

To: Professor Robert Cannistra

Class: CMPT\_307N\_113\_16S

From: Piradon (Tien) Liengtiraphan

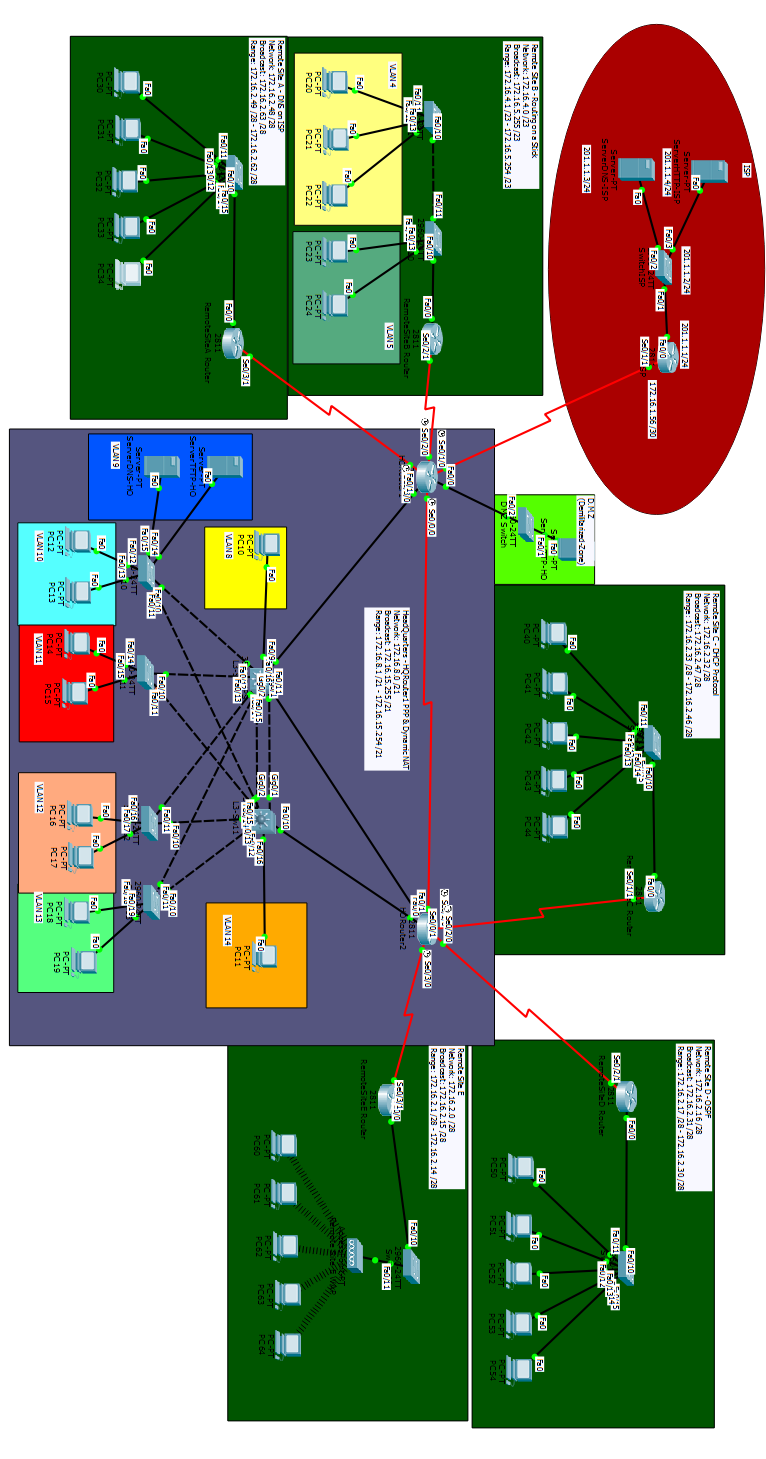
Date: May 8th, 2016

Subject: Project: Phase II - Network Design, Implementation, Configuration,

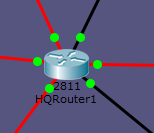
Documentation and Challenges

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

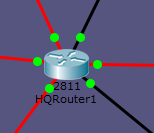
**Packet Tracer Topology**



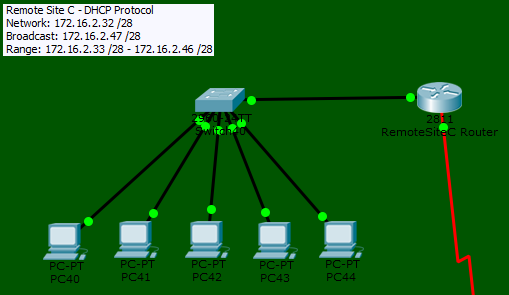
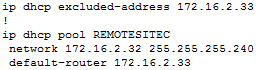
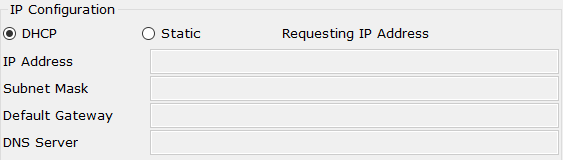
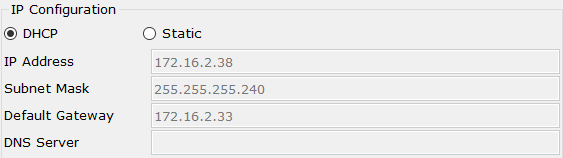
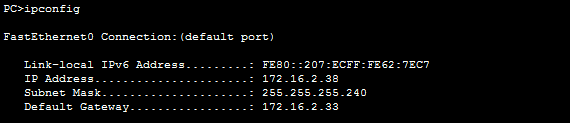
**Static NAT**

* Static NAT functions as a direct translation between an incoming real address(es) to a mapped address(es). The difference from Dynamic NAT and PAT being that the mapped address(es) are chosen by the network administrator. The advantage of those protocol being that it allows unique identification of the packet coming into the network where Static NAT has been configured via the assigned IP Address.
* 
* HQRouter1
  + HQRouter1 - Static NAT.PNG
* To troubleshoot the issue a network administrator would have to console into the HQRouter1 via a console cable from either one of the connected hosts or network capable device and do a show run in privileged mode, and then proceed to check the configuration the Static NAT. It is also recommended that the administrator do a show ip route in privileged mode to see whether the IP might overlap with any other networks. Another useful command to run to get an overhead view is show ip nat status.
* Citation
  + Cisco Engineers. 2014. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2 - Configuring Static NAT [Cisco ASA 5500-X Series Firewalls]. (November 2014). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/nat\_static.html

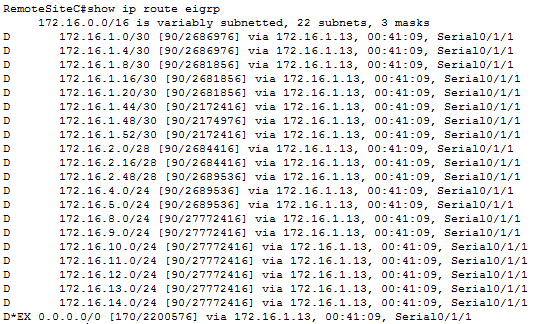
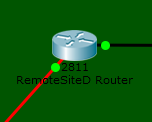
**Dynamic NAT**

* Dynamic NAT functions similar to Static NAT in the sense that it translates incoming real address(es) to a mapped address(es). Where it difference from Static NAT is that the incoming address(es) are assigned mapped address(es) “dynamically”, in other words, automatically by the router from the set pool of address(es).
* 
* HQRouter1
  + HQRouter1 - Dynamic NAT.PNG
* To troubleshoot Dynamic NAT is very similar to troubleshooting Static NAT, in that running a show run and show ip nat status in privileged mode is a good way to gain an overhead view. Another problem that could occur with Dynamic NAT is port assignment. Ensure that the correct ports are assigned to either in or out depending on the situation. Another thing to make sure is that you have enough addresses in your pool to assign to packets coming in.
* Citation
  + Cisco Engineers. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2 - Configuring Dynamic NAT and PAT [Cisco ASA 5500-X Series Firewalls]. Retrieved May 7, 2016 from http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/nat\_dynamic.html

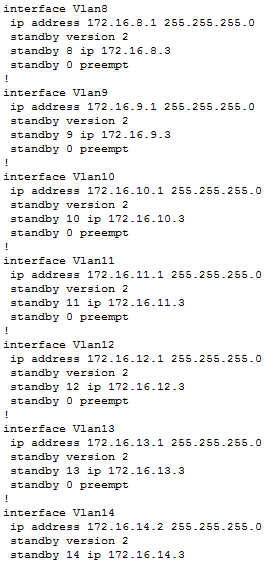
**DHCP**

* Dynamic Host Configuration Protocol, as the name implies is the protocol which allows the router or server to dynamically assign ip address(es) to host(s) connected to it. Theses are collected from an assigned pool of address(es) with sizes varying on the subnet mask. It should be noted the the host device(s) connected to the router or server setup with DHCP should be configured so that they attain their IP address(es) via DHCP.
* 
* RemoteSiteCRouter
  + 
* Host
  + Host - DHCP.PNG
  + 
  + Host - DHCP4.PNG
  + 
  + 
* An issue was encountered where the DHCP requests were failing, resulting in the host(s) being given a self-assigned IP Address. When this issue occurs, the first step is to check the configuration on the router itself to see if any errors occurred during the setup of DHCP (e.g. excluding all available ip addresses). If it seems that all the configurations are correct and errors still occur, remove DHCP and recreate it. (This is possible an error in Packet Tracer)
* Citation
  + Cisco Engineers. 2014. Cisco IOS IP Configuration Guide, Release 12.2 - Configuring DHCP [Cisco IOS Software Release 12.2]. (February 2014). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/td/docs/ios/12\_2/ip/configuration/guide/fipr\_c/1cfdhcp.html

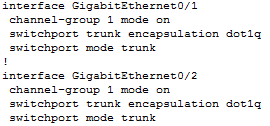
**Routing Protocol (EIGRP & OSPF)**

* EIGRP: Enhanced Interior Gateway Routing Protocol is one of three dynamic routing protocols (EIGRP, OSPF, and RIP) which allows routers directly connected to one another to dynamically learn each other’s routes via propagation across wires. The advantages of using EIGRP are: the low usage of network resources, propagation of only changes in network configuration instead of the entire routing table, and quick convergence times when changes occur in the topology. We can also use EIGRP to propagate the Gateway of last resort to other networks running EIGRP.
* RemoteSiteRouterA-C & E & HQRouter1-2
  + 
  + RemoteSiteCRouter - EIGRP.PNG
  + 
* OSPF: Open Shortest Path First in an interior gateway protocol that relies on link states over distance vectors, when compared to RIP. One of the differentiating features of OSPF is that it propagates link-states advertisements rather than generic routing table updates. OSPF works off of a link-state algorithm to find the shortest path to all available destinations.
* RemoteSiteD & HQRouter2
  + 
  + RemoteSiteDRouter - OSPF.PNG
* Troubleshooting EIGRP and OSPF start by running a show ip route in privileged mode to see the available routes. If either routing protocol have been incorrectly setup then the route(s) being advertised will not be propagated. Another way to view if the protocols have been properly setup is to run a show run in privileged mode. This will allow the network administrator to view if the protocol(s) have been configured on the router properly or not (e.g. same EIGRP Autonomous System Number and/or OSPF Process ID and Area Number)
* Citation
  + Cisco Engineers. 2015. Enhanced Interior Gateway Routing Protocol. (January 2015). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html
  + Cisco Engineers. 2013. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2 - Configuring OSPF [Cisco ASA 5500-X Series Firewalls]. (October 2013). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/route\_ospf.html

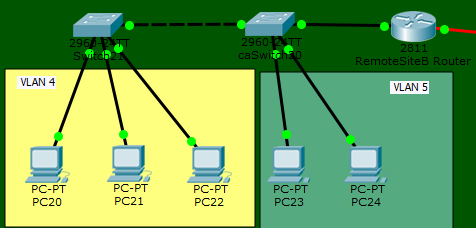
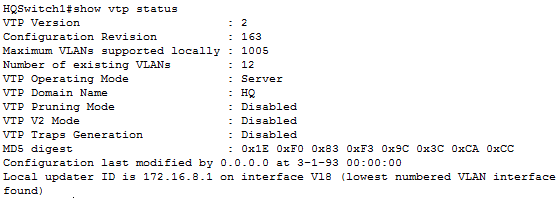
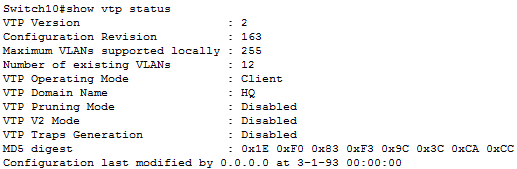
**First Hop Redundancy Protocol (ie: HSRP)**

* Hot Standby Router Protocol is used to achieve near 100% network uptime. The protocol provides redundancy on IP networks, thereby ensuring that traffic is almost immediately recovers from “first hop failures”. The protocol works by assigning a single IP address to two or more routers, allowing to to act as virtual routers, allowing one router to assume the role of the other should one go down for whatever reason.
* 
* L3-Sw10-11
  + 
* First recommended step is to do a show run in privileged mode, from there go down to the interfaces involved in HSRP and ensure that they have been assigned to the correct standby group. If not the assigning to assign the interface to the HSRP group simply go into the configuration mode of the interfaces and do a standby # where “#” is the group number.
* Citation
  + Cisco Engineers. 2006. Hot Standby Router Protocol Features and Functionality. (May 2006). Retrieved May 8, 2016 from http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html

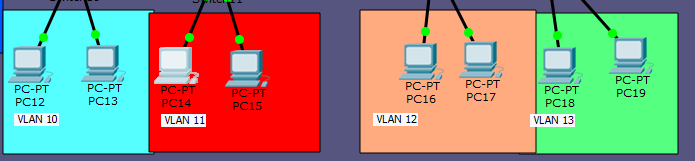
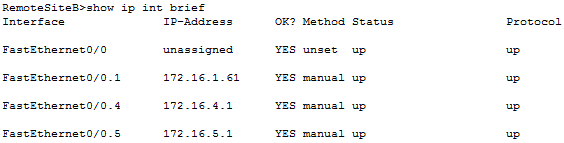
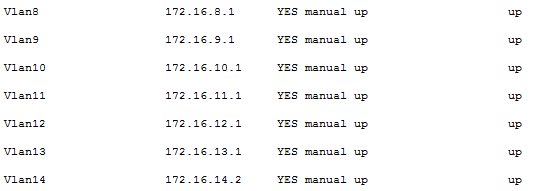
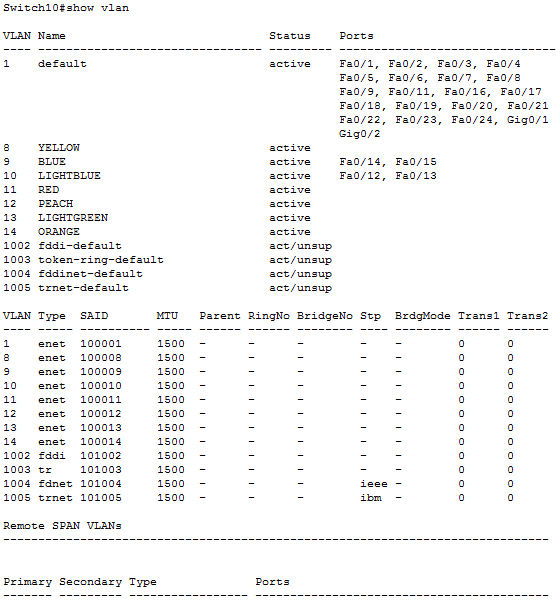
**Link Aggregation (ie: EtherChannel)**

* Also known as trunking, Link Aggregation allows multiple ports to appear and act as if they were one large link. This is usually used to increase bandwidth between connections and to increase the efficiency in which the ports operate. Link Aggregation exists on the Ethernet gateway and is used in conjunction with Layer 2 Bridging.
* 
* L3-Sw10-11
  + 
* As with many issues in networking your best bet when troubleshooting is to run a show run in privileged mode. This will allows the network administrator to verify the configurations on the applicable ports. Ensure that the ports involved are on the same channel-group (1 in this case) and that switchport trunk encapsulation dot1q and switchport mode trunk are running properly.
* Citation
  + Cisco Engineers. 2013. Cisco SFS InfiniBand Software Configuration Guide, Release 2.10 - Configuring Link Aggregation [Cisco SFS 3504 Multifabric Server Switch]. (October 2013). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/td/docs/server\_nw\_virtual/2-10-0\_release/configuration/guide/swcg210/3link.html

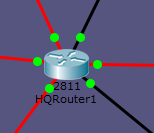
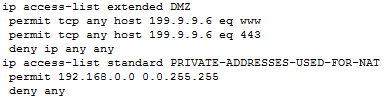
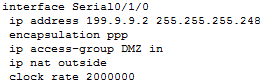
**VTP**

* VLAN Trunk Protocol is used to reduce administration within switched networks. When VTP is configured, VLAN(s) will be created on the switch serving as the VTP server, which are then distributed to all other switches in the domain. There are two modes that operate within VTP: Server & Client. The difference being that the Server Switches should be the place where the VLAN(s) are created, Client Switches only act as receivers of the VLAN(s) and handle port assignments to VLAN(s).
* 
* L3-Sw10-11 - Server
  + 
* L2-Sw10-13
  + 
* The first step in troubleshooting any issues with VTP would be to ensure that the respective servers are on the correct VTP domain. By running a show vtp status in privileged mode the network administrator will be able to view all the basic setup of VTP and then proceed to make changes. If the servers are on different VTP domains then to change to domain simple input (on the switch you want to change domains) vtp domain DOMAINNAME. To switch between client and server input vtp mode client | vtp mode server.
* Citation
  + Cisco Engineers. 2014. Understanding VLAN Trunk Protocol (VTP). (September 2014). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html

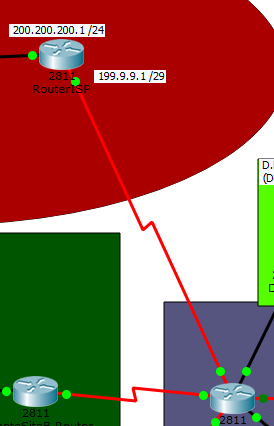
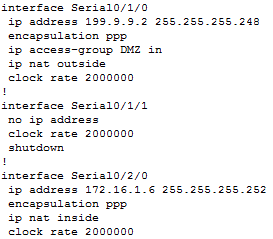
**VLAN(s)**

* Virtual Local Area Networks, are used to separate hosts on networks located within the same location. Incorporating VLANs makes use to switches, L3 switches, and/or routers. The purpose of the VLAN could be make for security or as a simply organization method (network-wise) for different roles in a network/company. VTP (mentioned above) is a way of distributing VLANs on a network.
* 
* RemoteSiteBRouter - Holds Sub-Interfaces in “router-on-a-stick” situations.
  + 
* L3-Sw - VTP int VLANs
  + 
* HQSwitch10 - Client
  + 
* To ensure that VLANs are working properly, depending on the situation one must either verify whether the router subinterfaces have been created properly or int vlans have been created and distributed properly. To view the subinterfaces or the int vlans the network administrator should type in show ip int brief and see whether the proper ip addresses have been assigned to each respective port. From there the NA would ensure that each host(s) has been properly assigned the correct default-gateway depending on which VLAN it is on.
* Citation
  + Cisco Engineers. 2013. Catalyst 6500 Release 12.2SX Software Configuration Guide - VLANs [Cisco Catalyst 6500 Series Switches]. (November 2013). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2sx/configuration/guide/book/vlans.html

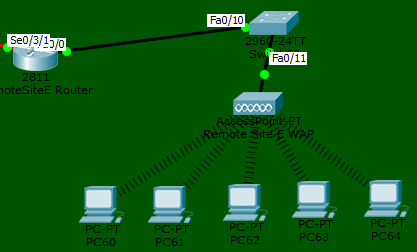
**Named Extended ACLs (for limiting traffic to specific protocols)**

* Access Control Lists are used for packet filtering on a network. Mostly used for the sake of security, packet filtering restricts users, devices, and/or protocols from being able to access or leave your network. Named Access Control Lists simply serve to make it easier for network administrators to identify the ACLs they’ve created.
* 
* HQRouter1
  + 
* Int s0/1/0
  + 
* First thing that should be understood when troubleshooting an ACL is what is the purpose of the ACL. If your problem is that you cannot ping any of the devices behind said ACL but on the ACL it was configured as deny icmp any any then the problem lies with the user not the ACL itself. That aside to check the settings of the ACL incase something truly is amiss then the first command that should be run on the Router is show run, this will allow the network administrator to see all the parts involved in the ACL and which ports are involved in said ACL.
* Citations
  + Cisco Engineers. 2015. Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S - IP Named Access Control Lists [Support]. (March 2015). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\_data\_acl/configuration/xe-3s/sec-data-acl-xe-3s-book/sec-acl-named.html

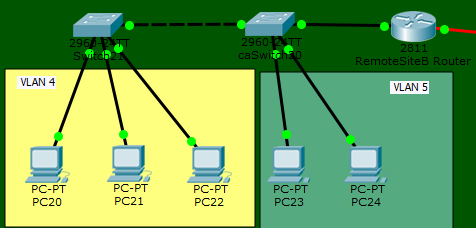
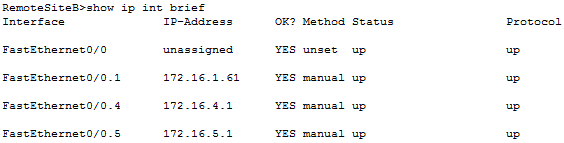
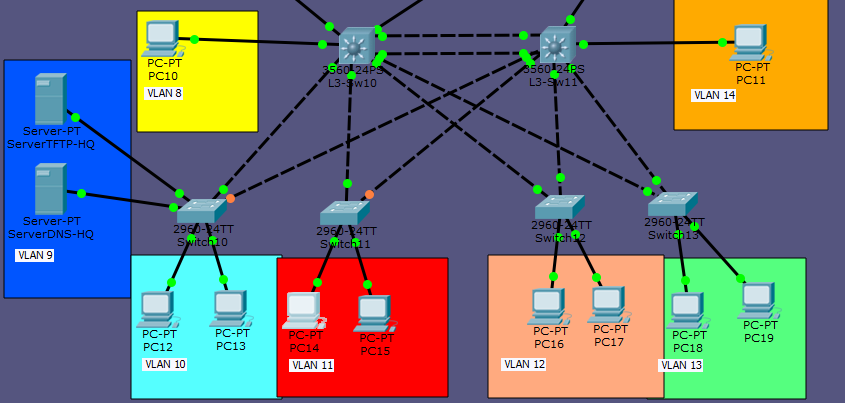
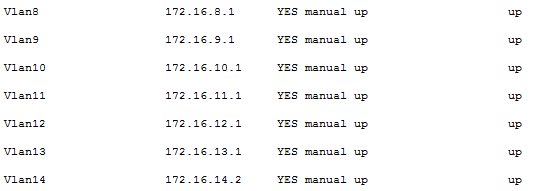
**PPP**

* Point-to-Point Protocol is used to transport multi-protocol datagrams over directly connected links. It consists of three main steps: encapsulation, LCPs (Link Control Protocol), and NCPs (Network Control Protocols).
* 
* ISP
  + ISP - PPP.PNG
* HQRouter1
  + 
* To ensure that PPP is working properly the network administrator must ensure that each interface involved in the transaction of packets are encapsulated with PPP. To view whether an interface has PPP encapsulation turned on do a show run in privileged mode and scroll down to the summary of interfaces.
* Citation
  + Cisco Engineers. Point-to-Point Protocol (PPP). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/tech/wan/point-to-point-protocol-ppp/index.html

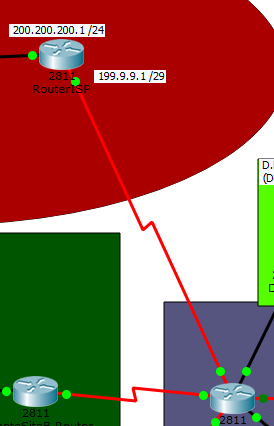
**Wireless**

* Also know as WLAN or IEEE 802.11 is an implementation of wireless computer communication.
* RemoteSiteE
  + 
* The host(s) connected to the wireless access point must be wireless or 802.11 capable. This can be achieve through built-in NICs or USB wireless adapters.

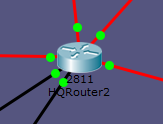
**InterVLAN Routing (Router-on-a-stick or SVIs)**

* As stated in the header of this section interVLAN Routing can be done via two major methods: router-on-a-stick (subinterfaces) and SVI (switch virtual interfaces). Both these are simply means to achieve interVLAN routing, the ability to communicate between two or more VLANS
  + Router-on-a-Stick: Uses subinterfaces and vtp to allow VLANS to communicate. The necessity of subinterfaces in this case is due to the fact that generally the two VLAN will be connected to a switch which is then connected to a router through one interface. Subinterfaces therefore allow one interface to hold multiple IP addresses.
  + 
    - 
  + Switch Virtual Interfaces: Uses virtual VLAN interfaces as the default gateway to for each VLAN. This information is then distributed to all the connected switches via VTP, all involved switches must be on the same VTP domain to receive information from the VTP server.
  + 
    - 
* Troubleshooting interVLAN routing depends on which method from the two above have been chosen.
  + Router-on-a-Stick: Ensure that the subinterfaces have been assigned to each respective VLAN. The IP addresses assigned to each subnet should be the respective default-gateway of each VLAN. To check the the ip addresses of the subinterfaces, run a show ip int brief in privileged mode. Ensure that the subinterfaces are encapsulated and assigned to their respective VLANS with an encapsulation dot1q vlan # where # = VLAN number on the subinterface.
  + Switch Virtual Interfaces: Ensure that there is an int vlan created for each respective vlan where their default-gateway will rest. Then it serves the network administrator well to ensure that all the involved interfaces involved in the connection between the core switch and the layer 2 switches are on the same vtp domain. To check you can run a show vtp status on each switch. You can also check each individual interface with a show ip int brief.
* Citation
  + Cisco Engineers. 2016. Configure InterVLAN Routing on Layer 3 Switches. (April 2016). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-l3-intervlanrouting.html
  + Cisco Engineers. 2005. Configuring InterVLAN Routing and ISL/802.1Q Trunking on a Catalyst 2900XL/3500XL/2950 Switch Using an External Router. (November 2005). Retrieved May 6, 2016 from http://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/14976-50.html

**Default Static Routing with Route Injection**

* Default Static Routing is used to move traffic to non-connected host(s) or network(s), by dictating the network and port in which you wish to move your packets. Static routes are generally used for: networks that do not use RIP, OSPF, or EIGRP, and/or smaller networks that are easy to manage and do not need to overhead provided by routing protocols. The command to set up a default static route is ip route 0.0.0.0 0.0.0.0 port ip address in global configuration mode. Once the default static route has been created, and if you’re using a routing protocol you must propagate the default static route within the routing protocol. For RIPv2 and OSPF the command is default-information originate within RIPv2 and OSPF configuration modes. For EIGRP the command is redistribute static in EIGRP configuration mode.
* 
* HQRouter1
  + HQRouter1 - Static Route.PNG
  + HQRouter1 - Static Route2.PNG
* ISP
  + ISP - Static Route.PNG
* To ensure that static routes work correctly the first step should be to view all the routes that the selected device is directly connected to with a show ip route in privileged mode. Ensure that the network exists on the directly connected networks, denounced by “C”. Then do a show run in privileged mode, and check to see whether the network address and subnet mask match the programmed static route and whether the designated port is correct.
* Citation
  + Cisco Engineers. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.2 - Configuring Static and Default Routes [Cisco ASA 5500-X Series Firewalls]. Retrieved May 7, 2016 from http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/route\_static.html

**Routing Protocol Redistribution**

* Routing Protocol Redistribution serves as a means for a router to advertise routes that are learned through different means (e.g. Between EIGRP and OSPF networks). A possible use case for redistribution is if a company buys out a competitor who is using a different network protocol to learn their routes, instead of reconfiguring the entire network one could use redistribution to simply connect the two sites between routers.
* 
* HQRouter2
  + EIGRP
    - HQRouter2 - Redistribute.PNG
  + OSPF
    - HQRouter2 - Redistribute2.PNG
* To ensure that routes are being redistributed properly one must go into the configuration mode of each protocol that is currently running and enter redistribute \*\*\*\*\* (\*\*\*\*\* = opposite protocol running). In the case to redistribute EIGRP one must include subnets in the redistribution command (see image above) or else only the classful addresses will be redistributed.
* Citation
  + Cisco Engineers. 2012. Redistributing Routing Protocols. (March 2012). Retrieved May 7, 2016 from http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/8606-redist.html

**Challenges**

One of the most difficult parts of this project was configuring the DMZ and Static/Dynamic NAT. This was because we had only recently learned about both processes and we had yet to do a lab to put our theoretical knowledge to test in packet tracer. Another aspect of this lab that was difficult to do, and was most likely do to my own design, ensuring that all the redundant connections did not overlap with each other when assigning IP addresses. At first I did not know that we couldn’t simply assign /21 addresses when working with VLANs due to them overlapping. This became a problem when working with the Head Quarters, to ensure that every IP address was unique and did not overlap I had to break down my /21 network into separate /24 networks. Other than the time it took to complete the project and helping explain concepts that were explained to me to other people I found the project quite doable and even slightly enjoyable.