Lecture 23:
The Internet (Abridged): Link + Network Layers

Professor Adam Bates

CS 461 / ECE 422

Fall 2019

Goals for Today

- <u>Learning Objectives</u>:
  - Conclude remarks on Key Management
  - Understand the fundamental building blocks of the Internet, specifically the Link and Network Layers
- <u>Announcements, etc</u>:
  - **Wednesday! Oct 23 Lecture:** *<u>Special Guest Lecture on Human Factors!</u>*
  - Tell us your ideas for special topic lectures! <u>https://piazza.com/class/jyhnjldpx864lb?cid=351</u>

Reminder: Please put away devices at the start of class

Key Management

The hard part of crypto: **Key-management**

Principles:

0. Always remember, key management is the hard part!

1. Each key should have only one purpose
   (in general, no guarantees when keys reused elsewhere)

1. Vulnerability of a key increases:
   a. The more you use it.
   b. The more places you store it.
   c. The longer you have it.

2. Keep your keys far from the attacker.

3. Protect yourself against compromise of old keys.

   Goal: **forward secrecy** — learning old key shouldn't help adversary learn new key.

   [How can we get this?]

Safely Building Secure Channels

What if you want confidentiality and integrity at the same time?

Encrypt, then MAC
not the other way around

Use separate keys for confidentiality and integrity.

Need two shared keys,
but only have one?
That's what PRGs are for!

If there's a reverse (Bob to Alice) channel, use separate keys for that too

How big should keys be?

Want probability of guessing to be infinitesimal… but watch out for Moore's law – safe size gets 1 bit larger every 18 months

128 bits usually safe for ciphers/PRGs

Need larger values for MACs/PRFs due to **birthday attack**

- Often trouble if adversary can find any two messages with same MAC
- Attack: Generate random values, look for coincidence.
- Requires $O(2^{|k|/2})$ time, $O(2^{|k|/2})$ space.
- For 128-bit output, takes 2^{64} steps: doable!

Upshot: Want output of MACs/PRFs to be twice as big as cipher keys e.g. use HMAC-SHA256 alongside AES-128

Key Type *Move the cursor over a type for description*	Cryptoperiod Originator Usage Period (OUP)	 Recipient Usage Period
Private Signature Key	1-3 years	-
Public Signature Key	Several years (depends on key size)	
Symmetric Authentication Key	<= 2 years	<= OUP + 3 years
Private Authentication Key	1-2 years	
Public Authentication Key	1-2 years	
Symmetric Data Encryption Key	<= 2 years	<= OUP + 3 years
Symmetric Key Wrapping Key	<= 2 years	<= OUP + 3 years
Symmetric RBG keys	Determined by design	-
Symmetric Master Key	About 1 year	-
Private Key Transport Key	<= 2 years (1)	
Public Key Transport Key	1-2 years	
Symmetric Key Agreement Key	1-2 years (2)	
Private Static Key Agreement Key	1-2 years (3)	
Public Static Key Agreement Key	1-2 years	
Private Ephemeral Key Agreement Key	One key agreement transaction	
Public Ephemeral Key Agreement Key	One key agreement transaction	
Symmetric Authorization Key	<= 2 years	
Private Authorization Key	<= 2 years	
Public Authorization Key	<= 2 years	

https://www.keylength.com/en/4/

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

https://www.keylength.com/en/4/

Attacks against Crypto

1. Brute force: trying all possible private keys
2. Mathematical attacks: factoring
3. Timing attacks: using the running time of decryption
4. Hardware-based fault attack: induce faults in hardware to generate digital signatures
5. Chosen ciphertext attack
6. Architectural Changes

Btw, Post-Quantum is a thing

Post Quantum:

When will a quantum computer be built?

15 years, $1 billion USD, nuclear power plant (PQCrypto 2014, Matteo Mariantoni)

What will be impacted?

Public key crypto:

~~RSA~~

~~Elliptic Curve Cryptography (ECDSA)~~

~~Finite Field Cryptography (DSA)~~

~~Diffie-Hellman key exchange~~

Symmetric key crypto:
AES, Triple DES

Need Larger Keys

Hash functions:
~~SHA-1~~, SHA-2 and SHA-3

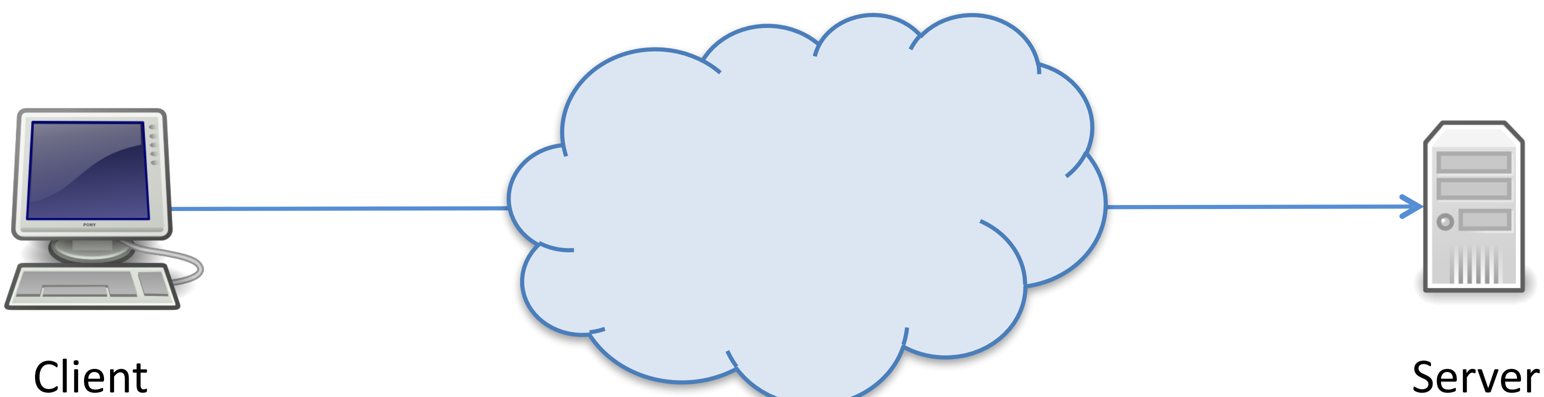
Use longer output

Key Concepts

- Packet switching
- Network attacker models
- Protocol layering
- Network address resolution
- TCP Sessions

What is the Internet?

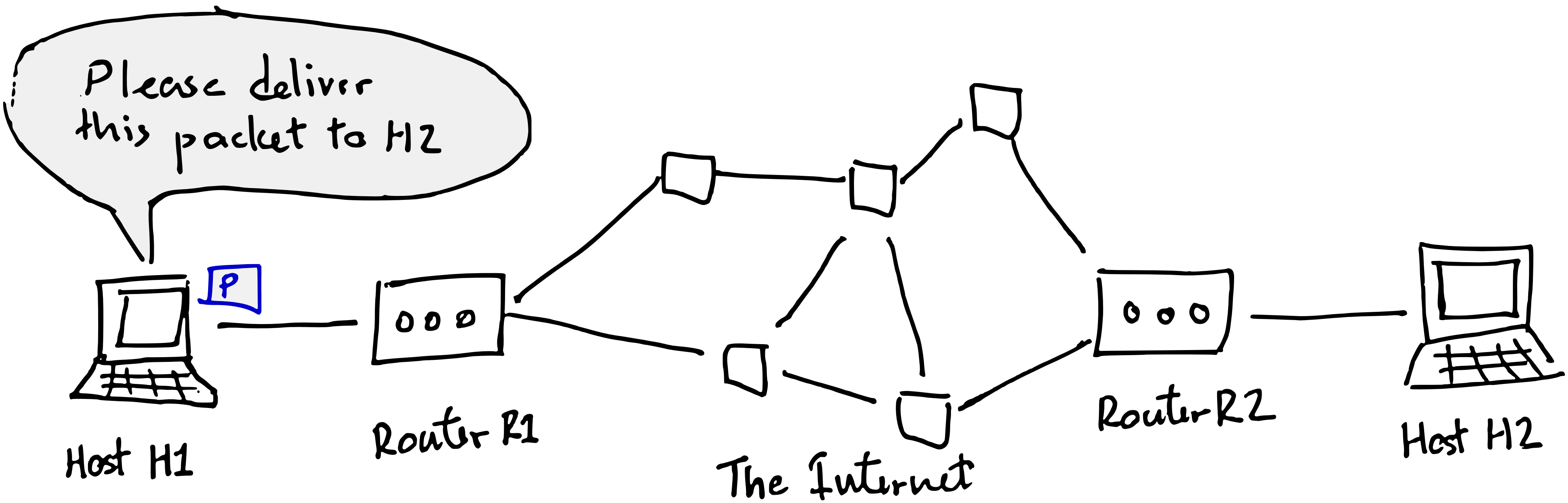
- To the layperson: useful services
  - Web, email, video, voice
- Technically: global system that lets *hosts* communicate
  - Physical infrastructure
    - switches, routers, links, radios
  - Protocols
    - WiFi, Ethernet, IP, TCP, HTTP



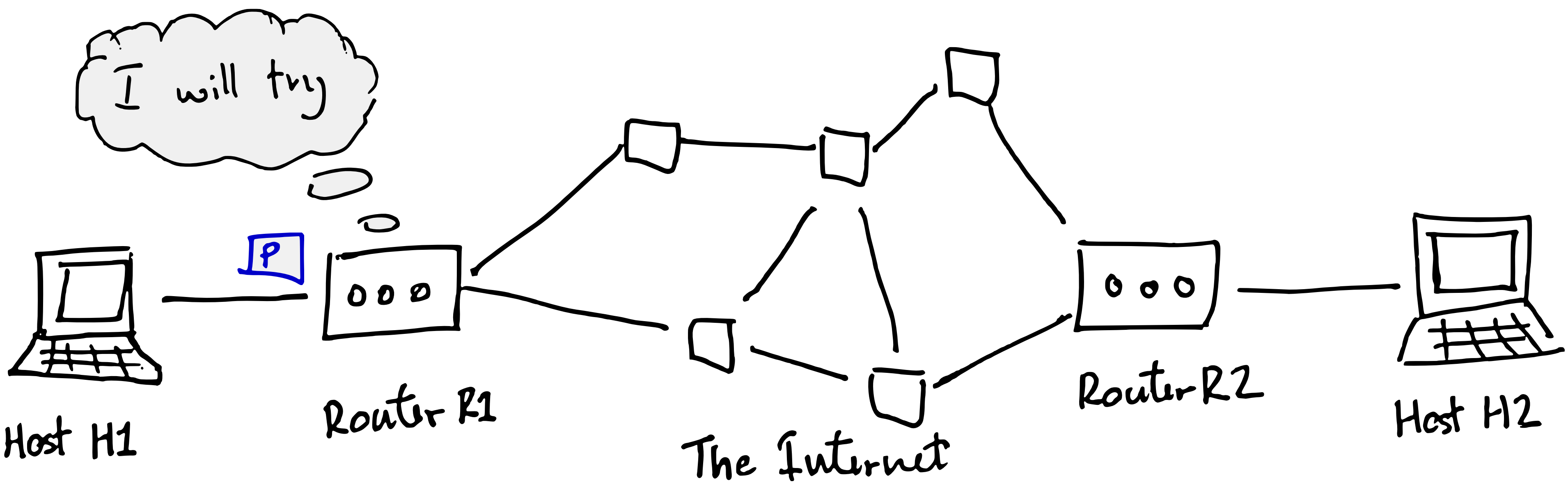
Packet Switching

- Internet provides best-effort delivery of *packets* between hosts
- **Packet:** a structured sequence of bytes
  - Header: metadata used by network
  - Payload: user data to be transported
- Packets are *forwarded* by *routers* from sender to destination host
  - Each packet is treated independently

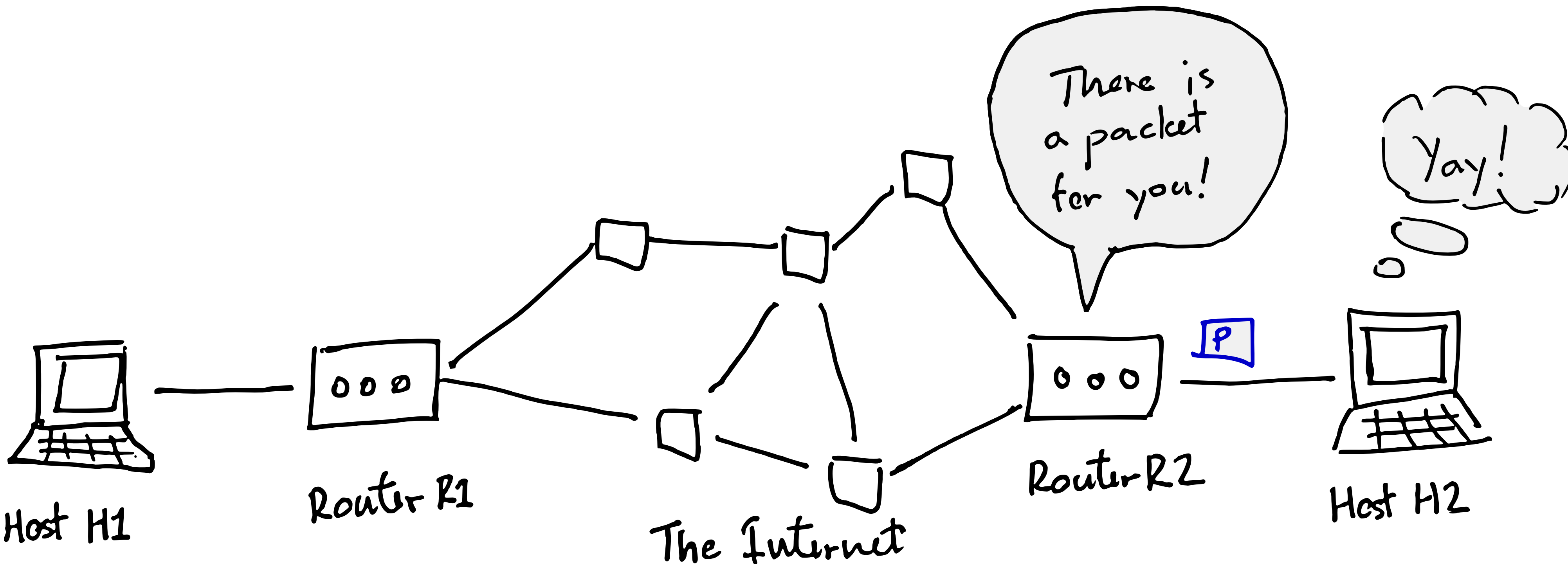
Packet Switching



Packet Switching

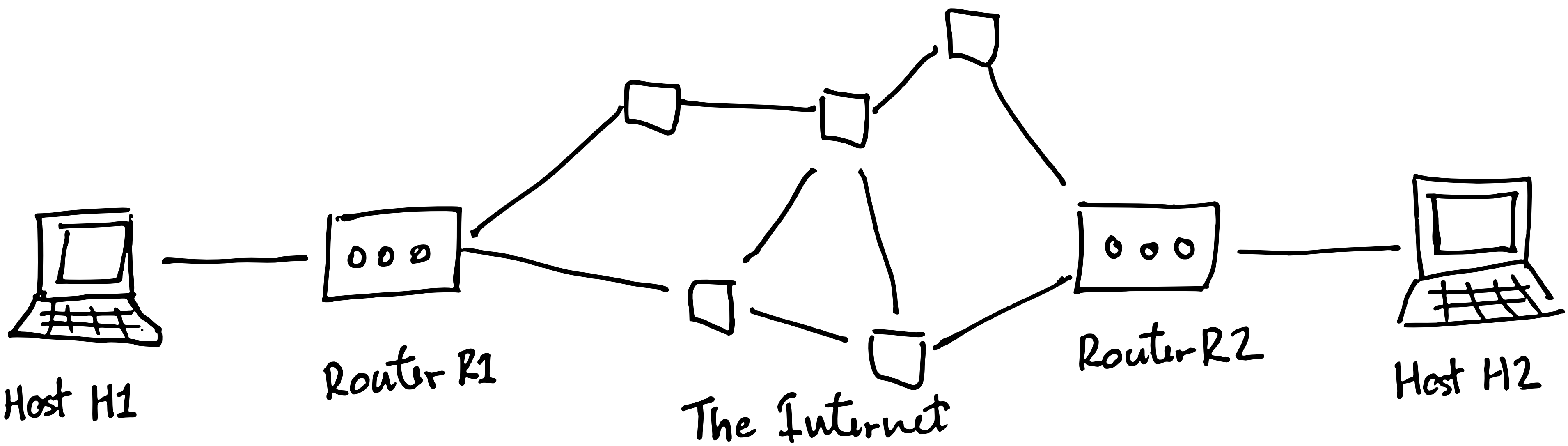


Packet Switching



Packet Switching

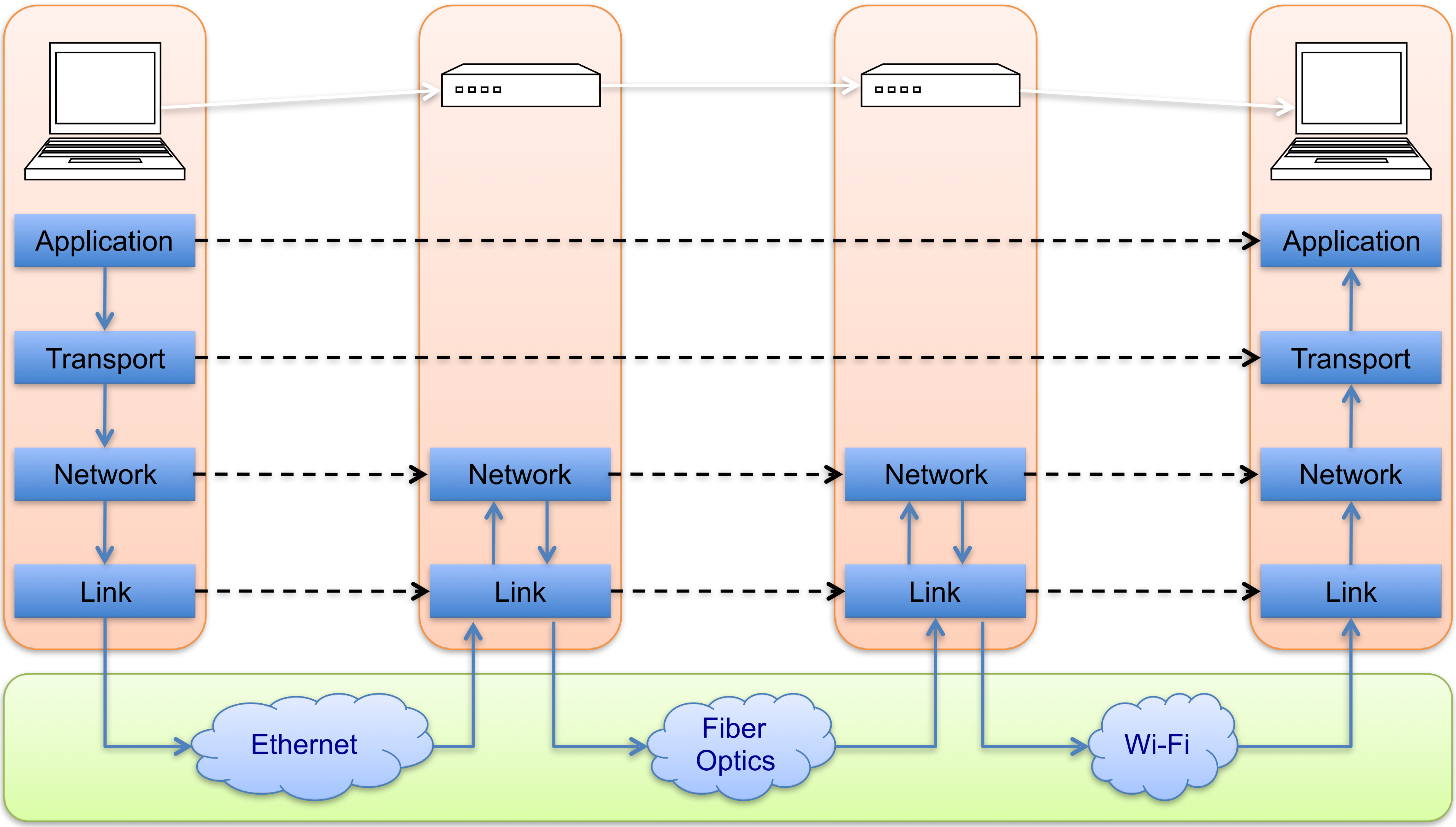
- Packets forwarded independently
- Each packet could take different path
  - Packets may be dropped or arrive out of order
- ***How is it done??***



Protocol Layering

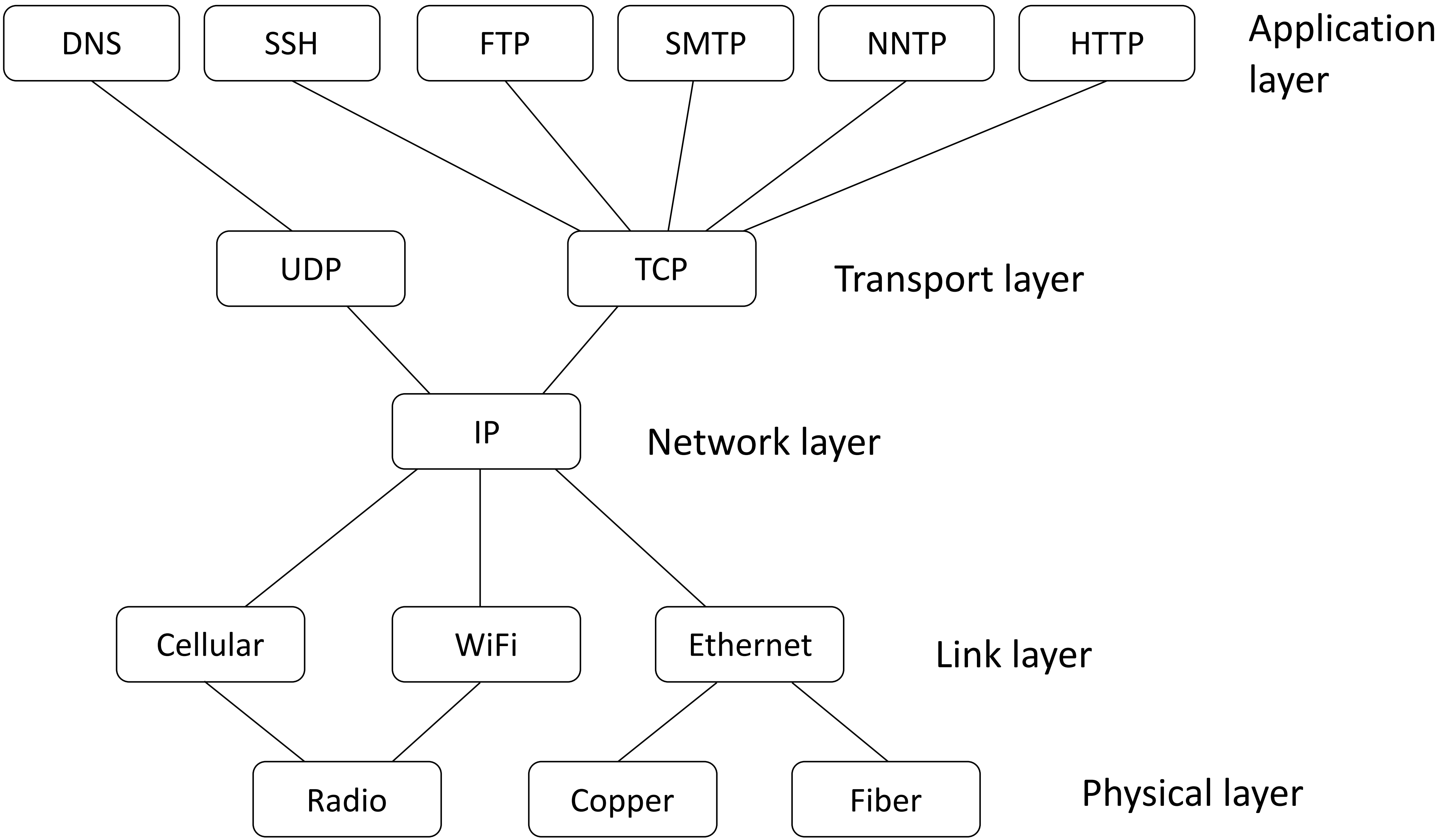
- Networks use a stack of layers
- Lower layers *provide* services to layers above
  - Don’t care what higher layers do
- Higher layers *use* services of layers below
  - Don’t care how lower layers implement services
- Layers define abstraction boundaries
  - At a given layer, all layers above and below are opaque

Internet Layers



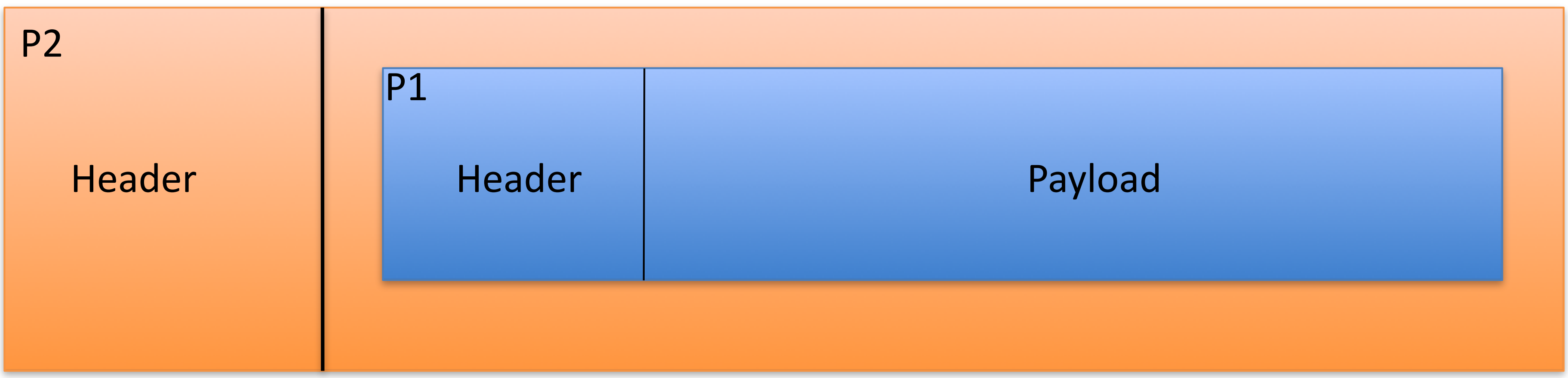
Physical Layer

Protocol Layering

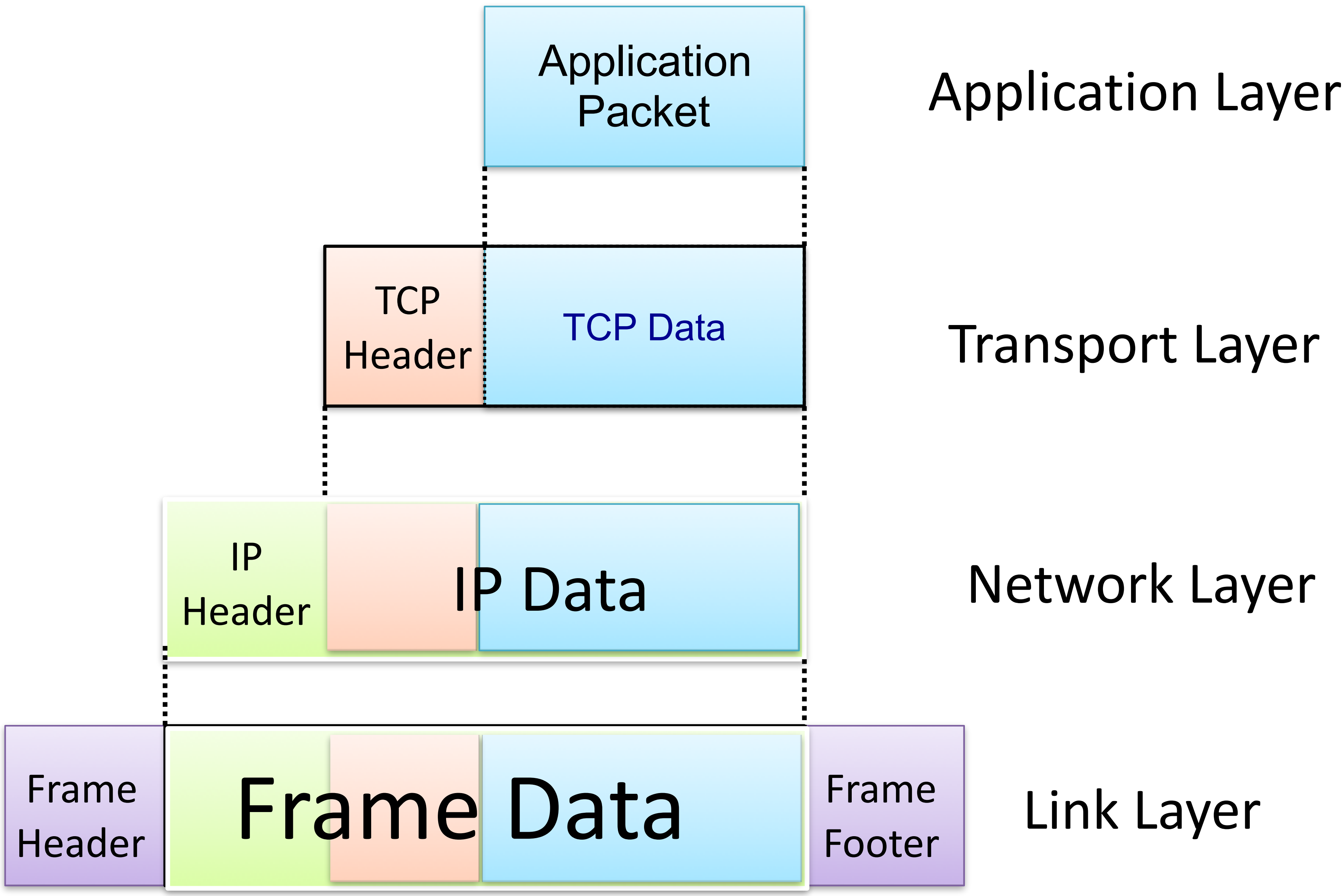


Protocol Layering

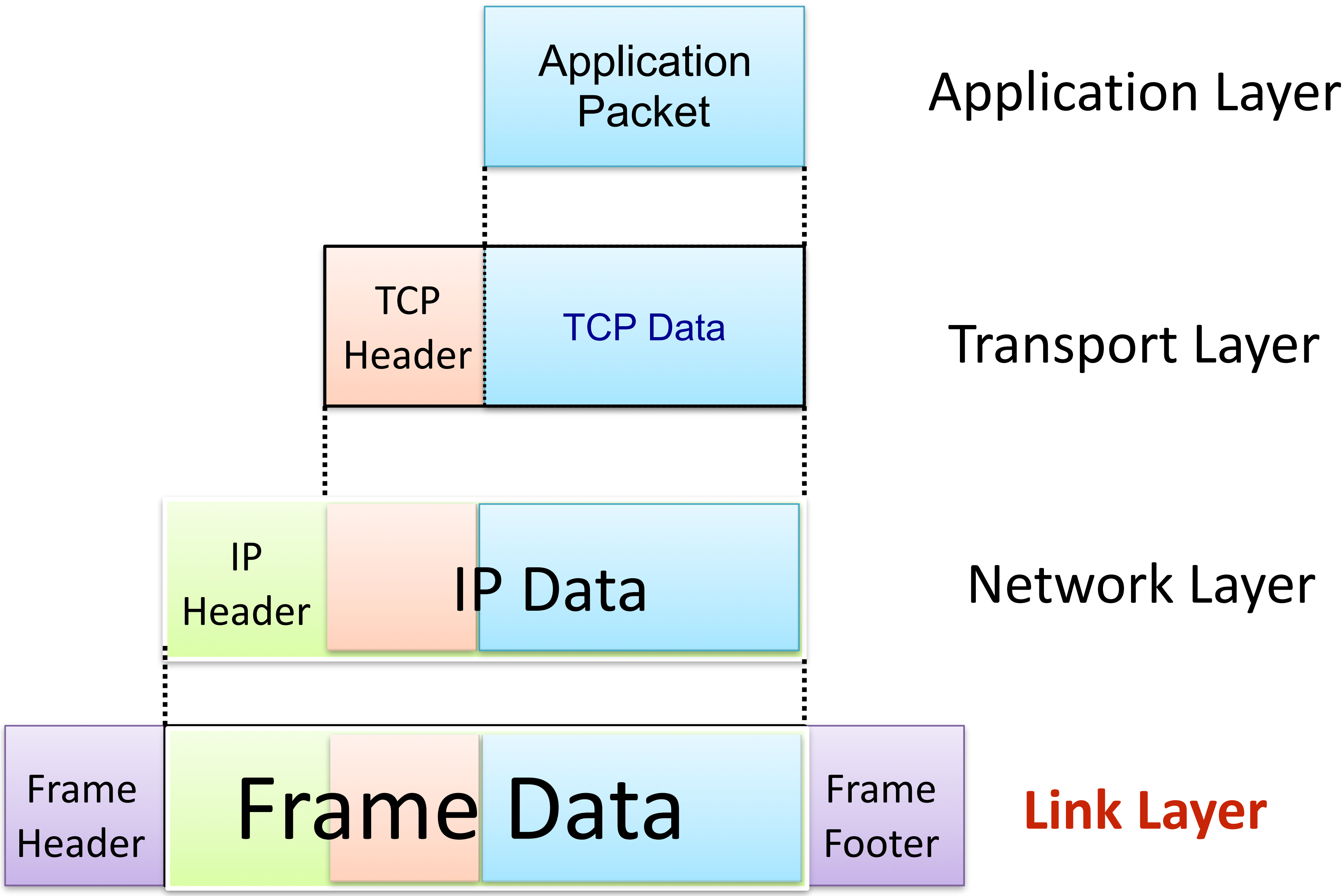
- Protocol N1 can use the services of lower layer protocol N2
  - A packet P1 of N1 is encapsulated into a packet P2 of N2
  - The payload of p2 is p1
  - The control information of p2 is derived from that of p1



Internet Packet Encapsulation

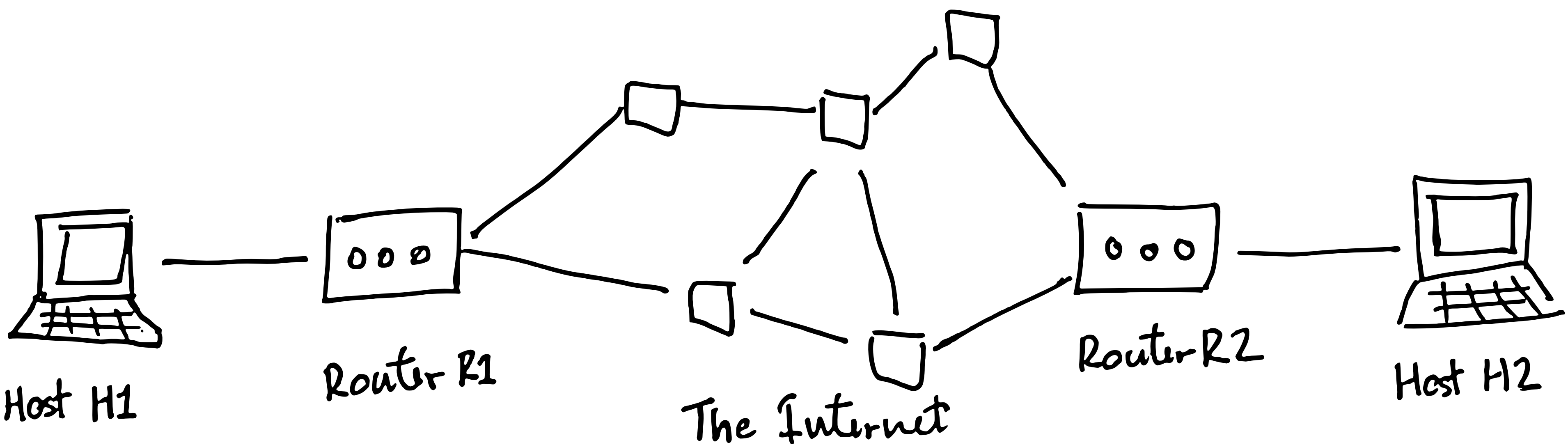


Internet Packet Encapsulation



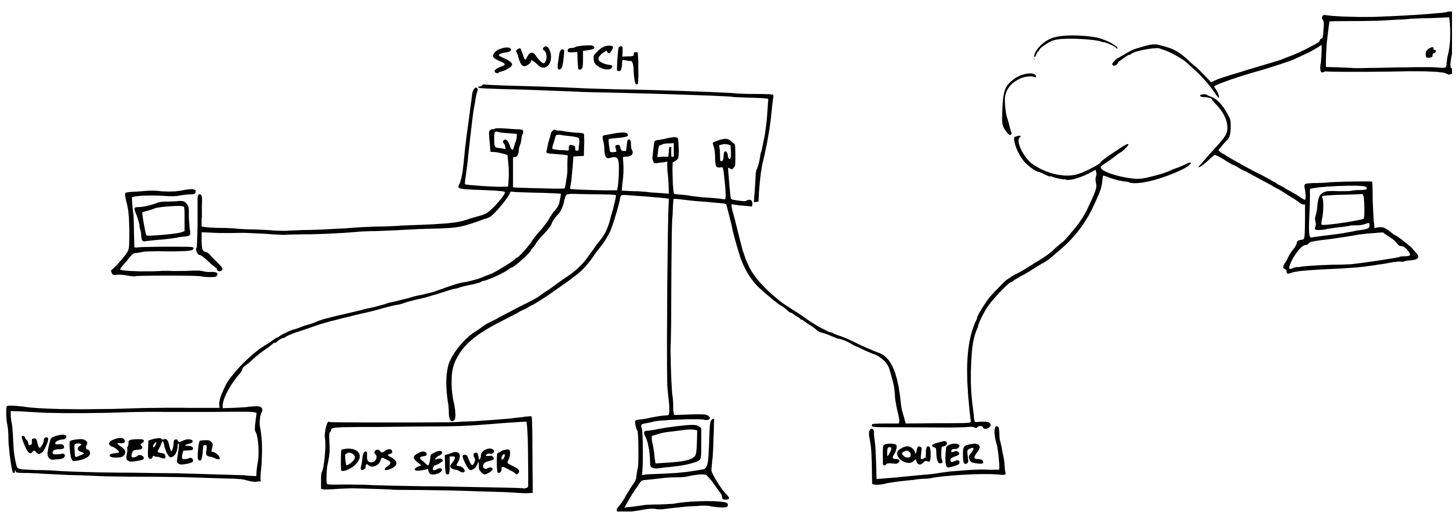
The Link Layer

- Our model so far assumes hosts can deliver and accept packets from Internet routers
- In practice, hosts *not* connected directly to router
- Another network layer provides connectivity between hosts and routers



Local Area Networks

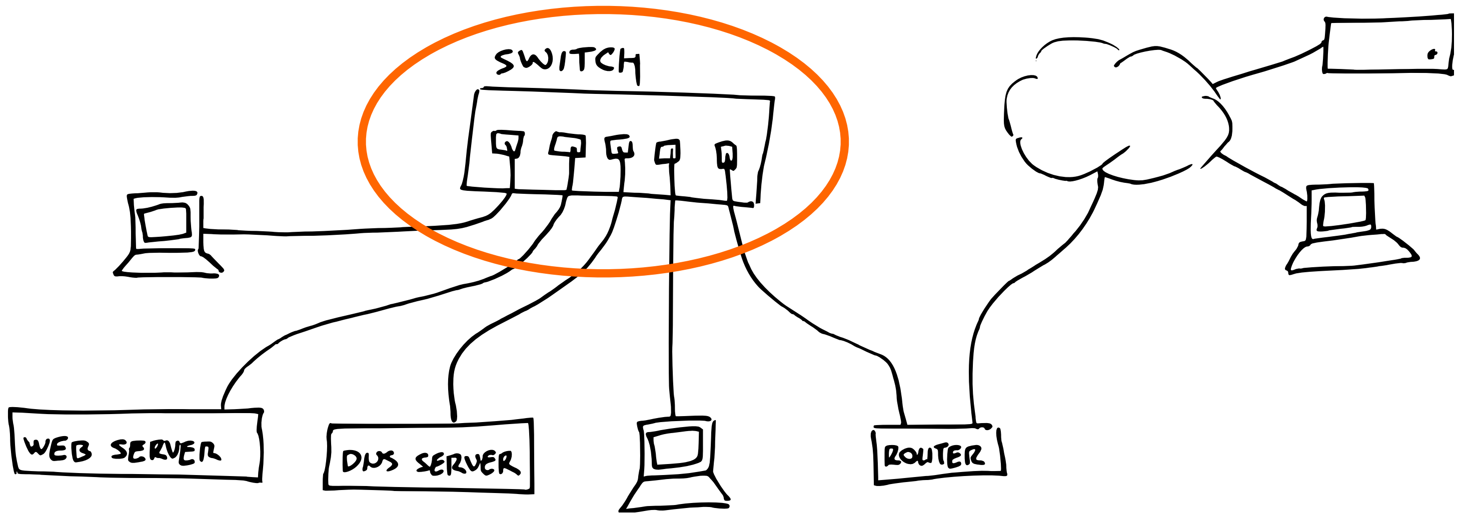
- Hosts interconnected by a *Local Area Network (LAN)* that allows them to communicate directly
- Router is just another device on this LAN that can forward IP datagrams to rest of Internet



Ethernet

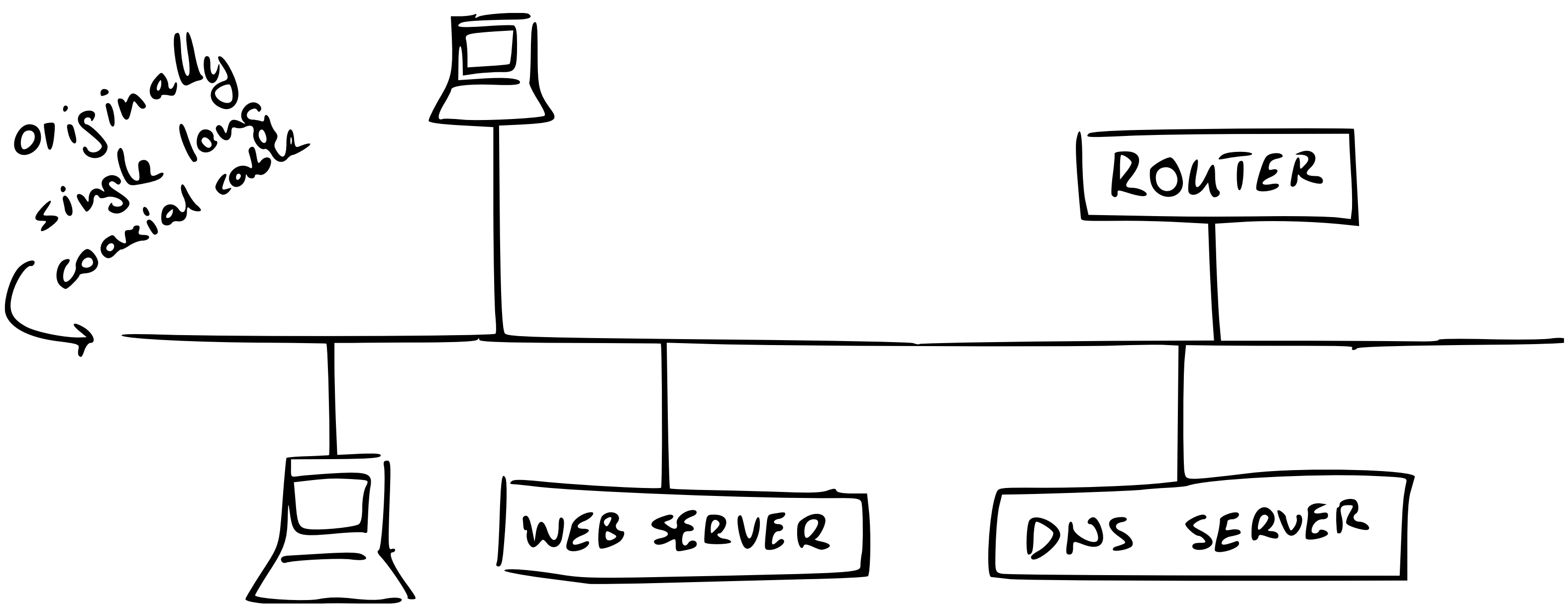
- Ethernet is most common wired LAN protocol
  - Encompasses layers 1 (physical) and 2 (link)
  - Many different physical layers in use
- WiFi uses Ethernet packet format

Speaks Ethernet only,
does not understand IP

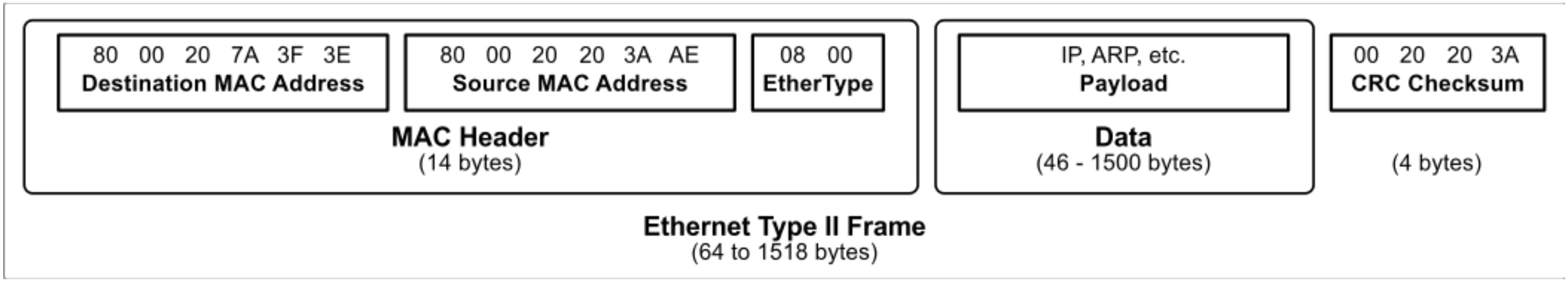


Ethernet (Logical View)

- All hosts can send packets to each other *individually* or *broadcast* to everyone
- Switch is invisible to hosts



Ethernet

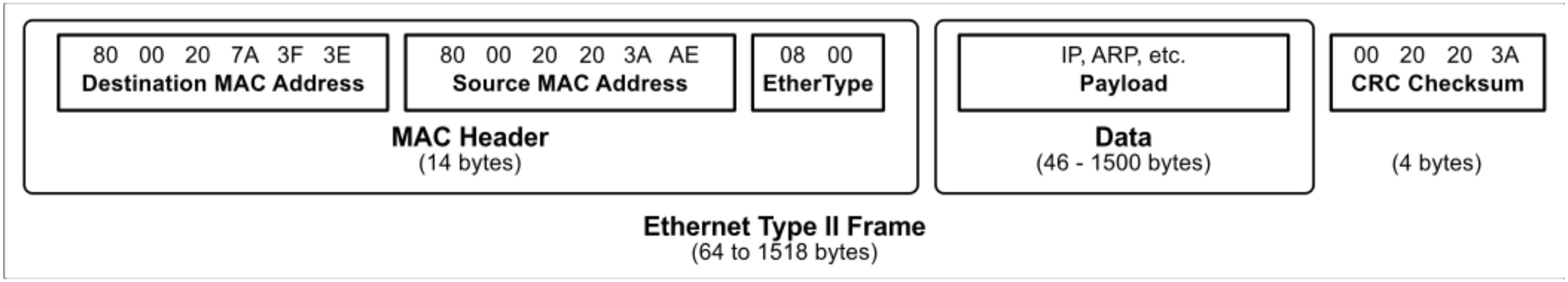


- At layer 2 (link layer) packets are called *frames*
- MAC addresses: 6 bytes, universally unique
- EtherType gives layer 3 protocol in payload
  - `0x0800`: IPv4
  - `0x0806`: ARP
  - `0x86DD`: IPv6

Switched Ethernet

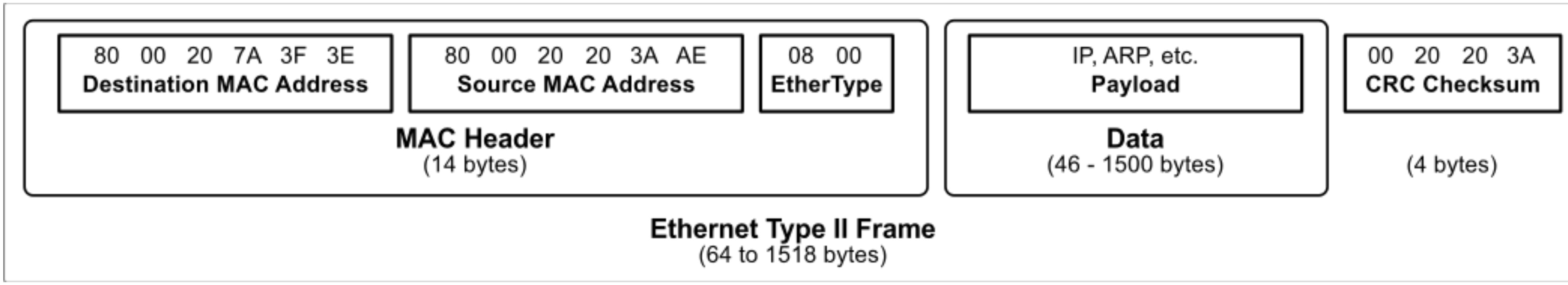
- Original Ethernet was a broadcast medium: every device heard every other device
- With switched Ethernet, the switch *learns* at which physical port each MAC address lives based on MAC source addresses
- If switch knows MAC address M is at port P,
  it will only send a packet for M out port P
- If switch does not know which port MAC address M lives at, will broadcast to all ports

IP over Ethernet



- To send an IP packet to a host on the LAN, sender creates an Ethernet frame with:
  - Destination host's Ethernet (MAC) address
  - EtherType: `0x0800` (IPv4) or `0x86DD` (IPv6)
  - Payload: IP packet with IP address of dest. host

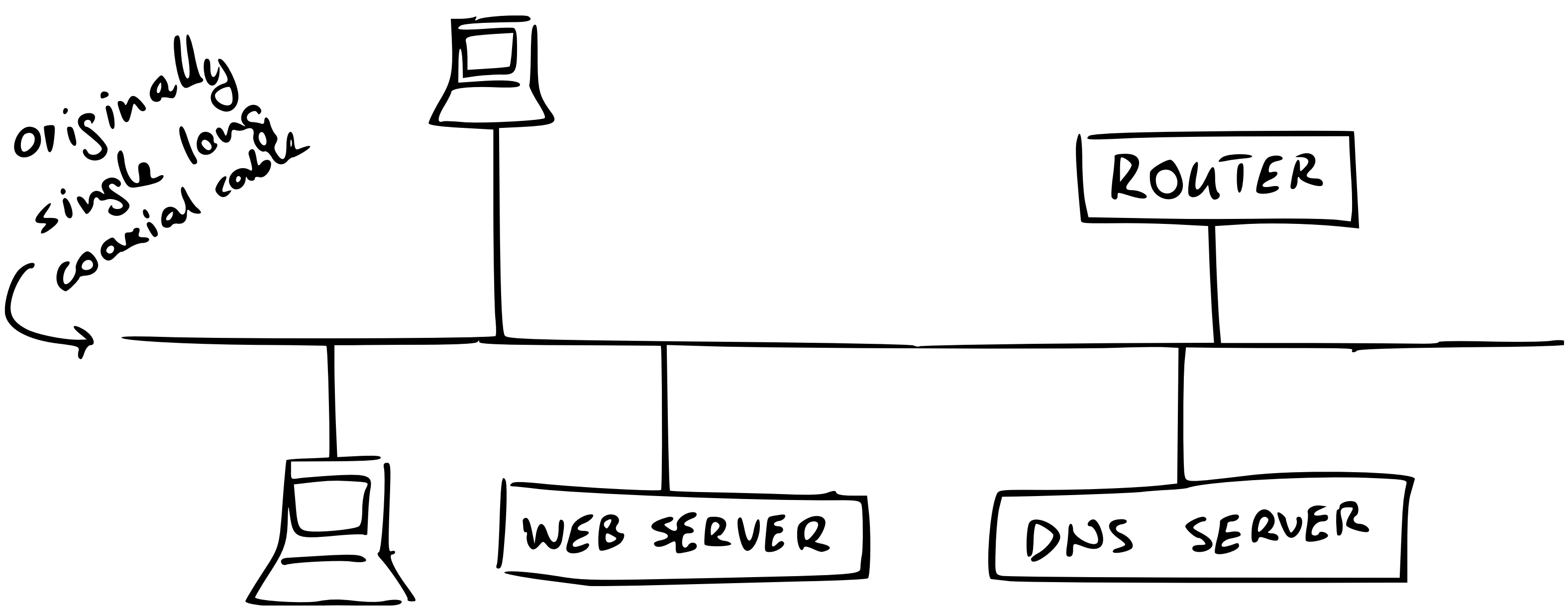
IP over Ethernet



- To send an IP packet to a host outside the LAN, sender creates an Ethernet frame with:
  - Router's Ethernet (MAC) address
  - EtherType: `0x0800` (IPv4) or `0x86DD` (IPv6)
  - Payload: IP packet with IP address of destination host
- Router receiver frame, forwards encapsulated IP packet to next router for delivery to IP destination

IP over Ethernet

- To send an IP packet to LAN host, sender needs to know the Ethernet (MAC) address of *destination host*
- To send an IP packet to outside host, sender needs to know the Ethernet (MAC) address of *router* (also called *gateway*)

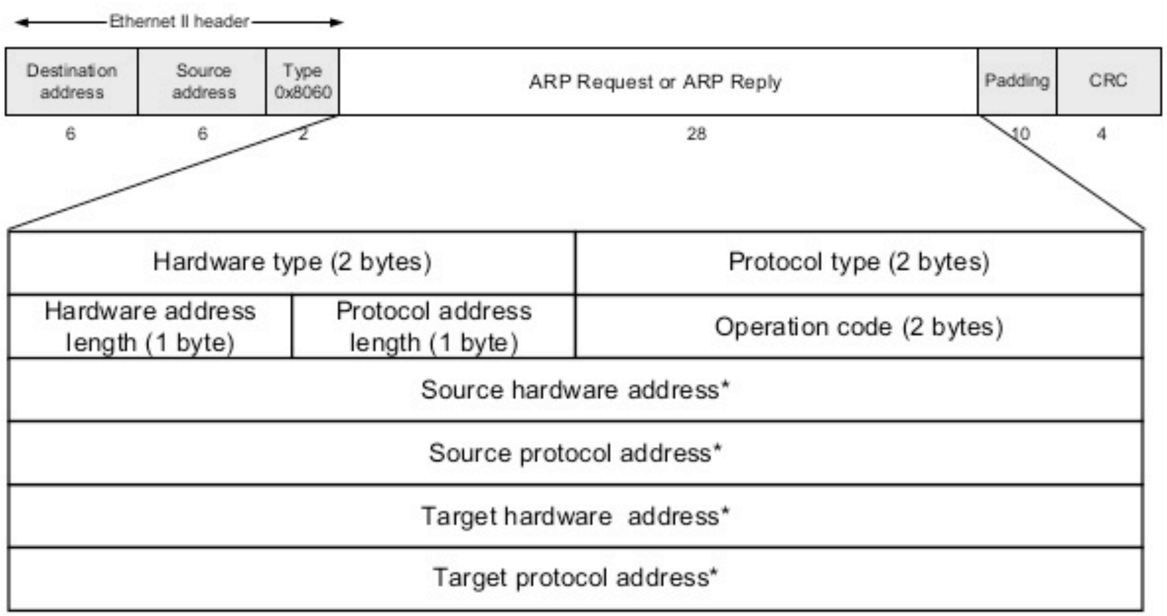


IP over Ethernet

- To send an IP packet to LAN host, sender needs to know the Ethernet (MAC) address of *destination host*
- To send an IP packet to outside host, sender needs to know the Ethernet (MAC) address of *router* (also called *gateway*)
- *How do hosts know this?*

Address Resolution Protocol

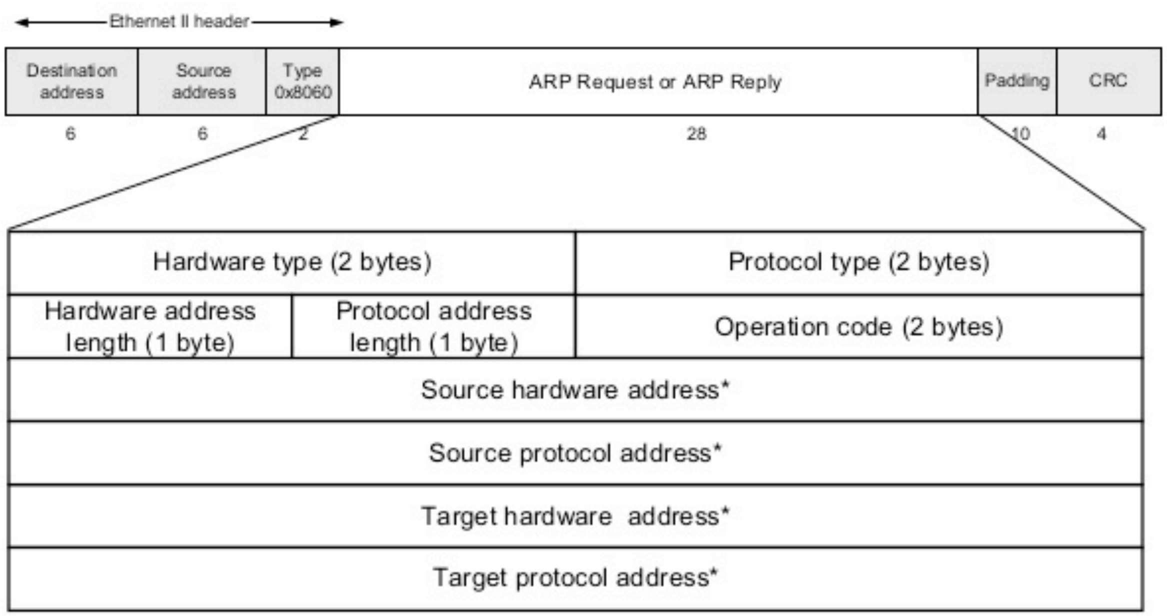
- Address Resolution Protocol (ARP) lets hosts map IP addresses to MAC addresses
- Host who needs MAC address *M* corresponding to IP address *N* broadcasts an ARP packet to LAN asking, "who has IP address *N*?"



* Note: The length of the address fields is determined by the corresponding address length fields

Address Resolution Protocol

- Host that has IP address N will reply,
  "IP *N* is at MAC address *M*."
- Host will cache this information for future use

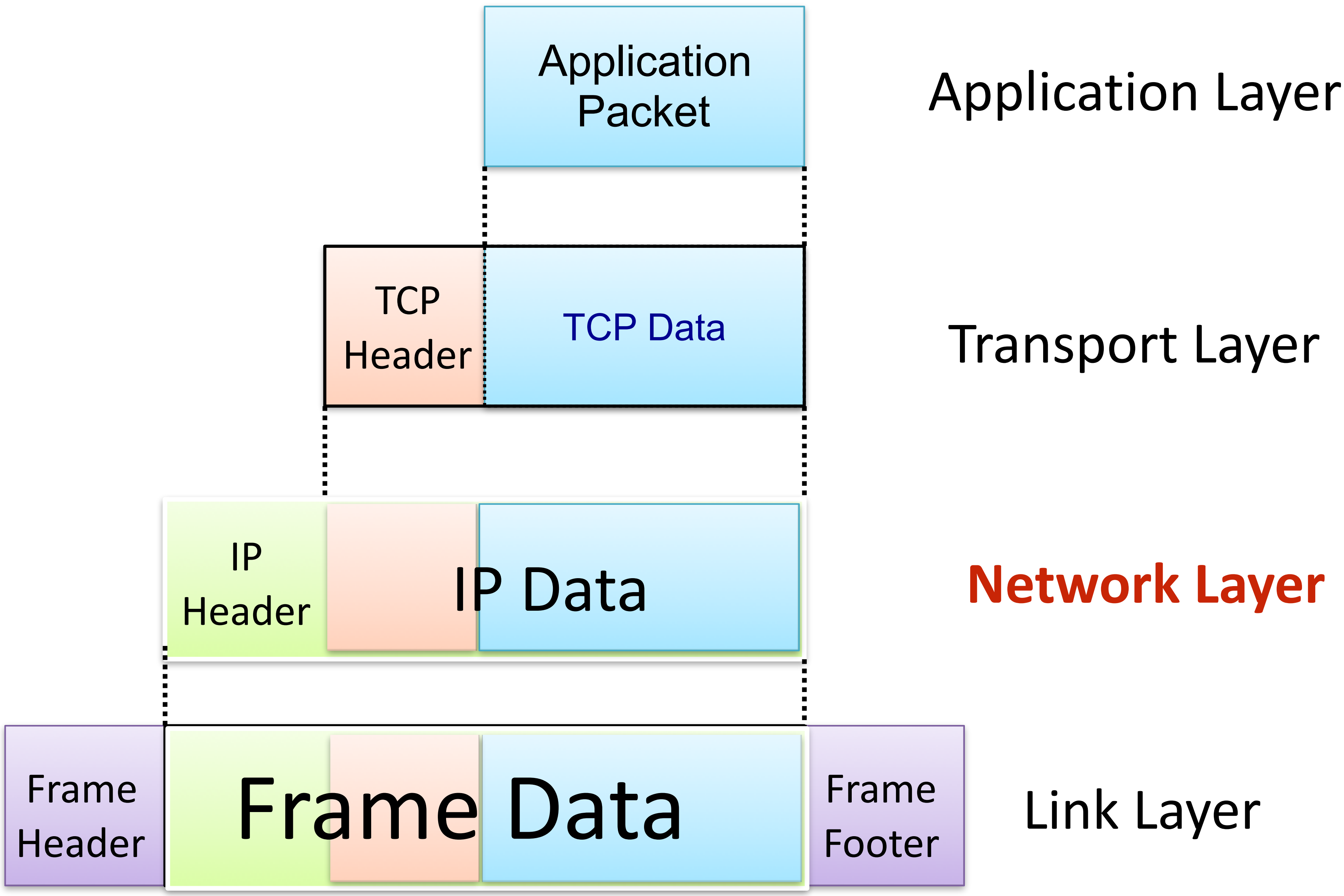


* Note: The length of the address fields is determined by the corresponding address length fields

ARP Security

- Any host on the LAN can send ARP requests and replies: *any host can claim to be another host on the local network!*
  - This is called *ARP spoofing*
- This allows any host X to force IP traffic between any two other hosts A and B to flow through X *(MitM!)*
  - Claim N_A is at attacker's MAC address M_X
  - Claim N_B is at attacker's MAC address M_X
  - Re-send traffic addressed to N_A to M_A, and vice versa
- *You will do this in MP4!*

Internet Packet Encapsulation



Internet Protocol

- **Internet Protocol (IP)** defines *structure* of packets and *how they are handled* by routers
  – IP packets are also called *datagrams*
- IP packets have an IP header that tells routers what to do with the packet
- Rest of packet (payload) is ignored by router
  – Not true anymore: *middleboxes* may examine and modify payload (e.g. to detect malware)

Routers

- Receive outgoing packets from local hosts and attempt to deliver onwards them to destination
- Deliver incoming packets to local hosts

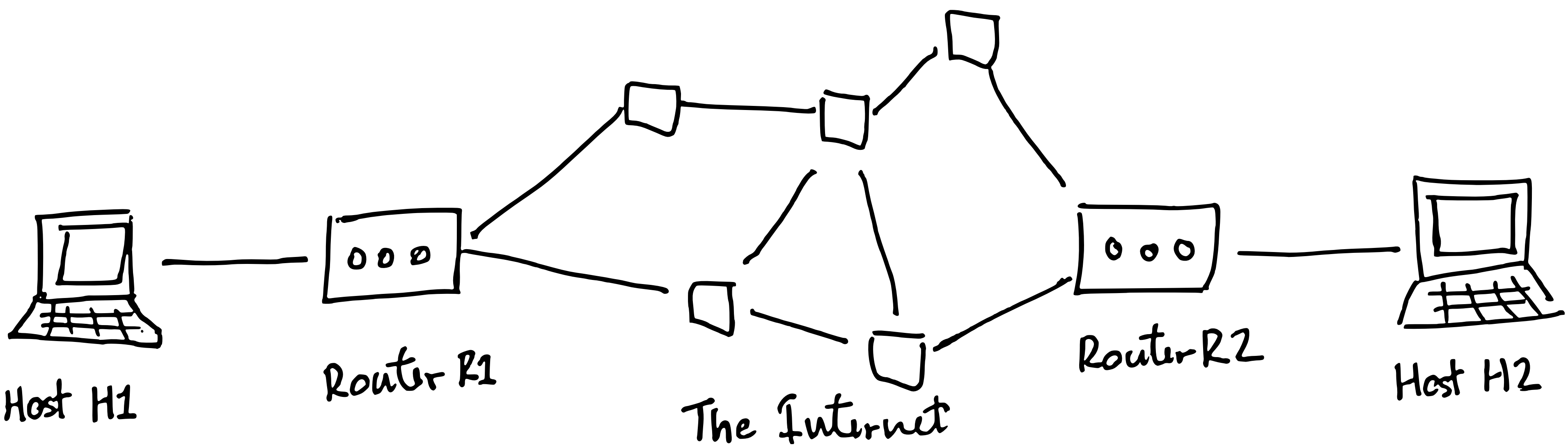
Internet Message Processor

Linksys WRT54G

Cisco CRS-1

Routing

- **Out of scope for this class:**
  How routers know where to forward packets so they get to destination
  – Has its own interesting security problems

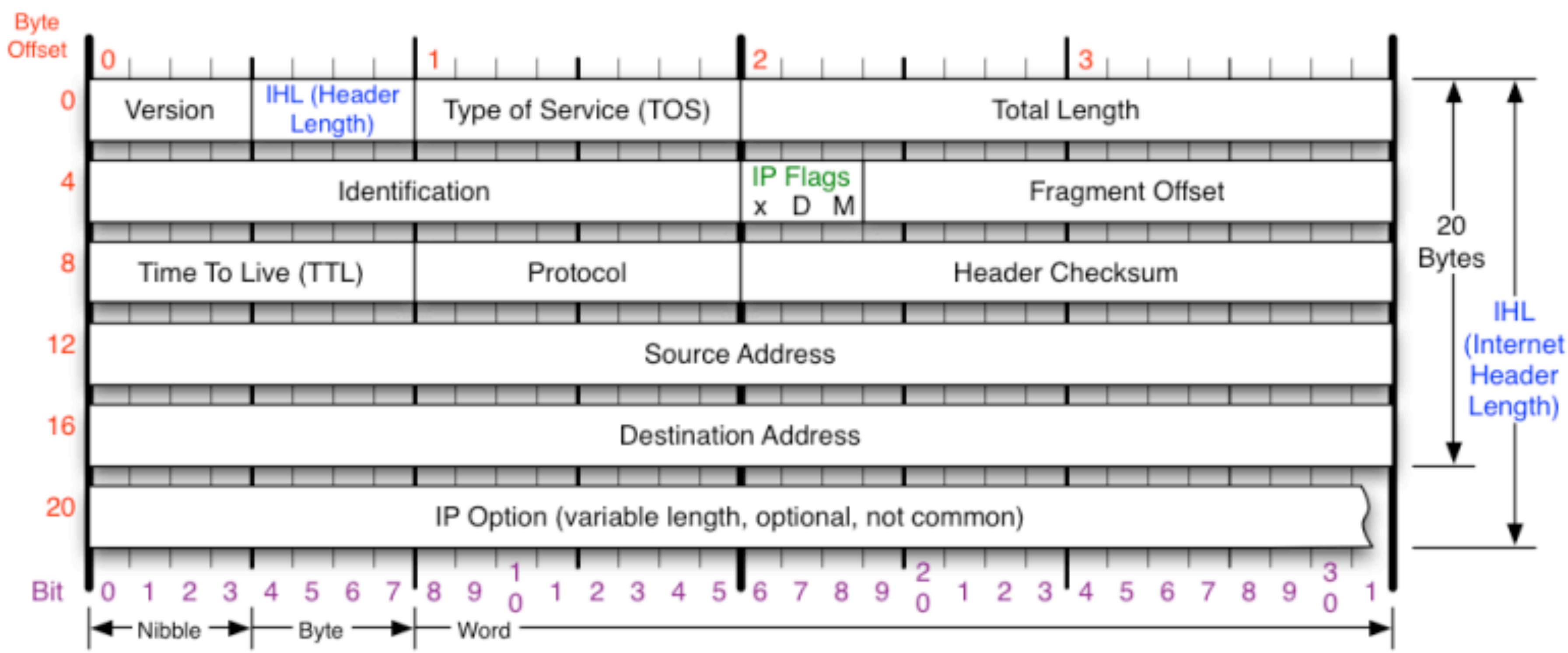


IPv4 vs. IPv6

- **IPv4:** 32-bit host addresses
  - Written as 4 bytes in form A.B.C.D where A,...,D are 8 bit integers in decimal (called *dotted quad*) *e.g.* 192.168.1.1
- **IPv6:** 128 bit host addresses
  - Written as 16 bytes in form AA:BB::XX:YY:ZZ where AA,...,ZZ are 16 bit integers in hexadecimal and :: implies zero bytes
    e.g. 2620:0:e00:b::53 = 2620:0:e00:b:0:0:0:53

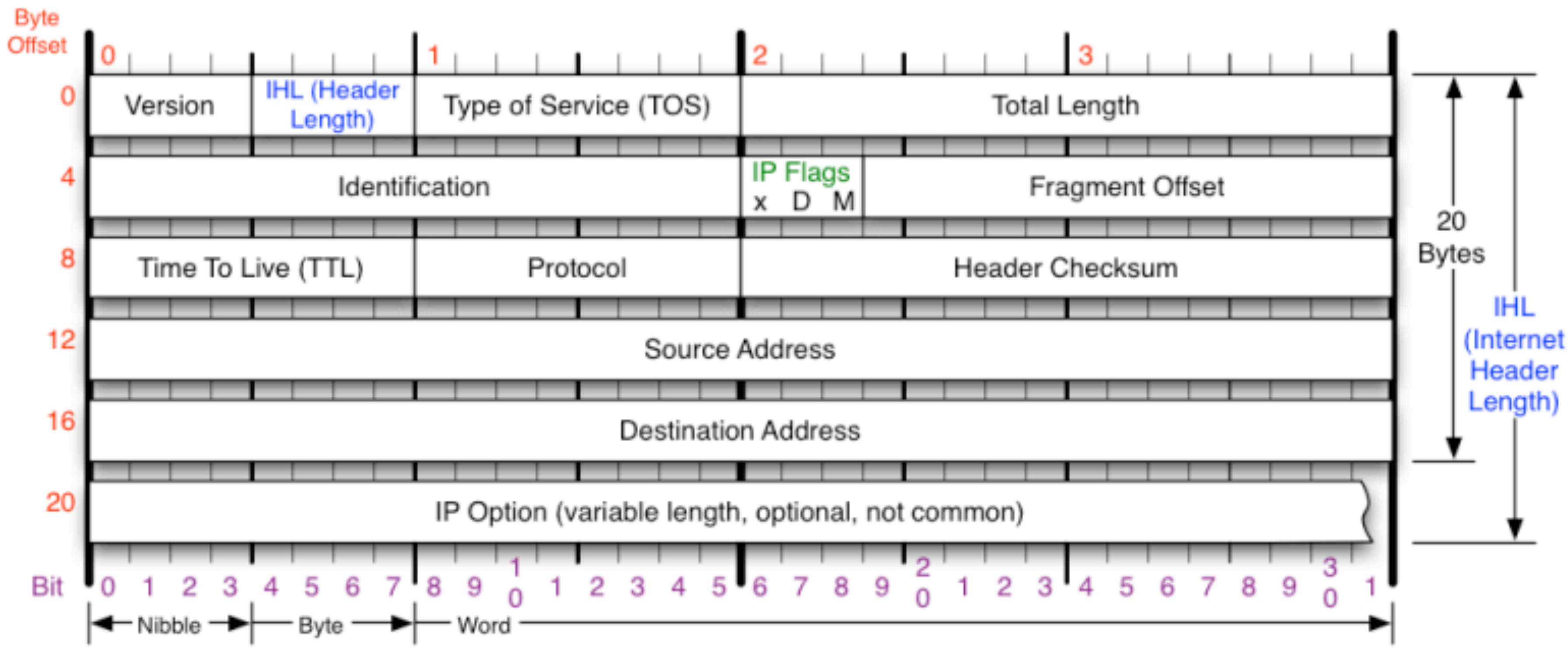
IPv4 Header

- Tells routers and hosts what to do with packet
- All values filled in by sending host



IPv4 Header

- Tells routers and hosts what to do with packet
- All values filled in by sending host

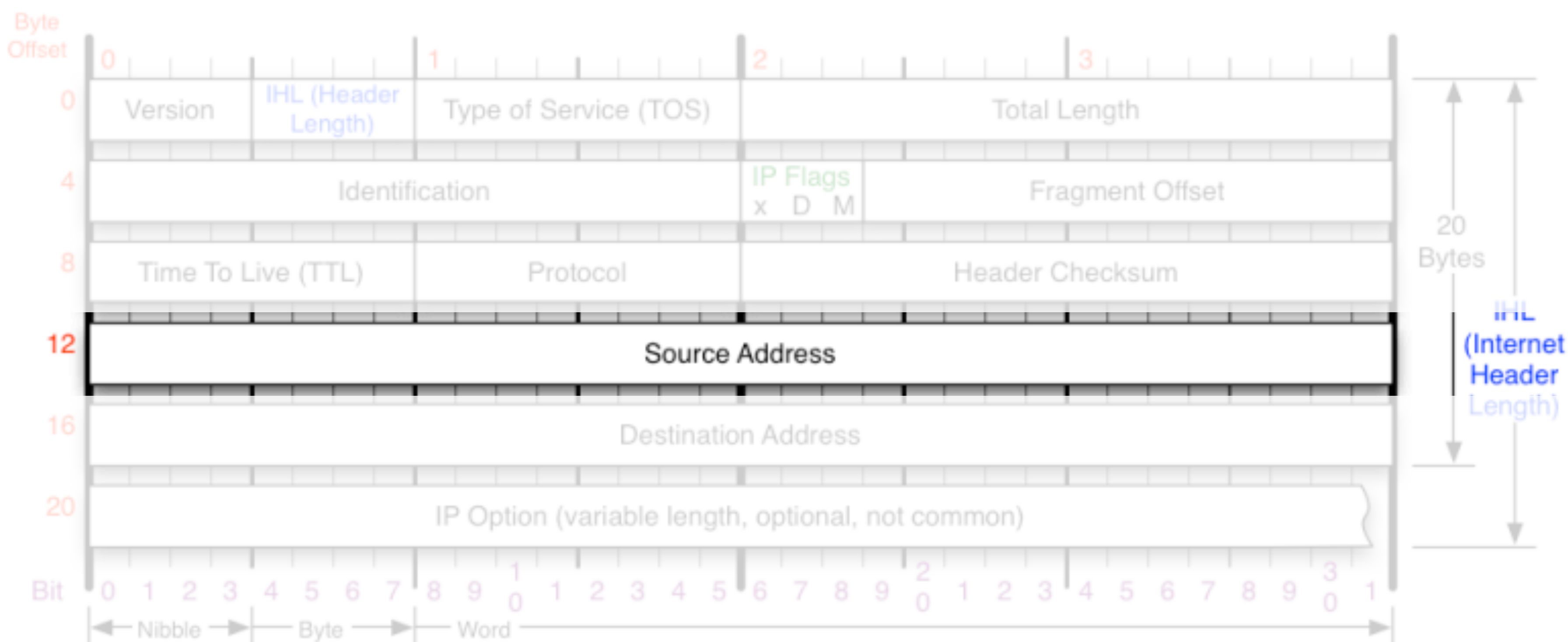


IPv4 Header

- Destination address (filled in by sender)
  - Packet forwarded based on this address

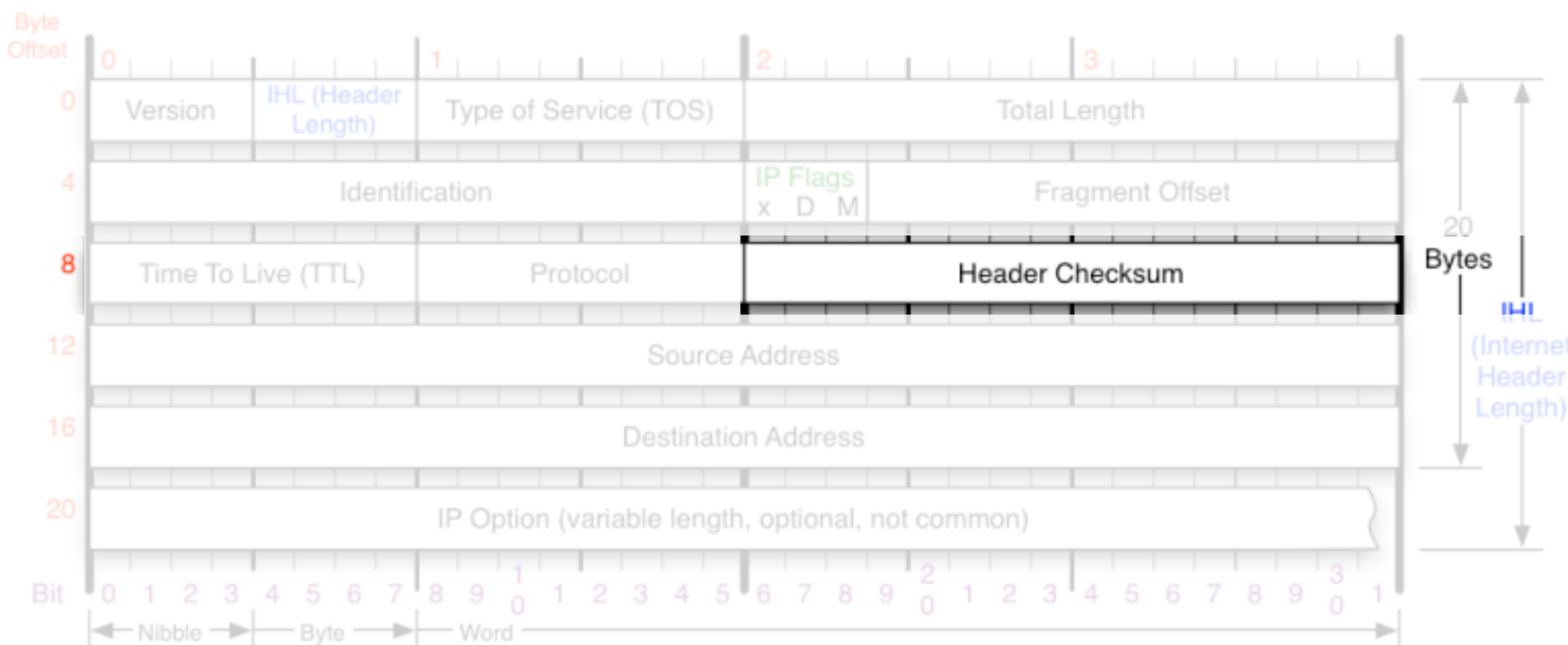
IPv4 Header

- Source address (filled in by sender)
  - Not verified by routers



IPv4 Header

- Header checksum (filled in by sender)
  - Must be set so that one's complement sum of header 16-bit (big-endian) words is zero



(Lay) Security Properties

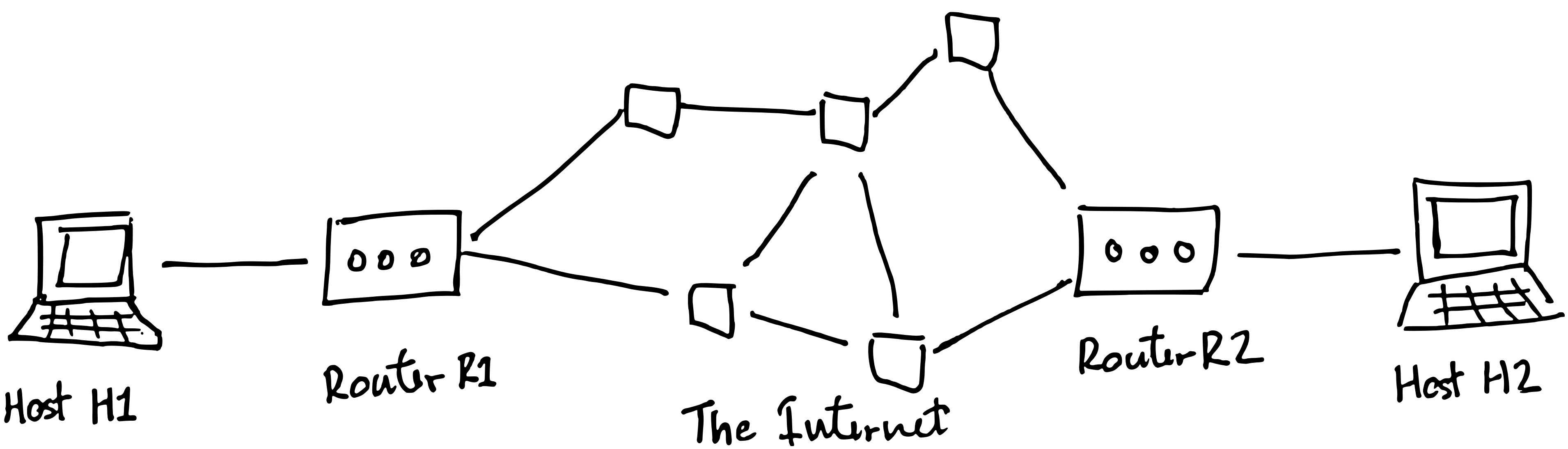
- **Availability:**
  no one can deny me access to services
- **Confidentiality:**
  no one can “see” my private information
- **Integrity:**
  no one can “mess with” my data
- **Authenticity:**
  no can pretend to be someone else

(Technical) Security Properties

- **Availability:**
  attacker can’t prevent communication
- **Confidentiality:**
  attacker can’t learn protected information
- **Integrity:**
  attacker can’t modify communications
- ***Authenticity:***
  attacker can’t forge communications

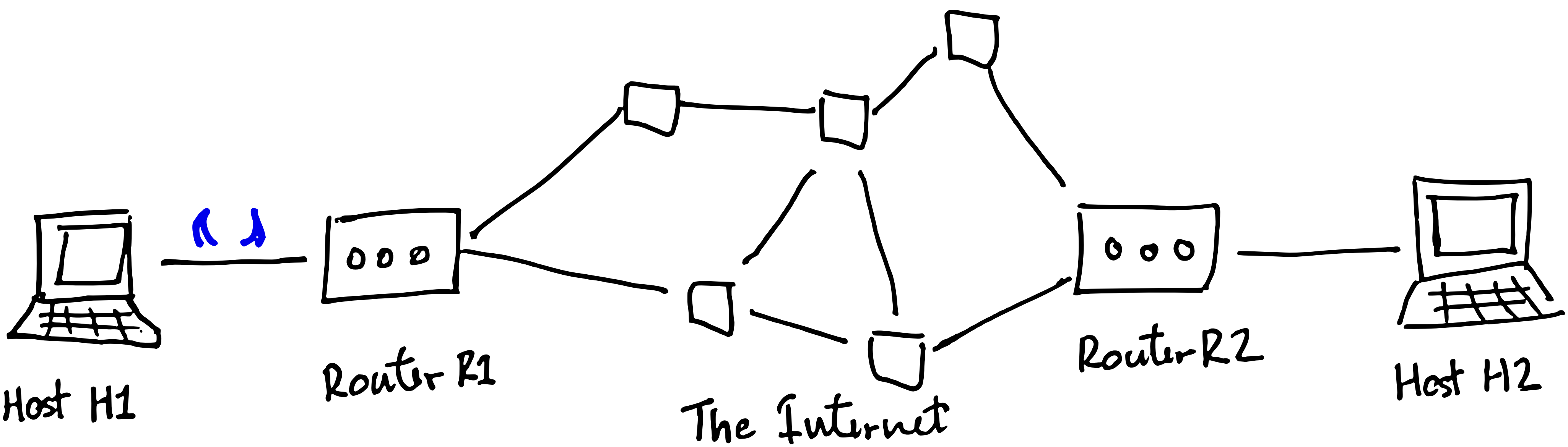
Security Properties

- What security properties does IP have?
- Availability? Confidentiality? Integrity? Authenticity?
- *Depends on attacker capability*
  - Passive Off-Path, Man-in-the-Middle



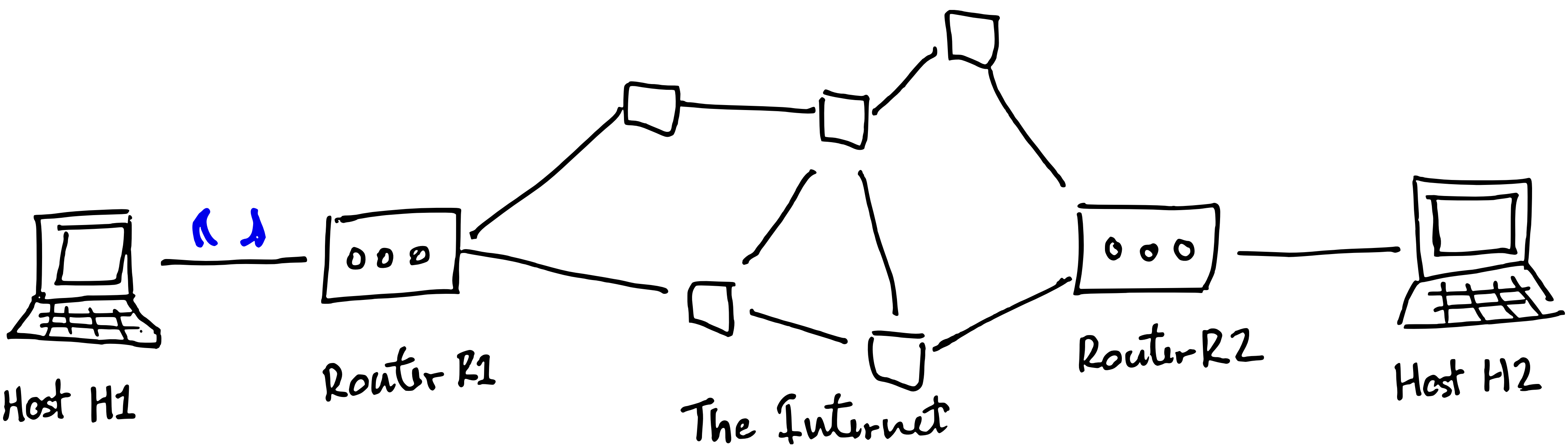
Network Attacker Models

- **Passive attacker:**
  can see all packets but cannot modify them
- Scenario?



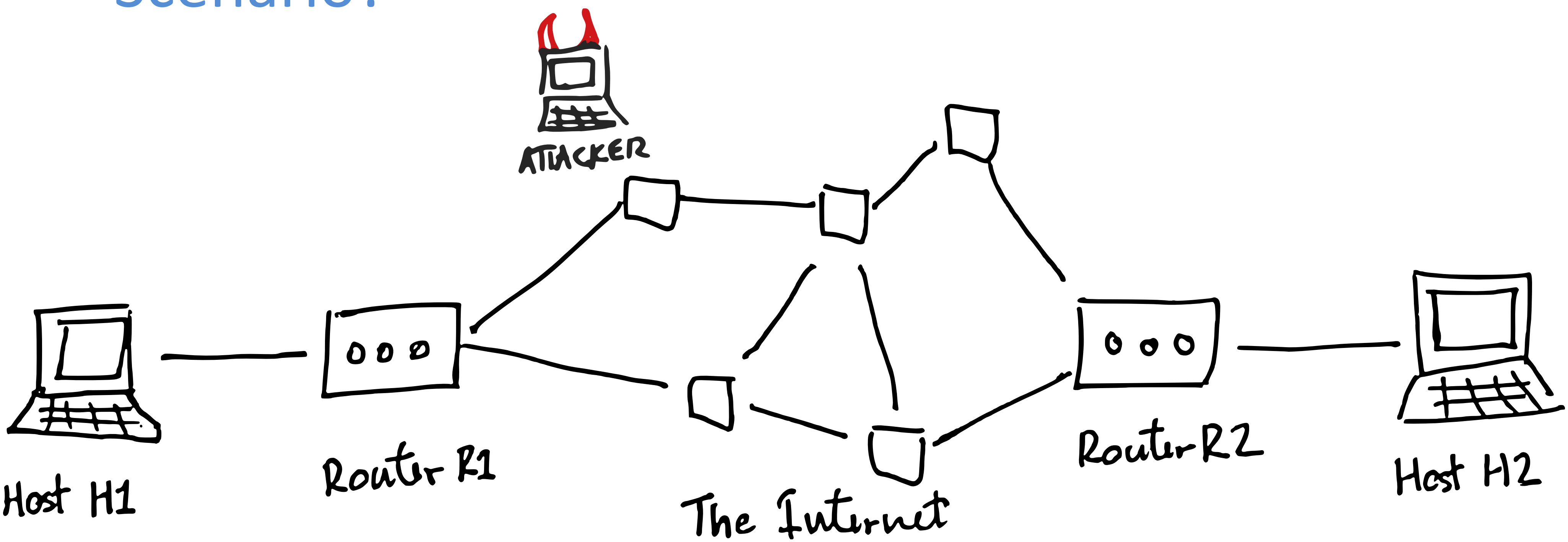
Network Attacker Models

- **Passive attacker:**
  can see all packets but cannot modify them
- Scenario?



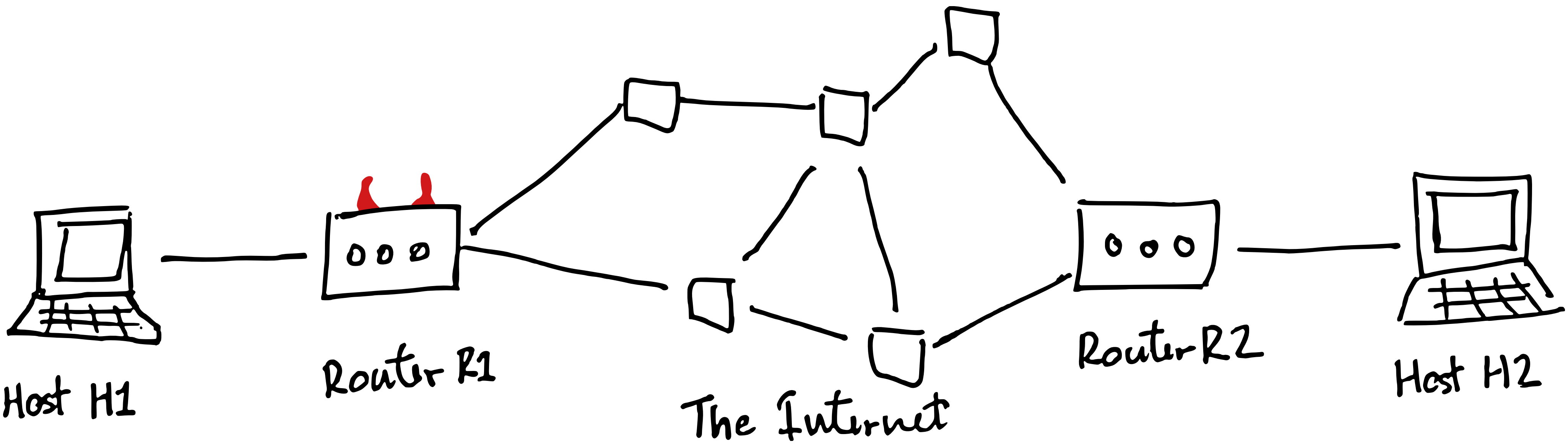
Network Attacker Models

- **Off-Path attacker:**
  can inject packets into network,
  but *cannot* see traffic between other hosts
- Scenario?



Network Attacker Models

- **Man-in-the-Middle attacker:**
  can see, inject, and drop all packets
- Scenario?



Security Properties

- **Availability?**
  attacker can't prevent communication
- **Confidentiality?**
  attacker can't learn protected information
- **Integrity?**
  attacker can't modify communications
- ***Authenticity?***
  attacker can't forge communications

IP Security Properties

	Passive	Off-Path	MitM
Availability			
Confidentiality			
Integrity			
Authenticity			

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality		—	
Integrity	—	—	
Authenticity	—		

- By definition:
  - Passive attacker cannot modify or send packets
  - Off-path attacker cannot see or modify packets
  - MitM attacker can always block packets

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality		—	
Integrity	—	—	
Authenticity	—		

- Confidentiality against a passive attacker?

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality	✗	—	✗
Integrity	—	—	
Authenticity	—		

- Confidentiality against a passive attacker? ✗
  – MitM can do whatever passive attacker can

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality	✗	—	✗
Integrity	—	—	
Authenticity	—		

- Integrity against a MitM attacker?
- What about header checksum?

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality	✗	—	✗
Integrity	—	—	✗
Authenticity	—		

- Integrity against a MitM attacker? ✗
- Header checksum can be updated by attacker
  – Requires no secret information to compute
  – Does not cover payload

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality	✗	—	✗
Integrity	—	—	✗
Authenticity	—		

- Authenticity? Source address indicates who sent the packet…

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality	✗	—	✗
Integrity	—	—	✗
Authenticity	—	✗	✗

- Authenticity? Source address indicates who sent the packet…
- Informational only: not enforced by routers
- Off-path or MitM can set source address to anything

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality	✗	—	✗
Integrity	—	—	✗
Authenticity	—	✗	✗

- Can an off-path attacker affect another host's ability to communicate with any other host?

IP Security Properties

	Passive	Off-Path	MitM
Availability	—		✗
Confidentiality	✗	—	✗
Integrity	—	—	✗
Authenticity	—	✗	✗

- Network denial-of-service attacks can saturate network preventing other communications
- Hosts and routers may have other limited resources
  - E.g. number of connections (we'll see this later)

IP Security Properties

	Passive	Off-Path	MitM
Availability	—	✗	✗
Confidentiality	✗	—	✗
Integrity	—	—	✗
Authenticity	—	✗	✗

- We'll see how we can build protocols built *on top of* IP to provide some of these security properties