi ngắn nhất (Shortest Path Tree) và dựa vào cây này để xây dựng nên bảng định tuyến.
 - Đường truyền ADSL sẽ được dùng cho kết nối wifi trong ngân hàng và không được kết nối vào hệ thống mạng nội bộ của ngân hàng nhằm ngăn chặn các kết nối lạ thông qua mạng không dây. Wifi được đưa vào nhằm mục đích phục vụ cho nhu cầu truy cập internet tại chỗ của khách hàng cũng như nhân viên ngân hàng BBB.

Hệ thống sử dụng 1 router chính để kết nối các workstation ở các tầng với hệ thống server, và kết nối ra ngoài Internet.

Kết nối Internet từ bên ngoài đi vào hệ thống mạng công ty thông qua thiết bị trung gian gateway và hệ thống tường lửa nhằm tăng độ bảo mật cho hệ thống mạng của ngân hàng BBB. Kết nối này được truyền qua đường leased line do ISP cung cấp.

Kết nối từ các Chi nhánh đi vào hệ thống mạng Trụ sở ngân hàng thông qua hệ thống tường lửa nhằm đề phòng trường hợp giả mạo. Kết nối này được truyền qua đường leased line do ISP cung cấp.

Hệ thống DMZ được sử dụng cho các tòa nhà để tăng độ an toàn cho hệ thống mạng. Các kết nối từ bên ngoài vào được xử lý, nếu an toàn sẽ cho phép truy cập đến hệ thống server. Chi tiết về cấu trúc của hệ thống DMZ sẽ được trình bày ở mục 2.2.

2.2 Kiến trúc mạng bảo mật cho các tòa nhà

Kiến trúc mạng được xây dựng theo mô hình 3 lớp, gồm: vùng mạng Internet, vùng mạng DMZ và vùng mạng nội bộ. Trong đó, ta đặt firewall thứ nhất giữa router kết nối với vùng mạng Internet và vùng DMZ, firewall thứ hai được đặt giữa vùng mạng DMZ và vùng mạng nội bộ.

- Phân vùng Internet: Còn gọi là mạng ngoài, kết nối với mạng Internet của ISP(Internet Service Provider).
- Phân vùng DMZ: Là nơi chứa các thông tin cho phép người dùng từ Internet truy xuất vào và chấp nhận các rủi ro tấn công từ Internet.Vùng này sẽ triển khai các dịch vụ như: Web server, Email server, DNS server, FTP server, ...
- Phân vùng mạng nội bộ: Là nơi đặt các thiết bị mạng, máy trạm và máy chủ thuộc mạng nội bộ của đơn vị.

Mỗi tòa nhà được xây dựng theo kiến trúc mạng LAN (Local Area Network). Việc sử dụng mạng LAN giúp nhân viên trong ngân hàng BBB sử dụng chung các tài nguyên quan trọng như máy in, máy fax, ổ đĩa CD-ROM, các phần mềm ứng dụng và các thông tin quan trọng khác.

3 Xác định các vùng có tải trọng lớn

Theo như thiết kế hạ tầng mạng của ngân hàng BBB như trên, các vùng có tải trọng lớn sẽ là phân vùng DMZ của các tòa nhà (phân vùng chứa các web server, mail server, DNS server, ... cho phép những người lạ truy cập vào). Để sử dụng tối ưu các nguồn lực, tối đa hóa thông lượng, giảm thời gian đáp ứng và tránh tình trạng quá tải trên máy chủ, ta sẽ sử dụng các load-balancing (cân bằng tải).

Các lợi ích khi sử dụng phương pháp cân bằng tải:

- Tăng khả năng đáp ứng, tránh tình trạng quá tải trên máy chủ, đảm bảo tính linh hoạt và mở rộng cho hệ thống.
- Tăng độ tin cậy và khả năng dự phòng cho hệ thống: Sử dụng cân bằng tải giúp tăng tính HA (High Availability) cho hệ thống, đồng thời đảm bảo cho người dùng không bị gián đoạn dịch vụ khi xảy ra lỗi sự cố lỗi tại một điểm cung cấp dịch vụ.
- Tăng tính bảo mật cho hệ thống: Thông thường khi người dùng gửi yêu cầu dịch vụ đến hệ thống, yêu cầu đó sẽ được xử lý trên bộ cân bằng tải, sau đó thành phần cân bằng tải mới chuyển tiếp các yêu cầu cho các máy chủ bên trong. Quá trình trả lời cho khách hàng cũng thông qua thành phần cân bằng tải, vì vậy mà người dùng không thể biết được chính xác các máy chủ bên trong cũng như phương pháp phân tải được sử dụng.

4 Phân tích cấu trúc mạng được áp dụng

4.1 Phân chia sever trên các phân vùng

Để đảm bảo an toàn và bảo mật thông tin, ngân hàng BBB phải phân chia các dịch vụ server trong phân vùng DMZ và phân vùng nội bộ. Theo như thiết kế tổng quan ở trên, phân vùng DMZ sẽ chứa các server cho phép người dùng giao tiếp với ngân hàng BBB như web server, mail server, ... Còn phân vùng nội bộ chỉ cho phép nhân viên công ty truy cập.

Các dịch vụ server được phân chia như sau:

STT	Tên Sever	Chức năng	Phân vùng
1	Web Server	Xử lý các yêu cầu client thông qua giao thức HTTP và 1 số giao thức liên quan khác	Phân vùng DMZ
2	Mail Sever	Nhận gửi và lưu trữ các mail từ khách hàng	Phân vùng DMZ
3	DNS Server	Chuyển đổi tên miền ra địa chỉ IP	Phân vùng DMZ
4	DHCP Server	Cấp phát địa chỉ IP động cùng các cấu hình liên quan đến gateway và subnet mask	Phân vùng DMZ
5	Database Server	Lưu trữ thông tin nhân viên	Phân vùng nội bộ
6	File Server	Chia sẻ thông tin của nhân viên	Phân vùng nội bộ
7	Backup Server	Sao lưu thông tin để tránh khi có sự cố xảy ra	Phân vùng nội bộ

4.2 Kiến trúc mạng của Trụ sở ở Thành phố Hồ Chí Minh

Trụ sở của ngân hàng BBB ở Thành phố Hồ Chí Minh là một tòa nhà 7 tầng, trong đó ở tầng 1 được trang bị phòng Kỹ thuật mạng và Cabling Central Local.

Ta cũng giả sử các workstations ở từng phòng ban sẽ cùng 1 mạng LAN.

Tất cả các router, switch, device sẽ được đặt ở ở Cabling Central Local tại tầng 1 và các cáp nối sẽ được kéo đến các workstation được sử dụng.

Từ các mô tả trên, ta có sơ đồ phòng ban và phân bố các network equipment, các work-station như sau:

Tầng	Phòng, ban	Các thiết bị
Tầng 1	Server	Switch, Servers, Server PC
Tầng 2	Điều hành	Switch, Workstations, Access Point
Tầng 3	Khách hàng	Switch, Workstations
Tầng 4	Dịch vụ	Switch, Workstations
Tầng 5	Kiểm toán	Switch, Workstations, Access Point
Tầng 6	Quản lý rủi ro	Switch, Workstations
Tầng 7	Marketing	Switch, Workstations, Access Point

Sơ đồ VLAN tại trụ sở được chia bằng IP sau:

Tầng	Phòng, ban	VLAN	Địa chỉ IP	Miền cung cấp IP
Tầng 1	Server	VLAN1	192.168.1.0/24	192.168.1.2 -> 192.168.1.254
Tầng 2	Điều hành	VLAN20	192.168.20.0/24	192.168.20.2 -> 192.168.20.254
Tầng 3	Khách hàng	VLAN30	192.168.30.0/24	192.168.30.2 -> 192.168.30.254
Tầng 4	Dịch vụ	VLAN40	192.168.40.0/24	192.168.40.2 -> 192.168.40.254
Tầng 5	Kiểm toán	VLAN50	192.168.50.0/24	192.168.50.2 -> 192.168.50.254
Tầng 6	Quản lý rủi ro	VLAN60	192.168.60.0/24	192.168.60.2 -> 192.168.60.254
Tầng 7	Marketing	VLAN70	192.168.70.0/24	192.168.70.2 -> 192.168.70.254

4.3 Kiến trúc mạng của Chi nhánh ở Đà Nẵng và Nha Trang

Chi nhánh của ngân hàng BBB ở Đà Nẵng và Nha Trang là một tòa nhà 2 tầng, trong đó ở tầng 1 được trang bị phòng Kỹ thuật mạng và Cabling Central Local.

Ta cũng giả sử các workstations ở từng phòng ban sẽ cùng 1 mạng LAN.

Tất cả các router, switch device sẽ được đặt ở ở Cabling Central Local tại tầng 1 và các cáp nối sẽ được kéo đến các workstation được sử dụng.

Từ các mô tả trên, ta có sơ đồ phòng ban và phân bố các network equipment, các work-station như sau:

Tầng	Phòng, ban	Các thiết bị
Tầng 1	Server	Switch, Servers
Tầng 1	Điều hành	Switch, Workstations, Access Point
Tầng 2	Khách hàng	Switch, Workstations, Access Point

Sơ đồ VLAN tại chi nhánh 1 được chia bằng IP dưới đây, sơ đồ VLAN tại chi nhánh 2 cũng được chia tương tự như trên với VLAN110, 120, 130.

Tầng	Phòng, ban	VLAN	Địa chỉ IP	Miền cung cấp IP
Tầng 1	Server	VLAN80	192.168.80.0/24	192.168.80.2 -> 102.168.80.254
Tầng 1	Điều hành	VLAN90	192.168.90.0/24	192.168.90.2 -> 102.168.90.254
Tầng 2	Khách hàng	VLAN100	192.168.100.0/24	192.168.100.2 -> 102.168.100.254

5 Danh sách các trang thiết bị

5.1 Các thiết bị kết nối mạng

5.1.1 Switch: Cisco Catalyst WS-C2960-24TC-S, Cisco Catalyst 3560

- Cisco WS-C2960+24TC-S được sử dụng chính để kết nối các thiết bị trong hệ thống mạng LAN với nhau. Nó thực hiện các tính năng quản lý thông dụng như SPAN, CiscoView, giao thức CDP, giao thức Trunking ảo (VTP)...
- Các thiết bị chuyển mạch dòng Cisco Catalyst 3560 là dòng sản phẩm thiết bị chuyển mạch cấp độ doanh nghiệp, cấu hình cố định trong đó có chuẩn IEEE 802.3af và chức năng cấp nguồn qua Ethernet tiên tiêu chuẩn trong các cấu hình Gigabit Ethernet và Fast Ethernet. Đây là những thiết bị chuyển mạch lớp truy nhập lý tưởng cho truy nhập mạng LAN doanh nghiệp nhỏ hay môi trường văn phòng chi nhánh. Kết hợp các cấu hình 10/100/1000 và PoE cho năng suất tối ưu và bảo vệ

đầu tư, các thiết bị này giúp bạn triển khai các ứng dụng mới như điện thoại IP, truy nhập vô tuyến, giám sát video, các hệ thống quản lý tòa nhà và kiosk video từ xa.

5.1.2 Router: Cisco ISR4321/K9

Bộ định tuyến Router Cisco ISR4321/K9 được thiết kế để cung cấp các dịch vụ nâng cao cho môi trường chỉ nhánh doanh nghiệp nhỏ. Nó cung cấp thông lượng 50Mbps theo mặc định. Cisco ISR4321/K9 là bộ định tuyến Cisco với gói Bundle w / UC & SEC, và CUBE-10 được thừa hưởng các tính năng và sự khác biệt chủ yếu về khả năng hoạt động và số lượng mô đun giao diện mạng (NIM) và khe cắm mô đun dịch vụ nâng cao (SM-X) được hỗ trợ.

5.1.3 Cable: AMP Cat 5e UTP

Cáp Cat. 5e (viết tắt của Category 5, enhanced) là loại cáp tương tự như cáp Cat. 5 nhưng đáp ứng được các tiêu chuẩn cao hơn trong việc truyền dữ liệu.

Trước đây, Cat. 5 rất phổ biến trong các hệ thống mạng, tuy nhiên ngày nay Cat. 5e gần như thay thế hoàn toàn Cat. 5 trong quá trình lắp đặt mới. Hơn nữa, Cat. 5e ít bị nhiễu chéo (cross-talk) hơn so với Cat. 5 và hỗ trợ ứng dụng Gigabit Ethernet (tốc độ truyền tín hiệu 1000 Mbps).

5.1.4 Access Point: Access Point PT

Một điểm truy cập Access Point kết nối người dùng với những người dùng khác trong cùng một mạng. Ngoài ra chúng còn đóng vai trò là điểm kết nối giữa mạng WLAN và mạng dây cố định. Trong một khu vực mạng được xác định thì mỗi điểm truy cập Access Point có thể phục vụ nhiều người dùng. Nếu khi mọi người di chuyển ra ngoài phạm vi của một điểm truy cập, thì chúng sẽ tự động được chuyển sang điểm tiếp theo.

5.2 Các thiết bị workstation và sever

5.2.1 Workstations

Là các thiết bị máy tính với cấu hình cơ bản, đáp ứng nhu cầu sử dụng và làm việc của nhân viên ngân hàng.

5.2.2 DNS server

Là máy chủ chứa cơ sở dữ liệu dùng cho việc chuyển đổi giữa tên miền và địa chỉ IP.

5.2.3 WEB server

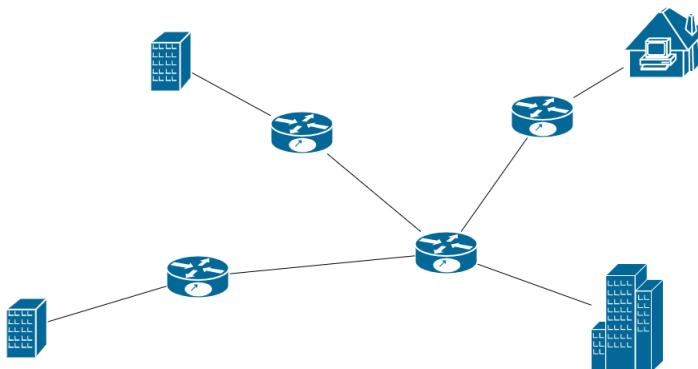
Là máy chủ cài đặt các chương trình phục vụ các ứng dụng web, cụ thể ở đây là trang web của ngân hàng: bbbbank.com.

5.2.4 DHCP server

Là máy chủ kết nối mạng, có chức năng gửi trả thông tin cần thiết khi DHCP client (máy trạm) yêu cầu. Bên cạnh đó, DHCP server còn giúp truyền thông tin đến các thiết bị sao cho hợp lý, thực hiện cấu hình cổng mặc định hay Subnet mask.

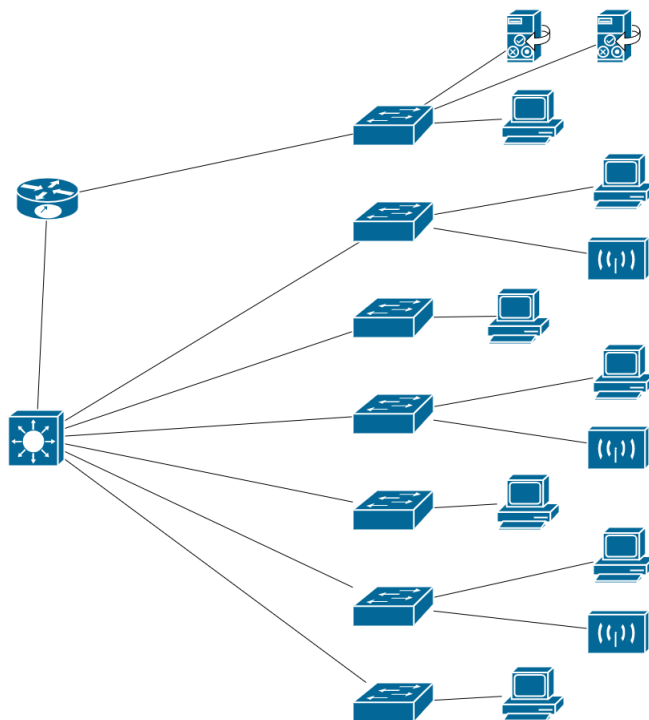
6 Sơ đồ đi dây của hệ thống

6.1 Sơ đồ đi dây kết nối Trụ sở và Chi nhánh



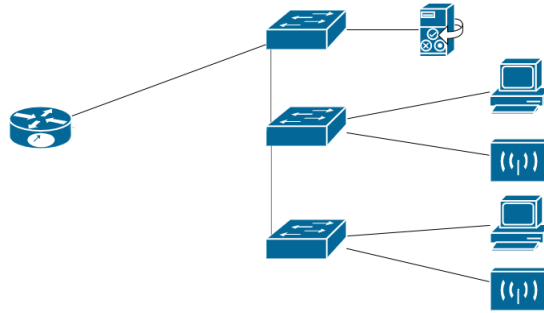
Hình 1: Sơ đồ hệ thống

6.2 Sơ đồ đi dây của Trụ sở ở Thành phố Hồ Chí Minh



Hình 2: Sơ đồ của trụ sở

6.3 Sơ đồ đi dây của Chi nhánh ở Đà Nẵng và Nha Trang



Hình 3: Sơ đồ của chi nhánh

7 Tính toán throughput, banwitch và các thông số an toàn cho mạng máy tính

- Băng thông là một giá trị lý thuyết đề cập đến lượng dữ liệu tối đa có thể được truyền từ điểm A đến điểm B trong một khoảng thời gian nhất định. Đó là tiềm năng lý thuyết cho dữ liệu để truyền trong một khoảng thời gian xác định. Đây là một số liệu hiệu suất được sử dụng để đo dung lượng truyền qua hệ thống truyền thông mạng.
- Thông lượng tương tự nhưng hơi khác so với băng thông. Thông lượng là một giá trị đạt được đề cập đến lượng dữ liệu thực tế được truyền từ điểm A đến điểm B trong một khoảng thời gian xác định

Việc xác định thông lượng và băng thông trong một hệ thống mạng là rất quan trọng vì nó giúp người quản trị mạng xác định được đường truyền để hệ thống mạng hoạt động trơn tru đồng thời tiết kiệm chi phí thuê mặt bằng.

7.1 Các thông số mạng tại Trụ sở tại Thành phố Hồ Chí Minh

Giả sử rằng trong một ngày ngân hàng làm việc 8 tiếng và các khung giờ cao điểm thuộc (9h -11h) và (15h-16h) nên ta có kết quả tính như sau:

7.1.1 Đối với hệ thống mạng có dây

Server: có 5 server và tổng dung lượng upload/download là 500 MB/day.

- Bandwidth (Băng thông) = $\frac{(5*500*0.8)}{(3*3600)} = 0.185 \text{ MB/s}$
- Throughput (Thông lượng) = $\frac{(5*500)}{(8*3600)} = 0.087 \text{ MB/s}$

Workstation: có 100 workstations và tổng dung lượng upload/download là 100 MB/day

- Bandwidth (Băng thông) = $\frac{(100*100*0.8)}{(3*3600)} = 0.741 \text{ MB/s}$
- Throughput (Thông lượng) = $\frac{(100*100)}{(8*3600)} = 0.347 \text{ MB/s}$

7.1.2 Đối với hệ thống mạng không dây

Laptop kết nối với Wifi cho khách hàng truy xuất có tổng dung lượng upload/download là 50MB/day và giả sử số lượng khách hàng truy cập trong một ngày khoảng 150 lượt và khách hàng truy cập vào khung giờ cao điểm khoảng 80 lượt

- Bandwidth (Băng thông) = $\frac{(80*50*0.8)}{(3*3600)} = 0.296 \text{ MB/s}$

- Throughput (Thông lượng) = $\frac{(150*50)}{(8*3600)} = 0.260 \text{ MB/s}$

Tổng bandwidth tại trụ sở là : $0.185 + 0.741 + 0.296 = 1.222 \text{ MB/s} = 9.776 \text{ Mbps}$

Tổng throughput tại trụ sở là : $0.087 + 0.347 + 0.296 = 0.73 \text{ MB/s} = 5.84 \text{ Mbps}$

Để đảm bảo hệ thống hoạt động ổn định khi có nhiều phát triển hơn trong 5 năm tới. Ta sẽ dự trữ thêm 20%:

- Bandwidth = $1.466 \text{ MB/s} = 11.7312 \text{ Mbps}$
- Throughput = $0.876 \text{ MB/s} = 7.008 \text{ Mbps}$

7.2 Các thông số mạng tại Chi nhánh tại Đà Nẵng và Nha Trang

7.2.1 Đối với hệ thống mạng có dây

Server: có 3 server và tổng dung lượng upload/download là 500 MB/day

- Bandwidth (Băng thông) = $\frac{(3*500*0.8)}{(3*3600)} = 0.111 \text{ MB/s}$
- Throughput (Thông lượng) = $\frac{(3*500)}{(8*3600)} = 0.052 \text{ MB/s}$

Workstation: có 50 workstations và tổng dung lượng upload/download là 100 MB/day

- Bandwidth (Băng thông) = $\frac{(50*100*0.8)}{(3*3600)} = 0.371 \text{ MB/s}$
- Throughput (Thông lượng) = $\frac{(50*100)}{(8*3600)} = 0.174 \text{ MB/s}$

7.2.2 Đối với hệ thống mạng không dây

Laptop kết nối với Wifi cho khách hàng truy xuất có tổng dung lượng upload/download là 50MB/d và giả sử số lượng khách hàng truy cập trong một ngày khoảng 100 lượt và khách hàng truy cập vào khung giờ cao điểm khoảng 50 lượt

- Bandwidth (Băng thông) = $\frac{(50*50*0.8)}{(3*3600)} = 0.231 \text{ MB/s}$
- Throughput (Thông lượng) = $\frac{(100*50)}{(8*3600)} = 0.174 \text{ MB/s}$

Tổng bandwidth tại một chi nhánh là : $0.111 + 0.371 + 0.231 = 0.712 \text{ MB/s} = 5.699 \text{ Mbps}$

Tổng throughput tại một chi nhánh là : $0.052 + 0.174 + 0.174 = 0.4 \text{ MB/s} = 3.2 \text{ Mbps}$

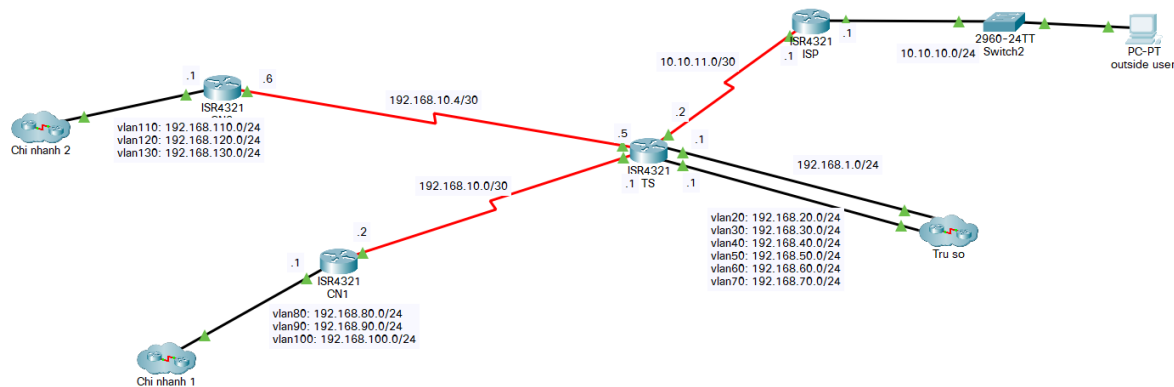
Để đảm bảo hệ thống hoạt động ổn định khi có nhiều phát triển hơn trong 5 năm tới. Ta sẽ dự trữ thêm 20%:

- Bandwidth = $0.8544 \text{ MB/s} = 6.8352 \text{ Mbps}$
- Throughput = $0.48 \text{ MB/s} = 3.84 \text{ Mbps}$

Qua việc tính bandwidth và throughput ta có thể nhận định rằng hệ thống của ta vẫn sẽ hoạt động tốt trong vòng 5 năm tới

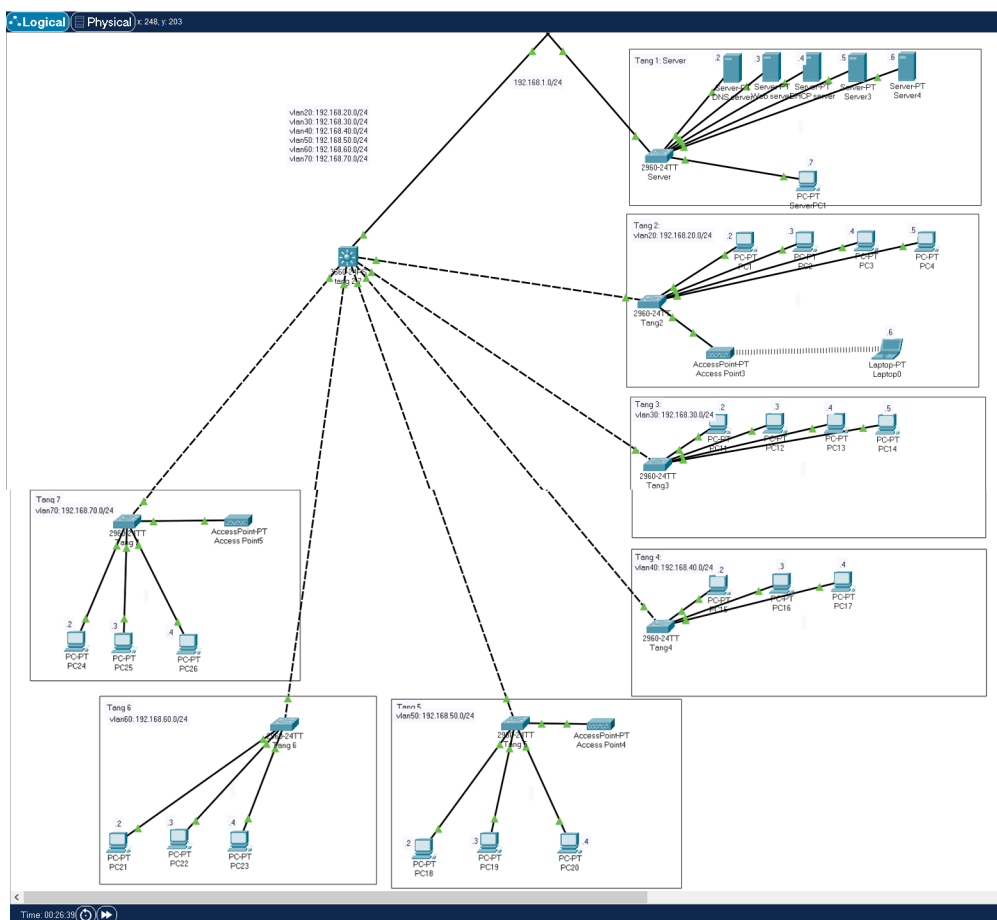
8 Thiết kế sơ đồ mạng sử dụng Cisco Packet Tracer

8.1 Tổng quan



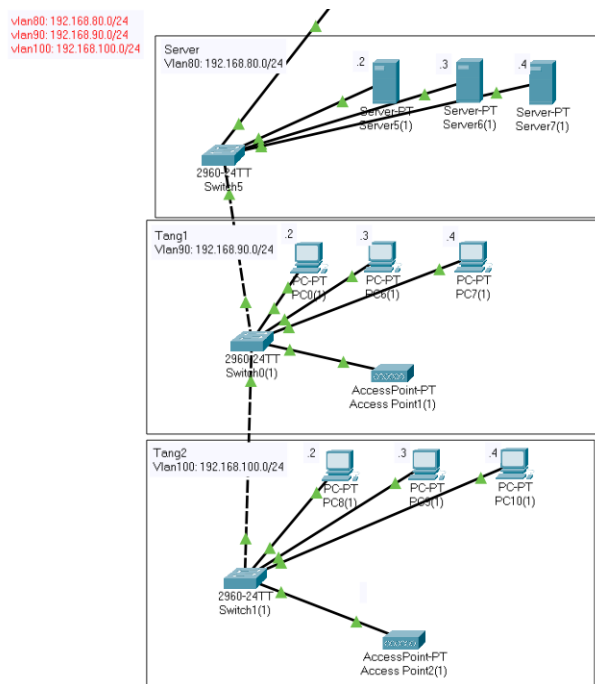
Hình 4: Tổng quan

8.2 Trụ sở



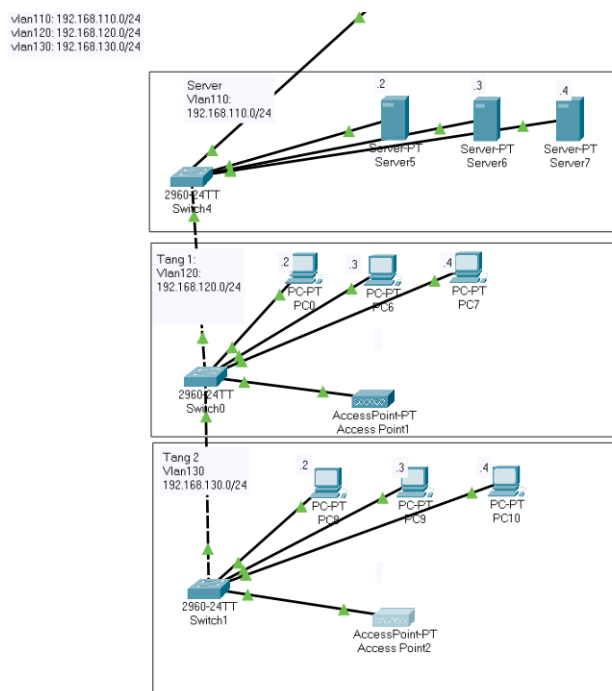
Hình 5: Trụ sở

8.3 Chi nhánh 1



Hình 6: Chi nhánh 1







8.4 Chi nhánh 2



Hình 7: Chi nhánh 2






9 Kiểm tra hệ thống mạng mô phỏng

9.1 Kiểm tra định tuyến giữa các Router

Fire	Last Status	Source	Destination	Type
	Successful	CN2	TS	ICMP
	Successful	CN1	TS	ICMP
	Successful	ISP	TS	ICMP
	Successful	TS	ISP	ICMP
	Successful	TS	CN2	ICMP
	Successful	TS	CN1	ICMP






Hình 8: Các router có thể ping được nhau

9.2 Kiểm tra kết nối giữa các VLAN với router

Fire	Last Status	Source	Destination	Type
	Successful	ServerPC1	TS	ICMP
	Successful	Tang1PC	TS	ICMP
	Successful	Tang7PC	TS	ICMP
	Successful	Tang5PC	TS	ICMP
	Successful	outside user	ISP	ICMP






Hình 9: Các thiết bị trong Vlan sẽ ping được tới router

9.3 Kiểm tra InterVlan

Fire	Last Status	Source	Destination	Type
	Successful	Tang2PC	Tang3PC	ICMP
	Successful	Tang3PC	Tang7PC	ICMP
	Successful	Tang7PC	Tang2PC	ICMP
	Successful	Tang3PC	Tang4PC	ICMP
	Successful	Tang4PC	Tang7PC	ICMP

Hình 10: Vì cấu hình intervlan, các vlan khác nhau sẽ ping được với nhau thông qua router

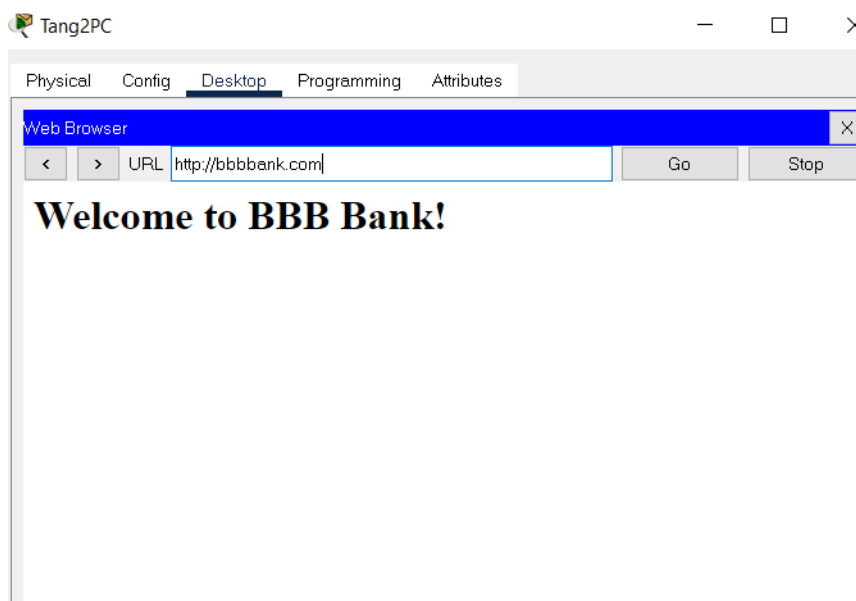
9.4 Kiểm tra kết nối tới DMZ

Fire	Last Status	Source	Destination	Type
	Successful	CN2PC	DNS server	ICMP
	Successful	CN1PC	Web server	ICMP
	Successful	outside user	Server3	ICMP
	Successful	Tang1PC	DHCP server	ICMP
	Successful	Tang2PC	Web server	ICMP

Hình 11: Ping tới vùng DMZ

9.5 Kiểm tra DNS server và Web server

Khi thiết lập DNS server của máy là 192.168.1.2 (địa chỉ của DNS server trụ sở) thì khi truy cập bbbbank.com thì sẽ phân giải ra địa chỉ 192.168.1.2 (địa chỉ của Web server trụ sở) browser hiển thị như dưới đây, chứng tỏ 2 server trên đã hoạt động.



Hình 12: Kiểm tra DNS server và Web server

10 Đánh giá hệ thống mạng đã thiết kế

10.1 Yêu cầu đối với hệ thống

Ngân hàng BBB phải xử lý một lượng lớn thông tin trong các hoạt động. Bên cạnh đó, dữ liệu giao dịch của khách hàng được xem là quan trọng nhất và phải được bảo mật một cách cẩn trọng. Do đó hạ tầng mạng được xây dựng phải đảm bảo được cái tiêu chí:

- Đảm bảo được đường truyền kết nối giữa Trụ sở ở Thành phố Hồ Chí Minh và hai Chi nhánh ở Đà Nẵng và Nha Trang luôn ổn định, đặc biệt trong các khung giờ cao điểm.
- Kiểm soát việc truy cập của mạng lưới, nhất là các hoạt động diễn ra trên server và không cho phép người ngoài có thể truy cập vào hệ thống nội bộ.
- Chi phí lắp đặt hạ tầng mạng phù hợp, tiết kiệm.
- Hệ thống đáp ứng được khả năng mở rộng trong tương lai của ngân hàng BBB.

10.2 Xác định các tài nguyên cần được bảo vệ, các mối đe dọa và biện pháp

- Các tài nguyên cần được bảo vệ
 - Phần cứng: Các máy chủ mạng, các máy trạm, các thiết bị mạng như Router, Access Servers..
 - Phần mềm: Hệ điều hành của các máy chủ Unix, Windows NT.., các chương trình ứng dụng quản lý tài khoản, tín dụng, các chương trình kế toán, tự động hóa văn phòng, truyền dữ liệu, ATM..
 - Dữ liệu: Đây là phần quan trọng cần được bảo vệ nhất của ngân hàng. Dữ liệu này sẽ gồm các dữ liệu tài khoản liên quan đến khách hàng.
 - Tài liệu: Các công văn, báo cáo, tài liệu, sách vở, tài liệu hướng dẫn sử dụng.
- Các mối đe dọa
 - Mối đe dọa từ bên ngoài: Nguy cơ bị nghe trộm, thay đổi thông tin truyền đi trên mạng công cộng (PSTN). Đây là một nguy cơ tiềm ẩn và ảnh hưởng trực tiếp đến hoạt động kinh doanh của ngân hàng. Hacker có thể sử dụng các công cụ, thiết bị đặc biệt để móc nối vào hệ thống cáp truyền thông của ngân hàng để nghe trộm thông tin, nguy hiểm hơn hacker có thể sửa chữa, thay đổi nội dung thông tin đó – ví dụ nội dung của điện chuyển tiền, thanh toán .. gây ra những tổn thất nghiêm trọng

- Mối đe dọa từ bên trong: Nhân viên hoặc người trong nội bộ hệ thống có cơ hội truy cập vào các tài nguyên hệ thống. Đối với hệ thống như ngân hàng nếu người sử dụng trong mạng có ý muốn truy cập vào những tài nguyên của hệ thống thì họ sẽ gây nên một mối đe dọa cho mạng.
- Biện pháp
 - Bảo mật mức mạng: Bảo mật đường truyền, bảo mật các thông tin lưu truyền trên mạng.
 - Bảo mật lớp truy cập: Bảo mật truy cập của người dùng quay số (dial-up): Tạo các kênh VPN cho các kết nối dial-up..
 - Bảo mật thiết bị và máy chủ: Các thiết bị mạng như Router, Switch, firewall là các điểm nút mạng hết sức quan trọng và cần được bảo vệ.
 - Bảo mật ở Hệ điều hành và ứng dụng: Thường xuyên sao lưu, cập nhật các bản vá lỗi của hệ điều hành
 - Bảo mật mức Cơ sở dữ liệu: Có thể nói CSDL là lõi của toàn bộ hệ thống bảo mật thông tin, toàn bộ thông tin quan trọng mang tính chất sống còn được tập trung trên các CSDL, trong thiết kế CSDL được đặt ở mức ưu tiên cao nhất.

10.3 Xử lý an toàn khi xảy ra sự cố

- Phải có cơ chế dự phòng, khi các thiết bị chính gặp sự cố phải có cơ chế chuyển qua để sử dụng các thiết bị dự phòng để hệ thống được trơn tru
- Có đội ngũ chuyên về an ninh mạng để ngăn chặn các cuộc tấn công mạng từ hacker

10.4 Nâng cấp hệ thống

Hệ thống mạng được xây dựng đảm bảo cho việc nâng cấp dễ dàng khi cần thiết, chẳng hạn như ngân hàng tăng thêm nhân sự, số lượng Chi nhánh cũng như các đối tác tăng lên, các server được truy xuất nhiều hơn.

10.5 Những hạn chế còn tồn tại

Do đặt nhiều giả thiết nên dự án còn một vài điểm chưa sát với thực tế. Giới hạn về số lượng thiết bị

Chưa có nhiều kiến thức về các thiết bị mạng như router, switch, firewall, server nên triển khai dự án còn nhiều điểm chưa hợp lí.

Hệ thống mạng chưa tối ưu.

10.6 Định hướng phát triển hệ thống trong tương lai

Trong tương lai, nếu ngân hàng BBB có thêm nhân viên hoặc mở thêm chi nhánh thì hệ thống vẫn đáp ứng nhu cầu trong vòng 2 năm tới.

11 Tài liệu tham khảo

- Computer Networking: A Top-Down Approach, James F. Kurose, Keith Ross, 2000, Pearson Education
- <https://computernetworking747640215.wordpress.com/2018/07/05/vlan-configuration-on-a-cisco-switch-in-packet-tracer/>
- <https://itexamanswers.net/cisco-packet-tracer-tutorial-for-beginners-how-to-use-packet-tracer>