

Lecture 10

Network Security I

Information &
Communications Security
(WS 2008)

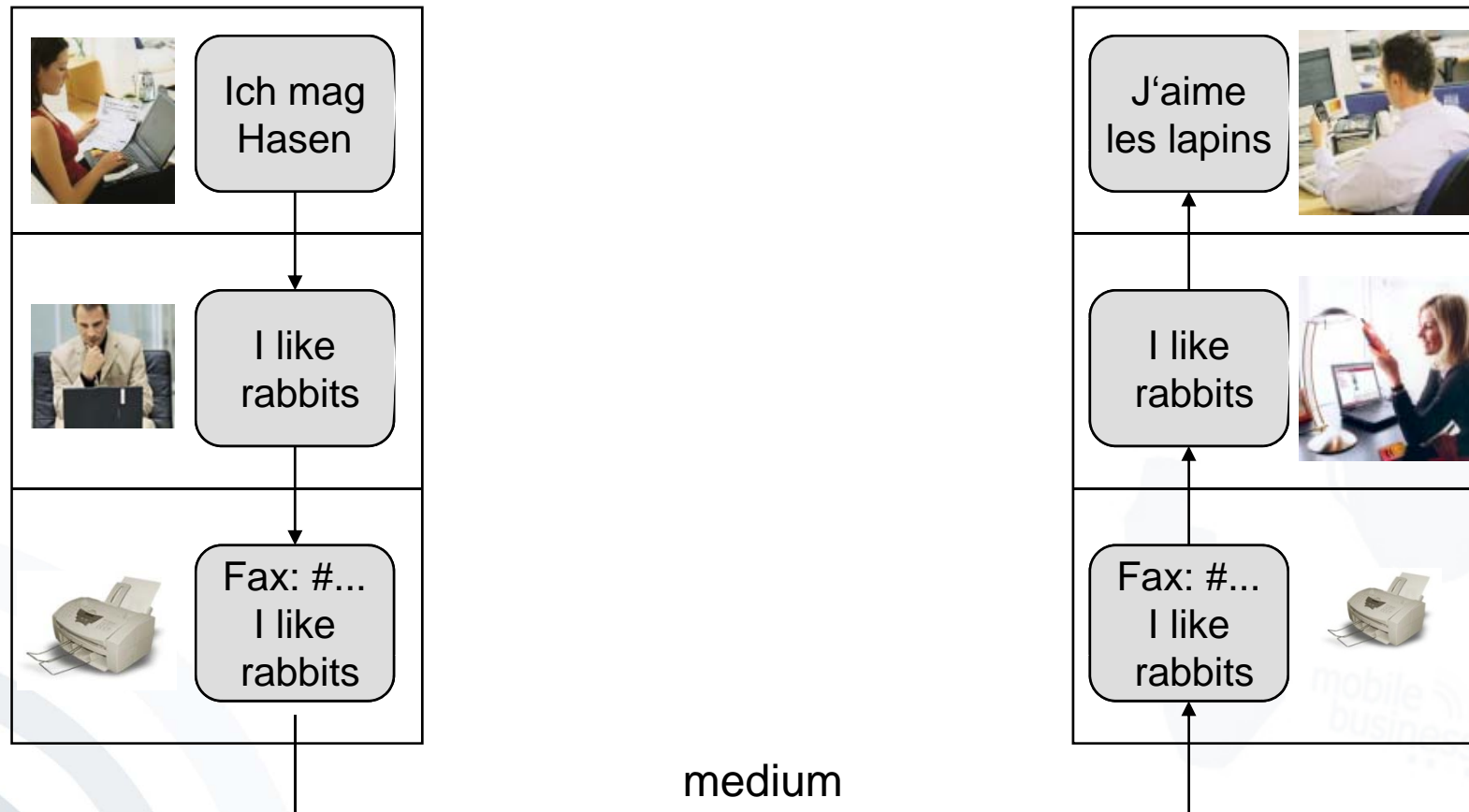
Guest Lecturer Dr. Martin Reichenbach

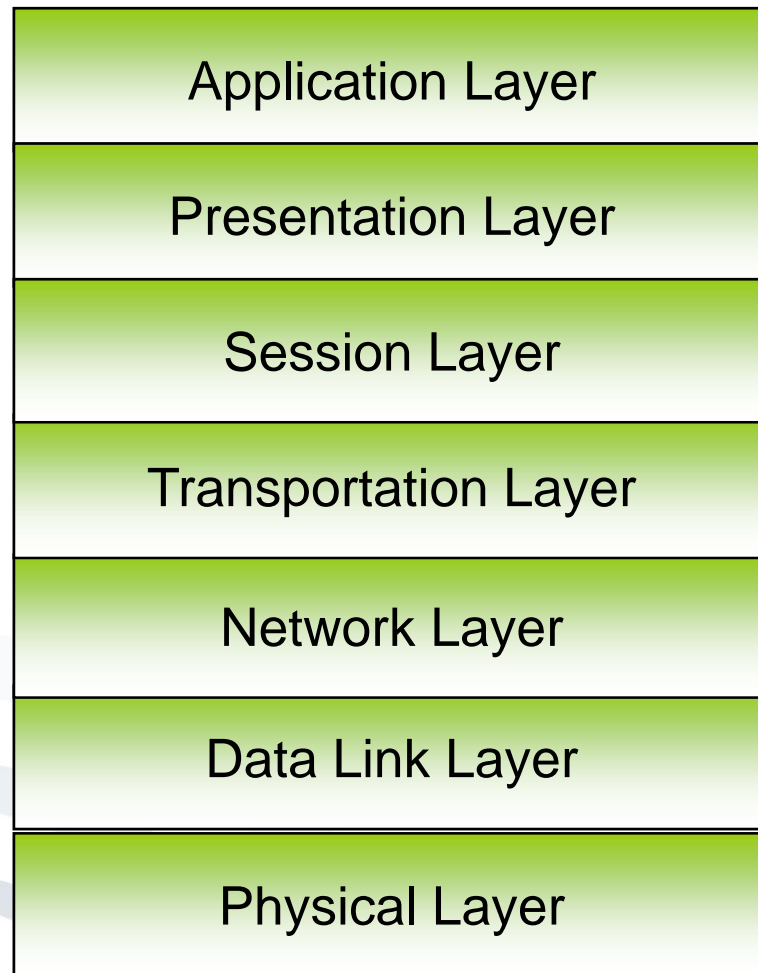
T-Mobile Chair for
Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.
www.whatismobile.de



- Introduction
- Network Organisation
- Security Protocols
- Wireless / Mobile Security

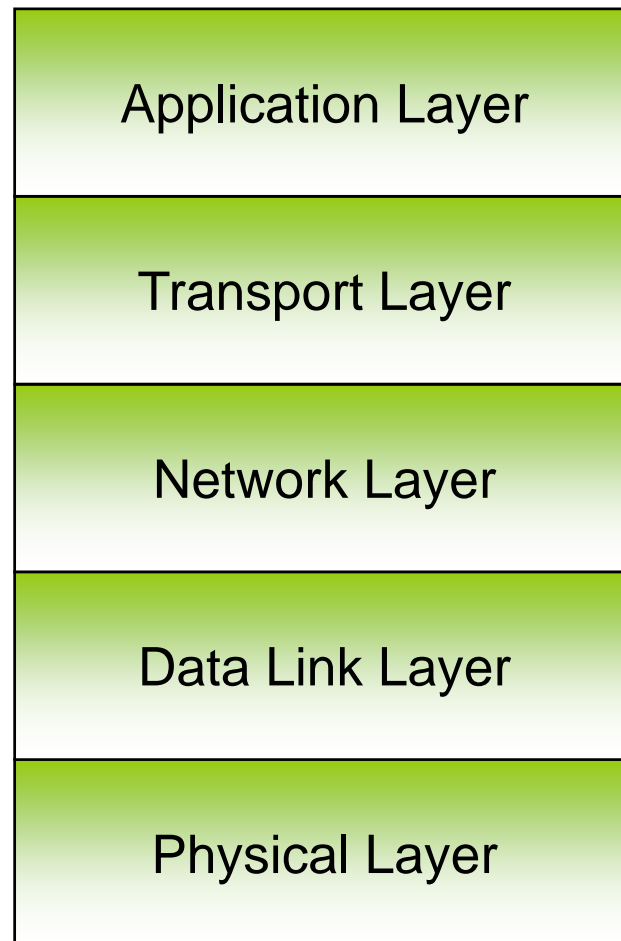
Layered Communication



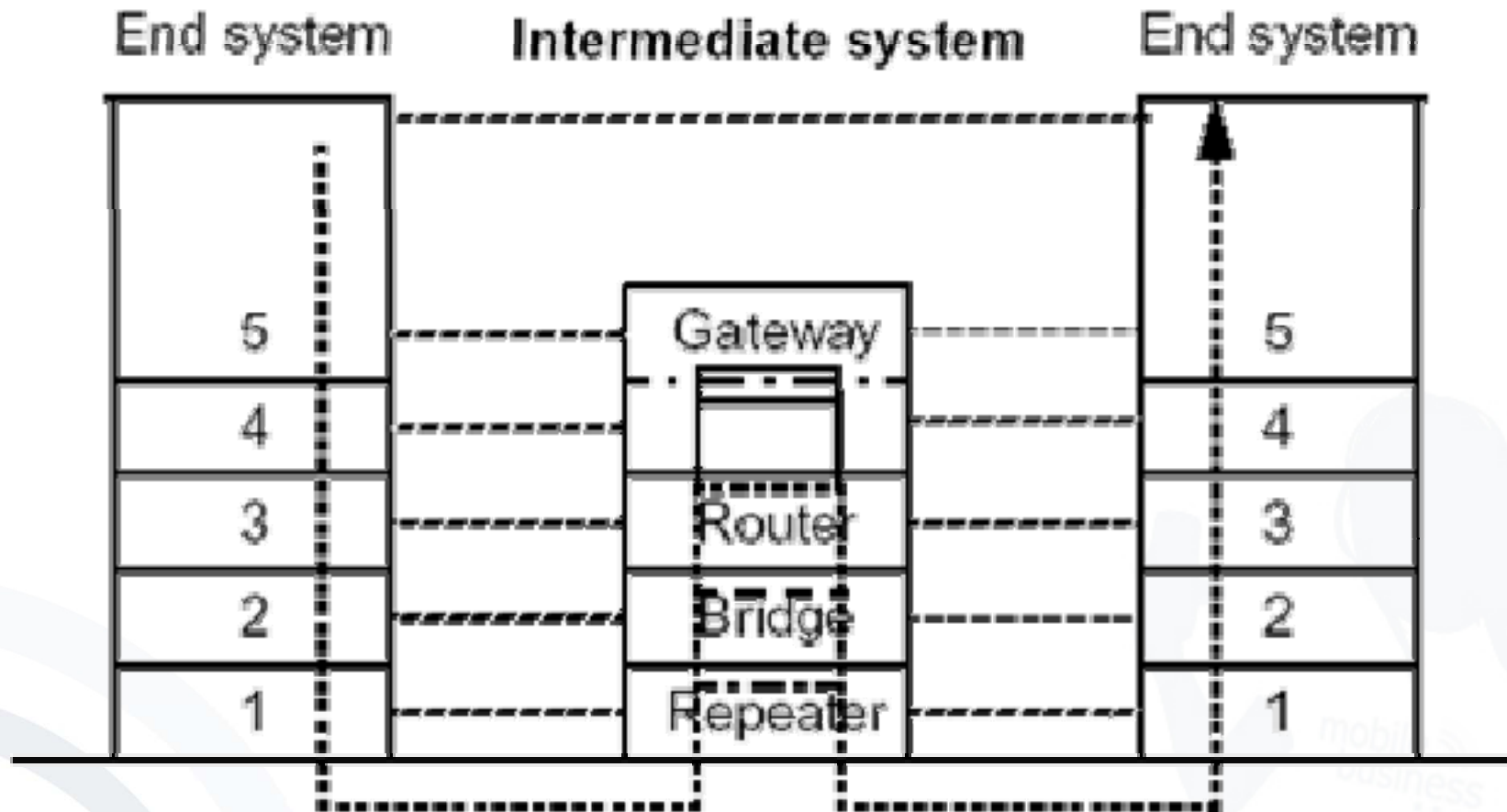


- Information technology – Open Systems Interconnection – Basic Reference Model
- „7-Layer-Model“
 - First version
ISO/IEC 7498-1:1984
 - Current version
ISO/IEC 7498-1:1994

Internet Reference Model



- Protocol
 - Common language used by computers for speaking
- Transmission Control Protocol/Internet Protocol (TCP/IP)
 - Most widely used protocol
- TCP/IP stack
 - Contains four different layers
 - Network
 - Internet
 - Transport
 - Application



OSI-7-Layer-Model (Open Systems Interconnection Reference Model)

Begriffe: Englisch - Deutsch

- | | |
|----------------------|---|
| 1 Application Layer | - Anwendungsschicht |
| 2 Presentation Layer | - Darstellungsschicht |
| 3 Session Layer | - Sitzungs- bzw. Kommunikations-schicht |
| 4 Transport Layer | - Transportschicht |
| 5 Network Layer | - Netzwerk- bzw. Vermittlungsschicht |
| 6 Data Link Layer | - Sicherungsschicht |
| 7 Physical Layer | - Bitübertragungsschicht |

PC im Netzwerk
A



<http://www.wikipedia.org>

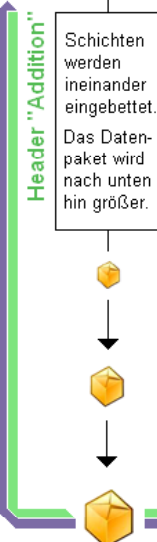
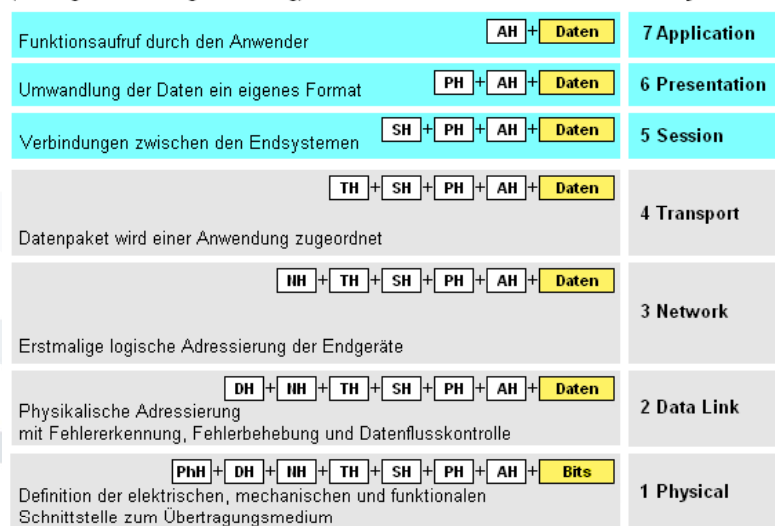
Der Benutzer empfängt lediglich die Antwort des Servers ("wikipedia.org"-Startseite). Im Allgemeinen bekommt er von der Schachtelung seines Seitenaufrufs durch die Ebenen seines PCs (abwärts) und vom Parsen der Antwort des Servers zurück durch die Ebenen seines PCs (aufwärts) nichts mit!

Server schickt die entsprechenden Daten über die selbe Methode zurück. (s.u.)

Server im Netzwerk
A



Zusammenbau des Pakets: (Package Assembling/Formatting)



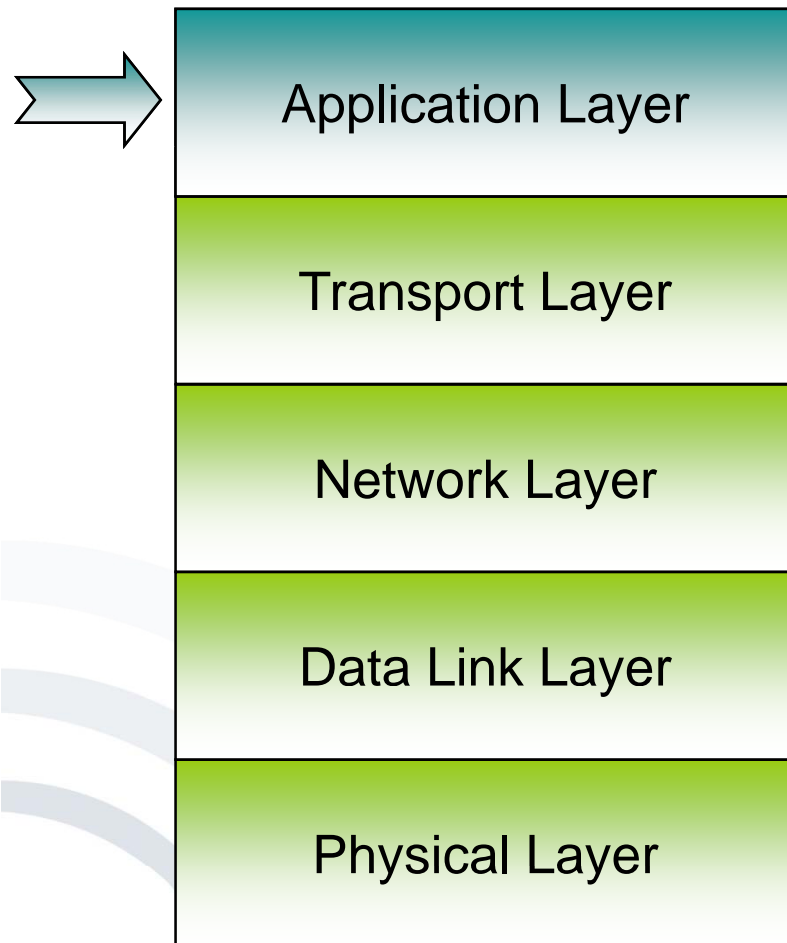
| Einordnung der Orientierung | Standard | TCP/IP Schicht | Einordnung der Verbindung | Protokoll | Request | Antwort |
|-----------------------------|-----------|----------------|---------------------------|--|---------|---------|
| Anwendungsorientiert | FTAM | Anwendung | Ende zu Ende (Multihop) | HTTP FTP HTTPS NCP | Request | Antwort |
| | ASN.1 | | | | | |
| | ISO 8326 | | | | | |
| Transportorientiert | ISO 8073 | Transport | Punkt zu Punkt | TCP UDP SPX | Request | Antwort |
| | CLNP | Internet | | ICMP IGMP IP IPX | | |
| | HDLC | Netzzugang | | Ethernet Token Ring FDDI ARCNET | | |
| | Token Bus | | | | | |



Parsen/Zerlegen der Daten durch die Ebenen

Zusammensetzung der Abkürzungen oben:
Anfangsbuchstabe der Schicht und "H" für Header.
z.B. Application Header = AH

physikalische oder logische Verbindung
Tatsächlicher Datendurchsatz / Übertragungspfad



Tasks:

- Front end to the lower-layer protocols
- provides network services to the user/applications
- Examples:
(service/protocol):
E-Mail / SMTP,
WWW / HTTP,
file transfer / FTP

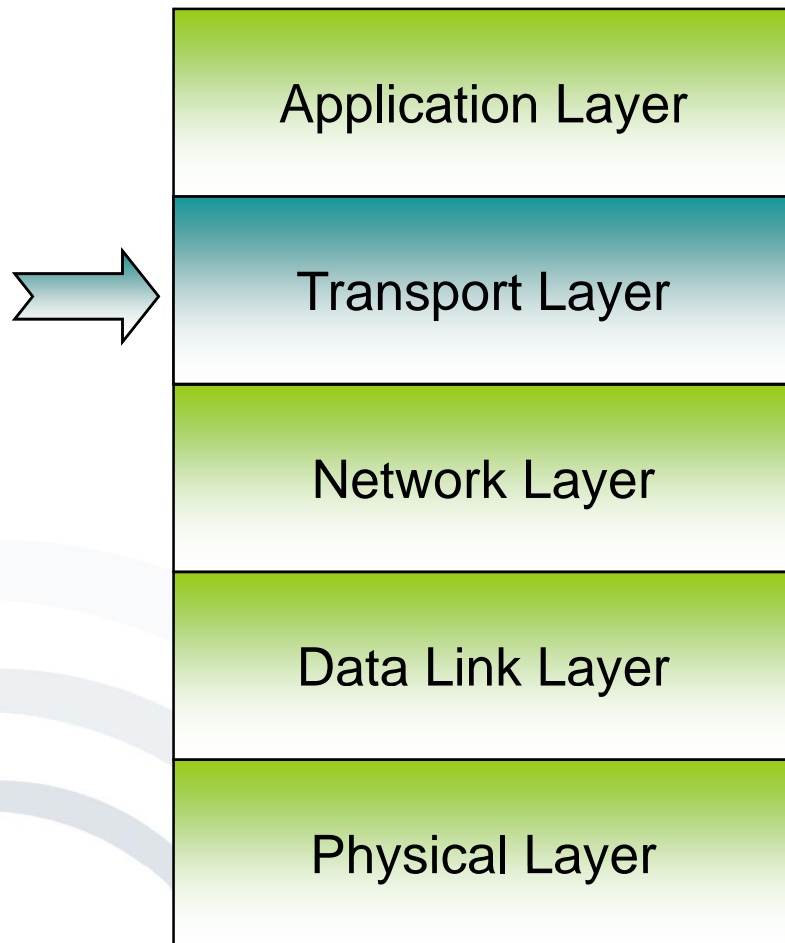
SMTP: Simple Mail Transfer Protocol

HTTP: Hyper Text Transfer Protocol

FTP: File Transfer Protocol

Table 2-1 Application layer programs

| Application | Description |
|---|---|
| Hypertext Transfer Protocol (HTTP) | The primary protocol used to communicate over the World Wide Web (see RFC-2616 at www.ietf.org for details) |
| File Transfer Protocol (FTP) | Allows different operating systems to transfer files between one another |
| Simple Mail Transfer Protocol (SMTP) | The main protocol for transmitting e-mail messages across the Internet |
| Simple Network Management Protocol (SNMP) | Primarily used to monitor devices on a network, such as remotely monitoring a router's state |
| Secure Shell (SSH) | Enables a remote user to log on to a server and issue commands |
| Internet Relay Chat (IRC) | Enables multiple users to communicate over the Internet in discussion forums |
| Telnet | Enables users to remotely log on to a server |



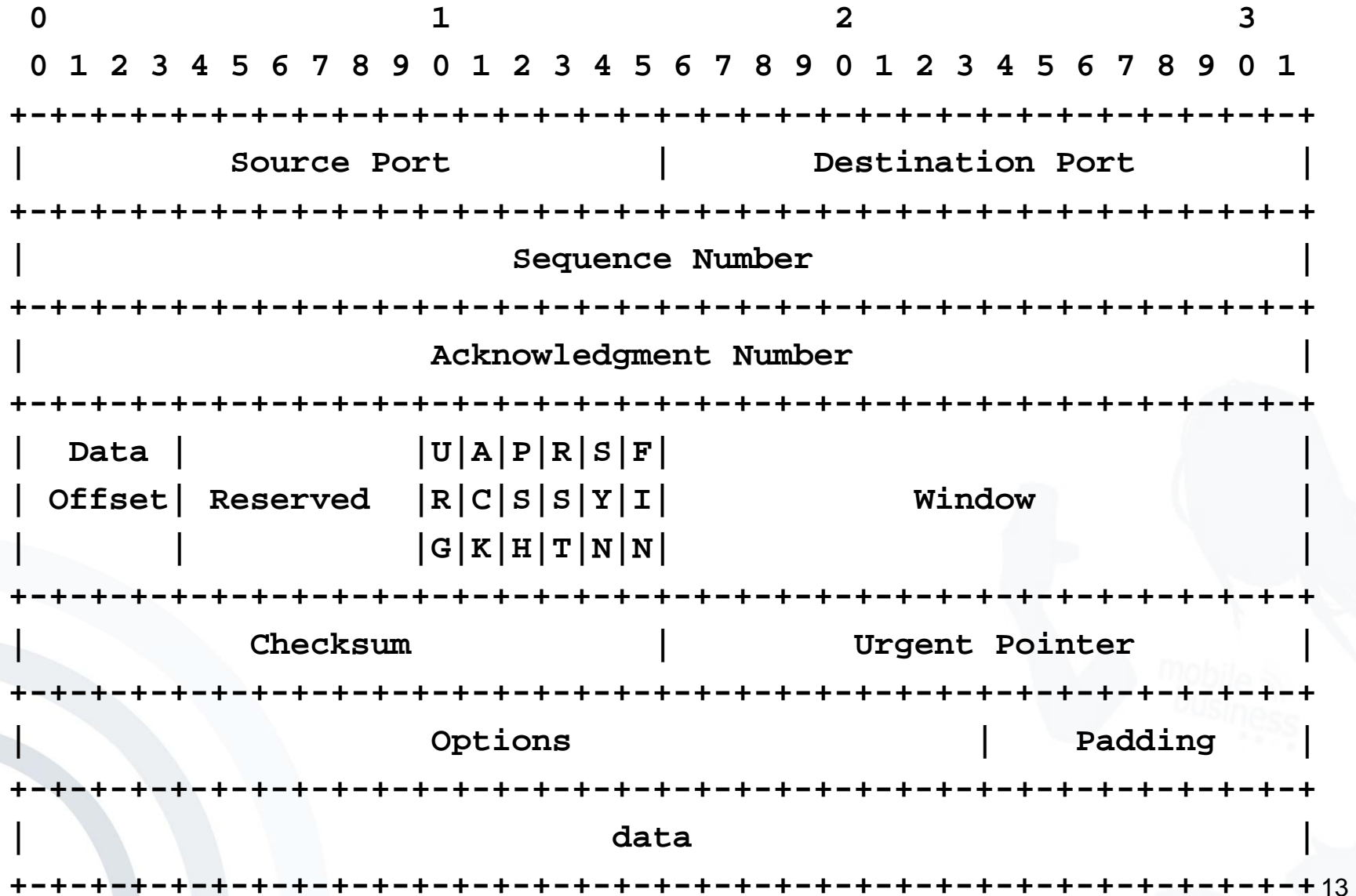
Tasks:

- Connection between source and target
- Optimisation of quality of service and service costs
- Flow control
- Connection management
- Getting Data packets to and from application layer by using port numbers

For example: TCP, UDP services

- Encapsulates data into segments
- Segments can use TCP or UDP to reach a destination host
 - TCP is a connection-oriented protocol
- TCP three-way handshake
 - Computer A sends a SYN packet
 - Computer B replies with a SYN-ACK packet
 - Computer A replies with an ACK packet

TCP Header Format



- Critical components:
 - TCP flags
 - Initial Sequence Number (ISN)
 - Source and destination port
- Abused by hackers finding vulnerabilities

- 32-bit number
- Tracks packets received
- Enables reassembly of large packets
- Sent on steps 1 and 2 of the TCP three-way handshake
 - By guessing ISN values, a hacker can hijack a TCP session, gaining access to a server without logging in

- Port
 - Logical, not physical, component of a TCP connection
 - Identifies the service that is running
 - Example: HTTP uses port 80
- A 16-bit number – 65,536 ports
- Each TCP packet has a source and destination port

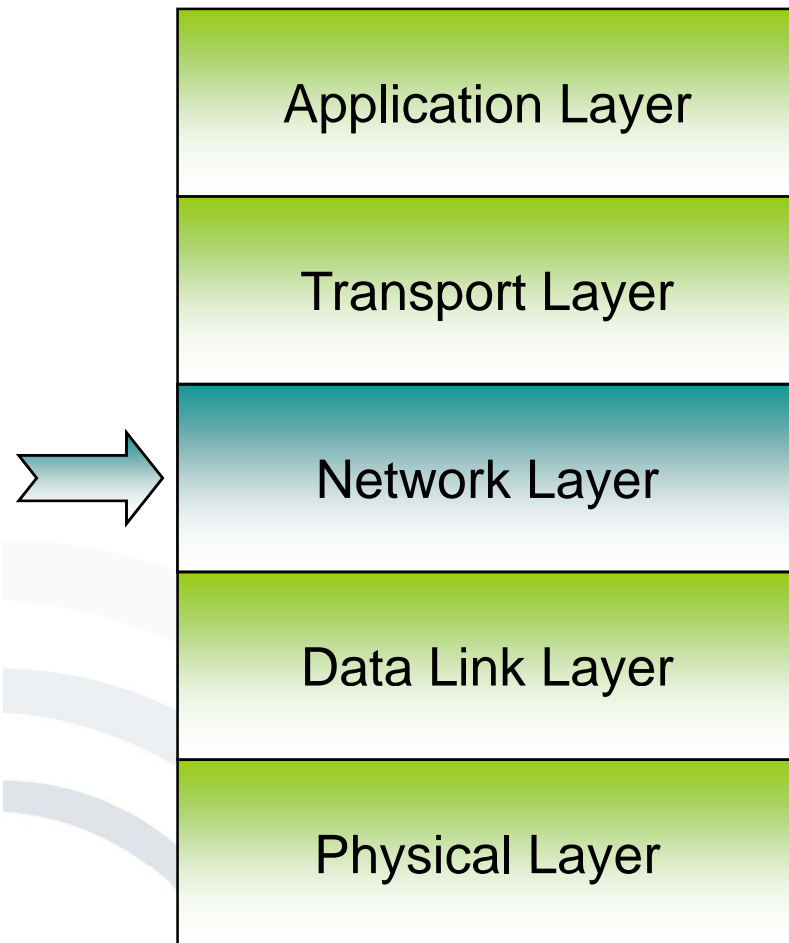
- Helps you stop or disable services that are not needed
 - Open ports are an invitation for an attack
- You can't block all the ports
 - That would stop all networking
 - At a minimum, ports 25 and 80 are usually open on a server, so it can send out Email and Web pages

- Wireshark Packet Sniffer
 - TCP Handshake: SYN, SYN/ACK, ACK
 - TCP Ports
 - TCP Status Flags

| o | Time | Source | Destination | Protocol | Info |
|---|----------|---------------|---------------|----------|--------------------------------------|
| 1 | 0.000000 | 192.168.2.14 | 82.165.134.55 | TCP | 1157 > http [SYN] Seq=0 Len=0 MSS=1 |
| 2 | 0.100187 | 82.165.134.55 | 192.168.2.14 | TCP | http > 1157 [SYN, ACK] Seq=0 Ack=1 |
| 3 | 0.100281 | 192.168.2.14 | 82.165.134.55 | TCP | 1157 > http [ACK] Seq=1 Ack=1 win=1 |
| 4 | 0.100656 | 192.168.2.14 | 82.165.134.55 | HTTP | GET /235/s214.html HTTP/1.1 |
| 5 | 0.214045 | 82.165.134.55 | 192.168.2.14 | TCP | http > 1157 [ACK] Seq=1 Ack=701 win= |
| 6 | 0.218748 | 82.165.134.55 | 192.168.2.14 | TCP | [TCP segment of a reassembled PDU] |
| 7 | 0.220002 | 82.165.134.55 | 192.168.2.14 | TCP | [TCP segment of a reassembled PDU] |

| | |
|---|---|
| + | Frame 1 (62 bytes on wire, 62 bytes captured) |
| + | Ethernet II, Src: AcctonTe_0e:5c:8a (00:10:b5:0e:5c:8a), Dst: BelkinCo_02:ed:7b (00:3 |
| + | Internet Protocol, Src: 192.168.2.14 (192.168.2.14), Dst: 82.165.134.55 (82.165.134.5 |
| - | Transmission Control Protocol, Src Port: 1157 (1157), Dst Port: http (80), Seq: 0, Le |
| | Source port: 1157 (1157) |
| | Destination port: http (80) |
| | Sequence number: 0 (relative sequence number) |
| | Header length: 28 bytes |
| - | Flags: 0x02 (SYN) |
| | 0... .. = Congestion window Reduced (CWR): Not set |
| | .0.. = ECN-Echo: Not set |
| | ..0. = Urgent: Not set |
| | ...0 = Acknowledgment: Not set |
| | 0... = Push: Not set |
| |0.. = Reset: Not set |
| |1. = Syn: Set |
| |0 = Fin: Not set |
| | window size: 16384 |
| | checksum: 0x6033 [correct] |
| + | Options: (8 bytes) |

- Fast but unreliable protocol
- Operates on transport layer
- Does not need to verify whether the receiver is listening
- Higher layers of the TCP/IP stack handle reliability problems
- Connectionless protocol
- E.g. for short DNS messages



Tasks:

- Responsible for routing packets to their destination address
- Routing
- Addressing Using a logical address, called e.g. an IP address
- Typically connectionless

For example: IP

- Operates in the Internet layer of the TCP/IP stack
- Used to send messages related to network operations
- Helps in troubleshooting a network
- Some commands include
 - Ping
 - Traceroute

- Consists of four bytes, like 147.144.20.1
- Two components
 - Network address
 - Host address
 - Neither portion may be all 1s or all 0s
- **Classes**
 - Class A
 - Class B
 - Class C

Table 2-3 TCP/IP address classes

| Address Class | Range | Address Bytes | Number of Networks | Host Bytes | Number of Hosts |
|---------------|---------|---------------|--------------------|------------|-----------------|
| Class A | 1–127 | 1 | 127 | 3 | 16,777,214 |
| Class B | 128–191 | 2 | 16,128 | 2 | 65,534 |
| Class C | 192–223 | 3 | 2,097,152 | 1 | 254 |

- Class A
 - First byte is reserved for network address
 - Last three bytes are for host address
 - Supports more than 16 million host computers
 - Limited number of Class A networks
 - Reserved for large corporations and governments (see link Ch 2b)
 - Format: *network.node.node.node*

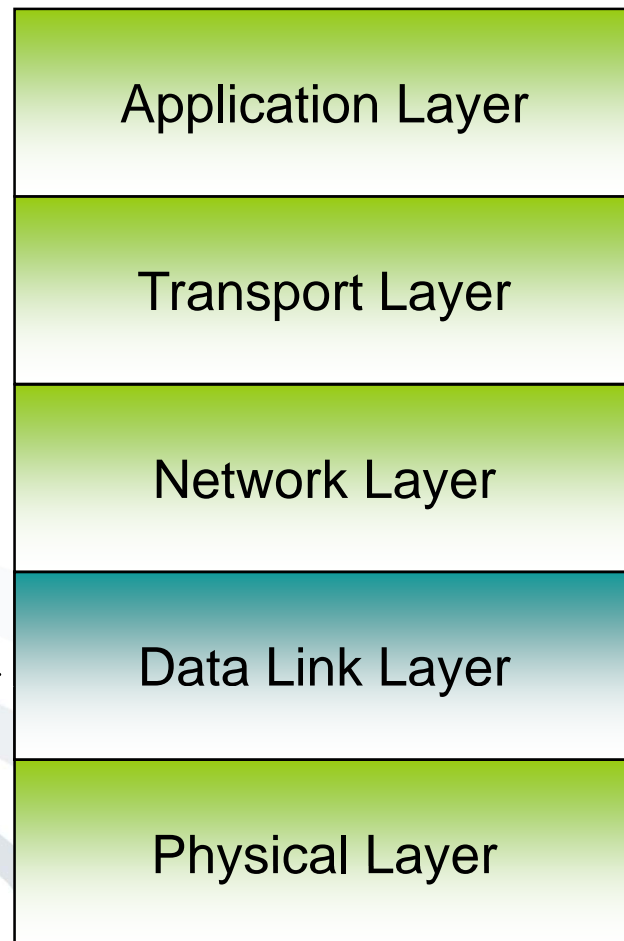
- Class B
 - First two bytes are reserved for network address
 - Last two bytes are for host address
 - Supports more than 65,000 host computers
 - Assigned to large corporations and Internet Service Providers (ISPs)
 - Format: *network.network.node.node*
 - CCSF has 147.144.0.0 – 147.144.255.255

- Class C
 - First three bytes are reserved for network address
 - Last byte is for host address
 - Supports up to 254 host computers
 - Usually available for small business and home networks
 - Format: *network.network.network.node*

- Subnetting
 - Each network can be assigned a subnet mask
 - Helps identify the network address bits from the host address bits
- Class A uses a subnet mask of 255.0.0.0
 - Also called /8
- Class B uses a subnet mask of 255.255.0.0
 - Also called /16
- Class C uses a subnet mask of 255.255.255.0
 - Also called /24

- TCP/IP uses subnet mask to determine if the destination computer is on the same network or a different network
 - If destination is on a different network, it relays packet to gateway
 - Gateway forwards packet to its next destination (routing)
 - Packet eventually reaches destination

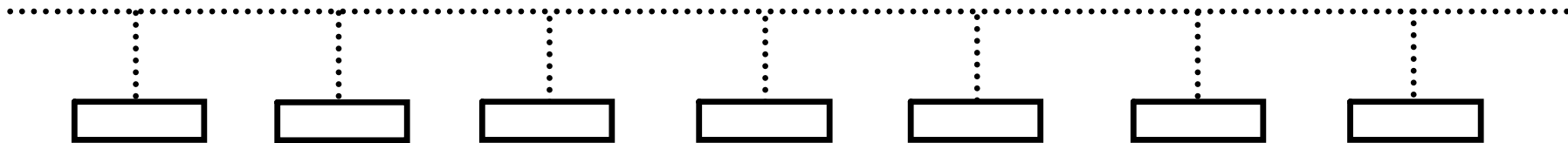
- Each network segment must have a unique network address
- Address cannot contain all 0s or all 1s
- To access computers on other networks
 - Each computer needs IP address of **gateway**



Tasks:

- data transmission between stations in the direct neighbourhood
- error detection and elimination
- flow control
- Medium access control (MAC)

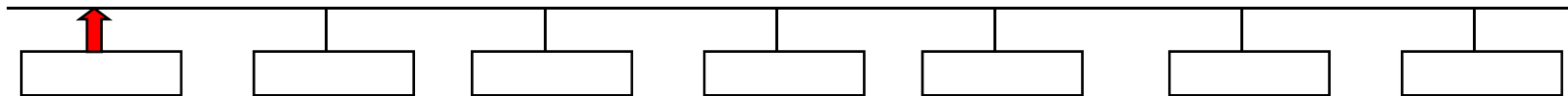
▪ Bus-Network



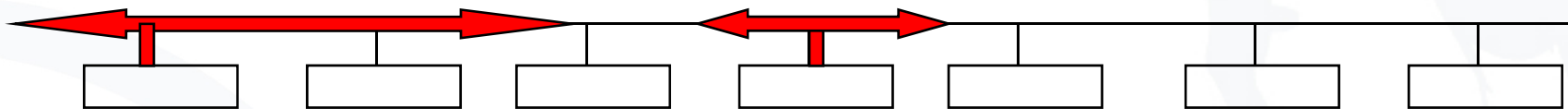
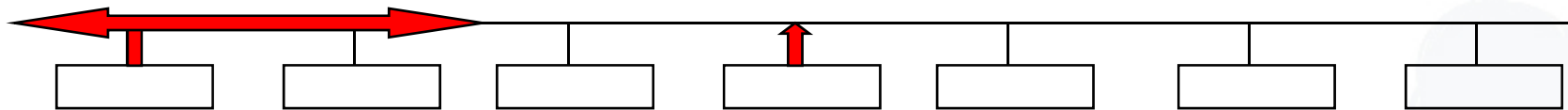
- Developed by XEROX
- Additional nodes can easily be added.
- Protocol: Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

CSMA/CD:

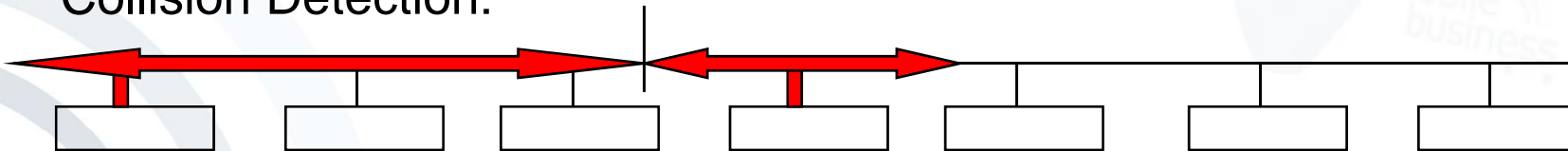
Carrier Sense:



Multiple Access:



Collision Detection:



Eavesdropping of all frames

i.e. Ethereal:

The screenshot shows the Ethereal interface with a list of captured packets. The first packet is selected, and its details are shown below. The details include Ethernet II, Internet Protocol, and Transmission Control Protocol information. The packet data is displayed in hexadecimal and ASCII format.

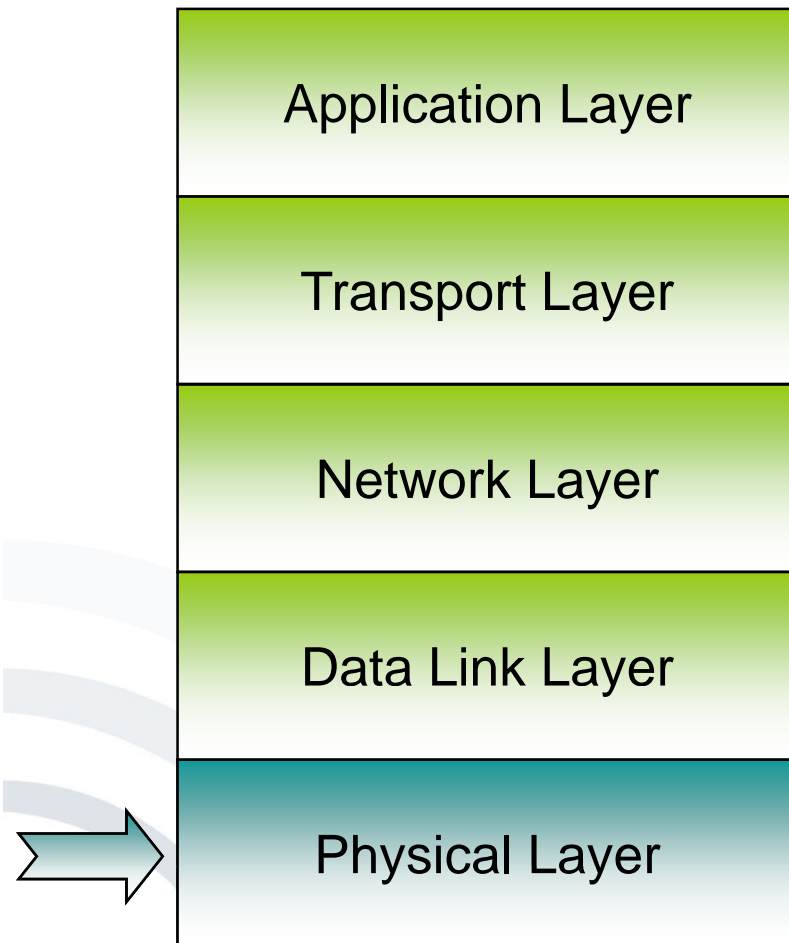
| No. | Time | Source | Destination | Protocol | Info |
|-----|----------|---------------|---------------|----------|-------------------------|
| 1 | 0.000000 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [PSH, ACK] |
| 2 | 0.122921 | 130.83.23.160 | 62.179.101.66 | TCP | 1757 > 7128 [ACK] Seq=1 |
| 3 | 0.184619 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [PSH, ACK] |
| 4 | 0.187568 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [ACK] Seq=1 |
| 5 | 0.187607 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [ACK] Seq=1 |
| 6 | 0.187706 | 130.83.23.160 | 62.179.101.66 | TCP | 1757 > 7128 [ACK] Seq=1 |
| 7 | 0.187718 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [ACK] Seq=1 |
| 8 | 0.188348 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [ACK] Seq=1 |
| 9 | 0.188399 | 130.83.23.160 | 62.179.101.66 | TCP | 1757 > 7128 [ACK] Seq=1 |
| 10 | 0.189682 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [ACK] Seq=1 |
| 11 | 0.232726 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [PSH, ACK] |
| 12 | 0.232854 | 130.83.23.160 | 62.179.101.66 | TCP | 1757 > 7128 [ACK] Seq=1 |
| 13 | 0.291815 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [PSH, ACK] |
| 14 | 0.298128 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [ACK] Seq=1 |
| 15 | 0.298191 | 62.179.101.66 | 130.83.23.160 | TCP | 7128 > 1757 [ACK] Seq=1 |
| 16 | 0.298208 | 130.83.23.160 | 62.179.101.66 | TCP | 1757 > 7128 [ACK] Seq=1 |

Frame 1 (1346 bytes on wire, 1346 bytes captured)
 Ethernet II, Src: 00:07:4f:55:b4:00, Dst: 00:06:5b:b9:15:8a
 Internet Protocol, src Addr: 62.179.101.66 (62.179.101.66), dst Addr: 130.83.23.160 (130.83.23.160)
 Transmission Control Protocol, Src Port: 7128 (7128), Dst Port: 1757 (1757), Seq: 1941500, Len: 1292 (1292 bytes)

```

0000  00 06 5b b9 15 8a 00 07 4f 55 b4 00 08 00 45 00  ..[.....OU....E.
0010  05 34 0f ba 40 00 74 06 b4 21 3e b3 65 42 82 53  .4..@.t. !>.eB.S
0020  17 a0 1b d8 06 dd 73 b8 f0 bc 76 44 b3 4b 50 18  .....s. ..vD.KP.
0030  fa 7a 09 37 00 00 8f f3 1c 3a da 81 e9 4a e0 64  .z.7.... :....J.d
0040  67 4b 50 31 2c 5c 0b 78 fb 6e 07 a0 cb 81 85 9f  gKP1,\.x .n.....
  
```

composite packets
of higher protocol
layers



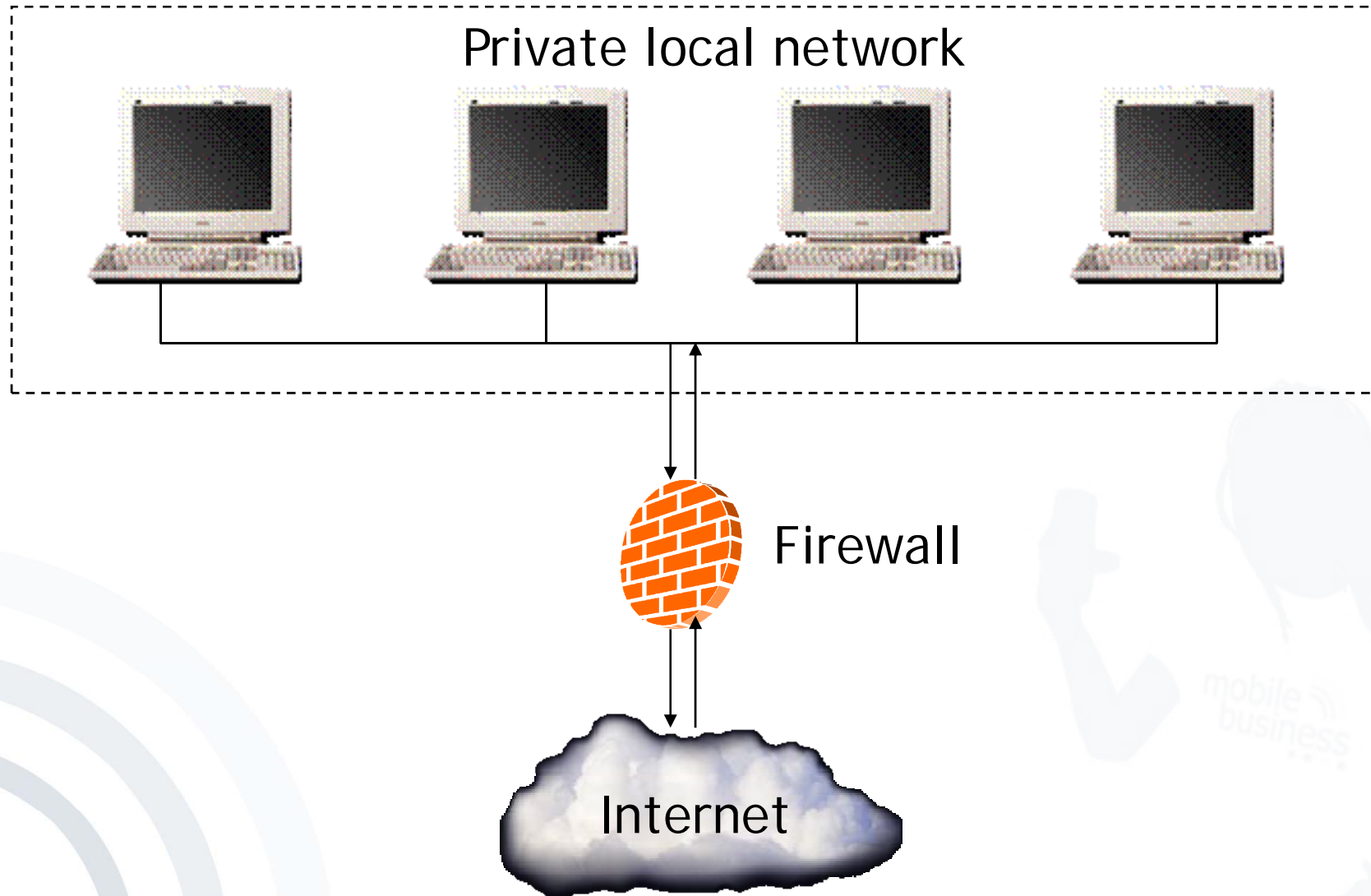
Tasks:

- Bit transfer
- Mechanic
(connector, medium)
- Electronic
(signal durability of a bit,
voltage)

- Introduction
- Network Organisation
 - Firewalls
 - Demilitarized Zone
 - Intrusion Detection
- Security Protocols
- Wireless / Mobile Security

- Introduction
- Network Organisation
 - Firewalls
 - Demilitarized Zone
 - Intrusion Detection
- Security Protocols
- Wireless / Mobile Security

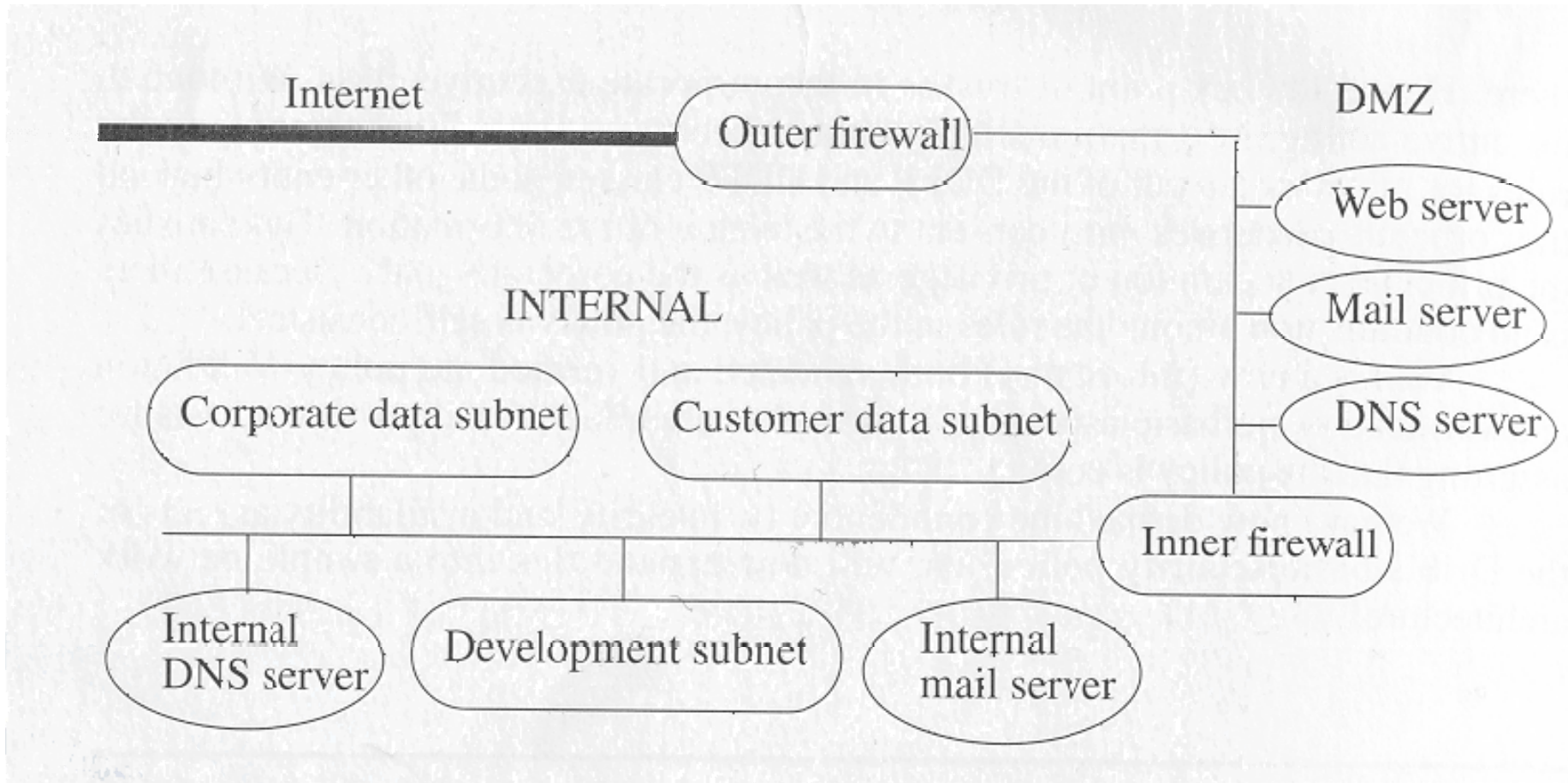
- „A firewall is an internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be *inside* the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be *outside* the firewall).“ [RFC 2828]

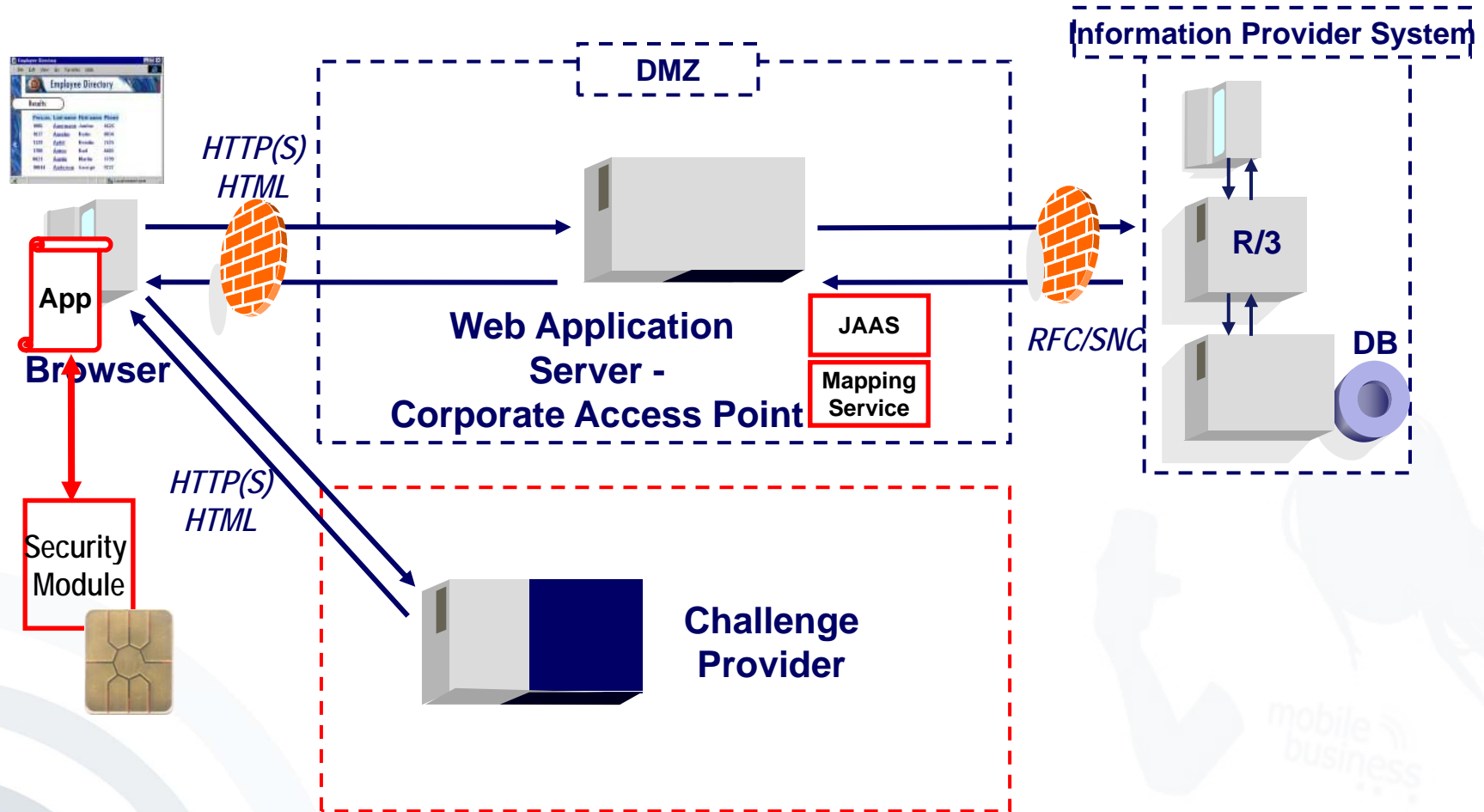


- Introduction
- Network Organisation
 - Firewalls
 - Demilitarized Zone
 - Intrusion Detection
- Security Protocols
- Wireless / Mobile Security

- The DMZ is a portion of a network, that separates a purely internal network from an external network. [Bi05]
- The “outer firewall” sits between the Internet and the internal network.
- The DMZ provides limited public access to various servers.
- The “inner firewall” sits between the DMZ and the subnets not to be accessed by the public.

Network using a DMZ





RFC: Remote Function Call
 SNC: Secure Network Connection

- Introduction
- Network Organisation
 - Firewalls
 - Demilitarized Zone
 - Intrusion Detection
- Security Protocols
- Wireless / Mobile Security

Computer systems that are not under attack exhibit several characteristics [Bi05]

1. The actions of users and processes generally conform to a statistically predictable pattern. A user who does only word processing when using the computer is unlikely to perform a system maintenance function.
2. The actions of users and processes do not include sequences of commands to subvert the security policy of the system. In theory, any such sequence is excluded; in practice, only sequences known to subvert the system can be detected.
3. The actions of processes conform to a set of specifications describing actions that the processes are allowed to do (or not allowed to do).

Denning [De87] hypothesized that systems under attack fail to meet at least one of these characteristics.

- An *attack tool* is an automated script designed to violate a security policy.
- Example: *Rootkit*

- Exists for many versions of the UNIX operating system
- Is designed to sniff passwords from the network and to conceal its presence
- Includes tools to automate the installation procedure and has modified versions of system utilities
- Can eliminate many errors arising from incorrect installation and perform routine steps to clean up detritus of the attack

- Detect a wide variety of intrusions:
 - Inside and outside attacks
 - Known and previously unknown attacks should be detected.
 - Adapt to new kinds of attacks
- Detect intrusions in a timely fashion
- Present the analysis in a simple, easy to understand format
- Be accurate:
 - False positives reduce confidence in the correctness of the results.
 - False negatives are even worse, since the purpose of an IDS is to report attacks.

- *Anomaly detection* analyzes a set of characteristics of the system and compares their behavior with a set of expected values.
- It reports when the computed statistics do not match the expected measurements.

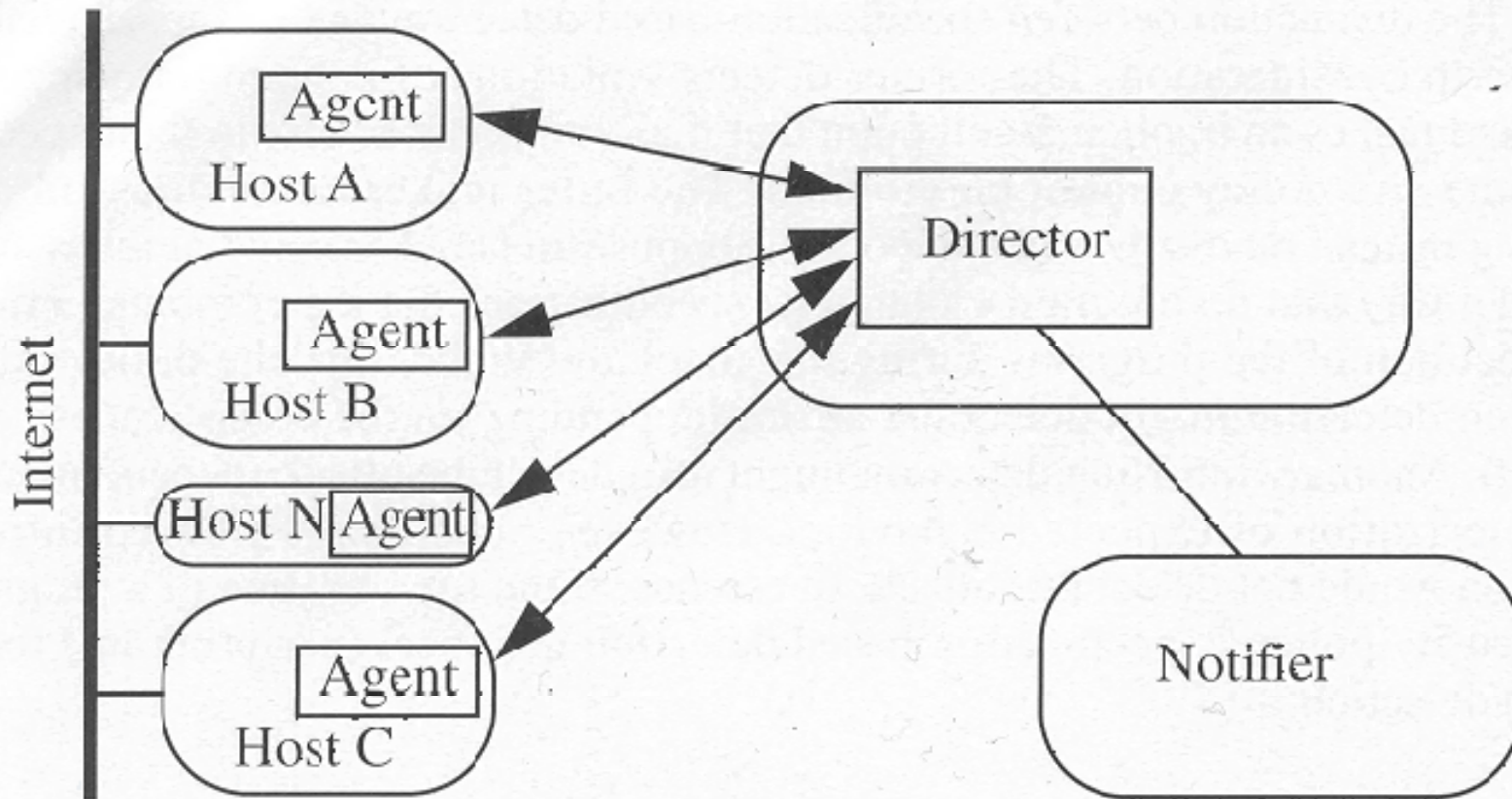
- *Misuse detection* determines whether a sequence of instructions being executed is known to violate the site security policy being executed. If so, it reports a potential intrusion.
- Example: *Network Flight Recorder (NFR)*

- NFR has three components
 - The *packet sucker* reads packets off the network.
 - The *decision engine* uses filters written in a language called N-code to extract information.
 - The *backend* writes the data generated by the filters to disk.

- *Specification-based detection* determines whether or not a sequence of instructions violates a specification of how a program, or system, should execute. If so, it reports a potential intrusion.
- Example threat source to be controlled: *The UNIX program rdist*

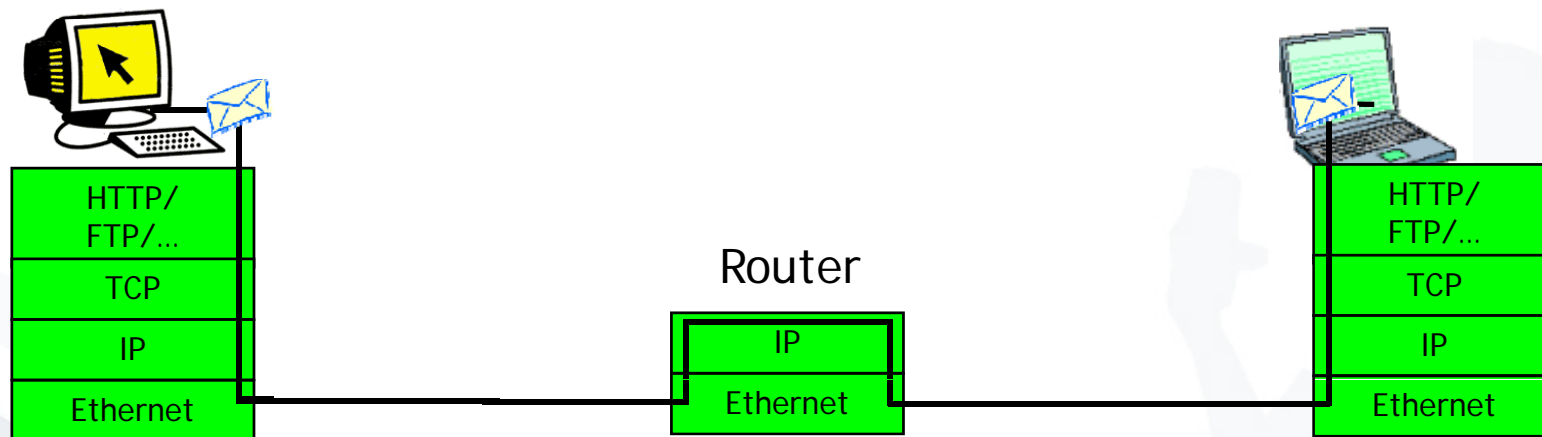
- An *autonomous agent* is a process that can act independently of the system of which it is a part.
- Example: *The Autonomous Agents for Intrusion Detection (AAFID)*

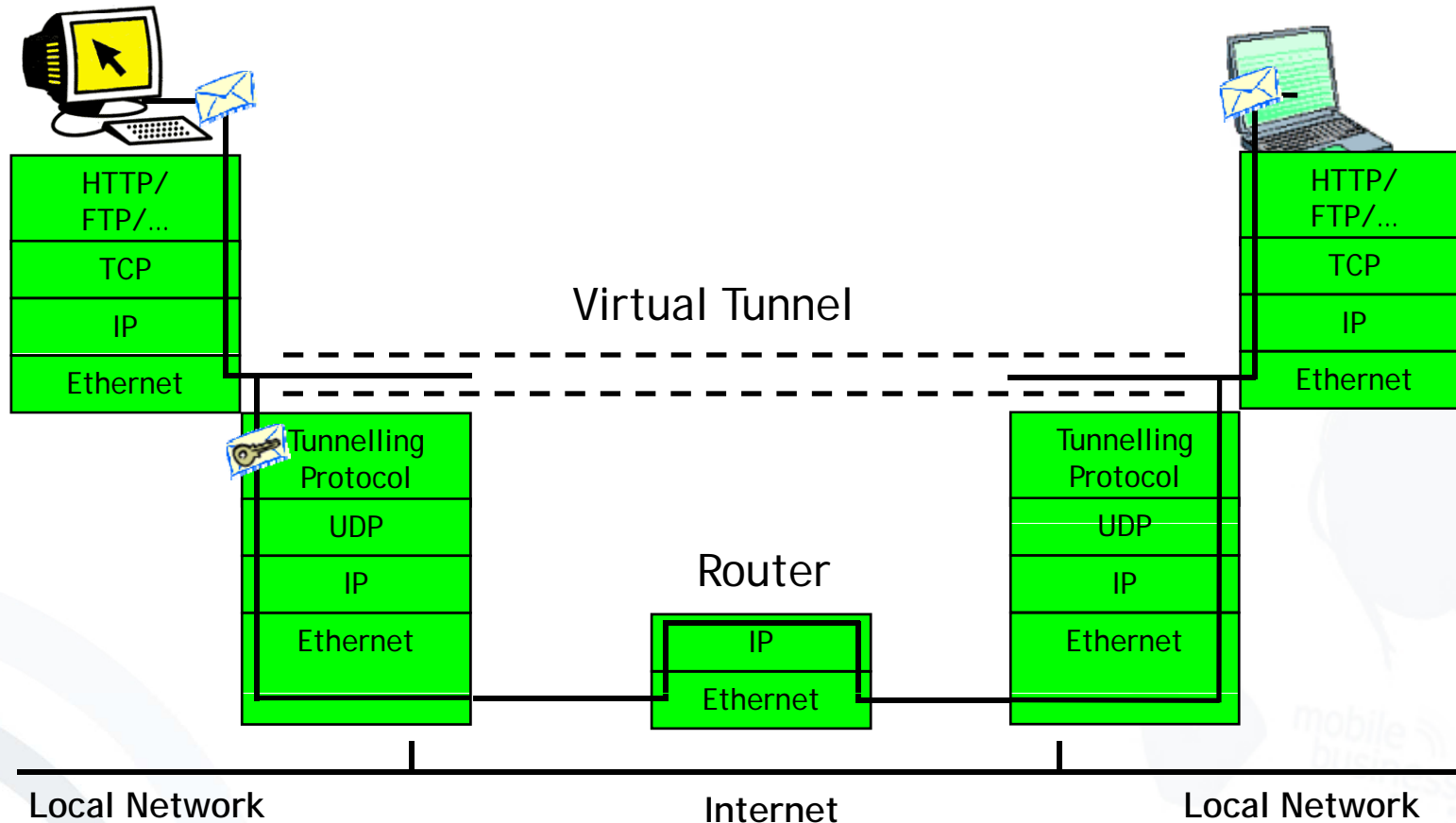
Intrusion Detection System



- Introduction
- Network Organisation
- Security Protocols
 - Virtual Private Networks
 - Secure Socket Layer
 - IPsec
- Wireless / Mobile Security

- Introduction
- Network Organisation
- Security Protocols
 - Virtual Private Networks
 - Secure Socket Layer
 - IPsec
- Wireless / Mobile Security



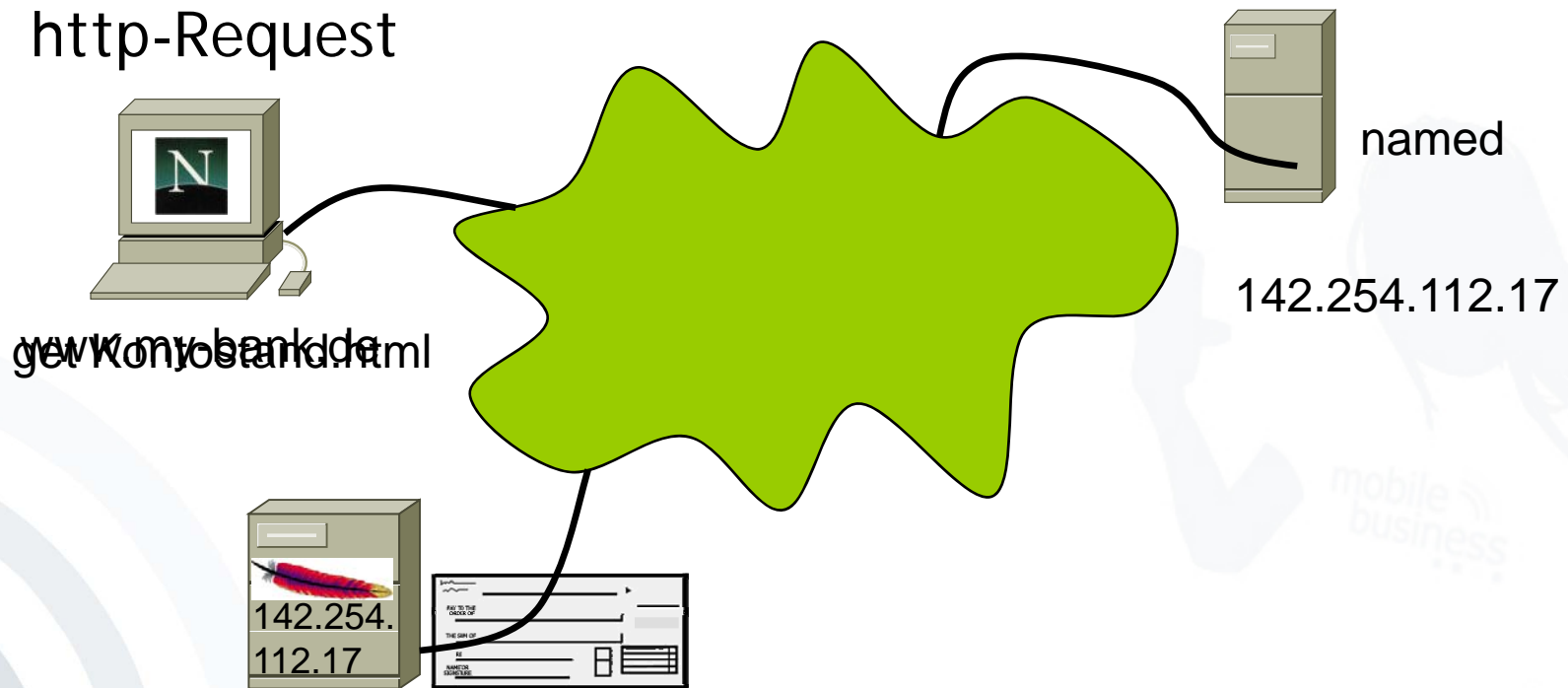


- Introduction
- Network Organisation
- Security Protocols
 - Virtual Private Networks
 - Secure Socket Layer
 - IPsec
- Wireless / Mobile Security

www.my-bank.de/Kontostand.html

Actions of the browser:

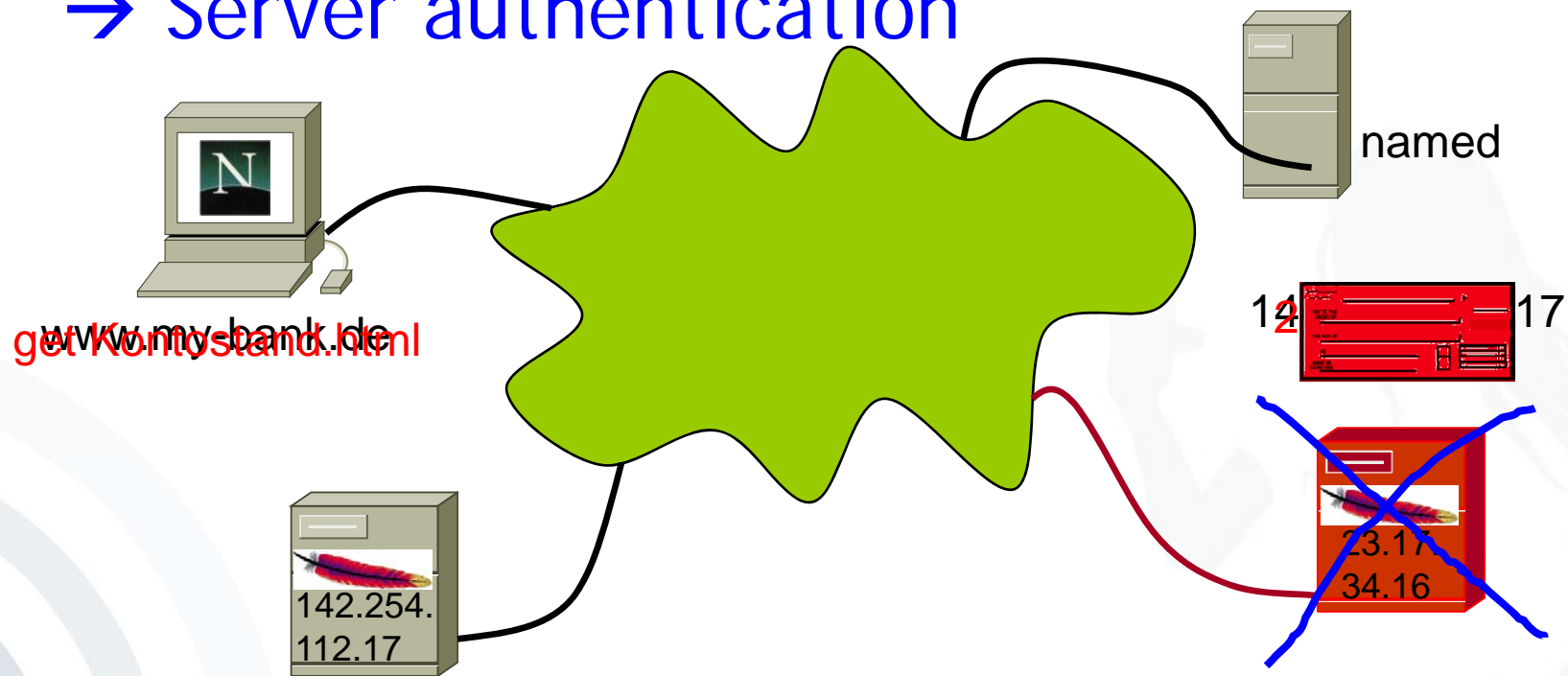
1. DNS-Request
2. http-Request



Possible attacks:

1. Compromise of DNS (DNS-Spoofing)

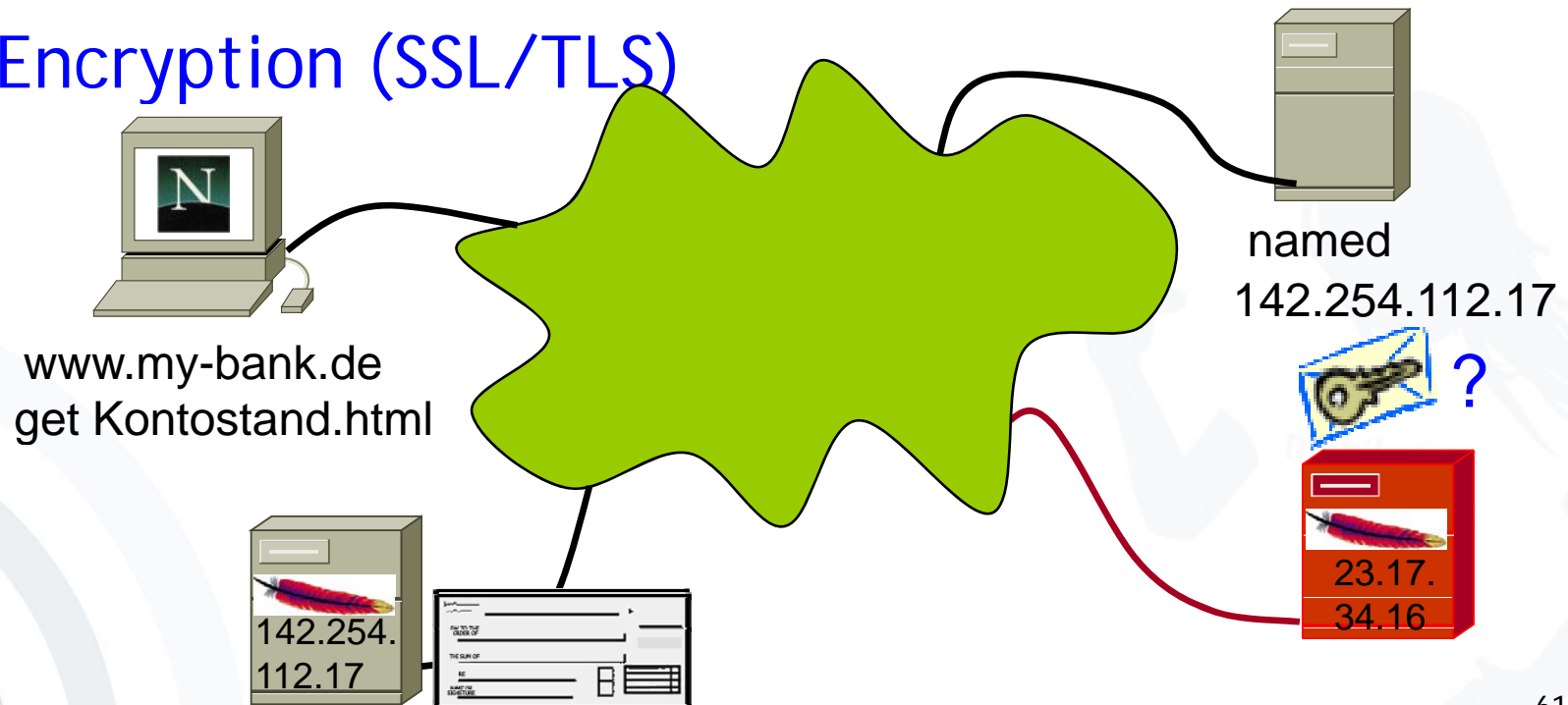
→ Server authentication



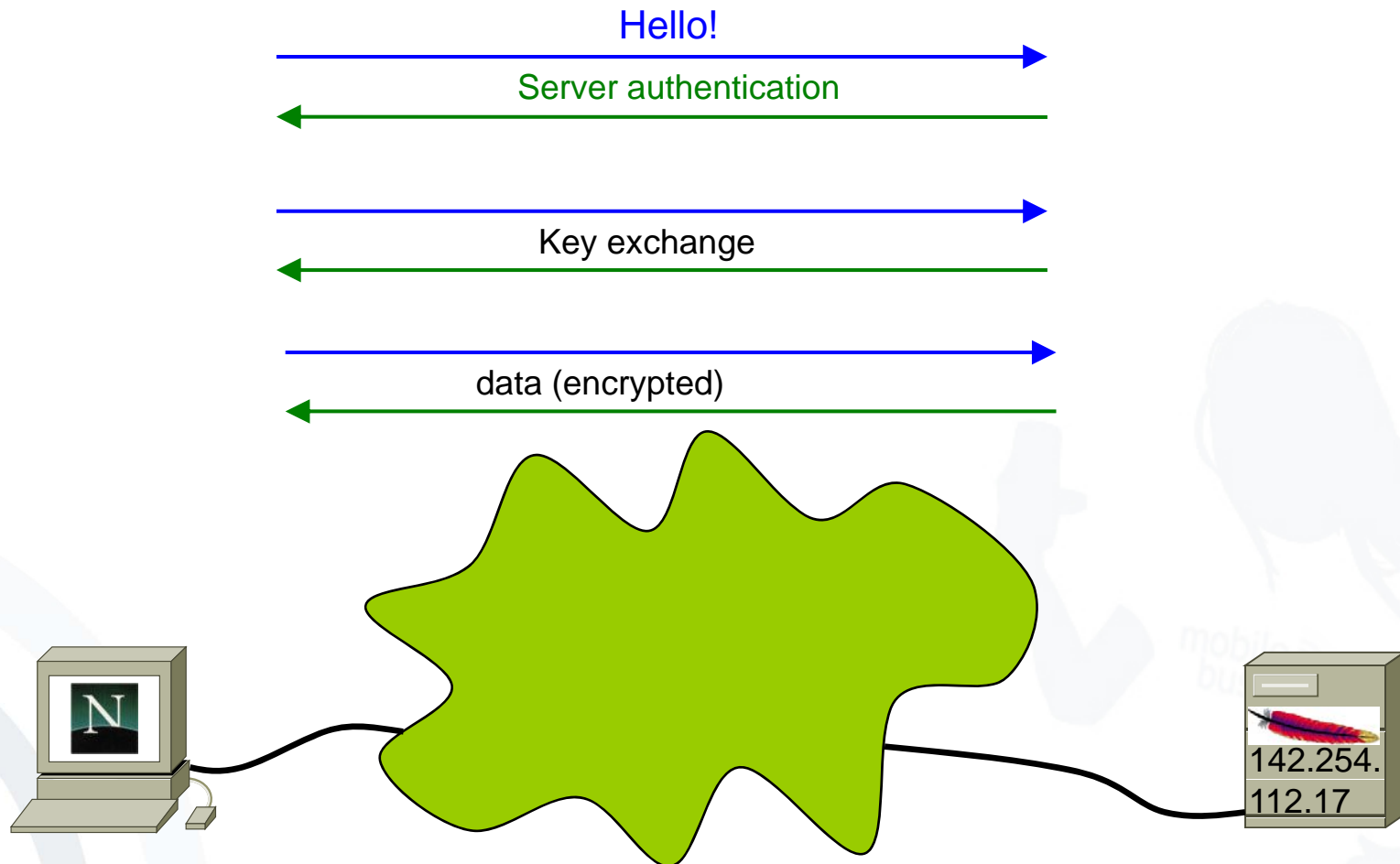
Possible attacks:

1. Compromise of DNS
2. Eavesdropping

→ Encryption (SSL/TLS)



SSL/TLS (simplified):



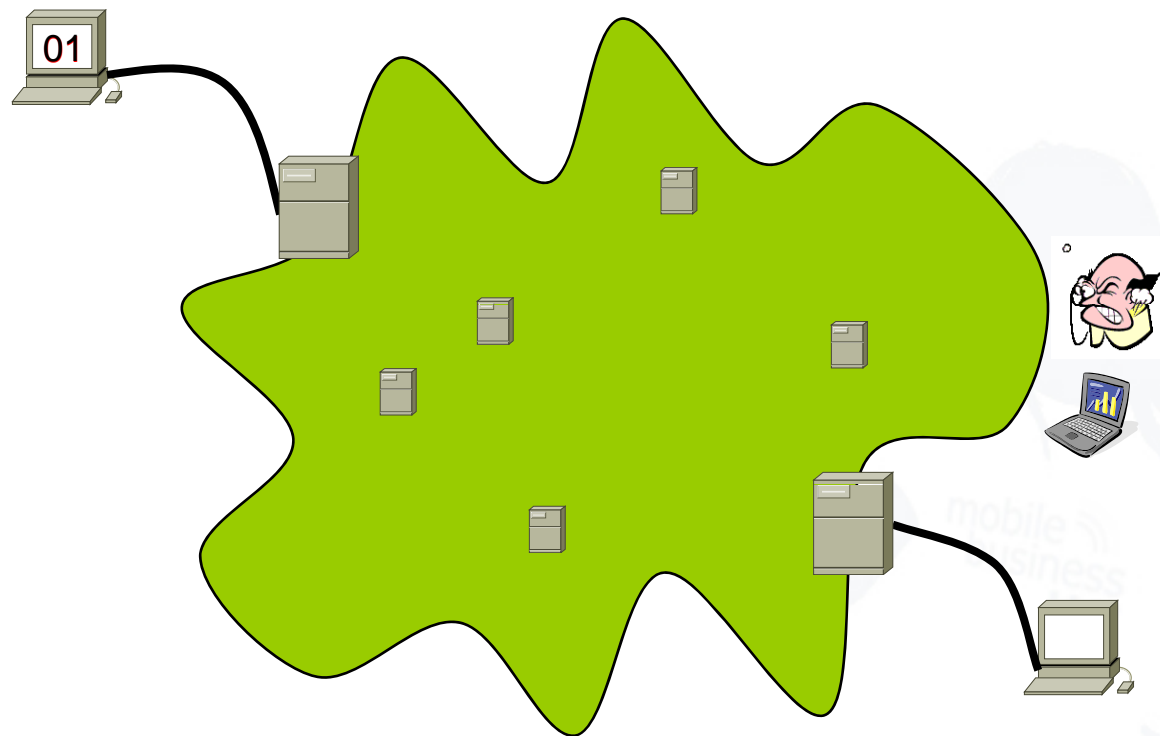
SSL/TLS:

- Server- and client-authentication
- Key exchange for symmetric encryption
- MACs to secure integrity

| Security Goal | http | https (SSL/TLS) |
|-----------------|------|------------------------|
| Authenticity | x | ✓ (mostly server only) |
| Non-Repudiation | x | x |
| Confidentiality | x | ✓ |
| Integrity | x | ✓ |
| Dated | x | x |

- Introduction
- Network Organisation
- Security Protocols
 - Virtual Private Networks
 - Secure Socket Layer
 - IPsec
- Wireless / Mobile Security

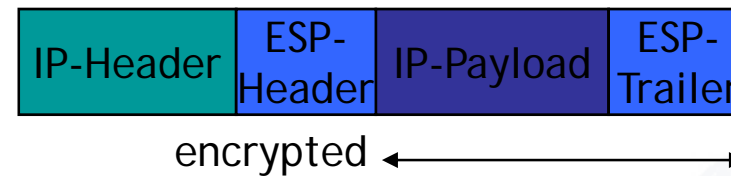
- Attacker is able to eavesdrop IP-Packets
- Ideal: At the sender- or recipient-gateway



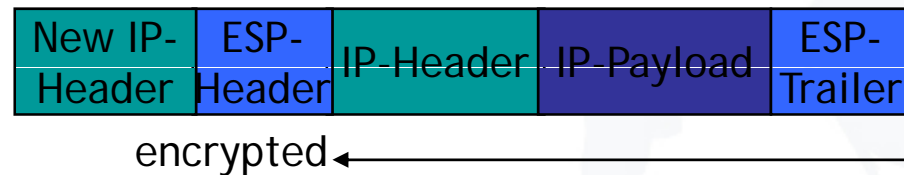
- Data Packet



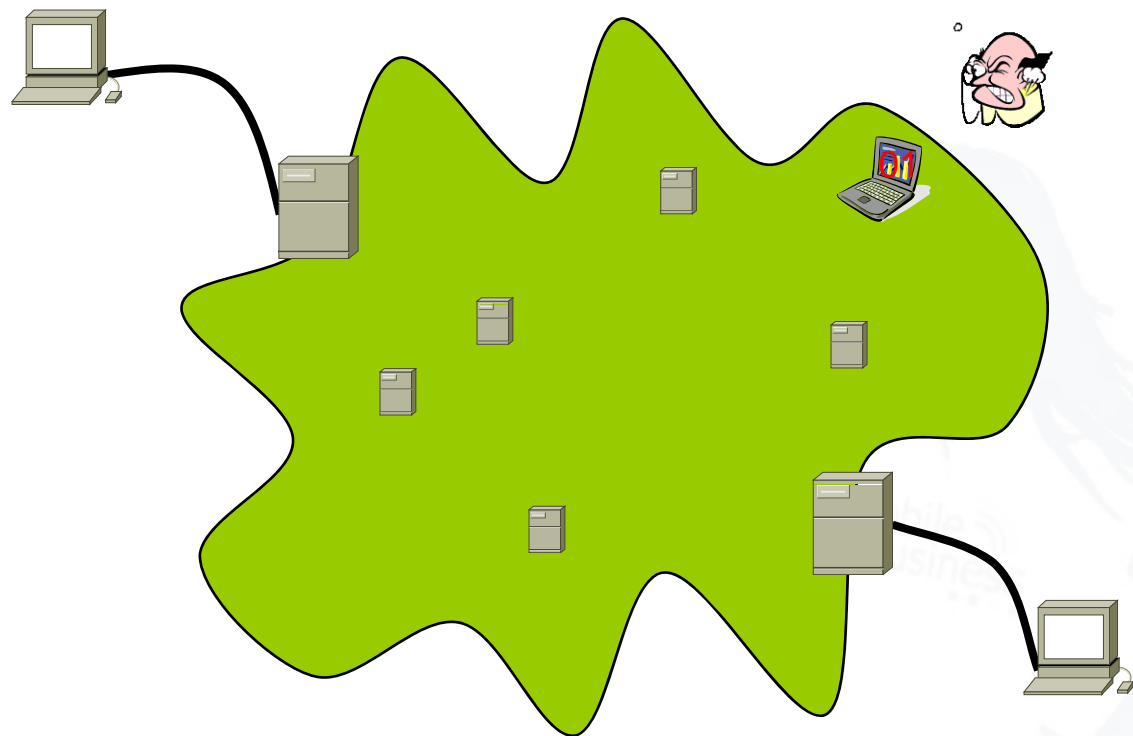
- ESP-Transport-Mode



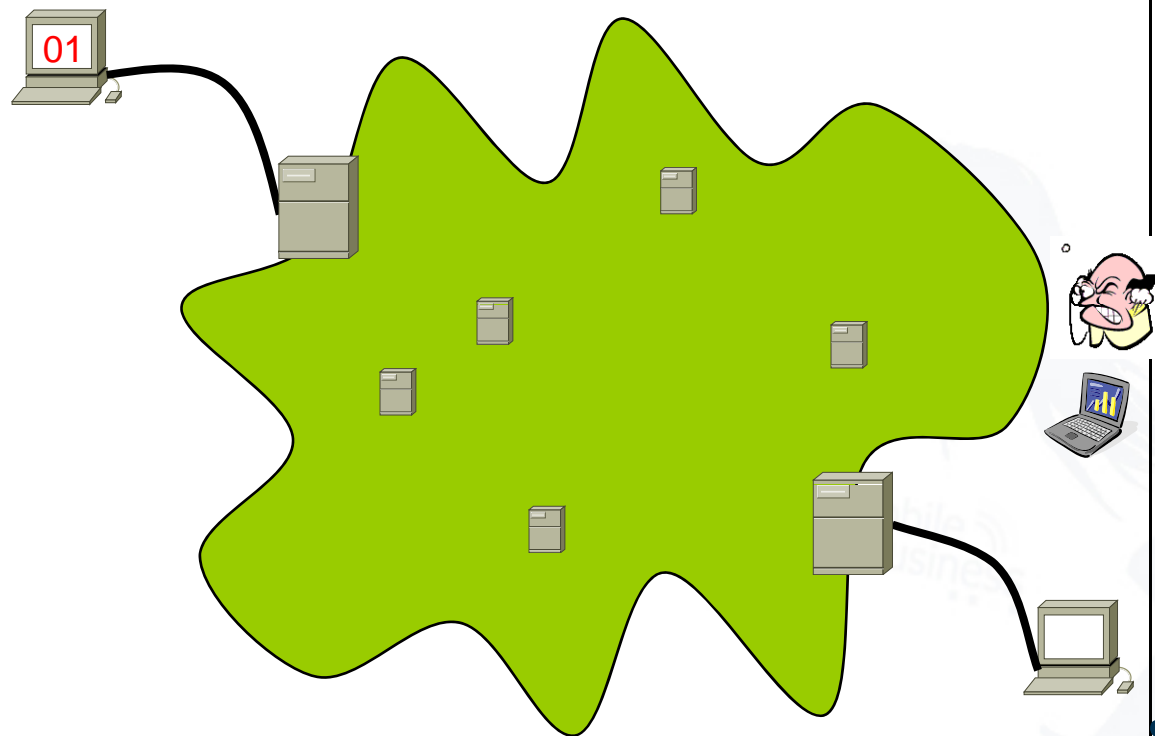
- ESP-Tunnel-Mode



- Attacker sends IP-packets with a faked sender address.



- Attacker impersonates the recipient.

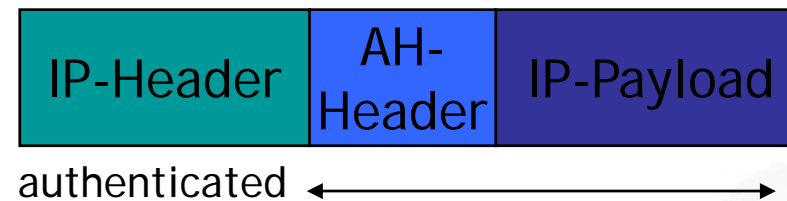


IPsec: Authentication Header

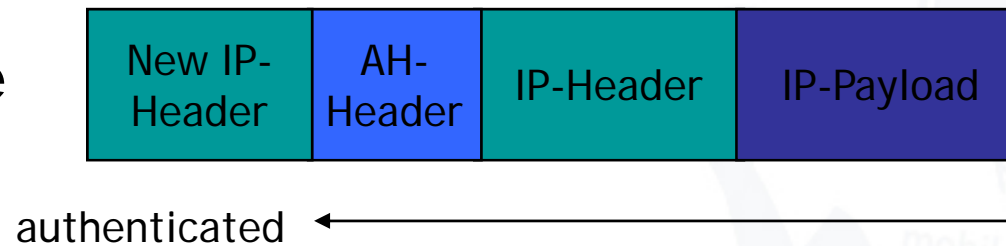
Data Packet



AH-Transport-Mode



AH-Tunneling-Mode



- [Bi05] Matt Bishop: *Introduction to Computer Security*. Boston: Addison Wesley, 2005, pp. 455-516
- [De87] Dorothy Denning: "An Intrusion- Detection Model", IEEE Transactions on Software Engineering, 13 (2), pp. 222-232
- [RFC 2828] Network Working Group: "Request for Comments 2828 - Internet Security Glossary", 2000, www.faqs.org/ftp/rfc/pdf/rfc2828.txt.pdf
- [Ta96] A.S. Tanenbaum: *Computer Networks*, 3rd Edition, 1996 [4th edition available]