Technische Universität Braunschweig

IAS | INSTITUTE FOR APPLICATION SECURITY

Network Attacks and Defenses

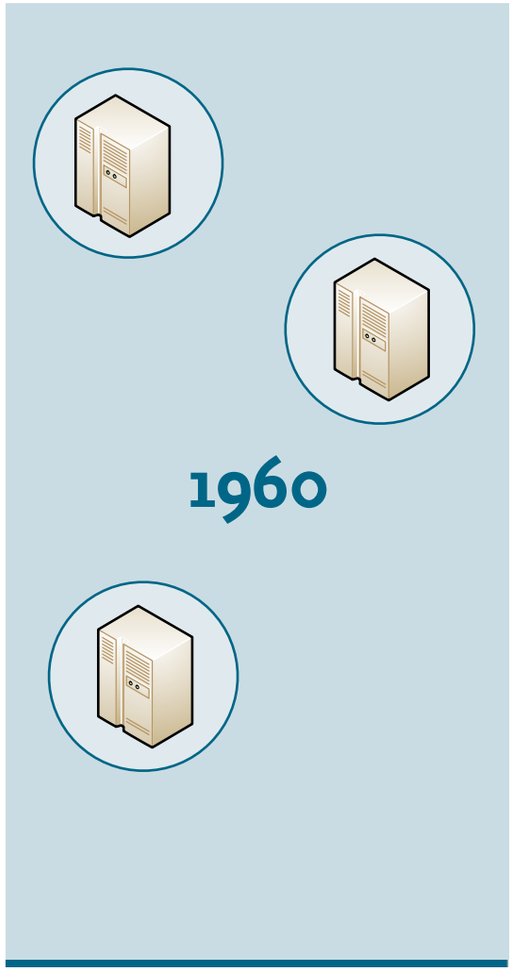
Vorlesung “Einführung in die IT-Sicherheit”

Prof. Dr. Martin Johns

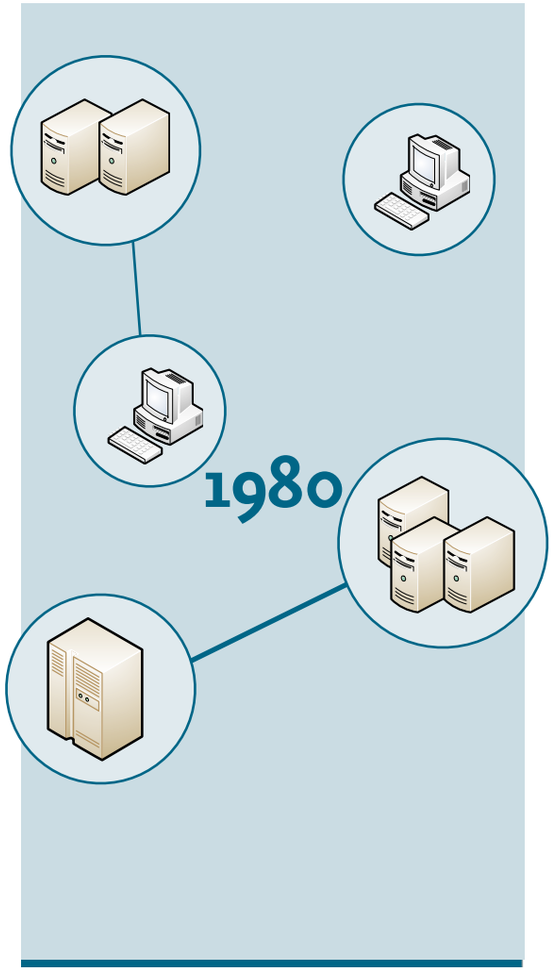
Overview

- **Topic of the unit**
  - Network Attacks and Defenses
- **Parts of the unit**
  - Part #1: Layered communication models
  - Part #2: Classic network attacks
  - Part #3: Network defenses

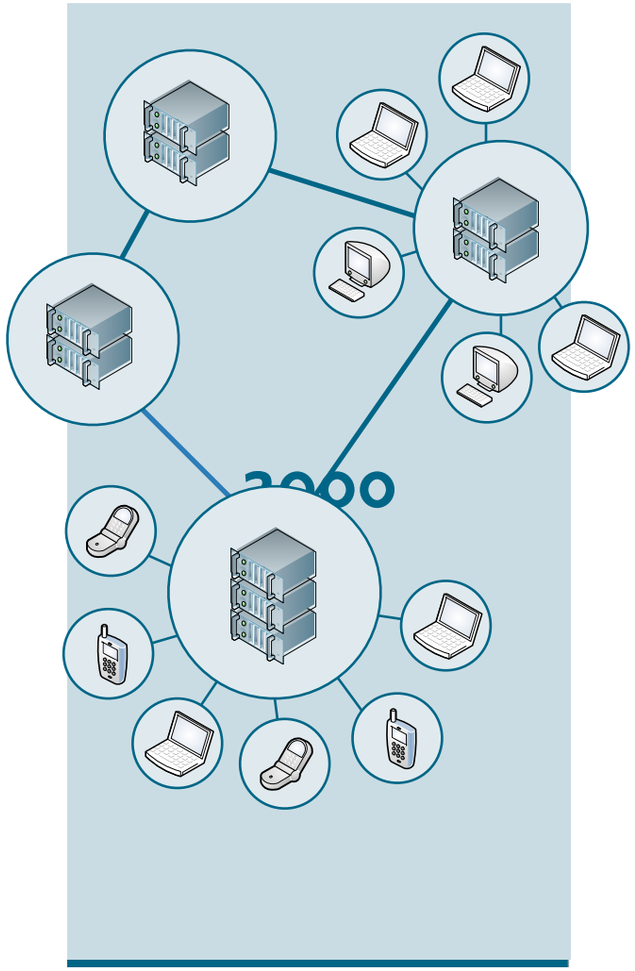
History of Computer Networks



First computers
(Mainframes)



Local networks &
personal computers



Global network
(Internet)

Security and Networks

- **Negative impact of networks on computer security**
  - Isolated system Networked systems
    - Physical access → Network access
    - Dozens of users → Thousands of hosts
    - Central resources → Distributed resources
    - Easy accountability → Hard accountability
- **Rapid growths of networks in last two decades**
  - Security failed to keep pace with development

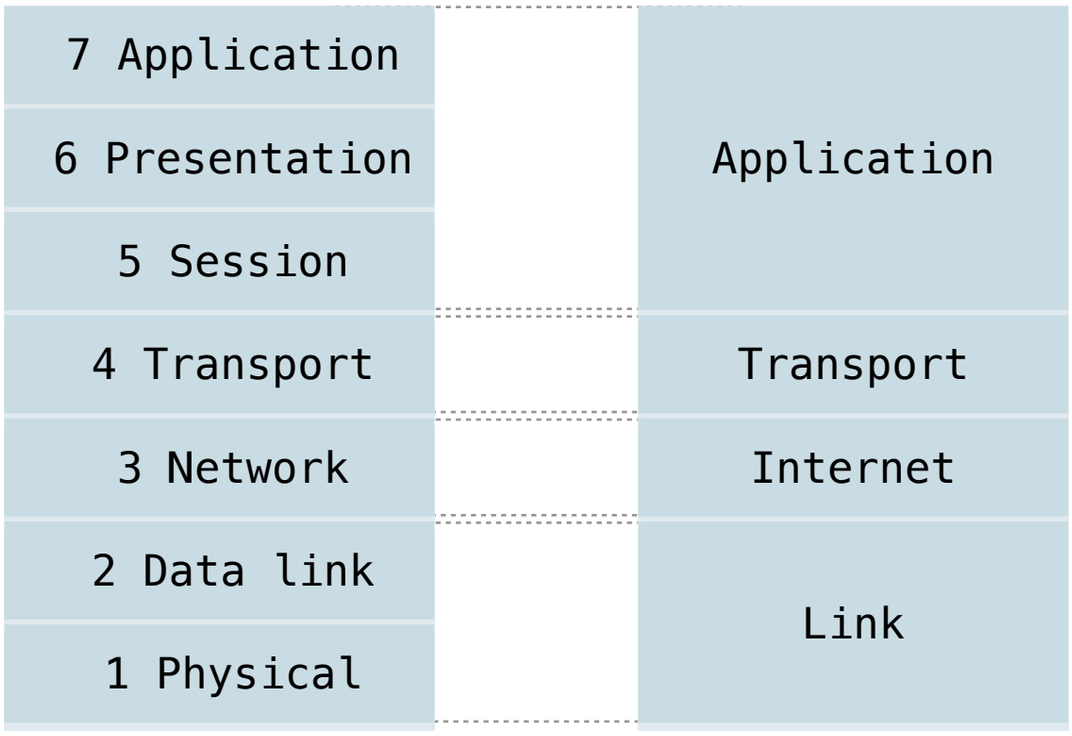
Layers of Communication

- **Communication organized in independent layers**
  - Encapsulation of concepts, e.g. addressing and transport
  - Lower layers transparent to higher layers

Theory-driven model:

OSI model

(ISO, 1983)



Practice-driven model:

TCP/IP model

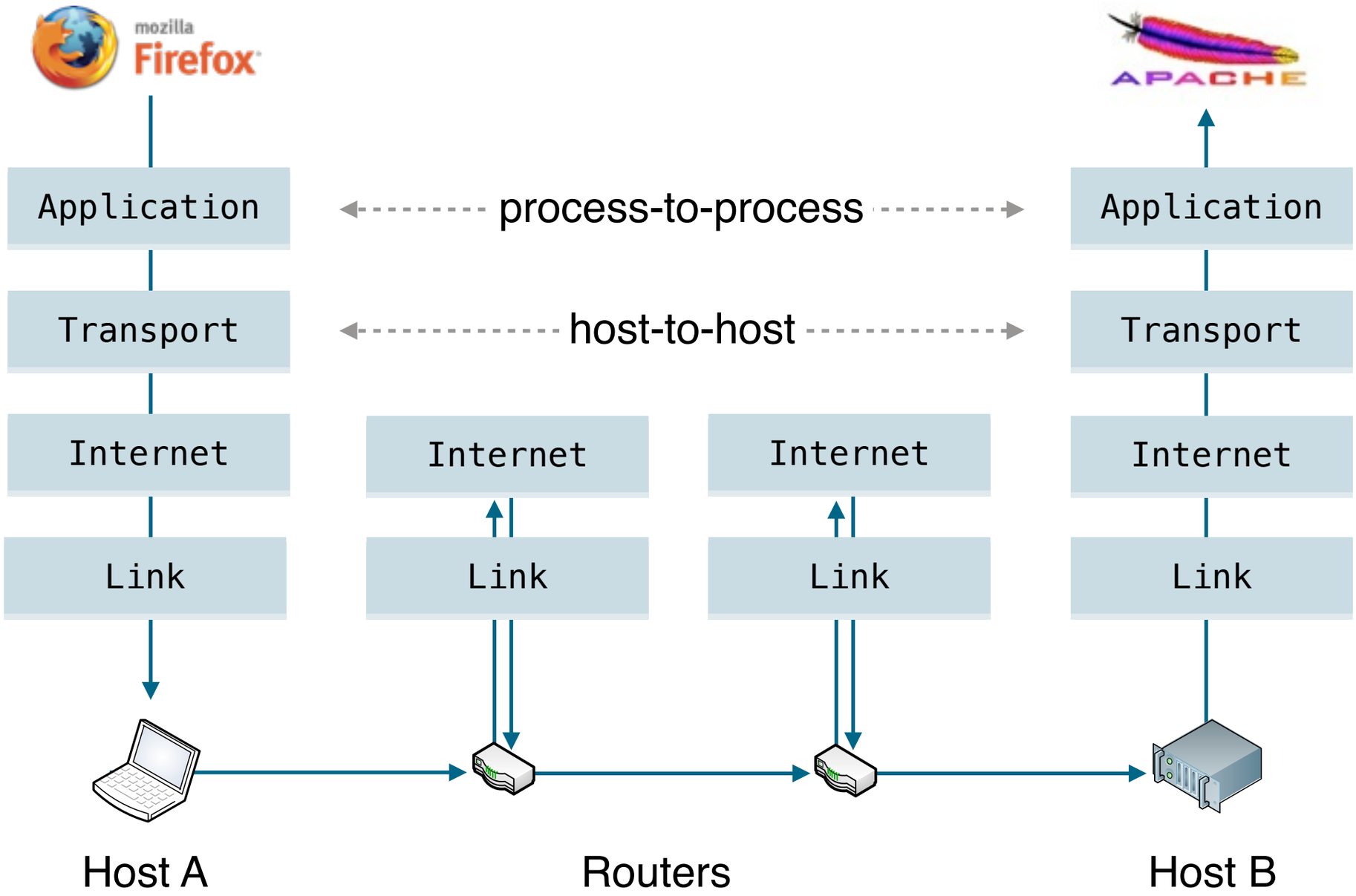
(DARPA ~70s)

The TCP/IP Model

- **Layer model underlying the Internet Protocol Suite**
  - Foundation of the Internet and its protocols

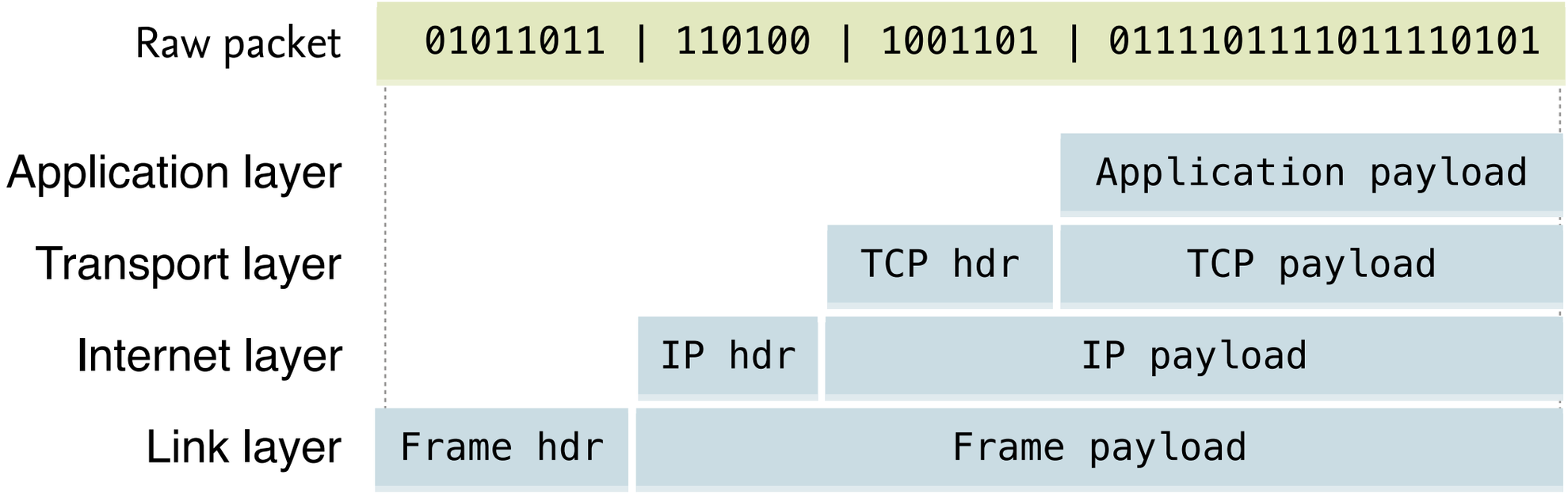
Layers	Functions	Examples
Application	Interfacing with network applications	HTTP, FTP
Transport	Delivery and multiplexing of data to network applications	TCP, UDP
Internet	Addressing and transfer of data	IP, ICMP
Link	Interfacing with and control of physical devices	PPP, ARP

TCP/IP Data Flow

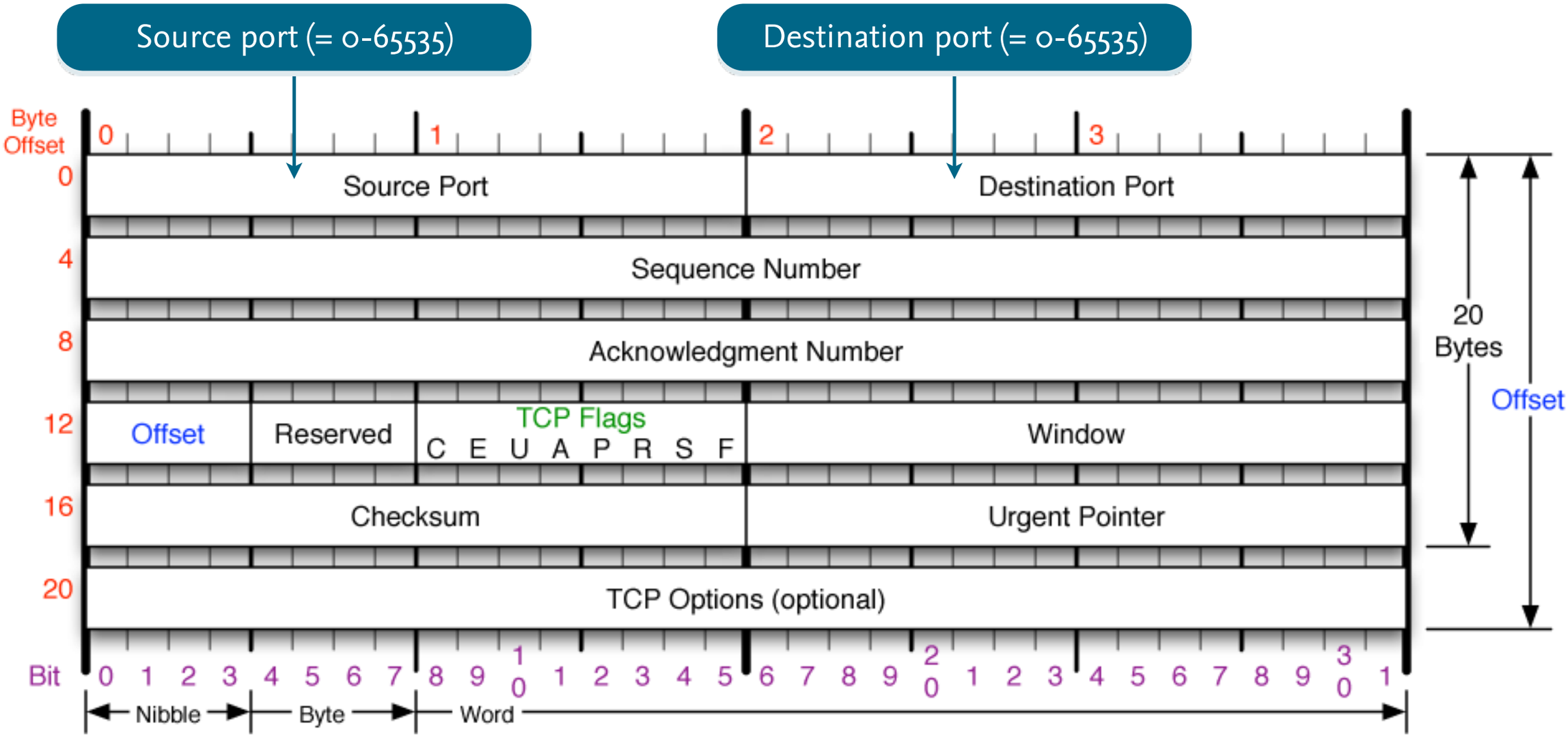


Network Packets

- **Computer networks** = packet-switched networks
  - Several advantages over circuit-switched networks
  - Packets structured by communication layers
  - Grouping of control (header) and payload data



Example: **TCP Header**



Example ports: 22 (ssh), 80 (http), 443 (https), …

(Figure by Matt Baxter)

Overview

- **Topic of the unit**
  - Network Attacks and Defenses
- **Parts of the unit**
  - Part #1: Layered communication models
  - Part #2: Classic network attacks
  - Part #3: Network defenses

Network Attacks

- **Network attacks**
  - Available at all layers of communication
  - Impact on confidentiality, integrity and availability
- **Root causes of attacks**
  - Failures in protocol and network design
  - Vulnerabilities in implementations
  - Misconfiguration of network services
  - Incorrect operation of network services

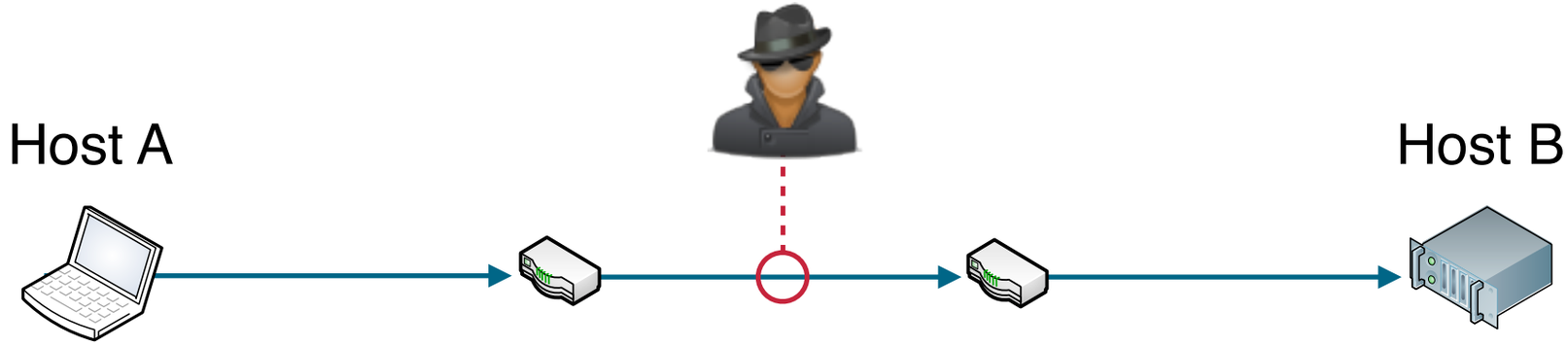
Classic Attacks

- **Classic network attacks** (oldschool)
  - Spoofing = network messages with spoofed data
  - Hijacking = takeover of connections and sessions
  - Flooding = (distributed) denial-of-service attack

- **Let's look at three examples**
  - Network sniffing (all layers)
  - ARP spoofing (Link layer)
  - Smurf attacks (Internet layer)

All Layers: **Sniffing**

- **Network sniffing** = eavesdropping of network packets
  - Physical access to communication media (wire, air, ...)
  - Passive and unnoticeable eavesdropping on route
  - Automatic parsing of protocols in packets



- Impact: Not really an attack. Mainly affects confidentiality

All Layers: **Sniffing**

Wireshark

Thunderbolt Ethernet: en5

Apply a display filter ... <⌘/> Expression... +

No.	Time	Source	Destination	Protocol	Length
145	10.594733	134.169.109.144	62.138.116.25	TCP	
146	10.605322	62.138.116.25	134.169.109.144	TCP	
147	10.605385	134.169.109.144	62.138.116.25	TCP	
148	10.605577	134.169.109.144	62.138.116.25	HTTP	
149	10.616180	62.138.116.25	134.169.109.144	TCP	
150	10.616371	62.138.116.25	134.169.109.144	TCP	
151	10.616442	62.138.116.25	134.169.109.144	TCP	
152	10.616443	62.138.116.25	134.169.109.144	TCP	

```
▶ Frame 150: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on
▶ Ethernet II, Src: CiscoInc_58:16:40 (00:23:04:58:16:40), Dst: Apple_2d:08:11 (a
▶ Internet Protocol Version 4, Src: 62.138.116.25, Dst: 134.169.109.144
▶ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 65203 (65203), Seq:
```

```
0000  ac 87 a3 2d 08 11 00 23  04 58 16 40 08 00 45 00   ...-...# .X.@..E.
0010  05 8c 53 e8 40 00 39 06  41 a7 3e 8a 74 19 86 a9   ..S.@.9. A.>.t...
0020  6d 90 00 50 fe b3 d8 16  4b 5b ff 8f 84 74 80 10   m..P.... K[...t..
0030  00 7b f5 92 00 00 01 01  08 0a 35 f5 30 03 3e 6a   .{...... ..5.0.>j
0040  e0 32 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f   .2HTTP/1 .1 200 O
0050  4b 0d 0a 44 61 74 65 3a  20 54 68 75 2c 20 31 35   K..Date:  Thu, 15
0060  20 53 65 70 20 32 30 31  36 20 31 35 3a 34 39 3a    Sep 201 6 15:49:
0070  32 36 20 47 4d 54 0d 0a  43 61 63 68 65 2d 43 6f   26 GMT.. Cache-Co
0080  6e 74 72 6f 6c 3a 20 6d  61 78 2d 61 67 65 3d 34   ntrol: m ax-age=4
0090  35 0d 0a 45 78 70 69 72  65 73 3a 20 54 68 75 2c   5..Expir es: Thu,
00a0  20 31 35 20 53 65 70 20  32 30 31 36 20 31 35 3a    15 Sep  2016 15:
00b0  35 30 3a 31 32 20 47 4d  54 0d 0a 58 2d 53 50 2d   50:12 GM T..X-SP-
00c0  54 45 3a 20 36 31 35 34  0d 0a 58 2d 52 6f 62 6f   TE: 6154 ..X-Robo
00d0  74 73 2d 54 61 67 3a 20  69 6e 64 65 78 2c 20 66   ts-Tag:  index, f
00e0  6f 6c 6c 6f 77 2c 20 6e  6f 61 72 63 68 69 76 65   ollow, n oarchive
00f0  2c 20 6e 6f 6f 64 70 0d  0a 43 6f 6e 74 65 6e 74   , noodp. .Content
0100  2d 54 79 70 65 3a 20 74  65 78 74 2f 68 74 6d 6c   -Type: t ext/html
```

wireshark_pcapng_en5_20160915174925_oRz3kH Packets: 2414 · Displaye

Wireshark · Follow TCP Stream (tcp.stream eq 3) · wireshark_pcapng_en5_20...

```
GET / HTTP/1.1
Host: www.spiegel.de
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/53.0.2785.116
Safari/537.36
Accept: text/html,application/xhtml+xml,application/
xml;q=0.9,image/webp,*/*;q=0.8
DNT: 1
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,de;q=0.6
Cookie: sponVideoplayerQuality=hq; _540p=a063ccb1-15c7-444d-bdbc-
c77d0c4b2e83; spiegelsans=1; fontawesome=1; misobold=1;
spiegelserif=1; spVcData2=9-47%3B46-60; jwplayer.captionLabel=Off

HTTP/1.1 200 OK
Date: Thu, 15 Sep 2016 15:49:26 GMT
Cache-Control: max-age=45
Expires: Thu, 15 Sep 2016 15:50:12 GMT
X-SP-TE: 6154
X-Robots-Tag: index, follow, noarchive, noodp
Content-Type: text/html;charset=UTF-8
X-SP-AP: 6129
Content-Encoding: gzip
```

5 client pkt(s), 44 server pkt(s), 9 turns.

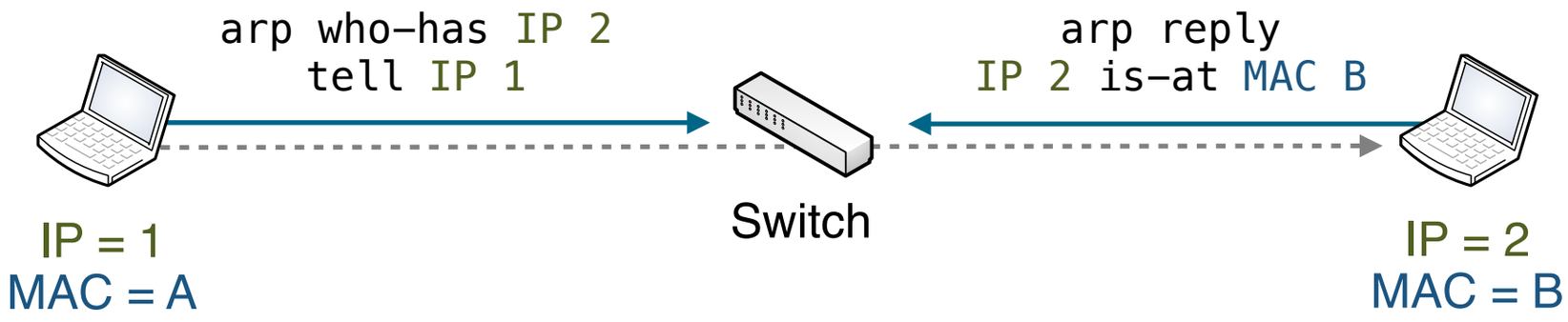
Entire conversation (58 kB) Show data as ASCII Stream 3

Find: Find Next

Help Hide this stream Print Save as... Close

Link Layer: **ARP Spoofing**

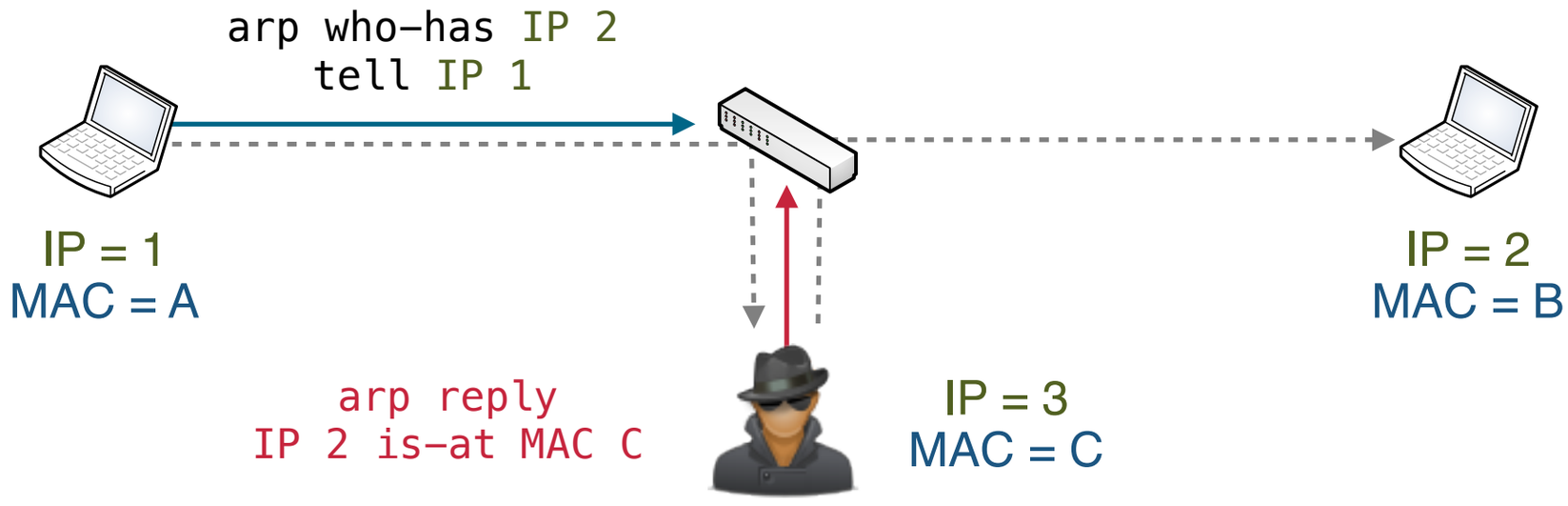
- Background: **Address Resolution Protocol (ARP)**
  - Standard link-layer protocol of Internet protocol suite
  - Mapping from logical addresses (IP) to devices (MAC)



- Map IP → MAC stored in ARP cache at hosts or switch
- Abstraction of logical addresses from network devices

Link Layer: **ARP Spoofing**

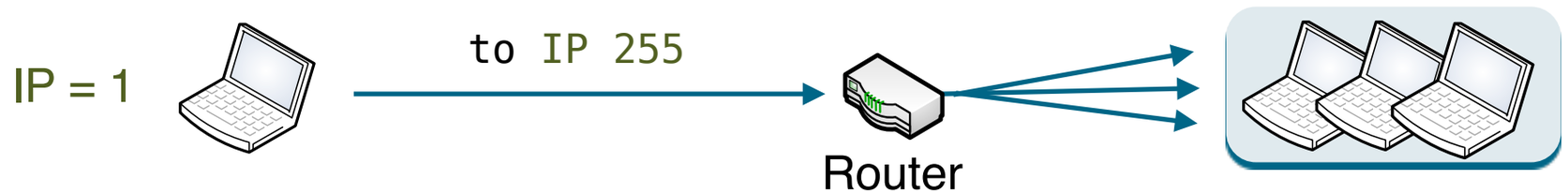
- **ARP spoofing** = ARP replies with forged IP addresses
  - ARP cache is poisoned with fake mapping
  - Victim directs traffic to attacker (man-in-the-middle attack)



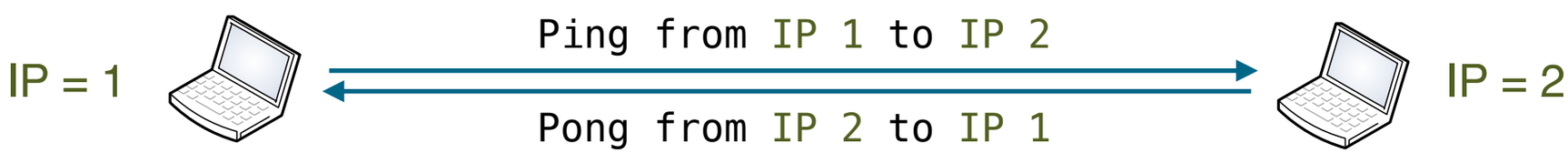
- Impact: Attack affects confidentiality and integrity

Internet Layer: **Smurf Attack**

- Background: **IP broadcast addresses**
  - Broadcasting of packets to an entire subnet
  - Destination = bit complement of address and subnet mask

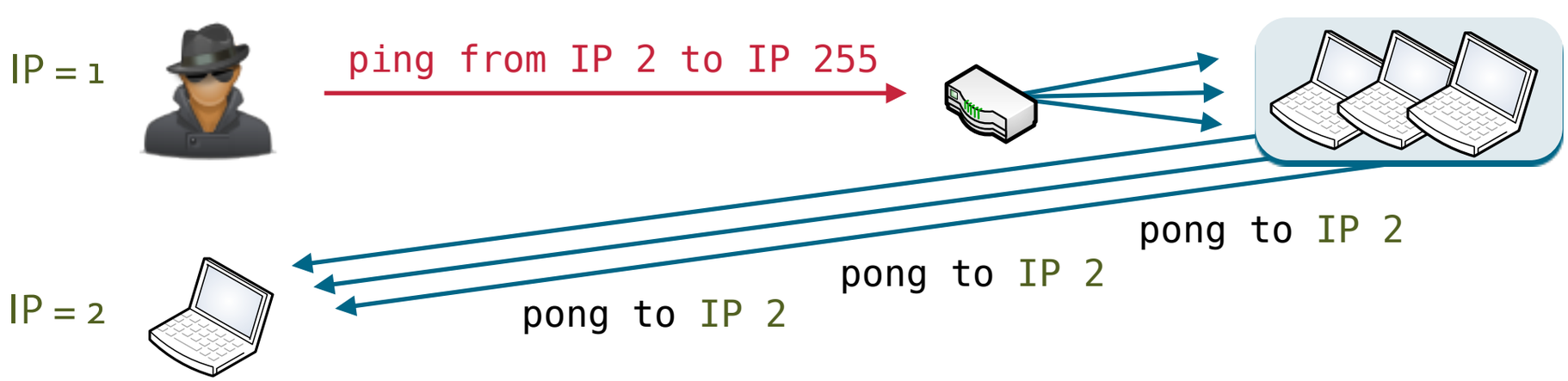


- Background: **Internet Control Messages Protocol (ICMP)**
  - Internet-layer protocol for control messages, e.g. Ping



Internet Layer: **Smurf Attack**

- **Smurf attack** = flooding with spoofed broadcast ping messages
  - Attacker spoofs source address of ICMP echo requests
  - Multiplication of replies due to IP broadcasting



- Impact: Attack affects availability of network bandwidth

Amplification Attacks

- **Amplification attacks**
  - Denial-of-service attack based on amplification of traffic
  - Asymmetry in incoming and outgoing traffic volume
  - Classic example: Smurf and Fraggle attacks
- **Modern amplification attacks**
  - NTP: Spoofed requests for last 600 hosts connecting the service
  - DNS: Spoofed requests for type “ANY” of DNS zone
  - See Rossow’s “Amplification Hell” paper (NDSS 2014)

Overview

- **Topic of the unit**
  - Network Attacks and Defenses
- **Parts of the unit**
  - Part #1: Layered communication models
  - Part #2: Classic network attacks
  - Part #3: Network defenses

Network Defenses

- **Application of basic security concepts**
  - Cryptography: encryption and verification of data
  - Authentication: (mutual) authentication of parties
  - Access control: restriction and control of communication

- **Reactive security concepts**
  - Vulnerability assessment “finding vulnerabilities”
  - Intrusion detection “finding attacks”
  - Computer forensics “finding attackers”

Cryptography in Networks

- **Network protocols with cryptographic extensions**
  - Protection of confidentiality and integrity
  - Applicable at different layers of communications
- **Symmetric-key cryptography**
  - Efficient encryption and verification of network data
  - Verification of data using hash functions
- **Public-key cryptography**
  - Exchange of session keys
  - Signing and verification of keys and data

Example: **IPSec**

- **IPSec** = Internet Protocol Security
  - Extension of IP protocol with security features
  - Protection of communication at Internet layer
  - Very versatile: host-to-host or network-to-network
- **Main features**
  - IKE: Internet Key Exchange
  - ESP: Encapsulating Security Payload
  - AH: Authentication Header
- Problems: **complexity; no end-to-end encryption**

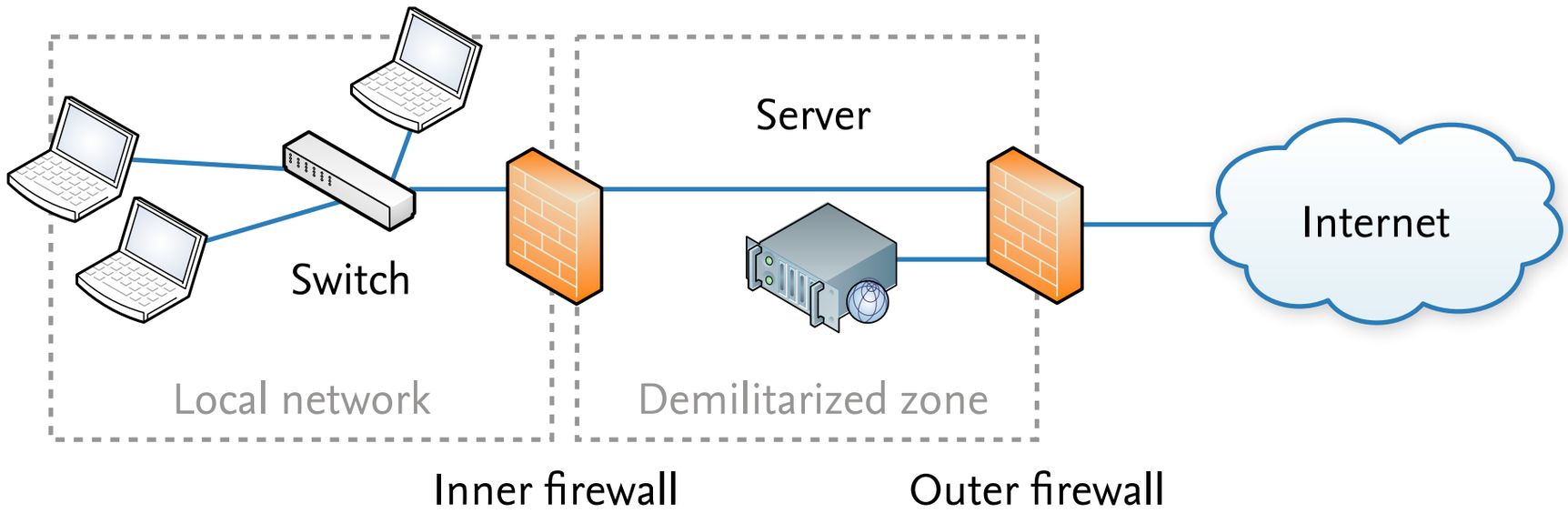
Access Control in Networks

- **Access control**
  - Often ACLs on network objects (e.g. nets, hosts, ports)
  - Applicable at different layers of communication
  - Realization using lists, rules and filters
- **Common mechanisms for access control**
  - Link layer: MAC filter
  - Internet layer: Packet filter
  - Transport layer: Packet filter
  - Application layer: Proxy and application-layer gateway

Firewall

Firewalls

- **Firewall** = a host that mediates access to a network
  - Inspection of all inbound and outbound packets
  - Access control on different communication layers
  - Semantics-aware protocol analysis (states, re-assembly)
  - Partitioning of network segments (e.g. DMZ)

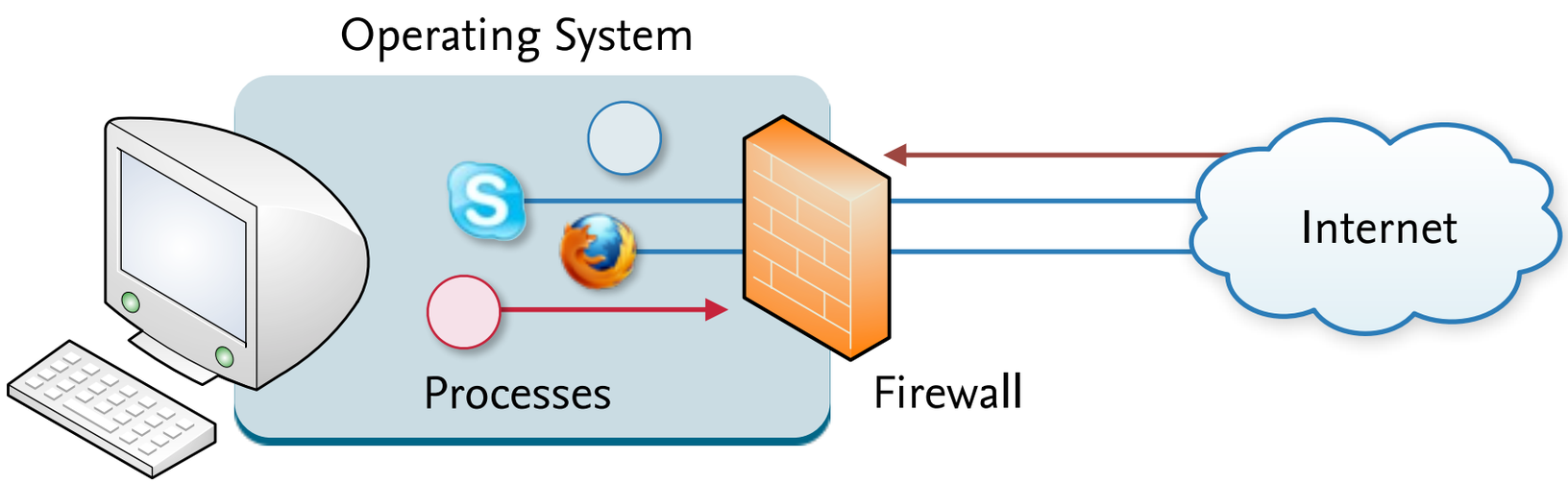


Firewalls

- **Protection of network services from inbound traffic**
  - Example: web server (HTTP) accessible to everybody
    file server (SMB) restricted to local network
- **Filtering of outbound traffic from network hosts**
  - Example: shell connections allowed to other hosts (SSH)
    chat services (ICQ, AIM) blocked by firewall
- **Design and operation of firewall rules non-trivial**
  - Common pitfalls: blocking of legitimate traffic
  - Filtering often only possible on application layer (e.g. Skype)

Desktop Firewall

- **Desktop firewall** = host-based variant of regular firewall
  - Blocks unwanted incoming network traffic
  - Alerts user about outgoing network traffic
  - Monitors applications that are listening for traffic
  - Drawback: Effectivity depends on security of host



Attacks vs. Defense

- **Arms race between attackers and defenses**
  - Cryptographic extensions stop sniffing and hijacking
  - Firewalls limit several classic attacks, e.g. spoofing
- **One hole fixed; another one opened**
  - Vulnerabilities in security systems, e.g. firewalls
- **Constant evolution of attack techniques**
  - Move to application-layer protocols and beyond
  - Move from server-based to client-based attacks

Summary

Summary

- **“The network is the computer”** - John Gage
  - Communication in different layers
  - Relevant to security due to global linkage
- **Network attacks and defenses**
  - Attacks at all communication layers
  - Defenses at all layers — but no silver bullet
  - Security needs to be part of network design