الجامعة الافتراضية السورية

أمن الشبكات

Network and Infrastructure Security

د. محمد العصورة

Dr. Mohammed Assora

دكتوراه في امن شبكات الحواسب

PhD. In Computer Network Security

Objectives of Lecture

- Understand the different components that are likely to be found in a network.
- Study the major network protocols (focussing on TCP/IP networks).
- Develop an awareness of the inherent security risks of using these components and protocols.
- Study a few ‘classic’ attacks on networks: ARP spoofing, TCP Denial of Service, network sniffing.

Contents

In this lecture, we take a layer-by-layer look at the most important network components and protocols, and associated security issues:

2.1 Cabling and Hubs (Layer 1); Sniffers

2.2 Switches and ARP (Layer 2)

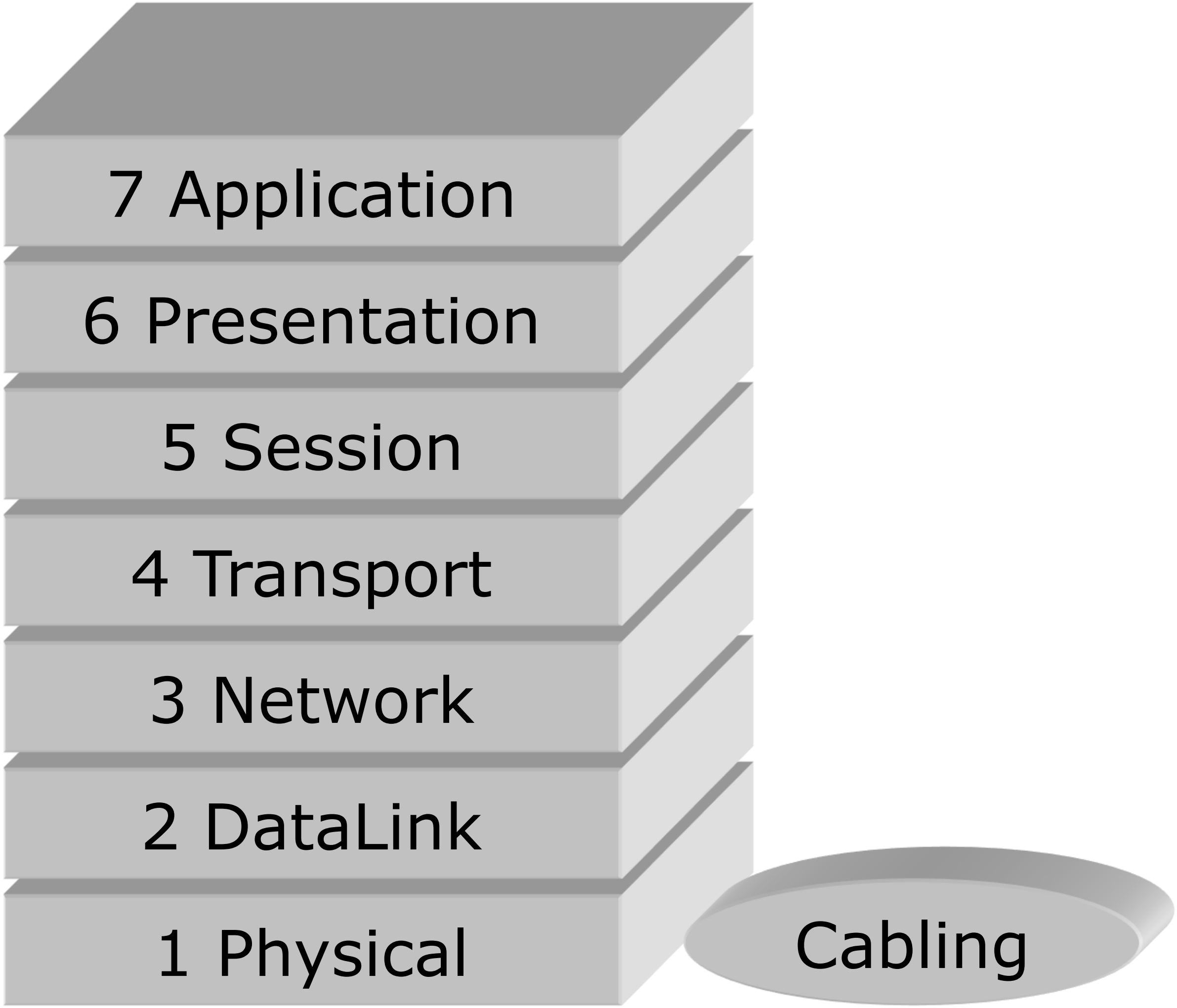
2.3 Routers and IP (Layer 3)

2.4 TCP and ICMP (Layer 4)

2.1 Cabling, Hubs and Sniffers

- Cabling and Hubs
  - TCP/IP Layer 1 (physical) devices.
  - Cabling connects other components together.
  - Hubs provide a point where data on one cable can be transferred to another cable.
  - We study their basic operation and associated security issues.
- Sniffers
  - Layer 2 devices for capturing and analysing network traffic.

Cabling in OSI Protocol Stack



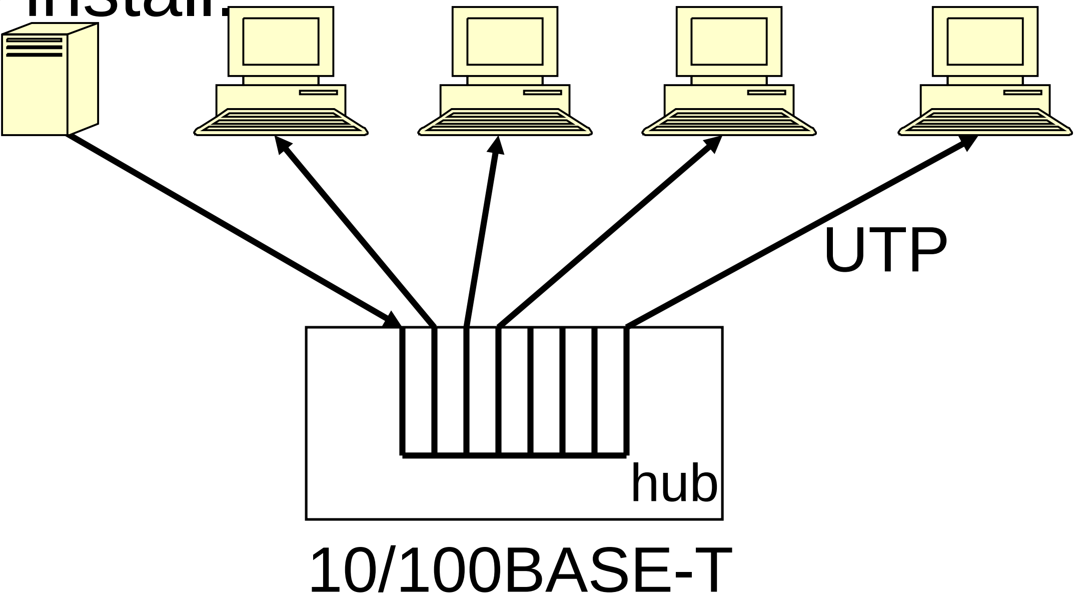
Cabling Security Issues

- All four fundamental threats can be realised by attacks on cabling:
  - Information Leakage: attacker taps cabling and reads traffic
  - Integrity Violation: attacker taps and injects traffic, or traffic corrupted in transit
  - Denial of Service: cabling damaged
  - Illegitimate Use: attacker taps cabling and uses network resources
- Some contributory factors in assessing risk:
  - Single or multi-occupancy building?
  - How is access controlled to floor/building?
  - Does network cabling pass through public areas?
  - Is the network infrastructure easily accessible or is it shared?
  - What is the electromagnetic environment like?
  - Is there any wireless connection in your network infrastructure?

- Safeguards: dedicated closets, electromagnetic shielding.

UTP and Hub

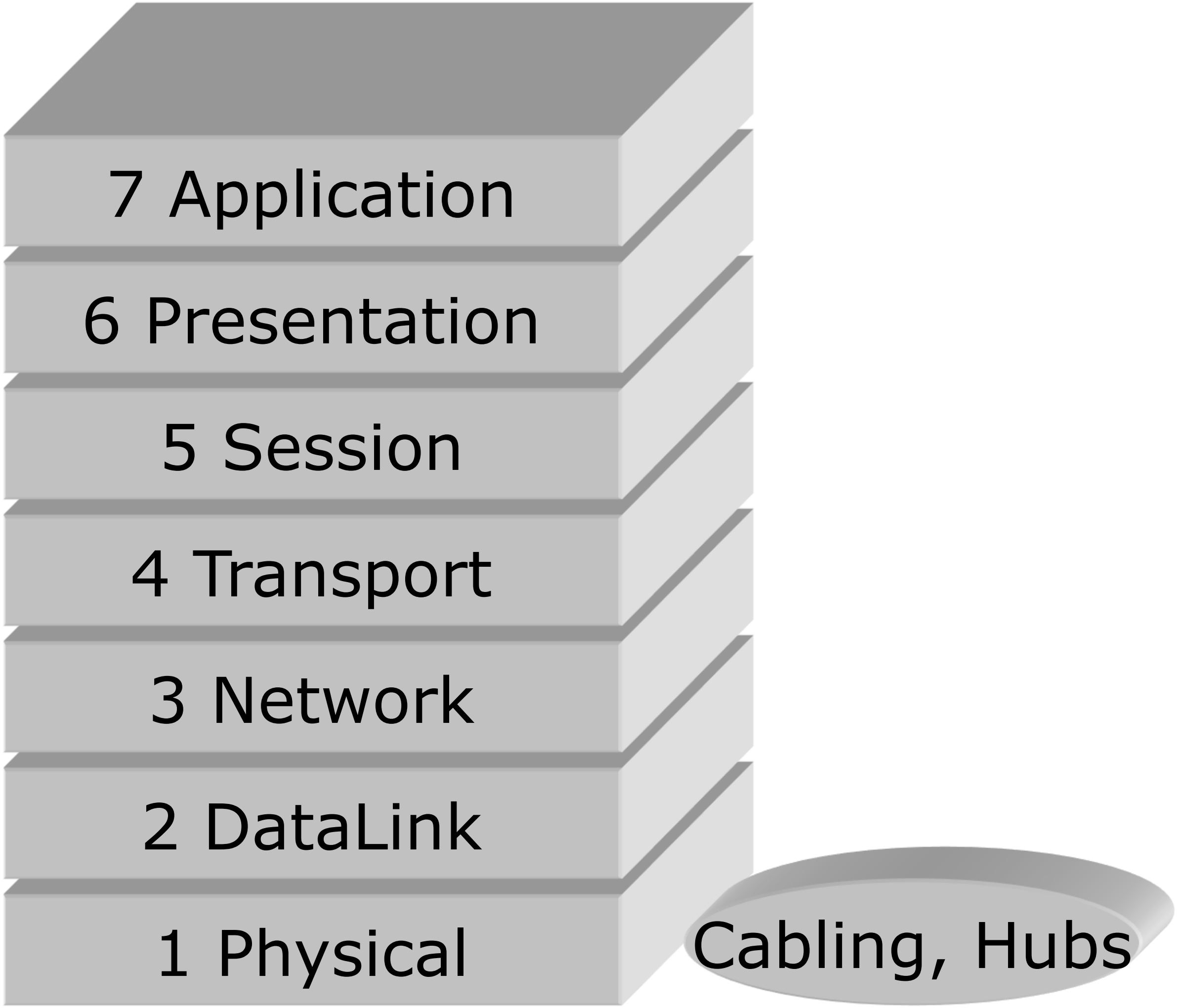
- Cable between hub and device is single entity.
- Only connectors are at the cable ends.
- Disconnection/cable break rarely affects other devices.
- Easy to install.



Hub Security Issues

- Data is broadcast to all devices on the hub.
  - Threat: Information Leakage.
- Easy to install and attach additional devices.
  - Good from a network management perspective.
  - But, unless hub physically secured, anyone can plug into hub.
  - Even if hub secured, attacker can unplug existing device or make use of currently unused cable end.
  - Threats: All four fundamental threats are enabled.

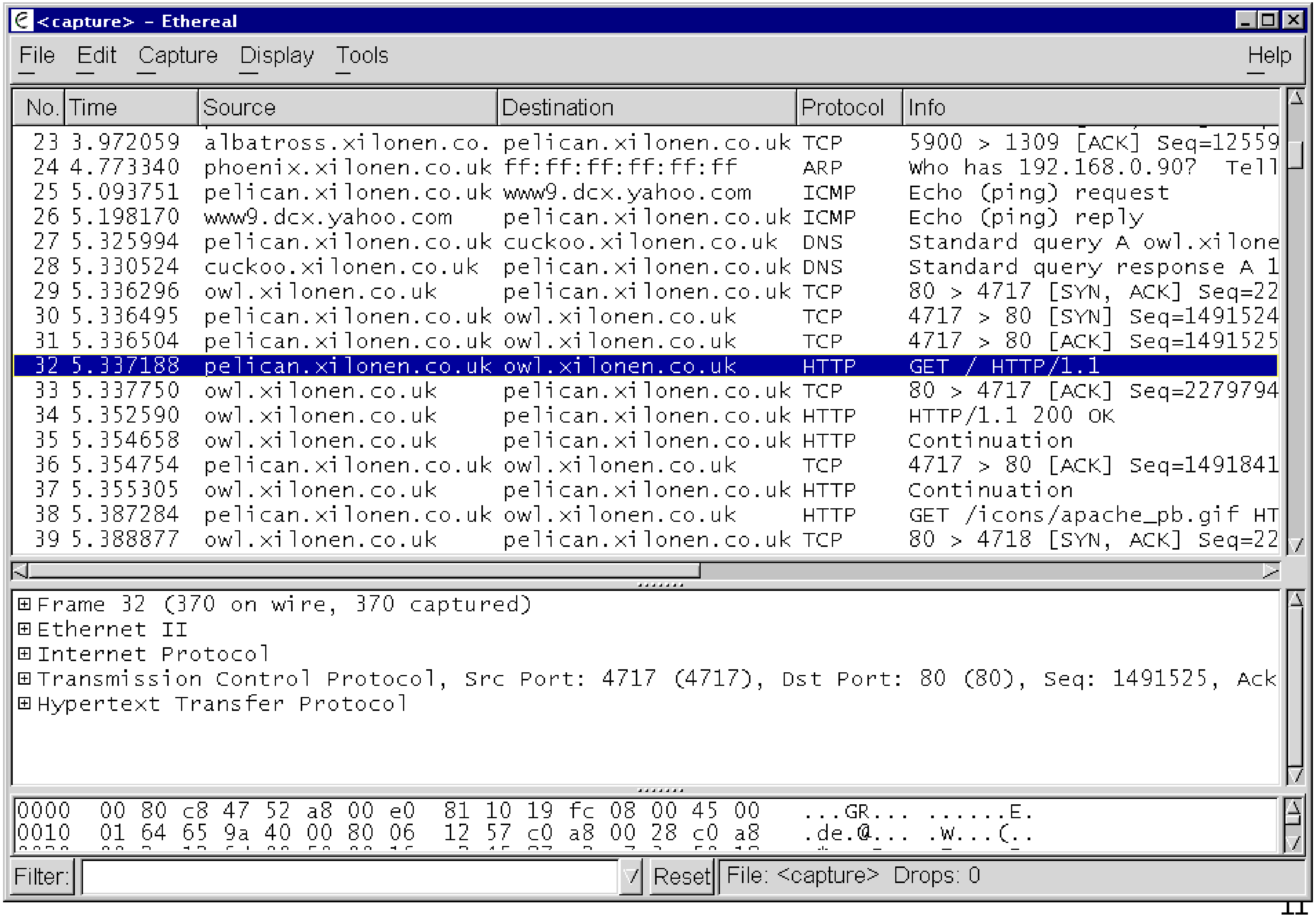
Hubs in OSI Protocol Stack



Network Sniffers

- Network Interface Cards (NICs) normally operate in non-promiscuous mode.
  - Only listen for frames with their MAC address.
- A sniffer changes a NIC into promiscuous mode.
  - Reads frames regardless of MAC address.
- Many different sniffers:
  - Tcpdump
  - Wireshark
  - Snort

Wireshark Screenshot



```
No. Time       Source                   Destination              Protocol   Info
 23 3.972059  albatross.xilonen.co.  pelican.xilonen.co.uk  TCP       5900 > 1309 [ACK] Seq=12559
 24 4.773340  phoenix.xilonen.co.uk  ff:ff:ff:ff:ff:ff      ARP       Who has 192.168.0.90?  Tell
 25 5.093751  pelican.xilonen.co.uk  www9.dcx.yahoo.com     ICMP      Echo (ping) request
 26 5.198170  www9.dcx.yahoo.com     pelican.xilonen.co.uk  ICMP      Echo (ping) reply
 27 5.325994  pelican.xilonen.co.uk  cuckoo.xilonen.co.uk   DNS       Standard query A owl.xilone
 28 5.330524  cuckoo.xilonen.co.uk   pelican.xilonen.co.uk  DNS       Standard query response A 1
 29 5.336296  owl.xilonen.co.uk      pelican.xilonen.co.uk  TCP       80 > 4717 [SYN, ACK] Seq=22
 30 5.336495  pelican.xilonen.co.uk  owl.xilonen.co.uk      TCP       4717 > 80 [SYN] Seq=1491524
 31 5.336504  pelican.xilonen.co.uk  owl.xilonen.co.uk      TCP       4717 > 80 [ACK] Seq=1491525
 32 5.337188  pelican.xilonen.co.uk  owl.xilonen.co.uk      HTTP      GET / HTTP/1.1
 33 5.337750  owl.xilonen.co.uk      pelican.xilonen.co.uk  TCP       80 > 4717 [ACK] Seq=2279794
 34 5.352590  owl.xilonen.co.uk      pelican.xilonen.co.uk  HTTP      HTTP/1.1 200 OK
 35 5.354658  owl.xilonen.co.uk      pelican.xilonen.co.uk  HTTP      Continuation
 36 5.354754  pelican.xilonen.co.uk  owl.xilonen.co.uk      TCP       4717 > 80 [ACK] Seq=1491841
 37 5.355305  owl.xilonen.co.uk      pelican.xilonen.co.uk  HTTP      Continuation
 38 5.387284  pelican.xilonen.co.uk  owl.xilonen.co.uk      HTTP      GET /icons/apache_pb.gif HT
 39 5.388877  owl.xilonen.co.uk      pelican.xilonen.co.uk  TCP       80 > 4718 [SYN, ACK] Seq=22
```

```
⊞ Frame 32 (370 on wire, 370 captured)
⊞ Ethernet II
⊞ Internet Protocol
⊞ Transmission Control Protocol, Src Port: 4717 (4717), Dst Port: 80 (80), Seq: 1491525, Ack
⊞ Hypertext Transfer Protocol
```

```
0000  00 80 c8 47 52 a8 00 e0  81 10 19 fc 08 00 45 00   ...GR... ......E.
0010  01 64 65 9a 40 00 80 06  12 57 c0 a8 00 28 c0 a8   .de.@... .W...(..
```

Sniffing Legitimately

- Do they have legitimate uses?
  - Yes … when used in an authorised and controlled manner.
  - Network analyzers or protocol analyzers.
  - With complex networks, they are used for fault investigation and performance measurement.
  - Useful when understanding how a product uses the network.
  - Network-based Intrusion Detection Systems (NIDS)
    - Monitor network traffic, looking for unusual behaviour or typical attack patterns.

Detecting Sniffers

- Very difficult, but sometimes possible.
  - Tough to check remotely whether a device is sniffing. Approaches include:
    - Sending large volumes of data, then sending ICMP ping request and observing delay as sniffer processes large amount of data.
    - Sending data to unused IP addresses and watching for DNS requests for those IP addresses.
  - AntiSniff, Security Software Technologies.
  - http://www.packetwatch.net/documents/papers/snifferdetection.pdf

Sniffer Safeguards

Examples of safeguards are:

- Use of non-promiscuous interfaces.
- Use of switched environments (but see next section!)
- Encryption of network traffic.
- One-time passwords, e.g. SecurID, skey, limiting usefulness of information gathered by sniffer.

2.2 Switches and Layer 2 Issues

- More on Ethernet and IP addressing.
- Switch operation.
- Security issues for layer 2/switches - ARP spoofing and MAC flooding.
- Safeguards.

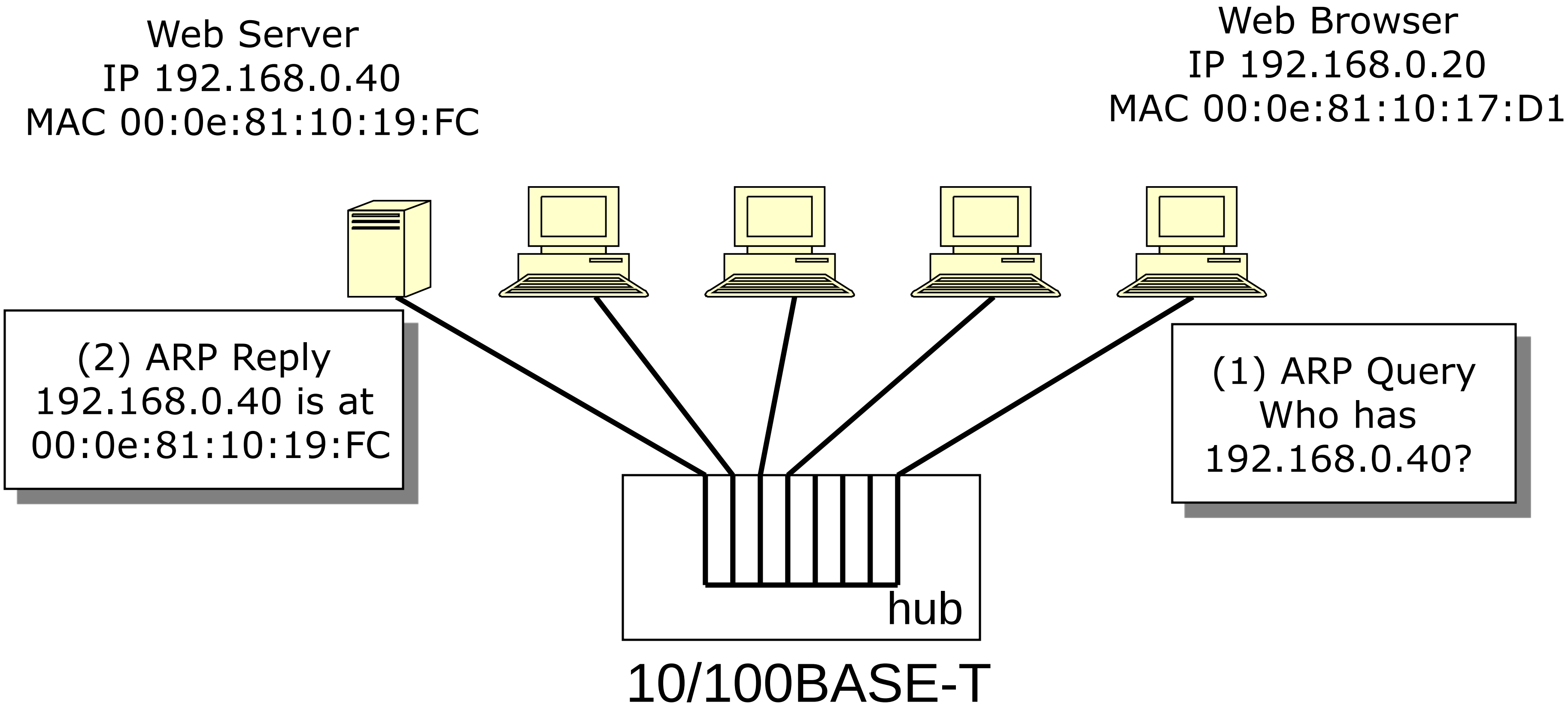
Ethernet Addressing

- Address of Network Interface Card.
- Unique 48 bit value.
  - first 24 bits indicate vendor.
- For example, 00:E0:81:10:19:FC.
  - 00:E0:81 indicates Tyan Corporation.
  - 10:19:FC indicates 1,055,228th NIC.
- Media Access Control (MAC) address.

IP Address to Ethernet Address

- Address Resolution Protocol (ARP):
  - Layer 3 protocol,
  - Maps IP address to MAC address.
- ARP Query
  - Who has 192.168.0.40? Tell 192.168.0.20.
- ARP Reply
  - 192.168.0.40 is at 00:0e:81:10:19:FC.
- ARP caches for speed:
  - Records previous ARP replies,
  - Entries are aged and eventually discarded.

ARP Query & ARP Reply



Web Server
IP 192.168.0.40
MAC 00:0e:81:10:19:FC

Web Browser
IP 192.168.0.20
MAC 00:0e:81:10:17:D1

(2) ARP Reply
192.168.0.40 is at
00:0e:81:10:19:FC

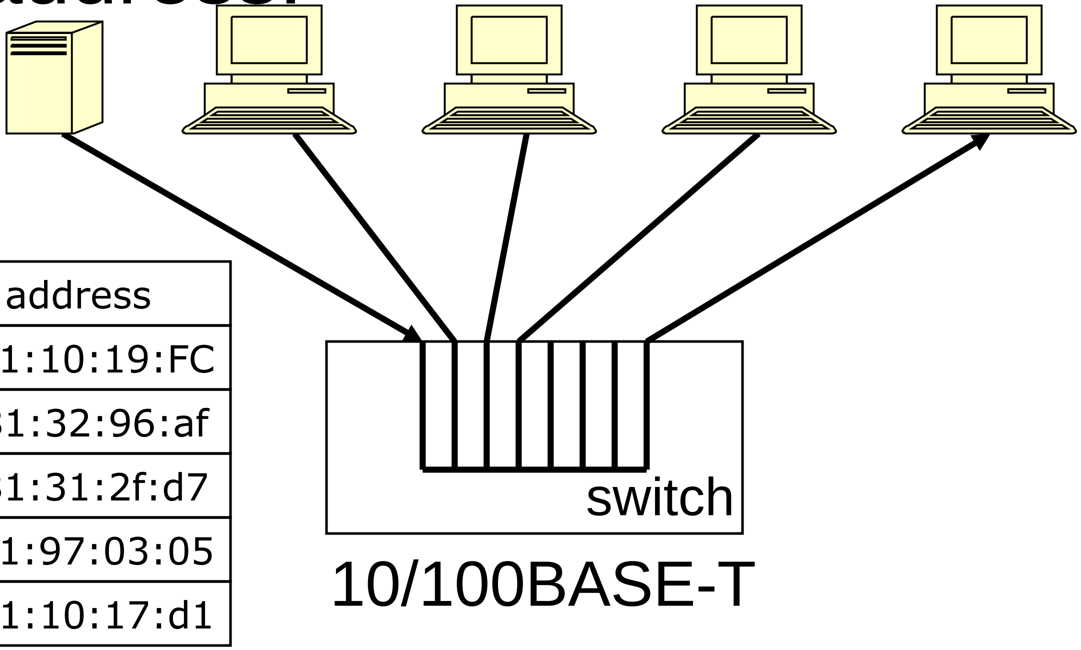
(1) ARP Query
Who has
192.168.0.40?

hub

10/100BASE-T

Switches

- Switches only send data to the intended receiver (an improvement on hubs).
- Builds an index of which device has which MAC address.

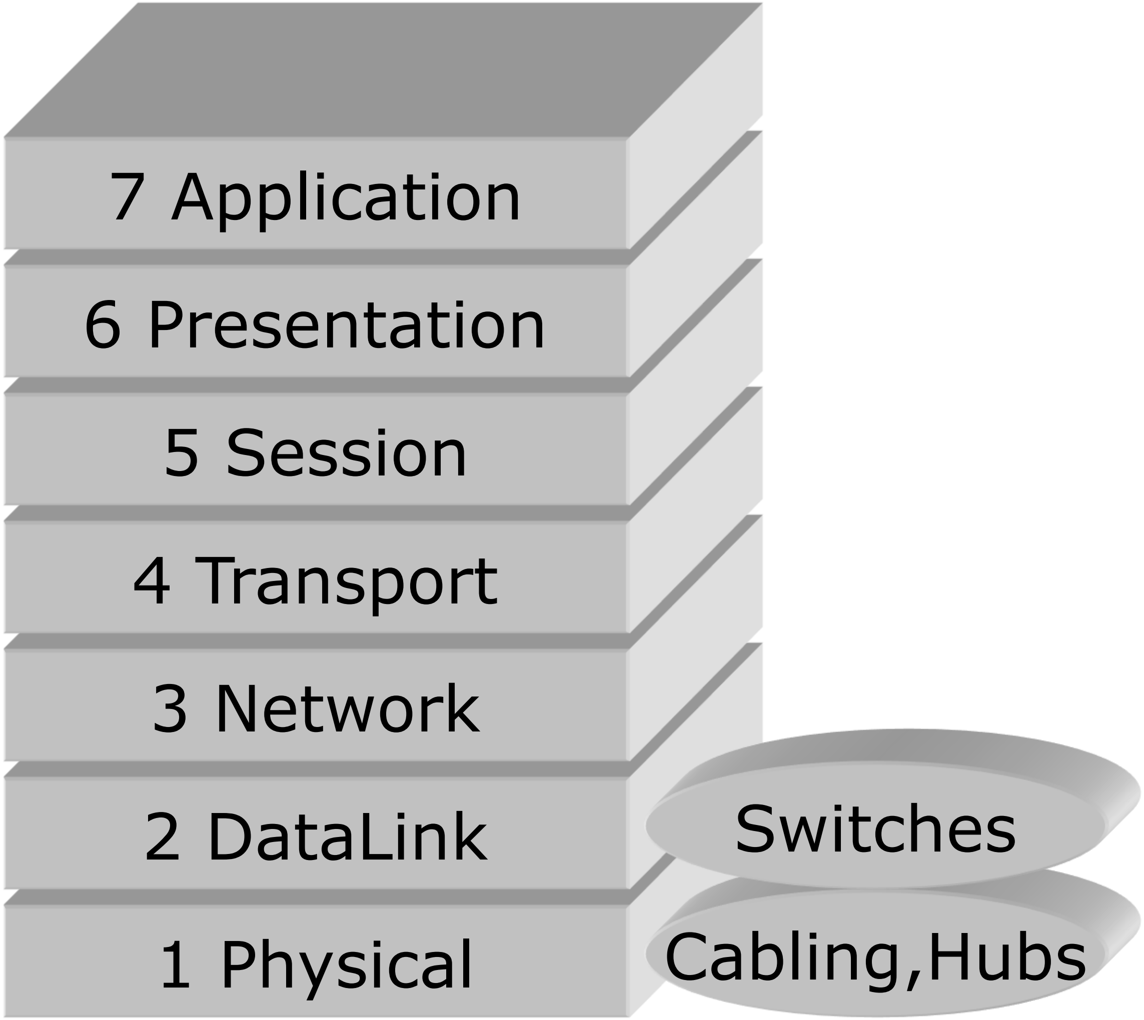


Device	MAC address
1	00:0e:81:10:19:FC
2	00:0e:81:32:96:af
3	00:0e:81:31:2f:d7
4	00:0e:81:97:03:05
8	00:0e:81:10:17:d1

Switch Operation

- When a frame arrives at switch:
  - – Switch looks up destination MAC address in index.
  - – Sends the frame to the device in the index that owns that MAC address.
- Switches are often intelligent:
  - – Traffic monitoring, remotely configurable.
- Switches operate at Layer 2.
- Switches reduce effectiveness of basic sniffing tools
  - – Now a promiscuous NIC only sees traffic intended for it.

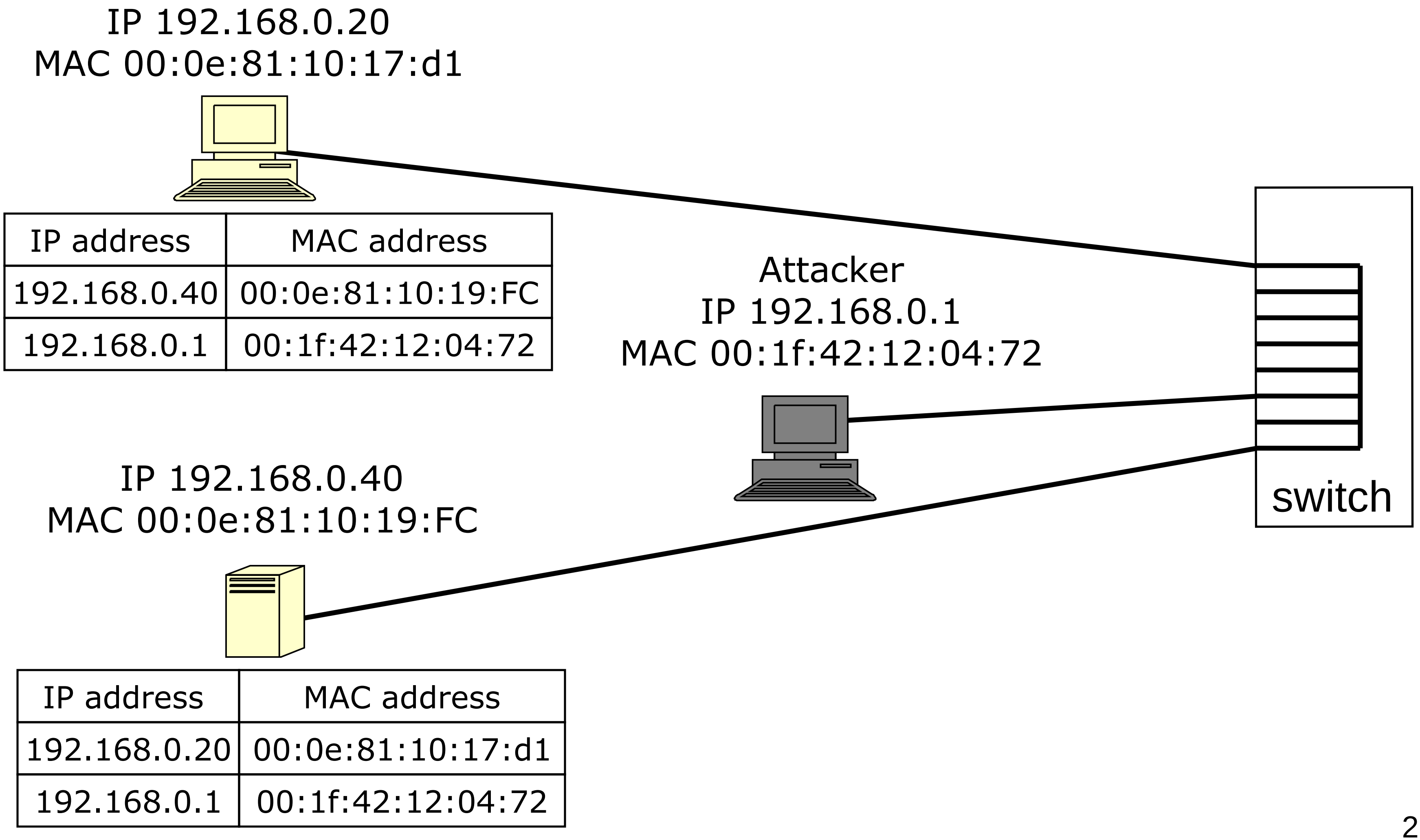
Switches in OSI Protocol Stack



ARP Vulnerability

- Gratuitous ARPs:
  - Sent by legitimate hosts on joining network or changing IP address.
  - Not in response to any ARP request.
  - Associates MAC address and IP address.
- ARP spoofing:
  - Masquerade threat can be realised by issuing gratuitous ARPs.
  - ARP replies have no proof of origin, so a malicious device can claim any MAC address.
  - Enables all fundamental threats!

Before ARP Spoofing



IP 192.168.0.20
MAC 00:0e:81:10:17:d1

IP address	MAC address
192.168.0.40	00:0e:81:10:19:FC
192.168.0.1	00:1f:42:12:04:72

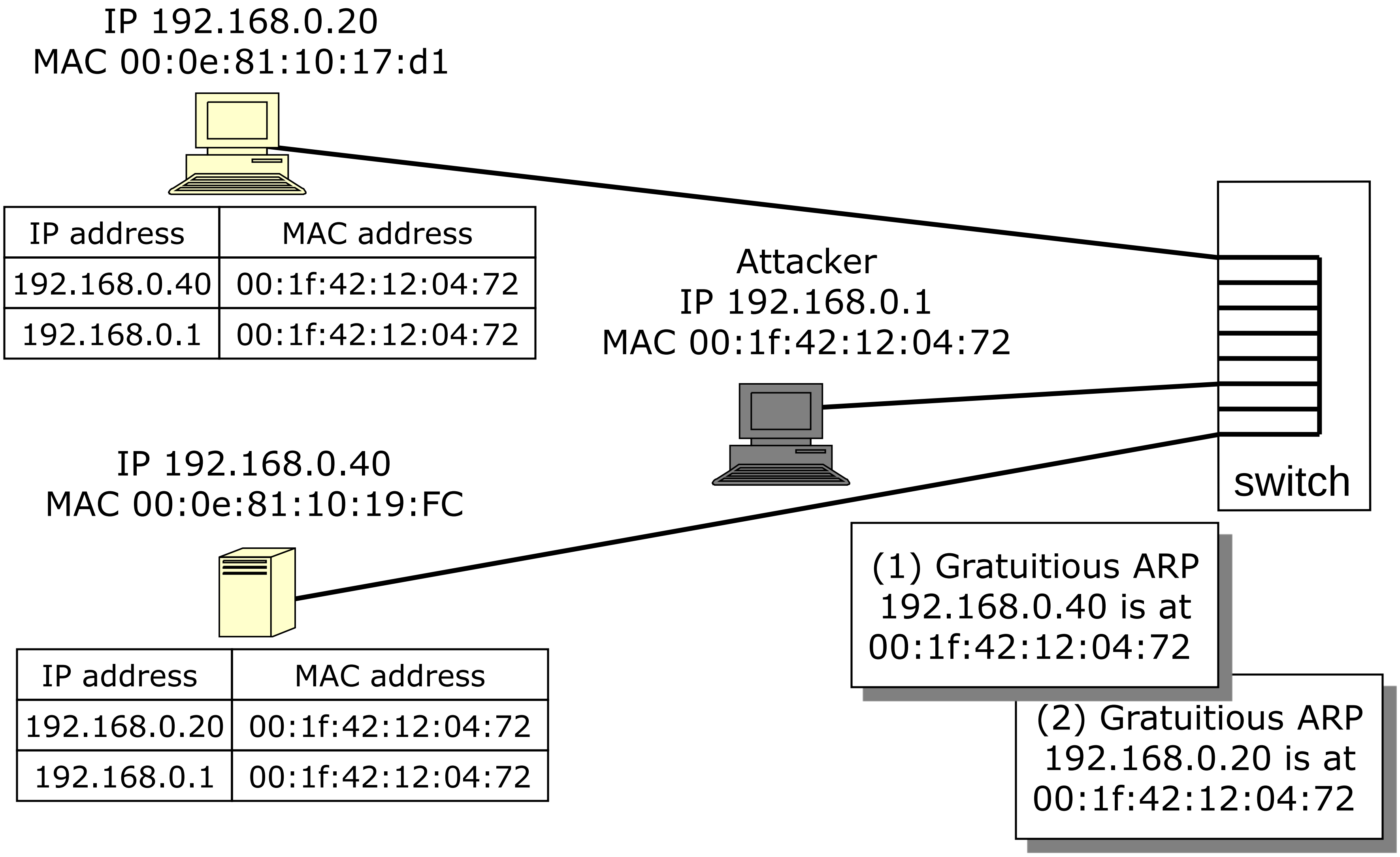
Attacker
IP 192.168.0.1
MAC 00:1f:42:12:04:72

IP 192.168.0.40
MAC 00:0e:81:10:19:FC

IP address	MAC address
192.168.0.20	00:0e:81:10:17:d1
192.168.0.1	00:1f:42:12:04:72

switch

After ARP Spoofing



IP 192.168.0.20
MAC 00:0e:81:10:17:d1

IP address	MAC address
192.168.0.40	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

Attacker
IP 192.168.0.1
MAC 00:1f:42:12:04:72

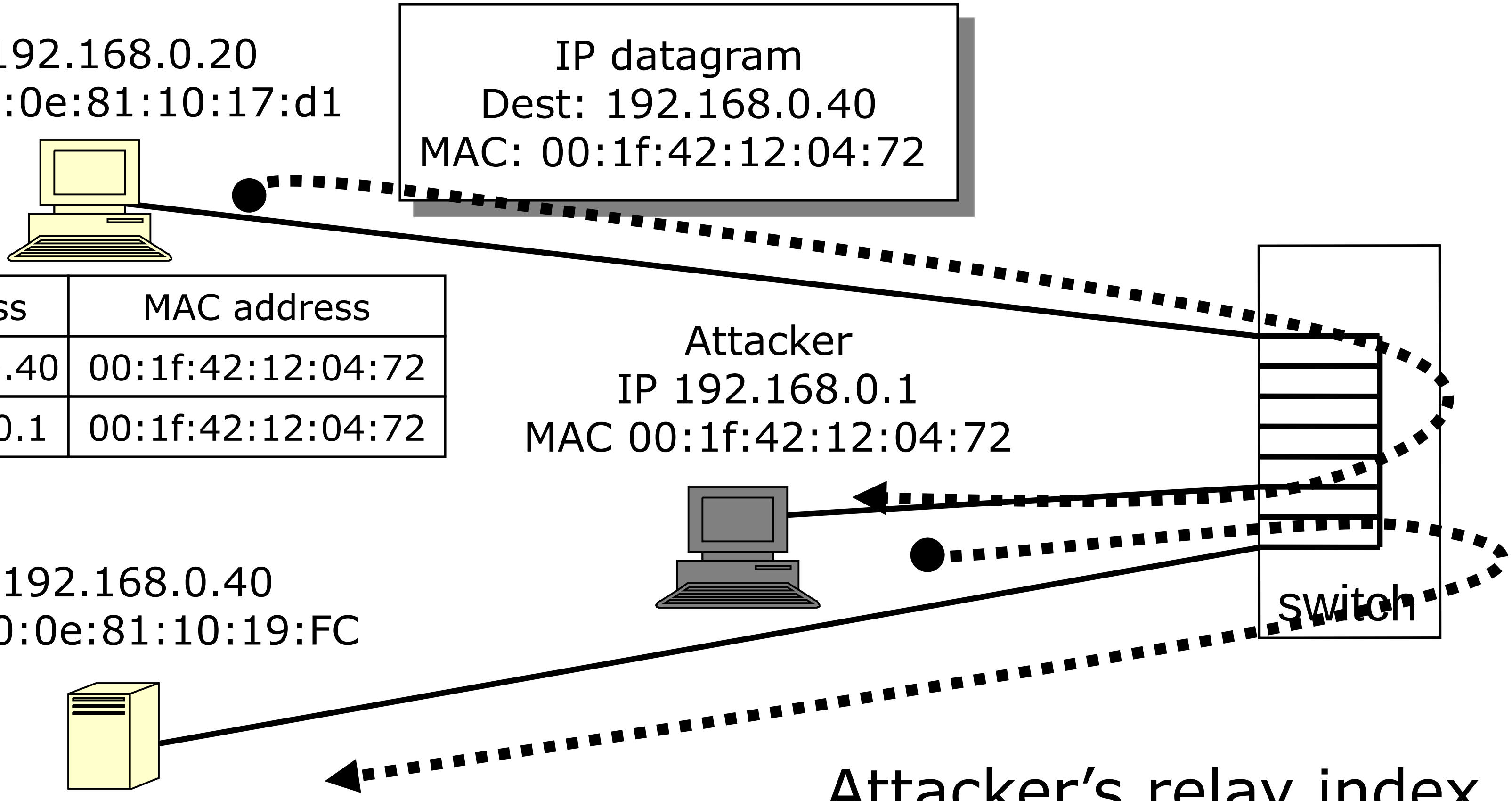
IP 192.168.0.40
MAC 00:0e:81:10:19:FC

IP address	MAC address
192.168.0.20	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

(1) Gratuitious ARP
192.168.0.40 is at
00:1f:42:12:04:72

(2) Gratuitious ARP
192.168.0.20 is at
00:1f:42:12:04:72

Effect of ARP Spoofing



IP 192.168.0.20
MAC 00:0e:81:10:17:d1

IP datagram
Dest: 192.168.0.40
MAC: 00:1f:42:12:04:72

IP address	MAC address
192.168.0.40	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

Attacker
IP 192.168.0.1
MAC 00:1f:42:12:04:72

IP 192.168.0.40
MAC 00:0e:81:10:19:FC

IP address	MAC address
192.168.0.20	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

Attacker’s relay index

IP address	MAC address
192.168.0.40	00:0e:81:10:19:FC
192.168.0.20	00:0e:81:10:17:d1

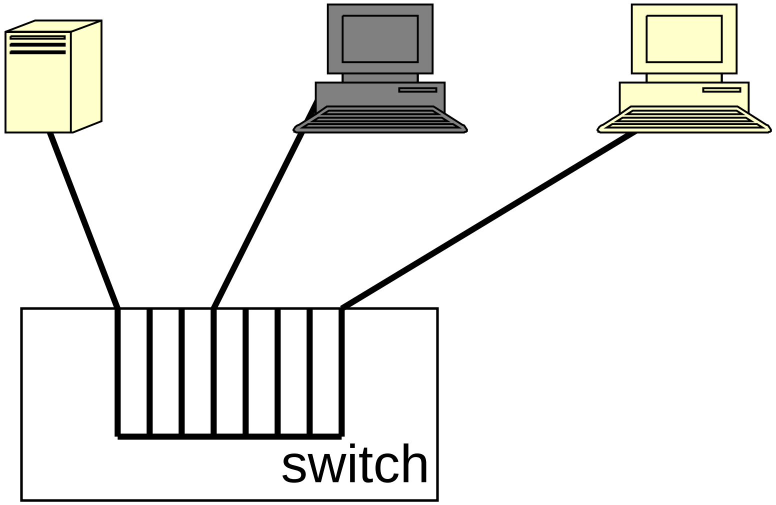
Effect of ARP Spoofing

- Attacker keeps a *relay index*: a table containing the true association between MAC addresses and IP addresses.
- But the two devices at 192.168.0.20 and 192.18.0.40 update their ARP caches with false information.
- All traffic for 192.168.0.20 and 192.168.0.40 gets sent to attacker by layer 2 protocol (Ethernet).
- Attacker can re-route this traffic to the correct devices using his relay index and layer 2 protocol.
- So these devices (and the switch) are oblivious to the attack.
- Attack implemented in dsniff tools.
- So sniffing *is* possible in a switched environment!

Switch Vulnerability

- MAC Flooding
  - Malicious device connected to switch.
  - Sends multiple gratuitous ARPs.
  - Each ARP claims a different MAC address.
  - When index fills:
    - Some switches ignore any new devices attempting to connect.
    - Some switches revert to hub behaviour: all data broadcast and sniffers become effective again.

	Device	MAC address
1	1	00:0e:81:10:19:FC
2	4	00:0e:81:32:96:af
3	4	00:0e:81:32:96:b0
4	4	00:0e:81:32:96:b1
	…	…
9999	4	00:0e:81:32:97:a4



Safeguards

- Physically secure the switch.
  - Prevents threat of illegitimate use.
- Switches should failsafe when flooded.
  - New threat: Denial of Service.
  - Provide notification to network admin.
- Arpwatch
  - Monitors MAC to IP address mappings.
  - Can issue alerts to network admin.
- Use static ARP caches
  - Loss of flexibility in network management.

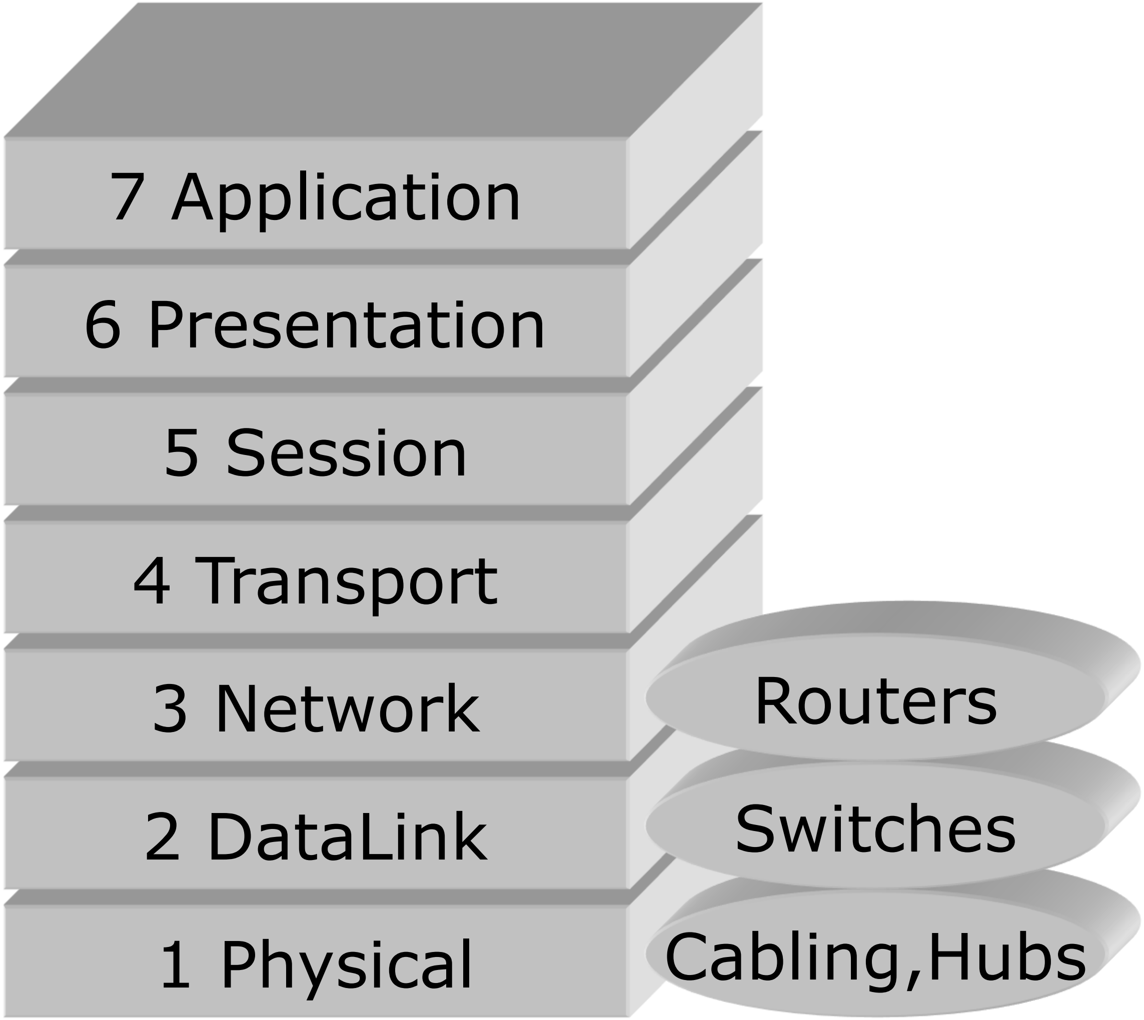
2.3 Routers and Layer 3 Issues

- Routers and routing.
- More on IP addressing.
- Some Layer 3 security issues.

Routers and Routing

- Routers support *indirect* delivery of IP datagrams.
- Employing routing tables.
  - Information about possible destinations and how to reach them.
- Three possible actions for a datagram:
  - Sent directly to destination host.
  - Sent to next router on way to known destination.
  - Sent to default router.
- Routers operate at Layer 3.

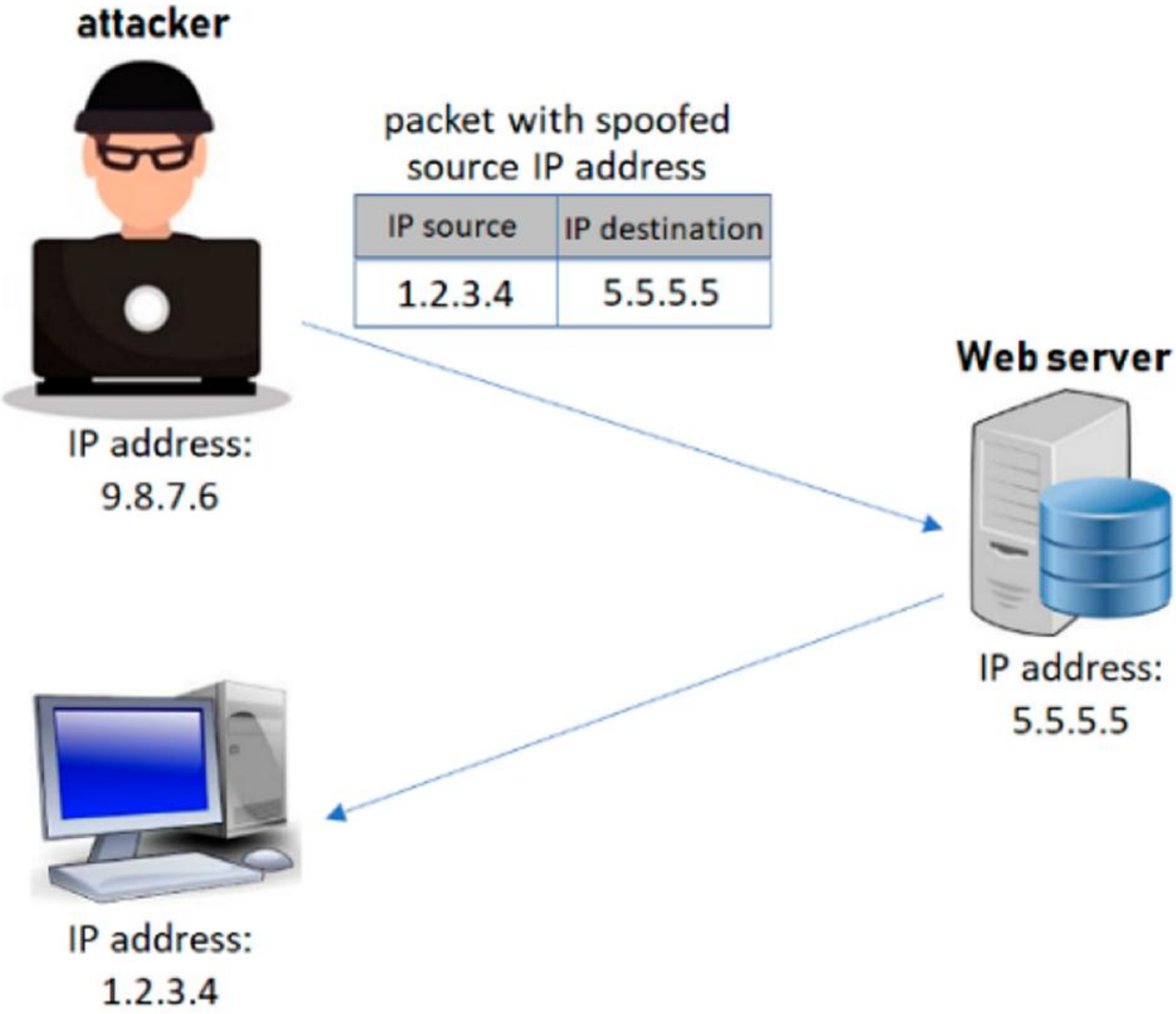
Routers in OSI Protocol Stack



IP Spoofing

- Any station can send packets pretending to be from any IP address
- Replies will be routed to the appropriate subnet
  - Route asymmetry
  - So, attacker might not get replies if spoofing a host on a different subnet
    - For some attacks this is not important
- Analogy
  - Nothing prevents you from physically mailing a letter with an invalid return address, or someone else’s, or your own.
  - Likewise, packets can be inserted in the network with invalid or other IP addresses.

IP Spoofing



IP source	IP destination
1.2.3.4	5.5.5.5

Reflected DoS Attack

- A reflected DoS attack uses IP spoofing to generate fake requests, apparently on behalf of a target, to produce responses from under protected intermediary servers.

- The perpetrator’s goal is to amplify their traffic output by triggering large responses from much smaller requests.

- It may use any IP protocol (ICMP, UDP, TCP), any application or service that replies using these protocols. Common reflected DoS attack methods include:
  - DNS amplification:
  - Smurf attack:
  - NTP amplification:.

IP spoofing Safeguards

- Ingress filtering
  - Forbid inbound broadcasts from the internet into your networks
  - Forbid inbound packets from non-routable networks
- Egress filtering
  - Prevent stations in networks you control from spoofing IPs from other networks by dropping their outbound packets
  - Drop outbound broadcasts

Use Log files to monitor any unlawful activities on your network.

Routing Information Threats

- Security of routing updates.
  - Attacker may be able to corrupt routing tables on routers by sending false updates.
  - Denial of Service threat.
- What security is applied to protect remote administration of routers?
  - Attacker may be able to reconfigure or take control of remote router and change its behaviour.
  - Eg advertise attractive routes to other routers and so bring interesting traffic its way.

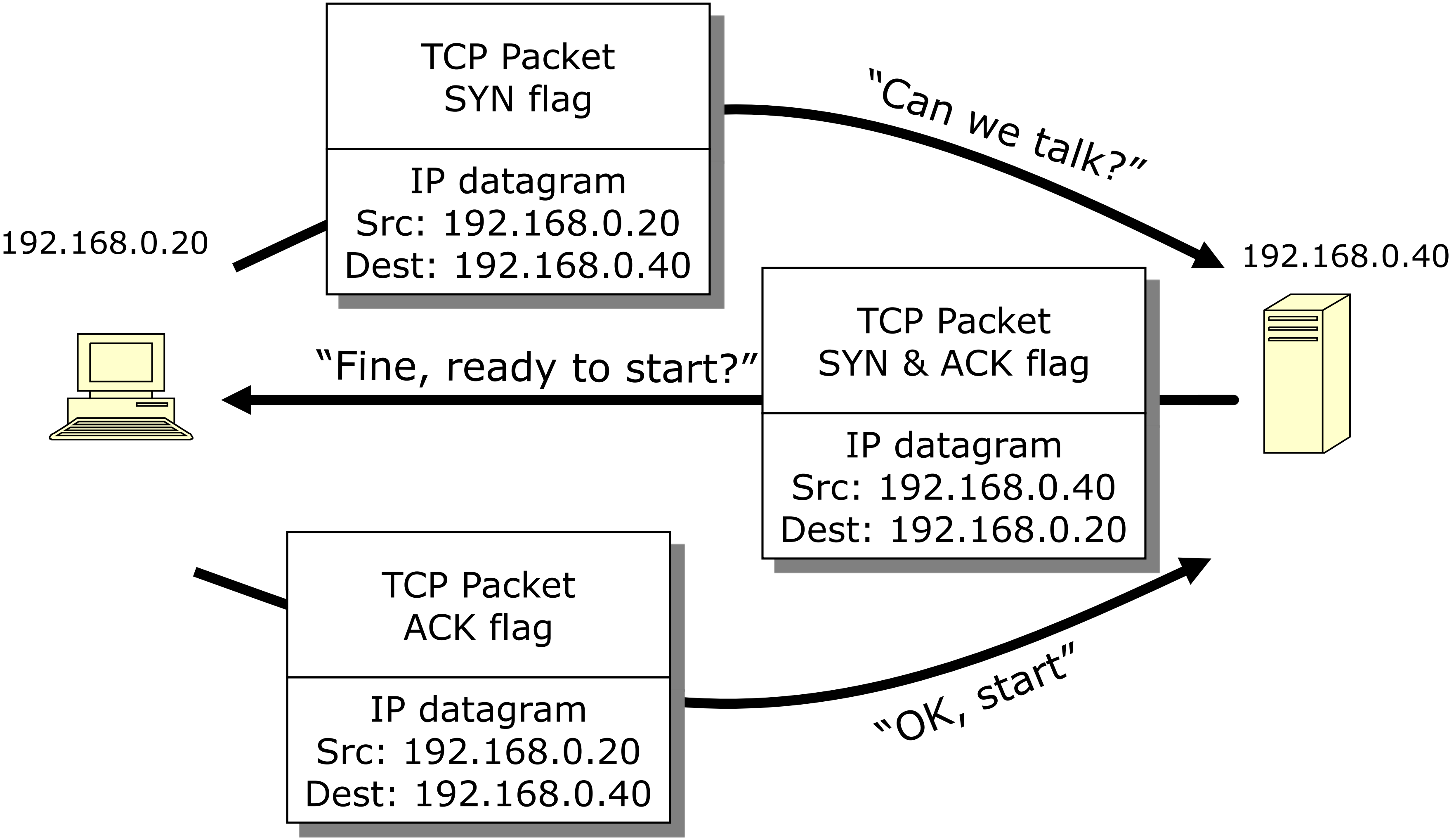
2.4 TCP, UDP, ICMP and Layer 4 issues

- TCP and Denial of Service (DoS) Attacks
- UDP flooding attack
- ICMP security vulnerabilities
- Securing against Denial of Service attacks

TCP and Denial of Service Attacks

- Each TCP connection begins with three packets:
  - A SYN packet from sender to receiver.
    - “Can we talk?”
  - An SYN/ACK packet from receiver to sender.
    - “Fine – ready to start?”
  - An ACK packet from sender to receiver.
    - “OK, start”
- The packet type is indicated by a flag in the packet header.

TCP Handshaking



192.168.0.20

192.168.0.40

TCP Packet
SYN flag

IP datagram
Src: 192.168.0.20
Dest: 192.168.0.40

"Can we talk?"

TCP Packet
SYN & ACK flag

IP datagram
Src: 192.168.0.40
Dest: 192.168.0.20

“Fine, ready to start?”

TCP Packet
ACK flag

IP datagram
Src: 192.168.0.20
Dest: 192.168.0.40

“OK, start"

Tracking TCP handshakes

- The destination host has to track which machines it has sent a “SYN+ACK” to
- Keeps a list of TCP SYN packets that have had a SYN+ACK returned.
- When ACK is received, packet removed from list as connection is open.

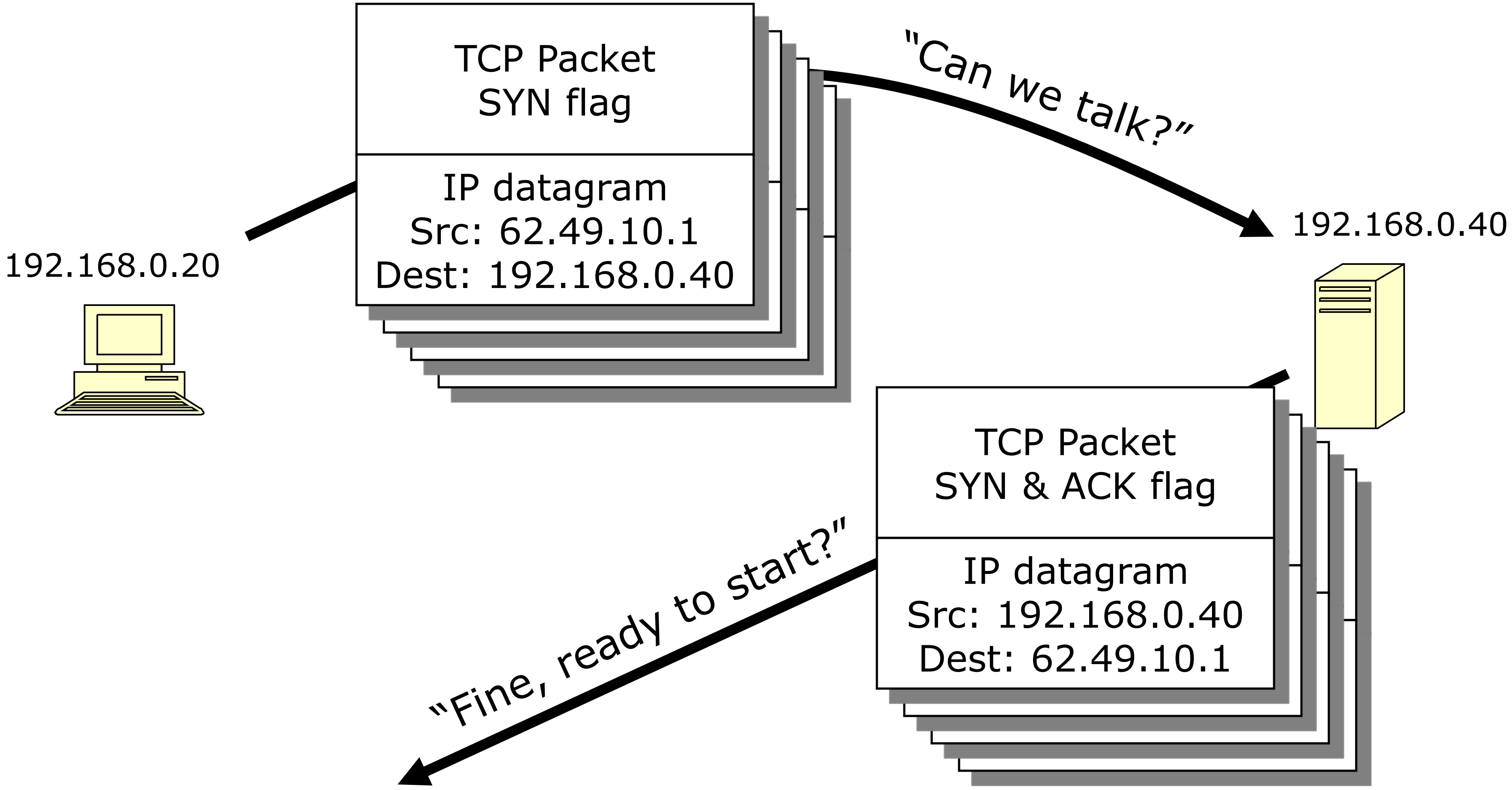
TCP Denial Of Service

- What if the sender doesn’t answer with an ACK?
  - A SYN packet from sender to receiver.
    - “Can we talk?”
  - An SYN/ACK packet from receiver to sender.
    - “Fine – ready to start?”
  - …………………..nothing……………..……
- If the sender sends 100 SYN packets per second
  - Eventually receiver runs out of memory to track the SYN+ACK replies.
  - SYN flooding.

TCP Denial Of Service + IP Spoofing

- A host can place any IP address in the source address of an IP datagram.
- Disadvantage: Any reply packet will return to the wrong place.
- Advantage (to an attacker): No-one knows who sent the packet.
- If the attacker sends 100 SYN packets per second with spoofed source addresses….

TCP Denial of Service



… the destination host will soon be unable to accept new connections from legitimate senders.

SYN Flood Safeguards

SYN cookies: using cryptographic hashing,

- the server sends its SYN-ACK response with a sequence number.
- the ACK packet must include the hash
- The server verifies the ACK, and only then allocates memory for the connection.

RST cookies: for the first request from a given client,

- the server intentionally sends an invalid SYN-ACK.
- This should result in the client generating an RST packet
- If this is received, the server knows the request is legitimate, and accepts subsequent incoming connections from it.

Stack tweaking: administrators can tweak TCP stacks to mitigate the effect of SYN floods

UDP Flooding attack

- A UDP flood is a form of volumetric DoS attack where the attacker targets and overwhelms random ports on the host with IP packets containing UDP packets.
- Each time a new UDP packet is received by the server, resources are used to process the request.
- The first step in this process involves the server determining if any programs are running at the specified port. If no programs at that port are receiving packets, then the server issues an ICMP packet (“Destination Unreachable”) to notify the sender that the destination could not be reached.
- The cumulative effect of being bombarded by such a flood is that the system becomes inundated and unresponsive to legitimate traffic.
- The attacker may also spoof the IP address of the packets.

UDP Flooding attack safeguard

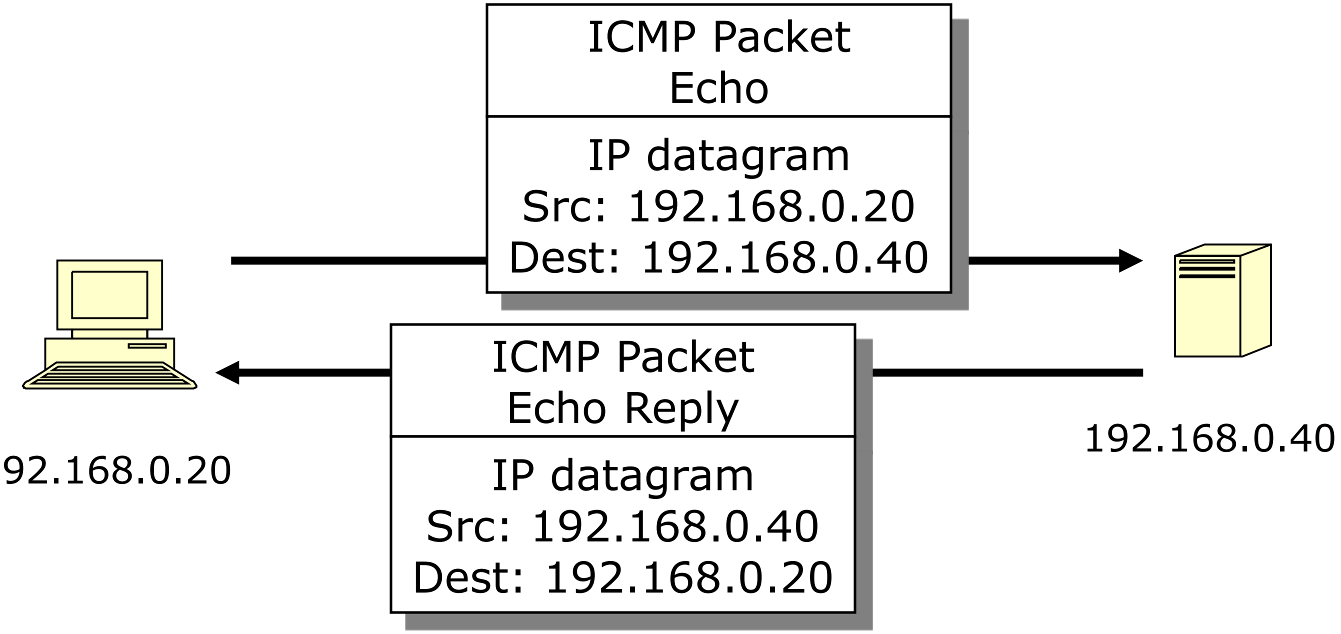
- What make this type of attack dangerous is that: There are no internal protections that can limit the rate of a UDP flood. As a result, UDP flood DOS attacks are exceptionally dangerous because they can be executed with a limited amount of resources.

- Most operating systems attempt to limit the response rate of ICMP packets with the goal of stopping DoS attacks.

- The downside to this form of mitigation is that it also filters out legitimate packets.

ICMP

- ICMP = Internet Control Message Protocol.
- Layer 4 protocol (like TCP) carried over IP, mandatory part of IP implementations.
- Carries IP error and control messages.
- ICMP Echo Request: test route to a particular host.
- Live host should reply with ICMP Echo Reply packet.



ICMP Security vulnerabilities

- Although ICMP is a handy tool for network management and fault diagnostic, network attacks can exploit this process, creating means of disruption, which include but are not limited to:
  - Ping sweep
  - Ping flood
  - ICMP tunneling
  - Forged ICMP redirects

Securing against DoS attacks

- It is very difficult to defend against a sophisticated DoS attack launched by a determined adversary.

- The more difficult is that attacks are perpetrated by means of using several source devices, i.e. requests made to target services come from a large number of different devices which may even be geographically separated. This type of attack is called distributed denial-of-service attack (DDoS attack)

- DDoS is usually carried out with the help of botnets.

- A botnet, in simple terms, is a network of infected computers that are controlled as a single entity by a malicious actor. That means the actor can have all the computers in the infected network carry out the same instructions at the same time.

How to Mitigate DoS Attacks (1)

Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services.

Attack Detection: Analyzing incoming traffic and determining whether or not it is legitimate is the first step in keeping your service available and responsive. Early detection of an attack dramatically increases the efficacy of any mitigation strategy.

IP Whitelisting/Blacklisting: The simplest defense against a DoS attack is either whitelisting only legitimate IP addresses or blocking ones from known attackers.

How to Mitigate DoS Attacks (2)

- **Rate Limiting:** Rate limiting is the practice of limiting the amount of traffic available to a specific NIC. It can be done at the hardware or software level to mitigate the chances of falling victim to a DoS attack.

- **Upstream Filtering:** There are many providers of "Mitigation Centers" that will filter the incoming network traffic.
-
- For example Amazon Shield and Cloudflare both offer products that allow for protection against DoS and DDoS attacks by checking incoming packet IPs against known attackers and botnets and attempt to only forward legitimate traffic.