Exercise 9 - Network Lab

IP configuration and ARP

- Configure network at runtime:
  - /sbin/ifconfig
  - /sbin/route
- Configure network persistently
  - /etc/sysconfig/network-scripts/ifcfg-eth*
  - /etc/sysconfig/network
  - /etc/resolv.conf
  - /etc/hosts
- Ping your default gw
- Open wireshark
- Ping the pc in the other network while wireshark is sniffing
- Check your arp cache
- Ping the pc in the other network
- Check your arp cache
- What do you notice?
- Change your default gw to 10.0.X.233
- Ping the pc in the other network
- What do you notice?
- Set your arp table in order to resolve the ip address 10.0.X.233 to the MAC address of 10.0.X.1
- Ping the pc in the other network
- What do you notice? Why?
- Reset your network configuration to the default one
  - /sbin/service network restart

Questions:

- What is an HOST?
- What is an IP address?
- What is a MAC address?
- What is the difference between a L2 SWITCH and an HUB?
- What is the difference between a L2 Switch and a Router?
- What is the difference between a L3 switch and a Router?
- What is the purpose of the ARP protocol?
- What happen if you have a static entry in the ARP cache and the NIC for that target computer is changed?

- If IP determines that the packet that it is currently processing is destined for a remote subnet, where does IP send the packet?
- How could you find the physical address of the Ethernet card installed on your computer?
- Which one is the protocol number of ARP? Check with wireshark
- A destination MAC address can be a:
    - UNICAST address?
    - BROADCAST address?
    - MULTICAST address?
- A source MAC address can be a:
    - UNICAST address?
    - BROADCAST address?
    - MULTICAST address?
- Is the target Ethernet address of an ARP request packet a unicast address, a broadcast address, or a multicast address?
-

Subnet masks

- Check your subnet mask
- Remove your default gw
- Change your subnet mask at runtime to 255.255.255.248 - /29
- Check your routing table
- Add your default gateway
- What do you notice?

Scenario

You are the network administrator of a Class C network. Your network consists of 100 computers. Your ISP assigns the address 137.138.111.0/24 to your network. Your network requires 10 subnets with at least 10 hosts per subnet. Which subnet mask should you configure to meet this requirement?

Questions

What is the dotted decimal notation of subnet masks for the following ip addresses?

- 192.168.10.1/23
- 5.5.5.5/16
- 203.40.21.58/27
- 9.2.3.1/9

What is the prefix notation of the following subnet masks?

- 255.255.0.0
- 255.248.0.0

- 255.255.255.255

IP fragmentation

- Using wireshark start a new capture
- ping your default gw using a 2900 as packet size
- Stop the capture and view the captured frames
- What do you notice?

IP Time To Live

- Open wireshark on both workstation
- Ping the workstation in another subnet
- Check the TTL on your local workstation
- Check the TTL of the same IP packet sniffed in the remote workstation
- What do you notice?
- Why?

Routing table

- Check your routing table
- Remove the address of your default gw
- Ping a host on your subnet, was the ping successful?
- Ping a host in another subnet, was the ping successful?
- Reset your network config to the default values
- Remove the link that interconnect your default gw to the other subnet.
- Ping an host in the other subnet, what is the error code?

Analyze ICMP Echo Request and Echo reply

Open wireshark, select an ICMP ECHO REQUEST packet and check for:

- ICMP TYPE
- ICMP CODE
- ICMP Identifier
- ICMP sequence number

Open wireshark, select an ICMP ECHO REPLY request packet and check for:

- ICMP TYPE
- ICMP CODE
- ICMP Identifier
- ICMP sequence number

Open wireshark, select a DESTINATION UNREACHABLE message and analyze it
What is the main difference between an ICMP ECHO REPLY message and a DESTINATION UNREACHBLE message?

Dynamic Host Configuration Protocol & UDP

Analyze the UDP header and four steps of the DHCP request together with your tutor

Transmission Control Protocol

Analyze the three way handshake together with your tutor

Practice with L3 switches

Check the configuration of the L3 switches together with your tutor

Bonus tasks

- Analyze the traffic generated by a sender from layer 7 of ISO/OSI pile to the layer 7 of the destination.
- Implement VLANs with your tutor
- What is the difference between a routing protocol and a routed protocol? Implement a routing protocol with your tutor.
- Implement Network Address Translation