








Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

Wireless LAN C072047

Unit 7: Filtering

Prof. Bill Buchanan

-  **Contact:** w.buchanan@napier.ac.uk
-  **Room:** C.63
-  **Telephone:** X2759
-  **MSN Messenger:** [w_j_buchanan@hotmail.com](msn://w_j_buchanan@hotmail.com)
-  **WWW:** <http://www.dcs.napier.ac.uk/~bill>
<http://buchananweb.co.uk>



INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

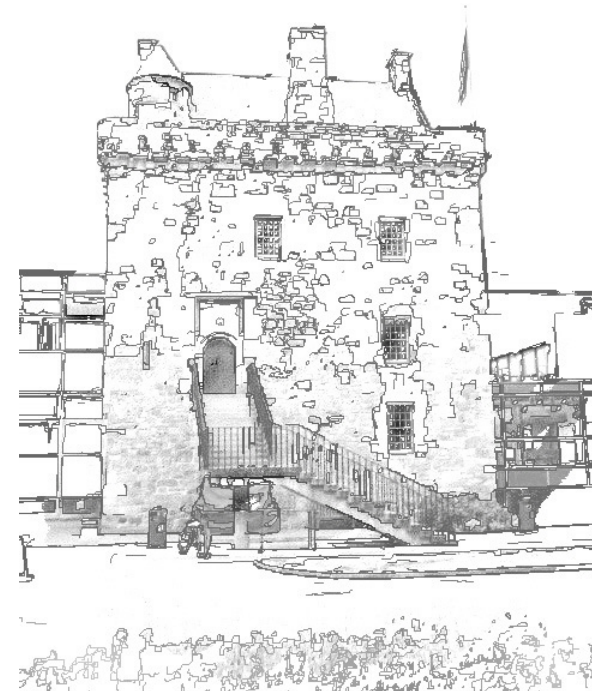
Author: Bill Buchanan



Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

Module Descriptor



INVESTOR IN PEOPLE

NAPIER UNIVERSITY
EDINBURGH

Author: Bill Buchanan

Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

Week	Date	Academic	Cisco	Lab/Tutorial
1	1 Oct	1: Radio Wave Fundamentals		
2	8 Oct	2: Wireless Fundamentals	Intro to Wireless LANs	Lab 1/2: Access Point Tutorial 1 (T)
3	15 Oct	3: Ad-hoc and Infrastructure Networks	IEEE 802.11 and NICs	Lab 3: Ad-hoc Networks
4	22 Oct	4: Encryption	Wireless Radio Technology	Lab 4: Infrastructure Networks
5	29 Oct	5: Authentication	Wireless Topologies	Lab 5: Remote Connections
6	5 Nov	6: Antennas	Access Points	Lab 6: Encryption/Authen
7	12 Nov	7: Filtering/8. VLANs	Bridges	Lab 7: Filter
8	19 Nov	Napier Test (40%)	Antennas	Lab 8: VLAN
9	26 Nov		Security	Lab 9: VLAN/802.1Q
10	3 Dec	Cisco Academy/Additional Material	Applications	Lab 10: IP Routing
11	10 Dec	Cisco Academy /Additional Material	Site Survey	Lab 11: RADIUS
12	17 Dec	Cisco Academy /Additional Material	Troubleshooting	Lab 12: SNMP
Holidays				
13	7 Jan	Revision/Cram (Cisco Exam)	Emerging Technologies	Coursework/Practical (50%)
14	14 Jan	Revision/Cram (Cisco Exam)	Cisco Exam (10%)	
15	21 Jan			

SWSCUST Module Individual - Windows Internet Explorer

http://timetableing.napier.ac.uk/reporting/individual;module;id;co72047%0D%0A?days=1-7&weeks=1-13;16-18&peric

File Edit View Favorites Tools Help

SWSCUST Module Individual

Module: co72047 - Wireless LANs Weeks: 0-12, 13-15 (24 Sep 2007-27 Jan 2008)

	9:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00
Mon												
Tue												
Wed	Prof William Buchanan Merch.F27 co72047.L01 1-12, 13		Prof William Buchanan, Mr Jamie Graves, Mr Lionel Saliou Merch.co.C6 co72047.P03 1-12, 13-15		Prof William Buchanan, Mr Jamie Graves, Mr Lionel Saliou Merch.co.C6 co72047.P01 1-12, 13-15		Prof William Buchanan, Mr Jamie Graves, Mr Lionel Saliou Merch.co.C6 co72047.P02 1-12, 13-15		Prof William Buchanan, Mr Jamie Graves, Mr Lionel Saliou Merch.co.C6 co72047.P04 1-12, 13-15			
Thu	Merch.co.C6 co72047.U01 1-12, 13-15											
Fri												
Sat												
Sun												

[<< Back](#)
[Print Timetable](#)
Date/Time: 1 Oct 2007 21:49

Template: SWSCUST Module Individual

Done Internet 100%



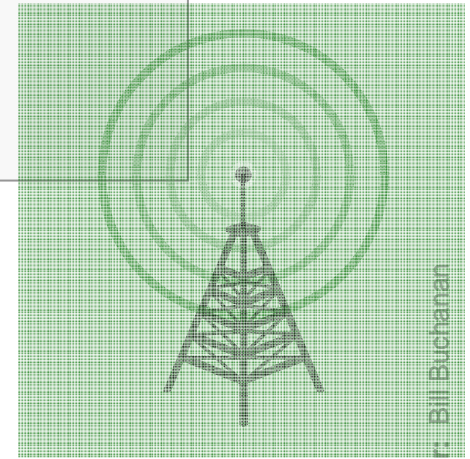
Wireless connections ... which technology?

Areas covered:

Filtering.

ACLs.

MAC address filtering.



Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

Site Survey - 350 Series - Passive Mode - [Enterprise]

Signal Strength 72%

Signal Quality 100%

Link Speed 11 Mbps

Overall Link Quality Good

Associated Access Point ap

Access Point IP Address 192.168.0.110

Channel (Frequency) 11 (2462 MHz)

Restart Card

350 Series Statistics - [Enterprise]

Receive Statistics		Transmit Statistics	
Multicast Packets Received	= 45	Multicast Packets Transmitted	= 27
Broadcast Packets Received	= 67	Broadcast Packets Transmitted	= 172
Unicast Packets Received	= 19	Unicast Packets Transmitted	= 19
Bytes Received	= 25,291	Bytes Transmitted	= 27,120
Beacons Received	= 11,901	Beacons Transmitted	= 0
Total Packets Received OK	= 32,076	Ack Packets Transmitted	= 672
Duplicate Packets Received	= 8	RTS Packets Transmitted	= 25
Overrun Errors	= 0	CTS Packets Transmitted	= 0
PLCP CRC Errors	= 48,793	Single Collisions	= 0
PLCP Format Errors	= 824	Multiple Collisions	= 0
PLCP Length Errors	= 0	Packets No Deferral	= 0
MAC CRC Errors	= 4,225	Packets Deferred Protocol	= 0
Partial Packets Received	= 0	Packets Deferred Energy Detect	= 483
SSID Mismatches	= 3,776	Packets Retry Long	= 11
AP Mismatches	= 0	Packets Retry Short	= 22
Data Rate Mismatches	= 0	Packets Max Retries	= 1
Authentication Rejects	= 0	Packets Ack Received	= 372
Authentication T/O	= 2	Packets No Ack Received	= 11
Association Rejects	= 9	Packets CTS Received	= 3
Association T/O	= 0	Packets No CTS Received	= 22
Packets Aged	= 0	Packets Aged	= 1
Up Time (hh:mm:ss)	= 00:33:57		
Total Up Time (hh:mm:ss)	= 00:37:17		

Reset Pause OK Help

350 Series Linktest - [Enterprise]

IP Address of Access Point: 192.168.0.110

Number of Packets: 100 Packet Size: 64

Continuous Linktest (Ignore Number of Packets)

Receive Statistics	Current	Cumulative Total
Packets Received OK	= 0	= 0

Transmit Statistics	Current	Cumulative Total
Packets Transmitted OK	= 0	= 0

Status = Associated
 Current Link Speed = 11 Mbps
 Associated Access Point Name = ap
 Associated Access Point MAC = 00:07:50:D5:BF:4C

Current Signal Strength

Current Signal Quality

Overall Link Quality

Defaults Stop OK

Link Status Meter - [Enterprise]

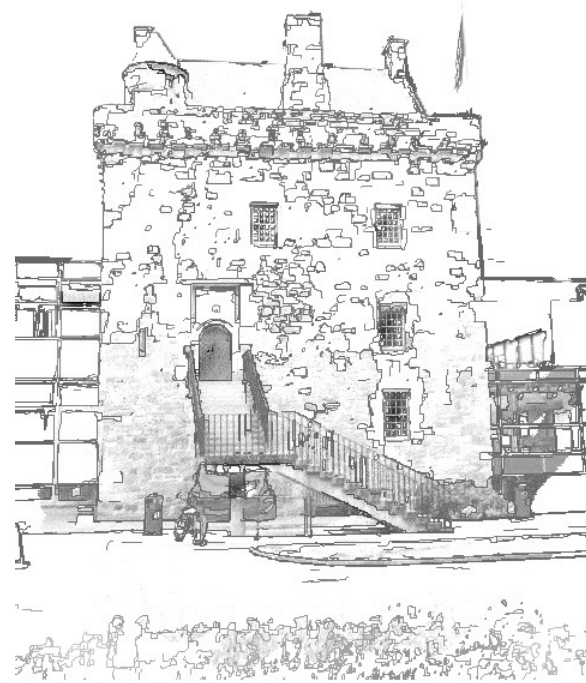
Signal Strength - 33%

Signal Quality - 93%

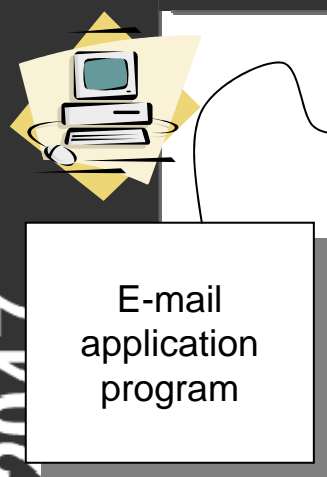
Link Quality to Access Point ap
 IP Address 192.168.0.110 MAC Address 00:07:50:D5:BF:4C is
FAIR

OK Help

Background



Data encapsulation



Application
 Application program makes contact with network application for e-mail

Hello.
 Fred.

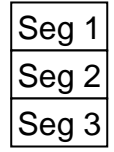
Presentation
 Convert data into a form which can be transmitted

To: Fred
 From: Bert
 Hello.
 Fred.

Session
 Contact remote system and request a transmission

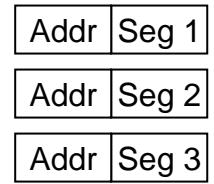
HELO sys.com
 FOR Fred
 To: Fred
 From: Bert
 Hello.
 Fred.

Transport
 Negotiate data transfer and split data into segments



Start	Addr	Seg 1	End
Start	Addr	Seg 2	End
Start	Addr	Seg 3	End

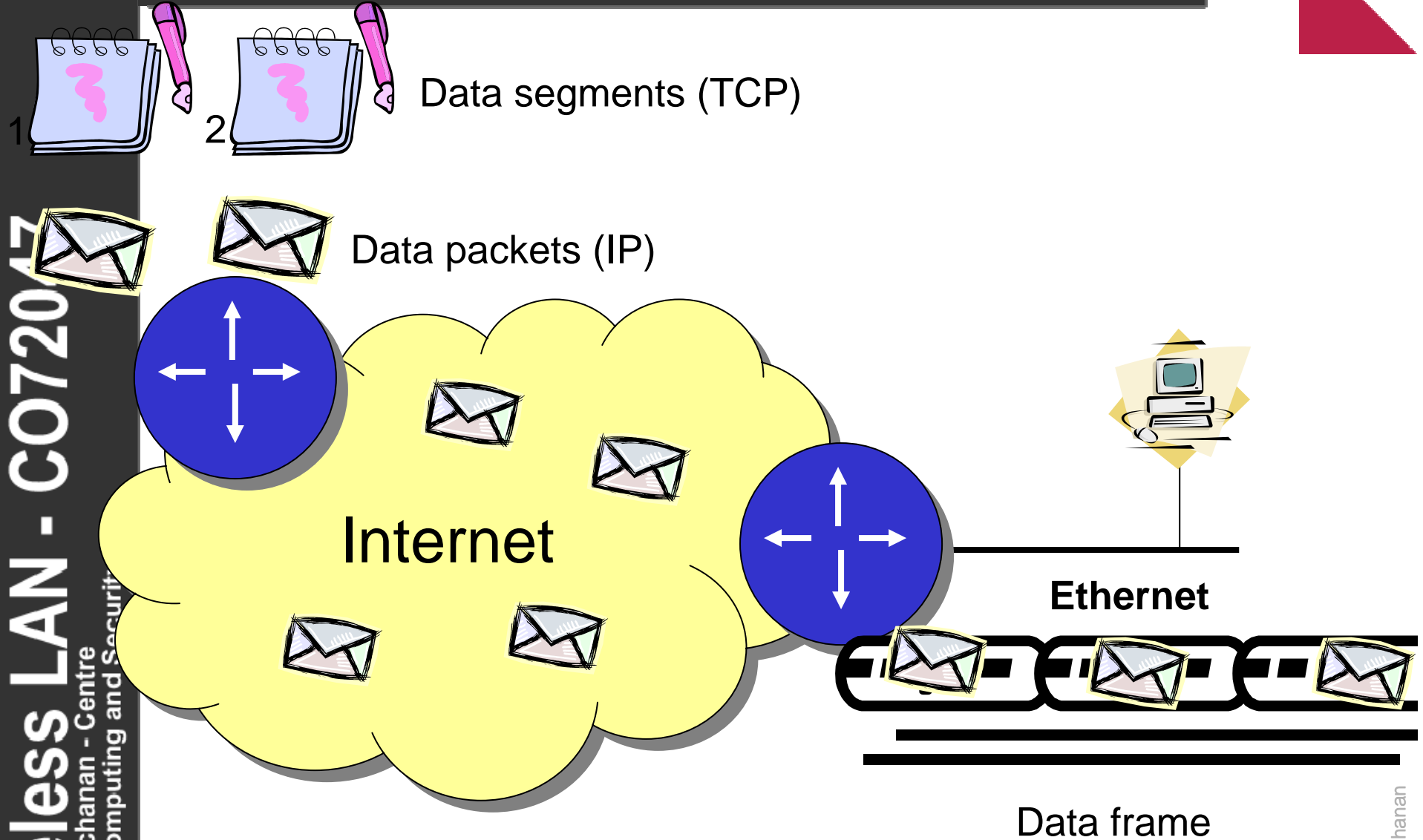
Network
 Add source and destination addresses



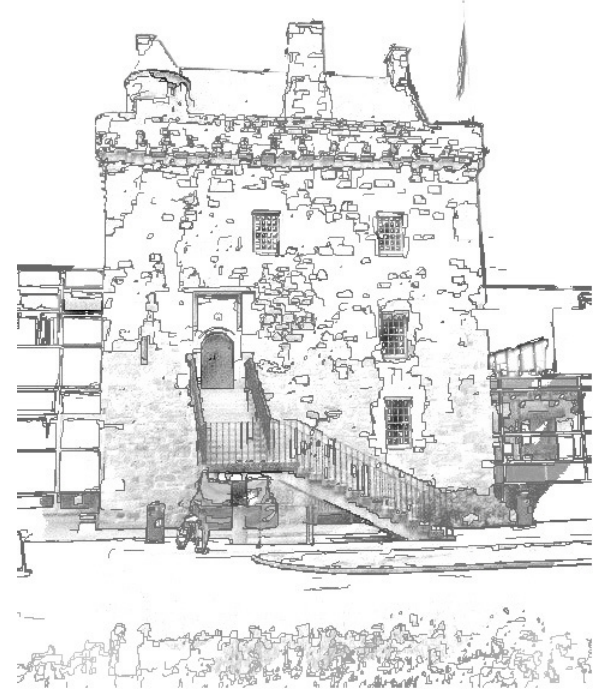
Data link
 Data packet converting into a form which can be transmitted over the network

Physical
 The data frame is converted into binary form and transmitted over a physical connection

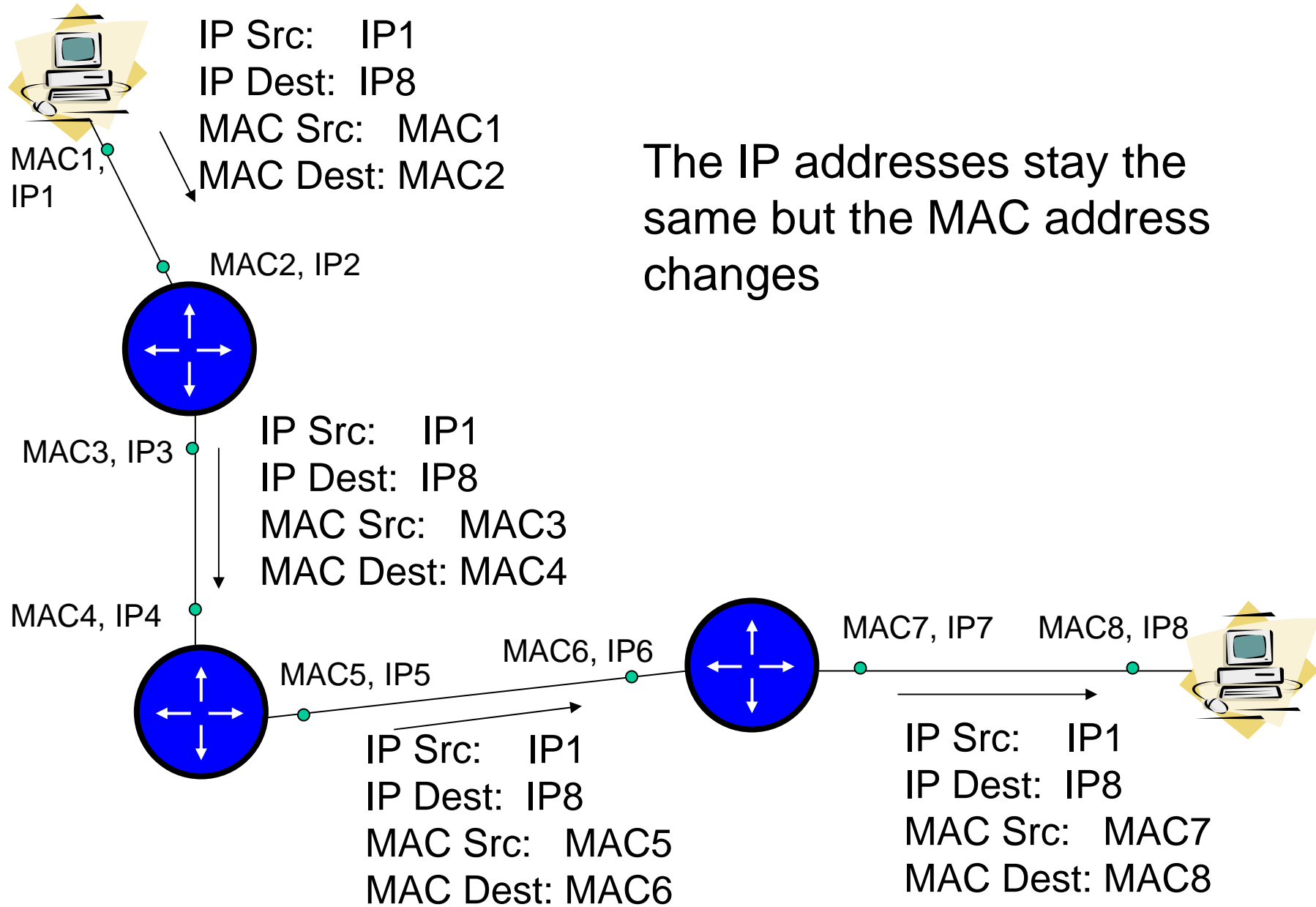
Terms for each layer



IP and TCP ... The Greatest of the Protocols!



IP and MAC Addresses

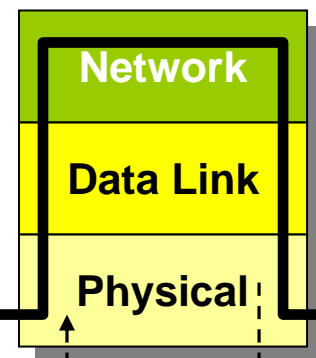
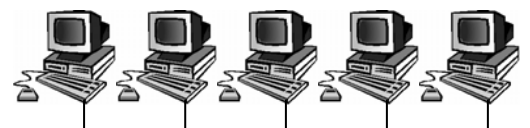
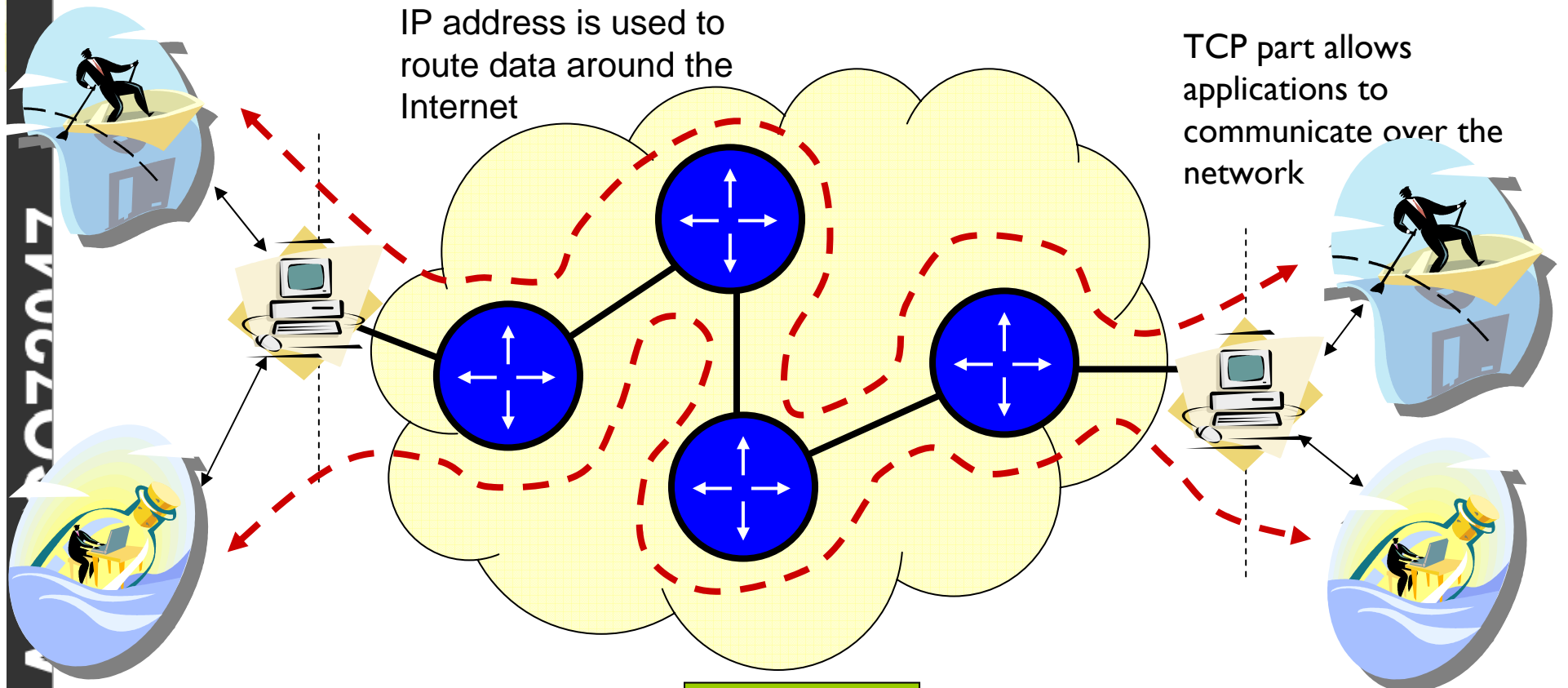


The IP addresses stay the same but the MAC address changes

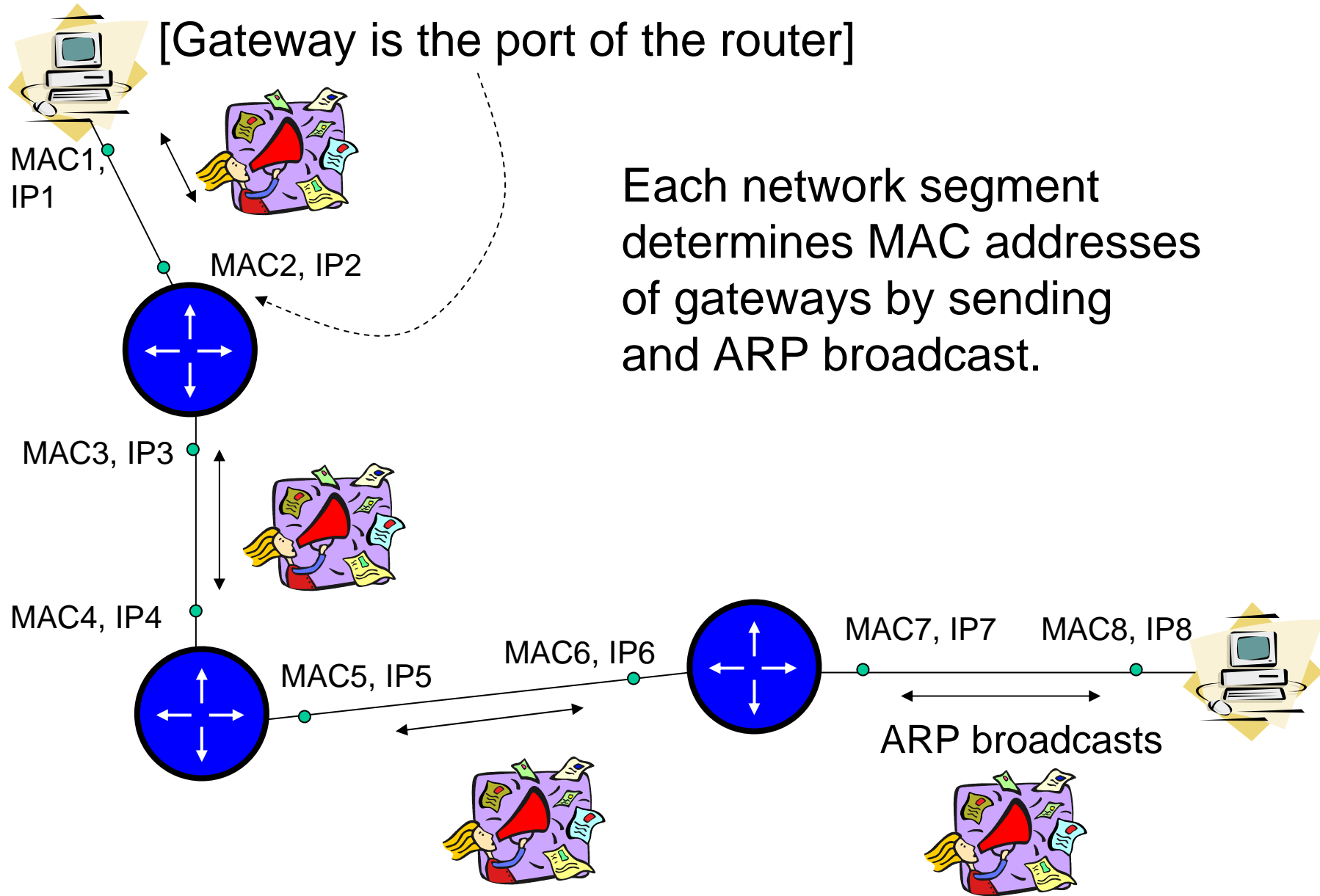
IP and TCP

IP address is used to route data around the Internet

TCP part allows applications to communicate over the network



IP and MAC Addresses



IP header



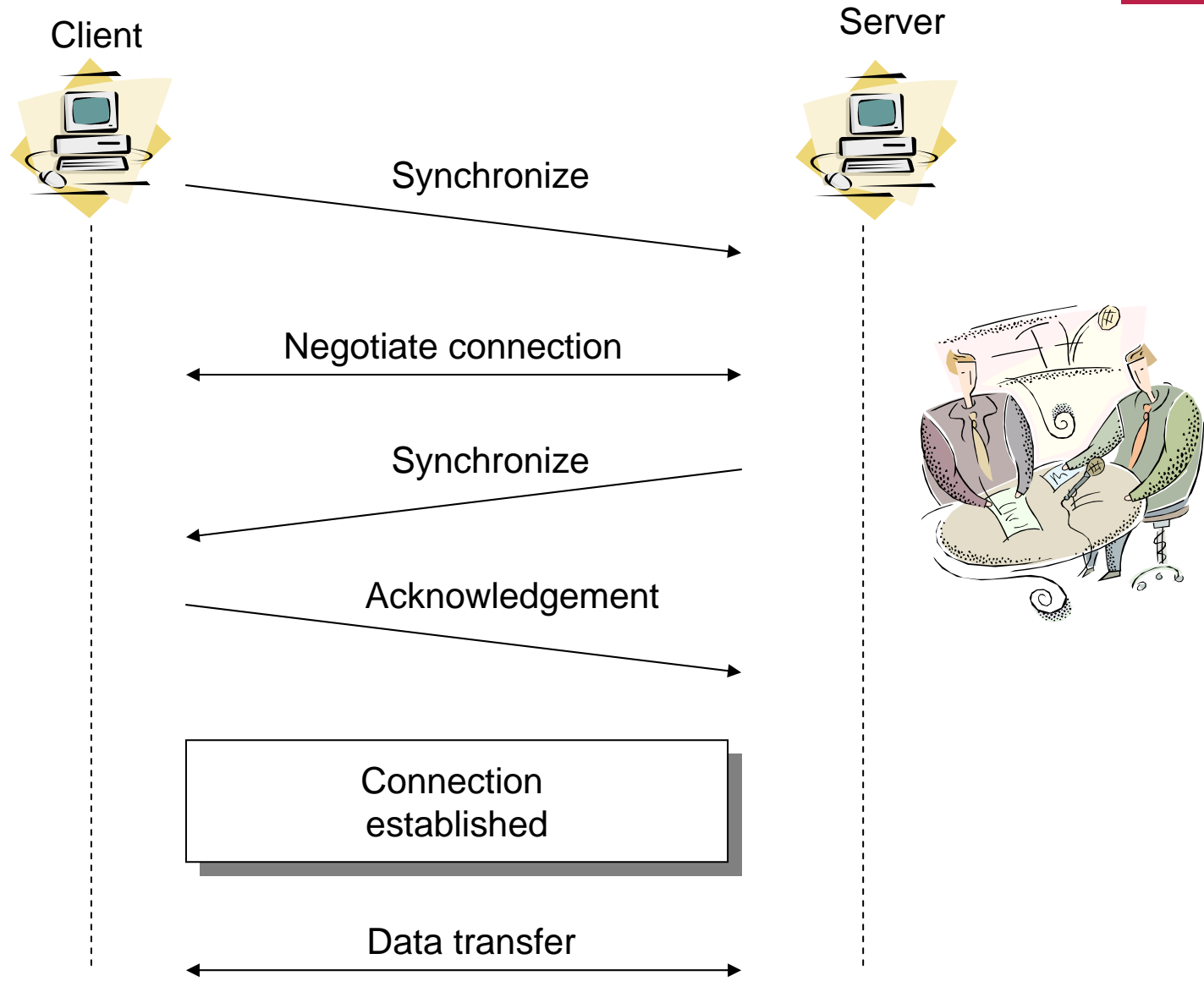
Data Packet

Version		Header length			Type of service										
Total length															
Identification															
0	D	M	Fragment Offset												
Time-to-Live								Protocol							
Header Checksum															
Source IP Address															
Destination IP Address															

Protocol (8 bits). Different transport protocols can be used on the datagram. The 8-bit protocol field defines the type to be used. E.g. 1 – ICMP and 6 – TCP.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----

Synchronization and acknowledgement



Windowing



Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

Transmitter

Window defined as three

Receiver



Data [S=1]

Data [S=2]

Data [S=3]

Ack [R=4]

Data [S=4]

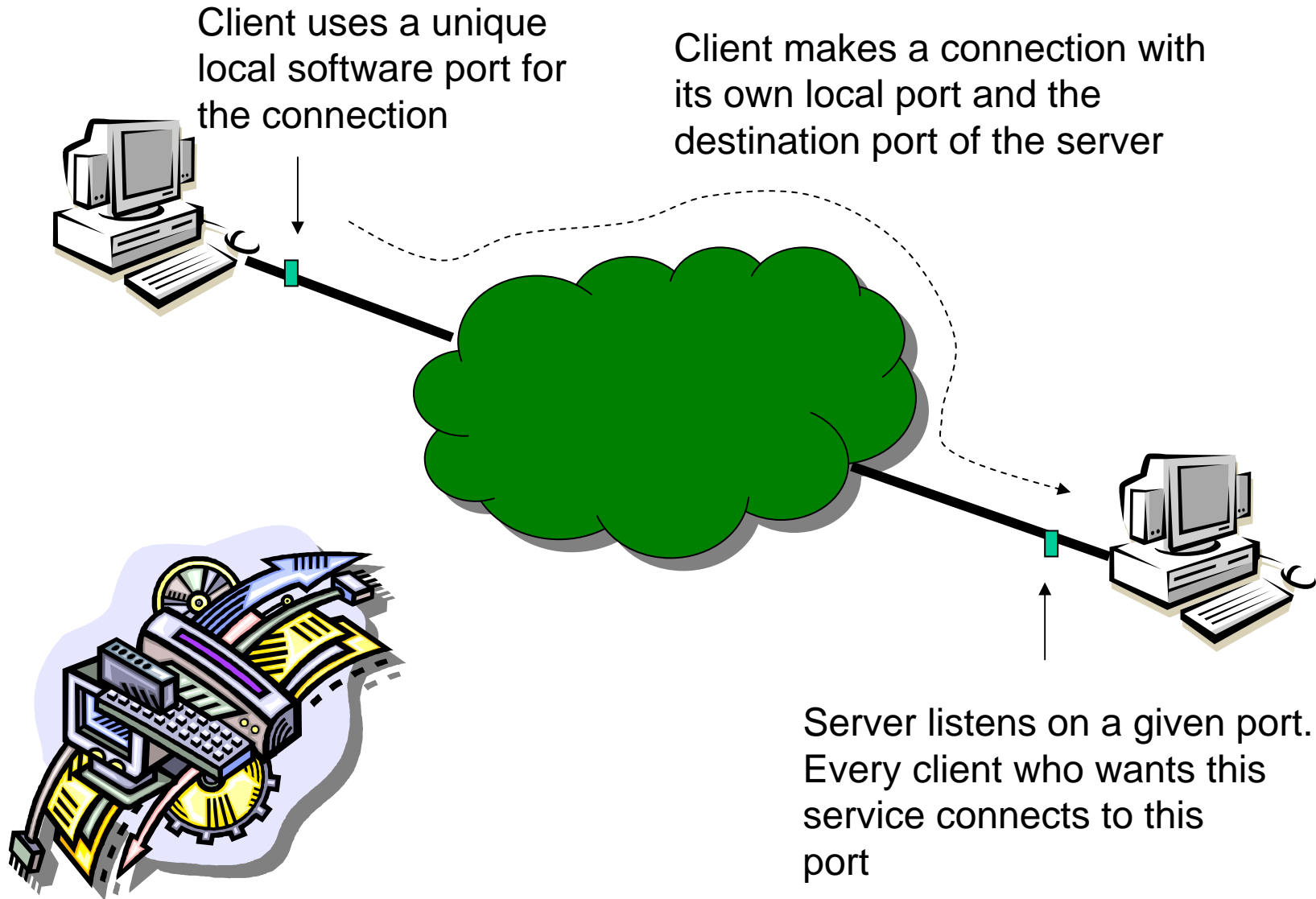
Data [S=5]

Data [S=6]

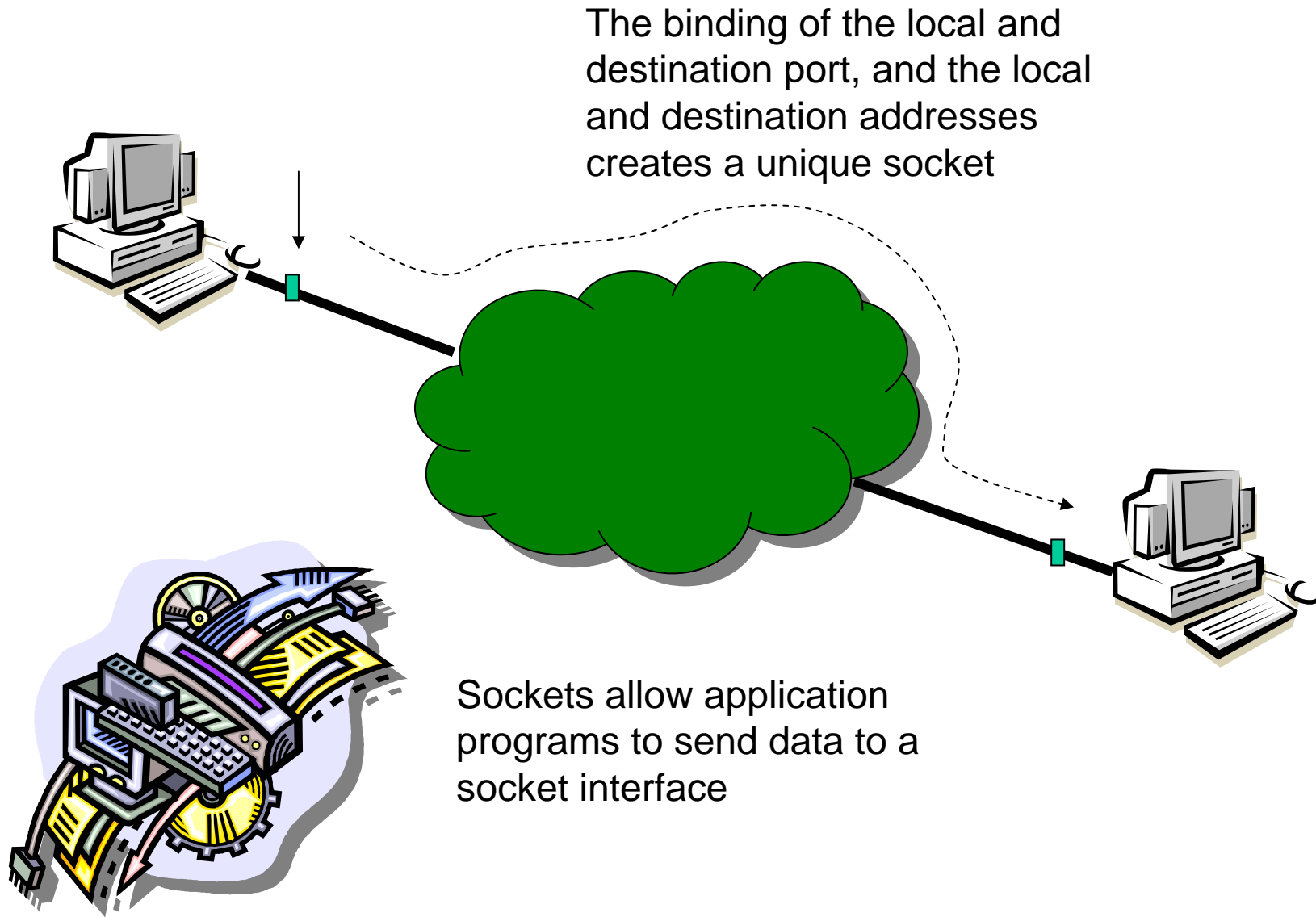
Ack [R=7]



TCP operation



TCP operation

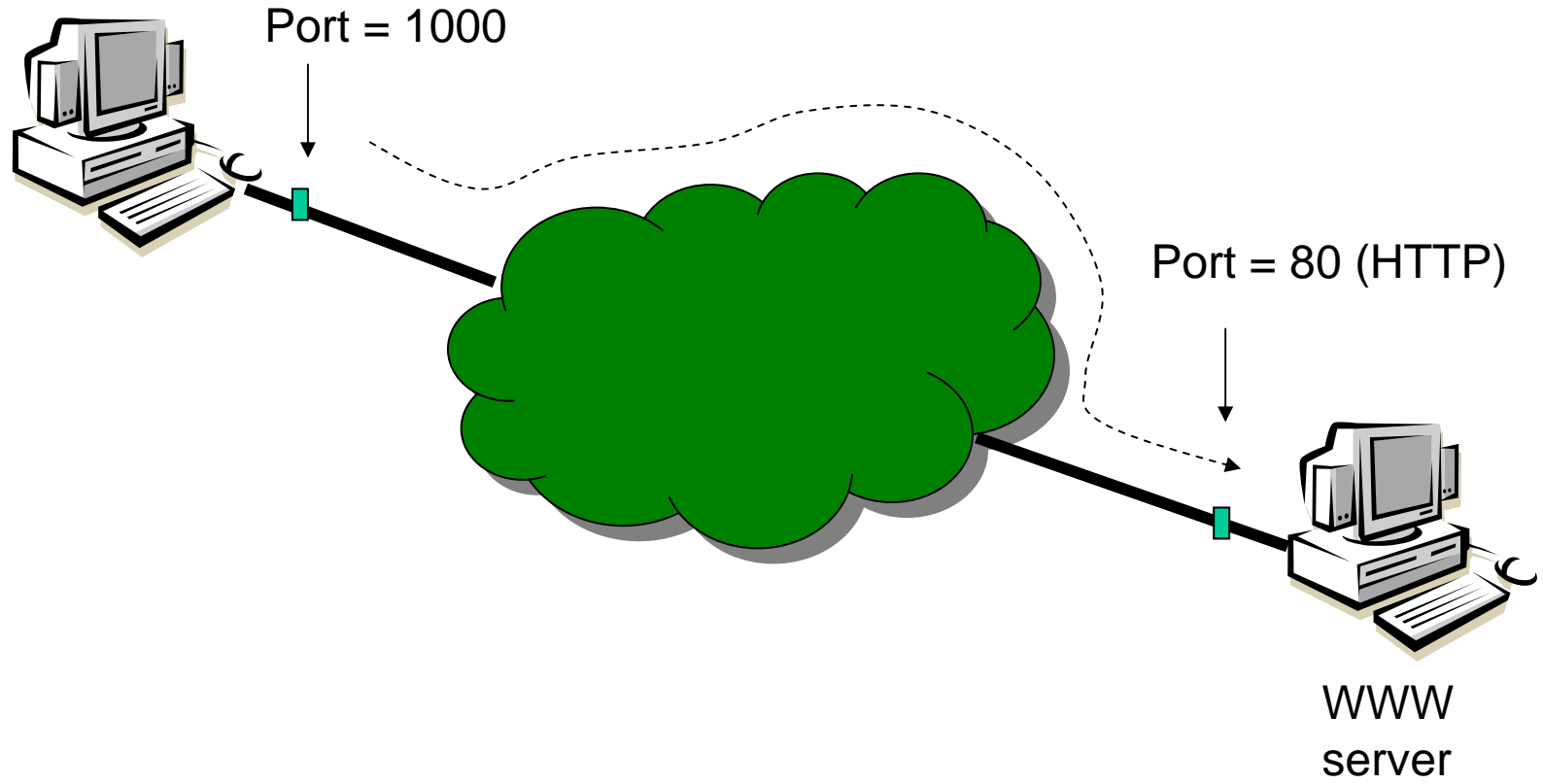


Example



Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

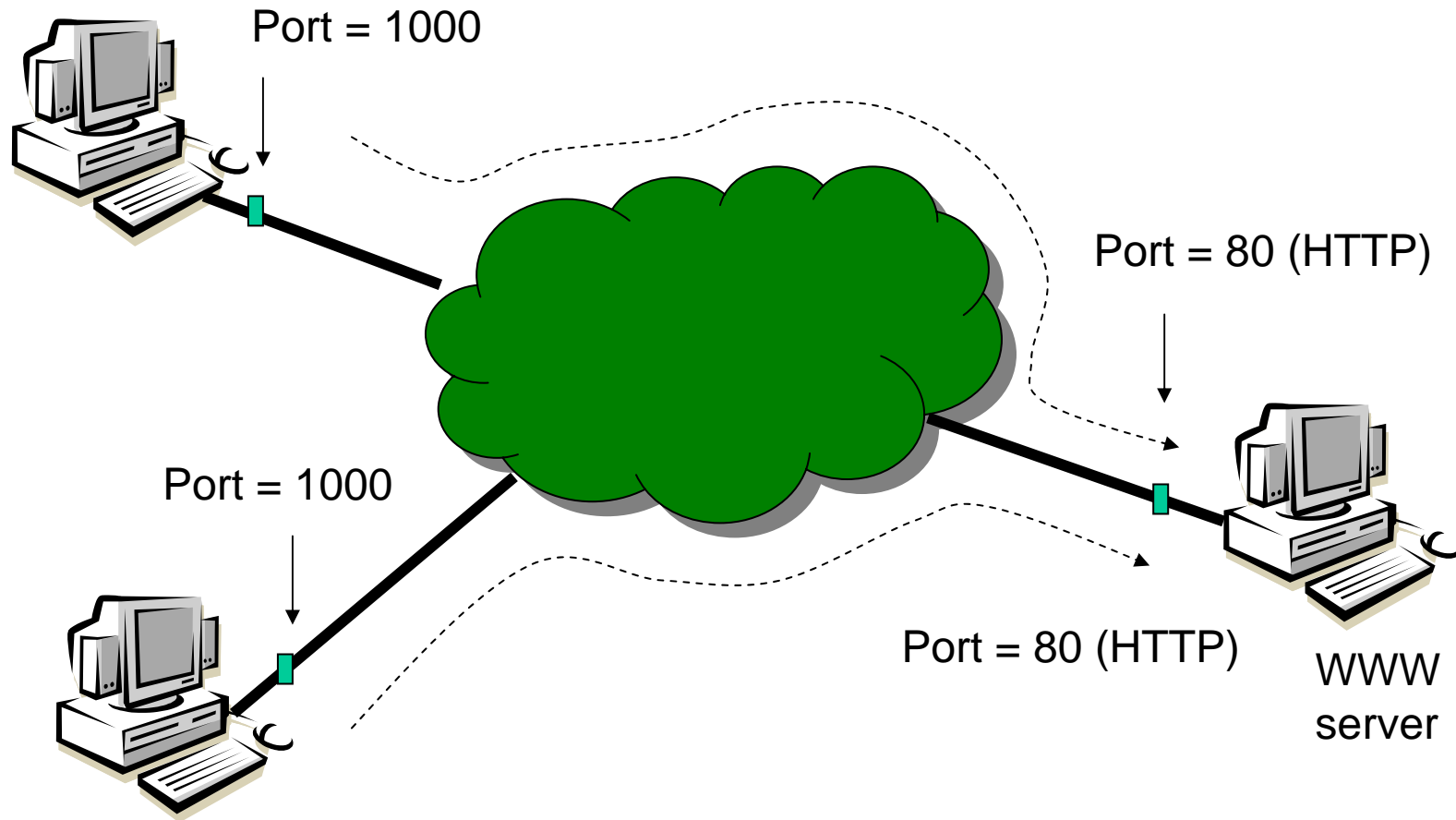


Example

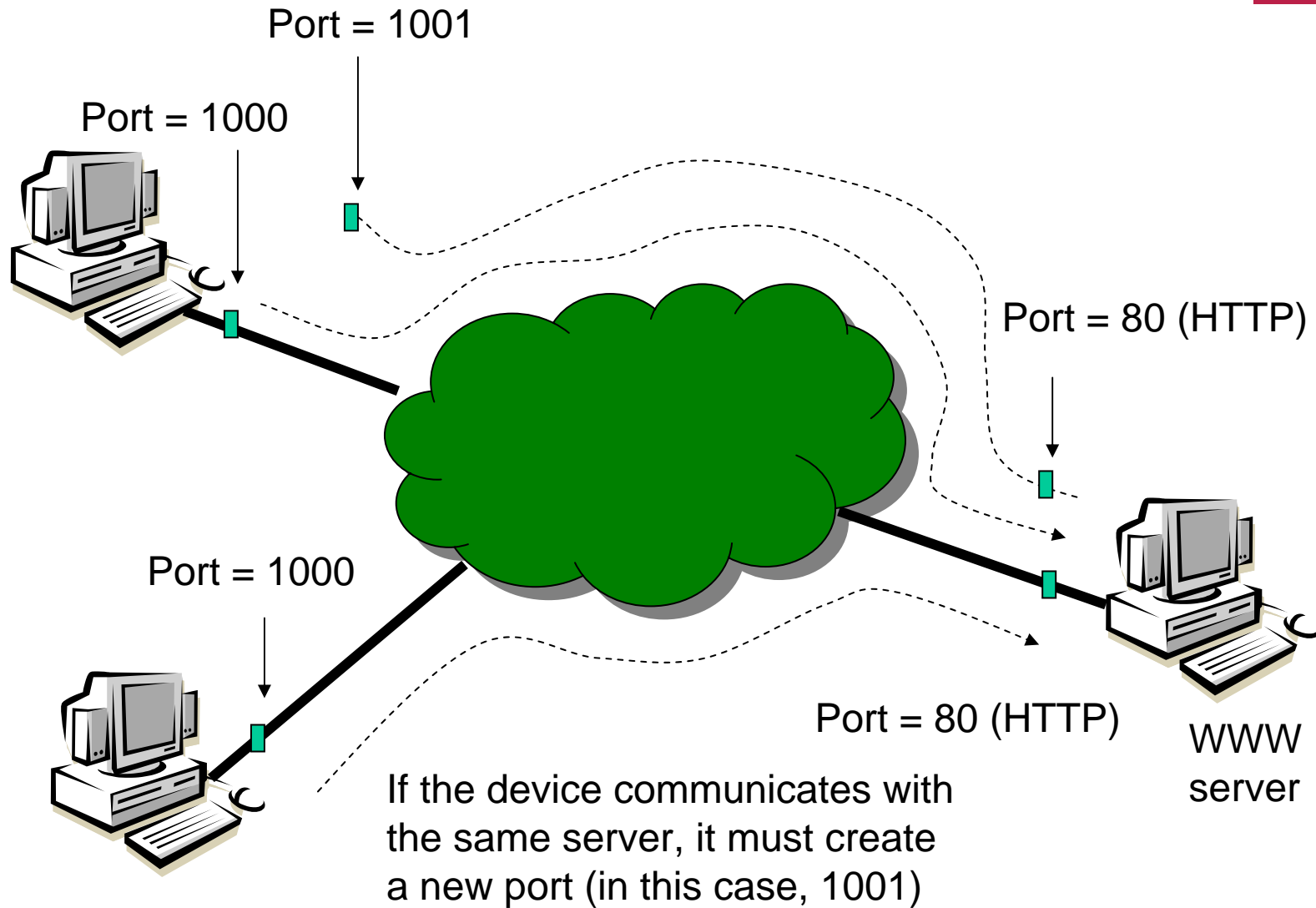


Wireless LAN - C072047

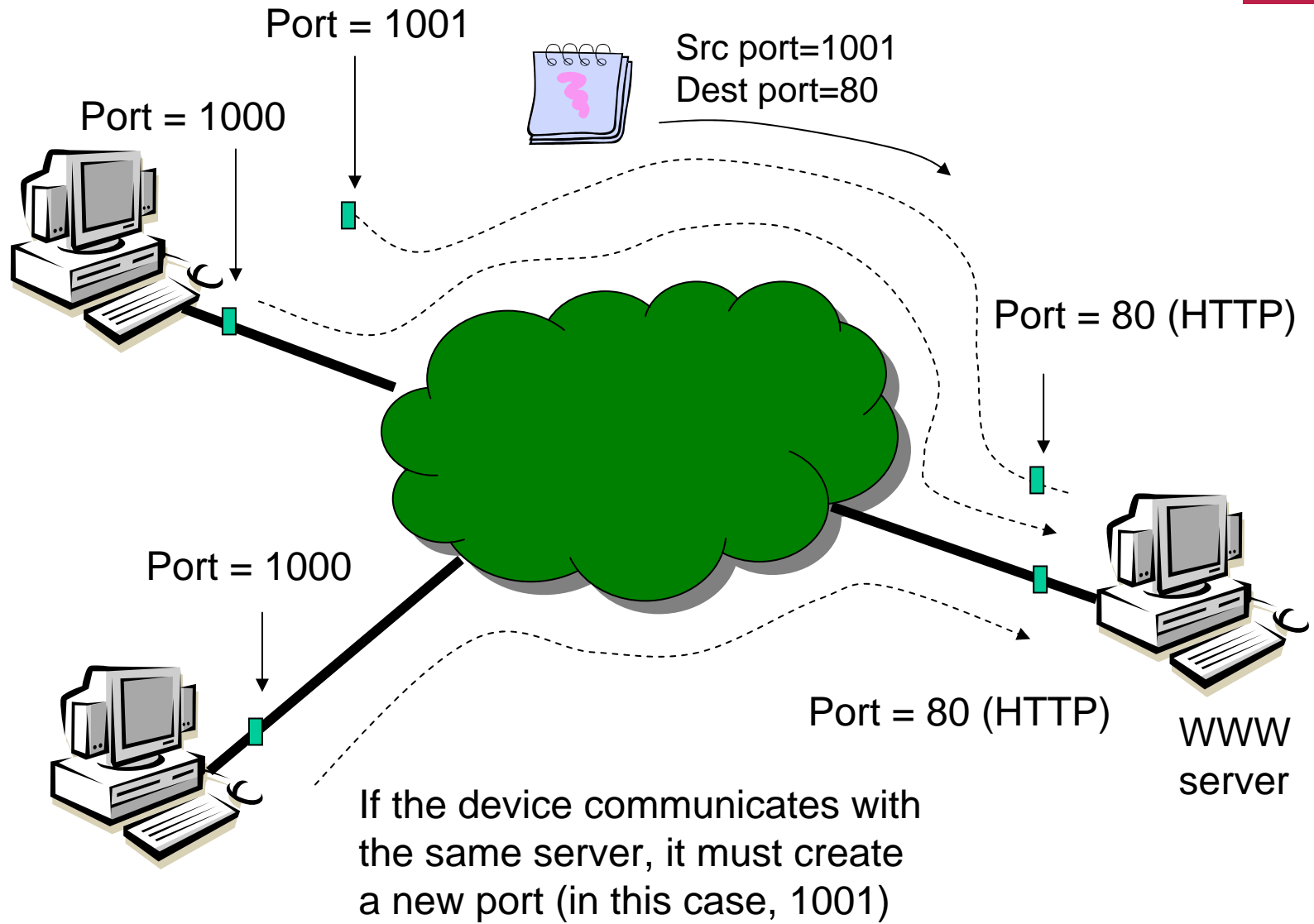
Prof W Buchanan - Centre
for Dist. Computing and Security



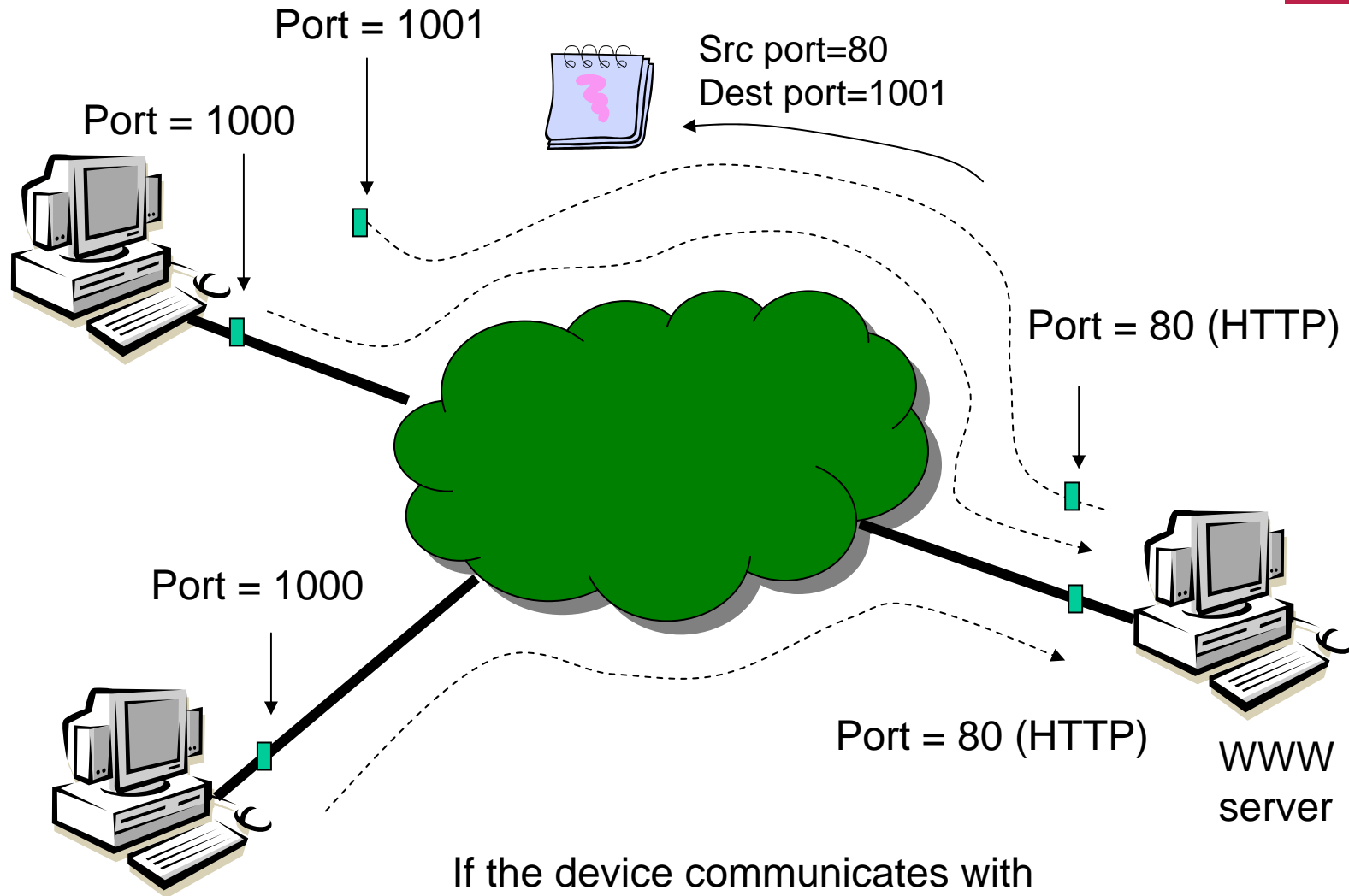
Example



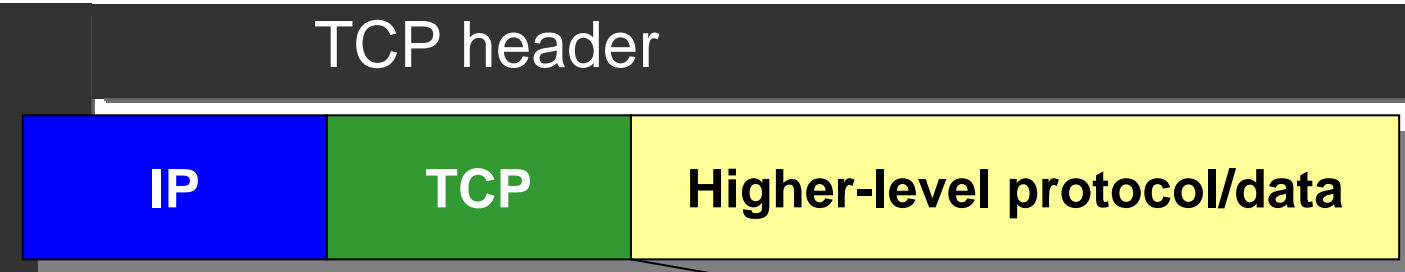
Example



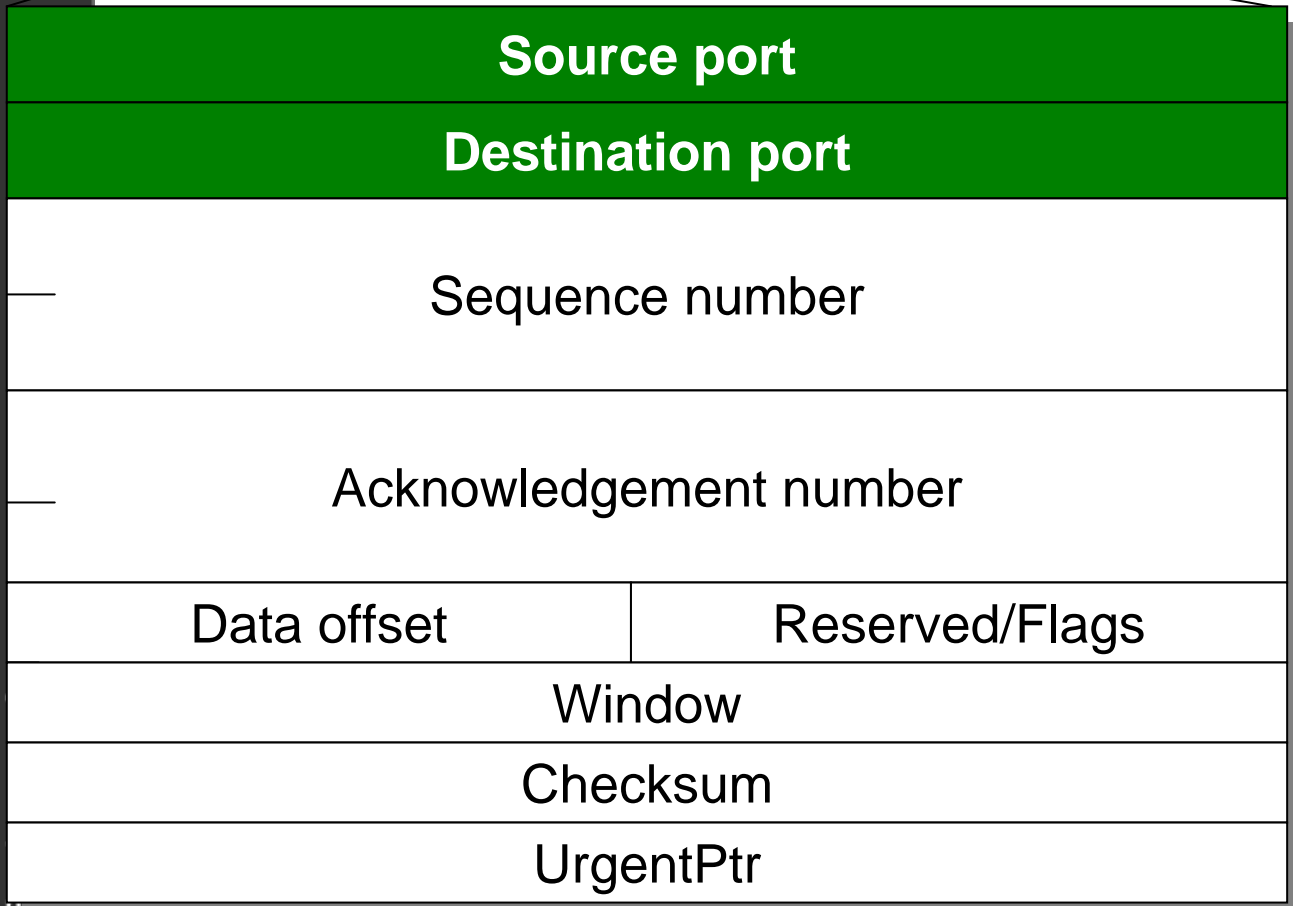
Example



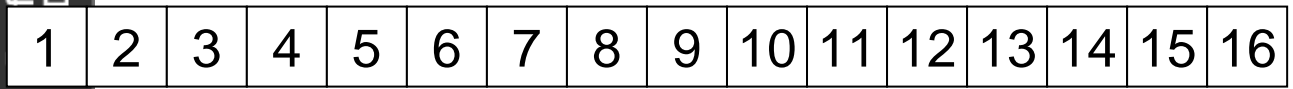
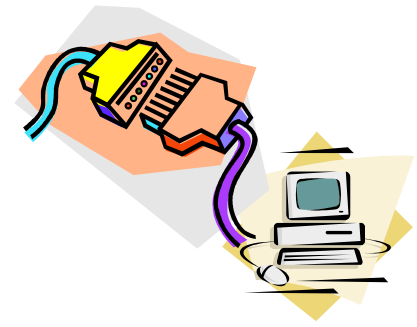
If the device communicates with the same server, it must create a new port (in this case, 1001)

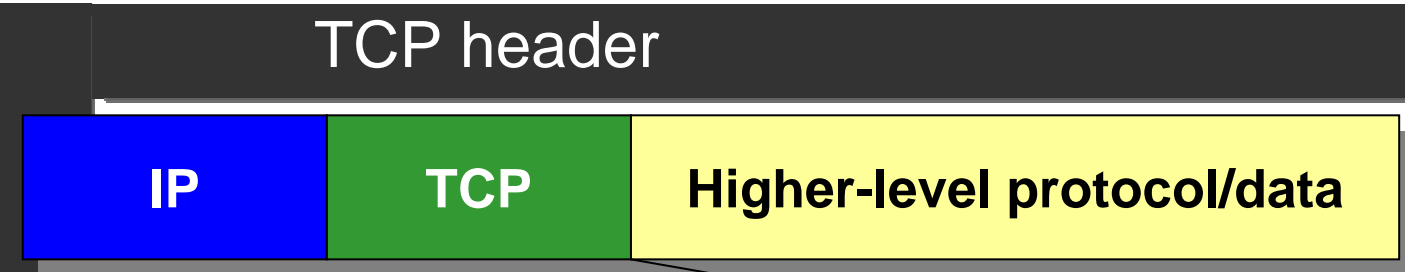


Data Packet

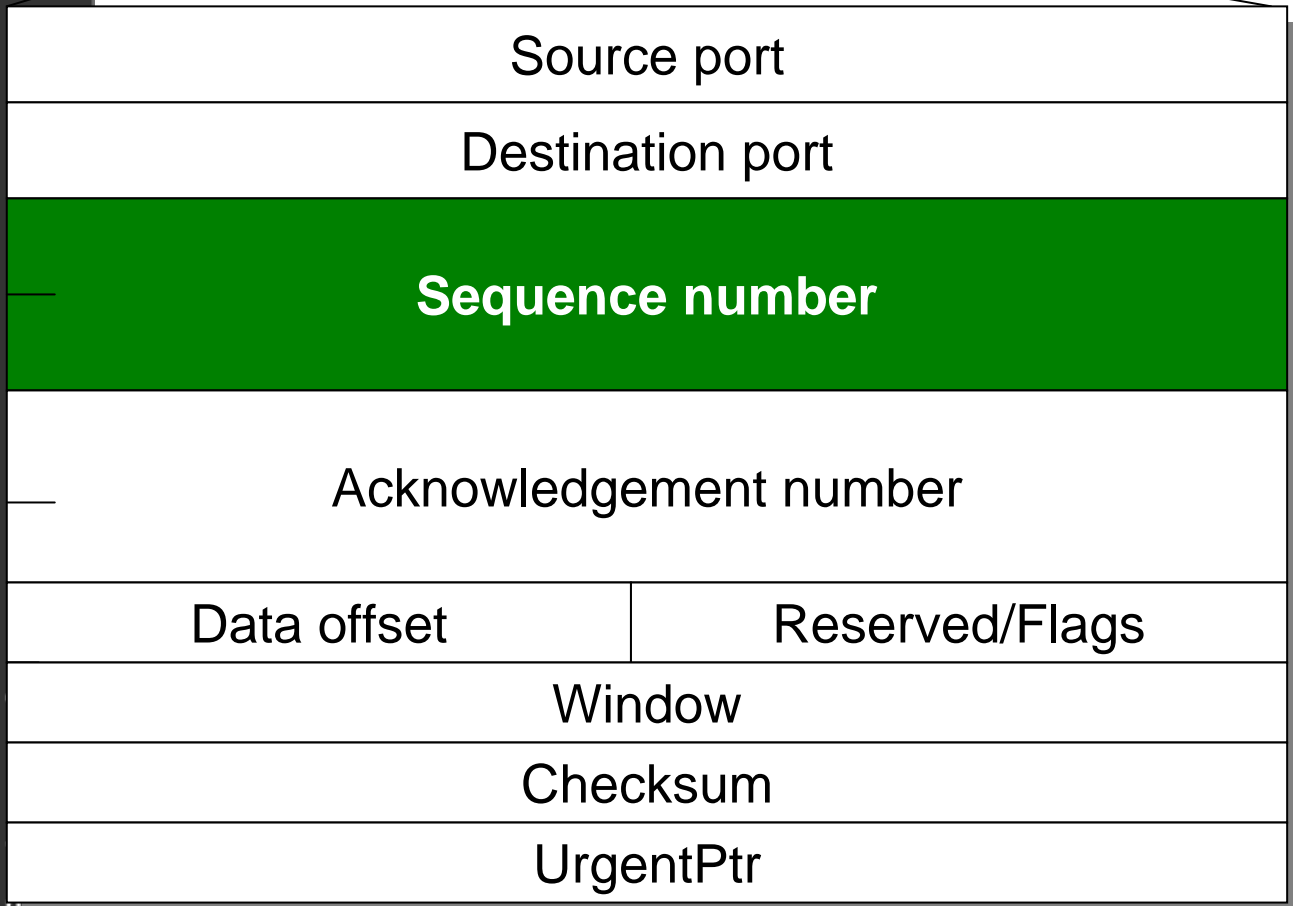


Source and destination port number – which are 16-bit values that identify the local port number (source number and destination port number or destination port).

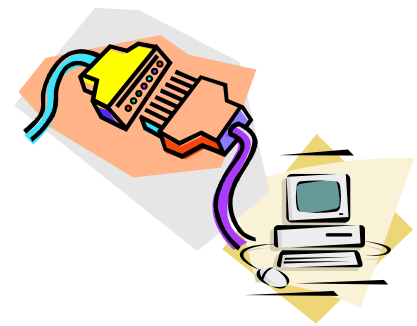
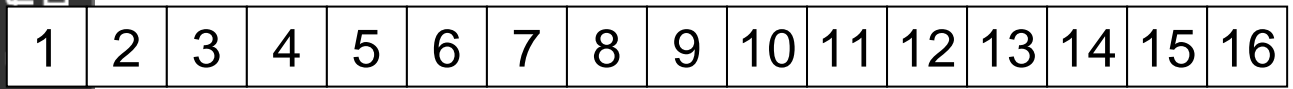


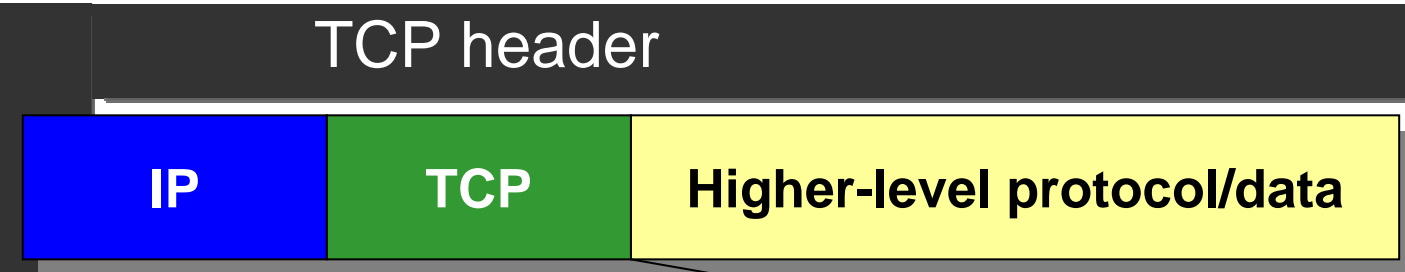


Data Packet

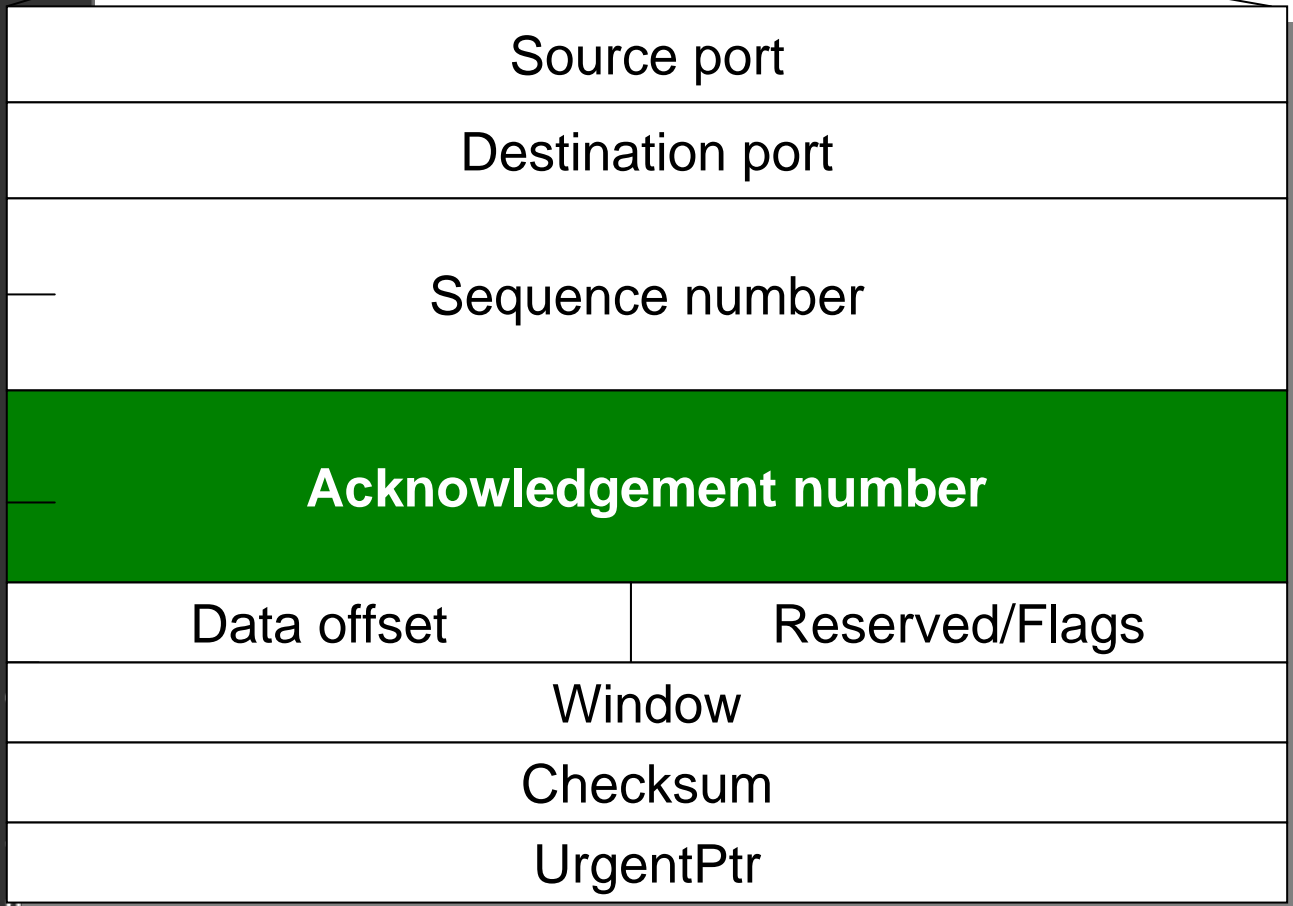


Sequence number – which identifies the current sequence number of the data segment. This allows the receiver to keep track of the data segments received. Any segments that are missing can be easily identified. The sequence number of the first data byte in this segment (except when SYN is present). If SYN is present the sequence number is the initial sequence number (ISN) and the first data octet is ISN+1.

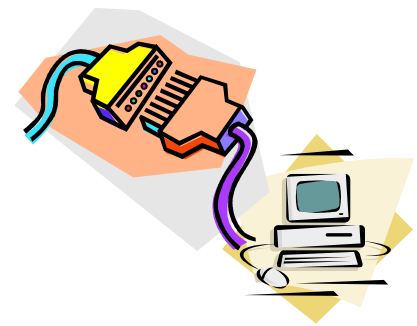
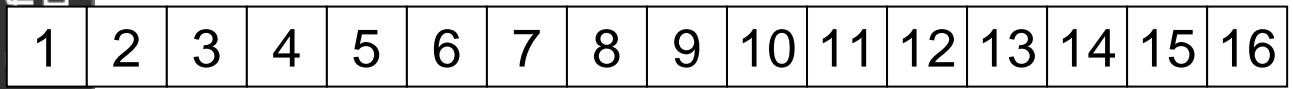


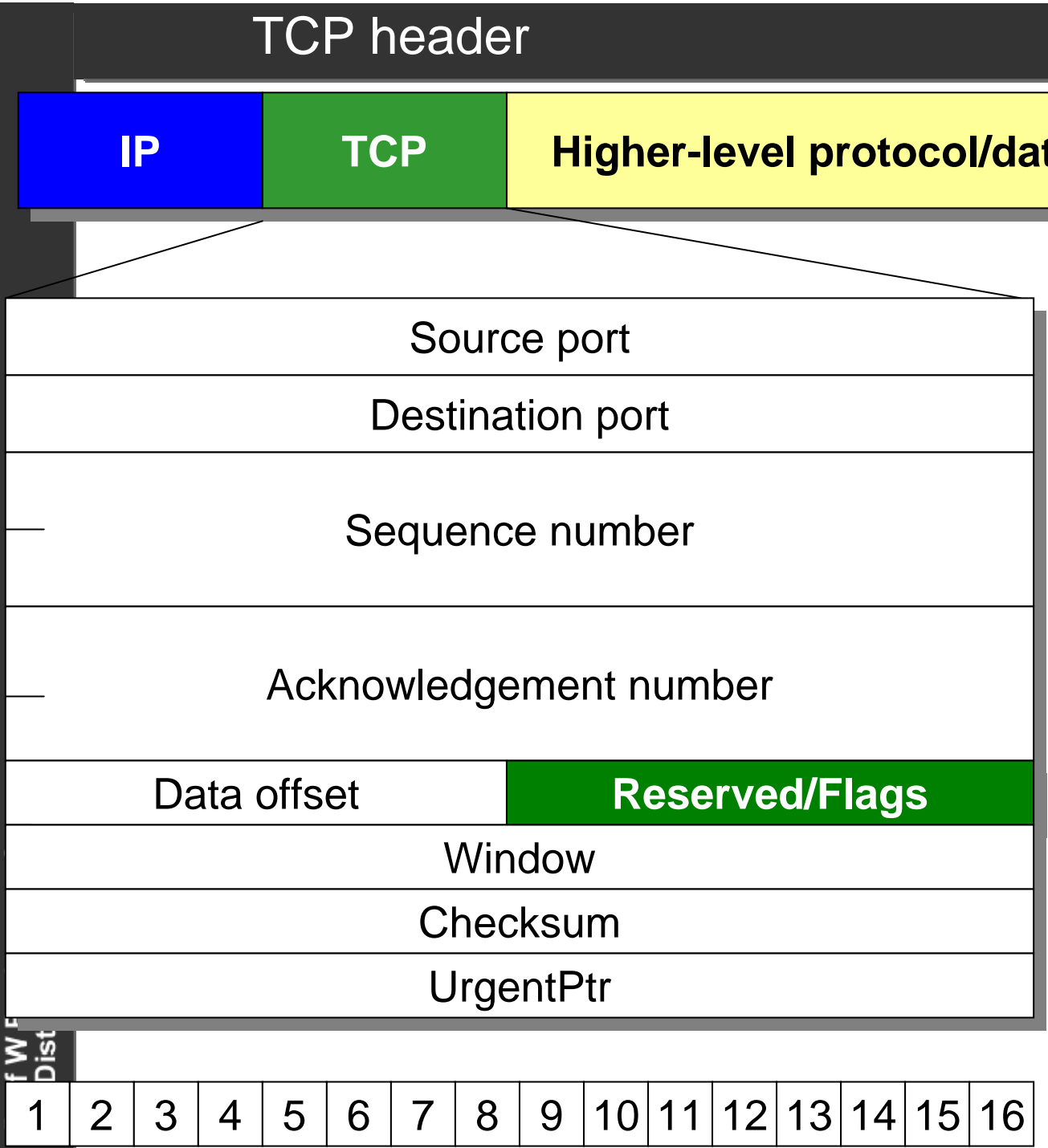


Data Packet



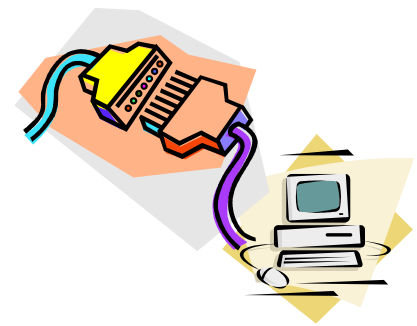
Acknowledgement number – when the ACK bit is set, it contains the value of the next sequence number the sender of the packet is expecting to receive. This is always set after the connection is made.





Data Packet

Flags – the flag field is defined as UAPRSF, where U is the urgent flag (URG), A the acknowledgement flag (ACK), P the push function (PSH), R the reset flag (RST), S the sequence synchronise flag (SYN) and F the end-of-transmission flag (FIN).



Examples of Data Exchange

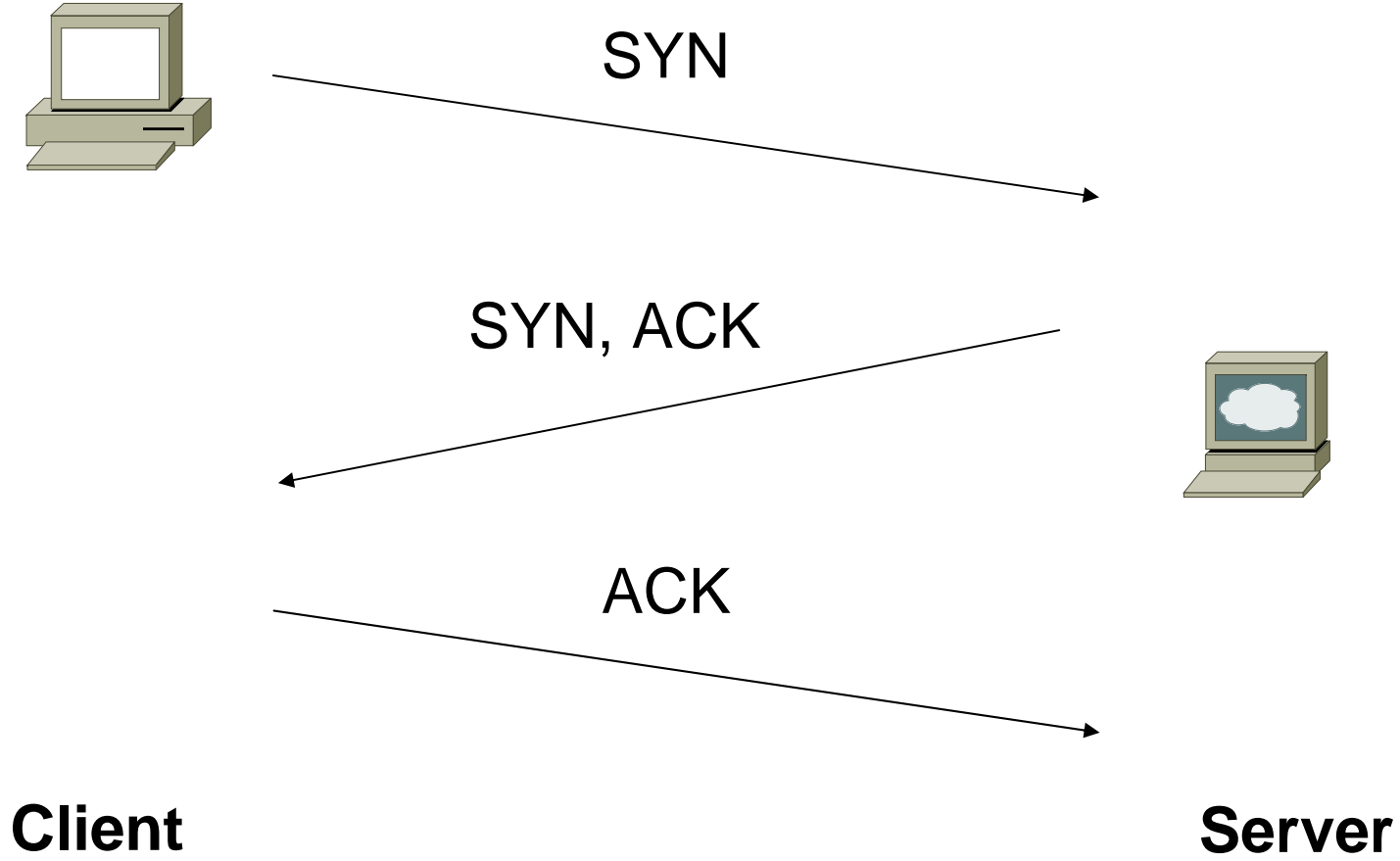


Originator		Recipient
1. CLOSED		LISTEN
2. SYN-SENT	→ <SEQ=999><CTL=SYN>	SYN-RECEIVED
3. ESTABLISHED	<SEQ=100><ACK=1000><CTL=SYN,ACK> ←	SYN-RECEIVED
4. ESTABLISHED	→ <SEQ=1000><ACK=101><CTL=ACK>	ESTABLISHED
5. ESTABLISHED	→ <SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED

Originator		Recipient
1. CLOSED		LISTEN
2. SYN-SENT	→ <SEQ=999><CTL=SYN>	
3. (duplicate)	→ <SEQ=900><CTL=SYN>	
4. SYN-SENT	<SEQ=100><ACK=901> <CTL=SYN,ACK>←	SYN-RECEIVED
5. SYN-SENT	→ <SEQ=901><CTL=RST>	LISTEN
(packet 2 received)	→	
7. SYN-SENT	<SEQ=100><ACK=1000><CTL=SYN,ACK>←	SYN-RECEIVED
8. ESTABLISHED	→ <SEQ=1000><ACK=101><CTL=ACK><DATA>	ESTABLISHED

Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security



SYN

Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

The screenshot shows the Wireshark interface with a packet list and packet details pane. The packet list shows a SYN packet (No. 72) from 192.168.1.101 to 146.176.1.188. The packet details pane shows the following information:

- Frame 72 (62 bytes on wire, 62 bytes captured)
- Ethernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
- Internet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)
- Transmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), Seq: 0, Ack: 0, Len: 0
 - Source port: 4213 (4213)
 - Destination port: http (80)
 - Sequence number: 0 (relative sequence number)
 - Header length: 28 bytes
 - Flags: 0x0002 (SYN)
 - window size: 16384
 - checksum: 0x3c0c (correct)
 - options: (8 bytes)

The packet bytes pane shows the following hex and ASCII data:

```
0000 00 0c 41 f5 23 d5 00 15 00 34 02 f0 08 00 45 00  ..A.#...4...E.
0010 00 30 6f 51 40 00 80 06 34 fd c0 a8 01 65 92 b0  .0oq@...4...e.
0020 01 bc 10 75 00 50 af c2 f0 d9 00 00 00 00 70 02  ...u.P...p.
0030 40 00 3c 0c 00 00 02 04 04 ec 01 01 04 02     @.<.....
```

SYN, ACK



Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. C

The screenshot shows the Wireshark interface with a packet capture list and a detailed view of a selected packet. The packet list shows a SYN, ACK packet from www.napier.ac.uk to 192.168.1.101. The detailed view shows the Ethernet II, Internet Protocol, and Transmission Control Protocol (TCP) layers. The TCP layer details include: source port: http (80), destination port: 4213 (4213), sequence number: 0 (relative sequence number), acknowledgement number: 1 (relative ack number), header length: 28 bytes, flags: 0x0012 (SYN, ACK), window size: 16384, and checksum: 0xa97c (correct). The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
59	9.271160	192.168.1.101	sqm.msn.com	HTTP	Continuation or non-HTTP traffic
60	9.469300	sqm.msn.com	192.168.1.101	TCP	http > 4212 [ACK] Seq=1 Ack=433 Win=8192 Len=0
61	9.470127	sqm.msn.com	192.168.1.101	HTTP	HTTP/1.1 100 Continue
62	9.493518	sqm.msn.com	192.168.1.101	HTTP	HTTP/1.1 200 OK
63	9.493559	192.168.1.101	sqm.msn.com	TCP	4212 > http [ACK] Seq=1061 Ack=266 win=17375 Len=0
64	9.493701	sqm.msn.com	192.168.1.101	TCP	http > 4212 [FIN, ACK] Seq=266 Ack=1061 win=64475 Len=0
65	9.493726	192.168.1.101	sqm.msn.com	TCP	4212 > http [ACK] Seq=1061 Ack=267 win=17375 Len=0
66	9.494057	192.168.1.101	sqm.msn.com	TCP	4212 > http [FIN, ACK] Seq=1061 Ack=267 win=17375 Len=0
67	9.683109	sqm.msn.com	192.168.1.101	TCP	http > 4212 [ACK] Seq=267 Ack=1062 win=64475 Len=0
68	9.980194	192.168.1.101	resolver2.svr.pol.	DNS	Standard query PTR 255.1.168.192.in-addr.arpa
69	10.005697	resolver2.svr.pol.	192.168.1.101	DNS	Standard query response, No such name
70	14.477532	192.168.1.101	resolver2.svr.pol.	DNS	Standard query A www.napier.ac.uk
71	14.503727	resolver2.svr.pol.	192.168.1.101	DNS	Standard query response A 146.176.1.188
72	14.512705	192.168.1.101	www.napier.ac.uk	TCP	4213 > http [SYN] Seq=0 Ack=0 win=16384 Len=0 MSS=1260
73	14.515118	192.168.1.1	192.168.1.255	SNMP	TRAP-v1 SNMPV2-SMI::enterprises.3955.1.1.0
74	14.553506	www.napier.ac.uk	192.168.1.101	TCP	http > 4213 [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MSS=1352
75	14.553533	192.168.1.101	www.napier.ac.uk	TCP	4213 > http [ACK] Seq=1 Ack=1 win=17640 Len=0
76	14.553687	192.168.1.101	www.napier.ac.uk	HTTP	GET / HTTP/1.1

Frame 74 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: 00:0c:41:f5:23:d5, Dst: 00:15:00:34:02:f0
Internet Protocol, Src Addr: www.napier.ac.uk (146.176.1.188), Dst Addr: 192.168.1.101 (192.168.1.101)
Transmission Control Protocol, Src Port: http (80), Dst Port: 4213 (4213), Seq: 0, Ack: 1, Len: 0
source port: http (80)
Destination port: 4213 (4213)
Sequence number: 0 (relative sequence number)
Acknowledgement number: 1 (relative ack number)
Header length: 28 bytes
Flags: 0x0012 (SYN, ACK)
window size: 16384
checksum: 0xa97c (correct)
Options: (8 bytes)
[SEQ/ACK analysis]

```
0000 00 15 00 34 02 f0 00 0c 41 f5 23 d5 08 00 45 00  ...4... A.#...E.
0010 00 30 9c 28 00 00 6e 06 5a 26 92 b0 01 bc c0 a8  .0(.n.Z&.....
0020 01 65 00 50 10 75 7d f8 14 2a af c2 f0 da 70 12  .e.P.u}:.*....p.
0030 40 00 a9 7c 00 00 02 04 05 48 01 01 04 02      @..|... .H....
```

Author: Bill Buchanan

ACK

Wireless LAN - C072047
Prof W Buchanan
for Dist. C

The screenshot shows the Wireshark interface with a packet capture list and a detailed view of a selected packet. The packet list shows an ACK packet (No. 75) from 192.168.1.101 to www.napier.ac.uk. The detailed view shows the following information:

- Frame 75 (54 bytes on wire, 54 bytes captured)
- Ethernet II, Src: 00:15:00:34:02:f0, Dst: 00:0c:41:f5:23:d5
- Internet Protocol, Src Addr: 192.168.1.101 (192.168.1.101), Dst Addr: www.napier.ac.uk (146.176.1.188)
- Transmission Control Protocol, Src Port: 4213 (4213), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
 - Source port: 4213 (4213)
 - Destination port: http (80)
 - Sequence number: 1 (relative sequence number)
 - Acknowledgement number: 1 (relative ack number)
 - Header length: 20 bytes
 - Flags: 0x0010 (ACK)
 - Window size: 17640
 - Checksum: 0xd0ec (correct)
 - [SEQ/ACK analysis]

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 0c 41 f5 23 d5 00 15 00 34 02 f0 08 00 45 00  ..A.#... .4...E.  
0010 00 28 6f 53 40 00 80 06 35 03 c0 a8 01 65 92 b0  :(os@... 5....e..  
0020 01 bc 10 75 00 50 af c2 f0 da 7d f8 14 2b 50 10  ...u.P.. ..]+P.  
0030 44 e8 d0 ec 00 00  D.....
```

Filtering

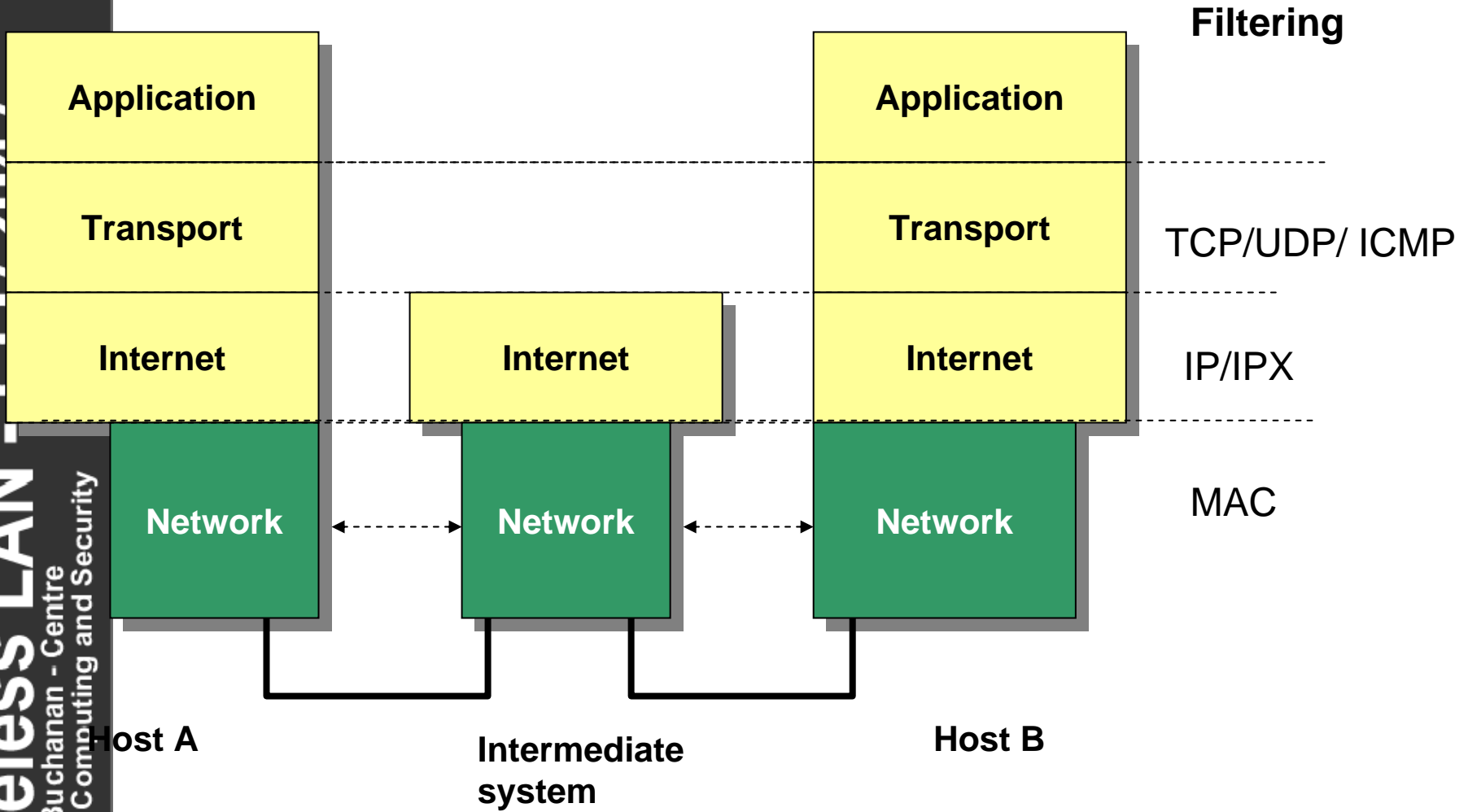


Layer filtering



CO72017

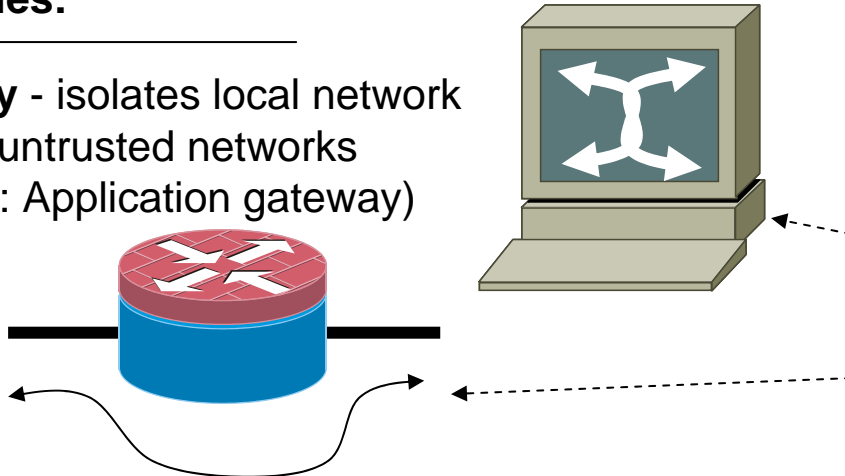
Wireless LAN
Prof W Buchanan - Centre
for Dist. Computing and Security



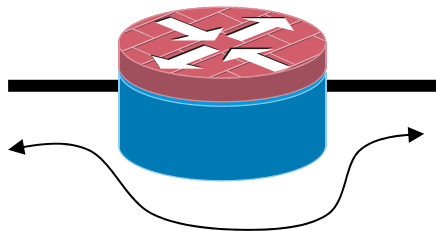
Firewalls

Screening Firewalls and Proxies:

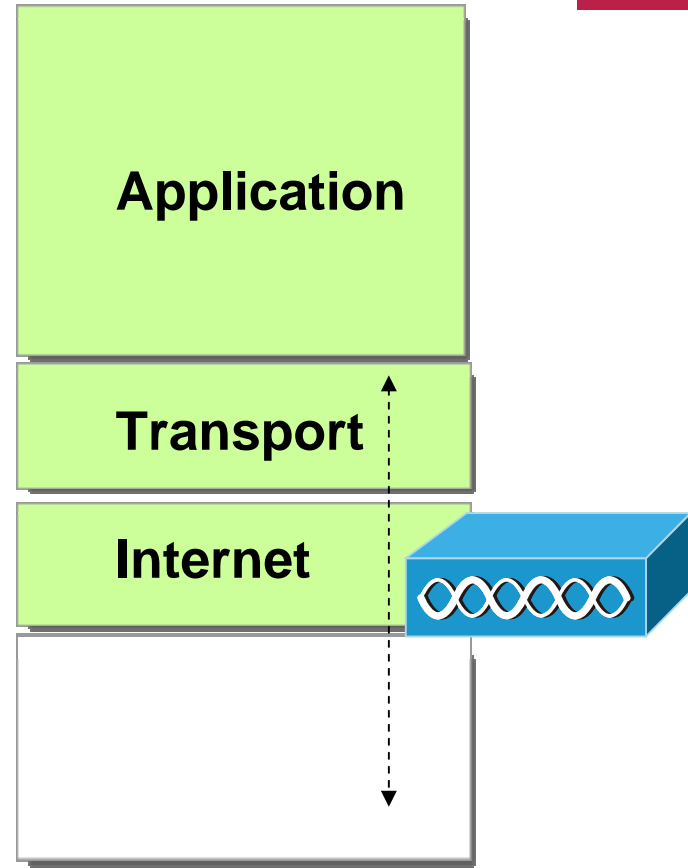
Proxy - isolates local network from untrusted networks (AKA: Application gateway)



Screening firewall: Filters for source and destination TCP ports



Screen firewall: Filters for source and destination IP addresses



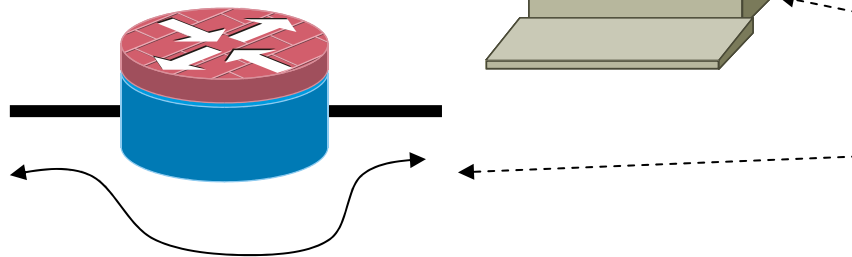
Internet model

Firewalls and Proxies



Screening Firewalls and Proxies:

Proxy - isolates local network from untrusted networks (AKA: Application gateway)



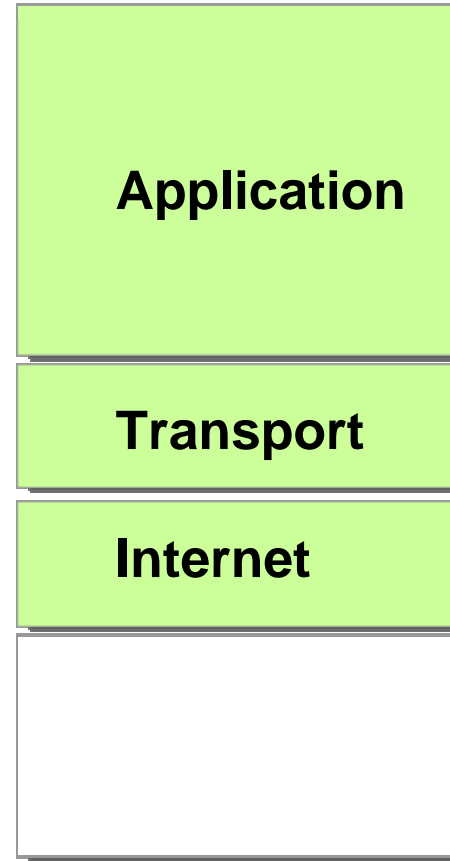
Screening firewall:

Advantages:

- Simple.
- Low costs

Disadvantages:

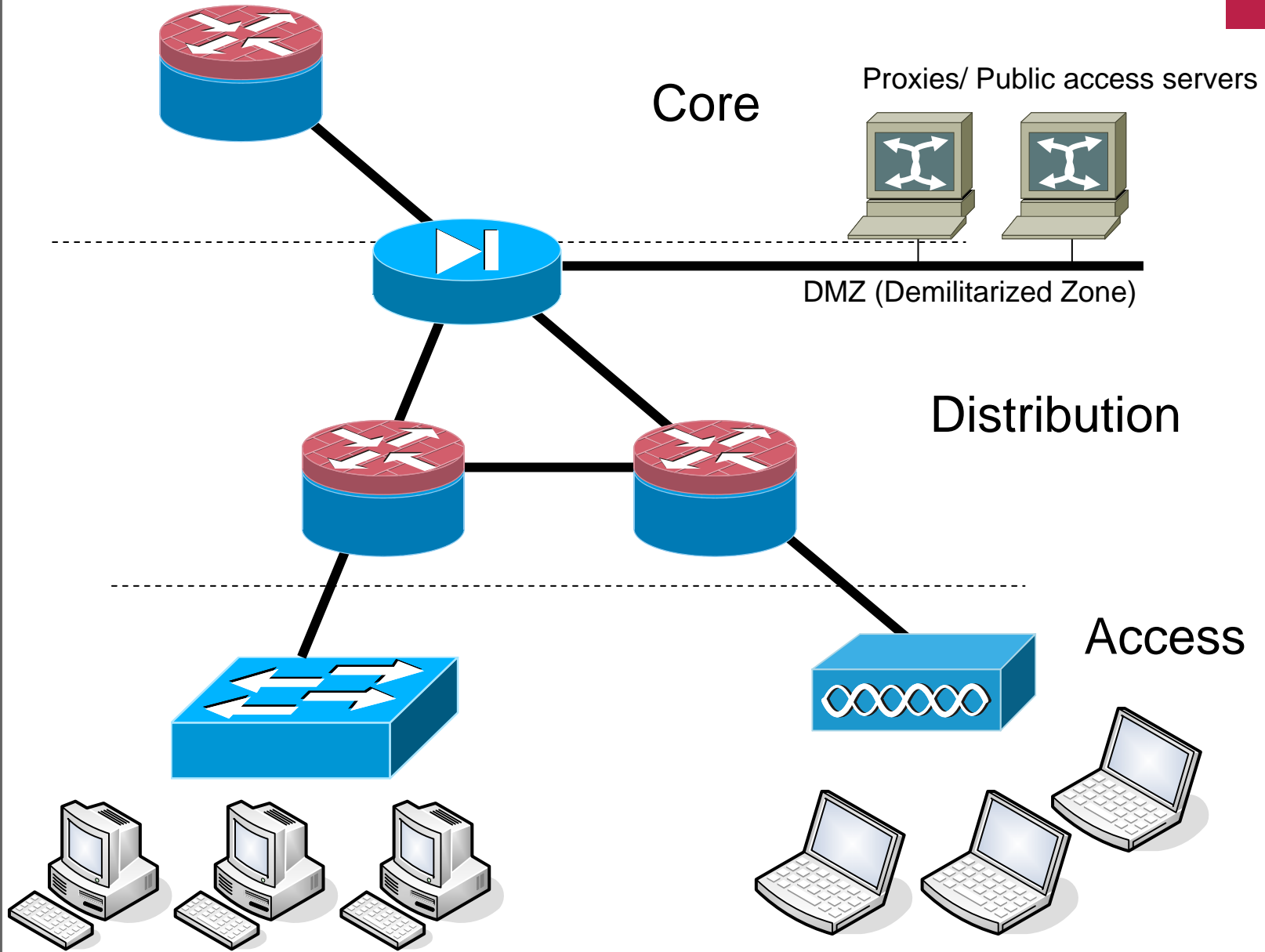
- Complexity of rules.
- Cost of managing firewall.
- Lack of user-authentication.



Internet model

Wireless LAN - C072047

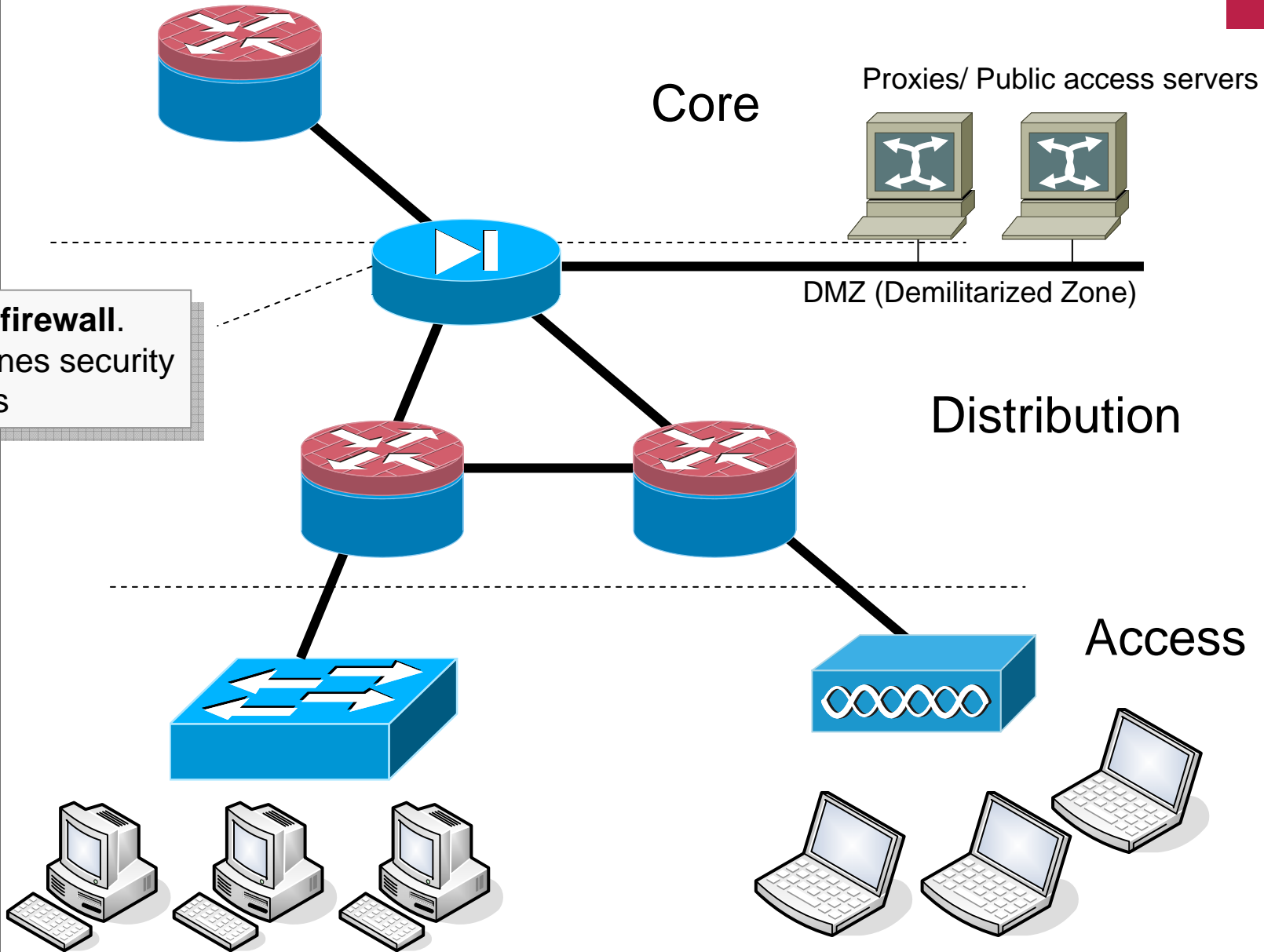
Prof W Buchanan - Centre
for Dist. Computing and Security



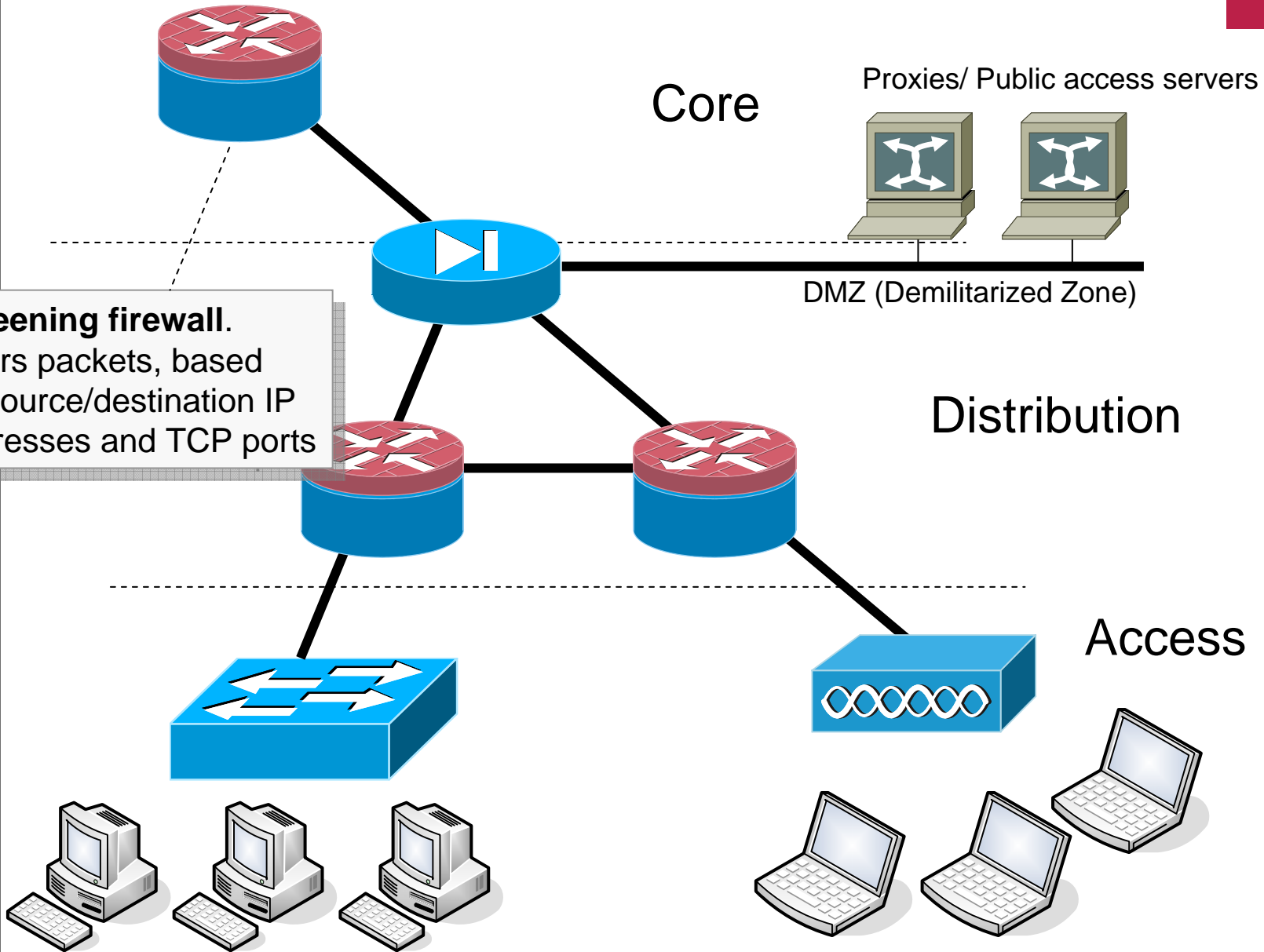
Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

PIX firewall.
Defines security
rules

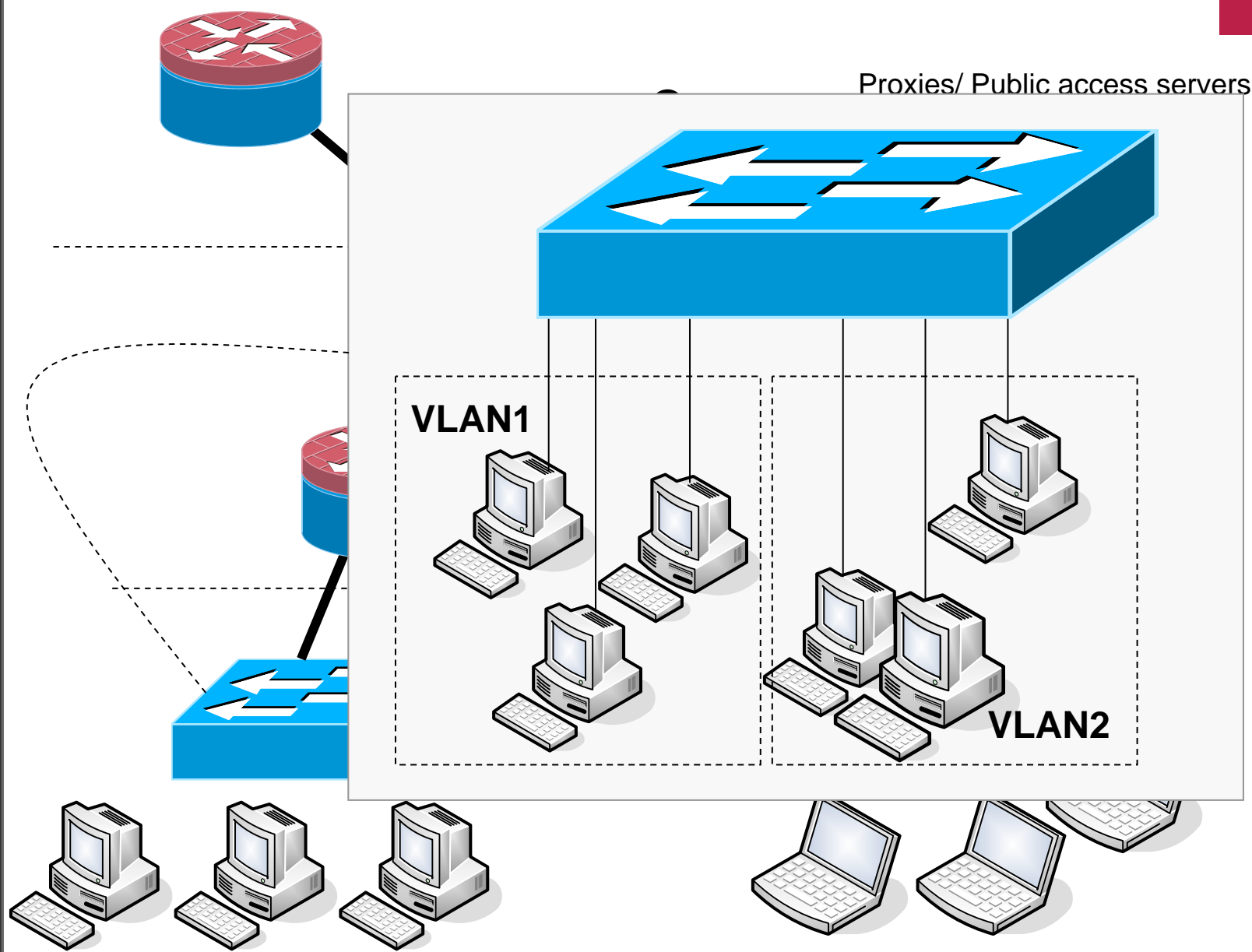


Screening firewall.
Filters packets, based on source/destination IP addresses and TCP ports



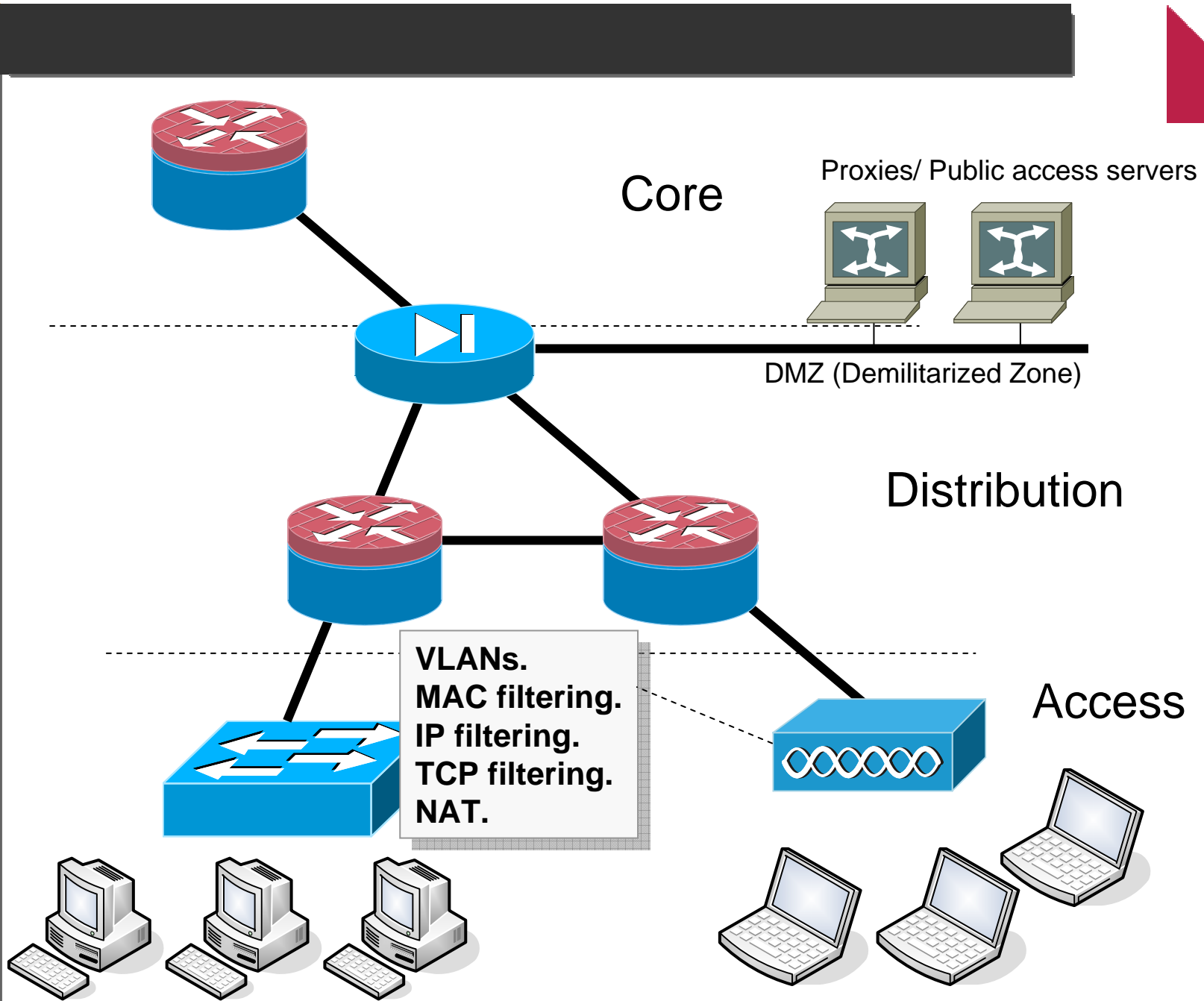
Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security



Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security



Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist. Computing and Security

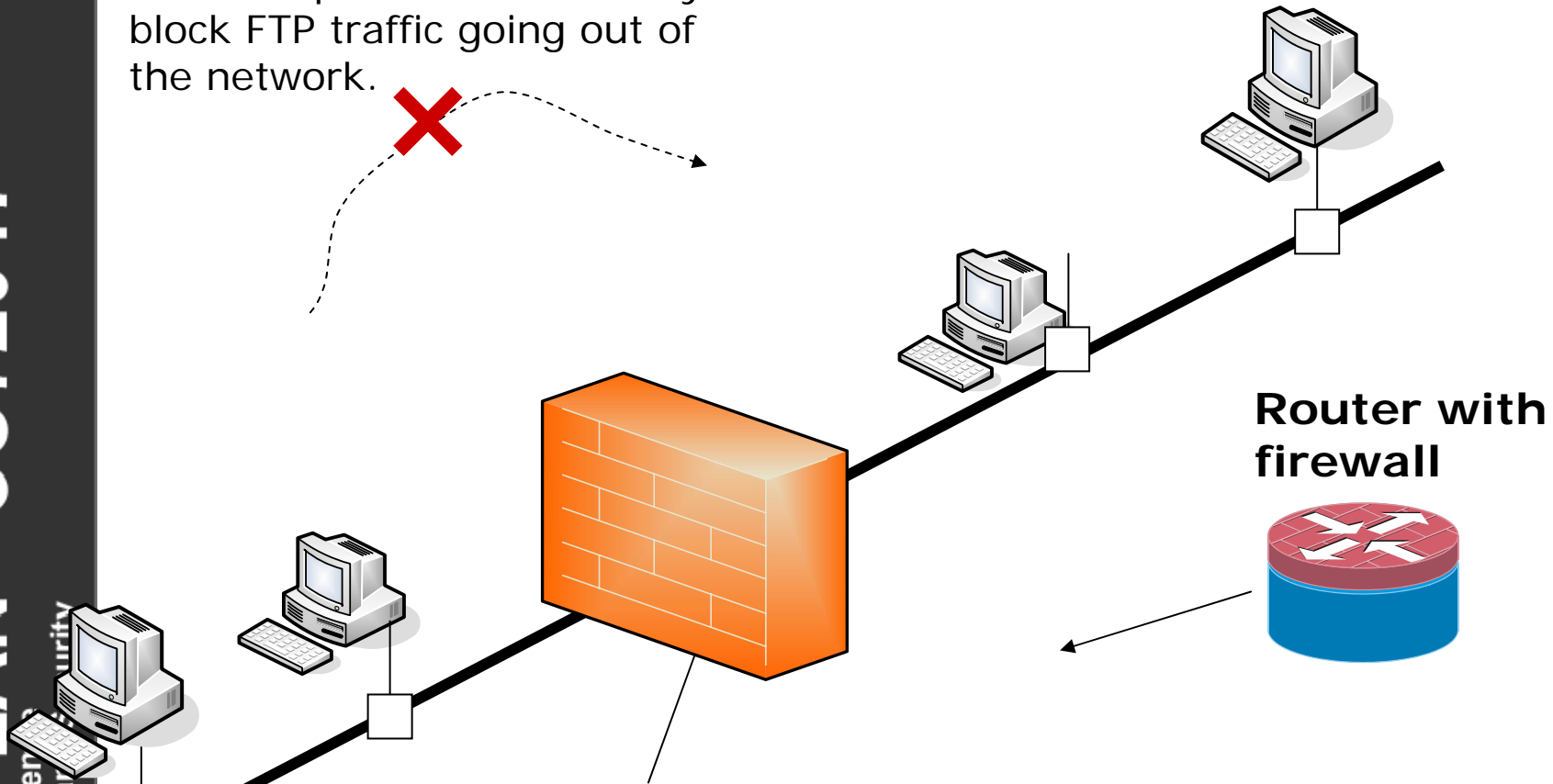
Screening Firewall



Author: Bill Buchanan

Screening Firewall

For example the firewall may block FTP traffic going out of the network.



A **port** on a router can be setup with **ACLs** to filter traffic based on the network address or the source or destination port number

ACLs

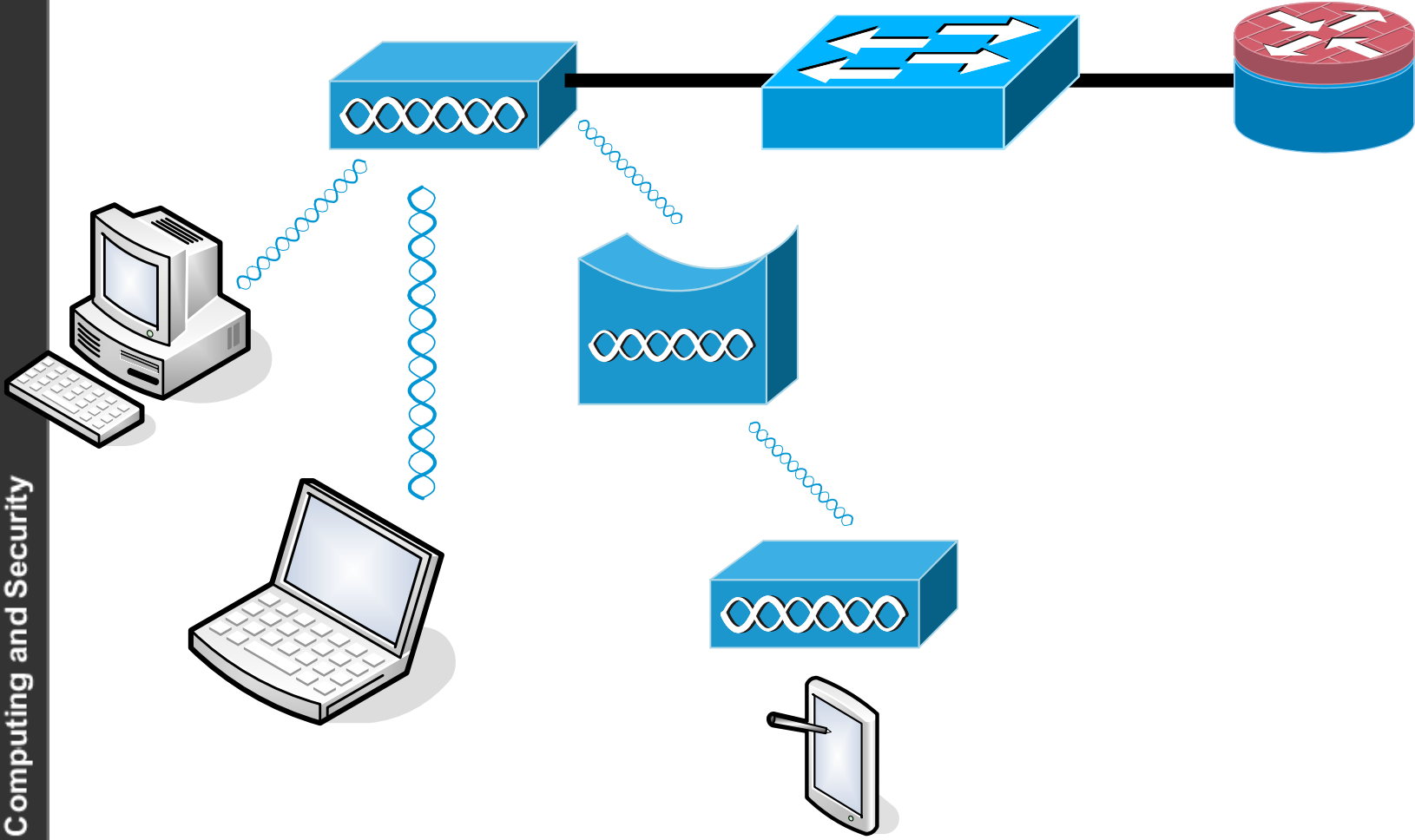
- **MAC address.**
- **Source IP address.** The address that the data packet was sent from.
- **Destination IP address.** The address that the data packet is destined for.
- **Source TCP port.** The port that the data segment originated from. Typical ports which could be blocked are FTP (port 21), TELNET (port 23), and WWW (port 80).
- **Destination TCP port.** The port that the data segment is destined for.
- **Protocol type.** This filters for UDP or TCP traffic.

MAC address filtering



Wireless LAN - C072047

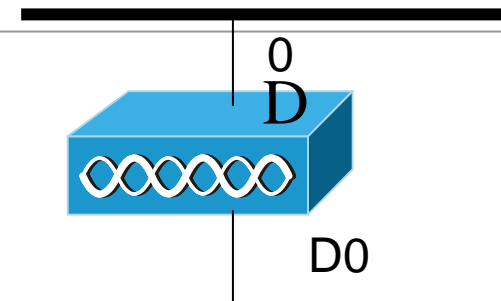
Prof W Buchanan - Centre
for Dist. Computing and Security




```
access-list [<700-799> | <1100-1199>] [deny | permit] [source  
ac] [source mask] [dest mac] [dest mask]
```

For example to disallow the node with the mac address of 0090.4b54.d83a access to 0060.b39f.cae1:

```
(config)# access-list 1101 deny 0090.4b54.d83a 0.0.0  
0060.b39f.cae1 0.0.0  
(config)# access-list 1101 permit 0.0.0 ffff.ffff.ffff 0.0.0  
ffff.ffff.ffff  
  
(config)# int d0  
(config-if)# 12-filter bridge-group-ac1  
(config-if)# bridge-group input-address-list 1101
```



Standard ACLs



Standard ACLs

```
Router# access-list access-list-value {permit | deny} source source-mask
```

```
Router# access-list 1 deny 156.1.1.10 0.0.0.0
```

```
Router# access-list 1 deny 156.1.1.0 0.0.0.255
```

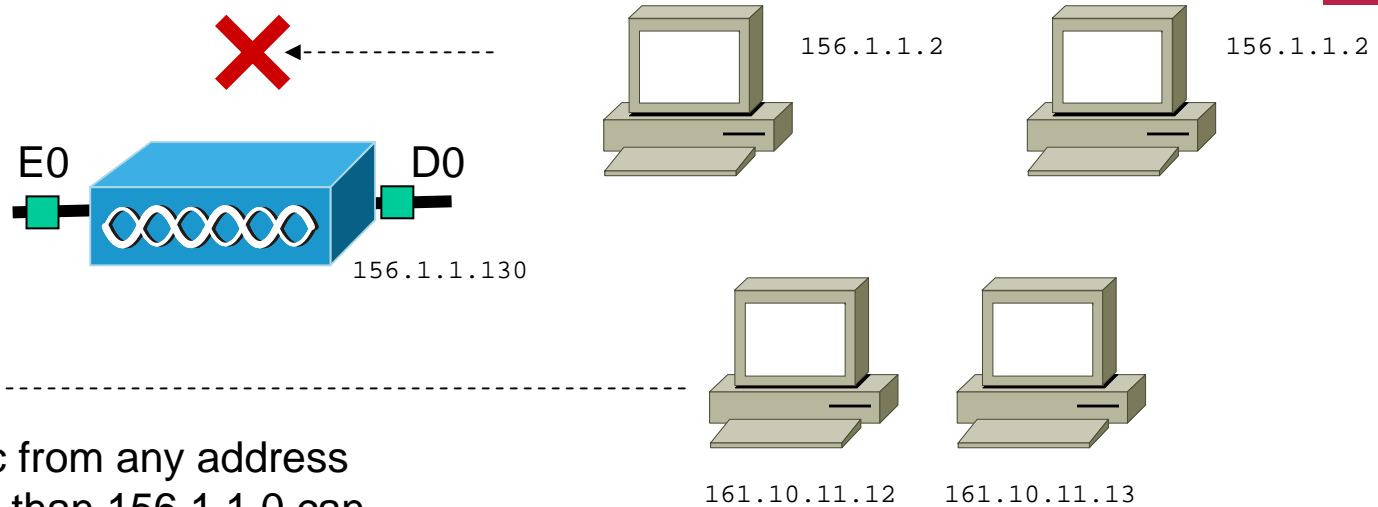
```
Router# access-list 1 deny 156.1.1.0 0.0.0.255  
Router# access-list 1 permit ip any any
```

```
Router (config)# interface Ethernet0  
Router (config-if)# ip address 156.1.1.130 255.255.255.0  
Router (config-if)# ip access-group 1 in
```



Standard ACLs
filter on the
source IP
address

Standard ACLs



Traffic from any address
rather than 156.1.1.0 can
pass

Match this part

```
Router# access-list 1 deny 156.1.1.0 0.0.0.255  
Router# access-list 1 permit any
```

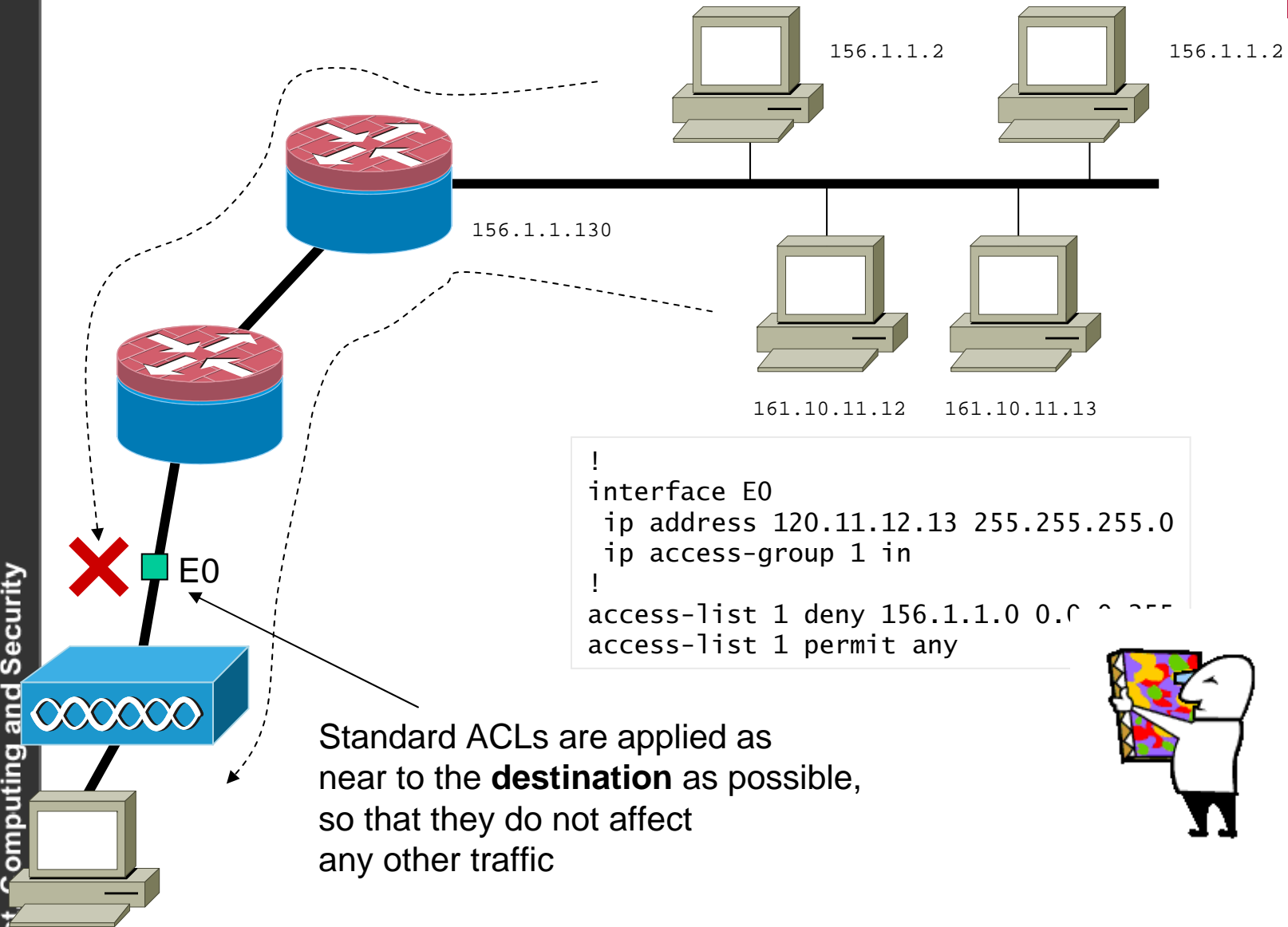
Ignore this part

```
Router (config)# interface D0  
Router (config-if)# ip address 156.1.1.130 255.255.255.0  
Router (config-if)# ip access-group 1 in
```

Standard ACLs

Wireless LAN - C072047

Prof W Buchanan - Centre
for Dist Computing and Security



```
!
interface E0
 ip address 120.11.12.13 255.255.255.0
 ip access-group 1 in
!
access-list 1 deny 156.1.1.0 0.0.0.255
access-list 1 permit any
```



```
(config)#ip access-list standard ?
<1-99>          Standard IP access-list number
<1300-1999>    Standard IP access-list number (expanded range)
WORD            Access-list name
where WORD is the name of the access-list is be defined. For example:

(config)#ip access-list standard Test

(config-std-nacl)#?
Standard Access List configuration commands:
deny           Specify packets to reject
exit           Exit from access-list configuration mode
no             Negate a command or set its defaults
permit        Specify packets to forward
and to define a standard access-list:
(config-std-nacl)#deny 156.1.1.0 0.0.0.255
(config-std-nacl)#permit ?
Hostname or A.B.C.D  Address to match
any                  Any source host
host                 A single host address
```



```
(config-std-nacl)#permit ?  
  Hostname or A.B.C.D  Address to match  
  any                  Any source host  
  host                 A single host address  
(config-std-nacl)#permit any ?  
  log  Log matches against this entry  
  <cr>  
(config-std-nacl)#permit any
```

It can then be applied with:

```
(config)#int e0  
(config-if)#ip access-group ?  
  <1-199>      IP access list (standard or extended)  
  <1300-2699> IP expanded access list (standard or extended)  
  WORD        Access-list name  
(config-if)#ip access-group Test ?  
  in  inbound packets  
  out outbound packets  
(config-if)#ip access-group Test in
```

Extended ACLs



Extended ACLs

```
Router# access-list access-list-value {permit | deny} {test-conditions}
```



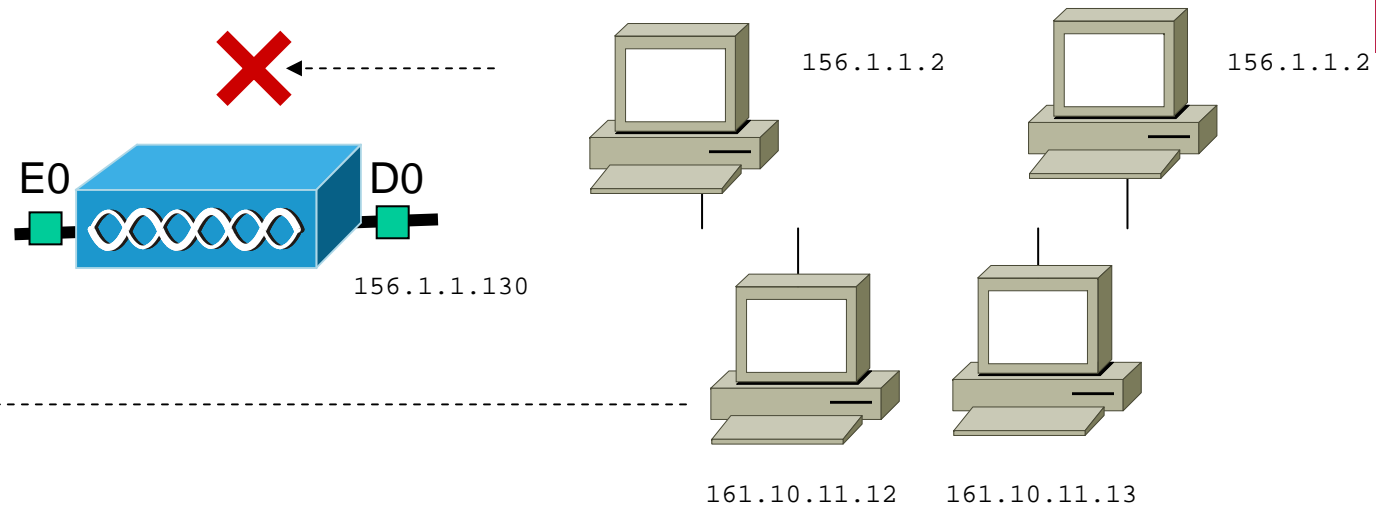
```
Router(config)#access-list 100 deny ip host 156.1.1.134 156.70.1.1 0.0.0.0  
Router(config)#access-list 100 permit ip any any
```

```
Router(config)#access-list 100 deny ip 156.1.1.0 0.0.0.255 156.70.1.0  
                                0.0.0.255  
Router(config)#access-list 100 permit ip any any
```

```
Router(config)#access-list 100 deny ip 156.1.1.0 0.0.0.254 host 156.70.1.1  
Router(config)#access-list 100 permit ip any any
```

```
Router (config)# interface Ethernet0  
Router (config-if)# ip address 156.1.1.130 255.255.255.192  
Router (config-if)# ip access-group 100 in
```

Extended ACLs



```
(config)#access-list 100 deny ip host 156.1.1.2 70.1.2.0 0.0.0.255  
(config)#access-list 100 permit ip any any
```

Denies traffic from 156.1.1.2 to the 70.1.2.0 network

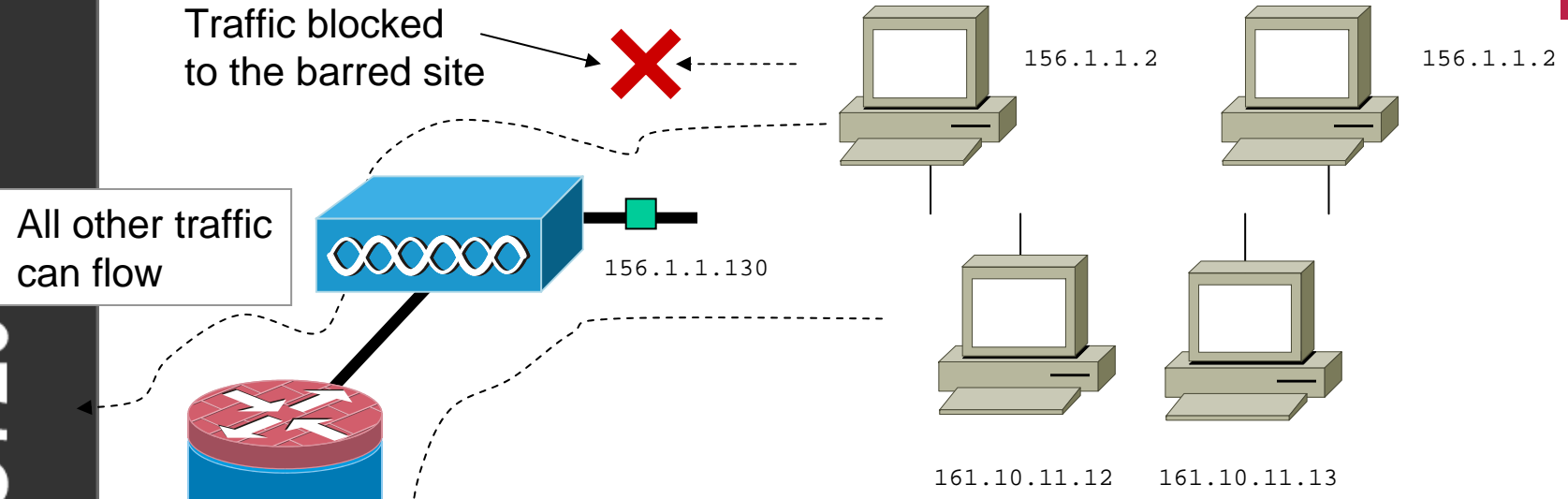
```
(config)#access-list 100 deny ip 156.1.1.0 0.0.0.255 70.1.2.0 0.0.0.255  
(config)#access-list 100 permit ip any any
```

Denies traffic from any host on 156.1.1.0 to the 70.1.2.0 network

Example of an Extended ACL

Wireless LAN - C072047

Prof W Buchanan - Centre for Distributed Computing and Security



```
!
interface D0
 ip address 156.1.1.130 255.255.255.0
 ip access-group 100 in
!
access-list 100 deny ip 156.1.1.0 0.0.0.255 140.5.6.7 0.0.0.255
access-list 100 permit ip any any
```



Extended ACLs are applied as near to the **source** as possible, as they are more targeted

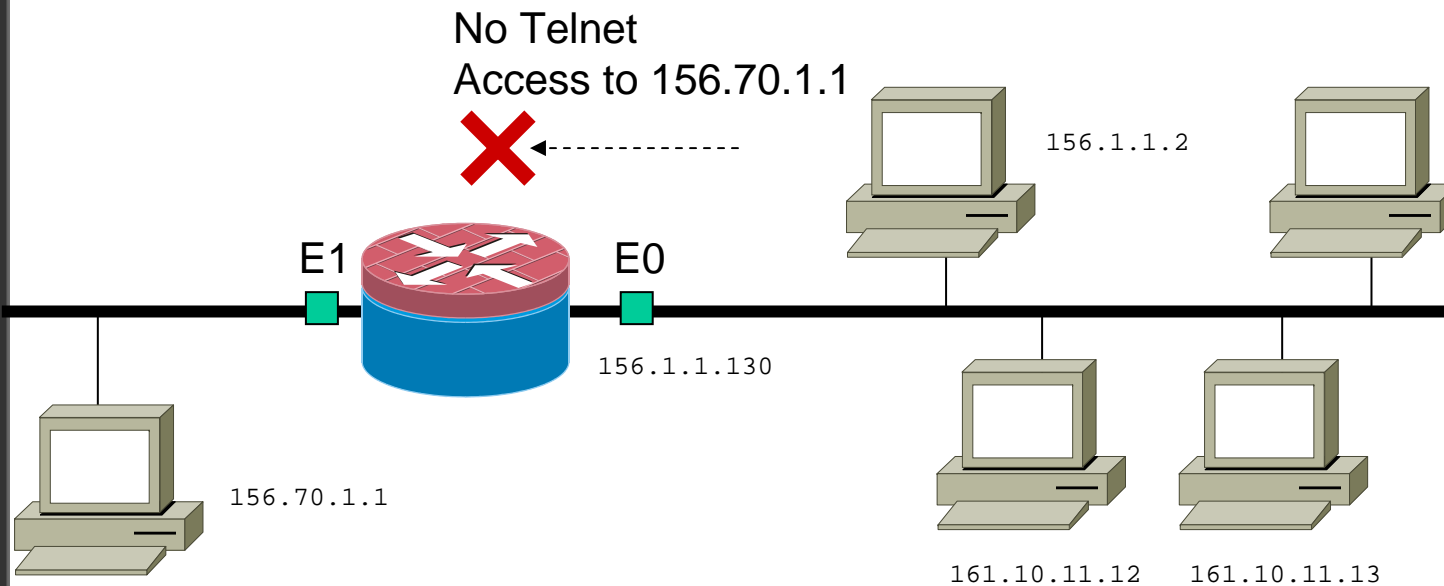
Extended ACLs filtering TCP traffic

An extended ACLs can also filter for TCP/UDP traffic, such as:

Optional field
in brackets

```
Router(config)#access-list access-list-value { permit | deny } {tcp | udp  
| igmp} source source-mask destination destination-mask {eq | neq | lt |  
gt} port
```

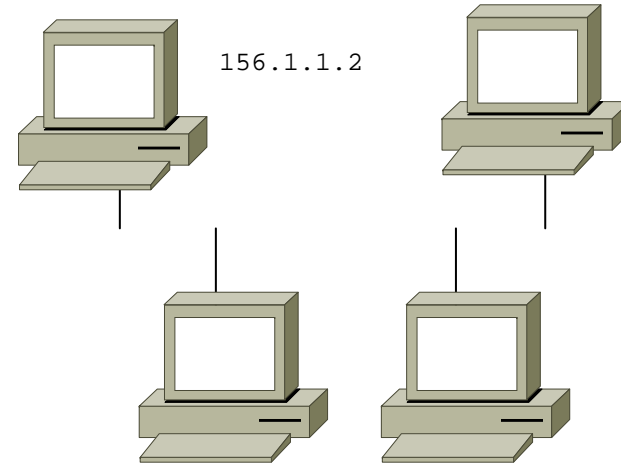
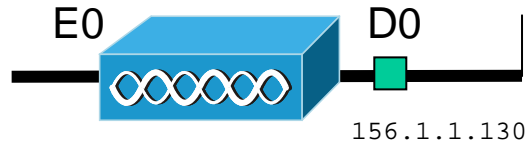
```
access-list 101 deny tcp 156.1.1.0 0.0.0.255 eq any host 156.70.1.1 eq telnet  
access-list 101 permit ip any any
```



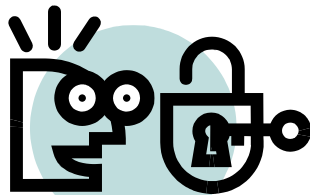
Open and closed firewalls



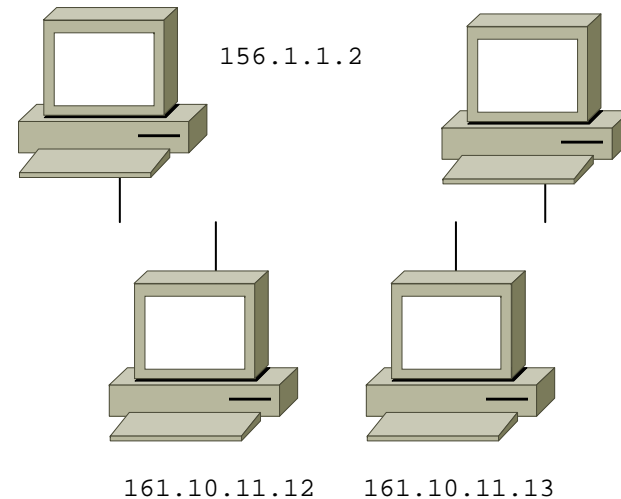
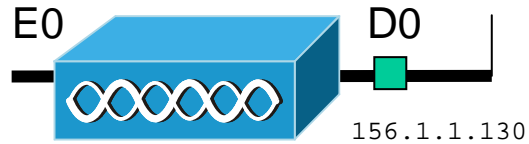
```
access-list 101 permit ...  
access-list 101 deny ip any any
```



A **closed** firewall, permits some things, and denies everything else



```
access-list 101 deny ...  
access-list 101 permit ip any any
```



An **open** firewall, denies some things, and permits everything else