NETWORK SECURITY:

NETWORK PRINCIPLES

→ communication in modern networks is characterized by the ff. fundamental principles:
- PACKET SWITCHING
- STACK OF LAYERS
- ENCAPSULATION

PACKET SWITCHING

→ Data split into packets

→ Each packet is
- transported independently through network
- handled on a best efforts basis by each device
  - ↳ Packet can be lost

→ Packets may follow diff. routes between the same endpoints and may be dropped by an intermediate device and never delivered.

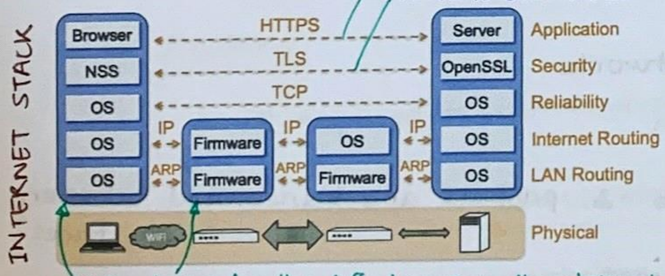
STACK OF LAYERS

→ Network communication models use a stack of layers

→ A network device implements several layers

→ A communication channel between 2 devices is established for each channel

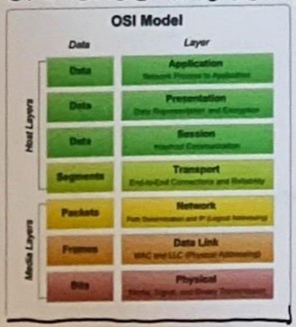
Dotted lines represent VIRTUAL CHANNELS

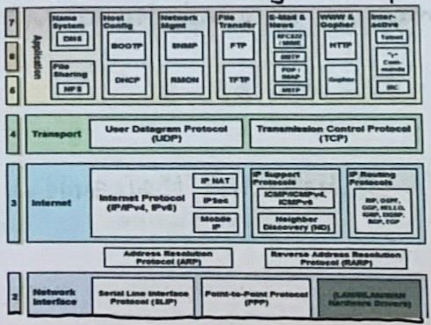


Diff. stacks for the diff. devices in the physical layer

→ Data flows from left to right of the devices in the physical layer and for each device, data flows from the top of the stack to the bottom.

→ Above pic. is the simplified model. In reality, we have the OSI (Open System Interconnect) reference model which is a network model consisting of 7 LAYERS





TCP/IP MODEL mapped onto OSI (4 layers)

ENCAPSULATION

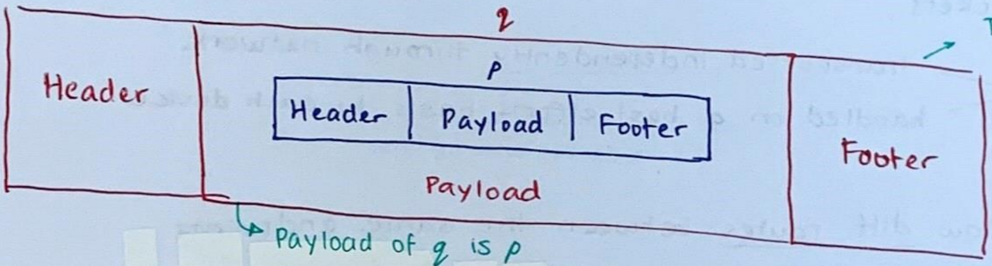
→ helps a packet to communicate between the diff. layers

→ A packet consists of:

- CONTROL INFORMATION — header / footer
- DATA — Payload

→ A protocol P uses the services of another protocol Q through encapsulation

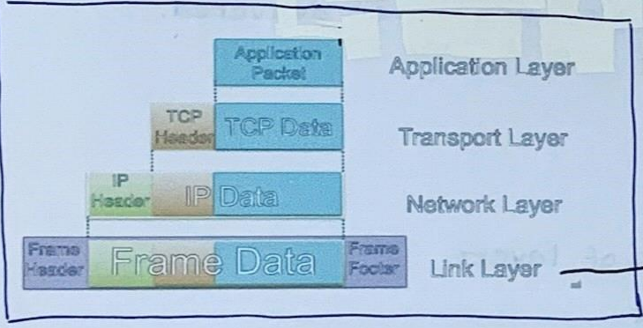
→ A packet p of P is encapsulated into a packet q of Q



The control info. of q is derived from tht. of p

Payload of q is p

INTERNET PACKET ENCAPSULATION



The frame packet at link layer will be sent to the physical layer over a wi-fi link /ethernet

NETWORK INTERFACES

→ are devices that connect a comp. to a network
i.e. Ethernet card, WiFi adapter, DSL modem

→ A comp. may have multiple network interfaces & packets are transmitted between network interfaces

→ Most LANs (incl. Ethernet & WiFi) broadcast frames

MEDIA ACCESS CONTROL (MAC) ADDRESS

→ Most NIs come w/ a predefined MAC address — 48 bit number represented in hex

e.g. 00 - 1A - 92 - D4 - BF - 86

The first three octets are IEEE assigned

The next three can be assigned by organizations as they please, w/ uniqueness being the only constraint

SWITCH

→ performs routing in a LAN

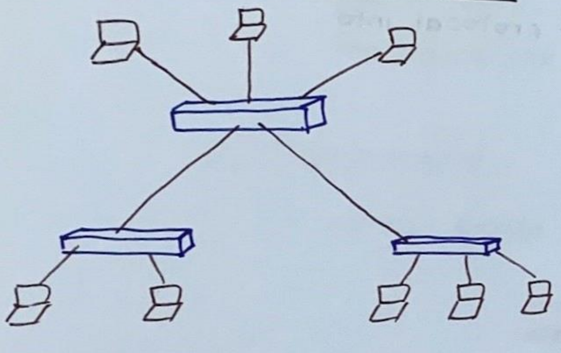
→ 1) Learns the MAC address of each comp. connected to it
2) Forwards frames only to the destination comp.

reduces the traffic on the network

→ Operates at the link layer

→ has multiple interfaces, each connected to a comp./segment

COMBINING SWITCHES



→ Switches can be arranged into a tree

→ This network of switches can be called a LAN

FNs OF INTERNET PROTOCOL (IP)

1) Addressing

→ In order to deliver data, IP needs to be aware of where to deliver data to, and hence includes addressing systems

2) Routing

→ IP required to communicate across networks

3) Fragmentation & Reassembly

→ IP allows fragmentation and reassembly of packets

→ The reason for this could be bc. the capacity of a channel is not large enough to accommodate the whole packet

IP ADDRESS

→ IPv4 (32-bit addresses)

→ IPv6 (128- bit addresses)

e.g. $\underbrace{128.\ 148.}_{\text{Network}}\ \underbrace{32.}_{\text{Subnet}}\ \underbrace{110}_{\text{Host}}$

→ Addresses thr. end w/ 255 (i.e. A.B.C.255) are broadcast addresses

→ these addresses live in the header of an IP packet

IP HEADER includes....

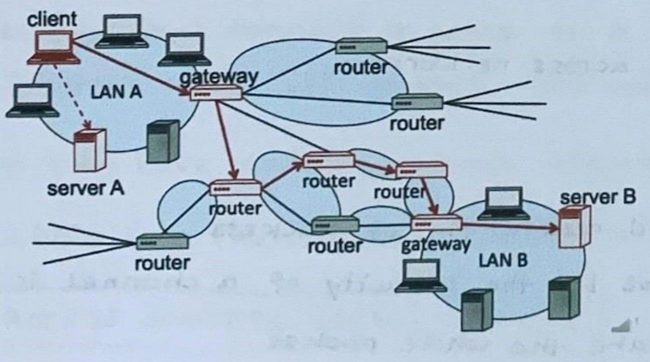
- Source address
- Destination address
- Packet length
- Time to live (TTL)
- IP version
- Fragmentation info.
- Transport layer protocal info.

IP ROUTING

→ A router bridges 2/more network

- Operates at network layer
- Maintains tables [Routing tables] to forward packets to the appropriate network by mapping ranges of addresses to LANs/gateway
- Forwarding decisions based solely on the destination address

e.g.



EXPLORING INTERNET ROUTES

→ Internet Control Message Protocol (ICMP) helps us to do this exploration

- used for network testing and debugging
- are simple messages encapsulated in a single IP packet
- is considered a network layer protocol

→ Tools that are based on ICMP are:

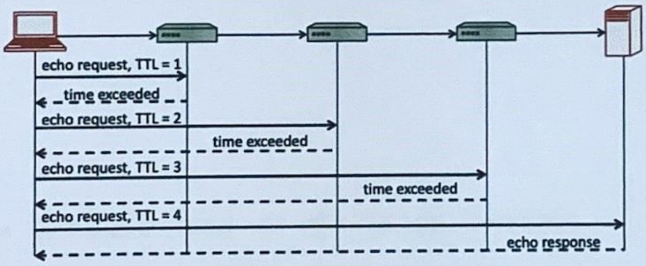
1) Ping

→ sends series of echo request messages and provides statistics on roundtrip times and packet loss

2) Traceroute

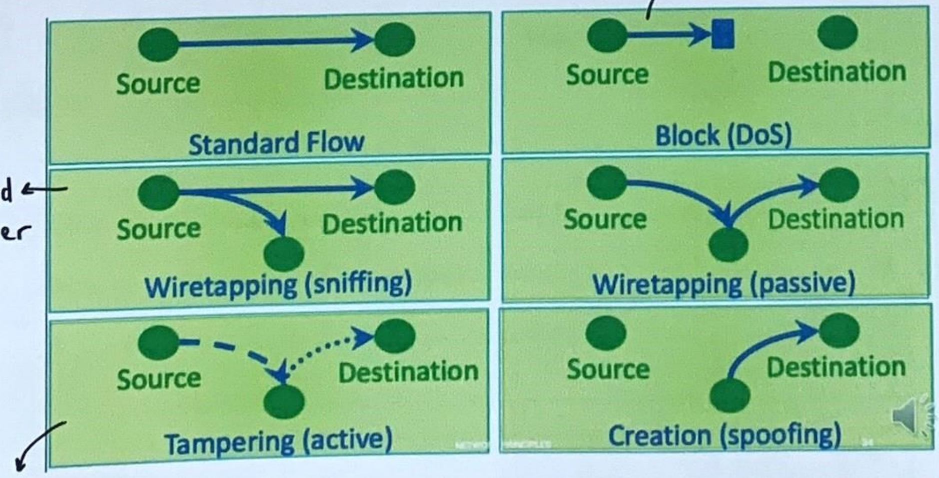
→ sends series of ICMP packets w/ increasing TTL value to discover routes

Time-to-live



NETWORK ATTACKS

source is prevented frm. being able to communicate w/ the dest.



Traffic is also copied and sent to another dest.

Data is changed by the intermediate node, so data is different when it arrived to the dest. than what is sent by the source

WIRESHARK

→ is a packet sniffer and protocol analyzer

→ When run in promiscuous mode, it captures traffic across the network

→ Captures & displays network-packets for analysis

→ supports plugins