

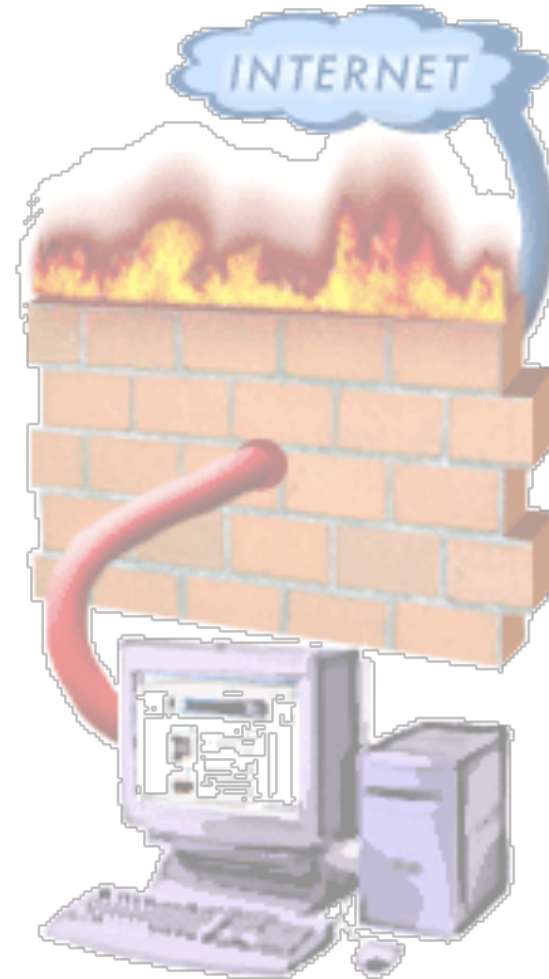
## *Lecture 10*

# Network Security I

Information & Communication Security  
(WS 2014)

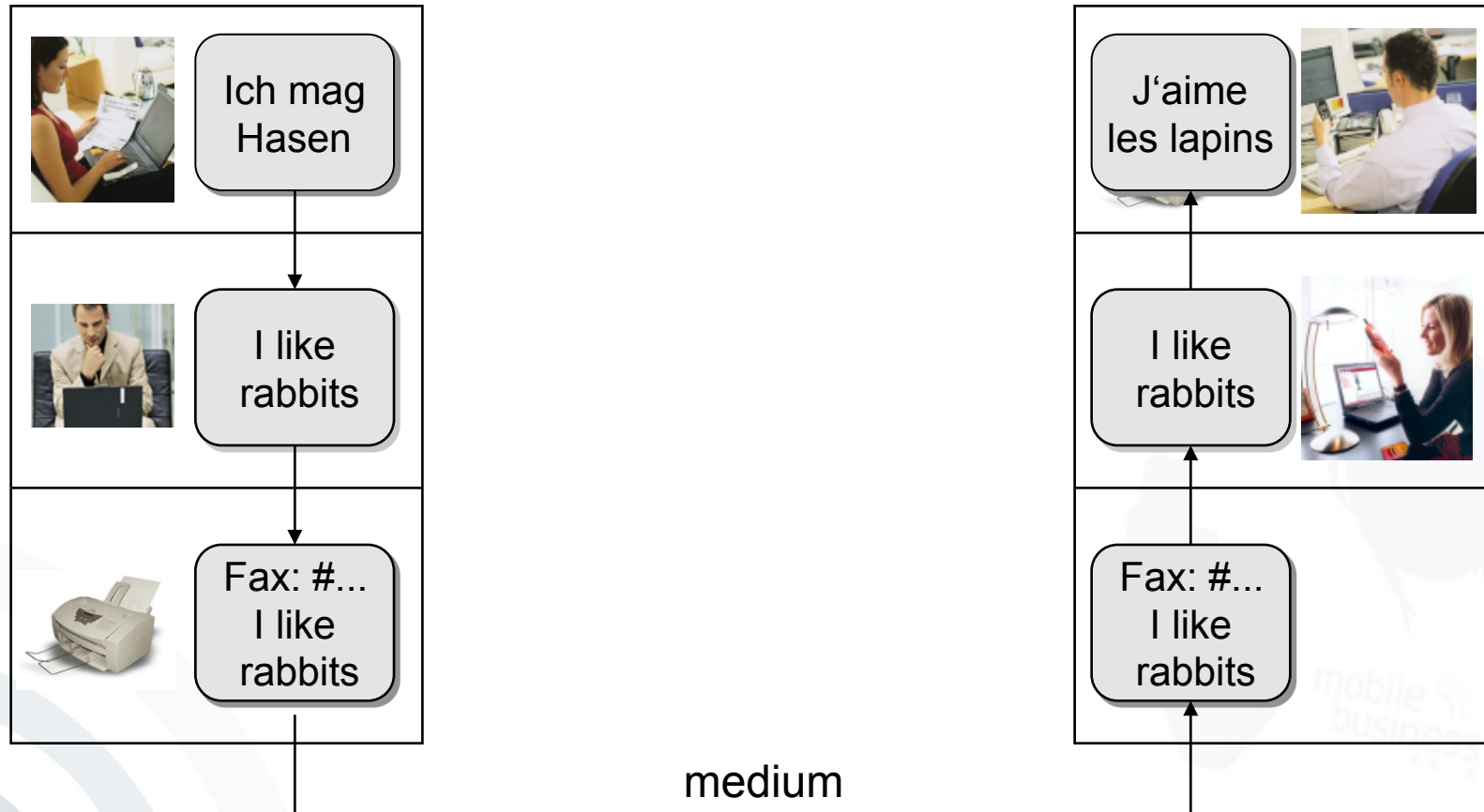
Prof. Dr. Kai Rannenberg

T-Mobile Chair of Mobile Business & Multilateral Security  
Goethe University Frankfurt a. M.

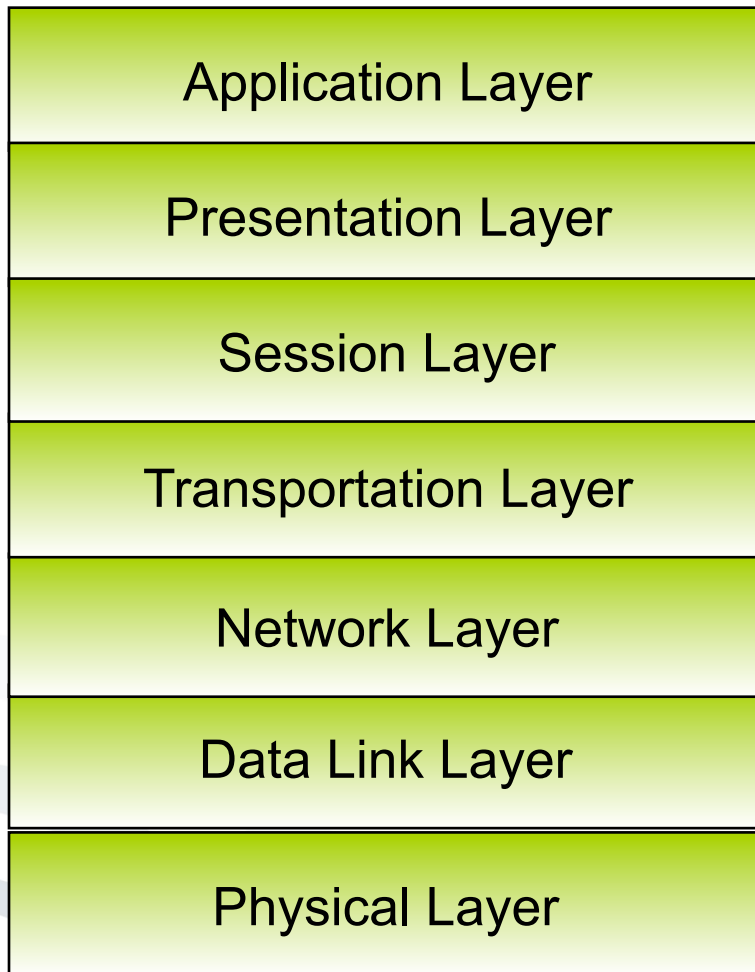


- Introduction
- Network Organisation
- Security Protocols
- Wireless / Mobile Security

# Layered Communication

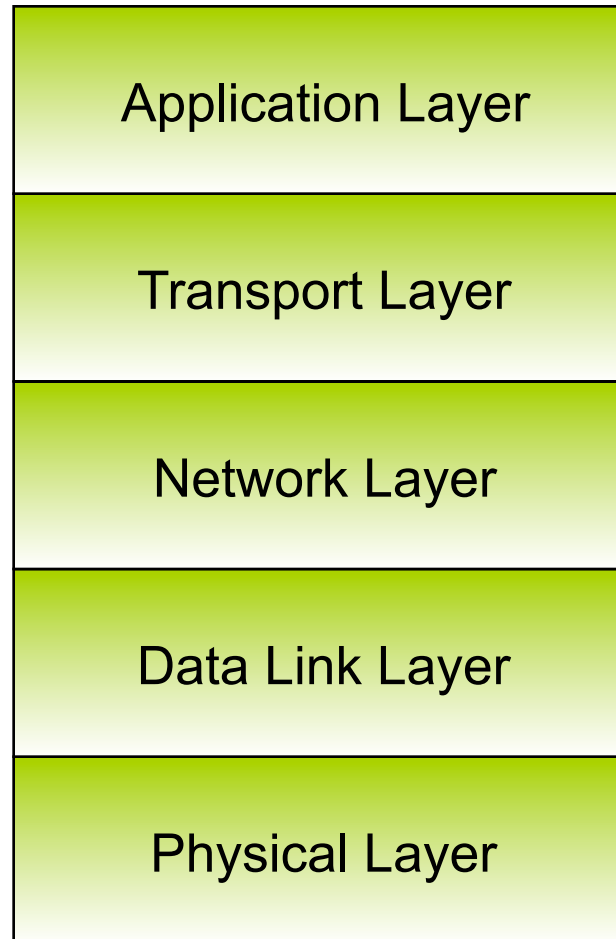


# ISO/OSI Reference Model

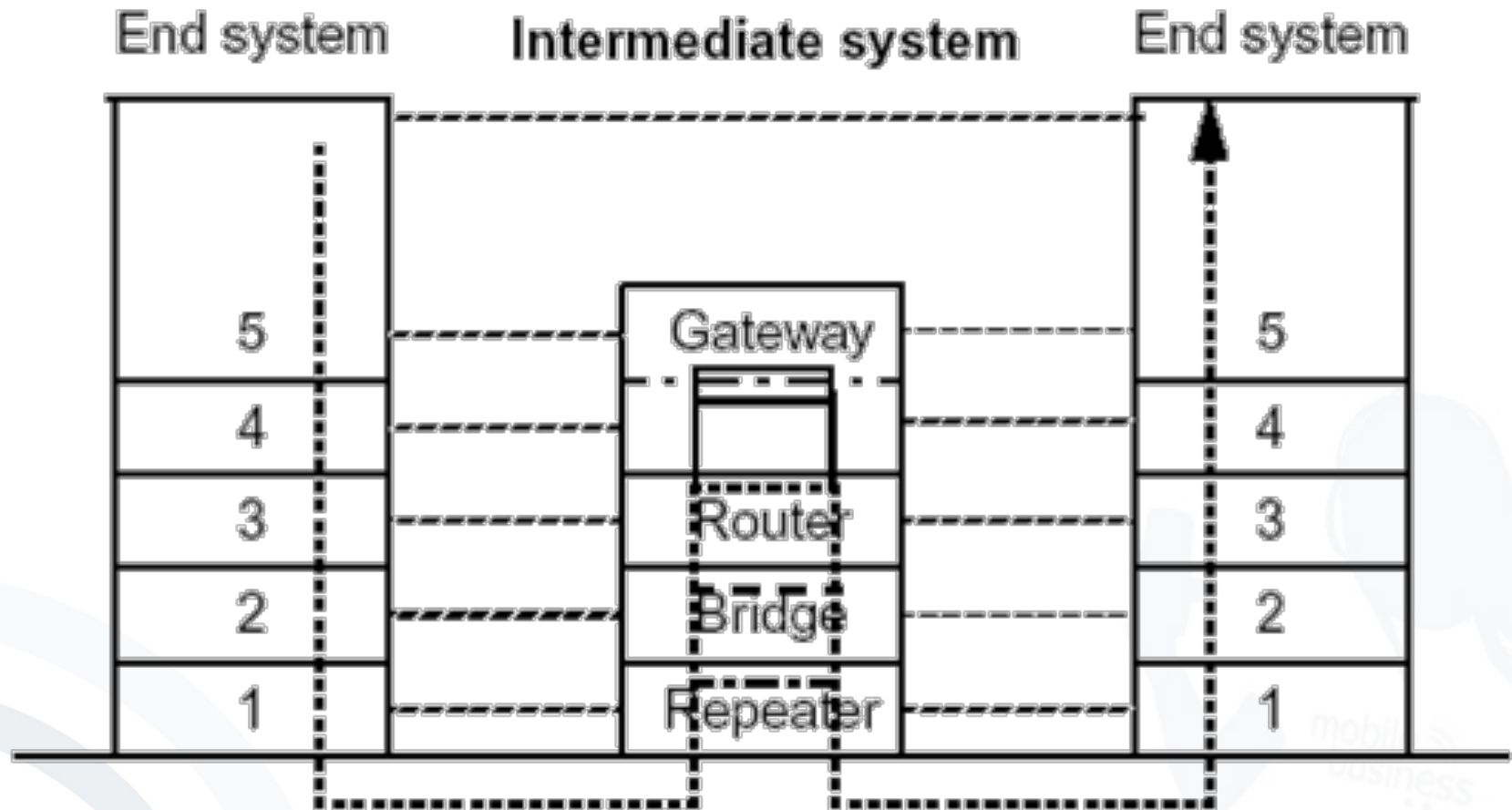


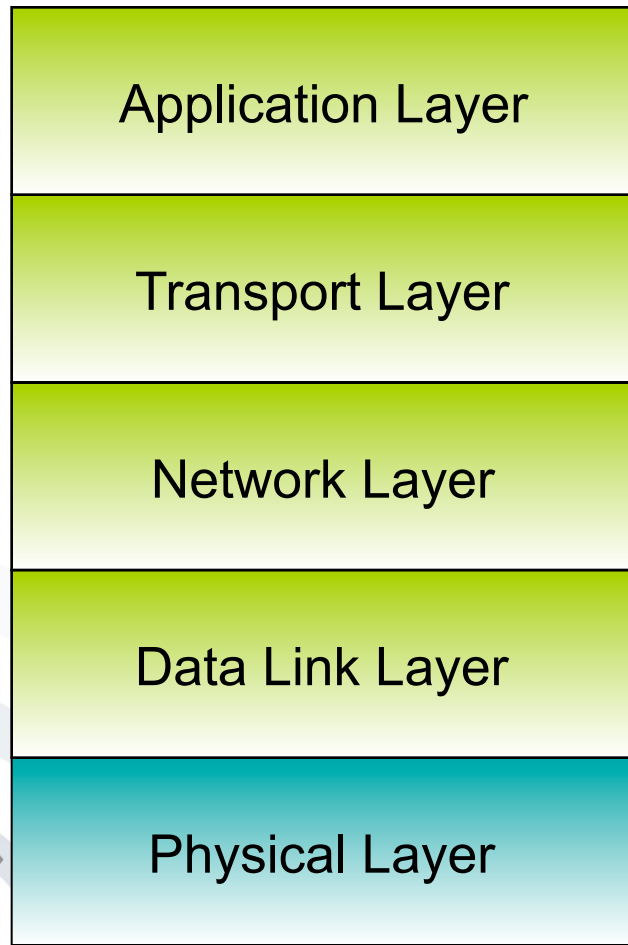
- Information technology – Open Systems Interconnection – Basic Reference Model
- „7-Layer-Model“
  - First version  
ISO/IEC 7498-1:1984
  - Current version  
ISO/IEC 7498-1:1994

# Internet Reference Model



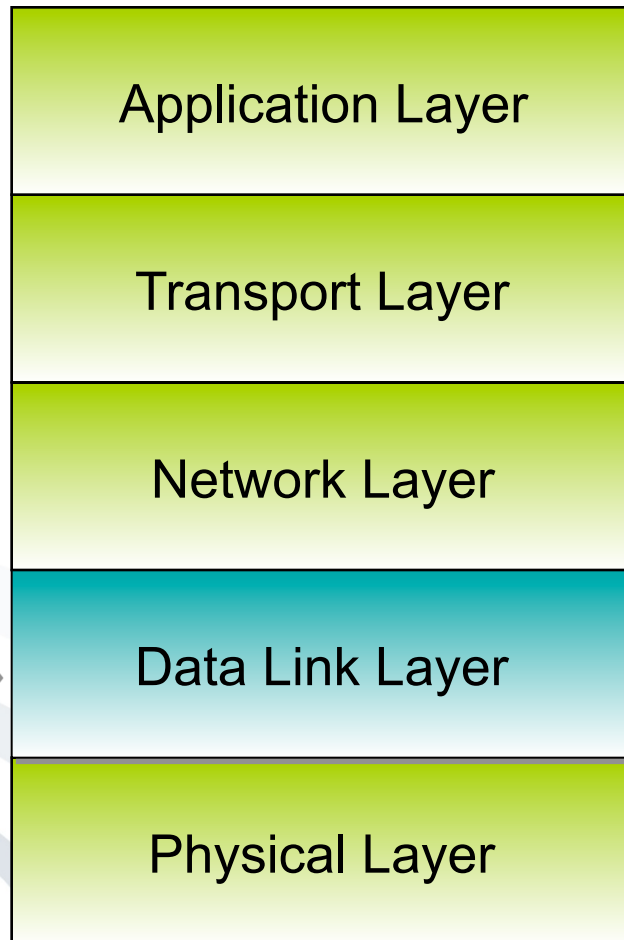
# Communication Example





## Tasks:

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

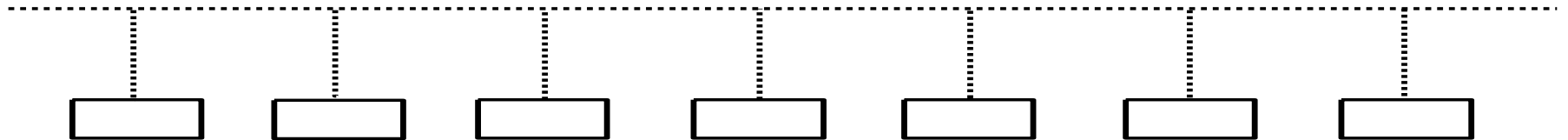


## Tasks:

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



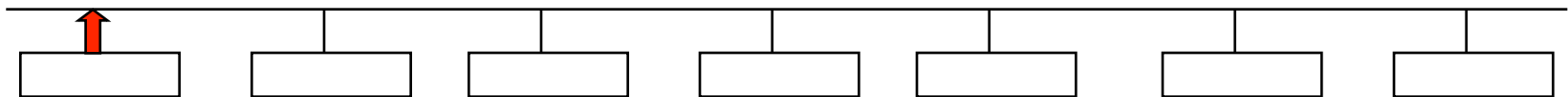
## ▪ Bus-Network



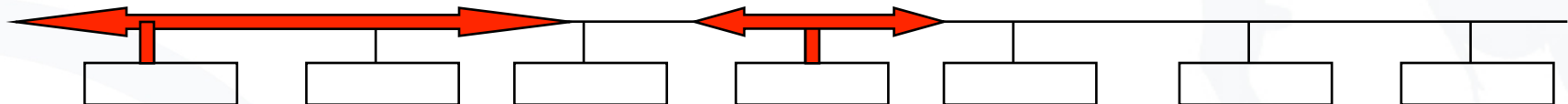
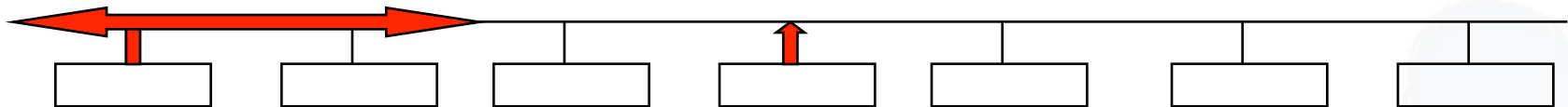
- Developed by XEROX
- Additional nodes can easily be added.
- Protocol: Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

## CSMA/CD:

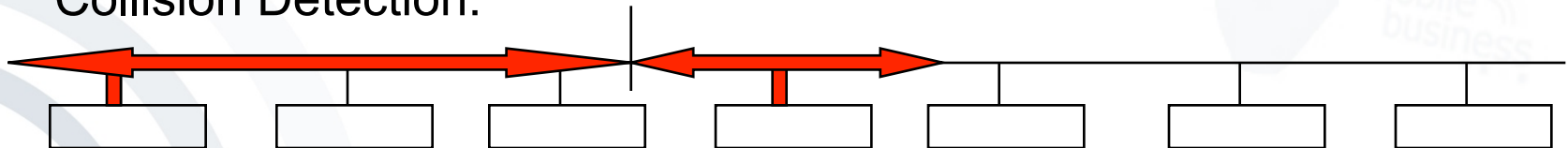
Carrier Sense:



Multiple Access:

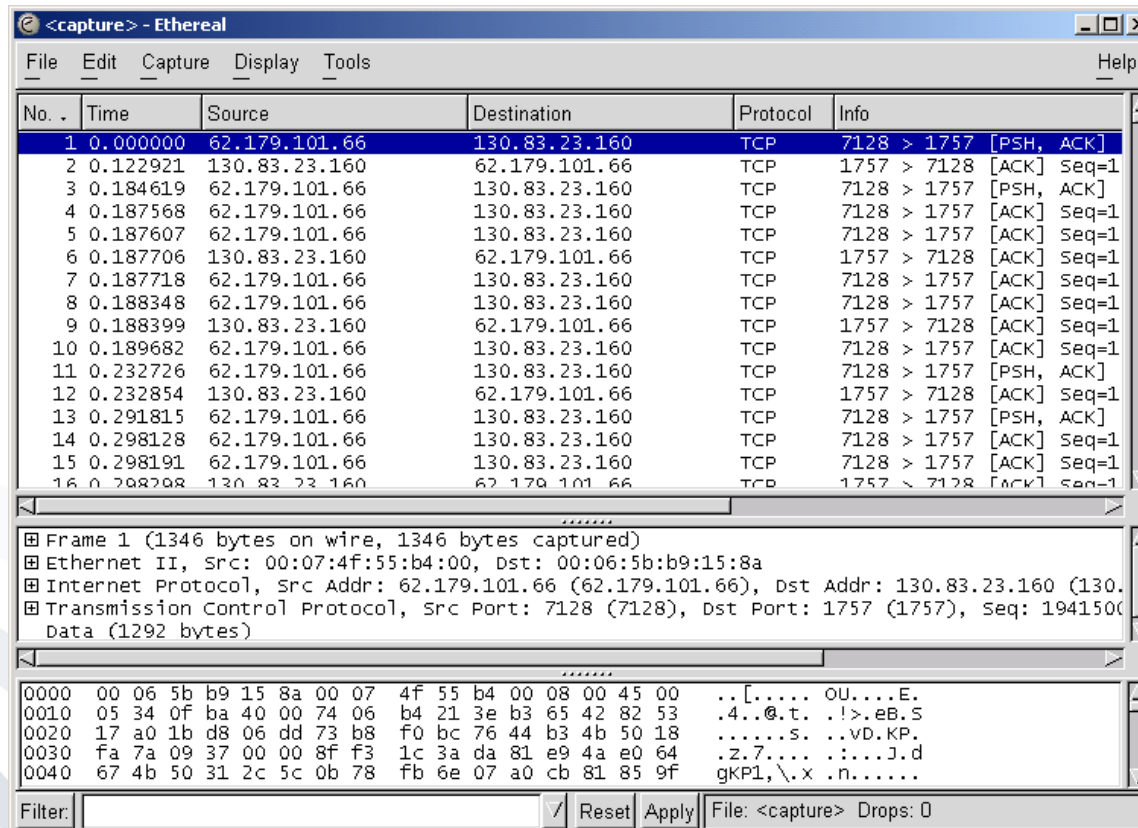


Collision Detection:



## Eavesdropping of all frames

i.e. Ethereal:



| 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  | 0.298298 | 130.83.23.160 | 62.179.101.66 | TCP      | 1757 > 7128 [ACK] Seq=1 |

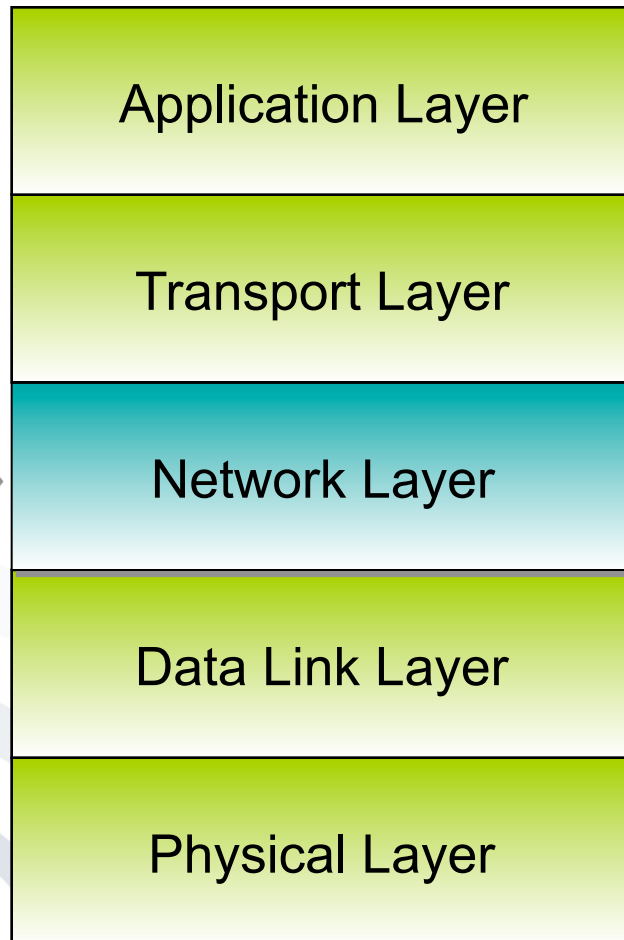
Frame 1 (1346 bytes on wire, 1346 bytes captured)

- 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, Data (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.....
  
```

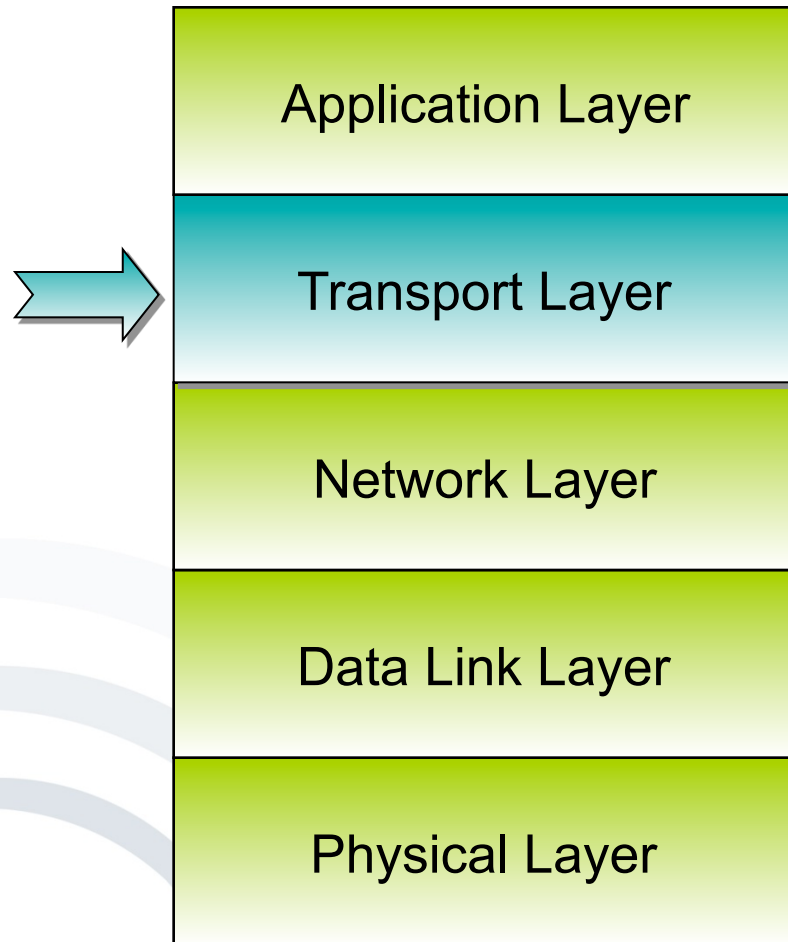
composite packets  
of higher protocol  
layers



## Tasks:

- End-to-end connections between systems
- Routing
- Addressing
- Typically connectionless

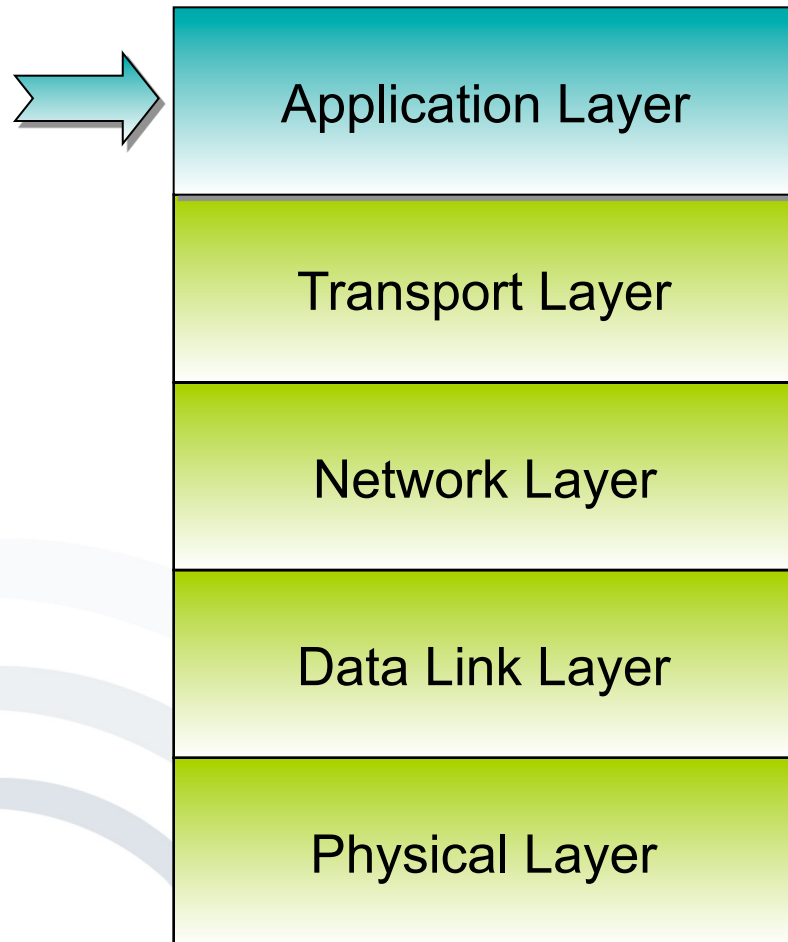
For example: IP



## Tasks:

- Connection between source and target
- Optimisation of quality of service and service costs
- Flow control
- Connection management

For example: TCP, UDP



## Tasks:

- provides 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

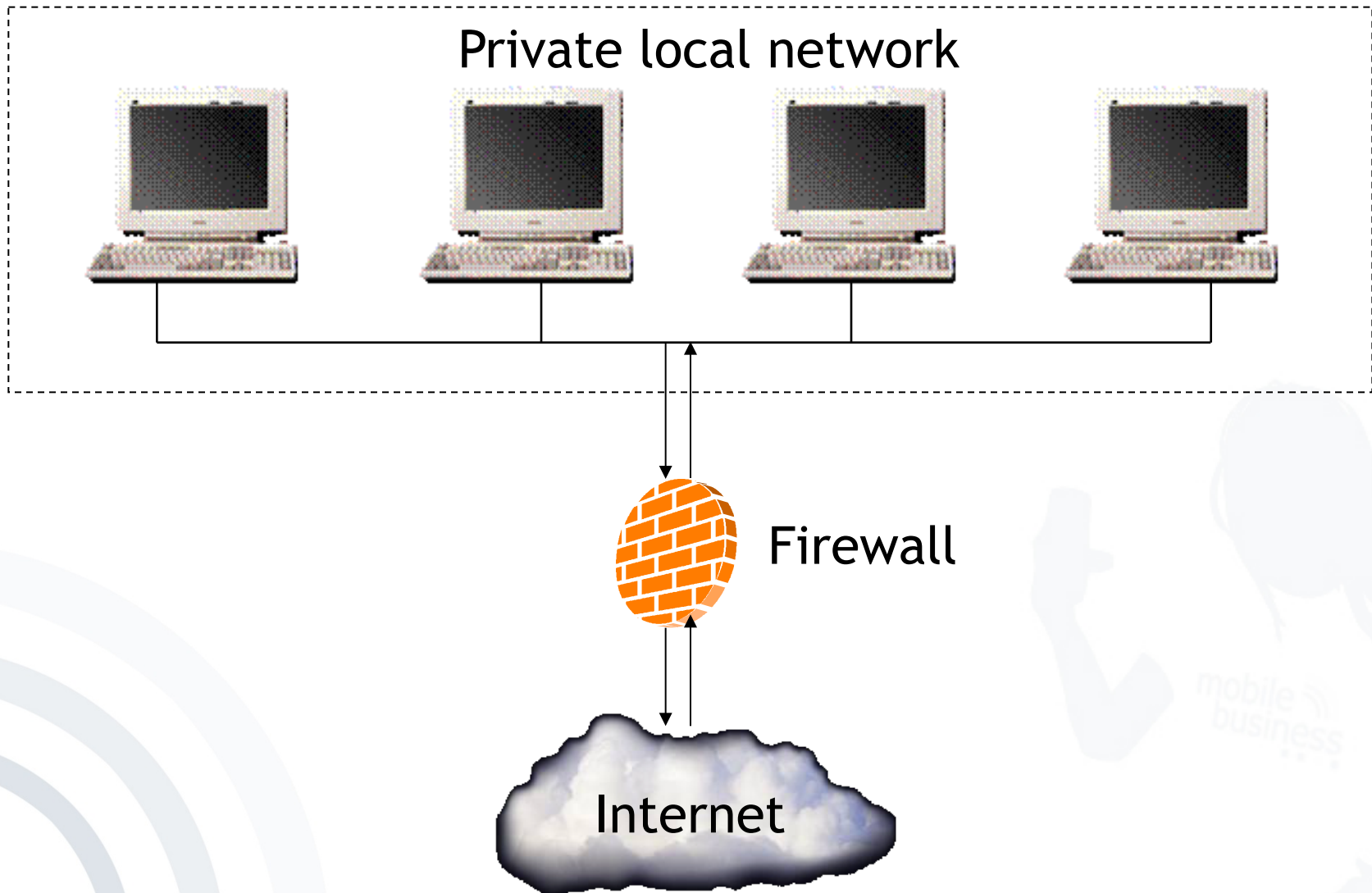
FTP: File Transfer Protocol

- 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



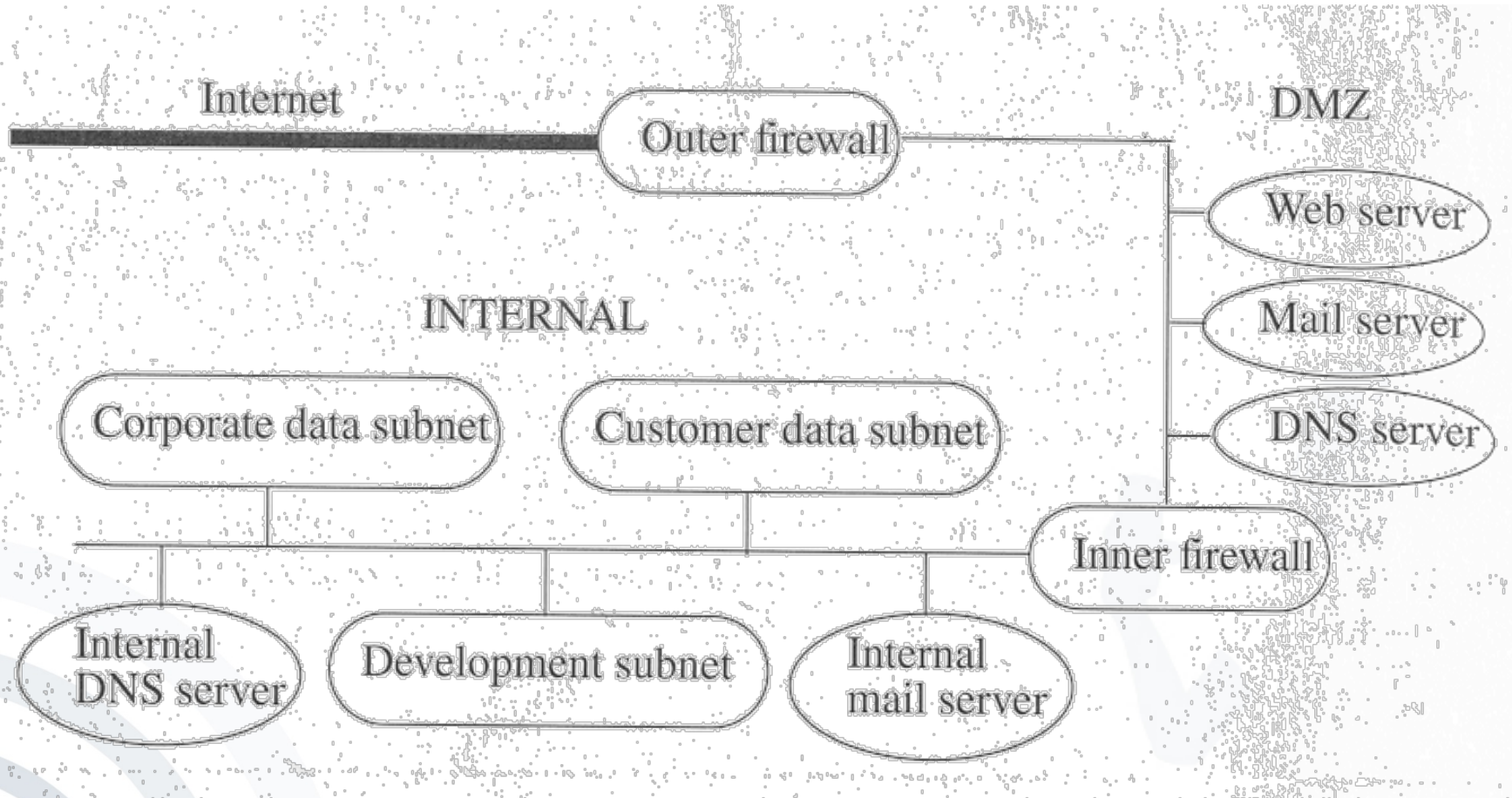
- „A firewall is an internetwork gateway that restricts data communication traffic to and from one of the connected networks (the one said to be *inside* the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be *outside* the firewall).“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

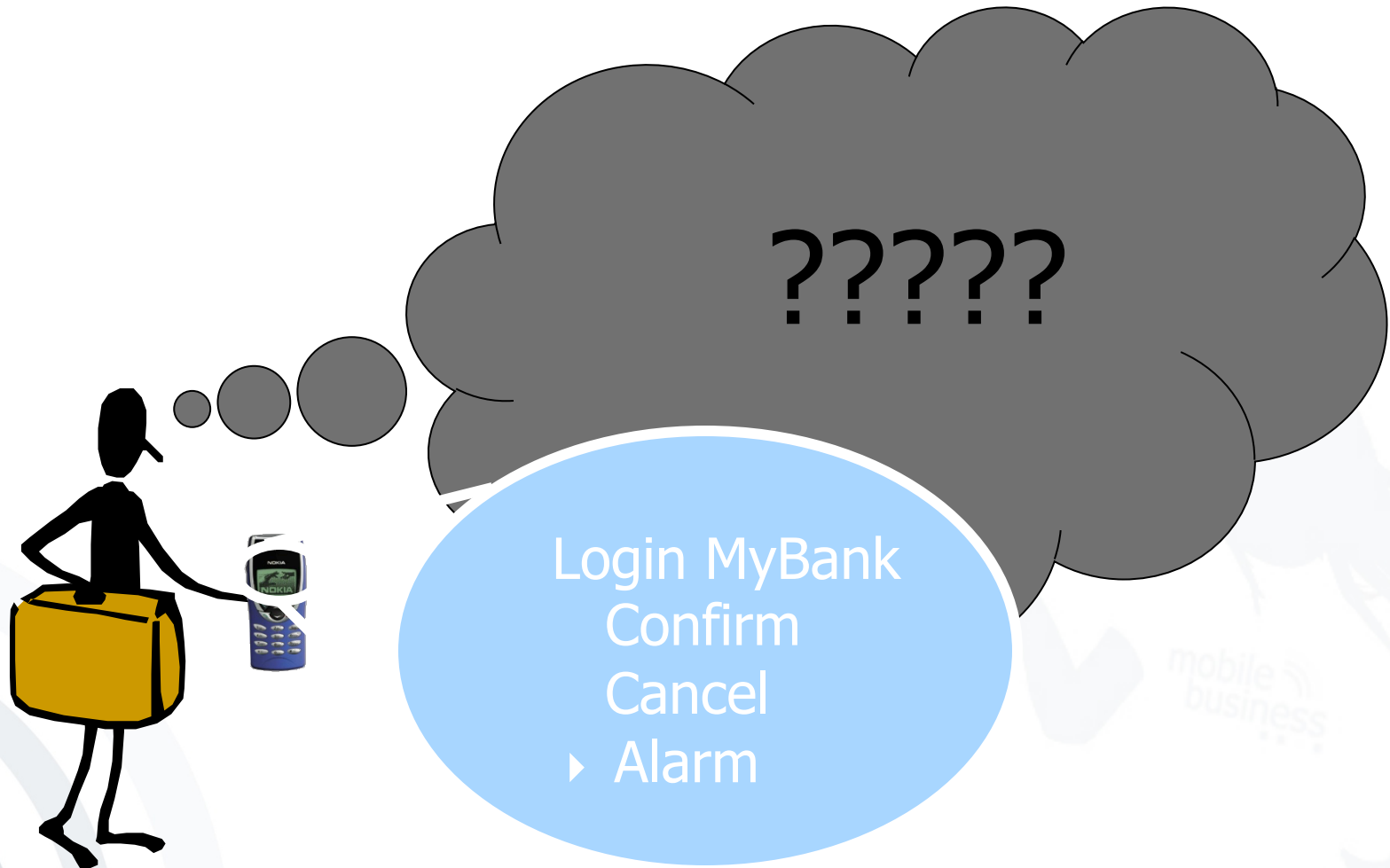


- Introduction
- Network Organisation
  - Firewalls
  - Demilitarized Zone
  - Intrusion Detection
- Security Protocols
- Wireless / Mobile Security

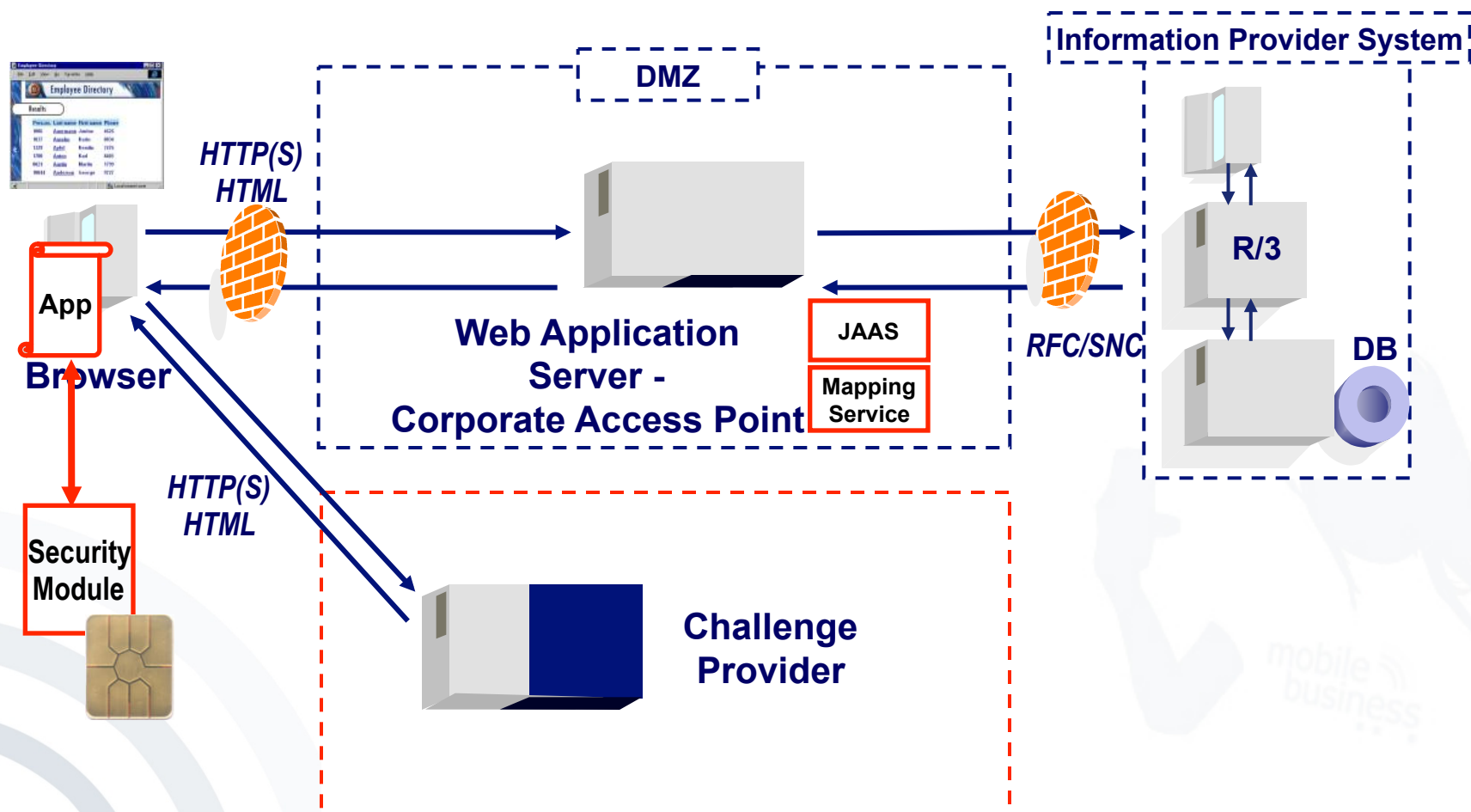
- The DMZ is a portion of a network, that separates a purely internal network from an external network. [Bi05]
- The “outer firewall” sits between the Internet and the internal network.
- The DMZ provides limited public access to various servers.
- The “inner firewall” sits between the DMZ and the subnets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

# Network using a DMZ





# Example: WiTness Security Module for Login Authorisation - System view



- 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: *Rootkits*
  - Exist for many versions of operating systems, i.e. Unix (but not only).
  - Can be designed to sniff passwords from the network and to conceal their presence.
  - Include tools to automate the installation procedure and has modified versions of system utilities.
  - Installer is assumed to have *root* privileges (hence the name - *rootkit*).
  - 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)*

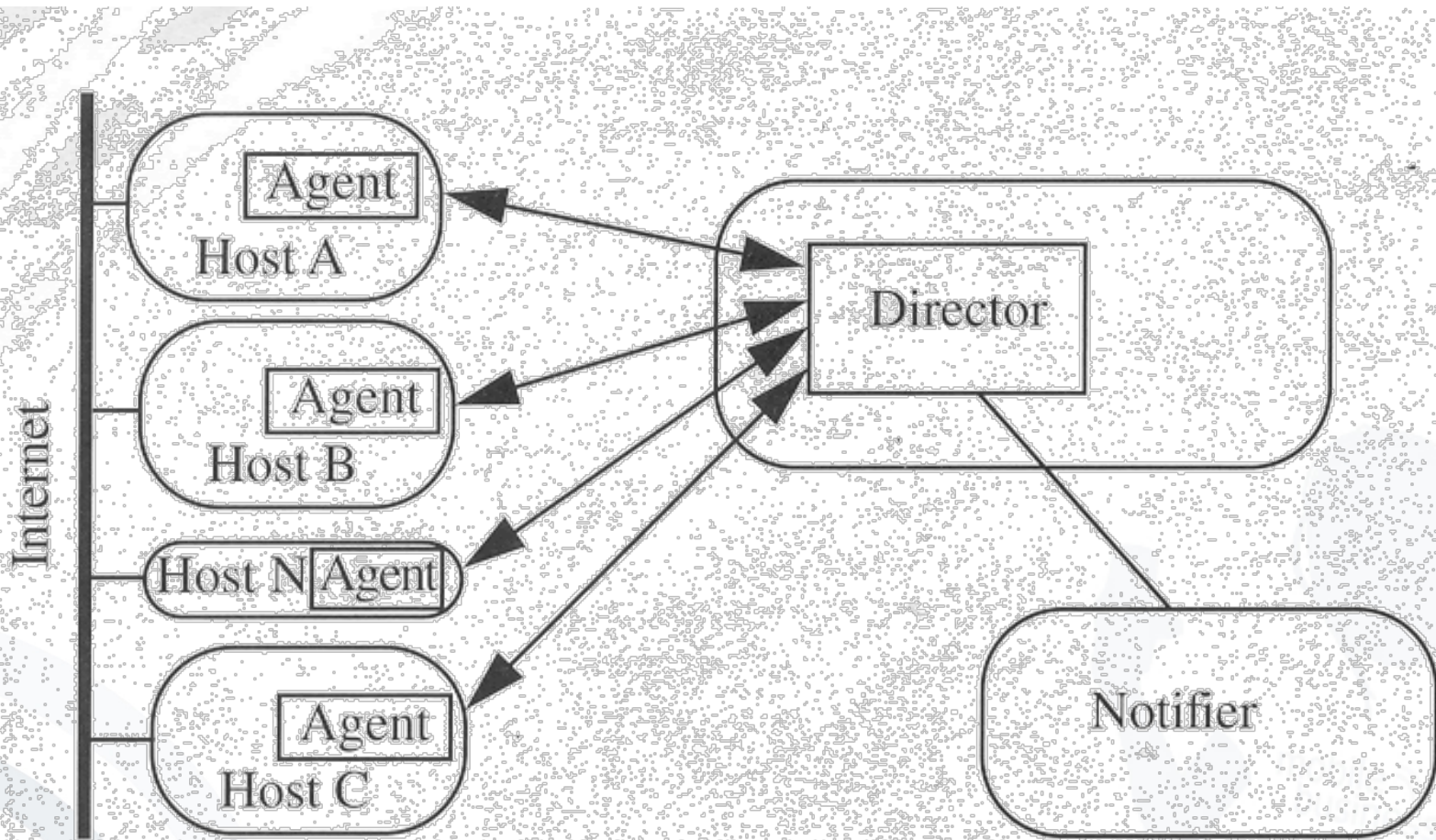
- NFR has three components:
  - The *packet sucker* reads packets off the network.
  - The *decision engine* uses filters written in a language called N-code to extract information.
  - The *backend* writes the data generated by the filters to disk.

- *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)*



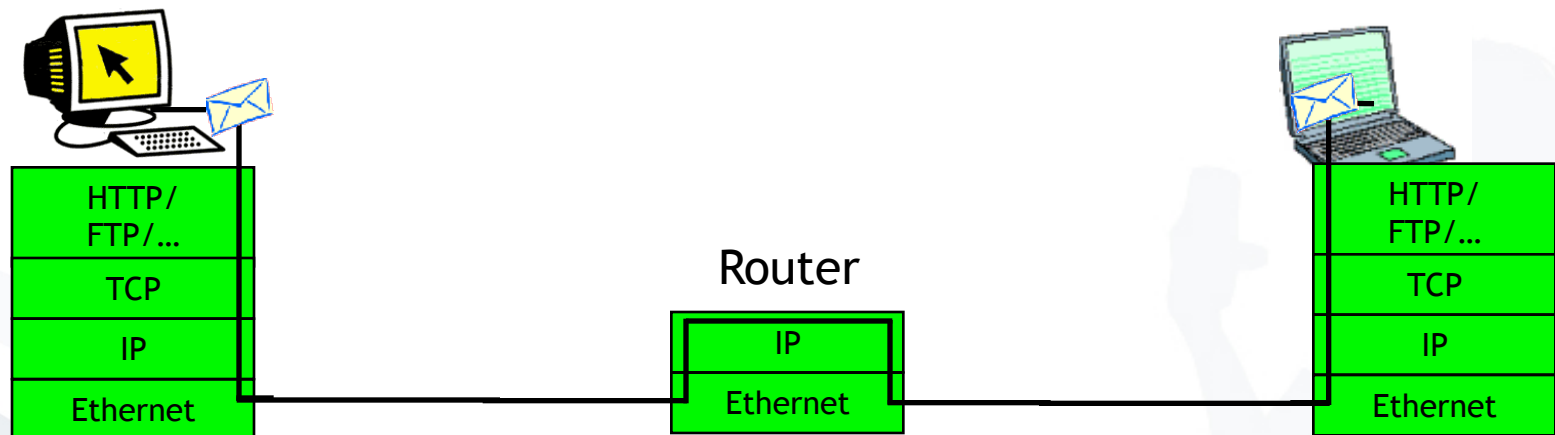
# Intrusion Detection System

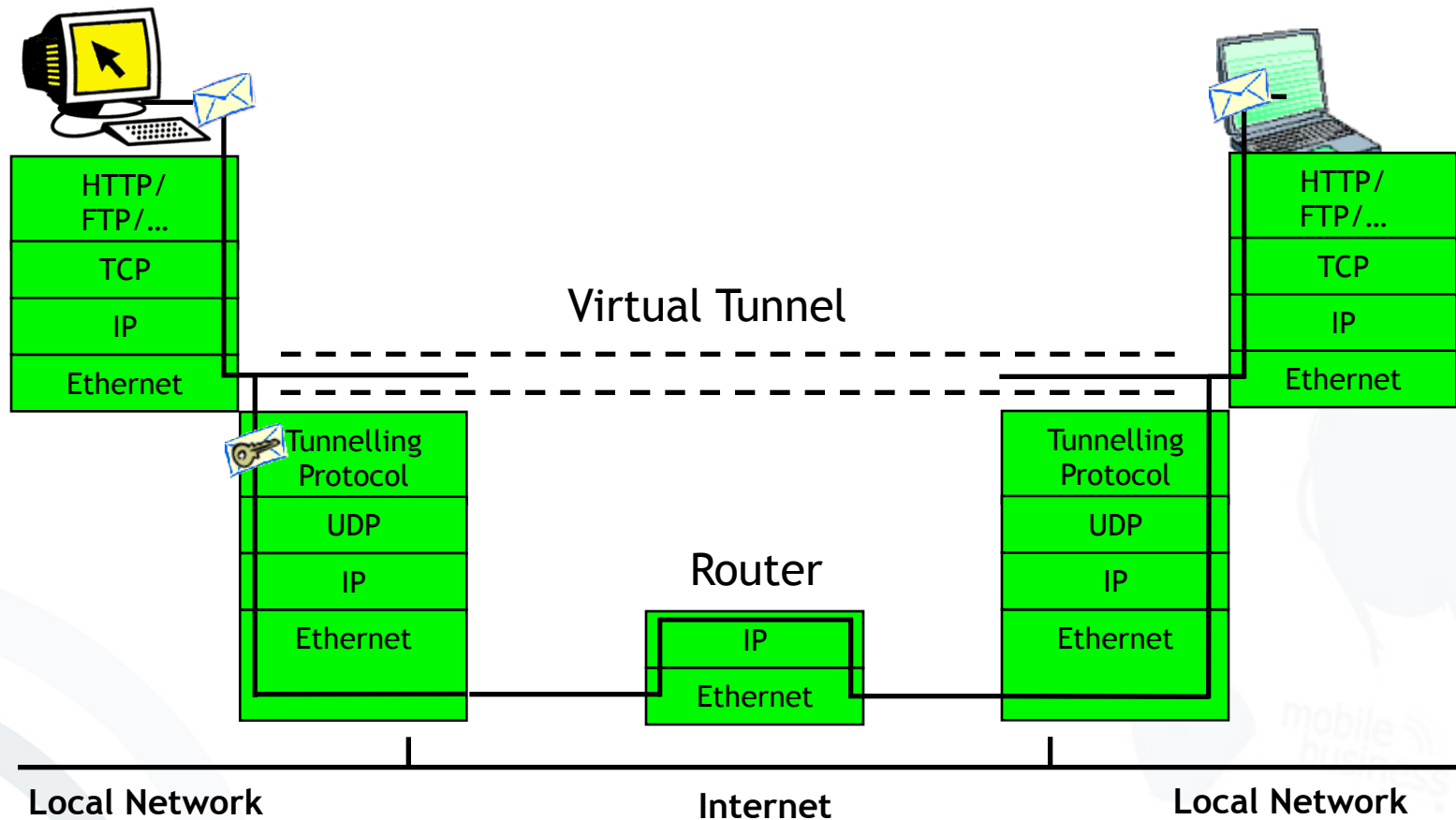


- Introduction
- Network Organisation
- Security Protocols
  - Virtual Private Networks
  - Secure Socket Layer
  - IPsec
- Wireless / Mobile Security

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

# Communication without a VPN



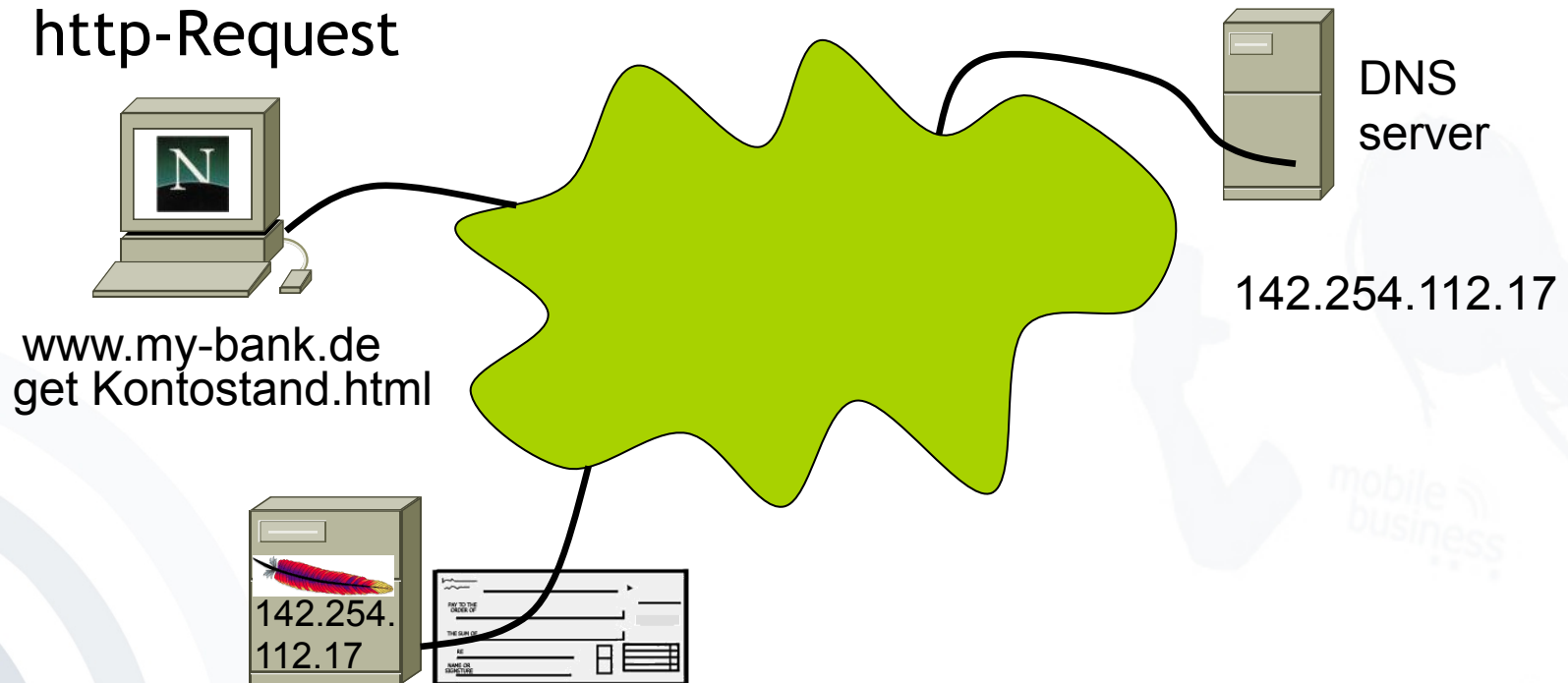


- Introduction
- Network Organisation
- Security Protocols
  - Virtual Private Networks
  - Secure Socket Layer
  - IPsec
- Wireless / Mobile Security

`www.my-bank.de/Kontostand.html`

Actions of the browser:

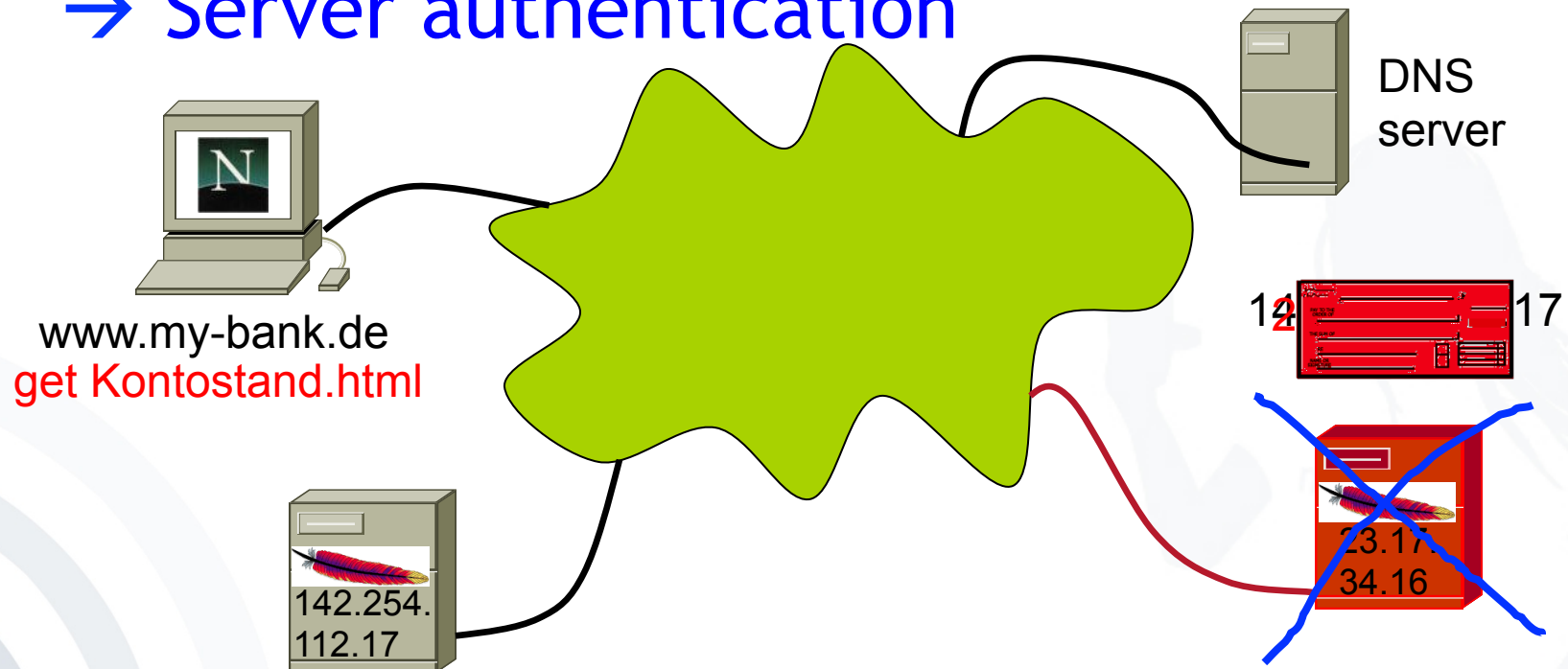
1. DNS-Request
2. http-Request



Possible attacks:

## 1. Compromise of DNS (DNS spoofing)

→ Server authentication

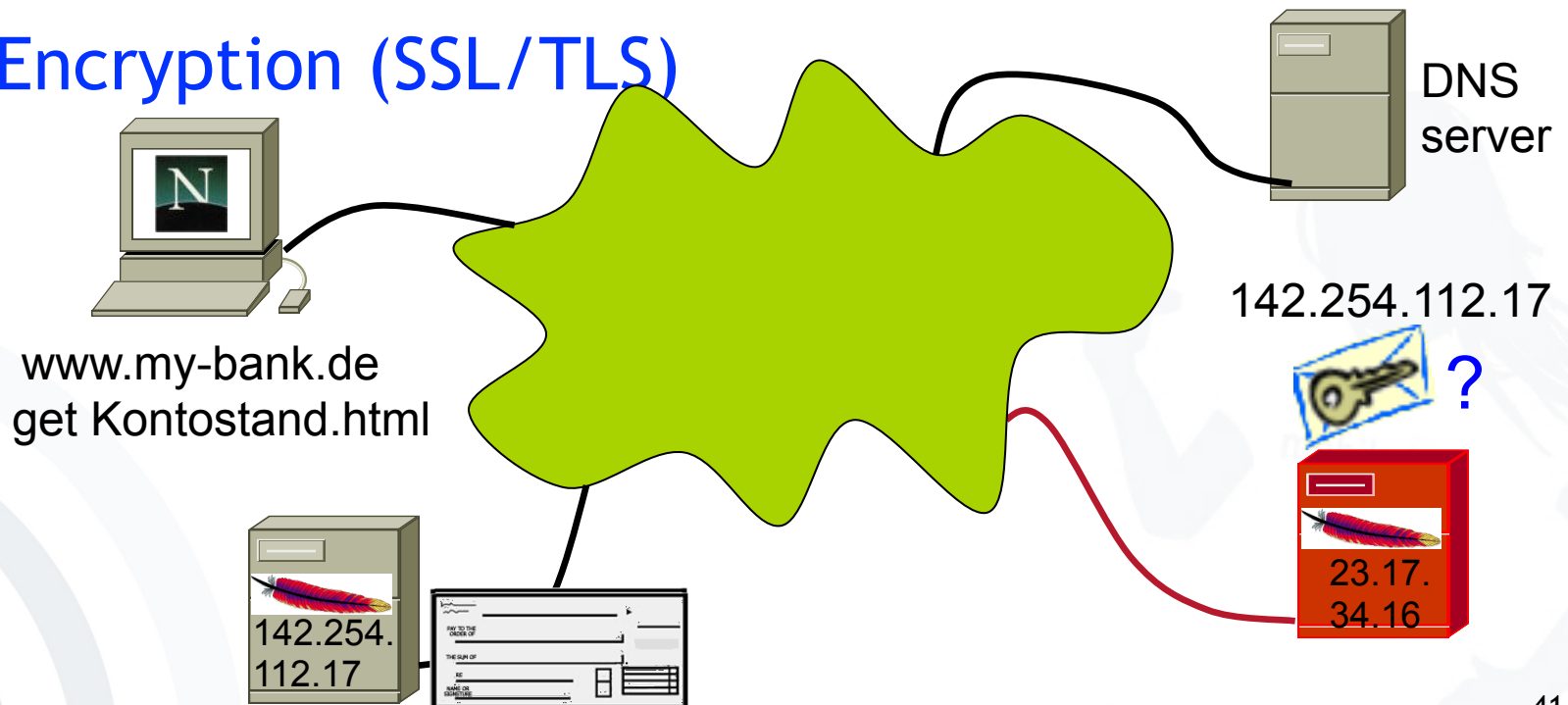




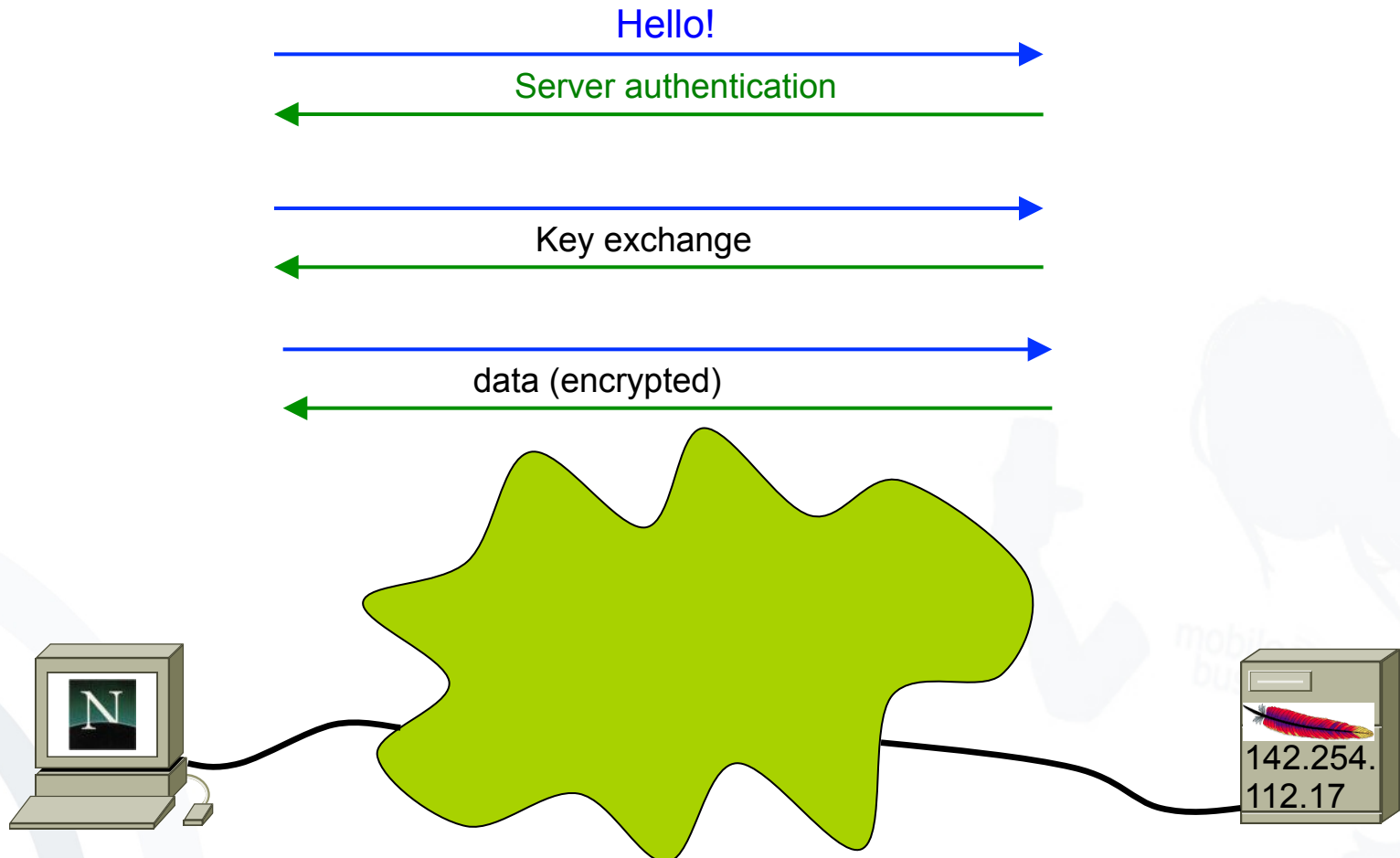
Possible attacks:

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

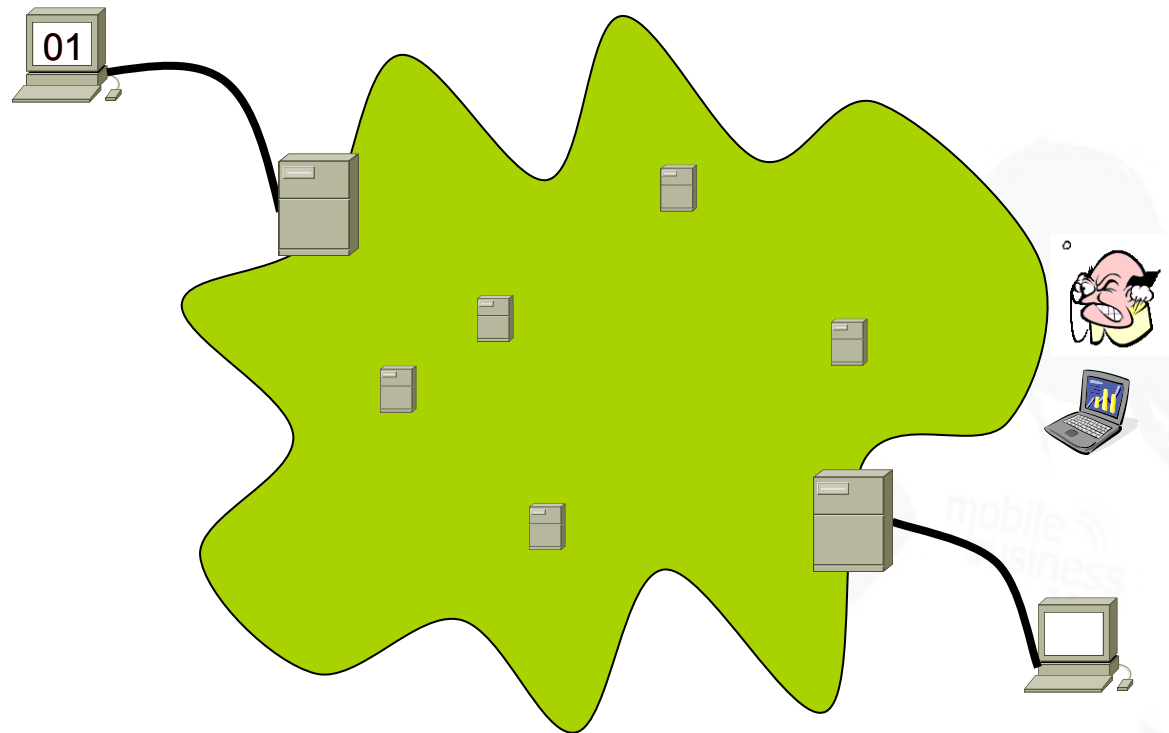
| Security Goal      | http | https (SSL/TLS)        |
|--------------------|------|------------------------|
| Authenticity       | ✗    | ✓ (mostly server only) |
| Non-Repudiation    | ✗    | ✗                      |
| Confidentiality    | ✗    | ✓                      |
| Integrity          | ✗ 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

- Serious vulnerability in the popular OpenSSL cryptographic software library
- OpenSSL is an open-source implementation of the SSL/TLS protocol.
- Heartbleed is **not** a design flaw in SSL/TLS protocol, but it is an **implementation problem** in the OpenSSL library.
- When the vulnerability is exploited, it leads to the leak of memory contents from the server to the client and from the client to the server.
- CVE-2014-0160 is the official reference to this bug ([www.cve.mitre.org](http://www.cve.mitre.org)).



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

- Attacker is able to eavesdrop IP packets.
- Ideally: at the gateway of sender or recipient

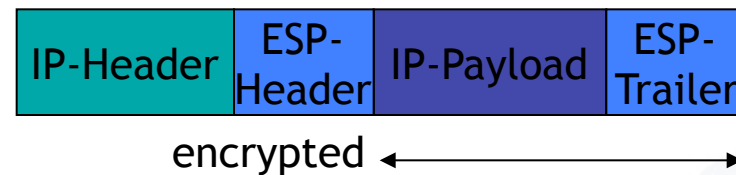


# Encapsulating Security Payload (ESP)

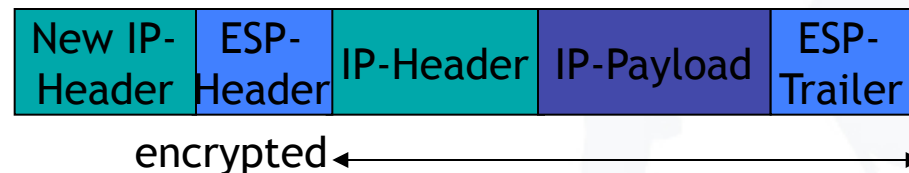
- Data Packet



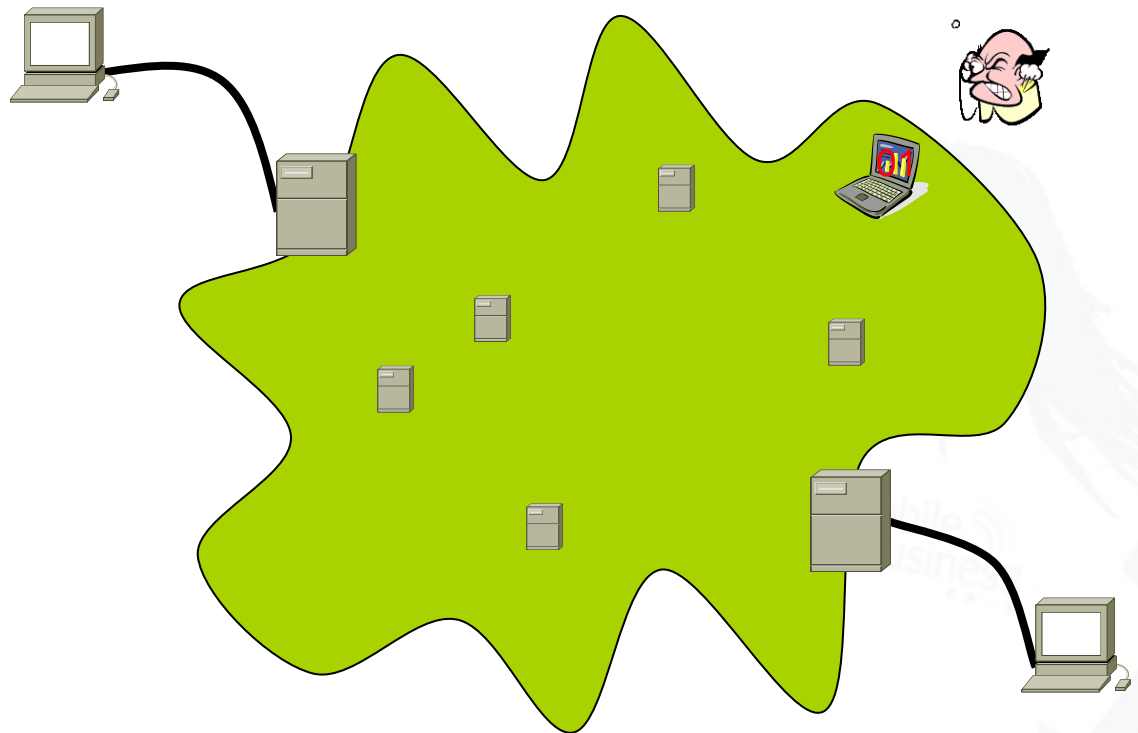
- ESP-Transport-Mode



- ESP-Tunnel-Mode

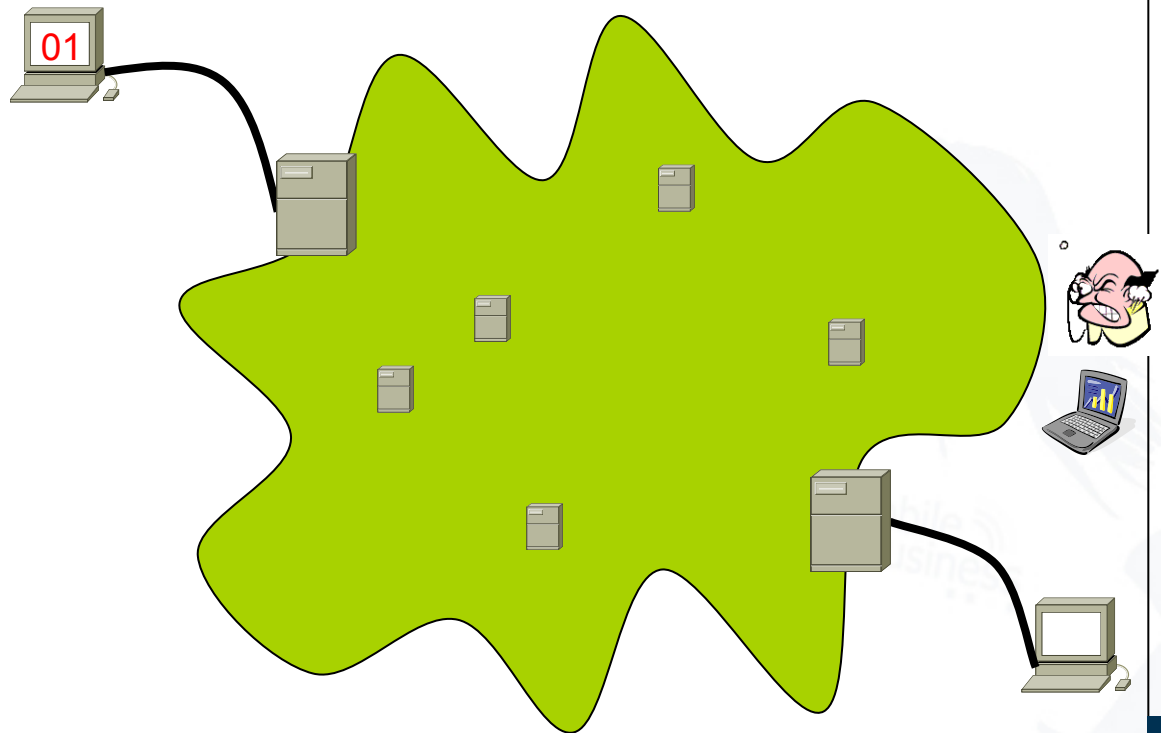


- Attacker sends IP-packets with a faked sender address.





- Attacker impersonates the recipient.

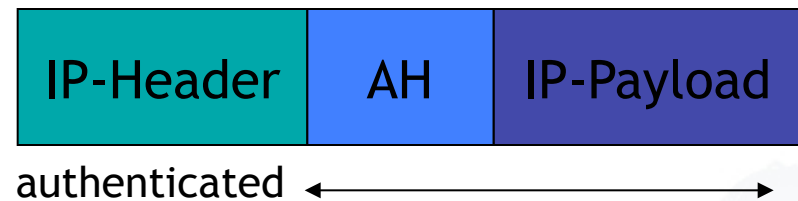


# IPsec Authentication Header (AH)

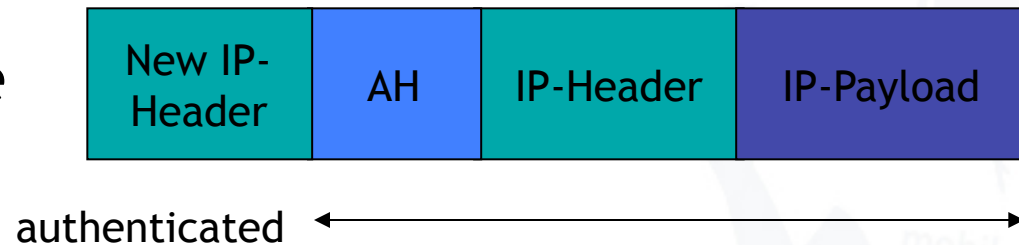
Data Packet



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
- **[He14] Heartbleed:** “The Heartbleed Bug”, [www.heartbleed.com](http://www.heartbleed.com)
- **[RFC 2828] Network Working Group:** “Request for Comments 2828 - Internet Security Glossary”, 2000, [www.faqs.org/ftp/rfc/pdf/rfc2828.txt.pdf](http://www.faqs.org/ftp/rfc/pdf/rfc2828.txt.pdf)
- **[Ta96] A.S. Tanenbaum:** Computer Networks, 3rd Edition, 1996 [4th edition available]