Alastair Van Maren and Matthew Getz

Q1: Because we have subnetted /24, and 192.168.x.x is not specific enough; it could be *any* of those networks.

Q2: 153.106.116.119 - We see this because we have statically assigned it to this computer.

Q3: Yes.

Q4: This rule rejects all attempted TCP connections via port 80.

Q5: No, neither computer can reach it. We cannot reach it because it is attempting to reach it on port 80, which we just built a rule to prevent from happening.

Q6: I had to block ports 22 and 23.

Q7: I added rules that said to accept incoming TCP connections on ports 80 and 22 from the IP of my Client LAN.

Q8: It is port 3389.

Q9: The process running on that port is svchost.exe (Network Service).

Q10: We can set up a port forward on any ports. The ports do not have to be the same on both sides.

Q11: This rule prevents connections from coming from the LAN computer.

Q12: I set up two rules one for UDP and one for TCP, each saying to accept and forward data coming from port 53 (the port DNS uses), and headed to the IP of the DNS server.

Q13: The addresses used are: 66.35.59.249 and 45.60.31.34.

Q14: I added four rules total, two each for the destination IPs listed above, with one of each pair being for HTTP on port 80 and HTTPS on port 443.