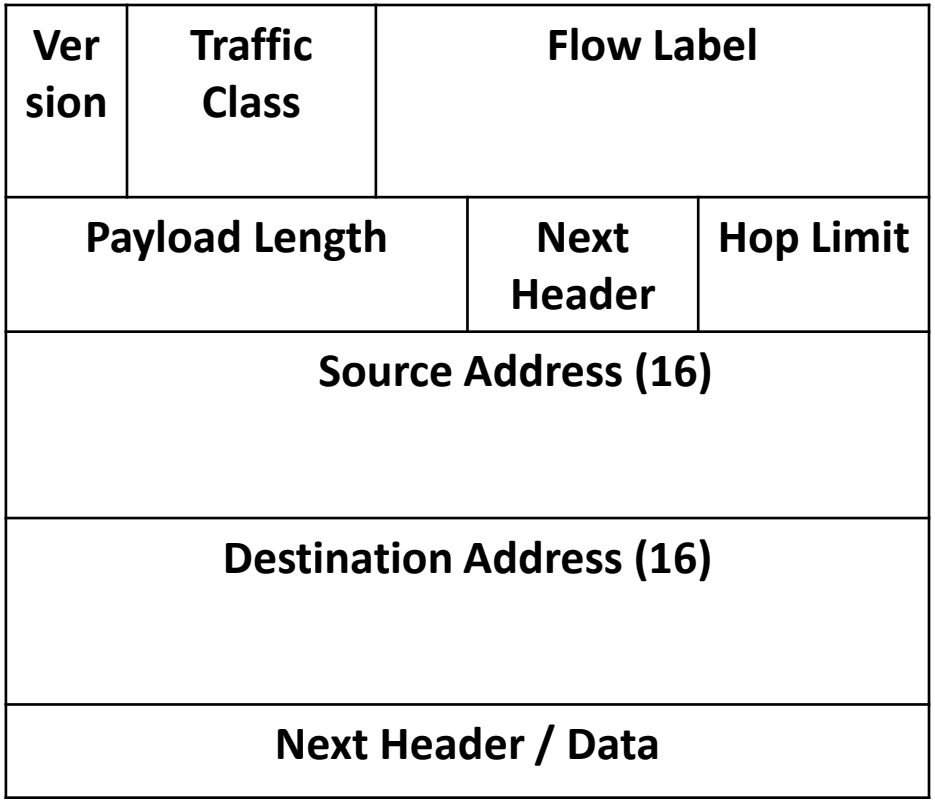
Tools Set-3: Digging deeper into Network Layer

(Computer Networks Lab)

Kameswari Chebrolu

Network Layer

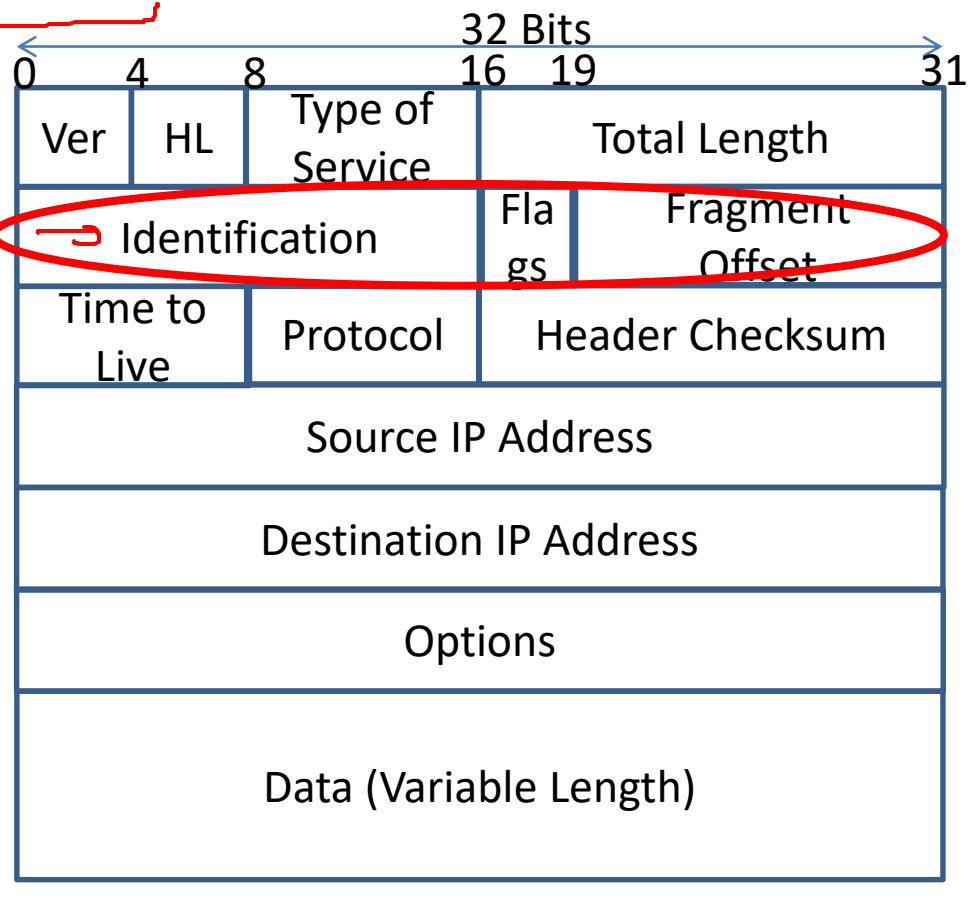
- IPv4, IPv6 packet format
- Addressing/Forwarding
- DHCP
- ARP
- ICMP
- NAT
- Routing



IPv6 Packet Format

Packet Format/NAT: "wireshark"

- Run Wireshark and explore IPv4 and IPv6 headers
  - "ping ipv6-address"
- Fragmentation: Send a large packet
- Wireshark trace that captures NATing



coming , sending are different...

Addressing/Forwarding: "ip"

- Which subnet do I belong to?
  - "ip addr" or "ifconfig"
    - IP prefix, Subnet mask
    - Broadcast address
- Forwarding at a host?
  - "ip route" or "route"
    - Default route
    - IP prefix based forwarding

ip addr

IP address → MAC

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 eno1” (may or may not see discover)
  - “dhclient –v –r eno1” (DHCP release message)
  - “dhclient –v eno1” (After release, you should see discover)

asking for ip adddr

release

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

Needs root permission to run

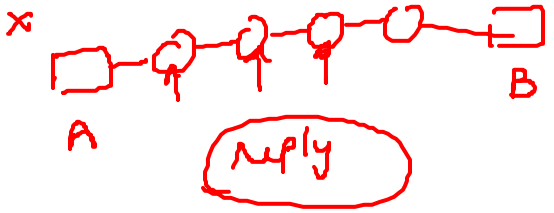
ARP: “ip”, “arping”, “wireshark”

- “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”

- Ping : covered before
- traceroute: determines the route to a destination
  - “traceroute www.iitb.ac.in”
- 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