Simple Network Management Protocol

Introduction

- SNMP – Simple Network Management Protocol
  - A set of standards for network management
    - Protocol
    - Database structure specification
    - Data objects
  - A set of standardized tools that
    - Control costs of network management
    - Across various product types
      - End system, bridges, routers, telecommunications, …
- History
  - In 1989
    - SNMP was adopted as TCP/IP-based Internet standards
  - In 1991
    - RMON – Remote network MONitoring
    - Supplement to SNMP to include management of LAN and LAN devices
  - In 1995
    - SNMPv2
      - Functional enhancements to SNMP
      - SNMP on OSI-based networks
    - RMON2
  - In 1998
    - SNMPv3
      - Further enhancements
      - Security capability for SNMP

Requirements of Network Management

- Fault Management
  - Detect, isolate, reconfigurate and repair the abnormal network environment
  - Problem tracking and control
    - Problem is truly resolved and no new ones are introduced
- Accounting Management
  - Track the use of network resources by end user to provide
    - Impropriate usage tracing, charging, statistics
- Configuration and Name Management
  - Startup, shutdown, reconfigure network component when
    - Upgrade, fault recovery or security checks
- Performance Management
  - Capacity utilization, throughput, response time, bottleneck
    - Collect information and assess current situation
- Security Management
  - Information protection and access control

Network Management System (1)

- A collection of tools for
  - Network monitoring
  - Network control

- These tools must be integrated
  - Single operator interface with powerful but user-friendly
  - Support of managed equipments.

Network Management System (2)

- Architecture of NMS
  - NMA
    - Operator interface
  - NME
    - Collect statistics
    - Response to NMA
    - Alert NMA when environment changing

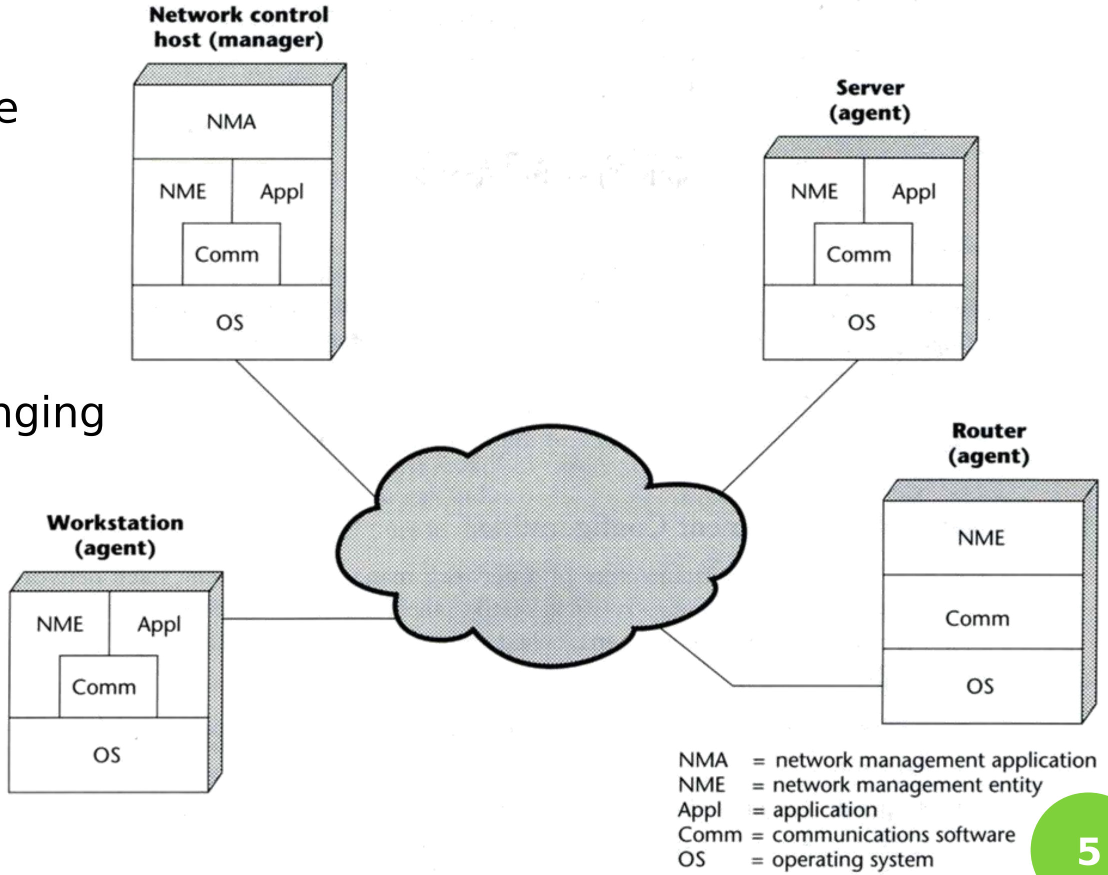
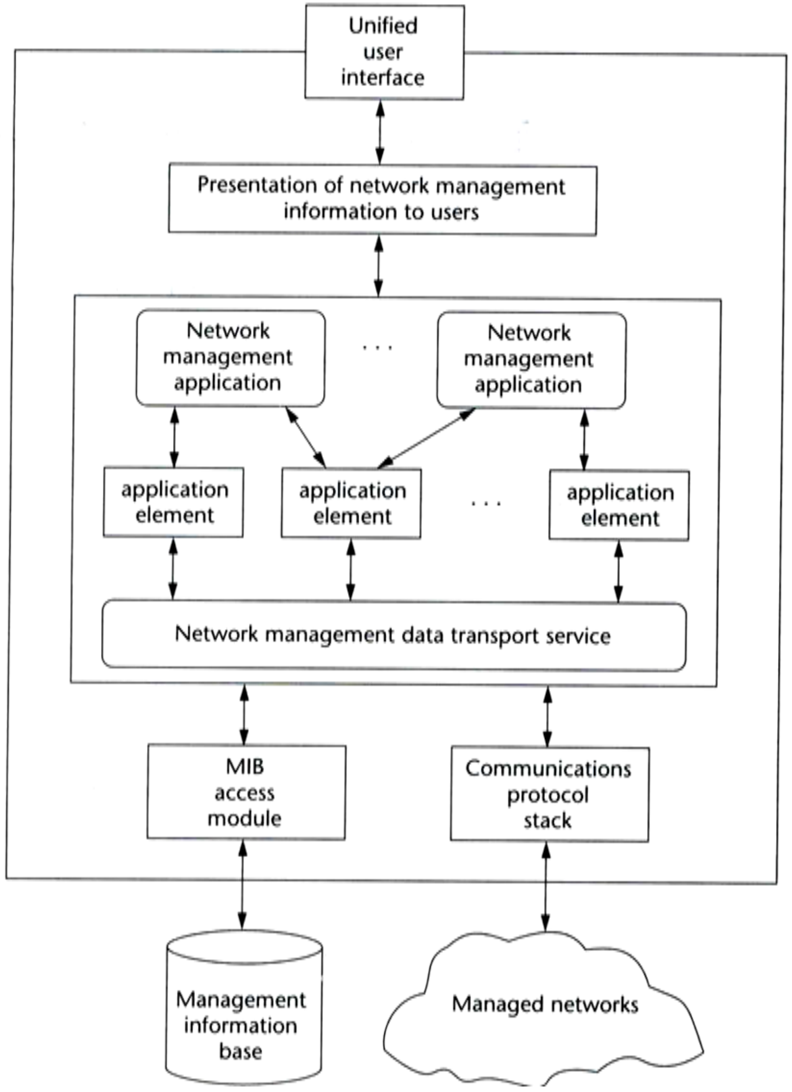


FIGURE 1.1 Elements of a network management system

NETWORK MANAGEMENT SOFTWARE

- Architecture
  - Presentation SW
    - Unified interface and handle information overload
  - Network Management SW
    - NM applications
      - Admin interested tools
      - Fault, security, accounting management
    - Application element
      - Primitive and general-purpose NM functions
      - Generating alarm, summarizing data
  - Communication SW
    - Exchange management information
    - Communication protocol stack
  - Database SW
    - MIB (Management Information Base)
      - Configuration and behavior
      - Operation parameters
    - MIB access modules
      - Convert local MIB to standard form



SNMP Network Management Concepts

In that time ..

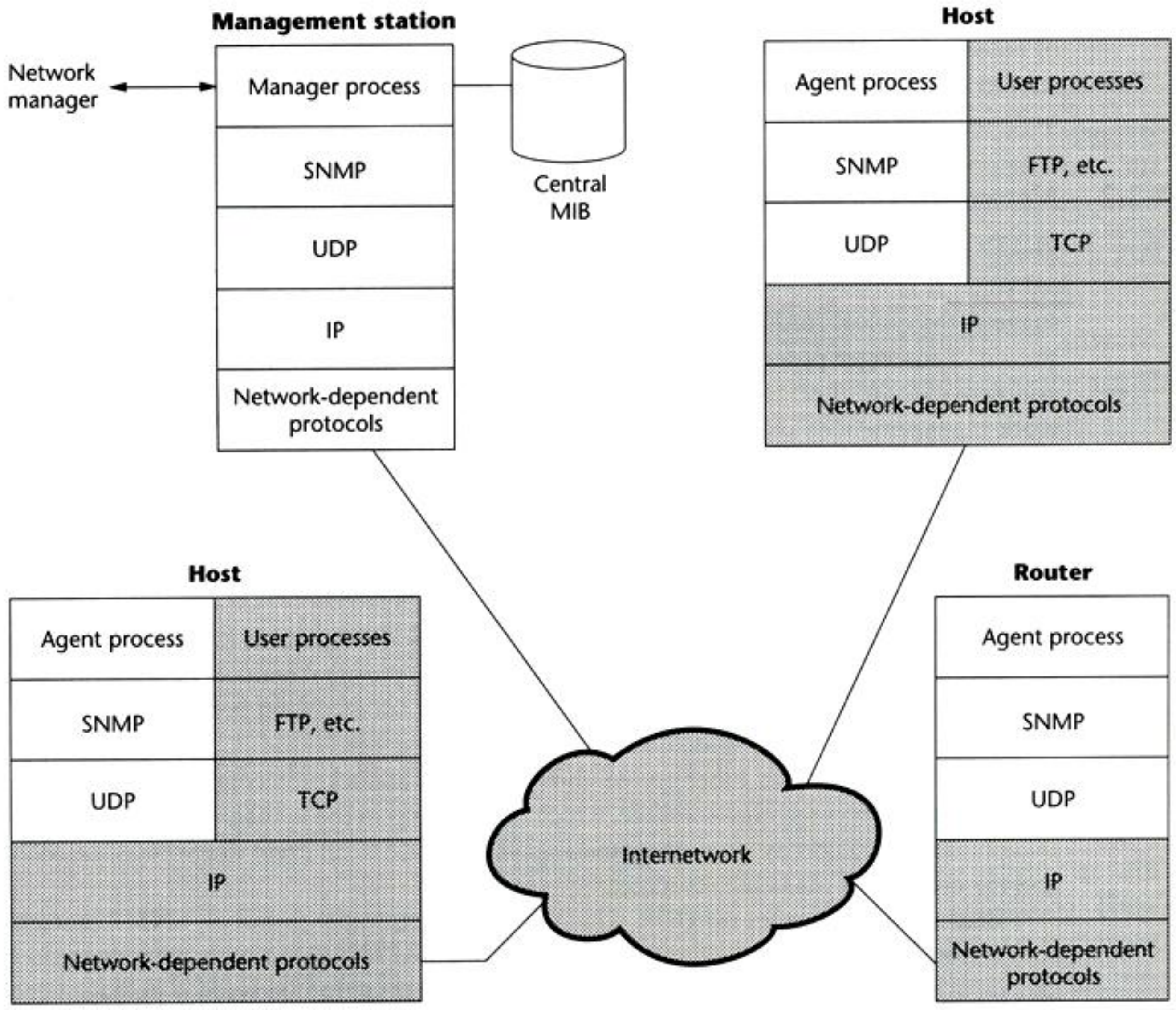
- Network environment is simple
  - ICMP is the only way to do network investigation
    - ping, traceroute, ...

- As Internet goes popular, three approaches are proposed:
  - HEMS: High-level Entity Management System
    - Considered to be the first network management tools
  - SGMP and SNMP
    - SNMP was an enhanced version of the Simple Gateway Management Protocol
    - For TCP/IP-based network management standards
    - Supposed to be short-term solution
  - CMIP over TCP/IP (CMOT)
    - Common Management Information Protocol
    - For ISO-based network management standards
    - Supposed to be long-term solution

Network Management Architecture in SNMP (1)

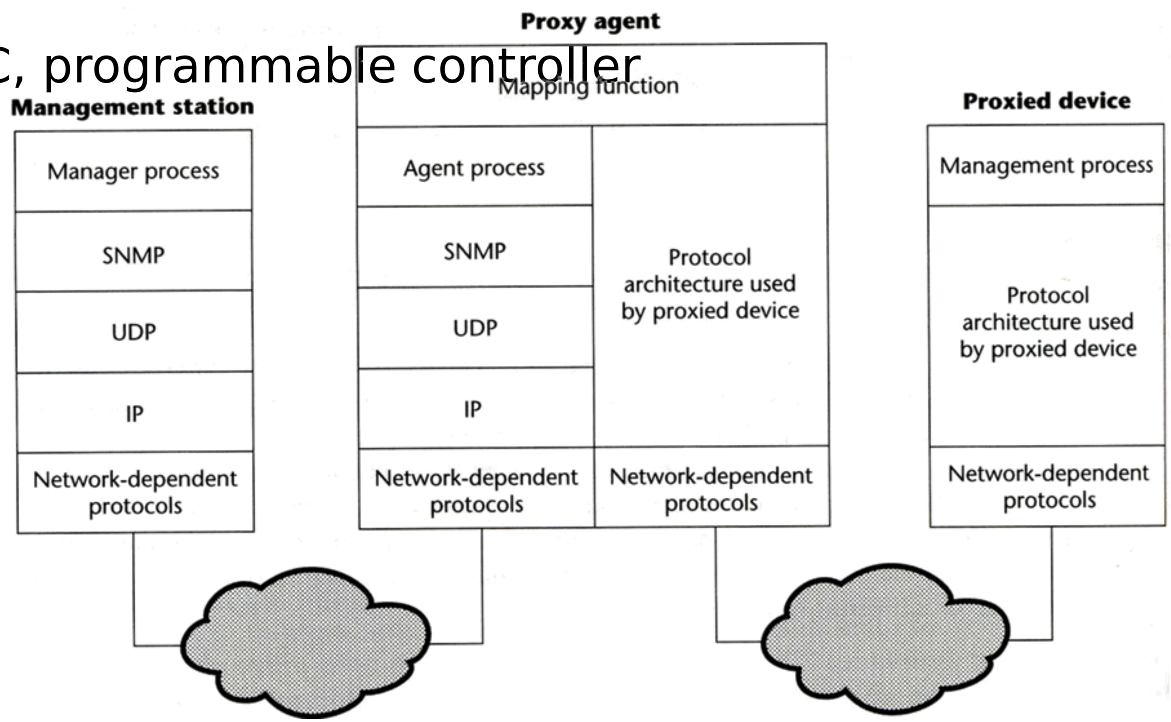
- 4 key elements
  - Management Station
    - Serve as the interface between manager and devices
      - Management applications
      - User-friendly interface
      - Translate manager’s requirements into actual monitoring or control operations
      - Database extracted from MIBs of all managed device
  - Management Agent
    - Respond to request from management station
    - Change settings in MIB of managed device
    - Asynchronously report abnormal event (Trap)
  - Management Information Base (MIB)
    - Each resource is represented as an object and
    - MIB is a collection of objects
  - Network Management Protocol
    - get, set, trap

Network Management Architecture in SNMP (2)



Network Management Architecture in SNMP (3)

- SNMP proxy
  - Devices that do not support UDP/IP
    - ex: Bridge, Modem
  - Devices that do not want to add burden of SNMP agent
    - ex: PC, programmable controller



SNMP Message Information

- Message Information Base (MIB)
  - Collection of objects and
  - Each object represents certain resource of managed device
- Interoperability of MIB
  - Object that represents a particular resource should be the same cross various system
    - What objects
    - MIB-I and MIB-II
  - Common representation format
    - SMI (Structure of Management Information)

SNMP Message Information – SMI (1)

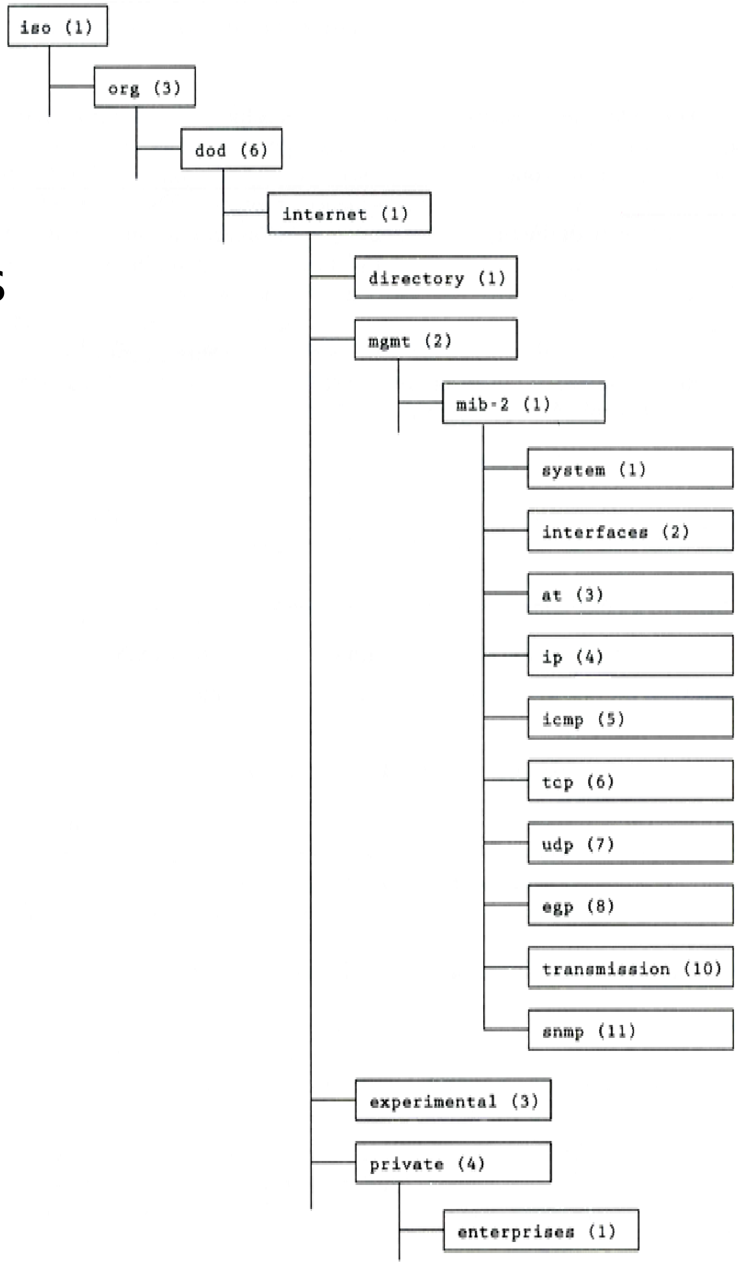
- SMI (RFC 1155)
  - Structure of Management Information
  - Identify the data type that can be used in MIB and how resources are represented and named, including
    - MIB structure
    - Syntax and value of each object
    - Encoding of object value

SNMP Message Information – SMI (2)

- MIB structure
  - Rooted tree
    - The leaves are the actual managed objects
    - Each object has an identifier (OBJECT IDENTIFIER)
      - Number with dot as delimiter
    - The internet node
      - iso -> org -> dod -> internet
      - object identifier of internet node: 1.3.6.1
    - Under internet node
      - directory :OSI X.500 directory
      - **mgmt: used for objects defined in IAB (Internet Activities Board)**
      - experimental: used for internet experiments
      - private: unilaterally usage

SNMP Message Information – SMI (3)

- MIB Tree
- Define additional objects
  - Under mib-2
  - Under experimental
  - Under enterprises



SNMP Message Information – Object Syntax (1)

- Definition of object
  - Data type
    - Application-independent type (UNIVERSAL type)
      - integer, octetstring, null, object identifier, sequence
    - Application-wide types (RFC 1155)
      - Networkaddress → IP Address
      - counter (0 ~ 2^{32} -1), increasing only, wrap to 0
      - gauge (0 ~ 2^{32} -1)
      - timeticks
      - opaque (encoded as OCTET STRING for transmission)
      - threshold
  - Value ranges
  - Relationship with other objects in MIB

SNMP Message Information – Object Syntax (2)

- ANS.1
  - Abstract Syntax Notation One
  - A formal language developed by CCITT and ISO
  - In SNMP, we use macro to define other types used to define managed objects
    - Macro definition (template)
    - Macro instance (particular type)
    - Macro instance value

SNMP Message Information – Object Syntax (3)

- OBJECT-Type macro

```
IMPORTS   ObjectName, Object Syntax FROM RFC-1155-SMI

OBJECT-TYPE MACRO ::=
BEGIN
     TYPE NOTATION ::=   "SYNTAX"   type (TYPE ObjectSyntax)
                         "ACCESS"   Access
                         "STATUS"   Status
                         DescrPart
                         ReferPart
                         IndexPart
                         DefValPart
     VALUE NOTATION ::= value (VALUE ObjectName)

     Access ::= "read-only"|"read-write"|"write-only"|"not-accessible"

     Status ::= "mandatory"|"optional"|"obsolete"|"deprecated"

     DescrPart ::= "DESCRIPTION" value (description DisplayString)|empty

     ReferPart ::= "REFERENCE" value (reference DisplayString)|empty

     IndexPart ::= "INDEX" "{" IndexTypes "}"

     IndexTypes ::= IndexType|IndexTypes "," IndexType

     IndexType ::= value (indexobject ObjectName)  --if indexobject, use the SYNTAX
                                                   --value of the correspondent
                                                   --OBJECT-TYPE invocation
                   |type (indextype)               --otherwise use named SMI type:
                                                   --must conform to IndexSyntax below

     DefValPart ::= "DEFVAL" "{" value (defvalue ObjectSyntax) "}" |empty

     DisplayString ::= OCTET STRING SIZE (0..255)

END

IndexSyntax ::= CHOICE { number INTEGER (0..MAX),
                         string OCTET STRING,
                         object OBJECT IDENTIFIER,
                         address NetworkAddress,
                         IpAddress IpAddress }
```

SNMP Message Information – Object Syntax (4)

- Example of object definition
  - iso.org.dod.internet.mgmt.mib-2.tcp.tcpMaxConn
  - 1.3.6.1.2.1.6.4

```
tcpMaxConn OBJECT-TYPE
     SYNTAX INTEGER
     ACCESS read-only
     STATUS mandatory
     DESCRIPTION
         "The limit on the total number of TCP connections the entity can
         support. In entities where the maximum number of connections is
         dynamic, this object should contain the value -1."
     ::= { tcp 4 }
```

SNMP Message Information – Object Syntax (5)

- 2-D table
  - Two-dimensional array with scalar-valued entries
  - Ex: tcpConnTable (RFC1213)

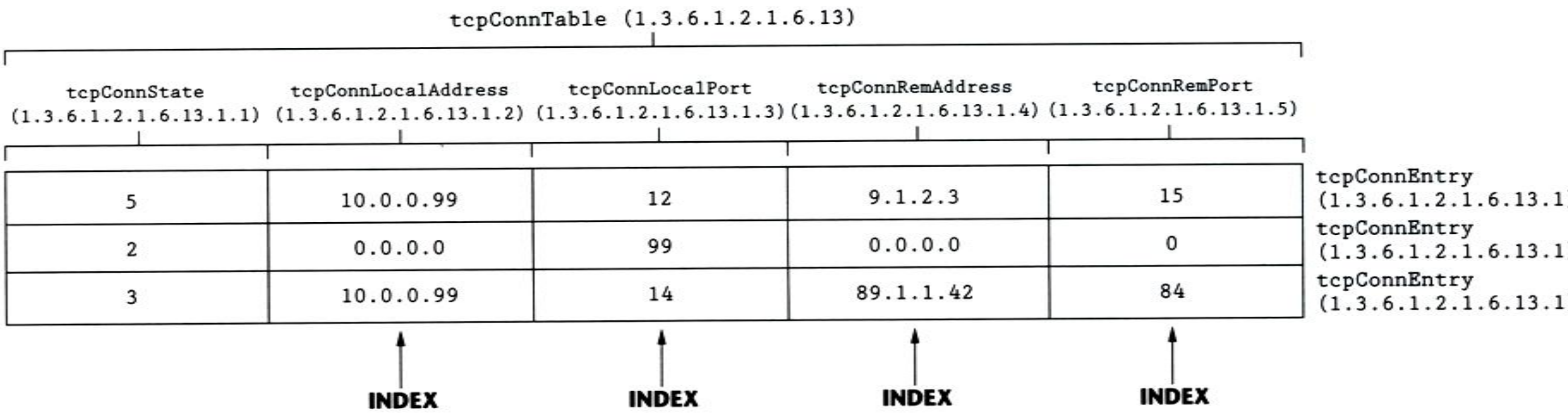
```
tcpConn Table OBJECT-TYPE
        SYNTAX   SEQUENCE OF TcpConnEntry
        ACCESS   not-accessible
        STATUS   mandatory
        DESCRIPTION
              "A table containing TCP connection-specific information."
        ::= { tcp 13 }

tcpConnEntry OBJECT-TYPE
       SYNTAX    TcpConnEntry
       ACCESS    not-accessible
       STATUS    mandatory
       DESCRIPTION
              "Information about a particular TCP connection. An object of this type is
              transient, in that it ceases to exist when (or soon after) the connection
              makes the transition to the CLOSED state."
       INDEX     { tcpConnLocalAddress,
                   tcpConnLocalPort,
                   tcpConnRemAddress,
                   tcpConnRemPort }
       ::= { tcpConnTable 1 }

TcpConnEntry ::= SEQUENCE { tcpConnState INTEGER,
                            tcpConnLocalAddress IpAddress,
                            tcpConnLocalPort INTEGER (0..65535),
                            tcpConnRemAddress IpAddress
                            tcpConnRemPort INTEGER (0..65535)}
```

SNMP Message Information – Object Syntax (6)

```
tcpConnState OBJECT-TYPE
      SYNTAX   INTEGER {closed (1),
                        listen (2),
                        synSent (3),
                        synReceived (4),
                        established (5),
                        finWait1 (6),
                        finWait2 (7),
                        closeWait (8),
                        lastAck (9),
                        closing (10),
                        timeWait (11),
                        delete TCB (12) }

      ACCESS      read-write
      STATUS      mandatory
      DESCRIPTION
            "The state of this TCP connection.
      ::= { tcpConnEntry 1 }

tcpConnLocalAddress OBJECT-TYPE
      SYNTAX      IpAddress
      ACCESS      read-only
      STATUS      mandatory
      DESCRIPTION
            "The local IP address for this TCP connection. In the case of a connec-
            tion in the listen state which is willing to accept connections for any
            IP interface associated with the node, the value 0.0.0.0 is used."
      ::= { tcpConnEntry 2 }

tcpConnLocalPort OBJECT-TYPE
      SYNTAX      INTEGER (0..65535)
      ACCESS      read-only
      STATUS      mandatory
      DESCRIPTION
            "The local port number for this TCP connection."
      ::= { tcpConnEntry 3 }

tcpConnRemAddress OBJECT-TYPE
      SYNTAX      IpAddress
      ACCESS      read-only
      STATUS      mandatory
      DESCRIPTION
            "The remote IP address for this TCP connection."
      ::= { tcpConnEntry 4 }

tcpConnRemPort OBJECT-TYPE
      SYNTAX       INTEGER (0..65535)
      ACCESS       read-only
      STATUS       mandatory
      DESCRIPTION
            "The remote port number for this TCP connection."
      ::= { tcpConnEntry 5 }
```

SNMP Message Information – Object Syntax (7)

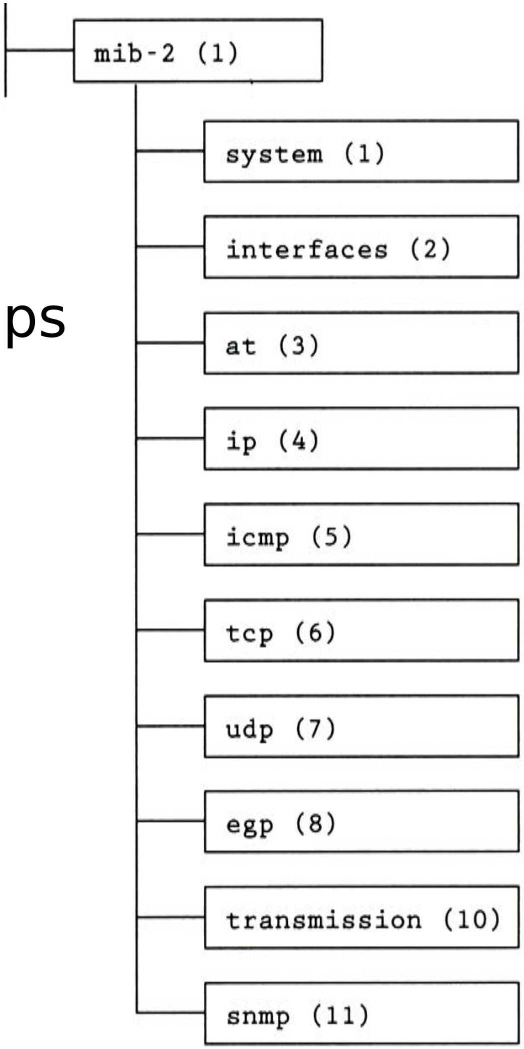
- iso (1) -> org (3) -> dod (6) -> internet (1) -> mgmt (2)
  - mib-2 (1) -> tcp (6) -> tcpConnTable(13)



Standard MIBs

MIB-II (1)

- RFC1213
  - MIB-I (RFC 1156)
  - MIB-II is a superset of MIB-I with some additional objects and groups



MIB-II (2)

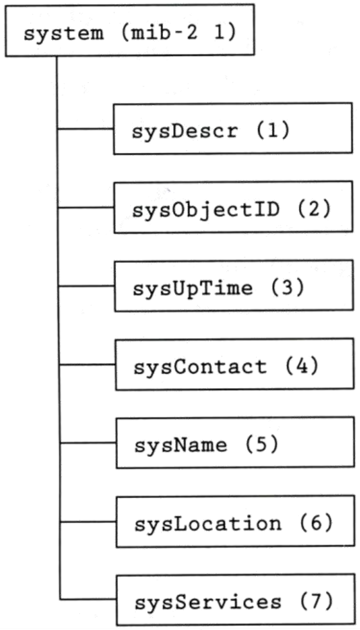
- First layer under mib-2
  - 1.3.6.1.2.1 (iso.org.dod.internet.mgmt.mib-2)

  - system
    - Overall information about the system
  - interfaces
    - Information about each interface
  - at
    - internet-to-subnet address mapping
  - ip, icmp, tcp, udp, egp
  - dot3
    - Transmission schemes and access protocol at each system interface
  - snmp

MIB-II

system group

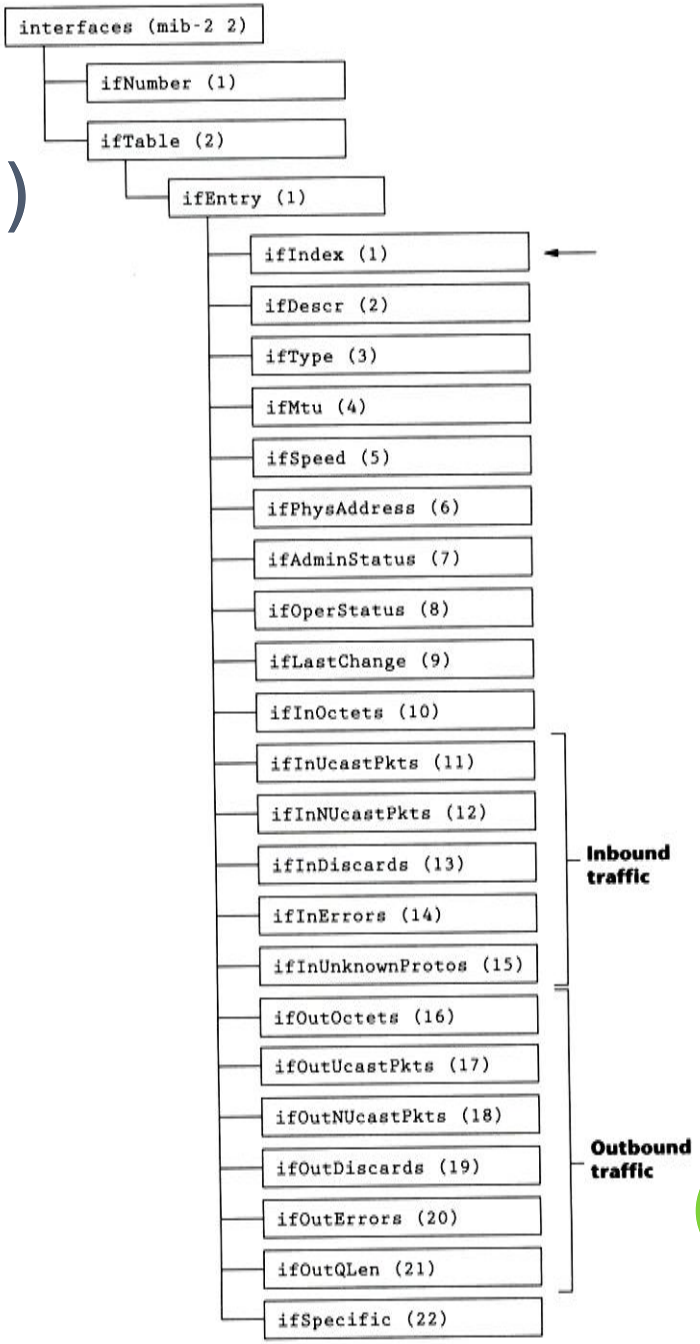
- sysServices
  - 1 physical (ex: repeater)
  - 2 datalink/subnetwork (ex: bridge)
  - 3 internet (ex: router)
  - 4 end-to-end (ex: IP hosts)
  - 7 applications (ex: mail relays)



Object	Syntax	Access	Description
sysDescr	DisplayString (SIZE (0 . . . 255))	RO	A description of the entity, such as hardware, operating system, etc.
sysObjectID	OBJECT IDENTIFIER	RO	The vendor's authoritative identification of the network management subsystem contained in the entity
sysUpTime	TimeTicks	RO	The time since the network management portion of the system was last reinitialized
sysContact	DisplayString (SIZE (0 . . . 255))	RW	The identification and contact information of the contact person for this managed node
sysName	DisplayString (SIZE (0 . . . 255))	RW	An administratively assigned name for this managed node
sysLocation	DisplayString (SIZE (0 . . . 255))	RW	The physical location of this node
sysServices	INTEGER (0 . . . 127)	RO	A value that indicates the set of services this entity primarily offers

MIB-II

INTERFACE GROUP (1)



MIB-II

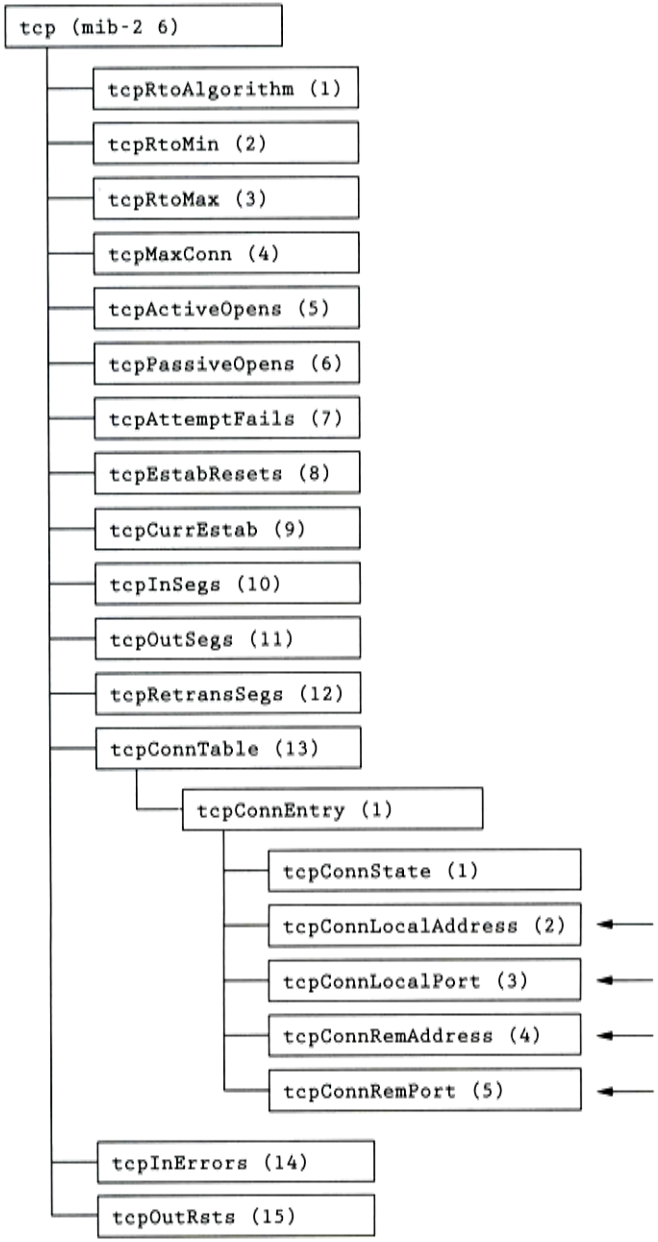
INTERFACE GROUP (2)

TABLE 6.2 interfaces Group Objects

Object	Syntax	Access	Description
ifNumber	INTEGER	RO	The number of network interfaces
ifTable	SEQUENCE OF ifEntry	NA	A list of interface entries
ifEntry	SEQUENCE	NA	An interface entry containing objects at the subnetwork layer and below for a particular interface
ifIndex	INTEGER	RO	A unique value for each interface
ifDescr	DisplayString (SIZE (0 . . . 255))	RO	Information about the interface, including name of manufacturer, product name, and version of the hardware interface
ifType	INTEGER	RO	Type of interface, distinguished according to the physical/link protocol(s)
ifMtu	INTEGER	RO	The size of the largest protocol data unit, in octets, that can be sent/received on the interface
ifSpeed	Gauge	RO	An estimate of the interface's current data rate capacity
ifPhysAddress	PhysAddress	RO	The interface's address at the protocol layer immediately below the network layer
ifAdminStatus	INTEGER	RW	Desired interface state (up(1), down(2), testing(3))
ifOperStatus	INTEGER	RO	Current operational interface state (up(1), down(2), testing(3))
ifLastChange	TimeTicks	RO	Value of sysUpTime at the time the interface entered its current operational state
ifInOctets	Counter	RO	Total number of octets received on the interface, including framing characters
ifInUcastPkts	Counter	RO	Number of subnetwork-unicast packets delivered to a higher-layer protocol
ifInNUcastPkts	Counter	RO	Number of nonunicast packets delivered to a higher-layer protocol
ifInDiscards	Counter	RO	Number of inbound packets discarded, even though no errors had been detected, to prevent their being deliverable to a higher-layer protocol (e.g., buffer overflow)
ifInErrors	Counter	RO	Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
ifInUnknownProtos	Counter	RO	Number of inbound packets that were discarded because of an unknown or unsupported protocol
ifOutOctets	Counter	RO	Total number of octets transmitted on the interface, including framing characters
ifOutUcastPkts	Counter	RO	Total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or otherwise not sent
ifOutNUcastPkts	Counter	RO	Total number of packets that higher-level protocols requested be transmitted to a nonunicast address, including those that were discarded or otherwise not sent
ifOutDiscards	Counter	RO	Number of outbound packets discarded even though no errors had been detected to prevent their being transmitted (e.g., buffer overflow)
ifOutErrors	Counter	RO	Number of outbound packets that could not be transmitted because of errors
ifOutQLen	Gauge	RO	Length of the output packet queue
ifSpecific	OBJECT IDENTIFIER	RO	Reference to MIB definitions specific to the particular media being used to realize the interface

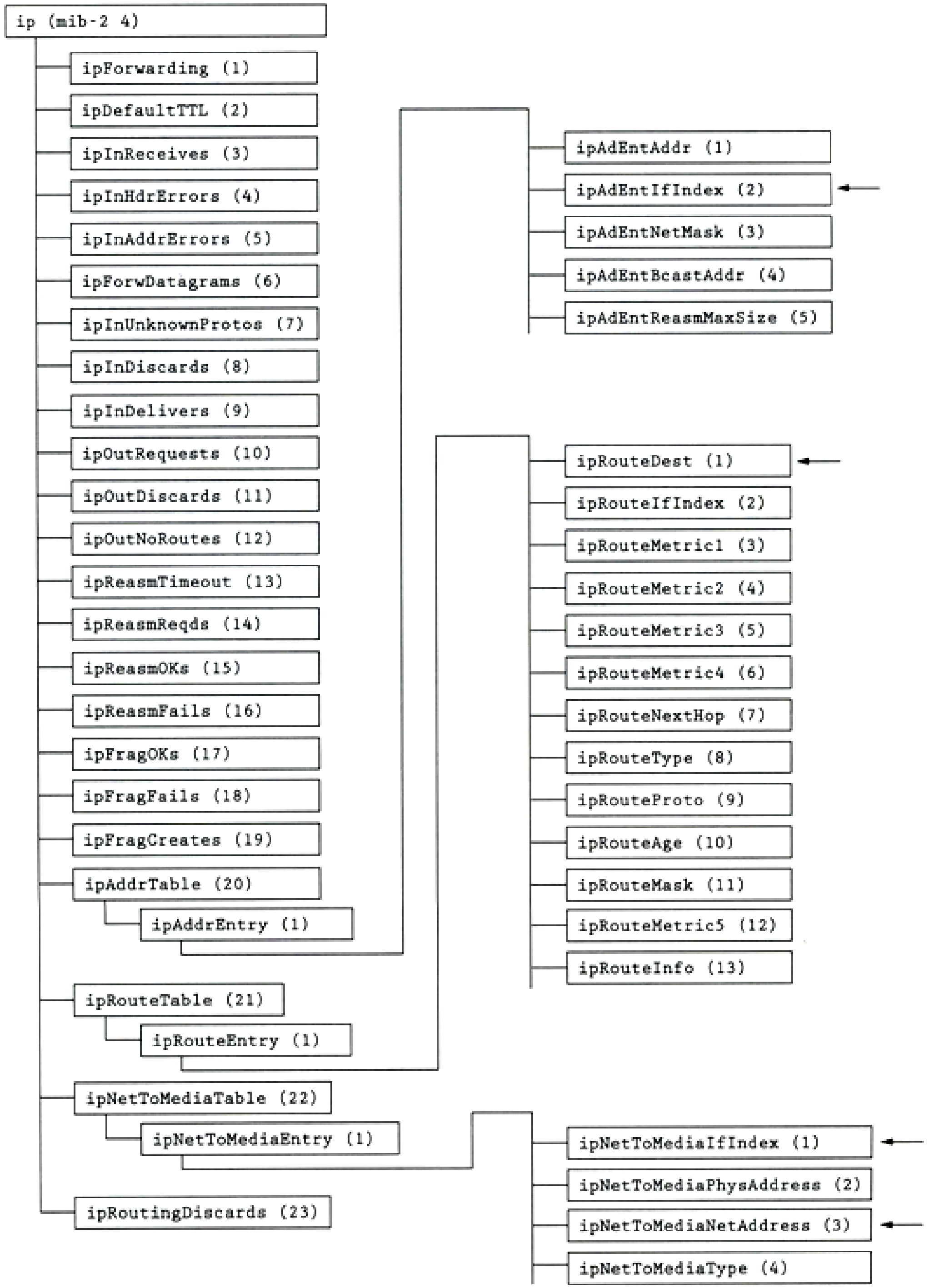
MIB-II

TCP GROUP



MIB-II

IP GROUP



RFC 1157

Simple Network Management Protocol

SNMP Protocol

- Supported operations
  - get, set, trap
- Simplicity vs. limitations
  - Not possible to change the structure of MIB by adding or deleting object instances
  - Access is provided only to leaf objects
    - Not possible to access entire table or row in single action

SNMP Protocol – security concern

- In management environment
  - The management station and managed agent
    - One-to-many relationship
    - One station may manage all or a subset of target
  - The managed station and management station
    - One-to-many relationship
    - Each managed agent controls its local MIB and must be able to control the use of that MIB
    - Three aspects
      - Authentication service
      - Access policy
      - Proxy service

SNMP Protocol – communities (1)

- An SNMP community
  - A relationship between an SNMP agent and a set of SNMP managers that defines
    - Authentication, access control and proxy
  - The managed system establishes one community for each combination of authentication, access control and proxy
  - Each community has a unique "community name"
  - Management station use certain community name in all get and set operations

SNMP Protocol – communities (2)

- Authentication
  - The community name (password)
- Access policy
  - Community profile
    - SNMP MIB view
      - A subset of MIB objects
    - SNMP access mode
      - READ-ONLY, READ-WRITE

UC Davis SNMP agent

UCD SNMP agent (1)

- /usr/ports/net-mgmt/net-snmp
  - To Install:
    - make NET_SNMP_SYS_CONTACT = "lwhsu@cs.nctu.edu.tw" \
      NET_SNMP_SYS_LOCATION = "NCTU EC314" \
      install clean
      - You can use portconf (ports-mgmt/portconf) to define these values
  - Firewall rules to restrict access to port 161
  - After installation, use "snmpconf -g basic_setup"
    - It will generate snmpd.conf
    - move it to /usr/local/etc/snmp/

UCD SNMP agent (2)

- snmpconf
  - % man snmpd

  - System Information Setup
    - Location, contact, service
  - Access Control Setup
    - SNMPv3 or SNMPv1 access community
  - Trap Destination
    - Where to send the trap
  - Monitor Various Aspects of the Running Host
    - Process, disk space, load, file
  - Extending the Agent
    - Let snmp agent to return information that yourself define
  - Agent Operating Mode
    - User/group, IP port,…

UCD SNMP agent (3)

- To get various value
  - man snmpget, snmpgetnext, snmptable

    % snmpget -c public -v 1 nabsd system.sysContact.0

    % snmpgetnext –c public –v 1 nabsd system.sysContact.0

    % snmptable -c public -v 1 nabsd mib-2.tcp.tcpConnTable

    % snmpwalk –c public –v 1 nabsd system

    % snmpwalk -c public -v 1 nabsd iso.org.dod.internet.private.enterprises