Network Management

- Internet network management framework
  - MIB: management information base
  - SMI: data definition language
  - SNMP: protocol for network management

What is network management?

- Autonomous systems : 1000s of interacting hardware/software components

"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."

Network management

- The **International Organization for Standardization (ISO**) has created a **network management model.**

- **Five areas of network management are defined:**

1. Performance management.
2. Fault management
3. Configuration management.
4. Accounting management.
5. Security management

Network management

- ***Performance management.*** *The goal of performance management is to quantify*, measure, report, analyze, and control the performance.

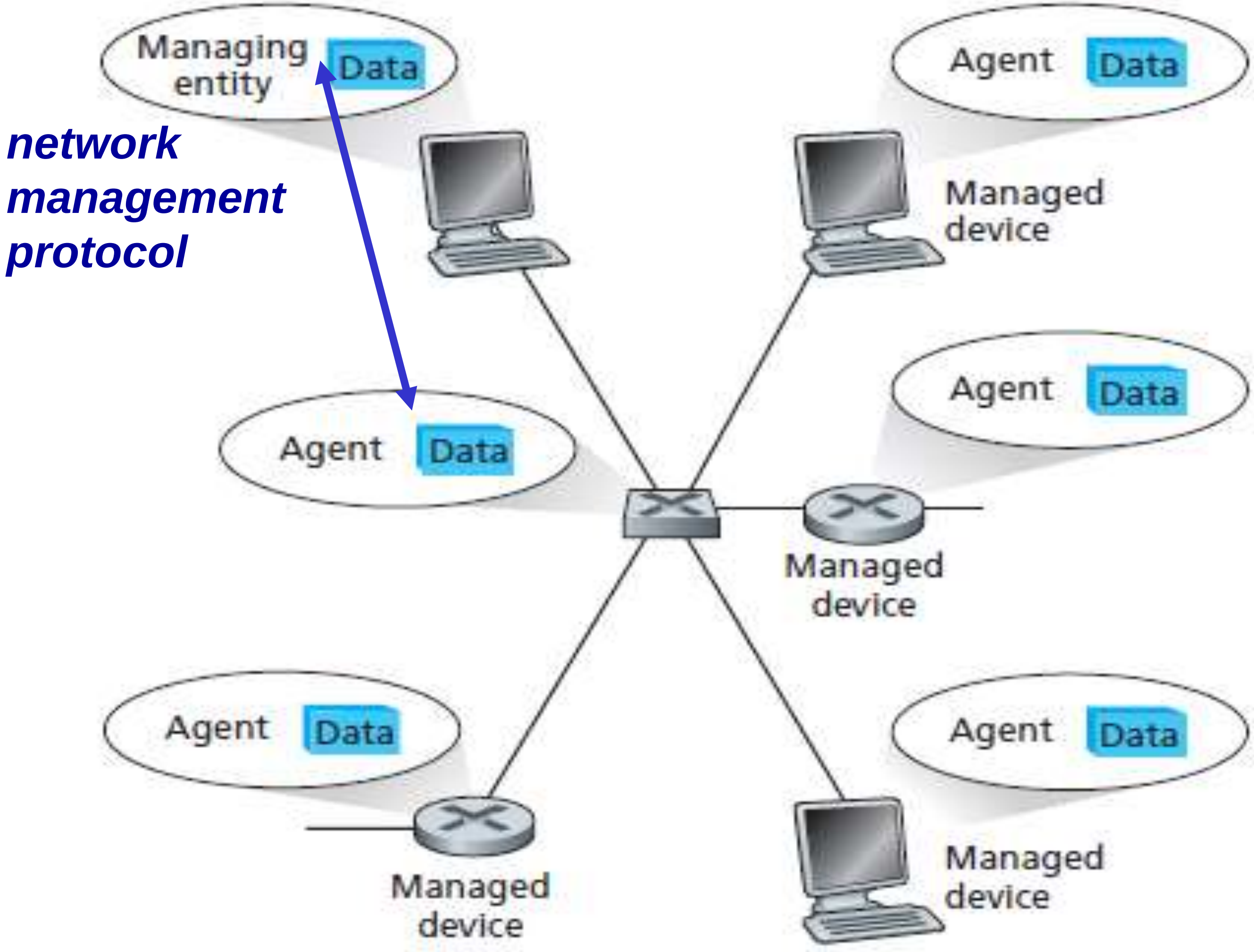
- (for example, utilization and throughput) of different network components.

- These components include individual devices (for example, links, routers, and hosts) as well as end-to-end abstractions such as a path through the network.

Network management

- ***Fault management***. *The goal of fault management is to log, detect, and respond* to fault conditions in the network.
- ***Configuration management***. *Configuration management allows a network manager* to track which devices are on the managed network and the hardware and software configurations of these devices.
- ***Accounting management.*** *Accounting management allows the network manager* to specify, log, and control user and device access to network resources.
- ***Security management.*** *The goal of security management is to control access to* network resources according to some well-defined policy

Components of Network management Architecture



Components of Network management Architecture

- There are three principal components of a network management architecture:

1. a managing entity
2. the managed devices
3. a network management protocol.

Components of Network management Architecture

A Managing Entity

- The **managing entity is an application, typically with a human in the loop,** running in a centralized network management station.
- The managing entity is the locus of activity for network management; **it controls the collection, processing, analysis, and/or display of network management information.**
- It is here that actions are initiated to control network behavior and here that the human network administrator interacts with the network devices.

Components of Network management Architecture

A Managed Device

- A **managed device is a piece of network equipment (including its software)** that resides on a managed network.
- Managed device might be a host, router, bridge, hub, printer, or modem.

- Within a managed device, there may be several so-called **managed objects.**
- **These** managed objects are the actual pieces of hardware within the managed device (for example, a network interface card), and the sets of configuration parameters for the pieces of hardware and software

Components of Network management Architecture

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

- Finally, also resident in each managed device is a **network management agent,**

---------A process running in the managed device that communicates with the managing entity, taking local actions at the managed device under the command and control of the managing entity.

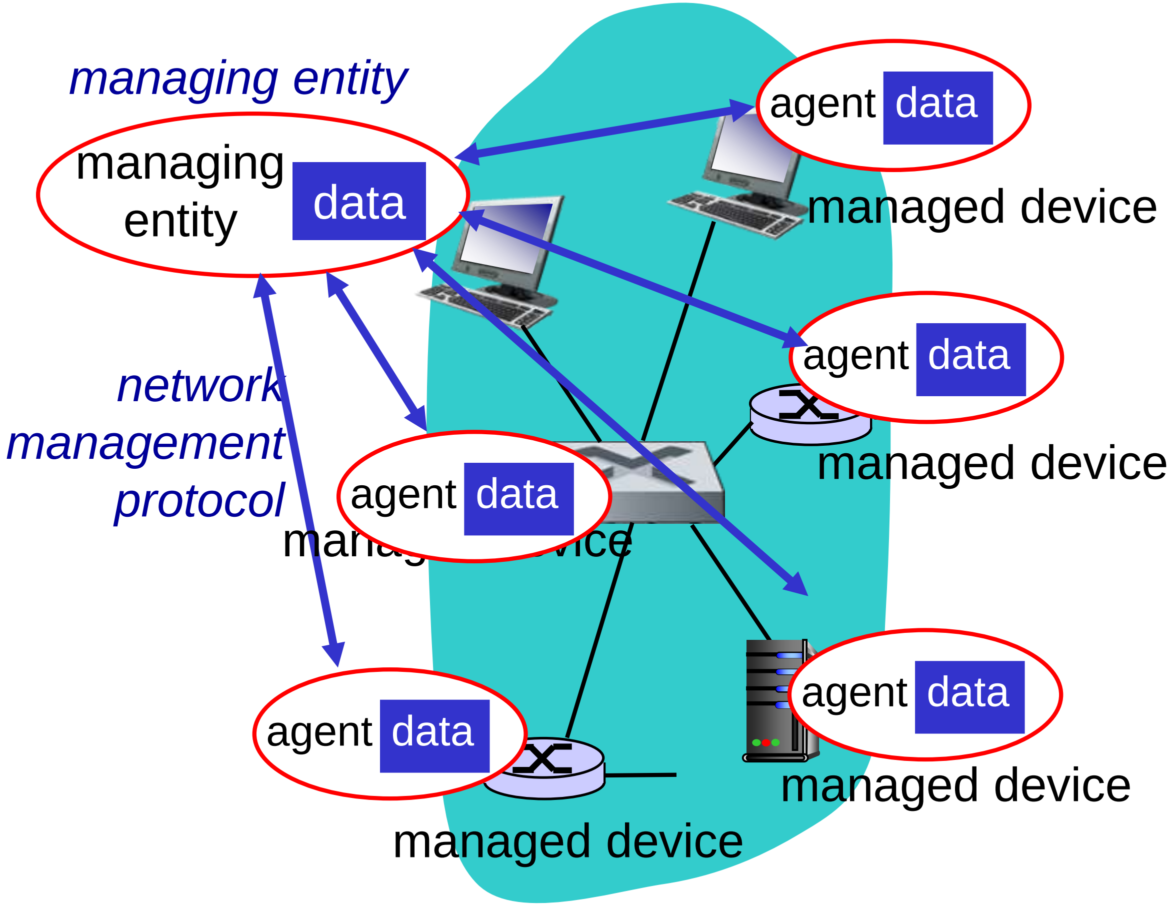
Components of Network management Architecture

- The third piece of a network management architecture is the **network management protocol.**

- **The protocol runs between the managing entity and the managed** devices, allowing the managing entity to query the status of managed devices and indirectly take actions at these devices via its agents.

Infrastructure for network management

definitions:



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

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

Management information base (MIB):

- **Definitions of *network management objects, known as MIB objects.***

- *In the Internet*- Standard Management Framework, management information is represented as a collection of managed objects that together form a virtual information store, known as the Management Information Base (MIB).

Management information base (MIB):

- An MIB object might be a counter, such as the number of IP datagrams discarded at a router due to errors in an IP datagram header,

- or the number of carrier sense errors in an Ethernet interface card; descriptive information such as the version of the software running on a DNS server;

- status information such as whether a particular device is functioning correctly; or protocol-specific information such as a routing path to a destination.
- MIB objects thus define the management information maintained by a managed device.
- Related MIB objects are gathered into **MIB modules.**

Structure of Management Information: SMI

- The language used to define the management information residing in a managed- network entity.
- Such a definition language is needed to ensure that the syntax and semantics of the network management data are well defined and unambiguous.

SMI: data definition language

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

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

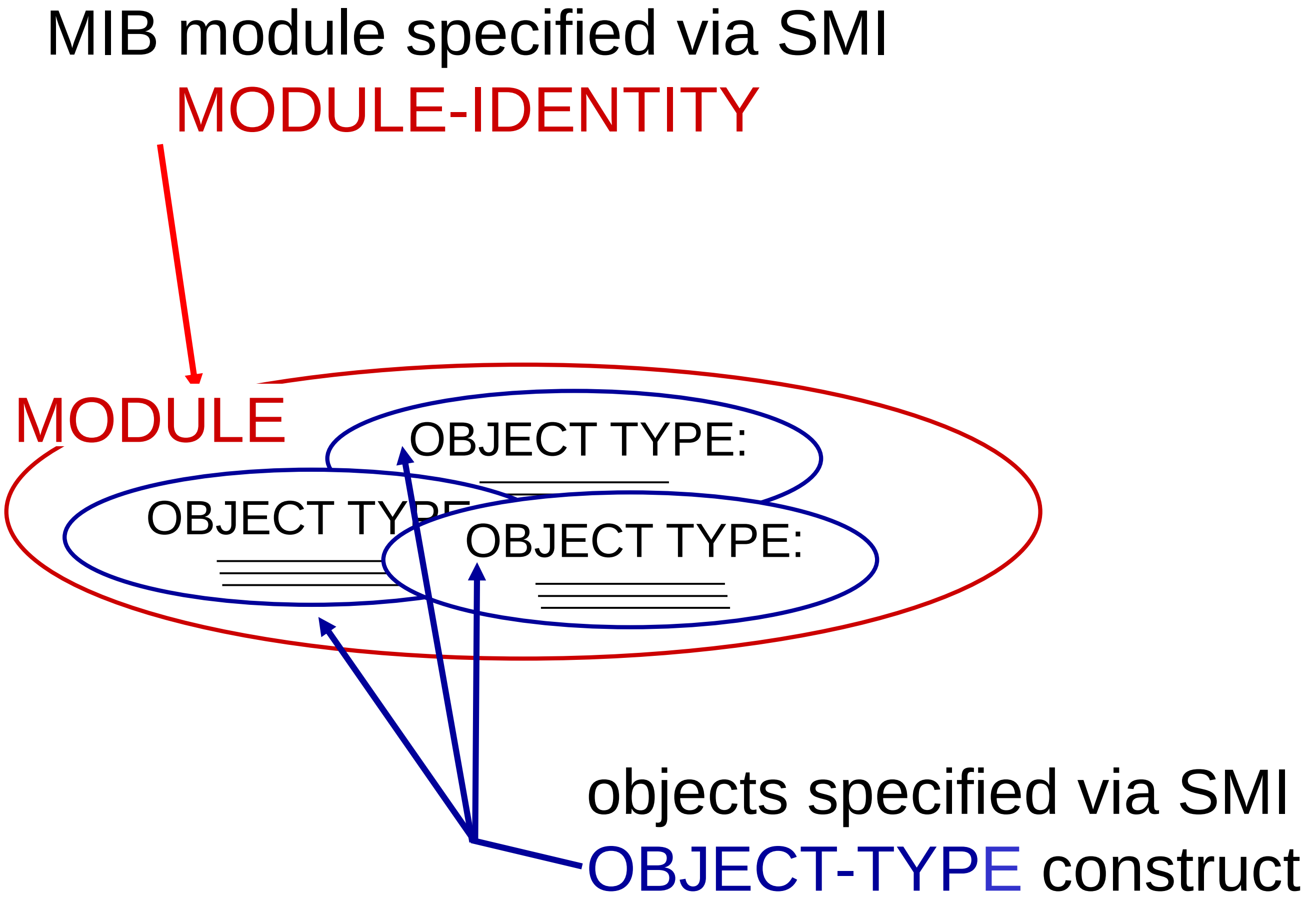
Basic Data Types

INTEGER
Integer32
Unsigned32
OBJECT IDENTIFIED
IPaddress
Counter32
Counter64

Data Type	Description
INTEGER	32-bit integer, as defined in ASN.1, with a value between -2^{31} and $2^{31} - 1$ inclusive, or a value from a list of possible named constant values.
Integer32	32-bit integer with a value between -2^{31} and $2^{31} - 1$ inclusive.
Unsigned32	Unsigned 32-bit integer in the range 0 to $2^{32} - 1$ inclusive.
OCTET STRING	ASN.1-format byte string representing arbitrary binary or textual data, up to 65,535 bytes long.
OBJECT IDENTIFIER	ASN.1-format administratively assigned (structured name); see Section 9.3.2.
IPaddress	32-bit Internet address, in network-byte order.
Counter32	32-bit counter that increases from 0 to $2^{32} - 1$ and then wraps around to 0.
Counter64	64-bit counter.
Gauge32	32-bit integer that will not count above $2^{32} - 1$ nor decrease beyond 0 when increased or decreased.
TimeTicks	Time, measured in 1/100ths of a second since some event.
Opaque	Uninterpreted ASN.1 string, needed for backward compatibility.

Table 9.1 ▲ Basic data types of the SMI

SNMP MIB



MIB module specified via SMI
MODULE-IDENTITY

objects specified via SMI
OBJECT-TYPE construct

MIB example: UDP module

Object ID	Name	Type	Comments
1.3.6.1.2.1.7.1	UDPInDatagrams	Counter32	total # datagrams delivered at this node
1.3.6.1.2.1.7.2	UDPNoPorts	Counter32	# underliverable datagrams: no application at port
1.3.6.1.2.1.7.3	UDInErrors	Counter32	# undeliverable datagrams: all other reasons
1.3.6.1.2.1.7.4	UDPOutDatagrams	Counter32	# datagrams sent

SNMP protocol

- **The Simple Network Management Protocol** is used to convey MIB information among managing entities and agents executing on behalf of managing entities.

- The most common usage of SNMP is in a **request-response mode in which an SNMP managing entity sends a request to an SNMP agent,** who receives the request, performs some action, and sends a reply to the request

SNMP protocol

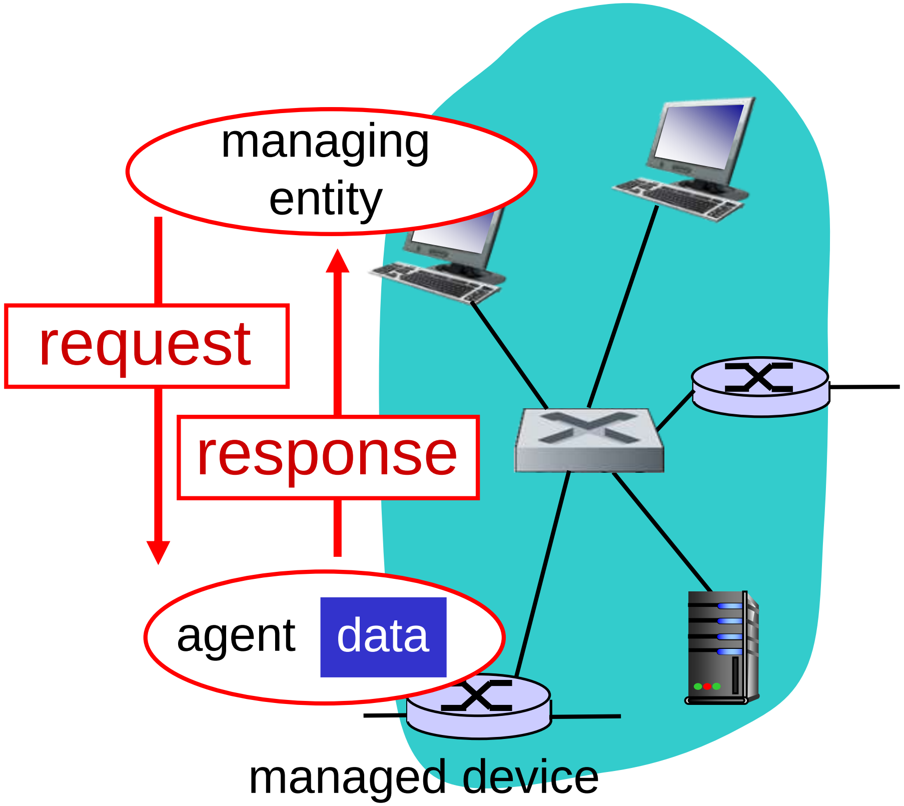
- Typically, a request will be used to query (retrieve) or modify (set) MIB object values associated with a managed device.

- A second common usage of SNMP is for an agent to send an unsolicited message, known as a **trap message, to a managing entity.**

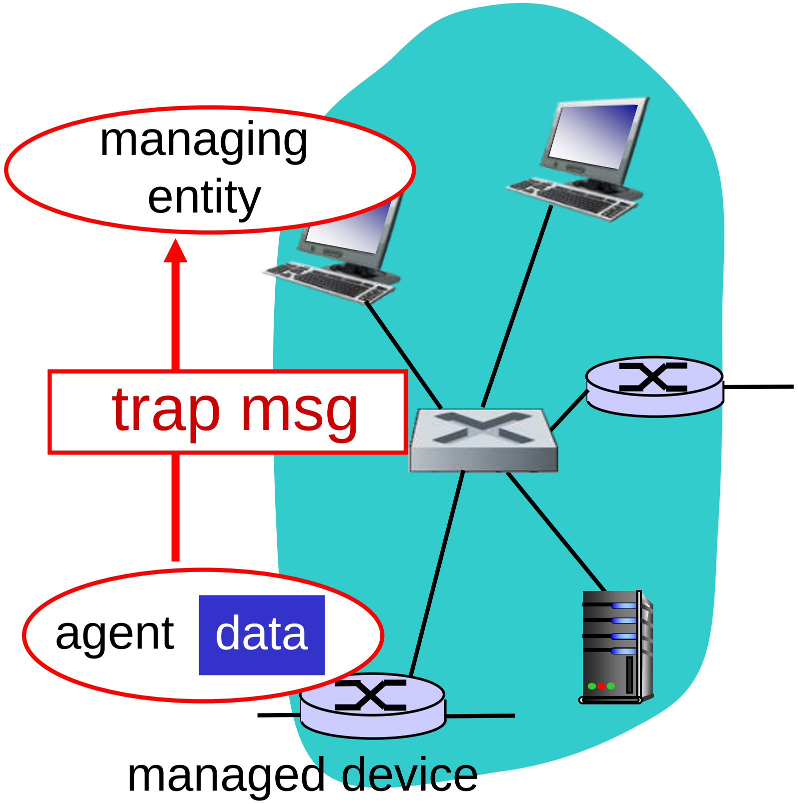
- **Trap** messages are used to notify a managing entity of an exceptional situation that has resulted in changes to MIB object values.

SNMP protocol

Two ways to convey MIB info, commands:



request/response mode



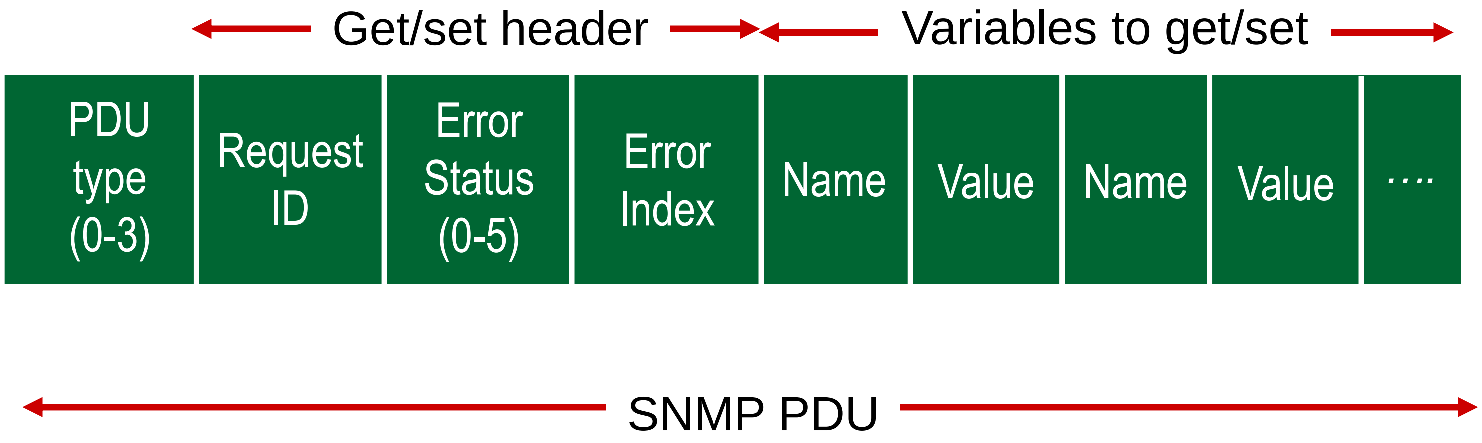
trap mode

SNMP protocol: message types

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

SNMP protocol: message formats

SNMPv2 defines seven types of messages, known generically as protocol data units—PDUs—



Get/set header

Variables to get/set

PDU type (0-3)	Request ID	Error Status (0-5)	Error Index	Name	Value	Name	Value	….

SNMP PDU

SNMP protocol: message formats

- The GetRequest, GetNextRequest, and GetBulkRequest PDUs are all sent from a managing entity to an agent to request the value of one or more MIB objects at the agent's managed device.

- The object identifiers of the MIB objects whose values are being requested are specified in the variable binding portion of the PDU.
- GetRequest, GetNextRequest, and GetBulkRequest differ in the granularity of their data requests.

- GetRequest can request an arbitrary set of MIB values;

SNMP protocol: message formats

- Multiple GetNextRequests can be used to sequence through a list or table of MIB objects;

- GetBulkRequest allows a large block of data to be returned, avoiding the overhead incurred if multiple GetRequest or GetNextRequest messages were to be sent.

- In all three cases, the agent responds with a Response PDU containing the object identifiers and their associated values.

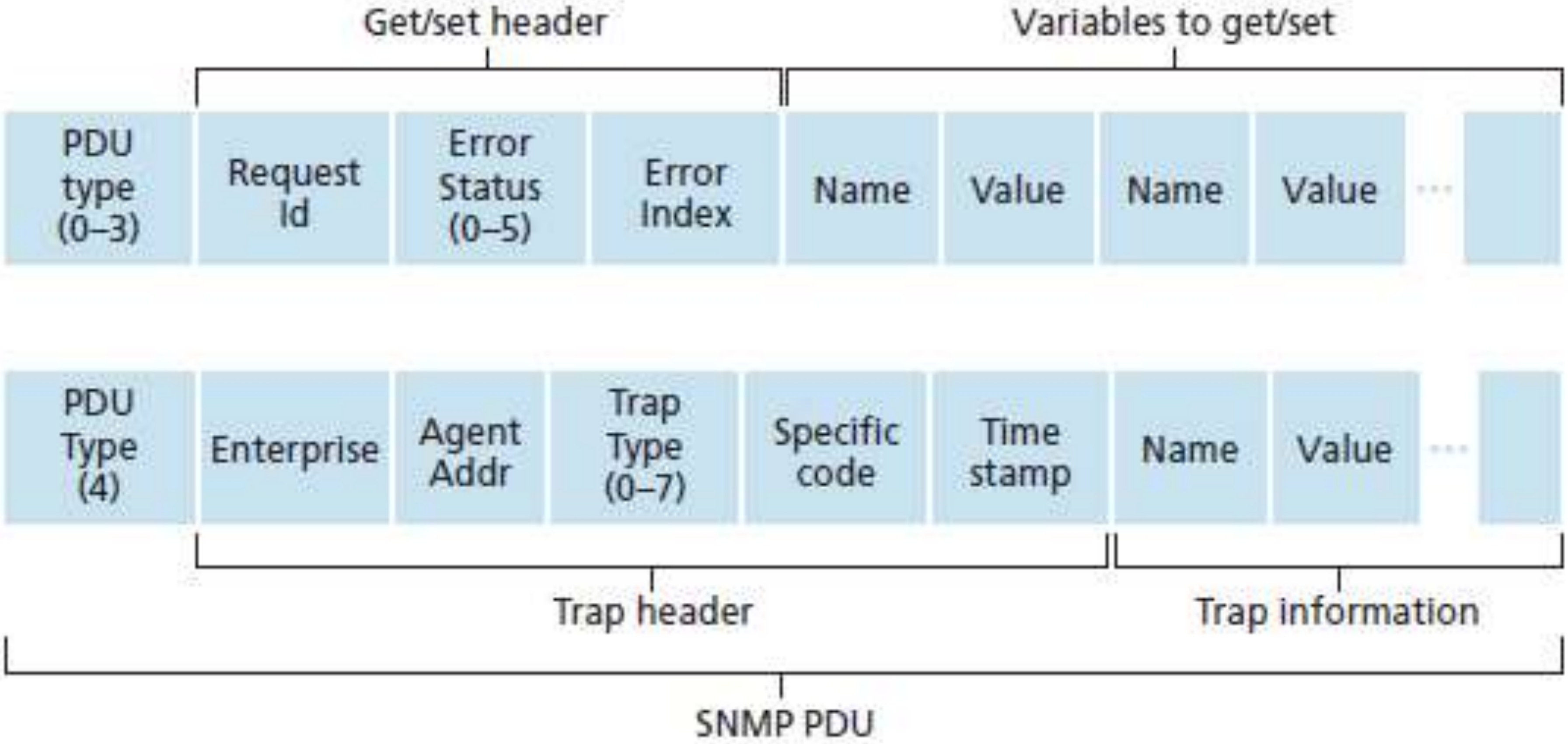


Figure 9.4 ♦ SNMP PDU format

SNMP protocol: message formats

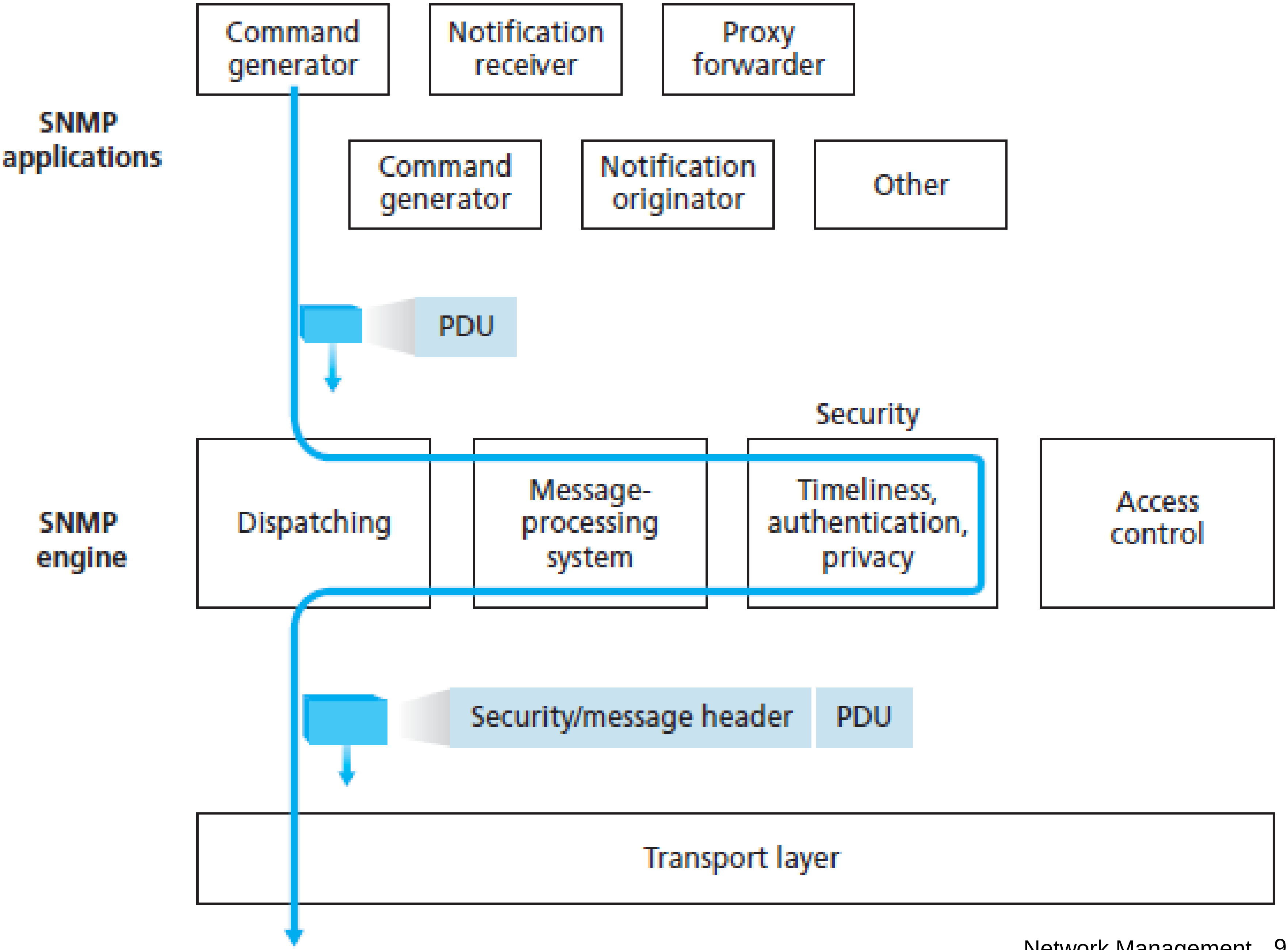
- The SetRequest PDU is used by a managing entity to set the value of one or more MIB objects in a managed device.

- An agent replies with a Response PDU with the “noError” error status to confirm that the value has indeed been set.

- SNMP PDUs can be carried via many different transport protocols, the SNMP PDU is typically carried in the payload of a UDP datagram.

Security and Administration

- The designers of SNMPv3 have said that "SNMPv3 can be thought of as SNMPv2 with additional security and administration capabilities"
- SNMPv3 provides for encryption, authentication, protection against playback attacks and access control.


SNMP applications
Command generator
Notification receiver
Proxy forwarder
Command generator
Notification originator
Other
PDU
Security
SNMP engine
Dispatching
Message-processing system
Timeliness, authentication, privacy
Access control
Security/message header
PDU
Transport layer

- *Encryption.* SNMP PDUs can be encrypted using the Data Encryption Standard (DES) in Cipher Block Chaining (CBC) mode.
- • *Authentication.* SNMP uses the Message Authentication Code (MAC) technique
- • *Protection against playback.* Nonces can be used to guard against playback attacks.
- • *Access control.* SNMPv3 provides a view-based access control that controls which network management information can be queried and/or set by which users.