Frank Siderio
Final Project
Fall 2015

CMPT307 (Internetworking)
Professor Robert M. Cannistra

Final Project – (200 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!

Part I – (150 Points):

There are a number of topics on here. 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 provide a detailed description and/or explanation of what the topic is (in your own words). 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. Next, you will provide a configuration for the topic listed based upon your example topology. 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.) After you have finished the topic configuration you should provide any show commands that would verify the configuration for that specific topic. Following the show commands, specify how you would test the topic configuration (possibly via specific debug commands, etc…).

*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 to receive full credit for that particular topic.*

For 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…

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.

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:

10. 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:

Then… Specify the show commands, test commands to verify the configuration is working properly and move onto the next topic. You should use telnet, ping, and traceroute for testing and troubleshooting. So, for each question you should have the following:

A. Description of Technology
B. Topology
C. Configuration
D. Show Commands
E. Troubleshooting/Verification

When answering each question, please keep your responses in this order.

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 point values, numbers or questions/statements below. Use this as a template and add your answers under each numbered question/ statement on each page.

Research Syntax Exam – (200 Points Total)

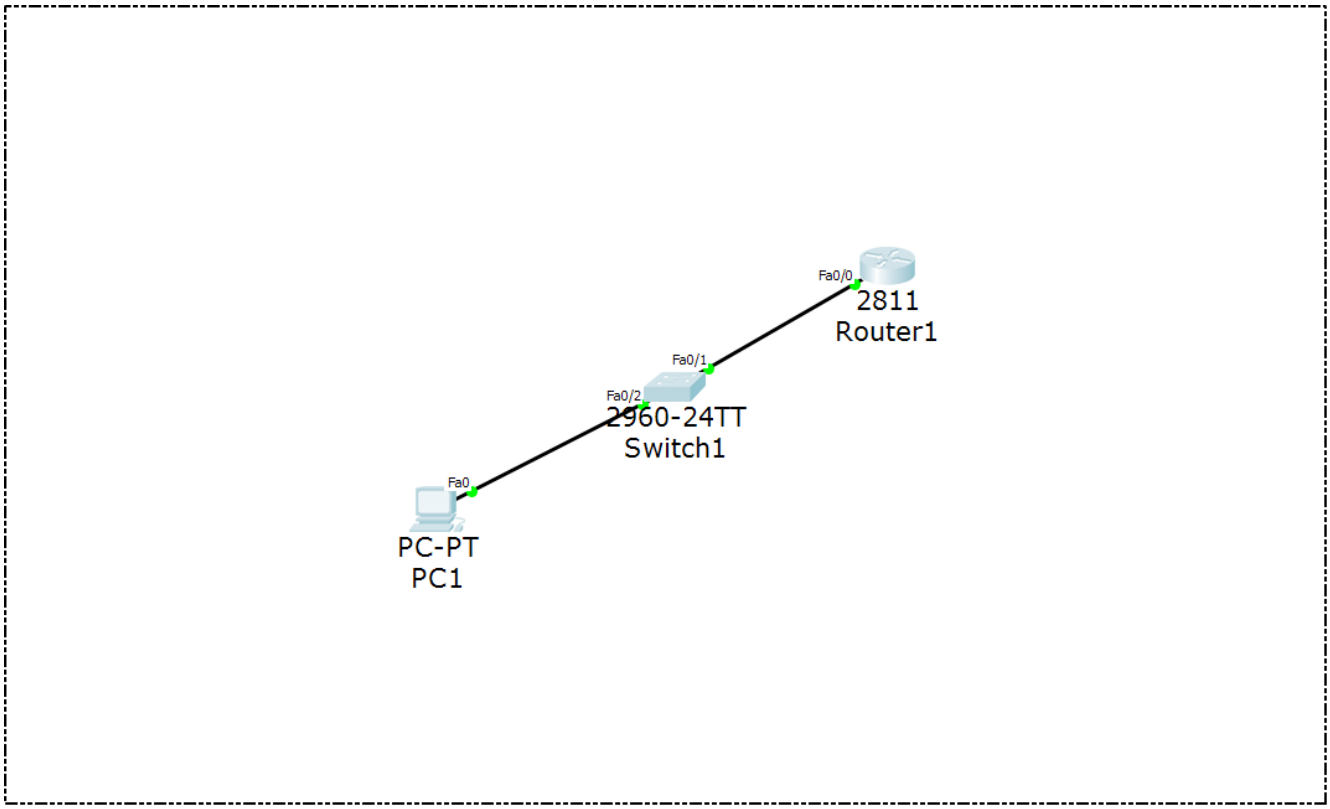
(10 points)

1. Basic router configuration (NOTE: hostname, ip addresses, passwords for each mode of the router or switch, enabling interfaces, etc…)

Router>	This says that the router is in user mode
Router>***enable***	Command takes the router into privilege mode
Router#	Now the router is in privilege mode
Router#***configure terminal***	Command takes the router into global configuration mode
Router(config)#	Now the router is in global configuration mode
Router(config)#***interface fastethernet0/0***	Command to go into interface configuration mode for that specific interface
Router(config-if)#	Now the router is in interface configuration mode
Router(config-if)# ip address 1.1.1.1 255.0.0.0	Sets the ip address for that specific intereface
Router(config-if)# no shutdown	Changes the interface state to an up state (enables the interface)
Router(config-if)# exit	Takes you out of interface configuration mode
Router(config)# hostname Router1	Sets the hostname to Router1
Router(config)# enable password cisco	Sets a password to enter in when trying to enter privilege mode
Router(config)# line console 0	Helps configure a password for login and telnet
Router(config-line)# password cisco	Sets a password cisco
Router(config-line)# login	Command to enable the user to enter in the password to get into the router

Router(config-line)# logging synchronous	Synchronizes console line
Router(config)# lin vty 0 4	Configure for 5 sessions and is for setting a password in the configuration line
Router(config)# do show run	Shows the entire configuration for that router

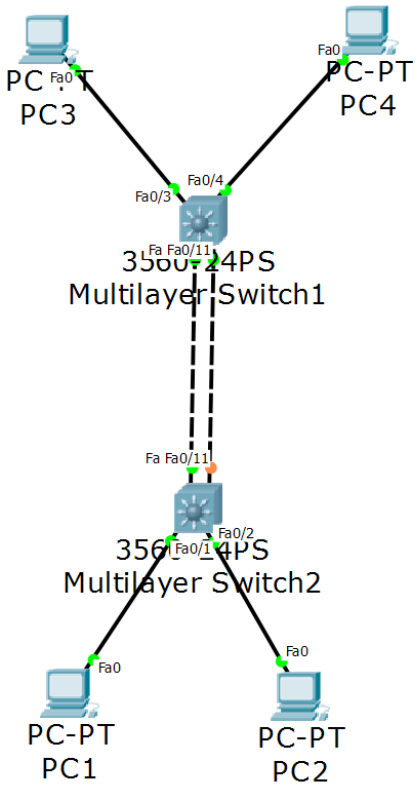
An IP address is a layer 3 address that is assigned to each host on the TCP/IP network. An IP address is 32 bits and is organized in 4 different octets (each 8 bits). It is represented in dotted decimal notation, for example 1.1.1.1. The IP address 1.1.1.1 is a class A address. The hostname is set in the CLI and is used to identify the router or switch. The passwords are used to enter in privilege mode and to enter into the router. Also they are used to telnet into the router.



(10 points)

2. STP and the use of portfast (Make sure you specify this for Cisco 2960 and 3560 series switches since this is what we are using this semester in the lab.)

   STP stands for Spanning-Tree Protocol and prevents loops from occurring. Spanning-Tree Protocol utilizes the 802.1D standard which is an algorithm that exchanges messages with other switches so it can detect loops. In this topology the switches automatically configure STP. Portfast is something that improves STP by allowing ports attached to devices like a PC to go from a blocked or disabled to a forwarding state.



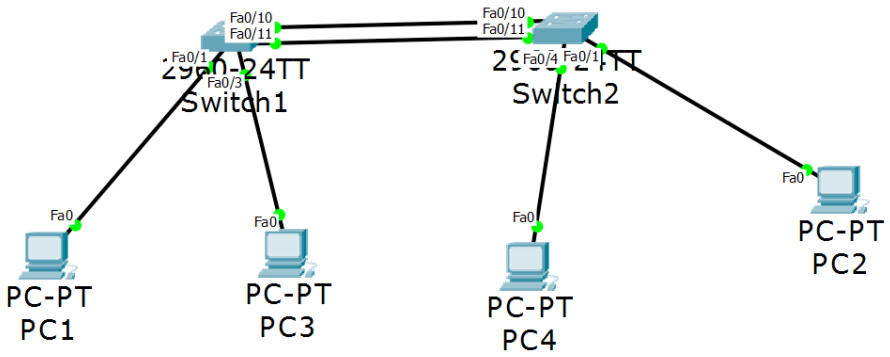
Switch(config)# int f 0/11	Interface f 0/11 configuration mode
Switch(config-if)# switchport trunk encapsulation dot1q Switch(config-if)# switchport mode trunk *Cisco 3560* switch	Enables trunking on that port Puts the interface into trunk mode
Switch(config-if)# switchport mode trunk *Cisco 2960*switch	Enables trunking on that port
Switch(config)# do show int trunk	Shows if you are trunking and on what interface. If you are not trunking at all then a blank space will appear
Switch(config)# spanning-tree portfast	Enable portfast on all access ports by default

After this configuration I would try to ping the PC's. I have full connectivity in this scenario.

(10 points)

3. VLANs, VTP with 802.1q (NOTE: how to create one or more with names, assigning different interfaces to VLANs, etc… (Make sure you accomplish this without going into VLAN Database mode (this is the deprecated way of configuration for VLANs!) Make sure you setup an IP Address on the administrative VLAN and show the syntax for both 2960 and 3560 switches!)

A VLAN is a virtual LAN and is configured on layer 2 (switches). The purpose of VLAN's is to segment the network and reduce congestion on the larger LAN. VTP stands for VLAN Trunking Protocol and is a cisco protocol that spreads the meaning of the VLAN to entire LAN. VTP carries the VLAN information to all the switches in the VTP domain. 802.1q is a networking standard from the IEEE that supports VLANS.



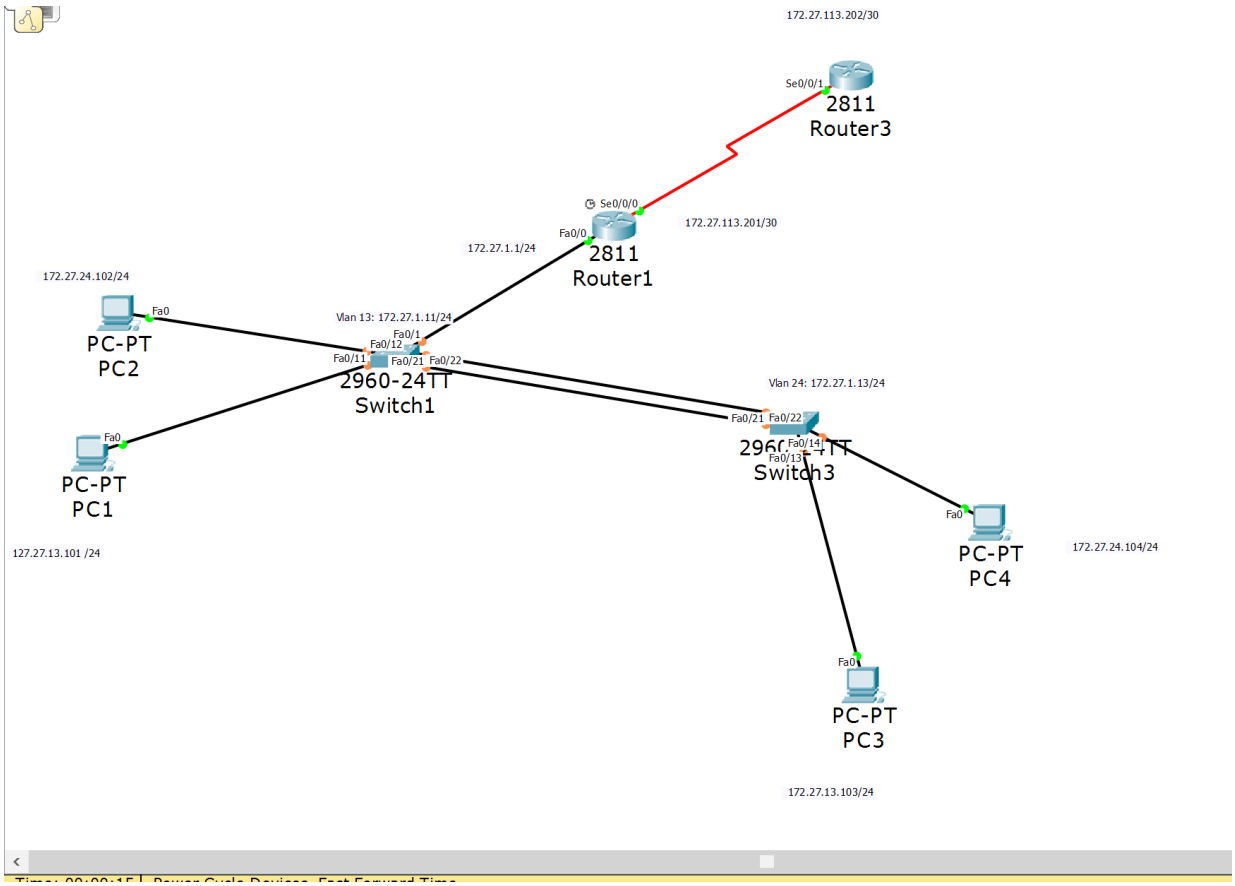
Switch(config)# vtp domain INETLAB	Creates the VTP domain called INETLAB

Switch(config)# vtp password cisco	Sets the VTP domain password to cisco
Switch(config)# vtp mode server	Sets the VTP mode to server mode (can create vlans in server mode, in client mode you cannont)
Switch(config)# int vlan1	Takes you into administrative vlan configuration mode
Switch(config-vlan)# ip address 172.17.34.11 255.255.255.0	Sets the ip address of the administrative vlan with a /24 subnet mask
Switch(config)# int f 0/1	Takes you into f 0/1 configuration mode
Switch(config-if)# switchport mode access	This interface will belong to one vlan and one vlan only
Switch(config-if)# switchport access vlan 12	Creates vlan 12 and now this interface will belong to vlan 12
Switch(config)# vlan 12	Takes you into vlan 12 configuration mode
Switch(config-vlan)# name VLAN-PC12	Sets the name of vlan 12 to VLAN-PC12
Switch(config)# int f 0/11	Takes you into f 0/11 configuration mode
Switch(config-if)# switchport mode trunk *2960 switch*	Enables trunking on this interface with encapsulation 802.1q
Switch(config-if)# switchport trunk encapsulation dot1q *3560 switch*	Enables trunking on this interface with encapsulation 802.1q
Switch(config)# do show int vlan	Shows you all the vlans configured and if they are configured on this interface
Switch(config)# do show vtp INETLAB status	Shows information about the vtp (Like if it's a client or server, and the name)

(10 points)

4. Inter-VLAN routing (NOTE: With a router-on-a-stick and SVIs)

Inter-VLAN routing is the process of routing traffic between virtual LAN networks. This process can be completed on the switch itself. A router on stick means that there is trunking enabled from a switch up to a router meaning that packets are sent up through the trunk to the router and back down to its destination. SVI stands for switched virtual interface and are represented by one of the interfaces on the router. The purpose of this is to provide the layer 3 handling for the packets that are coming from the switch ports associated with the VLAN.



Router(config)# int f 0/0	Takes you into interface f 0/0 configuration mode
Router(config-if)# no ip address	With inter-VLAN routing you do not need an ip address so if there is already one configured on this interface this command erases it
Router(config)# int f 0/0.1	This creates a subinterface on interface f 0/0
Router(config-subif)# encapsulation dot1q 1	Defines the encapsulation format as 802.1q and sets the VLAN 1 to this interface

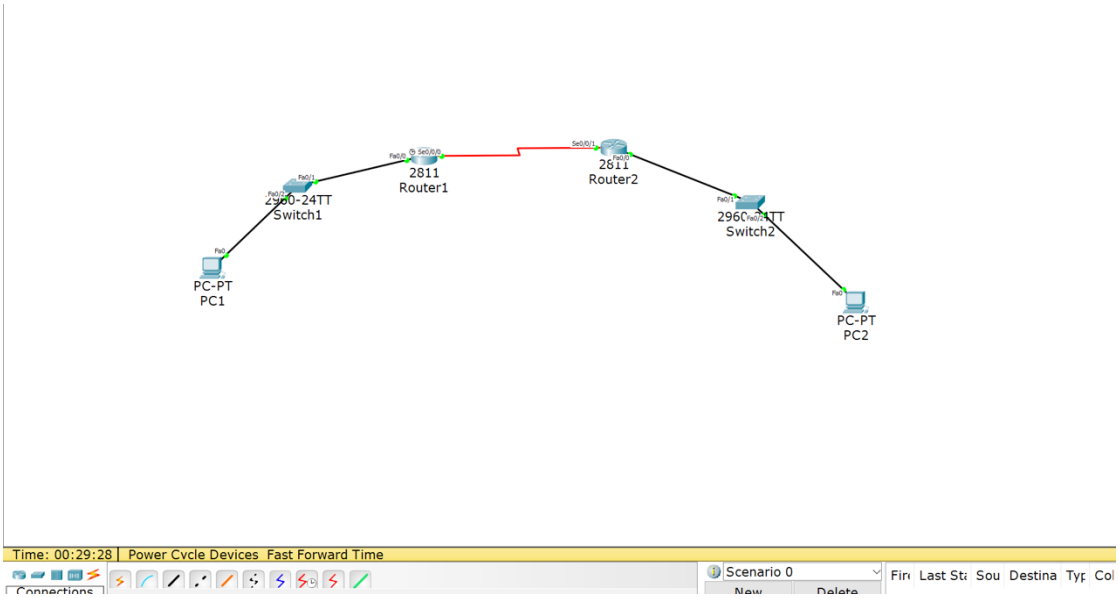
Router(config-subif)# ip address 172.17.34.1 255.255.255.0	Sets the ip address and subnet mask for this subinterface
Router(config)# int f 0/0.12	Creates another subinterface that will be used with vlan 12
Router(config-subif)# encapsulation dot1q 12	Defines the encapsulation format to 802.1q and identifies VLAN 12 to this interface
Router(config-subif)# ip address 172.17.30.1 255.255.255.0	Sets the ip address and subnet mask for this interface
Router(config)# int f 0/0.34	Creates another subinterface that will be used with vlan 34
Router(config-subif)# encapsulation dot1q 34	Defines the encapsulation format to 802.1q and identifies VLAN 12 to this interface
Router(config-subif)# ip address 172.17.27.1 255.255.255.0	Sets the ip address and subnet mask for this interface
Switch(config)# interface f 0/1	Interface f 0/1 configuration mode
Switch(config-if)# swithport mode trunk (do the same on the f 0/22 port) ***cisco 2960 switch***	Enables trunking on the f 0/1 port
Switch(config)# do show int trunk	Shows where the switch is trunking
Router(config)# do show run	Shows the entire running configuration. I would use this command to check if all my subinterfaces are configured correctly

(10 points)

5. Static routing (NOTE: With AND Without the use of a default static route.)

The process of static routing includes configuring each route a packet could take across the network. If there are three subnets you would need to configure routes for two of the networks. You would not configure the one that is directly connected to that router because it is not needed.

Router1(config)# ip route 172.34.17.0 255.255.255.0 1.1.1.2	This static route includes (in order) the destination network ip address, the subnet mask of that network and the next hop address.
Router2(config)# ip route 172.17.34.0 255.255.255.0 1.1.1.1	This static route includes (in order) the destination network ip address, the subnet mask of that network and the next hop address.
Router(could be either router)(config)# do show ip route	Displays the routing table on that router. We will see three different routes since there are three subnets. Two of them with be directly connected and one of them will be displayed as a static route

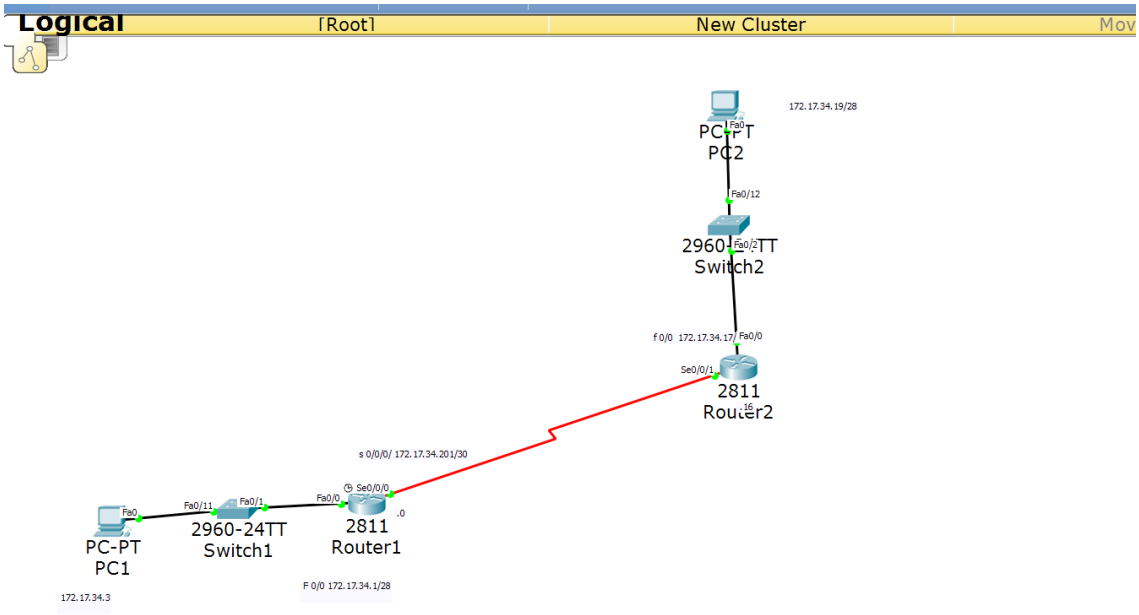


After configuring the static routes I would ping PC1 to PC2 and should get a reply.

(10 points)

6. RIP and RIPv2

RIP represents Routing Information Protocol and the way it is configured is by network advertisements. Router RIP metric is HOP and its administrative distance value is 120, also being a classful protocol. RIP routing version 2 is a classless which means it takes into account subnet mask. The default RIP is classful and looks at the default subnet mask.



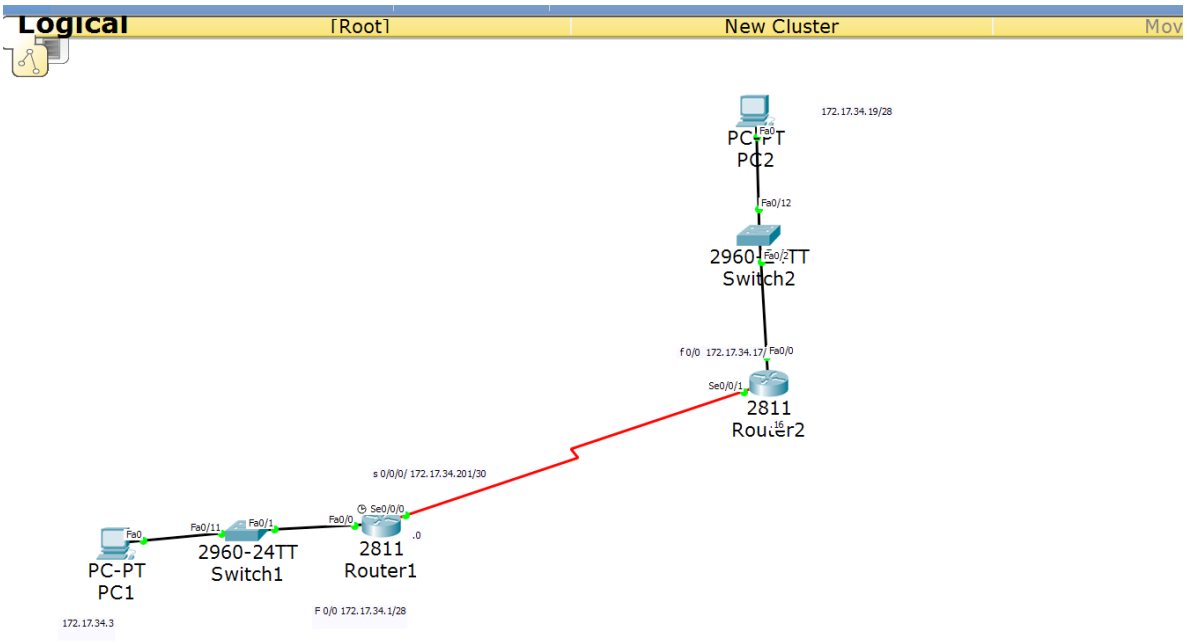
Router1(config)# router rip	*Takes the router into router rip configuration mode*
Router1(config-router)# passive-interface f 0/0	*This command tells the router not to send advertisements out of interface f 0/0*
Router1(config-router)# network 172.17.34.200 *Router1(config-router)#network 172.17.34.0*	*Advertises these network's (these address's are NETWORK address's)*
Router1(config-router)# version 2	*Tells the router to use RIP version 2*
Router(config)# do show ip route	Displays the routing table. Should see two directly connected routes and one route being a RIP learned route

Router(config)# do show ip protocol	Shows what routing protocol you have configured on that router. Also showing you which networks you are routing for After this configuration I ping my PC's and get a reply.

(10 points)

7. EIGRP (NOTE: Make sure you utilize VLSM in your topology and configuration without the use of automatic summarization.)

EIGRP represents Enhanced Interior Gateway Routing Protocol and by default is a classful protocol. It's metric is made up of composite, bandwidth, load, delay, reliability, and MTU-size with an administrative distance of 90. EIGRP's updates are based on topological change and also uses an AS number (Autonomous system).



Router(config)# router eigrp 307	Command to take the router into router EIGRP configuration mode (the number represents the AS number)
Router(config-router)# no auto-summary	This makes router EIGRP a classless protocol
Router(config-router)# network 172.17.34.0 0.0.0.15	Advertises this network and includes: the network address and the wildcard mask of that network

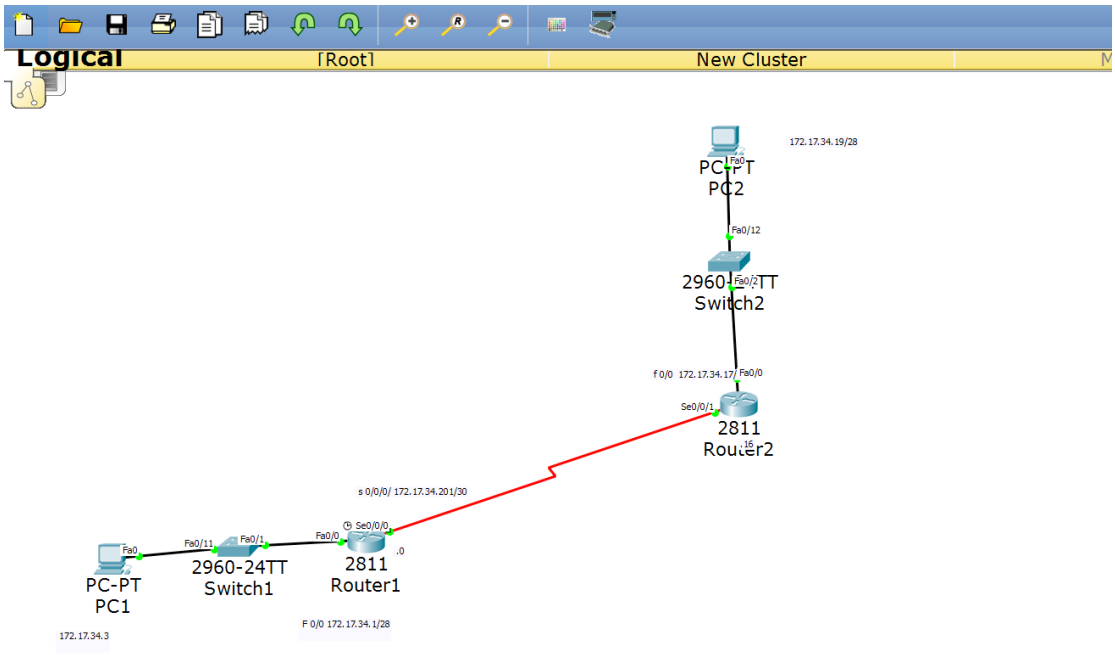
Router(config-router)# network 172.17.34.200 0.0.0.3	Advertises this network and includes: the network address and the wildcard mask of that network
Router(config)# do show ip route	Displays the routing table. In this topology we see two directly connected routes and one EIGRP learned route
Router(config)# do show ip protocol	Shows which protocol is configured (EIGRP) and the networks it is advertising. Also shows other information like no auto summary

After this configuration I tested by pinging the PC's. I have full connectivity in this topology.

(10 points)

8. OSPF (NOTE: Make sure you utilize loopback interfaces within your topology and configuration…and make sure you specify why you are utilizing them.)

OSPF stands for Open Shortest Path First and is an interior gateway protocol. Something that makes it different from the other protocol's is that it has a backbone area which is the core of OSPF. OSPF's metric refers to bandwidth and it's administrative distance value is 110. A loopback interface is a virtual interface that never changes. It can be used as the identifier for the router because it does not change. Also OSPF is professor Cannistra's favorite routing protocol.



Router(config)# router ospf 1	Takes you into router OSPF configuration mode
Router(config-router)# default-information originate	Generates a default external route into OSPF
Router(config-router) network 172.17.34.0 0.0.0.15 area 0	Advertises this network and includes: network address, wildcard mask for that network, and an area for that router
Router(config-router)network 172.17.34.200 0.0.0.3 area 0	Advertises this network and includes: network address, wildcard mask for that network, and an area for that router
Router(config)# int l 0	Loopback interface configuration mode

Router(config-if)# ip address 199.199.199.199 255.255.255.255	Sets ip address for loopback interface

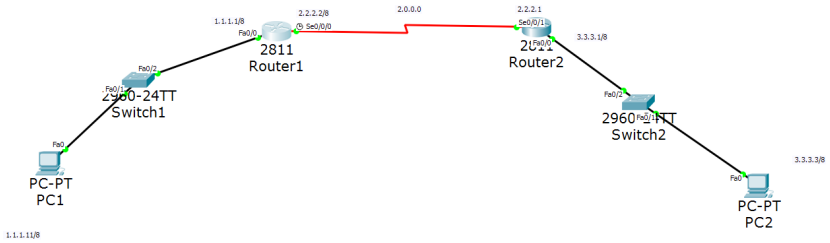
Router(config)# do show ip route	Displays the routing table. Should see two directly connected routes and one OSPF learned route
Router(config)# do show ip protocol	Displays information about what protocol (OSPF) you have configured also displaying the networks it is advertising After this I would ping my PC's showing that I have full connectivity

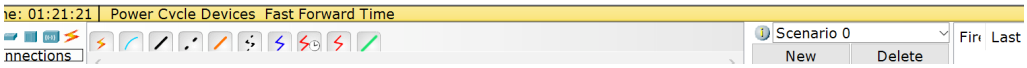
(10 points)

9. Standard ACLs and Standard Named ACLs (NOTE: how, where and why you applying these…)

ACL stands for Access Control List and it is a primitive form of a firewall. The purpose of ACL's is to filter packets and there are two types. The first being standard which is based on source address only and is place as close to the destination as possible.

In this scenario we wouldn't want PC-A access to anything so we would use a standard ACL. The ACL would be placed on RouterA which is closest to PC-A also being on interface f 0/0 (also being applied in an inbound direction).





RouterA(config)# access-list 7 deny 1.1.1.11 0.0.0.0	Creates an access list (the 7 can be any random number 1-99). Adding to the list to deny the source address of 1.1.1.11 and the source address's wildcard mask of 0.0.0.0 the wildcard mask represents the octets we want to look at
RouterA(config)# access-list 7 permit any	This command is very important because by default the access list has a deny any therefore not letting in any packets so this command lets all other packets through other than from the source of 1.1.1.11
RouterA(config)# int f 0/0	Goes into interface f 0/0 configuration mode
RouterA(config)# access-group 7 in	This command applies the access list in an inbound fashion
RouterA(config)# ip access-list ac deny 1.1.1.11 0.0.0.0	This is the same command as before but only if you wanted a named access list

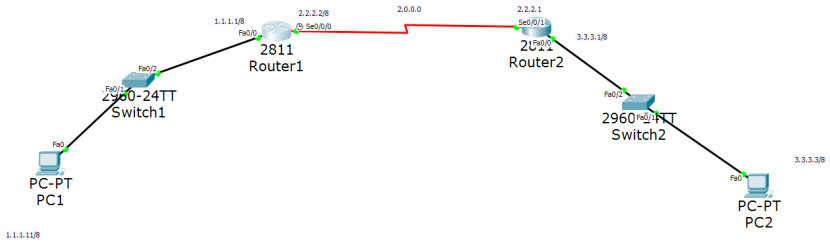
RouterA(config)# do show run	Shows the entire configuration for this router. I would use this command to make sure I configured the access-list correctly
After this I would try to ping anything from PC and see that it has failed.	

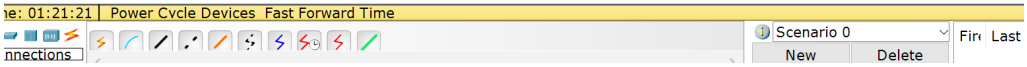
(10 points)

10. Extended ACLs and Extended Named ACLs (NOTE: how, where and why you applying these…)

    The second type of ACL's, extended is base on source address, destination address, protocol and optionally the port number and is placed as close to the source as possible.

    In this scenario if we wanted to block traffic from PC-1's LAN to a server via HTTP we would use the extended ACL and put it on Router1, interface f 0/0, going inbound.





Router(config)# ip access-list extended BLOCK	Creates an access-list named BLOCK
Router(config)# deny tcp 172.17.34.0 0.0.0.15 172.17.34.54 0.0.0.0 eq 80	This command puts into the list to deny any traffic coming from the 172.17.34.0 network including to the wildcard mask with the destination to the 172.17.34.54 (server) through port 80
Router(config)# permit ip any any	Since by default the ACL has a deny ip any any you need this command to let other packets get through
Router(config)# int f 0/0	Goes into interface f 0/0 configuration mode
Router(config-if)# ip access-group BLOCK in	Applies this ACL in an inbound fashion

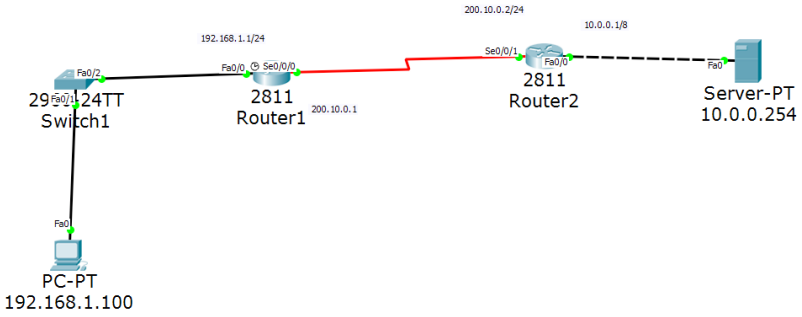
RouterA(config)# do show run	Shows the entire configuration for this router. I would use this command to make sure I configured the access-list correctly After this configuration I try to ping anything from PC 1 LAN and do not get a reply meaning that the access-list worked.

(10 points)

11. NAT/PAT (NOTE: Make sure you show a configuration with only NAT, then PAT...remember there are multiple ways to configure PAT. Also show a configuration with static NAT.)

    NAT stands for Network Address Translation and is used for security, and so we can utilize more ip address's. Static NAT is the simplest type of NAT because it is a one-to-one translation. In the command to configure NAT you only need the ip address you want to translate (usually a private ip) and the address you want it to translate to (a public ip). Dynamic NAT is different because instead of a one-to-one translation the router creates one-to-one mapping. When issuing the command, you have to define the NAT pool and the range of address's also including the network mask.

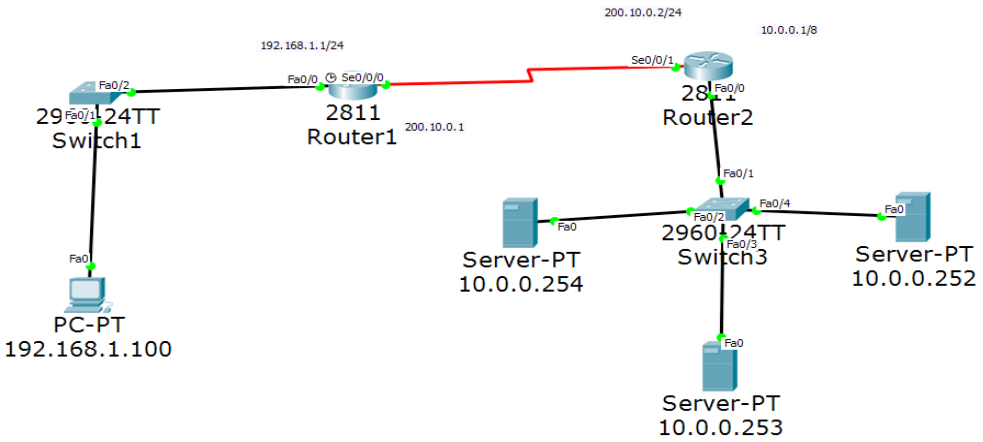
    PAT represents Port Address Translation and is an extension to NAT. The purpose of PAT is to save more IP addresses. When utilizing PAT the router is given a public ip address and assigns its users a port number which has it's own IP address. In practical use two users can have the same IP address but be on a different port therefore the router knows where to send packets to.



Static NAT configuration	

Router2(config)# ip nat inside source static 10.0.0.254 200.10.0.2	Statically configuring the server's address of 10.0.0.254 to translate to 200.10.0.2. Now PC-1 can access the server through the ip address of 200.10.0.2
Router2(config)# interface s 0/0/1	Interface s 0/0/1 configuration mode
Router2(config-if)# ip nat outside	This interface is on the outside of the translation
Router2(config)# interface f 0/0	Interface f 0/0 configuration mode
Router2(config-if)# ip nat inside	This interface is on the inside of the NAT translation
Router2(config)# do show nat translation	Displays the NAT table For verification I would go to my PC and go into the web browser. When I enter in the routers serial interface address it translates to the server's address and brings up the website hosted on the server. Meaning that the NAT translation worked!

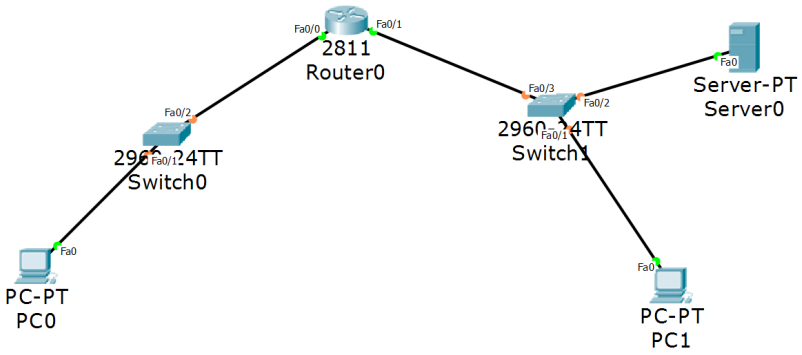
For this configuration I decided at to add a switch and more servers	
Router2(config)# ip nat pool NATPOOL 10.0.0.250 10.0.0.254 netmask 255.0.0.0	Creates a nat pool named NATPOOL with the range 10.0.0.250-10.0.0.254 and a netmask of 255.0.0.0



(10 points)

12. DHCP Server and client (NOTE: You should have a DHCP Server for a local and remote network.)

DHCP stands for Dynamic Host Configuration Protocol and is a protocol that contains IP address and can assign them to different devices. Usually it is configured on a server and on the server once you enable DHCP you must provide a range of address's and also enable DHCP on the devices (ex PC's). The PC broadcast's DHCP and the DHCP server assigns it an ip address in the given range.



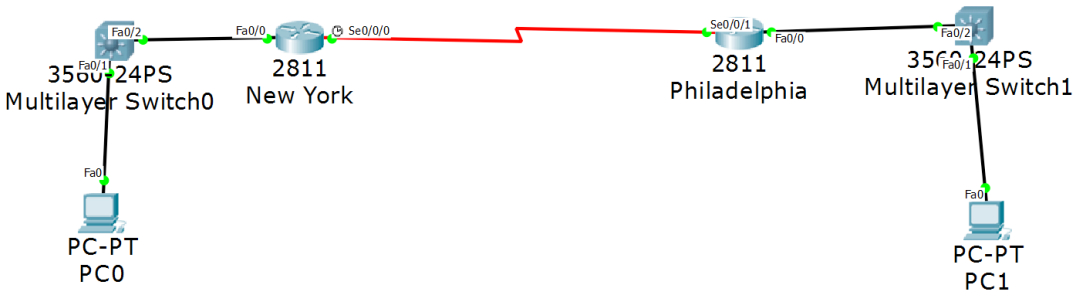
Router(config)# interface f 0/0	Interface f 0/0 configuration mode
Router(config-if)# ip helper-address 192.168.2.254	Command so that DHCP can be used across the network

Configuring DHCP on a router	
Router(config)# ip dhcp excluded	Enables DHCP on the router
Router(config)# ip dhcp excluded-address 192.168.201.1 192.168.201.12	Tells the router the IP addresses that the DHCP server should not assign to DHCP users
Router(config)# default-router 192.168.201.1	Clears the ip dhcp binding To test to see if this works go to your PC's and enable dhcp and see if it gives you an address
Router(config)# do show ip dhcp binding	Displays the bindings that are configured on the router

(10 points)

13. PPP, PPP PAP and PPP CHAP (NOTE: you may either provide a topology that utilizes both: PPP PAP and CHAP or create two separate topologies.)

    PPP (Point-to-Point Protocol) and is a protocol that can be implemented by any vender. Also, PPP provides authentication and HDLC (default encapsulation) does not. Another reason to use PPP is to prevent encapsulation mismatch especially if there is a cisco router on one end and a non cisco router on the other end.

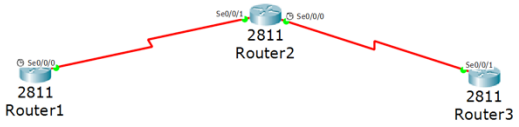


Router(config)# hostname NewYork	When configuring PPP a hostname makes it easier to configure CHAP
NewYork(config)# interface s 0/0/0	Interace serial 0/0/0
NewYork(config-if)# encapsulation ppp	Changes WAN encapsulation from HDLC (default) to PPP
Philadelphia(config-if)# encapsulation ppp	Doing the same thing on router Philadelphia on interface s 0/0/1
NewYork(config)# username Philadelphia password givemeanA	This is to setup the handshake between the NewYork and Philadelphia routers
NewYork(config)# interface s 0/0/0	Interace serial 0/0/0 configuration mode
NewYork(config-if)# ppp authentication chap	Authenticating the s 0/0/0 interface with the CHAP protocol
Philadelphia(config)# username NewYork password givemeanA	This will allow the routers to communicate with each other because they share the same password and know each other's hostname
Philadelphia(config)# interface s 0/0/1	Interface serial 0/0/1 configuration mode
Philadelphia(config-if)# ppp authentication chap	Authenticating the s 0/0/1 interface with the CHAP protocol (Now the two routers can actually communicate)
*Configuring PAP with some topology	
NewYork(config-if)# ppp pap authentication	Enables pap authentication on this interface s 0/0/0
NewYork(config-if)# ppp pap sent-username Philadelphia password givemeanA	Sets the username(the philly router) and password for PAP
Philadelphia(config-if)# ppp pap authentication	Enables pap authentication on this interface s 0/0/1
Philadelphia(config-if)# ppp pap sent-username NewYork password givemeanA	Sets the username and password for PAP now the routers can communicate using PAP
Router(config)# do show run	I would do a show run for both routers and compare them side by side to check if they are configured correctly

(10 points)

14. Frame Relay (NOTE: You should learn your DLCI numbers automatically from the Frame Relay Switch. Your LMI-Type should be altered from the default LMI-Type. You do NOT need to show a configuration with sub-interfaces for this semester.)

    Frame relay is a packet switching protocol for connecting deices via a WAN connection. Frame relay that maintains multiple virtual connections between routers. If there are three routers, using frame relay the middle router can handle traffic between networks. It handles the traffic without the use of ip addresses on the serial ports.



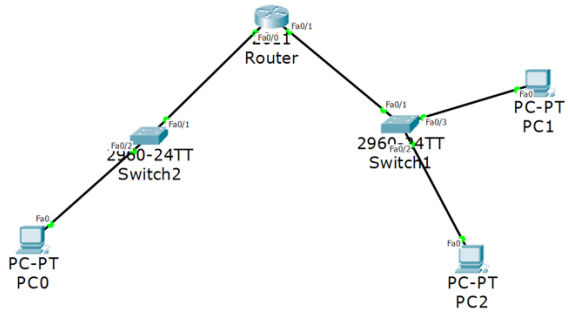
Router2(config)# frame-relay switching	Command to start the frame relay switching proccess
Router2(config)#interface s 0/0/0	Goes into interface s 0/0/0 configuration mode
Router2(config-if)# no ip address	No ip address for this interface
Router2(config-if)# encapsulation frame-relay	Changes the data link encapsulation from HDLC to frame-relay
Router2(config-if)# clock rate 64000	Sets the clock rate for this interface
Router2(config-if)# frame-relay intf-type dce	This interface is a DCE device
Router2(config-if)# frame-relay route 21 interface s 0/0/1 20	Defines a frame route so that any packet coming into interface s 0/0/0 DLCI 21 will go to s 0/0/1 DLCI 20
Router2(config-if)# no shutdown	Changes interface s 0/0/0 to an UP state
Router2(config)# interface s 0/0/1	Goes into interface s 0/0/1 configuration mode
Router2(config)# no ip address	No ip address for this interface
Router2(config)# encapsulation frame-relay	Changes the data link encapsulation from HDLC to frame-relay
Router2(config-if)# clock rate 64000	Sets the clock rate for this interface

Router2(config-if)# frame-relay intf-type dce	Specifies this interface as a DCE device
Router2(config-if)# frame-relay route 20 interface s 0/0/0 21	Defines a frame route so that any packet traveling into the interface s 0/0/1 DLCI 20 will go to the interface s 0/0/0 DCLI 21
Router2(config-if)#no shutdown	Changes interface s 0/0/1 to an UP state
Router2(config)# do show frame-relay map	Displays all the information about frame relay
Router2(config)# show controller s 0/0/0	Displays the information about the interface. Should see Frame-relay instead of HDLC After this I would test connection between the routers. I have full connectivity!

(10 points)

15. IPv6 (Please NOTE: You should still write a paragraph, create a topology, develop a configuration, display the show commands and provide a test case.)

    IPv6 (Internet Protocol version 6) is the newest version of the Internet protocol. The protocol that provides an identifier for devices so that they can communicate with other devices. IPv4 is only 32 bits and now IPv6 is 128 bits providing a much wider range for IP addresses. The address is also represented in hexadecimal notation instead of dotted decimal notation.



Router(config)# ipv6 unicast-routing	Enables ipv6 because it is disabled by default
Router(config)# int f 0/0	Interface f 0/0 configuration mode
Router(config-if)# ipv6 address FE80::1 link-local	Setting a local ipv6 address
Router(config-if)# ipv6 address 2001:DBB:AAAA:A::/64	Setting an ip address that can be routed (so the PC's can communicate across the router) with a / 64 subnet mask
Router(config-if)# no shutdown	Enables the f 0/0 interface
Router(config)# int f 0/1	Interface f 0/1 configuration mode

Router(config-if)# ipv6 address FE80::1 link-local	Setting a local ipv6 address (this is the same as the other interface because it is a LOCAL address, it is only know to this interfaces network)
Router(config-if)# ipv6 address 2001:DBB:AAAA:B::1/64	Setting an ip address that is routable so the PC's can communicate (subnet mask of /64)
Router(config-if)# no shutdown	Enables the f 0/1 interface
Router(config)# do show run	Shows the entire configuration. I would use this to see if the IPv6 addresses are configured correctly Also for verification I ping my PC's IPv6 addresses and get a reply.

Part II – (50 Points):

This part of the project is also extremely detail oriented! Please spend the time necessary to thoroughly complete this assignment since it will be most beneficial to you in the long run!

You should:

- Design your network topology using Cisco Packet Tracer. Your design should consist of Cisco Routers and Cisco Switches.
    - You should have two headquarters routers connected with redundancy to at least two multiple layer switches. The multiple layer switches should connect to at least four layer two switches with redundancy and fault tolerance in mind. At least two servers should exist within your headquarters location. One must be a TFTP server. The other service that exists on the server is up to you.
    - You should have at least five remote sites, each having at least one layer two switch each. At least one of these remote sites should have at least two switches connected together using port aggregation.
    - You should have one internet connection from the headquarters location out to an ISP. On the ISP, there should be at least two servers (ie: at least a DNS server and an HTTP server). The hosts will be great validation points in testing internet connectivity.
    - You should have at least 10 users per remote site and one remote site should have at least 255 users. You should show at least five hosts per location as a proof of concept within your design and within your implementation.
    - You should have at least 1025 users at the headquarters site. Again, you only need to show a subset of those users at key locations within the headquarters site (ie: 10 will be a good number of testing points).
- Design the IPv4 Addressing scheme for your network. Keep in mind you should be using RFC1918 Addressing internally and public ip addressing externally.
- Once your design is complete, configure the network within Cisco Packet Tracer 6.2 or greater as a "proof of concept" for your design.
- You must use at least ten of the technologies or protocols listed in Part I within your design and implementation.

PLEASE NOTE: There are topics that you must inherently include due to the design specifications. These may or may not be listed within the technologies above (ie: First Hop Redundancy Protocol (ie: HSRP) and Link Aggregation…just to name two).

This assignment should be **printed and turned in by 12:30pm Tuesday, December 08, 2015. 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! **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!!!**