Lecture 22 – Link and Network Layer Security

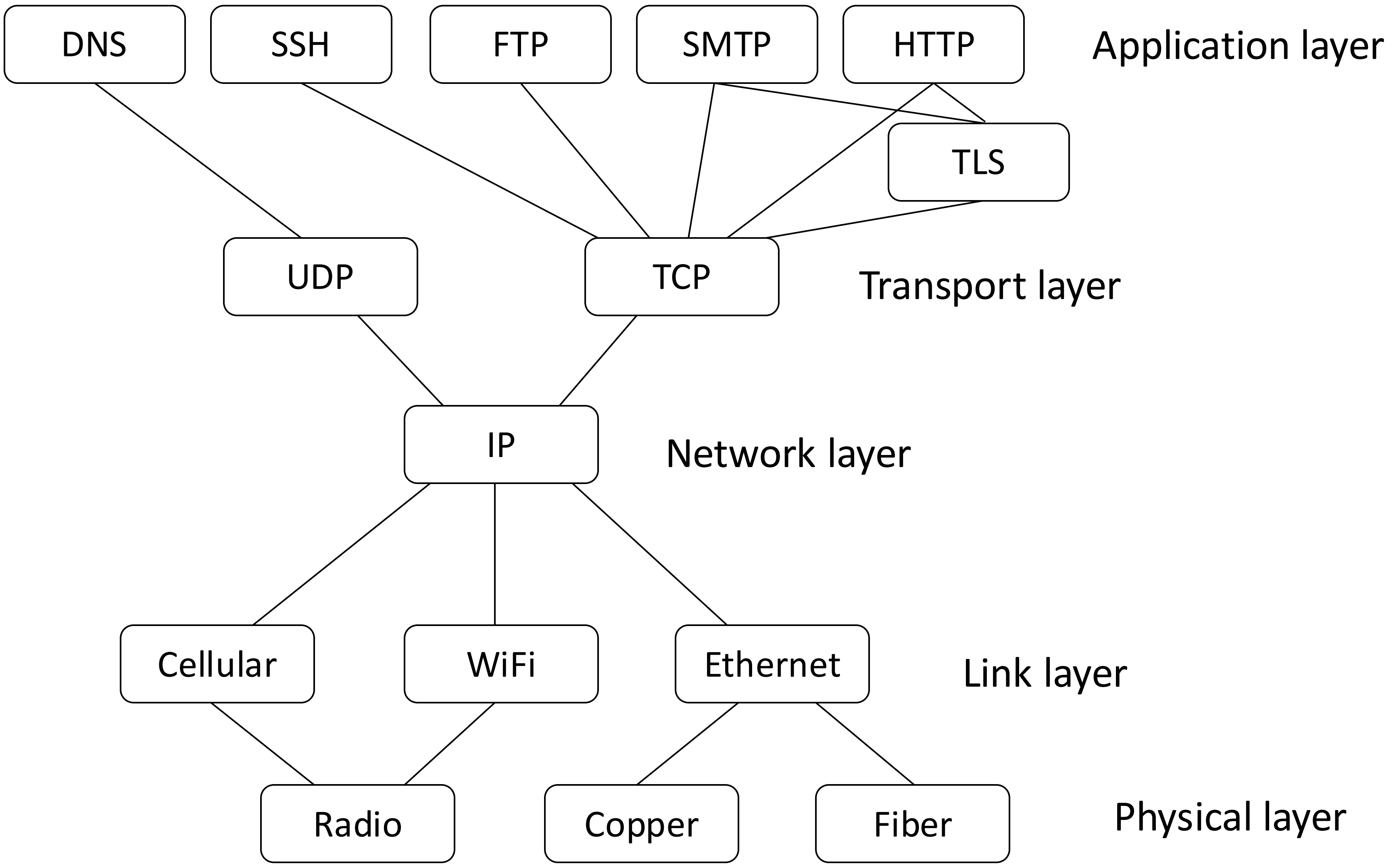
University of Illinois

ECE 422/CS 461

Goals of this Chapter

- By the end of this lecture you should…
  - Understand the (in)security of the IP, IPSec, and BGP protocol
  - Understand Ethernet and how it “glues” the link and network layers together
  - Be able to reason about the (in)security of the Address Resolution Protocol (ARP)

Layering of Protocols



TLS Security Properties

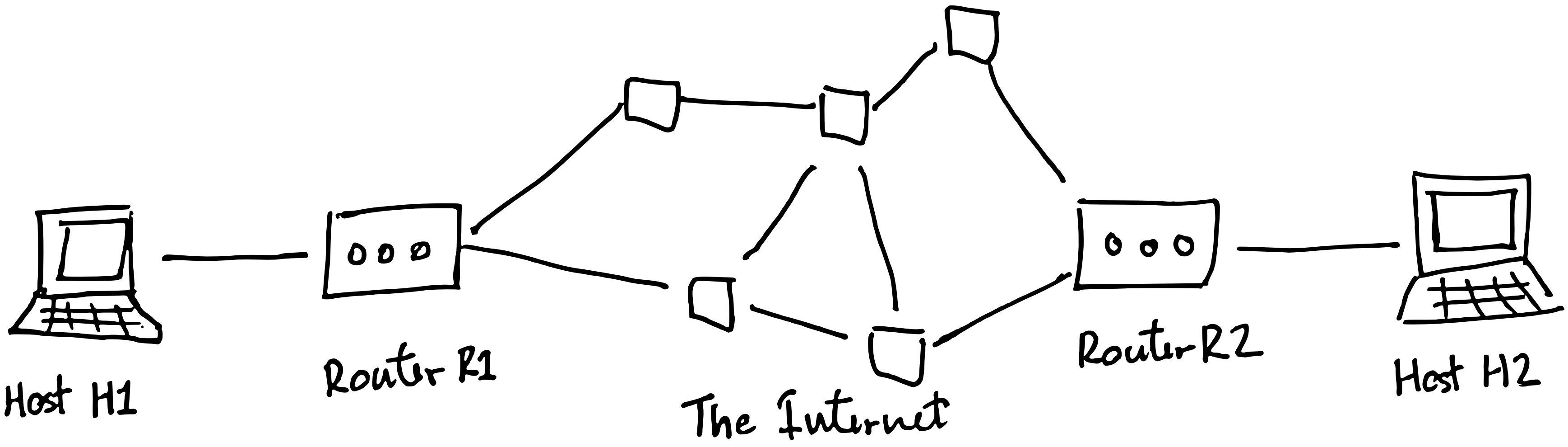
	Passive	Off-Path	MitM
Availability	—	✗	✗
Confidentiality	✓	—	✓
Integrity	—	—	✓
Authenticity	—	✓	✓

- Assumption: crypto + certificate + browser
  - More details in the TLS lecture
- No assumption on lower network layers
- In this lecture, we assume *no* TLS

Network Layer Security

Internet Protocol

- **Internet Protocol (IP)** defines *structure* of packets and *how they are handled* by routers
  - IP packets are also called *datagrams*



IPv4 vs IPv6

- **IPv4:** 32-bit host addresses
  - Written as A.B.C.D, four 8-bit integers in decimal (called *dotted quad*), *e.g.* 192.168.1.1

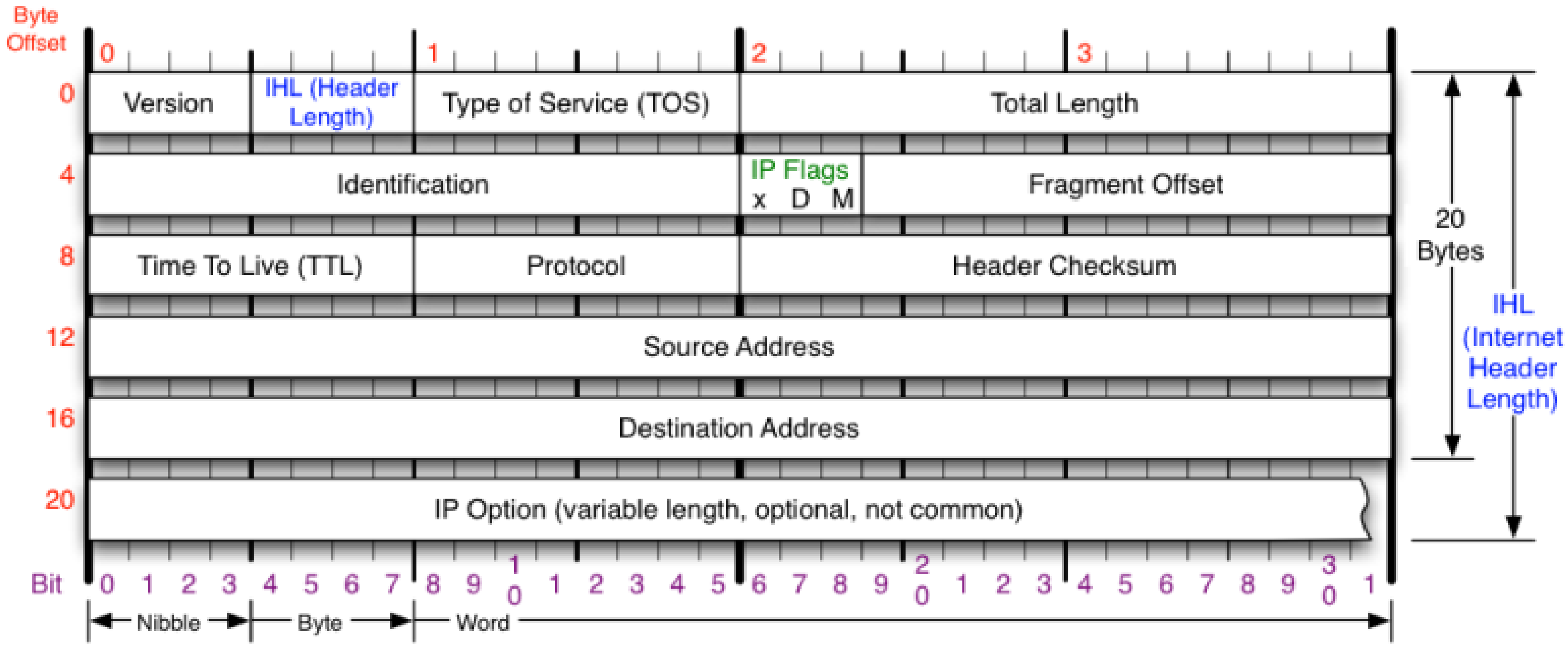
- **IPv6:** 128 bit host addresses
  - Written as A:B::X:Y:Z, 16-bit integers in hexadecimal and :: implies zero bytes
    e.g. 2620:0::e00:b:53 = 2620:0:0:0:0:e00:b:53

IP Packet

- IP header tells routers what to do with the packet
- Rest of packet (payload) is opaque to router
  - Not true anymore: *middleboxes* may examine and modify payload (e.g., to detect malware)
    - Becoming true again: as TLS adoption increases, middleboxes cannot read payload anymore

IPv4 Header

- Tells routers and hosts what to do with packet
- All values filled in by sending host
  - – Including source address, which is not verified



Security Properties of IP

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

- Recall that, by definition,
  - For a passive attacker, confidentiality is the only concern
  - An off-path attack cannot break confidentiality or integrity

Security Properties of IP

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

- As usually, no protection against on-path attackers
- What about off-path attackers?

Security Properties of IP

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

- An off-path attacker can easily inject packets into the network on behalf of other hosts, since source address is not verified by routers
- An off-path attacker can DoS a host by saturating its bandwidth

IPSec

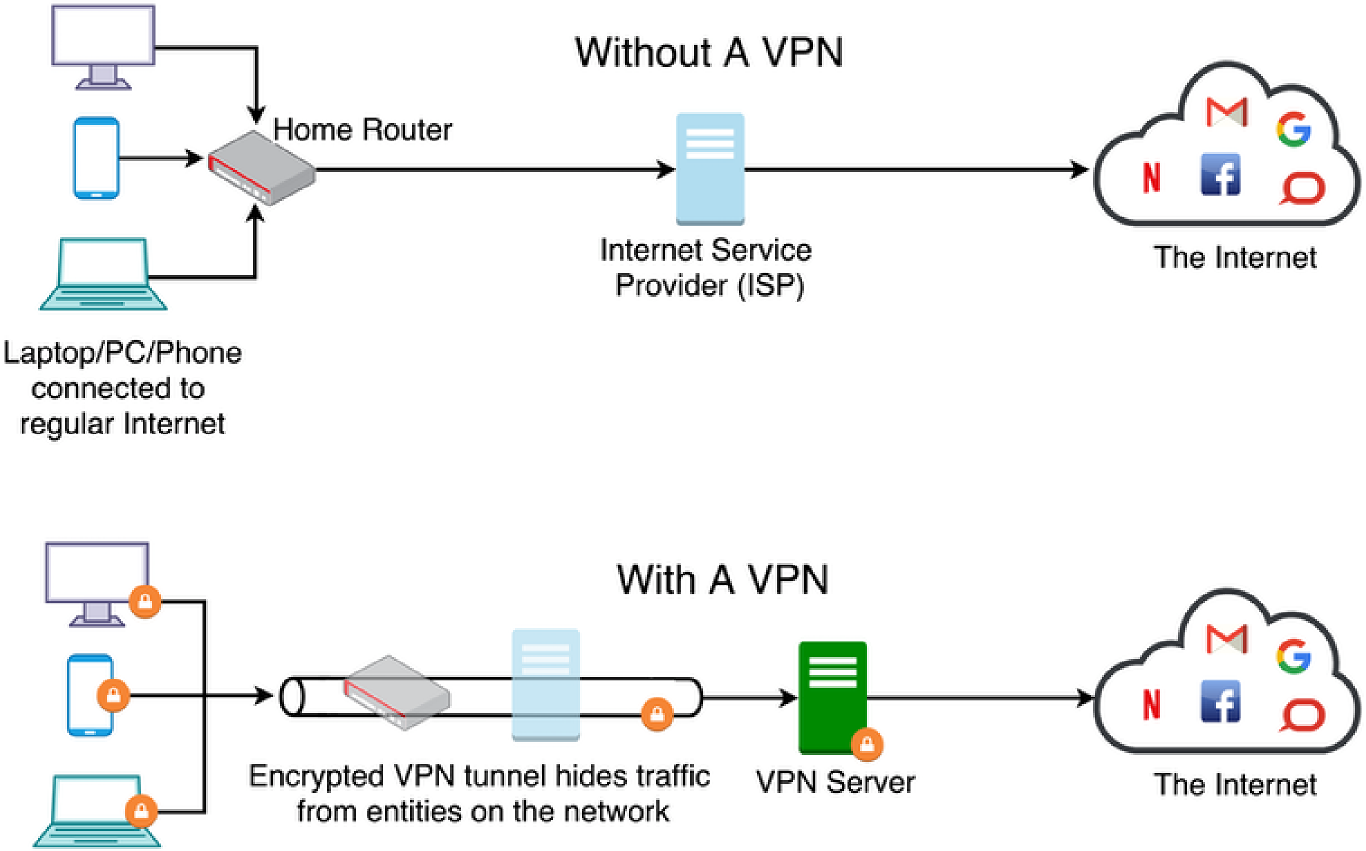
- Add cryptography on top of IP
  - Similar to TLS on top of TCP

- Two main protocols:
  - Authenticated Header (AH) provides integrity only
  - Encapsulation Security Payload (ESP) provides both confidentiality and integrity

- Is IPSec used in practice?

IPSec Adoption

- Is IPSec used in practice?
  - Yes! Many VPNs use IPSec


Without A VPN
Home Router
Internet Service Provider (ISP)
The Internet
Laptop/PC/Phone connected to regular Internet
With A VPN
Encrypted VPN tunnel hides traffic from entities on the network
VPN Server
The Internet

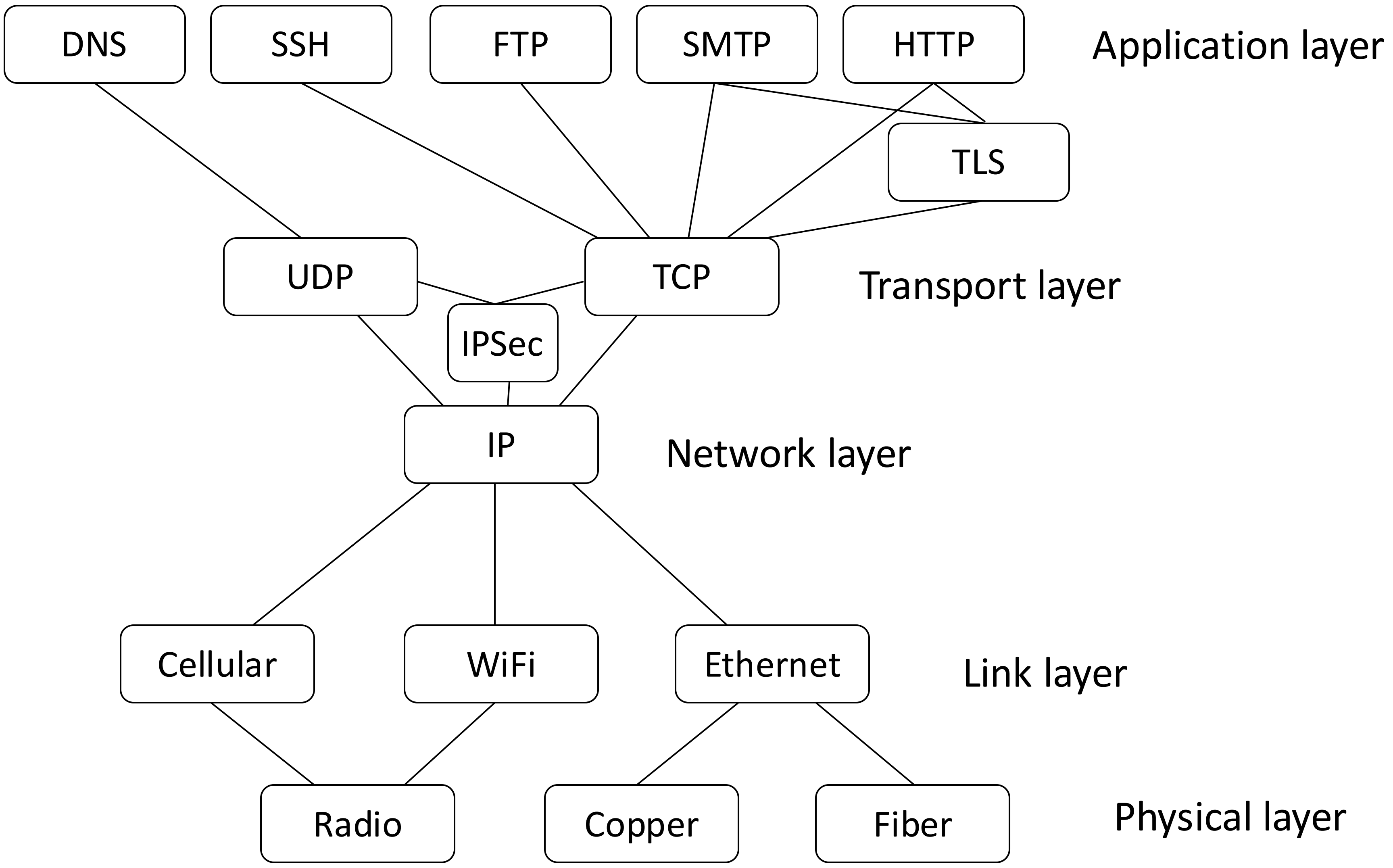
Picture courtesy of
Mohammad Taha Khan

IPSec Adoption

- Is IPSec used in practice?
  - Yes! Many VPNs use IPSec
  - There are also VPNs that use TLS

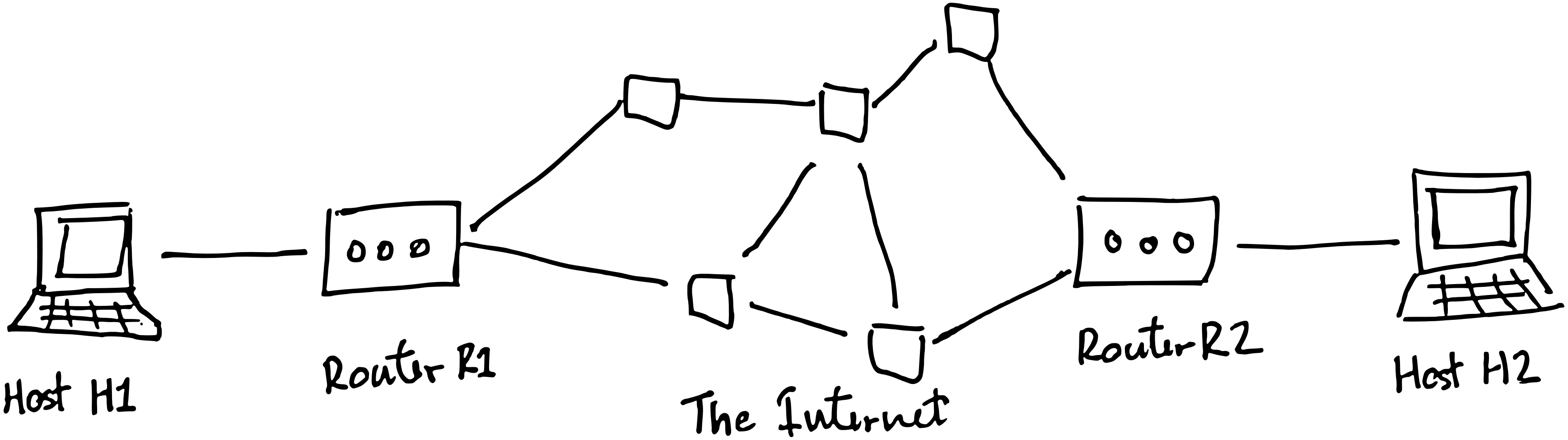
- Pros and cons of IPSec vs. TLS?
  - IPSec sits at a lower level and protects all network traffic; TLS only protects TCP traffic
  - IPSec VPN usually requires installing software; TLS VPN can use browser (and only protects browser)

Layering of Protocols



Routing

- How do routers know where to forward packets so they get to their destinations?

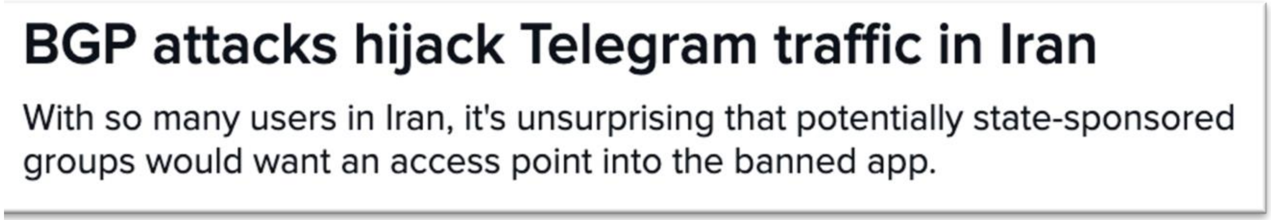


Routing

- Internet routing is handled by Autonomous Systems (AS)
  - Large networks under the control of a single administrator (e.g., AT&T and Verizon)
- Intra-AS, the admin handles routing
- Inter-AS, Border Gateway Protocol (BGP):
  - Obtain reachability info from neighboring ASs
  - Determine ”good routes”

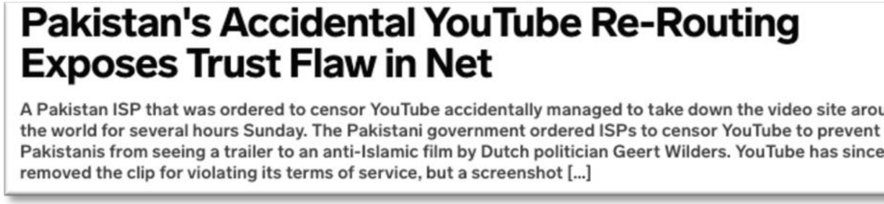
BGP Hijacking

- A malicious AS can falsely claim they have the shortest route to another AS



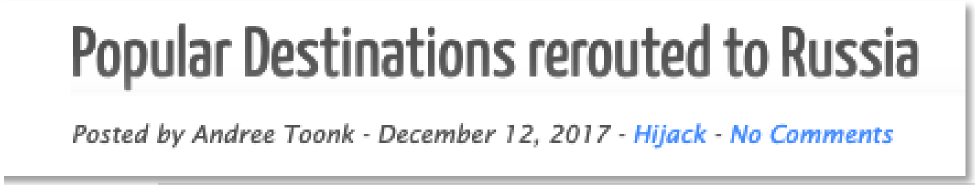
BGP attacks hijack Telegram traffic in Iran

With so many users in Iran, it's unsurprising that potentially state-sponsored groups would want an access point into the banned app.



Pakistan's Accidental YouTube Re-Routing Exposes Trust Flaw in Net

A Pakistan ISP that was ordered to censor YouTube accidentally managed to take down the video site arou
the world for several hours Sunday. The Pakistani government ordered ISPs to censor YouTube to prevent
Pakistanis from seeing a trailer to an anti-Islamic film by Dutch politician Geert Wilders. YouTube has since
removed the clip for violating its terms of service, but a screenshot [...]



Popular Destinations rerouted to Russia

Posted by Andree Toonk - December 12, 2017 - Hijack - No Comments

BGP Hijacking

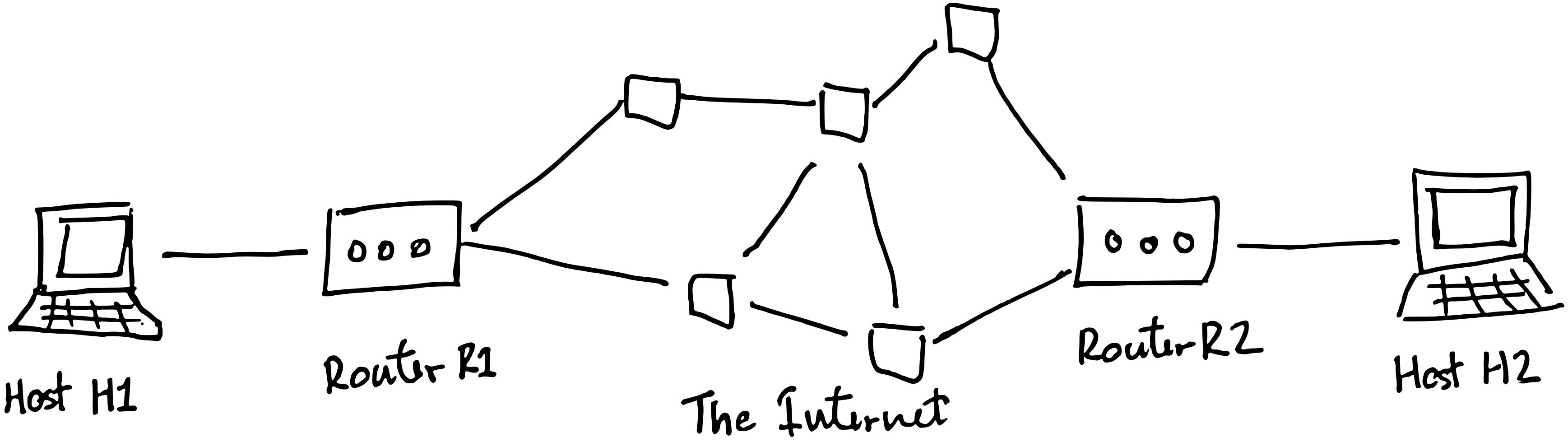
- A malicious AS can falsely claim they have the shortest route to another AS
  - Off-path attacker becomes on-path

- Can break all three properties of CIA (assuming TLS is not used)
  - Denial of service, redirect user to fake websites, eavesdrop (now on-path) traffic

Link Layer Security

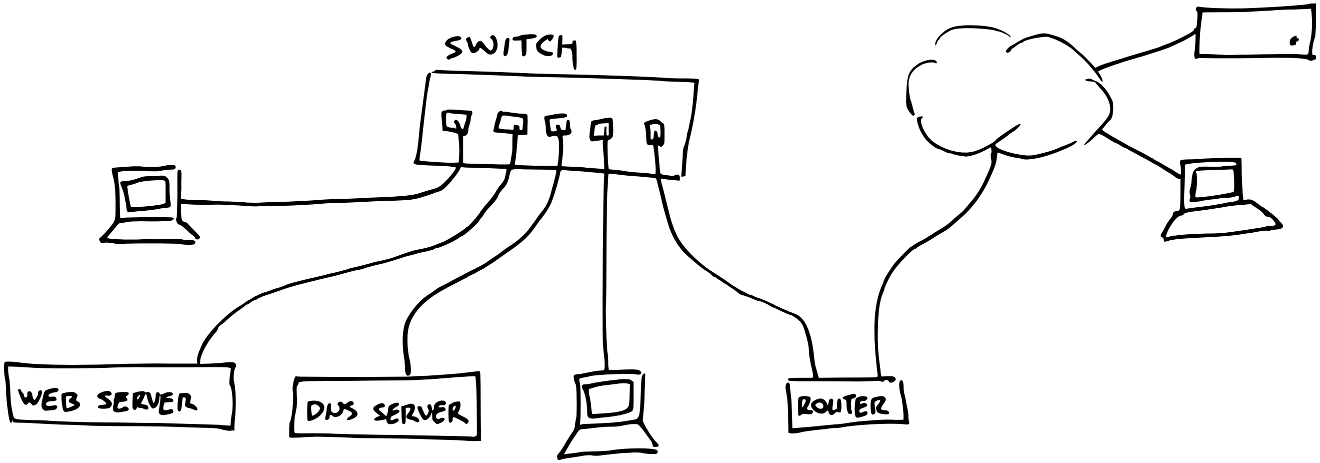
The Link Layer

- Transmits packet from one host to another host that it is physically connected to
- So far, we assumed that hosts deliver and accept packets from Internet routers. The link layer provides connectivity between hosts and routers.



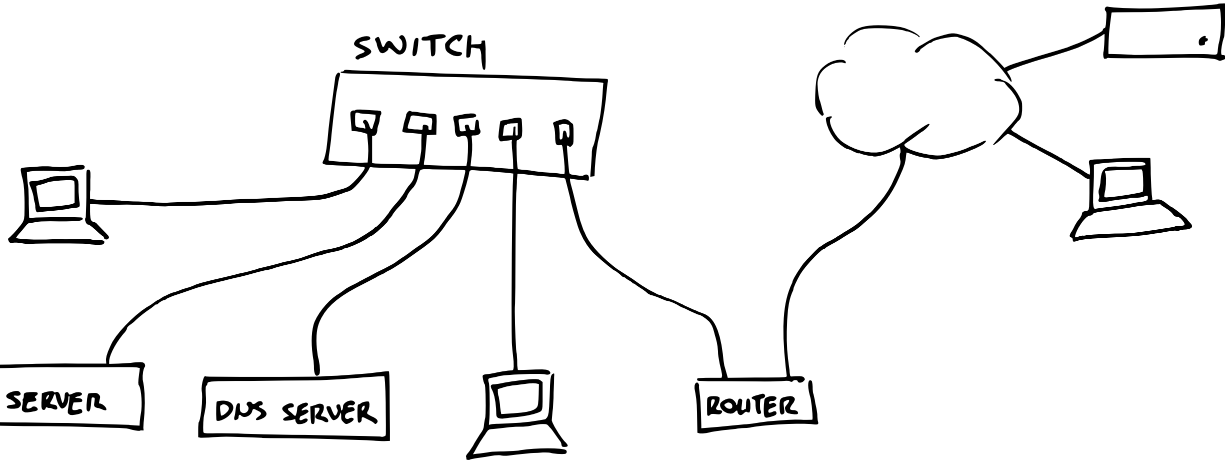
Local Area Networks (LAN)

- Hosts connected by a LAN can communicate directly with each other
- Router is just another device on this LAN that can forward IP datagrams to rest of Internet



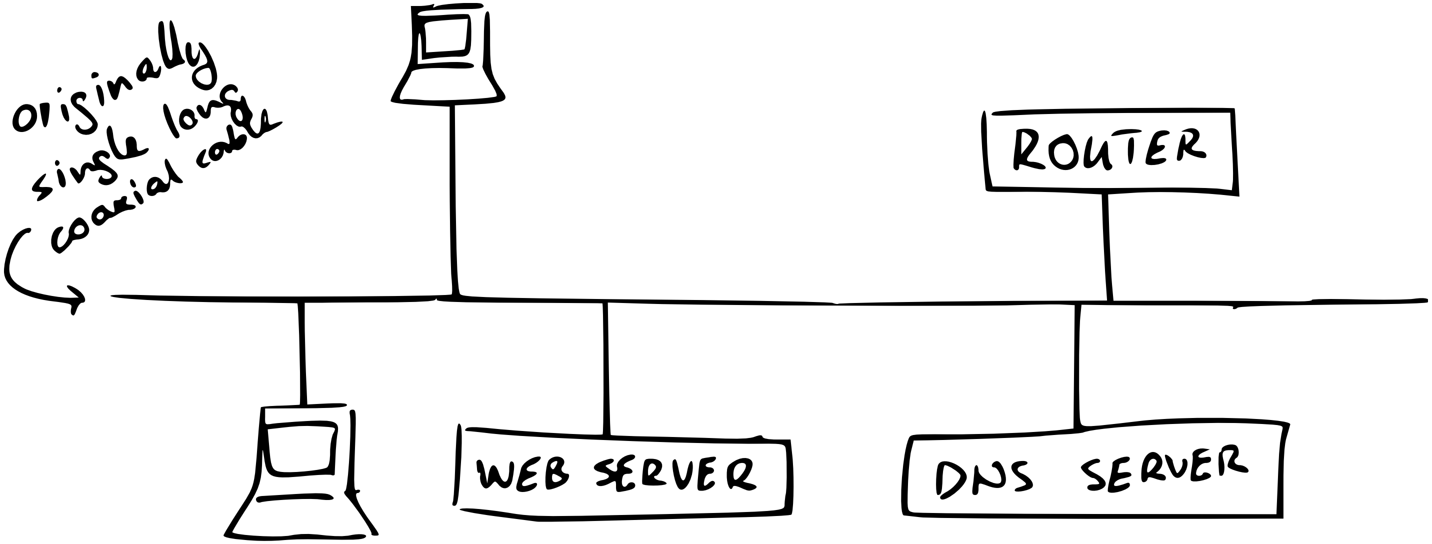
Ethernet

- Most common wired LAN protocol
  - Encompasses layers 1 (physical) and 2 (link)
  - Many different physical layers in use (e.g., WiFi also uses Ethernet packet format)

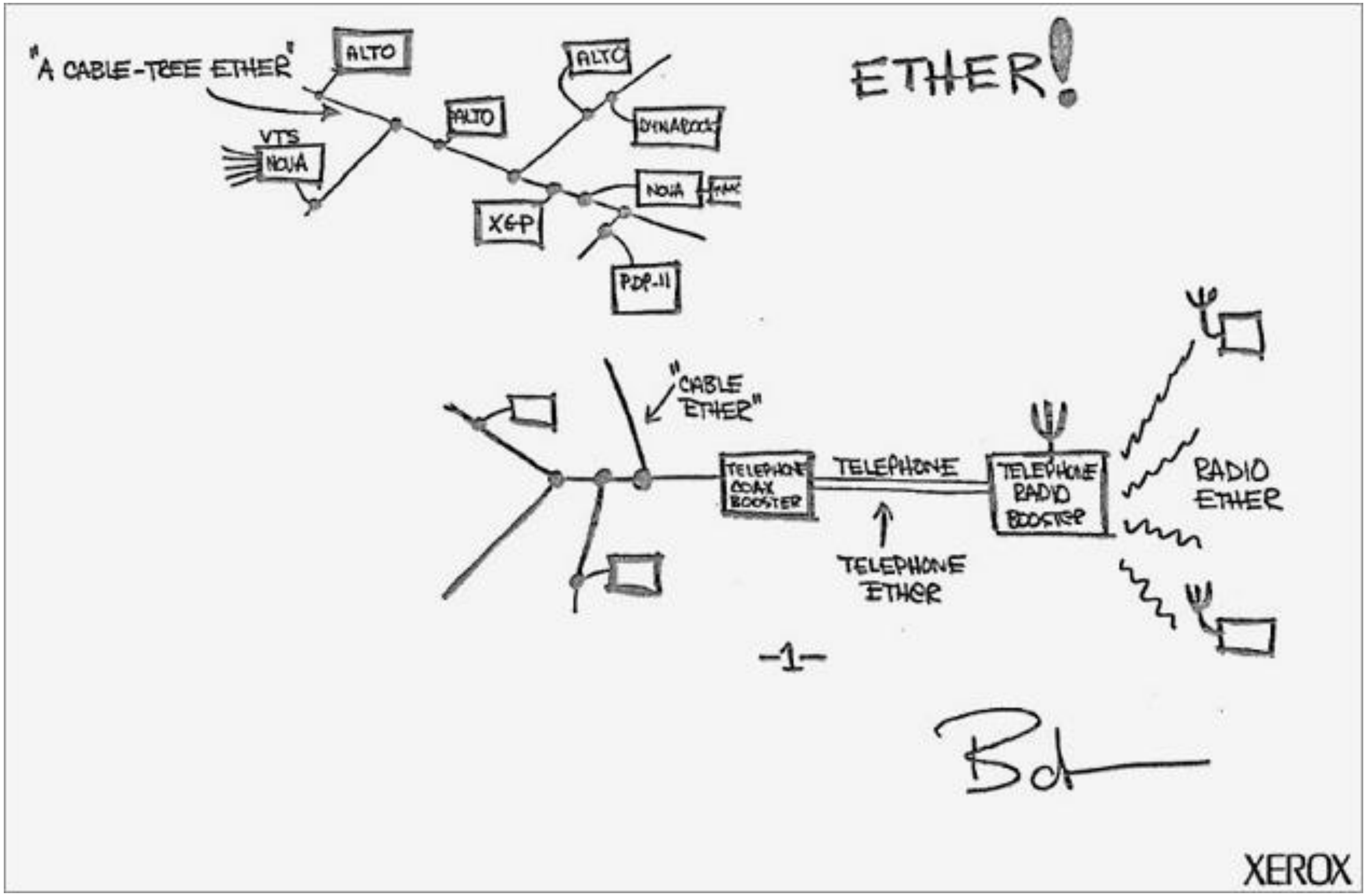


Ethernet (Logical View)

- Reflects the design from early days: a single shared cable
- All packets are *broadcast* to everyone



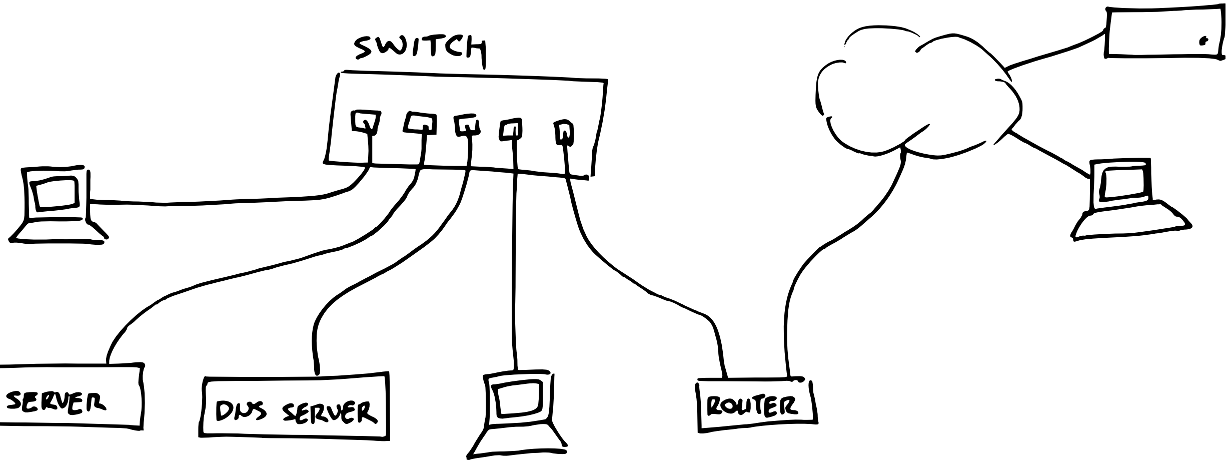
The Original Ethernet



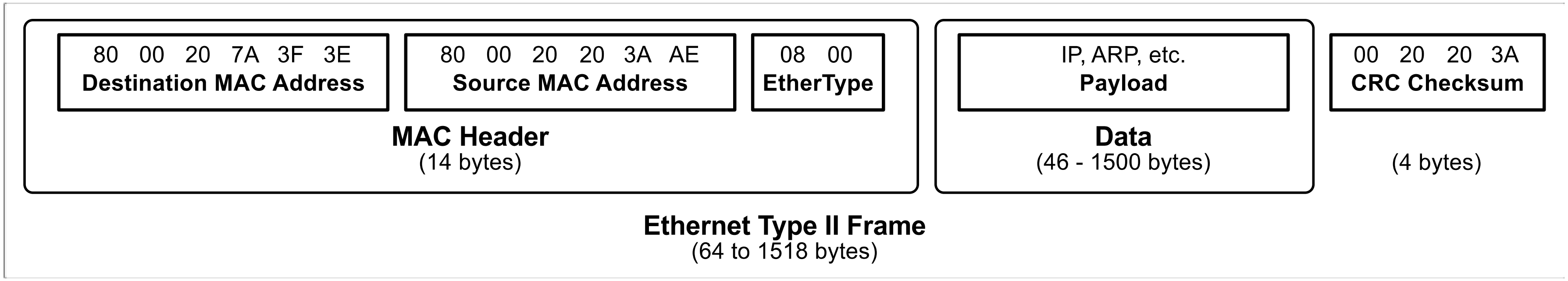
Drawing by Bob Metcalfe, May 22, 1973.

Switched Ethernet

- Switch learns the MAC address of the device at each port when the device sends packets.
  - Can *unicast* to the intended recipient.
  - Can still broadcast to all ports



IP over Ethernet



80 00 20 7A 3F 3E
Destination MAC Address

80 00 20 20 3A AE
Source MAC Address

08 00
EtherType

MAC Header
(14 bytes)

IP, ARP, etc.
Payload

Data
(46 - 1500 bytes)

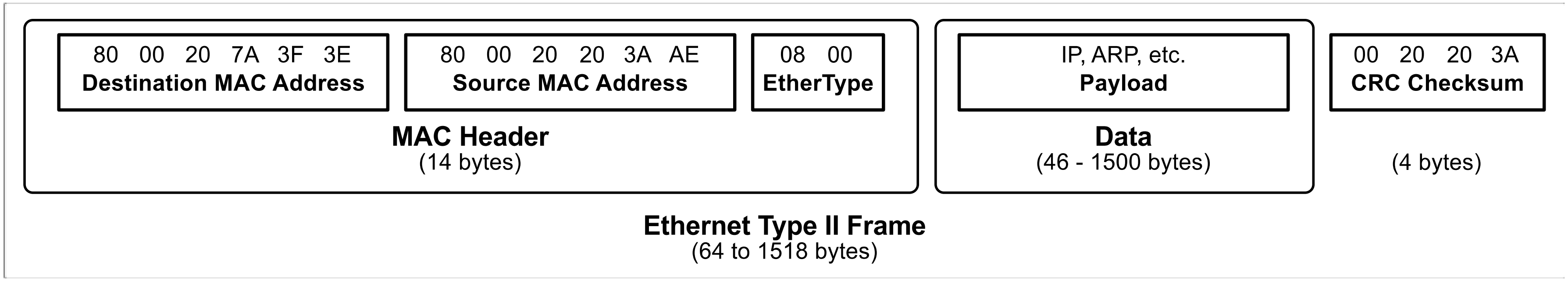
00 20 20 3A
CRC Checksum

(4 bytes)

Ethernet Type II Frame
(64 to 1518 bytes)

- At layer 2 (link layer), packets are called *frames*
- MAC addresses: 48 bits, universally unique
- Payload is often an IP packet

IP over Ethernet



80 00 20 7A 3F 3E
Destination MAC Address

80 00 20 20 3A AE
Source MAC Address

08 00
EtherType

MAC Header
(14 bytes)

IP, ARP, etc.
Payload

Data
(46 - 1500 bytes)

00 20 20 3A
CRC Checksum

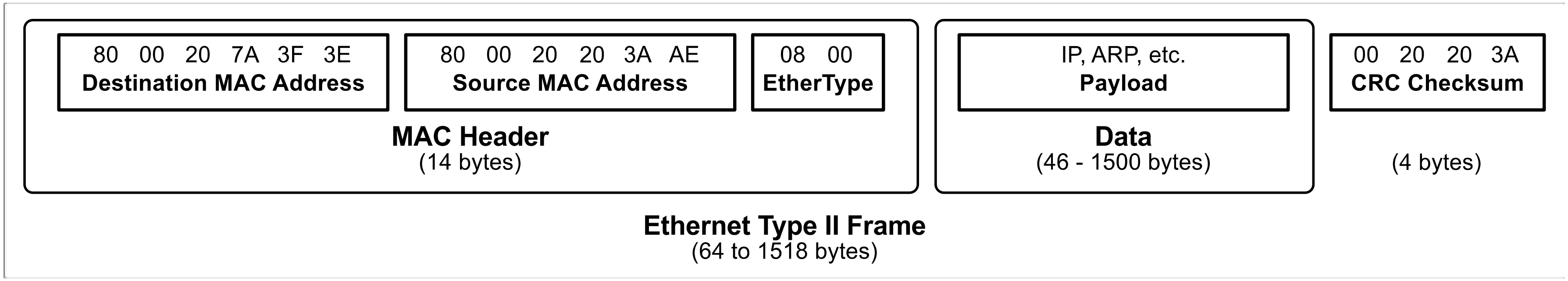
(4 bytes)

Ethernet Type II Frame
(64 to 1518 bytes)

- To send an IP packet to a host in the LAN, sender creates an Ethernet frame with:
  - Destination host’s Ethernet (MAC) address
  - Payload: IP packet

How does sender know this?

IP over Ethernet



80 00 20 7A 3F 3E
Destination MAC Address

80 00 20 20 3A AE
Source MAC Address

08 00
EtherType

MAC Header
(14 bytes)

IP, ARP, etc.
Payload

Data
(46 - 1500 bytes)

00 20 20 3A
CRC Checksum

(4 bytes)

Ethernet Type II Frame
(64 to 1518 bytes)

- To send an IP packet to a host outside the LAN, sender creates an Ethernet frame with:
  - Router’s Ethernet (MAC) address
  - Payload: IP packet

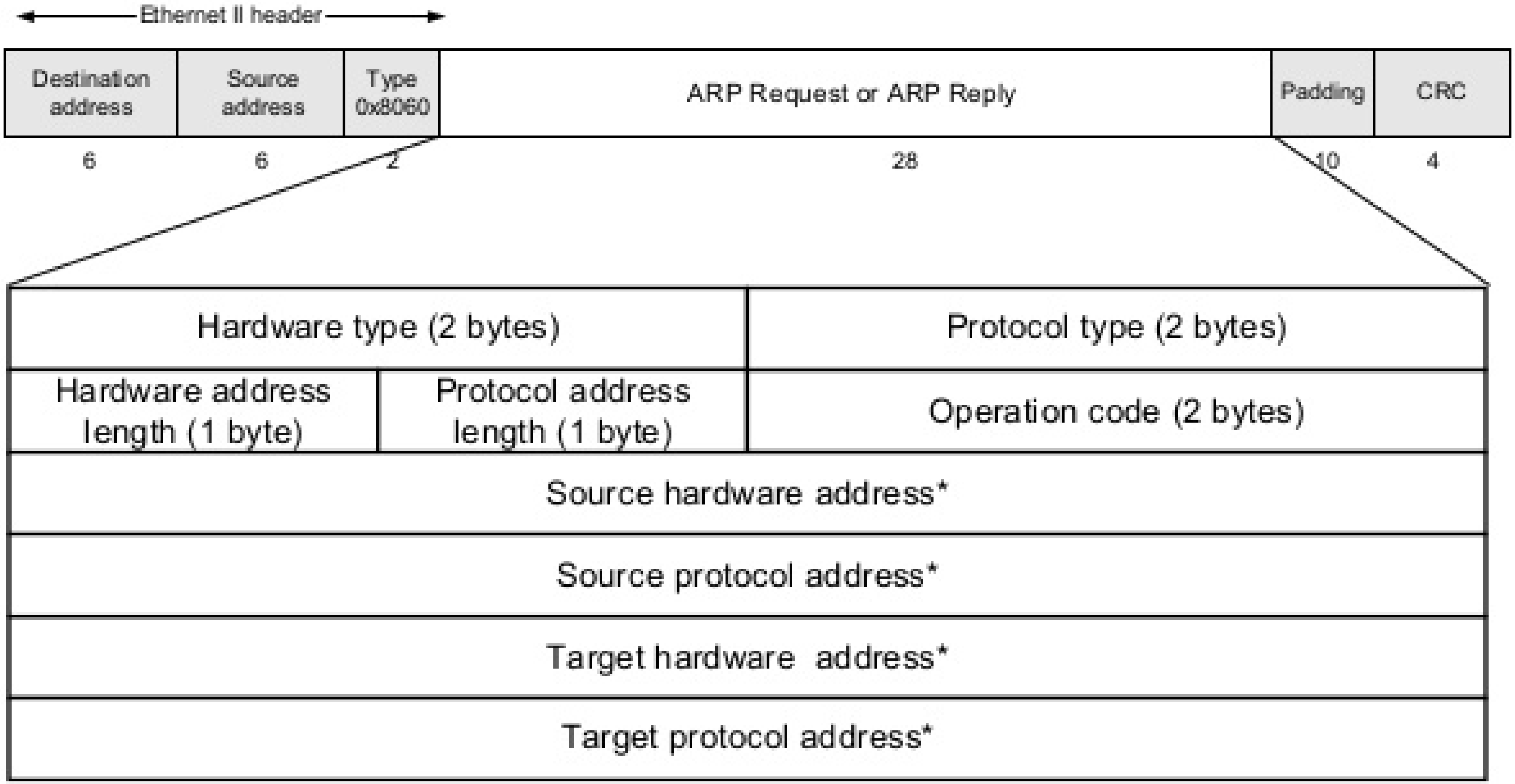
How does sender know this?

- Router receives Ethernet frame, forwards the encapsulated IP packet to next router, …

Address Resolution Protocol (ARP)

- Lets hosts map IP addresses to MAC addresses
- Requester broadcasts an ARP packet to LAN: “who has IP address 192.138.1.52?”
- Host that has the IP address will reply: “IP 192.138.1.52 is at MAC address 2C:54:91:88:C9:E3
- Requester will cache this reply for future use

ARP Packet Format



Ethernet II header

Destination address

Source address

Type 0x8060

ARP Request or ARP Reply

Padding

CRC

6

6

2

28

10

4

Hardware type (2 bytes)

Protocol type (2 bytes)

Hardware address length (1 byte)

Protocol address length (1 byte)

Operation code (2 bytes)

Source hardware address*

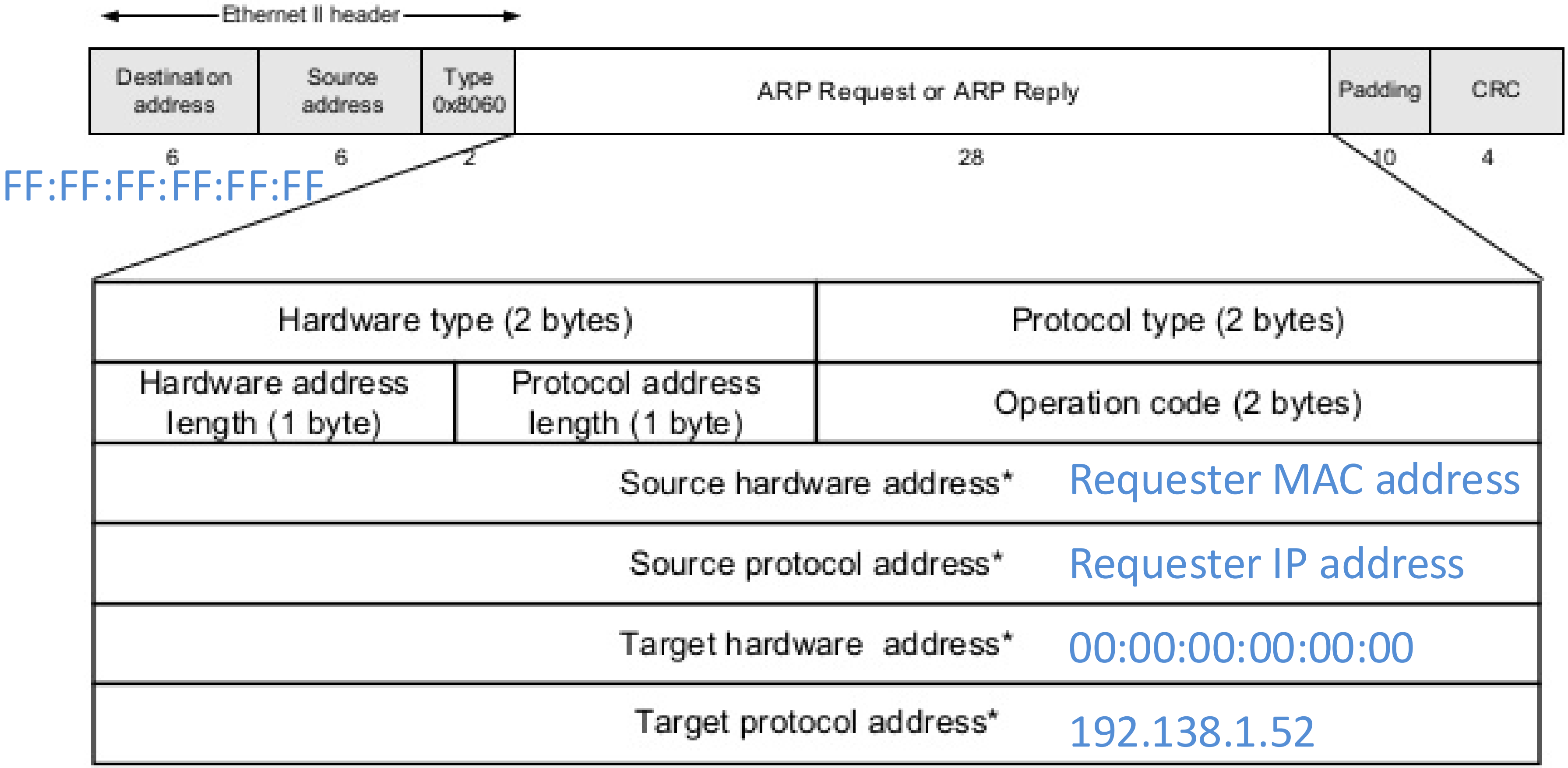
Source protocol address*

Target hardware address*

Target protocol address*

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

ARP Request



Ethernet II header

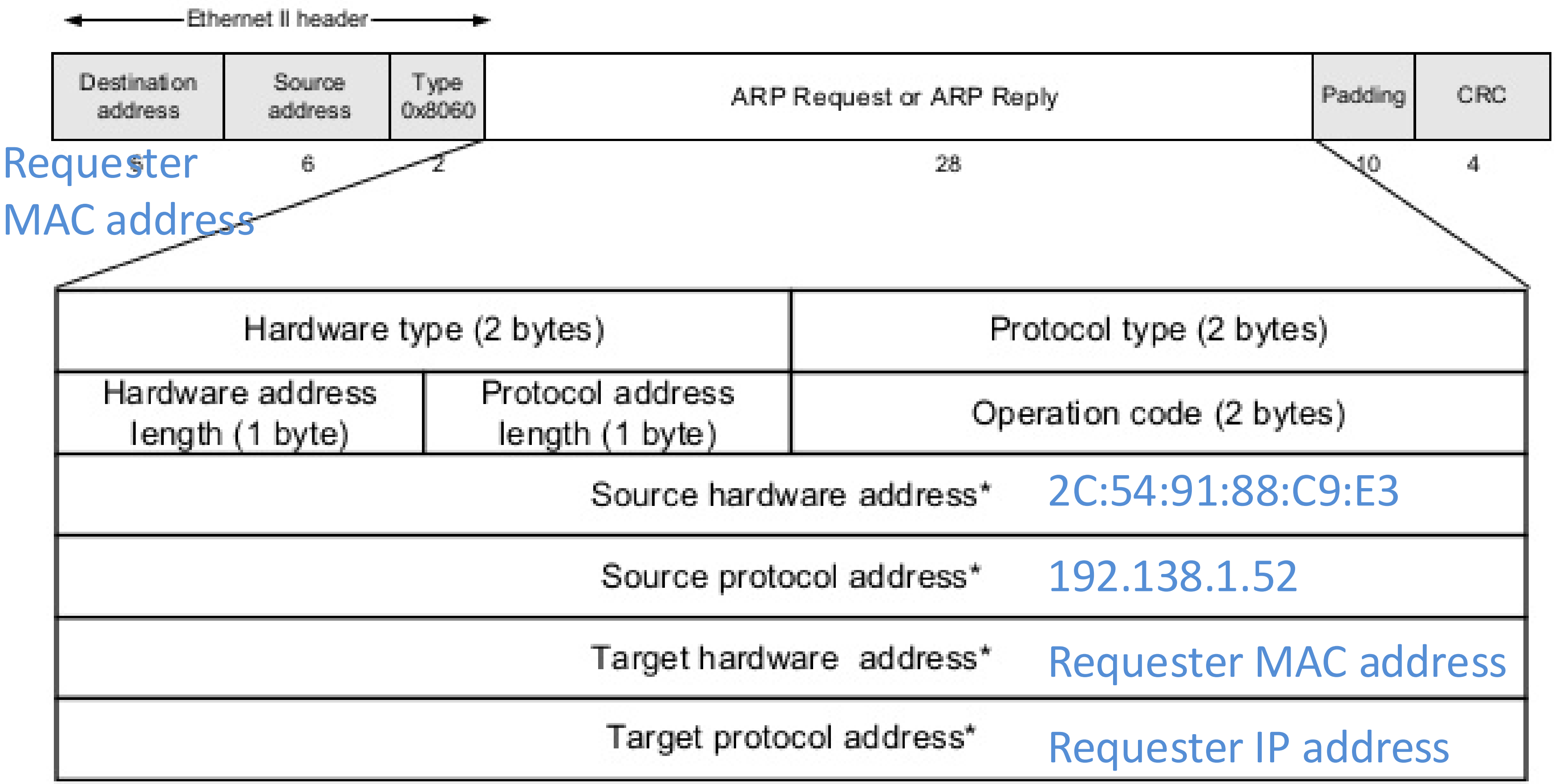
Destination address	Source address	Type 0x8060	ARP Request or ARP Reply	Padding	CRC
6	6	2	28	10	4

FF:FF:FF:FF:FF:FF

Hardware type (2 bytes)		Protocol type (2 bytes)	
Hardware address length (1 byte)	Protocol address length (1 byte)	Operation code (2 bytes)	
Source hardware address*			Requester MAC address
Source protocol address*			Requester IP address
Target hardware address*			00:00:00:00:00:00
Target protocol address*			192.138.1.52

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

ARP Response



Ethernet II header

Destination address	Source address	Type 0x8060	ARP Request or ARP Reply	Padding	CRC
6	6	2	28	10	4

Requester MAC address

Hardware type (2 bytes)		Protocol type (2 bytes)
Hardware address length (1 byte)	Protocol address length (1 byte)	Operation code (2 bytes)

Source hardware address* 2C:54:91:88:C9:E3

Source protocol address* 192.138.1.52

Target hardware address* Requester MAC address

Target protocol address* Requester IP address

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

ARP Security

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

- Recall that, by definition,
  - For a passive attacker, confidentiality is the only concern
  - An off-path attack cannot break confidentiality or integrity

ARP Security

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

- No protection against MitM attacker

- How about an off-path attacker?

ARP Spoofing

- Any host in the LAN can send ARP response to claim to be any other host!
  - Last response wins
- An off-path attacker can get on-path
  - Send ARP response to host A claiming to be host B, send ARP response to host B claiming to be host A.
- You will do these in MP4

ARP Security

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

- No protection against MitM attacker
- Off-Path attackers can get on-path via ARP Spoofing

Securing ARP

- Static ARP: manually add all IP-MAC mappings to each host’s cache
  - Con: maintenance cost
- Smarter switch: watch if a MAC claims many IPs
  - Con: may not detect targeted attacks
- Smarter hosts: raise alert if it sees someone impersonating it
  - Con: He-said-she-said (authenticity of alert?)
- Use crypto?
  - Con: maintenance cost of PKI

Securing ARP

- No significant defense deployed or planned
- Rely on higher layers for security (e.g., TLS)
- Rely on physical/peripheral security to keep attackers out

- Wireless networks cannot enforce peripheral security, so they often require passwords and use encryption + message authentication
  - WPA, WPA2, WPA3 (WiFi Protected Access)

Summary

- IP has no security features
- IPSec on top IP, similar to TLS on top of TCP
  - Used by many VPNs
- BGP for inter-AS routing; BGP hijacking
- ARP glues link and network layers
- ARP has no security feature
  - Rely on security of higher layers and physical security