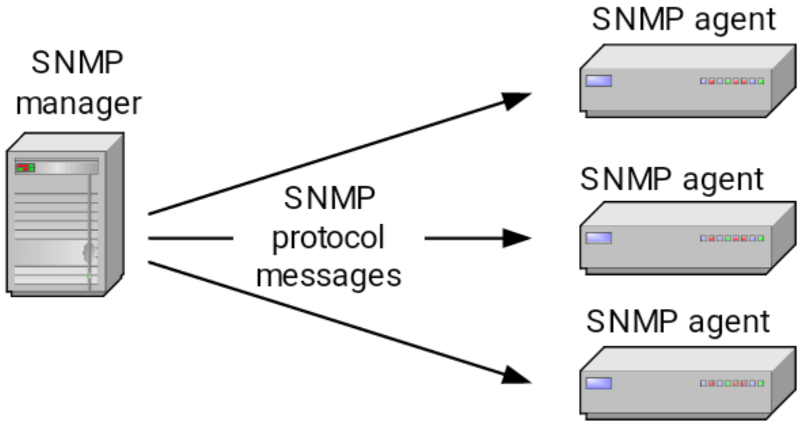
SNMP
Simple Network Management Protocol

Simple Network Management Protocol

- SNMP is a framework that provides facilities for managing and monitoring network resources on the Internet.
- Components of SNMP:
  - SNMP agents
  - SNMP managers
  - Management Information Bases (MIBs)
  - SNMP protocol itself

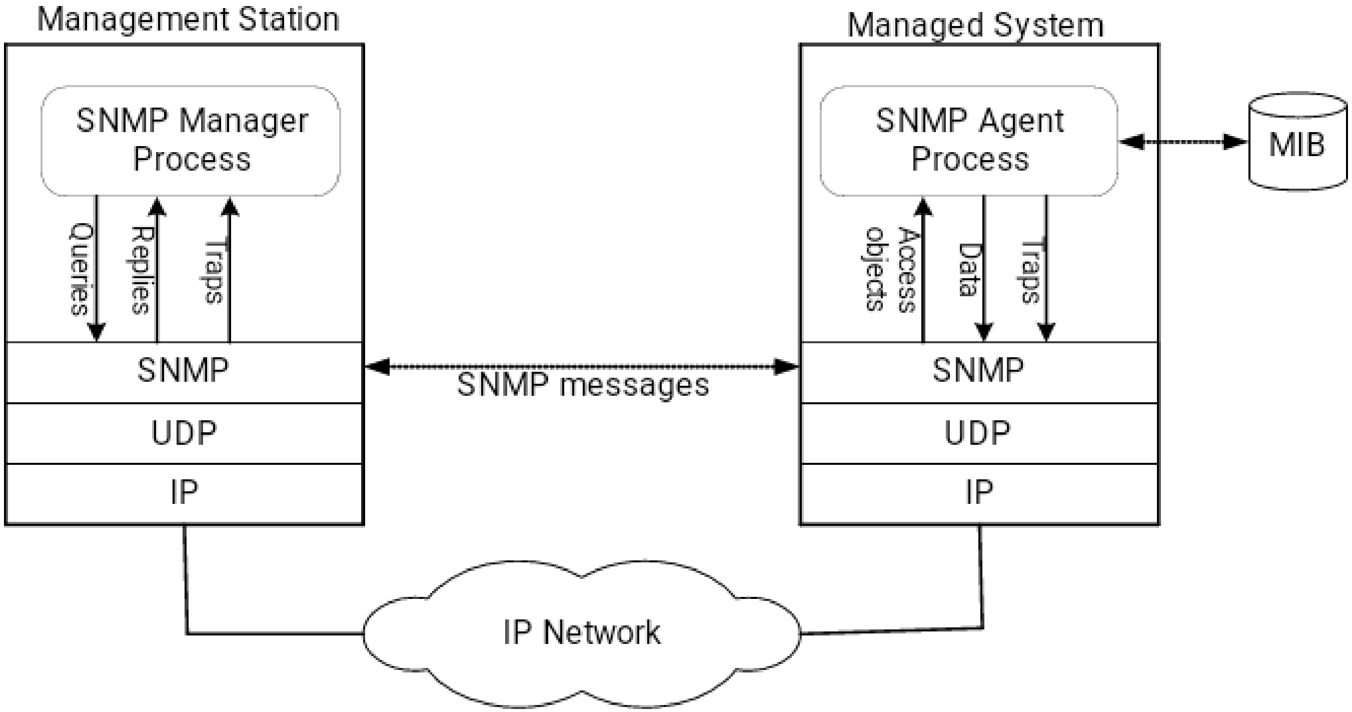


Simple Network Management Protocol

- **SNMP agent** is software that runs on a piece of network equipment (host, router, printer, or others) and that maintains information about its configuration and current state in a database
- Information in the database is described by **Management Information Bases (MIBs)**
- An **SNMP manager** is an application program that contacts an SNMP agent to query or modify the database at the agent.
- **SNMP protocol** is the application layer protocol used by SNMP agents and managers to send and receive data.

SNMP

- Interactions in SNMP



MIBS

- A MIB specifies the managed objects
- MIB is a text file that describes managed objects using the syntax of ASN.1 (Abstract Syntax Notation 1)
- ASN.1 is a formal language for describing data and its properties

- In Linux, MIB files are in the directory */usr/share/snmp/mibs*
  - *Multiple MIB files*
  - *MIB-II (defined in RFC 1213) defines the managed objects of TCP/IP networks*

Managed Objects

- Each managed object is assigned an *object identifier (OID)*
- The OID is specified in a MIB file.
- An OID can be represented as a sequence of integers separated by decimal points or by a text string:

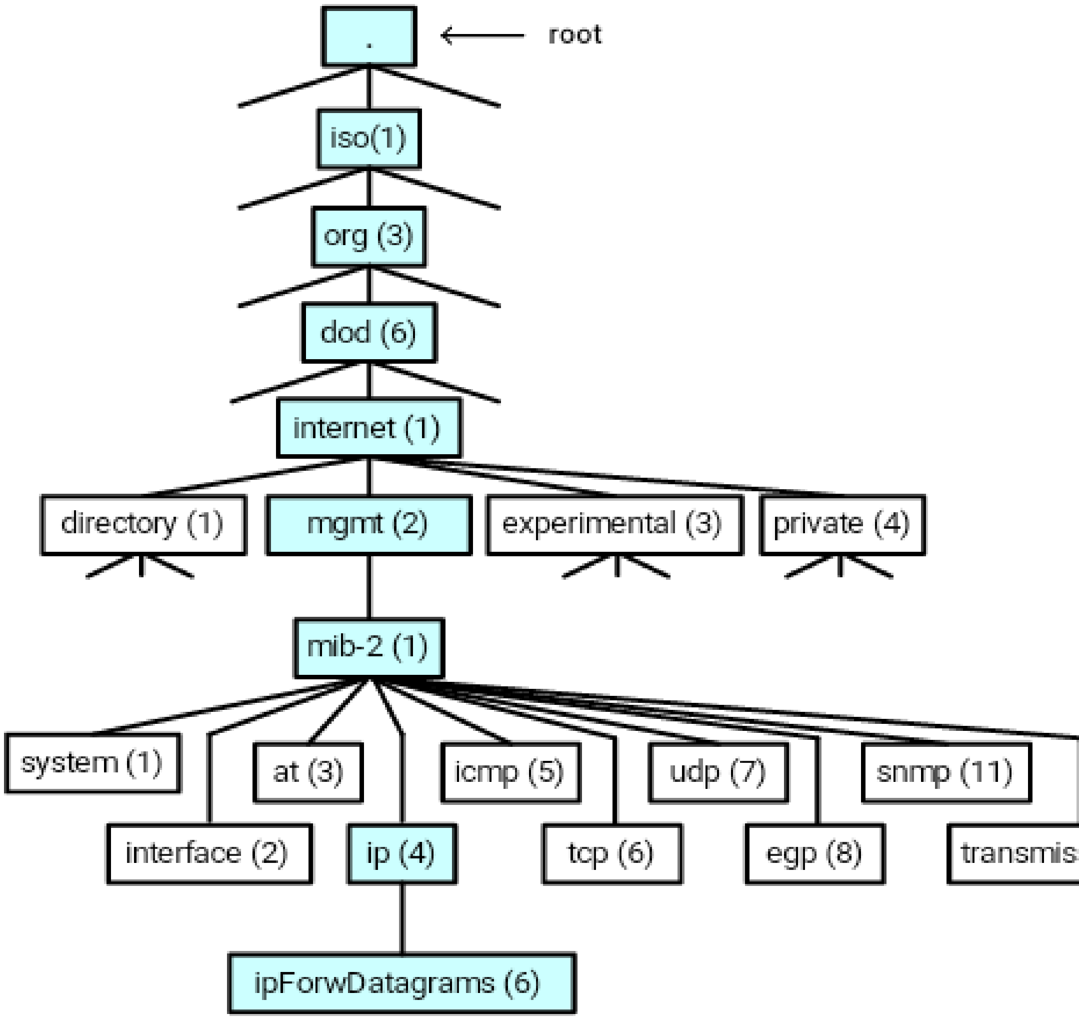
  Example:

  - *1.3.6.1.2.1.4.6.*
  - i*so.org.dod.internet.mgmt.mib-2.ip.ipForwDatagrams*

- When an SNMP manager requests an object, it sends the OID to the SNMP agent.

Organization of managed objects

- Managed objects are organized in a tree-like hierarchy and the OIDs reflect the structure of the hierarchy.
- Each OID represents a node in the tree.
- The OID 1.3.6.1.2.1 (*iso. org.dod.internet.mgmt. mib-2)* is at the top of the hierarchy for all managed objects of the MIB-II.
- Manufacturers of networking equipment can add product specific objects to the hierarchy.



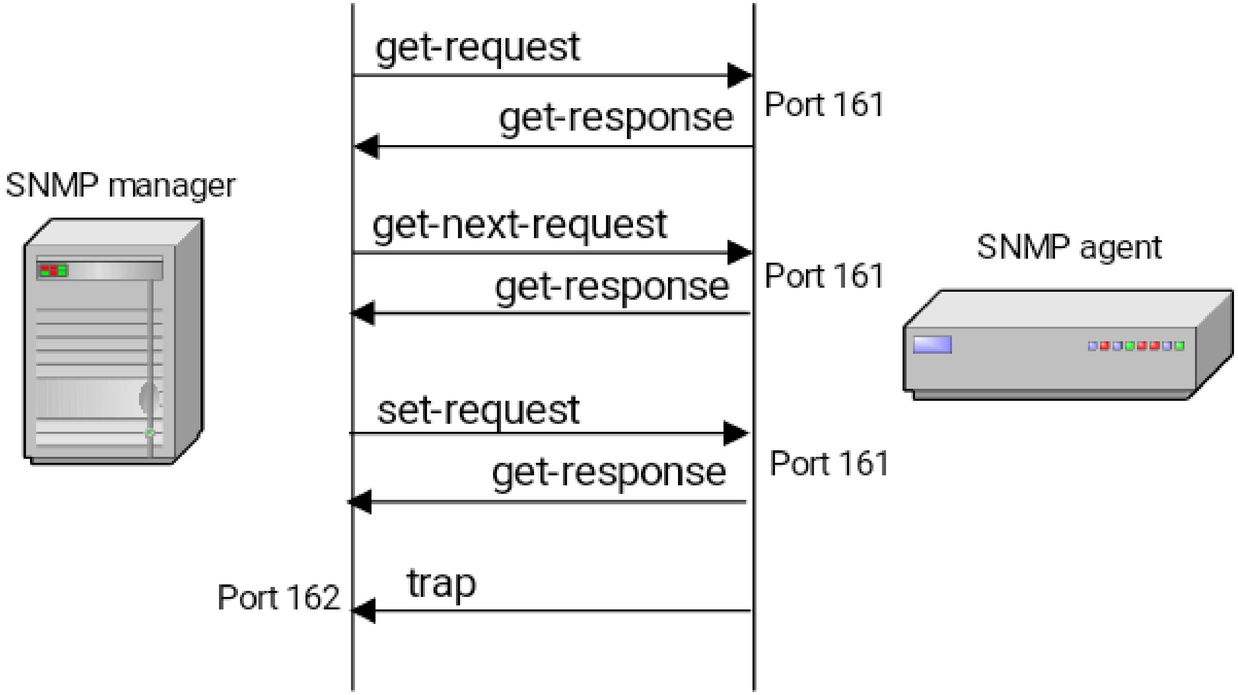
Definition of managed objects in a MIB

- Specification of ipForwDatagrams in MIB-II.

```
ipForwDatagrams OBJECT-TYPE
    SYNTAX  Counter
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
            "The number of input datagrams for which this
            entity was not their final IP destination, as a
            result of which an attempt was made to find a
            route to forward them to that final destination.
            In entities which do not act as IP Gateways, this
            counter will include only those packets which were
            Source-Routed via this entity, and the Source-
            Route option processing was successful."
    ::= { ip 6 }
```

SNMP Protocol

- SNMP manager and an SNMP agent communicate using the SNMP protocol
  - Generally: Manager sends queries and agent responds
  - Exception: Traps are initiated by agent.



SNMP Protocol

- **Get-request.** Requests the values of one or more objects
- **Get-next-request.** Requests the value of the next object, according to a lexicographical ordering of OIDs.
- **Set-request.** A request to modify the value of one or more objects
- **Get-response.** Sent by SNMP agent in response to a *get-request, get-next-request, or set-request* message.
- **Trap.** An SNMP trap is a notification sent by an SNMP agent to an SNMP manager, which is triggered by certain events at the agent.

Traps

- Traps are messages that asynchronously sent by an agent to a manager
- Traps are triggered by an event
- Defined traps include:
  - linkDown: Even that an interface went donw
  - coldStart - unexpected restart (i.e., system crash)
  - warmStart - soft reboot
  - linkUp - the opposite of linkDown
  - (SNMP) AuthenticationFailure
  - …

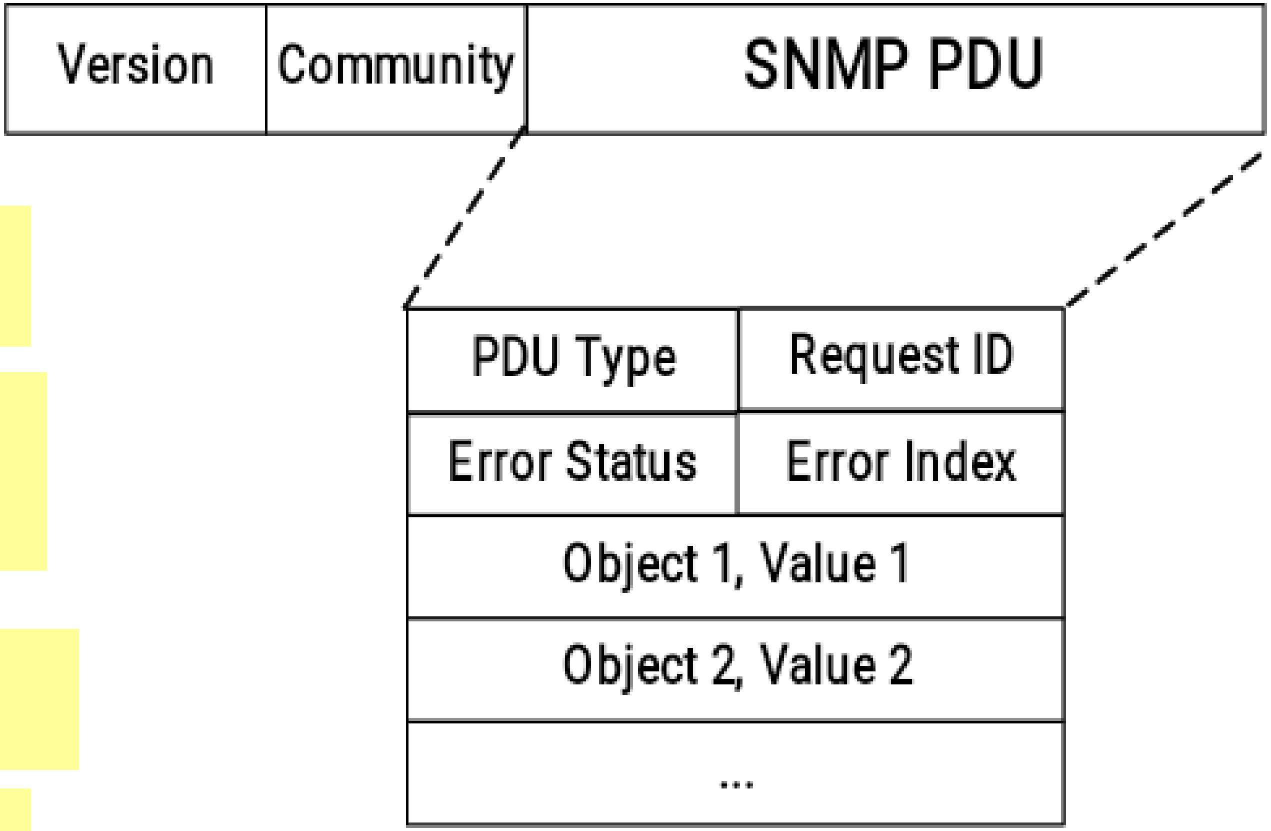
SNMP Versions

- Three versions are in use today:
  - SNMPv1 (1990)
  - SNMPv2c (1996)
    - *Adds “GetBulk” function and some new types*
    - *Adds RMON (remote monitoring) capability*
  - SNMPv3 (2002)
    - *SNMPv3 started from SNMPv1 (and not SNMPv2c)*
    - *Addresses security*

- All versions are still used today
- Many SNMP agents and managers support all three versions of the protocol.

Format of SNMP Packets

- SNMPv1 Get/Set messages:



Version

Community

SNMP PDU

PDU Type

Request ID

Error Status

Error Index

Object 1, Value 1

Object 2, Value 2

...

Cleartext string that is used as a password

PDU type, e.g.:
32: SNMPv1 Get
64: SNMPv2 Get

Unique ID to match requests with replies

Sequence of name-value pairs

SNMP Security

- SNMPv1 uses plain text community strings for authentication as plain text without encryption

- SNMPv2 was supposed to fix security problems, but effort de-railed (The “c” in SNMPv2c stands for “community”).
-
- SNMPv3 has numerous security features:
  - Ensure that a packet has not been tampered with (**integrity**),
  - Ensures that a message is from a valid source (**authentication**)
  - Ensures that a message cannot be read by unauthorized (**privacy**).

SNMP Security

- Security model of SNMPv3 has two components:
  1. Instead of granting access rights to a community, SNMPv3 grants access to users.
  2. Access can be restricted to sections of the MIB (V*ersion-based Access Control Module* (VACM). Access rights can be limited
     - by specifying a range of valid IP addresses for a user or community,
     - or by specifying the part of the MIB tree that can be accessed.

Security levels in SNMPv2

SNMP has three security levels:

- *noAuthNoPriv*: Authentication with matching a user name.
- *authNoPriv*: Authentication with MD5 or SHA message digests.
- *authPriv:* Authentication with MD5 or SHA message digests, and encryption with DES encryption

Compare this to SNMPv1 and SNMPv2c:

- *SNMPv1, SNMPv2*: Authentication with matching a community string.