Project – (250 Points Total):

This is an extremely detail oriented assignment! Please spend the time necessary to complete this assignment as thoroughly as you possibly can since it will be most beneficial to you in the long run!

There are a ten topics here. Each topic is worth twenty (25) points and may include multiple technologies within the topic. You may need to research certain topics and others you may have within your class notes from the labs and lectures. For each topic you should:

1. Provide a detailed description and/or explanation of what the topic is (in your own words). If there are multiple technologies in use, make sure you describe each one individually.
2. Following the description/explanation you will create an example topology that will be used for this question. (Yes, you may utilize this same topology on other questions – only if it directly relates to other questions.) Make sure you specify interfaces in use, ip addresses and subnet masks within your topology. Your topology should pertain to the topic and should not have more technologies configured within the topology than is necessary to demonstrate your mastery of the topic discussed.
3. Next, you will provide a configuration for the topic listed based upon your example topology.
   1. For the first few questions, you should provide detailed steps as to where you are within the router or switch when issuing a specific command so you demonstrate basic knowledge and manipulation of the Cisco IOS. Throughout all of the topics you should specify what each command does. (A brief example is listed below.)
4. Provide show commands for each topic. What are you looking for in order to verify this technology is working properly?
5. Provide debug commands for each topic. And, explain how you would go about troubleshooting this technology if something is not working correctly.

Please keep in mind… No assumptions are made! Some of the items have multiple steps so be sure to include **all** the steps in the configuration, etc...

**For example** *(please keep in mind this is abbreviated example):*

If you are asked to ***assign an IP Address to a router interface***, you may want to specify the following:

Create a sample topology, then write…

An IP Address is a Layer 3 logical address that is assigned to each host within a TCP/IP network. The IP Address assigned to the host is determined by the network administrator and is dependent upon the network it is directly connected to. An IP Address is a hierarchical address that consists of 4 octets, 8 bits each, 32 bits in total. An IP Address is typically written in dotted decimal notation:

* + - 1. is an example of a Class A IP Address

To assign an IP Address to a router interface you would proceed in the following manner:

|  |  |
| --- | --- |
| Router> | This prompt specifies the router is in USER mode |
| Router>***enable*** | this command is entered to go from USER mode to PRIVILEGE mode |
| Router# | You are now in PRIVILEGE mode |
| Router# ***configure terminal*** | used to enter GLOBAL CONFIGURATION mode from PRIVILEGE mode. This is needed to configure all parameters within the router |
| Router(config)# | You are now in GLOBAL CONFIGURATION mode |
| Router(config)#***interface fastethernet0/0*** | This is entered to go into INTERFACE CONFIGURATION mode to configure the fastethernet0/0 interface within the router |
| Router(config-if)# | You are now in INTERFACE CONFIGURATION mode |
| Router(config-if)#***ip address 1.1.1.1 255.0.0.0*** | This sets the IP Address to 1.1.1.1 with a subnet mask of 255.0.0.0 which is the default subnet mask for a Class A IP Address |
| Router(config-if)#***no shutdown*** | After the IP Address is set on the interface, it’s always a good idea to enable the interface and test connectivity. |

Specify the show commands, test commands to verify the configuration is working properly and move onto the next topic.

This assignment should be **printed and turned in by 11:00am, Thursday, December 8, 2016.** **In addition to your printed copy, please submit a softcopy in Microsoft Word (.docx or .doc) format via ilearn.** Make sure you cite your resources and do not plagiarize! Your citations should be placed at the end of each question, not at the end of the project. **All work should be completed individually!!!** **There will not be any extensions given for this assignment**, so make sure you **SUBMIT IT ON TIME otherwise you will receive a grade of ZERO!!!**

If you have any questions or concerns, please let me know!

Topics to research, explain, provide detail and provide examples for: (make sure you provide as much detail as possible in a concise manner and make it as legible as possible! Once this is graded and turned back to you, it will provide you with a detailed study guide for your final practical.) Please feel free to copy and paste the table from above and use it as a template for each question. Please do not remove the numbers or questions/statements below. Use this as a template and add your answers under each numbered question/statement on each page.

# Project – (250 Points Total)

1. VLANs, VTP with 802.1q and InterVLAN Routing with a Router-on-a-stick and SVIs (NOTE: Make sure you accomplish this without going into VLAN Database mode and show the syntax for both 2960 and 3560 switches!)

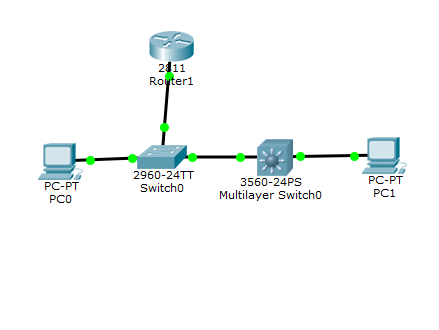
VLAN is a virtual local area network. With VLANs, a switch can take several interfaces and configure them into several different broadcast domains. The broadcast domains created by the switch are called VLANs. These broadcast domains take place at layer 2, the data link layer.

The VLAN Trunk Protocol (VTP) reduces the need for administration in a switched network. IEEE 802.1q is one of the two trunking protocols that cisco supports in a switching network. 802.1q helps to provide support to device connections that do not understand trunking. This allows a cisco switch to be cabled to a switch that does not understand 802.1q trunking.

InterVLAN routing allows traffic to be routed between VLANs. It is called a router-on-a-stick because the router has a single physical layer linked to the switch, making it look like it’s on a stick.

A Switched Virtual Interface (SVI) can perform inter-VLAN communication on a multilayer switch (layer 3 switch). SVI on a multilayer switch bypasses the need for a router in order to achieve inter-VLAN communication.

The following topology displays that hardware necessary to configure the above protocols ad interfaces:



In order to configure the above interfaces and protocols, one would proceed in the following manor:

|  |  |
| --- | --- |
| Switch2960(config)# ***vlan 1*** | This global configuration command creates the VLAN. |
| Switch2960(config-vlan)# ***name scooby*** | This VLAN command is a subcommand that names the VLAN. |
| Switch2960(config-vlan)# ***exit*** | Applies changes and returns to global configuration mode. |
| Switch3560(config)# ***vlan 2*** | This global configuration command creates the VLAN. |
| Switch3560(config-vlan)# ***name scrappy*** | This VLAN command is a subcommand that names the VLAN. |
| Switch3560(config-vlan)# ***exit*** | Applies changes and returns to global configuration mode. |
| Switch2960(config)# ***int f0/1*** | This global configuration command allows one to configure the FastEthernet port 0/1. |
| Switch2960(config-if)# ***switchport access vlan 1*** | This subcommand statically configures the FastEthernet 0/1 interface into VLAN 1. |
| Switch2960(config-if)# ***switchport mode access*** | This subcommand configures the trunking administrative mode on the FastEthernet 0/1 interface. |
| Switch2960(config-if)# ***end*** | Configures the trunk protocol on the VLAN and interface. |
| Switch3560(config)# ***int f0/1*** | This global configuration command allows one to configure the FastEthernet port 0/1. |
| Switch3560(config-if)# ***switchport trunk encapsulation dot1q*** | This subcommand defines that dot1q will be the type of trunking that is going to be used which specifies the 802.1qtagging on the trunk link. |
| Switch3560(config-if)# ***switchport mode trunk*** | This subcommand configures the trunking administrative mode on the FastEthernet 0/1 interface. |
| Switch3560(config-if)# ***end*** | Configures the trunk protocol on the VLAN and interface. |
| Switch3560(config)# ***ip routing*** | Enables IP routing on the device. |
| Switch2960# ***show vlan brief*** | This shows the VLANs and the interfaces assigned to each VLAN. |
| Switch3560# ***show vlan brief*** | This shows the VLANs and the interfaces assigned to each VLAN. |
| Switch2960(config)# ***vtp mode client*** | Configures the switch to VTP client mode |
| Switch2960(config)# ***vtp domain shaggy*** | Configures the VTP domain name to shaggy. |
| Switch2960(config)# ***vtp password cisco*** | Configures the VTP password to cisco |
| Switch2960(config)# ***int f0/1*** | This global configuration command allows one to configure the FastEthernet port 0/1. |
| Switch2960(config)# ***show vtp status*** | Displays the general information about the VTP configuration. |
| Router(config)# ***int f0/0*** | Moves to interface FastEthernet 0/0 |
| Router(config-if)# ***int f0/0.1*** | Moves to and creates a sub interface FastEthernet 0/0.1 |
| Router(config-subif)# ***encapsulation dot1q 1*** | Assigns VLAN 1 to this interface and configures the interface with 802.1q tagging protocol. |
| Router(config-subif)# ***ip address 10.10.10.1 255.255.255.224*** | Configures the IP address and subnet mask. |
| Switch3560(config)# ***int vlan 1*** | Creates and moves into interface VLAN 1 |
| Switch3560(config-if)# ***ip address 10.10.10.2 255.255.255.224*** | Assigns the IP address and subnet mask |
| Switch3560(config-if)# ***no shut*** | Enables the VLAN 1 interface |
| Switch3560(config-if)# ***ip routing*** | Enables routing on the switch |

Empson, Scott. *Ccna Routing and Switching Portable Command Guide*. 4th ed. Indianapolis, IN: Cisco, 2013. Print.

*Ccna Routing and Switching 200-125 Official Cert Guide Library Academic*. N.p.: Cisco Systems, 2016. Print.

1. First Hop Redundancy Protocol (ie: HSRP) and Link Aggregation (ie: LACP and PAgP) using two 3560 multilayer switches

First Hop Redundancy Protocol (FHRP) is a family of protocols that are used so that the host can take advantage of redundant routers in a subnet. Having redundant routers can benefit a system in supporting a LAN, but FHRP needs to also be used when these redundant routers exist. One of these FHRP protocols is the Hot Standby Router Protocol (HSRP). HSRP uses an active/standby model means that while one routers is working, there is always another router standing by and waiting to take over if the active HSRP has a problem.

1. IPv4 and IPv6 Static routing (NOTE: With AND Without the use of a default static route.)
2. EIGRP and EIGRP for IPv6 (NOTE: Make sure you utilize VLSM in your topology and configuration without the use of automatic summarization.)

Enhanced Interior Gateway Routing Protocol (EIGRP) is used to help routers make the best choice on which route to send a packet. EIGRP is quick and flexible when it comes to changing the best routes with a changing network.

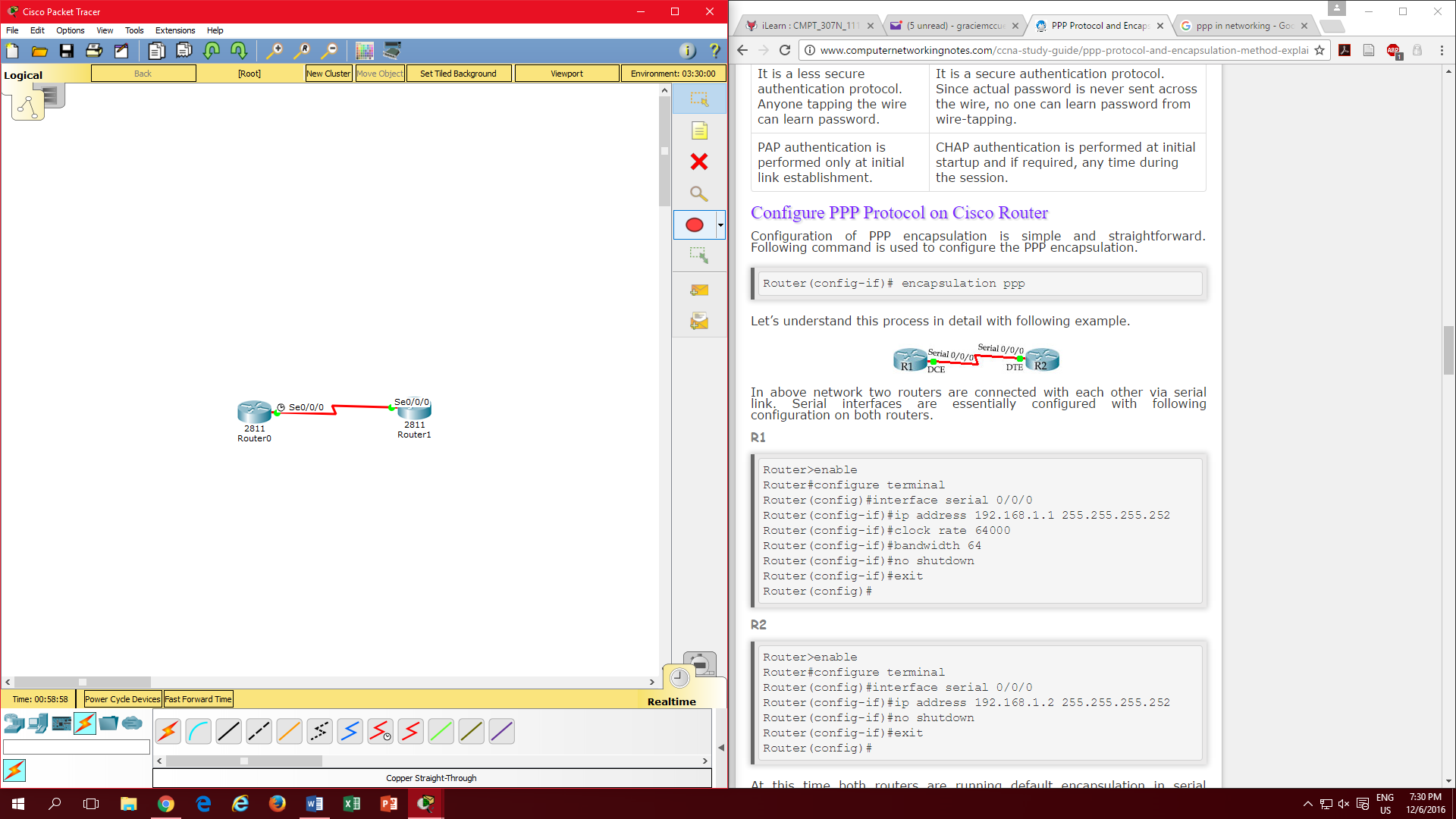
1. OSPFv2 and OSPFv3 (NOTE: Make sure you utilize loopback interfaces within your topology and configuration…and make sure you specify why you are utilizing them.)
2. External BGP

External Border Gateway Protocol (BGP) is a protocol that is mainly used to perform inter-domain routing within a network. A BGP router will be established

1. Extended ACLs and Extended Named ACLs for IPv4 and IPv6 (NOTE: how, where and why you applying these…)
2. Static NAT and Dynamic NAT/PAT for IPv4 (NOTE: Make sure you show a configuration with static NAT for a web server in the DMZ, then PAT using a pool of multiple addresses, and using just the interface IP Address.)
3. DHCP Server on the Router and a local DHCP client and a remote DHCP client (ie: using DHCP Relay.)
4. PPP, PPP CHAP, and MLPPP

Point-to-Point Protocol (PPP) is a layer 2 protocol that is used between two devices to establish a direct connection. It helps to protect against possible threats by providing better authentication and encryption.

Challenge Handshake Authentication Protocol (CHAP) is used along with PPP to continue the verification of the devices. They work alongside each other to make sure that the devices are communicating properly with each other.

Multilink Point-to-Point Protocol (MLPPP) enables a computer to use two PPP links and bond them together as if they were one link.

|  |  |
| --- | --- |
| Router(config-if)# ***encapsulation ppp*** | Changes default encapsulation protocol of routers to PPP |
| Router(config-if)# ***username r1 password test*** | This command sets the username and password for the remote router |
| Router(config-if)# ***ppp authentication chap*** |  |
| Router(config)#***int multilink*** | Creates a multilink interface |
| Router(config-if)#***show ppp multilink*** | Make sure the multilink interface is up and running |
| Router(config-if)# ***ppp multilink*** | Enables the ppp multilink protocol on the router |
| Router(config-if)# ***multilink group x*** | Enabled on each interface to |

<http://www.techrepublic.com/blog/data-center/use-multilink-ppp-to-combine-multiple-circuits-into-a-single-circuit-with-a-single-router-interface/>

<http://www.computernetworkingnotes.com/ccna-study-guide/ppp-protocol-and-encapsulation-method-explained.html>