Lab 8: MPLS VPN

Student Name: ....
Student No: ....

Objectives:

- ✓ Practice on MPLS VPN.

Content:

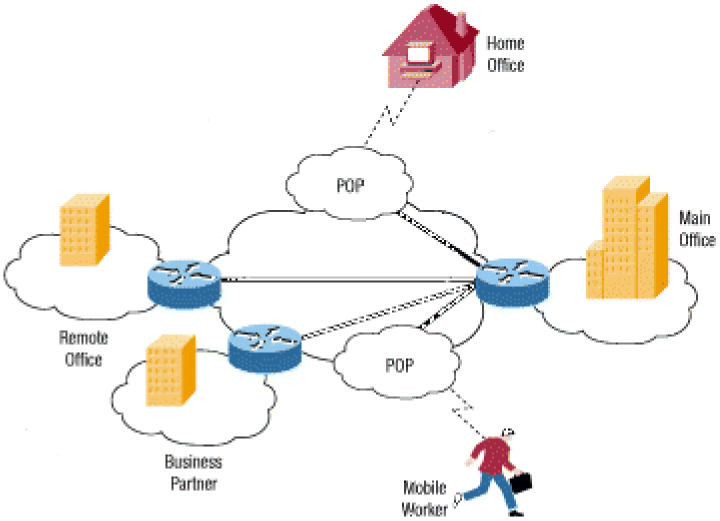
I. Introduction to VPN

The world has changed a lot in the last couple of decades. Instead of simply dealing with local or regional concerns, many businesses now have to think about global markets and logistics. Many companies have facilities spread out across the country, or even around the world. But there is one thing that all companies need: a way to maintain fast, secure, and reliable communications wherever their offices are located.

Until recently, reliable communication has meant the use of leased lines to maintain a wide-area network (WAN). Leased lines, ranging from Integrated Services Digital Network (ISDN, which runs at 144 Kbps) to Optical Carrier-3 (OC3, which runs at 155 Mbps) fiber, provide a company with a way to expand their private network beyond their immediate geographic area. A WAN has obvious advantages over a public network like the Internet when it comes to reliability, performance, and security; but maintaining a WAN, particularly when using leased lines, can become quite expensive (it often rises in cost as the distance between the offices increases). Additionally, leased lines are not a viable solution for organizations where part of the work force is highly mobile (as is the case with the marketing staff) and might frequently need to connect to the corporate network remotely and access sensitive data.

As the popularity of the Internet has grown, businesses have turned to it as a means of extending their own networks. First came intranets, which are sites designed for use only by company employees. Now, many companies create their own Virtual Private Networks (VPNs) to accommodate the needs of remote employees and distant offices.

A typical VPN might have a main local-area network (LAN) at the corporate headquarters of a company, other LANs at remote offices or facilities, and individual users that connect from out in the field.



A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection, such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

There are two common types of VPNs.

- Remote-Access—Also called a Virtual Private Dial-up Network (VPDN), this is a user-to-LAN connection used by a company that has employees who need to connect to the private network from various remote locations. Typically, a corporation that wishes to set up a large remote-access VPN provides some form of Internet dial-up account to their users using an Internet service provider (ISP). The telecommuters can then dial a 1-800 number to reach the Internet and use their VPN client software to access the corporate network. A good example of a company that needs a remote-access VPN would be a large firm with hundreds of sales people in the field. Remote-access VPNs permit secure, encrypted connections between a company's private network and remote users through a third-party service provider.
- Site-to-Site—Through the use of dedicated equipment and large-scale encryption, a company can connect multiple fixed sites over a public network such as the Internet. Each site needs only a local connection to the same public network, thereby saving money on long private leased-lines. Site-to-site VPNs can be further categorized into intranets or extranets. A site-to-site VPN built between offices of the same company is said to be an intranet VPN, while a VPN built to connect the company to its partner or customer is referred to as an extranet VPN.

A well-designed VPN can greatly benefit a company. For example, it can:

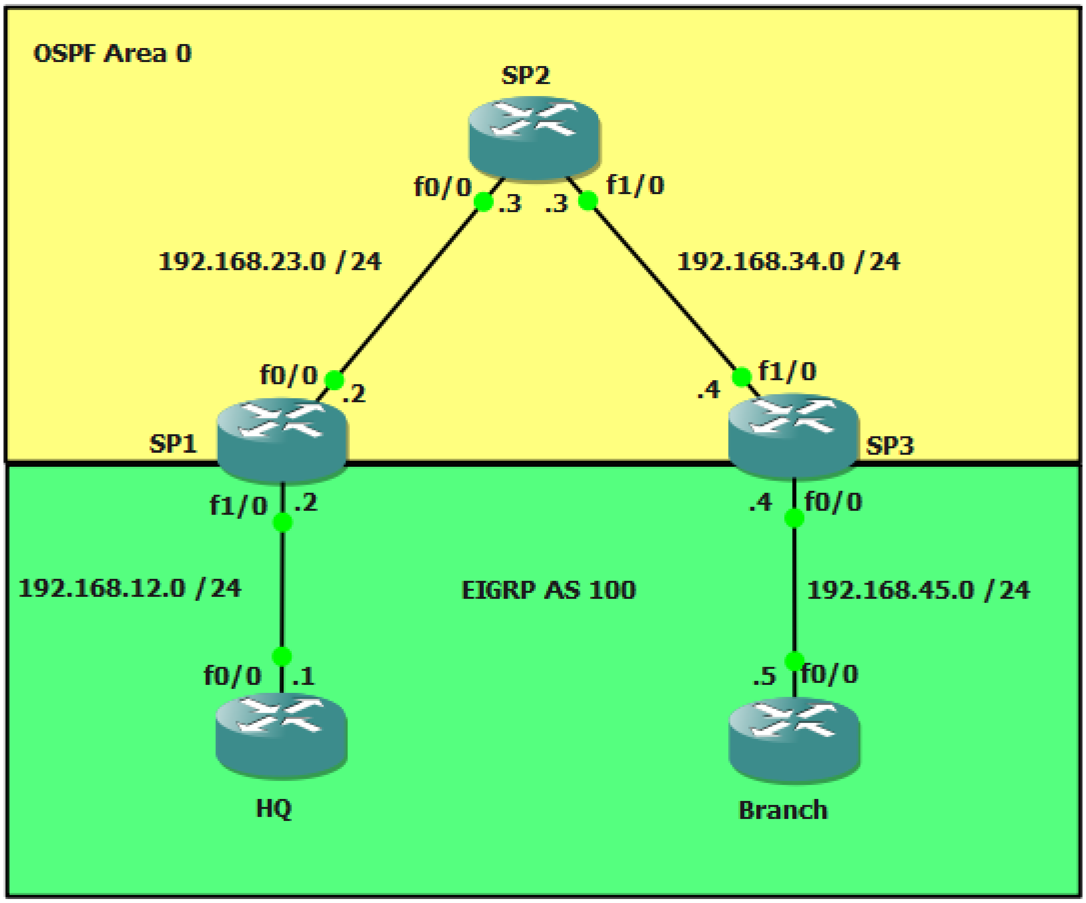
- Extend geographic connectivity
- Reduce operational costs versus traditional WANs
- Reduce transit times and traveling costs for remote users
- Improve productivity
- Simplify network topology

- Provide global networking opportunities
- Provide telecommuter support
- Provide faster Return On Investment (ROI) than traditional WAN

What features are needed in a well-designed VPN? It should incorporate these items:

- Security
- Reliability
- Scalability
- Network Management
- Policy Management

II. Practice



You are given the network topology and the IP for each device is pre-configured. You need to complete these tasks:

- Configure OSPF Area 0 at the provider side (Router SP1, SP2 and SP3).
- Advertise the loopback interfaces as well in OSPF.
- Ensure you have full reachability in the OSPF domain.
- Configure MPLS on all physical interfaces in the service provider domain, do not configure MPLS on physical interfaces pointing towards the customer.

- Force MPLS to use the loopback interface as router-id.
- Configure VRF "customer" on SP1 and SP3.
- On router SP1 and SP3 add the interfaces pointing towards the customer to the VRF you just created.
- Ensure you can ping from within the VRF, try this as following on SP1: ping vrf customer 192.168.12.1
- Configure EIGRP AS 100 on router HQ and Branch. Advertise the loopbacks as well.
- Disable EIGRP auto-summary.
- Configure EIGRP on router SP1 and SP3 for the correct VRF "customer".
- Ensure you have established a EIGRP neighbor relationship between Router HQ and SP1, and between SP3 and Branch.
- See if you have learned routes by using "show ip route vrf customer".
- Configure BGP AS 1 between Router SP1 and SP3, make sure updates are sources from the loopback interface.
- Configure the correct BGP address families and make sure communities are sent between neighbors.
- Redistribute EIGRP into BGP, use the correct address-family for the VRF "customer".
- Redistribute the information from BGP back into EIGRP, use the following metrics:
  bandwidth: 64kbps
  delay: 1000
  reliability: 255
  load: 1
  MTU: 1500
- Ensure you have full connectivity between router HQ and Branch. You should see each other's EIGRP routes that have been carried over the service provider's MPLS backbone.

III. Submission

Complete all tasks in section II. Compress the project into Lab8_<student_code>.zip and submit this file onto Sakai.

References:

http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html
http://gns3vault.com