# Network security: Networking Principles

COMPUTER SECURITY

MARKULF KOHLWEISS

Some slides adapted from those by Myrto Arapinis, Kami Vaniea, and Roberto Tamassia

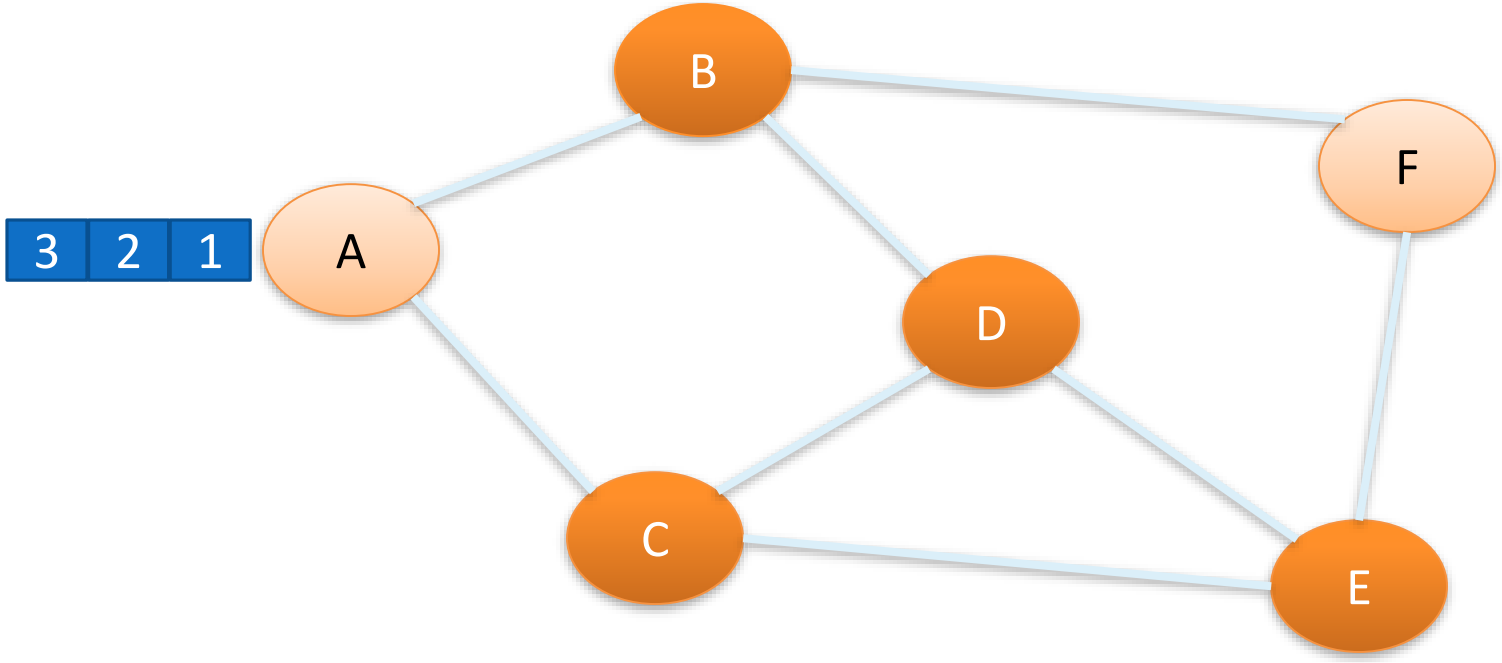
# Network Communication

- Communication in modern networks is characterized by the following fundamental principles
  - Packet switching
  - Stack of layers
  - Encapsulation

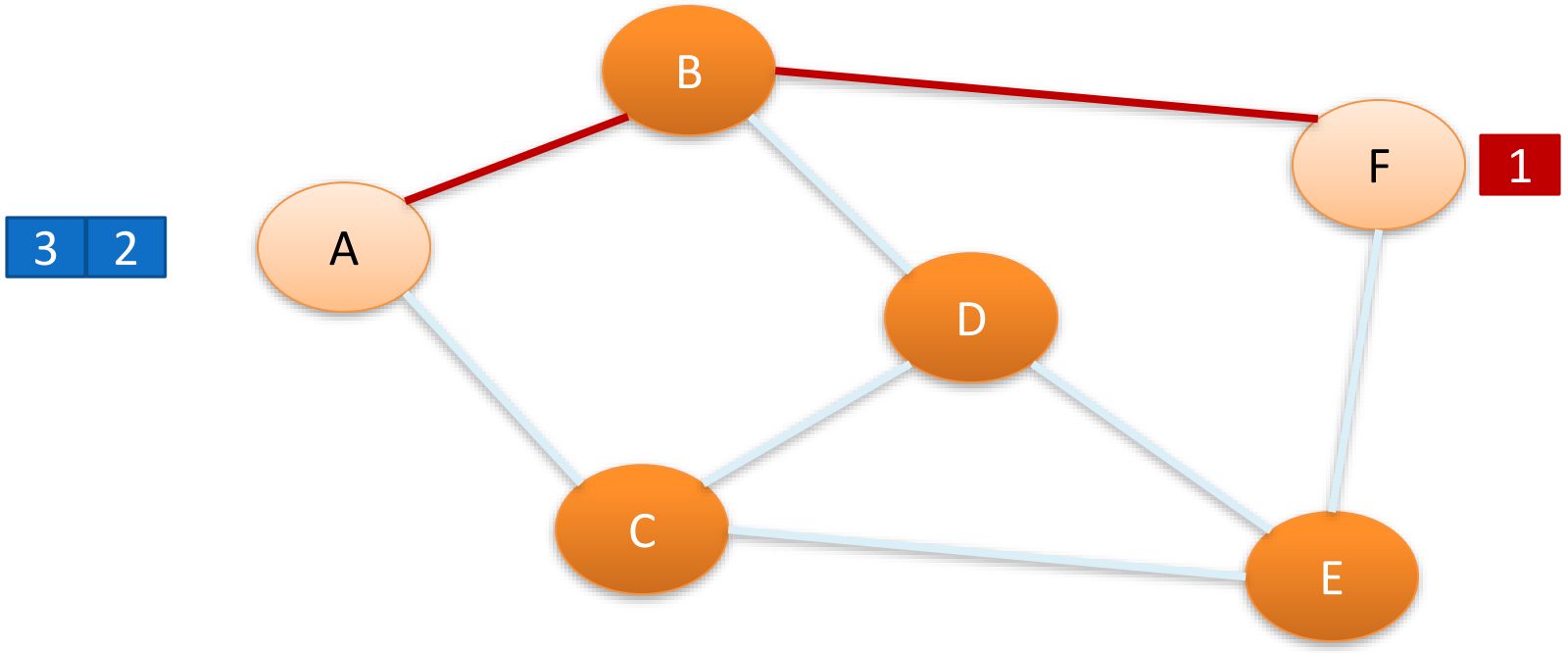
# Packet Switching

- Data split into packets
- Each packet is
  - Transported independently through network
  - Handled on a best efforts basis by each device
- Packets may
  - Follow different routes between the same endpoints
  - Be dropped by an intermediate device and never delivered

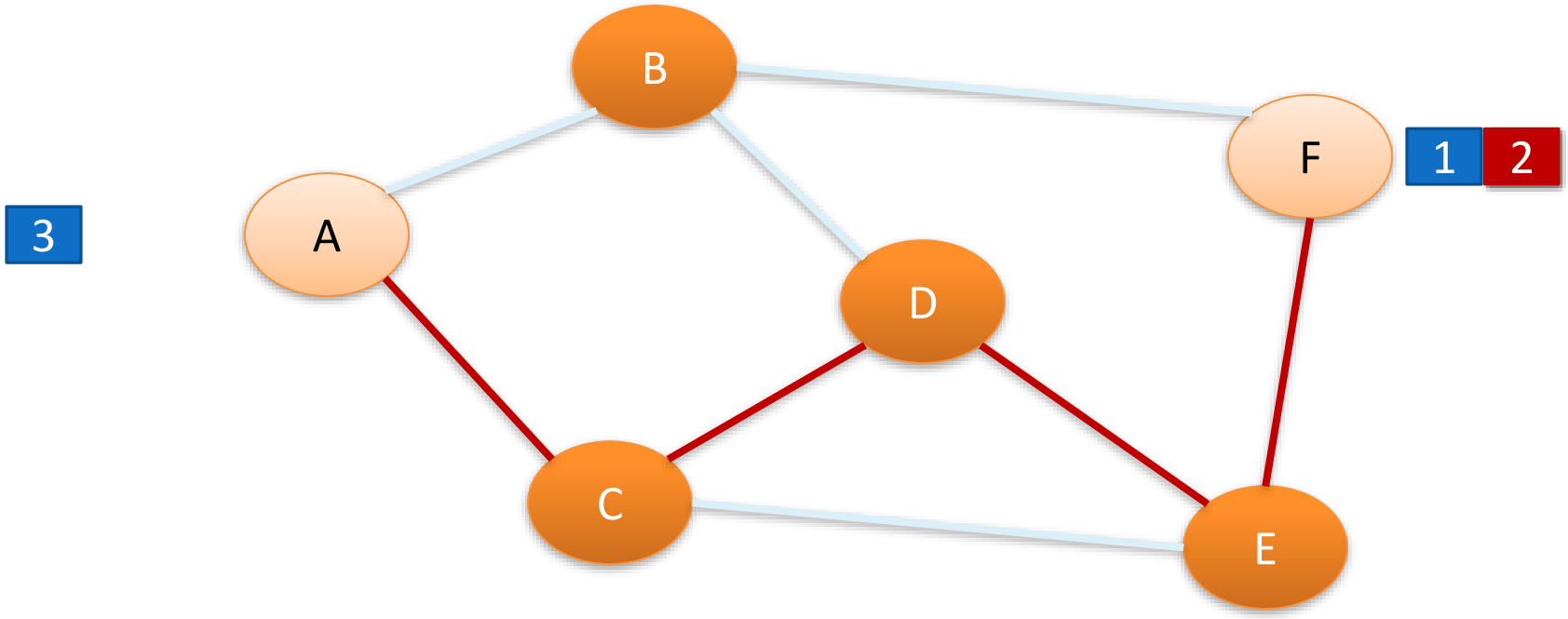
# Packet Switching



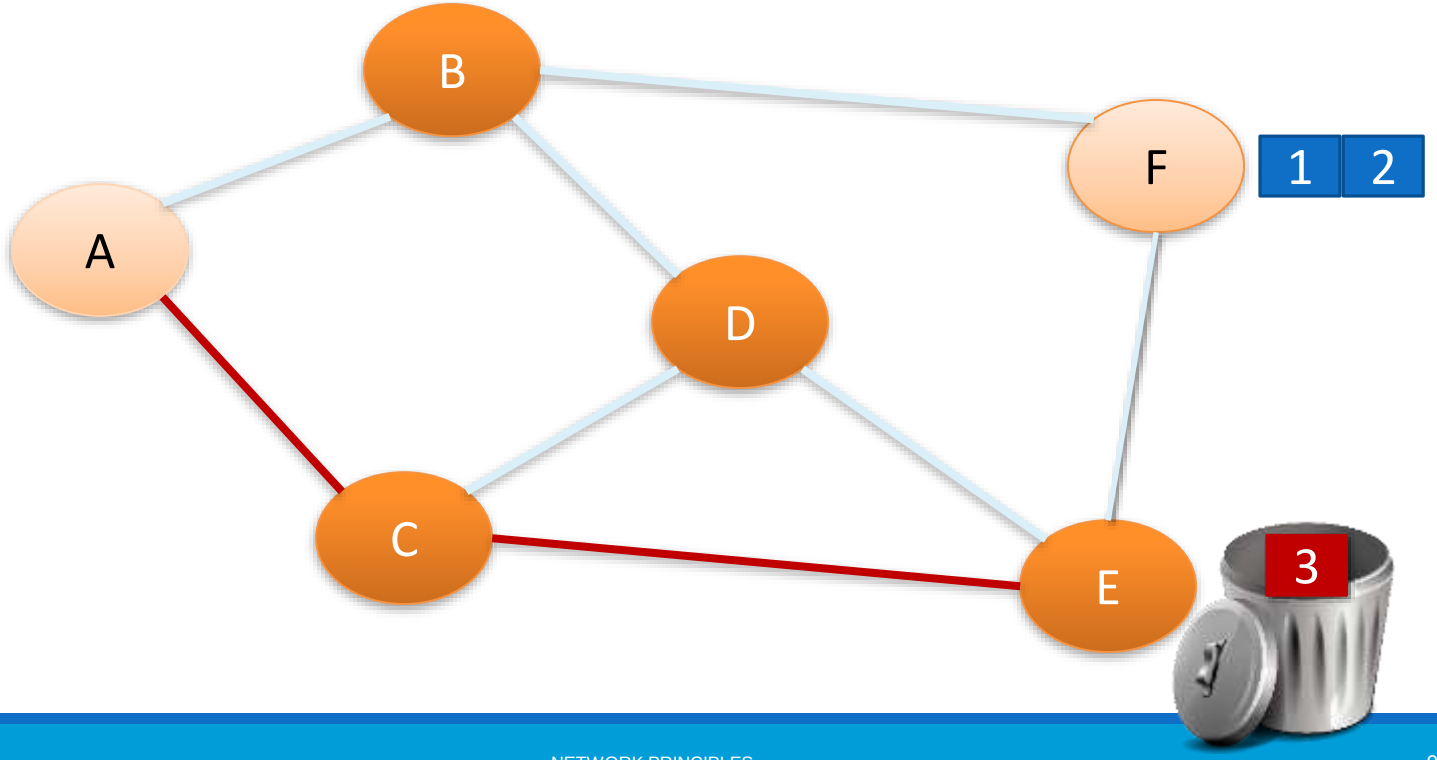
# Packet Switching



# Packet Switching



# Packet Switching



# Stack of Layers

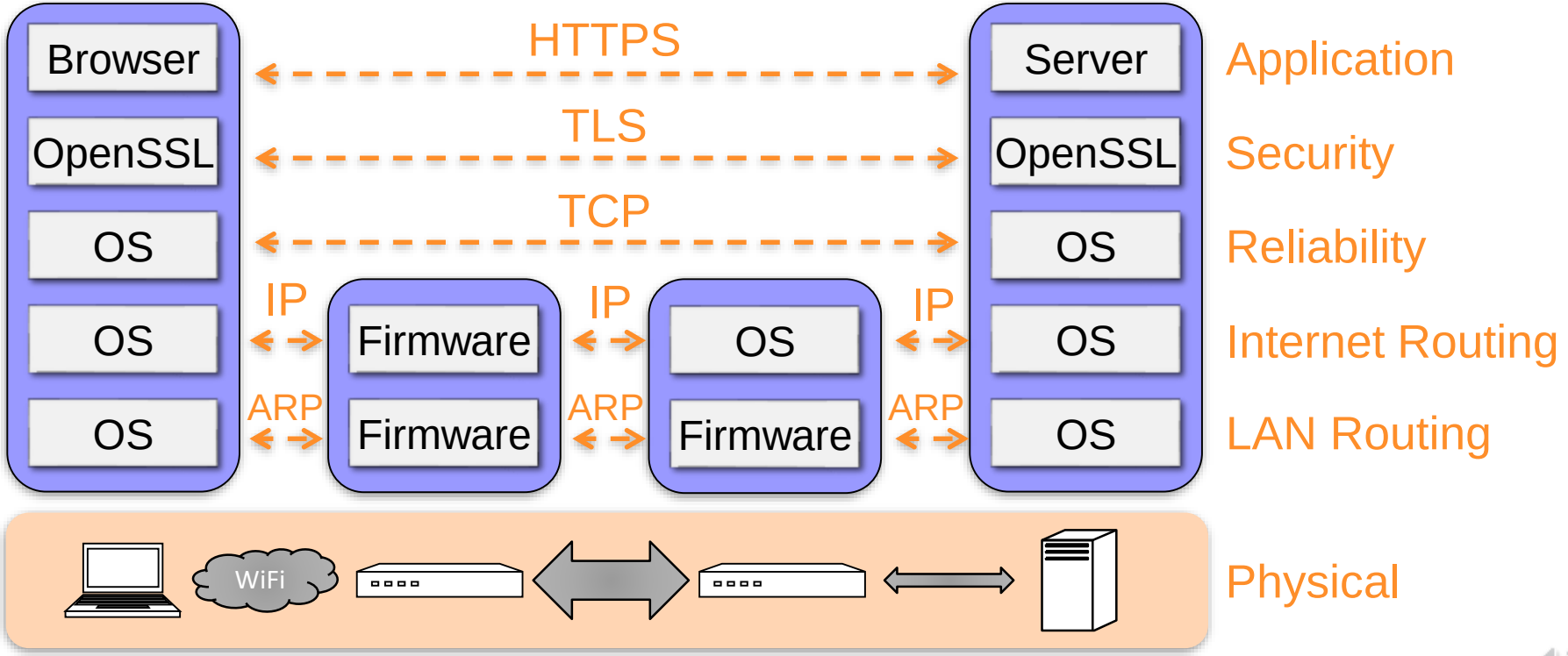
- Network communication models use a stack of layers
  - Higher layers use services of lower layers
  - Physical channel at the bottommost layer
- A network device implements several layers
- A communication channel between two devices is established for each layer
  - Actual channel at the bottom layer
  - Virtual channel at higher layers

# Think-pair-share

- **Think** quietly to yourself for 1 minute
- **Pair** and discuss with your neighbour for 3 minutes
- **Share** with the class – group discussion

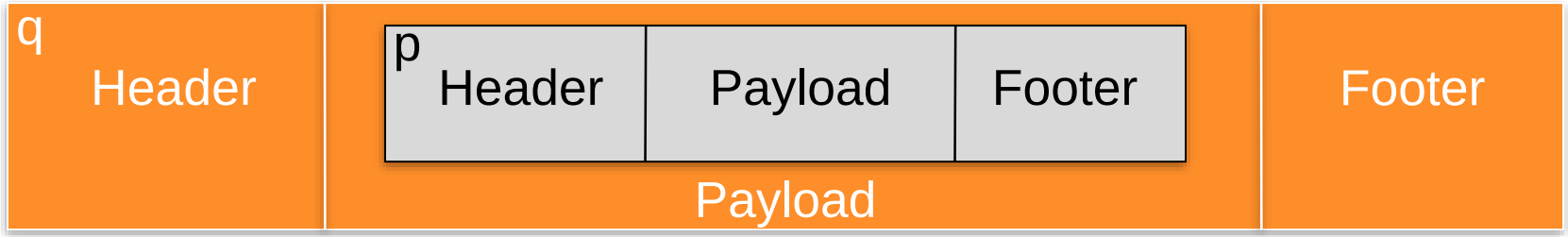
How does the physical network of the postal service differ from the Internet?
Are the principles of packet switching, layers, and encapsulation the same? Give examples.

# Internet Stack (simplified)

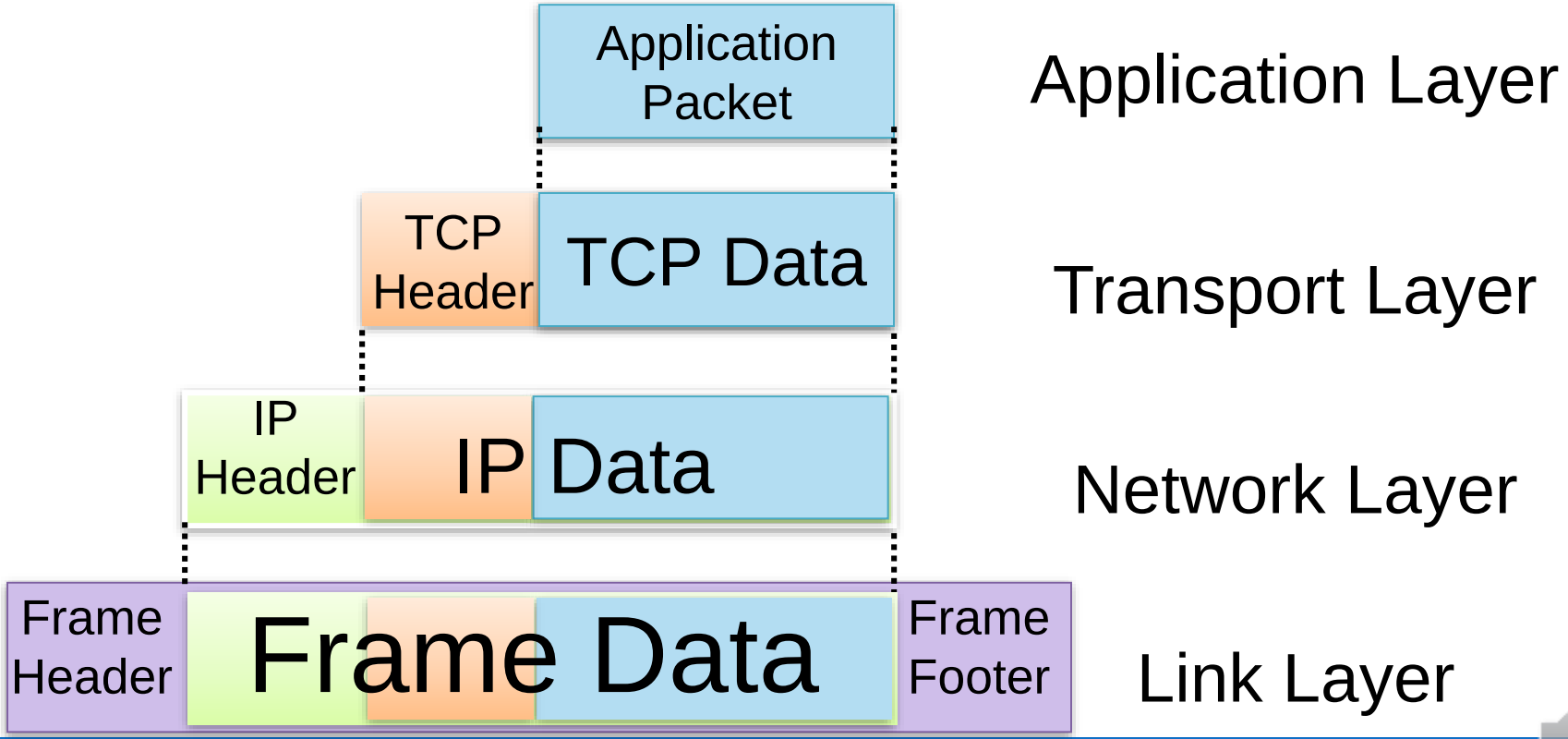


# Encapsulation

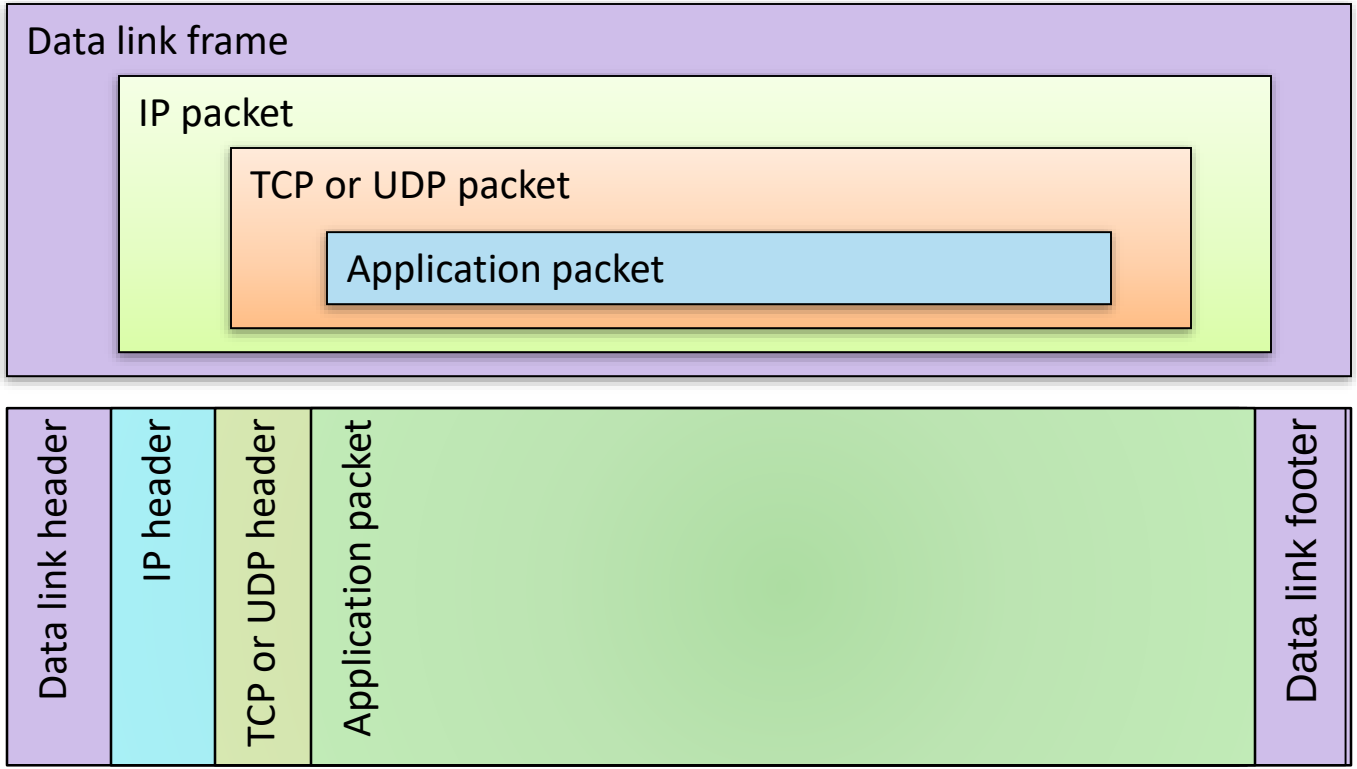
- A packet typically consists of
  - Control information: header and footer
  - Data: payload
- A protocol P uses the services of another protocol Q through encapsulation
  - A packet p of P is encapsulated into a packet q of Q
  - The payload of q is p
  - The control information of q is derived from that of p



# Internet Packet Encapsulation

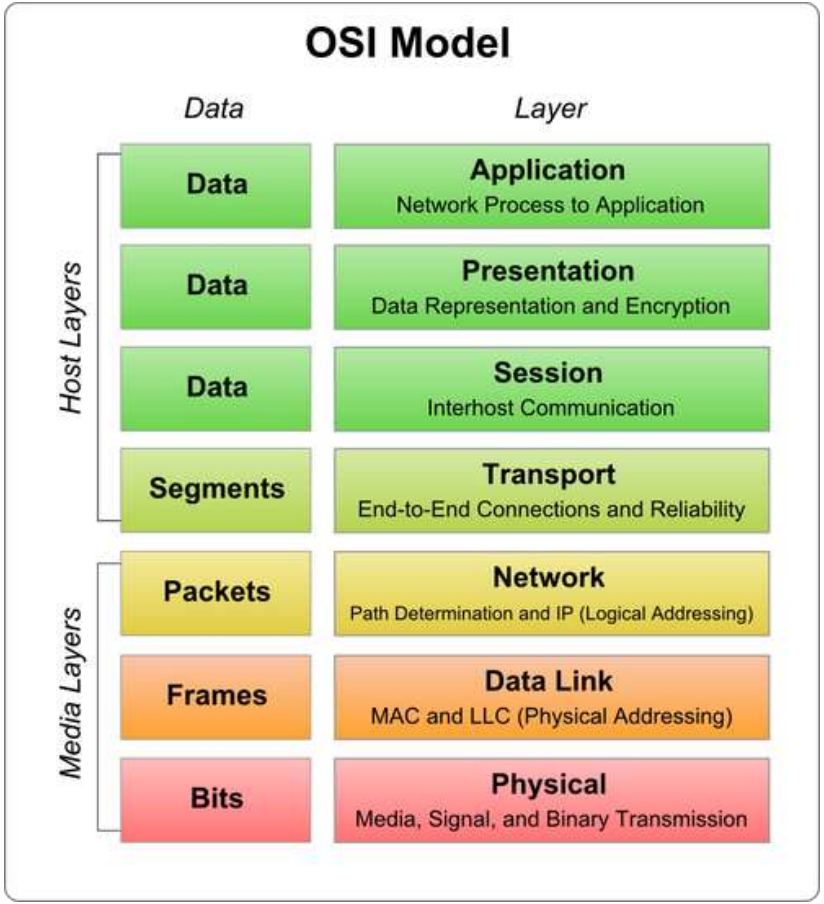


# Internet Packet Encapsulation

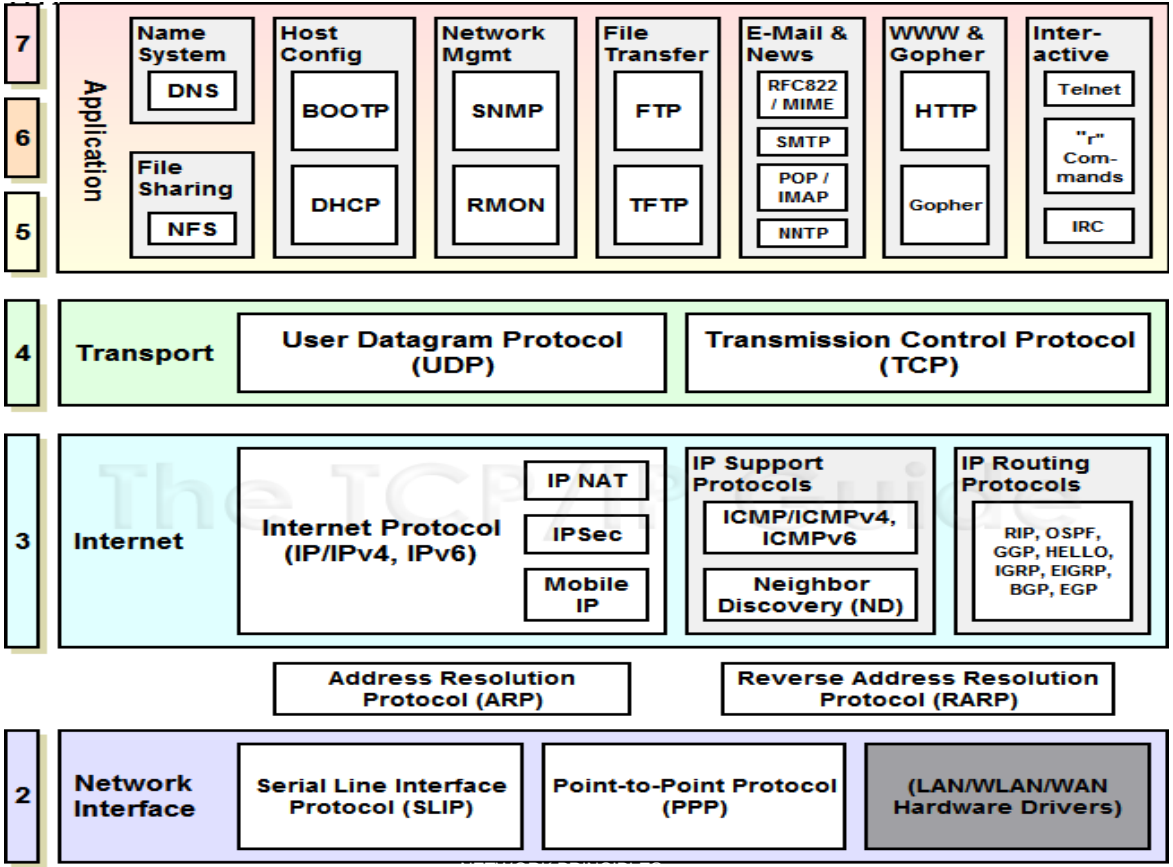


# The OSI Model

- The OSI (Open System Interconnect) Reference Model is a network model consisting of seven layers
- Created in 1983, OSI is promoted by the International Standard Organization (ISO)



# TCP/IP Model Mapped onto OSI



# Network Interfaces

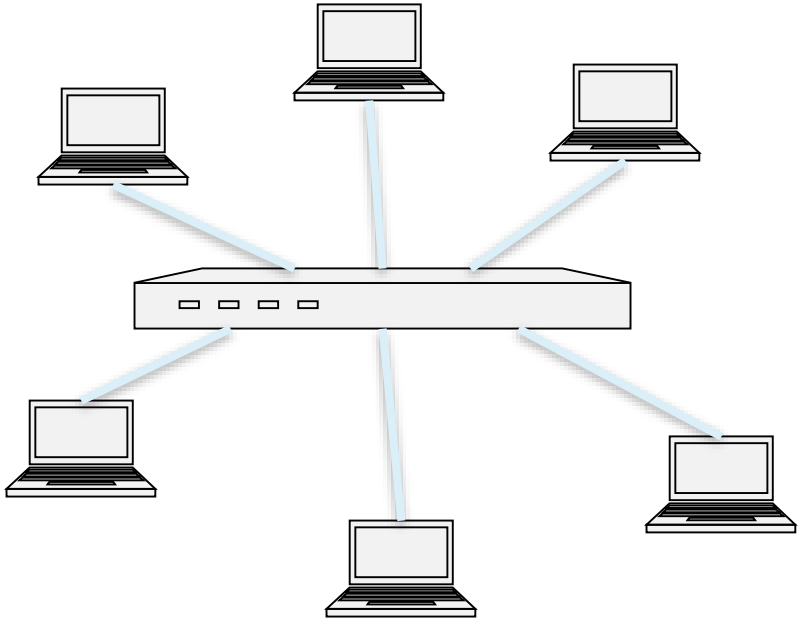
- Network interface: device connecting a computer to a network
  - Ethernet card
  - WiFi adapter
  - DSL modem
- A computer may have multiple network interfaces
- Packets transmitted between network interfaces
- Most local area networks, (including Ethernet and WiFi) broadcast frames

# Media Access Control (MAC) Addresses

- Most network interfaces come with a predefined MAC address
- A MAC address is a 48-bit number usually represented in hex
  - E.g., 00-1A-92-D4-BF-86
- The first three octets of any MAC address are IEEE-assigned Organizationally Unique Identifiers
  - E.g., Cisco 00-1A-A1, D-Link 00-1B-11, ASUSTek 00-1A-92, 00-0a-95 ??????
- The next three can be assigned by organizations as they please, with uniqueness being the only constraint

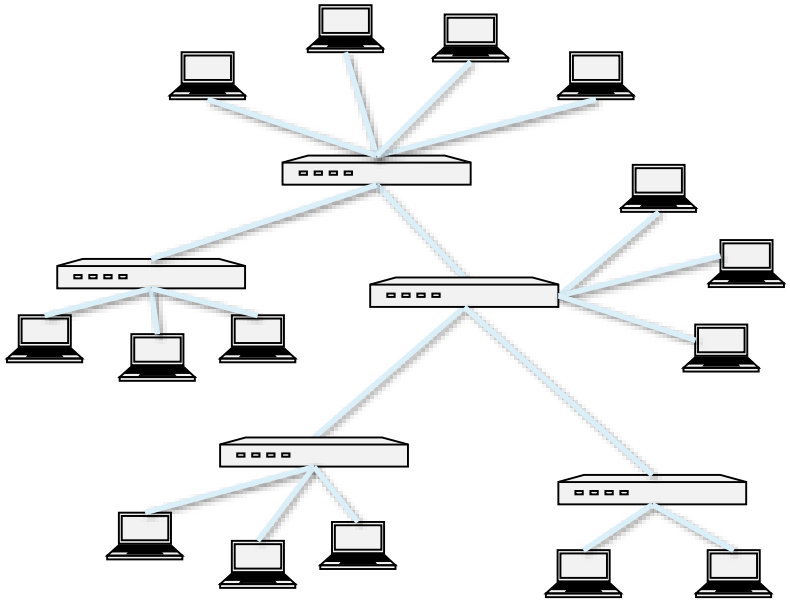
# Switch

- A switch performs routing in a local area network
  - Operates at the link layer
  - Has multiple interfaces, each connected to a computer/segment
- Operation of a switch
  - Learn the MAC address of each computer connected to it
  - Forward frames only to the destination computer

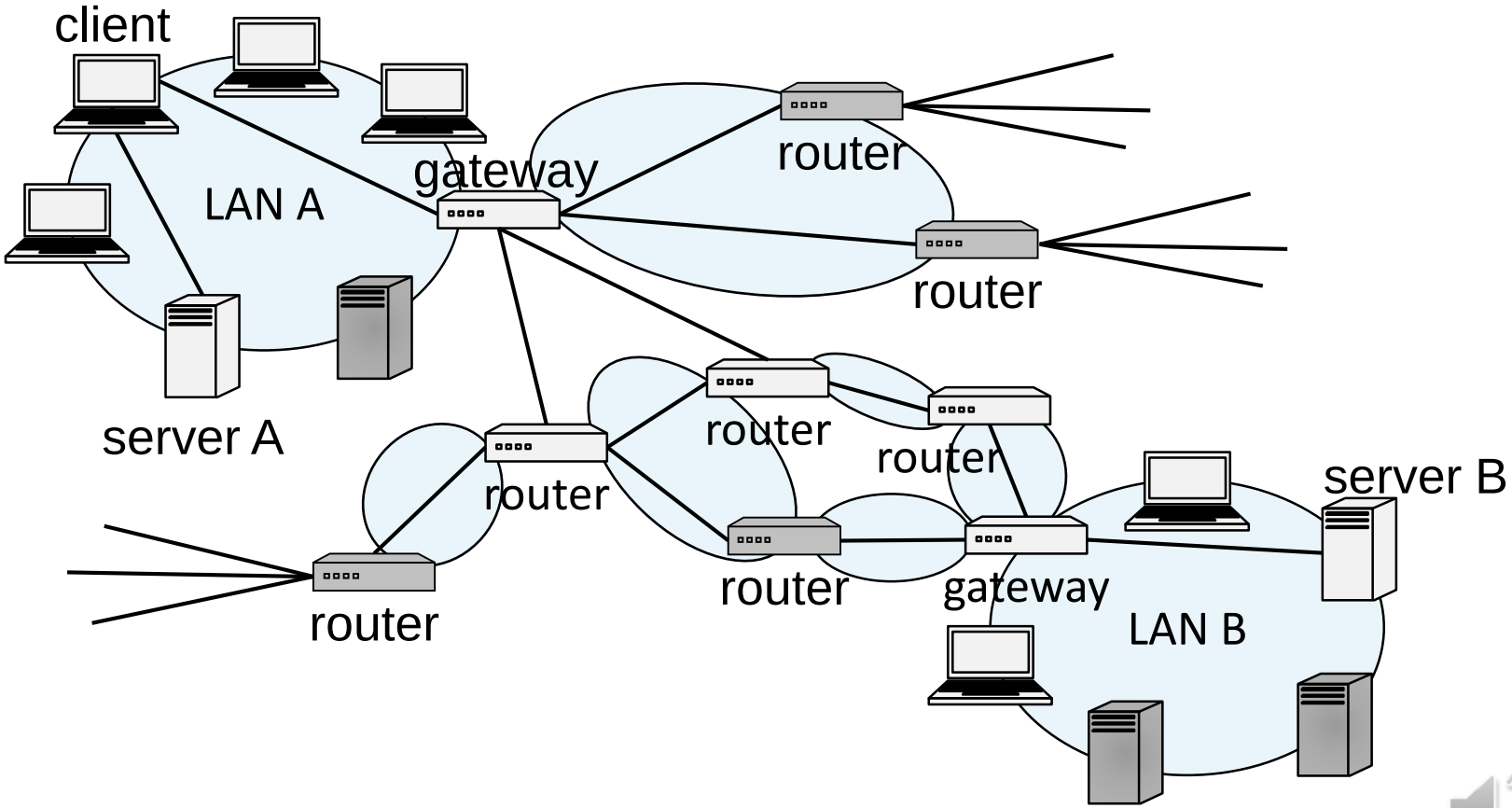


# Combining Switches

- Switches can be arranged into a tree
- Each forwards frames for the MAC addresses of the machines in the segments (subtrees) connected to it
- Frames to unknown MAC addresses are broadcast
- Frames to MAC addresses in the same segment as the sender are ignored

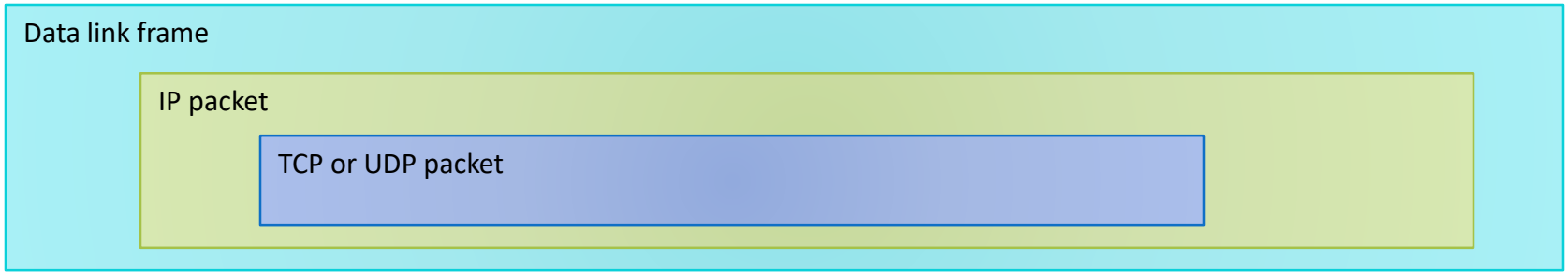


# The Internet



# Internet Protocol Functions

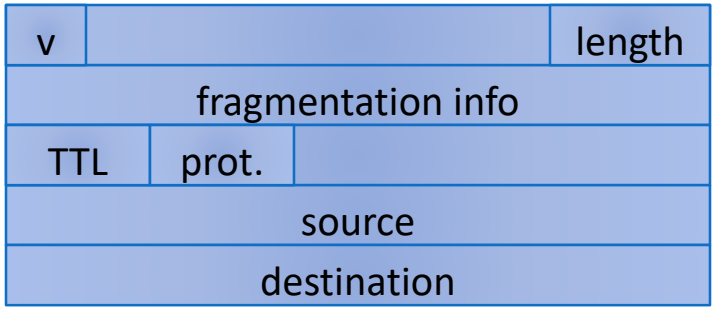
- Addressing: In order to deliver data, IP needs to be aware of where to deliver data to, and hence includes addressing systems
- Routing: IP might be required to communicate across networks, and communicate with networks not directly connected to the current network



# IP Addresses and Packets

- IP addresses
  - IPv4: 32-bit addresses
  - IPv6: 128-bit addresses
- Address subdivided into network, subnet, and host
  - E.g., 128.148.32.110
- Broadcast addresses
  - E.g., 128.148.32.255
- Private networks
  - not routed outside of a LAN
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16

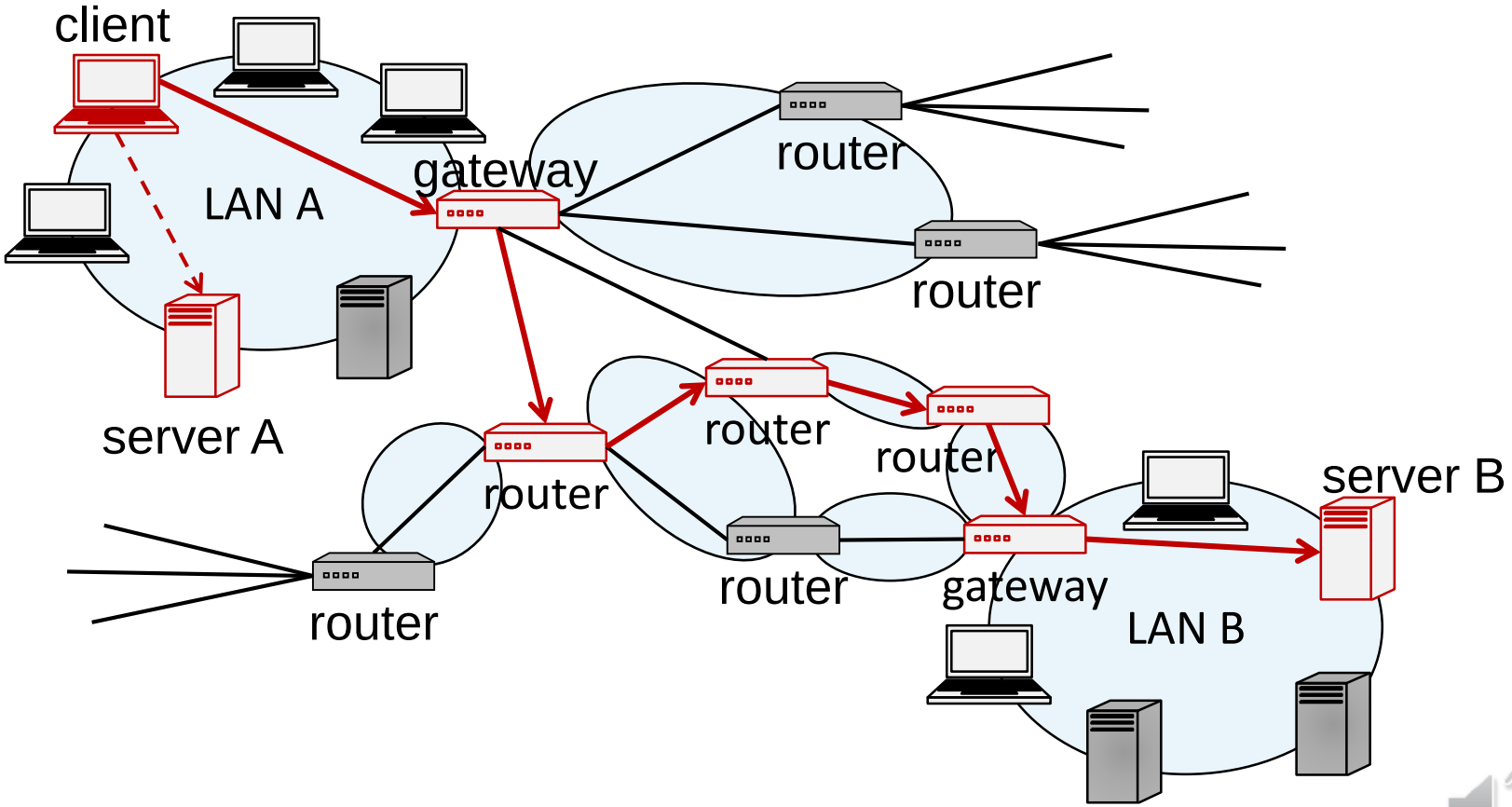
- IP header includes
  - Source address
  - Destination address
  - Packet length (up to 64KB)
  - Time to live (up to 255)
  - IP protocol version
  - Fragmentation information
  - Transport layer protocol information (e.g., TCP)



# IP Routing

- A router bridges two or more networks
  - Operates at the network layer
  - Maintains tables to forward packets to the appropriate network
  - Forwarding decisions based solely on the destination address
- Routing table
  - Maps ranges of addresses to LANs or other gateway routers

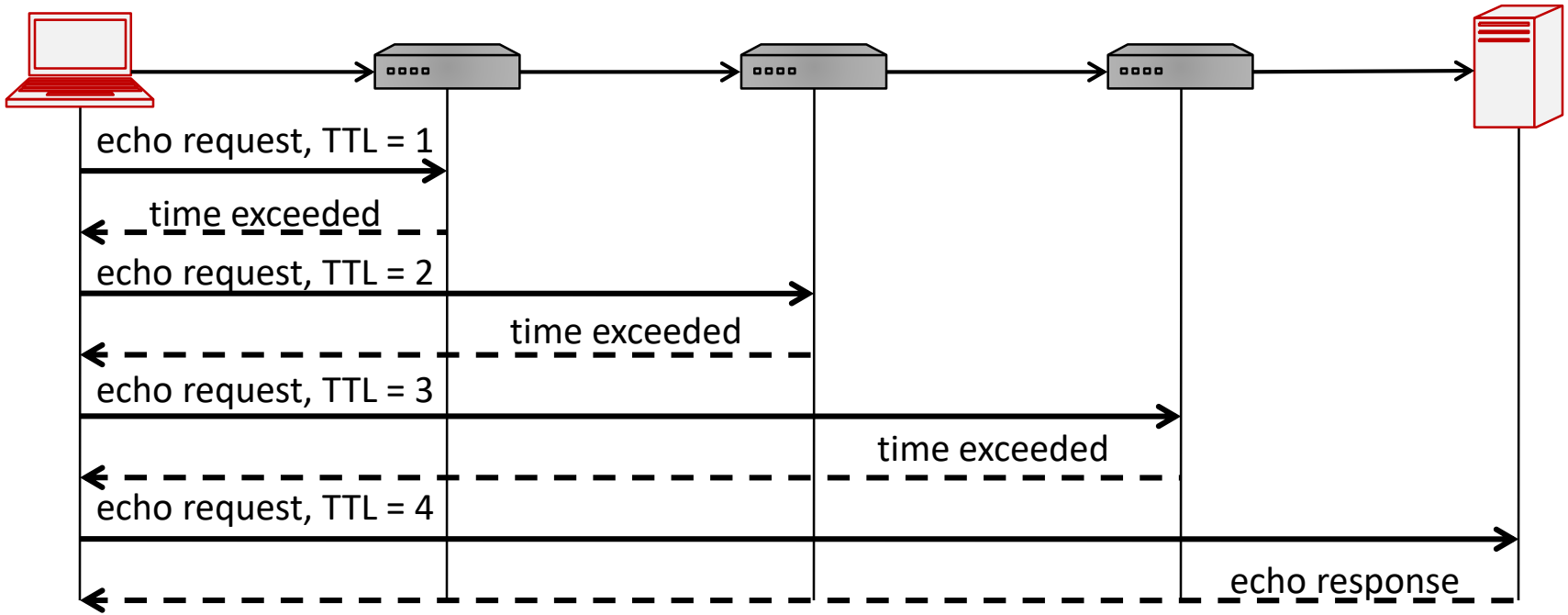
# Routing Examples



# Internet Routes

- Internet Control Message Protocol (ICMP)
  - Used for network testing and debugging
  - Simple messages encapsulated in single IP packets
  - Considered a network layer protocol
- Tools based on ICMP
  - Ping: sends series of echo request messages and provides statistics on roundtrip times and packet loss
  - Traceroute: sends series ICMP packets with increasing TTL value to discover routes

# Traceroute


echo request, TTL = 1
time exceeded
echo request, TTL = 2
time exceeded
echo request, TTL = 3
time exceeded
echo request, TTL = 4
echo response

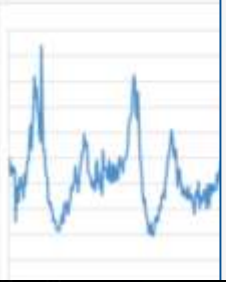
# A real world example

## How Syria Turned Off the Internet

*29 Nov 2012 by Matthew Prince.*

LinkedIn Like Tweet

Today, 29 November 2012, between 1026 and 1028 (UTC), all traffic from Syria to the rest of the Internet stopped. At CloudFlare, we witnessed the drop off. We've spent the morning studying the situation to understand what happened. The following graph shows the last several days of traffic coming to CloudFlare's network from Syria.



## What Happened?

The Syrian Minister of Information is being reported as saying that the government did not disable the Internet, but instead the outage was caused by a cable being cut. Specifically: "It is not true that the state cut the Internet. The terrorists targeted the Internet lines, resulting in some regions being cut off." From our investigation, that appears unlikely to be the case.

To begin, all connectivity to Syria, not just some regions, has been cut. The exclusive provider

https://blog.cloudflare.com/how-syria-turned-off-the-internet/

THE VERGE TECH SCIENCE CULTURE CARS REVIEWS LONGFORM VIDEO MORE

US & WORLD

## NSA was responsible for 2012 Syrian internet blackout, Snowden says

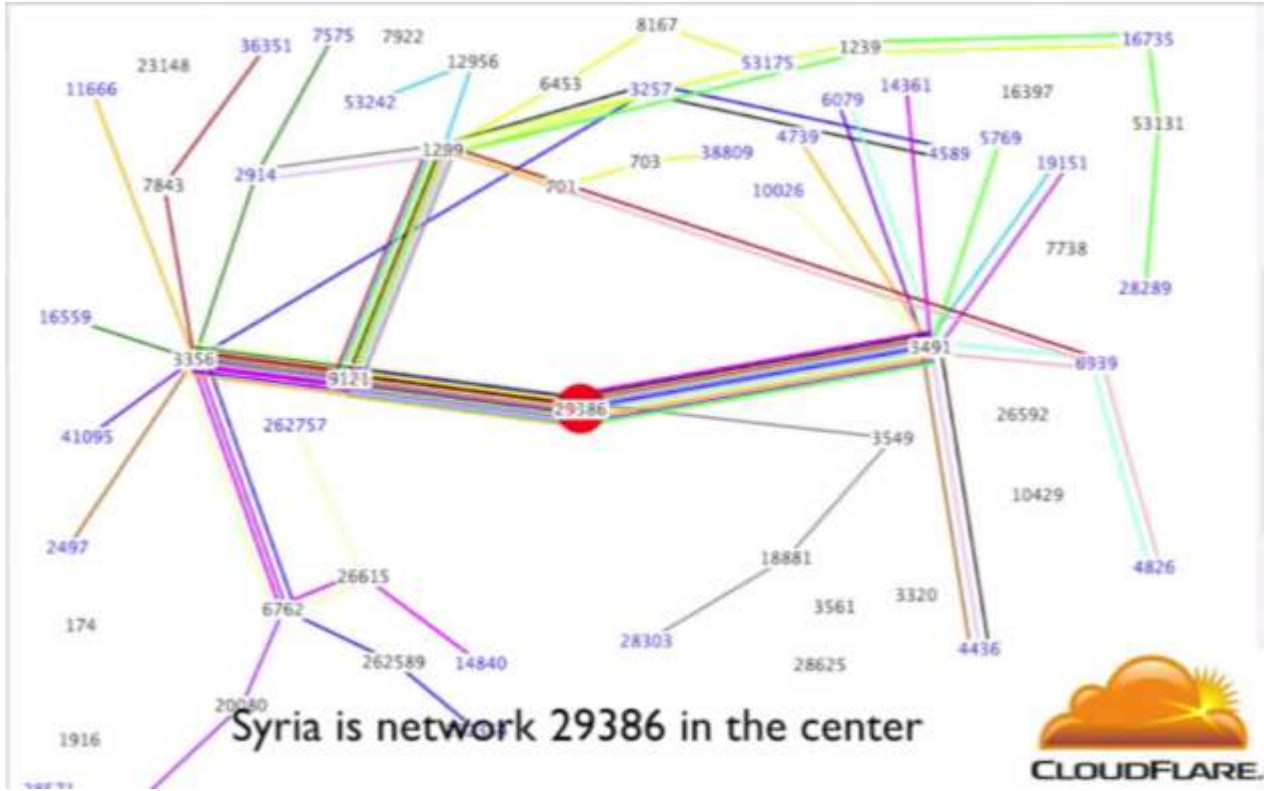
85

*An elite hacking unit broke a router*

By Jacob Kastrenakes | @jake_k | Aug 13, 2014, 10:28am EDT

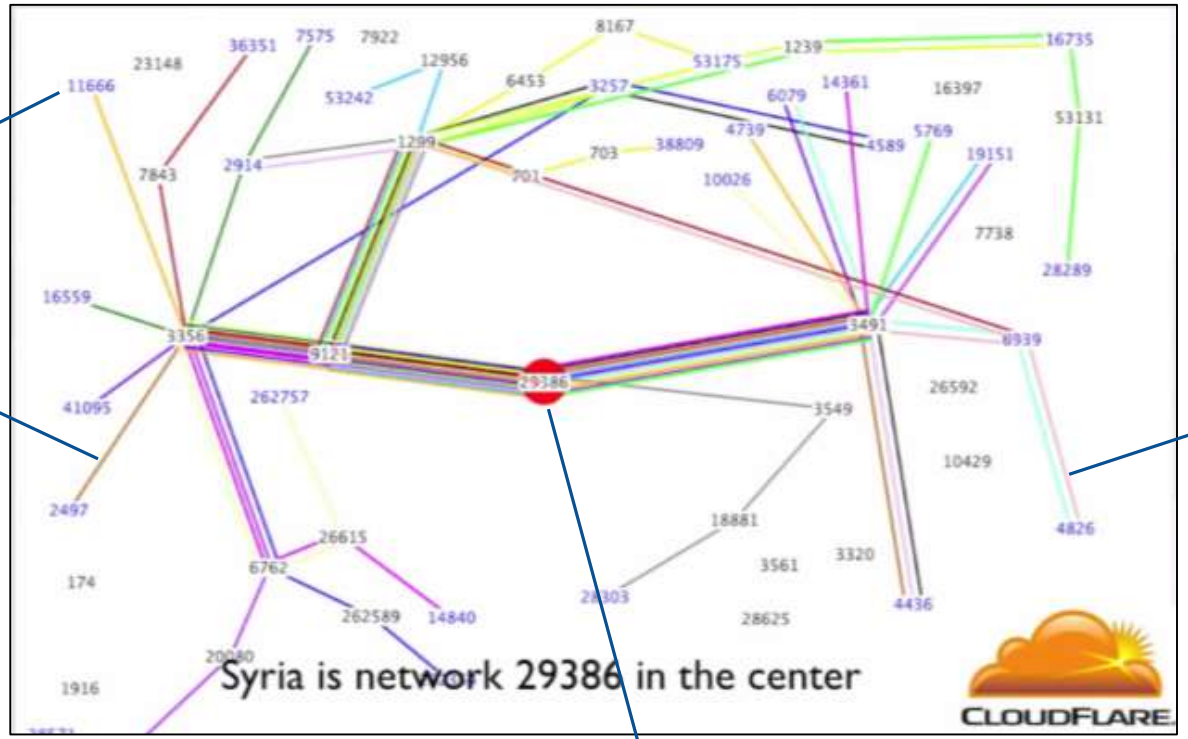
# Syria going offline – November 2012

- Article: https://blog.cloudflare.com/how-syria-turned-off-the-internet/
- Going offline: https://player.vimeo.com/video/54630037
- Going online: https://player.vimeo.com/video/54670123



Each number is an AS, which is a network run by a single group.

Each colored line is the current shortest path between two AS's. All lines on this graph connect Syria to other parts of the world.

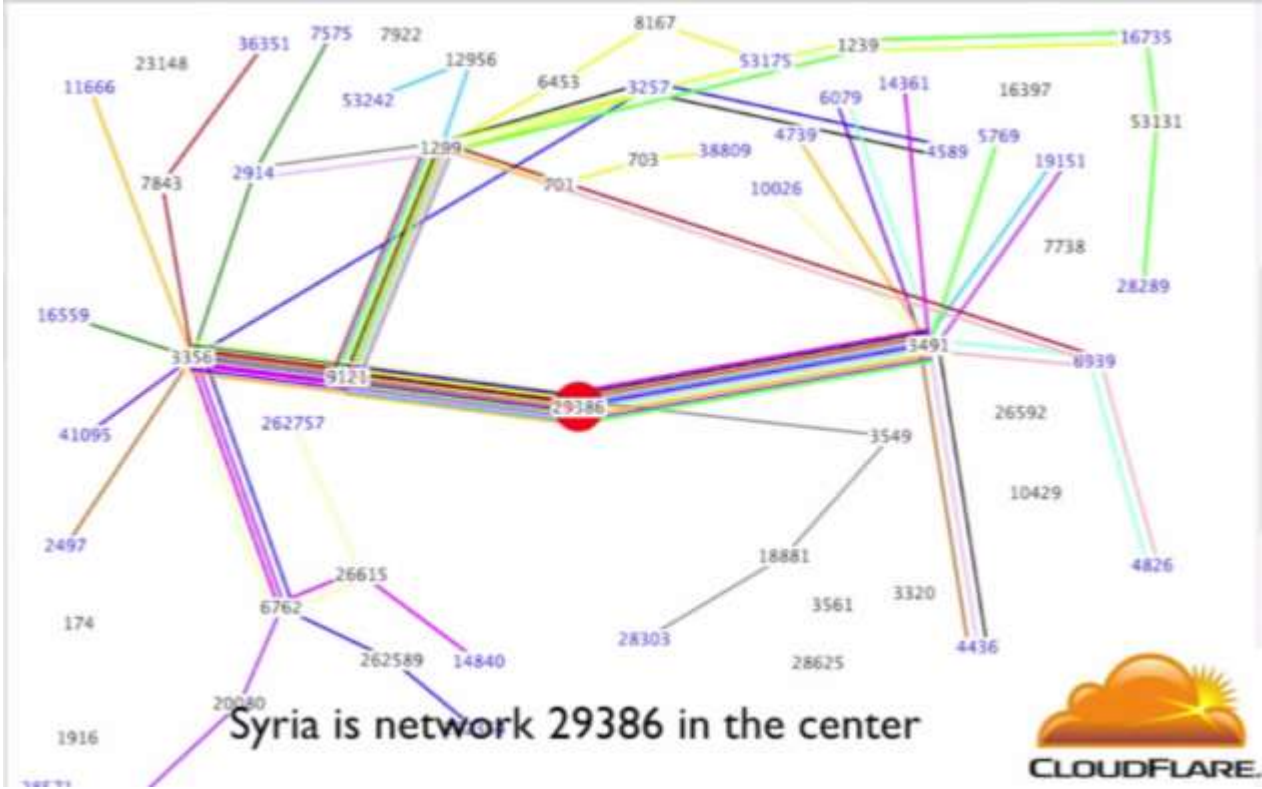



Paths shift all the time. This is normal on the internet as the current shortest path is dynamically negotiated (BGP routing).

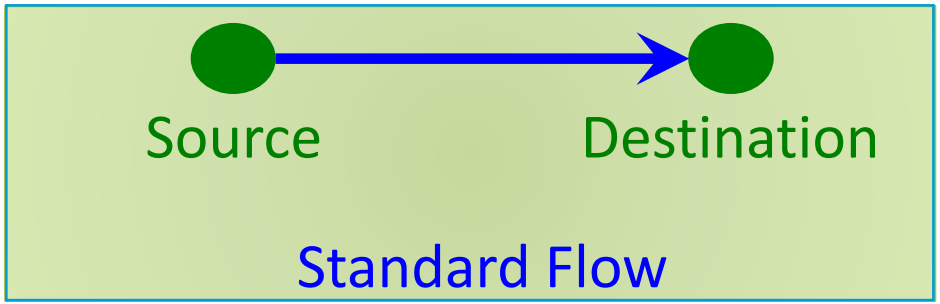
Syria's AS is, directly connected to three other AS's.

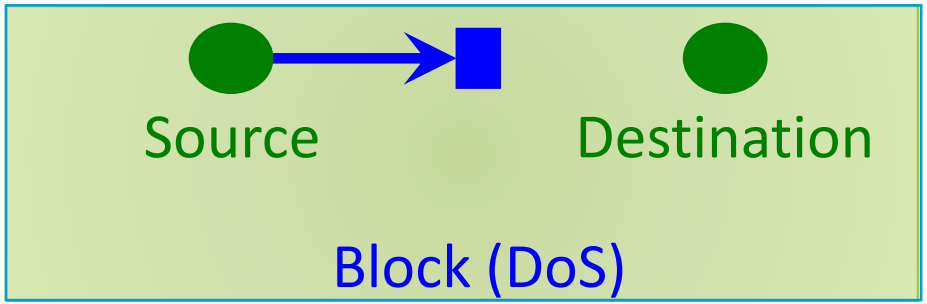
# Syria going offline – November 2012

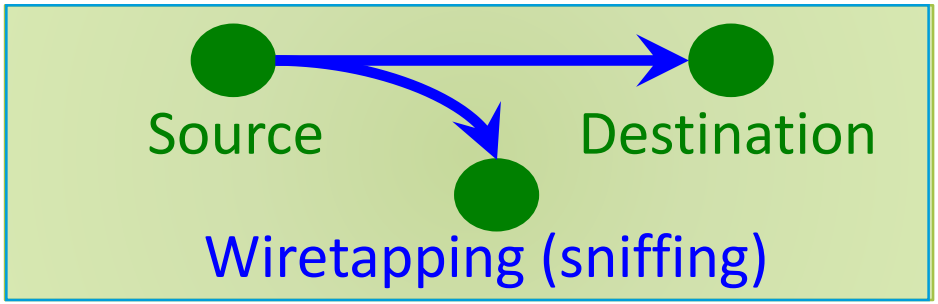
- Article: https://blog.cloudflare.com/how-syria-turned-off-the-internet/
- Going offline: https://player.vimeo.com/video/54630037
- Going online: https://player.vimeo.com/video/54670123

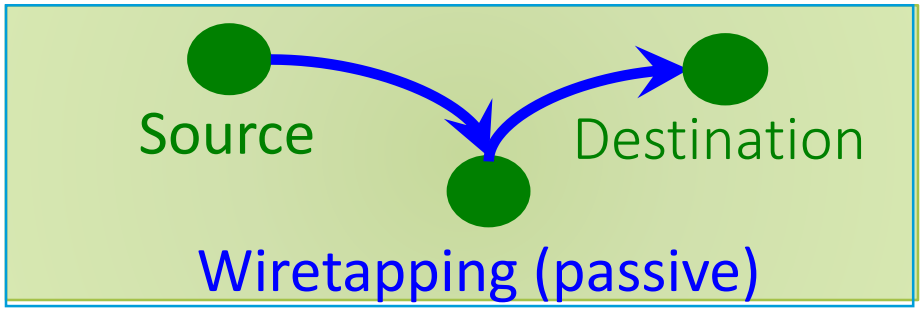


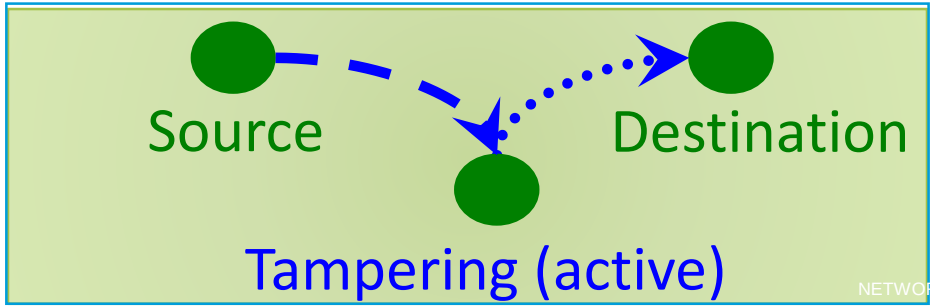
# Network Attacks

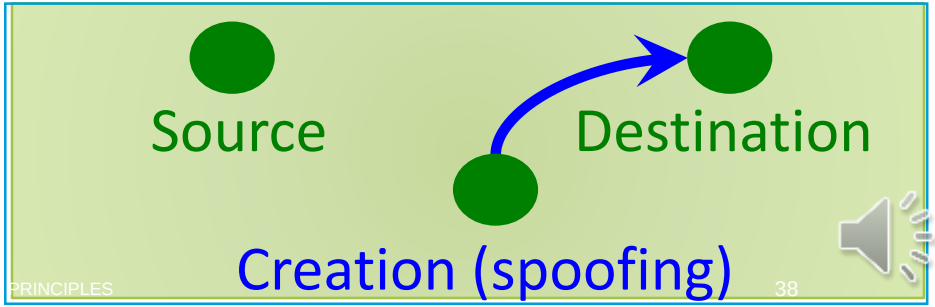


# Wireshark

- Packet sniffer and protocol analyzer
- Captures and displays network packets for analysis
- Supports plugins
- Usually requires administrator privileges because of security risks associated with the program
- When run in promiscuous mode, captures traffic across the network
- Freely available on www.wireshark.org