



Postgraduate Diploma in Strategic Business Information Technology

Module 4 Computer Networking and Management

Chapter 8 **Network Management**

Network management

Chapter goals:

- ❑ Introduction to network management
 - motivation
 - major components
- ❑ Internet network management framework
 - MIB: management information base
 - SMI: data definition language
 - SNMP: protocol for network management
 - security and administration
- ❑ Presentation services: ASN.1
- ❑ Firewalls

What is network management?

- ❑ **Autonomous systems (also known as 'network')**: 100s or 1000s of interacting hardware/software components
- ❑ Other complex systems requiring monitoring, control:
 - jet airplane
 - nuclear power plant
 - others?

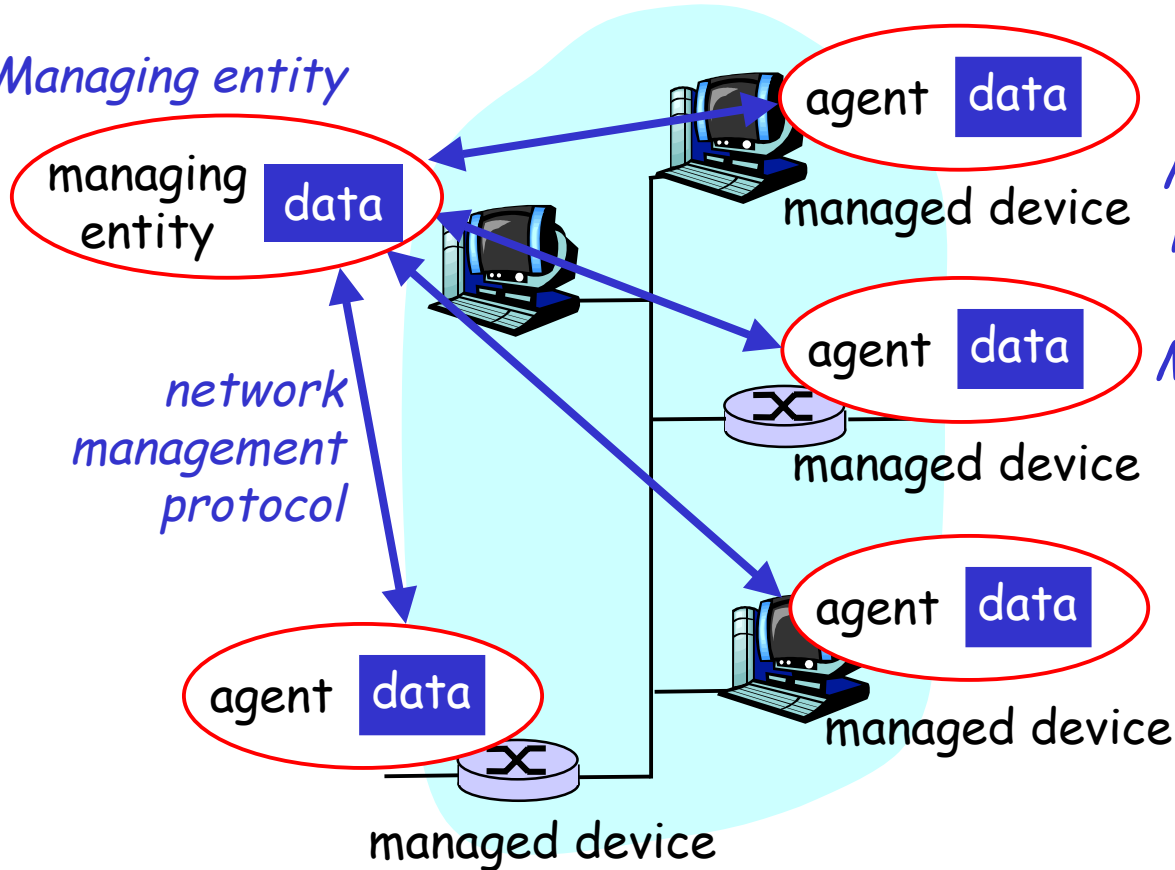


"**Network management** includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements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

Infrastructure for network management

Definitions:

Managing entity



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 1980s: *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

SNMP overview: 4 key parts

- ❑ **Management information base (MIB):**
 - distributed information store of network management data
- ❑ **Structure of Management Information (SMI):**
 - data definition language for MIB objects
- ❑ **SNMP protocol**
 - convey manager<->managed object info, commands
- ❑ **Security, administration capabilities**
 - major addition in SNMPv3

SMI: data definition language

Purpose: Syntax, semantics of management data well-defined, unambiguous

- Base data types:
 - straightforward, boring
- OBJECT-TYPE
 - data type, status, semantics of managed object
- MODULE-IDENTITY
 - groups related objects into MIB module

Basic Data Types

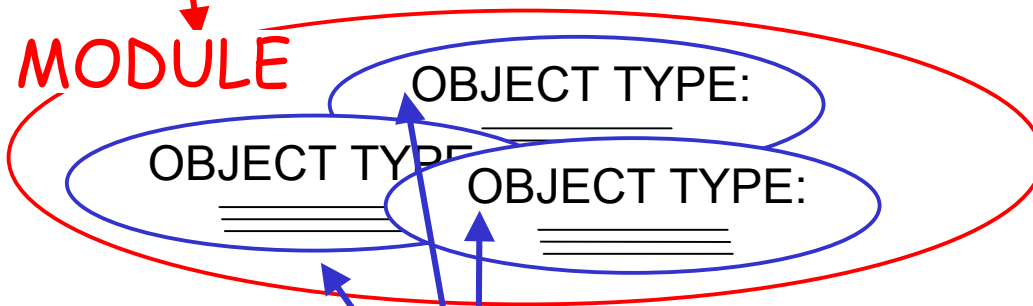
INTEGER
Integer32
Unsigned32
OCTET STRING
OBJECT IDENTIFIED
IPAddress
Counter32
Counter64
Gauge32
Tie Ticks
Opaque

SNMP MIB

MIB module specified via SMI

MODULE-IDENTITY

(100 standardized MIBs, more vendor-specific)



objects specified via SMI
OBJECT-TYPE construct

SNMP security and administration

- ❑ **Encryption:** DES-encrypt SNMP message
- ❑ **Authentication:** compute, send $MIC(m,k)$:
compute hash (MIC) over message (m),
secret shared key (k)
- ❑ **Protection against playback:** use nonce
- ❑ **View-based access control**
 - SNMP entity maintains database of access rights, policies for various users
 - database itself accessible as managed object!

Firewall

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

Two firewall types:

- packet filter
- application gateways

To prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections. Attacked host alloc's TCP buffers for bogus connections, none left for 'real' connections.

To prevent illegal modification of internal data.

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

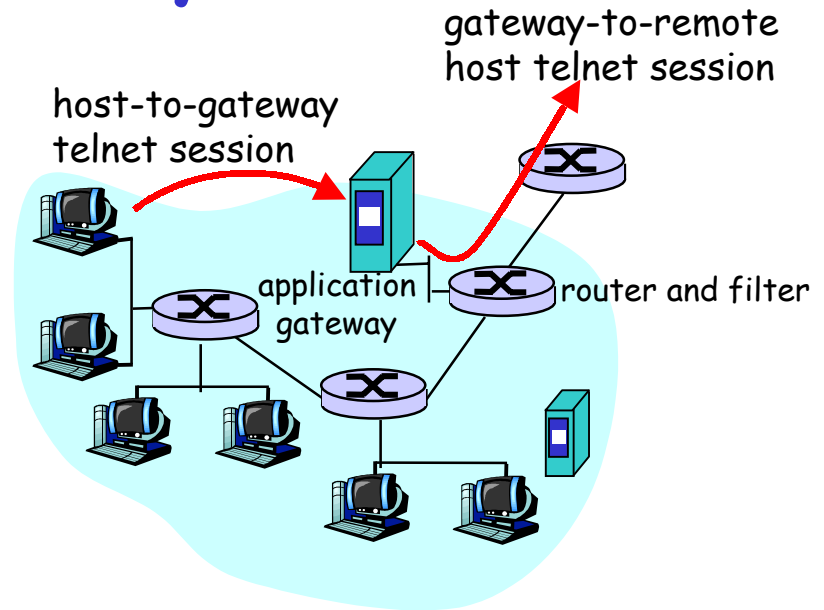
To prevent intruders from obtaining secret information.

Packet filtering

- ❑ Internal network is connected to Internet through a router.
- ❑ Router manufacturer provides options for filtering packets, based on:
 - source IP address
 - destination IP address
 - TCP/UDP source and destination port numbers
 - ICMP message type
 - TCP SYN and ACK bits
- ❑ Example 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23.
 - all incoming and outgoing UDP flows and telnet connections are blocked.
- ❑ Example 2: Block inbound TCP segments with ACK=0.
 - prevents external clients from making TCP connections with internal clients, but allows internal clients to connect to outside.

Application gateways

- ❑ Filters 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 and gateways

- ❑ IP spoofing: router can't know if data 'really' comes from claimed source
- ❑ If multiple applications need special treatment, each has own application 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.

Summary

- ❑ The architecture of network-management systems revolves around five key components
- ❑ How SNMP instantiates the five key components
- ❑ MIB objects, SMI, SNMP protocol
- ❑ Firewalls, packet filtering and application-level gateways