Lab 4

NAT/PAT, Redistribution and Access-List

Summer 2014

[redacted]

Objectives

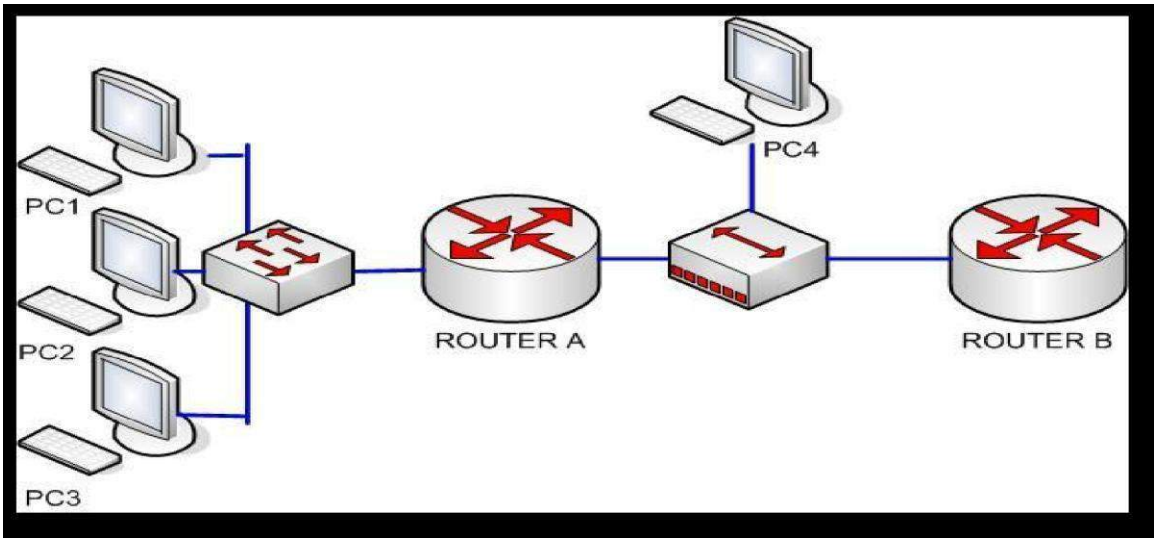
- Make use of different NAT variations in order to share scarce public IP addresses among multiple private IP users.

- Understand the use of redistribution as a way to communicate routing information between multiple routing protocols.

- Make use of basic and extended Access Lists to limit network reachability for specific IP nodes or IP services

- **This lab includes extra credits that could be used for your final grade!!! Valid only if you include them with all report questions**

NAT/PAT



Router A is your ASBR, PC1-3 are part of your company are using a private IP Range non-routable on the Internet; PC4 will be used to sniff the traffic flowing from your Internal Stations to the Router.

Your objective is to make use of different NAT/PAT configurations to connect to Router B in the following ways:

1. - Use static NAT to share 2 public IP addresses to provide for connectivity to router B to your internal PC's.
2. - Make use of Dynamic NAT to share 2 public IP addresses between your internal users.
3. - Make use of PAT to share only 1 public IP address between all your users.

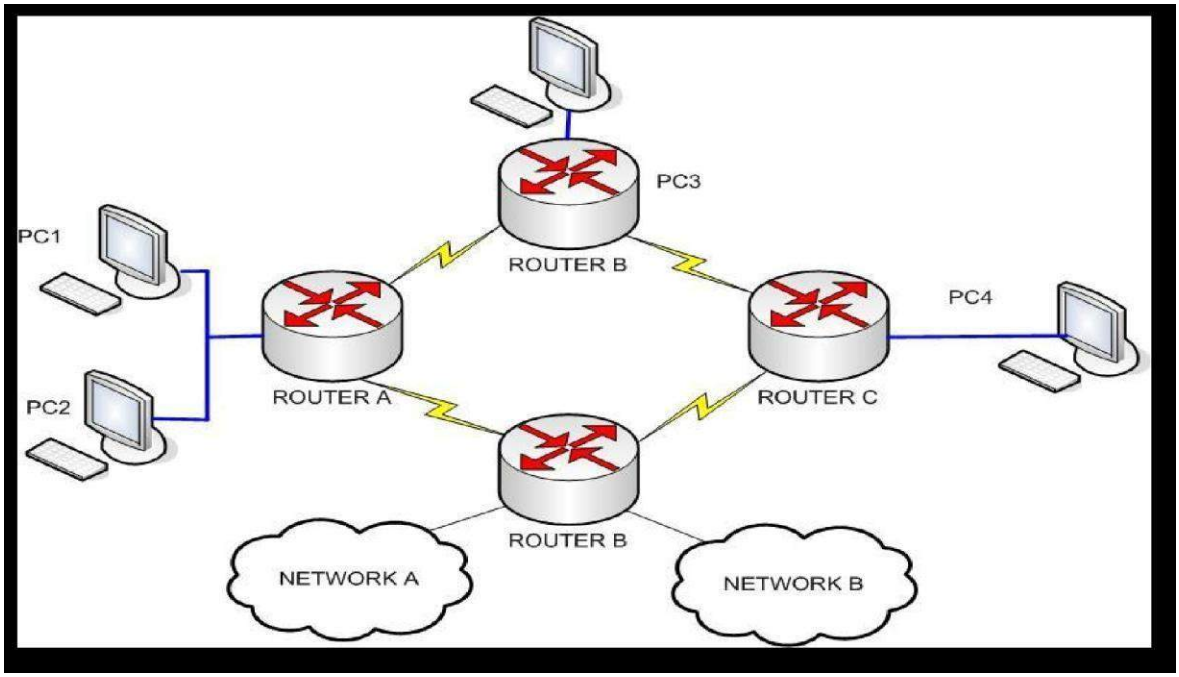
On your report include the following

- Router A's configuration for each scenario
- NAT translations for each scenario (at the router)
- NAT statistics for each scenario (at the router)
- Explain your NAT Translations captured by Ethereal (How do you differentiate between each telnet session to Router B?)
- Document the cases where NAT translations were not possible, and explain how you would solve them.

Use the following sequence to test your NAT/PAT configuration

1. Telnet from all internal PCs to Router B, and keep sessions open. Document your translations.
2. Open 2 additional Telnet sessions (to Router B) from PC1. Document your differences on your results for the translation of each telnet session to Router B.

Advanced NAT/PAT (optional: 3 points for Extra Credit)



CASE 1: 3 companies decide to merge their networks; the problem is that all of them had the same addressing 200.200.200.0 /29 on their Ethernet segments.

Make use of NAT/PAT commands of your preference to achieve end to end connectivity. Include in your report a copy of your NAT/PAT configuration on all routers plus explain the NAT process that a packet would follow while pinging from PC1 to PC4.

Consider the following for your design:

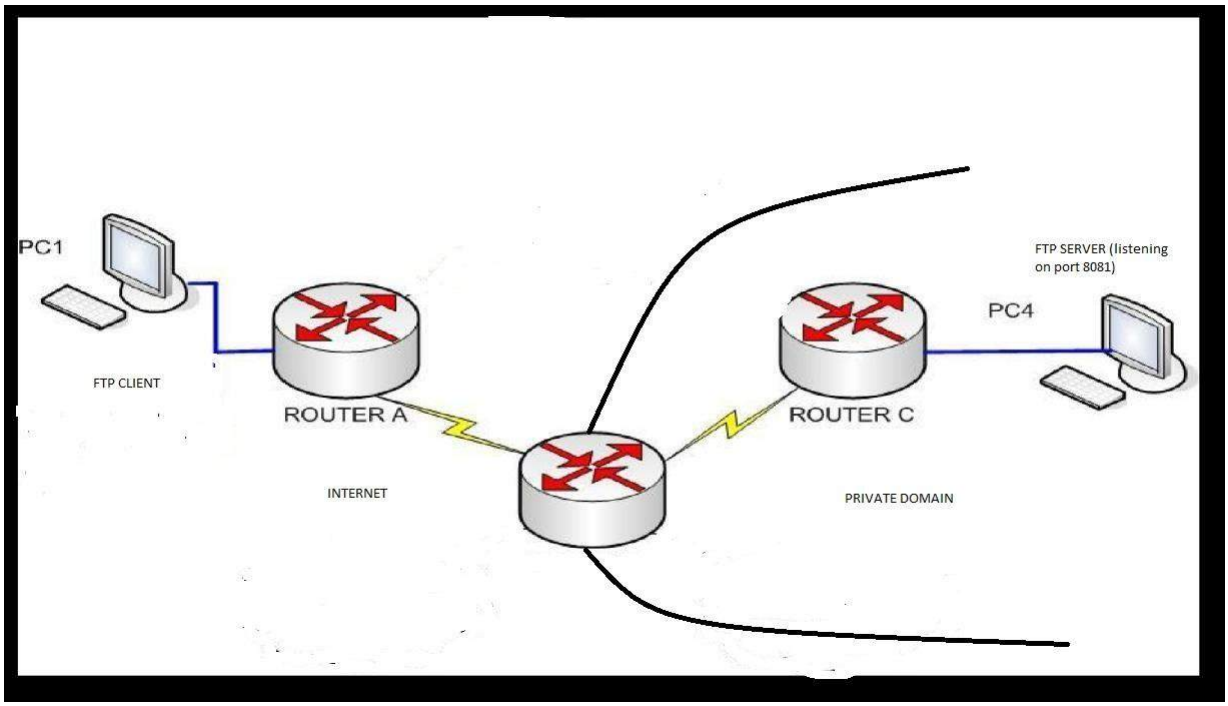
- You cannot change current IP subnetting on private networks
- Use the routing protocol of your preference
- Use an optimal class A subnet to cover all serial link addressing
- Ignore router B or networks A/B for the moment.

CASE 2: A year later these companies wanted to go online and they installed Router B (bottom) as their gateway to the internet. To make matters worse, none of these companies registered the address block 200.200.200.0/30 on ARIN before, and they just found out that the IP address 200.200.200.1/30 was registered by a new company: www.werecyclelint.com.

Be creative and solve the problem… without changing your internal subnets. All your users should be able to ping such public IP. Report your design considerations and findings.

Case 3 : Consider the diagram below. Establish NAT such that request coming from FTP client in the public domain are forwarded to the FTP server within the enterprise listening at port 8081.

Establish an active ftp connection and retrieve a file from ftp server.



Report Questions:

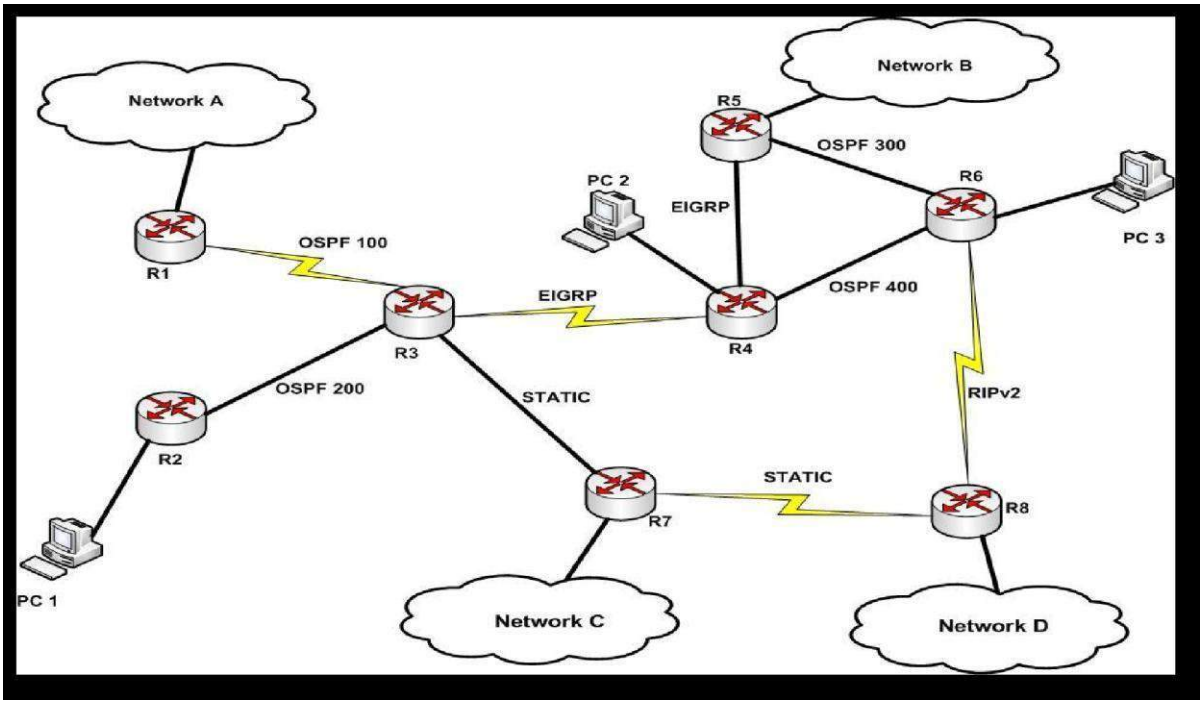
1) List the commands necessary to use PAT on Router A if we were to support more than 10 users from the private network, sharing only 2 IP address. Explain how this configuration would work if 3 computers access the network at the same time.

2) What will happen if PC3 opens multiple telnet windows to manage router A, is this possible? What would your NAT look like of you were to have only one public IP available? How will the mappings for each telnet window be handled by the 1:1 NAT? How do you differentiate between multiple windows of the same application, going to the same IP destination from the same IP source?

Redistribution

Select a different class C network address for each broadcast domain on your network

1) Use appropriate redistribution commands on each Router so you can achieve end to end / all-to-all connectivity. Report you router configurations and highlight the parameters you selected on each of the different redistribution points. Explain why you used them.



Report Question:

1) Write me a short story that explains in your own words about the use of administrative distance on the route selection process among multiple routing protocols; on what conditions would you change the default admin distance values; and how do you deal with the different metrics associated with each routing protocol when doing redistribution among different protocols. Give an example of each.

Access Lists

Make use of access lists so the following conditions are met:

- PC1 ping PC2 but cannot ping PC3
- PC1 can telnet to all routers with loopback except R8
- Network D is yahoo (221.22.2.22/32). All PCs can reach yahoo except PC2.
- R3 and R4 will not allow any incoming telnet requests
- (Remove ACL used for part1) PC1 should be able to ping PC3 and the path followed should be R2 – R3 – R4 …….
- The Ping between PC1 and PC3 should follow the path: R2 – R3 – R7 ……..

Report Question:

1. Assuming R8 is your gateway to the Internet; create an access list that will prevent any user from doing web browsing.

2. Create an access list that will not permit FTP transfers to the internet.

3. Create an access list that will permit ssh connections to your company form the IP subnet 100.100.100.0/24

4. To prevent denial of service attacks based on ping based utilities, create an access list that would protect this network from such attacks but still would allow you to ping the rest of the Internet. Explain where would you apply this rule, and how would it work.

Extra Credit (7 points)

- List and explain the Access list configuration commands necessary needed to permit VoIP calls into and from the Internet. Assume your company is using both SIP and H323 technologies. (Hint: don't forget about the audio streams). Assume R8 is still the gateway on the Internet and users still should meet all previous restrictions.

- Create an access list that will block napster, kazaa, skype and messenger from entering your company.

- Create an access list that will block adult content from entering your company.