

# Internet Protocols EBU5403

## Security + Network Management

Michael Chai (michael.chai@qmul.ac.uk)

Richard Clegg (r.clegg@qmul.ac.uk)

Adnan Kiani (adnankhal@gmail.com)

	Week 1	Week 2	Week 3	Week 4
Telecom	Adnan Kiani	Michael Chai		Adnan Kiani
E-Commerce	Richard Clegg	Michael Chai	Richard Clegg	

# Structure of course

- Week 1 (25<sup>th</sup>-29<sup>th</sup> September)
  - Introduction to IP Networks
  - The Transport layer (part I)
- Week 2 (16<sup>th</sup>-21<sup>st</sup> October)
  - The Transport layer (part II)
  - The Network layer (part I)
  - Class test (open book exam in class)
- Week 3 (20<sup>th</sup>-24<sup>th</sup> November)
  - The Network layer (part II)
  - The Data link layer (part I)
  - Router lab tutorial (assessed labwork after this week)
- Week 4 (18<sup>th</sup>-22<sup>nd</sup> December)
  - The Data link layer (part II)
  - **Security and network management**
  - Class test

# Security and Network Management: outline

- *Securing wireless LANs*
- Operational security: firewalls and IDS
- Network Management

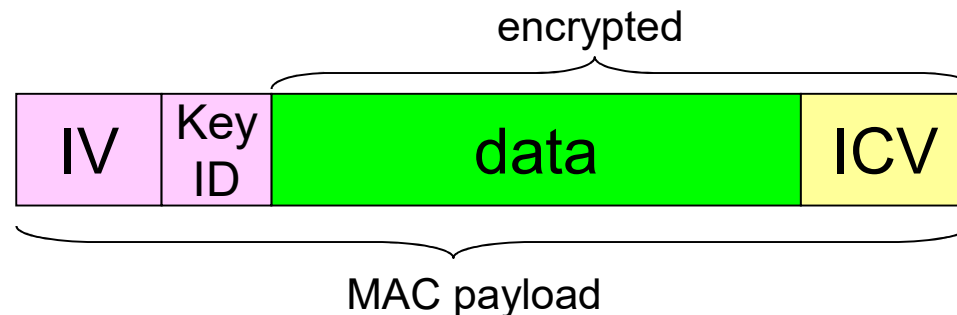
# WEP design goals



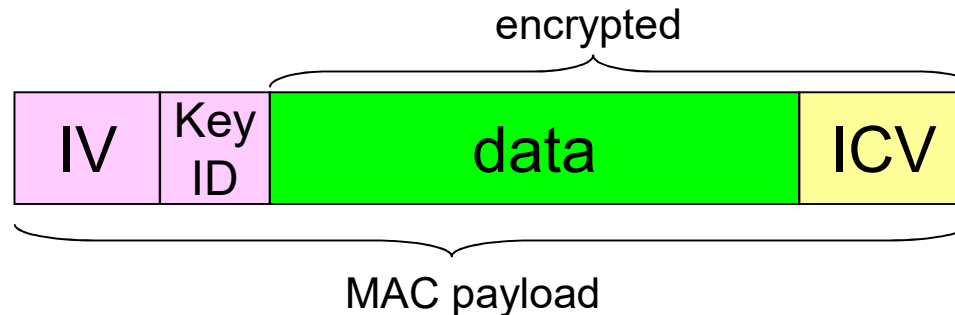
- symmetric key crypto
  - confidentiality
  - end host authorization
  - data integrity
- self-synchronizing: each packet separately encrypted
  - given encrypted packet and key, can decrypt; can continue to decrypt packets when preceding packet was lost (unlike Cipher Block Chaining (CBC) in block ciphers)
- Efficient
  - implementable in hardware or software

# WEP encryption

- sender calculates Integrity Check Value (ICV, four-byte hash/CRC over data)
- each side has 104-bit shared key
- sender creates 24-bit initialization vector (IV), appends to key: gives 128-bit key
- sender also appends keyID (in 8-bit field)
- 128-bit key inputted into pseudo random number generator to get keystream
- data in frame + ICV is encrypted with RC4:
  - bytes of keystream are XORed with bytes of data & ICV
  - IV & keyID are appended to encrypted data to create payload
  - payload inserted into 802.11 frame



# WEP decryption

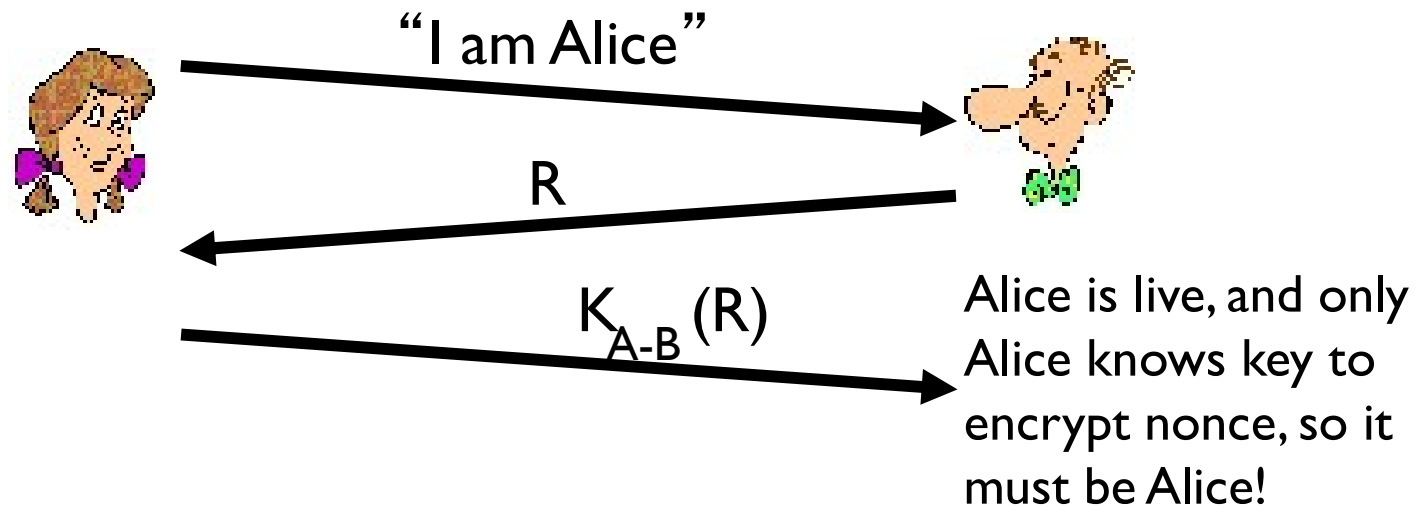


- receiver extracts IV
- inputs IV, shared secret key into pseudo random generator, gets keystream
- XORs keystream with encrypted data to decrypt data + ICV
- verifies integrity of data with ICV
  - note: message integrity approach used here is different from MAC (message authentication code) and signatures (using PKI).

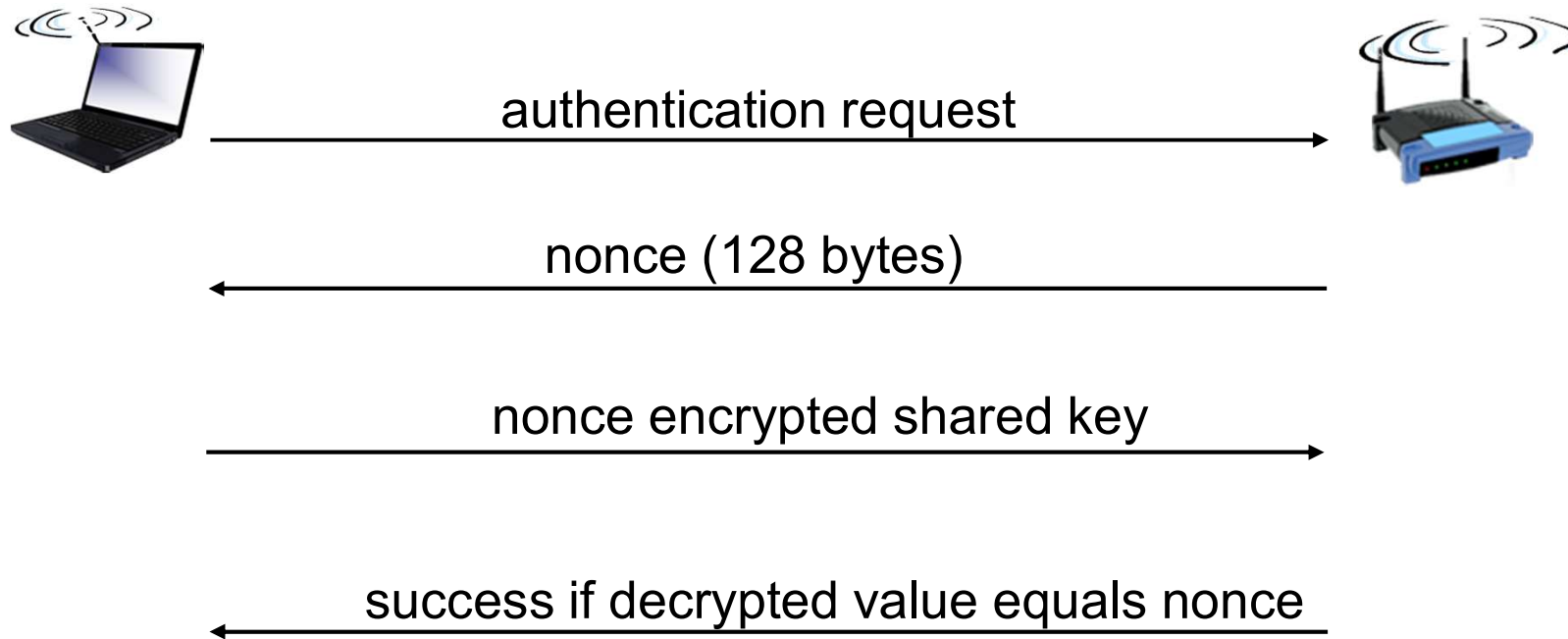
# End-point authentication w/ nonce

**Nonce:** number (R) used only *once* –*in-a-lifetime*

**How to prove Alice “live”:** Bob sends Alice **nonce**, R. Alice must return R, encrypted with shared secret key



# WEP authentication



## *Notes:*

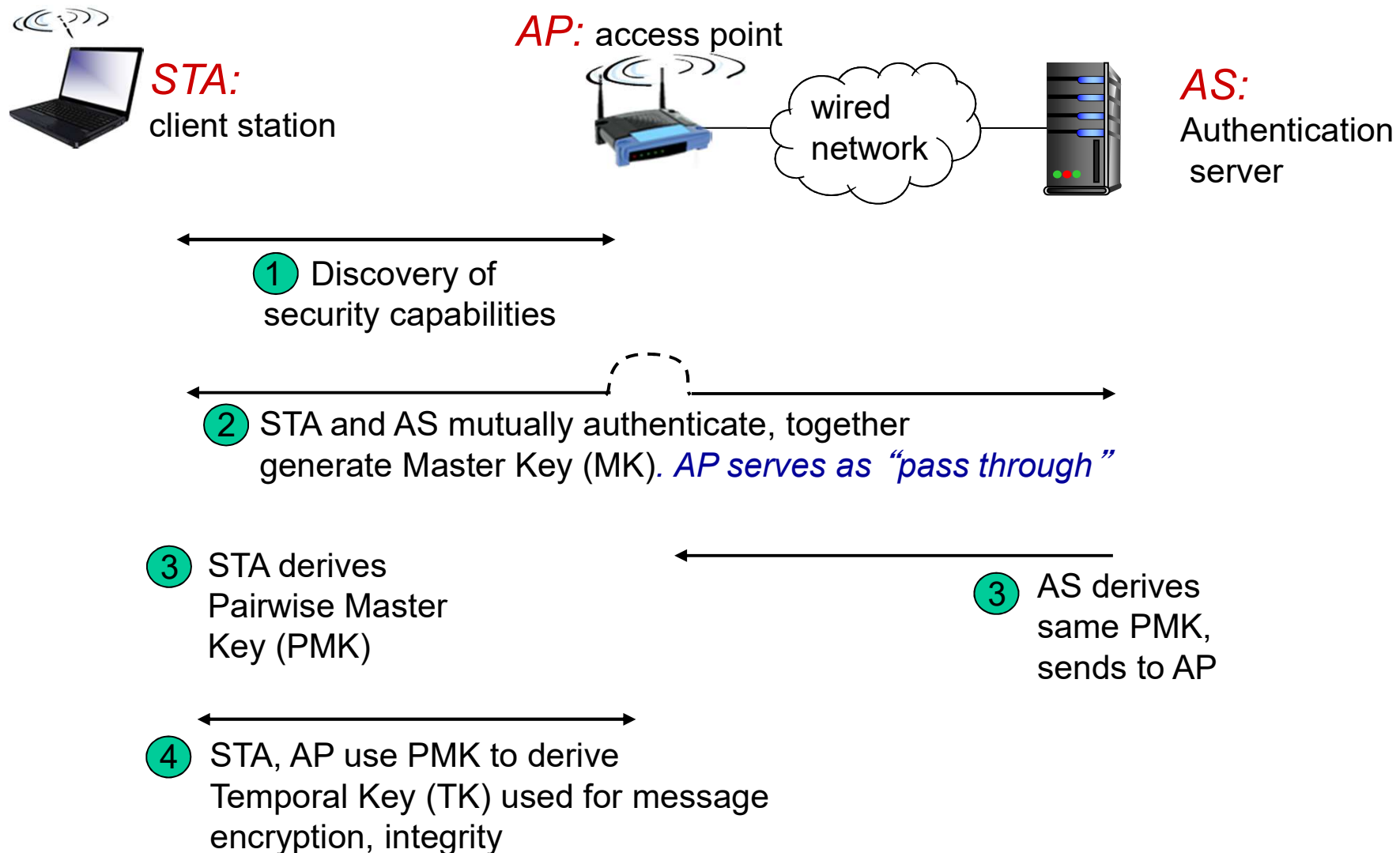
- not all APs do it, even if WEP is being used
- AP indicates if authentication is necessary in beacon frame
- done before association



# 802.11i: improved security

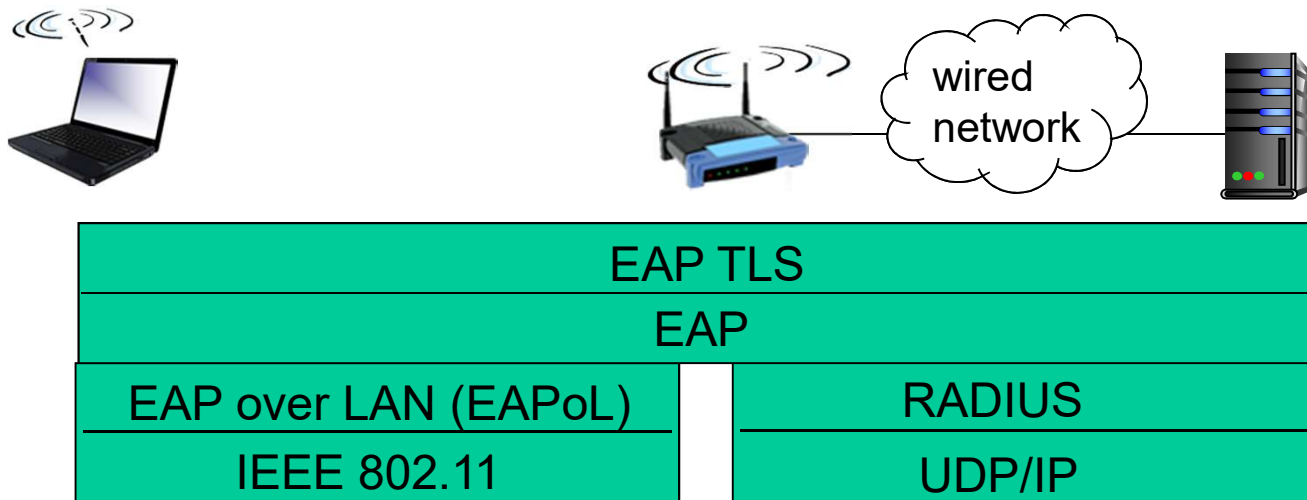
- numerous (stronger) forms of encryption possible
- provides key distribution
- uses authentication server separate from access point

# 802.11i: four phases of operation



# EAP: extensible authentication protocol

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate “links”
  - mobile-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)



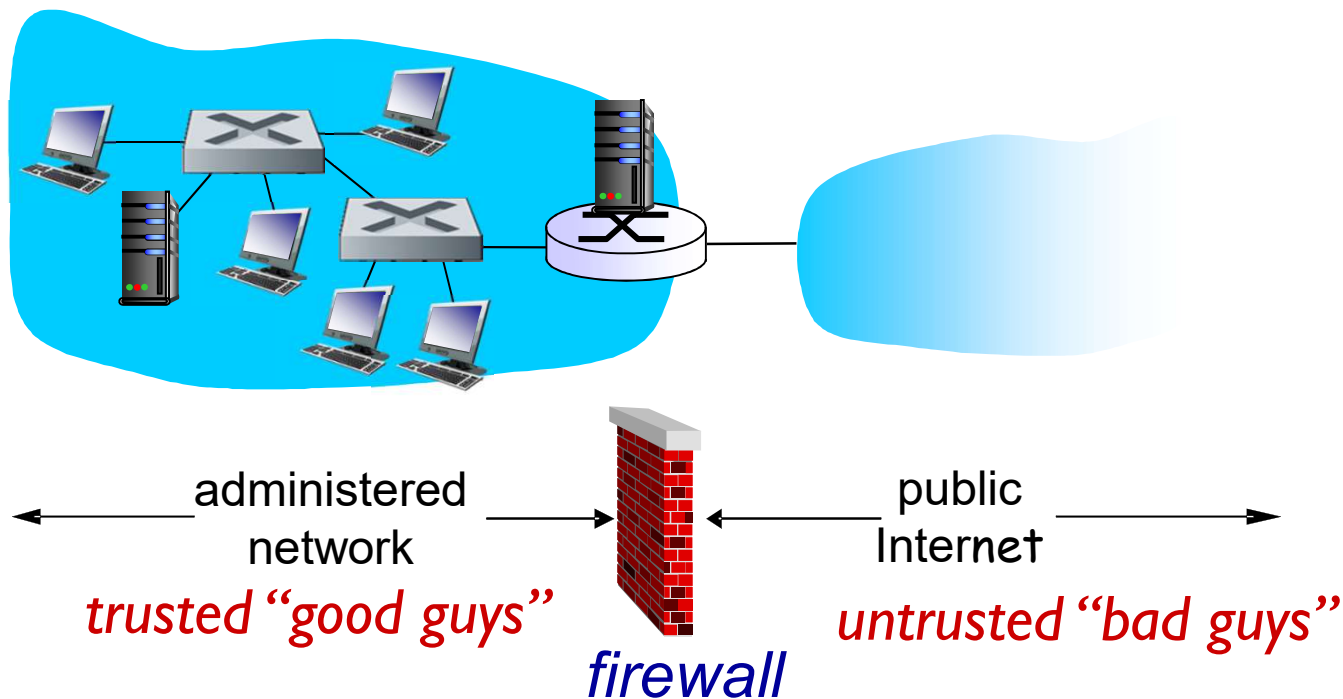
# Security and Network Management: outline

- *Securing wireless LANs*
- **Operational security: firewalls and IDS**
- Network Management

# Firewalls

## *firewall*

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



# 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

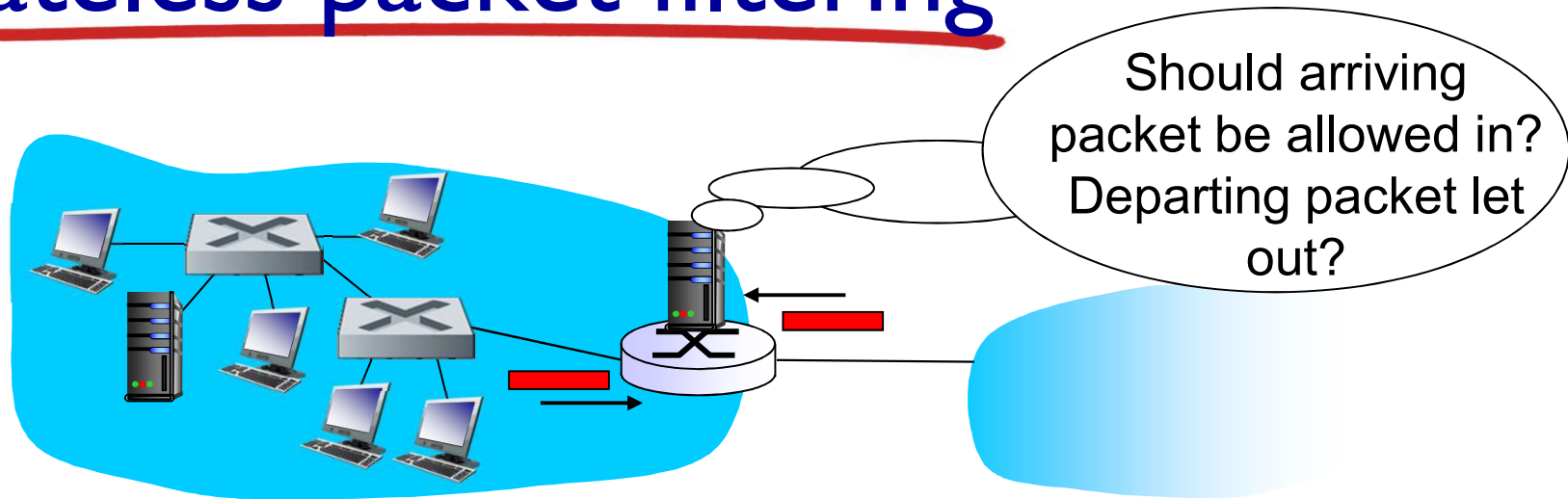
allow only authorized access to inside network

- set of authenticated users/hosts

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

# 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
- *example 2:* block inbound TCP segments with ACK=0.
  - *result:* prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.



# Stateless packet filtering: more examples

<i>Policy</i>	<i>Firewall Setting</i>
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

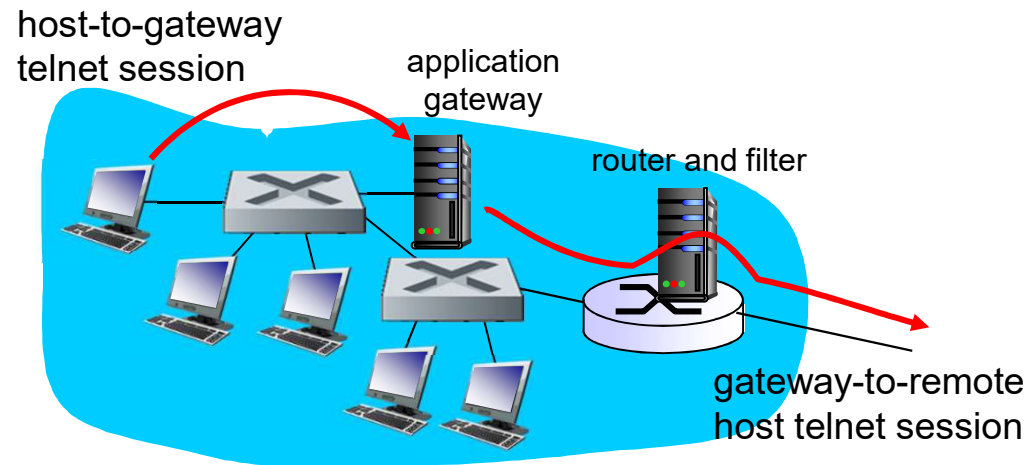
# Stateful packet filtering

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	

# 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.

# Limitations of firewalls, gateways

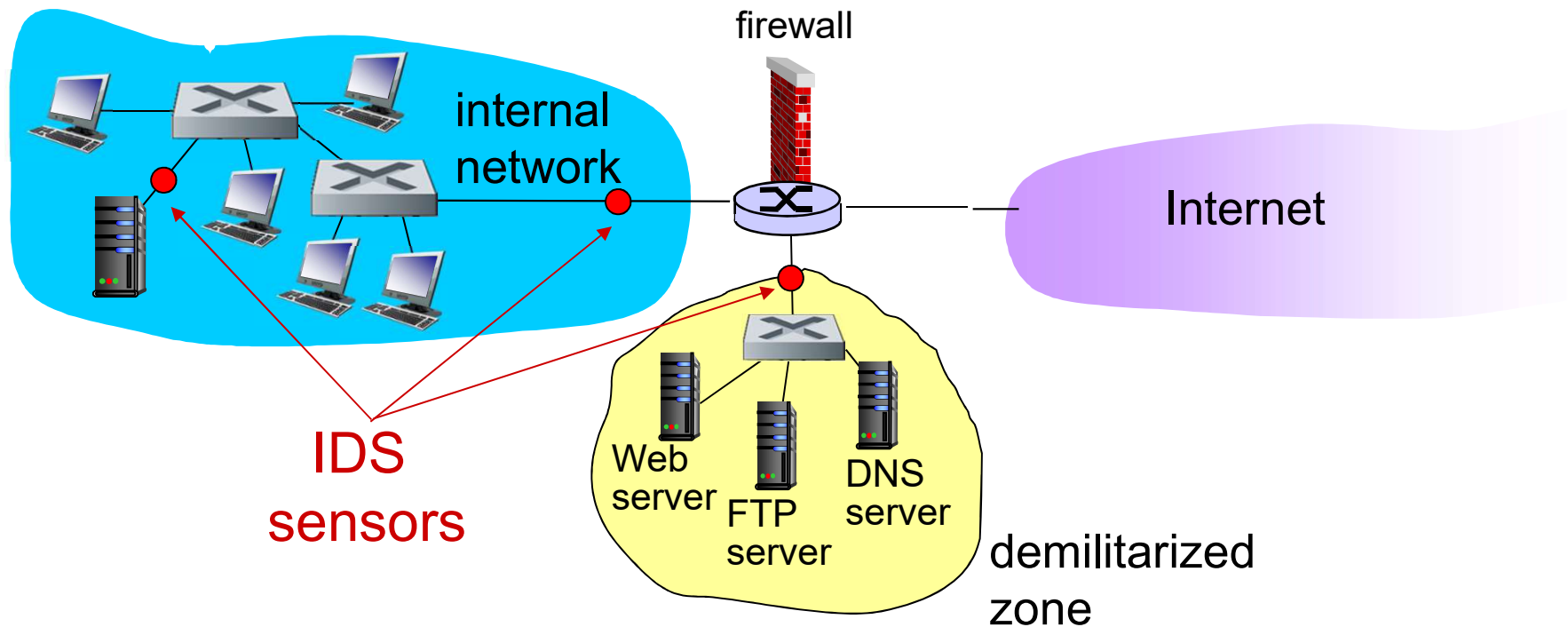
- *IP spoofing*: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- filters often use all or nothing policy for UDP
- *tradeoff*: degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks

# Intrusion detection systems

- packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection*: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - *examine correlation* among multiple packets
    - port scanning
    - network mapping
    - DoS attack

# Intrusion detection systems

multiple IDSs: different types of checking at different locations





# Security and Network Management: outline

- *Securing wireless LANs*
- Operational security: firewalls and IDS
- **Network Management**

# What is network management?

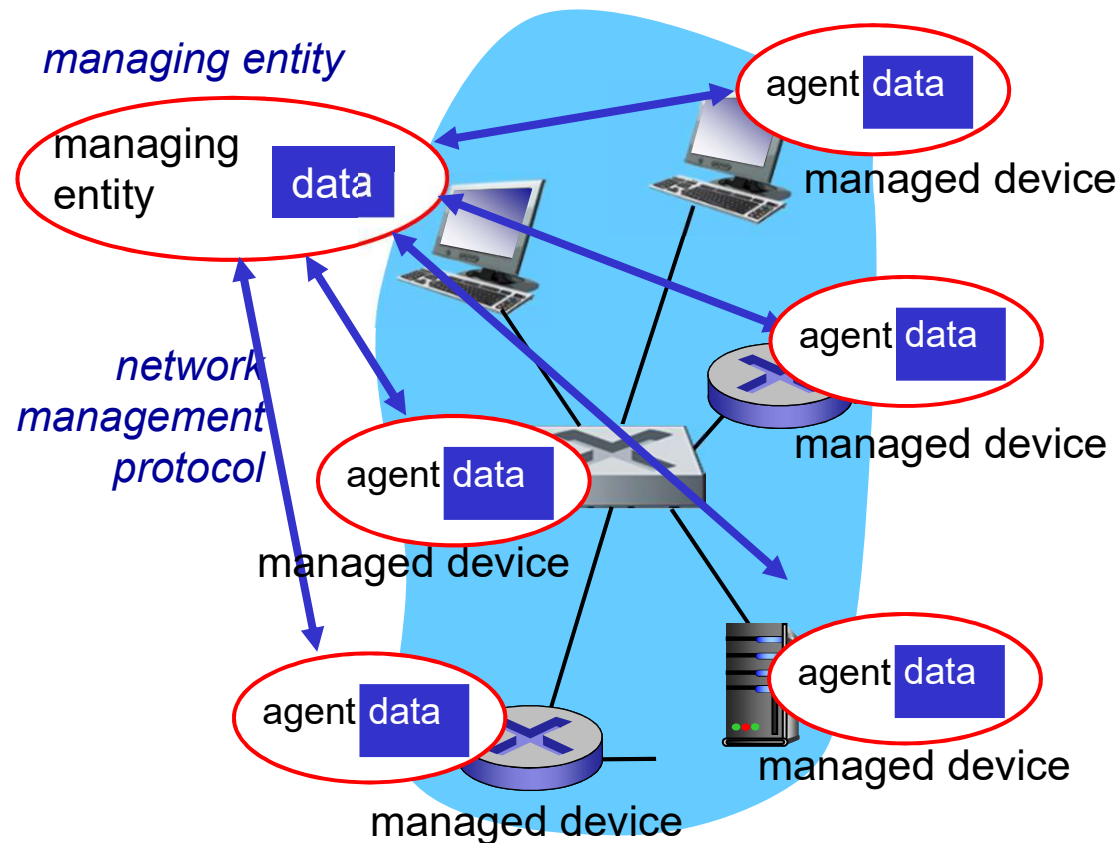
- **Autonomous systems (aka “network”)**: 100s or 1000s of interacting hardware/software components
- Other complex systems requiring monitoring, control:
  - jet airplane
  - nuclear power plant
  - others?



"**Network management** includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost."

# Infrastructure for network management

definitions:



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

# Network Management standards

## OSI CMIP

- Common Management Information Protocol
- designed 1980's: *the* unifying net management standard
- too slowly standardized

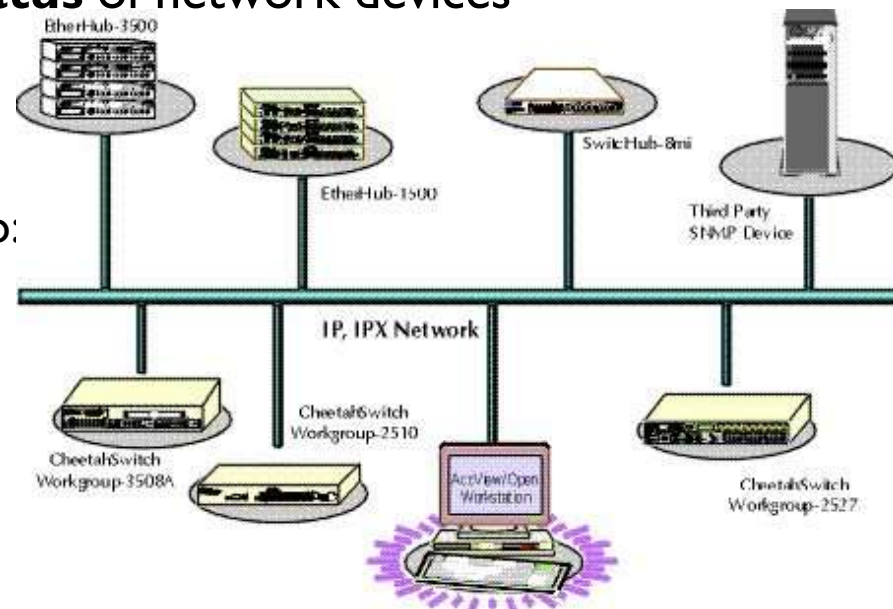
## SNMP: Simple Network Management Protocol

- Internet roots (SGMP)
- started simple
- deployed, adopted rapidly
- growth: size, complexity
- currently: SNMP V3
- *de facto* network management standard

# Simple Network Management Protocol (SNMP)

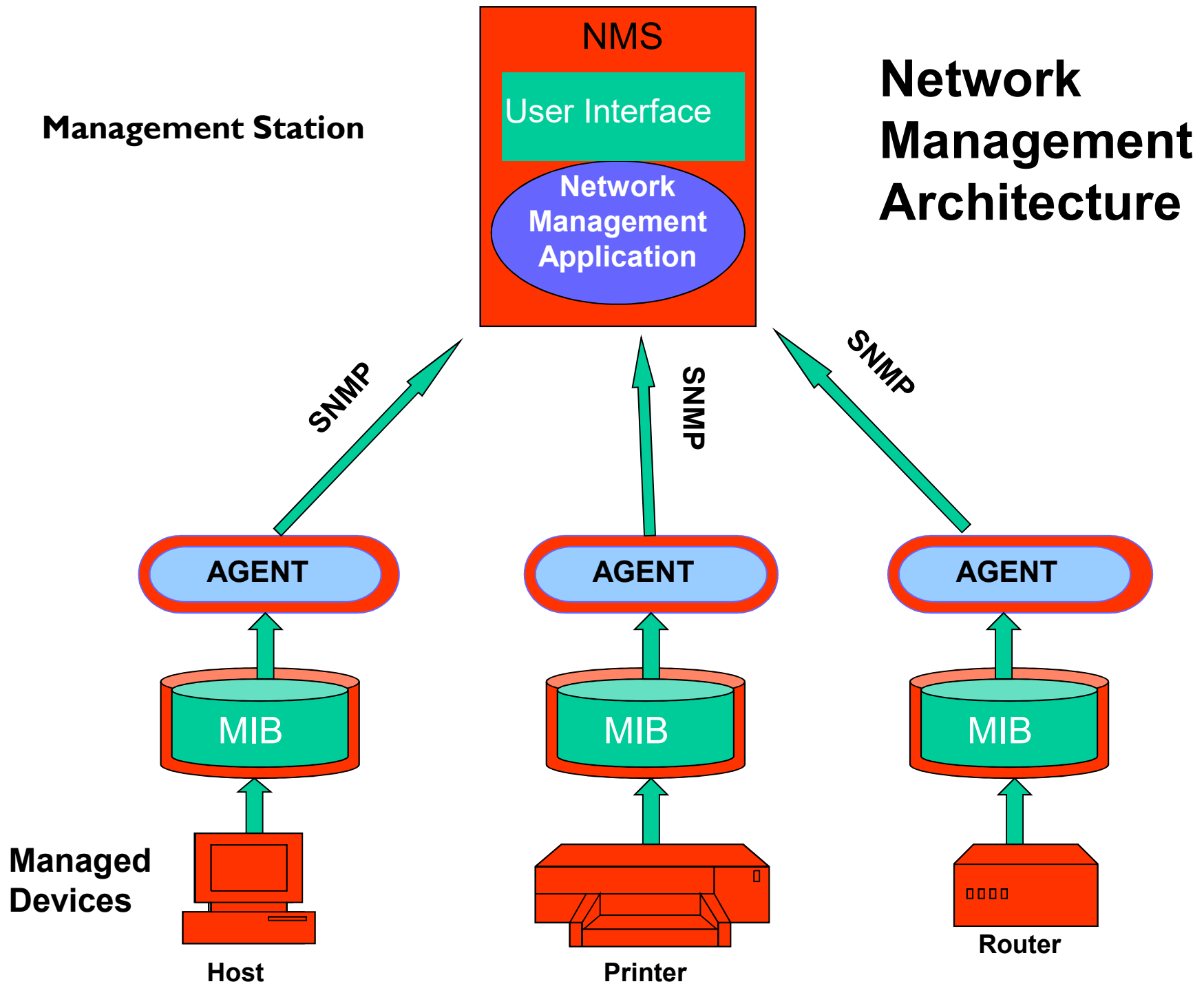
---

- 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



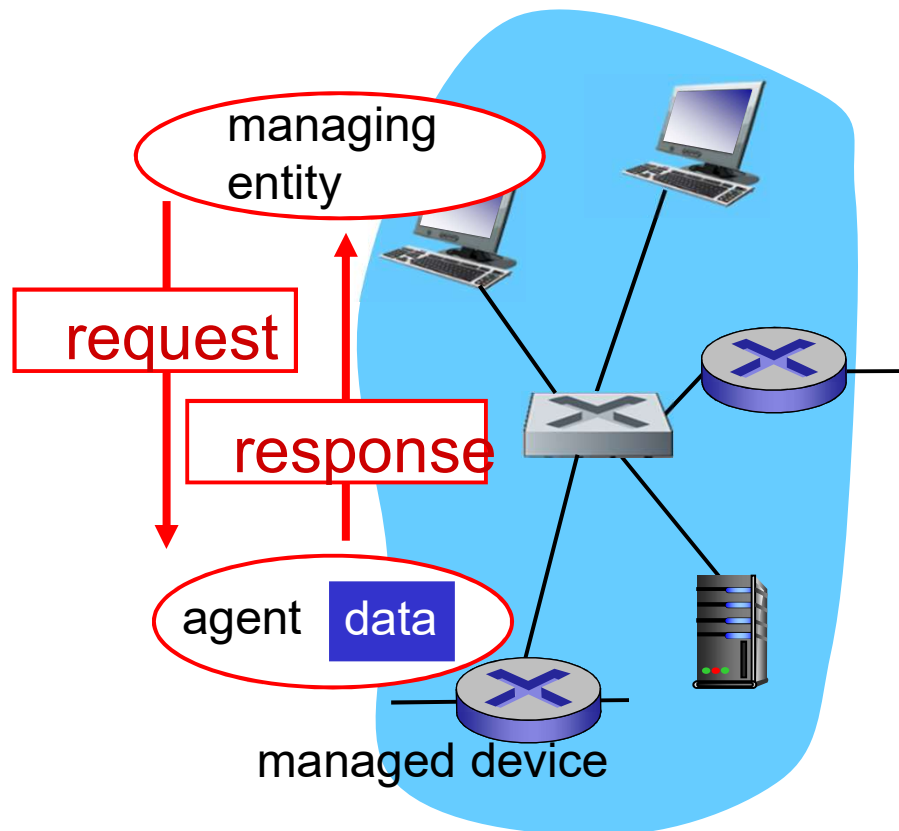
# SNMP Basic Components

- **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

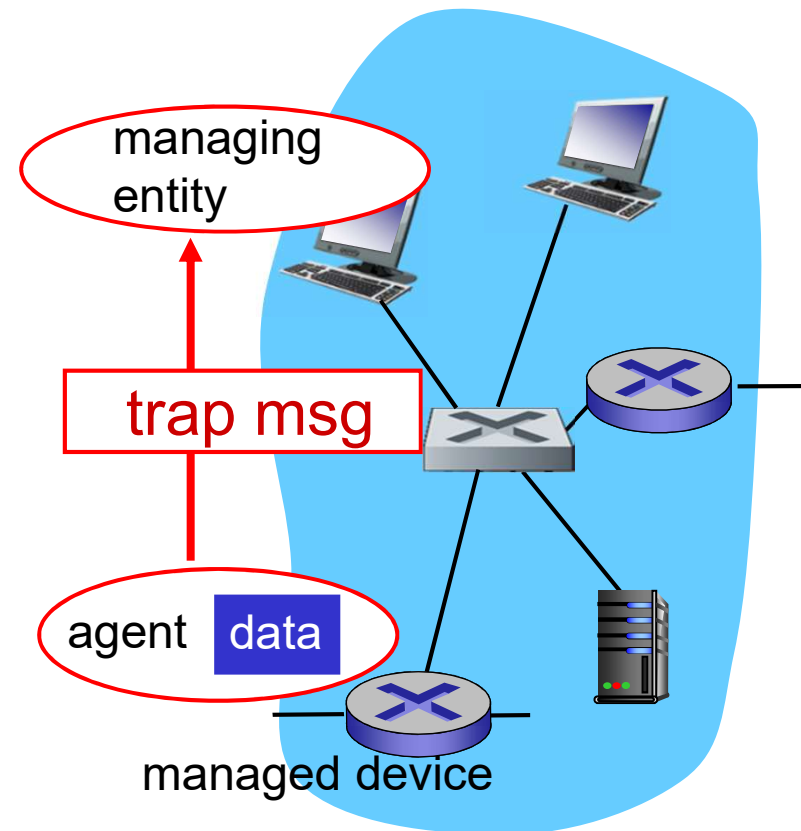


# SNMP protocol

Two ways to convey MIB info, commands:



request/response mode



trap mode



# SNMP protocol: message types

<u>Message type</u>	<u>Function</u>
GetRequest GetNextRequest GetBulkRequest	manager-to-agent: “get me data” (data instance, next data in list, block of data)
InformRequest	manager-to-manager: here’s MIB value
SetRequest	manager-to-agent: set MIB value
Response	Agent-to-manager: value, response to Request
Trap	Agent-to-manager: inform manager of exceptional event

# What have we learned?

- Securing wireless LANs: WEP encryption and decryption
- Operational security
  - Firewalls: Packet filtering and Access Control
  - IDS: Deep packet inspection and exam correlation
- Network Management
  - Simple Network Management Protocol