Network management:

SNMPv2, SNMPv3 and RMON

The coming of SNMP v2

- SNMP (i.e. version 1) was originally developed as an interim; OSI was expected to be the ultimate
- However
  - SNMP became popular; major vendors had incorporated SNMP modules in their systems and components and
  - it also became evident that OSI was not going to be implemented in the near future, thus motivating for developing ver 2

SNMPv2

SNMPv2 features

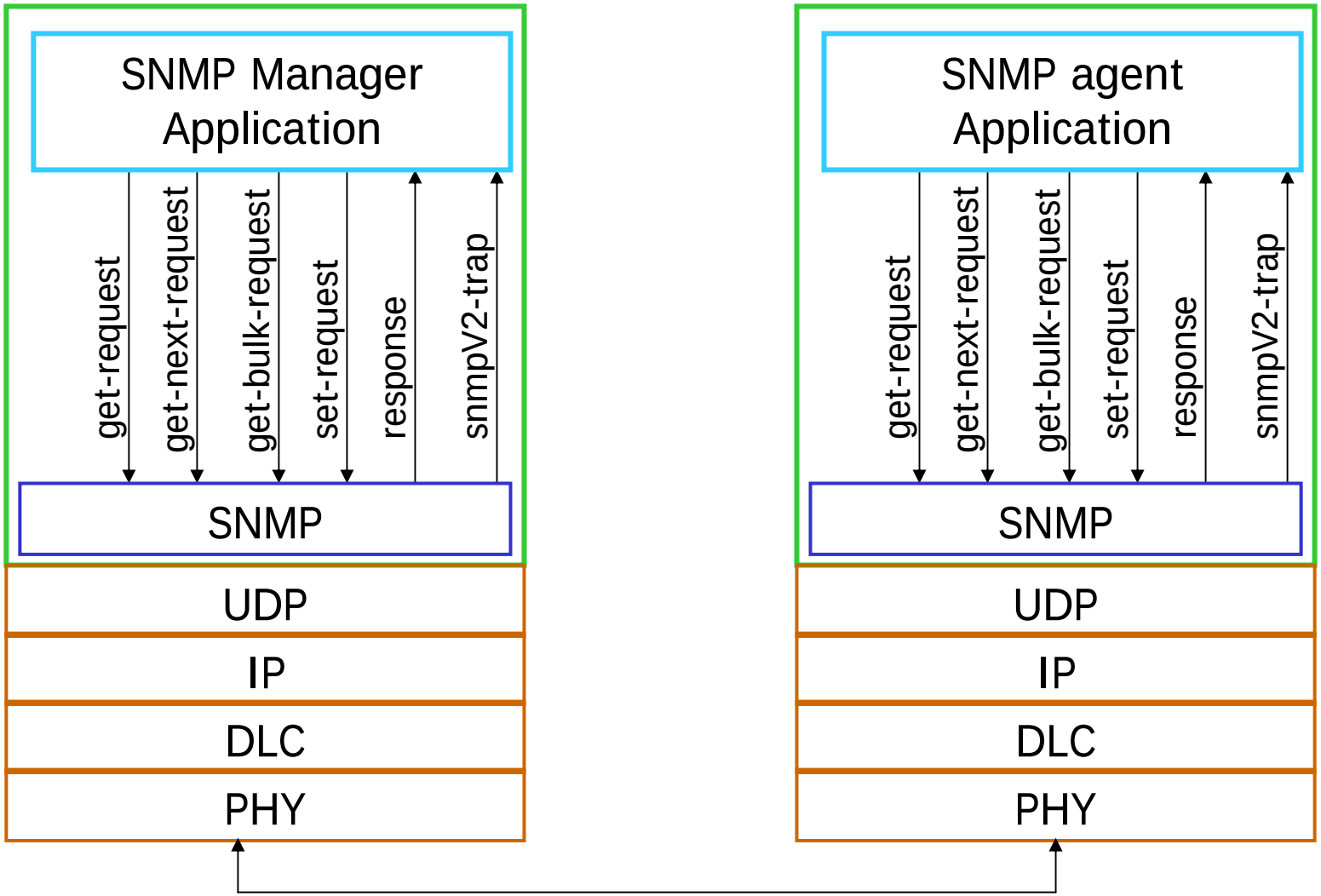
- Basic components are same.
- Improvements in the Documentation architecture
- Improvements and additions to SMI

- Security –
  - recommendations but no consensus. Retain the the framework based on community name. The summary of the frame work is referred to as SNMPv2C.
- Communication model: Two additional messages.
- Creation and deletion of rows in tables supported.

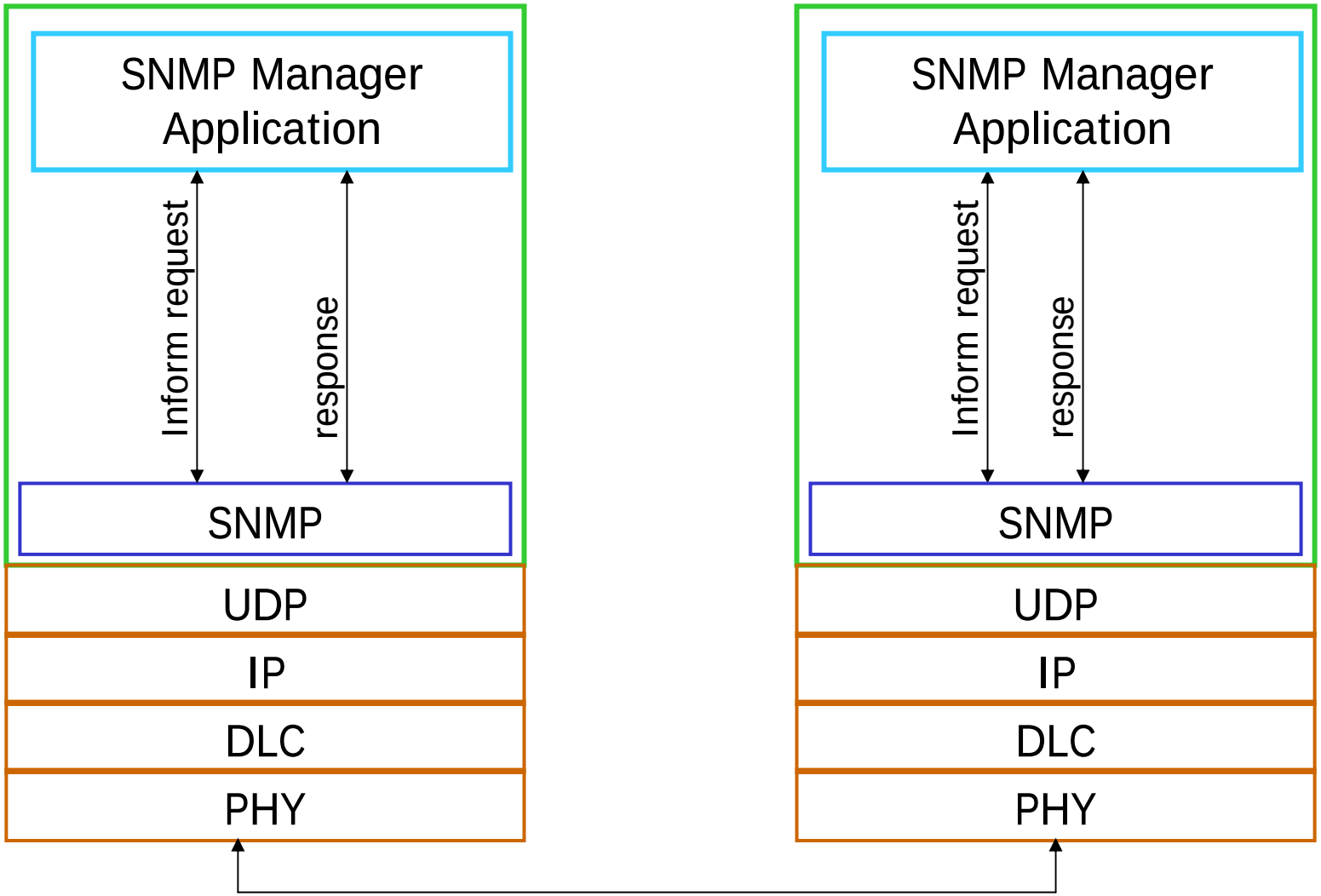
- Improvements in the Documentation architecture
- Improvements and additions to SMI specifications
  - Extremely important e.g. with regard to implementation and issues of compliance

- The communication model
  - Bulk data transfer message
  - Manager-to-manager message
  - Changes in notification/trap message structure

SNMPv2 : the communication model

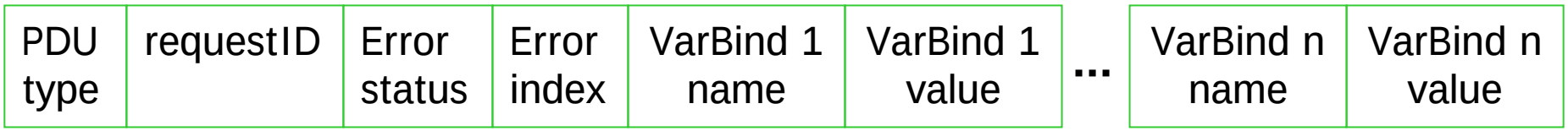


SNMPv2 : the communication model

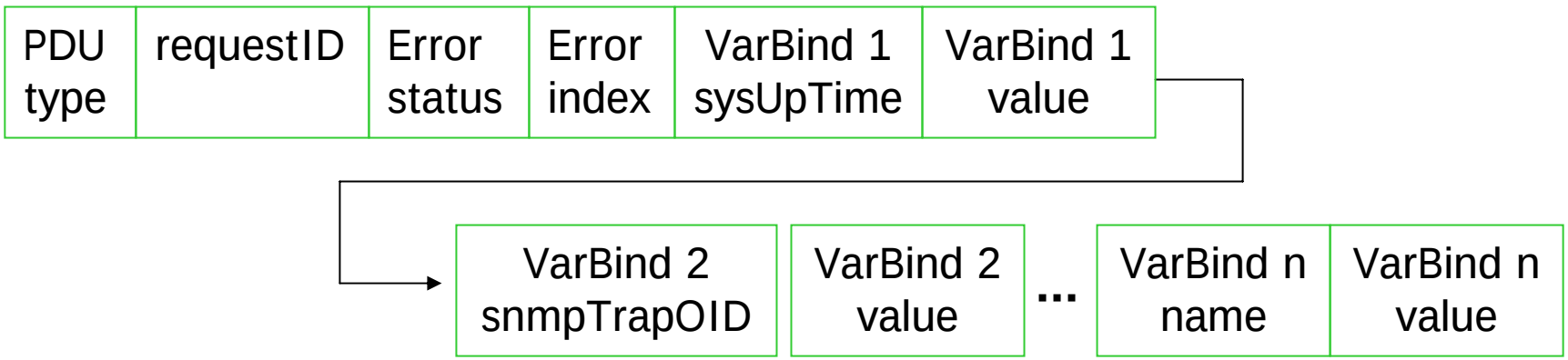


SNMPv2 : the communication model

Get, Set, response, inform Type PDUs



Trap or notification PDUs

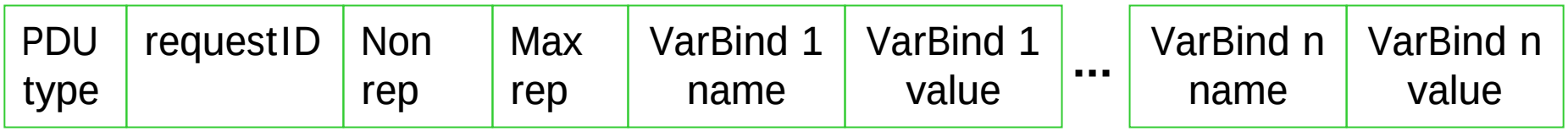


SNMPv2 : the communication model

Getting the elements of a structured object with

- get bulk request

Get bulk PDU



SNMPv2 : the communication model

- Changes in MIB to support notifications

Internet group

- Add

  security OBJECT DISCRIPTOR ::= {internet 5}

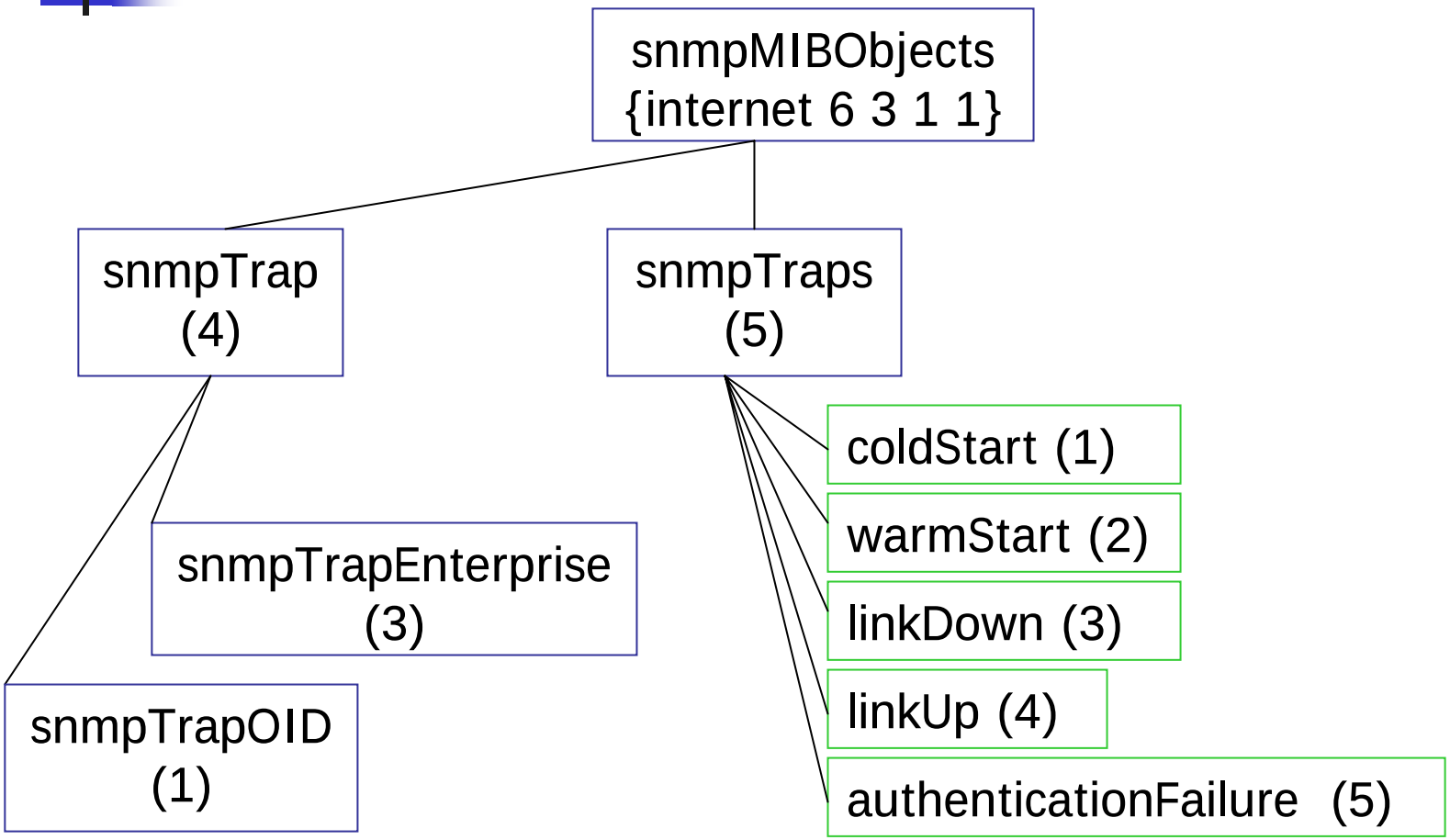
  snmpv2 OBJECT DISCRIPTOR ::= {internet 6}

  snmpModules OBJECT DISCRIPTOR ::= {snmpv2 3}

  snmpMIB OBJECT DISCRIPTOR ::= {snmpModules 1}

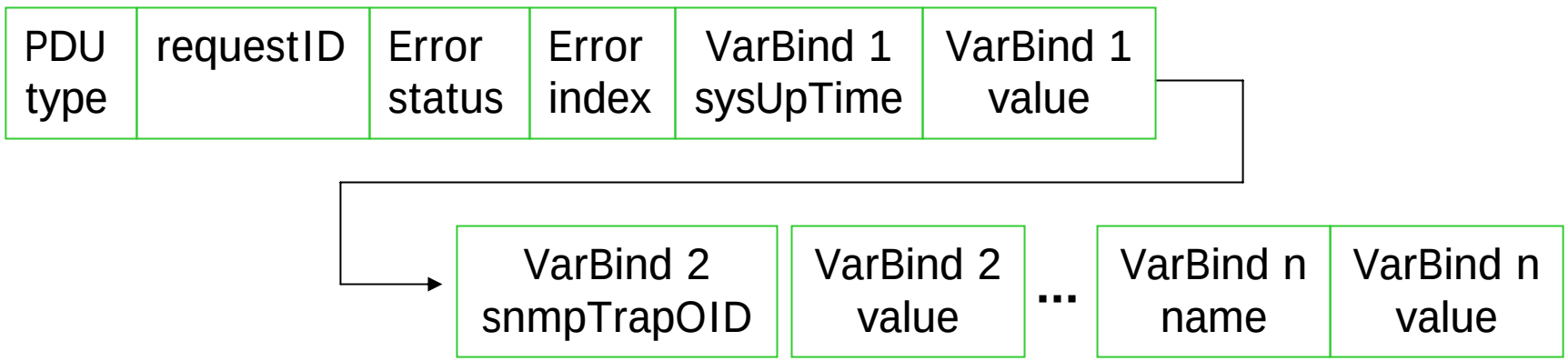
  snmpMIBObjects OBJECT DISCRIPTOR ::= {snmpMIB 1}

The snmpMIBObjects group



SNMPv2 : the communication model

Trap or notification PDUs



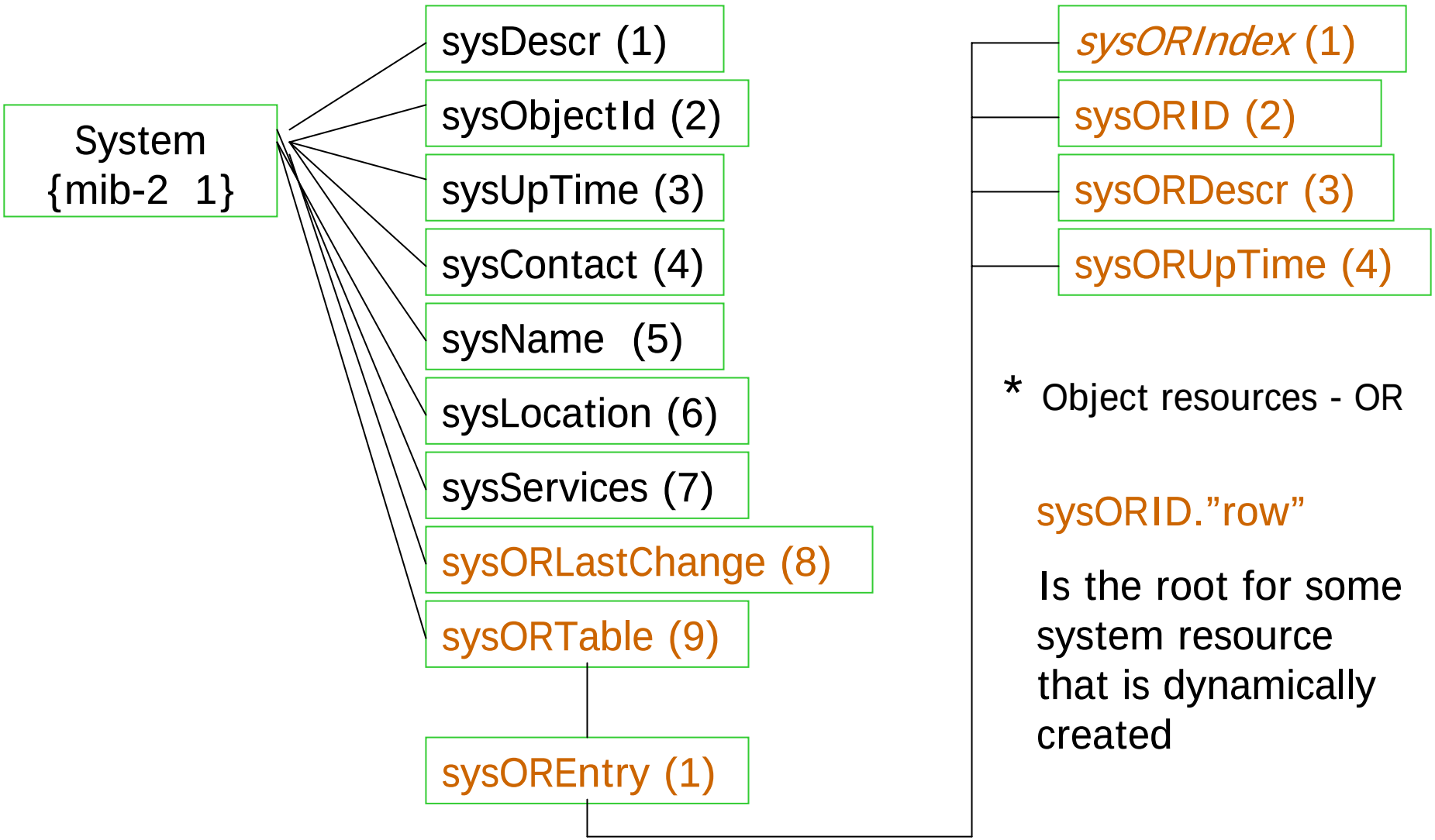
The system group additions in v2

Collection of objects called

- object resources
  - Object resources are configurable both statically and dynamically.

    E.g. virtual interfaces

The system group additions in v2



* Object resources - OR

sysORID."row"

Is the root for some system resource that is dynamically created

dynamic configuration of objects

- SNMPv2 supports the dynamic creation and deletion of table object entries
- Useful for dynamic resources e.g. VLANs
- Also for RMON

SNMPv2 : Creation and deletion of rows in tables

- Table entry structure
  - status (1)
  - index (2)
  - data(3)

```
status OBJECT-TYPE
        SYNTAX RowStatus
        MAX-ACCESS  read-create
        STATUS current
        DESCRIPTION “ ...    “
        ::= { tableEntry 1 ]
```

```
RowStatus ::= {
        active [1]
        notInService [2]
        notReady [3]
        createAndGo [4]
        createAndWait [5]
        destroy [6]
}
```

RowStatus

active [1]	;row exists & is operational
notInService [2]	;operation on row is suspended
notReady [3]	;row does not have all columnar objects needed
createAndGo [4]	;create row and make active
createAndWait [5]	;row under creation
destroy [6]	;delete row

SNMPv2 : Creation and deletion of rows in tables

To create

set-request (rowStatus.3 = 4, index.3 = 3,
data.3 = DefData)

To activate

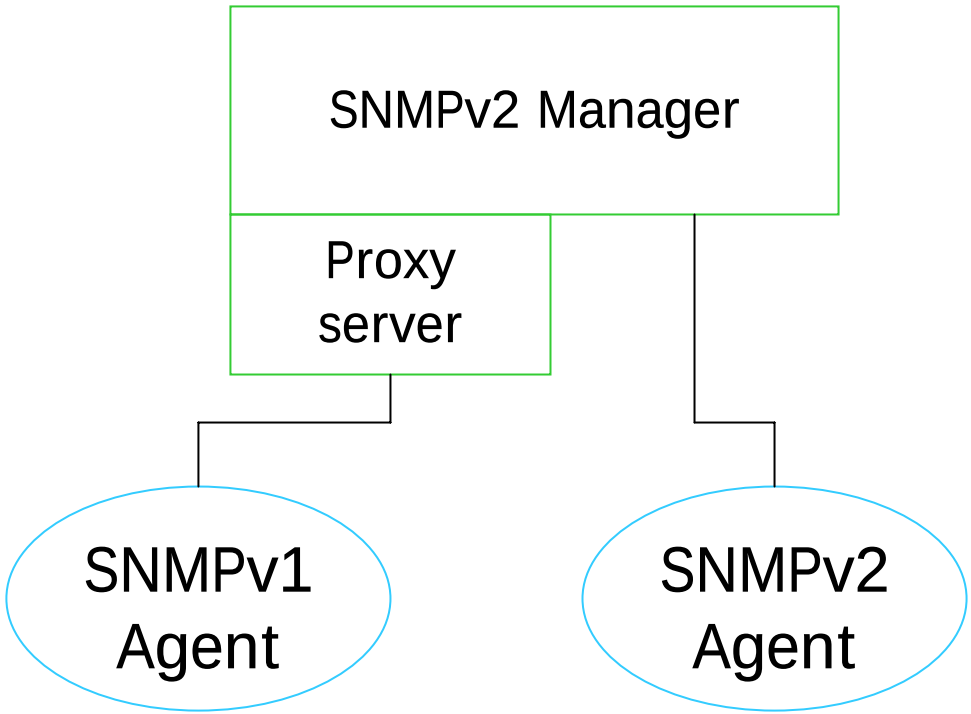
set-request (rowStatus.3 = 1)

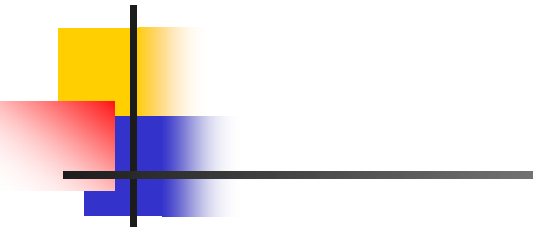
To delete

set-request (rowStatus.3 = 6)

Compatibility with SNMPv1 agents

- Proxy provided as below





- SNMPv3 features

  - Documentation architecture
  - SNMP Entity architecture definition
  - Notification target MIB
  - Security

- SNMPv3
  - SNMP Entity architecture defined
    - SNMP Engine
    - Application(s)

- SNMPv3
  - SNMP Engine
    - Dispatcher
    - Message processing subsystem
    - Security subsystem
    - Access control

- SNMPv3
  - Applications
    - Command generator
    - Notifications receiver
    - Proxy forwarder subsystem
    - Command responder
    - Notification originator
    - Other

SNMP Engine ID

- Intended to identify an SNMP entity (manager or agent); consists of
  - Enterprise ID and
  - Network address

SNMP Engine ID

e.g IP address

SNMP v1 &v2

Enterprise ID (octets 1-4)	Enterprise method (5th octet)	Function of the method (octet 6-12)

SNMP v3

Enterprise ID (octets 1-4)	Format indicator (5th octet)	format (variable number of octets)

1st bit 0 -> v1 or v2
else v3

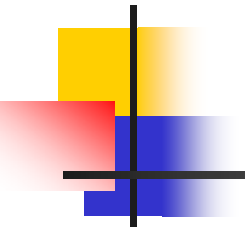
e.g. IPv4, IPv6 address, MAC, ...

Notification target

- Provide for a notification source to be configured with a target and related parameters

snmpTargetMIB ::= {snmpModules 12} and
snmpNotificationMIB ::= {snmpModules 13}

Both under the {internet snmpv2} MIB



- Security

- Security
  - Security threats
  - Security model
  - User-based security model
  - Access control

- Security threats
  - Modification
  - Masquerade
  - Message stream modification
  - Disclosure

Security model

Security model

- Defines authoritative and non-authoritative engines.
- Authentication module
  - Data integrity
  - Data origin authentication
- Privacy of information
- Timeliness of information

Authentication protocol

SNMPv3 : User-based security model (USM)

Authentication protocol

- Based on secret key shared by sender and receiver, authentication key
- Generated using HMAC-MD5-96 or HMAC=SHA-96
- Use MD5 or SHA hash function

- Authentication key
  - Replicate pw up to 2^{20} octets truncate as necessary $\rightarrow$ *digest0*
  - H(digest0) $\rightarrow$ digest1
  - digest2 = H(SNMP EngineID || digest1)
    - Digest2 is the *authKey*

Authentication protocol

HMAC

- Using functions K1 and K2
- K1 = (authKey-padto-64byte XOR ipad)
- K2 = (authKey-padto-64byte XOR ipad)

- x = H(K2, H(K1, message))

- HMAC = (octets 1-12 of x)

SNMPv3 : User-based security model (USM)

- Non-disclosure service

  Employ symmetric key cryptography

  - DES encrypt using a shared key

Access control – View-based access control model (VCAM)

Access control – View-based access control model (VCAM)

- Groups

  group: → set of one or more (security model, security name) pairs

- Security level

  Security level of a task (message)

  - no-authent + no-privacy, authent + no-privacy
  - authent + privacy

- Context

  - Collection of management information accessible by an SNMP entity (agent) and the access modes allowed

Access control – View-based access control model (VCAM)

- MIB views and Access Policy
  - The access policy defines the access rights to objects (organized by MIB views and view families) based on group, security model, security level and context name.

RMON

- RMON
  - What is RMON?
  - RMON functions and MIB groups

- RMON

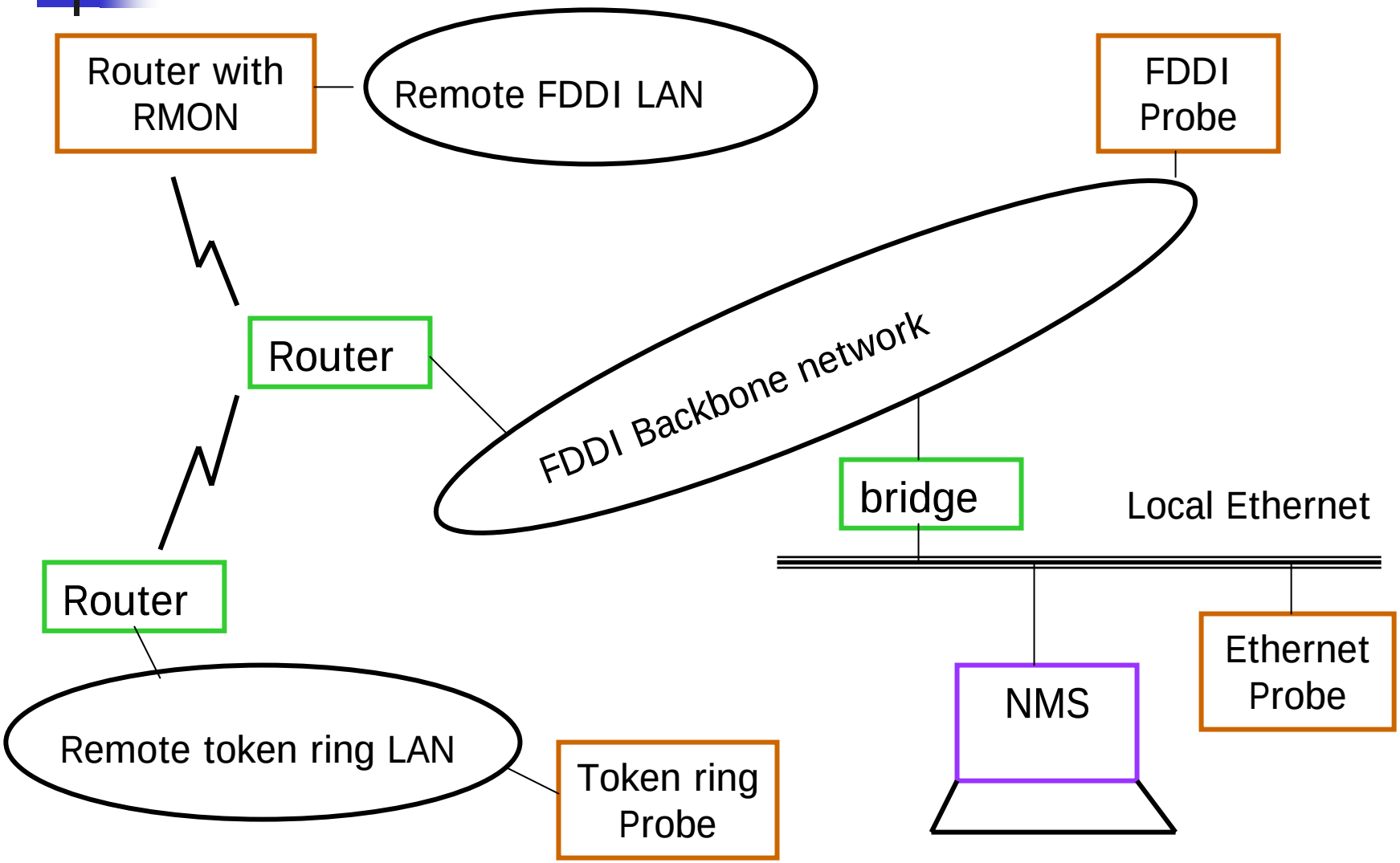
What is RMON?

- Monitoring
- Network monitor (probe)

- Components:
  - 1. physical object connected to medium,
  - 2. Processor that analyses the data

- RMON
  - Remote network monitor (RMON)
    - Information gathered and analyzed locally then sent to a remote NMS

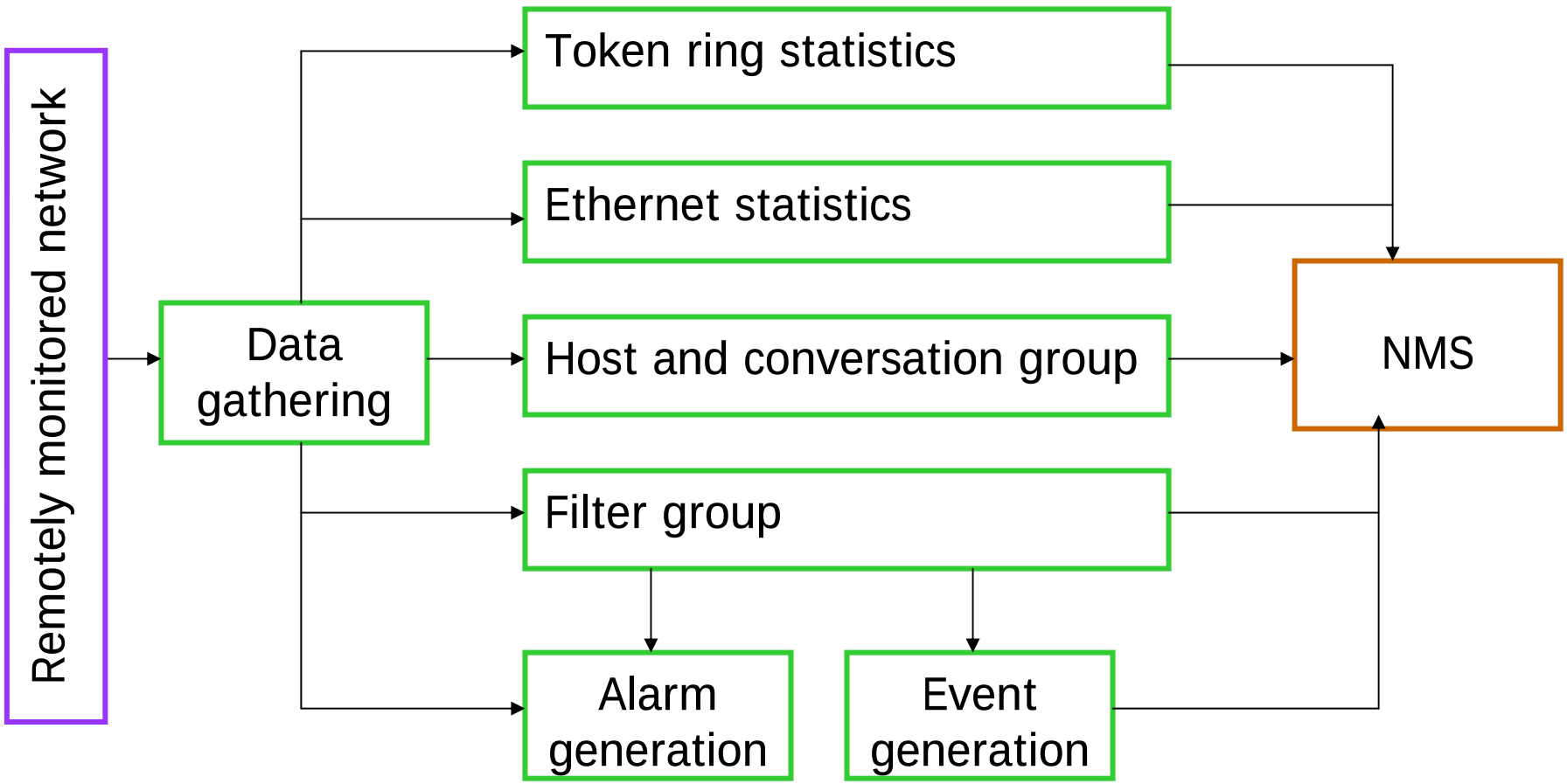
RMON - context



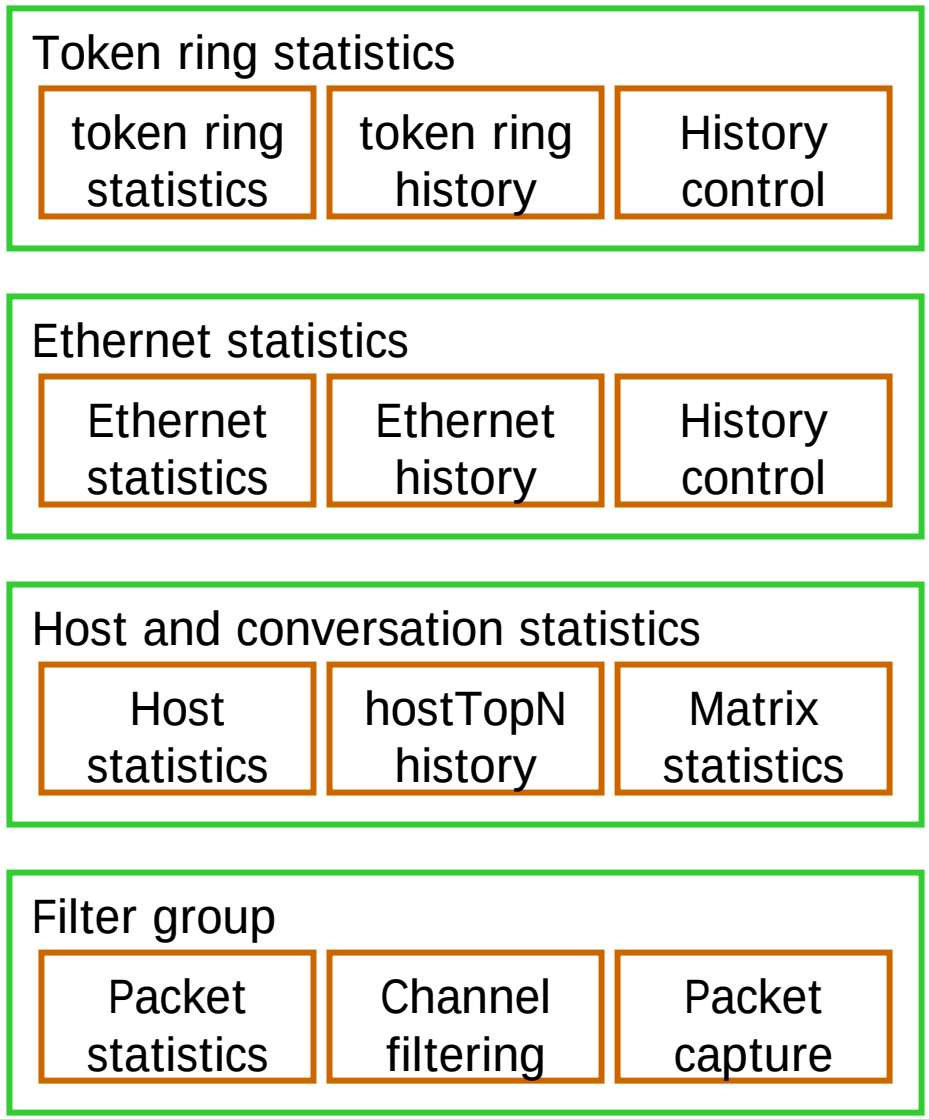
RMON - context

- Multi-vendor equipment, RMON devices included
- Need to establish common syntax and semantics for the use of RMON devices
  - ASN.1
  - SMIv2
  - RMON MIB

RMON functions



RMON - RMON 1 MIB groups and function



RMON – RMON 1 MIB groups and functions

- Statistics: provide link level statistics
- History: collect periodic statistical data and store for future retrieval.
- Alarm: generate event when data sample gathered crosses pre-established thresholds
- Host: gathers statistical data on hosts
- Host top N: compute the top N hosts on the respective categories of the traffic gathered.
- Matrix: gathers statistics on traffic between pairs of hosts.

RMON – RMON 1 MIB groups and functions

- Filter: performs filter function that enables capture of desired parameters.
- Packet capture: provide packet capture capability for gathering packets after they flow through a channel.
- Event: controls the generation of events and notifications.

RMON – RMON 1 MIB group and functions

Token ring MIB group and functions

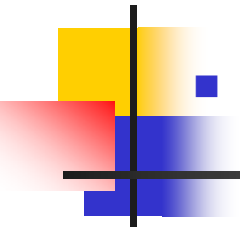
- Statistics: current utilization and error statistics of the MAC layer.
- Promiscuous statistics: current utilization and error statistics of promiscuous data.
- MAC layer history: historical utilization and error statistics of the MAC layer.
- Promiscuous history: historical utilization and error statistics of promiscuous data.
- Ring station order: Ring station order.
- Ring station configuration: active configuration of ring stations.
- Source routing: utilization statistics of source routing information.

RMON – RMON 2 MIB group and functions

- Protocol directory: inventory of protocols.
- Protocol distribution: relative statistics on octets and packets.
- Address map: MAC address to network address on the interfaces.
- Network layer host: traffic data from and to each host.
- Network layer matrix: traffic data from/to each pair of hosts.
- Application layer host: traffic data by protocol from/to each pair of hosts.
- Application layer matrix : traffic data by protocol between pairs of hosts..

RMON – RMON 2 MIB group and functions

- User history collection: user specified historical data on alarms and statistics.
- Probe configuration: configuration of probe parameters.



- atmRMON
  - .....

RMON –

Reading assignment

- Search the web for detailed information on RMON configuration
- Determine if the switch used for our experimental LAN has an RMON module. Consider how to configure it. Specifically you need to know how to use provided table to control the statistics collected and events generated. (note: the specifications for Cisco switches should be available on the Cisco site)

→network management tools