Network security: Networking Principles

COMPUTER SECURITY

TARIQ ELAHI

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

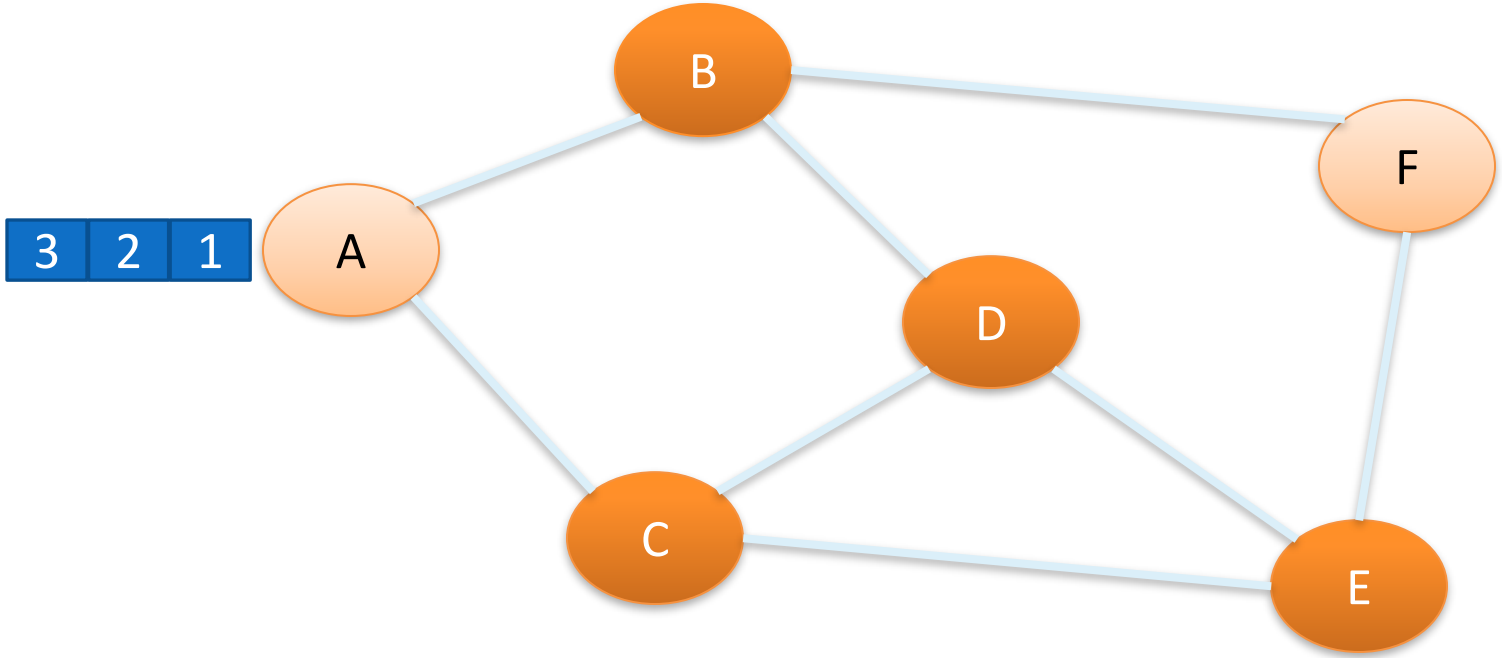
Network Communication

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

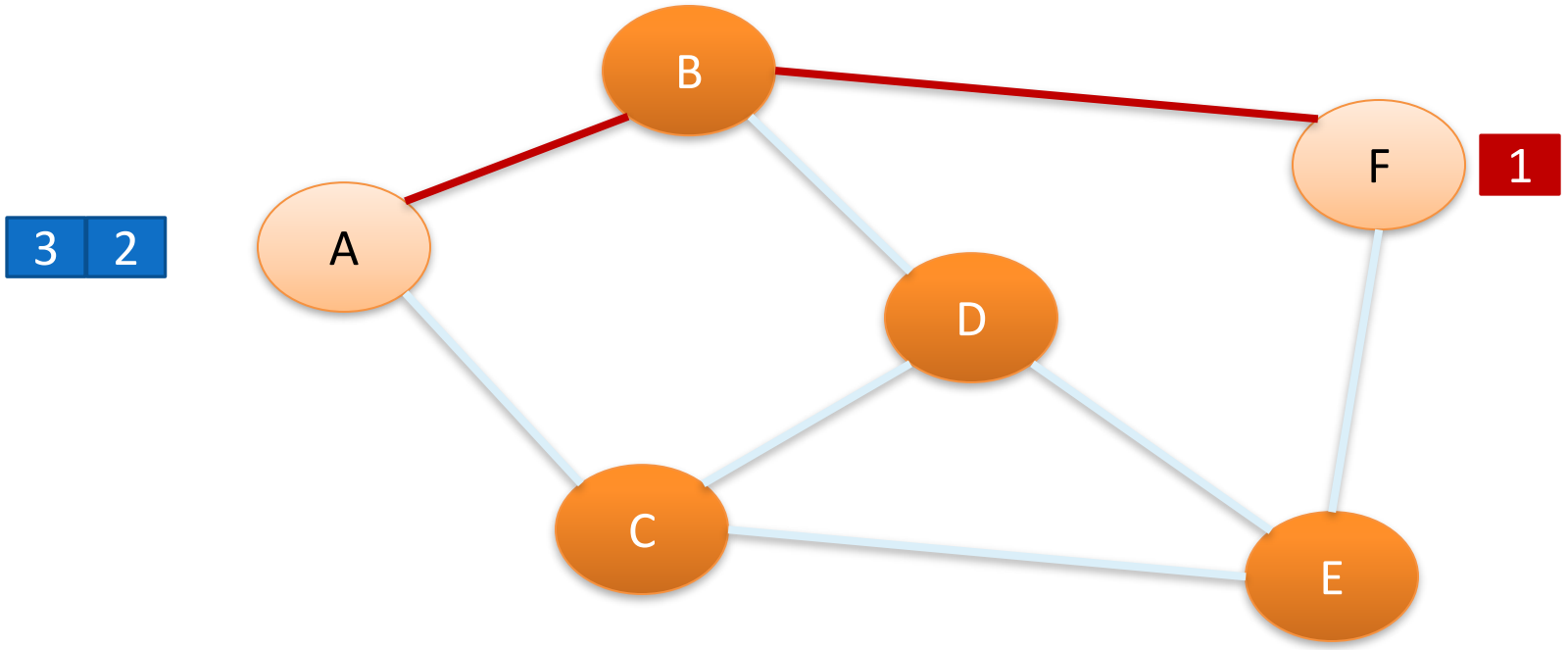
Packet Switching

- 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

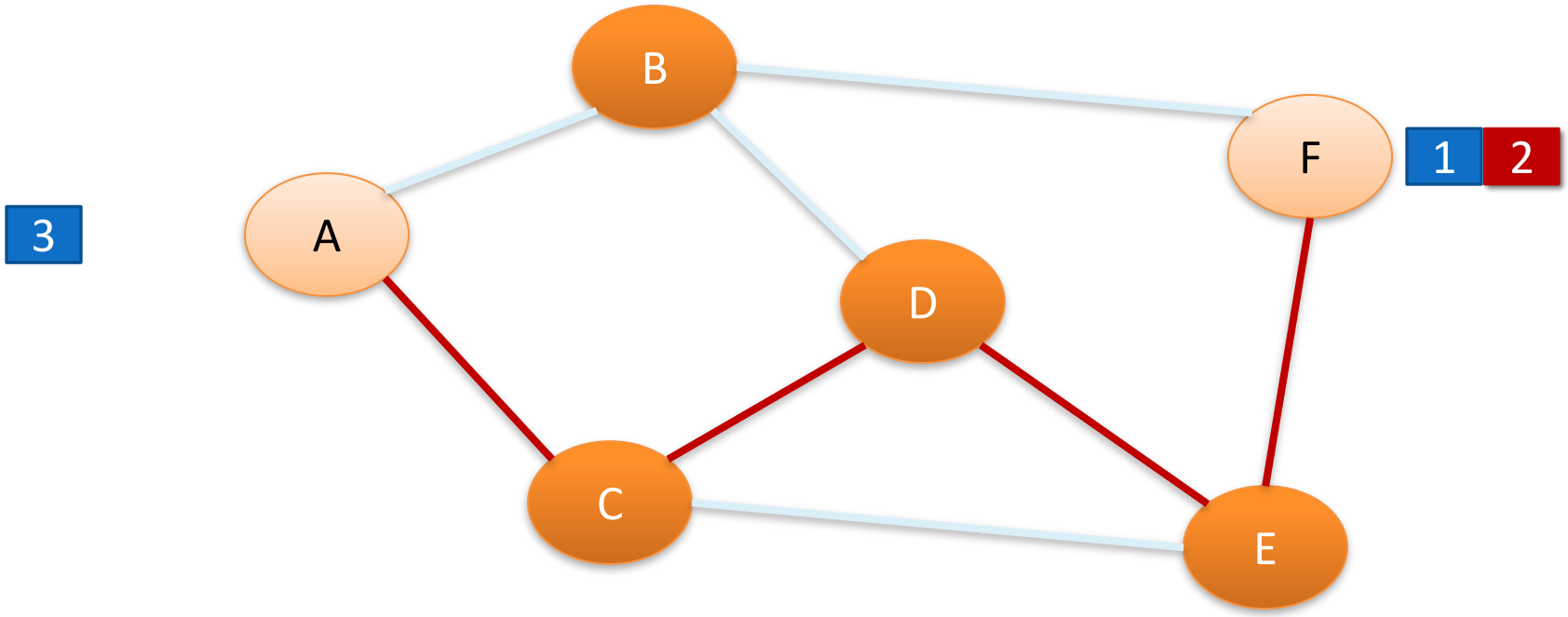
Packet Switching



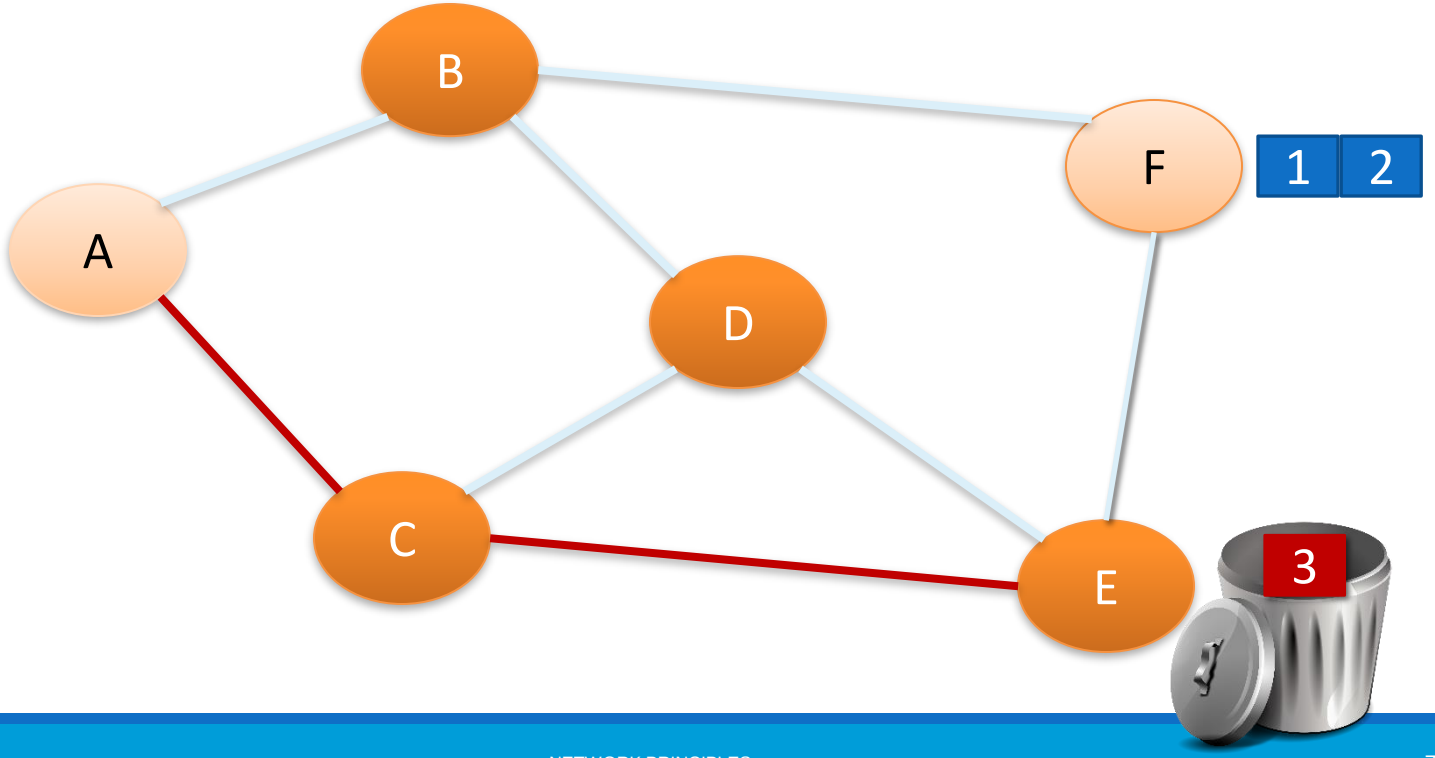
Packet Switching



Packet Switching



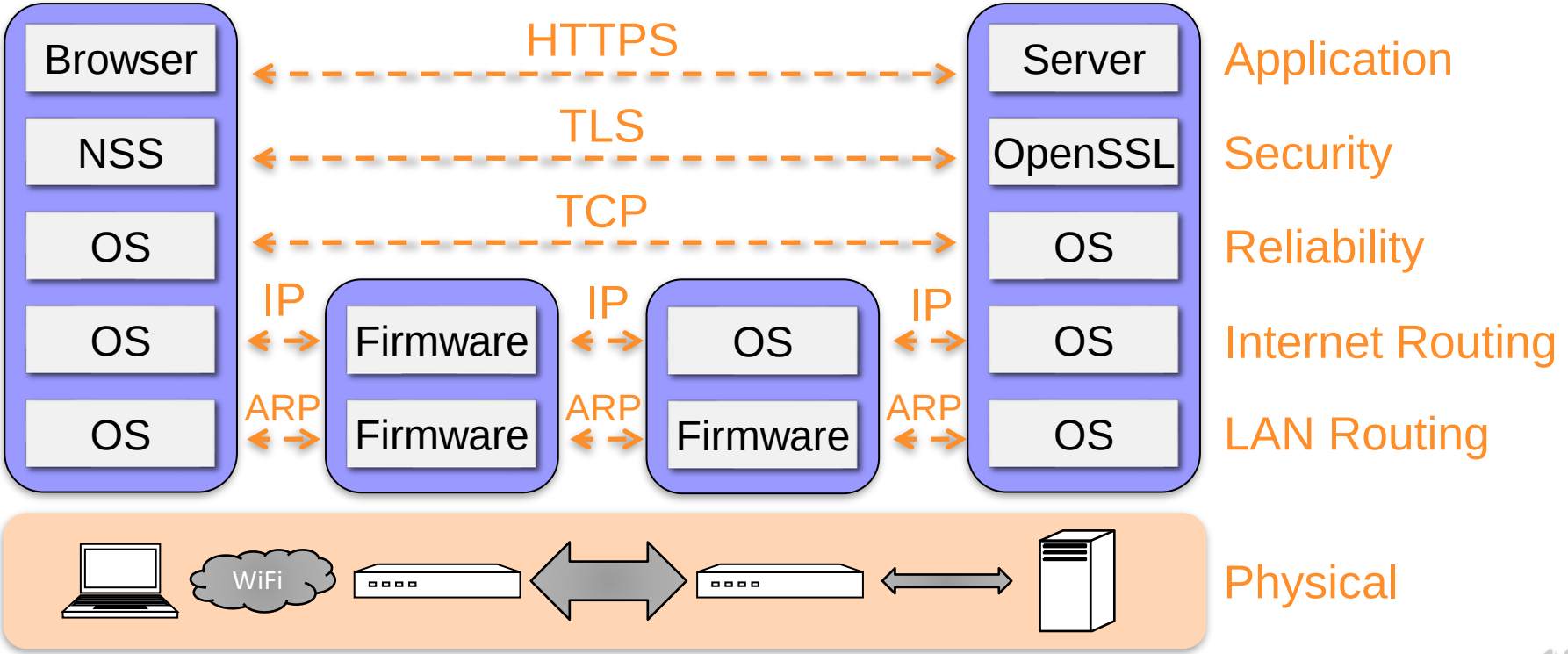
Packet Switching



Stack of Layers

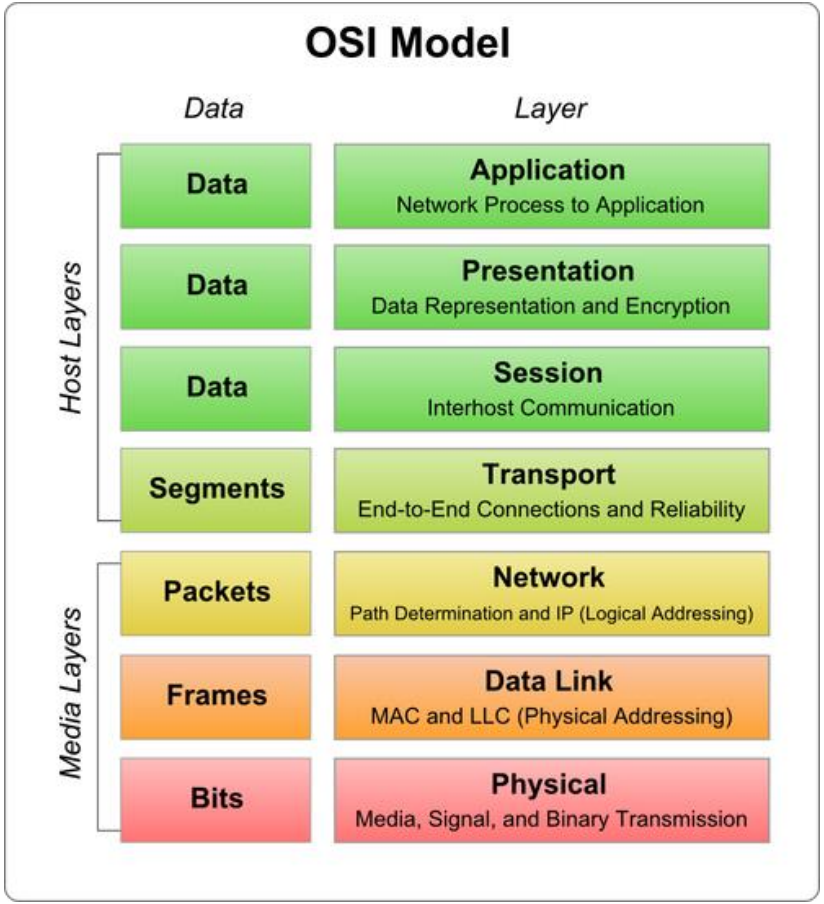
- Network communication models use a stack of layers
  - Higher layers use services of lower layers
  - Physical channel at the bottommost layer
- A network device implements several layers
- A communication channel between two devices is established for each layer
  - Actual channel at the bottom layer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

Internet Stack (simplified)

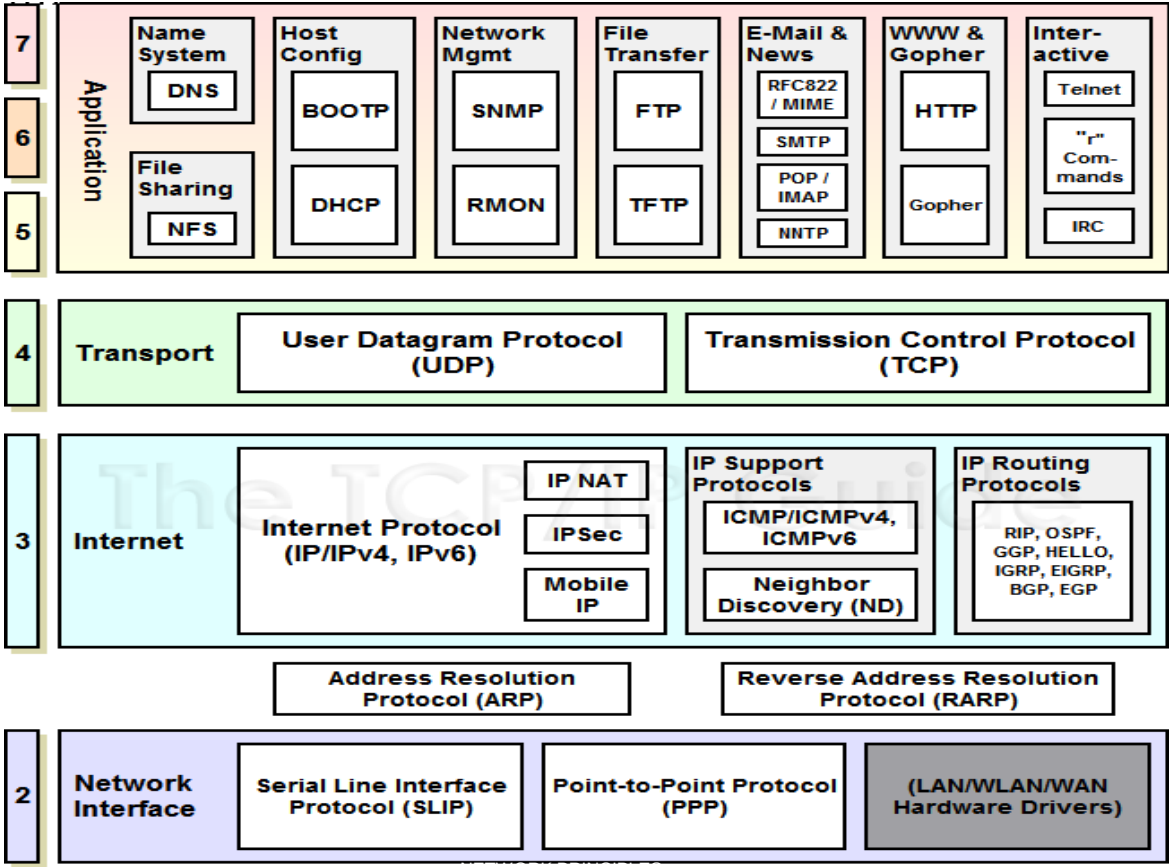


The OSI Model

- 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)

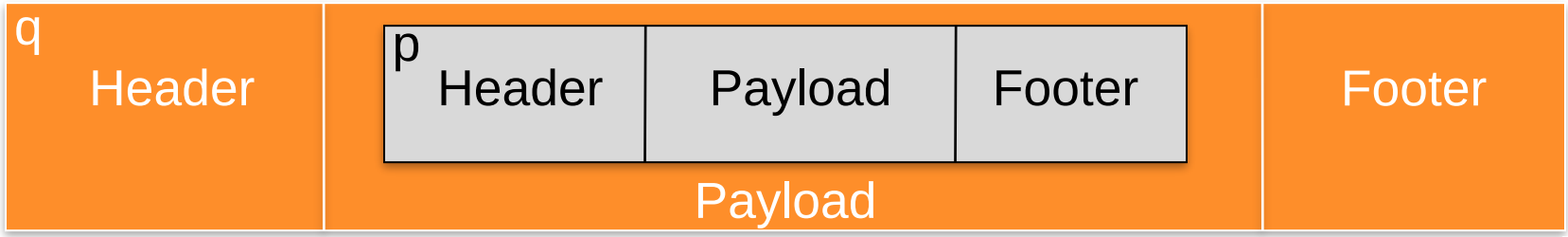


TCP/IP Model Mapped onto OSI

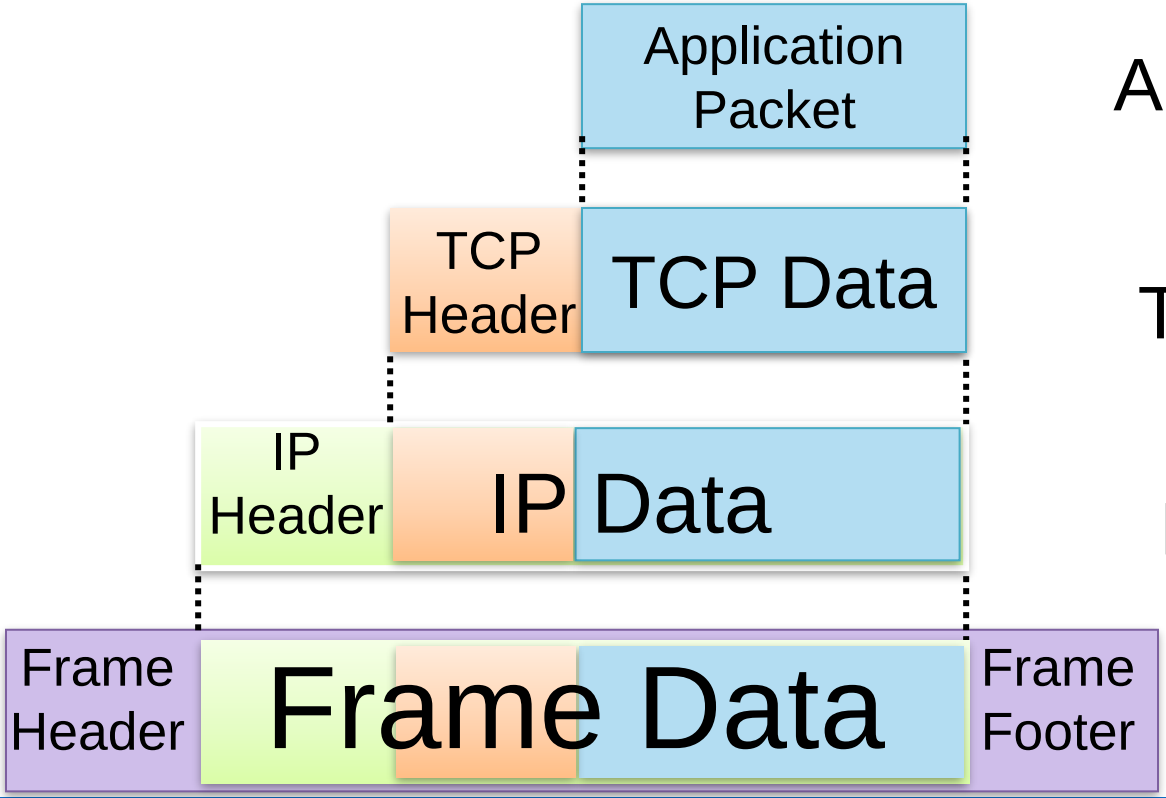


Encapsulation

- 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



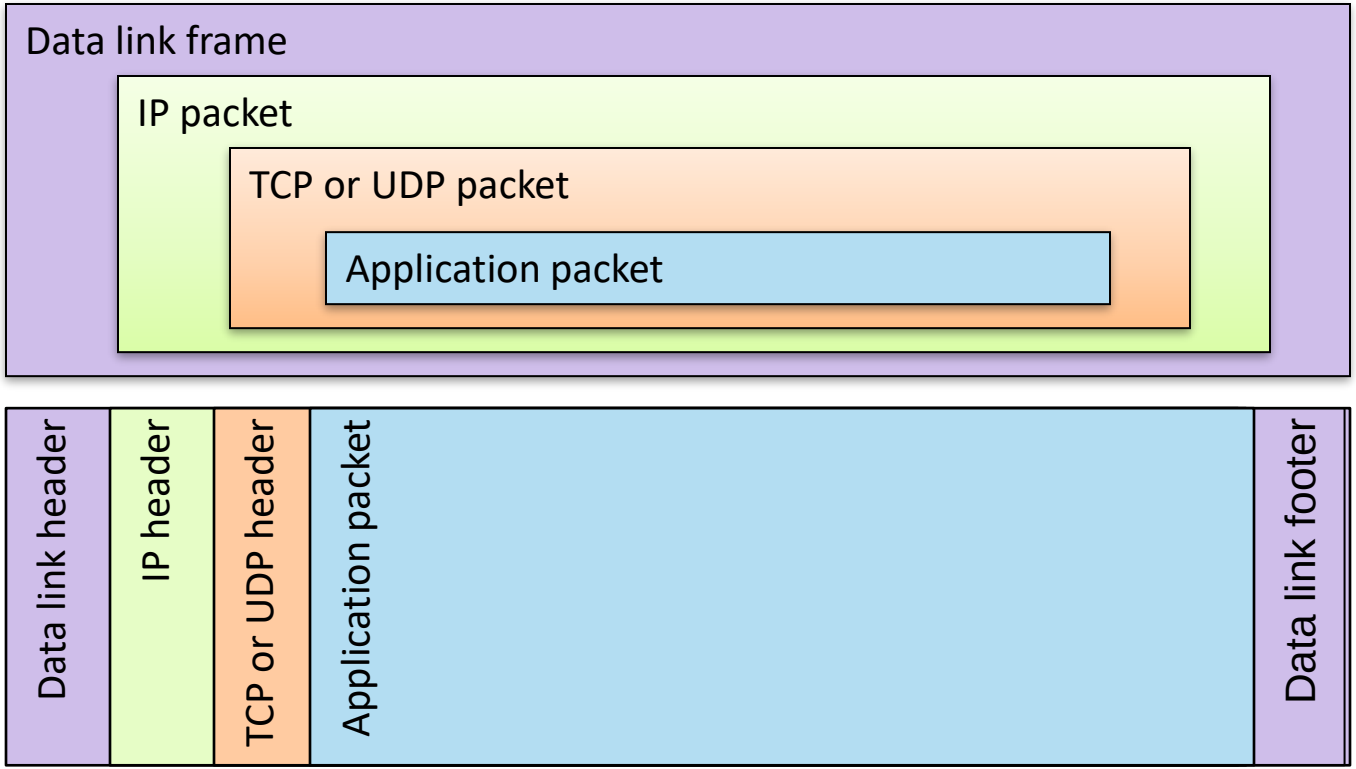
Application Layer

Transport Layer

Network Layer

Link Layer

Internet Packet Encapsulation



Network Interfaces

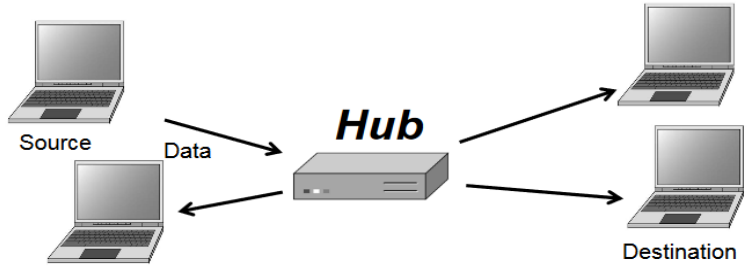
- Network interface: device connecting a computer to a network
  - Ethernet card
  - WiFi adapter
  - DSL modem
- A computer may have multiple network interfaces
- Packets transmitted between network interfaces
- Most local area networks, (including Ethernet and WiFi) broadcast frames

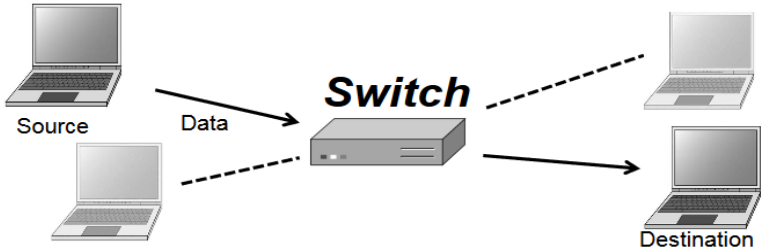
Media Access Control (MAC) Addresses

- 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

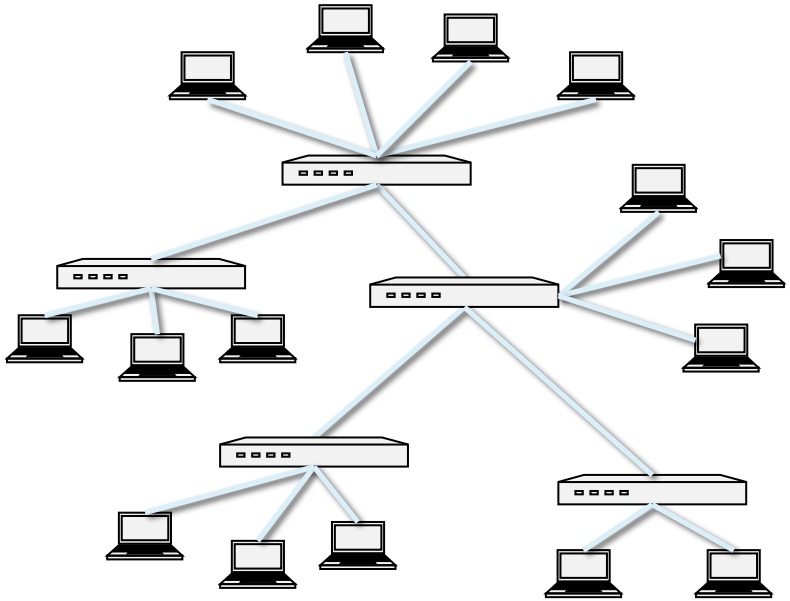
- A switch performs routing in a local area network
  - Operates at the link layer
  - Has multiple interfaces, each connected to a computer/segment
- Operation of a switch
  - Learn the MAC address of each computer connected to it
  - Forward frames only to the destination computer



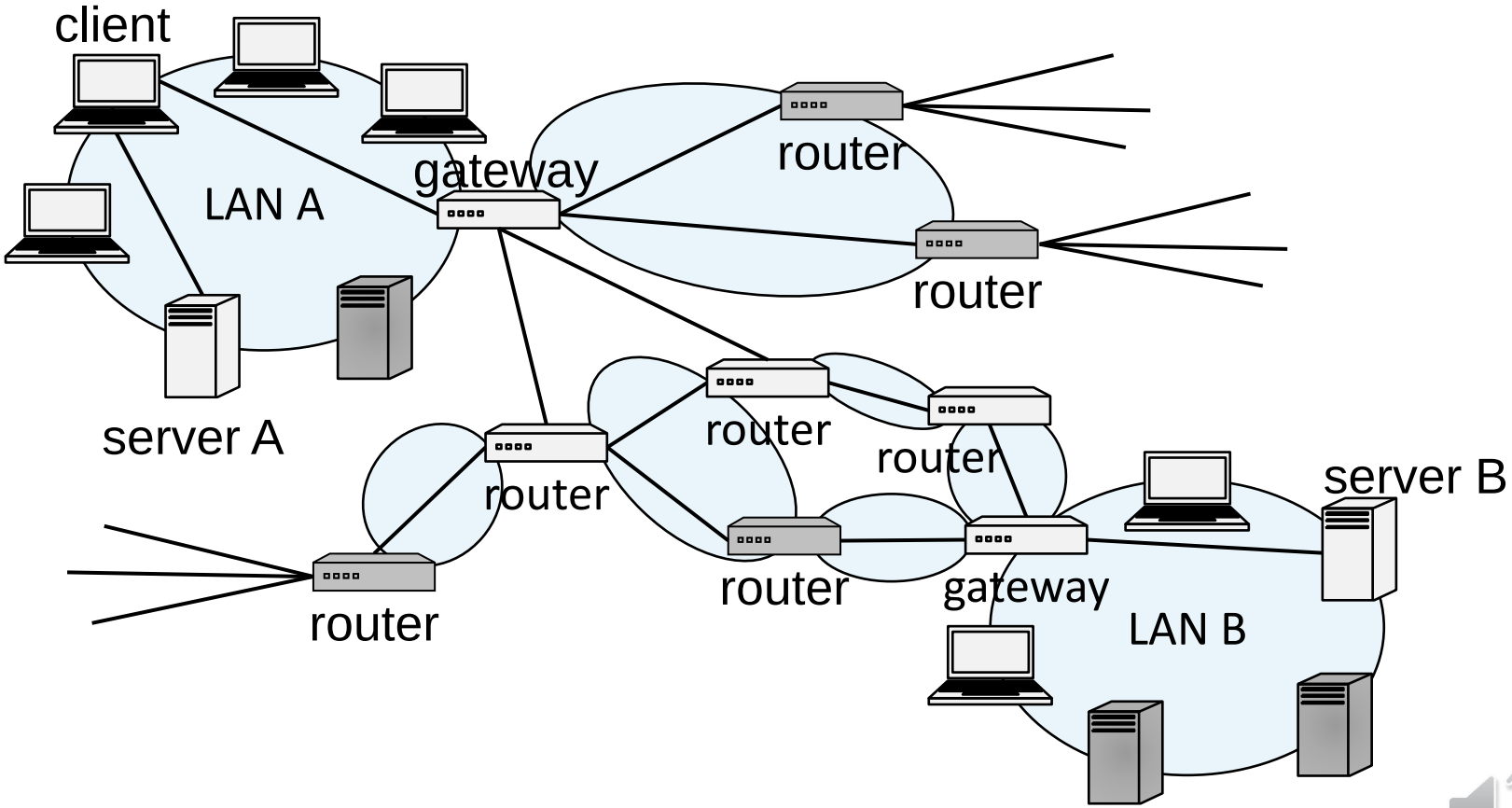


Combining Switches

- 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

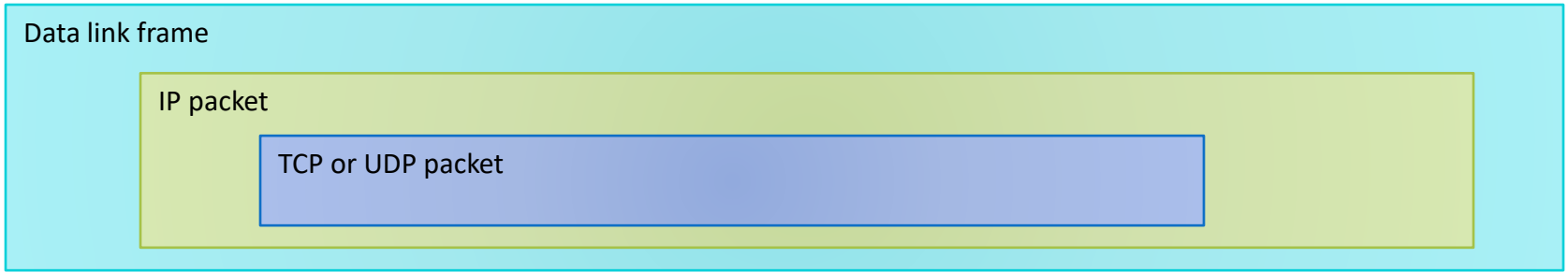


The Internet



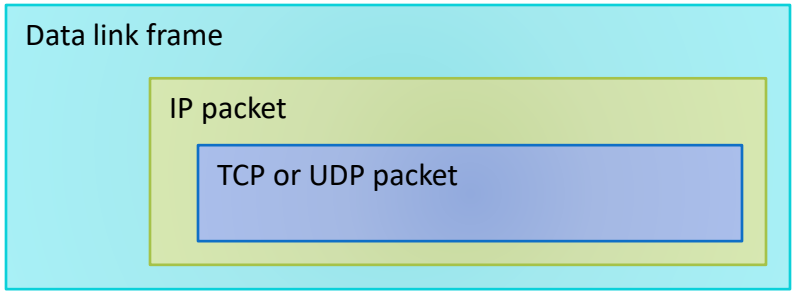
Internet Protocol (IP) Functions

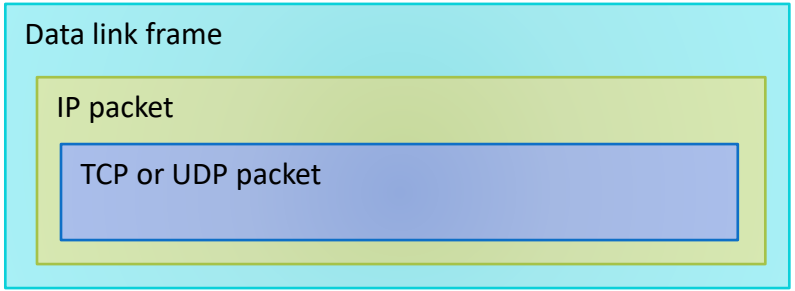
- Addressing: In order to deliver data, IP needs to be aware of where to deliver data to, and hence includes addressing systems
- Routing: IP might be required to communicate across networks, and communicate with networks not directly connected to the current network



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



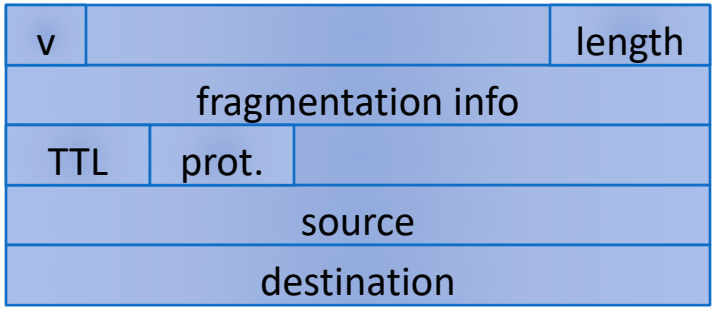


Fragmentation and Reassembly: IP packets are carried across networks which may have different maximum packet length.

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

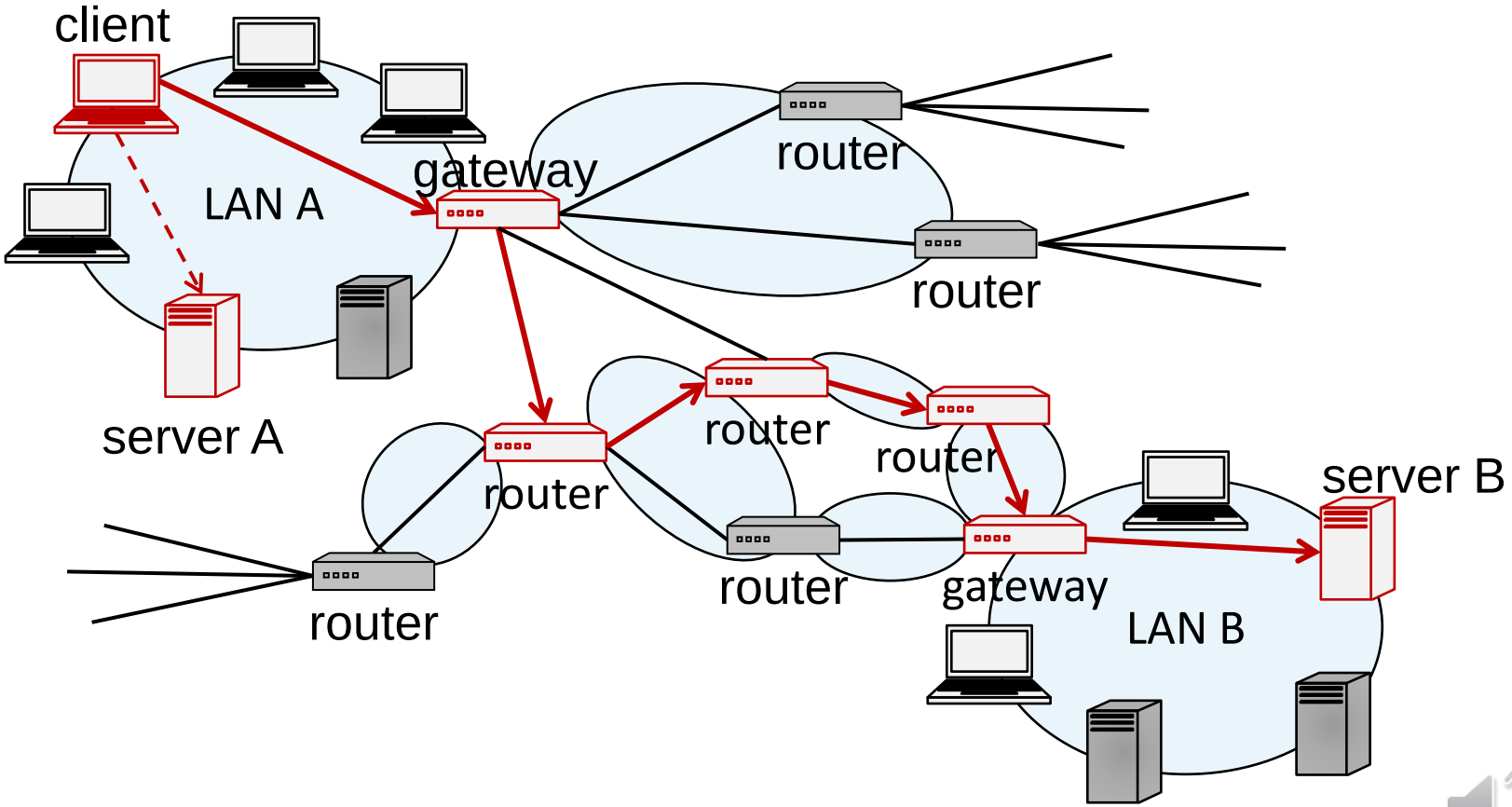
- IP header includes
  - Source address
  - Destination address
  - Packet length (up to 64KB)
  - Time to live (up to 255)
  - IP protocol version
  - Fragmentation information
  - Transport layer protocol information (e.g., TCP)



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

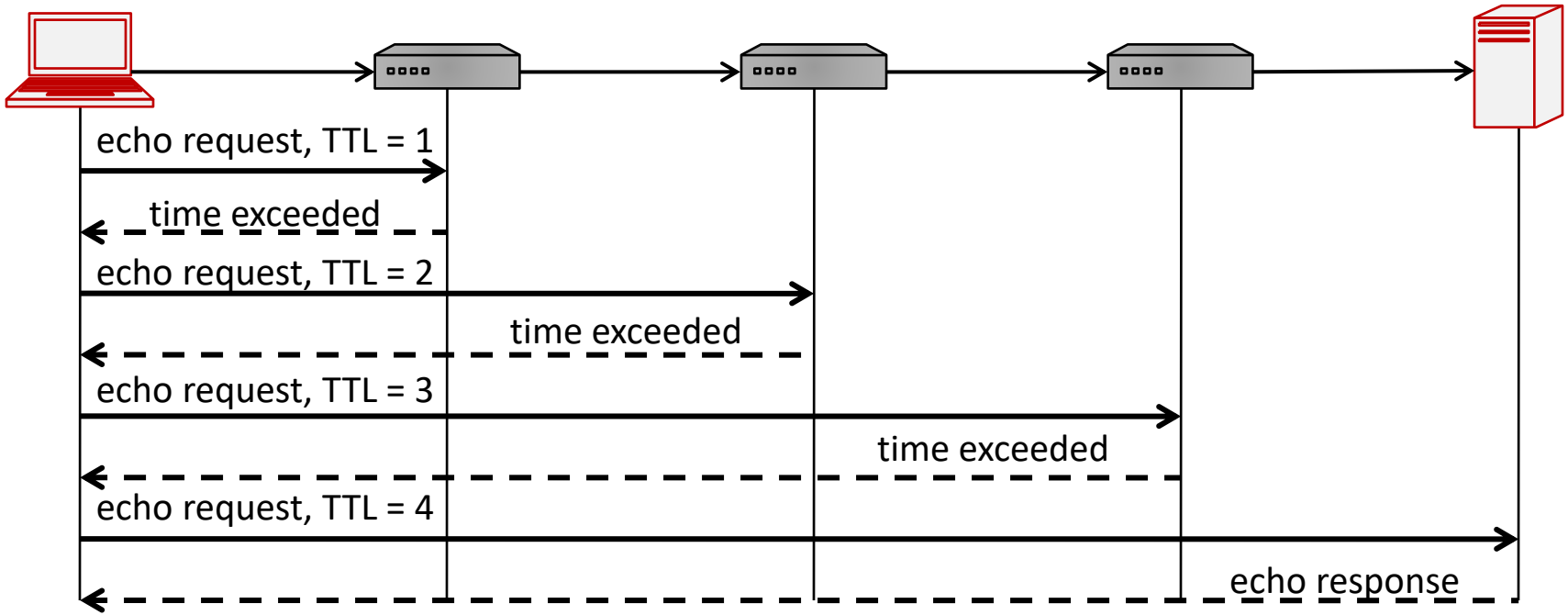
Routing Examples



Exploring Internet Routes

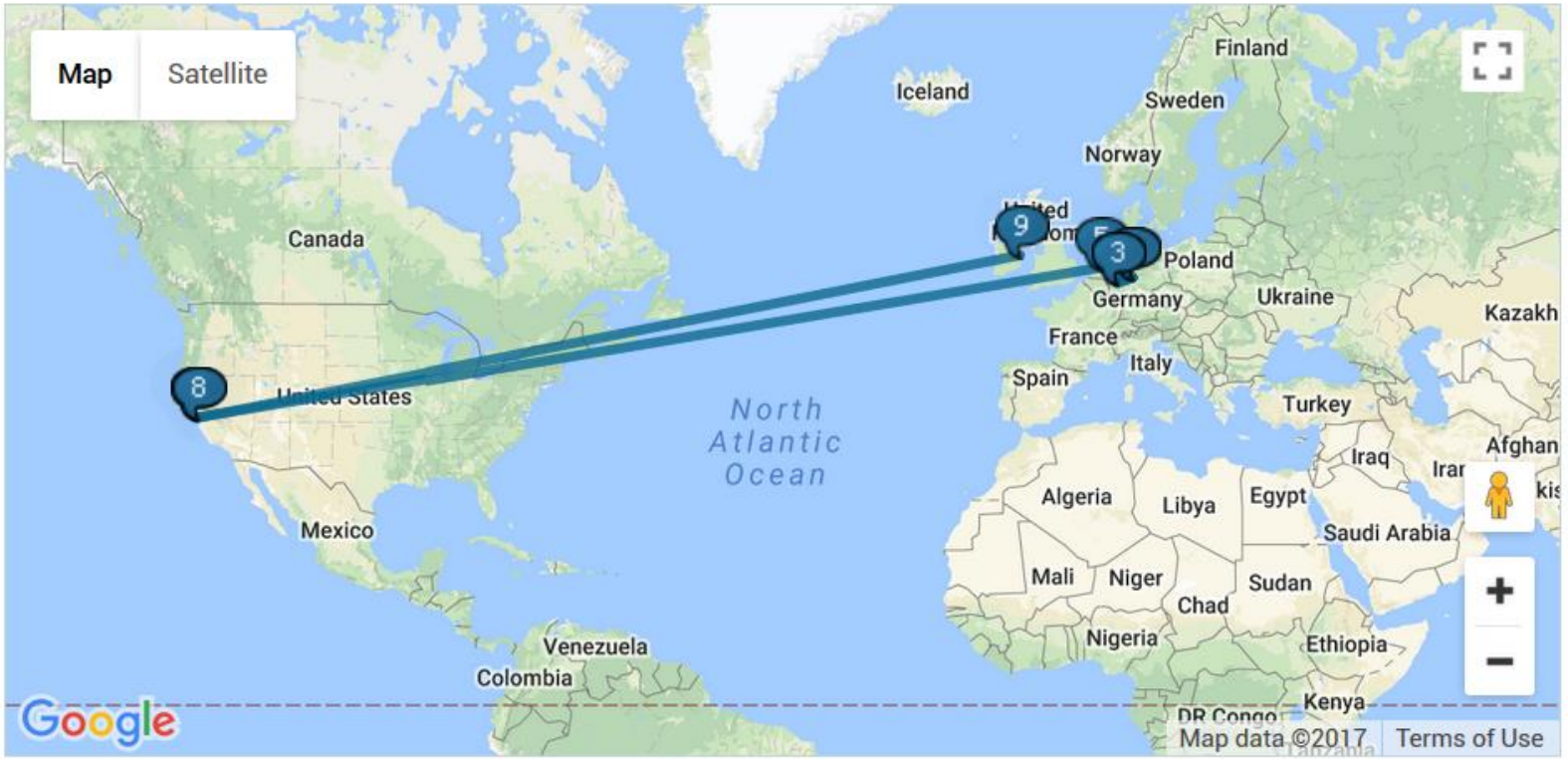
- Internet Control Message Protocol (ICMP)
  - Used for network testing and debugging
  - Simple messages encapsulated in single IP packets
  - Considered a network layer protocol
- Tools based on ICMP
  - Ping: sends series of echo request messages and provides statistics on roundtrip times and packet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

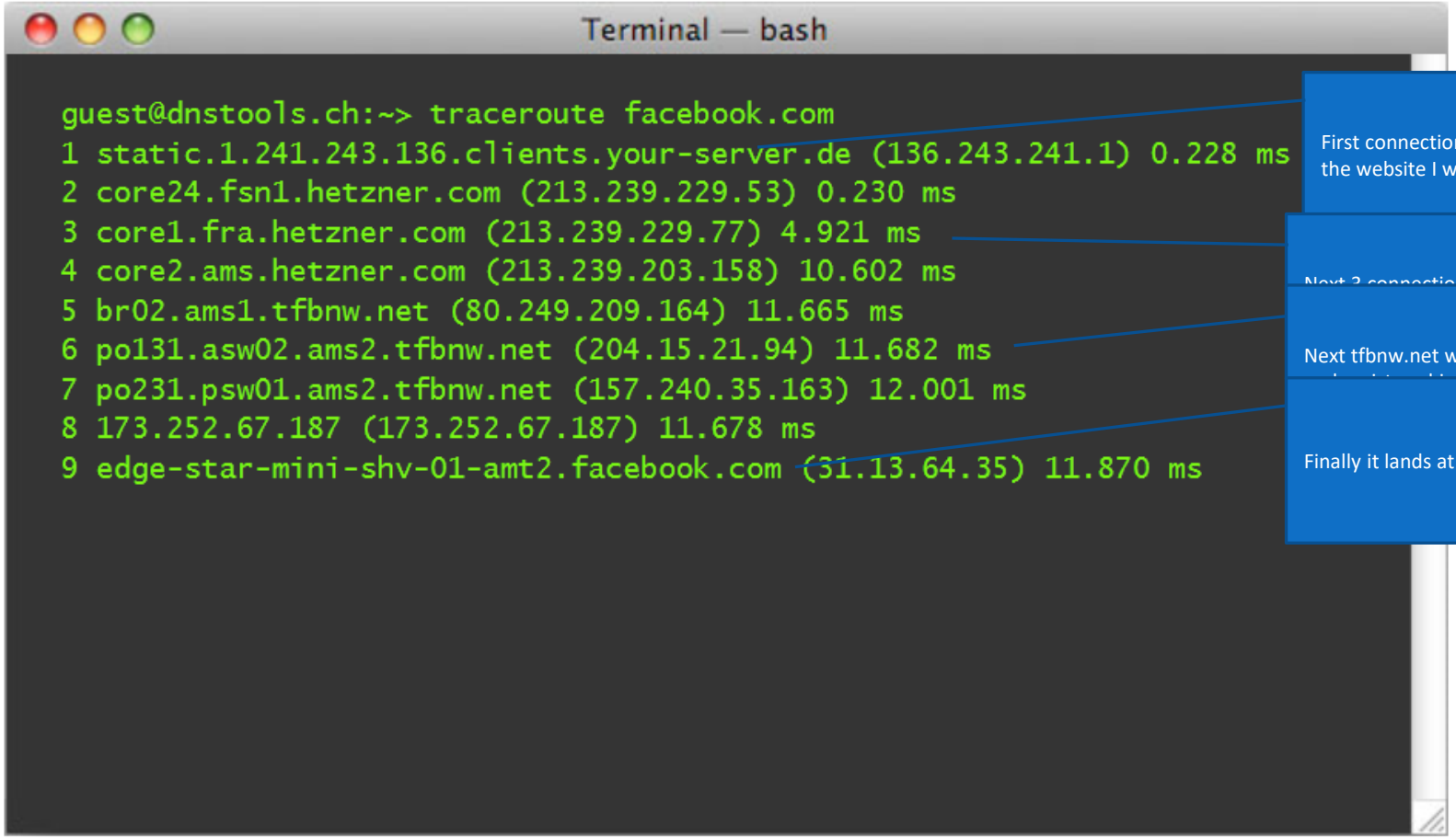
Traceroute


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

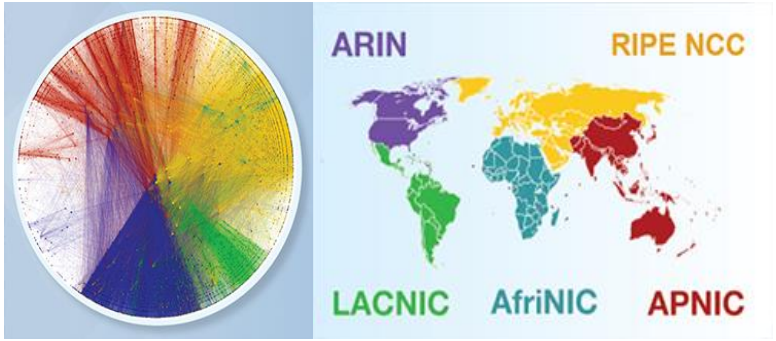
Host (Domain/IP) facebook.com **Trace**

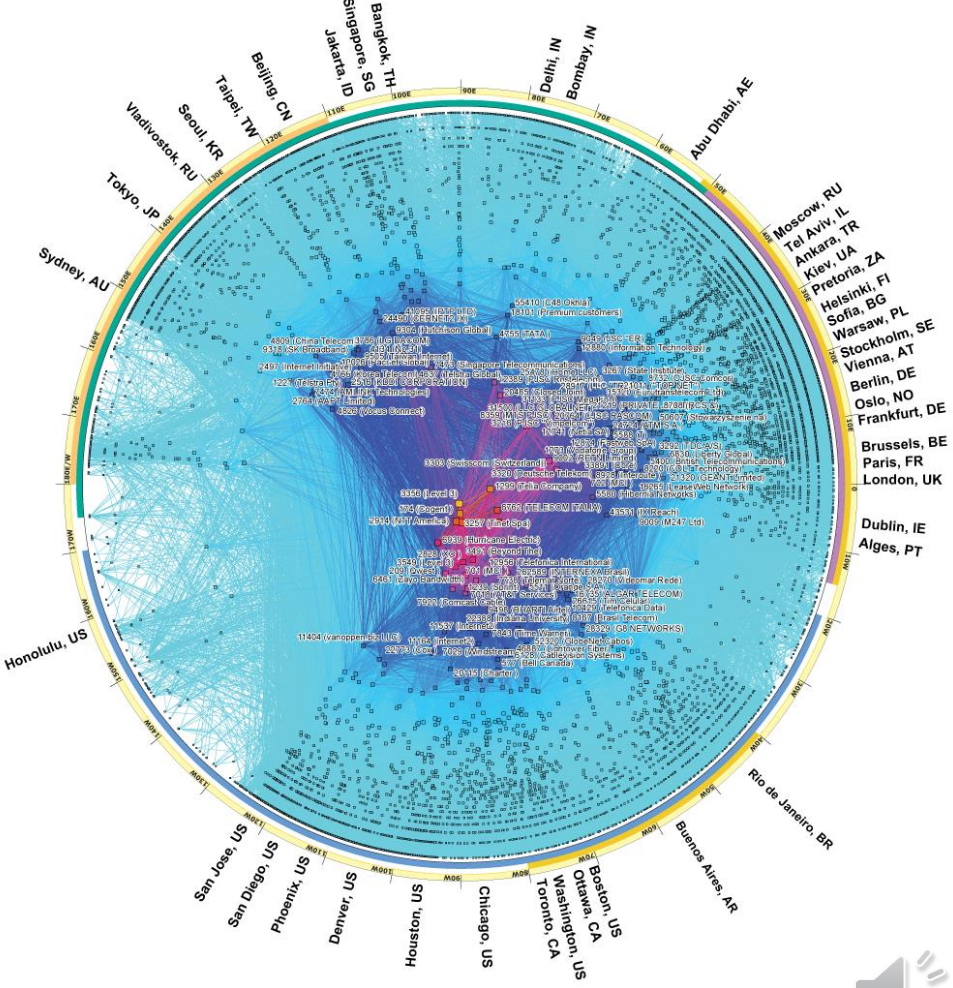
microsoft.com or bluewin.ch




Terminal — bash
guest@dnstools.ch:~> traceroute facebook.com
1 static.1.241.243.136.clients.your-server.de (136.243.241.1) 0.228 ms
2 core24.fsn1.hetzner.com (213.239.229.53) 0.230 ms
3 core1.fra.hetzner.com (213.239.229.77) 4.921 ms
4 core2.ams.hetzner.com (213.239.203.158) 10.602 ms
5 br02.ams1.tfbnw.net (80.249.209.164) 11.665 ms
6 po131.asw02.ams2.tfbnw.net (204.15.21.94) 11.682 ms
7 po231.psw01.ams2.tfbnw.net (157.240.35.163) 12.001 ms
8 173.252.67.187 (173.252.67.187) 11.678 ms
9 edge-star-mini-shv-01-amt2.facebook.com (31.13.64.35) 11.870 ms
First connection was in Germany (.de) where the website I was using is hosted.
Next 2 connections are to hetzner.com
Next tfbnw.net which is owned by Facebook
Finally it lands at Facebook

Caida's AS-level Internet Graph Jan 2017





https://www.caida.org/research/topology/as_core_network/pics/2017/ascore-2017-feb-ipv4-standalone-1000x1037.png

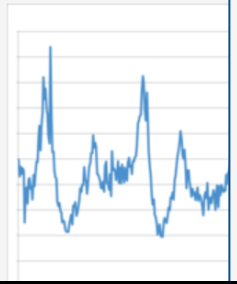
A real world example

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

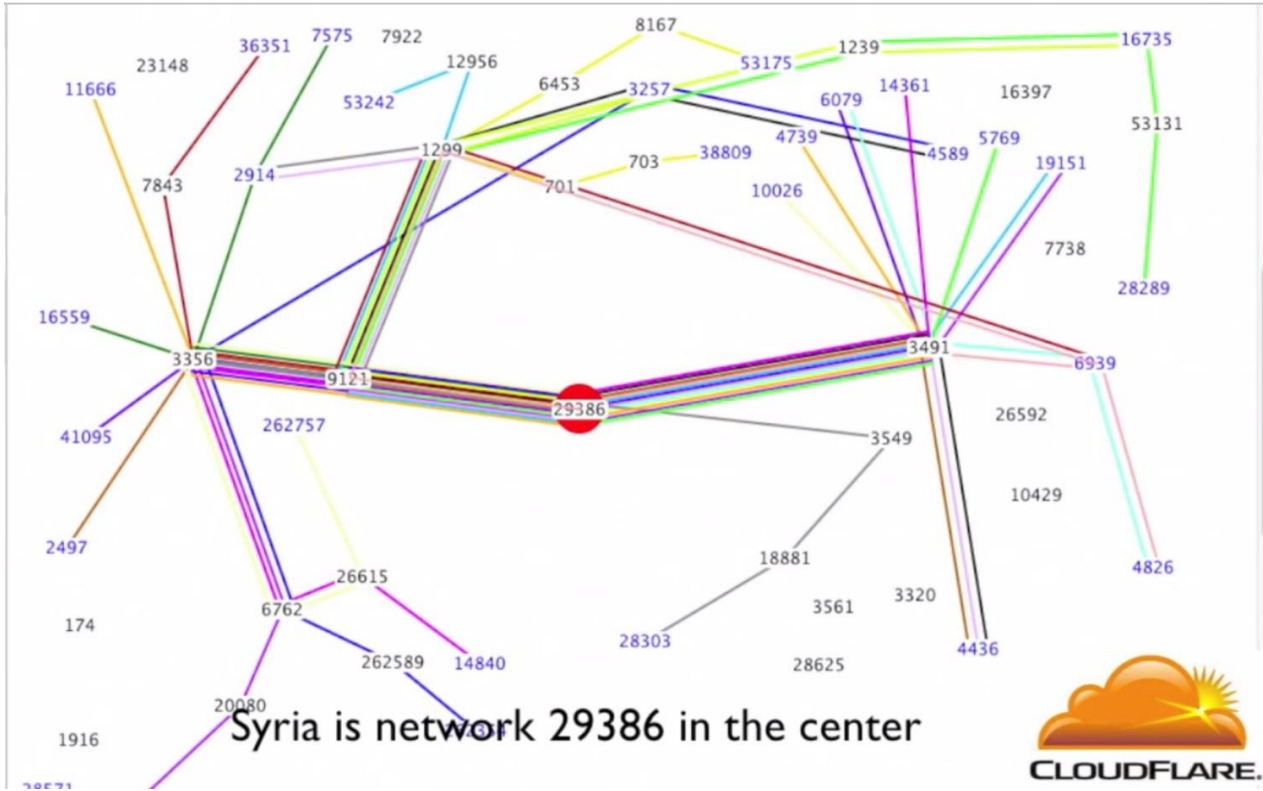
85

An elite hacking unit broke a router

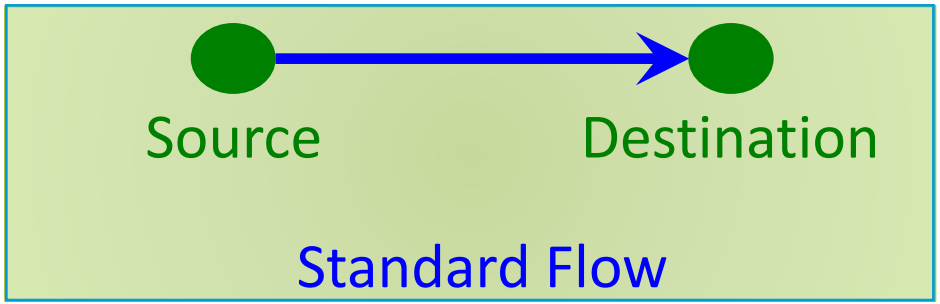
By Jacob Kastrenakes | @jake_k | Aug 13, 2014, 10:28am EDT

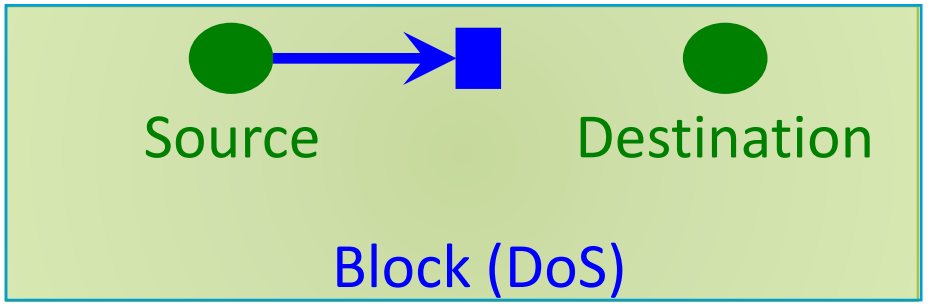
Syria going offline – November 2012

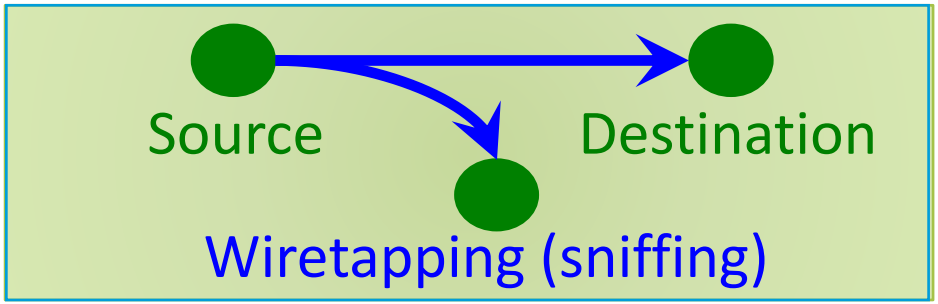
- Article: https://blog.cloudflare.com/how-syria-turned-off-the-internet/
- Going offline: https://www.youtube.com/watch?v=OZHKeYwnALc

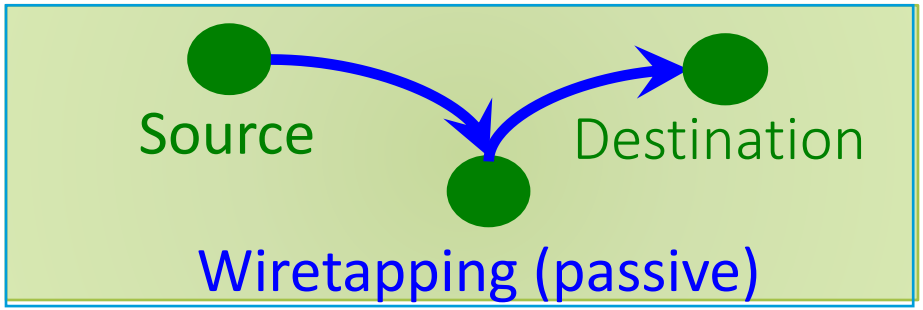


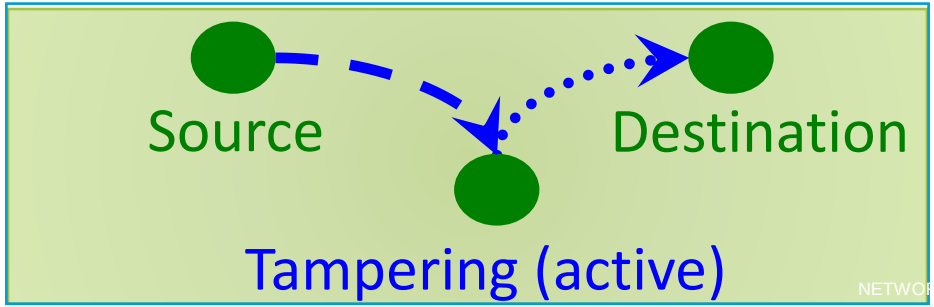
Network Attacks

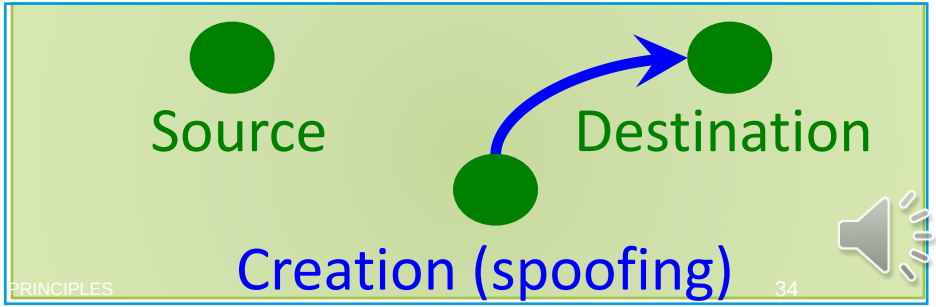




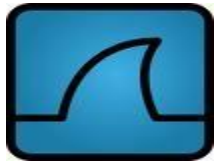




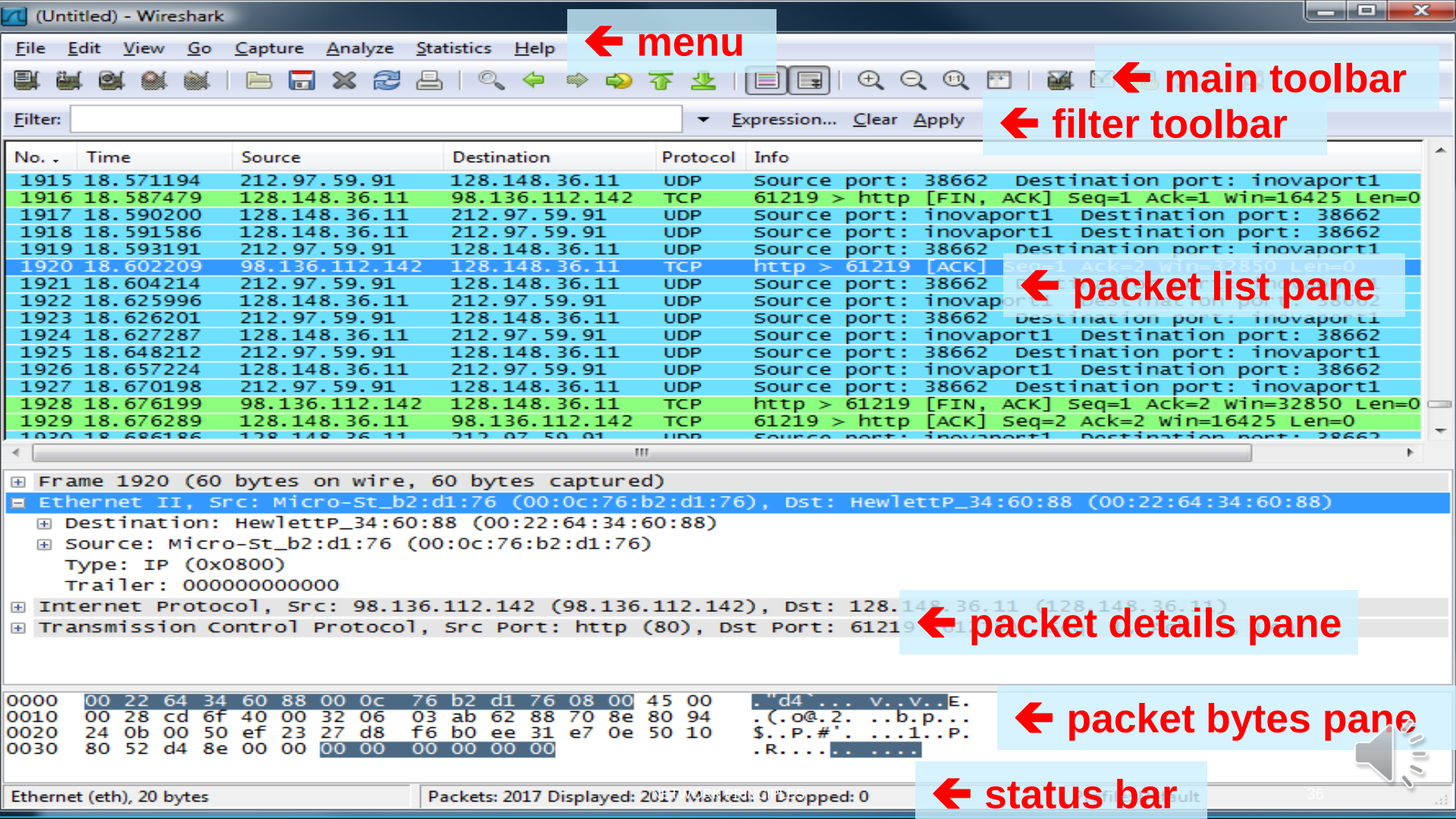




Wireshark



- 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


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
menu
main toolbar
Filter:
Expression... Clear Apply
filter toolbar
No. Time Source Destination Protocol Info
1915 18.571194 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1916 18.587479 128.148.36.11 98.136.112.142 TCP 61219 > http [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
1917 18.590200 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1918 18.591586 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1919 18.593191 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1920 18.602209 98.136.112.142 128.148.36.11 TCP http > 61219 [ACK]
1921 18.604214 212.97.59.91 128.148.36.11 UDP Source port: 38662
1922 18.625996 128.148.36.11 212.97.59.91 UDP Source port: inovaport1
1923 18.626201 212.97.59.91 128.148.36.11 UDP Source port: 38662
1924 18.627287 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1925 18.648212 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1926 18.657224 128.148.36.11 212.97.59.91 UDP Source port: inovaport1 Destination port: 38662
1927 18.670198 212.97.59.91 128.148.36.11 UDP Source port: 38662 Destination port: inovaport1
1928 18.676199 98.136.112.142 128.148.36.11 TCP http > 61219 [FIN, ACK] Seq=1 Ack=2 Win=32850 Len=0
1929 18.676289 128.148.36.11 98.136.112.142 TCP 61219 > http [ACK] Seq=2 Ack=2 Win=16425 Len=0
packet list pane
Frame 1920 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: Micro-St_b2:d1:76 (00:0c:76:b2:d1:76), Dst: HewlettP_34:60:88 (00:22:64:34:60:88)
Destination: HewlettP_34:60:88 (00:22:64:34:60:88)
Source: Micro-St_b2:d1:76 (00:0c:76:b2:d1:76)
Type: IP (0x0800)
Trailer: 000000000000
Internet Protocol, Src: 98.136.112.142 (98.136.112.142), Dst: 128.
Transmission Control Protocol, Src Port: http (80), Dst Port: 6121
packet details pane
0000 00 22 64 34 60 88 00 0c 76 b2 d1 76 08 00 45 00 ."d4`... v..v..E.
0010 00 28 cd 6f 40 00 32 06 03 ab 62 88 70 8e 80 94 .(.o@.2. ..b.p...
0020 24 0b 00 50 ef 23 27 d8 f6 b0 ee 31 e7 0e 50 10 $..P.#'. ...1..P.
0030 80 52 d4 8e 00 00 00 00 00 00 00 00 .R...... ....
packet bytes pane
Ethernet (eth), 20 bytes
Packets: 2017 Displayed: 2017 Marked: 0 Dropped: 0
status bar

What We Have Learned

- Networking principles
  - Packet switching
  - Stack of layers
  - Encapsulation
- Network interfaces, MAC addresses, and Switches
- Internet Protocol (IP) Routing, autonomous systems
- Types of network attacks
- Traceroute and Wireshark tool