Computer Networks - Top Down approach - Link Layer

Saurabh Barjatiya

2012-03-20 Tue

Contents

1 Link layer

Lowest or first layer in TCP/IP network stack is Link layer. TCP/IP link layer includes both Physical layer and Data link layer of OSI reference model. Physical layer of OSI reference model refers to physical medium like copper wire (CAT5, CAT6 etc. cables), fiber or air in case of wireless communication.

Data link layer of OSI reference model refers to MAC (Medium access control) protocols using which various devices share a physical medium and communicate with each other. In this lecture we will not talk about physical layer and topics related to physical layer like speed, delay, bandwidth, error rate, jitter, noise, etc. These topics will be deferred till a formal course in networking.

Following topics will be discussed in this lecture:

- MAC address or Layer 2 address or HW address
- Network devices
- Broadcasts
- ARP protocol

2 MAC addresses

Every machine on LAN has a unique MAC address (or every machine within a subnet **must** have unique MAC address for that particular machine or subnet to function properly). Since uniqueness of MAC address within a subnet is so important, this uniqueness is guaranteed at time of manufacturing NIC (Network Interface Card) by use of OUIs(Organizationally Unique Identifiers).

MAC addresses are 48-bit long and written in terms of twelve hexadecimal characters grouped in sets of two, where consecutive sets are separated by colon(:). For example, `aa:aa:aa:aa:aa:aa=` is a possible MAC address. Hexa-decimal characters can be written in either small letter or capital letters.

First 24-bits of MAC address are OUI and assigned to a particular organization. Only that organization can manufacture cards whose first 24-bits of MAC address are same as assigned OUI. Internally organizations ensure that they do not give same last 24-bits to any two cards while using a particular OUI. Big organizations like Dell, Linksys, Intel etc. which manufacture millions of cards are allotted thousands of different OUIs to ensure that they can continue producing NICs with world-wide unique MAC address.

2.1 Finding MAC address of particular interface

To find MAC address of particular interface we can use `/sbin/ifconfig` command. `ifconfig` reports MAC address associated with interface with label `HWaddr`. For example in below mentioned `ifconfig` output MAC address of `eth0` is `00:1E:C9:59:01:7F`.

```
eth1      Link encap:Ethernet  HWaddr 00:1E:C9:59:01:7F
          inet addr:10.5.1.222  Bcast:10.5.1.255  Mask:255.255.255.0
          inet6 addr: fe80::21e:c9ff:fe59:17f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3923250 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3107383 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1849345671 (1.7 GiB)  TX bytes:3333670770 (3.1 GiB)
          Interrupt:16 Memory:dfbf0000-dfc00000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:580027 errors:0 dropped:0 overruns:0 frame:0
          TX packets:580027 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:888336682 (847.1 MiB)  TX bytes:888336682 (847.1 MiB)
```

Not all possible 48-bit values can be used as MAC addresses on end hosts. Many MAC addresses have special meaning and are used to denote special information like broadcast, multicast, etc.

DHCP servers are able to assign same IP address to a given machine on subsequent requests because they can identify machines with help of MAC address. All DHCP requests contain MAC address of sender which can be used by DHCP server to allocate same IP to given client every time.

3 Network devices

3.1 Repeaters or Converters (L1 device)

Repeaters are layer 1 devices which transmit information received on one interface as it is on other interface. These devices just understand signals and voltage levels. They do not understand information (or garbage) that they transmit from one physical medium to other. In case of repeaters the physical medium on both ends is usually same like copper wire or fiber. In case of converters they can receive information through one physical medium like copper wire (LAN wire / CAT5 / CAT6 cable) and transmit it via fiber or vice-versa.

3.2 Hubs (L1 devices)

Hubs are L1 devices to which many PCs, other Hubs, switches etc. can connect at once. Hubs can have 8-ports, 16-ports or even 24-ports. Information received on one port is transmitted via all other ports as it is. Again hubs do not understand what information is being transmitted by them. They just understand signals and voltage levels. In case of hubs if multiple senders try to send information at same time, then their signals collide and mixed garbage noise will get transmitted to all receivers. Hubs will not realize that collision has occurred, nor can they do anything to prevent collision. All devices connected through hubs are said to be single collision domain and single broadcast domain.

3.3 L2 switches

L2 switches are layer2 devices and hence the term L2 is being used. Switches understand Layer 2 of OSI reference model and hence they understand medium access control (MAC) protocol in use. Switches understand packets and can read L2 information like Destination MAC address, Source MAC address, etc. from packets. Switches then use this information to forward packets intelligently rather than sending received packet via every other interface. Switches also understand special MAC addresses meant for broadcast and multicast. When switches receive such packets they transmit broadcast and multicast packets through large number of interfaces (or all other interfaces) except the one via which they had received the packet.

Switches divide network into multiple smaller collision domains while keeping the whole network in one single broadcast domain.

3.3.1 Working of L2 switches

L2 switches work by observing packets and reading MAC layer information present in each packet. When switch is started for first time they do not know any MAC address and do not have any idea where a host with particular MAC address is. In such situation when switch receives any packet, it transmits it via all other interfaces. This is called as learning mode of switch. Switch when it receives any packet, apart from looking at destination MAC address also looks at source MAC address in received packet. By looking at source MAC address switch learns location of device with given MAC address to be on port through which it has received the packet. Switch stores this information in table called MAC address table. Next time when switch receives any packet with destination address same as source address of previously received packet, it knows where exactly to send that packet with help of MAC address table without requiring to flood all the ports with given packet.

The same is illustrated below with time-line and events:

SNo	Event	Description	MAC address table
1	Switch started for first time	Since switch has just started MAC address table would be empty	
2	Switch receives packet for destination MAC M1 with source MAC M2 at port 3	Switch will learn that machine with mac address M2 is located at port 3 and store this information in MAC address table. Since switch does not knows where M1 is it will send this packet via all ports except port 3 from which it has received the packet	M2 -> 3
3	Switch receives packet for destination MAC M4 with source MAC M3 at port 5	Switch will learn that machine with MAC address M3 is located at port 5. Switch will transmit this packet via all interfaces except port 5.	M2 -> 3 M3 -> 5
4	Switch receives packet for destination M2 with source MAC M5 at port 7	Switch will learn M5 is located at port 7. Now switch will transmit this packet only via port 3 as it knows host with MAC address M2 is located at port number 3.	M2 -> 3 M3 -> 5 M5 -> 7

3.4 Manageable switches

Switches are of many different types because of layer at which they operate:

- L2 switches
- L3 switches
- L4 switches
- L7 switches

L2 switches are again of two types:

- Manageable L2 switches
- Unmanageable L2 switches

Advantages of L2 switches over unmanageable switches are:

- We can see MAC address table of manageable switches (remotely)

- We can shutdown / enable port of manageable switches (remotely)

- We can configure VLANs in manageable switches. What VLAN is may be covered in next lecture.

- Manageable switches use STP protocol and hence switching loops are not possible with manageable switches. Thus manageable switches prevent broadcast storms

- Many manageable switches support NAC (Network Admission Control).

- Many manageable switches support port security with help of which we can control which client MAC addresses will work on given port and other MAC addresses get rejected

- Many manageable switches support ACLs so that we can block / allow certain type of traffic

- We can mirror ports with manageable switches

3.5 MAC flooding and port mirroring

Given that switches by learning MAC addresses it is possible to disrupt the proper working of switches by MAC address flooding. In MAC address flooding an attacker sends packets with many different source addresses (>8k or >16k) within very short span of time (˜1 sec) so that switches' MAC address table is full and it can no longer learn new MAC addresses, till old addresses are aged out. Aging of address may take anywhere from 30 sec to 5 minutes. Now since switch cannot learn new MAC addresses it transmits packets for given MAC address through all ports. Thus all the machines connected to particular switch receive packet and not just the destination machine. Now attacker can use tools like wireshark to capture packets which were meant for other machines and read private information like emails, chat messages and in case of insecure protocols, even passwords.

Another possibility of attack is with bad or malicious network administrator. Network administrator can mirror any switch port and capture information sent / received on that port on some other switch port passively without letting any user realize that their ports are being mirrored. This also produces same threats as MAC address flooding as administrator can now read private information (including passwords in case of insecure protocols) being sent / received by user.

Users can protect themselves against MAC address flooding by being vigilant and observing whether they are able to receive packets belonging to other machines very often or not. Users cannot protect themselves against port mirroring. They can just maintain privacy by use of secure / encrypted communication and protocols instead of using their insecure counterparts.

3.6 Routers

Switches generally do not look at IP address within packets. Even if they read IP address to implement ACLs or to see whether packet is meant for them (Manageable switches), switches never route packets from one network to another. In other words we cannot connect two machines belonging to different networks (say 10.3.3.187/24 and 10.5.1.222/24) using an L2 switch (even manageable L2 switch) and expect them to be able to communicate.

Hence different types of devices which can route packets from one network to another are required to facilitate communication between different networks. Such devices work at OSI Layer 3 and are called routers. Routers are hardware devices like switches but usually contain very less number of ports 2/4 unlike switches which may have even more than 100 ports. Routers are usually slower than switches as routing requires more computation then switching which can be done very efficiently in pure hardware.

Routers typically also support many different types of physical mediums where switches dominantly support copper cables (CAT5/CAT6). Routers support number of routing protocols like BGP, OSPF, RIP, even static routing none of which are supported by L2 switches.

Routers divide network into smaller broadcast domains. They off-course also divide network into smaller collision domains.

3.7 Firewall

Firewalls are hardware devices or special software that are designed to restrict certain types of network connections. Usually firewalls are configured to block connections which are harmful for a particular organization or department. For example we have anti-virus and anti-spam firewall devices that block network connections that are used for spreading viruses or sending SPAM emails.

We can also have content filtering firewalls which can be configured to block access to particular domain (example `youtube.com`, `rapidshare.com`) or particular file type (example `mp3`, `avi`).

The common thing about all these firewalls is that they try to protect organization from attacker / harm that is origination from outside network. The simplest most basic firewalls are configured so that connections can be sent to a particular server or machine only on allowed set of ports. If someone tries to connect to a given server protected by firewall on a port not allowed by firewall then firewall blocks such connection and does not allows clients to communicate. This blocking of connection attempt is completely hidden from server in case of in-network hardware firewalls.

Hence firewalls are hardware or software designed to make network more secure by filtering traffic as per their (firewalls) understanding of threat based on configuration done by network administrators. We will try to learn configuration on one host based firewall named `iptables` which is available on all famous Linux platforms to understand how to configure firewall and how to protect ourselves against network attacks.

4 Broadcasts

It is possible for a node (machine / PC / laptop / router) to send packet to all the other nodes in same subnet. This type of communication is termed as broadcast as the information sent by one node is broadcast to all other nodes in subnet. There are two different types of broadcast

- L2 broadcasts
- L3 broadcasts

We will only look at L2 broadcasts in this course / lecture.

4.1 L2 broadcasts

With L2 broadcasts it is possible for a node to send some packet to all other nodes in same network. Usually this type of communication is done over IP / UDP and connection oriented protocols like TCP do not support broadcasts. In order for node to send packets to all other nodes it has to put special broadcast MAC address (`FF:FF:FF:FF:FF:FF`) as destination MAC address in the packet. Normally switches learn and forward packets based on MAC addresses. But all switches understand special MAC addresses reserved for broadcasts and multicasts.

Whenever a switch encounters a broadcast MAC address as destination it forwards the packet via all other ports except the one on which it had received the packet (same as if the destination MAC address in not in MAC address table).

4.2 L3 broadcasts and multicasts

Understanding and explaination of L3 broadcasts and multicasts is outside scope of this lecture / ITWS II course. The heading / section is created to indicate that there are things called L3 broadcasts and multicasts.

5 ARP protocol

Consider communication between two nodes in same network (say 10.3.3.230/24 and 10.3.3.187/24). If we want to ping from 10.3.3.230/24 to 10.3.3.187/24 then we need to know the MAC address of 10.3.3.187/24, as the destination MAC address (first six bytes) of the packet to be sent to 10.3.3.187 should be MAC address of 10.3.3.187. But how does one node (10.3.3.230 in this case) finds MAC address of other node in same network? The answer to this question is - 'through ARP protocol'.

ARP stands for Address Resolution Protocol. With the help of ARP protocol nodes which are in same sub-net can find each others MAC address. For one node to find other nodes MAC address it sends a broadcast ARP packet with ARP query asking which node has this IP address? If there is some node in the subnet which has given IP address, then it responds back with ARP reply that I have this IP address. Once nodes learn each others MAC address using ARP protocol they start normal IP based network communication.

Please note that ARP does not runs over IP, like ICMP, TCP or UDP. ARP header is created on top of Ethernet header and hence ARP runs directly over Ethernet. But ARP is part of IP protocol suite and is required for network based on IPv4 addresses to work.

5.1 ARP spoofing

With ARP spoofing it is possible for users of subnet to capture plain-text information sent by other users in the same subnet. Understanding working of ARP spoofing attack is outside scope of this course. The section is created to indicate that ARP spoofing attacks exist, so that we can explain how one can protect themselves against such attacks.

5.2 Protecting ourselves against ARP spoofing

Protecting our machine against ARP spoofing attack is very important in LAN based environment. The protection mechanism described below requires users to have administrative privileges:

Steps:
* Find gateway address using

```
route -n
```

command. Example output when `route -n` command is run on one machine is:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.5.1.0        0.0.0.0         255.255.255.0   U     0      0        0 eth1
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth1
0.0.0.0         10.5.1.1        0.0.0.0         UG    0      0        0 eth1
```

In this output gateway IP address is 10.5.1.1
* Ping gateway so that we get MAC address of gateway in ARP cache.

```
ping 10.x.x.1
```

It is assumed that system is not under attack at point of this configuration and hence we get correct gateway MAC address with help of ping. As per previous example the command would be `ping 10.5.1.1`.
* Find gateway MAC address with help of `arp -a` command

```
arp -a
```

As part of same example the output of `arp -a` command is:

```
? (10.5.1.1) at 00:1D:46:8C:21:C5 [ether] on eth1
```

There may be other lines in `arp -a` command output, but line of our interest in the line showing MAC address of gateway as shown above.
* Add gateway address permanently in ARP table using `arp` command using syntax:

```
arp -s <IP address> <MAC address>
```

In case of our example the command would be

```
arp -s 10.5.1.1 00:1D:46:8C:21:C5
```

* Verify using `arp -a` command that MAC address got permanently allocated. Notice the keyword `PERM` in line containing ARP entry of gateway (10.5.1.1 in case of our example).

```
? (10.5.1.1) at 00:1D:46:8C:21:C5 [ether] PERM on eth1
```

* Ping gateway and ensure that communication is not disrupted due to static ARP entry.

* Add command to start-up file to add this static entry automatically at system boot. For this edit `/etc/rc.d/rc.local` file and add command similar to: arp -s 10.5.1.1 00:1D:46:8C:21:C5 ‘sleep 200‘ &

Here sleep 200 is provided assuming IP address would be obtained using Network Manager within 3 minutes after system boot using GUI login to one of the users of the system.