TÉCNICO LISBOA

Network Vulnerabilities in OSI Layers 1 to 3

Segurança Informática em Redes e Sistemas
2024/25

David R. Matos, Ricardo Chaves

Ack: Miguel Pardal, Carlos Ribeiro,
André Zúquete, Miguel P. Correia

Roadmap

- Network models
  - OSI and Internet
  - Address resolution
- Network vulnerabilities
  - Physical layer
  - Data link layer
  - Network layer

Roadmap

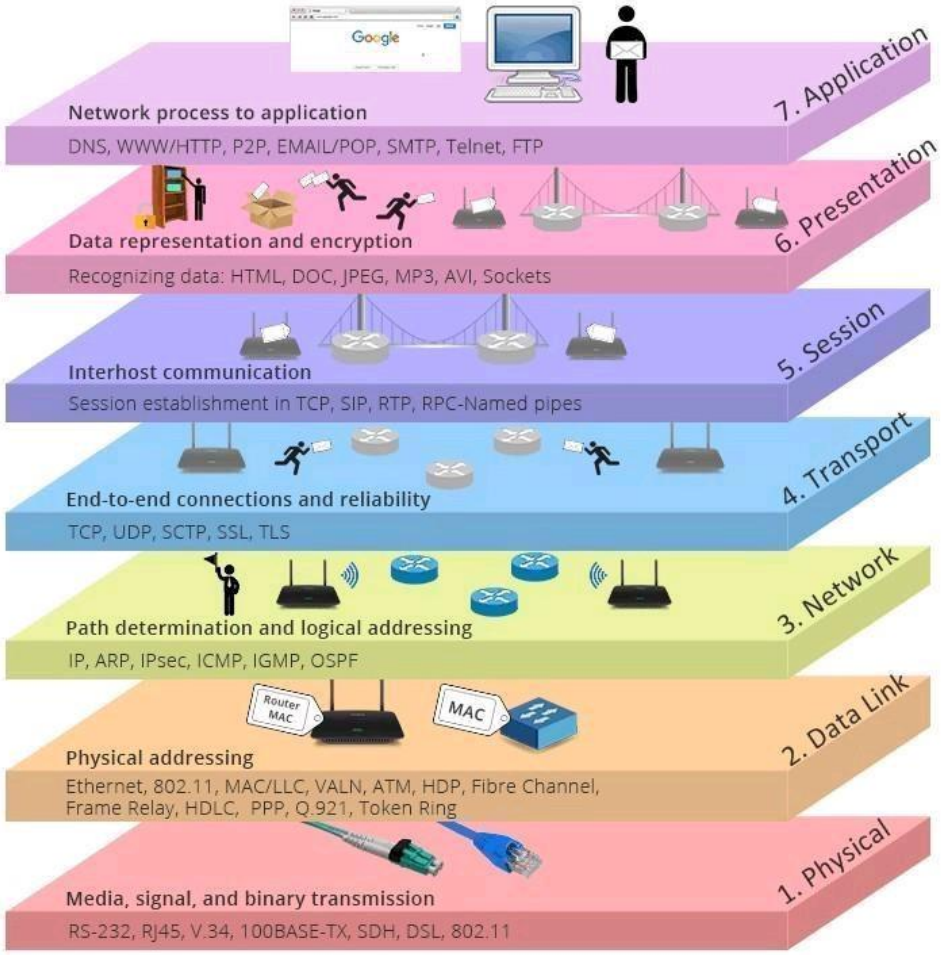
- **Network models**
  - **OSI and Internet**
  - Address resolution
- Network vulnerabilities
  - Physical layer
  - Data link layer
  - Network layer

OSI model

1. Physical (Ethernet, FDDI, B8ZS, V.35, V.24, RJ45)
2. Data Link (PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay)
3. Network (IP, IPX, AppleTalk DDP)
4. Transport (TCP, UDP, SPX)
5. Session (NFS, NetBios names, RPC, SQL)
6. Presentation (ASCII, EBCDIC, JPEG, MPEG, GIF, PICT, TIFF)
7. Application (HTTP, FTP, SNMP, NFS, Telnet)

Open **S**ystem **I**nterconnection

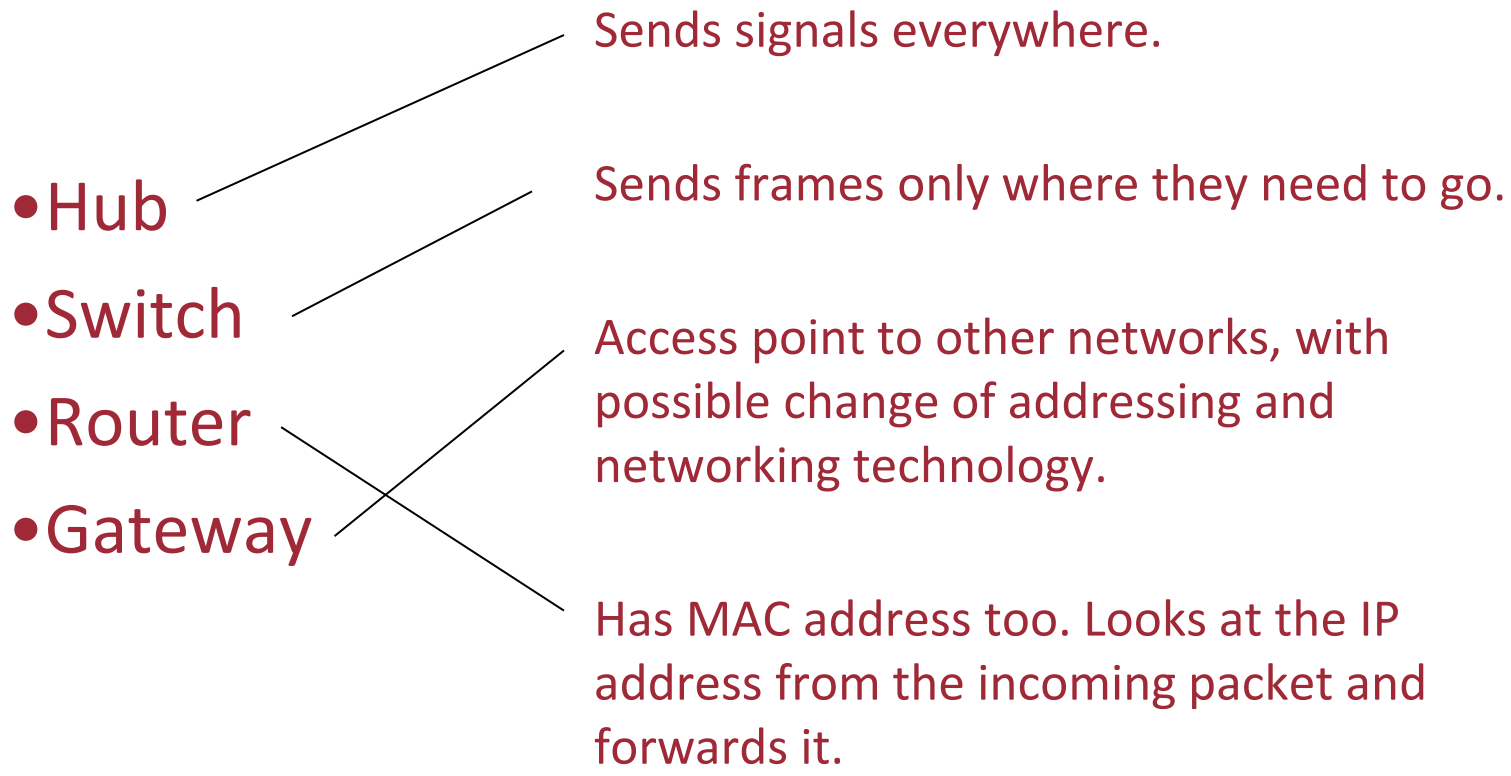
OSI model layer 7



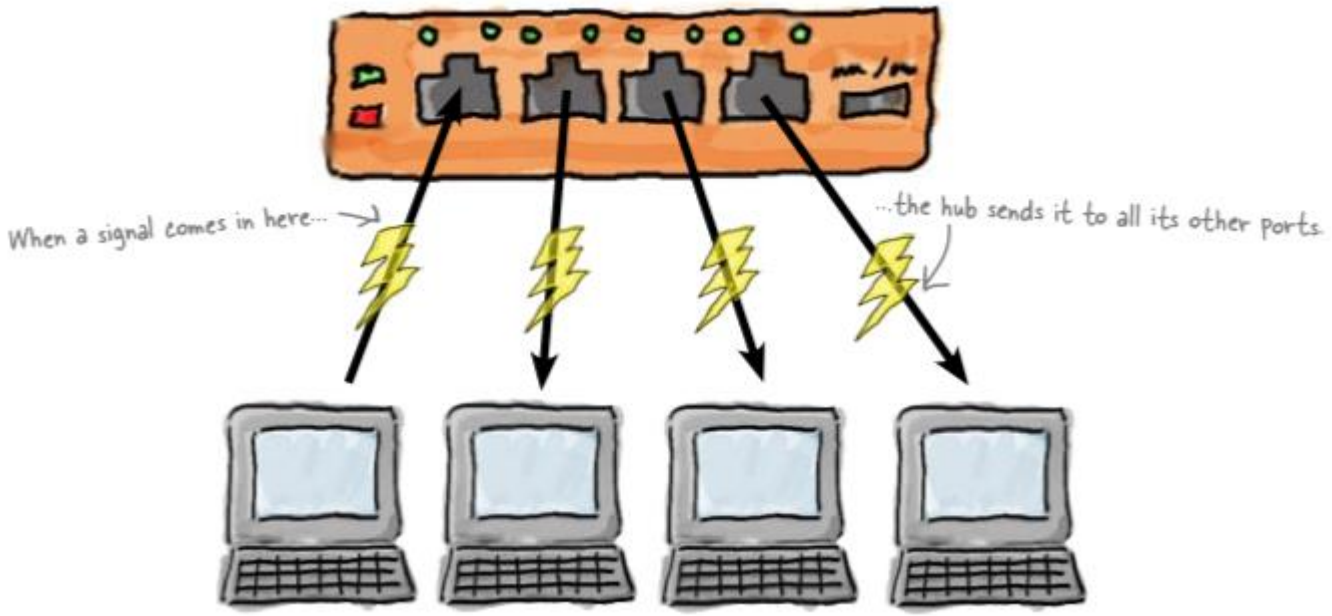
Open **S**ystem **I**nterconnection

Hubs vs Switches vs Routers vs Gateways

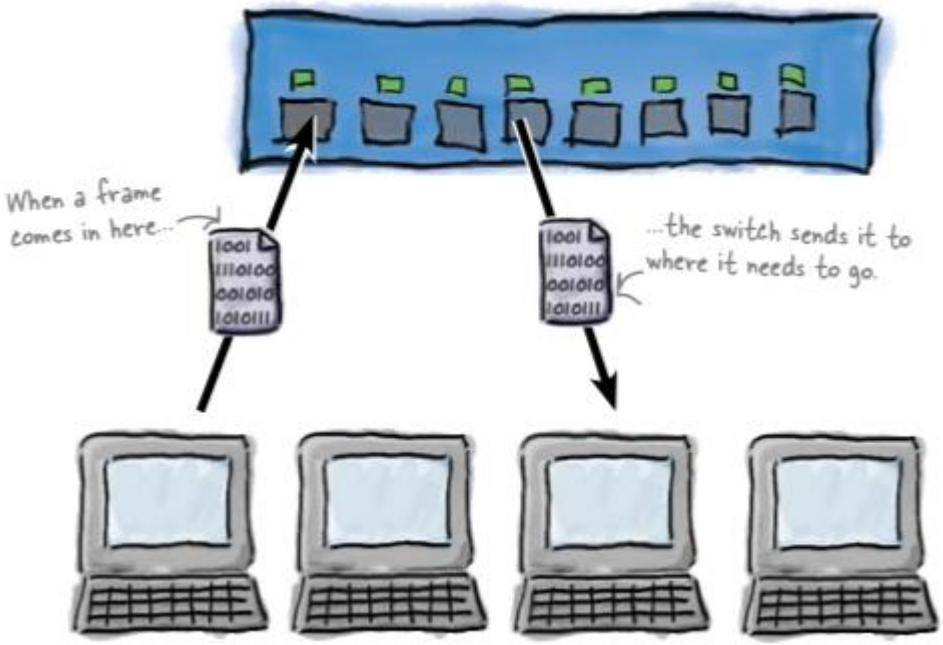
- The network is not just computers and servers
  - There are also network devices such as hubs, switches, routers, and gateways



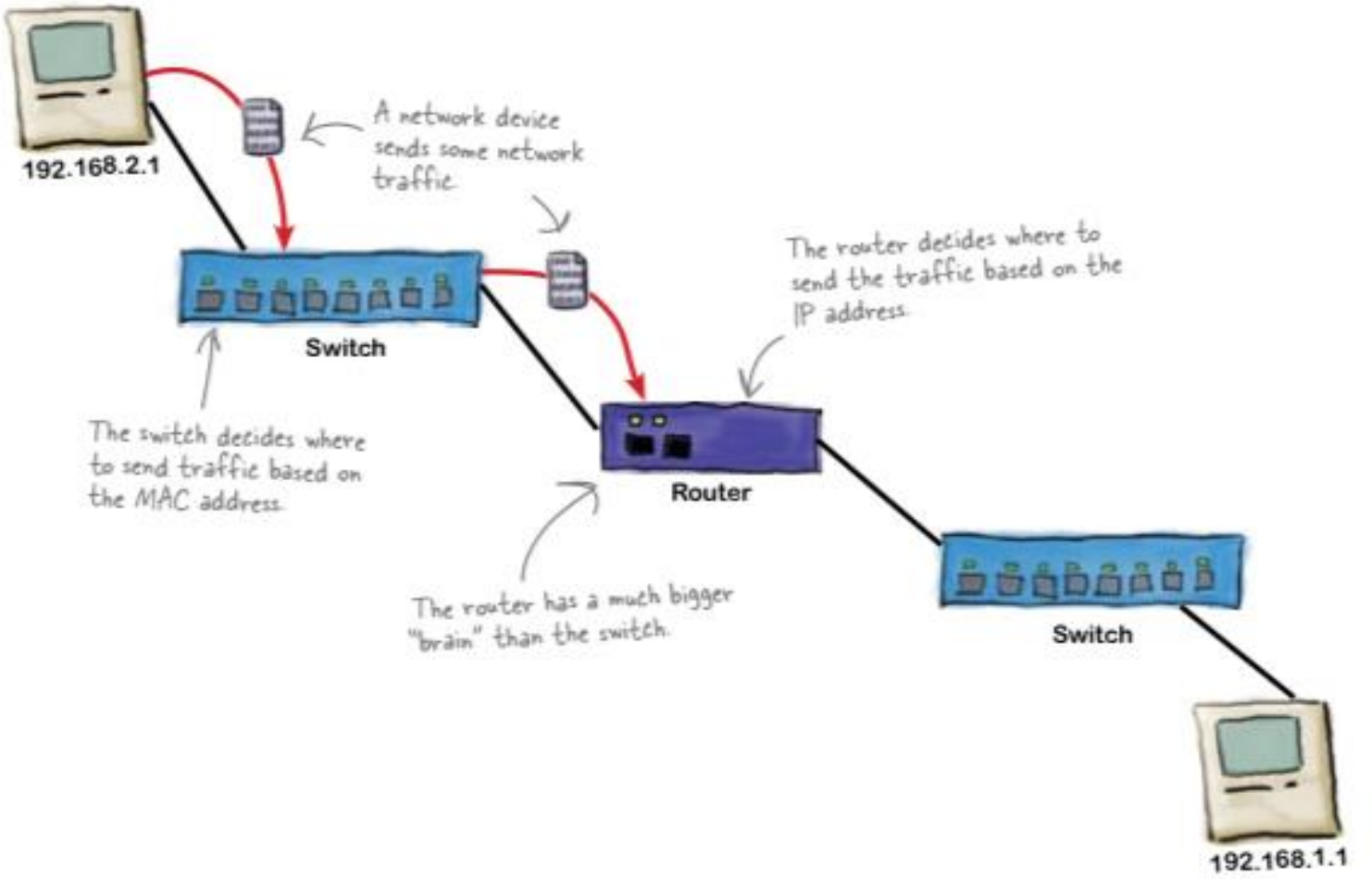
Hubs


When a signal comes in here...
...the hub sends it to all its other ports.

Switches


When a frame comes in here...
...the switch sends it to where it needs to go.

Routers

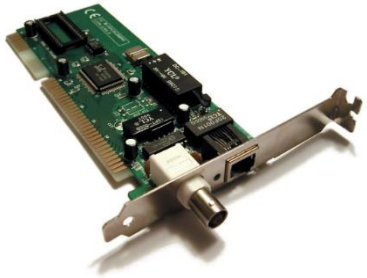

192.168.2.1
A network device sends some network traffic
Switch
The switch decides where to send traffic based on the MAC address.
The router decides where to send the traffic based on the IP address.
Router
The router has a much bigger "brain" than the switch.
Switch
192.168.1.1

Roadmap

- **Network models**
  - OSI and Internet
  - **Address resolution**
- Network vulnerabilities
  - Physical layer
  - Data link layer
  - Network layer

Network Addresses

- MAC address (layer 2)
  - MAC = Medium Access Control
  - Address of NIC (Network Interface Card)
  - Unique identifier with 48 bits
    - The first 24 identify the manufacturer



- IP address (layer 3)
  - IP = Internet Protocol ~= Inter-connect Net-works Protocol
  - IPv4 address has 32 bits
    - Usually represented as 4 separate decimal numbers
    - 131.159.15.24
  - IPv6 address has 128 bits
    - Represented as 8 groups of 4 hex digits (16 bits)
    - 2001:4ca0:2001:0013:0250:56ff:feba:37ac

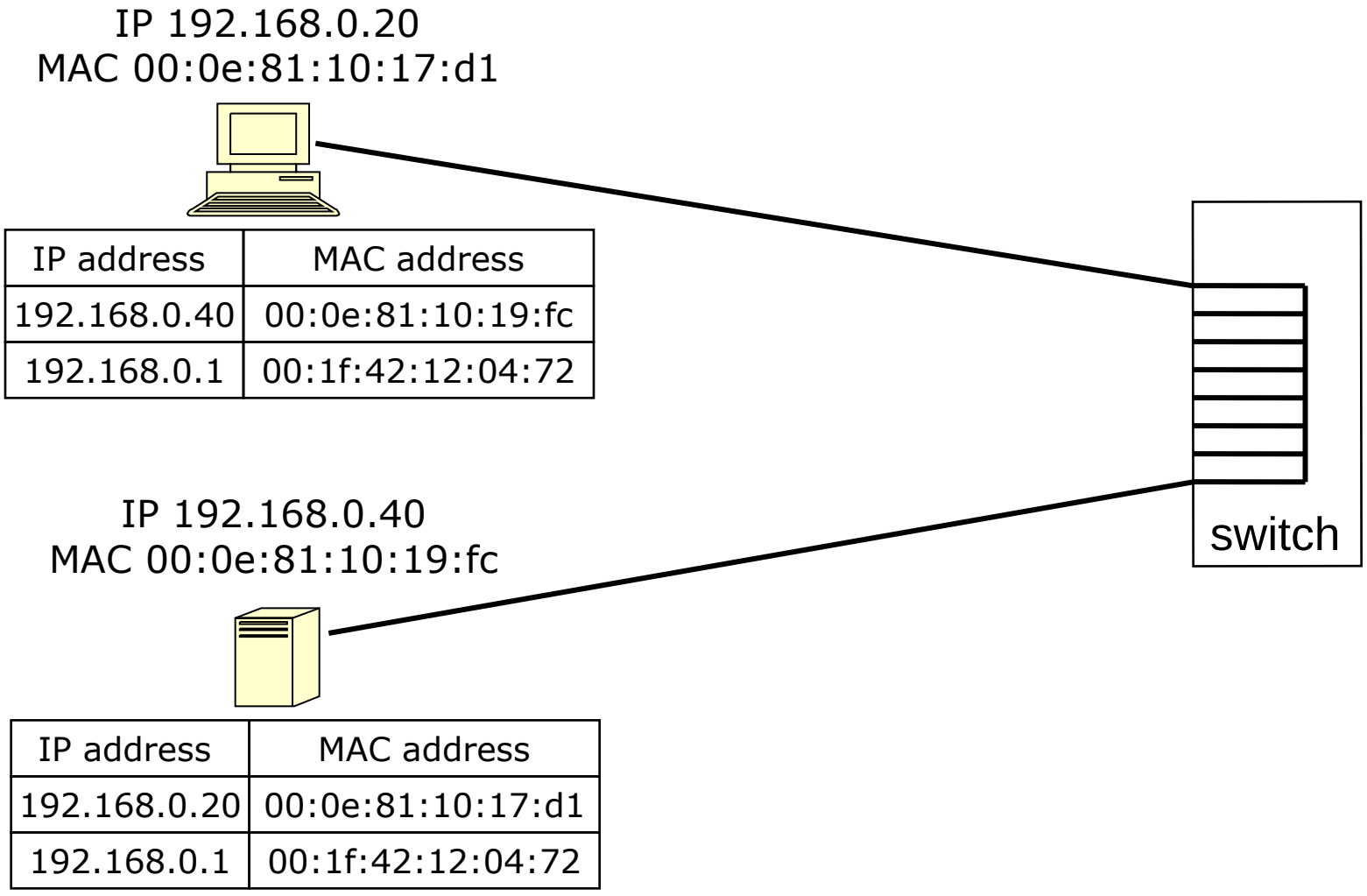
IP address

- IP addresses identify the network and the machine
- Example: 192.168.0.22 address:
  - In CIDR notation: 192.168.0.22 / 24
  - First 24 bits of IP address are significant for network routing
  - Network mask is 255.255.255.0
    - 192.168.0.* identifies the network
    - *.*.*.22 identifies the machine

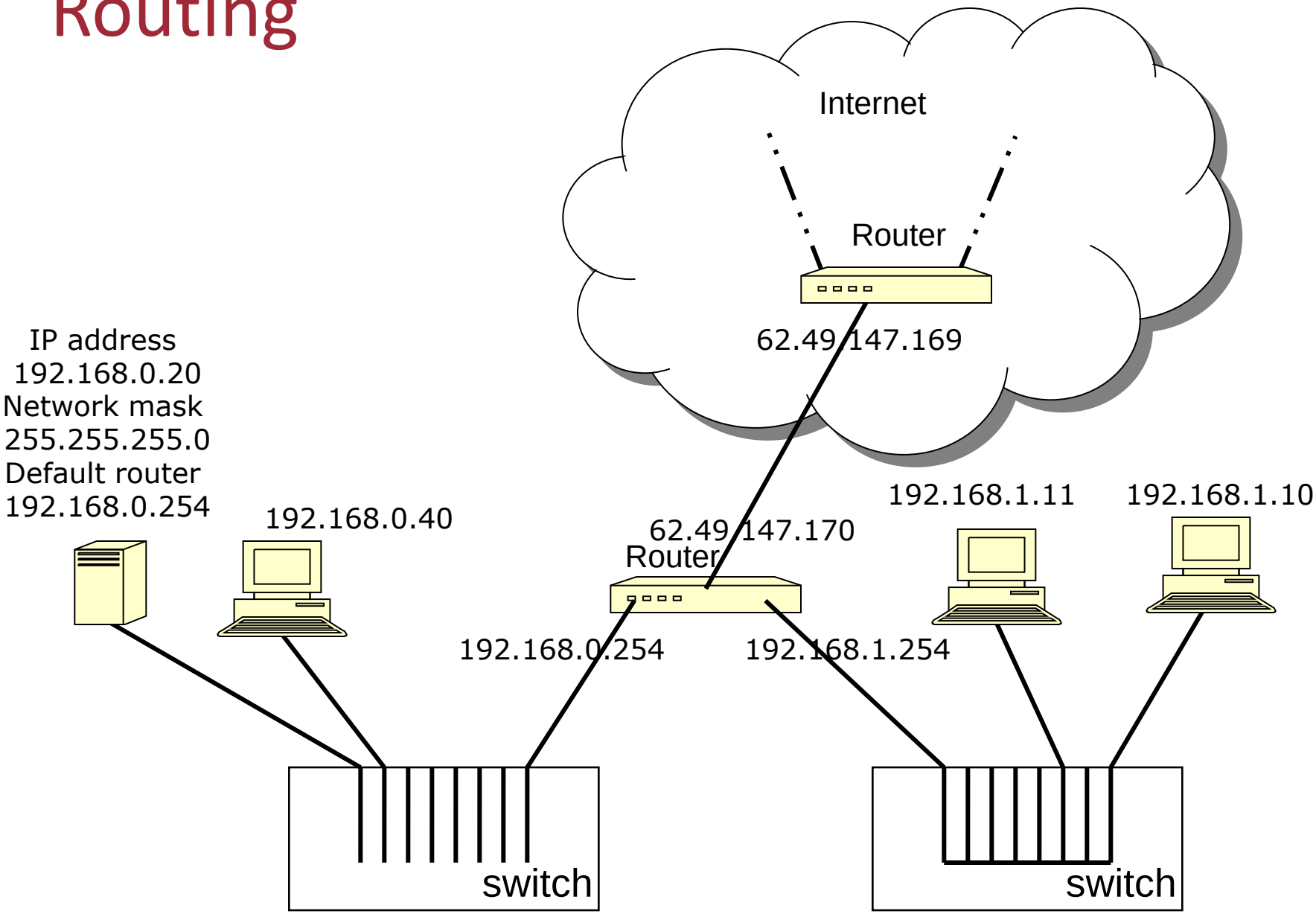
Address Resolution: MAC to IP

- Address Resolution Protocol (ARP)
  - Layer 3 Protocol (Network)
  - Translates an IP address into a MAC address
- ARP query
  - Who has the IP 192.168.0.40? Answer to 192.168.0.20
- ARP reply
  - 192.168.0.40 is at 00:0e:81:10:19:FC
- ARP caches:
  - Stores previous answers
  - When the answers are too old, they are removed

ARP tables

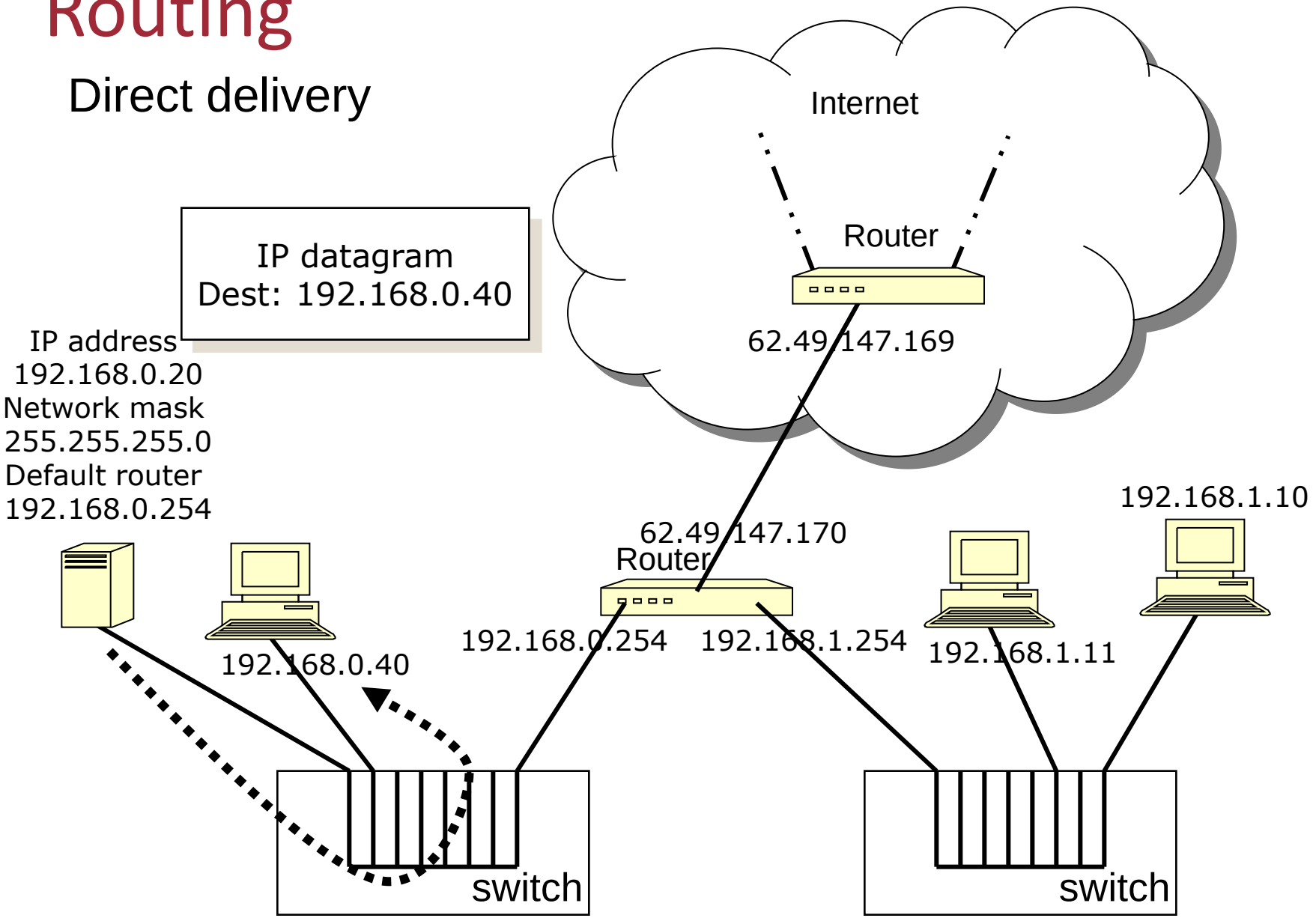

IP 192.168.0.20
MAC 00:0e:81:10:17:d1
IP address
MAC address
192.168.0.40
00:0e:81:10:19:fc
192.168.0.1
00:1f:42:12:04:72
switch
IP 192.168.0.40
MAC 00:0e:81:10:19:fc
IP address
MAC address
192.168.0.20
00:0e:81:10:17:d1
192.168.0.1
00:1f:42:12:04:72

Routing


Internet
Router
62.49.147.169
IP address
192.168.0.20
Network mask
255.255.255.0
Default router
192.168.0.254
192.168.0.40
62.49.147.170
Router
192.168.1.11
192.168.1.10
192.168.0.254
192.168.1.254
switch
switch

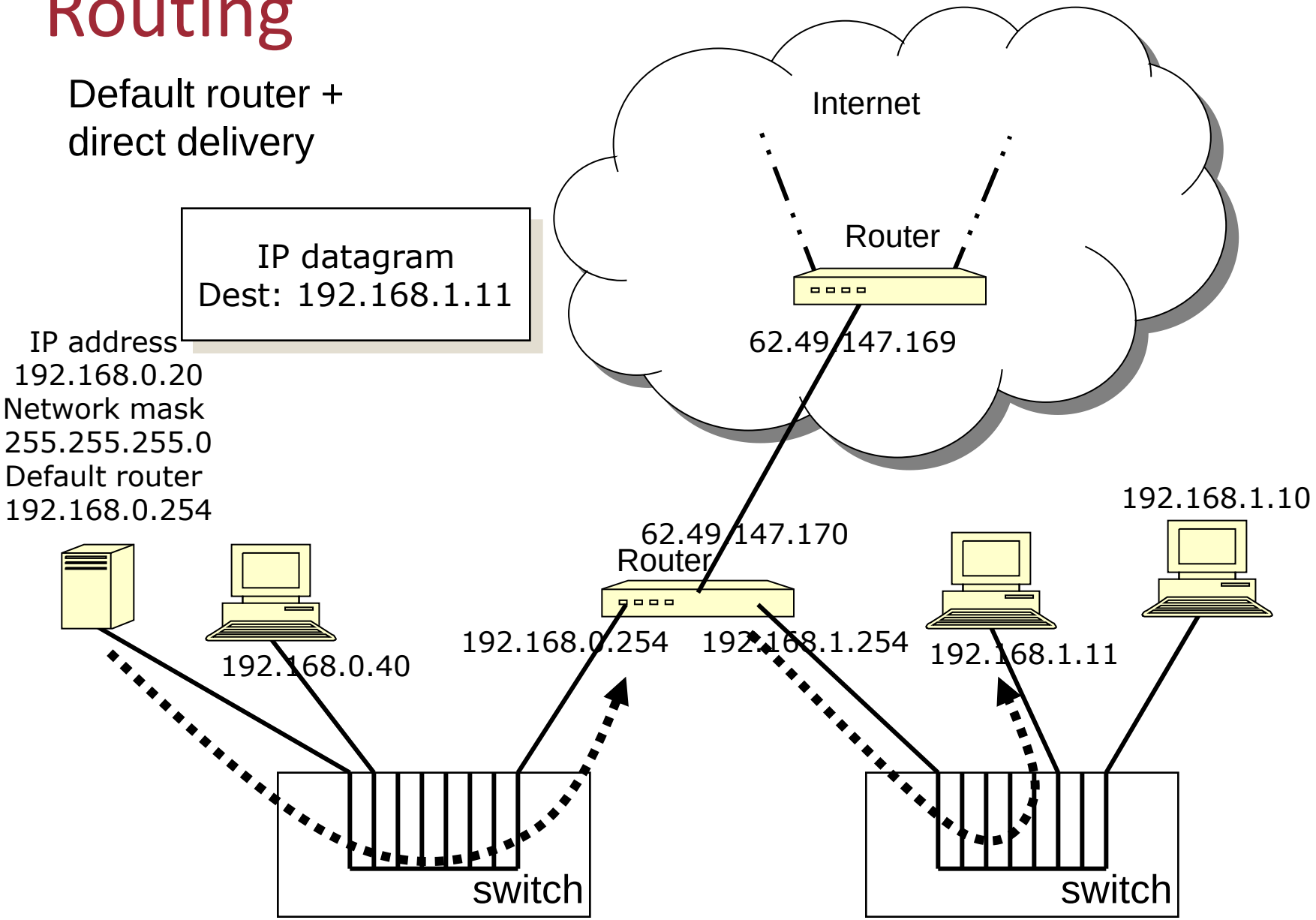
Routing

Direct delivery



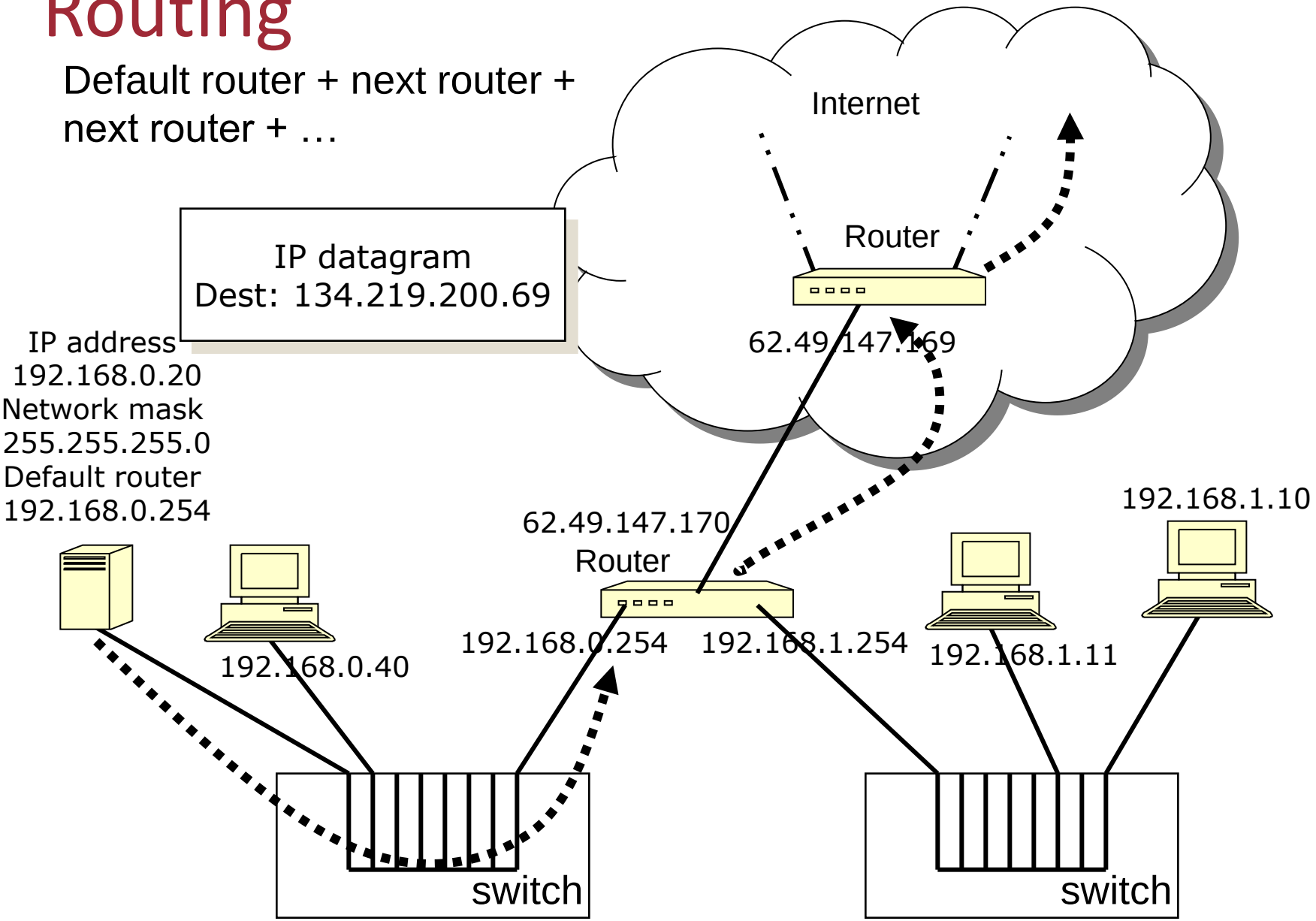
Routing

Default router +
direct delivery



Routing

Default router + next router + next router + …



Private Addresses

- Some network ranges were reserved for private addressing (IETF RFC 1918):
  - `10.0.0.0` to `10.255.255.255` (1 network, 2^{24} machines)
  - `172.16.0.0` to `172.31.255.255` (16 networks, 2^{16} machines each)
  - `192.168.0.0` to `192.168.255.255` (256 network, 2^{8} machines each)
- Packets with these addresses (origin or destination) should never be sent outside the network itself
  - An attempt to solve the lack of IP addresses
  - Adds security because machines cannot be addressed from outside the network
- In the previous example, the router has:
  - one public IP address: `62.49.147.170` and
  - two private addresses: `192.168.0.254` and `192.168.1.254`

Roadmap

- Network models
  - OSI and Internet
  - Address resolution
- **Network vulnerabilities**
  - **Physical layer**
  - Data link layer
  - Network layer

(Layer 1) Physical Layer: Hubs

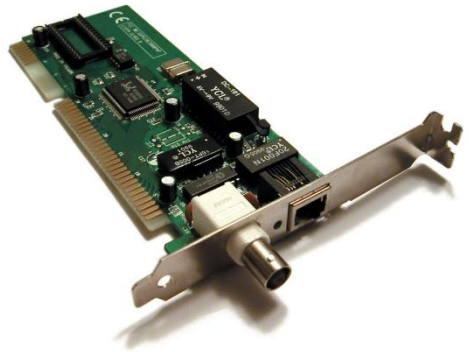
- Topics:
  - Behavior
  - Problems
  - Sniffers and anti-sniffers

Hub behavior

- Information broadcast on a shared medium
  - Threats: Information Leakage (sniffers)
- Easy to install more devices
  - But anyone can connect
  - Even if the Hub is physically secure

Sniffers

- Usually, network adapters operate in a non-promiscuous mode
  - Network adaptors only listen to what is sent to their MAC
- Sniffers work in a promiscuous mode
  - Read all frames, with any MAC
- Some sniffer tools:
  - Tcpdump
  - Wireshark (Ethereal)
  - Snort



Identifying sniffers

- AntiSniff tool
  - Latency Method
    - Send high volume of packets to target
    - Compare time needed to answer to 1 packet *vs* N packets
  - DNS Method
    - Detect large volume of reverse lookup DNS queries from Tcpdump, Wireshark running at sniffer machine
  - OS-specific Method
    - Sends packets to target system which certain operating systems respond to
      - Example: Windows in promiscuous mode always responds to MAC = ff:00:00:00:00:00

Identifying sniffers using ARP

- ARP method
  - Machines cache ARPs
  - Send a non-broadcast ARP with our correct MAC address
  - Then send a broadcast ping with the right IP but wrong MAC address
  - Only a machine which has our correct MAC address from the sniffed ARP will respond
    - i.e., the sniffer machine!

Preventing Sniffing

- Solutions:
  - Prevent the use of network adapters in promiscuous mode
  - Use of switches instead of hubs
    - But does not fully solve (as we will see later)

- Prevent effectiveness of sniffing:
  - One-time passwords
    - e.g. SecurID, S/Key
  - Use of encryption

Roadmap

- Network models
  - OSI and Internet
  - Address resolution
- **Network vulnerabilities**
  - Physical layer
  - **Data link layer**
  - Network layer

(Layer 2) Data Link

- Topics:
  - Switches
    - Behavior
    - MAC flooding
    - ARP spoofing/poisoning

Switch behavior

- Switches *typically* send frames only to the destination MAC address
  - They have a table with the MAC reachable from each of their ports

Port	MAC
1	00:0e:81:10:19:fc
2	00:1f:42:12:04:72
…	…

- When a frame reaches the switch:
  - Searches for the port where the device with that MAC is at
  - Sends the frame to that port
- Switches reduce the sniffing problem
  - The network adapter *typically* only sees what is meant for it

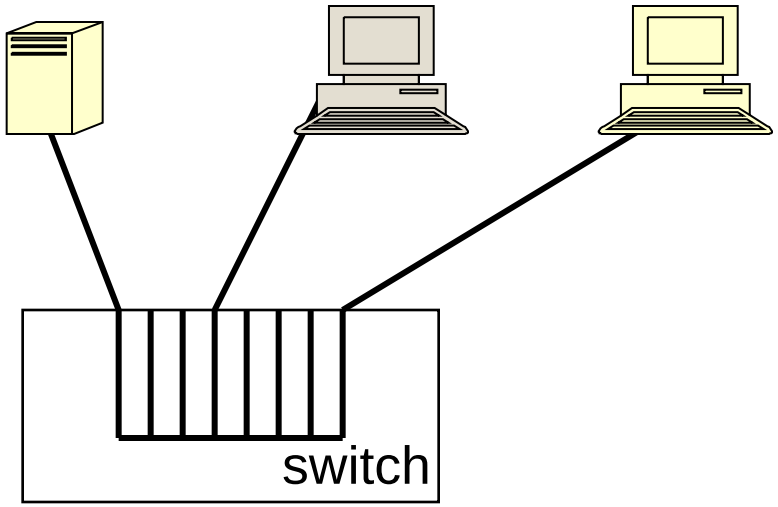
ARP Vulnerabilities

- MAC flooding
  - Overwhelm the switch with entries
- ARP spoofing/poisoning:
  - An attacker sends a non-requested ARP message with a false IP-MAC address correspondence
  - ARP messages are in no way signed, so it is easy to falsify a message from any given MAC

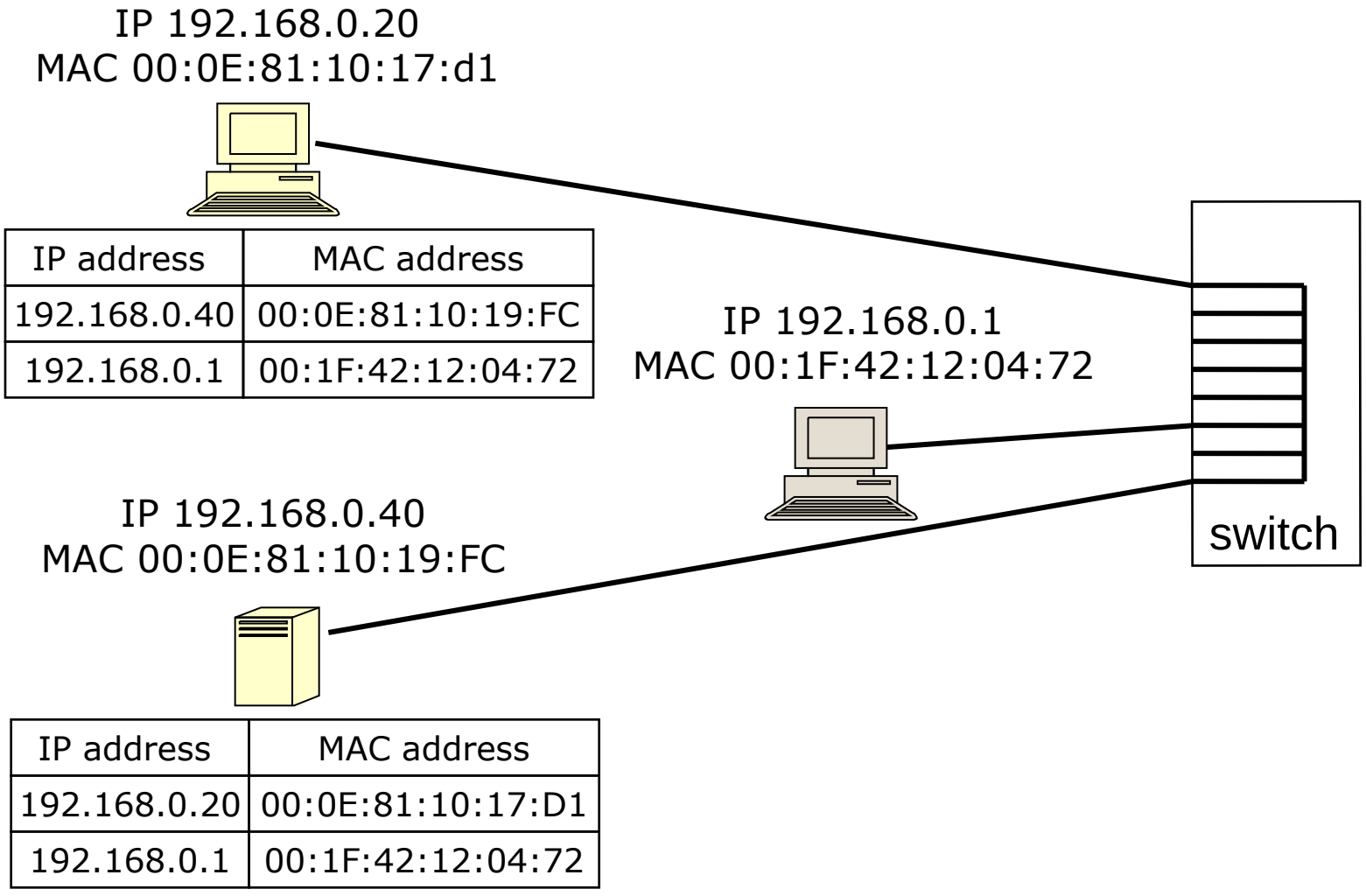
MAC Flooding

- Attacker sends several unsolicited ARP messages
  - Each ARP message is sent with a different MAC
- When the table is filled up:
  - Some switches stop accepting new connections (DoS)
  - Most switches revert to a Hub mode:
    - Allowing standard sniffing attacks to work 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



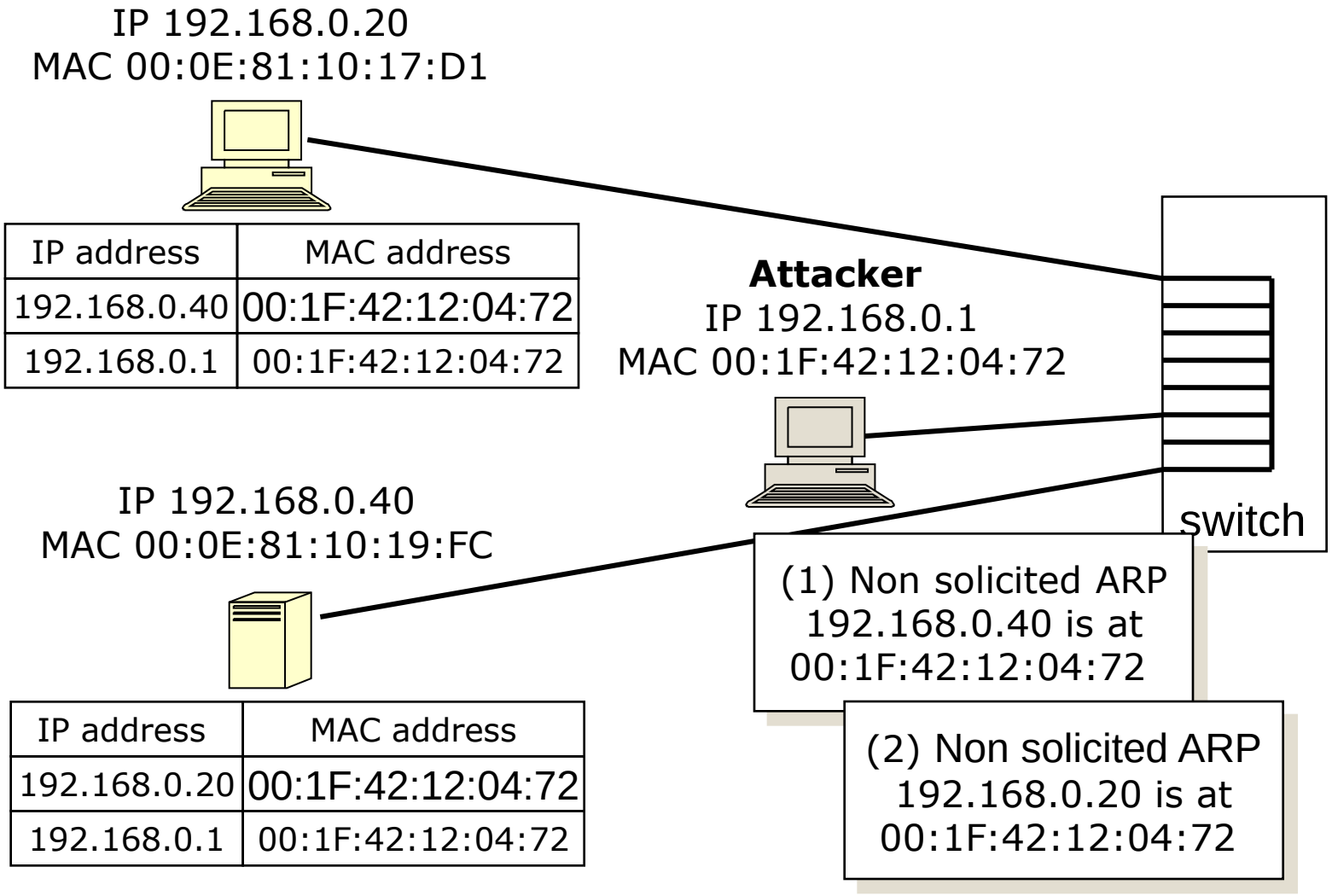
ARP Tables OK



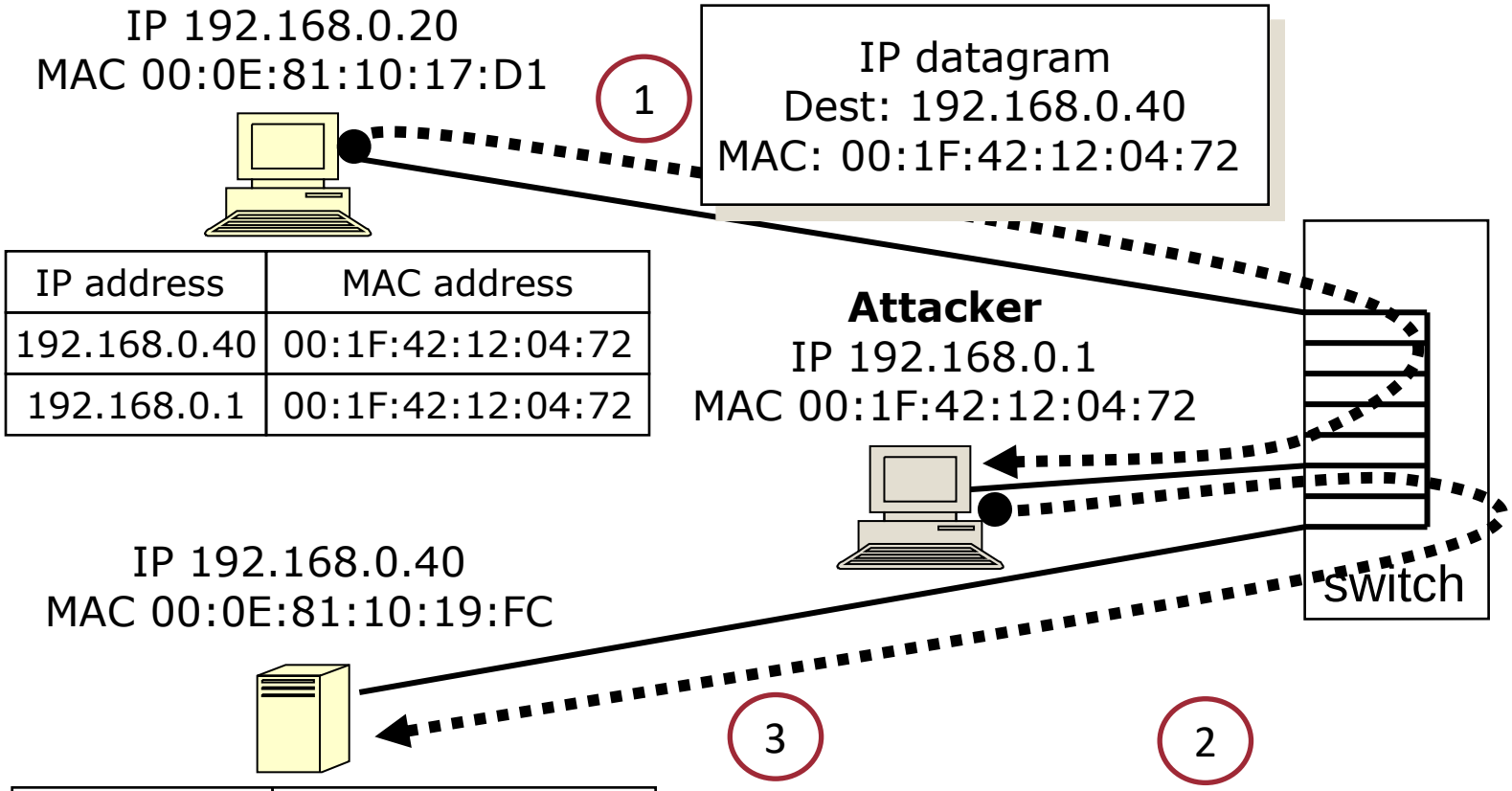
ARP Spoofing/Poisoning Attack Steps

- Intercepting Traffic
  - The attacker sends forged ARP messages onto a local network
- Associating MAC Address
  - These messages associate the attacker's MAC address with the IP address of a legitimate network member, typically a router or gateway
- Redirecting Data
  - Consequently, data intended for the legitimate member is misdirected to the attacker
- Data Interception or Modification
  - The attacker can intercept, modify, or block data
- Resending Data
  - The attacker typically forwards the data to the legitimate recipient, maintaining the illusion of a normal flow, to avoid detection
  - Typically done by sending the packets to the real MAC address associated with the IP address in the packet, which the attacker has knowledge of

ARP Tables Spoofing/Poisoning



ARP Tables Adversary-in-the-Middle attack

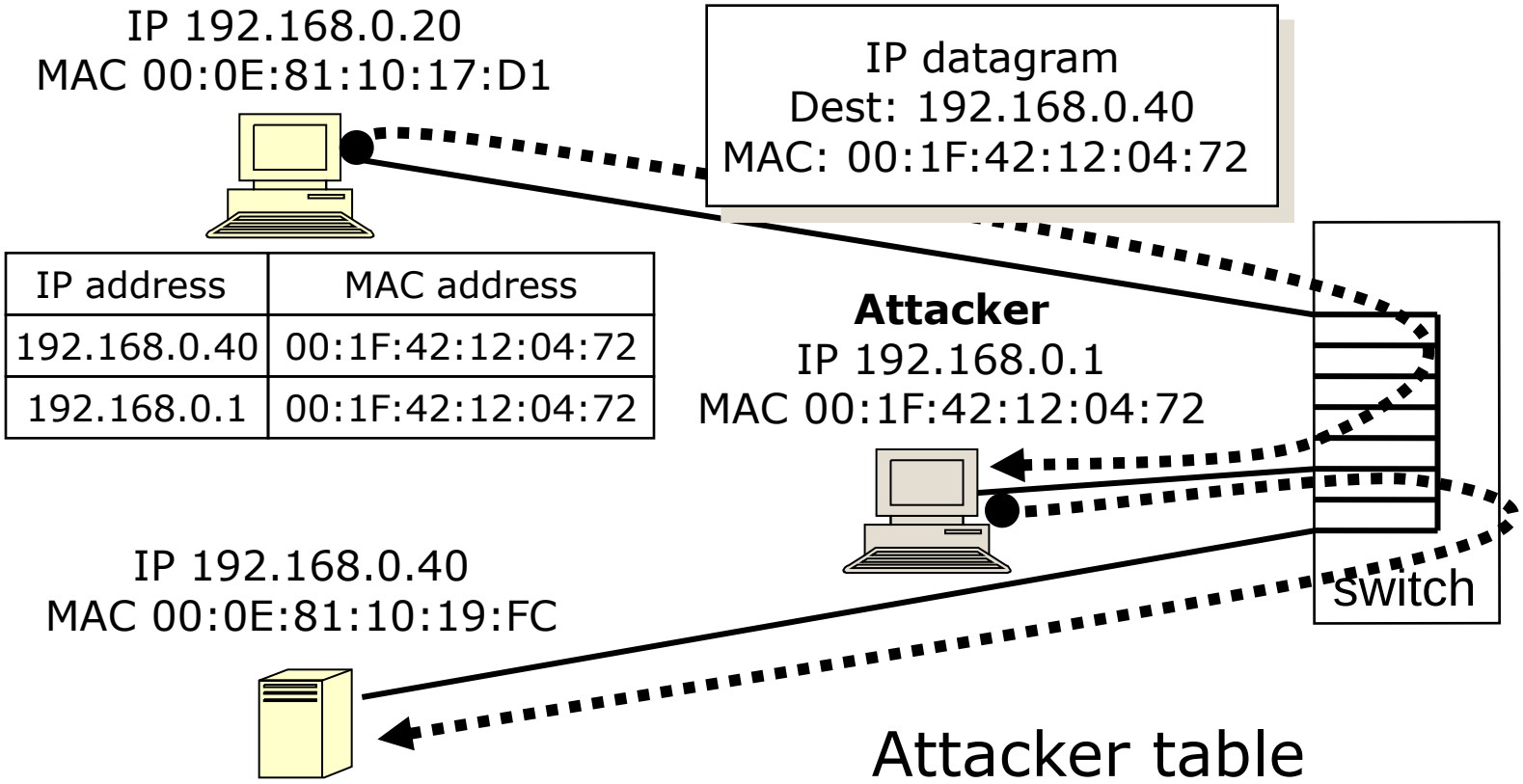


IP address	MAC address
192.168.0.40	00:1F:42:12:04:72
192.168.0.1	00:1F:42:12:04:72

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 broadcasts ARP Query "who has IP 192.168.0.40"?
- That host sends ARP Reply "I do, my MAC is 00:0E:81:10:19:FC"
- Switch updates its table

ARP Tables Poisoned



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

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 table

IP address	MAC address
192.168.0.40	00:0E:81:10:19:FC
192.168.0.20	00:0E:81:10:17:D1

Results from ARP Spoofing/Poisoning

- The devices 192.168.0.20 and 192.18.0.40 have poisoned ARP tables
- All the data sent from 192.168.0.20 to 192.168.0.40 is redirected to the attacker (Layer 2)
- The attacker may redirect the data to the intended receiver
- Neither the attacked machines nor the switch can detect the attack
- Tools example
  - dsniff - auditing and penetration testing tool set
  - Ettercap - packet sniffer and ARP cache poisoning
- In conclusion: switches do not eliminate the sniffing problem

A comment on “security tools”

- dsniff is one of many tools usable for good and bad:

dsniff

latest release: dsniff-2.3.tar.gz (CHANGES)
beta snapshots

Abstract

dsniff is a collection of tools for network auditing and penetration testing. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy passively monitor a network for interesting data (passwords, e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching). sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.

I wrote these tools with honest intentions - to audit my own network, and to demonstrate the insecurity of most network application protocols. Please do not abuse this software.

Preventive Measures

- Do not trust Layer 2 isolation
- Use tools like arpwatch
  - Monitor the ARP to IP translation
  - Alert the system administrators
- Use of switches with fixed tables
  - Has a cost in **loss of flexibility**

Roadmap

- Network models
  - OSI and Internet
  - Address resolution
- **Network vulnerabilities**
  - Physical layer
  - Data link layer
  - **Network layer**

(Layer 3) Network Layer

- Topics:
  - Routers and Routing
  - IP Addresses

Router behavior

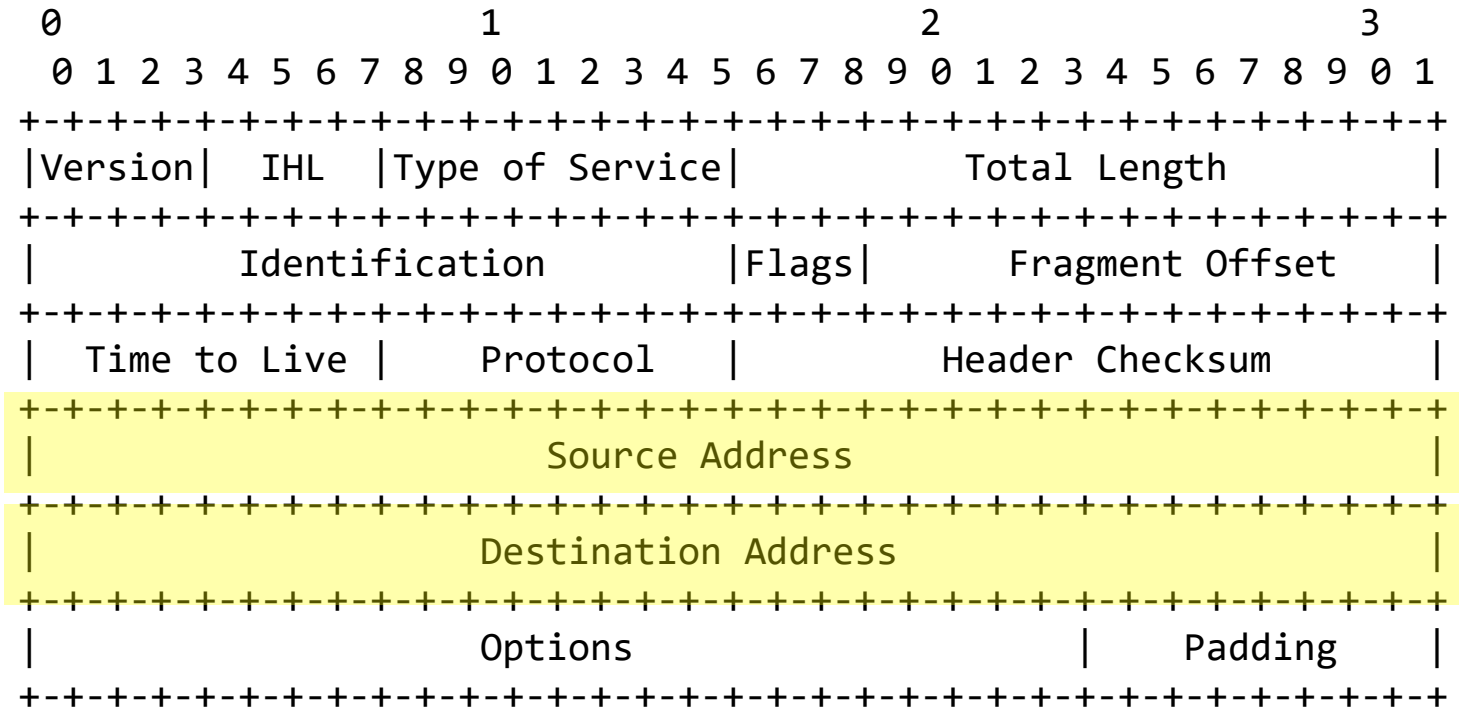
- Routers support the indirect delivery of IP datagrams
- Routing tables are used
- A datagram can usually be sent:
  - Directly to the final destination
  - To the next router in the direction of the destination
  - To the default router

Network Layer threats

- Packet integrity threat
  - IP spoofing
- Information leak threat
- Denial-of-Service (DoS) threat

IP packet header

(RFC 791)

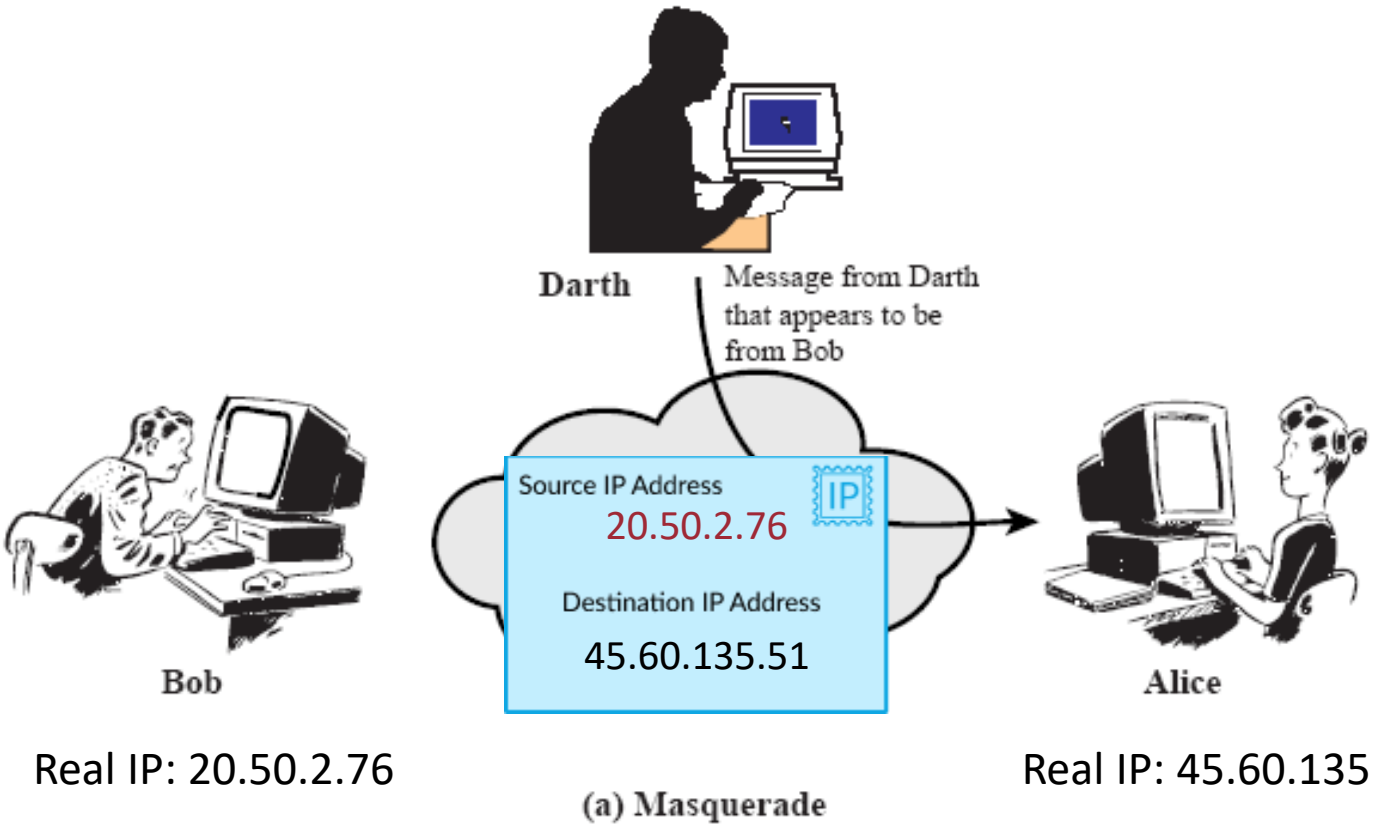


Network Layer attacks (1)

- IP spoofing:
  - Packet integrity threat
    - Data is **not** authenticated
  - Attacker can change the source address of IP packets
    - It is insecure to base access control on IP addresses
  - Attacker can *delay*, *reorder*, *replay*, *modify*, or *inject* IP packets and any of its fields

IP packet masquerade

Real IP: 45.60.65.43



Real IP: 20.50.2.76

Real IP: 45.60.135.51

(a) Masquerade

Network Layer attacks (2)

- Users have little to no guarantee concerning the routing path taken by the packets:
  - Information leak threat
  - DoS threat

Route hijacking

Network Layer attacks (3)

- Route update security
  - An attacker might corrupt the routing tables by sending routing-update messages
  - ICMP redirect packets
  - Intra-domain
    - RIPv1 and IGRP do not have authentication
  - Inter-domain
    - BGP also does not have authentication; based on policy
  - DoS, Man-in-the-Middle attacks are possible

Roadmap (to be continued)

- Network models
  - OSI and Internet
  - Address resolution
- **Network vulnerabilities**
  - Physical layer
  - Data link layer
  - Network layer
  - **Transport layer**
  - **Application layer**
- Network security models