CS456 Lab Report

Student 1: Ahmed Farra (a2farra)
Student 2: Boris Kravchenko (bkravche)

Lab 3 Static Routing

1(A)
What is the output on PC1 when the ping commands are issued?

```
[root@PC1 ~]# ping -c 5 10.0.1.21
PING 10.0.1.21 (10.0.1.21) 56(84) bytes of data.
64 bytes from 10.0.1.21: icmp_req=1 ttl=64 time=1.18 ms
64 bytes from 10.0.1.21: icmp_req=2 ttl=64 time=0.491 ms
64 bytes from 10.0.1.21: icmp_req=3 ttl=64 time=0.499 ms
64 bytes from 10.0.1.21: icmp_req=4 ttl=64 time=0.518 ms
64 bytes from 10.0.1.21: icmp_req=5 ttl=64 time=0.490 ms

--- 10.0.1.21 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.490/0.636/1.186/0.276 ms
[root@PC1 ~]# ping -c 5 10.0.2.1
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
From 10.0.1.11 icmp_seq=2 Destination Host Unreachable
From 10.0.1.11 icmp_seq=3 Destination Host Unreachable
From 10.0.1.11 icmp_seq=4 Destination Host Unreachable
From 10.0.1.11 icmp_seq=5 Destination Host Unreachable

--- 10.0.2.1 ping statistics ---
5 packets transmitted, 0 received, +4 errors, 100% packet loss, time 4000ms
pipe 3
[root@PC1 ~]# ping -c 5 10.0.3.41
PING 10.0.3.41 (10.0.3.41) 56(84) bytes of data.
From 10.0.1.11 icmp_seq=2 Destination Host Unreachable
From 10.0.1.11 icmp_seq=3 Destination Host Unreachable
From 10.0.1.11 icmp_seq=4 Destination Host Unreachable
From 10.0.1.11 icmp_seq=5 Destination Host Unreachable

--- 10.0.3.41 ping statistics ---
5 packets transmitted, 0 received, +4 errors, 100% packet loss, time 4001ms
pipe 3
```

Which packets, if any, are captured by Wireshark?

For all the ping commands it captures the packets. When pinging PC2 there are 10 ICMP echo packets captured (for each request and reply), and 14 ARP packets are captured for the unreachable IP addresses (PC4 and Router) as the network interface of PC1 tries to find the MAC address of the machines for the requested IPs but is unable to get them as there's no route.

Do you observe any ARP or ICMP packets? If so, what do they indicate?

Yes, we observe both. The ARP messages occur when we try pinging destinations that are not routed, which in this case are the router and PC4. It indicates that the network interface is trying to resolve the MAC addresses for the machines, but the machines are unreachable. The ICMP packets occur when we successfully ping PC2, and they indicate the request and reply packets. (We can see that the “type” of the ARP packets is “TELL” whereas the ICMP ones are “REQUESTS” and “REPLIES”)

Which destinations are not reachable? Explain.

The router destination is not reachable (10.0.2.1) and PC4 is unreachable (10.0.3.41). This is because there is no route to those hosts.

1(C)
Include the saved output of the routing table. Explain the entries in the routing table and discuss the values of the fields for each entry.

```
[root@PC1 ~]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.1.0        0.0.0.0         255.255.255.0   U         0 0          0 p1p1
10.0.2.0        10.0.1.21       255.255.255.0   UG        0 0          0 p1p1
10.0.3.0        10.0.1.21       255.255.255.0   UG        0 0          0 p1p1
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 em1
```

PC1 is routed to 10.0.2.0 and 10.0.3.0 through 10.0.1.21 (interface in the hub 10.0.1.0) Default gateways are 10.0.1.0 and 192.168.1.0

```
[root@PC2 ~]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.1.0        0.0.0.0         255.255.255.0   U         0   0          0 p1p1
10.0.2.0        0.0.0.0         255.255.255.0   U        0    0          0 p1p2
10.0.3.0        10.0.2.1        255.255.255.0   UG      0    0          0 p1p2
192.168.1.0     0.0.0.0         255.255.255.0   U       0    0          0 em1
```

PC2 is routed to 10.0.3.0 through 10.0.2.1 (interface in Router 1) Default gateways are 10.0.1.0, 10.0.2.0 and 192.168.1.0

```
[root@PC4 ~]# netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
10.0.1.0        10.0.3.1        255.255.255.0   UG       0    0          0 p1p1
10.0.2.0        10.0.3.1        255.255.255.0   UG       0    0          0 p1p1
10.0.3.0        0.0.0.0         255.255.255.0   U        0    0          0 p1p1
192.168.1.0     0.0.0.0         255.255.255.0   U        0    0          0 em1
```

PC4 is routed to 10.0.1.0 and 10.0.2.0 through 10.0.3.1 (interface in Router 1) Default gateways are 10.0.3.0 and 192.168.1.0

2(C)
Analyze the output to ensure you have configured the router correctly.

From the output:

```
GigabitEthernet0/0 is up, line protocol is up
    Hardware is CN Gigabit Ethernet, address is d48c.b58a.33a0 (bia
d48c.b58a.33a)
  Internet address is 10.0.2.1/24

GigabitEthernet0/1 is up, line protocol is up
    Hardware is CN Gigabit Ethernet, address is d48c.b58a.33a1 (bia
d48c.b58a.33a)
  Internet address is 10.0.3.1/24

interface GigabitEthernet0/0
 ip address 10.0.2.1 255.255.255.0
 duplex auto
 speed auto
```

```
interface GigabitEthernet0/1
 ip address 10.0.3.1 255.255.255.0
 duplex auto
 speed auto
```

The following parts of the output suggest that the interfaces in the router were configured as required in lab specification.

3(B)

Use the Wireshark output and the previously saved routing table to explain the operation of traceroute.

PC1 sent multiple UDP packets to 10.0.3.41 (PC4) with TTL1
As the TTL expired at the next hop, an ICMP packet was sent back with “Time-to-live exceeded” message.
PC1 sent multiple UDP packets to 10.0.3.41 (PC4) again, with TTL2
This process continued until the whole route is traced

3(C)

Determine the source and destination address in the Wireshark and IP headers for the ICMP Echo Request messages that were captured at PC1

Source: "10.0.1.11”, Destination: “10.0.3.41”

Determine the source and destination address in the Wireshark and IP headers for the ICMP Echo Request messages that were captured at PC4

The ARP packets suggest the following results:
Source: “d4:8c:b5:8a:33:a1", Destination: “IntelCor_8b:bc:20”

Use your previous answers to explain how the source and destination Ethernet and IP address are changed when a datagram is forwarded by a router.

In our scenario, the IP addresses were not changed in the ICMP packets, but since the ICMP protocol is part of the Link layer, the source/destination could possibly change to mac addresses.

3(E)
What is the output on PC1 when the ping command is issued?

```
[root@PC1 ~]# ping -c 5 10.0.10.110
PING 10.0.10.110 (10.0.10.110) 56(84) bytes of data.
From 10.0.2.1 icmp_seq=1 Destination Host Unreachable
From 10.0.2.1 icmp_seq=2 Destination Host Unreachable
From 10.0.2.1 icmp_seq=3 Destination Host Unreachable
From 10.0.2.1 icmp_seq=4 Destination Host Unreachable
From 10.0.2.1 icmp_seq=5 Destination Host Unreachable
```

Determine how far the ICMP Echo Request message travels?

ICMP echo travels to 10.0.2.1 (the router), which then replies with destination unreachable

Which, if any, ICMP Echo Reply message returns to PC1?

No replies reach PC1, since host doesn't exist

Lab 7 DHCP

2(C)
Explain the entries in the lease file dhcpd.leases. How is the content of the lease file used when a DHCP client connot contact the DHCP server?

The dhcpd.leases file stores a database of the IP addresses that have been assigned, and to whom these addresses have been assigned.
From the Linux Manual Page: “DHCP Server keeps a persistent database of leases that it has assigned. This database is a free-form ASCII file containing a series of lease declarations. Every time a lease is acquired, renewed or released, its new value is recorded at the end of the lease file. So if more than one declaration appears for a given lease, the last one in the file is the current one.”
(http://manpages.ubuntu.com/manpages/intrepid/man5/dhcpd.leases.5.html)

Our dhcpd.leases file (with explanation for each line):
lease 10.0.1.2 { – *Each lease declaration includes the single IP address that has been leased to the client. The statements within the braces define the duration of the lease and to whom it is assigned.*
  starts 4 2013/03/14 20:54:42; – *the start time of this lease*

ends 4 2013/03/14 21:04:42; – *the end time (expiry) of the lease*
cltt 4 2013/03/14 20:54:42; – *the client’s last transaction time*
binding state active; – *Specified when the failover protocol is not configured.*
next binding state free; – *specified what the lease’s current state will move to upon expiry (ends)*
rewind binding state free;
hardware ethernet 00:1b:21:8b:bb:80; – *the MAC address of the network interface on which the lease will be used*
}

Once half the time the lease has been granted for elapses, the DHCP client starts to contact the DHCP server by sending a unicast DHCPREQUEST to it in order to renew its lease. If it cannot reach it, it can continue to hold on to that IP Address until the expiry date specified. If it still cannot reach it for a long time, it will try contacting all DHCP servers by broadcasting the DHCPREQUEST instead of unicasting it, in hope that some DHCP server would be available and able to renew its lease. For this to work though, that server must have accurate information about that lease that was made earlier. That’s why the contents of this dhcpd.lease file are useful; so that the server can use it to know how to make that rebinding. Otherwise, if the lease isn’t there (or expires), the client will have to stop using that IP address and restart the entire DHCP process from scratch (DHCPDISCOVER) in order to get a new IP address. This will cause any connections the client has to break.

In most client-server applications, the port number of a server is a well-know number, while the client uses a currently available port number. However, DHCP uses both well-know port for client (UDP 68) and server (UDP 67). Explain why.

This is mainly because the nature of DHCP communication is that it is connectionless. Unlike TCP, in UDP the sender does not connect directly with the receiver, instead it just sends the packets in hopes that the computers in between will get the packet to its destination. For this reason, it is imperative that both ports are defined and well known, since there’s no mechanism like TCP where a connection is establish, through which the client tells its server of the port to use. That’s why port UDP 68 was specified by IANA to be the well-known port for the client.