ASSIGNMENT #1

COMP 535

Ivan Aslamov (260 228 181)
Simon Foucher (260 223 197)
Amin Mirzaee (260 209 556)

Part 1

1.1 EXPERIMENTAL QUESTIONS

3. RUN THE TCPDUMP ON HOST B. USE THE PING COMMAND TO COMMUNICATE (AN ECHO REQUEST AND REPLY SEQUENCE) BETWEEN HOST A AND HOST B. WHAT DO YOU OBSERVE IN THE TCPDUMP RUNNING ON HOST B?

Every second, we can observe an incoming ICMP echo request packet from Host A (192.168.0.6) to host B (192.168.0.7), where the tcpdump is captured. At the same time stamp, host B sends an ICMP echo reply to host A. This process is repeated as long as the ping sequence lasts.

5. THE GBUILDER WOULD HAVE ASSIGNED THE HOSTS IP ADDRESSES FROM A SUB NETWORK. IDENTIFY HE HOST AND NETWORK PARTS OF THE IP ADDRESSES.

IP address: 192.168.1.XXX
Subnet mask: 255.255.255.0
Network address: 192.168.1.0
Host IPs : 192.168.1.[1-254]

NOTE THE SIMPLE PROCEDURE USED BY GBUILDERFOR ADDRESS ASSIGNMENT. USING THE IFCONFIG COMMAND CHANGE THE IP ADDRESS OF A HOST SO THAT IT GETS A NEW ADDRESS FROM THE SAME NETWORK AS THE OTHER MACHINES. DOES THIS ADDRESS CHANGE DISRUPT THE CONNECTIVITY (I.E., ABILITY OF THE HOSTS TO REACH ONE NOTHER) WIHN THELAN? WHAT TYPE OF CONNECTIONS WOULD BE DISRUPTED BY THE ADDRESS CHANGE?

Changing host IP within the subnet's host IP range does not disrupt connectivity between computers connected via a Layer 2 device (i.e. Switch). To break connectivity, we need to mess with the network address, in which case, the hosts would need help of a Layer3 device (i.e. router) to communicate with one another by crossing networks.

6. AS IN THE ABOVE STEP CHANGE THE IP ADDRESS OF A HOST TO A VALUE OUTSIDE THE NETWORK USED BY OTHER HOSTS IN THE LAN. FOR EXAMPLE, IF 192.168.2/24 IS THE NETWORK ADDRESS OF THE LAN, CHANGE THE IP ADDRESS OF A HOST TO 192.168.3.12. CAN THE HOSTS CONNECT TO EACH OTHER (I.E., SEND AND RECEIVE PACKETS). IF NOT, WHAT HAPPENS TO THE SENDING AND RECEIVING? AN APPLICATION SUCH AS PING REQUIRES BOTH SEND AND RECEIVE CAPABILITIES. IF THE ADDRESS CHANGE BREAKS COMMUNICATION, WHICH ONE IS BROKEN: SEND, RECEIVE, OR BOTH?

Only the sending on Host A is down; host A can’t send the ICMP echo request because it cannot resolve Host B's MAC address by broadcasting an arp on the wire (Host B will not respond)

On the otherhand, if Host B somehow knew how to reach host A (if it had access to a routing table), it would potentially have the ability to respond to the pings. In this specific case, host A's ability to receive packets from host B is not down, but Host B can’t forward its packets to host A.

7. IF THE COMMUNICATION IS BROKEN, CAN IT BE RESTORED WITHOUT CHANGING THE IP ADDRESS BACK TO OLD VALUE?

Yes, we could change the subnet masks to include more hosts within a larger subnet.

In this particular example, to connect 192.168.2.x to 192.168.3.12, a subnet mask of /22 or less would suffice to reestablish connectivity.

8. CHANGE THE IP ADDRESS OF ONE OF THE HOSTS (E.G., HOST A) SUCH IT IS SAME AS ONE OF THE OTHER HOSTS. SUPPOSE HOST A AND HOST B HAVE SAME IP ADDRESSES, TRY TO REACH ONE OF THEM FROM HOST C. CAN YOU REACH (I.E., A PING SUCCEED)? IF IT SUCCEEDS, WHICH HOST DID YOU REACH?

Running tcpdump on both Host A and Host B, we can observe the reception of an arp "who has IP" request, and both hosts responded with their MACs. Host A responded first, followed a few milliseconds later by host B. After the arp check, only host B began responding to the pings. It seems that Host C's MAC table got updates twice; the first time by Host A's arp response, quickly followed by Host B's MAC address overwriting the table. A confirmation of this fact is given by running arp -a on host C and observing host B's MAC address on its lookup table.

9. SUPPOSE HOST C WAS REACHING HOST A IN THE ABOVE STEP. CAN FORCE HOST C TO CONNECT TO HOST B?

Yes, we can manually assign static values in host C's arp table by running:

$ arp -s [targer IP] [targt MAC]

Running ping afterwards will reach the targeted MAC.

Note: entering a MAC address not existing on the LAN will make both hosts sharing the same IP receive the ping.

1.2 REVIEW QUESTIONS

1. WHAT IS THE PACKET ROUTING PROCESS IN A SINGLE IP LAN? SKETCH IT WITH ALL THE DETAILS. WHAT IS THE FUNCTION OF THE ADDRESS RESOLUTION PROTOCOL (ARP)?

Steps in Layer 3 routing:

1. Look at packet's target IP and try to match it with an entry on arp routing table. If there is a match, go to step 4.
2. If there is no match, broadcast an arp "who has IP [x] tell IP [me]" to the entire LAN using the LAN's broadcast IP address and wait for a response.
    a. Once/if a response arrives, update IP Routing table.
    b. If no response, drop the packet
3. Repeat step 1
4. Forward the packet on the router's interface according to routing table.

2. WHAT ROLE DOES THE SWITCH PLAY IN ROUTING PACKETS?

The switch forward Layer 2 frames within a LAN, using MAC addresses as targets. One great advantage that a switch has over a hub is that it places every hosts connected to it within its own collision domain, which allows data flow in full duplex mode.

A switch cannot route to devices based on Layer 3 IP addresses. Typically, a switch will build a MAC routing table dynamically by associating the source MAC of incoming frames to the Ethernet port which received that frame. If the destination MAC does not yet appear on the switch's MAC table, the switch will flood the frame on all of its Ethernet ports except the one on which the frame arrived with the broadcast MAC ff:ff:ff:ff:ff:ff:ff:ff. In upper communication protocols, the target unknown host should reply eventually to the frame, at which point the switch will record its MAC.

3. COMPARE HUB MODE VERSUS BRIDGE MODE IN THE SWITCH. YOU CAN TOGGLE BETWEEN THE TWO MODES IN THE PROPERTIES MENU OF THE SWITCH. WHAT ARE THE SECURITY IMPLICATIONS OF HUB MODE? DOES THE BRIDGE SETTING OF THE SWITCH FIX ALL THESE ISSUES?

The main security issues in a hub is that it is only a wire tap and does not perform any kinds of forwarding algorithm on packet; it simply broadcasts received packets on all of its interfaces. A switch actually knows who is where and does intelligent packet forwarding. It can be used as a barrier between hosts to filter communications.

4. WHAT IS THE STRUCTURE OF A MAC ADDRESS?

The first 3 bytes are OUI (Organizationally Unique Identifier) bytes and give information on the hardware Manufacturer.

In this OUI, the 7th bit from the front is set to 0 for uncast address and to 1 for multicast addresses. The 8th bit is set to 0 for globally unique MAC addresses, and set to 1 for locally administered MAC addresses (administered by the OUI).

The last 3 bytes are NIC (Network interface Controller) Specific bytes. They are used a unique identifier for the specific device and offer share a lot of commonality with the PCB's serial number.

4.1 CAN MAC ADDRESSES HAVE DUPLICATES?

Theoretically, as long as they are not on the same LAN, 2 devices *could* have the same address and function normally. But in practice, organizations do not assign the same MAC twice to 2 devices, such that every device it produces has a unique NIC filed. And since every organization has its own unique OUI, there *should not* be any 2 devices sharing a MAC out in the world.

5. HOW SHOULD WE ASSIGN IP ADDRESSES TO MACHINES ON A LAN? WHAT ARE THE CONSTRAINTS IF THE LAN IS WORKING IN ISOLATION (NOT CONNECTED TO THE INTERNET)?

The most popular was to assign IP addresses on a LAN is by using a DHCP server that handles any request from newly connected machines. It would also be possible to manually configure IPs on hosts, but it would take some time to configure and wouldn't be a flexible system.

As far as choosing an IP for a host, they can be any 32 bit number as long as:

- There are no duplicates within a LAN
- Every host on a LAN share the same network address and subnet mask.
- The first IP address on the LAN's host IP range is reserved (for network address)
- The last IP address on the LAN's host IP range is reserved (for LAN broadcast address)
- Even though the machines are not yes connected to the internet, it might be good practice to restrain the IP within the range of the reserved IPs of the network class. Not essential, but would save a whole lot of headaches if we are enable WAN connection in the future

Part 2

2.1 EXPERIMENTAL QUESTIONS

4. THE GBUILDER WOULD HAVE ASSIGNED THE HOSTS IP ADDRESSES FROM SUB NETWORKS. IDENTIFY THE HOST AND NETWORK PARTS OF THE IP ADDRESSES.

The default subnet Mask given by GINI is 255.255.255.0, so whenever assigning IPs, the network part of the IP is the first 3 numbers and the host part of the IP is the last number.

IP address: 192.168.1.XXX
Subnet mask: 255.255.255.0
Network address: 192.168.1.0
Host IPs : 192.168.1.[1-254]

HOW ARE THE SUB NETWORKS CHOSEN BY THE GBUILDER TO HANDLE MULTIPLE LANS?

gBiulder assigns the first available Class C reserved IP to subnets (pooled sequentially from 192.168.0.0 – 192.168.255.255), using the standard class C subnet mask 255.255.255.0.

USING THE IFCONFIG COMMAND CHANGE THE IP ADDRESS OF A HOST SO THAT IT GETS A NEW ADDRESS FROM THE SAME NETWORK AS THE OTHER MACHINES IN ITS LAN. DOES THIS ADDRESS CHANGE DISRUPT THE CONNECTIVITY (I.E., ABILITY OF THE HOSTS TO REACH ONE ANOTHER) WITH OTHER MACHINES? WHAT TYPE OF CONNECTIONS WOULD BE DISRUPTED BY THE ADDRESS CHANGE?

As long as the new IP is within the same LAN, changing it should only generate a new ARP query when engaging communication, but not damage communication.

5. AS IN THE ABOVE STEP CHANGE THE IP ADDRESS OF A HOST TO A VALUE OUTSIDE THE NETWORK USED BY OTHER HOSTS IN THE LAN. FOR EXAMPLE, IF 192.168.2/24 IS THE NETWORK ADDRESS OF A LAN, CHANGE THE IP ADDRESS OF THE HOST TO 192.168.3.12. CAN THE HOSTS CONNECT TO EACH OTHER (I.E., SEND AND RECEIVE PACKETS). IF NOT, WHAT HAPPENS TO THE SENDING AND RECEIVING. AN APPLICATION SUCH AS PING REQUIRES BOTH SEND AND RECEIVE CAPABILITIES. IF THE ADDRESS CHANGE BREAKS COMMUNICATION, WHICH ONE IS BROKEN: SEND, RECEIVE, OR BOTH?

Hosts cannot connect to each other even from within the same LAN.

The attached router doesn't receive any packages since the switch connecting it to the hosts doesn't let them go through. Thus send and receive is broken.

6. IF THE COMMUNICATION IS BROKEN, CAN IT BE RESTORED WITHOUT CHANGING THE IP ADDRESS BACK TO OLD VALUE? THERE MAY BE MULTIPLE WAYS OF RESTORING THE COMMUNICATION. DESCRIBE THE POSSIBLE ONES.

Yes, we can fix it by changing subnet mask to accommodate wider range of IP addresses.

7. CHANGE THE IP ADDRESS OF ONE OF THE HOSTS IN A LAN SUCH IT IS SAME AS ONE OF THE OTHER HOSTS IN THE LAN. HOW IS THE REACHABILITY AFFECTED? DOES IT AFFECT OUTWARD AND INWARD CONNECTIVITY, OR BOTH? HOW CAN YOU FIX THIS PROBLEM? YOUR SOLUTION MAY NOT WORK IN GINI DUE TO A LIMITATION OF THE GROUTER.

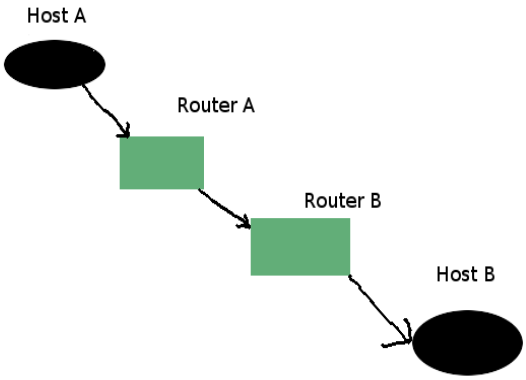
The Host with changed IP address cannot neither receive nor send packets. Host with original IP can only send packets but not receive.

With the same command from Part 1 we can still fix it if we know MAC addresses of computers we need to reach. But we can reach only one computer at a time.

$ arp -s [targer IP] [targt MAC]

2.2 REVIEW QUESTIONS

1. WHAT IS THE PACKET ROUTING PROCESS IN A MULTIPLE LAN IP NETWORK? SKETCH IT WITH ALL THE DETAILS. HOW DOES THE ADDRESS RESOLUTION PROCESS AND ROUTING PROCESS INTEROPERATE TO MAINTAIN COMMUNICATION BETWEEN TWO STATIONS ON DIFFERENT LANS?



Sending host A – asks router A for his MAC address through arp if it is not already present on its arp table.

Host A encapsulates packet into a frame with router A's MAC address and sends it to router A.

Router A receives frame and extract the packet from it the checks destination IP address. By using its routing table it will get MAC address of the next hop router, encapsulates the packet into a frame and send it to the next hop's MAC (assuming full Ethernet connected path), and so on, until packet reaches Router B where Host B is attached to.

Router B then will finally encapsulate it in a frame with MAC address of the Host B and get send to its destination.

2. THE IP NETWORK ROUTE LOOKUP PROCESS PERFORMS A "LONGEST PREFIX" MATCHING TO CHOOSE THE ROUTE. DOES THIS MECHANISM ALLOW REDUNDANT ROUTES? WHAT ARE THE ADVANTAGES OF USING THE LONGEST PREFIX MATCHING SCHEME? WHAT ARE THE DISADVANTAGES?

Yes it allows some redundancy since 2 paths could potentially be pointing to the same place.

Advantages is that with longest prefix matching, the router forwards the packet as 'deeply' as it can towards its destination, in an effort to skip redundant links.

The disadvantage is that the IP address in the packet's header doesn't explicitly carry a subnet mask, therefore the router could be forwarding the packet towards the wrong subnet.

3. DO A TRACEROUTE FROM ONE STATION TO ANOTHER STATION ON ANOTHER LAN. GIVE A HIGH-LEVEL TRACE OF THE PACKETS THAT WERE GENERATED DUE TO THIS OPERATION. INCLUDE THE ARP PACKETS, IF THERE ARE ANY, IN THE DISCUSSION.

As seen in WireShark:

295 0.000000 fe:fd:02:00:00:01 Broadcast ARP Who has 192.168.1.3? Tell 192.168.1.2

296 0.000000 fe:fd:02:00:00:01 Broadcast ARP Who has 192.168.1.128? Tell 192.168.1.2

297 0.000000 fe:fd:03:01:00:03 fe:fd:02:00:00:01 ARP 192.168.1.128 is at fe:fd:03:01:00:03

host checks to which router in belongs to, router responds with its MAC address

299 0.000000 192.168.1.128 192.168.1.2 ICMP Time-to-live exceeded (Time to live exceeded in transit)

host sends packet that gets killed by router, and ICMP message gets sended to the host with ip of the router which kills it.

306 0.000000 192.168.4.129 192.168.1.2 ICMP Time-to-live exceeded (Time to live exceeded in transit)

second router shows himself.

Redundant packages were avoided, for simplicity.

4. DO AN SSH CONNECTION FROM ONE STATION TO ANOTHER STATION. GIVE A HIGH-LEVEL TRACE OF THE PACKETS THAT WERE GENERATED DUE TO THIS OPERATION. DO NOT INCLUDE ANY ARP PACKETS IN THIS DISCUSSION. IS THIS ANY DIFFERENT FROM THE SINGLE LAN IP NETWORK? EXPLAIN YOUR FINDINGS.

As seen in WireShark

267 0.000000 192.168.1.2 192.168.5.4 SSHv2 Encrypted request packet len=48

105 0.000000 192.168.5.4 192.168.1.2 SSH Server Protocol: SSH-2.0-OpenSSH_5.0

client tells router which SSH he wants to use.

108 0.000000 192.168.1.2 192.168.5.4 SSH Client Protocol: SSH-2.0-OpenSSH_5.0

server response

113 0.000000 192.168.1.2 192.168.5.4 SSHv2 Client: Key Exchange Init

114 0.000000 192.168.5.4 192.168.1.2 SSHv2 Server: Key Exchange Init

key protocol handshaking

121 0.000000 192.168.1.2 192.168.5.4 SSHv2 Client: Diffie-Hellman GEX Request

key exchange

267 0.000000 192.168.1.2 192.168.5.4 SSHv2 Encrypted request packet len=48

encrypted messages

.....

283 0.000000 192.168.1.2 192.168.5.4 TCP 39210 > ssh [FIN, ACK] Seq=2069 Ack=2493 Win=8976 Len=0 TSV=4294956832 TSER=42949567

close message

285 0.000000 192.168.5.4 192.168.1.2 TCP ssh > 39210 [FIN, ACK] Seq=2493 Ack=2070 Win=8960 Len=0 TSV=4294956785 TSER=4294956832

close message acknowledgement

There should not be any difference. We could not see any package exchange when ssh session gets initiated between 2 computers on the same LAN.