Introduction to Computer Networks Security

CS 1660: Introduction to Computer Systems Security

Let me briefly introduce myself…

Bernardo Palazzi

Advisor for Awareness Division at ACN (Italian Agency for Cybersecurity)

Other professional experiences:

- First Data Protection Officer (DPO) oversaw privacy regulation (GDPR) for the whole population at the Italian National Institute of Statistics.
  - Managed the cyber security of the first online population census.
- Founder and CTO of a cloud data security startup based on an international patent developed during my PhD thesis

Academic experiences:

- In 2007, started collaborating with Brown University in the USA and teaching CS1660 ☺
- 2015-2020 Founder and Academic Director of the Brown EMCS (Executive Master in Cyber Security)
- 2020-2023 Founder and Director of Graduate Study of Master in Cyber Security
- 2022-present Co-chair of the Strategic Planning Committee for the Master on Cyber

Networking's Role in Cybersecurity

- **Remote Communication**: Networks enable distant interactions.
- **Data Exchange Infrastructure**: Network devices allow the creation of an efficient digital domain.
- **Cyber Attack Vectors**: Networks are common targets needing solid defenses.
- There is a dual nature of networks as both enablers and potential risks.
- So, what is a network?

A very easy… network

Source

Destination

Communication Channel

Virtual Circuit

- Analogic rotatory phone lines:

Virtual Circuit vs Packet Switching

- Virtual Circuit
  - Legacy phone network
  - Single route through sequence of hardware devices established when two nodes start communication
  - Data sent along route
  - Route maintained until communication ends

- Packet switching
  - Internet
  - Data split into packets
  - Packets transported independently through network
  - Each packet handled on a best efforts basis
  - Packets may follow different routes

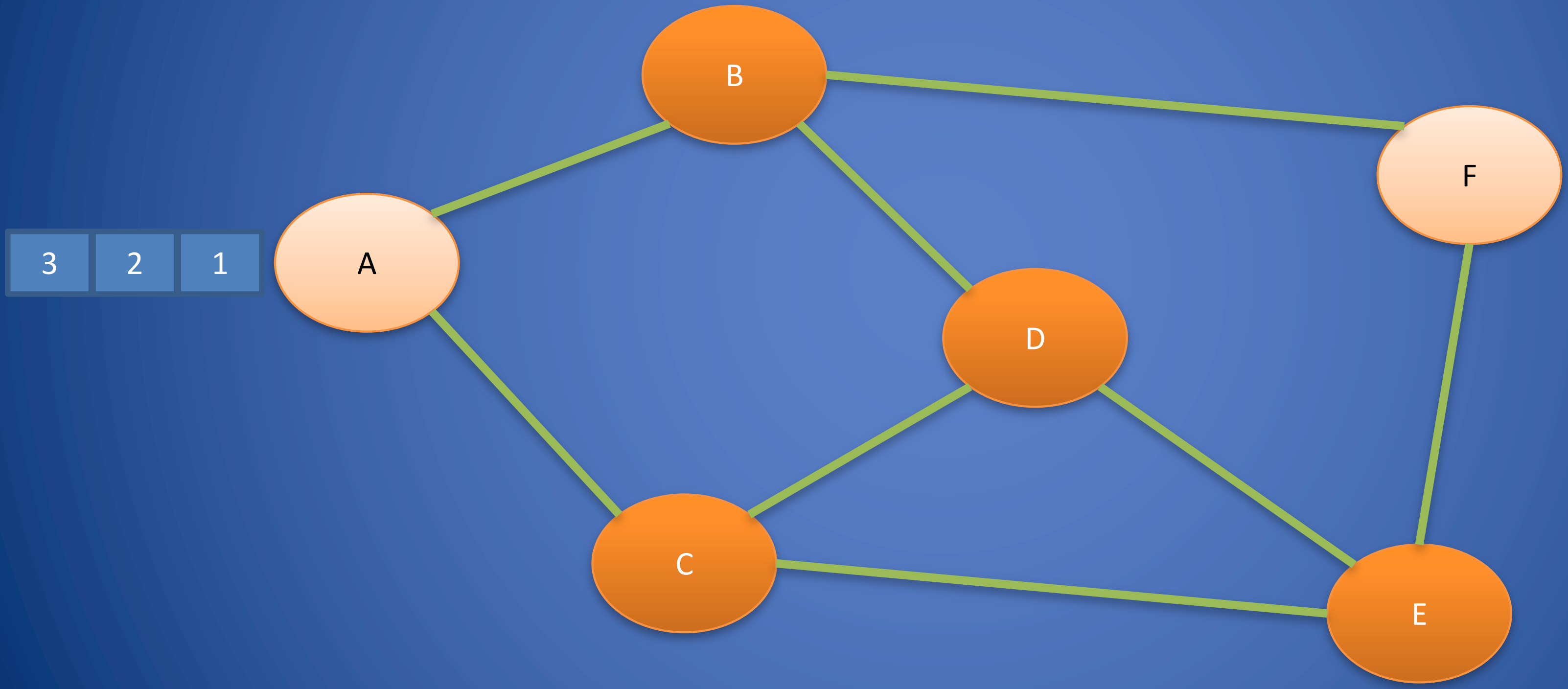
Network Communication

- Communication in modern networks is characterized by the following fundamental principles
  - Packet routing (aka switching)
  - Stack of layers (virtual layers)
  - Encapsulation

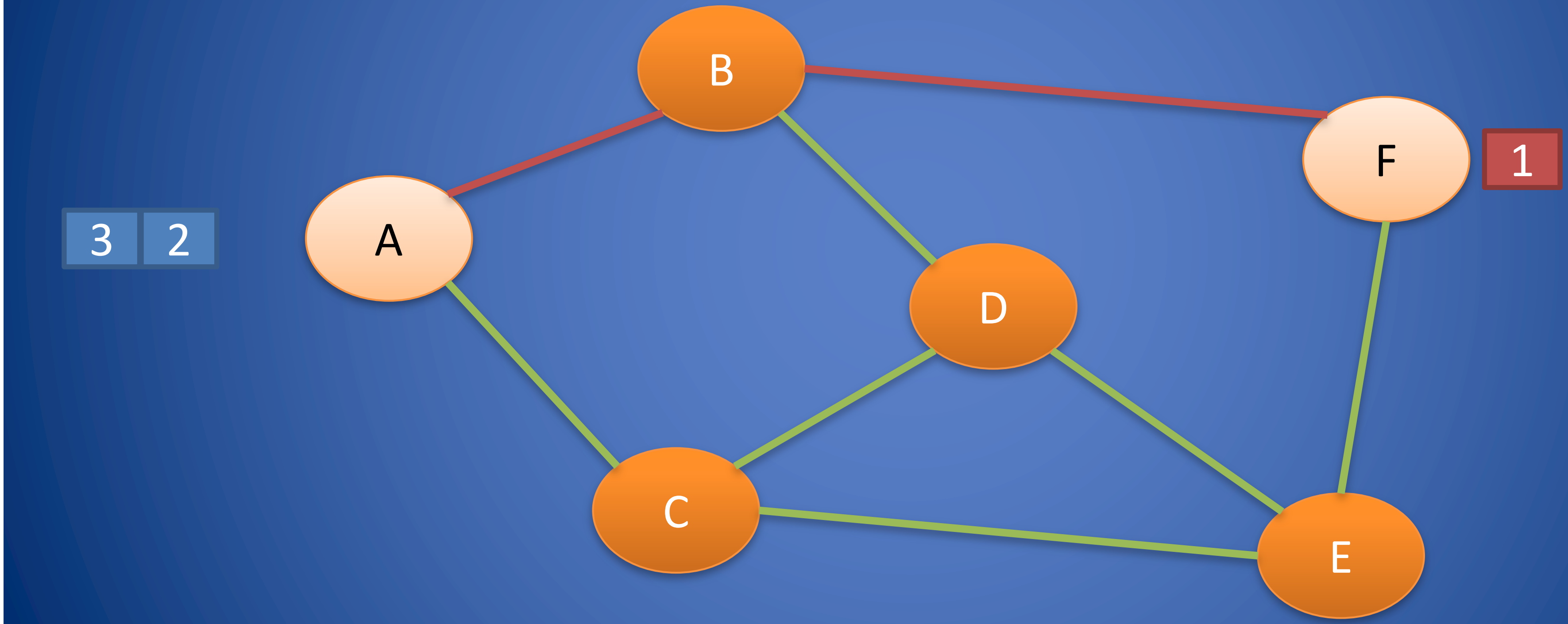
Packet Routing

- 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

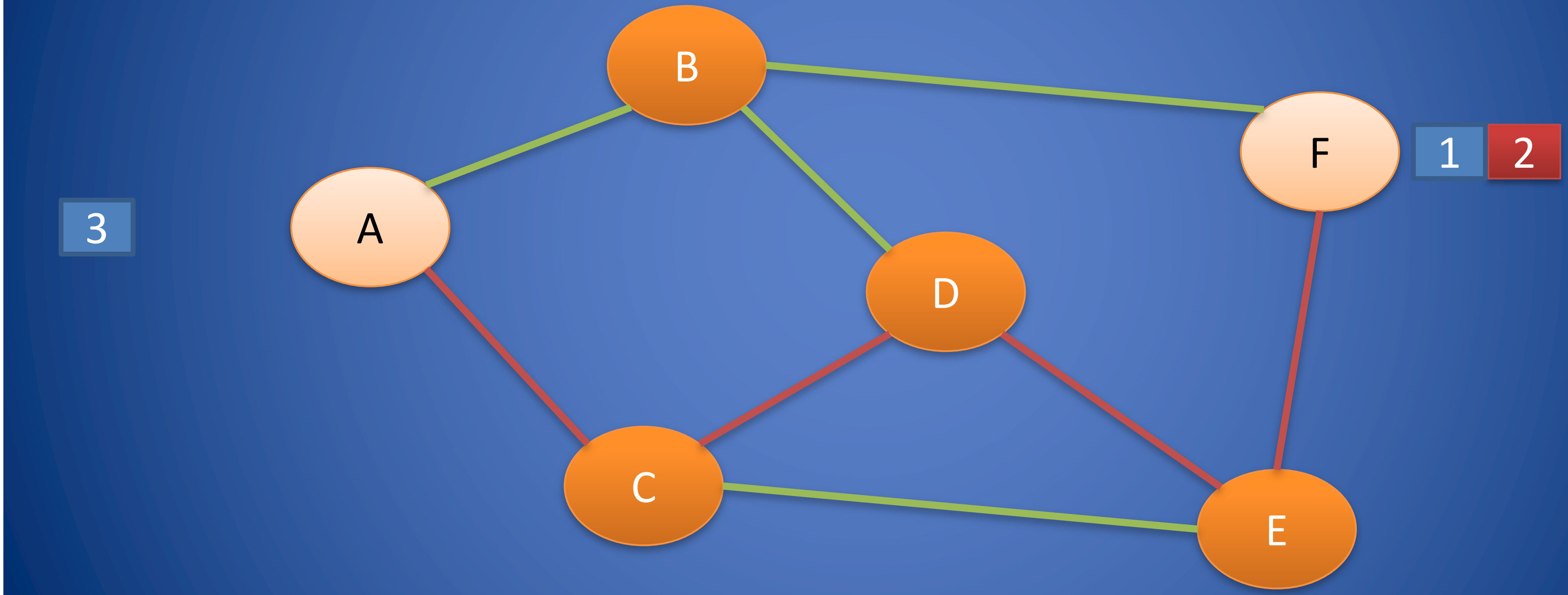
Packet Routing Example



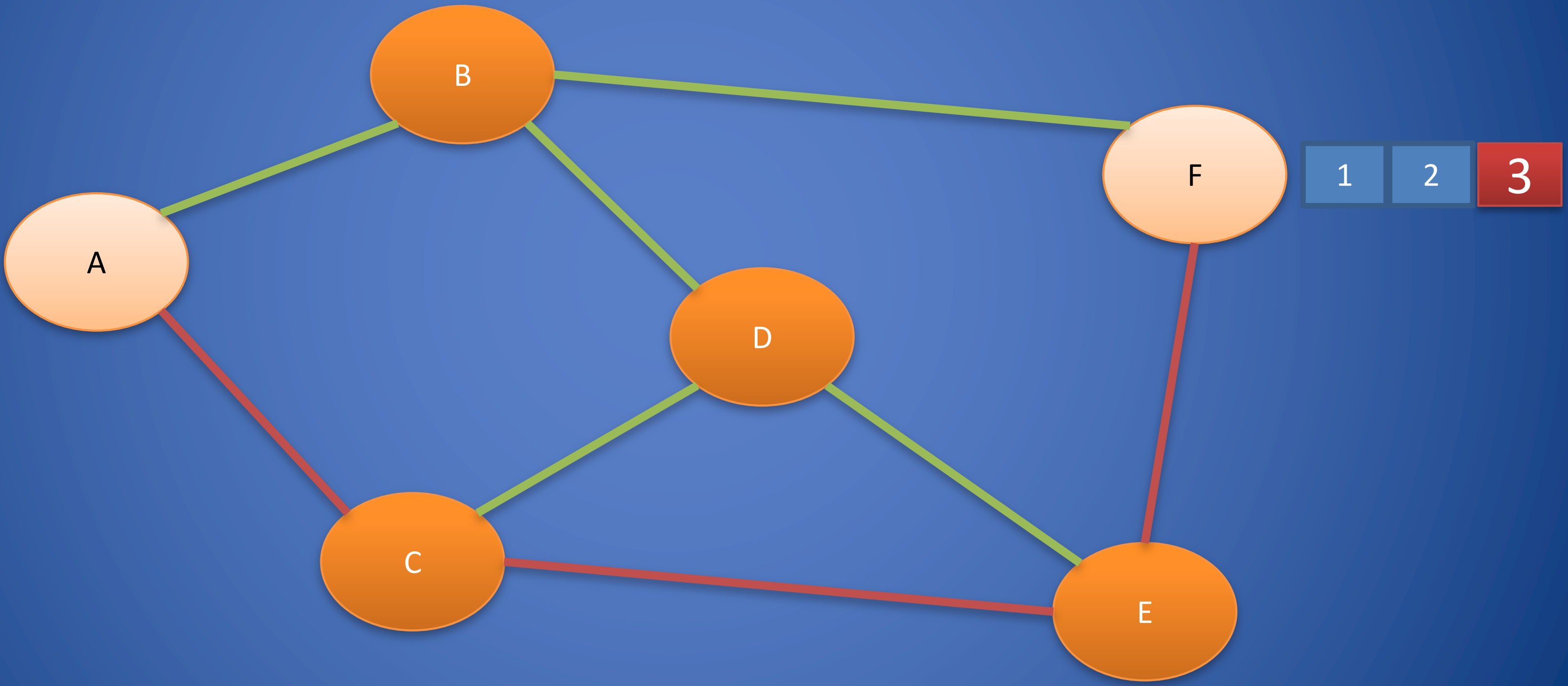
Packet Routing Example



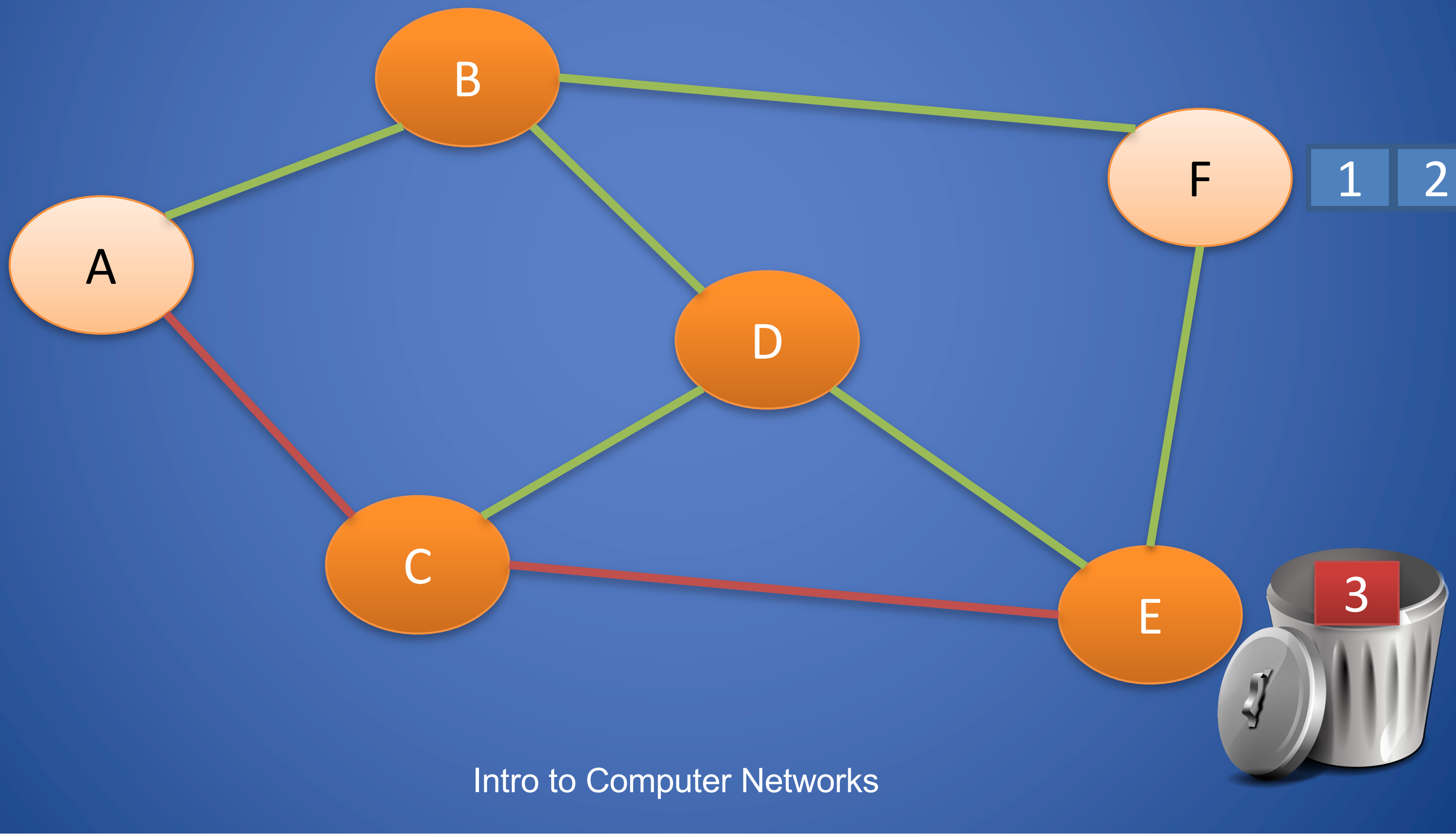
Packet Routing Example



Packet Routing Example

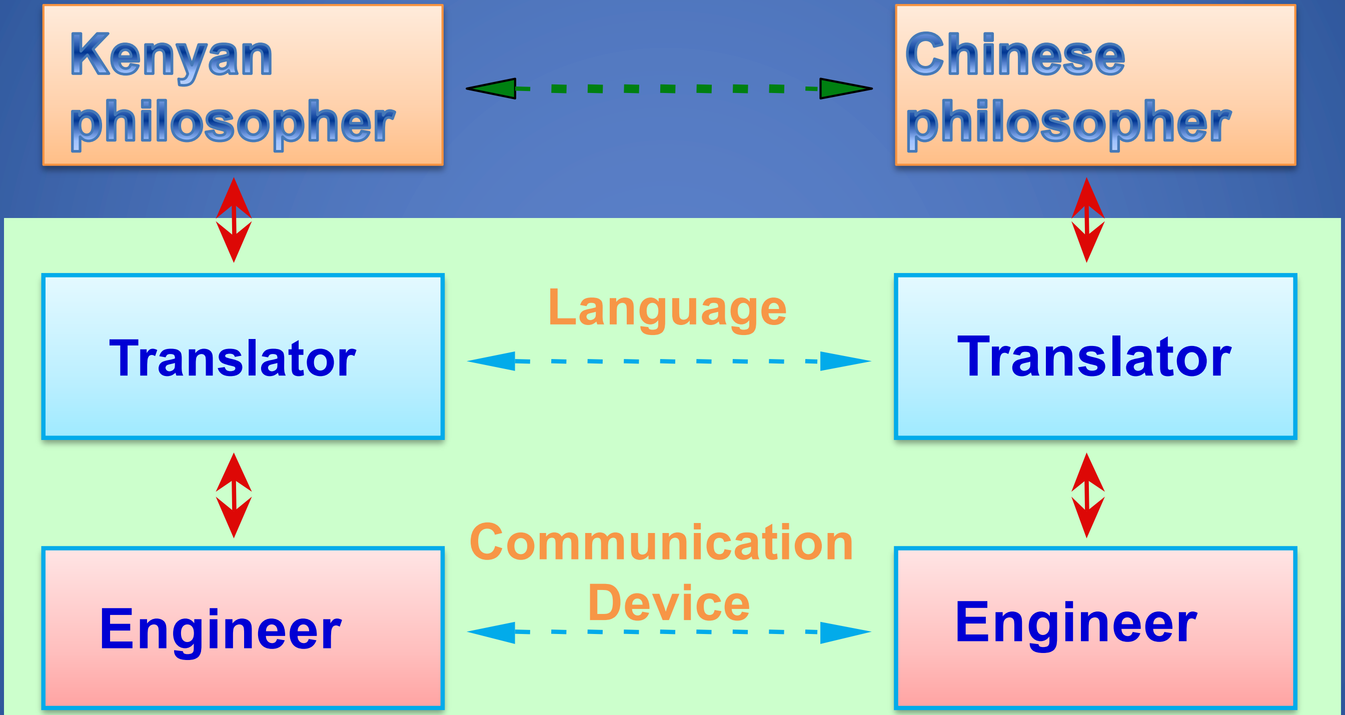


Packet Routing Example (Problem)



Protocol Layers and Encapsulation

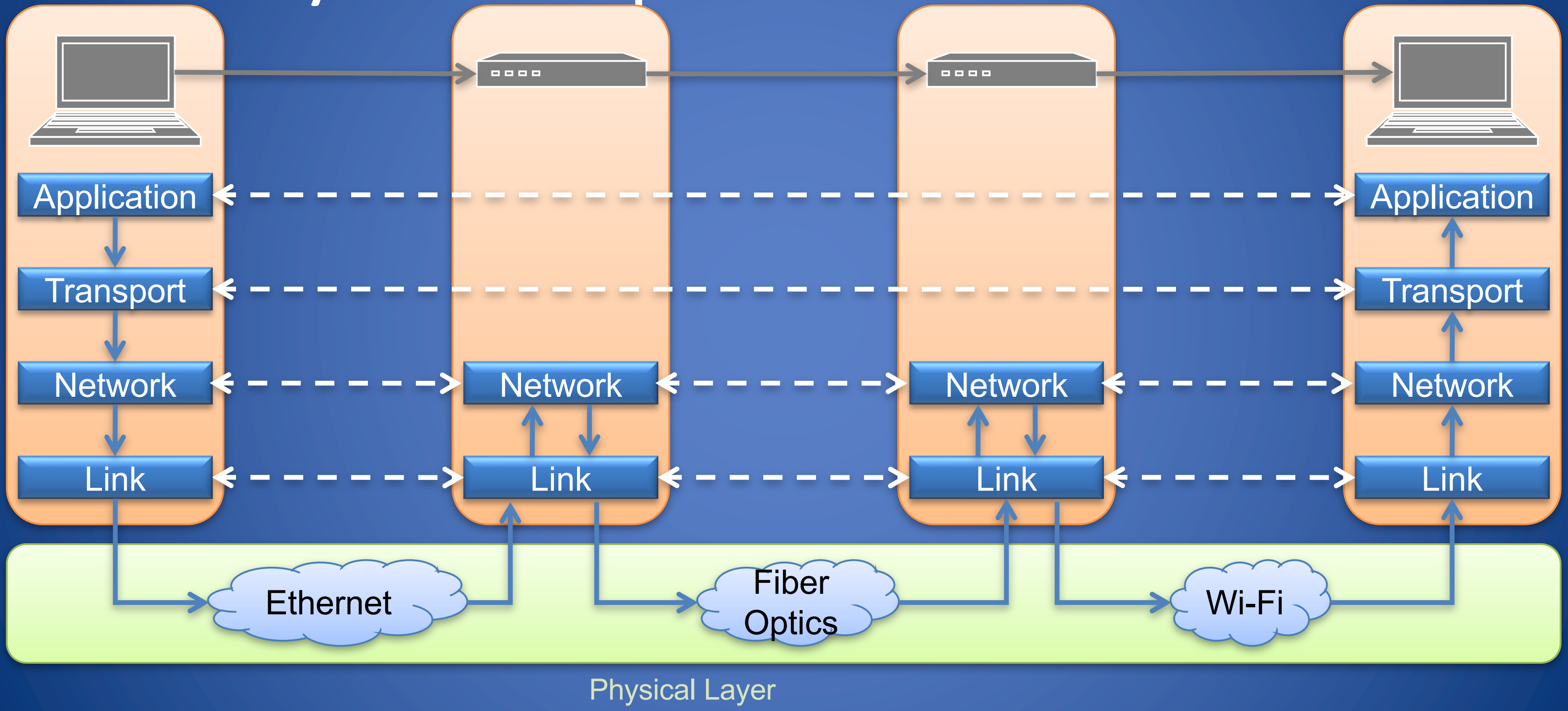
Two philosophers example



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

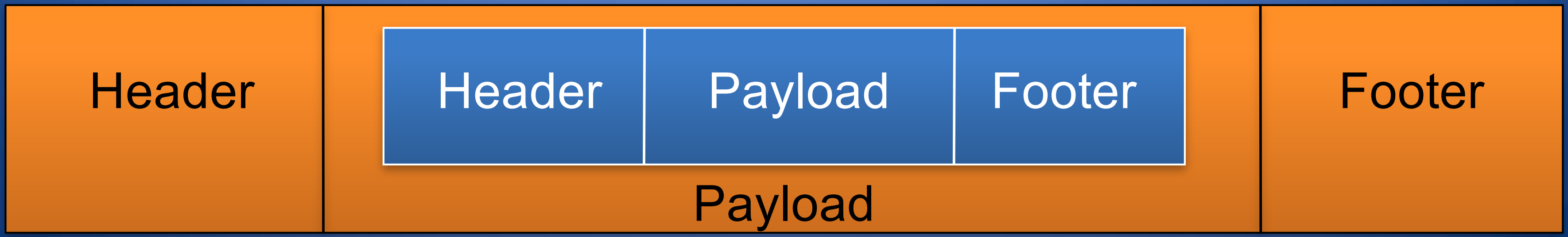
Internet Layers:
How your computer talks to a website



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

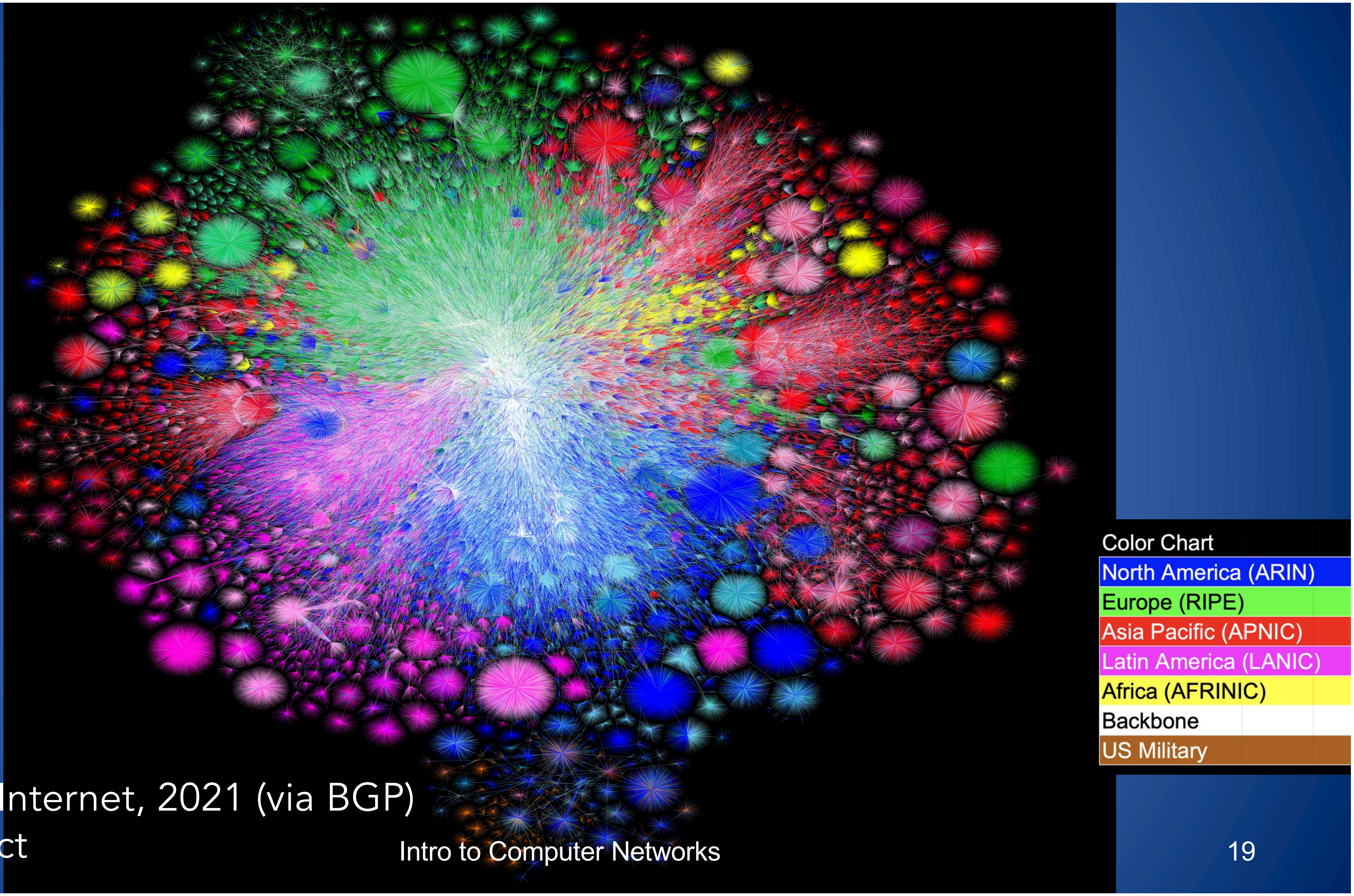


Header

Header | Payload | Footer

Payload

Footer



Map of the Internet, 2021 (via BGP)
OPTE project

How do we make sense of this?

Network abstractions model how we build protocols and applications:

- How data gets encapsulated
- What services are provided at each later (and what they rely on from other layers)

Network Layers

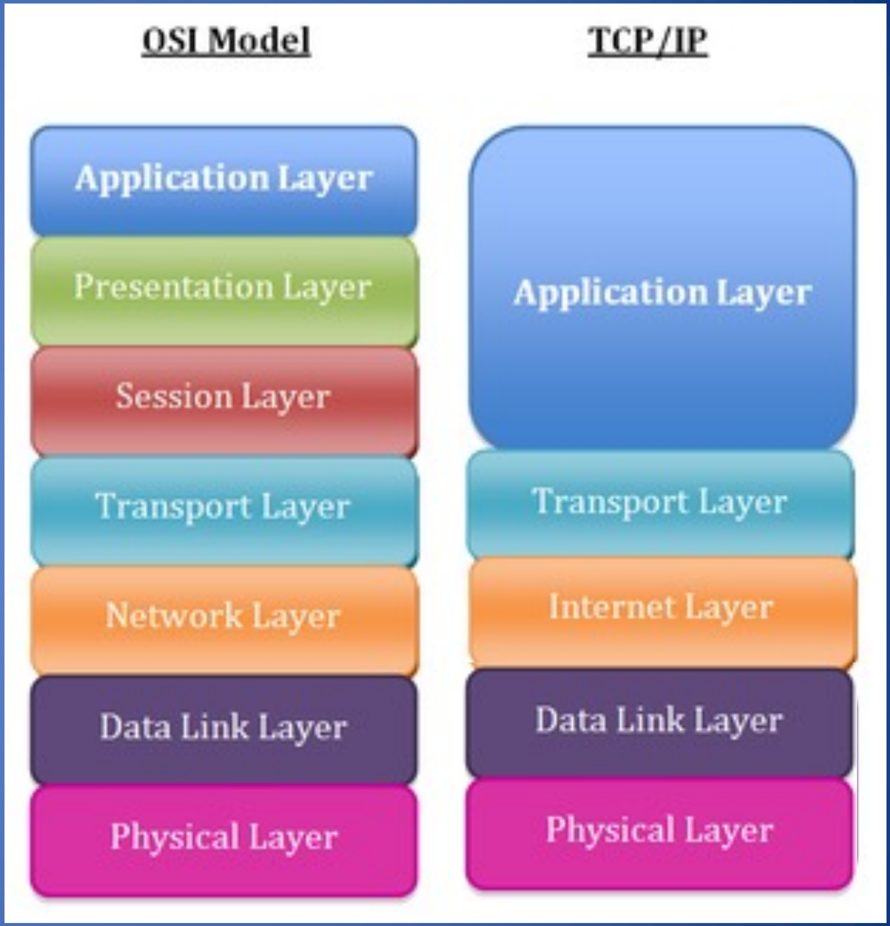
Networks are complex. Abstractions help us deal with them and build extensible, scalable systems

Some problems:

- Different media: Wifi, Ethernet, Cellular, Bluetooth, ..
- No single managing entity: many ISPs, organizations, countries with different goals/policies
- Need to support different types of applications, which use network in different ways

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)



OSI Model

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

Data Link Layer

Physical Layer

TCP/IP

Application Layer

Transport Layer

Internet Layer

Data Link Layer

Physical Layer

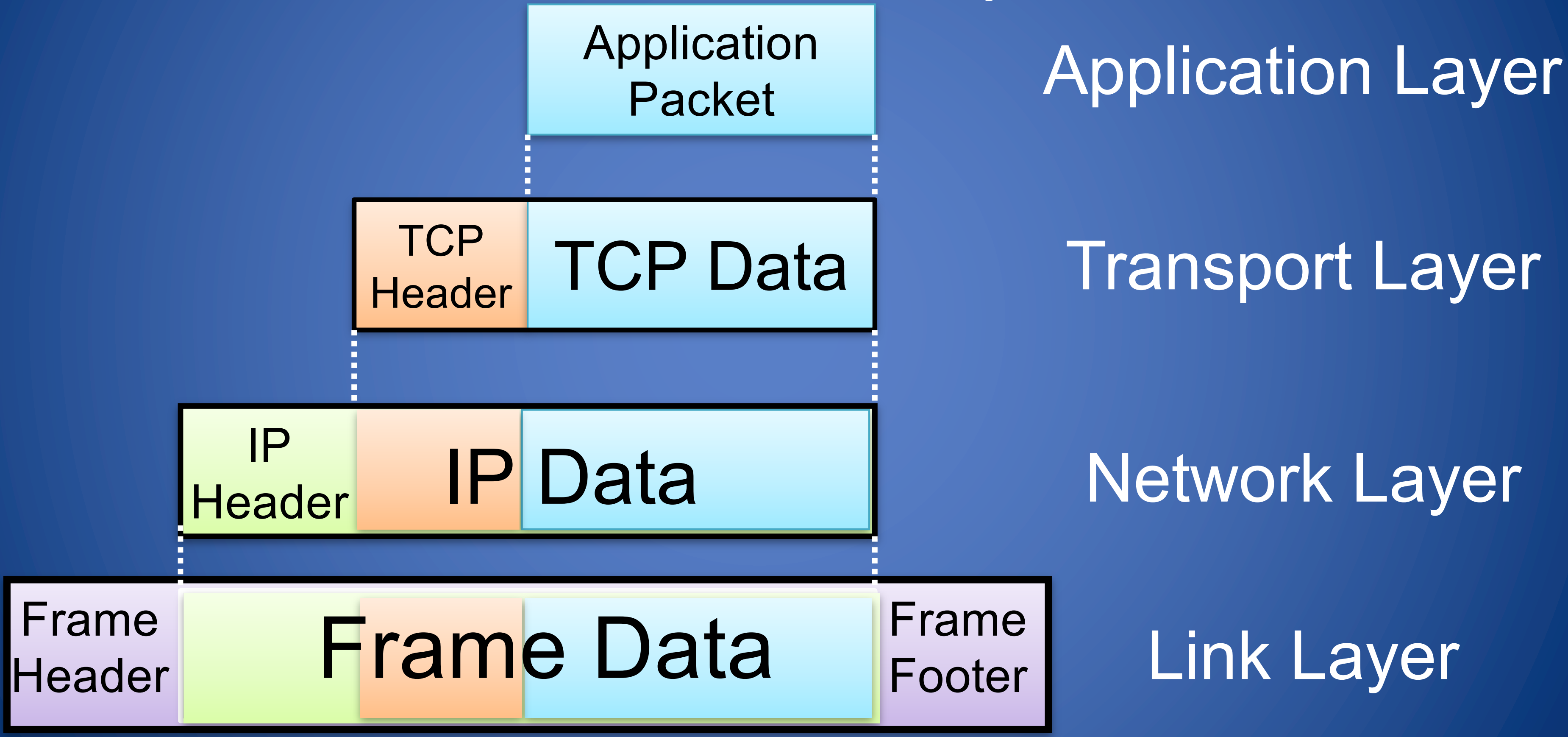
Layers: the classical picture

- Application – what users see, *e.g.*, web page via HTTP
- Presentation – crypto, conversion between representations
- Session – can tie together multiple streams (*e.g.*, audio & video)
- Transport – abstractions for getting data data between applications
- Network – consider *packets* moving across entire network
- Link layer – consider *frames* moving between individual *links*
- Physical – moving bits across a link

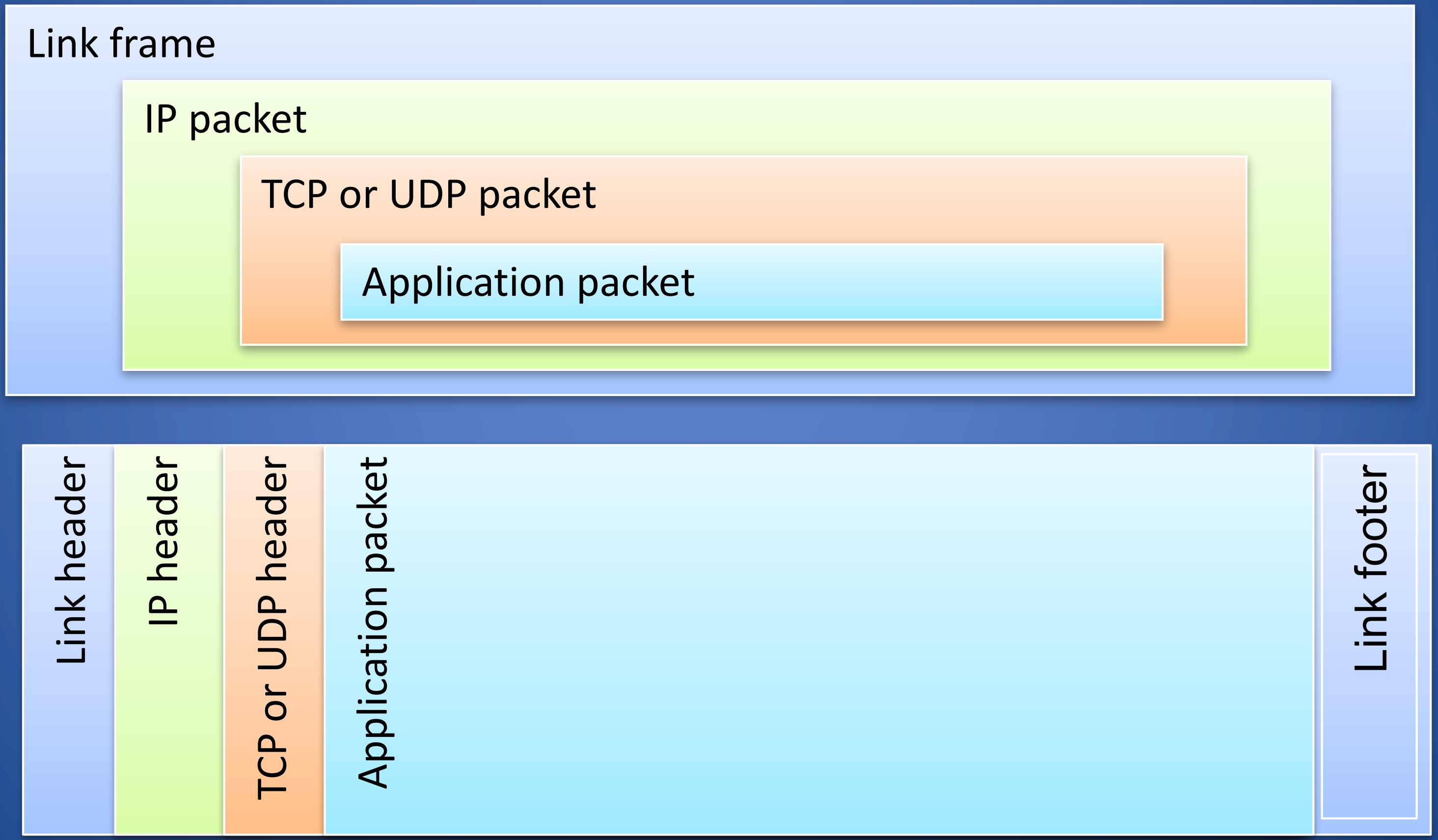
A high-level picture

7. Application	Provides applications to users (eg. HTTP, SSH, …) Application-defined messages
4. Transport	Abstracts methods use to send data Examples: TCP, UDP Defines: port numbers;
3. Network	Provides way to get a packet to any other node on the Internet Protocols: IP (IPv4, IPv6) Defines: IP address (eg. 1.2.3.4)
2. Link	Protocols for sending data on individual links Examples: Wifi, Ethernet, Bluetooth, … Defines: MAC address *(more on this later)*
1. Physical	Service: move bits to other node across link (Electrical engineering problem)

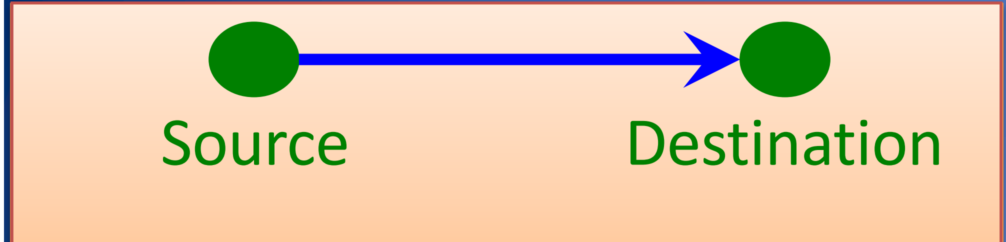
Internet Packet Encapsulation



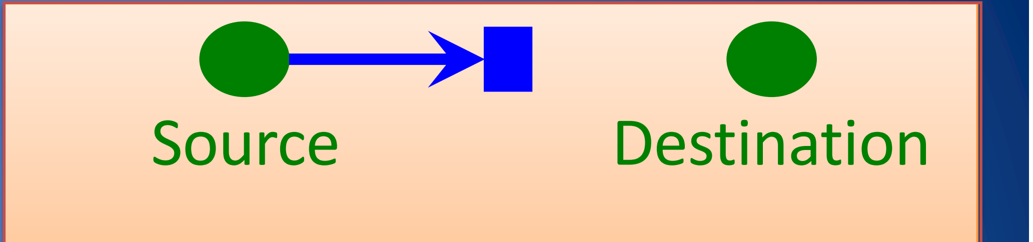
Internet Packet Encapsulation



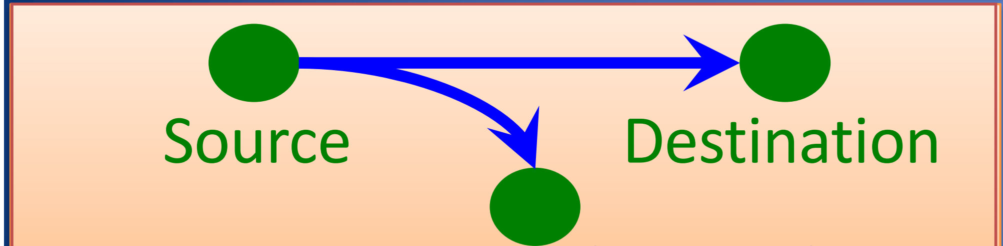
Network Attacks



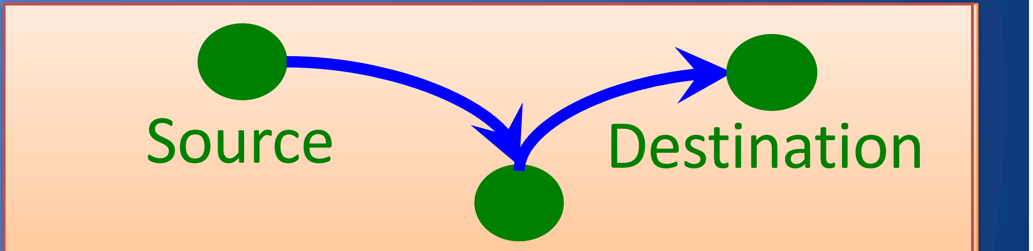
Standard Flow



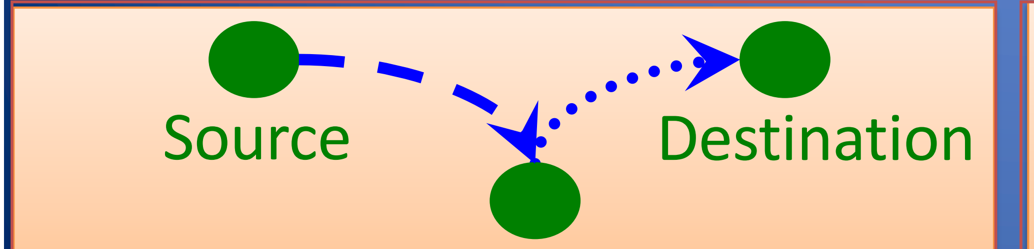
Block (DoS)



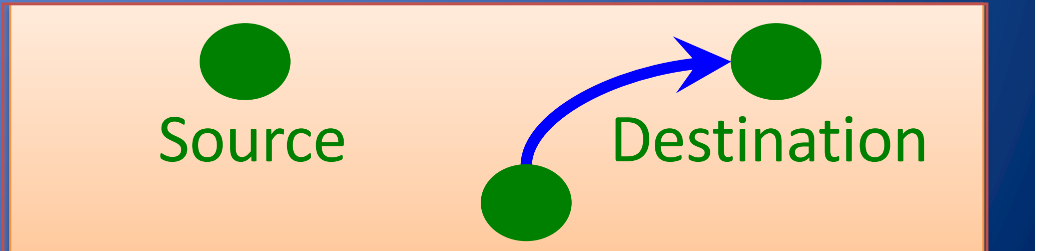
Wiretapping (sniffing)



Wiretapping (passive)



Tampering (active)



Creation (spoofing)

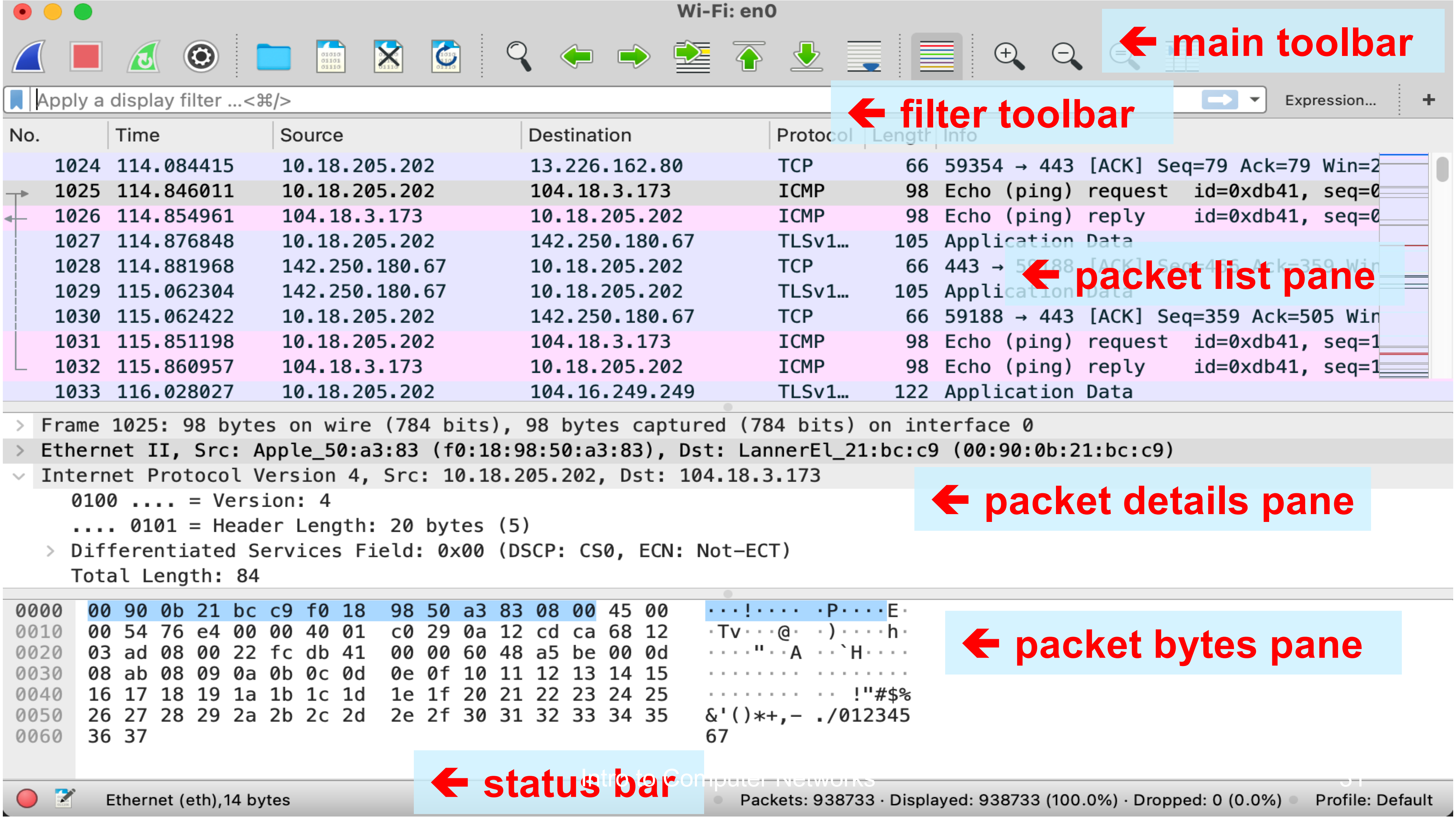
A Framework of possible threats: the STRIDE model

Threats (STRIDE)	Description	Violation
Spoofing	Creating content by impersonating another account	Authentication
Tampering	Alteration of data or system	**Integrity**
Repudiation	Do not recognize actions performed	Non-repudiation (Certification)
Information Revelation	Exposing information to an unauthorized party	**Confidentiality**
Denial of Service	Inability to use services	**Availability**
Elevation of privileges	Possibility to carry out privileges without authorization	Authorization

Let’s see networks in action…

Wireshark

- Wireshark is a packet sniffer, protocol analyzer used for network troubleshooting, analysis and protocol development
- Wireshark allows for capturing of raw data from the network and for analysis
- Freely available on www.wireshark.org



```
No.   Time        Source           Destination      Protocol  Length Info
 1024 114.084415  10.18.205.202    13.226.162.80    TCP        66 59354 → 443 [ACK] Seq=79 Ack=79 Win=2
 1025 114.846011  10.18.205.202    104.18.3.173     ICMP       98 Echo (ping) request  id=0xdb41, seq=0
 1026 114.854961  104.18.3.173     10.18.205.202    ICMP       98 Echo (ping) reply    id=0xdb41, seq=0
 1027 114.876848  10.18.205.202    142.250.180.67   TLSv1…    105 Application Data
 1028 114.881968  142.250.180.67   10.18.205.202    TCP        66 443 → 59188 [ACK] Seq=435 Ack=359 Win
 1029 115.062304  142.250.180.67   10.18.205.202    TLSv1…    105 Application Data
 1030 115.062422  10.18.205.202    142.250.180.67   TCP        66 59188 → 443 [ACK] Seq=359 Ack=505 Win
 1031 115.851198  10.18.205.202    104.18.3.173     ICMP       98 Echo (ping) request  id=0xdb41, seq=1
 1032 115.860957  104.18.3.173     10.18.205.202    ICMP       98 Echo (ping) reply    id=0xdb41, seq=1
 1033 116.028027  10.18.205.202    104.16.249.249   TLSv1…    122 Application Data
```

```
> Frame 1025: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
> Ethernet II, Src: Apple_50:a3:83 (f0:18:98:50:a3:83), Dst: LannerEl_21:bc:c9 (00:90:0b:21:bc:c9)
v Internet Protocol Version 4, Src: 10.18.205.202, Dst: 104.18.3.173
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
```

```
0000  00 90 0b 21 bc c9 f0 18  98 50 a3 83 08 00 45 00   ···!···· ·P····E·
0010  00 54 76 e4 00 00 40 01  c0 29 0a 12 cd ca 68 12   ·Tv···@· ·)····h·
0020  03 ad 08 00 22 fc db 41  00 00 60 48 a5 be 00 0d   ····"··A ··`H····
0030  08 ab 08 09 0a 0b 0c 0d  0e 0f 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

Ethernet (eth),14 bytes

Packets: 938733 · Displayed: 938733 (100.0%) · Dropped: 0 (0.0%)

Profile: Default

🡐 main toolbar

🡐 filter toolbar

🡐 packet list pane

🡐 packet details pane

🡐 packet bytes pane

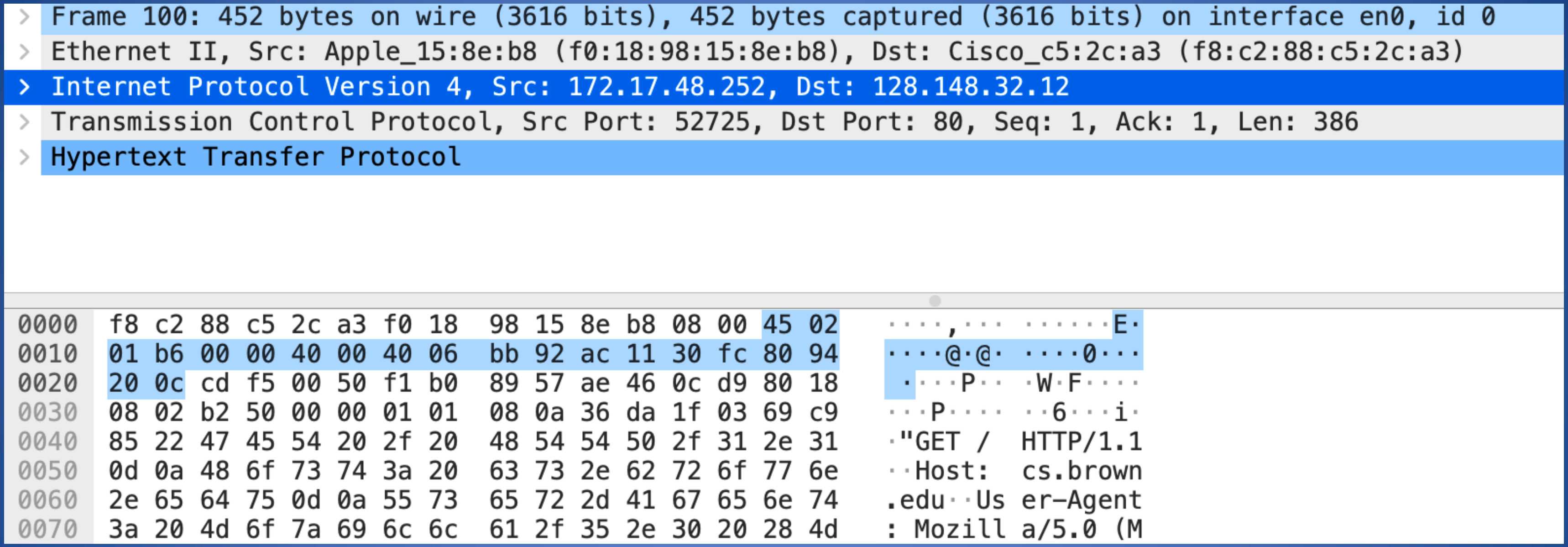
🡐 status bar

Demo: wireshark

- Make an HTTP request, examine packets
- Show stack of layers, point out IP addresses

- CERN The first website:
  – http://info.cern.ch/hypertext/WWW/TheProject.html
  – https://info.cern.ch/hypertext/WWW/TheProject.html

Anatomy of a packet



```
> Frame 100: 452 bytes on wire (3616 bits), 452 bytes captured (3616 bits) on interface en0, id 0
> Ethernet II, Src: Apple_15:8e:b8 (f0:18:98:15:8e:b8), Dst: Cisco_c5:2c:a3 (f8:c2:88:c5:2c:a3)
> Internet Protocol Version 4, Src: 172.17.48.252, Dst: 128.148.32.12
> Transmission Control Protocol, Src Port: 52725, Dst Port: 80, Seq: 1, Ack: 1, Len: 386
> Hypertext Transfer Protocol

0000  f8 c2 88 c5 2c a3 f0 18  98 15 8e b8 08 00 45 02   ····,··· ······E·
0010  01 b6 00 00 40 00 40 06  bb 92 ac 11 30 fc 80 94   ····@·@· ····0···
0020  20 0c cd f5 00 50 f1 b0  89 57 ae 46 0c d9 80 18   ·····P·· ·W·F····
0030  08 02 b2 50 00 00 01 01  08 0a 36 da 1f 03 69 c9   ···P···· ··6···i·
0040  85 22 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ·"GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  63 73 2e 62 72 6f 77 6e   ··Host:  cs.brown
0060  2e 65 64 75 0d 0a 55 73  65 72 2d 41 67 65 6e 74   .edu··Us er-Agent
0070  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 4d   : Mozill a/5.0 (M
```

Key point: packet header info tells network how to handle packet

BREAK!

5

4

3

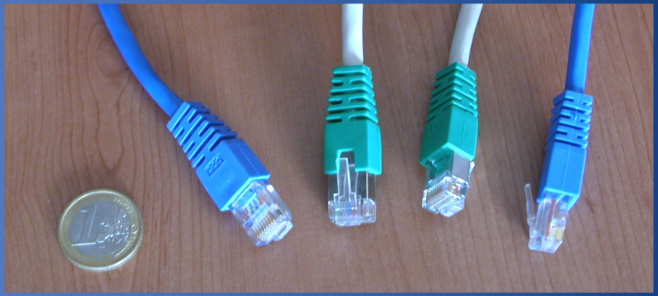
2

1

Physical & Link layer

Network Interfaces

- Network interface: connects a computer or other device to a network
  - Ethernet card, RJ-45 plug and cables
  - WiFi adapter
  - Bluetooth
  - Cellular
  - …



- A device may have multiple network interfaces

MAC Addresses

- All interfaces have a MAC address
  - 48-bit number in hex (eg. 00-1A-92-D4-BF-86)
- Used to identify devices on a *local* network (eg. single house or building)

- First three bytes: assigned to manufacturers
  - E.g., 00-1A-A1 Cisco, 00-1B-11 D-Link , 00-0a-95 Apple
- Next three bytes: assigned per device, by manufacturer

  => Pre-programmed at factory, but can be changed by OS

More on this later…

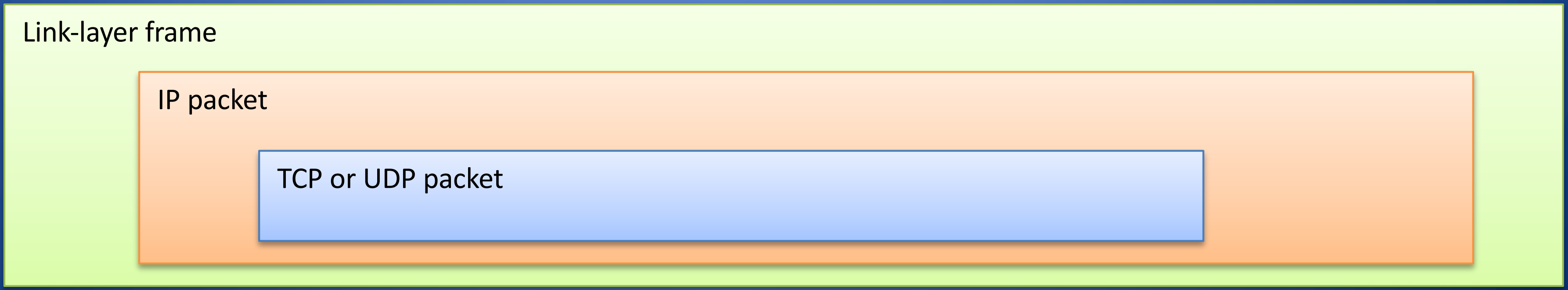
Network Layer

Internet Protocol (IP) Goals

- Addressing: Provide a unique identifier to every host on the Internet

- Routing: Unified abstraction to route between any two hosts, regardless of the type of networks involved (Ethernet, Wifi, Cellular, ...)

The Internet = > A network of networks!



IP Addressing

128.148.16.7

IP Version 4: Each address is a 32-bit number:

128.148.16.7

10000000 10010100 00010000 00000111

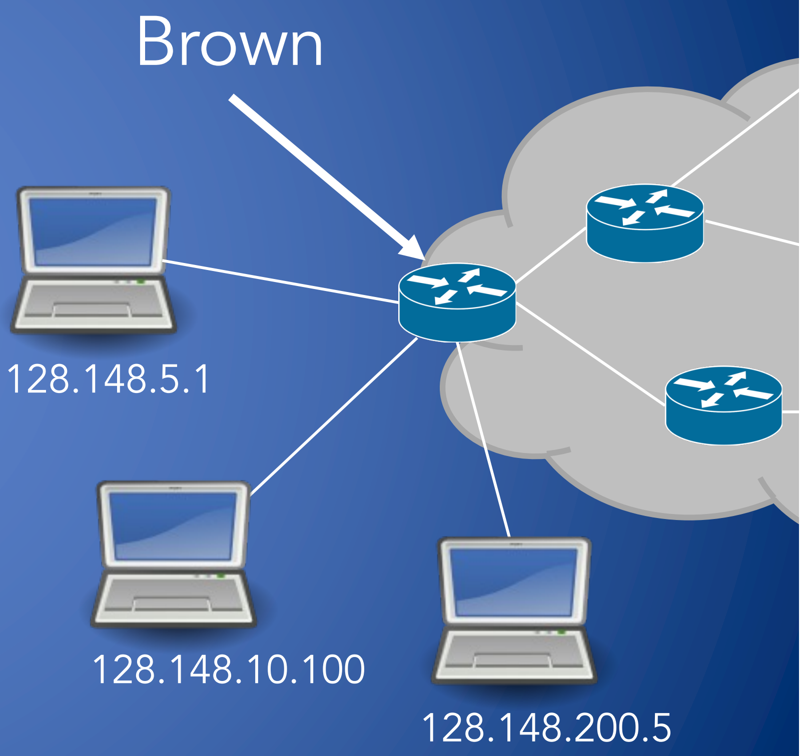
32 bits => 2^{32} possible addresses… problem?

Notation

- Write each byte ("octet") as a decimal number 0-255
- Called "dotted decimal" or "dotted quad" notation

IP Addressing

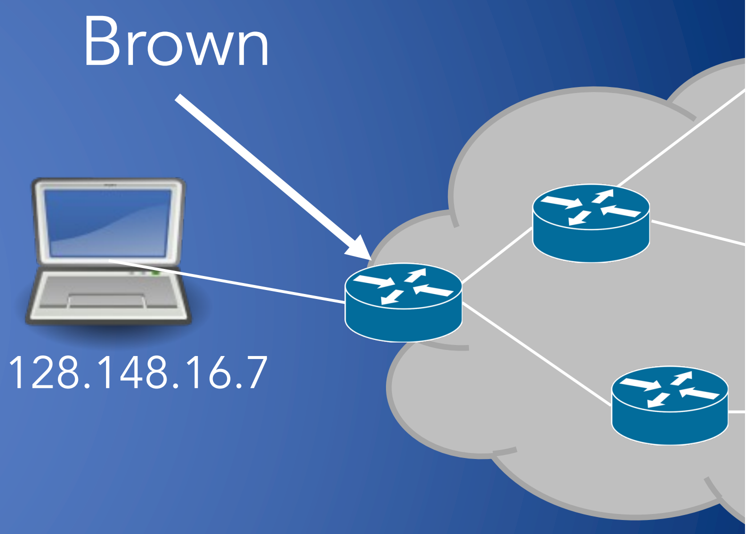
A network can designate IP addresses for its own hosts within its address range



IP Addressing

An IP address identifies…

- *Who* a host is: A unique number
- *Where* it is on the Internet



Brown

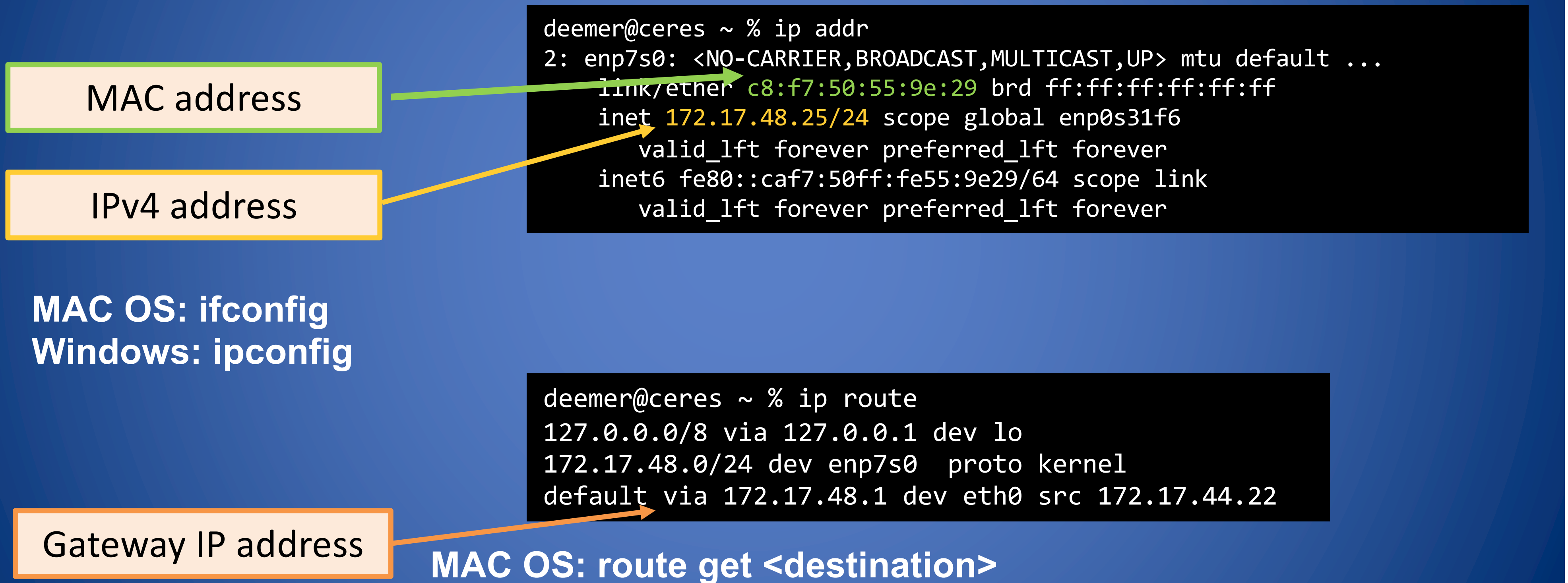
128.148.16.7

- Networks are allocated ranges of IPs by global authority (ICANN)
  - Further subdivided by regions, ISPs, …
  - US-biased, especially in early internet
- Some IPs have special uses (eg. 127.0.0.1)

eg. Brown owns 128.148.xxx.xxx, 138.16.xxx.xxx

*ICANN (Internet Corporation for Assigned Names and Numbers)

Viewing Network Configuration



MAC address

IPv4 address

```
deemer@ceres ~ % ip addr
2: enp7s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu default ...
    link/ether c8:f7:50:55:9e:29 brd ff:ff:ff:ff:ff:ff
    inet 172.17.48.25/24 scope global enp0s31f6
       valid_lft forever preferred_lft forever
    inet6 fe80::caf7:50ff:fe55:9e29/64 scope link
       valid_lft forever preferred_lft forever
```

MAC OS: ifconfig
Windows: ipconfig

```
deemer@ceres ~ % ip route
127.0.0.0/8 via 127.0.0.1 dev lo
172.17.48.0/24 dev enp7s0  proto kernel
default via 172.17.48.1 dev eth0 src 172.17.44.22
```

Gateway IP address

MAC OS: route get <destination>
Windows: route print

Brown's IP Space

- Brown separates the network connecting dorms and the network connecting offices and academic buildings
  - Class B network 138.16.0.0/16 (64K addresses)
  - Class B network 128.148.0.0/16 (64K addresses)
- CS department
  - Several class C (/24) networks, each with 254 addresses
  - Tstaff supported machines: 128.148.31.0/24, 128.148.33.0/24, 128.148.38.0/24
  - Unsupported machines:128.148.36.0/24

– Public information available: e.g. bgp.he.net

A Simple Internet Protocol

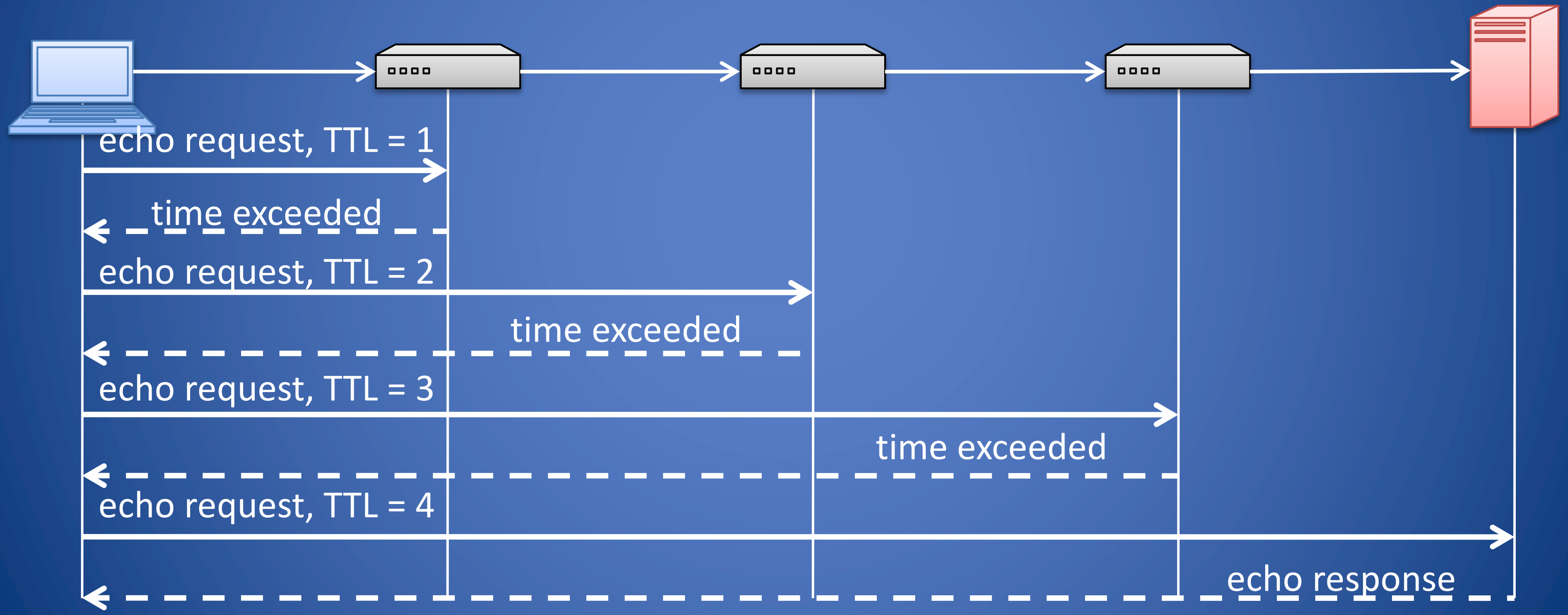
- Internet Control Message Protocol (ICMP)
  - Used for network testing and debugging
  - Network-layer protocol: simple messages about IP forwarding/routing
- Tools based on ICMP
  - Ping: send a message to an IP, get a response back
  - Traceroute: sends series ICMP packets with increasing TTL value to discover routes

TTL: Time to Live

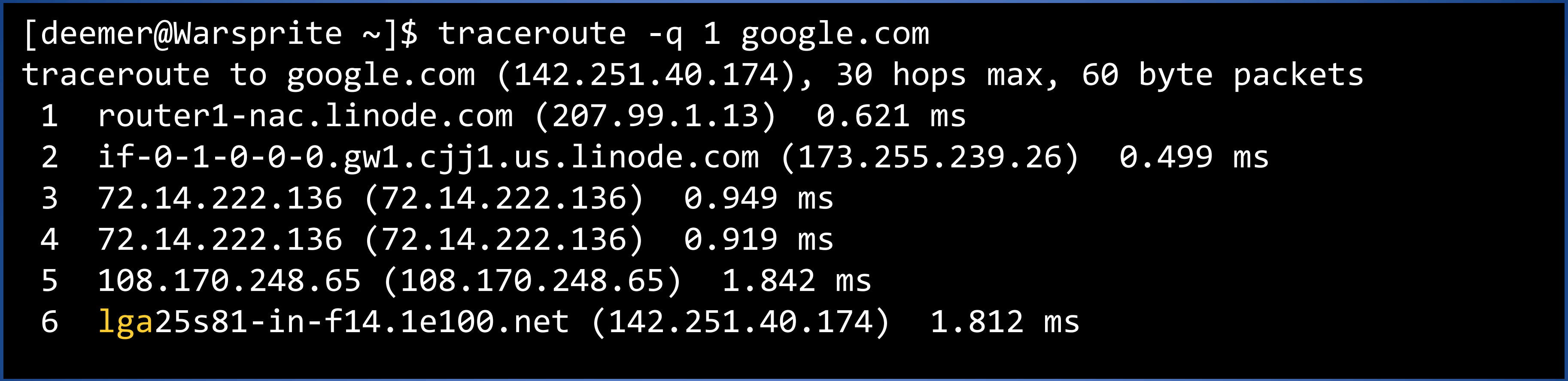
- When TTL reaches 0, router may send back an error
  - "ICMP TTL exceeded" message
- If it does, we can identify a path used by a packet!

=> Traceroute takes advantage of this

Traceroute

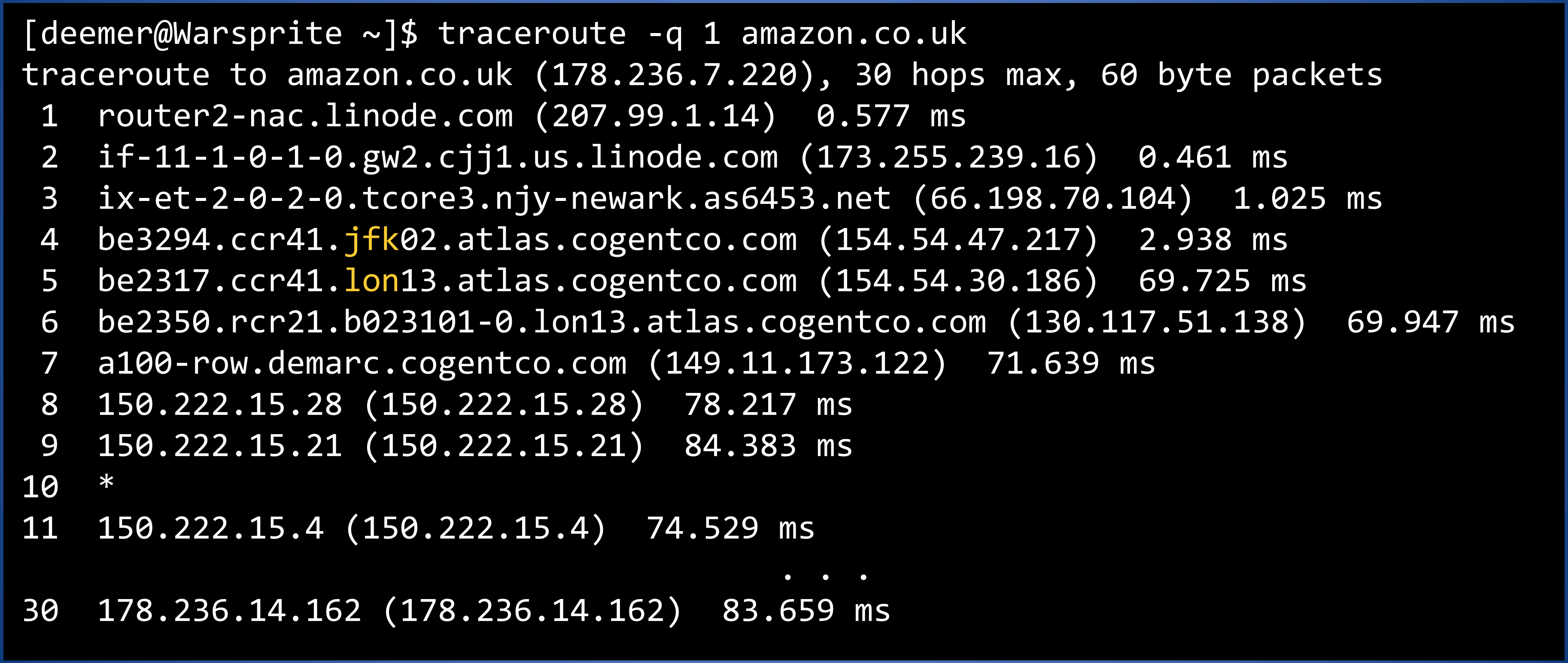

echo request, TTL = 1
time exceeded
echo request, TTL = 2
time exceeded
echo request, TTL = 3
time exceeded
echo request, TTL = 4
echo response

Traceroute example



```
[deemer@Warsprite ~]$ traceroute -q 1 google.com
traceroute to google.com (142.251.40.174), 30 hops max, 60 byte packets
 1  router1-nac.linode.com (207.99.1.13)  0.621 ms
 2  if-0-1-0-0-0.gw1.cjj1.us.linode.com (173.255.239.26)  0.499 ms
 3  72.14.222.136 (72.14.222.136)  0.949 ms
 4  72.14.222.136 (72.14.222.136)  0.919 ms
 5  108.170.248.65 (108.170.248.65)  1.842 ms
 6  lga25s81-in-f14.1e100.net (142.251.40.174)  1.812 ms
```

Traceroute example



```
[deemer@Warsprite ~]$ traceroute -q 1 amazon.co.uk
traceroute to amazon.co.uk (178.236.7.220), 30 hops max, 60 byte packets
 1  router2-nac.linode.com (207.99.1.14)  0.577 ms
 2  if-11-1-0-1-0.gw2.cjj1.us.linode.com (173.255.239.16)  0.461 ms
 3  ix-et-2-0-2-0.tcore3.njy-newark.as6453.net (66.198.70.104)  1.025 ms
 4  be3294.ccr41.jfk02.atlas.cogentco.com (154.54.47.217)  2.938 ms
 5  be2317.ccr41.lon13.atlas.cogentco.com (154.54.30.186)  69.725 ms
 6  be2350.rcr21.b023101-0.lon13.atlas.cogentco.com (130.117.51.138)  69.947 ms
 7  a100-row.demarc.cogentco.com (149.11.173.122)  71.639 ms
 8  150.222.15.28 (150.222.15.28)  78.217 ms
 9  150.222.15.21 (150.222.15.21)  84.383 ms
10  *
11  150.222.15.4 (150.222.15.4)  74.529 ms
                                        . . .
30  178.236.14.162 (178.236.14.162)  83.659 ms
```

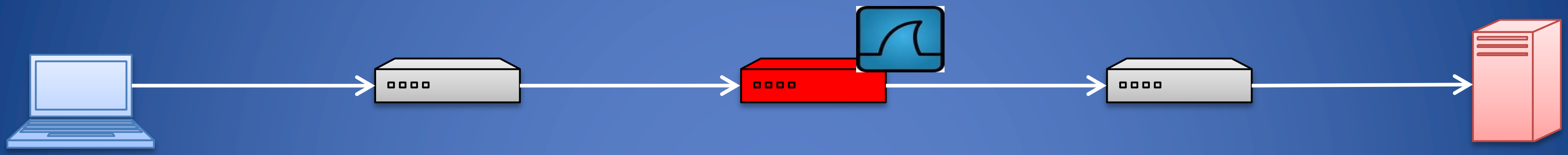
Practicing Ping and Traceroute

- Linux/Unix/Macos
  - ifconfig
  - ping www.brown.edu
  - traceroute www.brown.edu
- Windows
  - ipconfig
  - tracert www.brown.edu

Practice with Wireshark

- Checking a connection
  - Ping 127.0.0.1 (localhost)
  - Ping <your-ip-address> (ifconfig)
  - Ping www.brown.edu
- Traceroute www.brown.edu
- Let’s see in Wireshark
- Let’s see in geotraceroute.com

Sniffing: not just for hosts?



- Any network device that sees packets could be an eavesdropper

- This is why we encrypt traffic in transit!

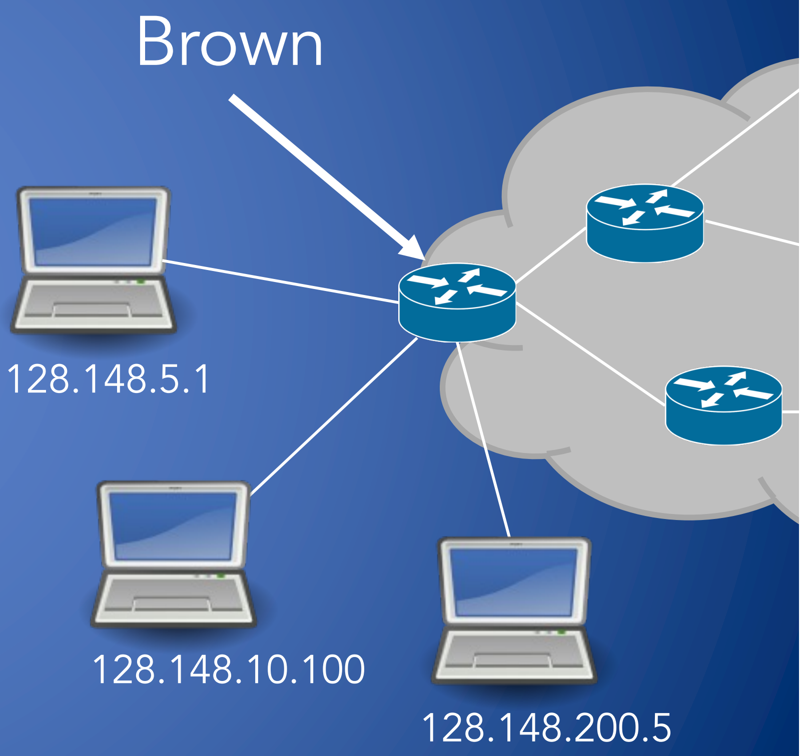
How do we move packets *between* networks?

IP Addressing

A network can designate IP addresses for its own hosts within its address range

How? Every address has two parts:

- Network part: identifies the network (eg. "Brown") to the Internet
- Host part: identifies individual hosts within Brown

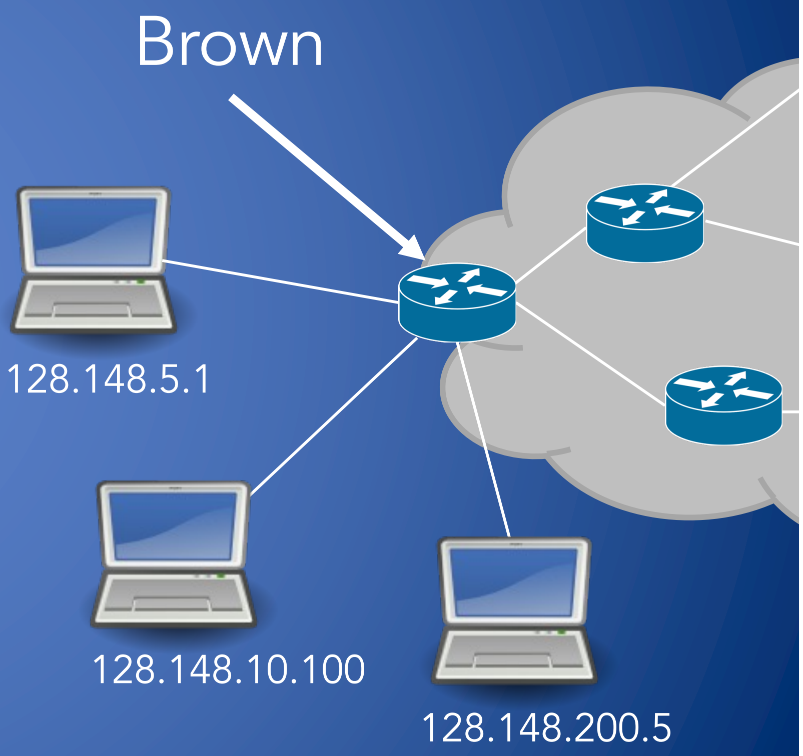


IP Addressing

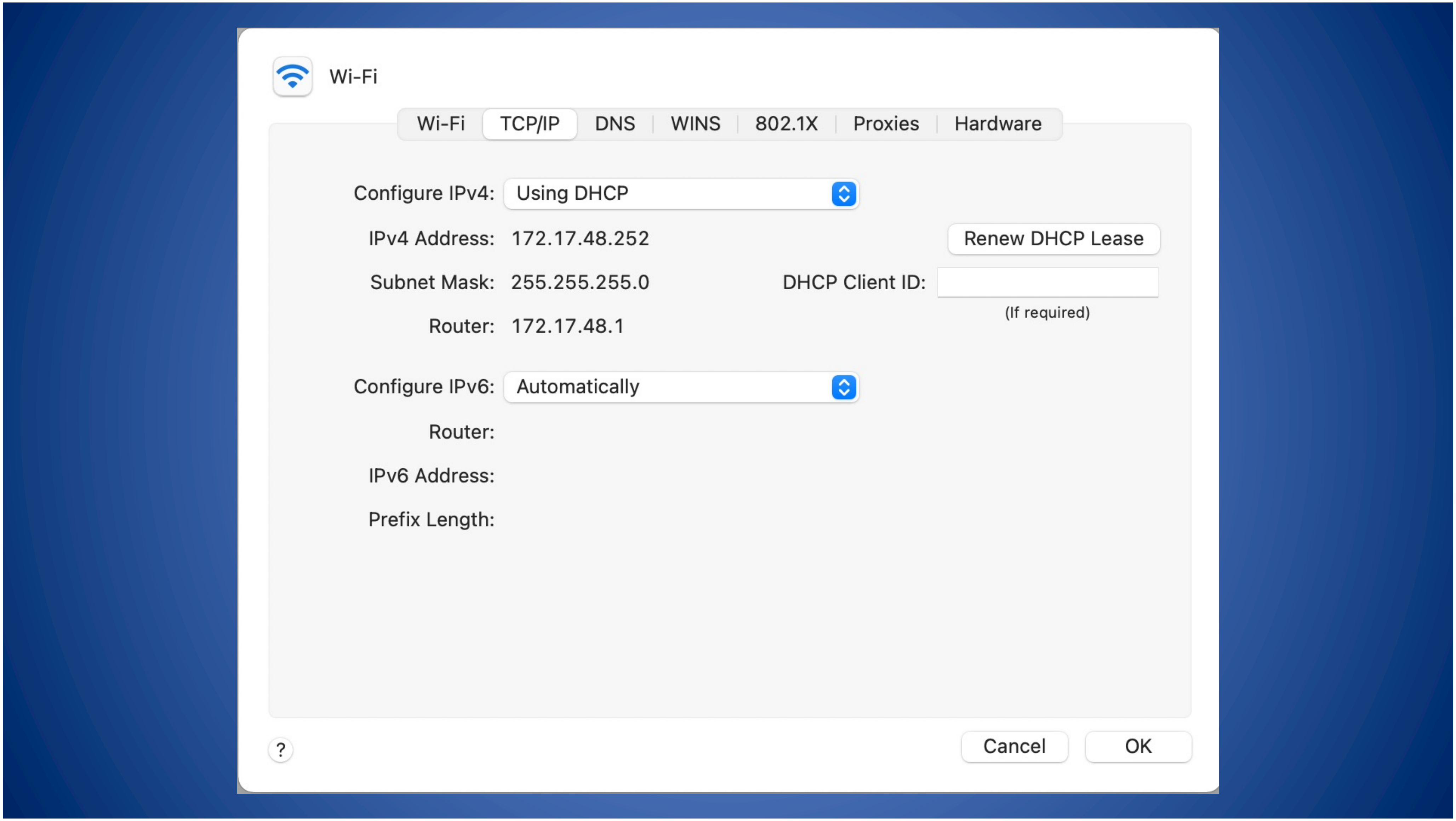
A network can designate IP addresses for its own hosts within its address range

How? Every address has two parts:

- Network part: identifies the network (eg. "Brown") to the Internet
- Host part: identifies individual hosts within Brown



Why? Routers need to check which *network* an address belongs to



Configure IPv4: Using DHCP

IPv4 Address: 172.17.48.252

Subnet Mask: 255.255.255.0

DHCP Client ID:

(If required)

Router: 172.17.48.1

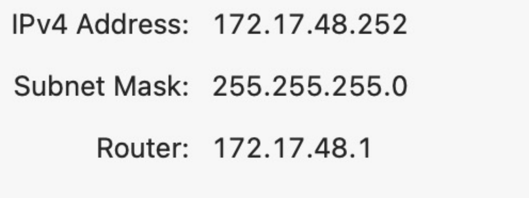
Configure IPv6: Automatically

Router:

IPv6 Address:

Prefix Length:

Components of an IP



IPv4 Address: 172.17.48.252

Subnet Mask: 255.255.255.0

Router: 172.17.48.1

172.17.48.252

Addr: 172.17.48.252   10101100 00010001 00110000 11111100

Mask: 255.255.255.0   11111111 11111111 11111111 00000000

Key point: networks can be of different sizes!
=>The "subnet mask" defines what part of is the network part

Common Prefix Sizes

Prefix	IPs	Number of hosts	Note
1.2.3.0/24	1.2.3.*	2^8 = 256	Common for local networks (LANs) Old term: "Class C"
1.2.0.0/16	1.2.*.*	2^16 = 65536	Old term: "Class B" Large (or older) organizations
1.0.0.0/8	1.*.*.*	2^24 = ~16M	Old term: "Class A"
1.2.3.100/30	1.2.3.1-1.2.3.3	4	A smaller prefix

Special/private IP ranges

Prefix	Note
127.0.0.0/8	Localhost (for networks on same system), usually 127.0.0.1
192.168.0.0/16	Private: often used for home networks
10.0.0.0/8	Private: often used for larger organizations (eg. Brown)
172.16.0.0/12	Private: larger space for organizations, systems (eg. Docker)

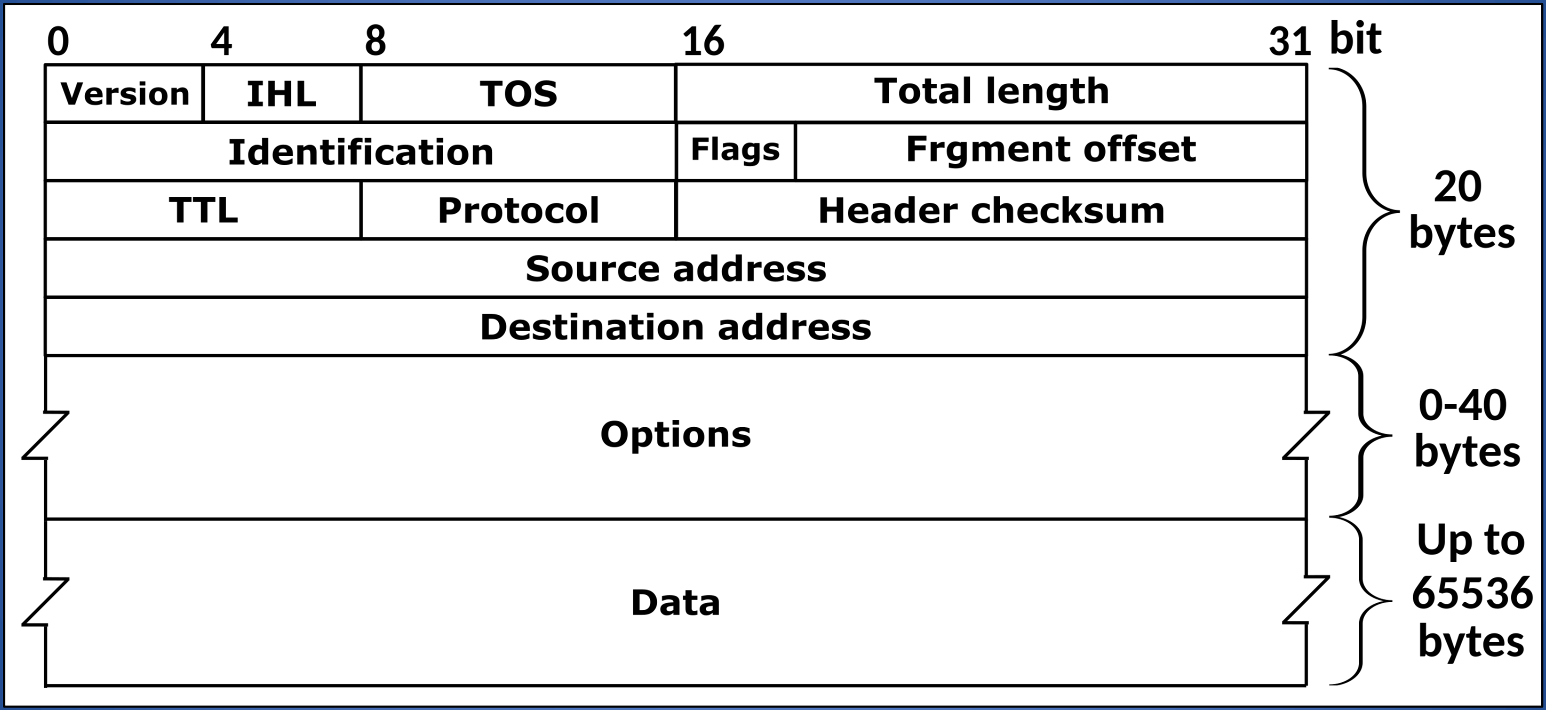
- Used for LANs, private networks *not* publicly routable on the global internet RFC 1918
- More on this later

IP Address Space and ICANN

- Hosts on the internet must have unique IP addresses
- Internet Corporation for Assigned Names and Numbers
  - International nonprofit organization
  - Incorporated in the US
  - Allocates IP address space
  - Manages top-level domains
- Historical bias in favor of US corporations and nonprofit organizations

003/8	May 94	General Electric
009/8	Aug 92	IBM
012/8	Jun 95	AT&T Bell Labs
013/8	Sep 91	Xerox Corporation
015/8	Jul 94	Hewlett-Packard
017/8	Jul 92	Apple Computer
018/8	Jan 94	MIT
019/8	May 95	Ford Motor
040/8	Jun 94	Eli Lily
043/8	Jan 91	Japan Inet
044/8	Jul 92	Amateur Radio Digital
047/8	Jan 91	Bell-Northern Res.
048/8	May 95	Prudential Securities
054/8	Mar 92	Merck
055/8	Apr 95	Boeing
056/8	Jun 94	U.S. Postal Service

The IPv4 Header



0 4 8 16 31 bit

Version | IHL | TOS | Total length

Identification | Flags | Frgment offset

TTL | Protocol | Header checksum

Source address

Destination address

Options

Data

20 bytes

0-40 bytes

Up to 65536 bytes

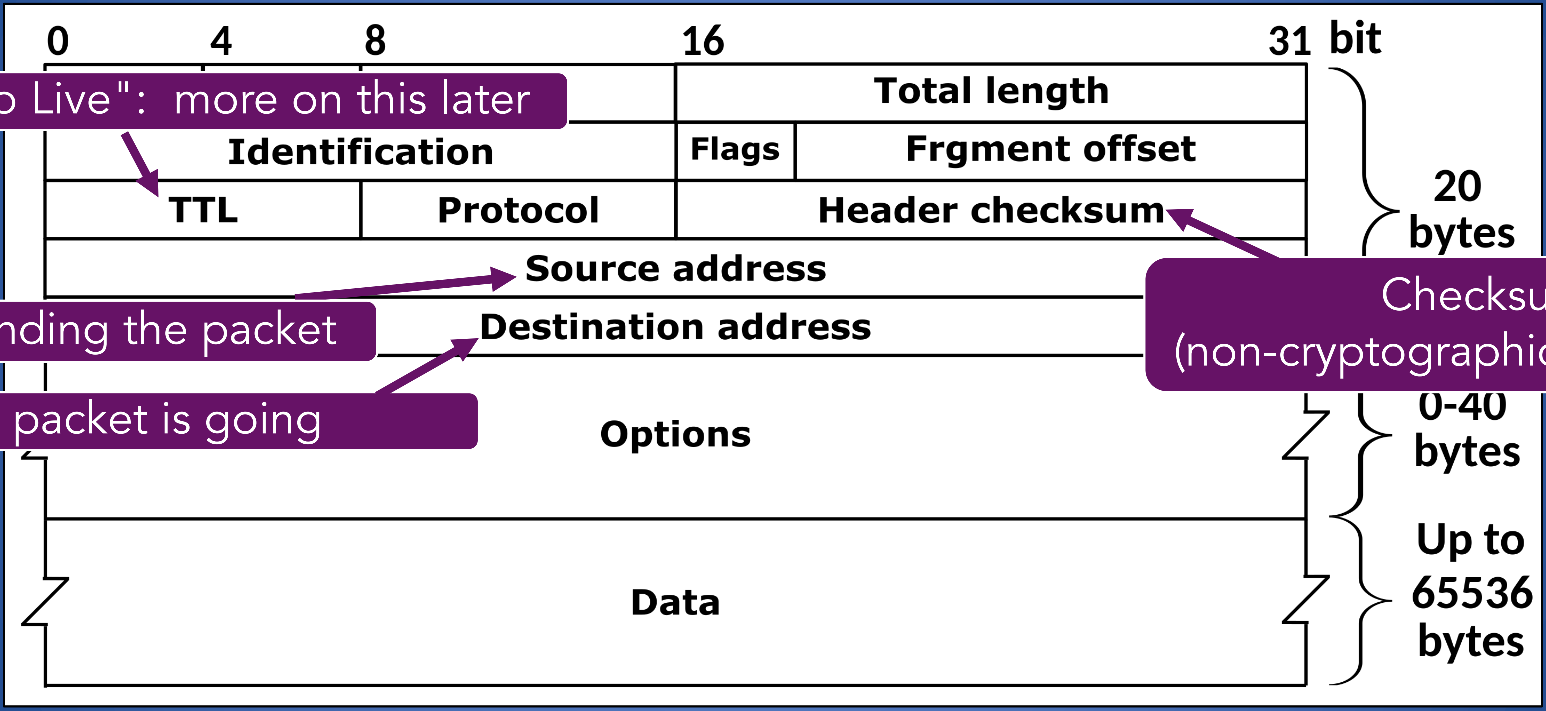
Defined by RFC 791

RFC (Request for Comment): defines network standard

IP Routing

- A router connects two or more networks
  - Maintains tables to forward packets to the appropriate network
  - Forwarding decisions based solely on the destination address
  - Hosts (regular systems) can be routers too!
- Routing table
  - Maps ranges of addresses to LANs or other gateway routers

The IPv4 Header



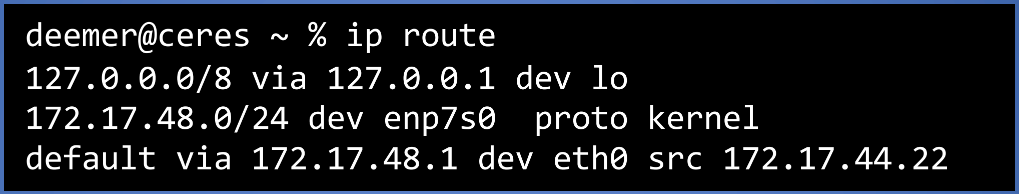
"Time to Live": more on this later

Host sending the packet

Where packet is going

Checksum
(non-cryptographic, very weak!

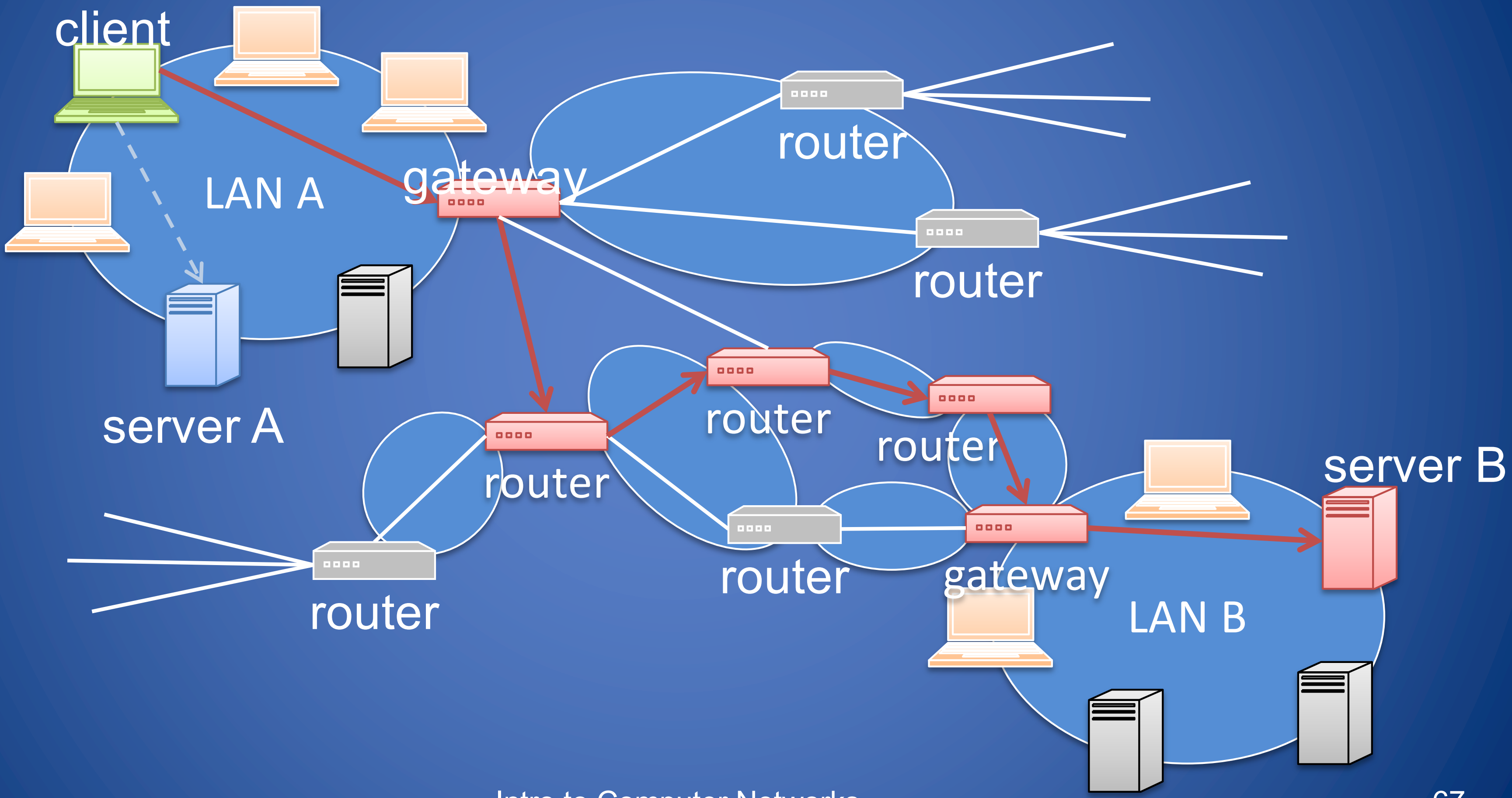
Example routing table



```
deemer@ceres ~ % ip route
127.0.0.0/8 via 127.0.0.1 dev lo
172.17.48.0/24 dev enp7s0  proto kernel
default via 172.17.48.1 dev eth0 src 172.17.44.22
```

- "Default": where to send packets when they go to a network you don't know about
- Also known as "next hop"

Routing Examples



What we Have Learned

- Packet routing
- Internet protocol layers
  - Encapsulation
- Link layer
  - MAC addresses
  - Operation of switches
  - MAC access control
- Network layer
  - IP addresses
  - Operation of routers
- Practicing ping and traceroute utilities
- Industry of Anonymity