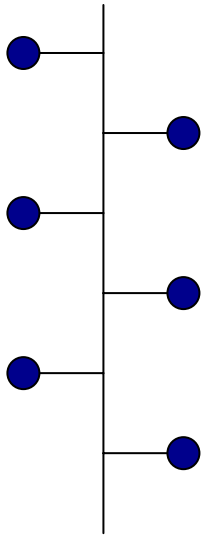
Unit 25
Network Management
Network Security



Network Management

Acknowledgements – slides coming from:

- Based to big extent on slides from the books of WIliam Stallings and Kurose/Ross.

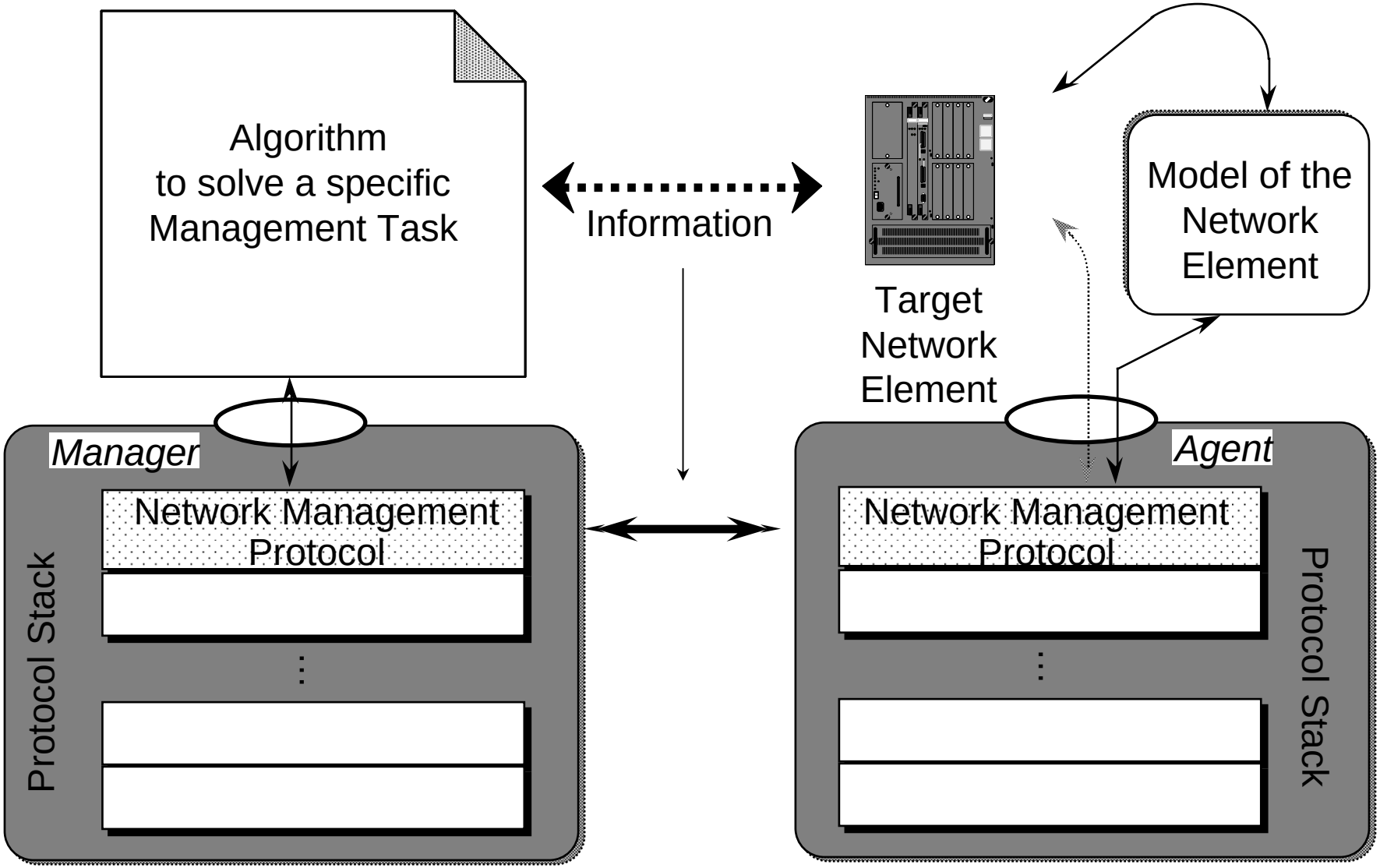
Network Management

- Networks are becoming indispensable
- More complexity makes failure more likely
- Require automatic network management tools
- Standards required to allow multi-vendor networks
- Covering:
  - services
  - protocols
  - data Structures.

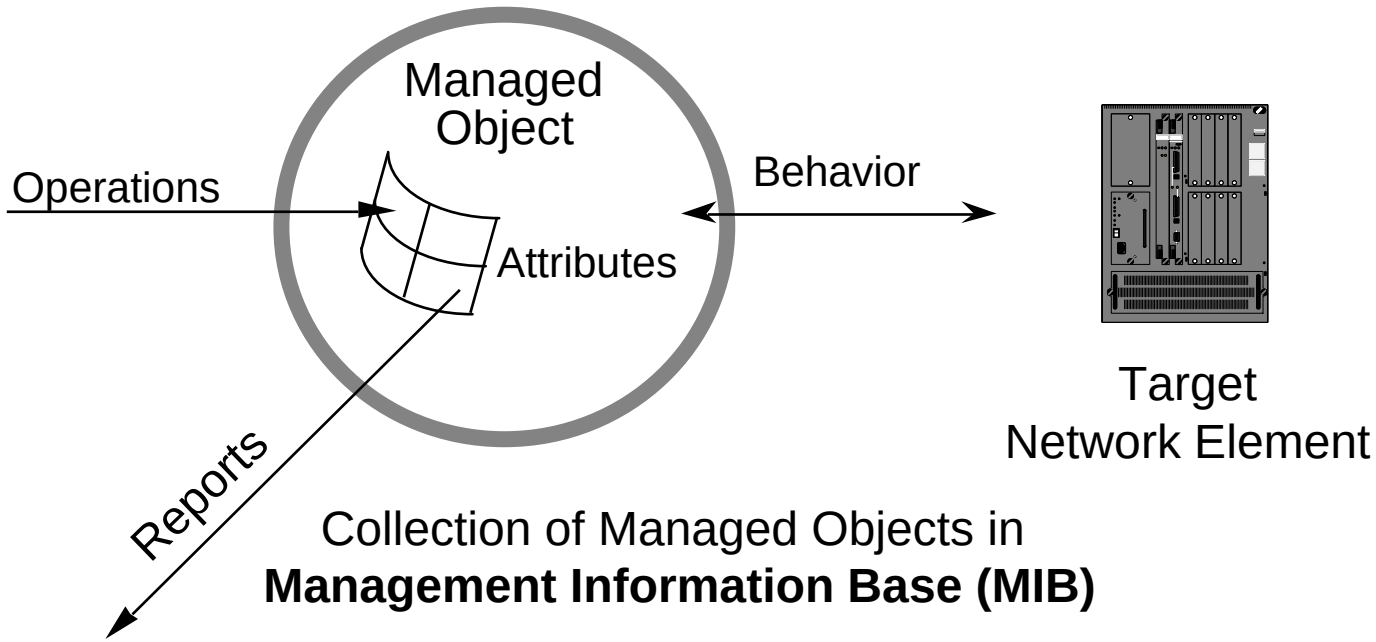
Network Management Systems

- Collection of tools for network management
- Operator interface
- Powerful, user friendly command set
- Minimal amount of separate equipment
  - i.e. use existing equipment
- View entire network as unified architecture
- Active elements provide regular feedback

Network Management: Architecture Overview



Network Management: Managed Objects

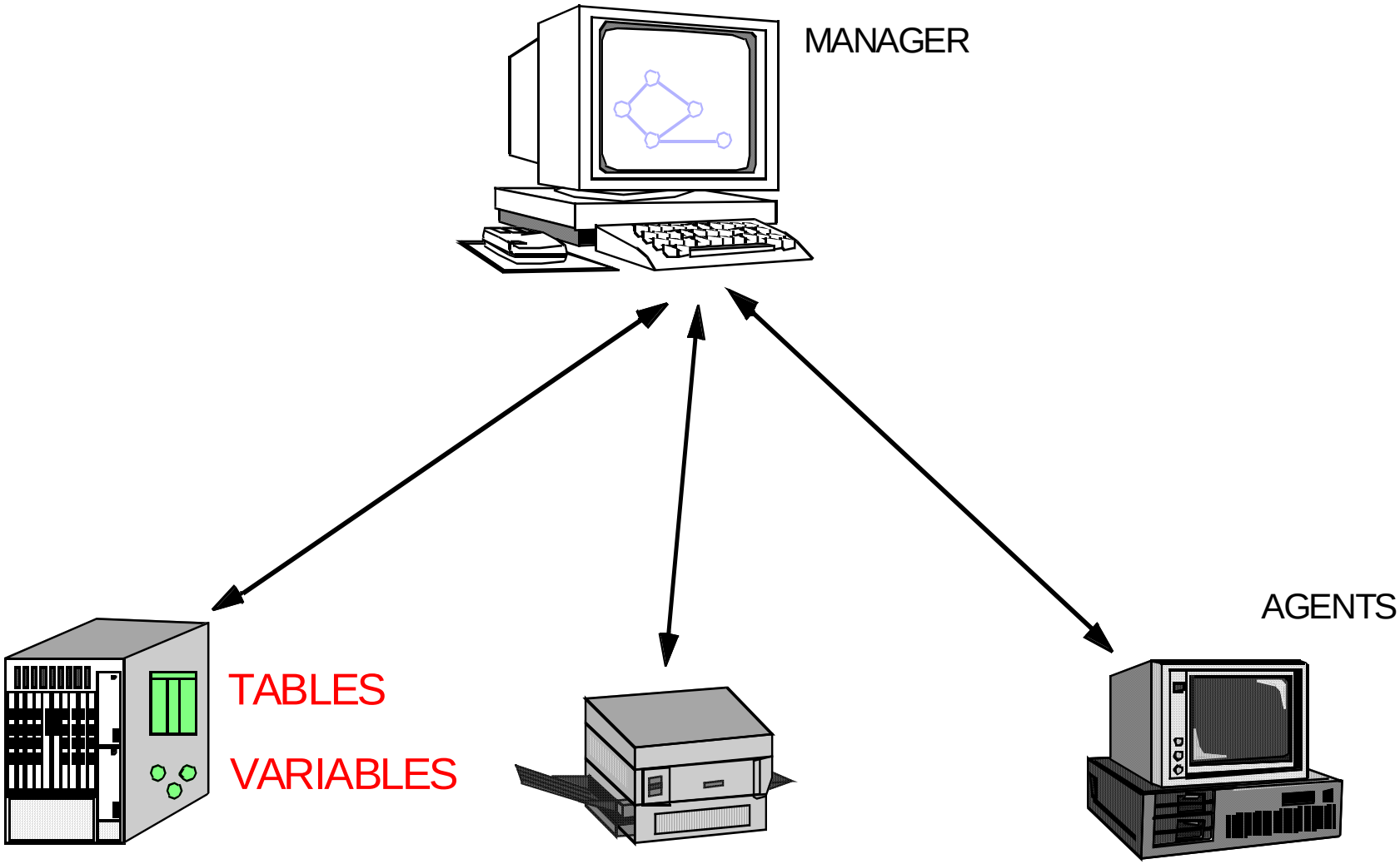


- *Managed Objects* logically represent certain properties of network elements for the purpose of network management
- Managed Objects are organized in a conceptual *Management Information Base (MIB)* with the MIB as a whole representing the management capabilities of a specific component

SNMP: Internet Network Management

- Management is done from the management station *(manager)*
- It communicates via the *SNMP protocol* with *agents*
- Information from a node not being able to run an agent can be retrieved from a *proxy agent* running on another node
- The biggest part of SNMP describes the kind of information that a specific type of agent provides and the format of it
- Each managed node holds the information that can be retrieved by SNMP in a special information base called MIB (Management Information Base) (RFC 1213)
- The MIB uses ASN.1 to describe the managed information as objects. The ASN.1 “OBJECT IDENTIFIER” is used to uniquely identify every object

PRINCIPLE OPERATION



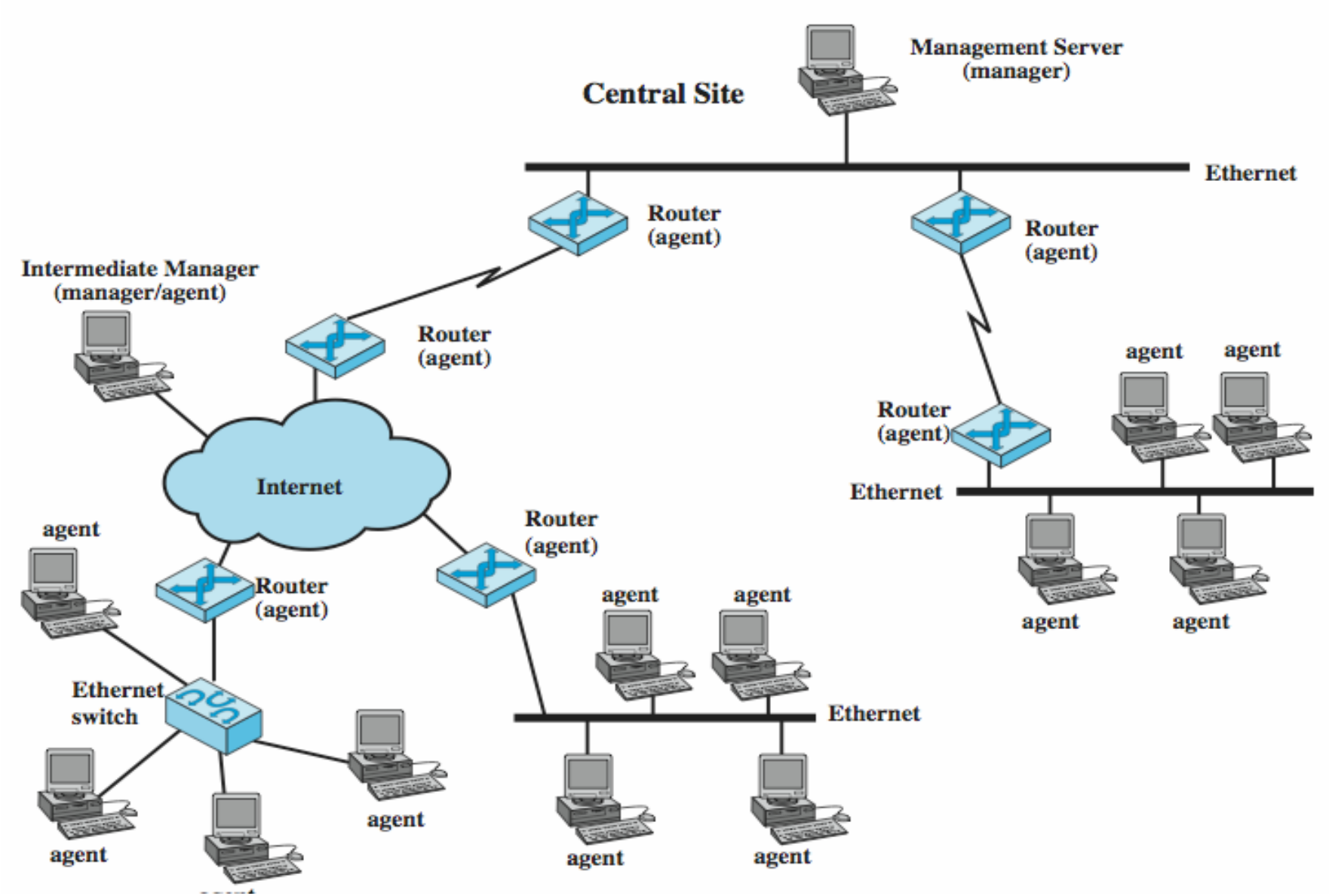
Management Station

- stand alone system or part of shared system
- interface for human network manager
- set of management applications
  - data analysis
  - fault recovery
- interface to monitor and control network
- translate manager's requirements into monitoring and control of remote elements
- data base of network management information extracted from managed entities

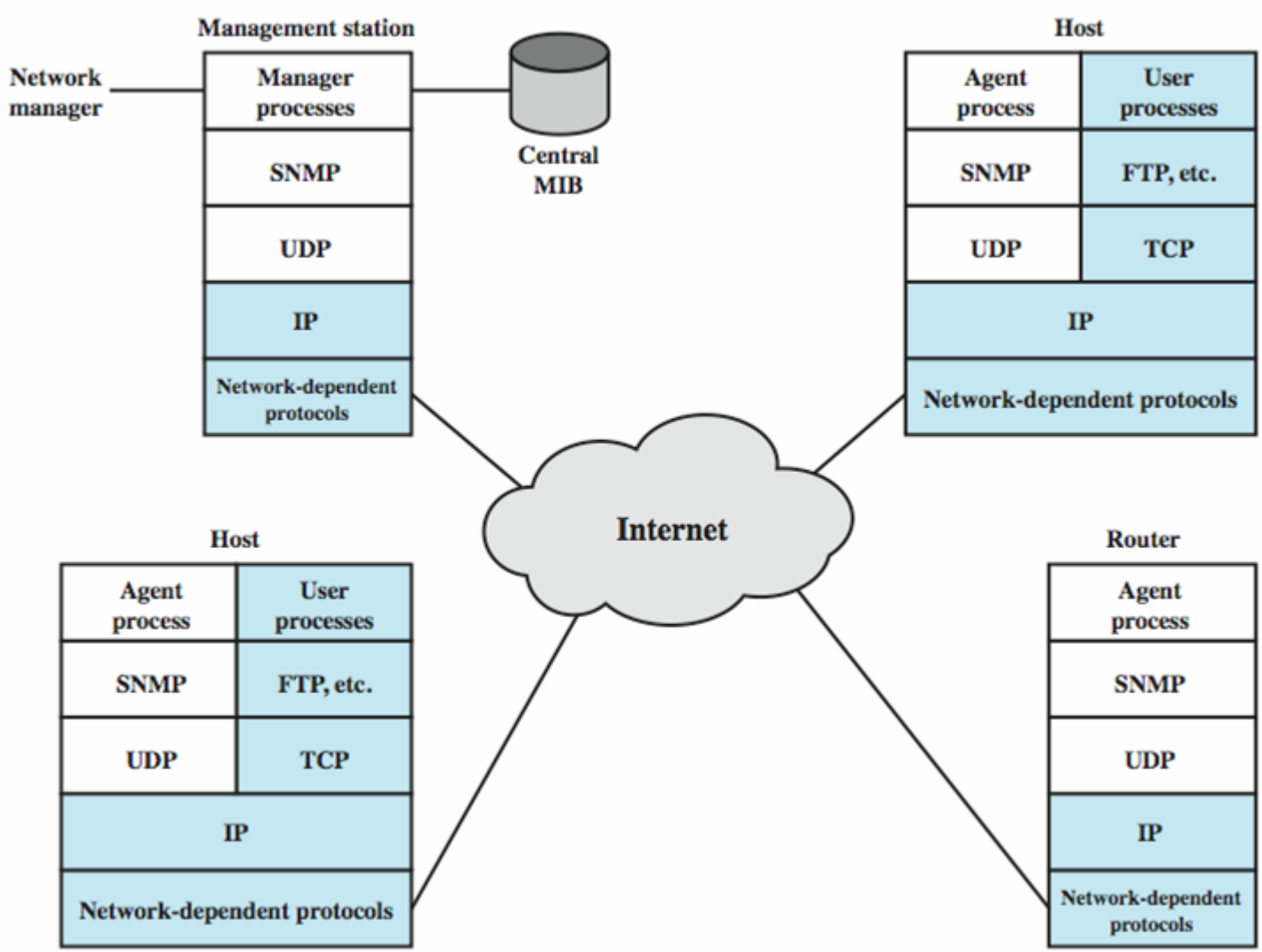
Management Agent

- equip key platforms with agent software
  - e.g. hosts, bridges, hubs, routers
- allows their management by management station
- respond to requests for information
- respond to requests for action
- asynchronously supply unsolicited information

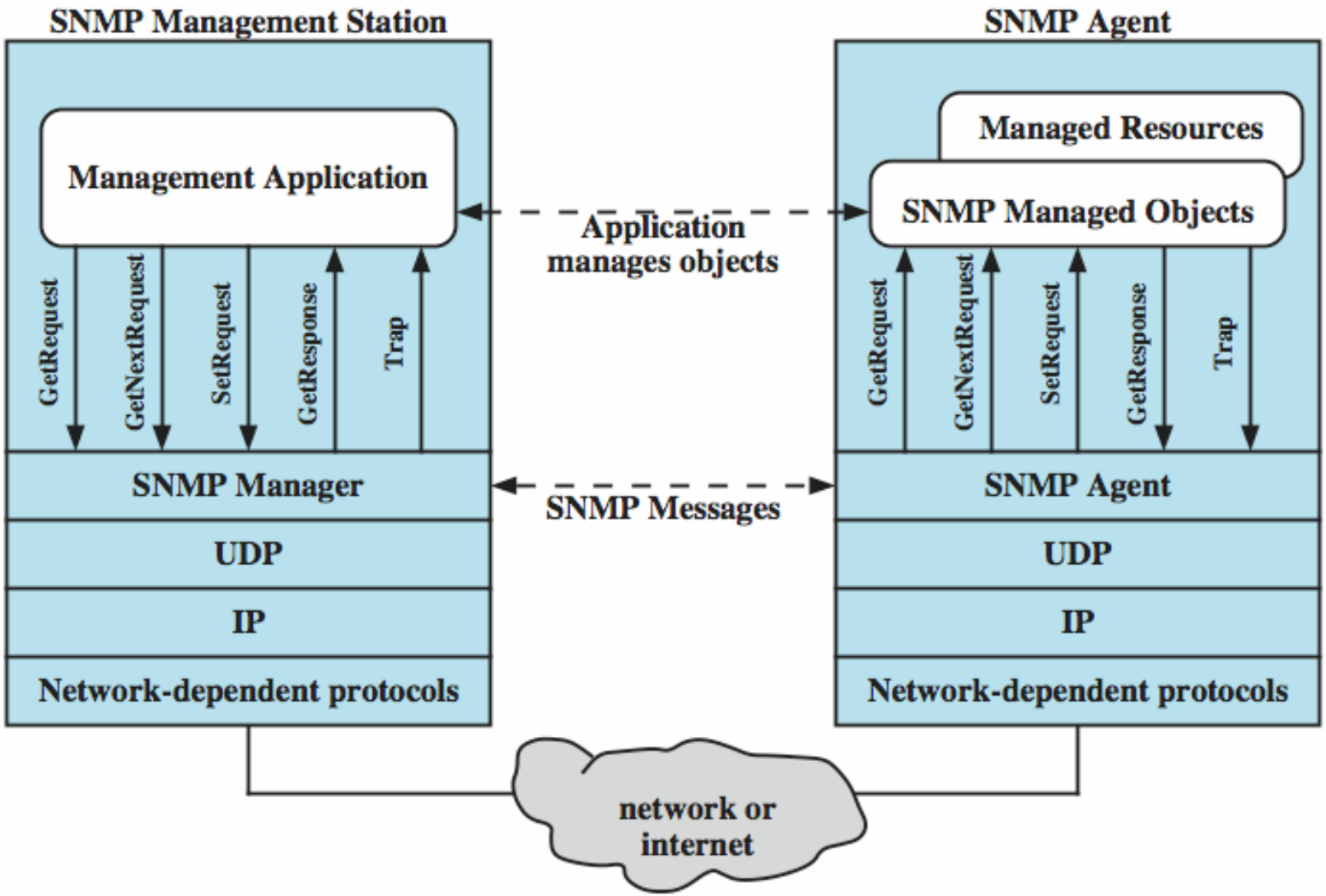
Distributed Network Management Example



SNMP Architecture

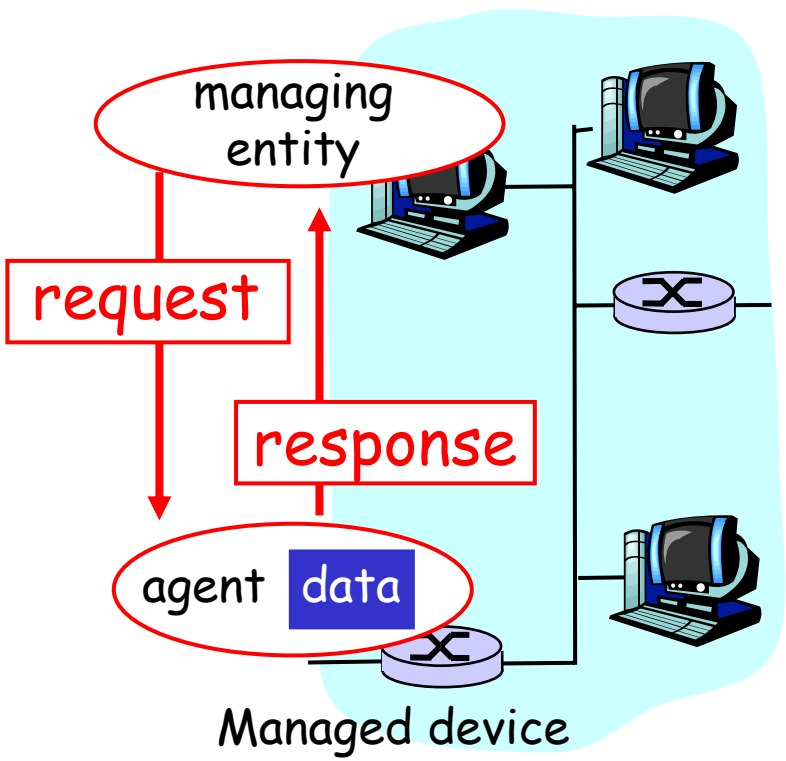


SNMP Architecture

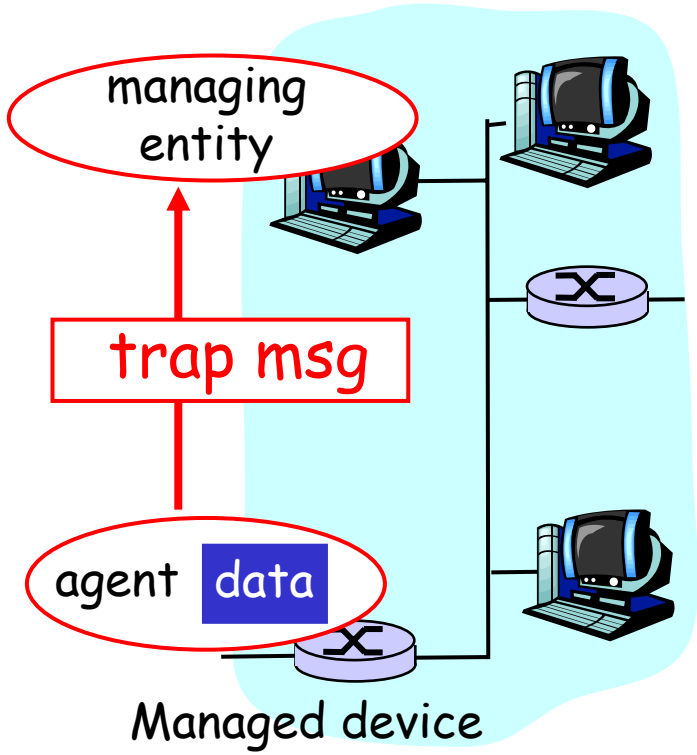


SNMP protocol

Two ways to convey MIB info, commands:



request/response mode



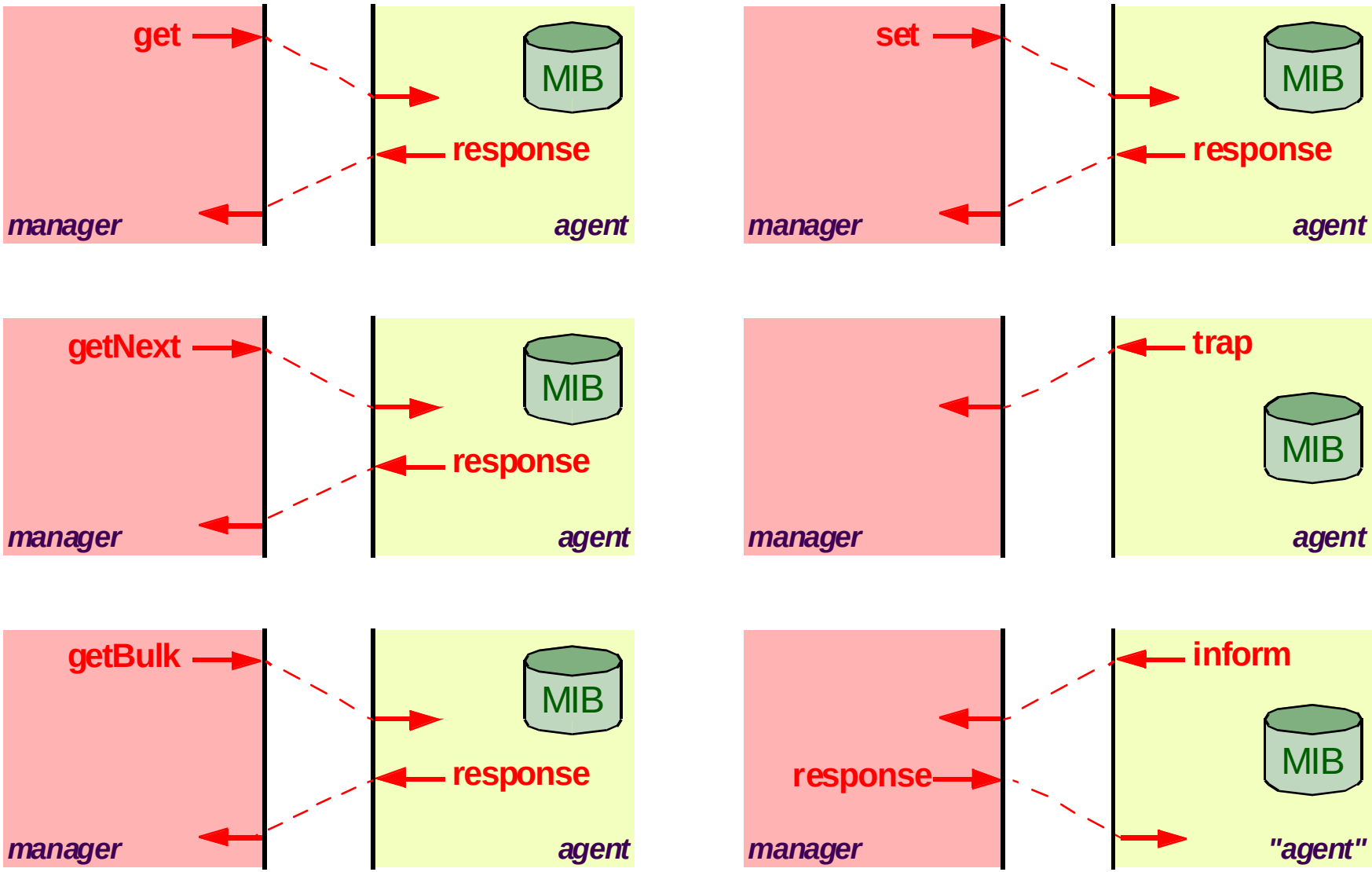
trap mode

SNMP: Protocol Elements

- The SNMP protocol is request - response based:
  - A request is sent to an agent from the management station
  - Normally the agent replies with the requested information or confirms the update
  - Various errors can also be reported

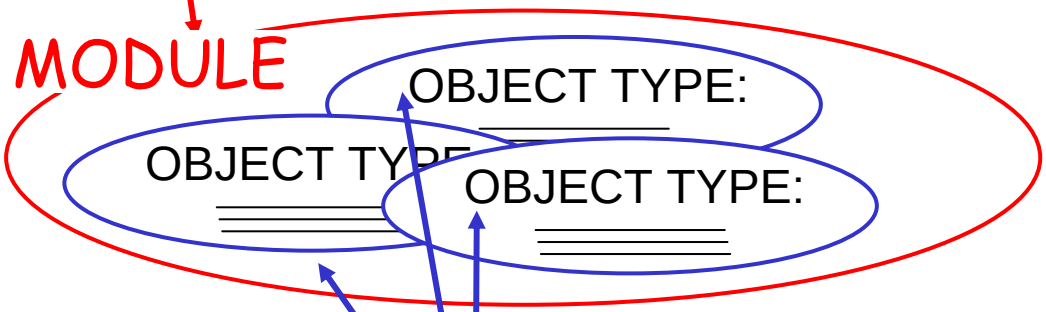
SNMP Messages	
Get-request	Requests the value of one or more variables
Get-next-request	Requests the variable following this one
Get-bulk-request	Fetches a large table
Get-response	Responds the requested values
Set-request	Updates one or more variables
Trap	Agent-to-manager: report an event
Inform-request	Manager-to-manager message describing local MIB

SNMPv2 PROTOCOL OPERATIONS



SNMP MIB

MIB module specified via SMI
MODULE-IDENTITY
(100 standardized MIBs, more vendor-specific)



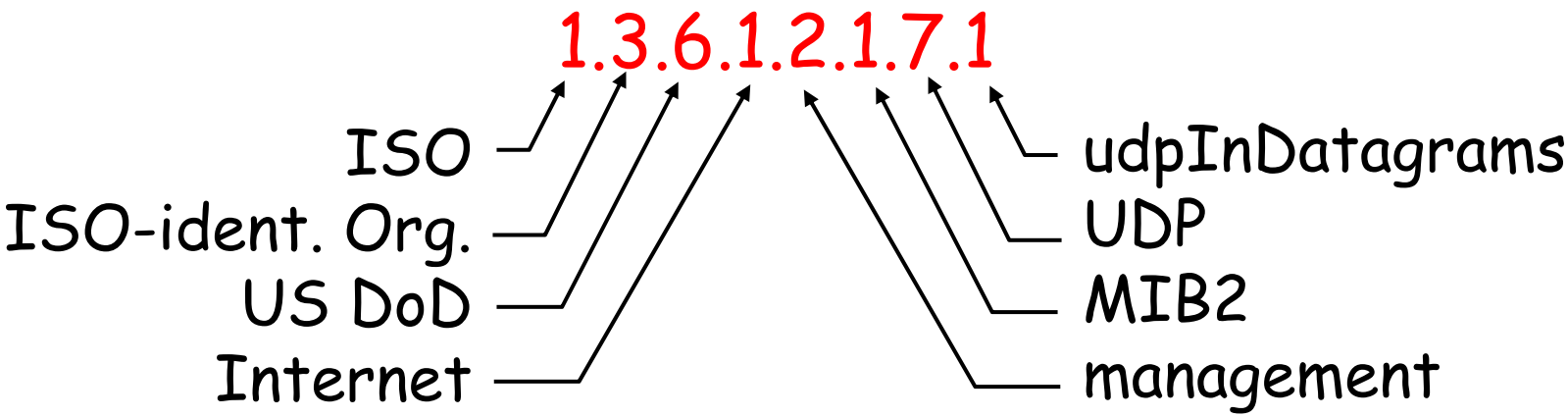
objects specified via SMI
OBJECT-TYPE construct

SNMP Naming

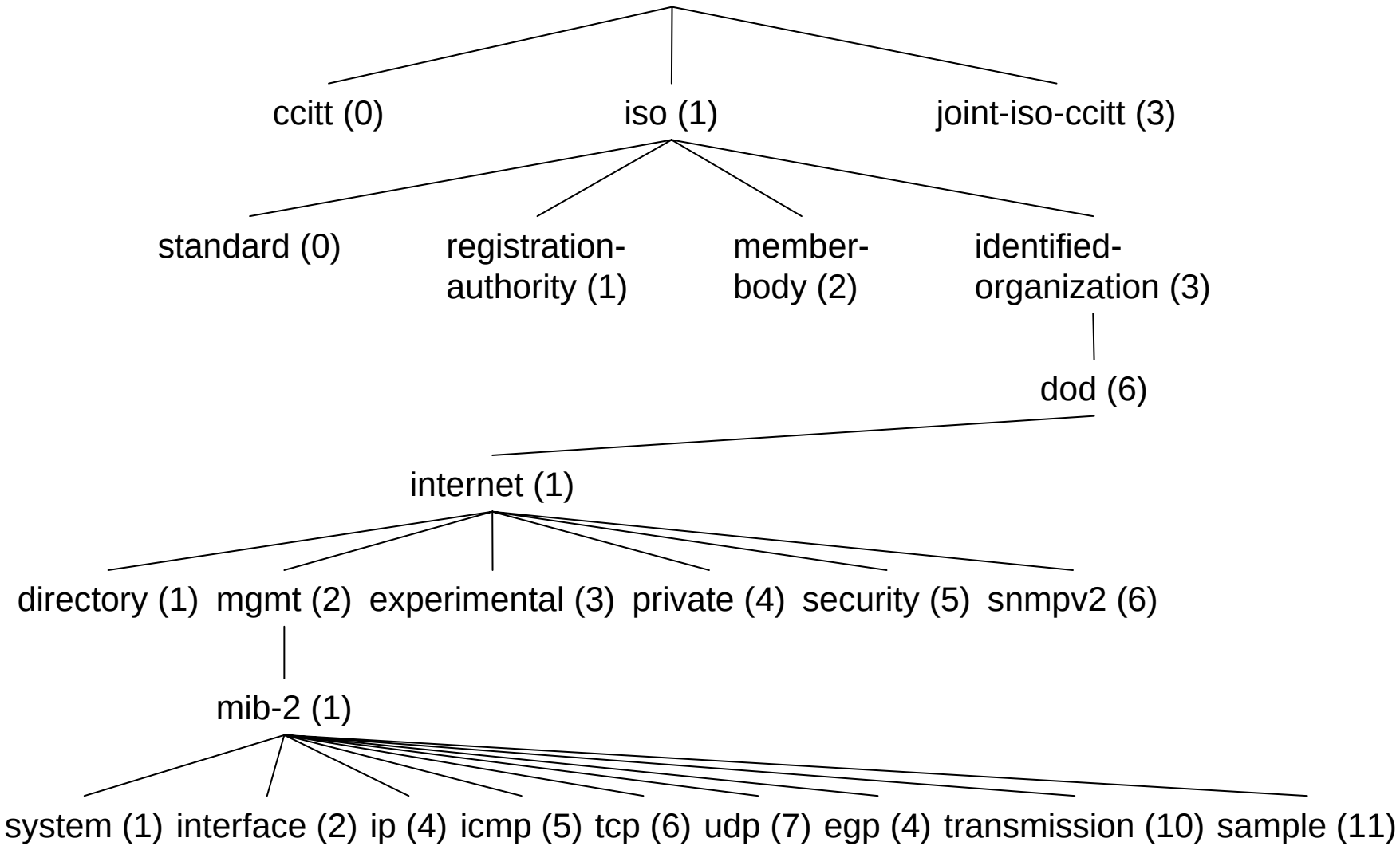
question: how to name every possible standard object (protocol, data, more..) in every possible network standard??

answer: *ISO Object Identifier tree:*

- hierarchical naming of all objects
- each branchpoint has name, number



SNMP: Organization of Management Information



Part of the ASN.1 Object Naming Tree

SNMP: Structure of Management Information

- SNMP uses a subset of ASN.1 with some new definitions called *structure of management information (SMI)* [RFC1442]

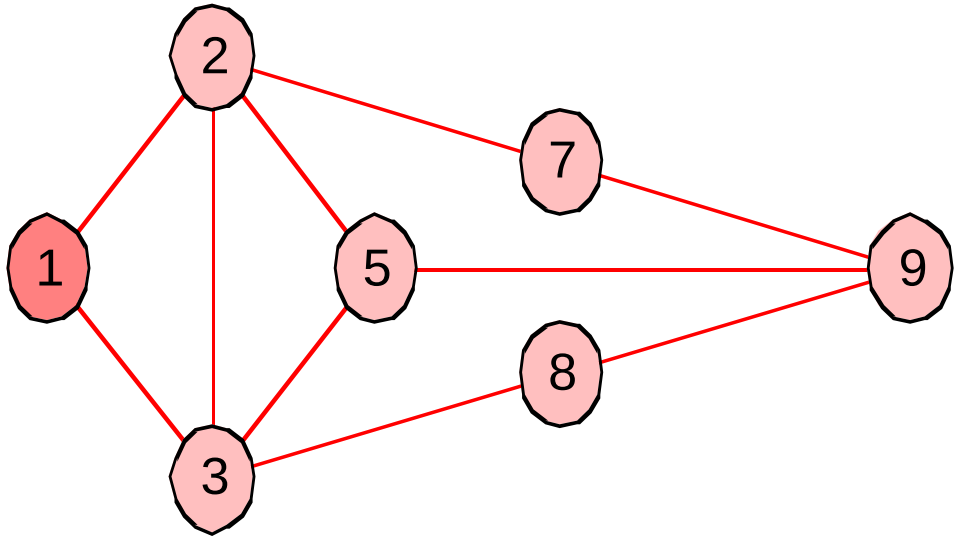
Basic Data Types of SMI

Name	Type	Bytes	Meaning
Integer	Numeric	4	Integer (32 bits in current implementations)
Counter32	Numeric	4	Unsigned 32-bit counter that wraps
Gauge32	Numeric	4	Unsigned value that does not wrap
Integer32	Numeric	4	32 bits even on a 64-bit CPU
UInteger32	Numeric	4	Like Integer32 but unsigned
Counter64	Numeric	8	A 64-bit counter
Time Ticks	Numeric	4	In hundredths of a second since some epoch
Bit String	String	4	Bit map of 1 to 32 bits
Octet String	String	≥ 0	Variable length byte string
Opaque	String	≥ 0	Obsolete; for backward compatibility only
Object Identifier	String	> 0	A list of integers (see figure on preceding page)
IPAddress	String	4	A dotted decimal Internet address
NsapAddress	String	< 22	An OSI NSAP address

TABLES

- **EXAMPLE: ROUTING TABLE**

destination	next
2	*2*
3	*3*
5	*2*
7	*2*
8	*3*
9	*3*

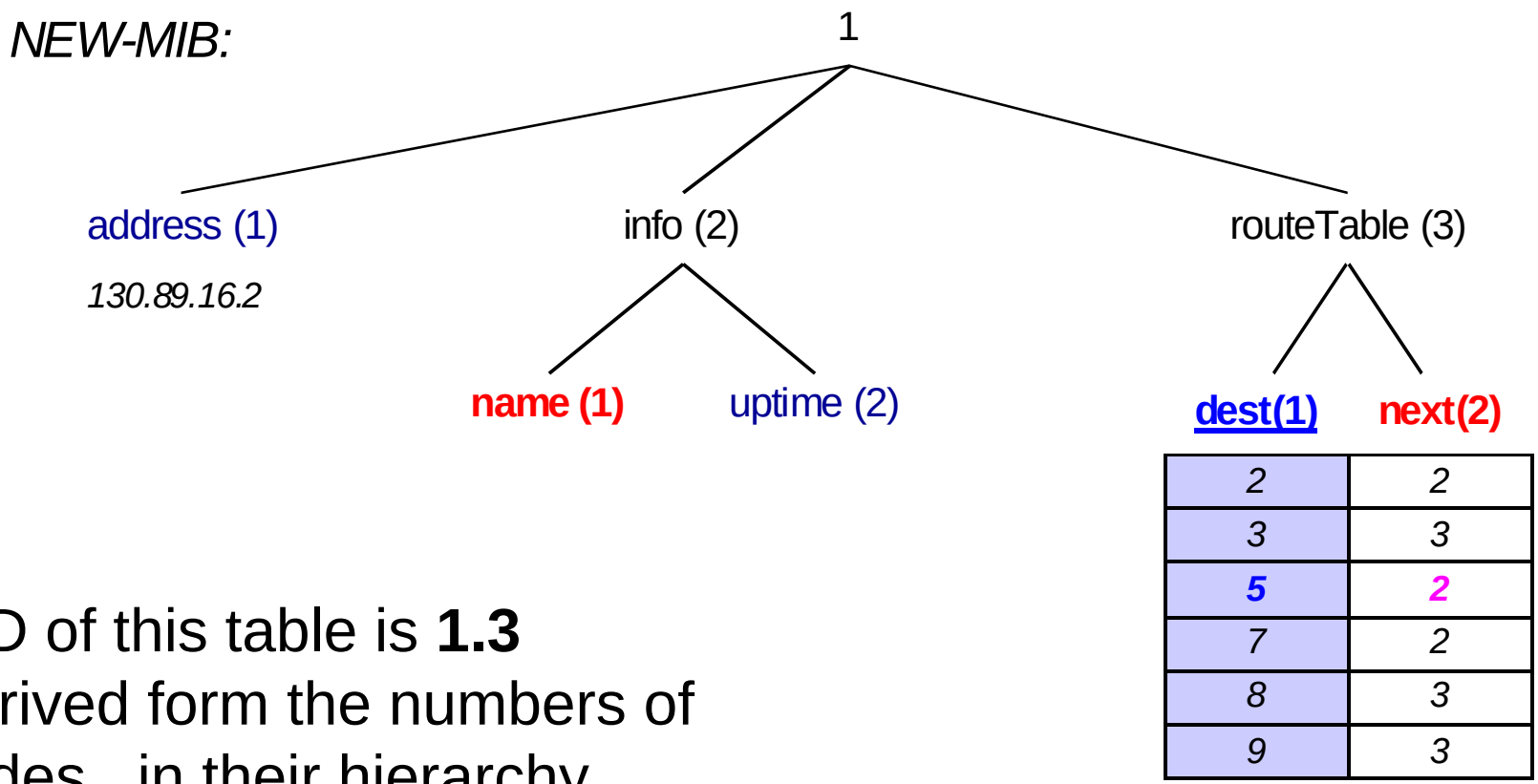


TO RETRIEVE INDIVIDUAL TABLE ENTRIES

EACH ENTRY SHOULD GET A NAME

NAMING OF TABLE ENTRIES - II

- **POSSIBILITY 2 (USED BY SNMP): INTRODUCE AN INDEX COLUMN**



OID of this table is **1.3**
Derived form the numbers of nodes...in their hierarchy...

EXAMPLE: THE VALUE OF *NEW-MIB routeTable next* 5 IS *2*

TABLE INDEXING - MULTIPLE INDEX FIELDS: EXAMPLE

1 = low costs
2 = high reliability

routeTable (3)

dest (1)	policy (2)	next (3)
130.89.16.23	*1*	*130.89.16.23*
130.89.16.23	*2*	*130.89.16.23*
130.89.19.121	*1*	*130.89.16.1*
192.1.23.24	*1*	*130.89.16.1*
192.1.23.24	*2*	*130.89.16.4*
193.22.11.97	*1*	*130.89.16.1*

X.C.I1.I2

OID of Table Column number Index value 1 Index value 2

1.3.3.192.1.23.24.1 => *130.89.16.1*

1.3.3.192.1.23.24.2 => *130.89.16.4*

TABLE DEFINITION: eg. Route table

```
routeTable                    OBJECT-TYPE
 SYNTAX            SEQUENCE OF RouteEntry
 MAX-ACCESS        not-accessible
 STATUS            current
 DESCRIPTION       "This entity's routing table"
 ::= {NEW-MIB  3}

routeEntry                    OBJECT-TYPE
 SYNTAX            RouteEntry
 MAX-ACCESS        not-accessible
 STATUS            current
 DESCRIPTION       "A route to a particular destination"
 INDEX             {dest, policy}
 ::= {routeTable  1}

RouteEntry ::=
 SEQUENCE          {
  dest      ipAddress,
  policy    INTEGER,
  next      ipAddress
  }
```

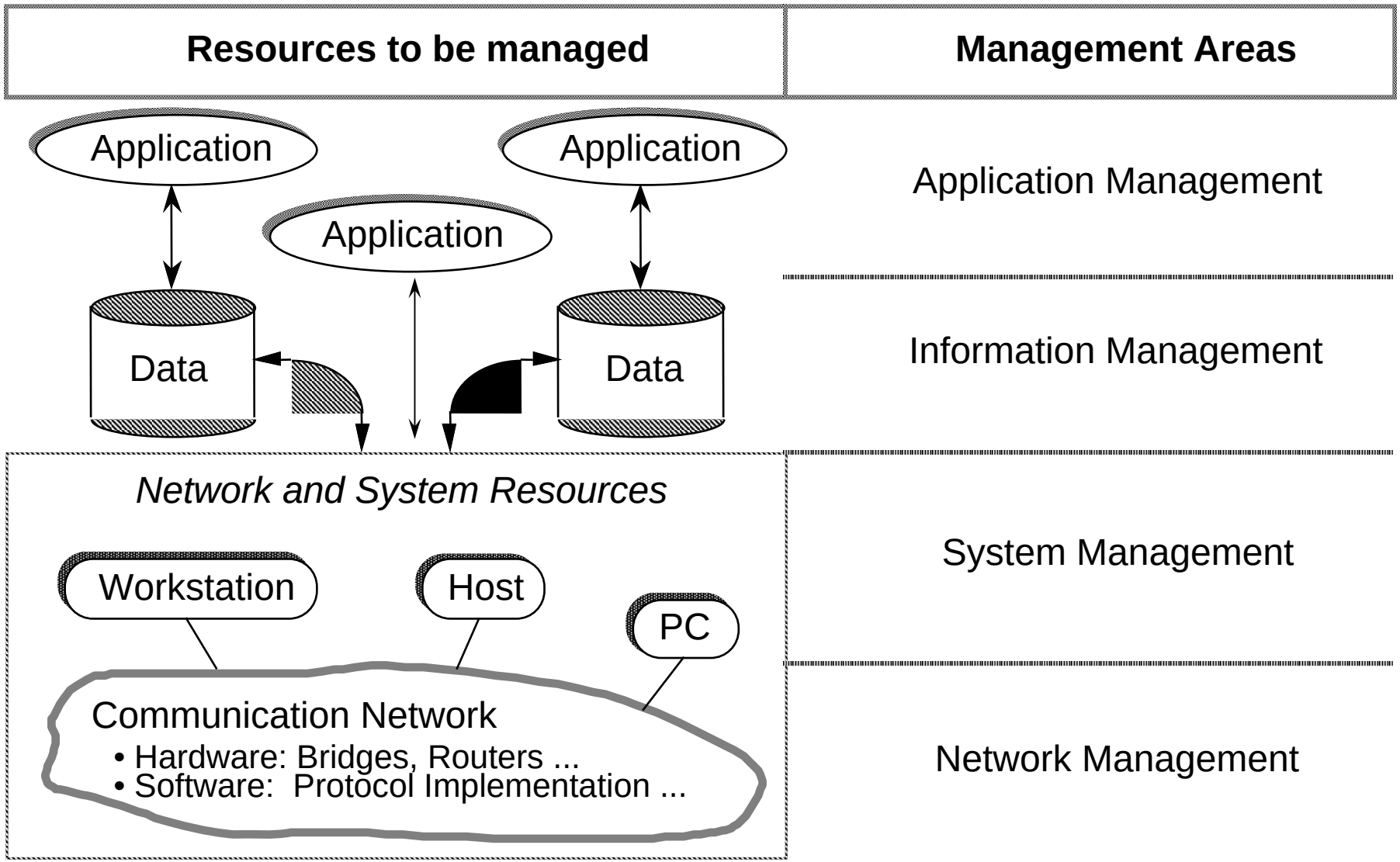
TABLE DEFINITION (cont. 2)

```
dest                    OBJECT-TYPE
  SYNTAX            ipAddress
  ACCESS            read-only
  STATUS            current
  DESCRIPTION               "The address of a particular destination"
  ::= {route-entry  1}


policy                  OBJECT-TYPE
  SYNTAX            INTEGER {
                            costs(1)            -- lowest delay
                            reliability(2)}     -- highest reliability
  ACCESS            read-only
  STATUS            current
  DESCRIPTION               "The routing policy to reach that destination"
  ::= {route-entry  2}


next                    OBJECT-TYPE
  SYNTAX            ipAddress
  ACCESS            read-write
  STATUS            current
  DESCRIPTION               "The internet address of the next hop"
  ::= {route-entry  3}
```

Network Management: Global perspective



SNMP v3

- addresses security issues of SNMP v1/2
- RFC 2570-2575
- defines overall architecture and security capability
- to be used with SNMP v2
- defines three security services
  - authentication
  - privacy
  - access control

SNMP v3 Services

- authentication assures that message is:
  - from identified source, not altered, not delayed or replayed
  - includes HMAC message authentication code
- privacy
  - encrypts messages using DES
- access control
  - pre configure agents to provide a number of levels of access to MIB for different managers
  - restricting access to information
  - limit operations

Security

Some very very short intro…

Goals of this part

- Give a brief glimpse of security in communication networks
- Basic goals and mechanisms
- Example: Firewalls

- Acknowledgment: based on (slightly modified) slides by Prof. Günther Schäfer, autor of the very good book: G. „*Security in Fixed and Wireless Networks*“. John Wiley & Sons, Ltd, UK, 2003

Security goals technically defined

- Confidentiality:
  - Data transmitted or stored should only be revealed to an intended audience
  - Confidentiality of entities is also referred to as anonymity
- Data Integrity:
  - It should be possible to detect any modification of data
  - This requires to be able to identify the creator of some data
- Accountability:
  - It should be possible to identify the entity responsible for any communication event
- Availability:
  - Services should be available and function correctly
- Controlled Access:
  - Only authorized entities should be able to access certain services or information

What is a threat in a communication network?

- Abstract Definition:
  - A *threat* in a communication network is any possible event or sequence of actions that might lead to a violation of one or more *security goals*
  - The actual realization of a threat is called an *attack*
- Examples:
  - A hacker breaking into a corporate computer
  - Disclosure of emails in transit
  - Someone changing financial accounting data
  - A hacker temporarily shutting down a website
  - Someone using services or ordering goods in the name of others

Threats technically defined

- Masquerade:
  - An entity claims to be another entity
- Eavesdropping:
  - An entity reads information it is not intended to read
- Authorization Violation:
  - An entity uses a service or resources it is not intended to use
- Loss or Modification of (transmitted) Information:
  - Data is being altered or destroyed
- Denial of Communication Acts (Repudiation):
  - An entity falsely denies its' participation in a communication act
- Forgery of Information:
  - An entity creates new information in the name of another entity
- Sabotage:
  - Any action that aims to reduce the availability and / or correct functioning of services or systems

Threats and technical security goals

Technical Security Goals	General Threats						
	Masquer-ade	Eaves-dropping	Authori-sation Violation	Loss or Mo-dification of (transmitted) information	Denial of Communi-cation acts	Forgery of Infor-mation	Sabotage (e.g. by overload)
Confidentiality	x	x	x				
Data Integrity	x		x	x		x	
Accountability	x		x		x	x	
Availability	x		x	x			x
Controlled Access	x		x			x	

These threats are often combined in order to perform an attack!

Safeguards Against Information Security Threats 1

- *Physical Security:*
  - Locks or other physical access control
  - Tamper-proofing of sensitive equipment
  - Environmental controls
- *Personnel Security:*
  - Identification of position sensitivity
  - Employee screening processes
  - Security training and awareness
- *Administrative Security:*
  - Controlling import of foreign software
  - Procedures for investigating security breaches
  - Reviewing audit trails
  - Reviewing accountability controls
- *Emanations Security:*
  - Radio Frequency and other electromagnetic emanations controls

Safeguards Against Information Security Threats 2

- *Media Security:*
  - Safeguarding storage of information
  - Controlling marking, reproduction and destruction of information
  - Ensuring that media containing information are destroyed securely
  - Scanning media for viruses
- *Lifecycle Controls:*
  - Trusted system design, implementation, evaluation and endorsement
  - Programming standards and controls
  - Documentation controls
- *Computer Security:*
  - Protection of information while stored / processed in a computer system
  - Protection of the computing devices itself
- *Communications Security:* (the main subject of this lecture)
  - Protection of information during transport from one system to another
  - Protection of the communication infrastructure itself

Communications security: Some terminology

- Security Service:
  - An abstract service that seeks to ensure a specific security property
  - A security service can be realised with the help of cryptographic algorithms and protocols as well as with conventional means:
    - One can keep an electronic document on a floppy disk confidential by storing it on the disk in an encrypted format as well as locking away the disk in a safe
    - Usually a combination of cryptographic and other means is most effective
- Cryptographic Algorithm:
  - A mathematical transformation of input data (e.g. data, key) to output data
  - Cryptographic algorithms are used in cryptographic protocols
- Cryptographic Protocol:
  - A series of steps and message exchanges between multiple entities in order to achieve a specific security objective

Security services – Overview

- Authentication
  - The most fundamental security service which ensures, that an entity has in fact the identity it claims to have
- Integrity
  - In some kind, the “small brother” of the authentication service, as it ensures, that data created by specific entities may not be modified without detection
- Confidentiality
  - The most popular security service, ensuring secrecy of protected data
- Access Control
  - Controls that each identity accesses only those services and information it is entitled to
- Non-Repudiation
  - Protects against that entities participating in a communication exchange can later falsely deny that the exchange occurred

Cryptology – Definition and terminology

- Cryptology:
  - Science concerned with communications in secure and usually secret form
  - The term is derived from the Greek kryptós (hidden) and lógos (word)
  - Cryptology encompasses:
    - Cryptography (gráphein = to write): the study of the principles and techniques by which information can be concealed in ciphertext and later revealed by legitimate users employing a secret key
    - Cryptanalysis (analýein = to loosen, to untie): the science (and art) of recovering information from ciphers without knowledge of the key
- Cipher:
  - Method of transforming a message (plaintext) to conceal its meaning
  - Also used as synonym for the concealed ciphertext
  - The transformation usually takes the message and a (secret) key as input

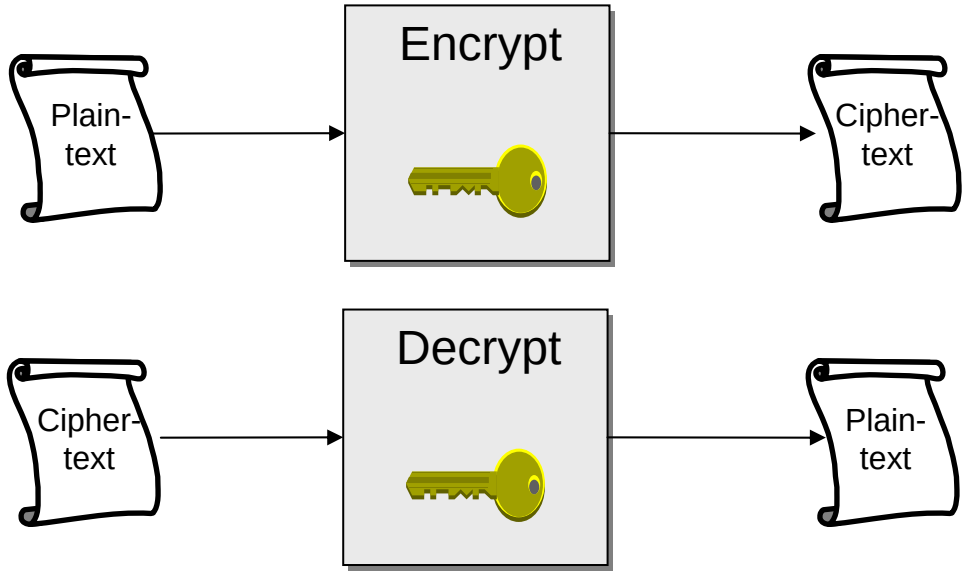
(Source: Encyclopaedia Britannica)

Cryptographic algorithms

- For network security two main applications of cryptographic algorithms are of principal interest:
  - Encryption of data: transforms plaintext data into ciphertext in order to conceal its' meaning
  - Signing of data: computes a check value or digital signature to a given plain- or ciphertext that can be verified by some or all entities being able to access the signed data
  - Some cryptographic algorithms can be used for both purposes, some are only secure and / or efficient for one of them.
- Principal categories of cryptographic algorithms:
  - Symmetric cryptography using 1 key for en-/decryption or signing/checking
  - Asymmetric cryptography using 2 different keys for en-/decryption or signing/checking
  - Cryptographic hash functions using 0 keys (the "key" is not a separate input but "appended" to or "mixed" with the data).

Symmetric encryption

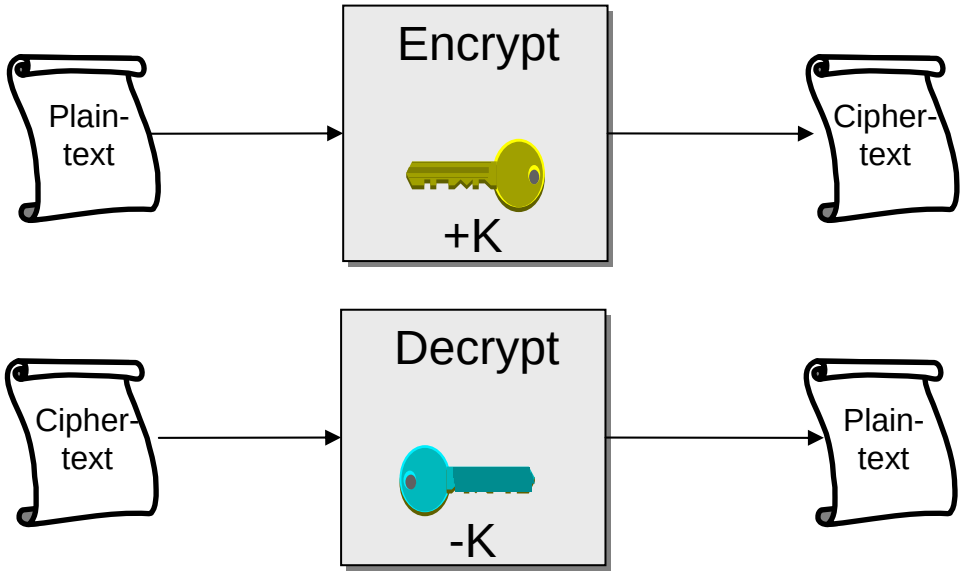
- General description:
  - The same key $K_{A,B}$ is used for enciphering and deciphering of messages:



- Notation:
  - If P denotes the plaintext message $E(K_{A,B}, P)$ denotes the ciphertext and it holds $D(K_{A,B}, E(K_{A,B}, P)) = P$
  - Alternatively we sometimes write $\{P\}_{K_{A,B}}$ for $E(K_{A,B}, P)$
- Examples: DES, 3DES, IDEA, …

Asymmetric cryptography (1)

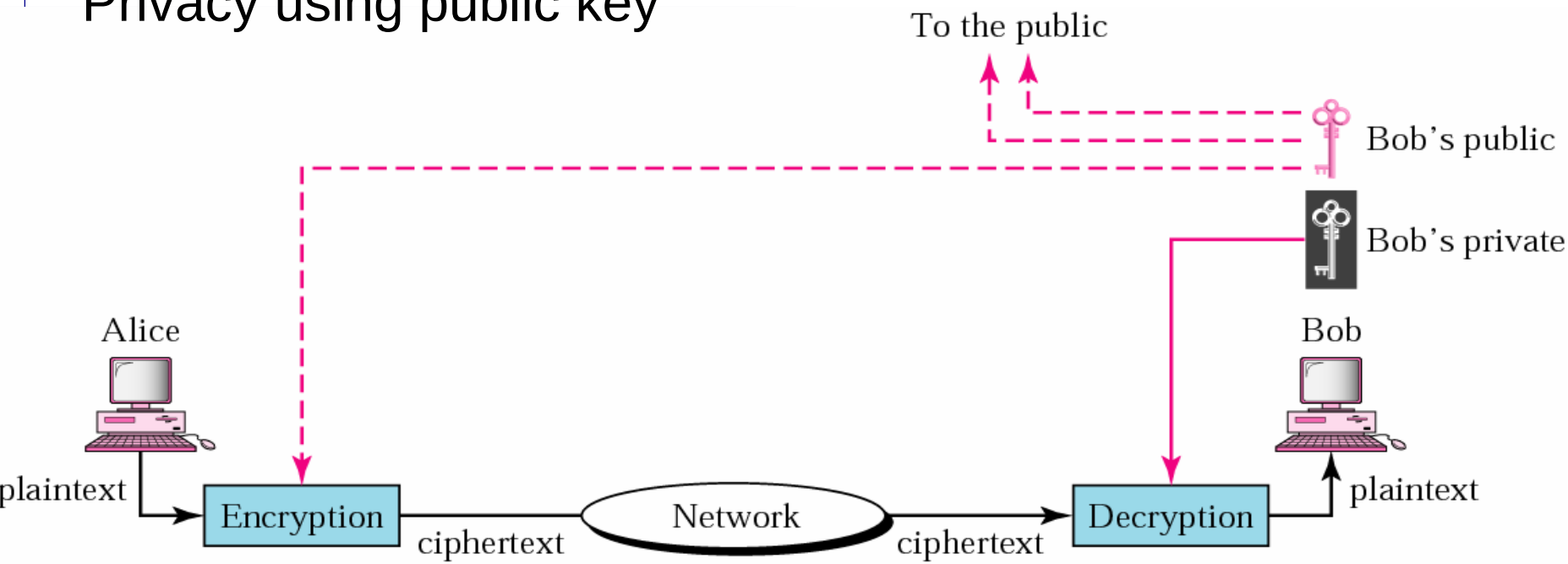
- General idea:
  - Use two different keys +K for encryption and -K for decryption
  - Given a random ciphertext c = E(+K, m) and +K it should be infeasible to compute m = D(-K, c) = D(-K, E(+K, m))
    - This implies that it should be infeasible to compute -K when given +K
  - The key -K is only known to one entity A and is called A's private key $-K_A$
  - The key +K can be publicly announced and is called A's public key $+K_A$



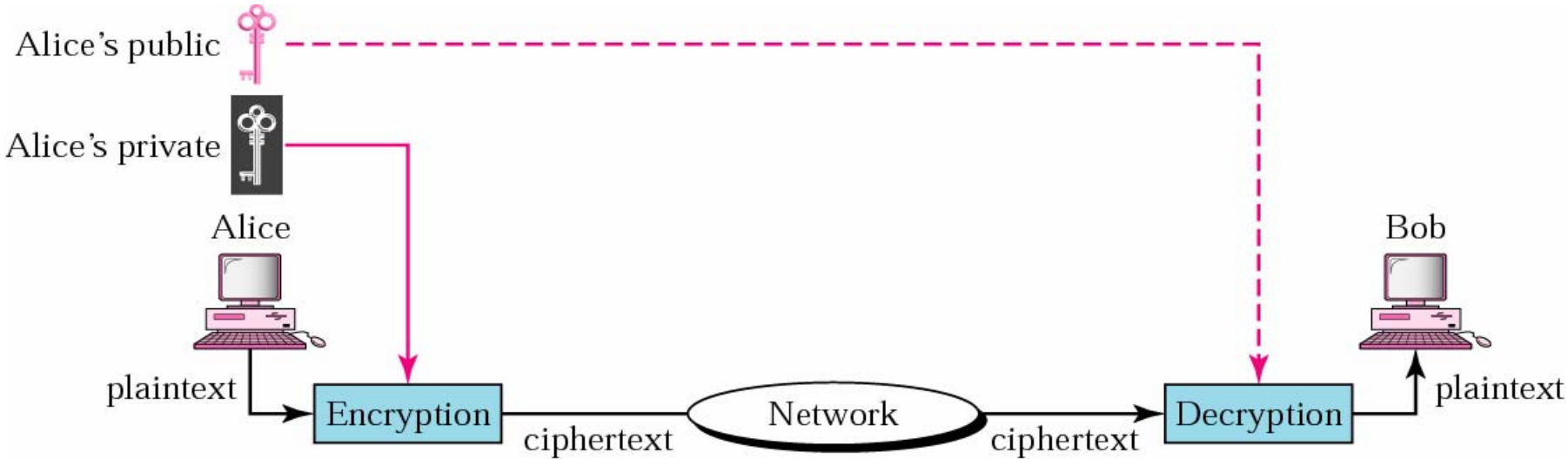
Asymmetric cryptography (2)

- Applications:
  - Encryption:
    - If B encrypts a message with A's public key $+K_A$, he can be sure that only A can decrypt it using $-K_A$
  - Signing:
    - If A encrypts a message with his own private key $-K_A$, everyone can verify this signature by decrypting it with A's public key $+K_A$
  - Attention:
    - It is crucial that everyone can verify that he really knows A's public key and not the key of an adversary!
- Practical considerations:
  - Asymmetric cryptographic operations are about magnitudes slower than symmetric ones
  - Therefore, they are often not used for encrypting / signing bulk data
  - Symmetric techniques are used to encrypt / compute a cryptographic hash value and asymmetric cryptography is just used to encrypt a key / hash value

Privacy using public key



Signing a document using public key



Cryptographic Protocols

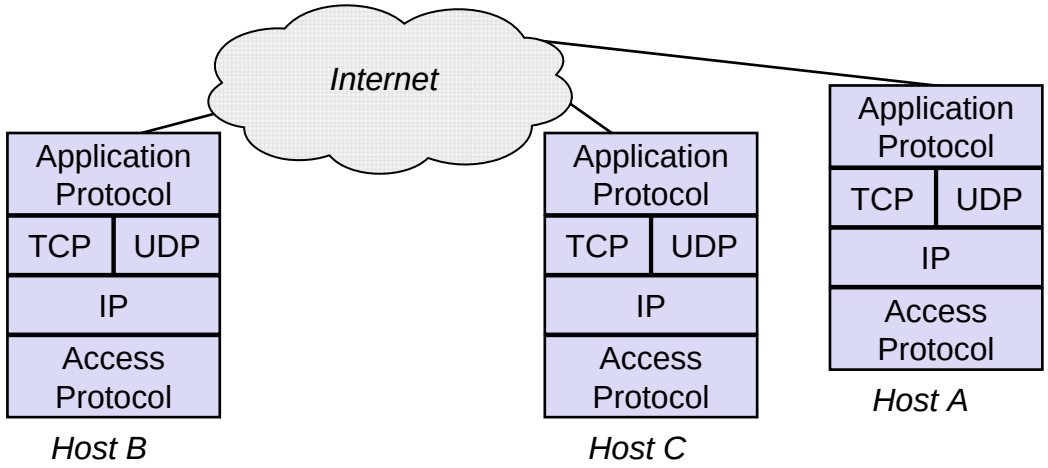
- Definition:

  A *cryptographic protocol* is defined as a series of steps and message exchanges between multiple entities in order to achieve a specific security objective

- Applications of cryptographic protocols:
  - Key exchange
  - Authentication
    - Data origin authentication: the security service, that enables a receiver to verify by whom a message was created and that it has not been modified
    - Entity authentication: the security service, that enables communication partners to verify the identity of their peer entities
  - Combined authentication and key exchange

Security Problems of the Internet Protocol

- When an entity receives an IP packet, it has no assurance of:
  - *Data origin authentication / data integrity:*
    - The packet has actually been send by the entity which is referenced by the source address of the packet
    - The packet contains the original content the sender placed into it, so that it has not been modified during transport
    - The receiving entity is in fact the entity to which the sender wanted to send the packet
  - *Confidentiality:*
    - The original data was not inspected by a third party while the packet was sent from the sender to the receiver

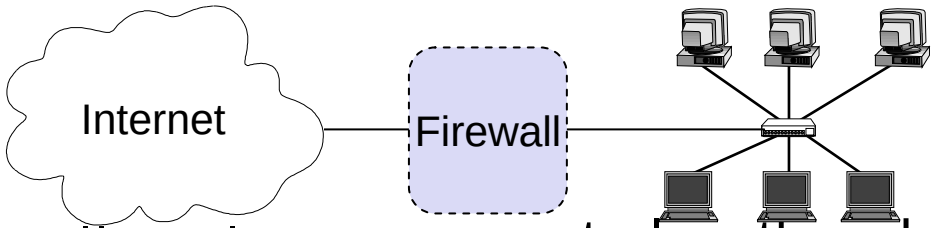


Security Objectives of IPSec

- IPSec aims to ensure the following security objectives:
  - *Data origin authentication / connectionless data integrity:*
    - It is not possible to send an IP datagram with neither a masqueraded IP source nor destination address without the receiver being able to detect this
    - It is not possible to modify an IP datagram in transit, without the receiver being able to detect the modification
    - *Replay protection:* it is not possible to later replay a recorded IP packet without the receiver being able to detect this
  - *Confidentiality:*
    - It is not possible to eavesdrop on the content of IP datagrams
    - Limited traffic flow confidentiality
- Security policy:
  - Sender, receiver and intermediate nodes can determine the required protection for an IP packet according to a local security policy
  - Intermediate nodes and the receiver will drop IP packets that do not meet these requirements

Internet firewalls

- A network firewall can be compared to a castle moat
  - It restricts people to entering at one carefully controlled point
  - It prevents attackers from getting close to other defenses
  - It restricts people to leaving at one carefully controlled point
- Usually, a network firewall is installed at a point where the protected subnetwork is connected to a less trusted network
  - Example: Connection of a corporate local area network to the Internet



  - Basically firewalls realize access control on the subnetwork level

Firewalls: Terminology (1)

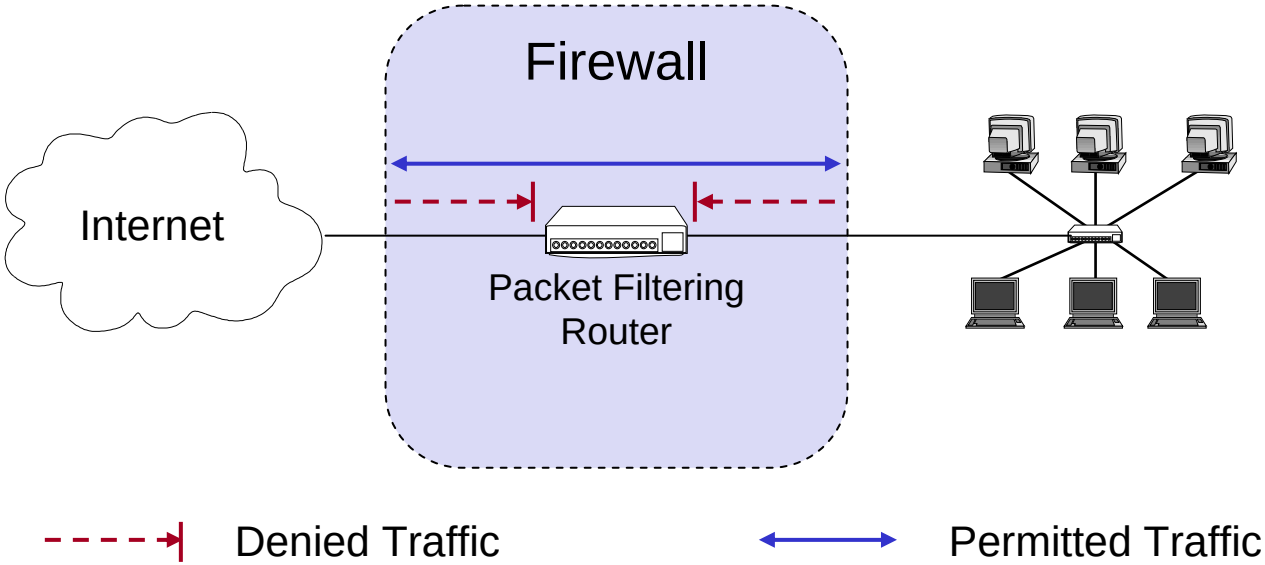
- Firewall
  - A component or a set of components that restricts access between a protected network and the Internet or between other sets of networks
- Packet Filtering
  - The action a device takes to selectively control the flow of data to and from a network
  - Packet filtering is an important technique to implement access control on the subnetwork-level for packet oriented networks, e.g. the Internet
  - A synonym for packet filtering is screening
- Bastion Host
  - A computer that must be highly secured because it is more vulnerable to attacks than other hosts on a subnetwork
  - A bastion host in a firewall is usually the main point of contact for user processes of hosts of internal networks with processes of external hosts
- Dual-homed host
  - A general purpose computer with at least two network interfaces

Firewalls: Terminology (2)

- Proxy:
  - A program that deals with external servers on behalf of internal clients
  - Proxies relay approved client requests to real servers and also relay the servers' answers back to the clients
- Network Address Translation (NAT):
  - A procedure by which a router changes data in packets to modify the network addresses
  - This allows to conceal the internal network addresses (even though NAT is not actually a security technique)
- Perimeter Network:
  - A subnetwork added between an external and an internal network, in order to provide an additional layer of security
  - A synonym for perimeter network is de-militarized zone (DMZ)

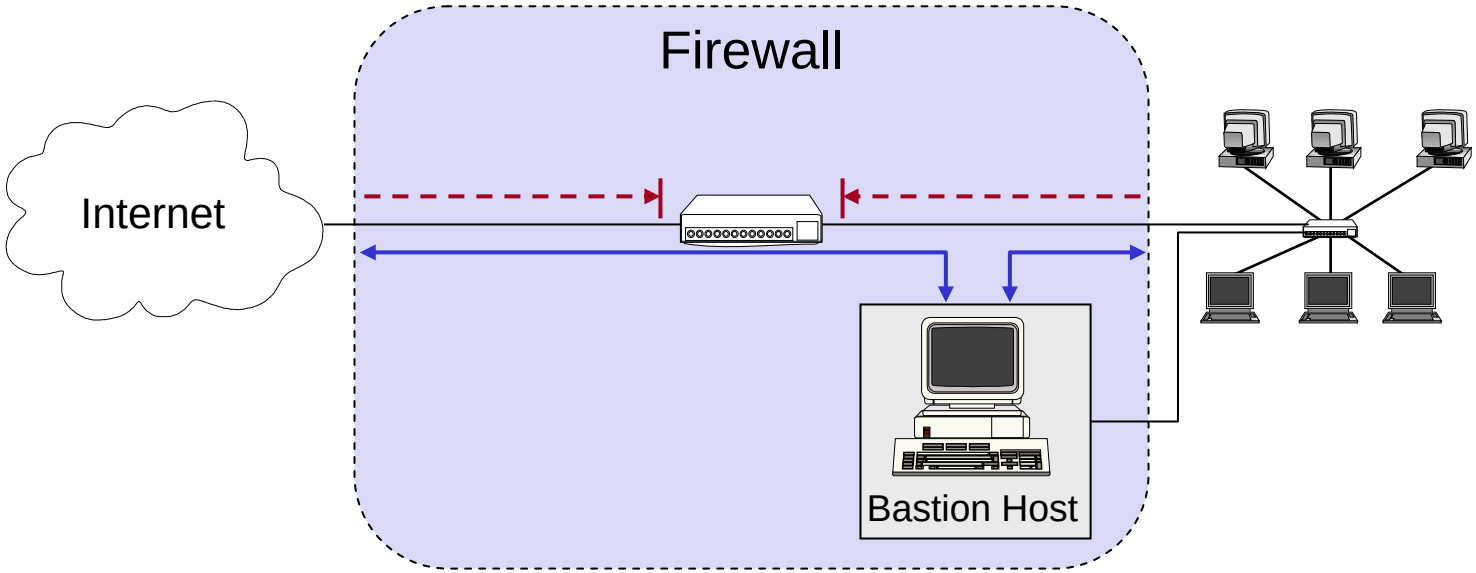
Firewalls architecture: Simple packet filter

- The most simple architecture just consists of a packet filtering router
- It can be either realized with:
  - A standard workstation (e.g. Linux PC) with at least two network interfaces plus routing and filtering software
  - A dedicated router device, which usually also offers filtering capabilities



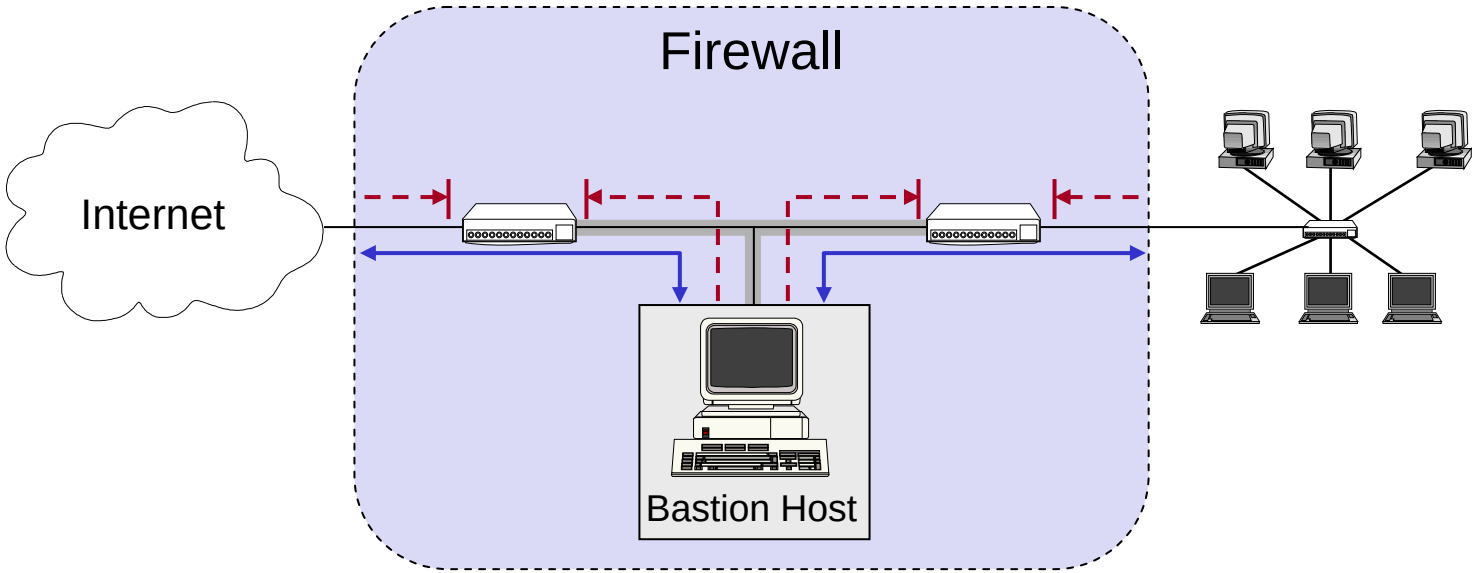
Firewall architecture: Screened host

- The packet filter:
  - Allows permitted IP traffic between the screened host and the Internet
  - Blocks all direct traffic between other internal hosts and the Internet
- The screened host provides proxy services:
  - Despite partial protection by the packet filter the screened host acts as a bastion host



Firewall architecture: Screened subnet

- A perimeter network is created between two packet filters
- The inner packet filter serves as additional protection in case the bastion host is ever compromised
  - For example, this avoids a compromised bastion host to sniff on internal traffic
- The perimeter network is also a good place to host a publicly accessible information server, e.g. a WWW server



Firewalls: Packet filtering

- What can be done with packet filtering?
  - Theoretically speaking everything, as all information exchanged in a communication relation is transported via packets
  - In practice, efficiency tradeoffs against proxy approaches have to be considered
- Basic packet filtering enables to control data transfer based on:
  - Source IP Address
  - Destination IP Address
  - Transport protocol
  - Source and destination application port
  - Potentially, specific protocol flags (e.g. TCP's ACK- and SYN-flag)
  - The network interface a packet has been received on

Firewalls: An example packet filtering ruleset

- This ruleset specifies that incoming and outgoing email is the only allowed traffic into and out of a protected network
  - Email is relayed between two servers by transferring it to an SMTP daemon on the target server (server port 25, client port > 1023)
  - Rule A allows incoming email to flow to the bastion host and rule B allows the bastion host's acknowledgements to exit the network
  - Rules C and D are analogous for outgoing email
  - Rule E denies all other traffic

Rule	Direction	Src. Addr.	Dest. Addr.	Protocol	Src. Port	Dest. Port	ACK	Action
A	Inbound	External	Bastion	TCP	>1023	25	Any	Permit
B	Outbound	Bastion	External	TCP	25	>1023	Yes	Permit
C	Outbound	Bastion	External	TCP	>1023	25	Any	Permit
D	Inbound	External	Bastion	TCP	25	>1023	Yes	Permit
E	Either	Any	Any	Any	Any	Any	Any	Deny