# Computer Networks Lecture 5

Jack Chandler - jtc4hnu

8 September 2021

## 1 Introduction

Ethernet is a type of local area connection (LAN). The name originated from the idea of a shared line passing through several households that a user could tap in to in order to access the internet.

An etherenet connection has 8 internal wires in which the NIC MDI of a sending machine is connected to the NIC MDI of a receiving machine.

### 1.1 Local Area Network Configurations

The idea of the "ether" that would be tapped in to is a BUS configuration, in which all physically connected devices would receive the same traffic.

The star configuration is the prevalent configuration today, in which a switch is used to distribute data to multiple connected devices. This creates a more distributed network, but now switches must be able to identify where packets are going.

On the Link level, switches use addresses of machines to identify where a packet of data is supposed to be sent to. These addresses are called media access control (MAC) addresses, formatted as a 12 digit hexadecimal number (6 byte binary number).

2C:54:91:88:C9:E3

A packet is then composed of the following:

Preamble — Source — Destination — Type — Payload — CRC

At this layer, the destination will be used to identify what connected machine the packet should be sent to from the switch.

### 1.2 Note On Encoding

Manchester Encoding is used in early Ethernet standards as a self-clocking

The signal is decoded at the falling edge of the clock using

Data XOR Clock

# 2 Address Resolution Protocol (ARP)

Given a MAC Address, the switch must know what machine to send the packet to. This will be done by storing a table of connected devices to relate MAC address to the interface that the switch will send the packet on.

## 2.1 ARP Table

This would work, but packets contain IP addresses instead of MAC addresses. The workaround for this is the ARP Table. MAC IP TTL

| MAC | IP | TTL |
|---|---|---|
| AA.BB.CC.DD.EE.FF | 10.40.15.4 | 7395 |
| AA.BB.CC.DD.EE.FE | 10.40.15.5 | 847 |

Reading from this table, incoming packets can be distributed directly to the target device after decoding the MAC from the IP.

## 2.2 ARP Table Filling

In order for to know the MAC associated with each IP, the ARP Table must first be populated. This is done when the first packet is sent.

A broadcast message is sent to all locally-connected devices. ARP sets the destination address to FF.FF.FF.FF.FF.FF, which is calls the broadcast address. The packet type field would be 0x806 to identify the type of message. The broadcast is translated as an ask for the router:

Who has 192.168.1.1?

This is an ARP Query. The contents of the packet should also include:

source MAC (ex. AA.BB.CC.DD.EE.FD),
source IP (ex. 192.168.1.2),
target IP (ex. 192.168.1.1)

An ARP response would be of the form

requester MAC
target IP
target MAC

from the ARP repsonse, the ARP Table may be filled with the IP, returned MAC, and some time-to-live (TTL).

## 2.3 ARP Spoofing

This processes introduces a vulnerability for a "man in the middle" attack. In this attack, a device may respond to a broadcast and declare itself as the router. After being populated in the ARP Table, the compromised computer will route its internet traffic to the other device instead of the router.

### 2.4 Time to Live (TTL)

An ARP Table cannot have infinite size, so entries must eventually be removed. This is handled with a TTL value, which will represent the time the connection has remaining before it is dropped from the ARP Table.

### 2.5 Viewing the ARP Table

A command is included for viewing the ARP table.

arp -a

This command allows the user to see

- the current arp table on machine
- a list of neighbors on network

## 3 IP-Routing

Internet traffic must also be routed outside the local network. For this, a router has both an internal and external IP. Either side of the router is denoted a subnet.

### 3.1 Subnet Mask

A Subnet mask is component of IP address that is the same for all IPs within a subnet.

This may be used to tell if a device is in the same subnet by comparing the IP ANDed with the subnet mask.

Example notation 1: 2.2.2.2 / 16
Example notation 2: 255.255.0.0

### 3.2 CiDAR Notation

CiDAR is a compact way of expressing both an IP and an associated subnet mask. The notation is written as the IP address followed by a division. The divisor represents the number of bits in the subnet mask, which will start left to right.

Subnet given: 2.2.1.0 / 16
Decomposition: 00000010.00000010.00000001.00000000 / 16
00000010.00000010.00000001.00000000
IP Range: 2.2.0.0 → 2.2.255.255
Subnet Mask: 255.255.0.0

Is the IP Address 2.2.255.0 in the subnet 2.2.1.0 / 16 ?
Yes! first 16 bits : 2.2 == 2.2