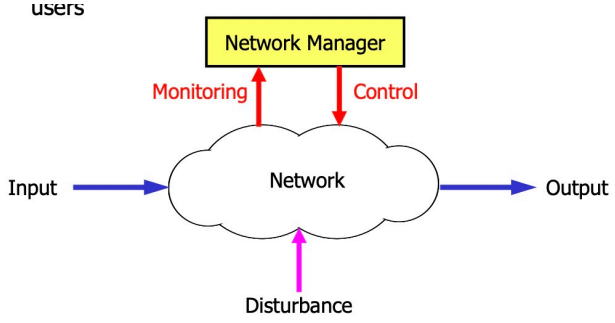
SNMP

Network Management
Definition: a service that employs a variety of tools, applications, and devices to assist human network managers in monitoring and maintaining networks
Goal: ensure data to go across it with maximum efficiency and transparency to the users



Functional Areas (ISO defined): FCAPS
Fault, Configuration, Accounting, Performance, Security

Fault management: locating problems/faults
Discover the problem, isolate the problem, fix the problem

Configuration management: finding and setting up critical devices

Accounting management: tracking individual's utilization

Performance management: measuring the performance of the network hardware, software and media

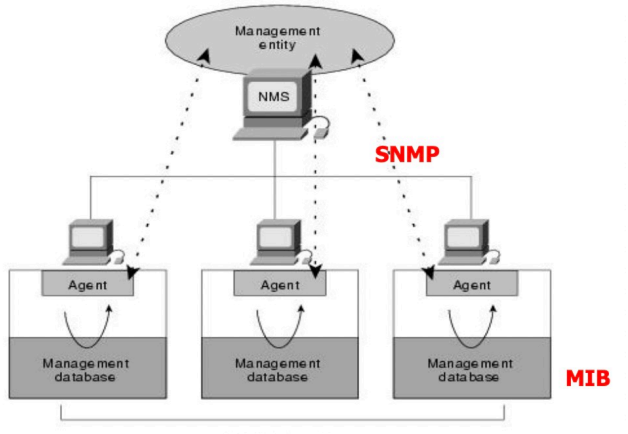
Security management:
- Controlling access to information on the data network
- Monitor access points and records information on a periodic basis
- Audit trails and sounds alarms for security breaches

Network Management protocol: SNMP

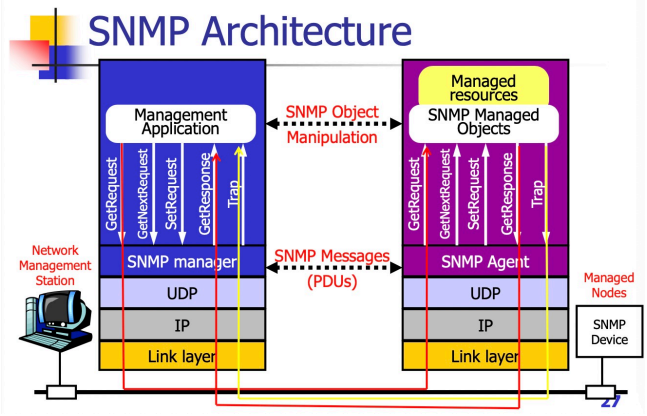
SNMP
SNMP: an application layer protocol that provides a way of monitoring and managing a heterogeneous computer network
Based on client/server model, UDP
Well-known ports
- UDP Port 161: SNMP Get/Set Messages
- UDP Port 162: SNMP Trap Messages

SNMP v.s. Network Management
SNMP does not cover all the function areas of network management (F-C-P only)
Network management — systematic work; SNMP — tool and protocol

The SNMP **model**
consists of four components:
- Managed Nodes (Agent)
- Management Stations (NMS) — network management station
- Management Information (MIB) — management information base
- A Management Protocol (SNMP)



SNMP Architecture



SNMP Network Management **Framework**
SMI: structure of management information
- Data definition language for MIB objects

SNMP protocol: convey information, commands between manager — managed object

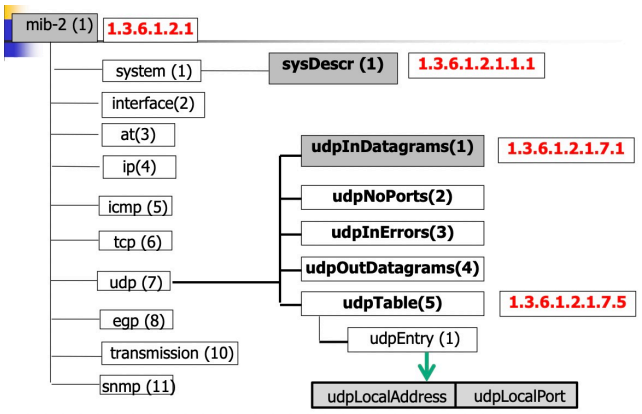
SMI and ASN.1
SMI: structure of management information
SMI作用: defines the rules for describing management information
SMI is a subset of ASN.1

ASN.1
An international standard defining the data structure used and how these are transferred between systems

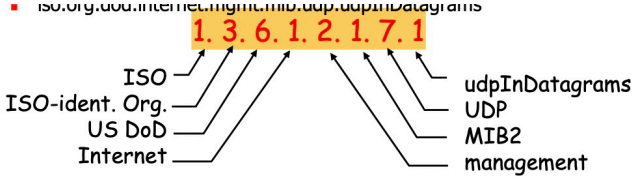
MIBs are written using ASN.1 and must adhere to SMI

MIB: management information base
MIB: a collection of information that is organized hierarchically
• MIBs are comprised of managed objects, identified by OIDs (object identifiers)
Two types of managed objects (2)
• Scalar objects: define a single object instance
• Tabular objects: define multiple related object instances that are grouped in MIB tables
SMI: data definition language for MIB objects

SMI MIB



MIB — Naming
Each objects has a unique OID consign of numbers separated by decimal points, and a more readable name

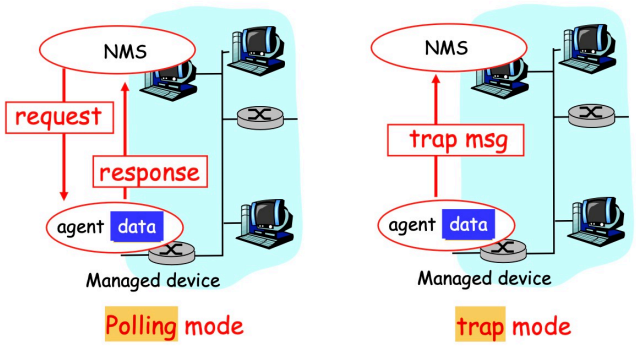


过程
SNMP manager: want to know the value of an object, GetRequest packet that includes the OID for that objects
The agent: receives the request and looks up the OID in its MIB, response packet contains the value of the object, if not found, special error response is sent

MIB two parts:
A textual part: objects paced into groups
A MIB module: objects are described solely in terms of OBJET-TYPE (data type, status, semantics of managed objet)

SNMP Protocol
• SNMP traps/polling
• SNMP commands

SNMP Traps/Polling
Two ways to deliver MIB information, commands (两种模式)

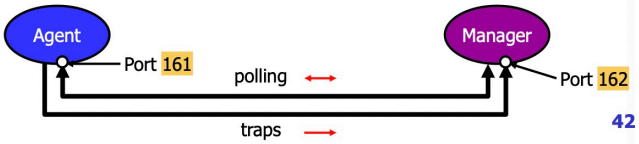


Polling: request/response
Trap: trap msg from agent (主动上报)

Traps
When abnormal event occurs, an agent sends a trap message to NMS
- Trap indicates error type, network device name, which objects should be queried
- Keep the message short and simple

NMS then query the agent for more information
NMS must be listening for TRAP messages

Polling
The NMS periodically queries the network devices for information
- The advantage is NMS is in control and knows the "big picture"
- The disadvantage is the amount of delay (delay: when an event occurs to when it's noticed) —> 不能及时被发现

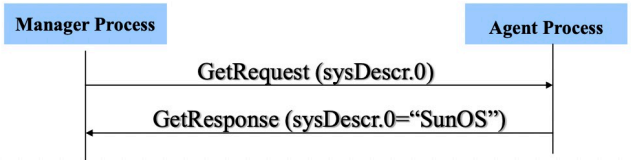


Traps: server port 162 (request from NMS, response from agent)
Polling: agent port 161 (request from agent)

SNMP Commands

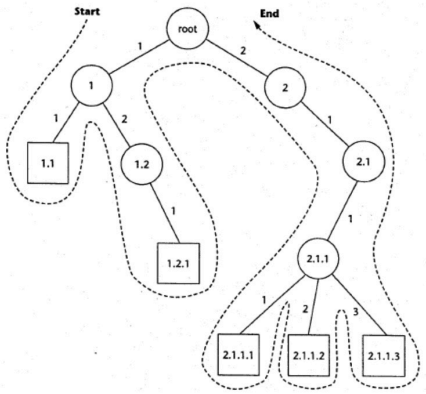
Command	Description	Version
GetRequest	NMS-to-Agent: get data (instance)	SNMPv1
GetNextRequest	NMS-to-Agent: get data (next in list)	SNMPv1
GetBulkRequest	NMS-to-Agent: get data (block)	SNMPv2
InformRequest	NMS-to-NMS: MIB information exchange	SNMPv2
SetRequest	NMS-to-Agent: set MIB value	SNMPv1
GetResponse	Agent-to-NMS: value, response to request	SNMPv1
Trap	Agent-to-NMS: report exceptional event to NMS	SNMPv1

GetRequest [Get]: use to ask SNMP agent for value of a particular MIB agent, NMS sends out 1 Get PDU for each instance, which is a unique OID string

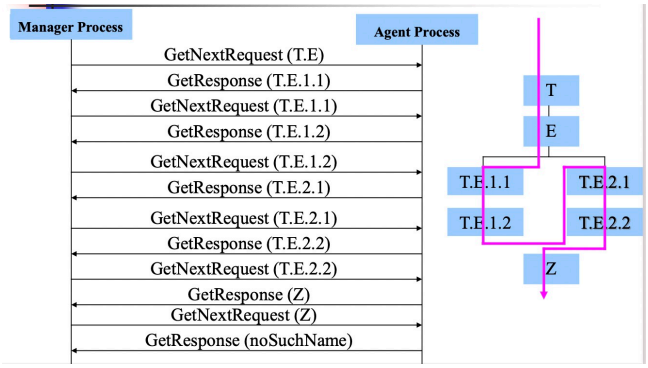


GetNextRequest: retrieves the NEXT variable instance existing on the agent in the tree of objects, it will returns the next existing object, or error if none
作用: traverse any part or all of the objects present on an agent
Start from known mandatory **sysDescr** object, a NMS can find all the others
Simple, powerful mechanism

Lexicographic ordering



snmpwalk: an SNMP application using SNMP GetNextRequest to query a network entity for a tree of information



SNMPv3: security and administration
- Encryption
- Authentication
- Protection against playback
- Access control

SNMP (summary)
SNMP: simple network management protocol —> monitor and manage the heterogeneous computer network

MIB: Management information base —> a collection of information that is organized hierarchically

SMI: structure of management information —> define the rules for describing management information

SNMP
Definition: assist human managers to monitor and manage network
Goals: ensure data to go with maximum efficiency and transparency to users
Functional areas: FCAPS
- Fault: discover, isolate, fix
- Configuration: set up critical devices
- Accounting: track user's utilization
- Performance: measure performance of network
- Security: 1. Control access to information 2. Monitor access points 3. Audit trails and sounds alarm for security breaches

SNMP features
1. Application layer protocol
2. Based on UDP, client/server model
3. Ports: 1. Polling (client: 162), 2. Trap (server: 161)

SNMP v.s. Management
1. SNMP —> F-C-P not all functions

SNMP Model (4 component)
1. Agent — managed nodes
2. NMS — network management station
3. MIB — management information base
4. SNMP — a management protocol

SNMP framework
SMI: data definition language for MIB objects, define the rules for describing management information
SMI and ASN.1: SMI is a subset of ASN.1

MIB: a collection of information that is organized hierarchically
MIB comprised of managed objects and are identified by OIDs
Managed objects (2)
- Scalar object
- Tabular object

MIB — naming
Each object has a unique OID consisting of numbers separated by decimal points, and a more readable name

Want to know the value of an object
SNMP manager: send a GetRequest packet that includes the OID for the object
SNMP agent: receives the request and looks up the OID in its MIB.

MIB Definition (two parts): textual part, MIB module

SNMP Protocol
Two ways to deliver MIB information, commands (2):
- Polling mode
- Trap mode

Traps (server: 162)
- When abnormal event occurs, an agent sends a trap message to nominated NMS(s)
- Short and simple
- NMS must be listening for TRAP message

Polling (client: 161)
- The NMS queries the network devices for information
- The advantage: NMS is control and knows the "big picture"
- The disadvantage: amount of delay (event occurs, event detect)

Commands
- NMS-to-Agent: GetRequest, GetNextRequest, GetBulkRequest, SetRequest
- NMS-to-NMS: InformRequest
- Agent-to-NMS: GetResponse, Trap

GetNextRequest: retrieves the next variable instance
作用: traverse any part or all of the objects (start from the known mandatory: ***sysDescr*** object)
snmpwalk: an SNMP application using SNMP GetNextRequest to query a network entity for a tree of information