

Tools Set-3: Digging deeper into Network Layer

(Computer Networks Lab)

Kameswari Chebrolu

Network Layer

- IPv4, IPv6 packet format
- Addressing/Forwarding
- DHCP
- ARP
- ICMP
- NAT
- Routing

Ver sion	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address (16)			
Destination Address (16)			
Next Header / Data			

IPv6 Packet Format

-

SEE I DO AGAIN USED ACTED MAT

The diagram illustrates the structure of an IPv4 packet header, which is 32 bits long. The fields are as follows:

Field	Start Bit	End Bit	Length (bits)
Ver	0	3	4
HL	4	7	4
Type of Service	8	15	8
Total Length	16	31	16
Identification	0	15	16
Flags	16	19	4
Fragment Offset	20	31	12
Time to Live	0	7	8
Protocol	8	15	8
Header Checksum	16	31	16
Source IP Address	0	31	32
Destination IP Address	0	31	32
Options	0	31	32
Data (Variable Length)	0	31	32

A red oval highlights the Identification, Flags, and Fragment Offset fields, which are used for fragmentation and reassembly.

Addressing/Forwarding: “ip”

- Which subnet do I belong to?

- “ip addr” or “ifconfig”

- IP prefix, Subnet mask
- Broadcast address

ip addr
IP address → .
MAC

- Forwarding at a host?

- “ip route” or “route”

- Default route
- IP prefix based forwarding

ip route
default ↑

lower metric : more preference

ip route..... table entries along with a default entry

DHCP: “dhclient”, “wireshark”

- Run wireshark and then run
 - “dhclient -v ^{reboot} eno1” (may or may not ^{asking for ip addr} see discover)
 - “dhclient -v -r eno1” (DHCP ^{release} release message)
 - “dhclient -v eno1” (After release, you should see discover)

dhcp servers try to give same addr to us again to all extent possible

Needs root permission to run

ARP: “ip”, “arping”, “wireshark”

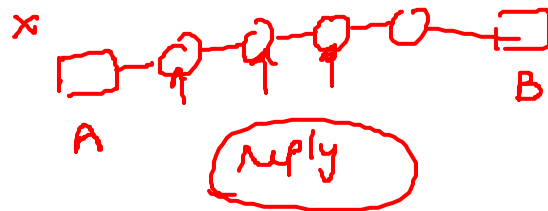
- “ip neigh” (arp cache)
- Sending gratuitous ARPs
 - arping -I wlp1s0 -A own-ip-address (Request)
 - arping -I wlp1s0 -U -P own-ip-address (Reply)

“arping” may not be installed by default (then do
“sudo apt-get install arping”). Normally needs root permissions to run

ICMP: “ping”, “traceroute/mtr”, “wireshark”

ICMP

- Ping : covered before
- traceroute: determines the route to a destination
 - “traceroute www.iitb.ac.in”^{✓ IP addr}
- mtr: combines ping with traceroute
 - Does traceroute continuously
 - “mtr www.iitb.ac.in”[↑]



“traceroute” may not be installed by default, then do “sudo apt-get install traceroute”.

Summary

- Concepts: Packet formats, Addressing/forwarding, DHCP, ARP and ICMP
 - ip, dhclient, arping, mtr/traceroute and our usual friend wireshark