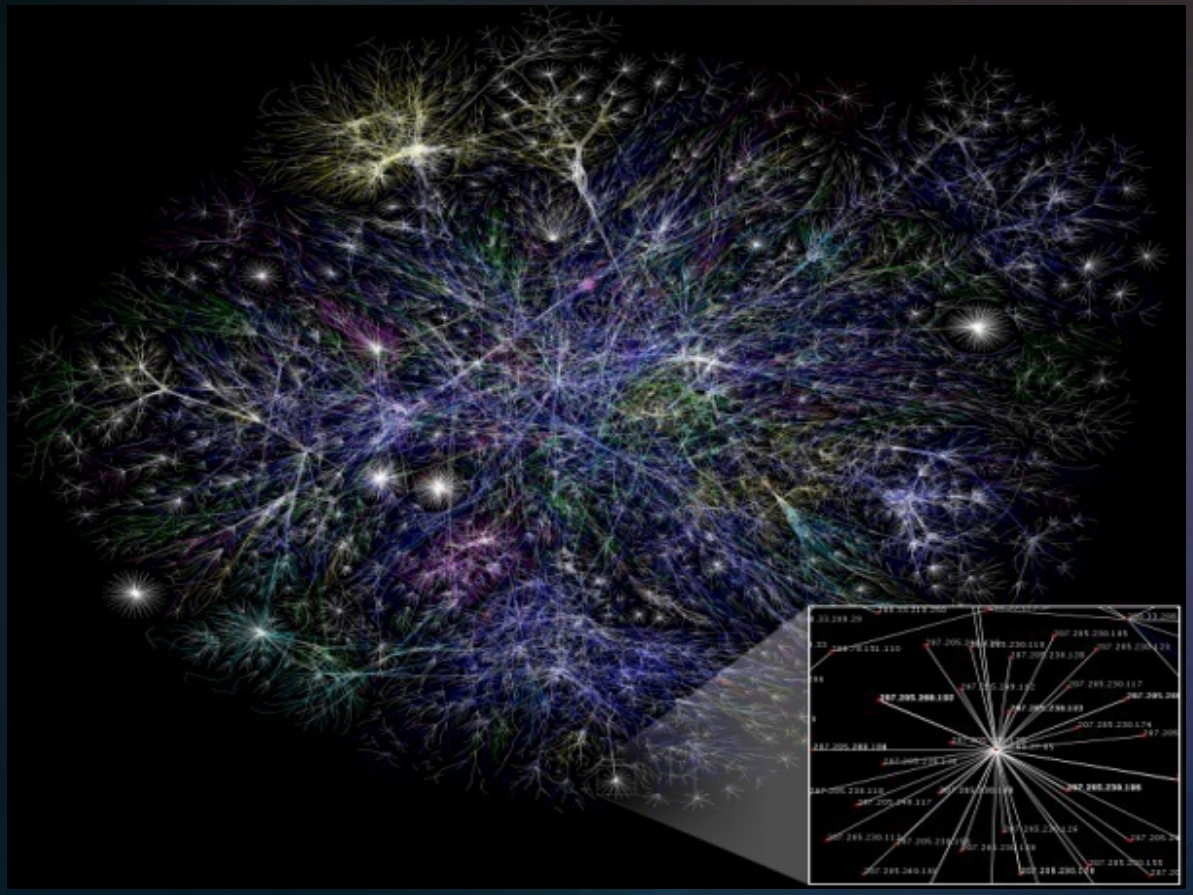
TCP/IP Networking in a Nutshell



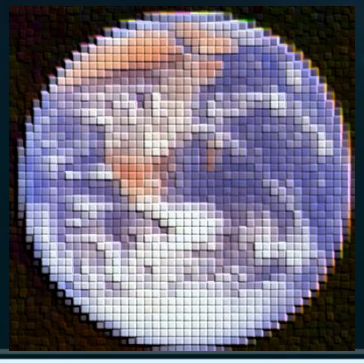
Tanmay Bhagwat

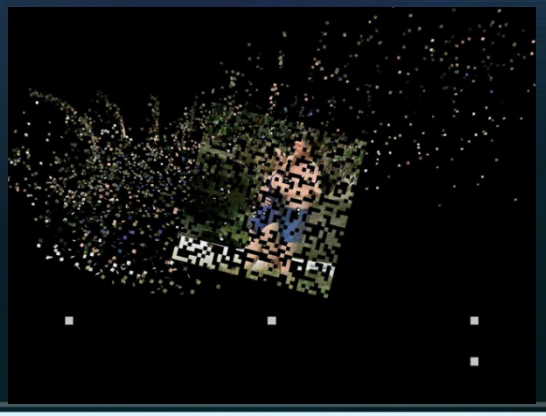
(Slides borrowed from Kevin Cleary and modified as required)

UB Cyber and Network Defense

The Internet

- The Internet is governed by a series of protocols that form the rules for how communications should happen
- The Internet is a network of networks.
  - There is no centralized point.
  - There are no boundaries.
- Information that is sent from one location on the internet to another is broken down into smaller, more manageable pieces called “packets”.

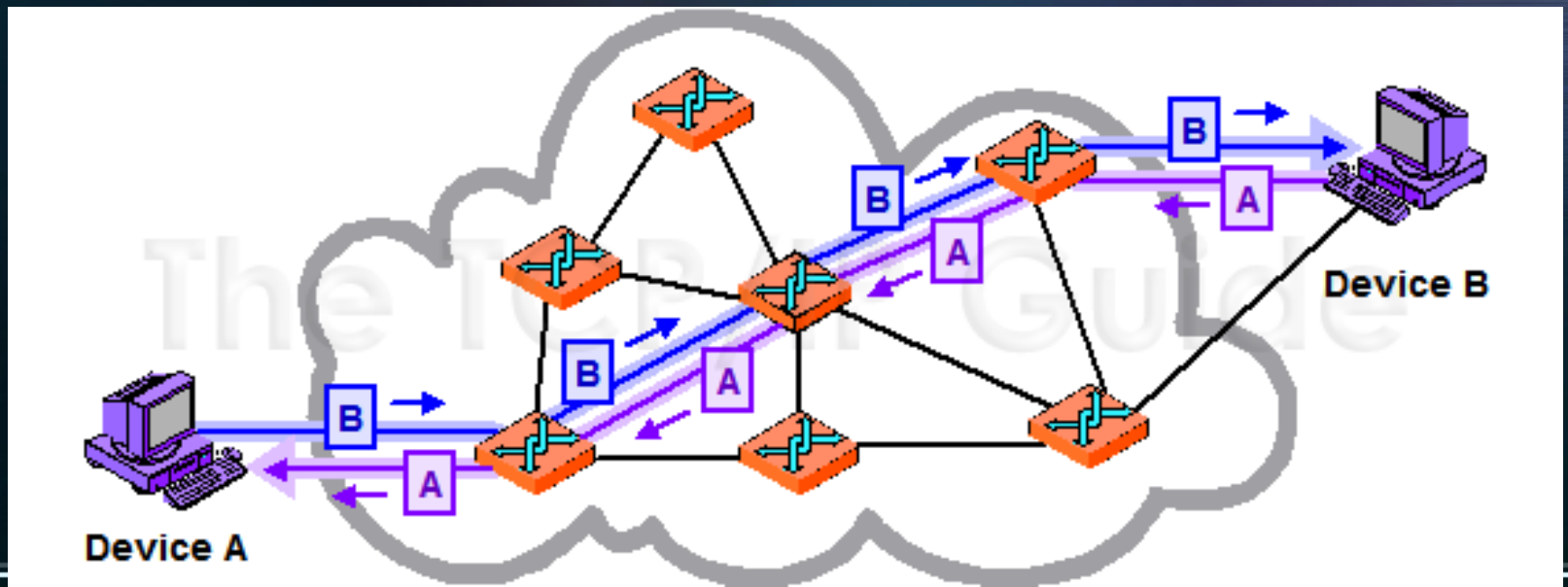




DARPA

Circuit (Message) Switching

- A means of connecting two devices in which there is a dedicated “line” or connection between the two devices.
- The established connection remains active for the duration of the message transmission.
- This is how the public switched telephone network works.

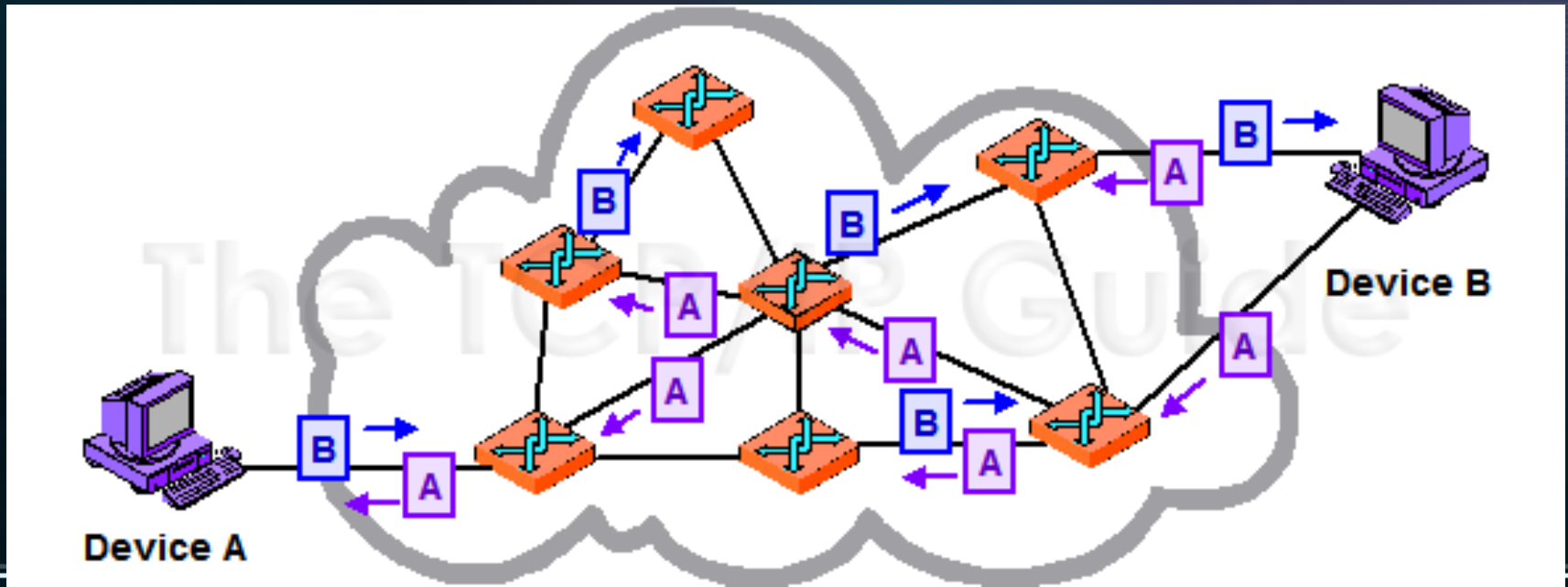


Circuit (Message) Switching

- Advantages:
  - Good for when communicated information must be received in order.
- Disadvantages:
  - This form of communication is very inefficient for computers.
    - Low Link utilization
  - A single failure anywhere along the communication path will stop all packet flow.

Packet Switching

- Packets are sent on their own, independently, to their destination.
  - Packets may take different routes.
  - Packets may arrive out of order.
  - A small number may not even arrive.
- Packet switching does not require a dedicated communications circuit.



Packet Switching

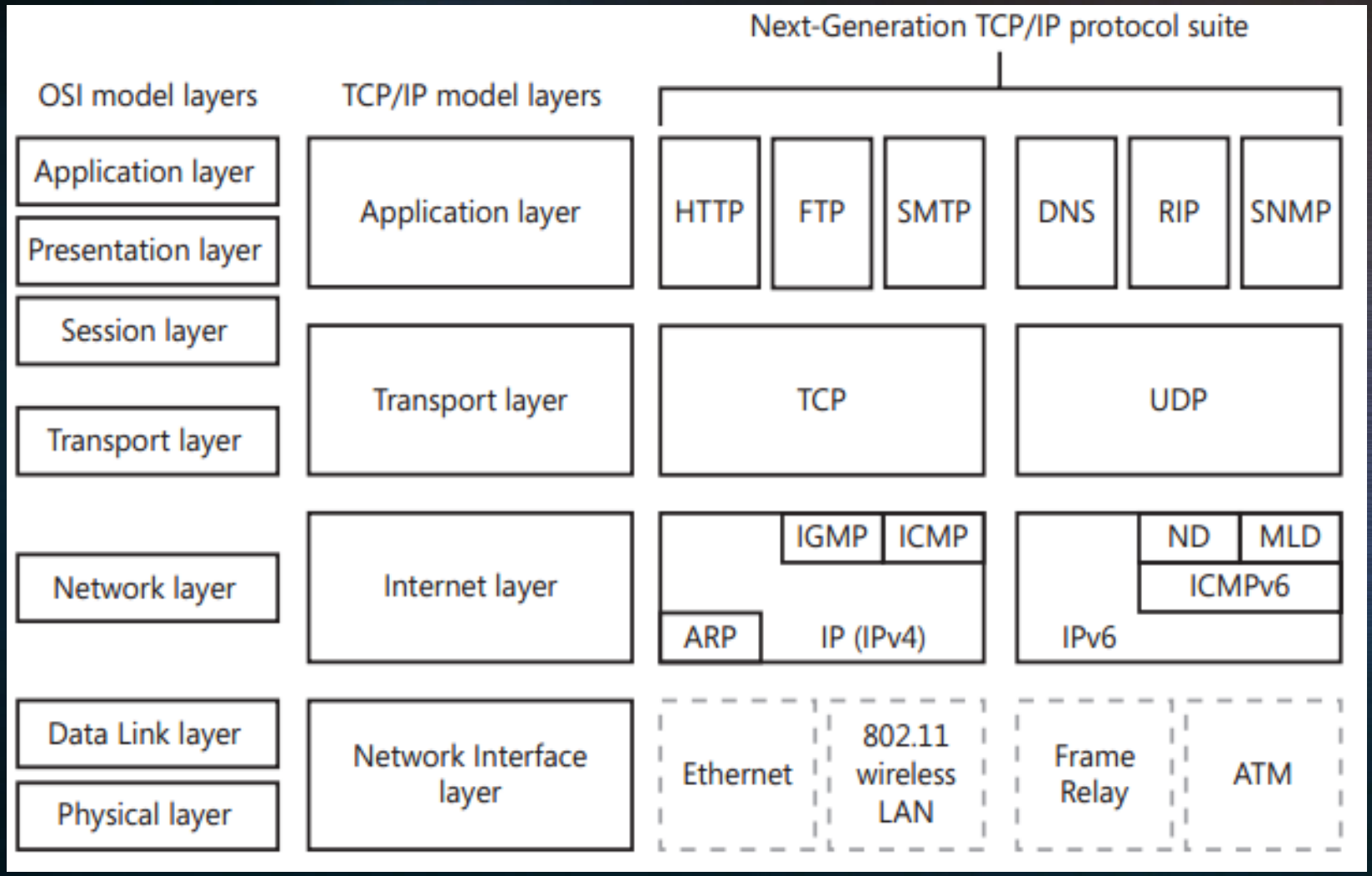
- Advantages:
  - More tolerant to failures
  - Better utilization of an internet connection
- Disadvantages:
  - Packets may arrive out of order
  - Packets may not arrive at all!

Protocol Stacks

- The protocol stack used by every computer on the Internet is known as TCP/IP.

- The TCP/IP protocol stack takes care of how computer communications get routed to the correct computer and how the applications assemble and make sense of newly arrived packets.

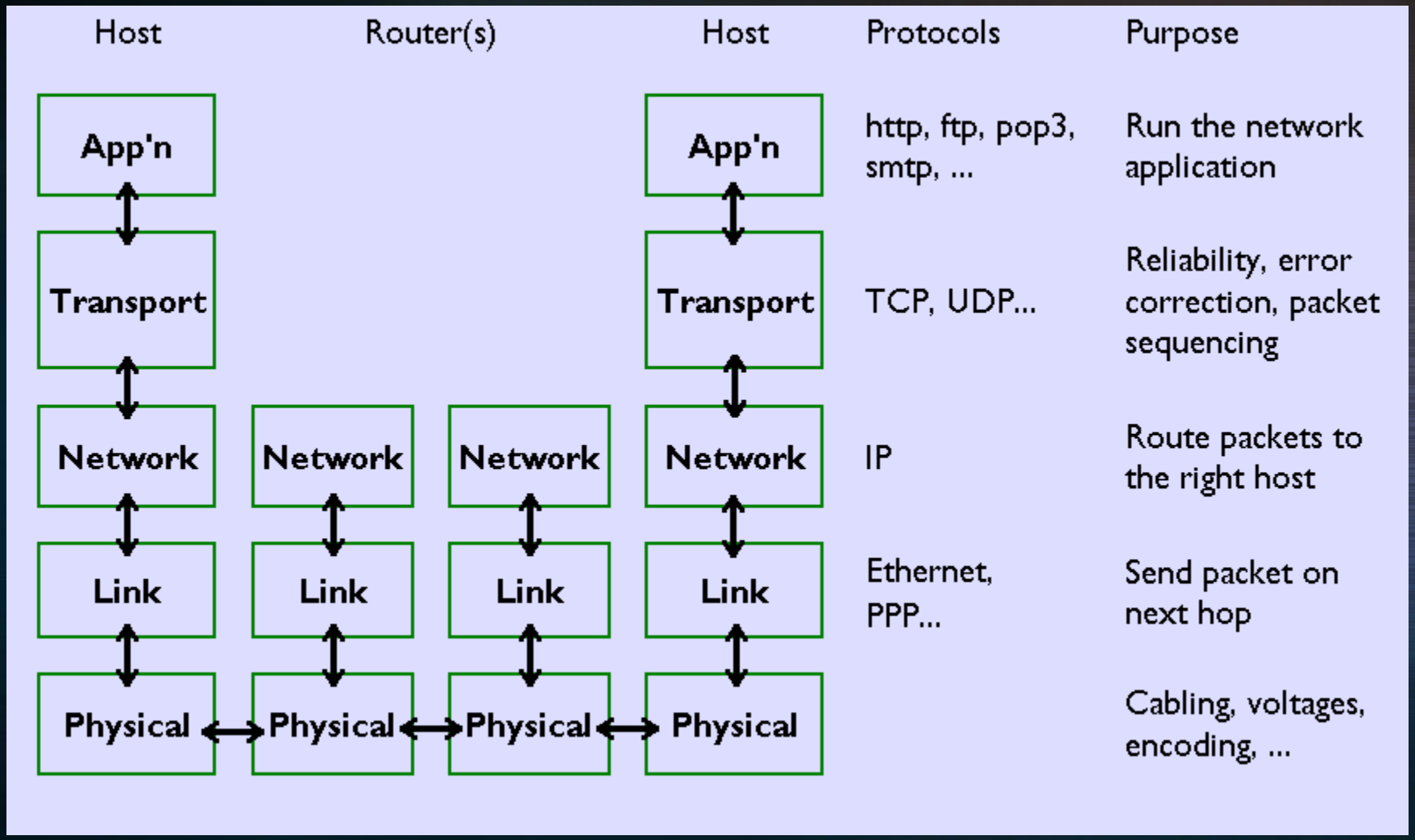
TCP/IP Stack


Next-Generation TCP/IP protocol suite
OSI model layers
TCP/IP model layers
Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data Link layer
Physical layer
Application layer
Transport layer
Internet layer
Network Interface layer
HTTP
FTP
SMTP
DNS
RIP
SNMP
TCP
UDP
IGMP
ICMP
ARP
IP (IPv4)
ND
MLD
ICMPv6
IPv6
Ethernet
802.11 wireless LAN
Frame Relay
ATM

Protocol Stacks

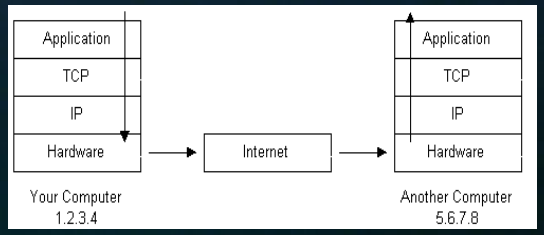
- When an applications whishes to send a message over the internet it hands the message off to the protocol stack. Each protocol within the stack has some task.
- Your application passes information on to the TCP layer to be broken up in to manageable chunks called packets.
  - Information is added to the packet headers for re-assembly.
    - Sequencing numbers
    - Session IDs
- The IP layer takes care of steering these packets.
- The Hardware physical transmits packets (frames).

Wait what?


Host
Router(s)
Host
Protocols
Purpose
App'n
Transport
Network
Link
Physical
App'n
Transport
Network
Link
Physical
Network
Link
Physical
Network
Link
Physical
http, ftp, pop3, smtp, ...
TCP, UDP...
IP
Ethernet, PPP...
Run the network application
Reliability, error correction, packet sequencing
Route packets to the right host
Send packet on next hop
Cabling, voltages, encoding, ...

The Transport Layer

- This layer takes care of breaking application information in to chunks, known as “packets” and assigning those packets information such as:
  - Port number - help to separate what data is destined to which applications.
    - Email and Web browsers have a specific, unique port number
  - Number of packets sent
  - The number the packet in the series being sent.
  - On the receiving end the TCP protocol helps to arrange packets as they arrive in the correct order for the applications.



Protocol Stacks

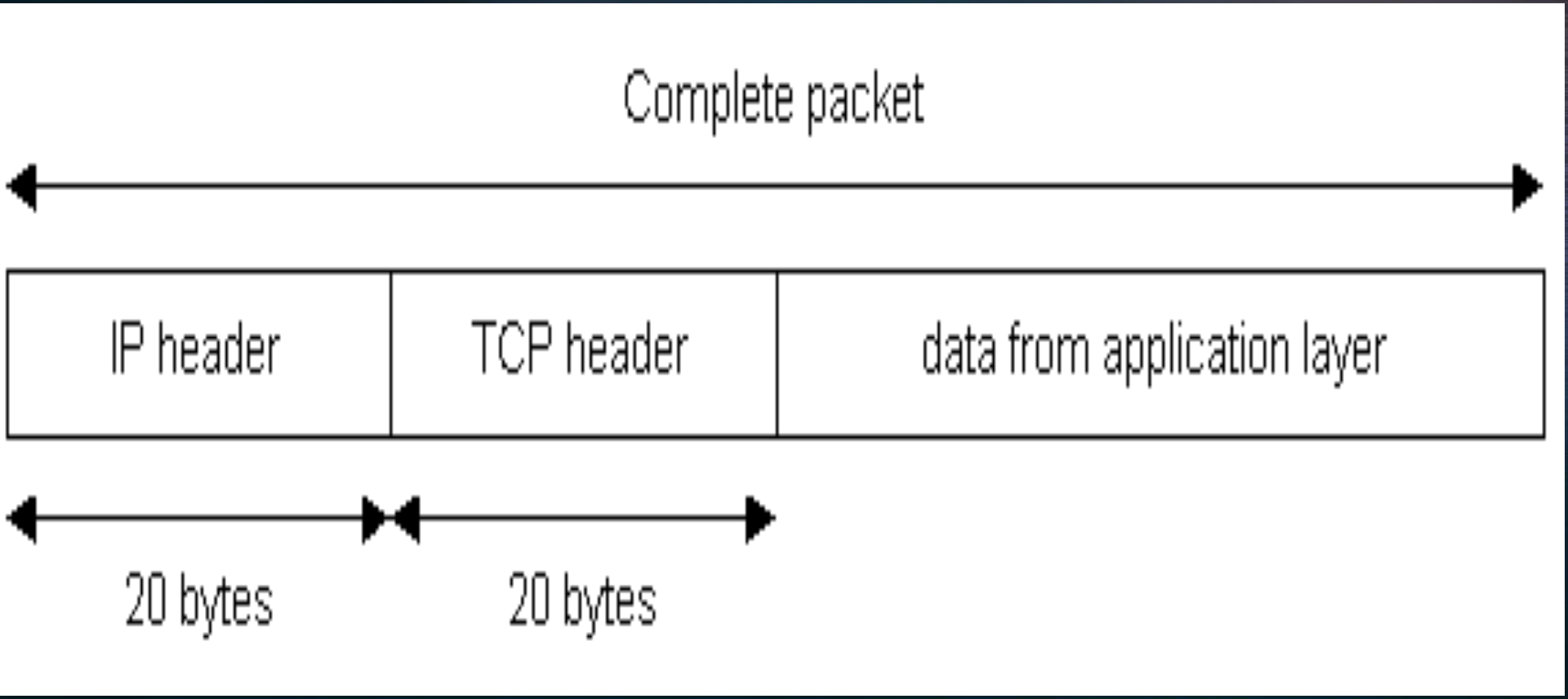
- TCP is a connection-oriented, message switched, reliable, byte stream service.
  - Connection-oriented means that two applications using TCP must first establish a connection before exchanging data (a handshake).
  - TCP is reliable because for each packet received, an acknowledgement is sent to the sender.
  - A cousin of TCP, User Datagram Protocol (UDP) is commonly used for streaming.
    - A connectionless, unreliable protocol
  - A series of diagnostic tools exist at the TCP layer, the Internet Control Messaging Protocol ICMP.
    - Popular tools include “ping” and “traceroute”.

Protocol Stacks

- IP is an unreliable, connectionless, packet switched protocol.
  - IP's job is to send and route packets to other routers / computers.
  - IP packets are independent entities and may arrive out of order or not at all.
  - IP does not guarantee packet delivery.
- Steering devices called routers maintain multiple connections to one another.
  - These form the backbones of the Internet
  - Routers continually “talk” to each other to keep track of:
    - Links speeds
    - Latency
    - Health

Protocol Stacks

- Each layer places its information in the "packet header".
  - This is information needed to deliver and re-order the packet once it has arrived to its destination.



Packet Routing at the IP Layer

- IP packet routing is similar to mailing a letter.
- The steps you take in mailing a letter include…
  - Sealing your message in to an envelope.
  - Looking up the address to write on the envelope.
  - Determine if you can hand deliver your message or if it needs to be given to the mail man.
  - If the mailman must deliver the message you must hand the message off to them. The mailman works with other mailmen to then deliver your envelope.
  - Wait for a response.

Local Area Networks

- LANs are the most basic type of network.
  - These small networks are the building blocks of the Internet.
  - Can be thought of as a “local neighborhood” of computers or devices
  - All devices on the same LAN communicate directly with one another across a “switch” (collision domain).
  - Network and LAN segmentation is a fundamental security concept.
    - LANs can be organized by :
      - Geographic area
      - Device type
      - Administrative boundary

Wide Area Networks

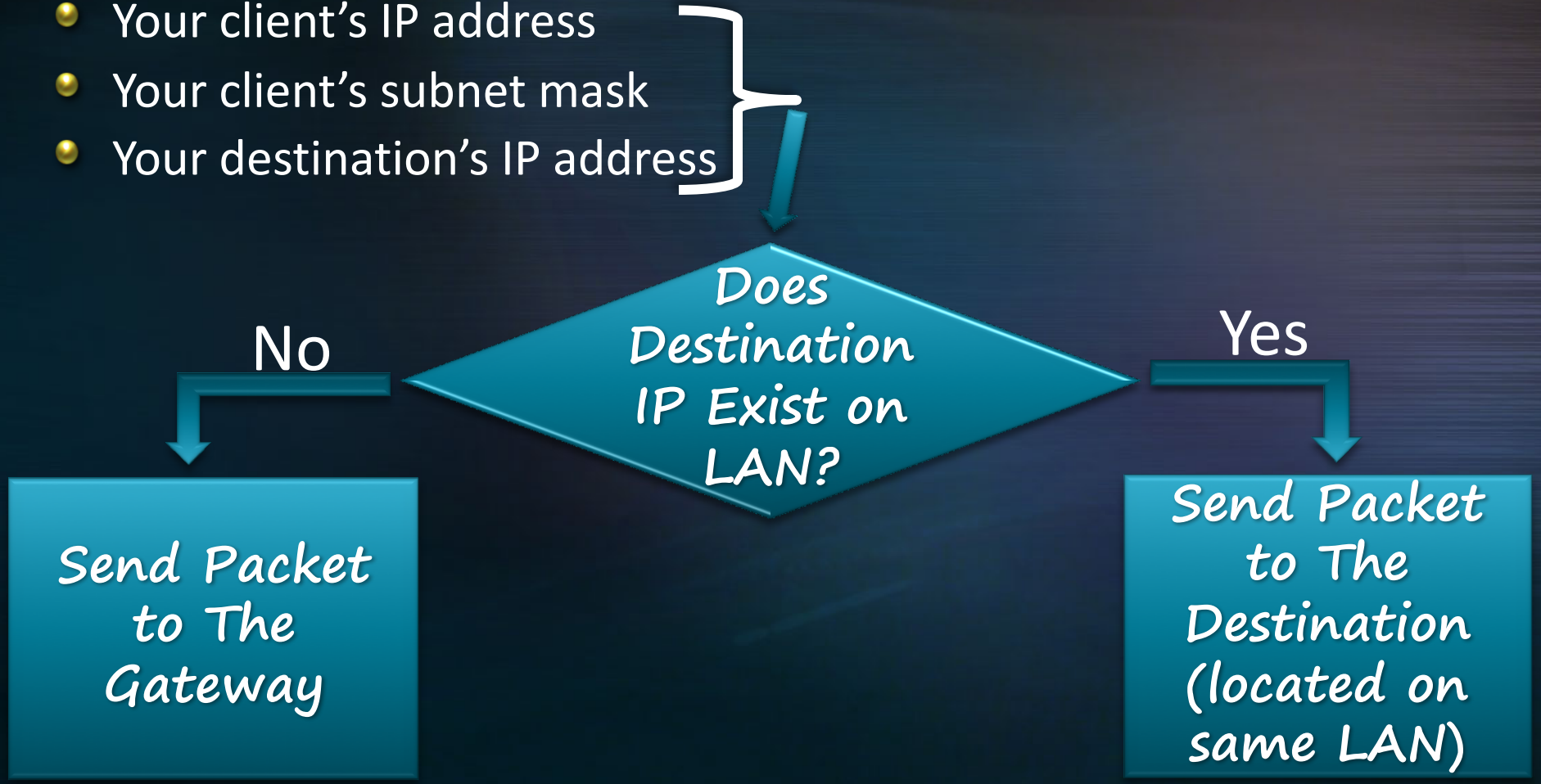
- LANs are connected together to form WANs
  - LANs get connected to WANs through routers.
  - The “Internet” is one big WAN.
  - We can connect LANs to WANs through both wireless and Wired Connections.
  - WANs can span much larger geographic distances than LANs.

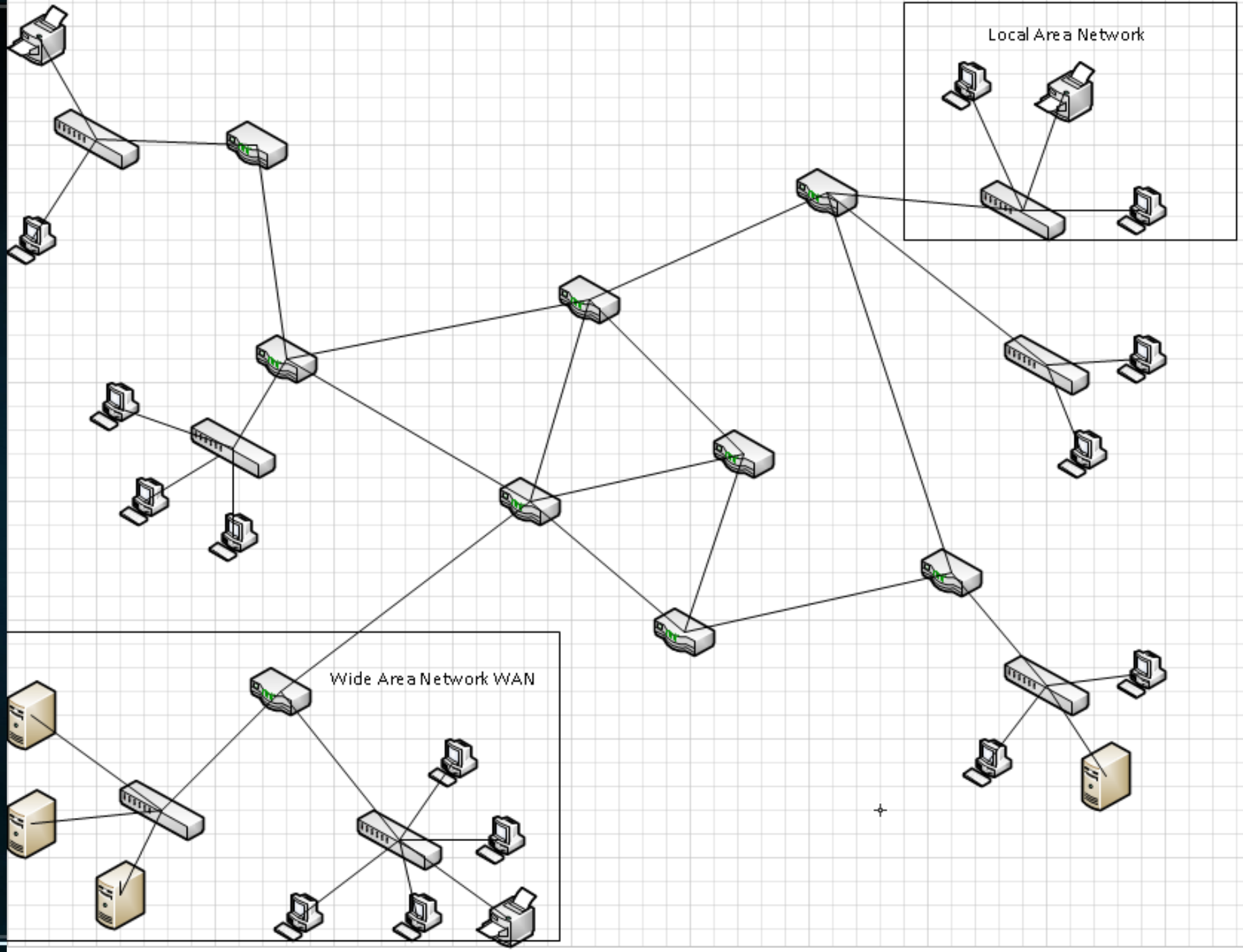
IP Client Information

- For the IP layer to route packets correctly, a device must be configured with:
  - IP address: Every IP address on the internet is unique. An address takes the form of:
    - 4 x 8 bit (32 bit) numbers represented in decimal notation separated by '.'s. For example 128.205.34.66. – IPV4
    - 8 x 16 bit (128 bit) alphanumeric addresses in decimal notation separated by '.'s. For example 2001:0000:3238:DFE1:63:0000:0000:FEFB – IPV6
    - IP addresses (To and From) are placed in packet headers, similar to how one would label an envelop.
  - Subnet Mask – used to determine the boundaries of a Local Area Network (LAN).
    - A subnet mask resembles an IP address. Ex 255.255.255.0
  - Gateway IP Address – where packets destined for outside our LAN are handed off.

The Flow of Internet Data

- The IP layer determines if the client your sending a packet to resided on you LAN by looking at:
  - Your client's IP address
  - Your client's subnet mask
  - Your destination's IP address




Local Area Network
Wide Area Network WAN

The Flow of Internet Data

- Gateways will communicate with one or more other gateways and devices called “routers”.
  - Routers are usually connected between subnets and take care of handing off massive amounts of packets.
- Routers constantly keep track of other routers around them.
  - They will look at things like:
    - link speeds
    - delay times
    - network congestion.
  - Routers are connected to “backbones”. Backbones are the information super highways of the internet.