Rafael Marmol

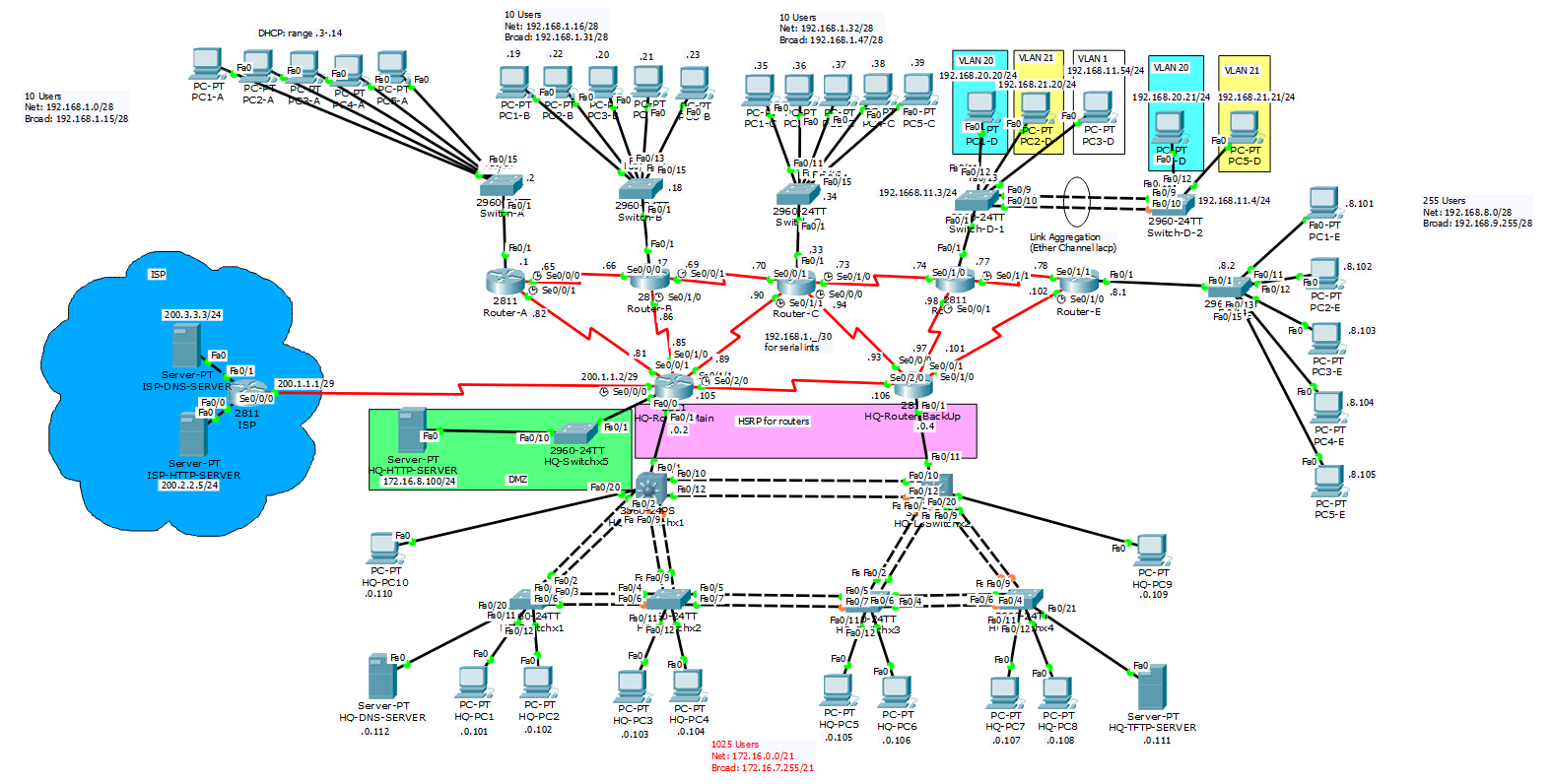
Internetworking

Professor Cannistra

6 May 2016

Project Phase II

**Topology**

****

**Network Documentation**

1. Static Nat
   1. How it works

A Network Address Translation in which a single private IP address is bound to a single public IP address. This allows for an internal host, such as a HTTP server to have a private IP and still be accessible over the Internet. In this project, the static NAT can be used for a DMZ or a demilitarized zone in which there is an HTTP server, which has a private IP of 172.16.8.100/24 in HQ which is only accessible from the ISP through its public address of 200.1.1.6/29 through HTTP or HTTP and anything else is denied.

* 1. Configuration

HQ-Router-Main

ip nat inside source static 172.16.8.100 200.1.1.6

!

ip access-list extended DMZ

permit tcp any host 200.1.1.6 eq www

permit tcp any host 200.1.1.6 eq 443

deny ip any any

!

Interface s0/0/0

Ip nat outside

!

Interface s0/0/1

Ip nat inside

!

Interface s0/1/0

Ip nat inside

!

Interface s0/1/1

Ip nat inside

!

Interface s0/2/0

Ip nat inside

!

Interface f0/0

Ip nat inside

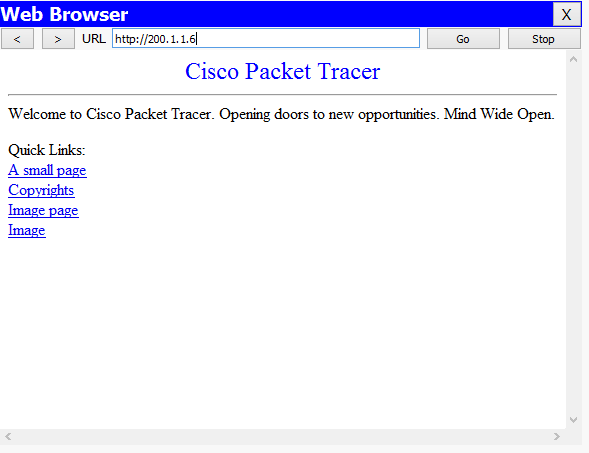
!

Interface f0/1

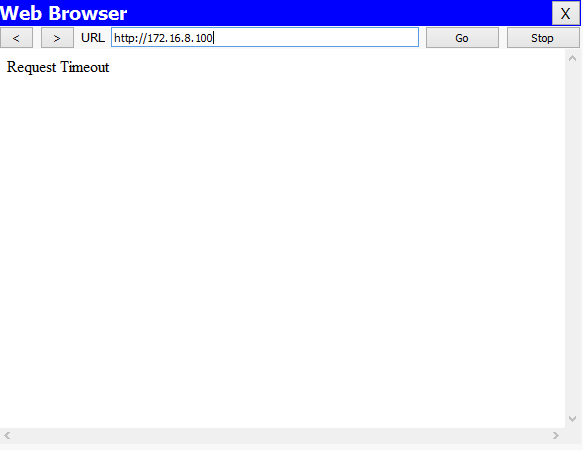
Ip nat inside

* 1. Verification

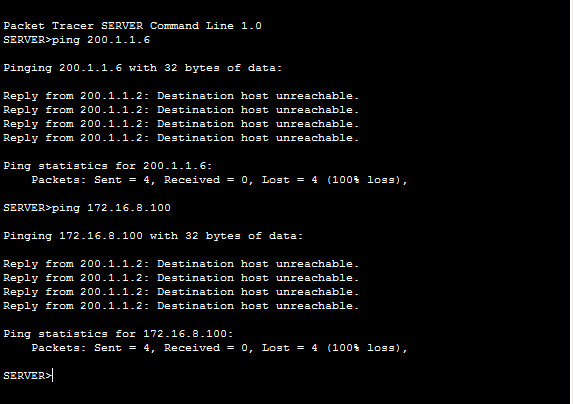
On the isp server’s web browser, it is able to access the DMZ HTTP server through its static NAT public address.



Any attempt to web browse its private IP will be blocked



Also, since anything but HTTP and HTTPS request are allowed, pings cannot go through.



You can also see where its bound in the HQ-Router-Main using “show ip nat translations”



* 1. Troubleshooting

To troubleshoot, I would first test by issuing “show ip nat statistics” to show inside sources and access-lists and see which interfaces are inside and which are outside. I feel like a common problem would be putting interfaces on the wrong side so it would be helpful to check that. Also, “show ip nat translations” will show me if any nat translations are going on and if there are none, then it shows that it’s not even set up.

1. Dynamic NAT/PAT
   1. How it works

This Network Address Translation translates a group of private addresses to a specific, premade pool of public addresses to access a destination network. First an access-list PRIVATE-ADDRESSES-USED-FOR-NAT was created to only allow the wanted private ip addresses to be translated. Then the Dynamic NAT/PAT is used to bind all IP’s from the access-list to the pool of public IP addresses defined in PUBLIC-NAT-POOL. Now, any private address will be translated to one of the public IP’s in the pool and that’s how it will be seen on the ISP.

* 1. Configuration

HQ-Router-Main

ip nat pool PUBLIC-NAT-POOL 200.1.1.3 200.1.1.5 netmask 255.255.255.248

ip nat inside source list PRIVATE-ADDRESSES-USED-FOR-NAT pool PUBLIC-NAT-POOL overload

ip nat inside source static 172.16.8.100 200.1.1.6

!

ip access-list standard PRIVATE-ADDRESSES-USED-FOR-NAT

permit 192.168.0.0 0.0.255.255

permit 172.16.0.0 0.0.255.255

deny any

!

Interface s0/0/0

Ip nat outside

!

Interface s0/0/1

Ip nat inside

!

Interface s0/1/0

Ip nat inside

!

Interface s0/1/1

Ip nat inside

!

Interface s0/2/0

Ip nat inside

!

Interface f0/0

Ip nat inside

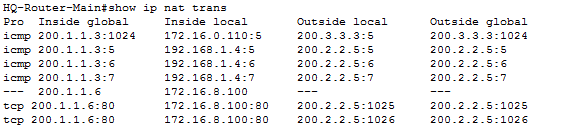
!

Interface f0/1

Ip nat inside

* 1. Verification

PC1-A (192.168.1.4) and HQ-PC10 (172.168.0.110) pinged the two ISP servers and using the “show ip nat translations” command, we can see where each private address is translated into the public addresses.



* 1. Troubleshooting

To troubleshoot this, I would ping out and then check the nat translations through the “show ip nat translations” to see what’s going on. I would also check to make sure the access-list is set up correctly and its added to the right pool by checking the running-config. Again, check that the right interfaces are on the outside and inside.

1. DHCP
   1. How it works

Dynamic Host Configuration Protocol is a client/server protocol that automatically provides hosts with an IP address, subnet mask, and default-gateway from a pool of designated ip addresses. In this case, Router-A acts as the DHCP server providing PC1-A to PC5-A their own ip addresses and additional information. For the PC to receive this, you have to go into configuration and select DHCP. Also, in the router the pool, A-PC-POOL, is defined to exclude certain addresses and the first available address comes after that range.

* 1. Configuration

Router-A

ip dhcp excluded-address 192.168.1.1 192.168.1.2

!

ip dhcp pool A-PC-POOL

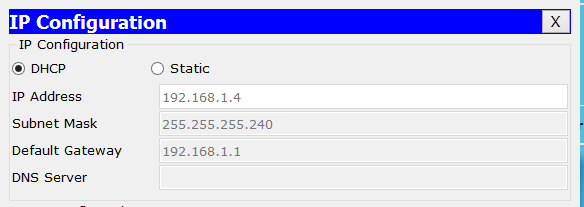
network 192.168.1.0 255.255.255.240

default-router 192.168.1.1

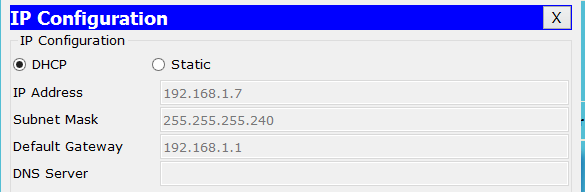
* 1. Verification

In PC1-A and PC2-A’s ip configuration you can see that it is through DHCP and what it has been leased

PC1-A



PC2-A



* 1. Troubleshooting

To troubleshoot this, I would first disconnect the PC from DHCP and reconnect to see if it just needed to be updated and if that didn’t work, I would check the running-config of the router that has the DHCP server to see if a pool was made and check its parameters, making sure its range and network address was correct.

1. Routing Protocol (EIGRP)
   1. How it works

First off, a routing protocol is how routers communicate with each other and it determines the path of routes. I used EIGRP or Enhanced Interior Gateway Routing Protocol, which is a hybrid routing protocol developed by Cisco Systems and uses the same distance vector algorithm and distance information as IGRP, but it uses more advanced features to avoid routing loops and to speed convergence times. It also supports VLSMs and route summarization. One should use EIGRP with medium to large networks, which this project is and because it is fast and cost effective. In the project, I used EIGRP to connect all of the routers through the service area of 307. In EIGRP, on each router, you advertise the networks you’re directly connected to and its wildcard mask and use no auto-summary to disable the default behavior of automatic summarization of subnet routes into network level routes. For the HQ-Router-Main, which has a static route, you can inject it through the command “redistribute static” so that the other routers can use that path as well.

Sources:

https://www.informit.com/library/content.aspx?b=CCNA\_Practical\_Studies&seqNum=54

http://www.cisco.com/c/en/us/td/docs/ios/12\_2/iproute/command/reference/fiprrp\_r/1rfeigrp.html

* 1. Configuration

Router-A

router eigrp 307

network 192.168.1.0 0.0.0.15

network 192.168.1.64 0.0.0.3

network 192.168.1.80 0.0.0.3

no auto-summary

Router-B

router eigrp 307

network 192.168.1.16 0.0.0.15

network 192.168.1.64 0.0.0.3

network 192.168.1.68 0.0.0.3

network 192.168.1.84 0.0.0.3

no auto-summary

Router-C

router eigrp 307

network 192.168.1.32 0.0.0.15

network 192.168.1.68 0.0.0.3

network 192.168.1.72 0.0.0.3

network 192.168.1.88 0.0.0.3

network 192.168.1.92 0.0.0.3

no auto-summary

Router-D

router eigrp 307

network 192.168.1.72 0.0.0.3

network 192.168.1.76 0.0.0.3

network 192.168.1.96 0.0.0.3

network 192.168.11.0

network 192.168.20.0

network 192.168.21.0

no auto-summary

Router-E

router eigrp 307

network 192.168.8.0 0.0.1.255

network 192.168.1.76 0.0.0.3

network 192.168.1.100 0.0.0.3

no auto-summary

HQ-Router-Main

router eigrp 307

redistribute static

network 172.16.0.0 0.0.7.255

network 192.168.1.80 0.0.0.3

network 192.168.1.84 0.0.0.3

network 192.168.1.88 0.0.0.3

network 192.168.1.104 0.0.0.3

network 172.16.8.0 0.0.0.255

no auto-summary

HQ-Router-BackUp

router eigrp 307

network 172.16.0.0 0.0.7.255

network 192.168.1.104 0.0.0.3

network 192.168.1.92 0.0.0.3

network 192.168.1.96 0.0.0.3

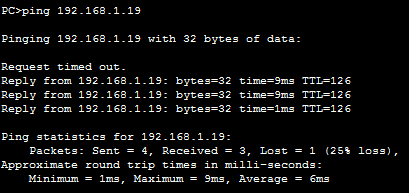
network 192.168.1.100 0.0.0.3

no auto-summary

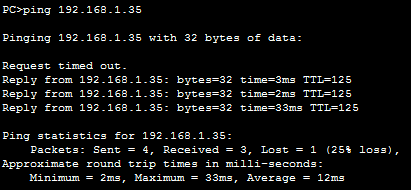
* 1. Verification

This project has full connectivity through EIGRP.

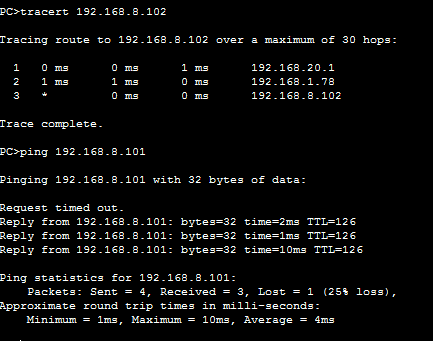
PC1-A to PC1-B



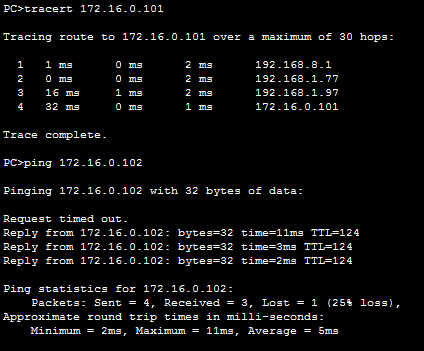
PC1-A to PC1-C



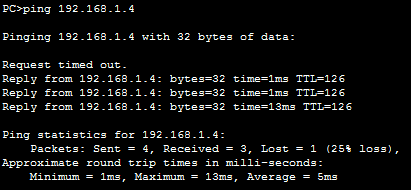
PC1-D to PC1-E and PC2-E



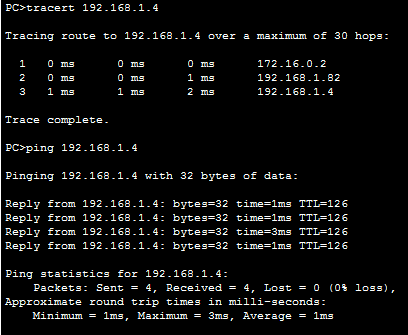
PC4-E to HQ-PC1



HQ-PC1 to PC1-E

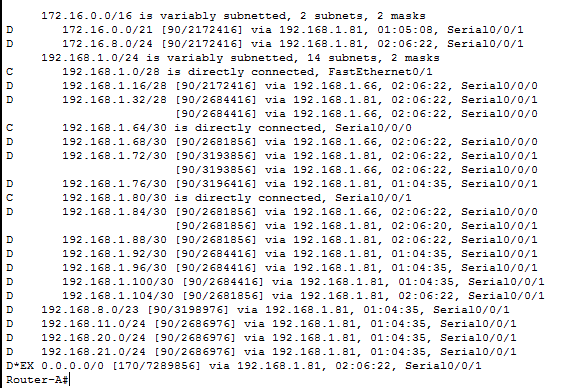


HQ-PC5 to PC1-A

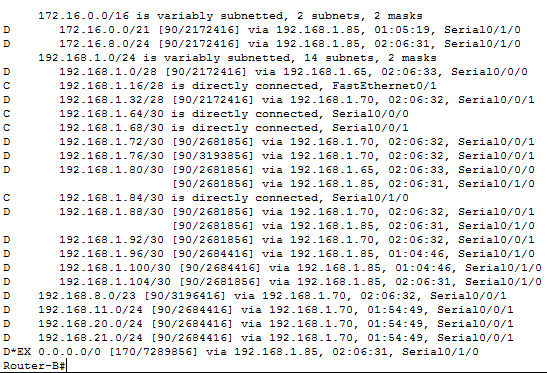


“show ip route”

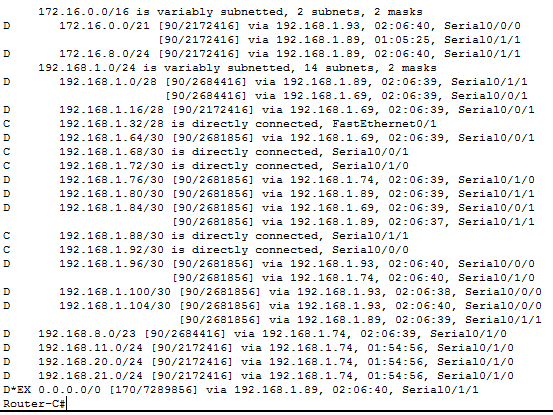
Router-A



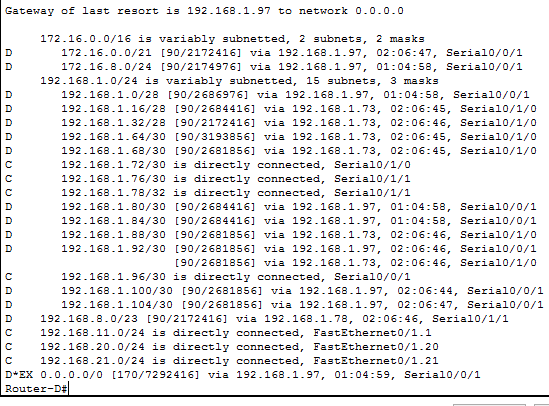
Router-B



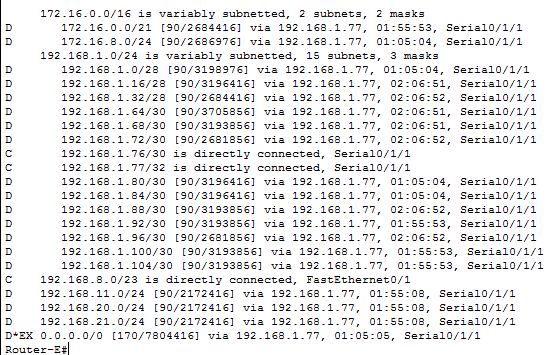
Router-C



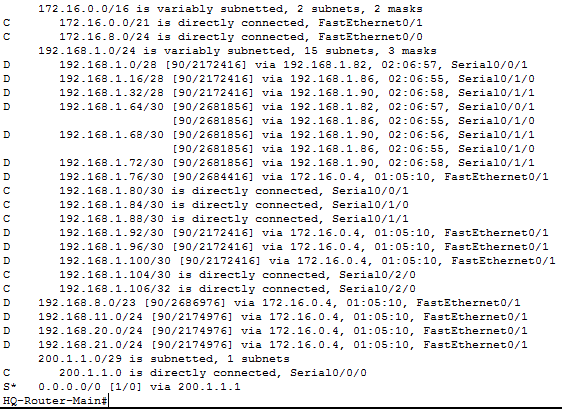
Router-D



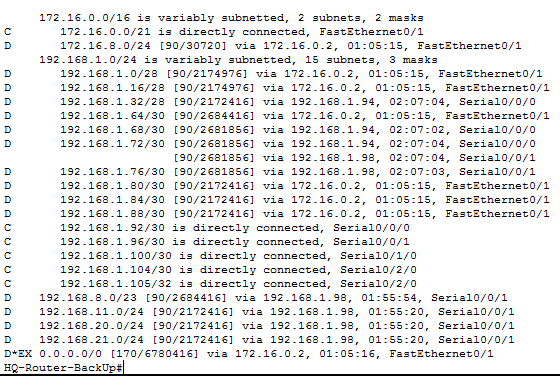
Router-E



HQ-Router-Main



HQ-Router-BackUp



* 1. Troubleshooting

To troubleshoot this, I would ping from PC’s to PC’s in different networks checking which ones connect. If there was a problem, I’d go into the router’s running config and checking their eigrp setup and double-checking all the numbers and wildcard masks were correct. Also, making sure the service area is the same. In addition, I would issue “show ip route” to see which networks it’s connected and not connected to and issue “show ip protocol” to make sure each router is within the same protocol.

1. First Hop Redundancy Protocol (HSRP)
   1. How it works

First Hop Redundancy Protocols are used in case any devices go down and provides a backup path to take. In HSRP or Hot Standby Router Protocol, the protocol establishes a fault-tolerant default-gateway. In this project, HQ-Router-Main acts as the main path for users on that network to take and if it were to burn in a fiery explosion, HQ-Router-BackUp would act as the default-gateway for users on that same network. In both routers, you have to set up the same standby ip while the interfaces which act as the gateway get different IP addresses and since HQ-Router-Main is the main router its given a higher priority number of 150 and HQ-Router-BackUp gets a smaller priority of 105. The higher priority gets the main path.

* 1. Configuration

HQ-Router-Main

interface FastEthernet0/1

ip address 172.16.0.2 255.255.248.0

standby version 2

standby 0 ip 172.16.0.1

standby priority 150

standby preempt

HQ-Router-BackUp

interface FastEthernet0/1

ip address 172.16.0.4 255.255.248.0

standby version 2

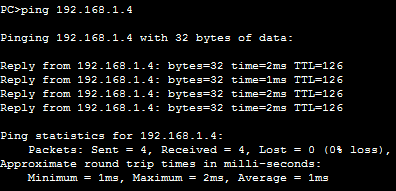
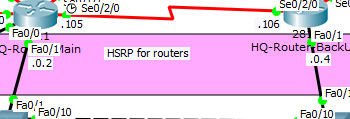
standby 0 ip 172.16.0.1

standby priority 105

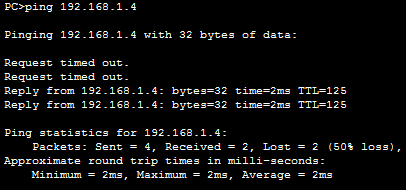
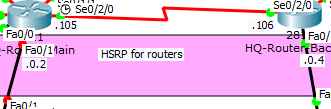
standby preempt

* 1. Verification

Before (HQ-Router-Main’s f0/1 is up)



After(HQ-Router-Main’s f0/1 is down and HQ-Router-BackUp takes over)



* 1. Troubleshooting

1. Link Aggregation (EtherChannel lacp)
   1. How it works

Link aggregation involves combining multiple interfaces into one aggregate channel. EtherChannel is port aggregation used for switches which makes one port-channel. Link Aggregation Protocol or LACP allows for bundling of ports together to form a single channel. In this project, on switches Switch-D-1 and Switch-D-2, I used lacp on both their f0/9 and f0/10 interfaces to make the one interface port-channel 1 on each side and configured it to be a trunk for the vlans in the network.

* 1. Configuration

Switch-D-1

interface FastEthernet0/9

channel-protocol lacp

channel-group 1 mode active

switchport mode trunk

!

interface FastEthernet0/10

channel-protocol lacp

channel-group 1 mode active

switchport mode trunk

!

interface Port-channel 1

switchport mode trunk

Switch-D-2

interface FastEthernet0/9

channel-protocol lacp

channel-group 1 mode passive

switchport mode trunk

!

interface FastEthernet0/10

channel-protocol lacp

channel-group 1 mode passive

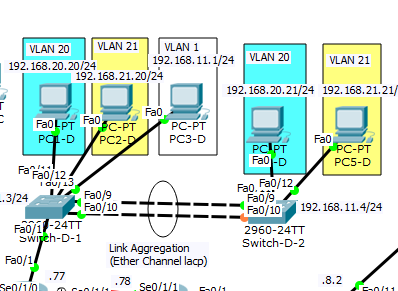
switchport mode trunk

!

interface Port-channel 1

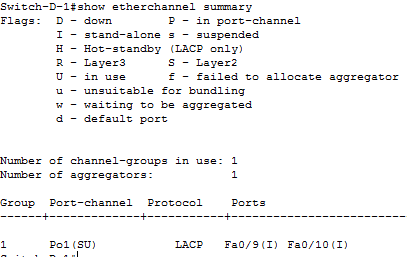
switchport mode trunk

* 1. Verification

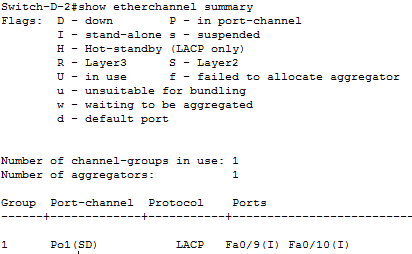


Show etherchannel summary

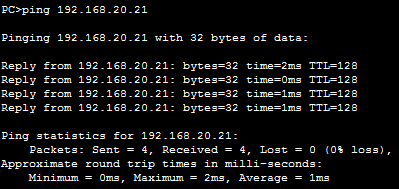
Switch-D-1



Switch-D-2



Ping across Port-Channel from PC1-D to PC4-D



* 1. Troubleshooting

To troubleshoot this, I would first ping out to the routers and then turn off one router and see if it still connects. I would then check the running-config of both routers to make sure the desired one has higher priority and the backup one is lower. Also, check the ip address of the standbys and make sure they’re correct.

1. VTP
   1. How it works

VTP or VLAN Trunking Protocol controls the definition of VLANS on the whole LAN by the VTP carrying VLAN information to all switches in the vtp domain. In this project, I used VTP on Switch-D-1 and Switch-D-2 on the domain INETLAB, where Switch-D-1 is the VTP Server and Switch-D-2 is the VTP client. The difference between a vtp server and client is that clients can’t create, change or delete vlans, while the server can. I also made the vtp password cisco. If an added switch does not share the same vtp password, than it cannot accept vtp advertisements.

Sources:

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\_52\_se/configuration/guide/3560scg/swvtp.html

* 1. Configuration

Switch-D-1

vtp domain INETLAB

vtp mode server

vtp password cisco

Switch-D-2

vtp domain INETLAB

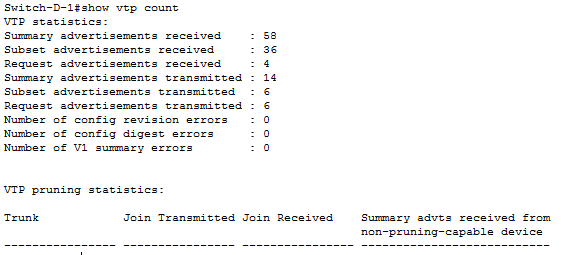
vtp mode client

vtp password cisco

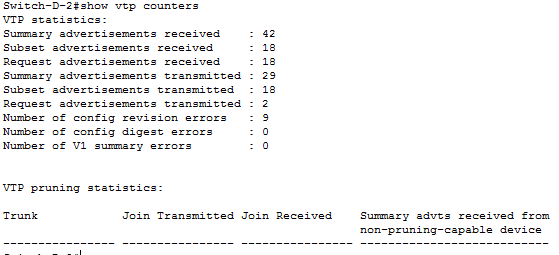
* 1. Verification

Show vtp counters

Switch-D-1

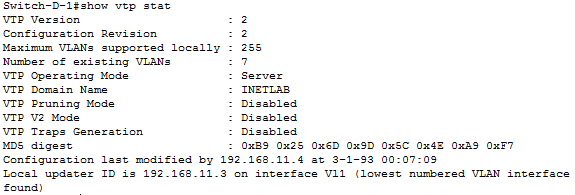


Switch-D-2

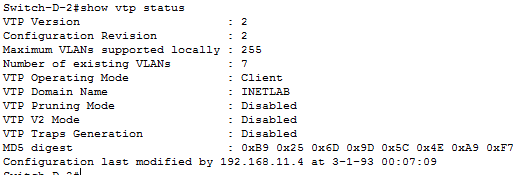


Show vtp statistics

Switch-D-1



Switch-D-2



Show vtp password

Switch-D-1



Switch-D-2



* 1. Troubleshooting

To troubleshoot this, I would go into the switches and issue “show vtp domain” to make sure it’s on the same one, “show vtp password” to make sure the passwords are the same, and finally check the “show vtp mode” to make sure it’s in the correct mode it’s supposed to be in.

1. VLANs
   1. How it works

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when they are really located on different LAN segments. Considered a logical not a physical connection. In this project, I used VLANS on the D network. VLAN 1 is always set on the switches with Switch-D-1 having the vlan 1 ip address as 192.168.11.3 and Switch-D-2 having the vlan 1 ip address as 192.168.11.4 and the default gateway as 192.168.11.1. On both switches, the interfaces connected to the end devices are configured with access mode and a specific vlan. On Switch-D-1, int f0/11 is assigned vlan 20, int f0/12 is assigned vlan 21, and int f0/13 is assigned vlan 1. On Switch-D-2, int f0/11 is assigned vlan 20 and int f0/12 is assigned vlan 21. The aggregate channel between the switches is in trunk mode which allows multiple vlans to cross. Normally, one vlan can only talk to other members in its own vlan, but since I have interVlan Routing setup they can.

* 1. Configuration

Switch-D-1

interface Vlan1

ip address 192.168.11.3 255.255.255.0

!

interface FastEthernet0/11

switchport access vlan 20

switchport mode access

!

interface FastEthernet0/12

switchport access vlan 21

switchport mode access

!

interface FastEthernet0/13

switchport mode access

Switch-D-2

interface Vlan1

ip address 192.168.11.4 255.255.255.0

!

interface FastEthernet0/11

switchport access vlan 20

switchport mode access

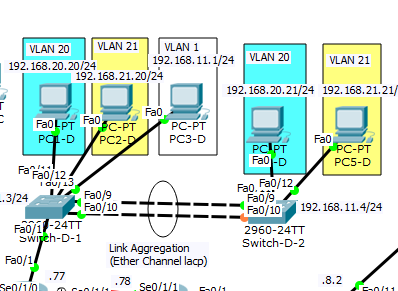
!

interface FastEthernet0/12

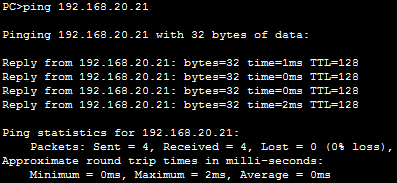
switchport access vlan 21

switchport mode access

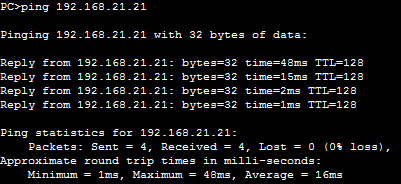
* 1. Verification



PC1-D ping PC4-D on vlan 20



PC2-D ping P52-D on vlan 21



* 1. Troubleshooting

To troubleshoot this, I would first ping from a PC to another PC in the same VLAN and if that didn’t work check the switch’s running-config to make sure all the interfaces connected to PC’s are in access mode, between switches and switches are in trunk mode, and between routers and switches are also in trunk mode. Then I’d check if the correct VLANs were applied to the right interfaces.

1. Named Extended ACLs
   1. How it works

Extended Access Control Lists are groups of commands that can deny or permit packets based on source/destination IP addresses, port numbers and upper-layer protocols. In this project, I utilized an extended ACL with the dynamic nat/pat where the extended ACL, PRIVATE-ADDRESSES-USED-FOR-NAT, which permits anything from the 192.168.0.0 or 172.16.0.0 addresses with wildcard mask 0.0.255.255 and anything else is denied, was bound to the public address pool PUBLIC-NAT-POOL. This extended ACL was used to define specific addresses that are allowed. The extended ACL, DMZ was also made which only permits tcp packets going to 200.1.1.6 where the port number being accessed is 80 (HTTP) or 443 (HTTPS). This was used in the DMZ configuration to add security to the HQ-HTTP-Server.

* 1. Configuration

HQ-Router-Main

ip access-list standard PRIVATE-ADDRESSES-USED-FOR-NAT

permit 192.168.0.0 0.0.255.255

permit 172.16.0.0 0.0.255.255

deny any

!

ip access-list extended DMZ

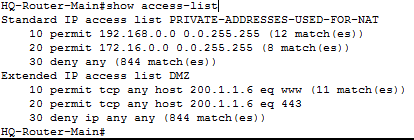
permit tcp any host 200.1.1.6 eq www

permit tcp any host 200.1.1.6 eq 443

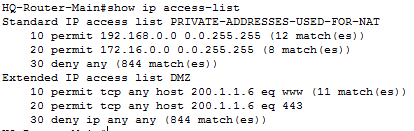
deny ip any any

* 1. Verification

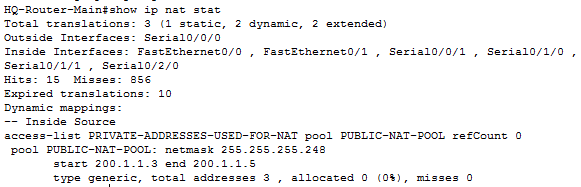
Show access-list



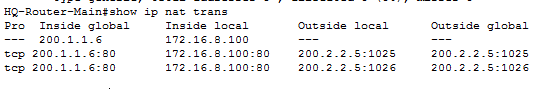
Show ip access-list



Show ip nat statistics



Show ip nat translations



* 1. Troubleshooting

To troubleshoot this, I would ping from a host that is permitted and then one that is denied and see how that goes. Then I would issue “show access-list” and “show ip access-list” to show me if there are any access-lists applied. Also, I’d check if the addresses being permitted are correct and the port number is correct as well.

1. PPP
   1. How it works

Point-to-Point Protocol is a layer 2 protocol used to establish direct connection between two nodes. It can provide connection authentication, authentication, transmission encryption, and compression.

* 1. Configuration

Router-D

interface Serial0/1/1

encapsulation ppp

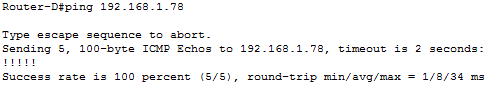
Router-E

interface Serial0/1/1

encapsulation ppp

* 1. Verification

Router-D and Router-E are directly connected and have full connectivity



* 1. Troubleshooting

To troubleshoot this, I would go into the router’s running-config to see if the interface connected to a router with PPP is in “encapsulation ppp” and if it’s not I would add it and test connectivity.

1. InterVLAN Routing (Router-on-a-stick)
   1. How it works

InterVLAN Routing is when VLANs are able to communicate with each other. One way to accomplish this is to do Router-on-a-stick which breaks down the default-gateway interface into sub interfaces for each vlan. In this project, I broke down the interface f0/1 on Router-D into the sub interfaces f0/1.1 for vlan 1, f0/1.20 for vlan 20, and f0/1.21 for vlan 21. Each one needs to be configured with encapsulation dot1q for the standard and they all must be in trunk mode as long as the f0/1 interface on Switch-D-1 which it connects to. This allows for communication between VLANs 1, 20, and 21.

* 1. Configuration

Router-D-1

interface FastEthernet0/1

no ip address

!

interface FastEthernet0/1.1

encapsulation dot1Q 1 native

ip address 192.168.11.1 255.255.255.0

!

interface FastEthernet0/1.20

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

!

interface FastEthernet0/1.21

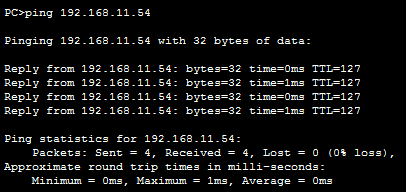
encapsulation dot1Q 21

ip address 192.168.21.1 255.255.255.0

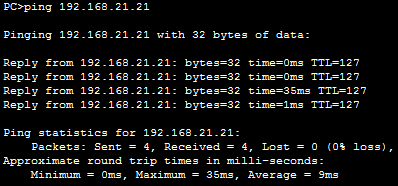
* 1. Verification

All VLANs can communicate

VLAN 21 to VLAN 1



VLAN 21 to VALN 20



* 1. Troubleshooting

1. Default Static Routing with route injection
   1. How it works

To route traffic to a non-connected host or network, you must use a default static route especially if you’re going from a private router to a public router like an ISP so the other networks aren’t shared, like in this project. In the HQ-ROUTER-MAIN, there is a default static route to the ISP router and one from the ISP to the HQ-ROUTER-MAIN. To reach any address on the ISP 0.0.0.0 is put in with a subnet mask of 0.0.0.0 and the next hop of 200.1.1.1 which is in the interface that connects the ISP router to the HQ router. However, other routers cannot recognize this path. In order to do so, in EIGRP, the “redistribute static” command injects that static route to be shared and on the other routers, it comes up as injected static and they can now connect to it as well.

* 1. Configuration

HQ-Router-Main

Ip route 0.0.0.0 0.0.0.0 200.1.1.1

!

Router eigrp 307

Redistribute static

ISP-Router

Ip route 0.0.0.0 0.0.0.0 200.1.1.2

* 1. Verification

Router-A



Router-B



Router-C



Router-D



Router-E



HQ-Router-BackUp



* 1. Troubleshooting

To troubleshoot this, I would first ping between PC’s on the same VLAN to see if it’s a bad connection and then ping between different VLANS. I would then check if the correct interfaces are access or trunk. Then I would go into the router’s running-config and check if the sub-interfaces are correctly allocated to each vlan and addressed properly.

**Challenges**

This was a fairly difficult project with multiple problems. Some of them include changing IP’s from the original design, using layer 3 switching, and packet tracer just flat out not working. Also, making sure the interfaces are not left off and finding the smallest typo, which results in nothing working and having to comb through every host and CLI command to find and fix. I didn’t know that much off the top of my head and had to constantly refer back to the notes and previous labs. Another problem encountered was setting up interVlan routing which just wouldn’t work for some reason, but after I deleted that whole section and put back in the same running-config as before it worked. What I might have done differently was add more VLANs to the headquarters site and add more redundancy like HSRP for the layer 3 switches.