Network Security

- Network Stack

  - Physical communication
  - Point-to-point communication
  - Internetworking
  - Transmission Control
  - Domain name system
  - Hypertext transport protocol
  - The OSI model.

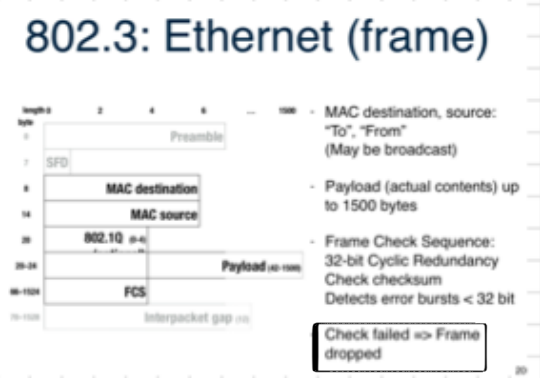
- Adversary capabilities – Dolev-Yao model
  - In this case the adversary has complete control of the network.
  - It may:
    - Intercept messages
    - Replay messages
    - Transform messages
    - Insert messages
    - Delete messages
  - It may not:
    - Guess our secrets
  - An attack that it cannot do is:
    - Steal a file stored in a user's computer

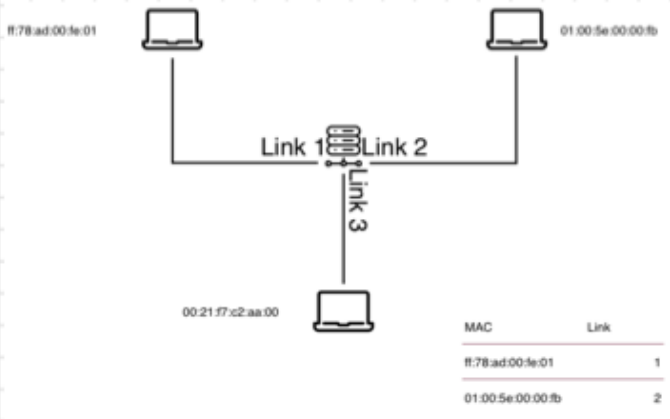
Physical Layer

- Responsible for transmitting binary data across physical link.
- Usually broadcast IEEE 802.3 Ethernet.
- Provides no guarantees.
- Possible attacks:
  - Eavesdropping [breaks confidentiality]
    - Frames are broadcast
    - Can see them even if they aren't for me.
  - Tampering [breaks integrity]
    - Won't detect my change
  - Denial-of-Service [breaks availability]
    - Put enough noise on the line, won't send or receive any messages.
  - Message Injection
    - Can put arbitrary messages on the wire.
- Cutting a network cable is a kind of Denial of Service.

Data Link Layer

- Responsible for transmitting packets between hosts connected by a physical layer
- Solves addressing - MAC addresses
- Solves reliability - checksums, CRC
- Performance gains by using switches
- Possible attacks:
  - * Tampering [breaks integrity]
    - CRC is weak, won't detect change
  - * Message Injection / MAC spoofing
    - Put arbitrary messages on the wire
  - * Eavesdropping [breaks confidentiality]
    - Frames are broadcast, can see them

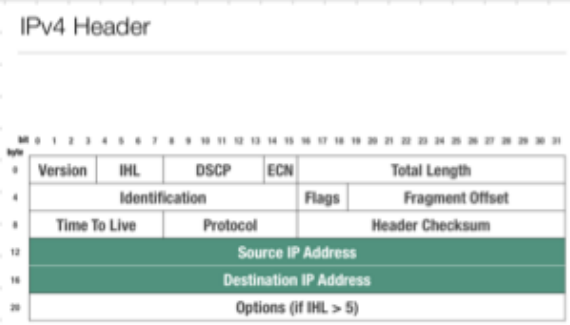


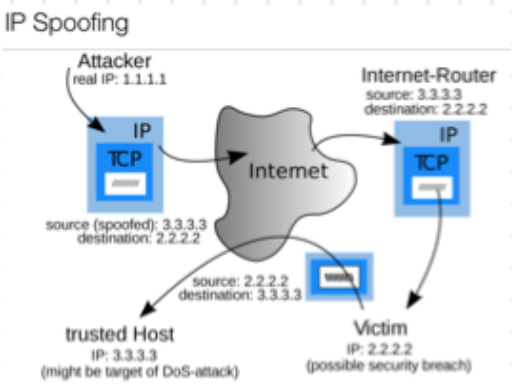


- MAC flooding -> transmitting many fake frames
  - Switch table contains no actual addr.
  - Switch must broadcast all frames
- To impersonate a user in the data-link layer an attacker would use MAC spoofing.

Network Layer

- IP protocol (IPv4)
- Hosts identified by IP addresses
- Best effort but unreliable delivery.
- May introduce packet duplication, out-of-order delivery
- IP operations:
  - Next-hop routing
  - BGP, ARP, DHCP
  - MTU (v4 only), Fragmentation
- Spoofing:
  - * ARP Cache Poisoning (ARP spoofing)
    - Spoof ARP - packets redirecting traffic for others to my machine!
  - * IP Spoofing
  - * DHCP Starvation





- IPv4 fragmentation attacks:
  - * Overlapping Fragments
  - * Fragmentation Buffer

Local Denial-Service attacks

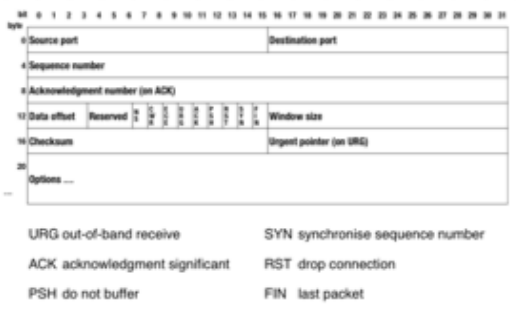
Remedies:

- * Ping Flooding
- * IP fragmentation attack
- * Distribute attack from many machines

* too many fragments
  - Rose attack: Send first & last bytes of large volumes
- IP spoofing is not effective for eavesdropping!!:
  - Remember: Hijacking identity will redirect traffic to that hijacked identity!

Transport Layer

- TCP:
  - Connection oriented, reliable, streaming protocol.
  - Achieved by message/acknowledgement seq #, timeouts.
  - Protocol specified as a fairly complex state machine.
  - Flow control, congestion control.



- Connection Setup:
  - 3-way handshake
  - TCP connection identified by an of (ip1, port1, ip2, port2)
  - ... i.e a webserver at 130.226.133.67:80 can have multiple conn. at a single port
- TCP sequence prediction attack:
  - Wanna hi-jack connection 

  - TCP seq #s are sent cleartext [eavesdropping]
  - Listen to traffic from B. Kill B's end of connection.
  - Spoof TCP packets to A
- TCP reset attack
  - Spoof TCP packet with RST = 1
  - Remote system should drop connection
  - Bypass IDS/Firewall may require seq prediction.
- TCP syn flood
  - Send large volume of illegal syn
  - Very cheap
  - Ties up buffer at receiving end.
- To use TCP seq pred to hi-jack a connection, the adversary has to DOS on the host communication.

Application Layer

- Domain names
  - Find IP addr for www.itu.dk
  - Use UDP query to Domain-name sys.
  - Premise: you must know nameserver.
- Attacks on FTP, telnet:
  - Login credentials in cleartext

- ADV MAY OBTAIN USERNAME/PASSWORD MERELY BY EAVESDROPPING
- ADV MAY OBTAIN SESSION TRAFFIC BY EAVESDROPPING.

FIREWALLS & IDS

- **FIREWALL:**
  - SELECTIVELY BLOCK OR REROUTE NETWORK TRAFFIC
  - ADVERSARY CAN'T ATTACK ME IF HE CANNOT SEND ME NETWORK PACKETS.
- **PACKET FILTERING FIREWALL:**
  - FILTER BASED ON PACKET CONTENTS
  - DEFAULT: DISCARD, FORWARD
- **INTRUSION DETECTION SYSTEM (IDS)**
  - DETECTS POTENTIAL MALICIOUS ACTIVITY
  - DOES SO BY ANALYZING NETWORK TRAFFIC
  - LOCATION: NETWORK OR HOST
  - DETECTS KNOWN PATTERNS

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Table 9.1, Stallings & Brown