Veilig op Internet - 2

Toen werd het lastiger
hardware, protocollen & port basics

DSE, 12 jan 2010
Egbert-Jan Sol

Veilig op Internet

essentiële basiskennis

DSE, 12 juni 2010

Eric Ideler

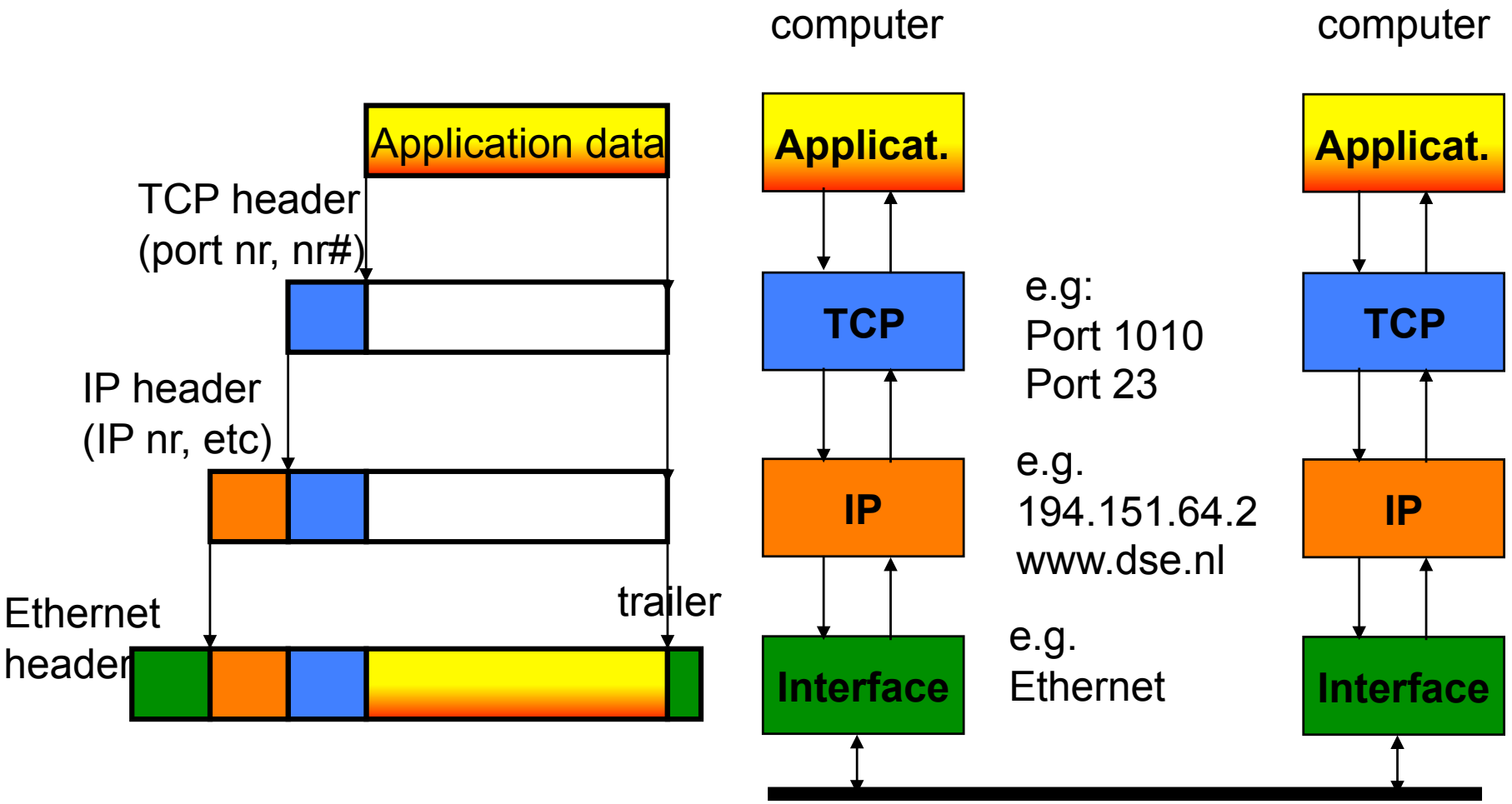
Veilig op Internet - 3

Firewalls, Man-in-middle, trojean horses, D-DoS, IPSec, keys

DSE, ??

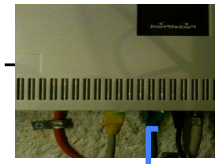
Bij belangstelling & goede spreker

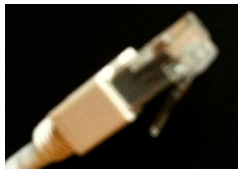
IP: The Internet Protocol with TCP



UPC (Cable), KPN (xDSL), OnsNet (Glasvezel)

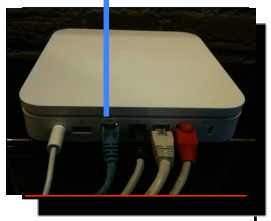
(Kabel, Glasvezel) **Modem**





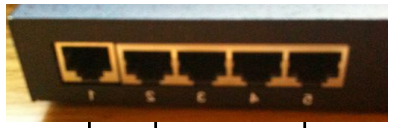
Ethernet
10Mbps UTP (untwisted pair)
100Mbps UTP (Cat 5, RJ45 stekker)
1000Mbps = 1Giga bits per seconde

Home Network:

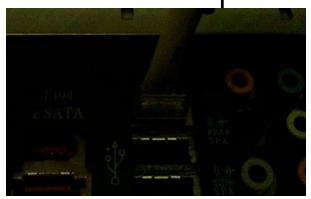


Router met Firewall

Ethernet **Switch**



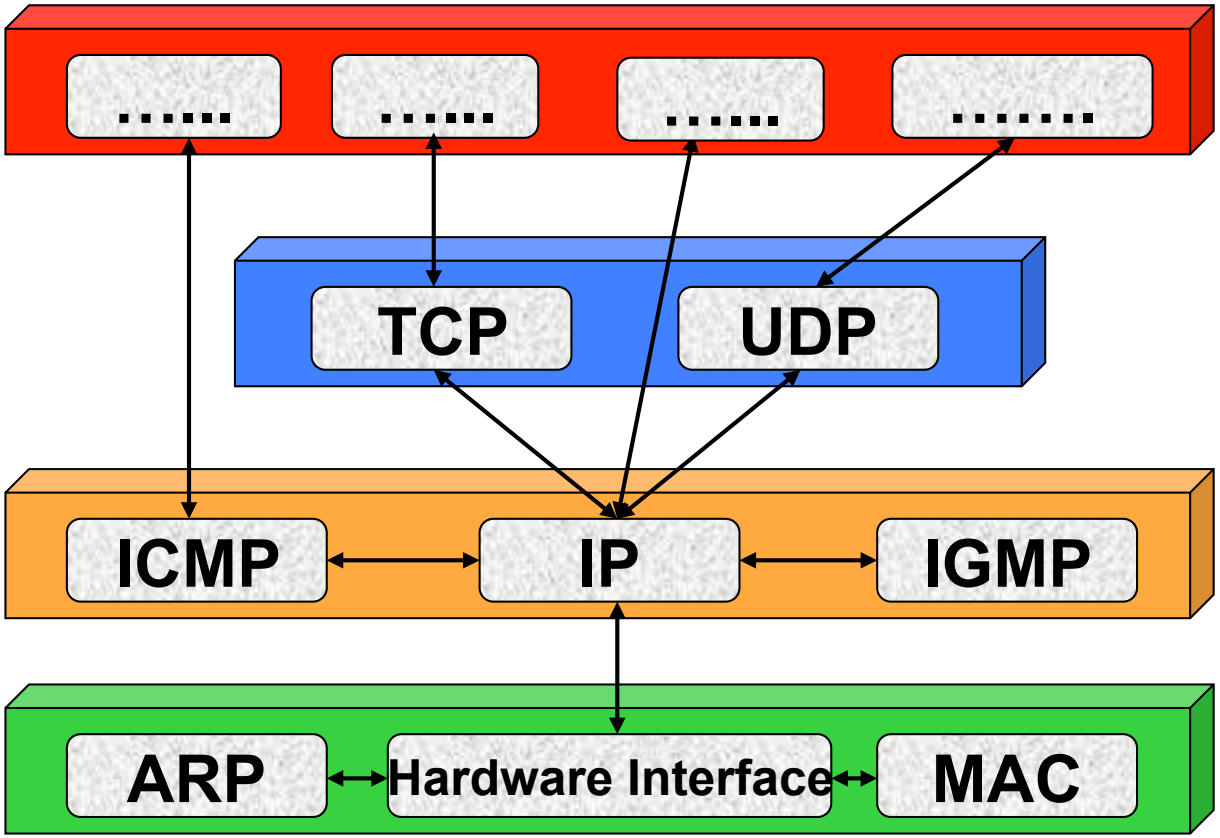
TV (IPTV)



PC/MAC (MS-Windows & Mac OS X)
(Ethernet draad: 1Gbps, 100Mbps),

Draadloos Netwerk (WiFi)
(Wireless LAN, max 54 Mbps)
Notebooks (802.11a/b/e/n)
Tables (iPad, Android) &
Smart Phones (iPhone, etc)

Protocol layers



Application

Transport

Network
(IETF RFC)

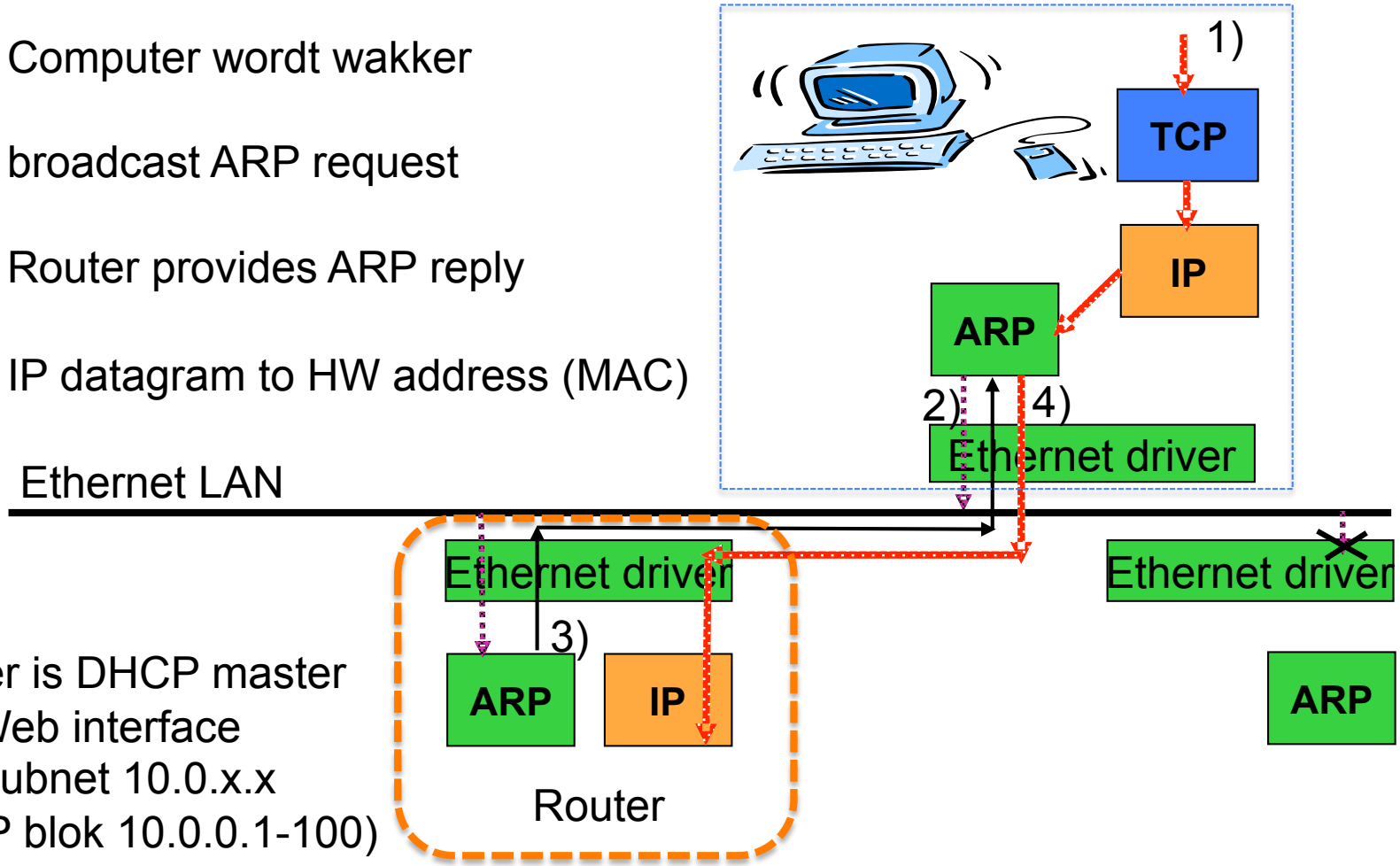
Link
(IEEE 802.1-16)

IP = Internet Protocol met IP Adres: 10.0.0.1 (IPv4)

IEEE 802.1 MAC (media access control) F8:1E:DF:9A:52:20
IEEE 802.3 Ethernet (draad)
IEEE 802.11 Wireless LAN (WiFi)
IEEE 802.15 Bluetooth (ook MAC adressen)

Address Resolution Protocol
(ARP)

1) Computer wordt wakker
2) broadcast ARP request
3) Router provides ARP reply
4) IP datagram to HW address (MAC)

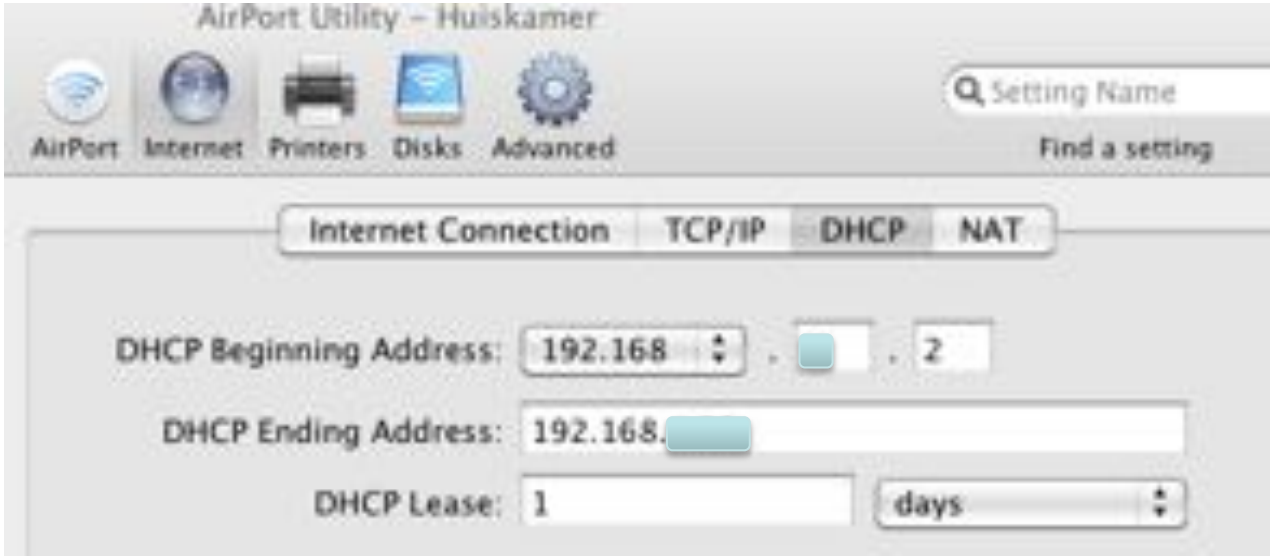


Router is DHCP master
(via Web interface
bijv subnet 10.0.x.x
DHCP blok 10.0.0.1-100)

Dynamic Host Configuration Protocol (DHCP)
(De allereerste keer en bij totale reset)

- Without DHCP:
  - each host must be configured individually (Name - IP address)
  - moving a host requires adaptation of the configuration

- With DHCP: Router with DHCP server needed to configure hosts at start-up

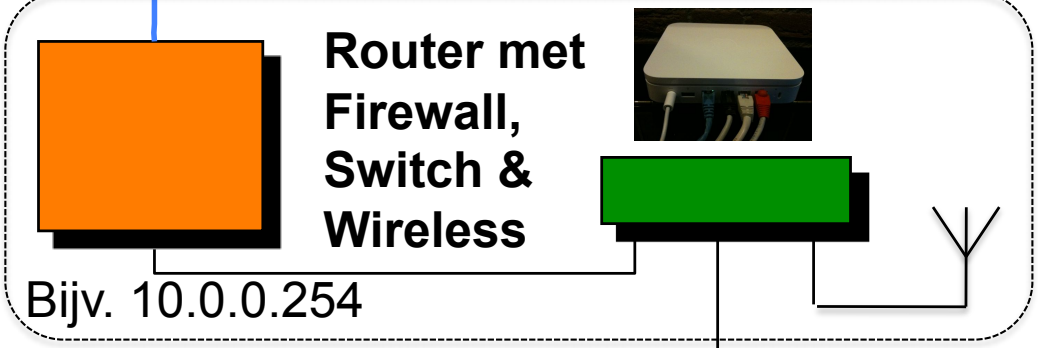


- DHCP issues
  - IP-address is 'leased'

(Kabel, Glasvezel)
Modem

Bijv. IP van provider
195.83.72.145

Home Network:



Bijv. 10.0.0.x (met 1<x<254)

Bijv. 10.0.0.1

PC/MAC

Draadloos Netwerk (WiFi)
(Wireless LAN, max 54 Mbps)
Notebooks (802.11a/b/e/n)
Tables (iPad, Android) &
Smart Phones (iPhone, etc)

Intermezzo: Wireless LAN (WiFi)

802.11 a/n (2.4 Ghz (magnetron freq) en b/g/n (5Ghz)) (is geen Mbps)

Wireless LAN (tot 150 m) altijd met beveiling/security WPA, liefst WPA2

Aktie lijstje

1. Modem, Router, Switch installeren en kabels klaar zetten
2. Router aan Modem en dan PC met fix adres (afh. Router bijv. 10….)
   router configureren (soms via web http://10.0.0.254 of Airport Utility config.)

3. (PC van vast weer naar dynamisch IP en uitzetten)
4. Router en PC's, etc aanzetten en controleren.

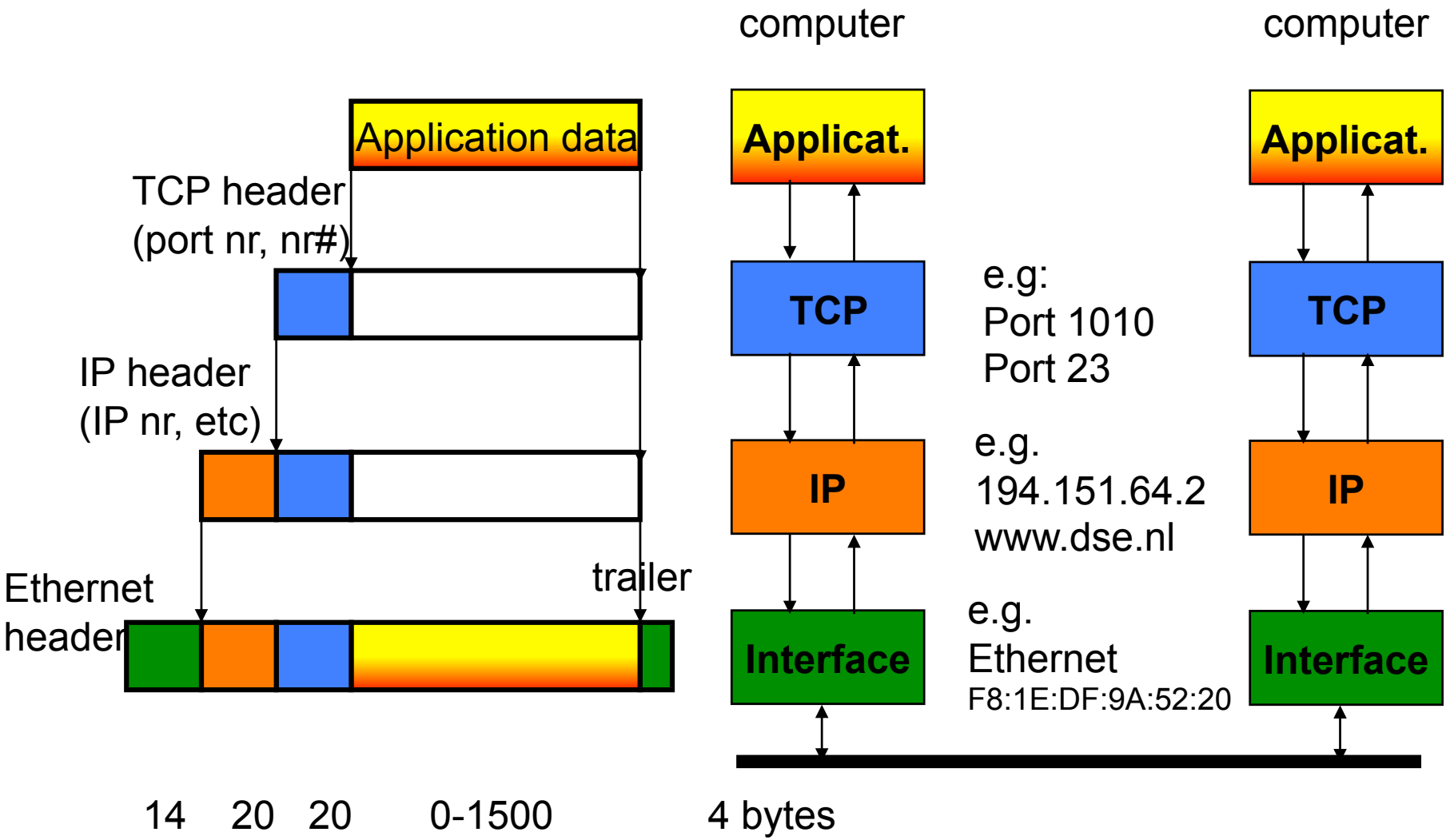
5. (PC, tablets, notebooks, etc) zend hun MAC met een ARP uit en krijgen IP)

6. In Router worden subnet IP (10.0.0.x) omgezet in een IP zoals 125.45.3.80
   en met port mapping vindt NAT (network address translation) plaats

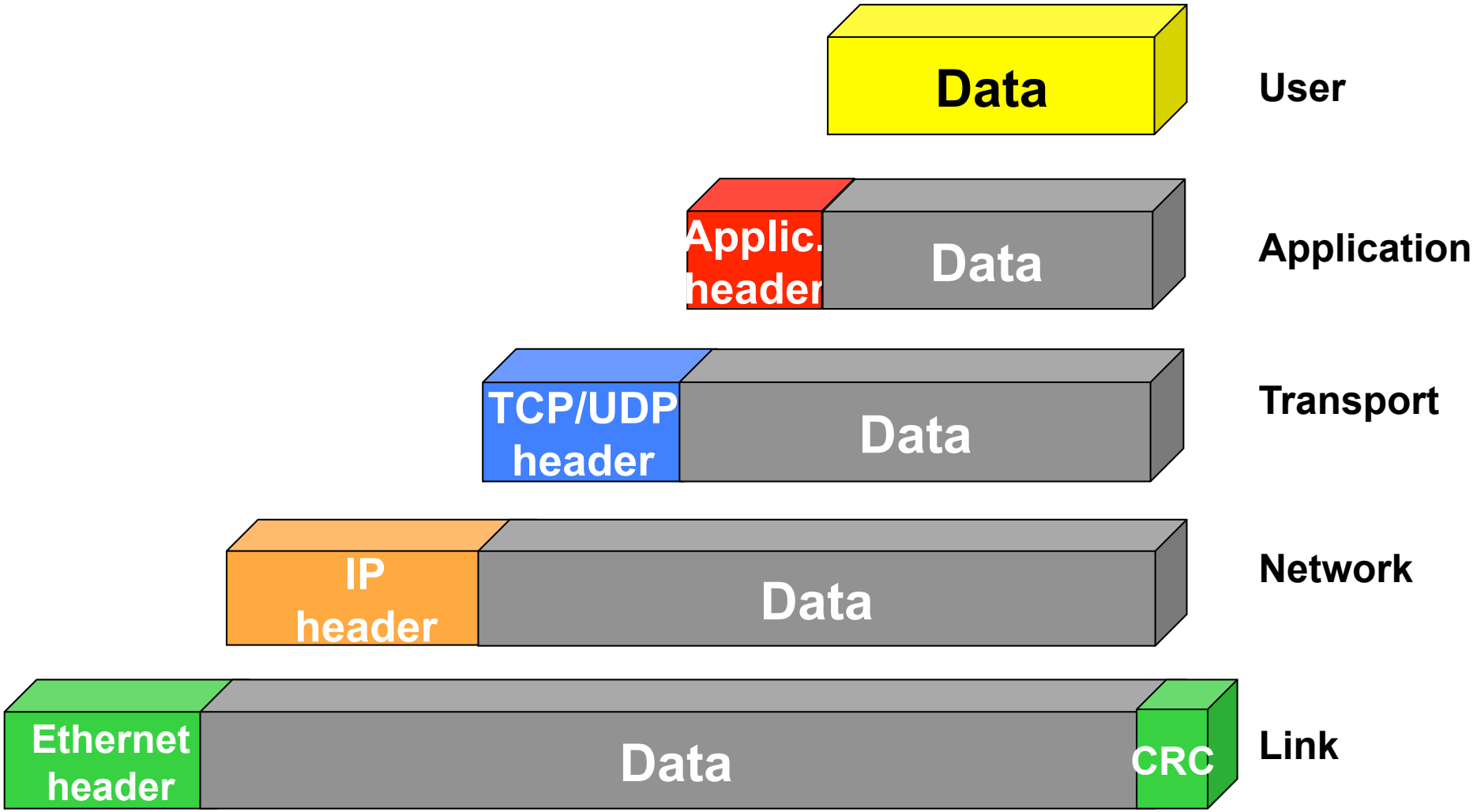
Wat moet je weten (en wat niet): Alleen IP nummers
(Ethernet MAC naar IP en IP-TCP-portnummers naar NAT niet),

Alleen de eerste keer is DHCP en bij firewall soms port nummers van belang
EN BIJ WIRELESS LAN security instellingen (WPA/WPA2)

IP: The Internet Protocol with TCP

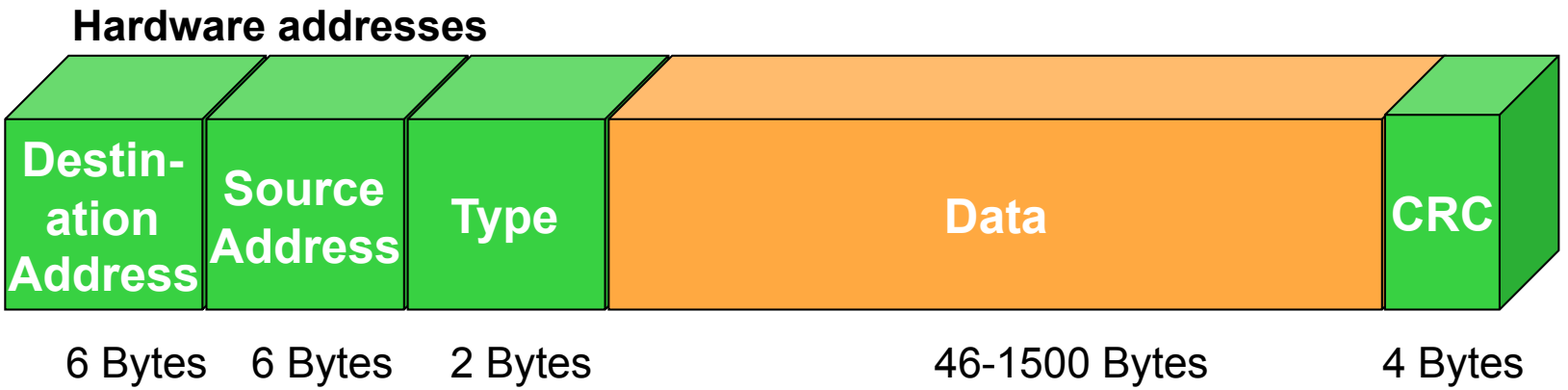


Encapsulation



Ethernet encapsulation

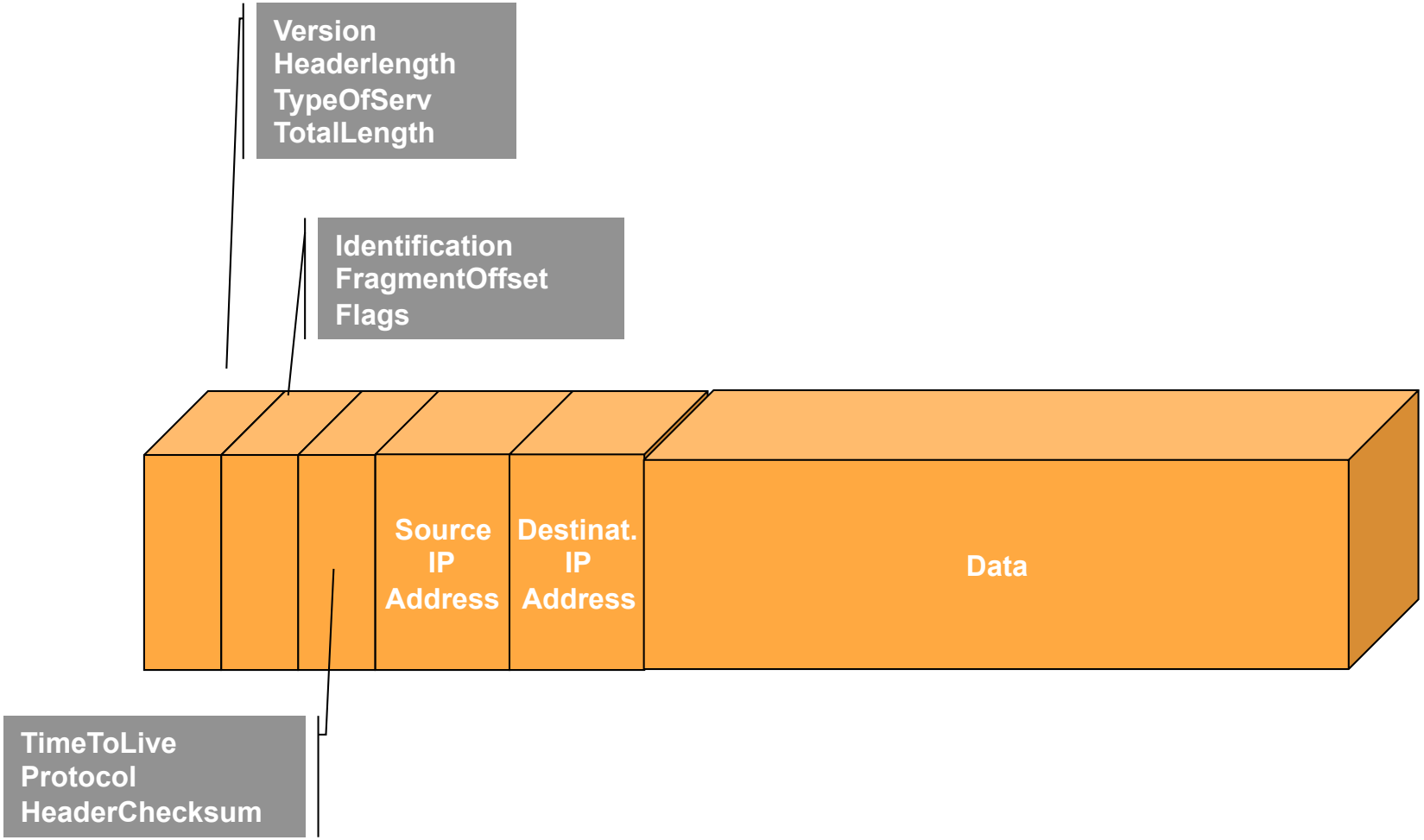
RFC 894



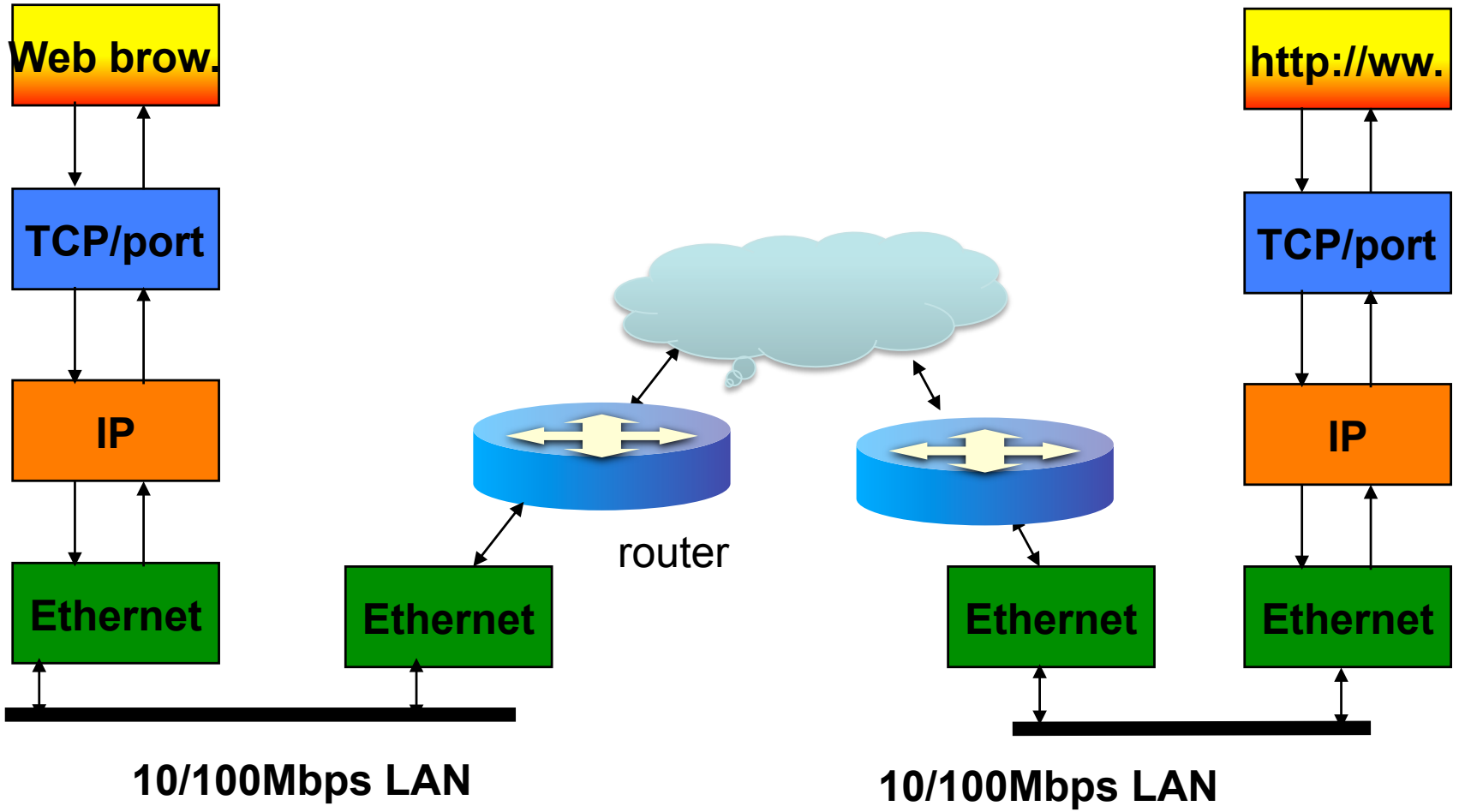
F8:1E:DF:9A:52:20

F4:1C:D2:97:52:8B

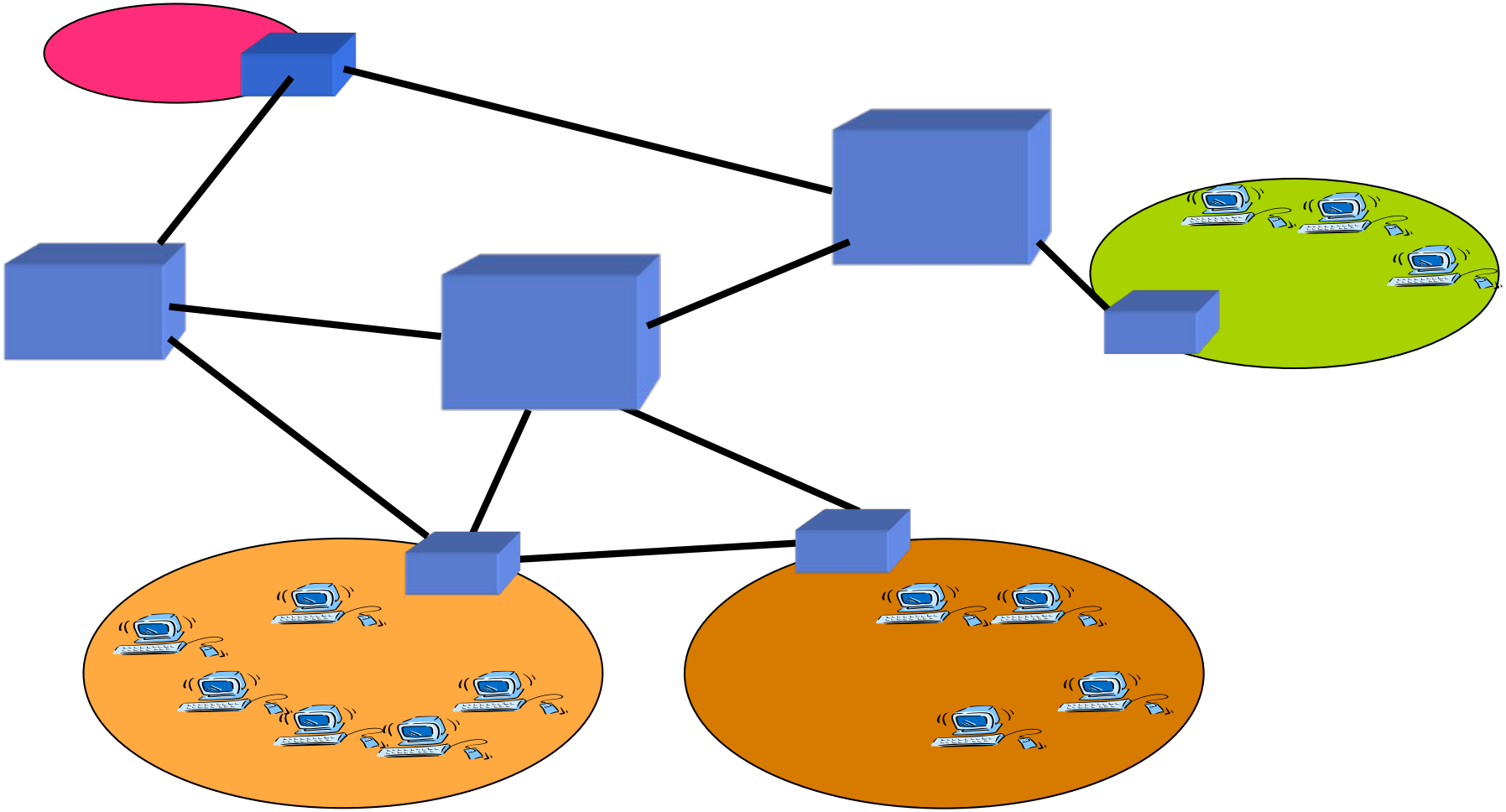
Internet Protocol IP



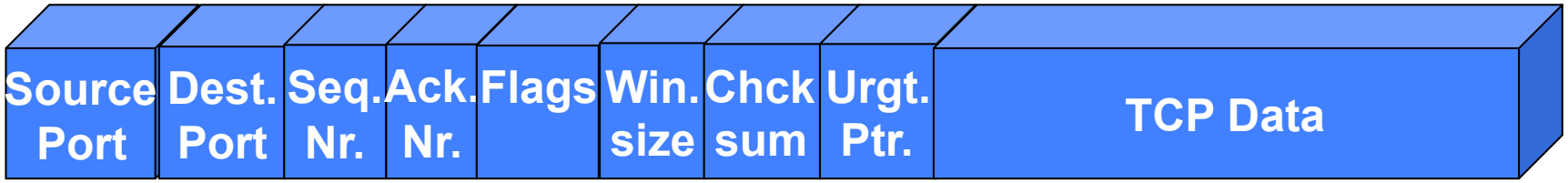
Simple IP network: e.g. from home by dial-in to office



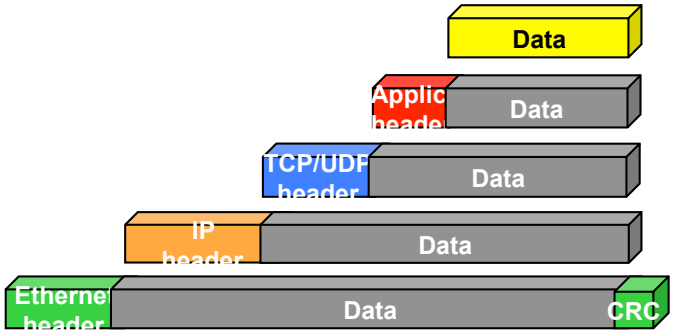
Routing



Transmission Control Protocol: TCP

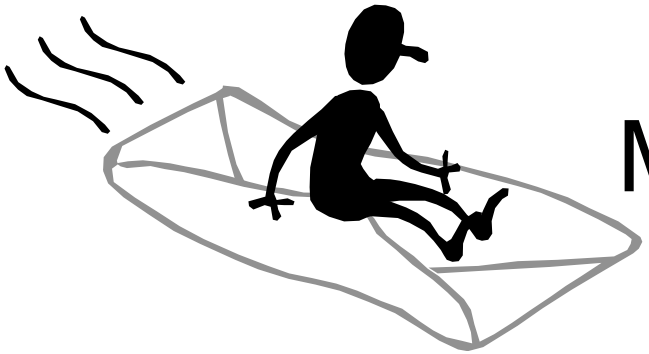


- TCP provides reliable logical circuit or connection service between pairs of processes
  - stream data transfer
  - reliability
  - flow control
  - multiplexing
  - logical connections
  - full duplex



Standard Ports

- 20/21 File Transfer Protocol (FTP)
- 23 Telnet
- 25 Simple Mail Transfer Protocol (SMTP)
- 79 Finger
- 80 HyperText Transfer Protocol (HTTP)
- 110 Post Office Protocol (POP3)
- 143 Internet Message Access Protocol (IMAP)



Mail Service

protocols

- Post Office Protocol (POP3)
  - Client uses POP3 to fetch email from server port 110
  - downloads all mail to client (can be prevented)
- Simple Mail Transfer Protocol (SMTP)
  - Client accesses port 25 to send email
  - no authentication !
- Internet Message Access Protocol (IMAP)
  - Client accesses server port 143
  - mail stays on server

Post Office Protocol

commands / responses

Commands		***Description***
• USER	<userid>	
• PASS	**********	
• STAT		status of mailbox
• LIST	[message-nr]	list info about message
• RETR	message-nr	retrieve message
• DELE	message-nr	delete message
• RSET		return all ‘delete marked’ to original
• QUIT		close connection
Responses		
• +OK	response	command accepted
• -ERR	reason	problem

HyperText Transfer Protocol (HTTP)

WWW

- WWW-server uses normally port 80

- Two versions exists:
  - HTTP 1.0
    separate connections are required to retrieve in-page info
  - HTTP 1.1
    - allows for persistent connections, same connection used for additional information fetching
    - provides virtual hosting

HTTP 1.1 structure

rfc 2068

- Request from server after connection is opened
  - requestline = Method SP Request-URI Version CRLF [message]
  - example: GET http://www.w3.org/index.html HTTP/1.1

- Response
  - responseline= Version SP Status-Code SP Phrase CRLF [message]
  - example :
    HTTP/1.1 200 OK
    <TITLE>Demo Page</TITLE>
    <BODY>
    …
    </BODY>

HTTP 1.1

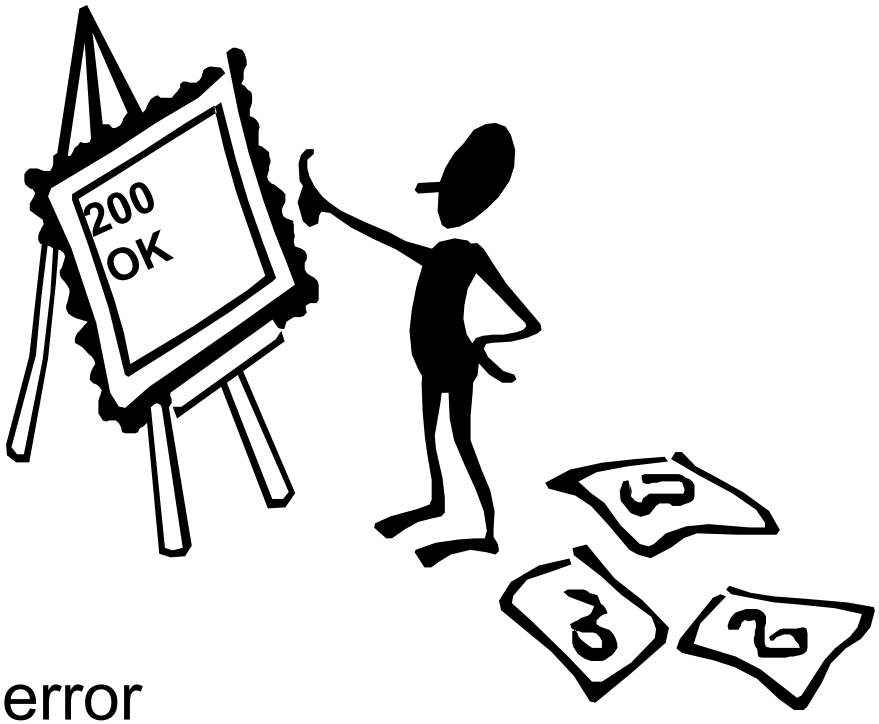
Command Methods

- GET Normal command to get pages/info
- HEAD Only gives page data (date-time,size and type)
- OPTIONS Provides communication options of the server
- POST The client sends information to the server
- PUT The client tries to store information in a server resource
- DELETE Removes the resource and its information
- TRACE Provides a loopback of the request message

HTTP 1.1

status codes

- 100 Continue
- 200 OK
- 400 Bad Request
- 401 Unauthorized
- 402 Payment Required
- 403 Forbidden
- 404 Not Found
- 500 Internal server error



Monitoring Ports

Netstat command

```
C:\WINDOWS>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:573            0.0.0.0:0              LISTENING
  TCP    192.168.0.140:6667     0.0.0.0:0              LISTENING
  TCP    192.168.0.140:6667     192.168.0.124:1027     ESTABLISHED
  TCP    192.168.0.140:6667     192.168.0.121:1623     ESTABLISHED
  TCP    192.168.0.140:6667     192.168.0.144:1834     ESTABLISHED
  TCP    192.168.0.140:137      0.0.0.0:0              LISTENING
  TCP    192.168.0.140:138      0.0.0.0:0              LISTENING
  TCP    192.168.0.140:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:573            *:*
  UDP    192.168.0.140:137      *:*
  UDP    192.168.0.140:138      *:*
```

IP Addresses

```
00000000 00000000 00000000 00000000     0.0.0.0
00000000 00000000 00000000 00000001     0.0.0.1
00000000 00000000 00000000 00000002     0.0.0.2
00000000 00000000 00000000 00000003     0.0.0.3
    :        :        :        :
11000010 10100001 01001110 00100001     194.161.78.33
11000010 10100001 01001110 00100010     194.161.78.34
11000010 10100001 01001110 00100011     194.161.78.35
    :        :        :        :
11111111 11111111 11111111 11111100     255.255.255.252
11111111 11111111 11111111 11111101     255.255.255.253
11111111 11111111 11111111 11111110     255.255.255.254
11111111 11111111 11111111 11111111     255.255.255.255
```

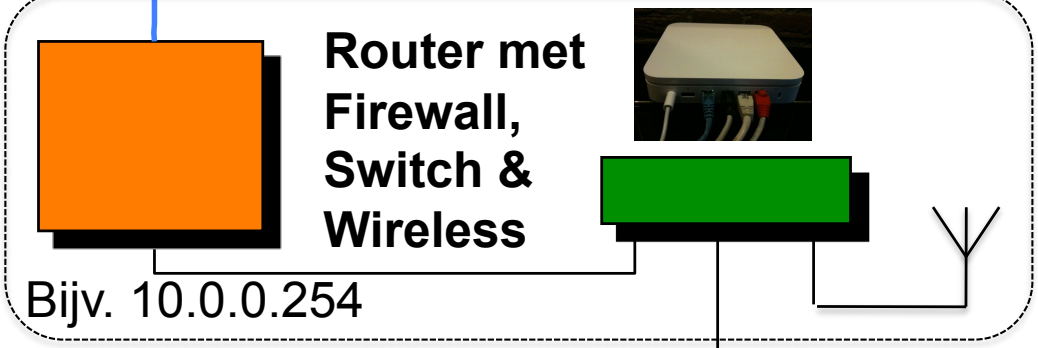
Internet Security
firewall

- Based on an ‘intelligent router’
- All packets are parsed and subjected to ‘rules’
- Different rule-sets are applied to externally vs. internally originated packets
- Possible checks:
  - destination and source IP-addresses
  - format (and size) also for application protocols
  - accessed ports
  - corrupt packets

(Kabel, Glasvezel)
Modem

Bijv. IP van provider
195.83.72.145

Home Network:



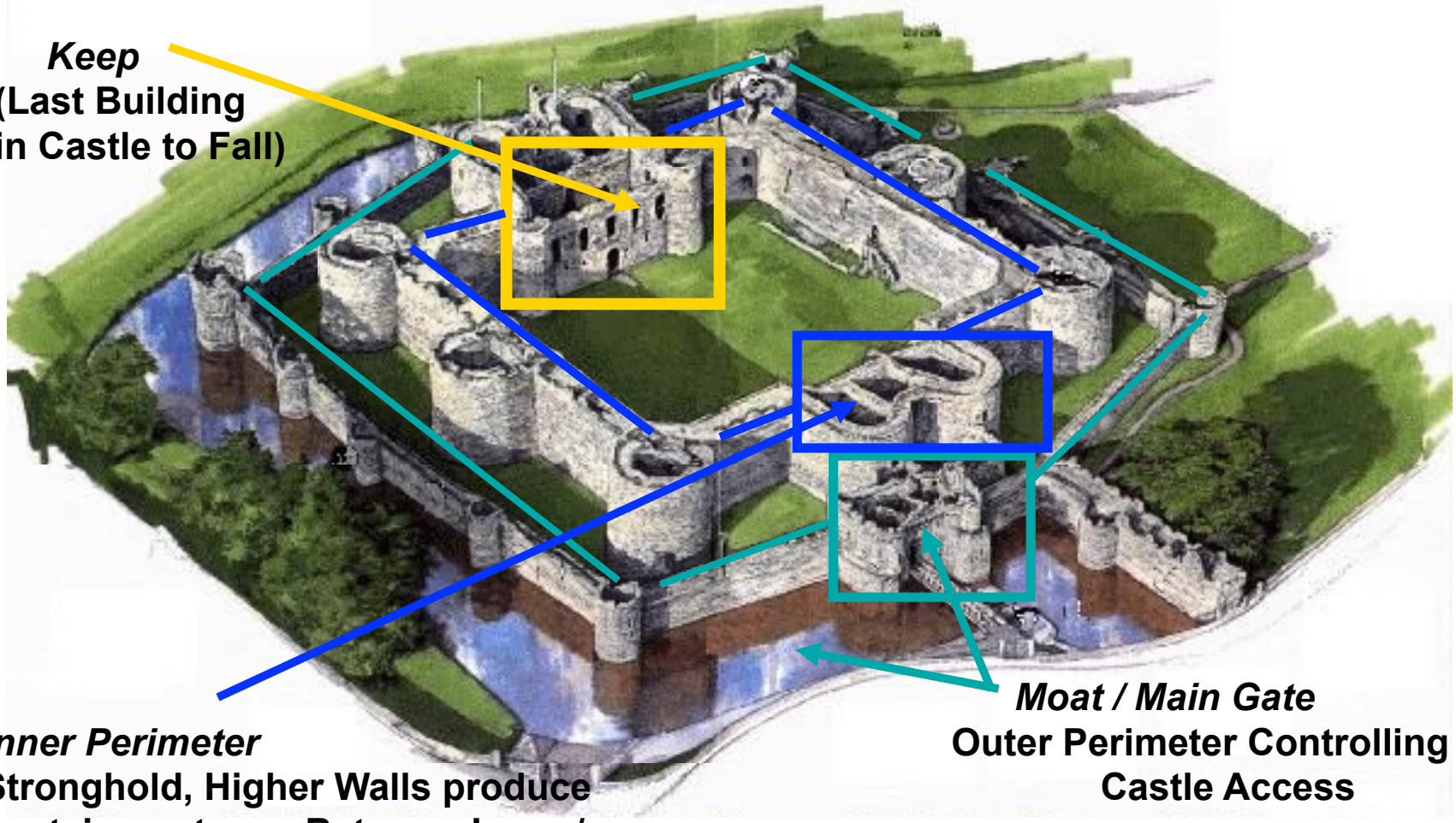
Bijv. 10.0.0.x (met 1<x<254)

Bijv. 10.0.0.1

PC/MAC

Draadloos Netwerk (WiFi)
(Wireless LAN, max 54 Mbps)
Notebooks (802.11a/b/e/n)
Tables (iPad, Android) &
Smart Phones (iPhone, etc)

Internet Security Analogy

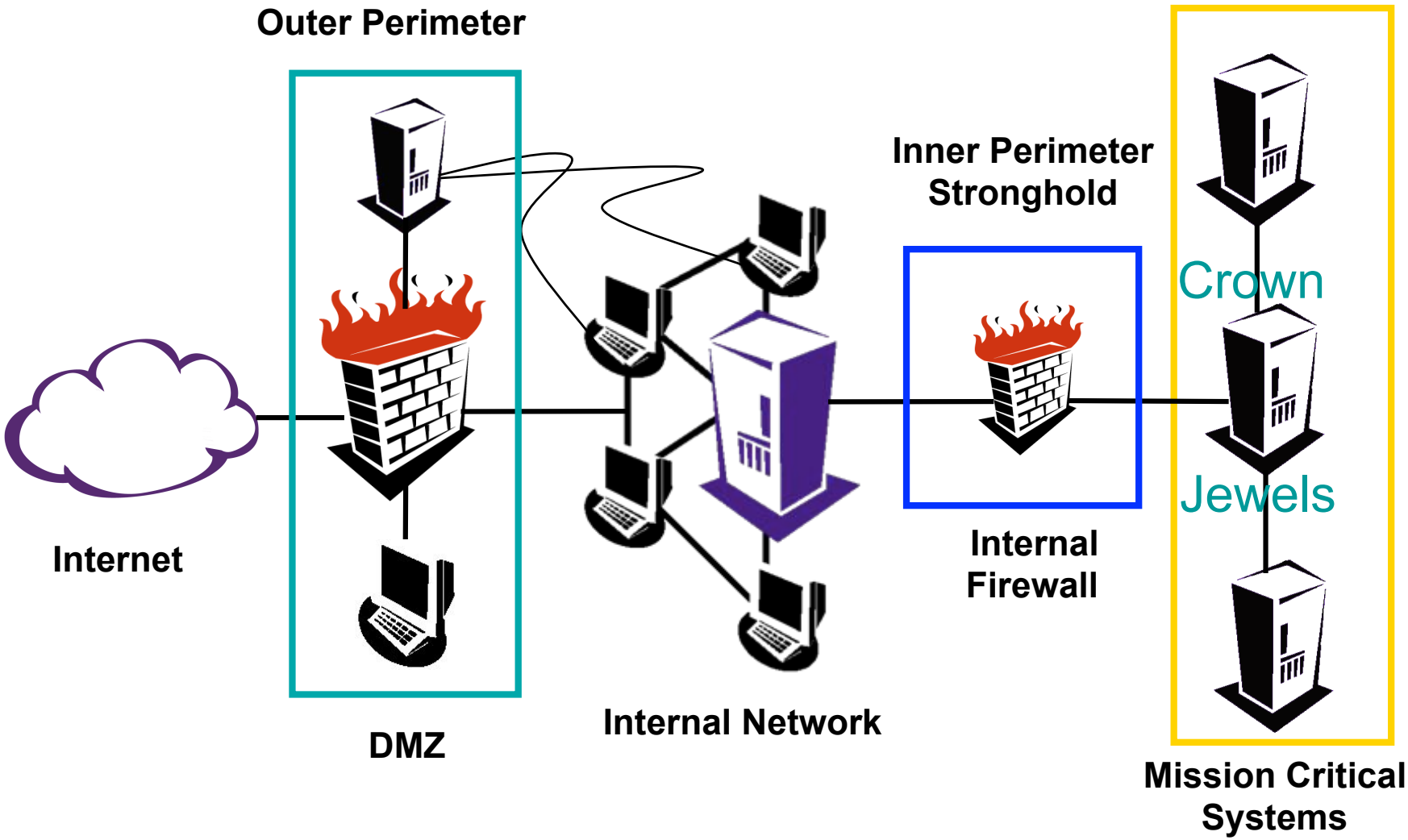


Keep
(Last Building in Castle to Fall)

Inner Perimeter
Stronghold, Higher Walls produce containment area Between Inner / Outer Perimeters

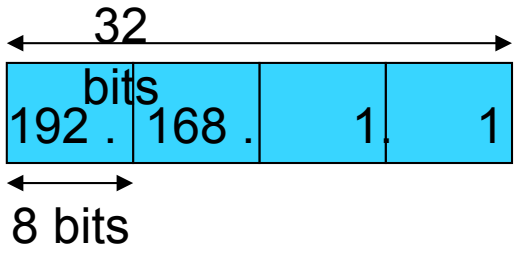
Moat / Main Gate
Outer Perimeter Controlling Castle Access

Internet Security Analogy

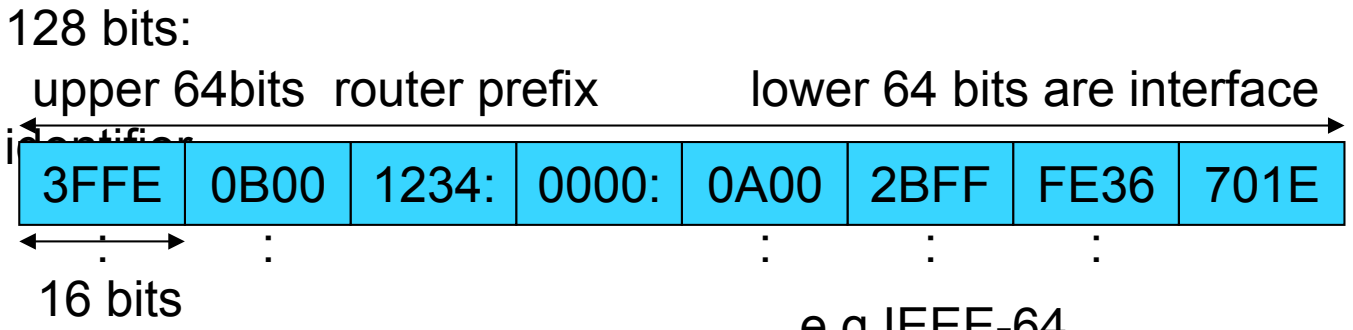


Why care about addressing schemes

- IPv4, 32 bit address (4 Bytes, written decimal 192.168.1.1 (0-255))



- IPv6, 128 bit address (16 Bytes, written hexadecimal)

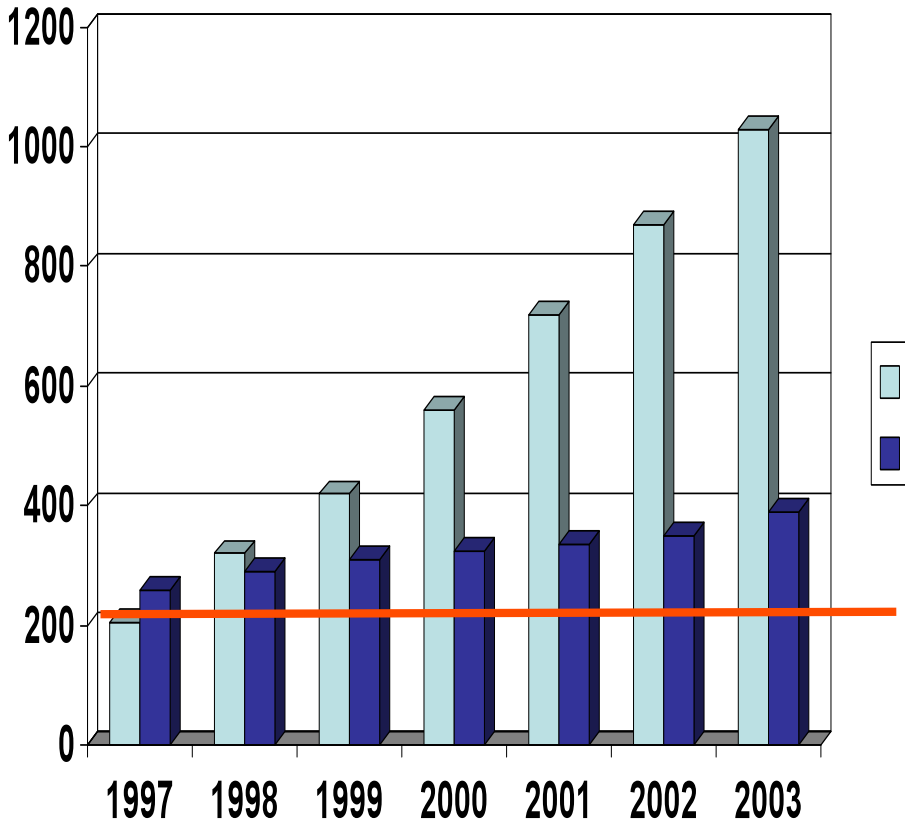


IPv6 Addresses can be abbreviated

3FFE:0B00::0001 or even 3FFE:B00::1

The Huitema formula (RFC 1715)

Hierarchical address scheme efficiency $H = \dfrac{\log(\text{nr object})}{\text{nr address bits}}$



Installed PC and mobile subscribers (1999)

In real life H_{min}=0.14 to H_{max}=0.26 (DECnet, SITA, US Telephone)

IPv4 32 bits max 4B numbers

Huitema factor implies at 0.26

200 M always-on, active hierarchical numbered IPv4

Today we have 300 Million PCs in LAN's behinds NAT's (firewalls) and dial-in ISP with DHCP

Veilig op Internet - 3

Firewalls, Man-in-middle, D-DoS,
IPSec, keys

Datum ??

Bij belangstelling & goede spreker

Veilig op Internet

essentiële basiskennis

DSE, 12 juni 2010

Eric Ideler

Aktie lijstje

1. Gebruik je gezonde verstand
2. Een sterk wachtwoord
3. Anti-virus/spam software
4. Update je programma's
5. Voorzichtig met (onbekende) software (en kids met games)
6. Surf verstandig
7. Bewaak je privacy
8. Maak back-up's
9. Geloof niet alles
10. SPAM – nooit op reageren en nooit doorzenden

Veilig op Internet - 2

Toen werd het lastiger
hardware, protocollen & port basics

DSE, 12 jan 2010
Egbert-Jan Sol

Aktie lijstje

1. Modem, Router, Switch installeren en kabels klaar zetten
2. Router aan Modem en dan PC met fix adres (afh. Router bijv. 10….)
   router configureren (soms via web http://10.0.0.254 of Airport Utility config.)

3. (PC van vast weer naar dynamisch IP en uitzetten)
4. Router en PC's, etc aanzetten en controleren.

5. (PC, tablets, notebooks, etc) zend hun MAC met een ARP uit en krijgen IP)

6. In Router worden subnet IP (10.0.0.x) omgezet in een IP zoals 125.45.3.80
   en met port mapping vindt NAT (network address translation) plaats

Wat moet je weten (en wat niet): Alleen IP nummers
(Ethernet MAC naar IP en IP-TCP-portnummers naar NAT niet),

Alleen de eerste keer is DHCP en bij firewall soms port nummers van belang
EN BIJ WIRELESS LAN security instellingen (WPA/WPA2)