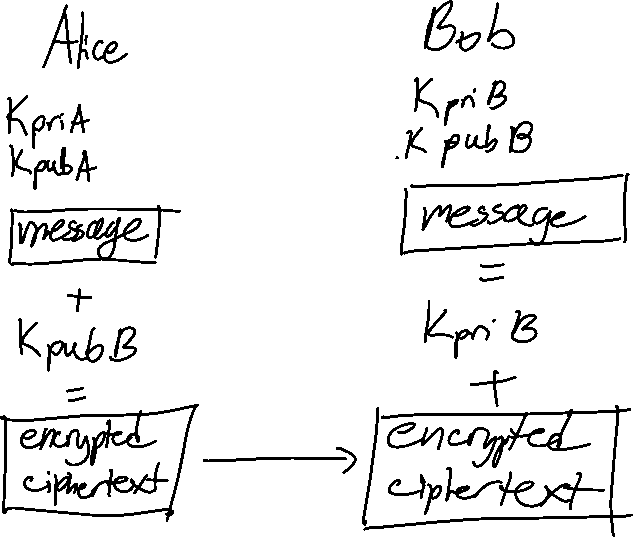
HW2

Part 1

1. Confidentiality refers to an adversary cannot find out who sent the message or to whom it will reach. Integrity refers to the adversary not being able to change the message without it having noticeable effect. You can have confidentiality without integrity by sending a message that when tampered with will just be lost and losing only integrity. You can have integrity without confidentiality by sending a cleartext message that will show signs if it is tampered with.
2. A non-forgeable, verifiable document requires that the signature require some near-impossible task that the other party can use a process to see if it is genuine. In the past, special inks and codes were used to protect documents, but now digital signatures are used. Digital signatures use a one-way hashing encryption algorithm that is near-impossible to forge and a low compute time, decryption algorithm that can be used to verify the message bits that matches the signature of the party sending it.
3. 1. No, without a public key that Alice can use to create her own signature she cannot send a message that can be verified by Bob with the hash function.



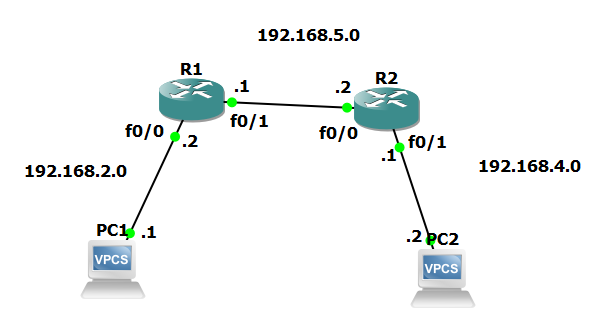
1. 1. You would need sequence numbers in order to send the correct NACK to the sender to make sure that particular data is sent again.
   2. The receiver would need a timer to make sure the sender didn’t send the data and the NACK needed to be sent again.
   3. The sender would send a packet of data to the receiver with a unique sequence number. The receiver would only send a NACK if it received a packet with an unexpected sequence number. The receiver would set a timer for the NACKs and resend when it times out. The NACK-only protocol would fail in flow control since the receiver never sends a message to the sender if it is overloaded.

S would send packet to AS 100 since it is the only link available. AS 100 would then run a check to see the shortest way to D using inter and intra domain algorithms, Distance Vector and Link State. AS 100 will see that the response time from AS 200 to interior router R4 is faster than routing iBGP through R2 and R3 and thus send the packet to AS 200 R5. AS 200 will use interdomain eBGP to send the packet back through AS 100 where the packet is received by gateway router R4. R4 will then send the packet to D.



Part 2







Panther ID is 002074252.

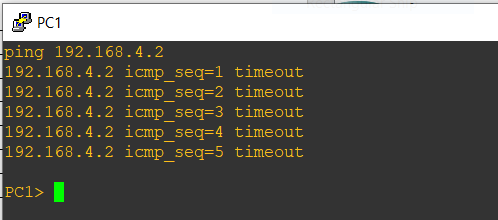
There are 3 subnets.

1 subnet between PC1 and R1.0, 192.168.2.0

1 subnet between R1.1 and R2.0, 192.168.5.0

1 subnet between PC2 and R2.1, 192.168.4.0 (used next number to avoid conflicts)

|  |  |  |
| --- | --- | --- |
| IP Address | MAC Address | Hostname |
| 192.168.2.1 | 00:50:79:66:68:00 | PC1 |
| 192.168.2.2 | c803.282c.0001 | R1.0 |
| 192.168.5.1 | c803.282c.0010 | R1.1 |
| 192.168.5.2 | c804.29dc.0001 | R2.0 |
| 192.168.4.1 | c804.29dc.0010 | R2.1 |
| 192.168.4.2 | 00:50:79:66:68:01 | PC2 |

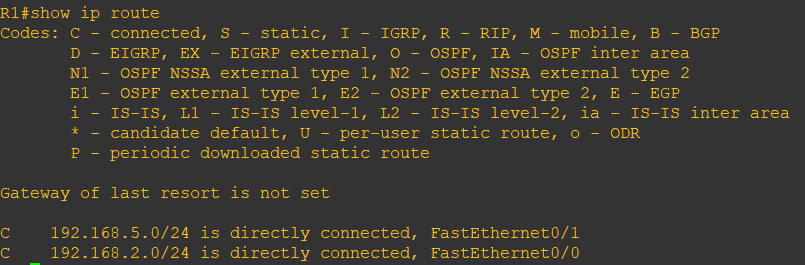


Our ping results in a timeout since while physically connected, there are no routes between PC1 and PC2 that can deliver the ICMP packet. We need to config the routers to route through the subnets.



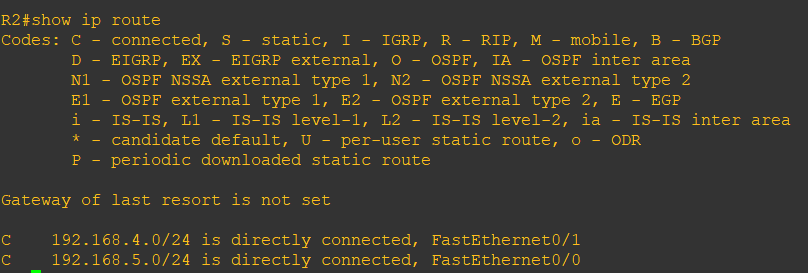
For R1:

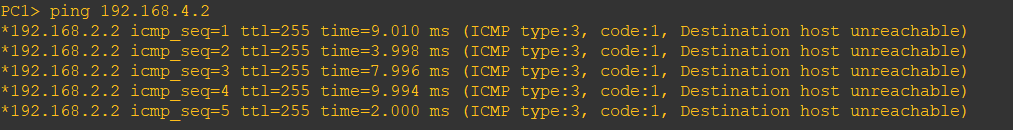




For R2:







Here we have configured the routes required to reach the destination ip address 192.168.4.2 (PC2). Destination host unreachable is expected behavior since that indicates to the ping that the destination host was found and is the end of route.