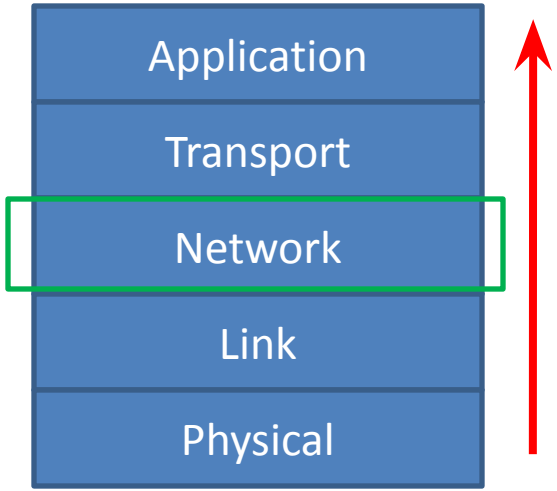
Computer and Network Security: Network Layer Attacks and Solutions

Kameswari Chebrolu

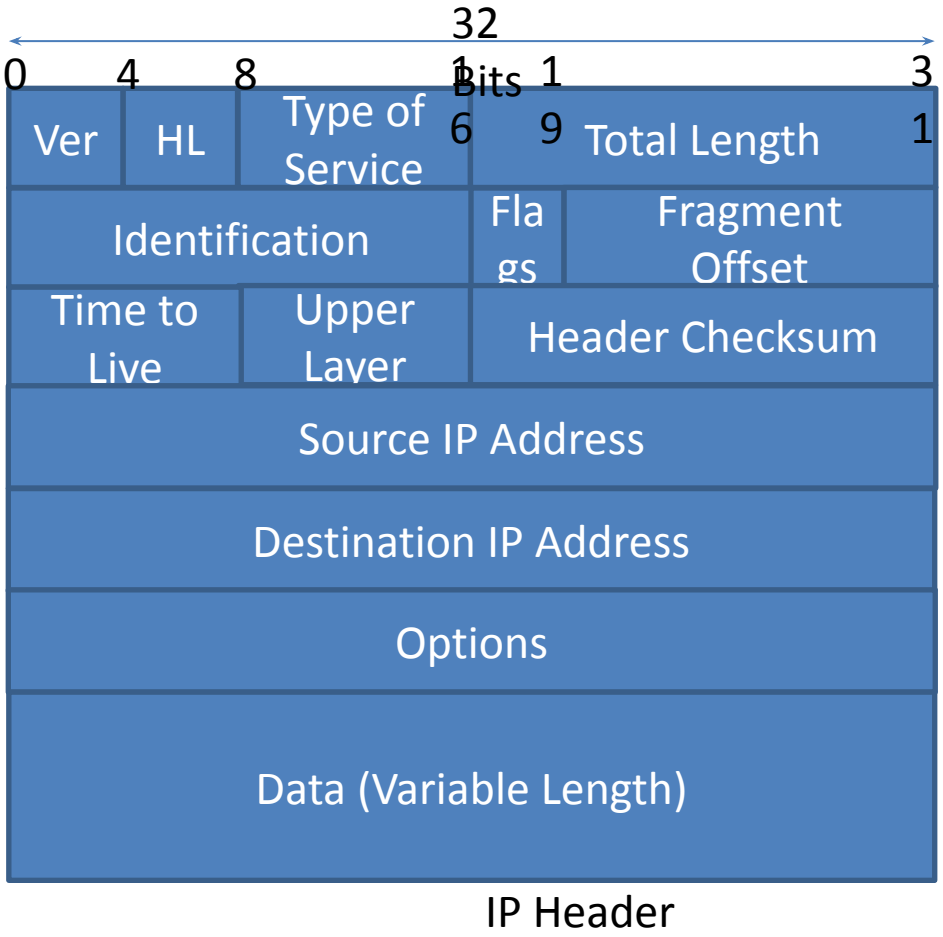
Outline

- Background
- Attacks at different layers of the protocol stack
- Solutions to the same



Network Layer Role

- What is the role of the network layer?
  - End-host delivery
- Best effort service model based on common IP standard



IP Header

Background

- IP addresses: hierarchical structure for efficient routing
  - Network part identifies the network to which host is connected (subnet id)
  - Host part uniquely identifies each host in the network
- Before any communication, the host needs an IP address and default router's IP address
- How does a host get an IP address?
  - Address needs to be unique and location (subnet) dependent
  - Solution: Dynamic Host Configuration Protocol (DHCP)

DHCP

- Dynamically get IP address from DHCP server
  - Server maintains a pool of available addresses
  - Addresses handed out on demand (leased for some specific time)
  - Host periodically needs to renew the lease
- Advantages: Ease of configuration (automated), reuse of IP addresses, supports portability
- But how does the host know address of DHCP server?

DHCP Operation

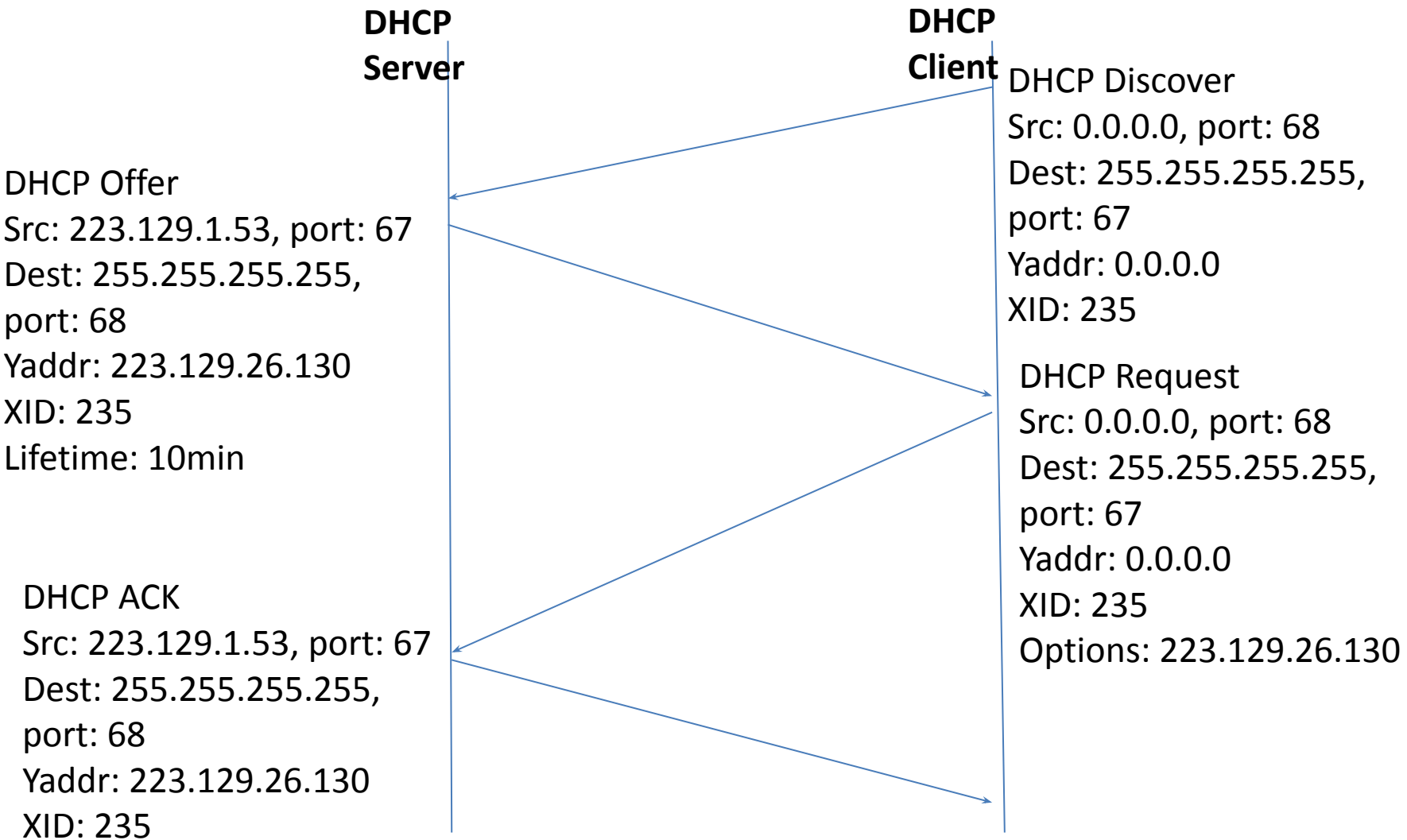
- Operates at application layer using UDP protocol
- A newly booted/attached host ‘broadcasts’ DHCP discover message
  - IP address: 255.255.255.255 goes as link-layer broadcast (broadcast restricted to physical network)
  - Received by all hosts/routers in the physical network
- DHCP Server replies to host (others ignore message)

Message Exchange

- Host broadcasts “DHCP discover” msg
- DHCP server responds with “DHCP offer” msg
- Host requests IP address: “DHCP request” msg
- DHCP server confirms address: “DHCP ack” msg
- DHCP server also passes subnet mask, default router, domain name, DNS server info etc if host asks for it

DHCP Packet Format

Operation (1)	Htype (1)	Hlen (1)	Hops (1)
Xid (4)			
Secs (2)		Flags (2)	
Ciaadr (4)			
Yiaddr (4)			
Siaddr (4)			
Giaddr (4)			
Chaddr (4)			
Sname (64)			
File (128)			
Options (312)			

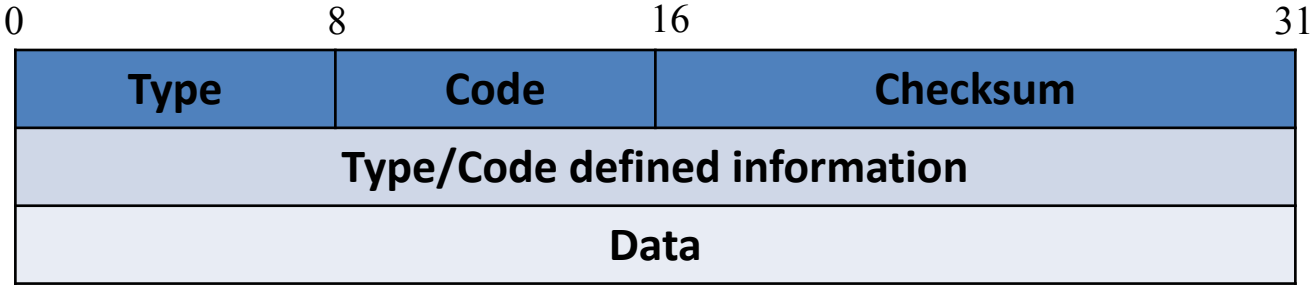

DHCP Server
DHCP Client
DHCP Discover
Src: 0.0.0.0, port: 68
Dest: 255.255.255.255,
port: 67
Yaddr: 0.0.0.0
XID: 235
DHCP Offer
Src: 223.129.1.53, port: 67
Dest: 255.255.255.255,
port: 68
Yaddr: 223.129.26.130
XID: 235
Lifetime: 10min
DHCP Request
Src: 0.0.0.0, port: 68
Dest: 255.255.255.255,
port: 67
Yaddr: 0.0.0.0
XID: 235
Options: 223.129.26.130
DHCP ACK
Src: 223.129.1.53, port: 67
Dest: 255.255.255.255,
port: 68
Yaddr: 223.129.26.130
XID: 235

ICMP: Internet Control Message Protocol

- Used by hosts & routers to communicate network-level information
  - Error reporting: unreachable host, network, port, protocol
  - Diagnostic purposes: Echo request/reply (used by ping)

ICMP Packet Format

- ICMP messages carried in IP datagrams
- 8 bytes of header followed by data.
- Data field in error messages carry
  - entire IP header and first 8 bytes of data of IP packet that caused the error



Select ICMP Messages

Type	Code	Description
0	0	Echo Reply (Ping)
3	0	Destination network unreachable
3	1	Destination host unreachable
3	3	Destination port unreachable
3	4	Fragmentation required, DF flag set
3	6	Destination network unknown
3	7	Destination host unknown

Select ICMP Messages

Type	Code	Description
4	0	Source Quench
5	0	Redirect datagram for the network
8	0	Echo request (Ping)
11	0	TTL expired
12	0	Bad IP header
13	0	Timestamp
14	0	Timestamp reply
17	0	Address mask request
18	0	Address mask reply

Attacks and Defences

- Eavesdropping
- Disruption
- Spoofing
- Protocol specific attacks: DHCP

Attacks and Defences

Eavesdropping (at network layer): Not easy unless one hacks a router

Disruption

- Can deny service via IP flooding based on ICMP (DOS attack)
  - E.g. bombard server with many ping requests
  - Overwhelmed host will drop legitimate connections
- More treatment under ‘DOS’ topic

IP Spoofing

- Can spoof source IP address
  - Overwrite source address in the packet
  - Does not imply attacker obtained that address (replies to the packet will not come to the attacker)
- Uses: DOS (to cover later), TCP session hijacking
- Solutions:
  - Border routers can drop packets not originating from proper domain
  - IP trace-back (covered under DOS) to originator of spoofed packets (and block the host)

DHCP Starvation Attack

- Vulnerability: Un-authenticated protocol
- Attacker requests many IP addresses and exhausts the pool (DOS attack)
  - Use spoofed MAC addresses (or slave machines)
  - Genuine host cannot get an IP address
- Solution: Switch can limit number of MAC addresses per port (Port security)
  - Important to check the DHCP payload also (DHCP snooping). Why?
    - Attacker can use his MAC and simply change MAC in DHCP payload (chaddr)
    - DHCP snooping: check if source MAC matches the chaddr in DHCP packet

DHCP Spoofing Attack

- Vulnerability: DHCP discover is broadcast
- A rogue DHCP server can reply to the broadcast
  - Can pass on fake DNS server which can resolve hostnames to fake machines
  - Can pass on fake gateway (router) □ router can inspect traffic, drop traffic, act as man-in-the-middle
  - Both very dangerous
- Solution: Switch configured with trusted ports (DHCP snooping)
  - trusted ports can source all DHCP messages
  - untrusted ports only requests (DHCP discover/request)

Summary

- Looked at network layer attacks
  - Eavesdropping, disruption and spoofing
- Specific protocol related attacks and solutions as well
  - DHCP starvation, DHCP spoofing
- Next: Transport and application layer attacks