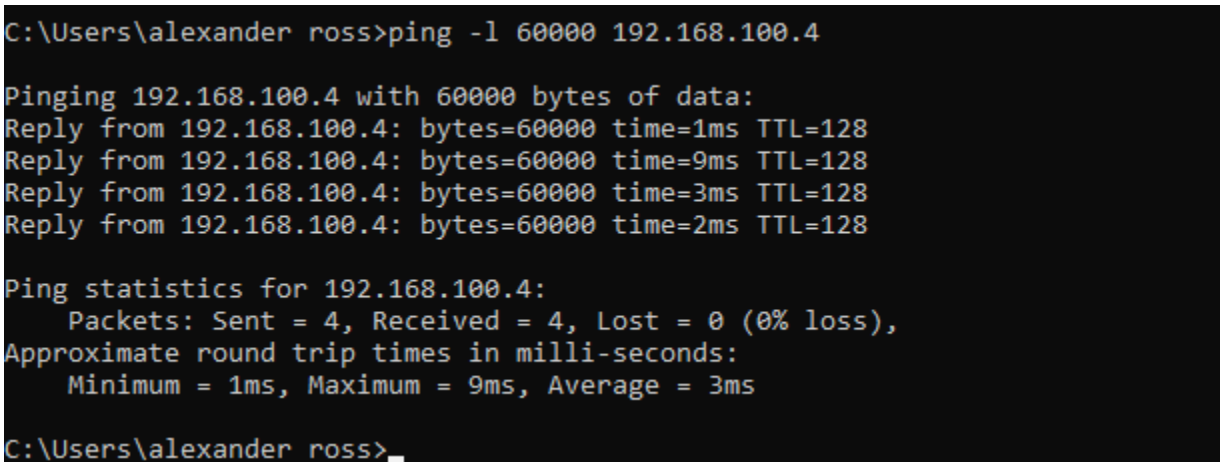
Lab 5:
Alexander Ross
300213662

Exercise 1:
3-2
Step 4:
Speed 1.0 Gbps
Variety: 1000BaseT cat 5 UTP

Ping reply: 1,9,3,2 ms
3-2 Step 5: Screenshot

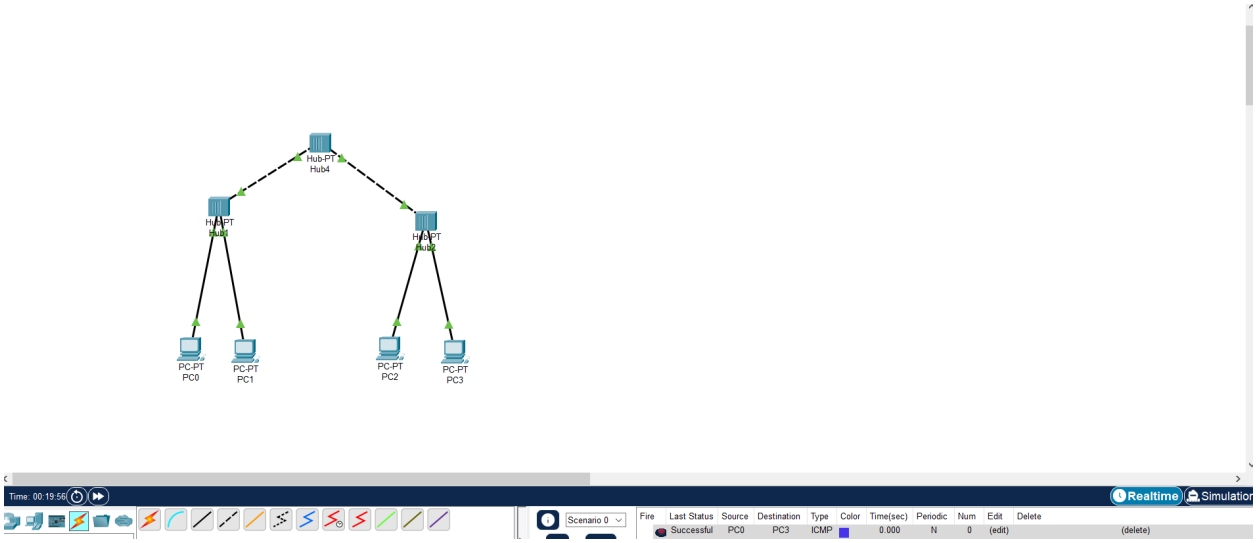


Step 8:
Speed: 5 mbps due to running at half speed due to collisions/acknowledgements
Variety: 10Base T

Step 9: Screenshot
Every Time i change my duplex my VM Crashes sorry :^)

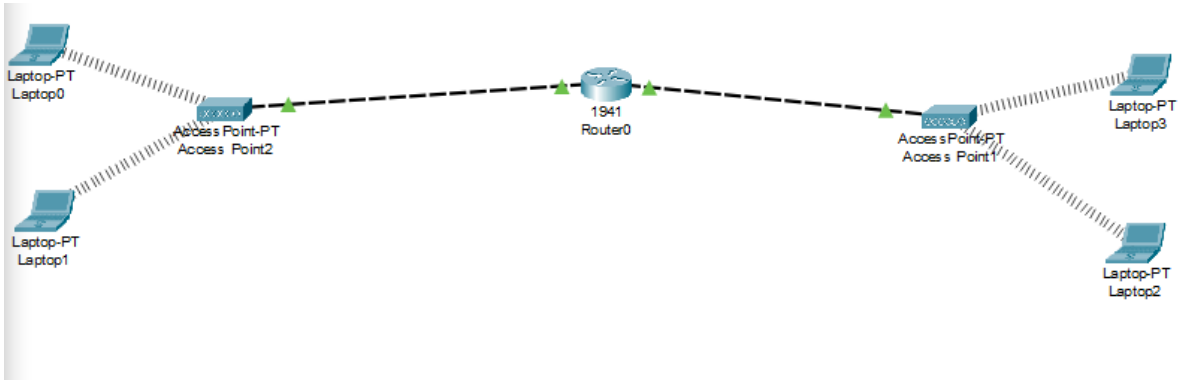
Step 9: Written
I imagine that the ms would jump to somewhere around 100ms for an average reply and that pings would become very slow as we would have to wait for a acknowledgement and would make our pings slow to a crawl

Exercise 2:Challenge lab 3-1
Screenshot



B: the computers are attached to a hub
C: The Device at the center of the star topology is a hub
D: There are 3 collision domains

Exercise 3: challenge lab 3-2



B: I connected the AP to a router because it allows the two networks to communicate with eachother and possibly the internet
C: We are using infrastructure wireless mode

D: adding wireless brings new access physical topology to the network such as router and wireless access points. For logical topology we have now created a network topology that is still an extended star topology

Case Project 3-1

I would upgrade the companies to use a Full Duplex transmission for its transferring to increase the speed of using multiple channels on the ethernet system that the company is using. The second would be to increase the transmission capacity of the ethernet hubs they are using from 10 mbps to 100 or even a gigabit system for easier transmission of files. Also to run the cables if we cannot use a step ladder, then the best solution would be to upgrade to WAN points would be a good option as not so many cables are required for running WAN's

For topology in the manufacturing areas, you could easily use multiple extended star topologies but one single gigabit switch would probably be the most useful on a maintenance + ease of install and cost.

Case Project 3-2
They should keep using a extended star network and the bus between floors for its ease of reconfiguration, ease of maintenance and security but it should be upgraded to the newest cat6, upgraded switches and routers for allowing the information to transport faster with more ease.

The network would be server based as it is a multi floor company with many computers exchanging information and would be more secure than a p2p based network

Two hundred and fifty five devices not including what could be added on later

Switch networking devices are easy to configure, in this project we would be using switches as they are very easy to modify, swap and repair/replace. Switches are made for access to a network between pairs of devices and would excel at offering the best access. To medium bandwidth between devices

Exercise 6: Research Wi-Fi Encryption Protocols

WEP:
Wired equivalent privacy uses a one of two keys key that are 64 bit or 128 bit and it uses the key to encrypt packets to the receiver. The CRC is calculated which appends to the plain text packet and will report any errors. A initialization vector is then randomly generated to create a random seed for the key generator which then creates a Key Stream which then has an XOR function that encrypts the plain text to create a cipher text. In order to decrypt the Cipher text, the receiver receives the initialization vector which then generates the seed for the key

generator and produces the same process in which we used to generate the cipher text in the beginning. The flaws that come with WEP is that computers have gotten much better at generating and monitoring the initialization vector and can generate the keys with such speed that the encryption protocol no longer is viable.

WPA:
WPA is much better than WEP because WPA uses TKIP(temporal key integrity protocol) which dynamically changes the key that the system uses. This stops hackers and sniffers from being able to create a key to match that of the uses. WPA also uses occasionally integrity checks to make sure that attackers have not captured or altered packets .

WPA2:
Is an improved version of the WPA programbut instead of using TKIP it uses CCMP which is an improved version of TKIP but is based on AES algorithms which are much stronger but using substitution of bytes , mixing columns and adding specific keys which make it very hard to break in terms of computational power. WPA2 is still vulnerable to hacking such as KRACK attacks but are much safer than WPA and WEP as most OS's have reduced their vulnerability to KRACK attacks

WPA3:
WPA3 is an even more improved version of WPA2 but uses 256 encryption rather than 128 bit and uses a much more secure, secure handshake on both devices. WPA3 also does not allow offline password guesses by users allowing only one password guess which makes brute force attacks on public wifi much harder to achieve.