Internet Protocols EBU5403
Live Lecture D3/D4
Tutorial and Office hour

Module organiser: Richard Clegg
(r.clegg@qmul.ac.uk)
Michael Chai (michael.chai@qmul.ac.uk)
Cunhua Pan(c.pan@qmul.ac.uk)

	Part 1	Part 2	Part 3	Part 4
Ecommerce + Telecoms 1	Richard Clegg		Cunhua Pan	
Telecoms 2	Michael Chai			

Structure of course

- Week 1
  - Introduction to IP Networks
  - The Transport layer (part I)
- Week 2
  - The Transport layer (part II)
  - The Network layer (part I)
  - Class test (open book exam in class)
- Week 3
  - The Network layer (part II)
  - The Data link layer (part I)
  - Router lab tutorial (assessed labwork after this week)
- Week 4
  - The Data link layer (part II)
  - Security and network management
  - Class test

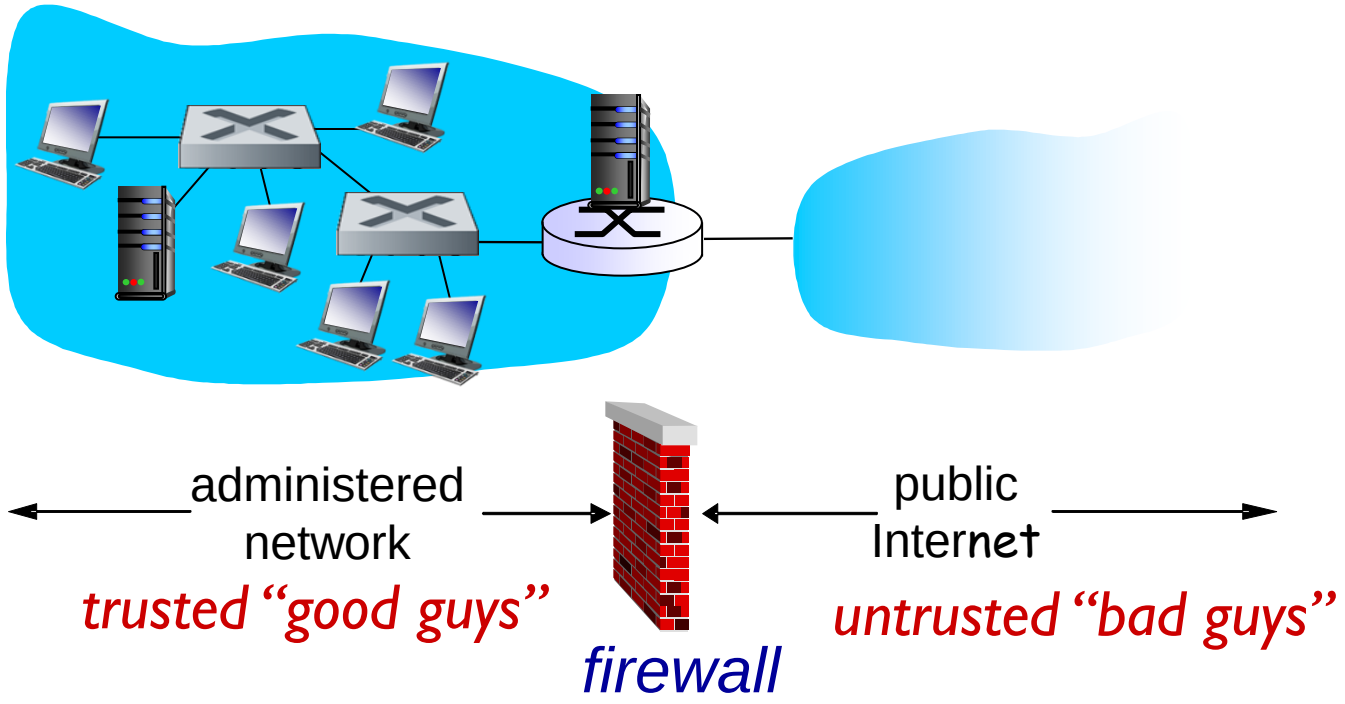
Reminder of lecture contents

- Lecture D3/D4
  - Security
  - Network management
- Tutorial
- Review Part C and Part D

Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others



Firewalls

Question: What are the three types of firewalls?

Firewalls

Question: What are the three types of firewalls?

Answer:

- stateless packet filters
- stateful packet filters
- application gateways

Firewalls: why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for "real" connections

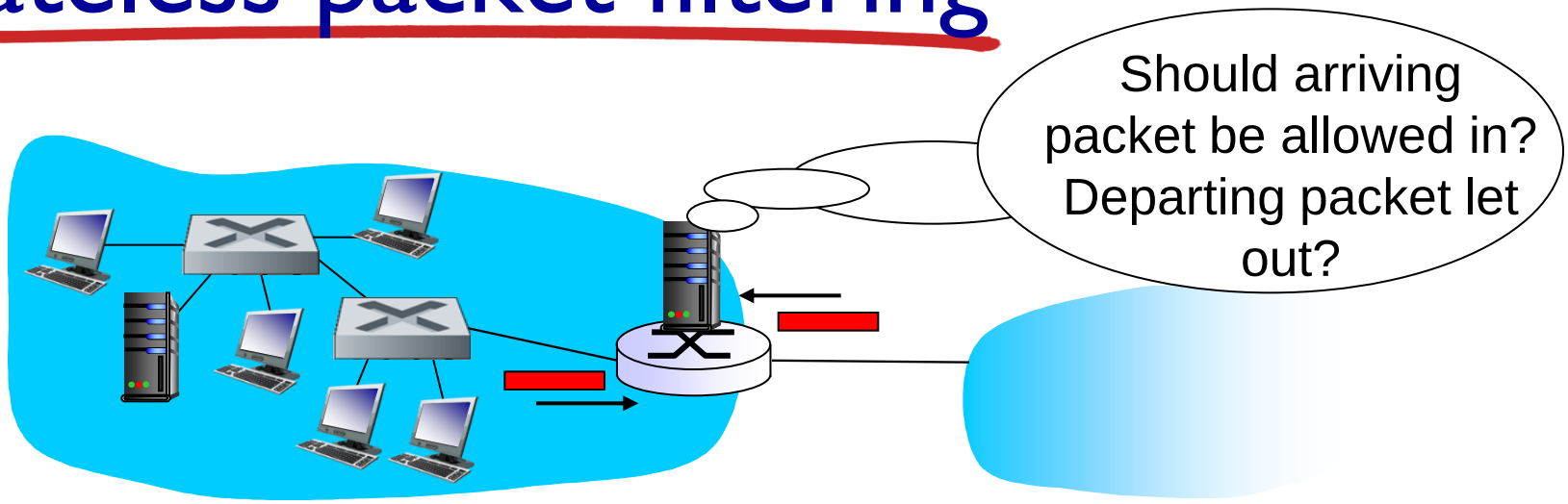
prevent illegal modification/access of internal data

- e.g., attacker replaces CIA's homepage with something else

allow only authorized access to inside network

- set of authenticated users/hosts

Stateless packet filtering



- internal network connected to Internet via *router firewall*
- router *filters packet-by-packet,* decision to forward/drop packet based on:
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Stateless packet filtering: example

- *example 1:* block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23
  - *result:* all incoming, outgoing UDP flows and telnet connections are blocked

Stateless packet filtering

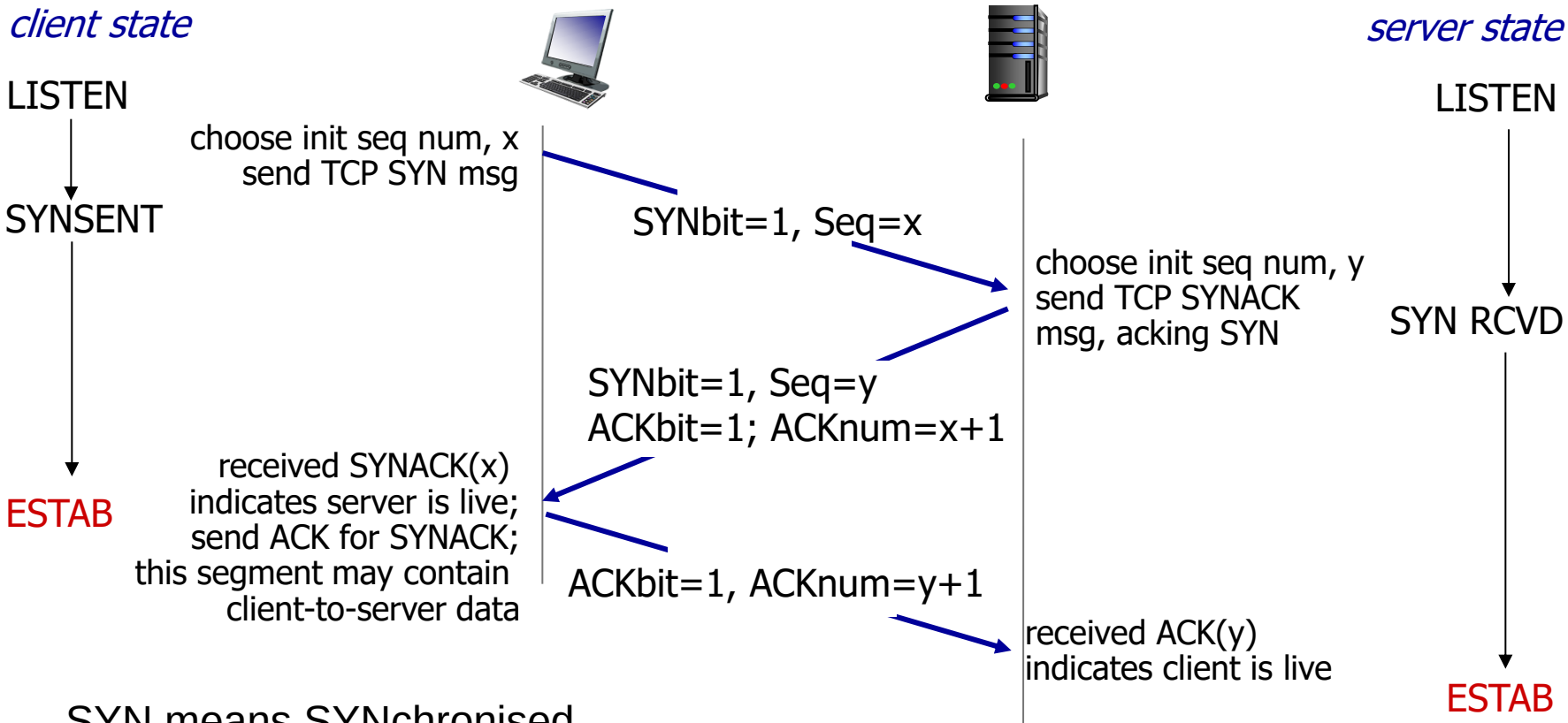
- **Question:** Assume that the filter blocks inbound TCP segments with ACK=0. What is the result?

Stateless packet filtering

- **Question:** Assume that the filter blocks inbound TCP segments with ACK=0. What is the result?
- **Answer:**

It prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

TCP 3-way handshake



SYN means SYNchronised

SYNbit = bit in TCP header saying this is SYN packet

ACKbit = bit in TCP header saying this is ACK packet

Stateless packet filtering: more examples

Policy	*Firewall Setting*
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (e.g. 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Access Control Lists

ACL: table of rules, applied top to bottom to incoming packets: (action, condition) pairs: looks like OpenFlow forwarding (Ch. 4)!

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

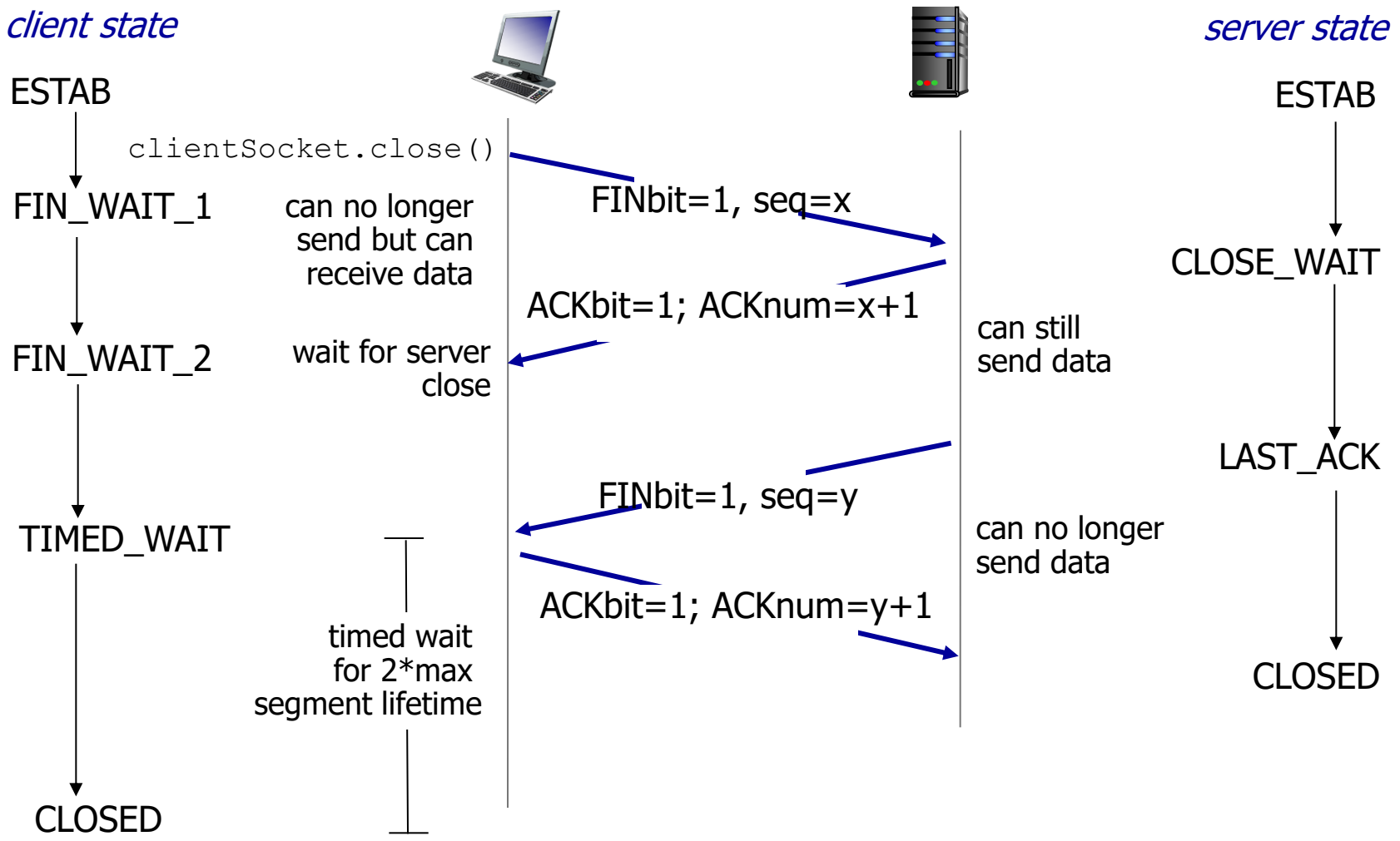
Stateful packet filtering

- *stateless packet filter:* heavy handed tool
  - admits packets that "make no sense," e.g., dest port = 80, ACK bit set, even though no TCP connection established:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter:* track status of every TCP connection
  - track connection setup (SYN), teardown (FIN): determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no longer admit packets

TCP: closing a connection



Stateful packet filtering

ACL augmented to indicate need to check connection state table before admitting packet

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Stateful vs stateless packet filtering

Question: What are the difference between stateful and stateless packet filtering?

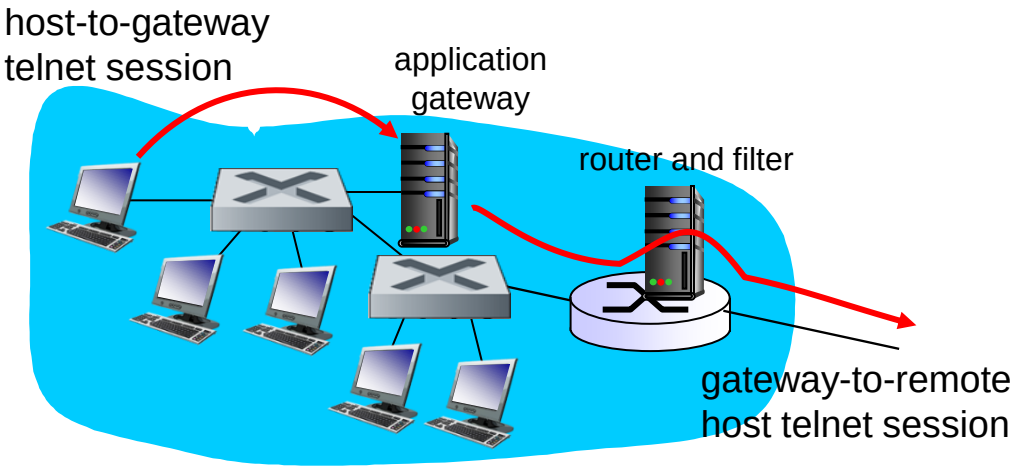
Stateful vs stateless packet filtering

Question: What are the difference between stateful and stateless packet filtering?

Answer:
Stateless, each packet independent/no memory
Stateful, remember each flow/connection

Application gateways

- filter packets on application data as well as on IP/TCP/UDP fields.
- *example:* allow select internal users to telnet outside



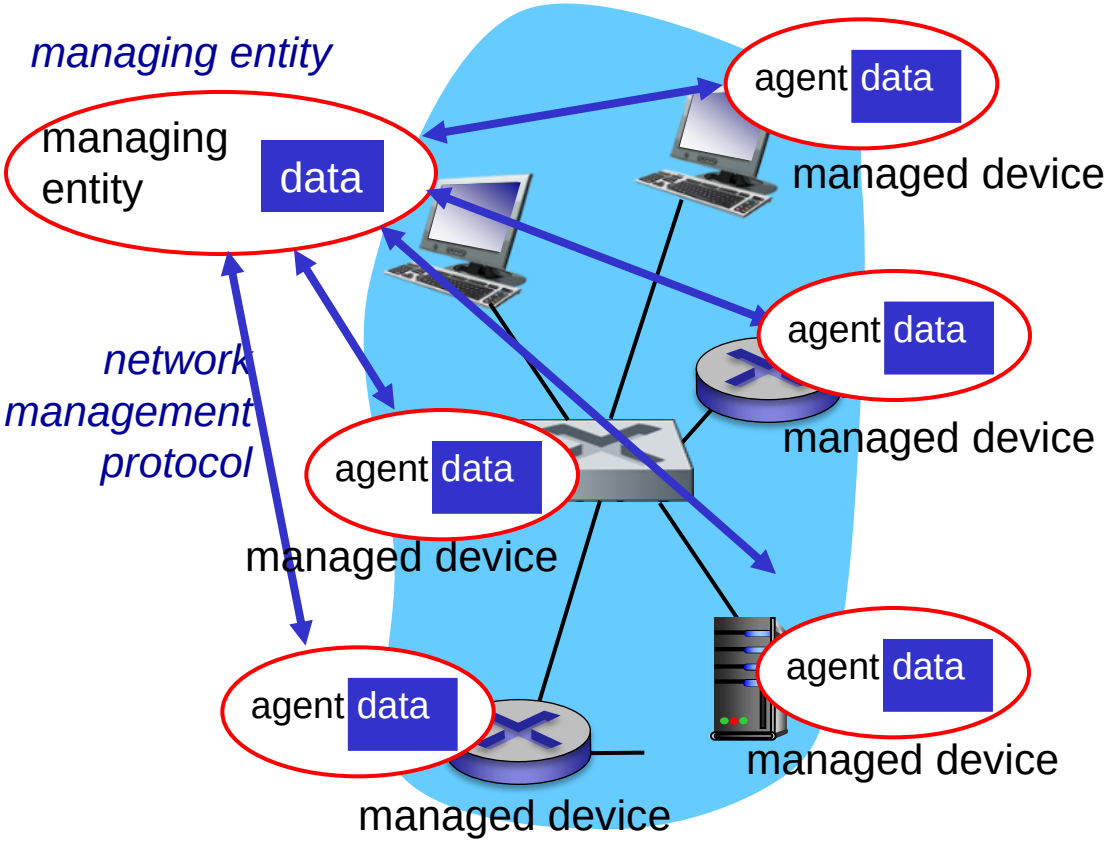
1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

What is network management?

- Autonomous systems (aka "network"): 100s or 1000s of interacting hardware/software components
- How do we know when something is wrong?
  - Too much data on the network?
  - Router or switch is broken?
  - Part of network is slow or unreliable?
- Can't wait for user reports:
  - May take too long to process.
  - Might not have right cause ("my computer is working slowly").
  - May not spot some things (data back up is broken).
- Need automatic way to report on large number of hosts, switches and routers

Infrastructure for network management

definitions:



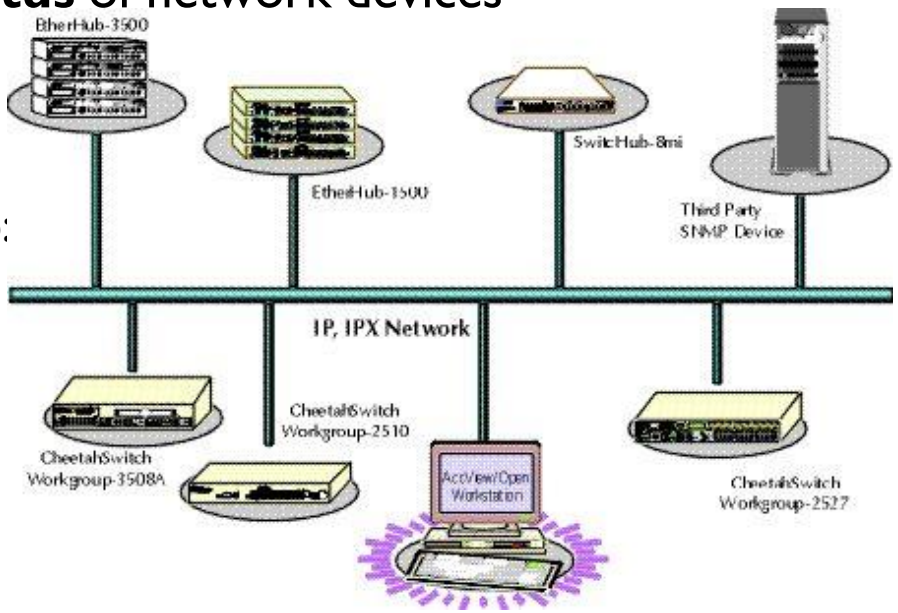
managed devices contain *managed objects* whose data is gathered into a *Management Information Base (MIB)*

Simple Network Management Protocol (SNMP)

- What is it?
  - A Protocol that Facilitates the exchange of management information
  - between network devices.

- Why was it developed?
  - To **control and monitor status** of network devices

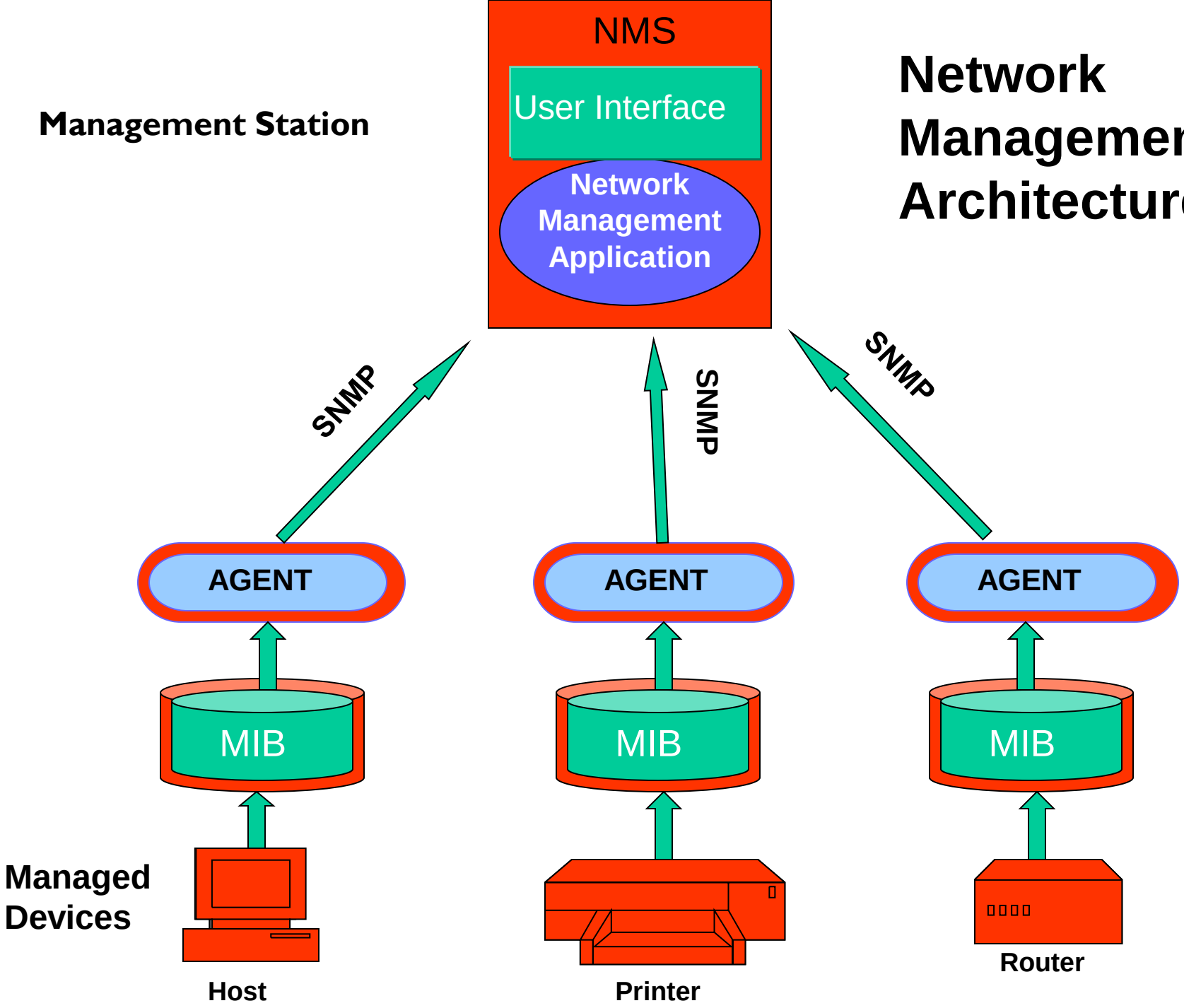
- How is it beneficial?
  - Enables network administrators to:
    - Manage network performance
    - Find and solve network problems
    - Plan for network growth



SNMP Basic Components

- Network Management station
  - Collects and stores management information, and makes this information available to NMS using SNMP
  - Could be a work station or PC
- Network Management System (NMS)
  - Executes applications that monitor and control managed devices
- Agent
  - A network-management software module that resides in a managed device
- Management Information Base (MIB)
  - Used by both the manager and the agent to store and exchange management information

Network Management Architecture



What have we learned?

- Operational security
  - Firewalls: Packet filtering and Access Control
- Network Management
  - Simple Network Management Protocol

Tutorial/Office Hour

- Please feel free to ask questions if you do not understand.
- Do not be shy.

Student questions: Back-off algorithm

- Initially, if a collision arises, a station increments its collision counter and waits either 0 or 1 slot times before trying again (each with probability = 1/2).
- If second collision occurs, the station increments its collision counter again and waits either {0, 1, 2, 3} slot times (with a uniform probability distribution).
- In general, after i collisions a station waits between 0 and (2^i - 1) slots each with probability of 1/(2^i)).
- To prevent excessive delays, if a packet has failed to be transmitted 10 or more times the maximum delay is limited to 1023 slots.
- On the sixteenth collision, a station is required to discard the packet and reset its collision counter.

2012 question 4

An IEEE 802.3 CSMA/CD network is designed with a maximum one-way propagation delay of 1ms and a bit-rate of 1Mbps.

ii) If the span of the network in part i) remains the same, such that the one-way propagation delay is still 1ms, calculate the minimum frame size if the transmission speed was increased to 1Gbps.

The RTT remains 2ms but the minimum frame size is very large. 1,000,000,000x 0.002 = 2,000,000 bits or 250,000 bytes.

2016/2017 paper A 1 c)

In Carrier Sense Multiple Access/Collision Avoidance, give the full name and briefly explain the role of ACK, RTS and CTS

[9 marks]

2016/2017 paper A 1 c)

- ACK = Acknowledgement is used to indicate that a message has been successfully received (1 mark expansion 2 marks definition)
- RTS = Request to Send is used by a sender to ask for permission to send a message and reserve space on the channel (1 mark expansion 2 marks definition)
- CTS = Clear to Send indicates the sender is allowed to send their message. (1 mark expansion 2 marks definition)

2017/2018 paper B 4 a)

- Explain how Carrier Sense Multiple Access (CSMA) works. [3 marks]

2017/2018 paper B 4 a)

- Explain how Carrier Sense Multiple Access (CSMA) works. **[3 marks]**

- Answer:

When a device wants to send a message, it first listens to the medium. [1 mark] If it is idle the message is sent immediately [1 mark], however, if it is busy the device continues to listen to the medium until it becomes idle for some time and then sends the message. [1 mark]

2017/2018 paper B 4 b)

- Define the term “collision window” and how it is used in CSMA/Collision Detection (CSMA/CD) networks. **[5 marks]**

2017/2018 paper B 4 b)

- Define the term "collision window" and how it is used in CSMA/Collision Detection (CSMA/CD) networks. **[5 marks]**

- Answer:

  [max 5 marks]
- The collision window is defined as the time that needed for a device to detect the collision at the further end of the network. [2 marks]

2017/2018 paper B 4 b)

- A device sends a message, which takes 1 propagation delay to reach the last device on the medium. [1 mark] This last device on the medium could then send a message just before the original message reaches it (i.e. just before 1 propagation delay). [1 mark]This new message would take an additional propagation delay to reach the original device[1 mark], which means that this device would not know that a collision had occurred until after 2 propagation delays. [1 mark]
- The collision window is approximately equal to twice the signal propagation time between the two most-distant stations on the network. [1 mark]

2017/2018 paper B 4 c)

- Calculate the size of this minimum frame, given a maximum one-way propagation delay of 2 ms and a bit-rate of 100Mbps. **(6 marks)**

2017/2018 paper B 4 c)

- Calculate the size of this minimum frame, given a maximum one-way propagation delay of 2 ms and a bit-rate of 100Mbps. **[6 marks]**
- If one-way propagation delay, Tp, is 2msec then the RTT is 4msec [2 marks].
- At a transmission rate of 10Mb/sec the transmitter must have enough bits to send to keep the transmission active for 4msec [2 marks].
- Therefore, in 4msec 400,000 bits (or 50,000 bytes) would be transmitted, hence the minimum frame size is 50K bytes [2 marks].
-

2018/2019 paper A 4 b)

- Explain the steps a user needs to perform to send data to a base station in IEEE 802.11 MAC Protocol: CSMA/CA using ACK, CTS and RTS (and saying what each of those is) and including what happens if an RTS is lost.

2018/2019 paper A 4 b)

- Before sending the user sends a "request-to-send" to reserve the channel (1 mark acronym 1 mark reserve the channel). If this is received the user gets a CTS ("clear to send") giving them the channel (1 mark acronym 1 mark concept of granting access). If the user does not hear any CTS they will not send but will "backoff" and send another RTS (2 marks backoff and resend RTS). If the user gets a CTS they send their data (1 mark). After sending the data the BS sends an ACKnowledgement (1 mark expansion 1 mark after data).