a

i) <http://192.168.1.1:80/>

ii) NAT (Network Address Translation)

iii) 3000. It is outside of the first 1024 ports (0-1023) so it wouldn't interfere with existing "well known" applications. And it is below 49151, which means that it is free for any user application to use and register.

iv) Firewalls that might be blocking this port.

b

R = L / (t2 – t1) = 2Mbps = 2000000 bps

L = 1GB = 8000000000 b

packetization = L / R = 4000 s

d = Δ - L / R = 182

distance = d \* c = 54600000000 m = 54600000 km

It takes light 182s to get to Mars, therefore 54600000 km.

c

Assuming lines beginning with # is replies from the other side, it appears that the protocol is similar to FTP, and is being used to transfer files.

The protocol dictates that the start of a connection is OHAI, and then a domain name is specified. Presumably, the IP address of the server is looked up through a DNS server.

The server responds with MKAY, indicating that the connection is successful.

The end-user then tells the example.edu to connect to its local port at 12345 if it sends files in the future, then requests a file.txt from the server. The server then connects to port 12345 and sends the requested file.

Finally, the closing handshake is initiated by the client via KTHXBAI, at which point the server responds by disconnecting.

d

Assuming the data is sent without null byte string termination and the protocol being used is Slow start. then it will be sent over in 3 steps.

Step # CWND Size (B) Congestion Protocol Data

1 1 SS A

2 2 SS BC

3 4 CA DEFG

The window size is increase by 2x at every transmission in SS mode, starting at MSS(=1B) and until 4B where the transmission ends.

* Step 2 is CA I think, therefore the next CWND size is 3, and one extra step. +1

**Would it not be**:

Step # CWND Size (B) Congestion Protocol Data

1 1 SS A

2 2 CA BC

3 3 CA DEF

4 4 CA G

e

(i) Allow

(ii) \*

(iii) Allow

(iv) 20, 21

(v) TCP

(vi) 25, 110

(vii) TCP

(viii) Enable POP3, SMTP mail access

(ix) Allow

(x) \*

(xi) 53

(xii) Deny

2

a

Initially:

RouterA = {(A,B,3),(A,C,4),(A,D,5), (A,E,10)}

RouterB = {(B,A,3),(B,C,5),(B,D,8),(B,E,7)}

RouterC = {(C,A,4),(C,B,5),(C,D,7), (C,E,12)}

RouterD = {(D,A,5),(D,B,8),(D,C,7),(D,E,9)}

RouterE = {(E, A, 10), (E,B,7),(E,C,12)(E,D,9)}

After RouterD down:

RouterA = {(A,B,3),(A,C,4),(A,D,11), (A,E,10)}

RouterB = {(B,A,3),(B,C,5),(B,D 8,),(B,E,7)}

RouterC = {(C,A,4),(C,B,5),(C,D,7), (C,E,13)}

RouterE = {(E, A, 10), (E,B,7),(E,C,12)nnnnn(E,D,15)}

b

*Fun fact: decrypting 72ea7aca using crc32 returns virus!*

localhost has a mail server listening on port 25.

The virus then sends TCP SYN requests from user ports on the same machine to connect to the mail server, and when the connection is established, simply goes into TIME\_WAIT, like a local version of a SYN flood attack.

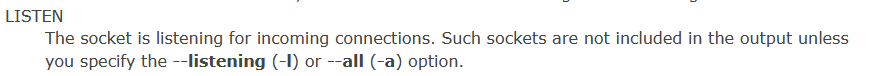
This is done presumably to deny legitimate services trying to connect to this mail server the ability to serve real customers, causing economic harm.

---

Another possible solution, not sure:

The virus setups up an SMTP mail server on the host. It then forks and creates multiple mail clients that connect to this mail server. This is probably to spam phishing/malicious emails to target/random email addresses via the public IP address of the hosts router. Essentially you abuse someone elses network to send out phishing emails probably eventually getting this IP marked as a bad one by other SMTP servers

The previous answer saying it connects to the mail server doesn’t make sense as the state is LISTENING. With the process being the virus exe meaning that process is itself listening on port 25 and its not connecting to some existing mail server on the host already





c

i) This is an ARP spoofing attack. The attacker is hoping to link their own MAC address with the address of the legitimate server on the network. In this case, they are hoping to redirect traffic from server0 to outside the network via Router0.

ii) Connect Server0 to Switch0 via an additional router (Router1).

iii) Replace Hub0 with another switch (switch1) so that wireless networks are separated.

d

i. They would need ethernet cables to connect everything together. Simple UTP Cat5 cables could serve the needs of the employees, but depending on the traffic on the servers, optical fibre might be needed to serve customers.

ii. They would need a wireless access point to allow employees to use mobile devices. Switches to separate the wireless access point from the rest of the network, and allow multiple desktops to connect to the network. A DHCP server to assign IP addresses to desktops and mobile devices (but not servers). And a router that allows a static public IP address to connect the network to the internet.

\

e

i)

1. BGP is not an intra-AS routing algorithm, it is inter-AS routing.

2. SHA is not an encryption method as the data cannot be decrypted by design, it is a hash function.

3. ACL (Access Control List) is a stateless way of packet filtering. It checks source and destination IP addresses and ports but not content of current or previous packets. <-- This is irrelevant (Should be stateless not statelike on line 2)

4. QUIC is implemented in 2012 and announced in 2013. Can't possibly have 10+ years of experience. So Maximum of 8 years experience (if google employee)

5. OSFP should be OSPF

ii)

1. The focus in intra-AS routing means that the employee needs to maintain infrastructure across different networks.

2. The firewall and ACL implies the job needs a security aspect. i.e. can identify and correctly block malicious traffic.

3. The data encryption aspect means that the employee needs to know how to handle sensitive data (e.g. passwords).

4. The experience in optimisation of TCP means that the employee needs to know how TCP congestion control works, and fix problems when congestion is detected.