Network Security

Network Components and Protocols

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:

Cabling and Hubs (Layer 1); Sniffers

Switches and ARP (Layer 2)

Routers and IP (Layer 3)

TCP and ICMP (Layer 4)

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.

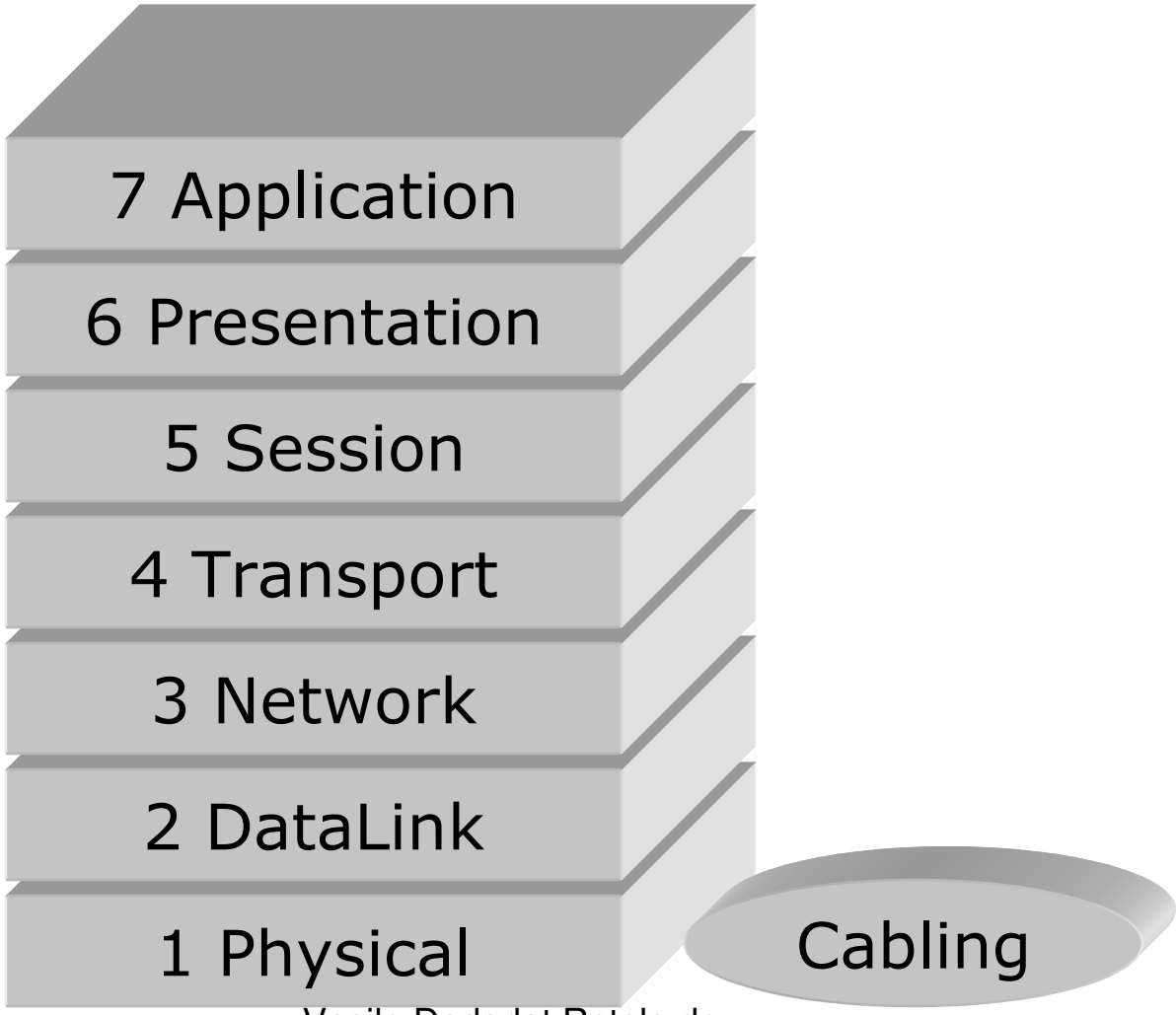
Network Cabling

- Different Cabling Types:
  - Thin Ethernet – 10BASE-2
    - 10Mbps, 200m range
  - Thick Ethernet – 10BASE-5
    - 10Mbps, 500m range
  - Unshielded Twisted Pair (UTP)
    - Telephone (Cat 1), 10BASE-T (Cat 3), 100BASE-T (Cat 5)
  - Shielded Twisted Pair (STP)
    - Token ring networks and high-interference environments

Other Layer 1 options

- Fibre Optic
  - Cable between hub and device is a single entity,
  - Tapping or altering the cable is difficult,
  - Installation is more difficult,
  - Much higher speeds – Gigabit Ethernet.
- Wireless LAN
  - Popular where building restrictions apply,
  - IEEE 802.11b, 802.11g,
  - Advertised at 11Mbps, 54 Mbps,
  - Several disadvantages:
    - Radio signals are subject to interference, interception, and alteration.
    - Difficult to restrict to building perimeter.
    - Security must be built in from initial network design.

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

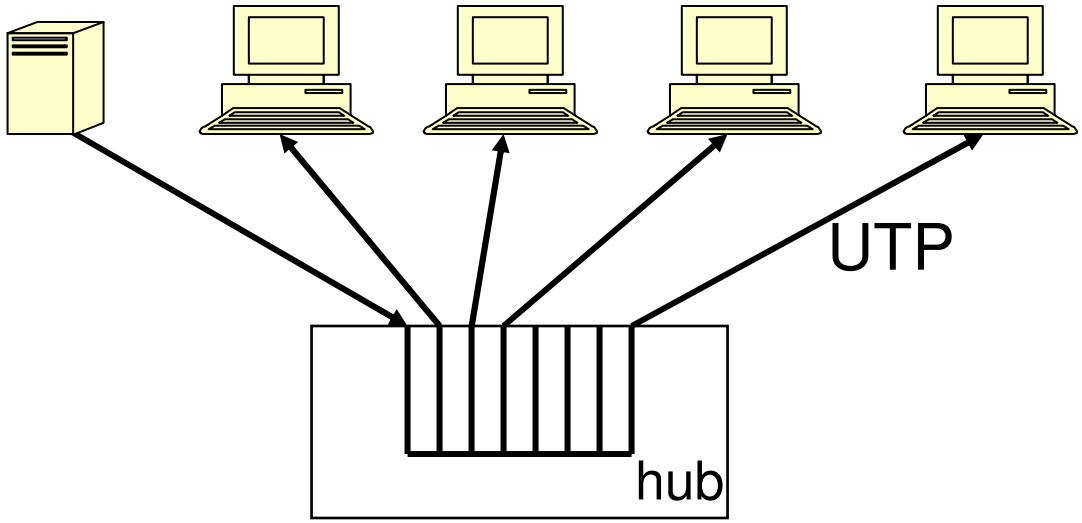
Some contributory factors in assessing risk:

- 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?

Safeguards: protective trunking, dedicated closets, electromagnetic shielding.

UTP and Hub

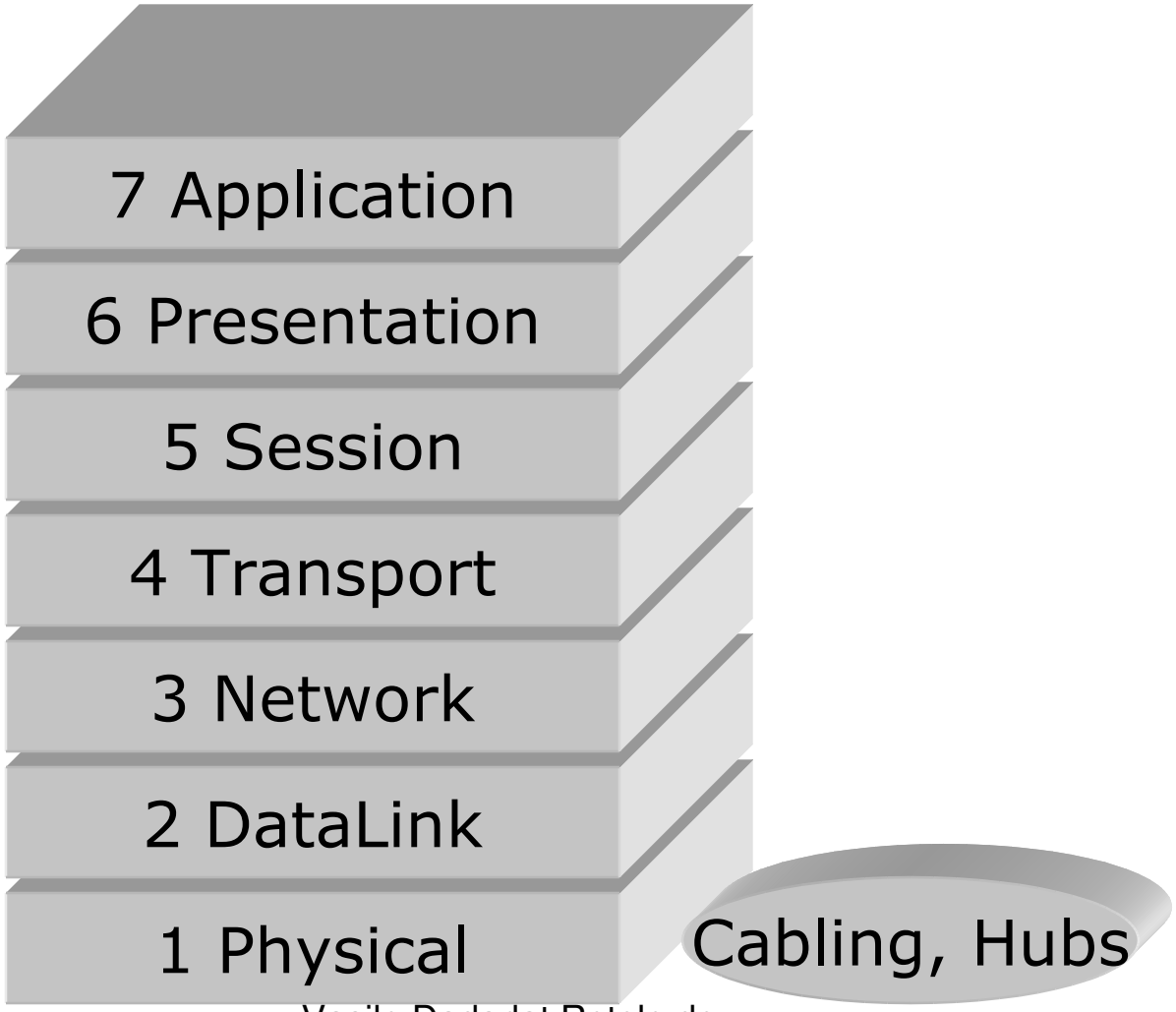
- Cable between hub and device is single entity.
- Only connectors are at the cable ends.
- Disconnection/cable break rarely affects other devices.
- Easy to install.



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.

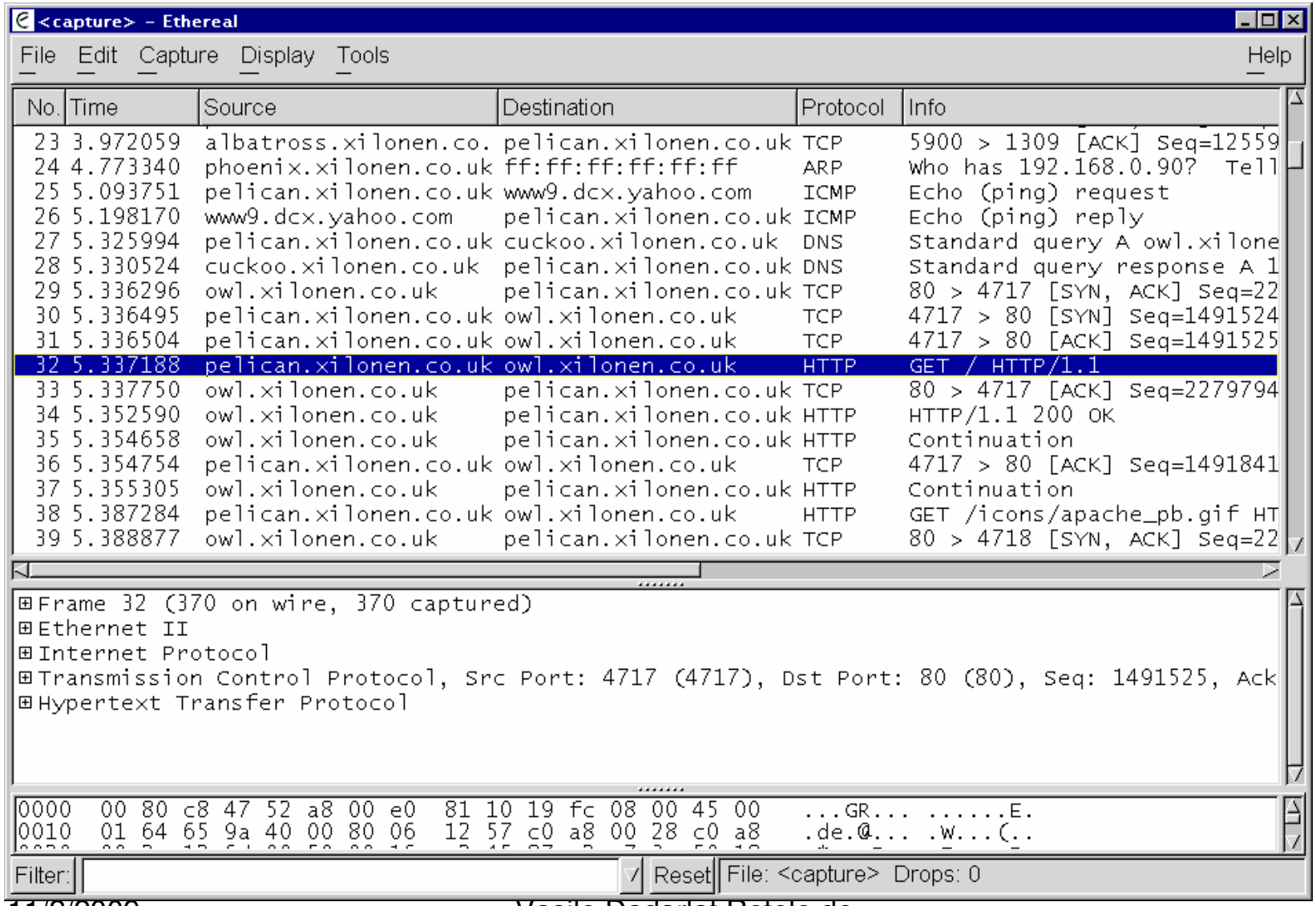
Hubs in OSI Protocol Stack



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
  - ethereal
  - Snort

Popular network sniffer Ethereal: Screenshot



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.
  - 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.
    - Exploiting operating system quirks.
    - AntiSniff, Security Software Technologies

    Article at:
    http://www.packetwatch.net/documents/papers/snifferdetection.pdf

Sniffer Safeguards

Examples of safeguards are:

- Use of non-promiscuous interfaces.
- Use of switched environments
- Encryption of network traffic.
- One-time passwords, e.g. SecurID, skey, limiting usefulness of information gathered by sniffer.

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.

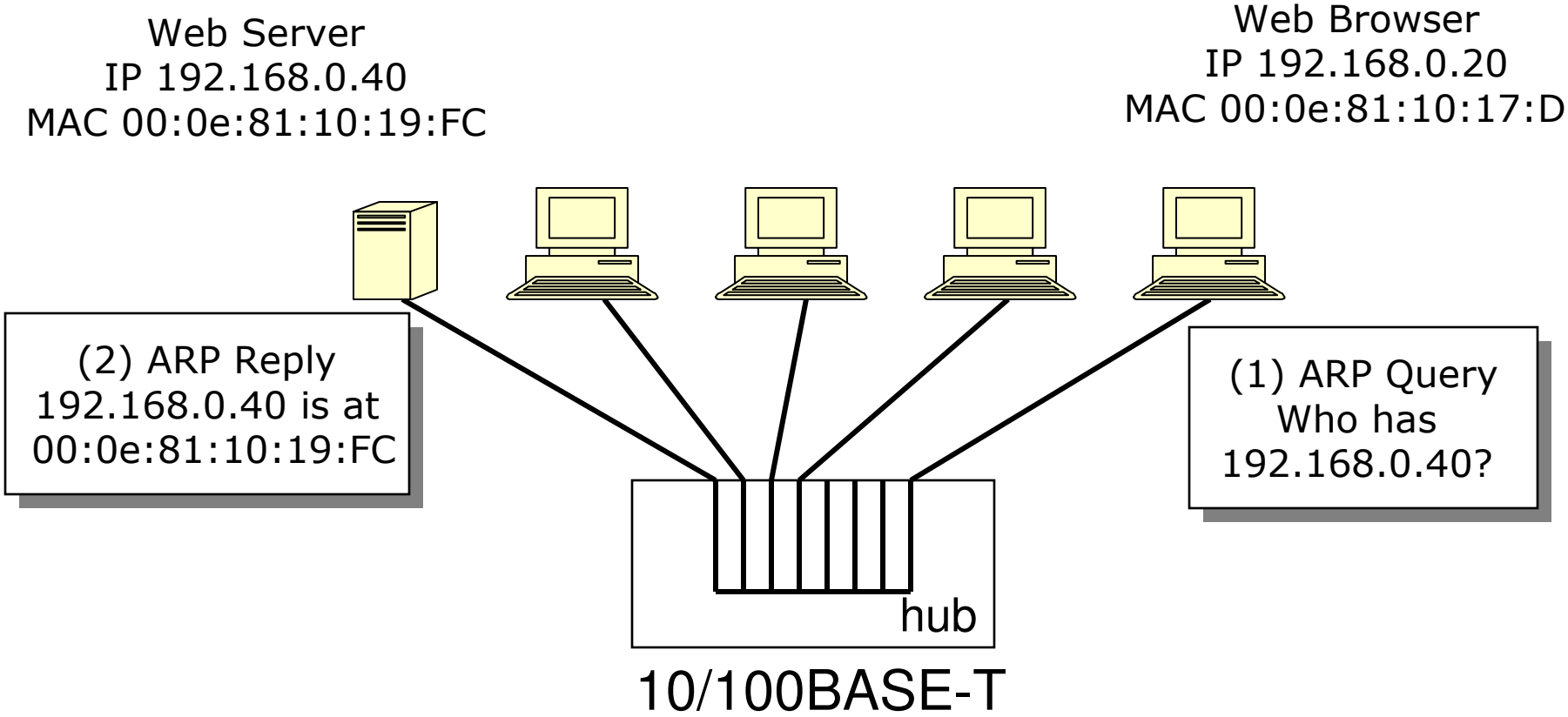
IP Addressing

- IP address is 32 bits long – hence 4 billion ‘raw’ addresses available.
- Usually expressed as 4 decimal numbers separated by dots:
  - 0.0.0.0 to 255.255.255.255
  - Typical IP address: 134.219.200.162.
- Many large ranges already assigned:
  - 13.x.x.x Xerox, 18.x.x.x MIT, 54.x.x.x Merck.
  - Shortage of IP addresses solved using private IP addresses and subnetting/supernetting.

IP Address to Ethernet Address

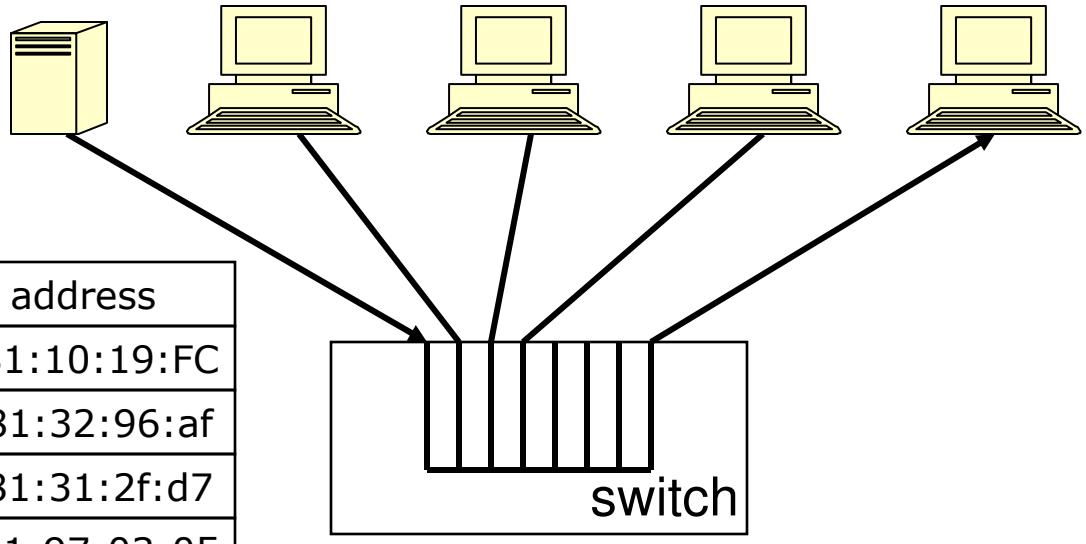
- Address Resolution Protocol (ARP):
  - Layer 3 protocol,
  - Maps IP address to MAC address.
- ARP Query
  - Who has 192.168.0.40? Tell 192.168.0.20.
- ARP Reply
  - 192.168.0.40 is at 00:0e:81:10:19:FC.
- ARP caches for speed:
  - Records previous ARP replies,
  - Entries are aged and eventually discarded.

ARP Query & ARP Reply



Switches

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



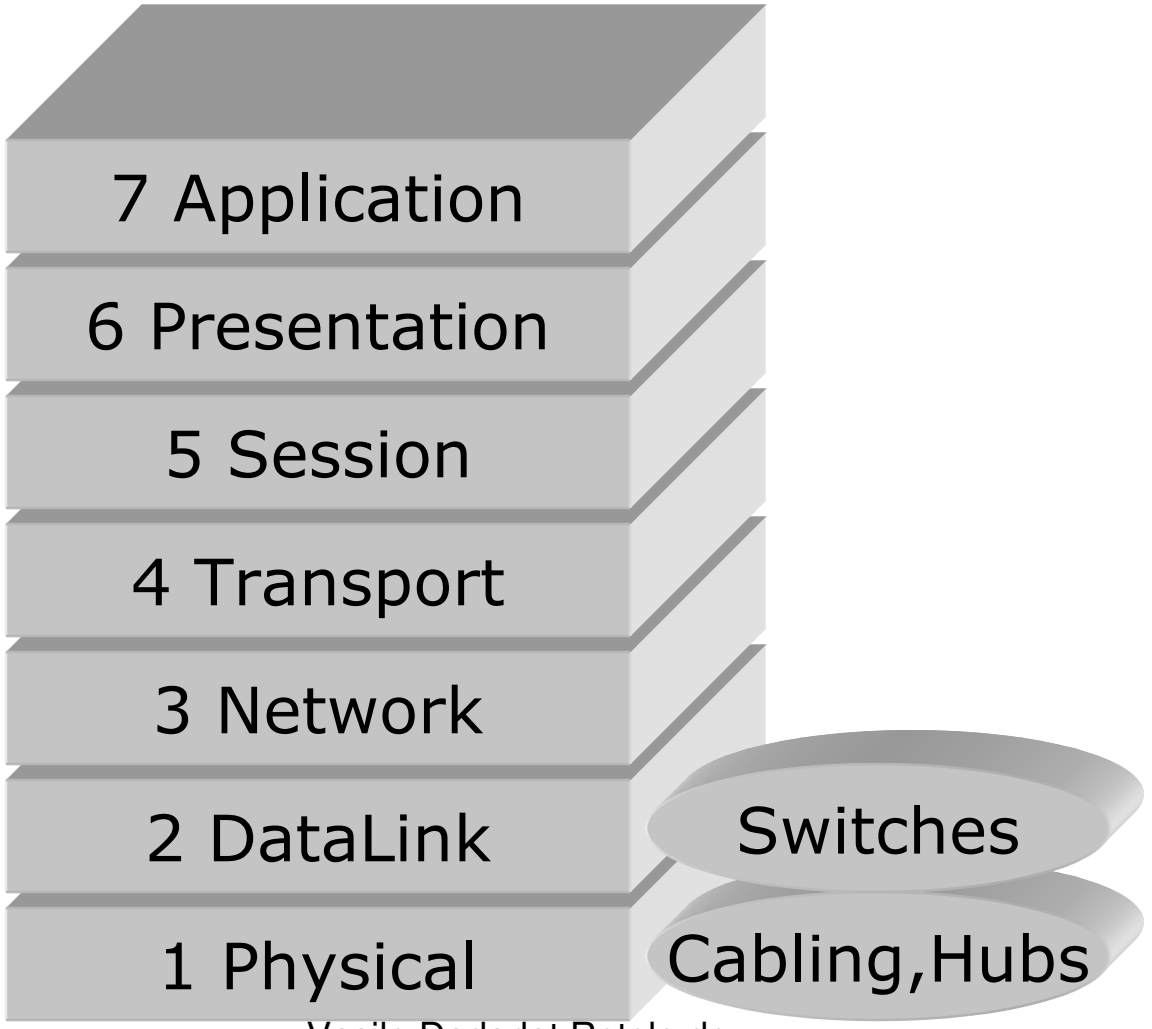
Device	MAC address
1	00:0e:81:10:19:FC
2	00:0e:81:32:96:af
3	00:0e:81:31:2f:d7
4	00:0e:81:97:03:05
8	00:0e:81:10:17:d1

10/100BASE-T

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.

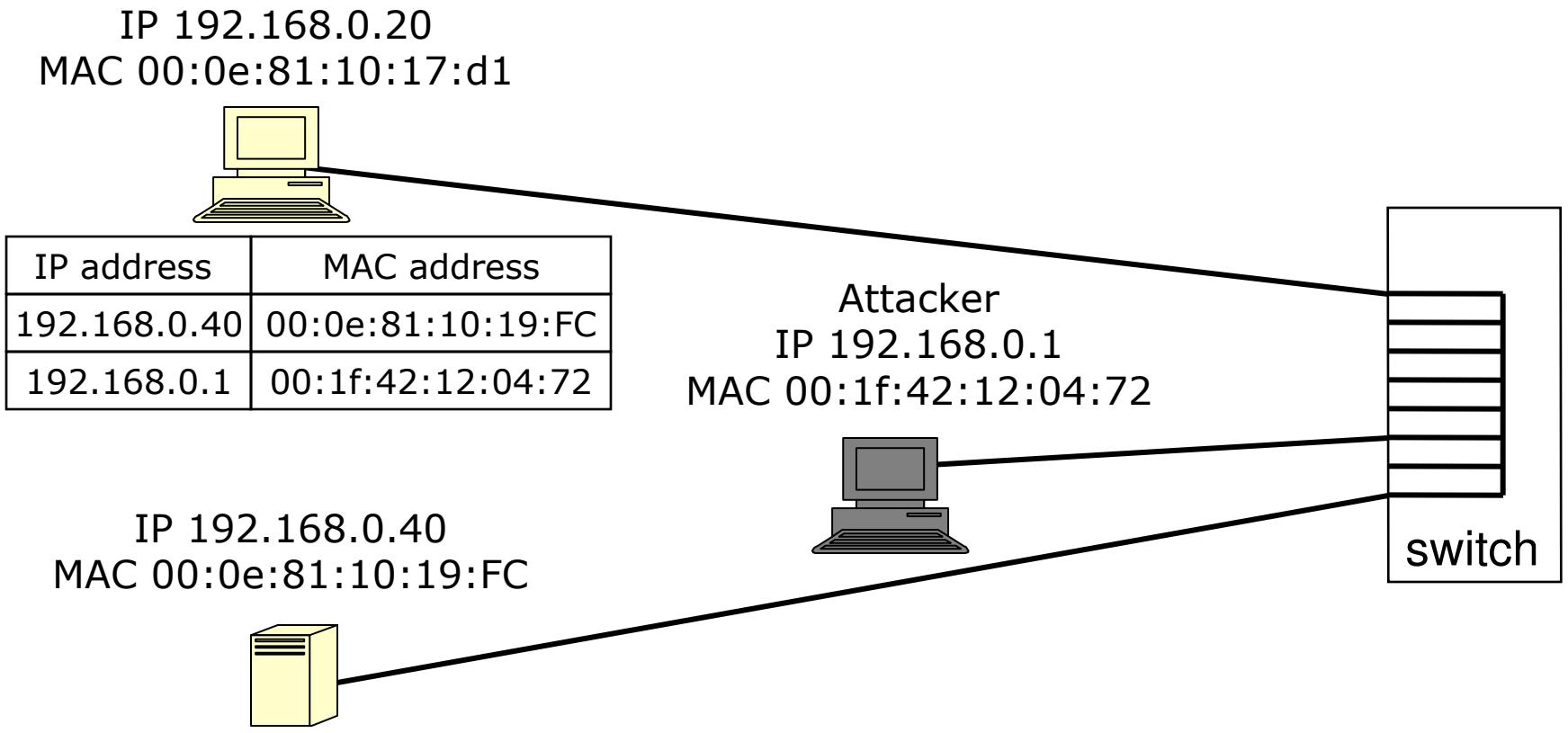
Switches in OSI Protocol Stack



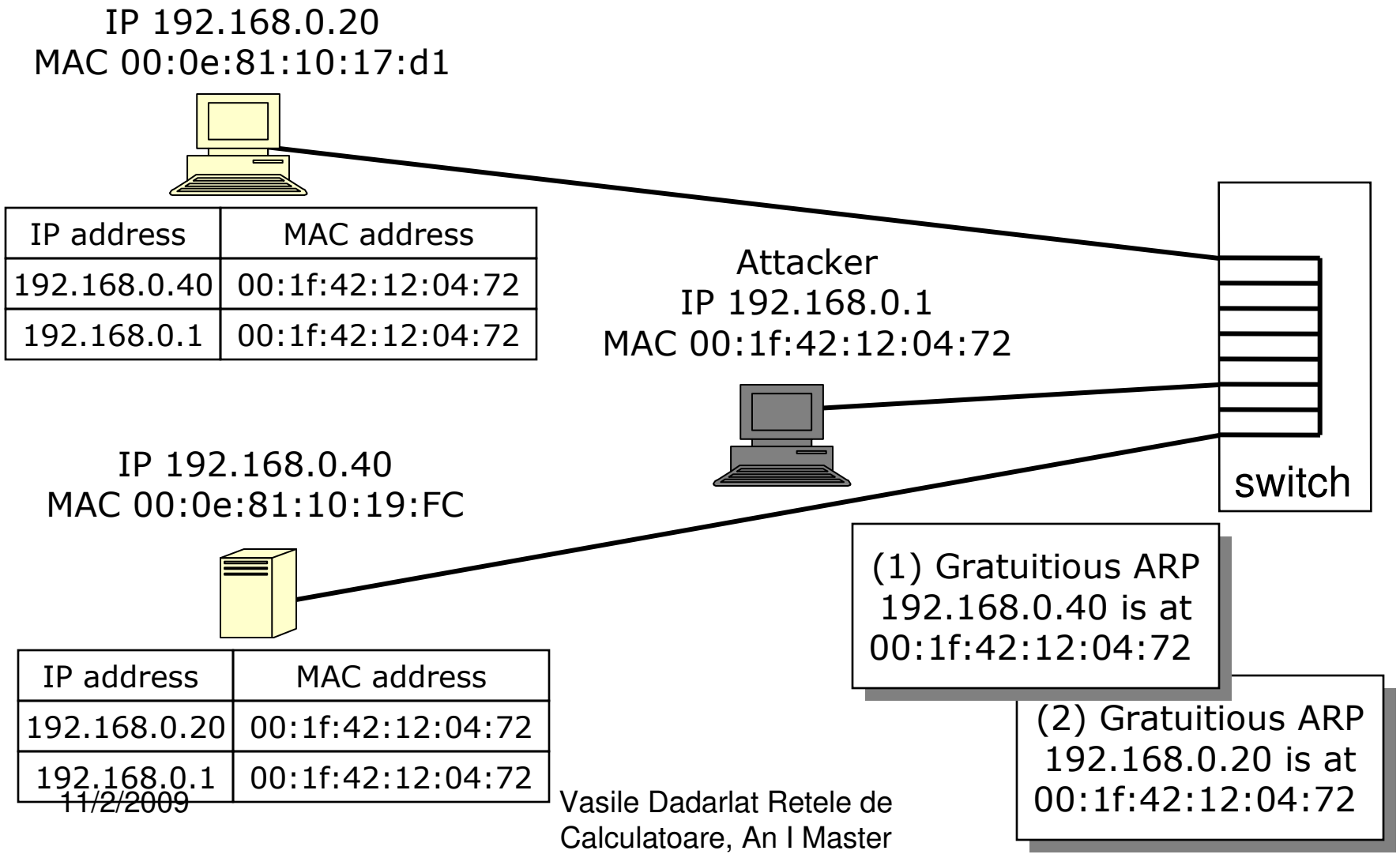
ARP Vulnerability

- 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!

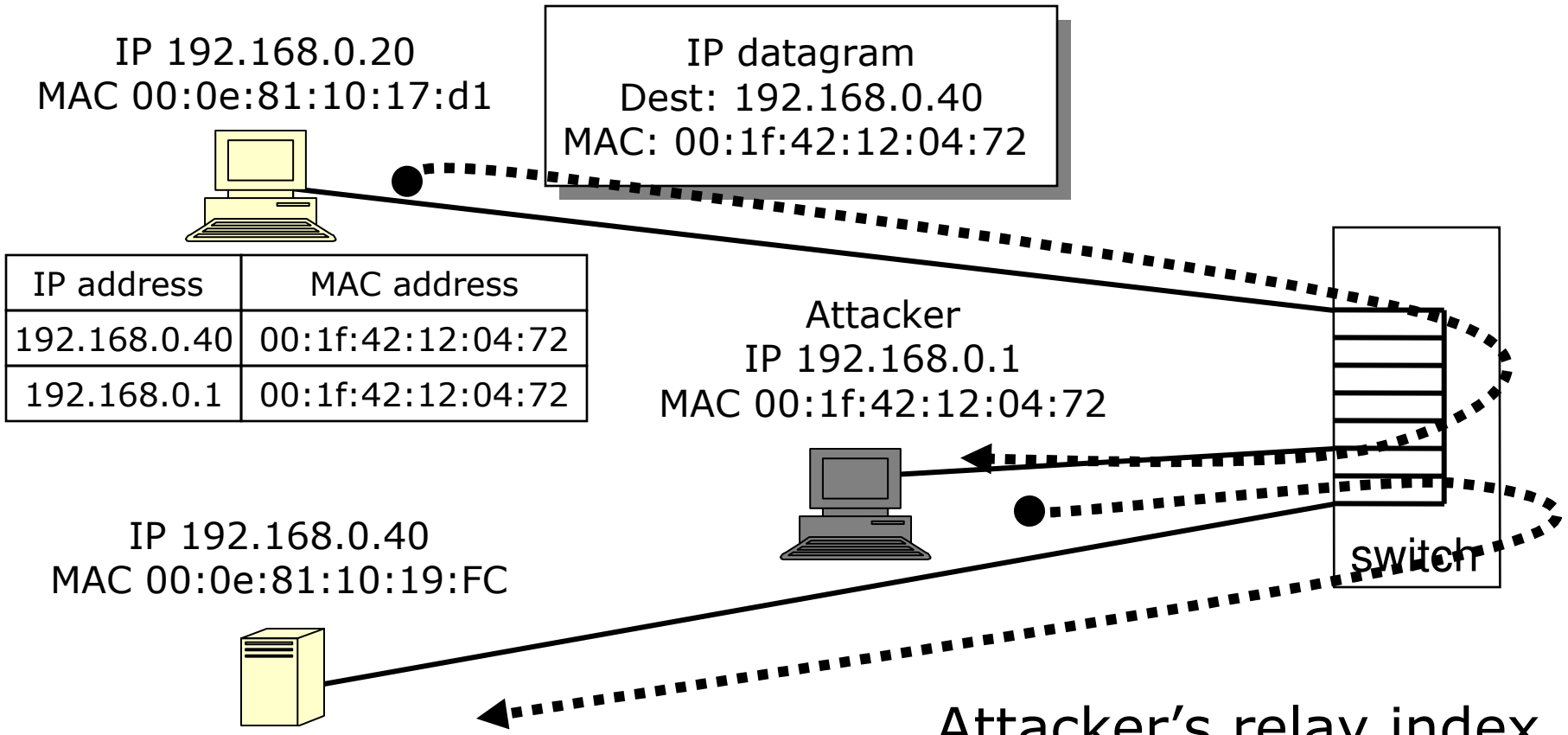
Before ARP Spoofing



After ARP Spoofing



Effect of ARP Spoofing



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

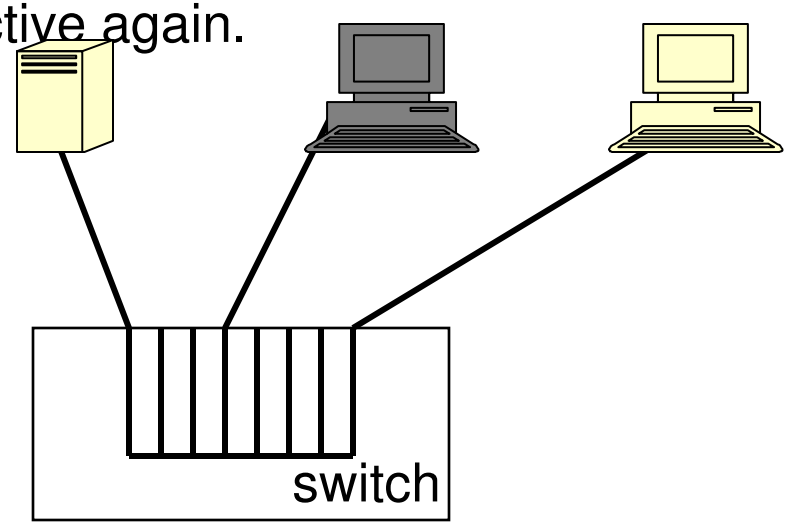
Effect of ARP Spoofing

- 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.

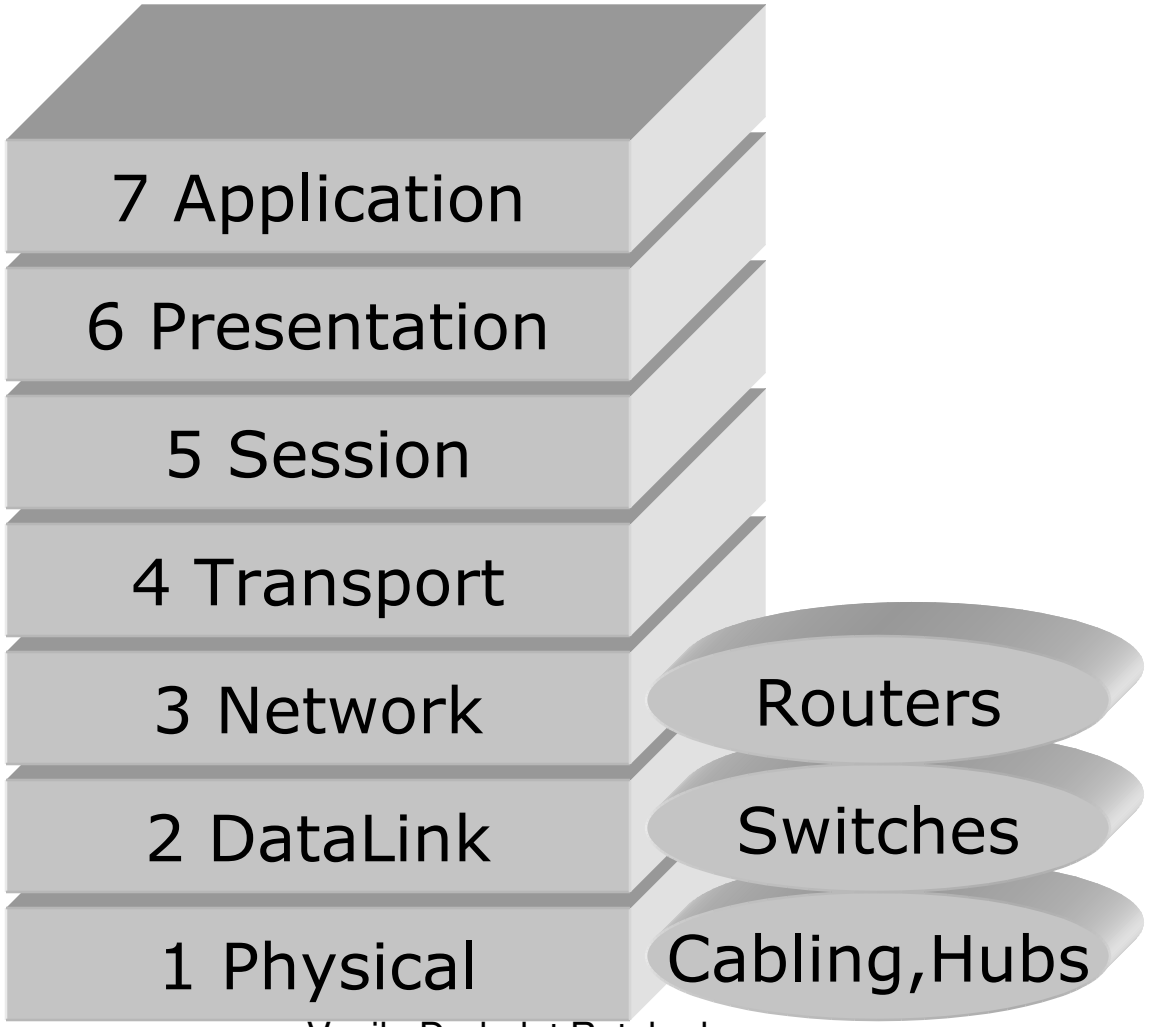
Routers and Layer 3 Issues

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

Routers and Routing

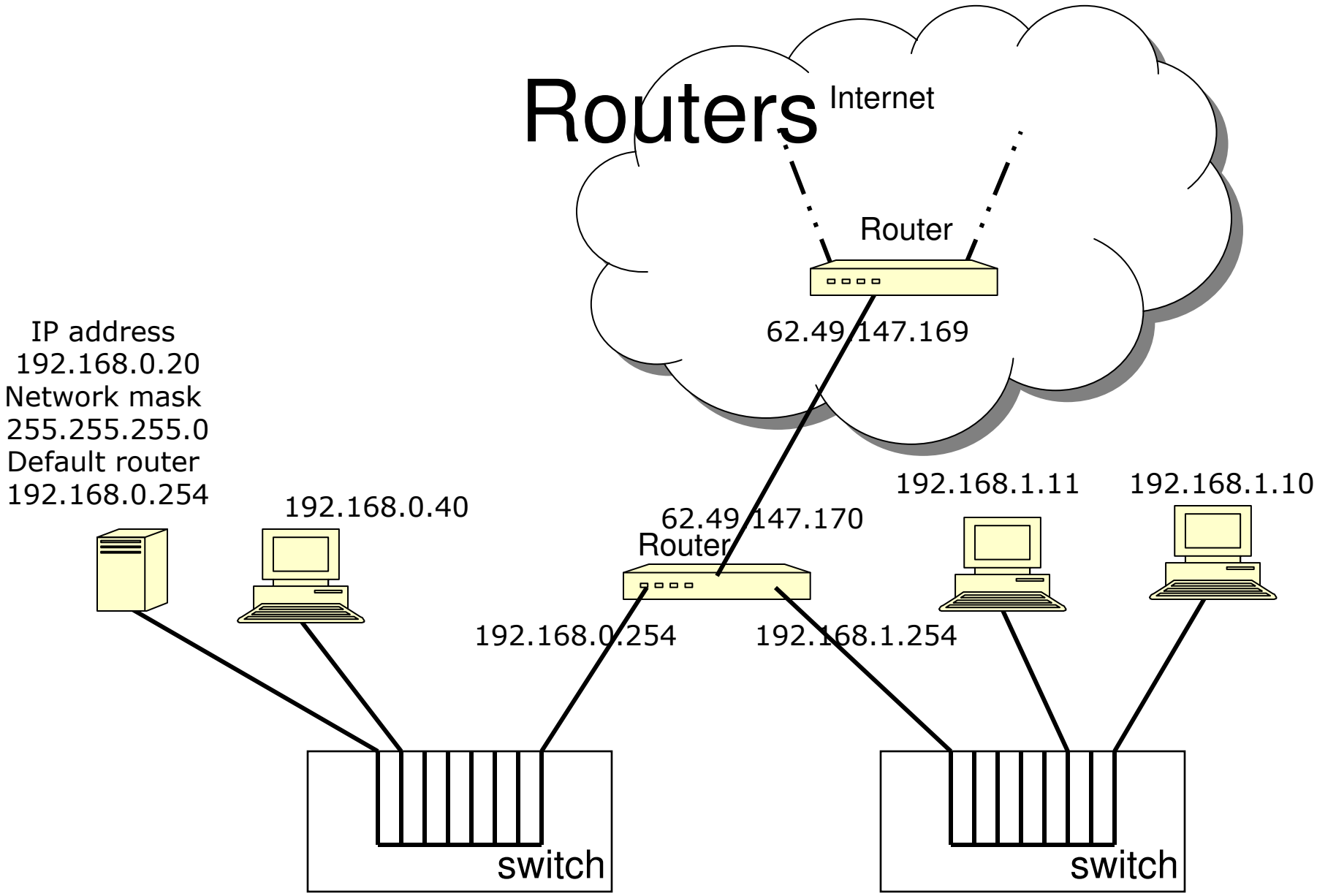
- Routers support *indirect* delivery of IP datagrams.
- Employing routing tables.
  - Information about possible destinations and how to reach them.
- Three possible actions for a datagram:
  - Sent directly to destination host.
  - Sent to next router on way to known destination.
  - Sent to default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

Routers in OSI Protocol Stack

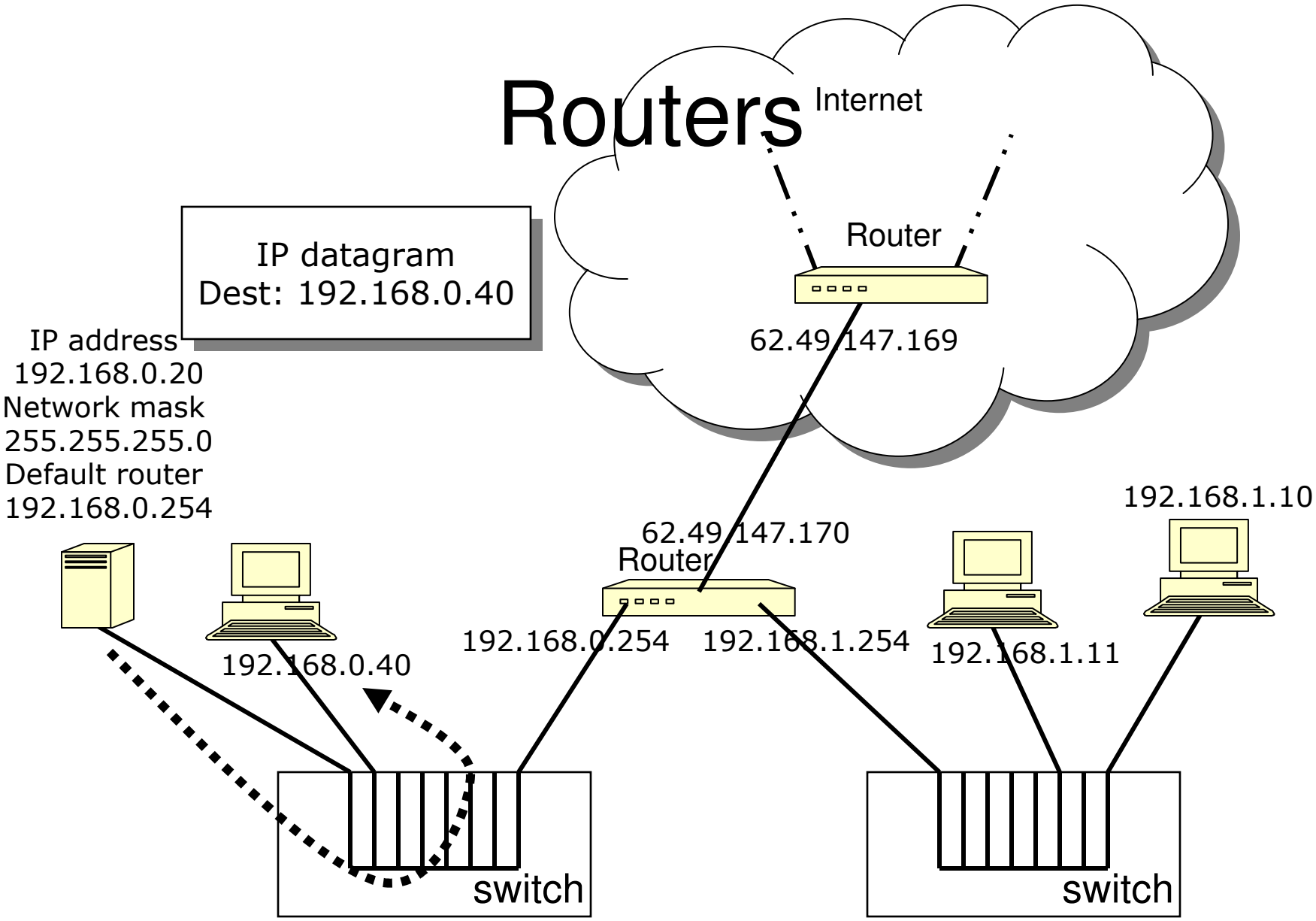


More on IP Addressing

- IP addresses logically split into two parts.
- First part identifies network.
- Second part identifies host on that network.
- Example: the IP address 192.168.0.20:
  - 192.168.0.x identifies network.
  - y.y.y.20 identifies host on network.
  - We have a network with up to 256 (in fact 254) hosts (.0 and .255 are reserved).
  - The *network mask* 255.255.255.0 identifies the size of the network and the addresses of all hosts that are locally reachable.
  - This mask can be fetched from network's default router using ICMP Address Mask Request message.

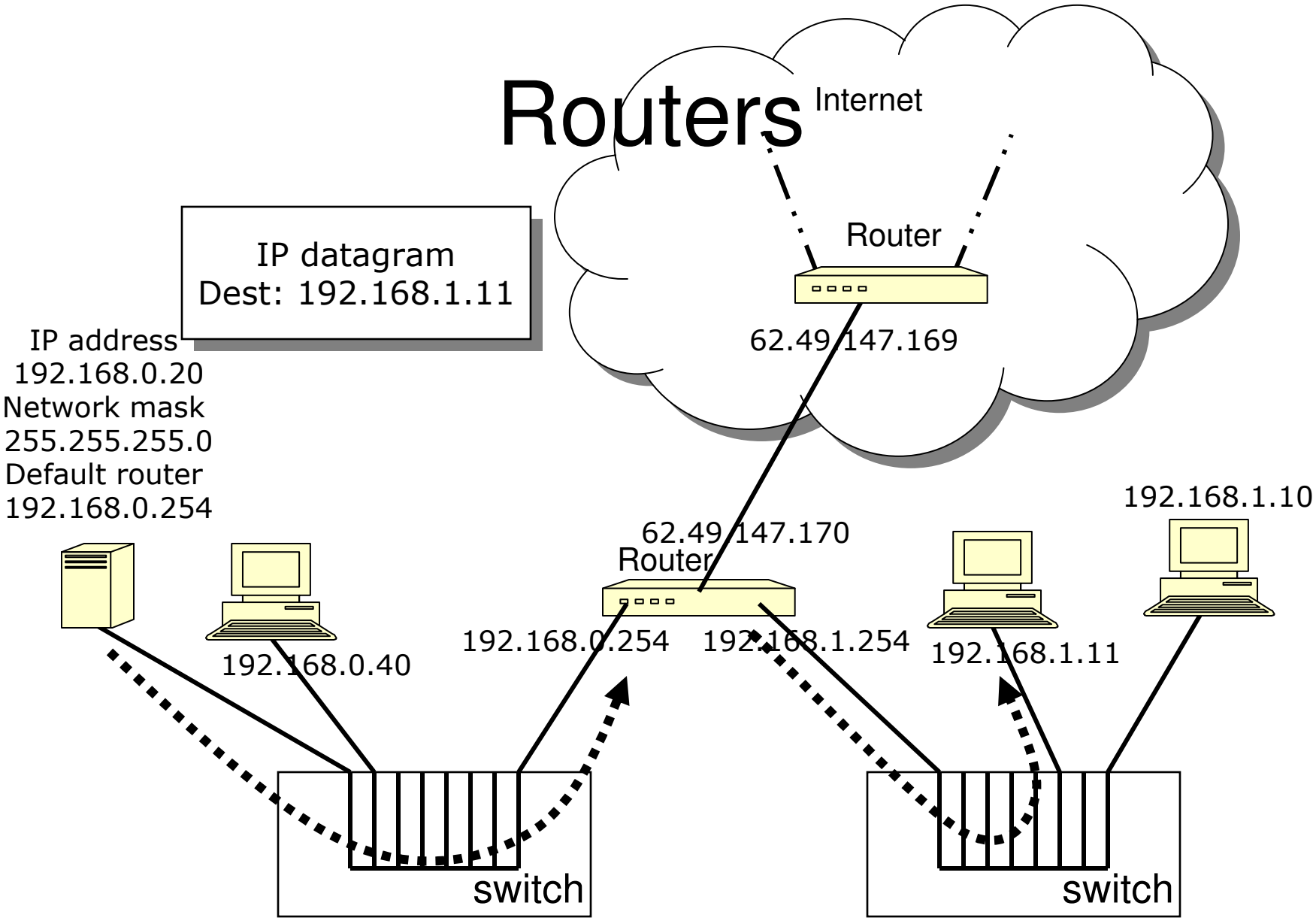

Routers
Internet
Router
62.49.147.169
IP address
192.168.0.20
Network mask
255.255.255.0
Default router
192.168.0.254
192.168.0.40
62.49.147.170
Router
192.168.1.11
192.168.1.10
192.168.0.254
192.168.1.254
switch
switch

Routers



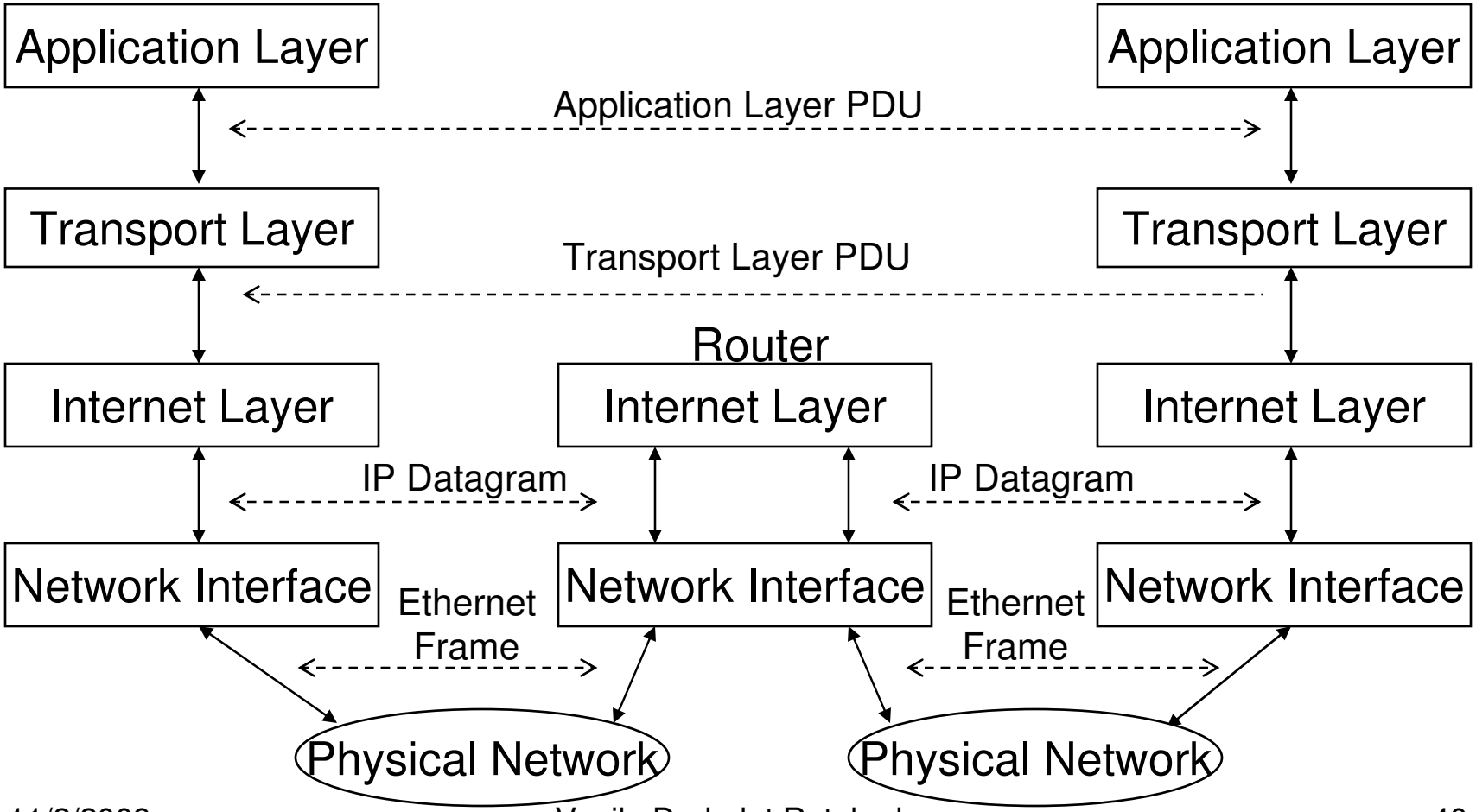
Direct delivery

Routers

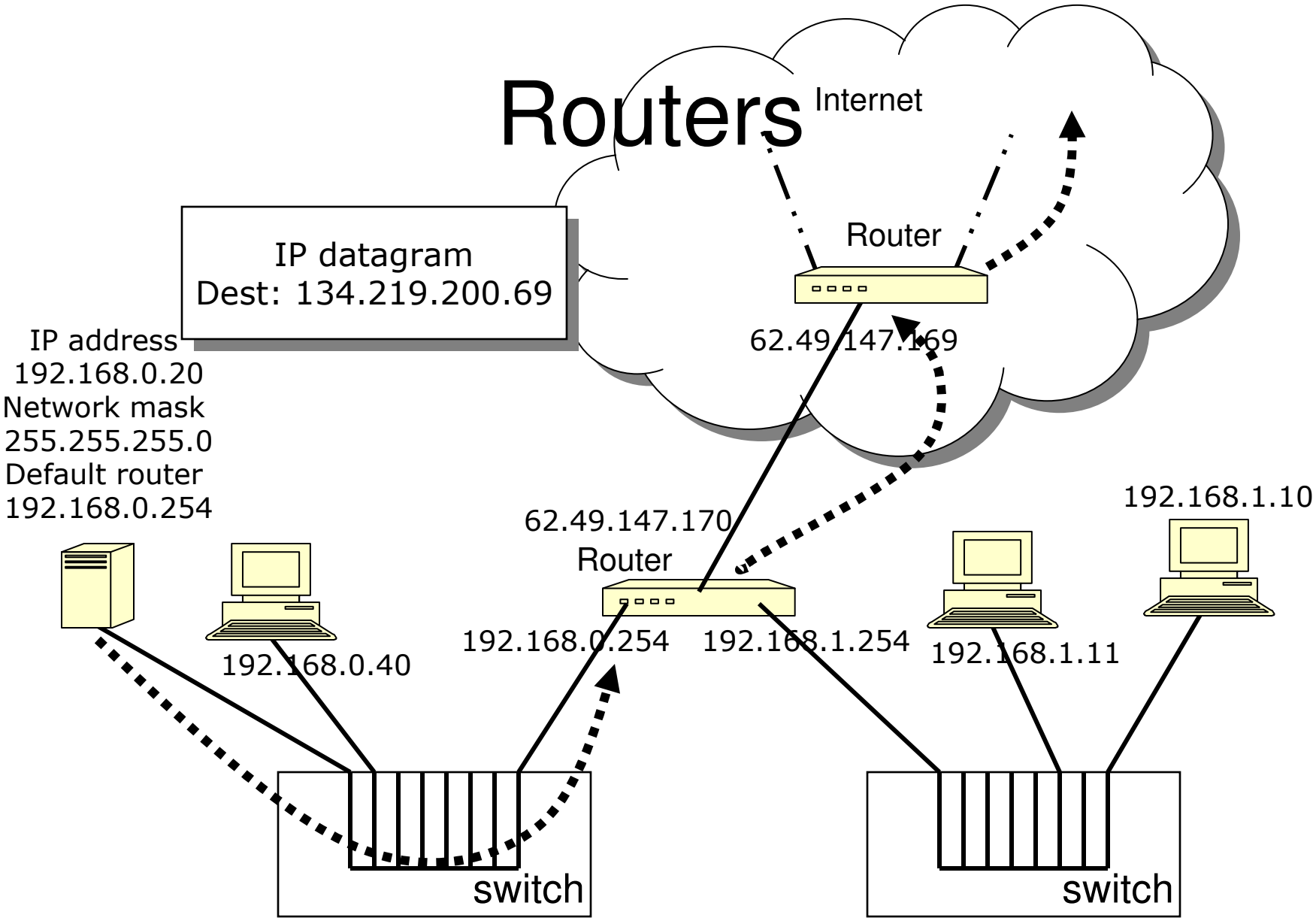


Default router + direct delivery

Protocol Layering Equivalent

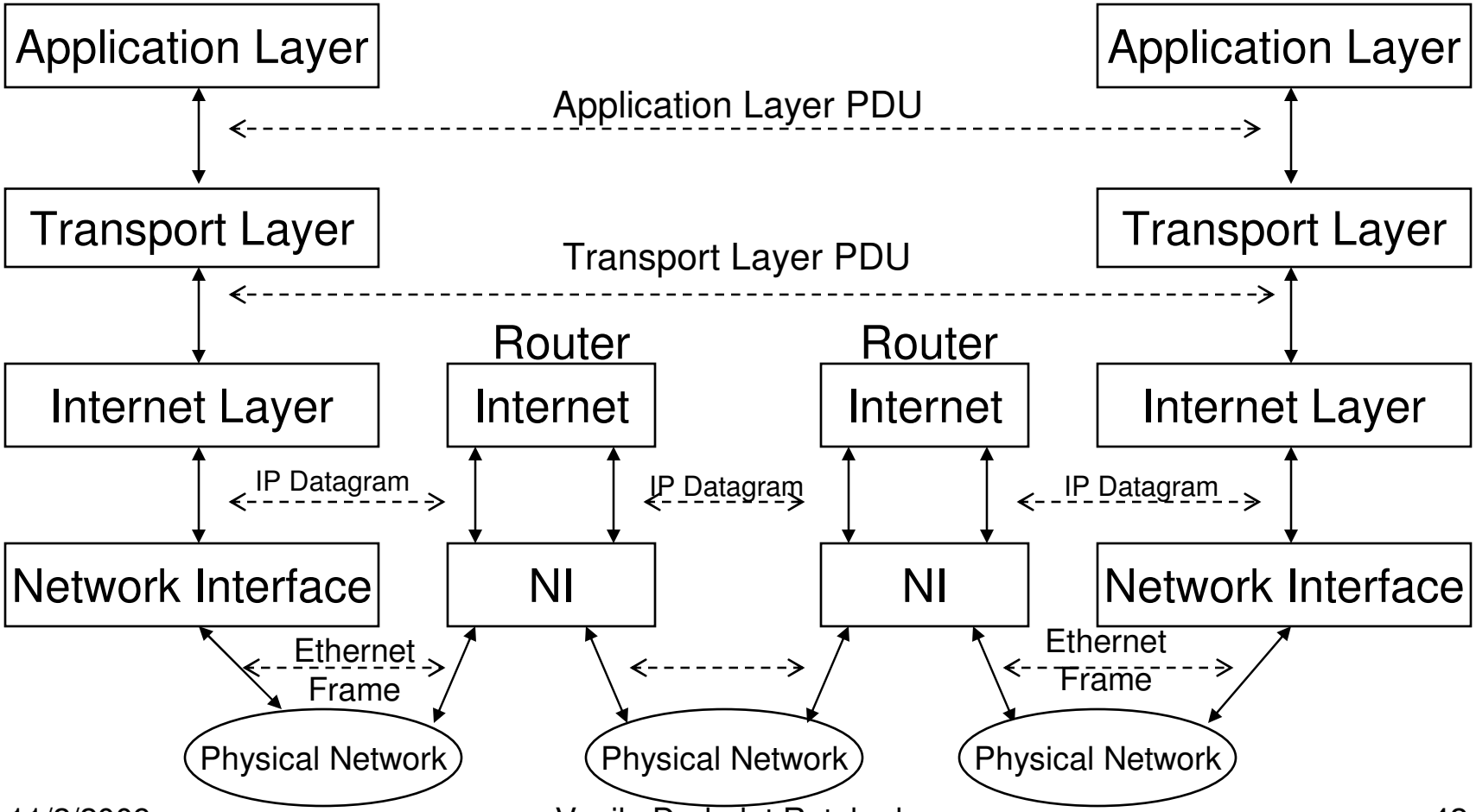


Routers



Default router + next hop + next hop +…

Protocol Layering Equivalent



Private Addressing

- Sets of addresses have been reserved for use on private networks (IETF RFC 1918):
  - 10.0.0.0 to 10.255.255.255 (1 network, 2^{24} hosts),
  - 172.16.0.0 to 172.31.255.255 (16 networks, 2^{16} hosts each),
  - 192.168.0.0 to 192.168.255.255 (256 networks, 2^{8} hosts each).
- Packets with src/dest addresses in these ranges will never be routed outside private network.
  - Helps to solve problem of shortage of IP addresses.
  - Security?
- Previous example: router has external IP address 62.49.147.170 and two internal addresses: 192.168.0.254 and 192.168.1.254:
  - It acts as default router for two small, private networks.

Some Layer 3 Security Issues – 1

- IP spoofing:
  - IP packets are not authenticated in any way.
  - An attacker can place any IP address as the source address of an IP datagram, so can be dangerous to base access control decisions on raw IP addresses alone.
  - An attacker may be able to replay, delay, reorder, modify or inject IP datagrams.
  - Masquerade, integrity violation and illegitimate use threats.
- Users have few guarantees about route taken by data.
  - Information leakage threat.
  - Integrity violation threat.
  - Denial of Service threat.

Some Layer 3 Security Issues – 2

- 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.

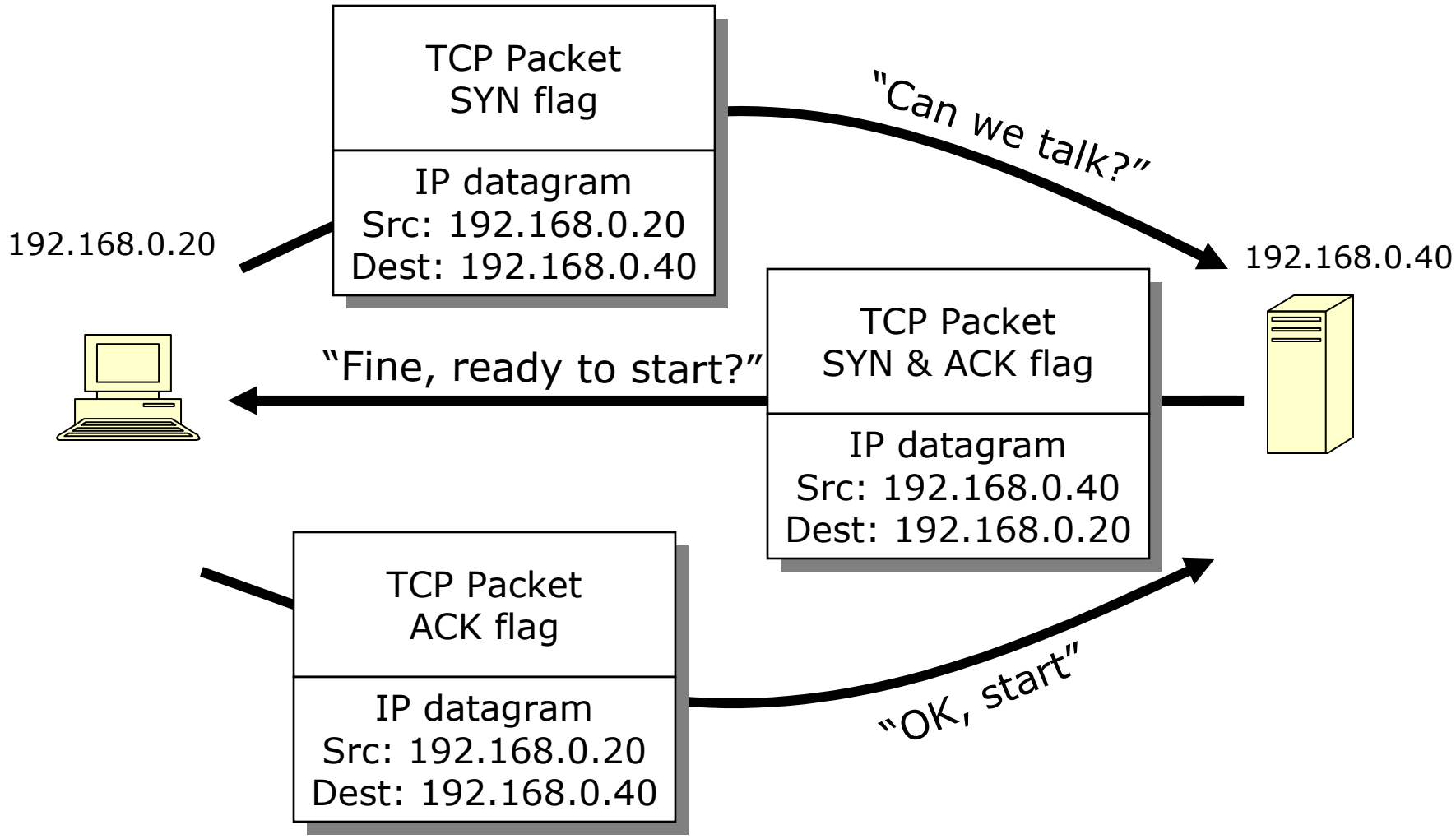
TCP, ICMP and Layer 4 issues

- TCP and Denial of Service (DoS) Attacks
- TCP ports
- ICMP and SMURF DoS Attack
- Safeguards

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



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

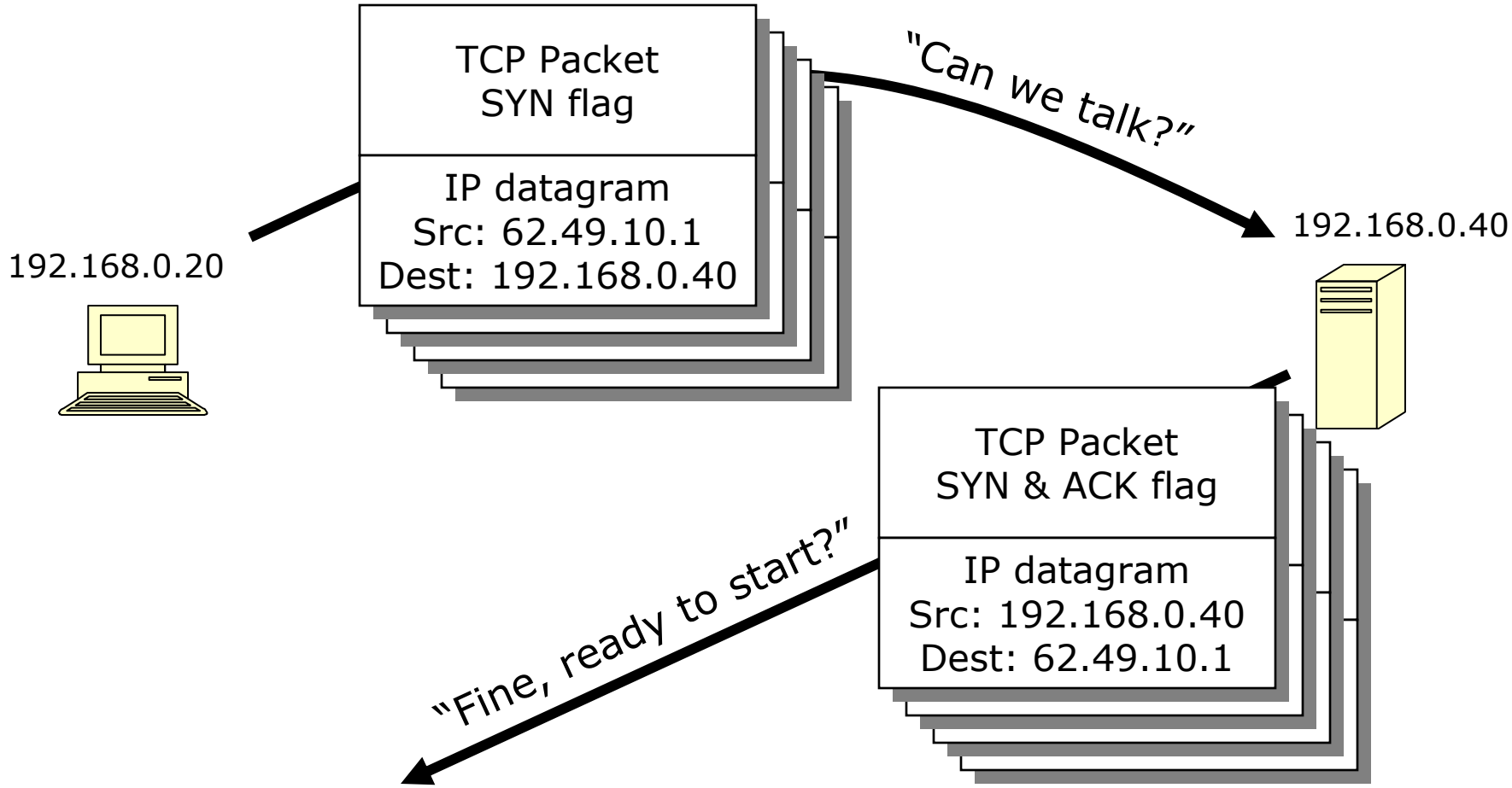
- What if the sender doesn't answer with an ACK?
  - A SYN packet from sender to receiver.
    - "Can we talk?"
  - An SYN/ACK packet from receiver to sender.
    - "Fine – ready to start?"
  - ……..nothing……..……
- If the sender sends 100 SYN packets per second
  - Eventually receiver runs out of memory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

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

TCP Denial of Service



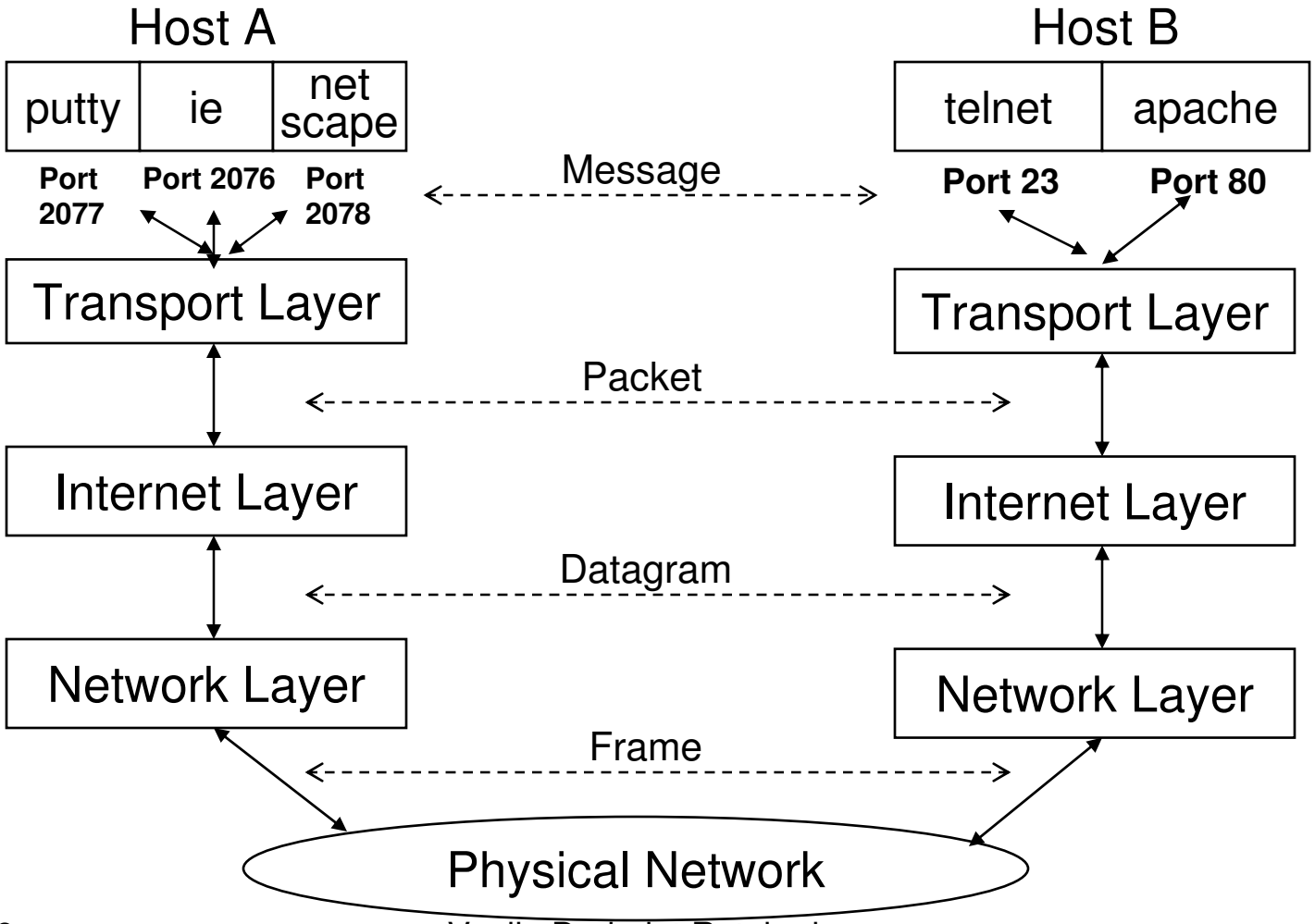
TCP/IP Ports

- Many processes on a single machine may be waiting for network traffic.
- When a packet arrives, how does the transport layer know which process it is for?
- The port allows the transport layer to deliver the packet to the application layer.
- TCP packets have source and destination ports.
  - Source port is used by receiver as destination of replies.

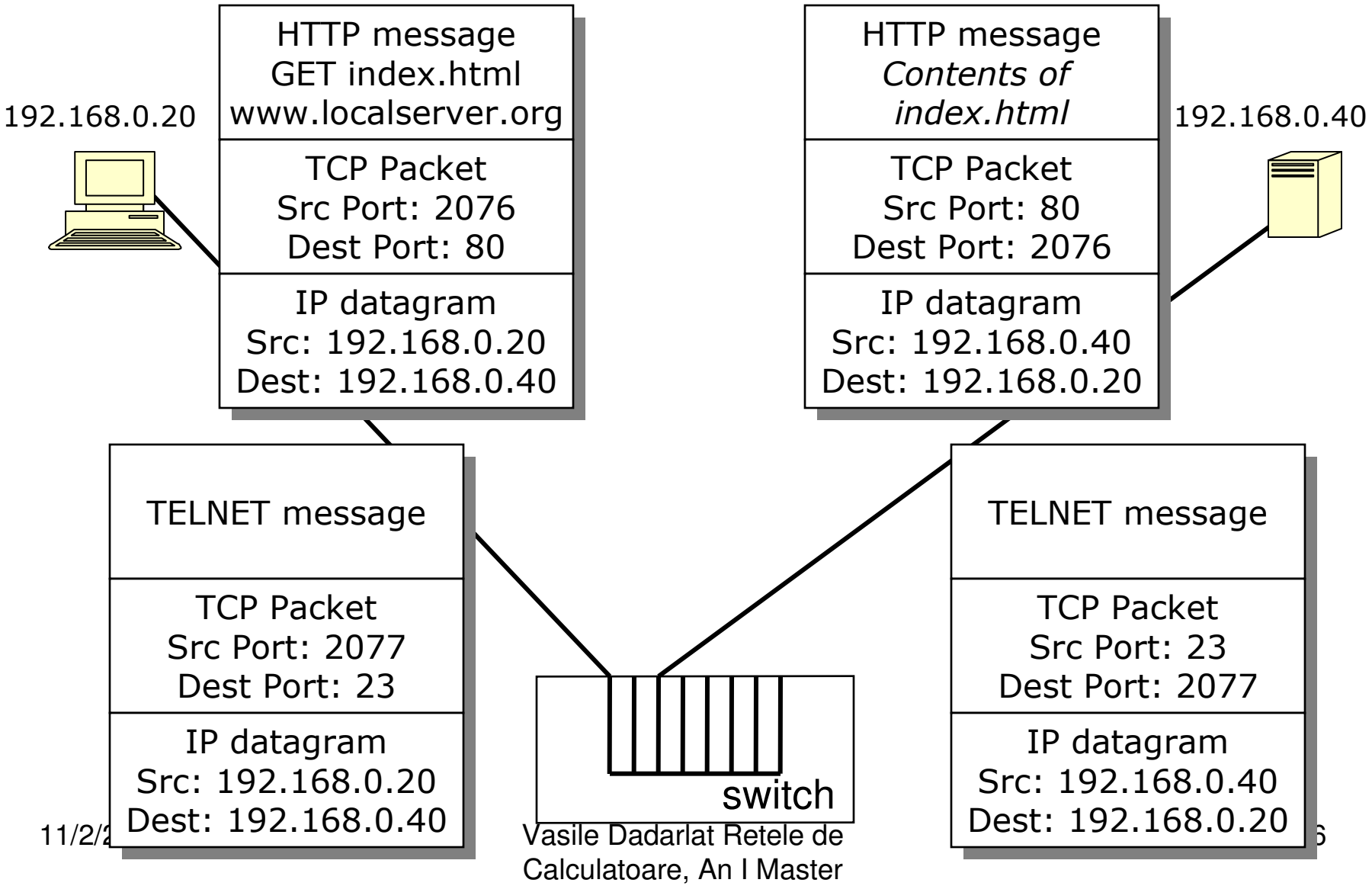
Port Assignments

- Well known ports from 0 to 1023
  - http=port 80
  - smtp=port 25
  - syslog=port 514
  - telnet=23
  - ssh=22
  - ftp=21 + more…
- Registered ports from 1024 to 49151
- Dynamic or private ports from 49152 to 65535

Port Multiplexing



Ports in Action

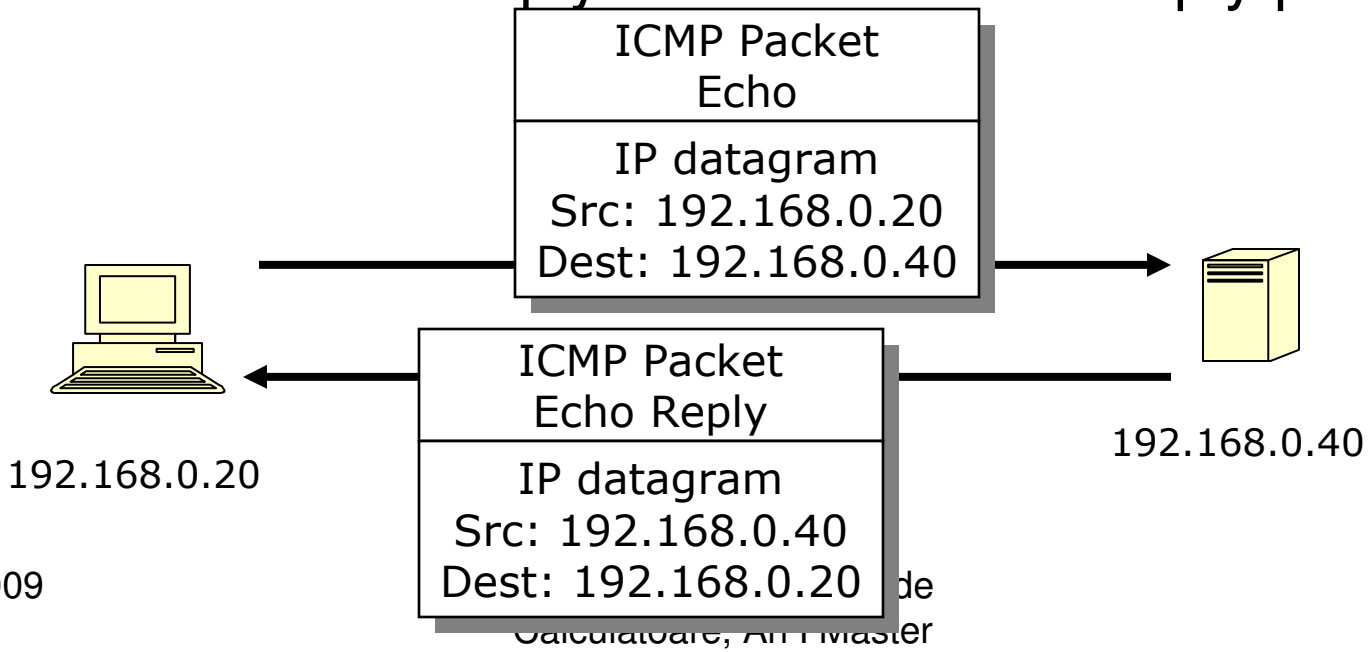


Broadcast Addressing

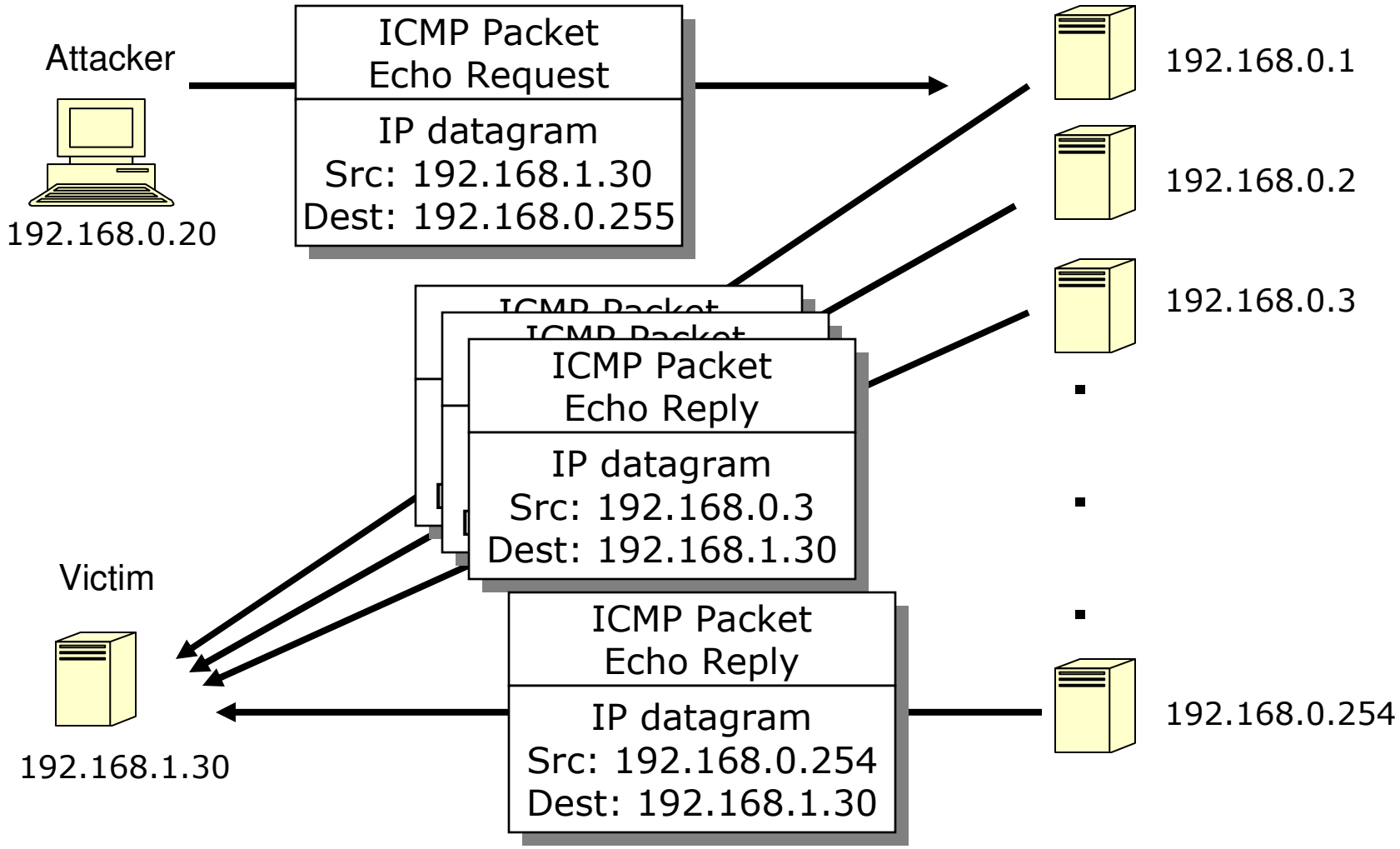
- Broadcast IP addresses:
  - Any packet with destination IP address ending .255 in a network with network mask 255.255.255.0 gets sent to *all* hosts on that network.
  - Similarly for other sizes of networks.
  - A handy feature for network management, fault diagnosis and some applications.
  - Security?

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 ‘SMURF’ Denial of Service



Safeguards

- TCP Denial of Service is hard to defend against
- Even more virulent: Distributed Denial of Service (DDoS).
  - attacker launches from many hosts simultaneously.
- Aggressively age incomplete TCP connections?
- Use firewall/IDS/IPS to detect attack in progress.
- Use relationship with IP service provider to investigate and shut down DoS traffic.
- SMURF: drop most external ICMP traffic at boundary firewall.
  - There are other good reasons to do this: ICMP can be used as tool by hacker to investigate your network…

Network Security

Network Types

Objectives of Lecture

- Examine the major different types of networks, in increasing order of size and complexity: LANs, MANs, WANs, Internet.
- Understand additional security threats for each network type.
- Look at some possible safeguards for each network type.

Local Area Networks

- Local Area Networks (LANs) used within limited areas (e.g. a building) as opposed to MANs and WANs.
- Workgroup LAN:
  - '*An identifiable grouping of computer and networking resources which may be treated as a single entity*.'
  - The basic building block of larger networks.
  - Large networks typically consist of interconnected workgroup LANs.
  - Security of workgroup LAN an essential component of the overall network security in an organisation.

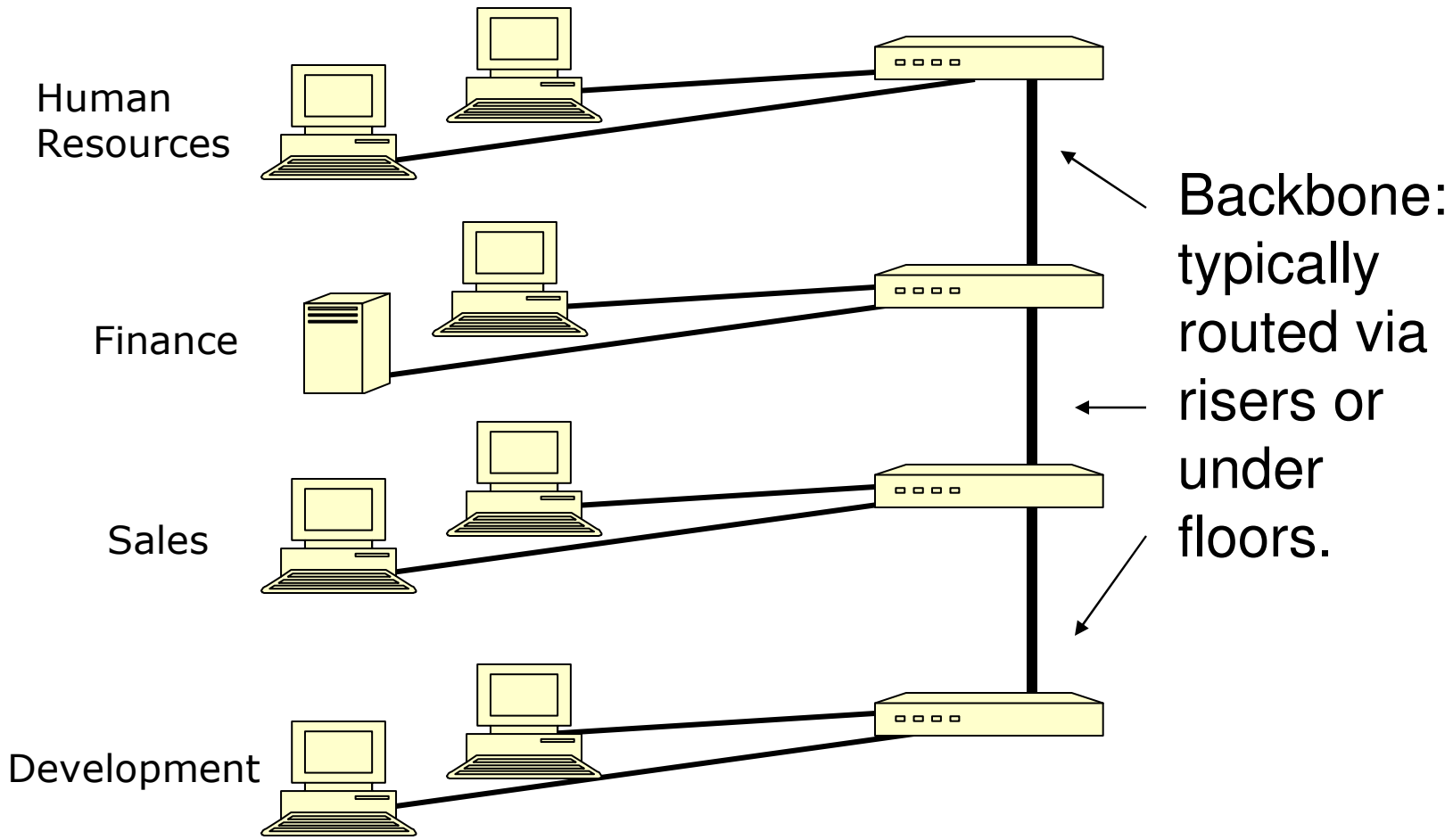
LAN Threats

- We have already seen several threats pertinent to LANs:
  - Deficiencies of Thin Ethernet and Hubs: broadcast data.
  - Layer 1 threats: who has access to cabling, broadcast wireless signals?
  - Layer 2 threats: ARP spoofing, MAC flooding of switches.
  - Layer 3: IP spoofing.
  - Layer 4 threats: TCP flooding, ICMP SMURF.
  - Sniffing.

Networks at the building level

- New security issues:
  - Failures and attacks on the backbone which connects multiple workgroup LANs.
  - Failures and attacks on the interconnections between the LAN and the backbone.
  - Control of information flow within a larger network.
- Network management also becomes an issue:
    - Fault diagnosis for cabling and devices,
    - Performance measurement,
    - Cable management systems.
    - Security of network management systems and protocols discussed later

Backbone


Human Resources
Finance
Sales
Development
Backbone: typically routed via risers or under floors.

Network Backbone Threats – 1

Overview of threats:

- Backbone carries all inter-LAN traffic.
- Confidentiality:
  - All data could be eavesdropped.
- Integrity:
  - Any corruption of data could affect all the network traffic.
- Availability:
  - Loss of backbone means that workgroups would be unable to communicate with each other.

Network Backbone Threats – 2

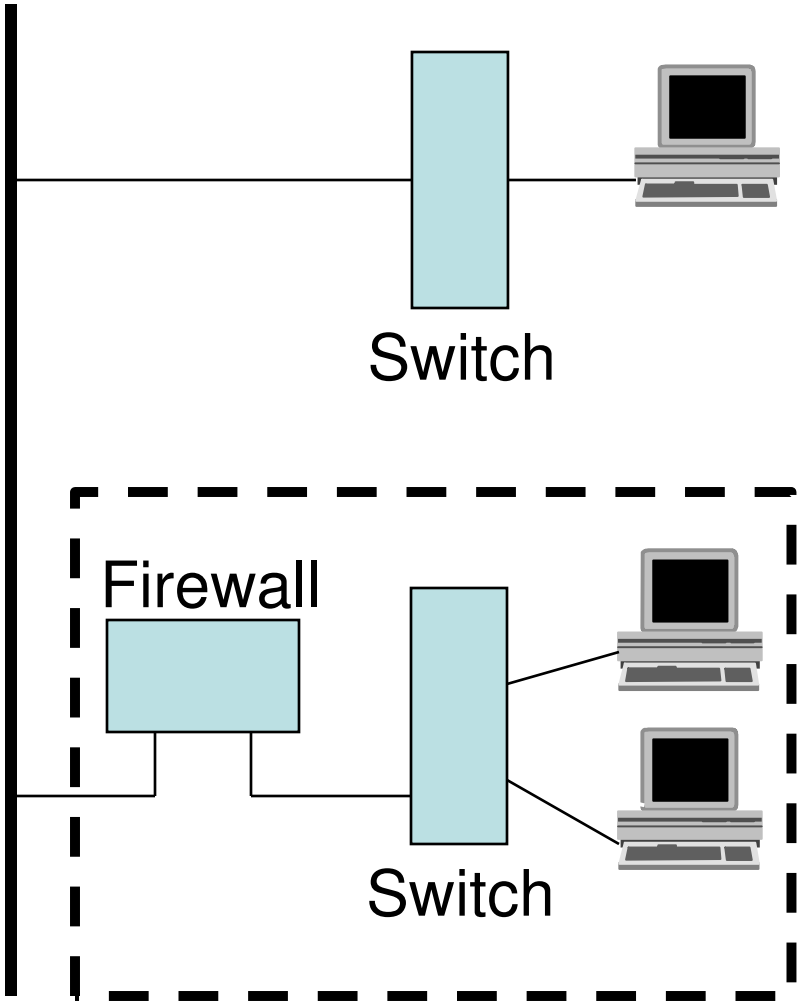
- Point of interconnection between workgroup and backbone is a particularly sensitive area.
- From security viewpoint it:
  - Provides a point of access to the backbone.
  - Provides a point of access to all the data associated with a workgroup.
- Damage at this point could affect both the workgroup and the backbone.

LAN Safeguards – 1

- Partitioning
  - With a building network there will be different types of information being processed.
  - Some types of data will require extra protection, e.g.
    - Finance
    - Personnel / Human Resources
    - Internal Audit
    - Divisional heads
  - Partitioning is a basic technique to control the flow of data and, through this, increase security.

LAN Safeguards – 2

- Partitioning
  - Network configured so that:
    - Group of workstations cabled to their own switch.
    - Switch programmed to force data flowing onto the backbone to go via a router which can control that flow.
  - Add a Firewall
    - Control all traffic to and from hosts behind firewall.
    - Firewalls covered in detail later.



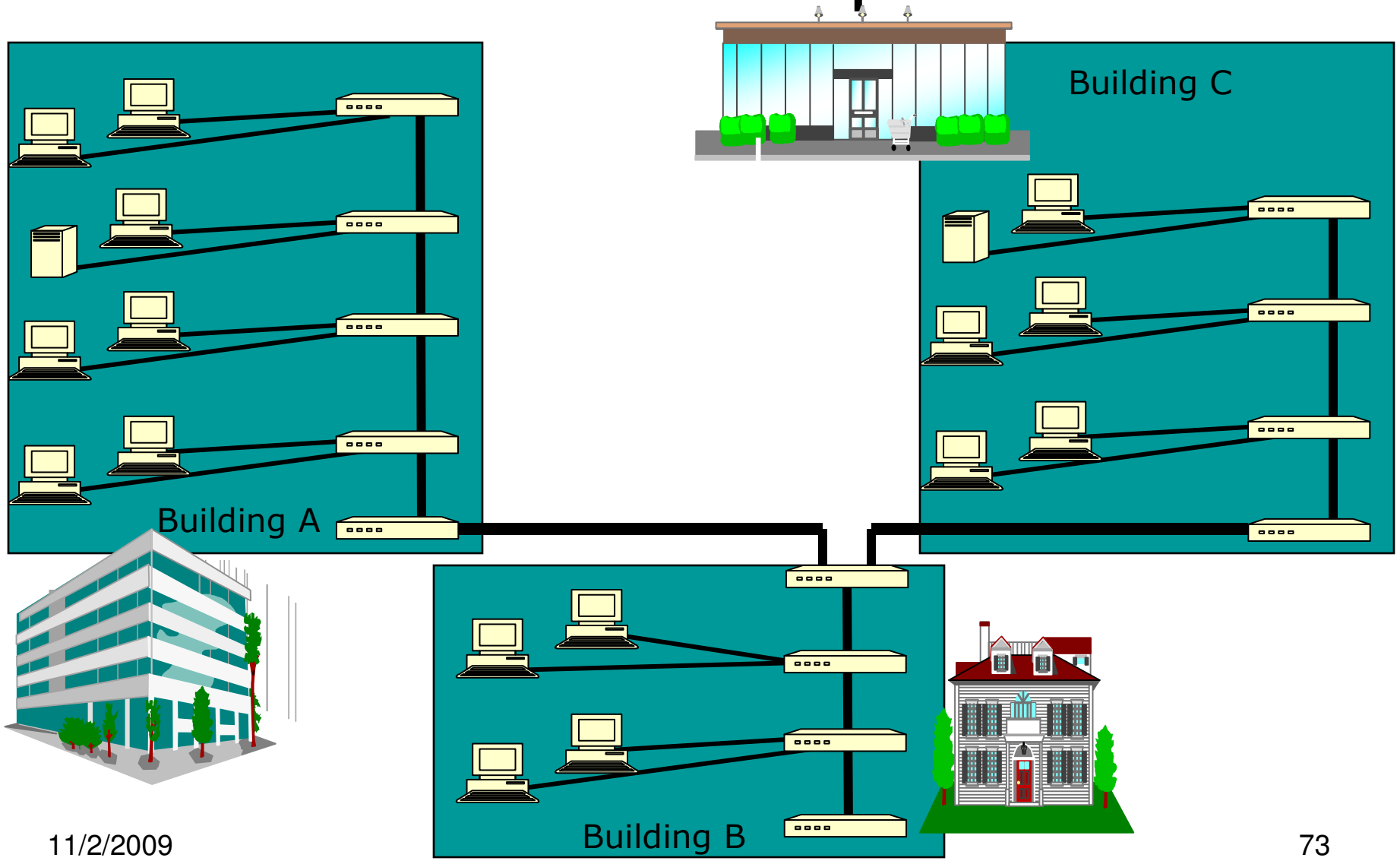
LAN Safeguards – 3

- If workgroup users are not located in a single area but need to communicate, then different measures must be adopted.
- Flow controls in switches and firewalls can be used to control traffic flow, but these do not prevent traffic being read in transit.
- Higher level of security can be provided by encryption, but:
  - What is the performance impact of encryption?
  - How are encryption keys generated, distributed, and stored?
  - Will a workstation in the encrypted workgroup be able to communicate with an unencrypted server?

MANs

- Metropolitan Area Network.
- New Environment
  - A network which encompasses several closely located buildings (sometimes also called a campus network).
- Such expanded network environments bring additional security concerns:
  - Network has left the physical security of the building and is exposed to outside world.
  - Problems of scale.

MAN example



MAN Threats

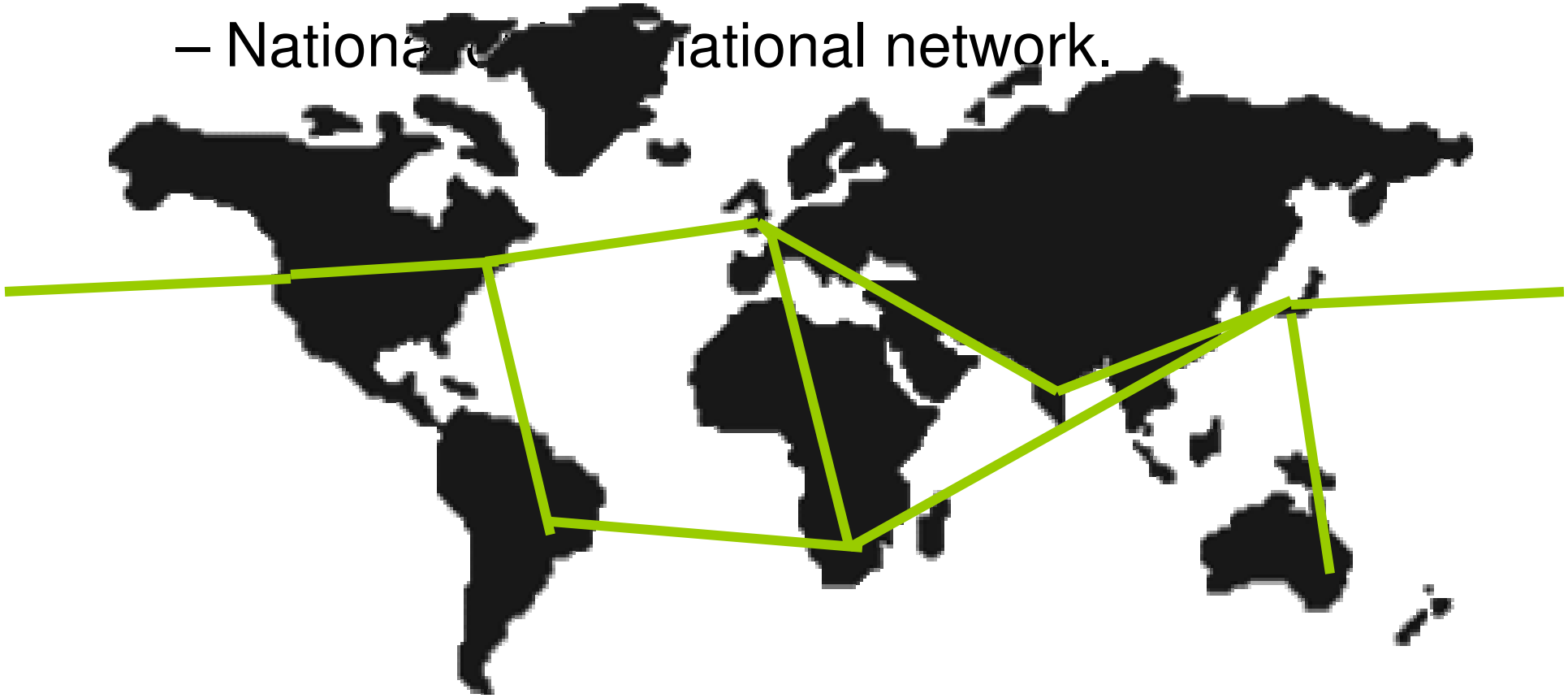
- Exposure to outside world:
  - Network has left the security of the building.
  - Small scale may rule out encryption.
  - New risks must be assessed:
    - Private campus or network crossing public areas?
    - Links to business partners? What are there security policies? Who are their staff?
    - Dial-up access for remote users?
  - Investigate constraints on solution:
    - e.g. buried or elevated links.
  - May need non-physical links:
    - e.g. laser, infra-red, microwave, wireless.

MAN Threats

- Problem of scale
  - Information flow must be controlled, and faulty network components (in one building) must not affect other buildings.
  - Network Information Centre (NIC) may be required.
  - Specialized network management tools become essential (manual approach no longer feasible).
    - Possibility for greater integration – cable management systems, device location maps, server disk space monitoring, printer status,…
  - Normally a second level backbone is used.

2.7 WANs

- Wide Area Network
  - Nationa[illegible]national network.



WAN Threats

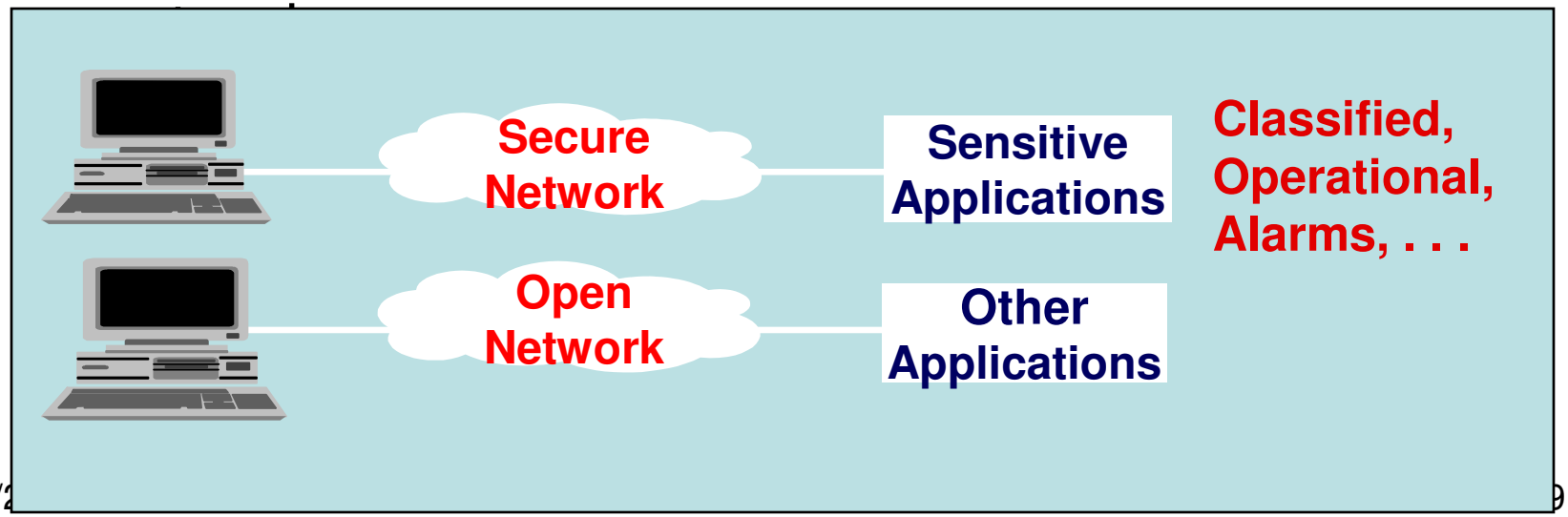
- Threats become more significant:
  - Sensitive data (including passwords) much more widely transmitted.
  - Greater organizational distances.
  - Control may be more distributed.
  - Outsourcing of network infrastructure to 3rd parties, sharing of infrastructure with other customers.
  - Likely to be unstaffed equipment rooms that are managed remotely.
  - More changes, hence greater risk of change management errors.

Choice of Media for WANs

- Impact of different media on confidentiality:
  - Fibre:
    - Minimal external radiation,
    - Special equipment required for tapping,
    - Normally a tap causes disruption of service.
  - Satellite, radio or microwave:
    - Extensive external radiation,
    - Special (but easily available) equipment needed for tapping,
    - Tapping does not disrupt services,
    - Carrier might provide some encryption.

WAN Partitioning – 1

- Partitioning of networks using physical separation:
  - Provides perfect separation and conceptually simple.
  - Legacy approach - in the days when adequate logical separation was not possible, still done in very secure



WAN Partitioning – 2

- Partitioning of networks using logical separation:
  - Closed User Groups:
    - Multiple virtual networks on one physical network.
    - Separation based on network addresses.
    - Managed by the Network Management Centre.
    - Achieved using Permanent Virtual Circuits (PVCs) or cryptography.
    - May have to rely on separation and security provided by 3rd party WAN service provider.
  - Encryption

Data confidentiality in WANs

- Can provide data confidentiality (and hence logical partitioning) in WANs using encryption.
- Encryption options and issues:
  - Link encryption
    - Security at physical/datalink layers (layers 1 and 2).
    - Covers data on only one network link, while many hops may be involved in end-to-end communications.
    - Covers all traffic on that link, no matter what protocol.
  - End-to-end security
    - Can be provided at layers 3, 4: e.g. IPSec, SSL
    - Or at layer 7 (application): e.g. SSH, secure e-mail,…
    - No longer protocol independent.

Link Encryption

- Link encryption:
  - Offers data confidentiality for individual links,
  - Protocol independent (operates at layer 1/2),
  - Throughput is not normally an issue,
  - Moderate cost (£700-£1000 per unit).
- But link encryption for larger networks has problems:
  - Expense,
  - Management burden,
  - Does not scale well to large distributed networks,
  - Data may not be protected at intermediate sites, in switches, etc.

The Internet

- The Internet evolved out of a US Government funded network (ARPANET).
- Essentially a large collection of internetworked networks, with IP addressing as the ``glue''.
- Developed in parallel with OSI so some conflict between standards.
- Has its own protocols at layers 3 and 4: TCP (layer 4) and IP (layer 3).
- Has pushed OSI out (de facto beats de jure).
- 250 million registered domains, trillions of users
- Internet communities, as: http://www.isc.org/
- IETF: Internet Engineering Task Force, www.ietf.org
- RFC: Request For Comments – IETF standards.

The Internet

- Internet presence and connection a prerequisite for most corporations.
- Web browsing, email, file sharing and transfer, e-commerce, b2b commerce, e-government….
- Increasingly used for business critical applications.
- Possible to replace expensive WAN link with Internet virtual private network (VPN) link.
- Threats become critical
  - Route taken by sensitive data not guaranteed
  - Availability not guaranteed
    - Denial of service attacks are real risk
  - Any Internet host can probe any other host
  - Plenty of malicious code and activity (viruses, worms, trojans)

Some Internet Safeguards

- Firewalls to filter IP traffic, Intrusion Detection Systems to detect penetrations.
- De-Militarized Zones to isolate Internet-facing machines from internal networks.
- Content filters to filter email & web traffic content.
- VPNs to protect critical data routed over public Internet.
- Non-technical safeguards: policy, conditions of use for employees, sanctions.