



Revision Exercises with SNMP, DHCP

1 Background

1.1 SNMP

- SNMP is a Internet IETF standard, open protocol, broadly supported by most network equipment vendors.
- A networked device that supports SNMP runs software called an *agent*
- The *agent* provides many *managed objects*
- Each *managed object* is identified by an *object identifier*, OID, which has a numeric form, (e.g., .1.3.6.1.2.1) and may also have a named form (e.g., .iso.org.dod.internet.mgmt.mib-2)

1.1.1 Management Information Base, ASN.1

- The definition of each *managed object* is in the *Management Information Base*, MIB, which is defined by text files written in *Abstract Syntax Notation One*, ASN.1.
- Standard MIBs are written in the standards documents of the Internet, *Request For Comments*, RFCs, which are freely downloadable from many sites on the Internet

1.1.2 Structure of Management Information

- The format of each entry in the MIB is defined by the *Structure of Management Information*, SMI.
- The SMI defines (among other things):
 - part of the MIB tree structure;
 - the *syntax* (data types) that are allowed;
 - the *access* allowed to a managed object (for example, *read-only*, *read-write*, *not-accessible*)
- ASN.1 defines these basic types used in SMI:
 - INTEGER a number; allowable range of values can be specified.
 - OCTET STRING: a string of bytes
 - OBJECT IDENTIFIER: an OID

1.1.3 Versions of SNMP, SMI

- There are two versions of SMI: SMI v1 for SNMP version 1, and SMI v2 for SNMP versions 2 and 3:
SMI version 1 defines the following types in terms of the basic ASN.1 types above:
 - Counter: 32 unsigned value that wraps (i.e, after reaching $2^{32} - 1$, it goes back to zero)
 - Gauge: 32-bit unsigned value that can increase or decrease but not wrap

- **IpAddress**: 32-bit IP version 4 address
- **TimeTicks**: 32-bit count in hundredths of a second
- **Opaque**: allows any kind of data

SMI version 2 defines these data types:

- **Integer32**: a 32-bit integer
 - **Counter32**: same as **Counter** (wraps; count to $2^{32} - 1$ then back to 0)
 - **Gauge32**: Same as **Gauge** (doesn't wrap)
 - **Unsigned32**: 32-bit unsigned value
 - **Counter64**: Same as **Counter32**, except uses 64 bits, a useful extension to cope with fast networks, where a **Counter32** would wrap in less than one hour. If a counter wraps too fast, the management station may miss the wrapping, and report a much lower data flow than actually occurred.
 - **BITS**: a set of named bits
- SNMP operations (all versions) are:
 - **get-request**: given an *exact* OID, *complete with instance number*, manager requests exactly that managed object's data
 - **get-next-request**: given an OID as a starting point, manager asks agent to do a *depth-first search* of the MIB tree, find the next OID, and return its data.
 - **set-request**: manager writes a new value to a writable object on the agent
 - **response**: the answer sent back by the agent to a **get-request**, **get-next-request**, or **set-request** operation sent by the management station
 - **trap**: a PDU sent by the agent to the manager indicating that something needs attention. Manager does *not* send any acknowledgement back.
 - SNMP versions 2 and 3 add these operations:
 - **get-bulk-request**: sent by the manager to the agent, requesting the efficient transfer of large amounts of data; especially used for table data.
 - **inform-request**: sent by manager or agent to manager; reply is a **response**. It is like a **trap**, but has an acknowledgment.
 - **Report**: is named but details of use are not defined, so is *not used*.
 - Each operation is authenticated; in versions 1 and 2, the authentication is by a plain-text shared password called a *community string*. Since these *community strings* can be easily read by any network sniffer, such as **ethereal** or **tcpdump**, community string based SNMP must *never* be accessible on the Internet. Version 3 has a much more comprehensive (and complex) authentication and encryption scheme that is *much* more secure. SNMP v3 products are now available from a number of companies, including Cisco.
 - SNMP version 2 introduces additional standard MIBs, in particular the **security** and **snmpv2** MIB subgroups. There are also changes to the **system** and **snmp** subgroups in version 1.

1.1.4 mib-2 group, tables and instance numbers

- We studied the **ifTable** (interface table) in the **mib-2** MIB group, because it contains information about all the network interfaces on a managed device.
- Each interface has one row in the table, distinguished by an index called an *instance number*.
- We can recognise each interface by the **ifDescr** (interface description) field:

```
$ snmpwalk ictlab public ifDescr
interfaces.ifTable.ifEntry.ifDescr.1 = lo
interfaces.ifTable.ifEntry.ifDescr.2 = eth0
```

- This allows us to determine that the row in the table with instance number 1 is the loopback interface `lo`, and the row in the table with instance number 2 is the Ethernet interface, `eth0`.
- Cricket uses this method to automatically map names to entries in the table—called *instance mapping*.
- You monitored network traffic in and out of each network interface using the entries in the `ifTable`: `ifInOctets` and `ifOutOctets`.
- Scalar objects, such as `system.sysUpTime` have an instance number of zero.
- The `get-request` SNMP operation requires the *exact* specific OID required, including the *instance number*:

```
$ snmpget -v 2c ictlab public sysUpTime
system.sysUpTime = No Such Instance currently exists
$ snmpget -v 2c ictlab public sysUpTime.0
system.sysUpTime.0 = Timeticks: (103721046) 12 days, 0:06:50.46
```

1.2 DHCP

The DHCP client moves through the states shown in the state diagram in figure 1. Table 1 on the next page lists all the DHCP messages, and their purpose.

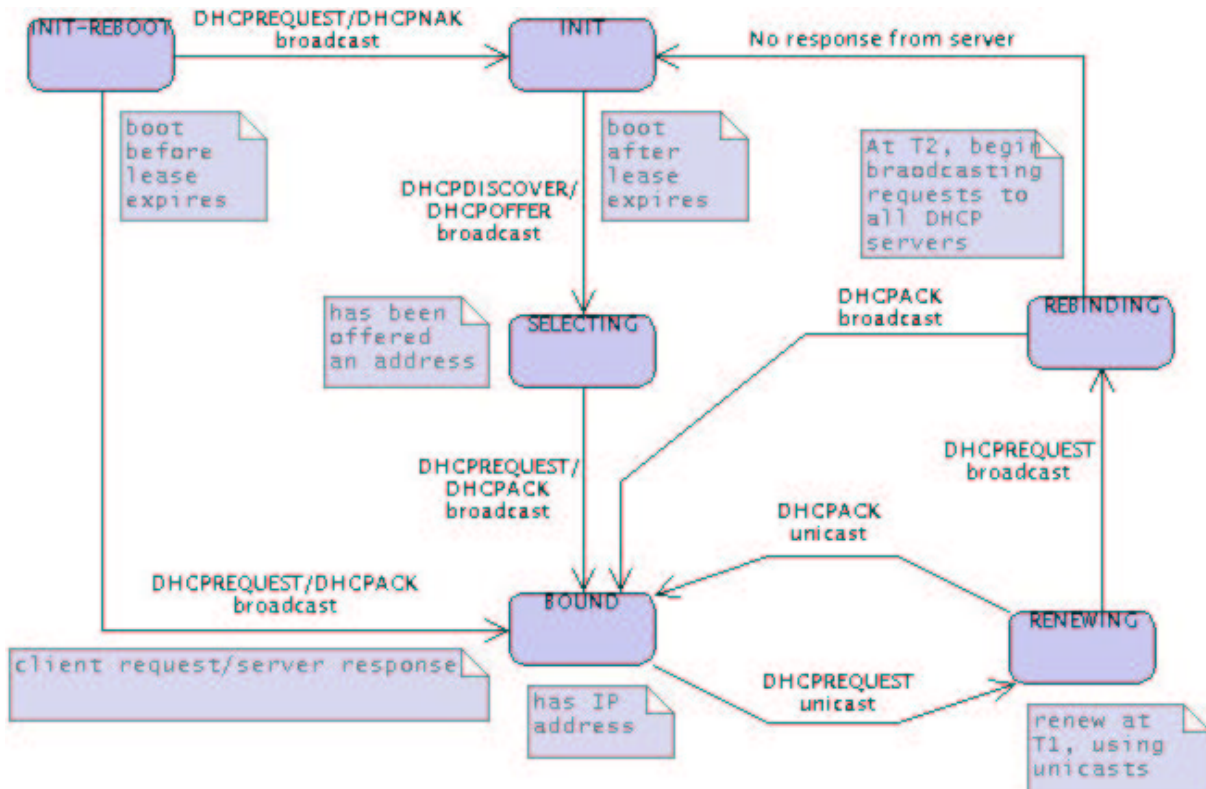


Figure 1: The DHCP client moves through the states shown in this state diagram.

DHCPDISCOVER	- Client broadcast to locate available servers.
DHCPOFFER	- Server to client in response to DHCPDISCOVER with offer of configuration parameters.
DHCPREQUEST	- Client message to servers either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming correctness of previously allocated address after, e.g., system reboot, or (c) extending the lease on a particular network address.
DHCPACK	- Server to client with configuration parameters, including committed network address.
DHCPNAK	- Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease as expired
DHCPDECLINE	- Client to server indicating network address is already in use.
DHCPRELEASE	- Client to server relinquishing network address and cancelling remaining lease.
DHCPINFORM	- Client to server, asking only for local configuration parameters; client already has externally configured network address.


Table 1: DHCP Messages extracted from RFC 2131

2 Questions


2.1 SNMP

1. An Internet Service Provider (ISP) has a Cisco router on the Internet. Discuss the advantages and disadvantages of managing this using SNMP version 2.

2. Determine the full numerical OID of the `snmpv2` subgroup.



3. What is the lowest possible value of an instance number for an entry in a table?




4. List the major differences between SNMP version 1 and 2

5. List the major differences between SNMP version 2 and 3

2.2 DHCP and DNS

1. When a computer has just been turned on, and it has no DHCP lease, what state is

 the client in?

2. List the states through which a client will pass when it is turned on, with no DHCP lease.



3. List the states through which a client will pass when it is turned on, with a current DHCP lease.



4. List the states through which a client will pass when it is turned on, with a current DHCP lease, but for a different subnet.



5. Under what circumstances will a client move into the **rebinding** state?



6. Briefly describe how the current DHCP system used in the Institute allocates addresses. (Refer to the link from the subject page).

7. List some of the shortcomings of the DHCP system used in this Institute, and ways that it could be improved.