

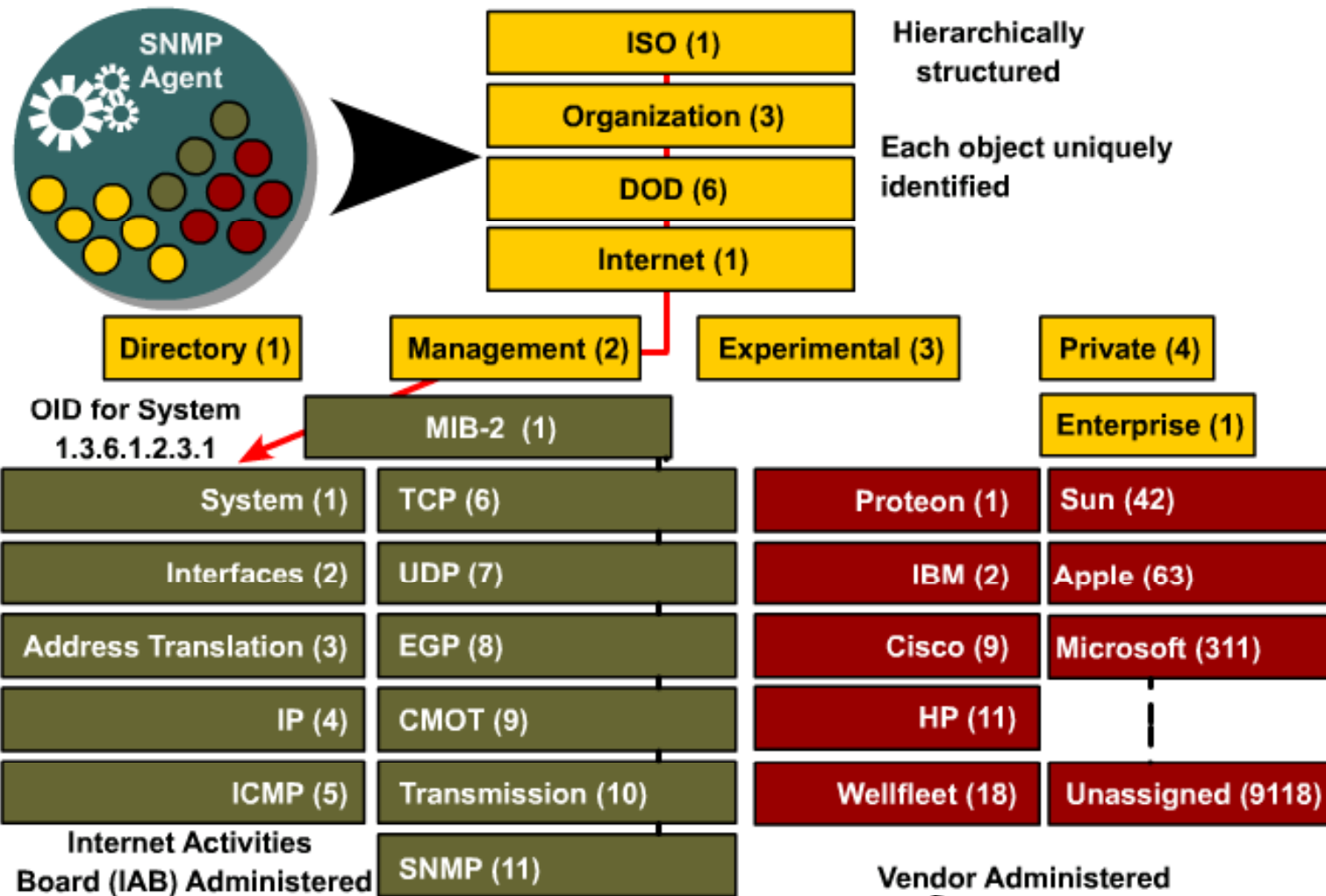
Object Identifiers

FIGURES

6.2.5 Structure of management information and MIBs

1

2

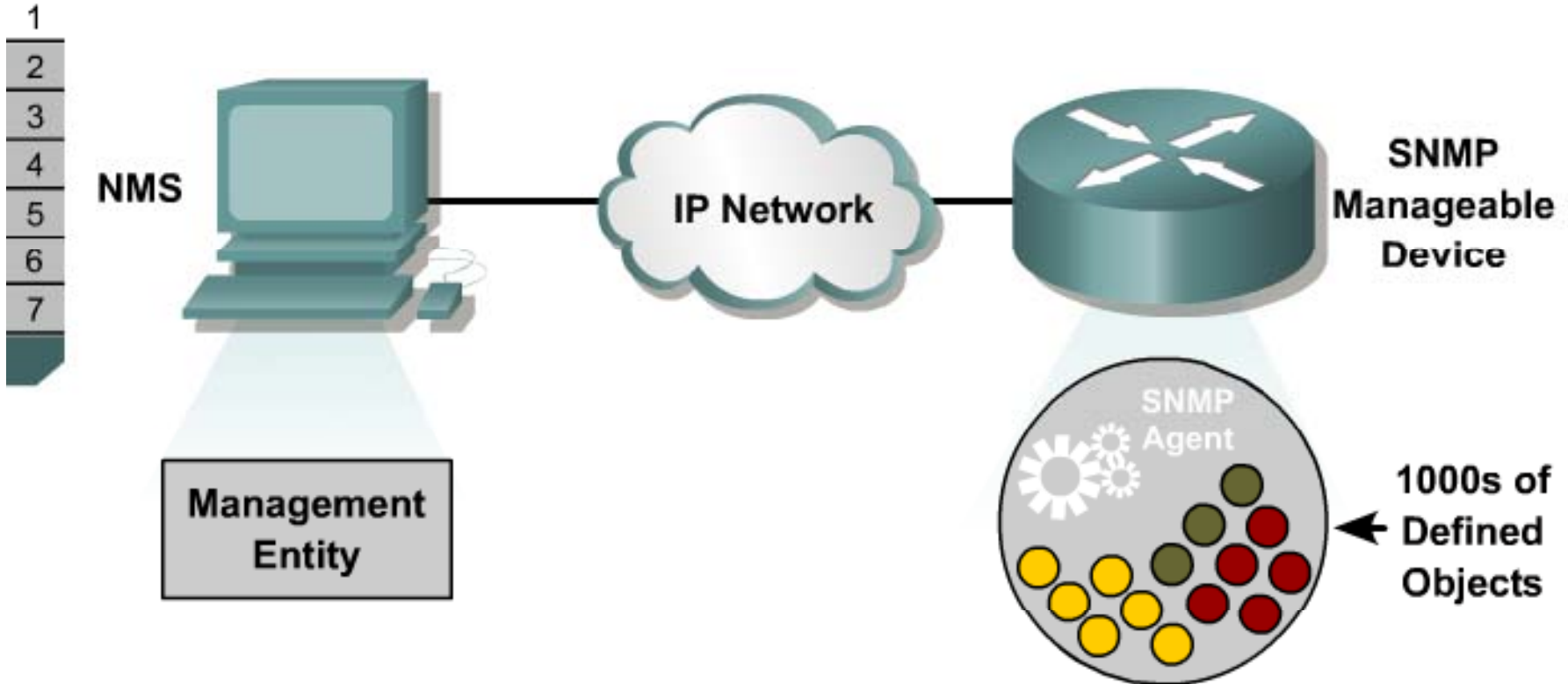


Once an assigned enterprise value has been given, the vendor is responsible for creating and maintaining sub-trees.

Understanding the Agent

FIGURES

6.2.6 SNMP protocol



- Information storehouse
- Information structured as per Structure of Management Information (SMI) standards
- Object definitions provided in many Management Information Bases (MIBs)

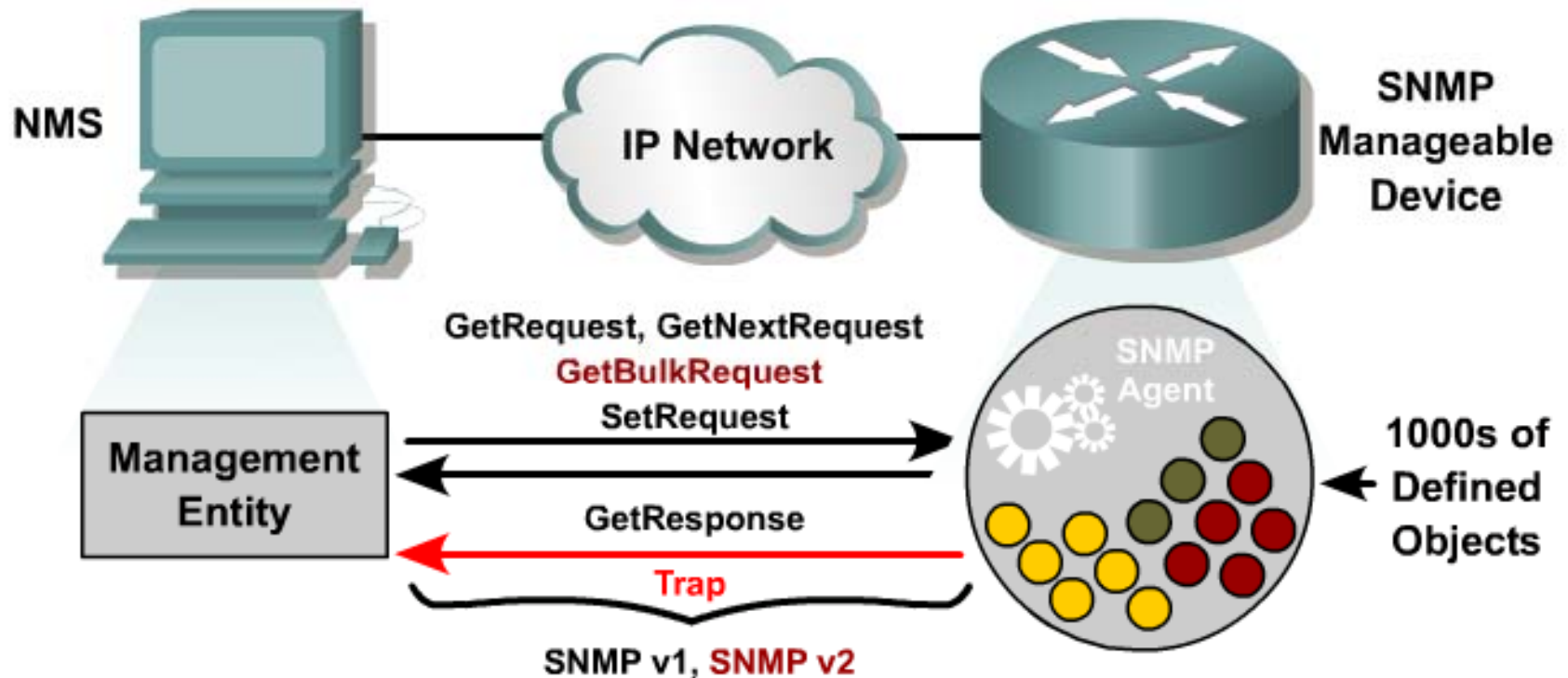
The agent is a software function embedded in most networked devices, such as routers, switches, managed hubs, printers, and servers.

Understanding the Protocol

FIGURES

6.2.6 SNMP protocol

The initial protocol specification is referred to as SNMPv1



- GetRequests used to read the value of object
- SetRequests used to modify the value of object
- Traps provide asynchronous event notification

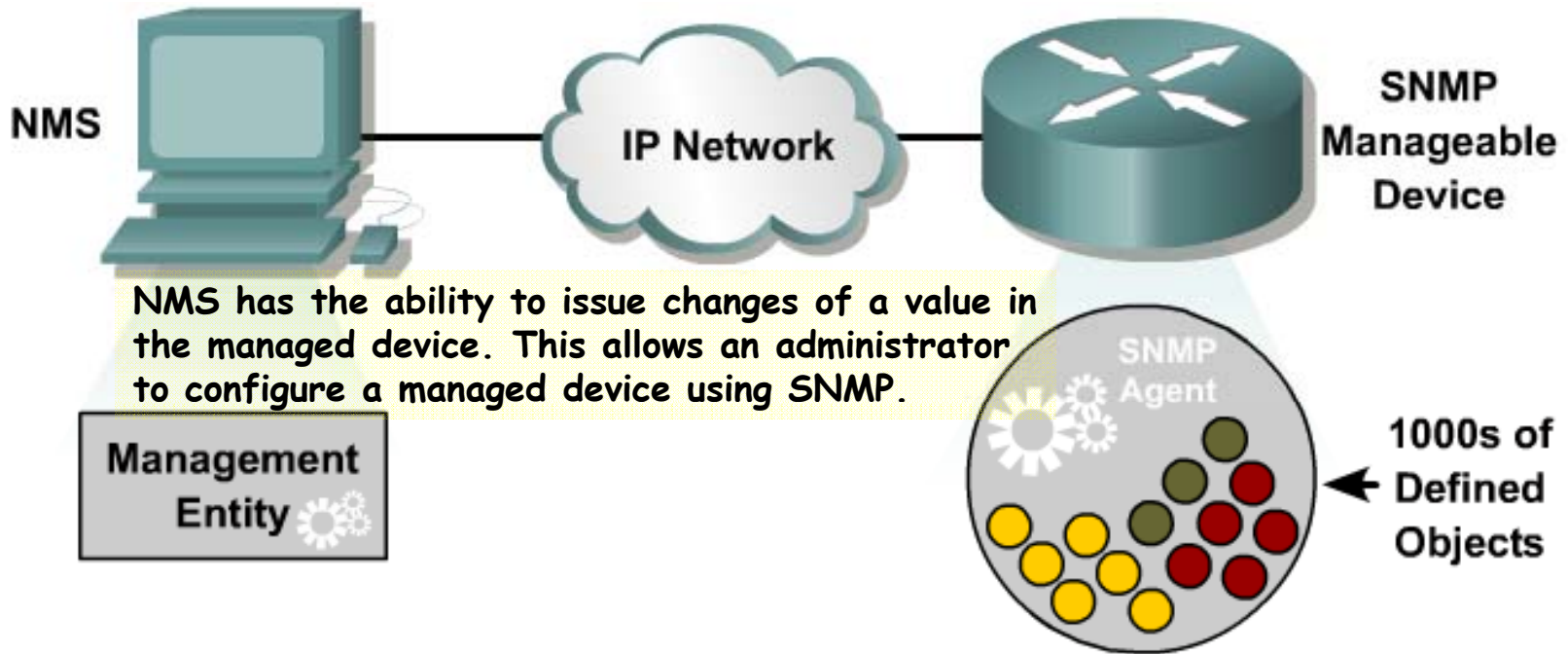
- Interaction between the manager and the agent is facilitated by (SNMP).
- The term **simple** comes from the restricted number of message types that are part of the initial protocol specification.

Understanding the Management Entity

FIGURES

6.2.6 SNMP protocol

- 1
- 2
- 3
- 4
- 5
- 6
- 7



- Management entity collects data by generating requests. This causes in-band traffic coexisting with production traffic.
- Management entity receives notifications of network alarms or events. This can be forwarded to the manager through email, or SMS.
- Management entity runs applications to analyze or interpret management data.

SNMPv2c addressed limitations in SNMPv1 introduced the *GetBulkRequest* message type and the addition of 64-bit counters to the MIB.

6.2.6 SNMP protocol

- The interaction between the manager and the managed device introduces traffic to the network.
 - Aggressive monitoring strategies can negatively affect network performance.
 - Bandwidth utilizations will go up, which may be an issue for WAN environments.
 - Moreover, monitoring has a performance impact on the devices themselves being monitored, since they are required to process the manager requests.
 - This processing should not take precedence over production services.
 - A general rule is that a minimum amount of information should be polled as infrequently as possible.
 - Determine which devices and links are most critical and what type of data is required.
-

Understanding Community Strings

FIGURES

6.2.6 SNMP protocol

1

2

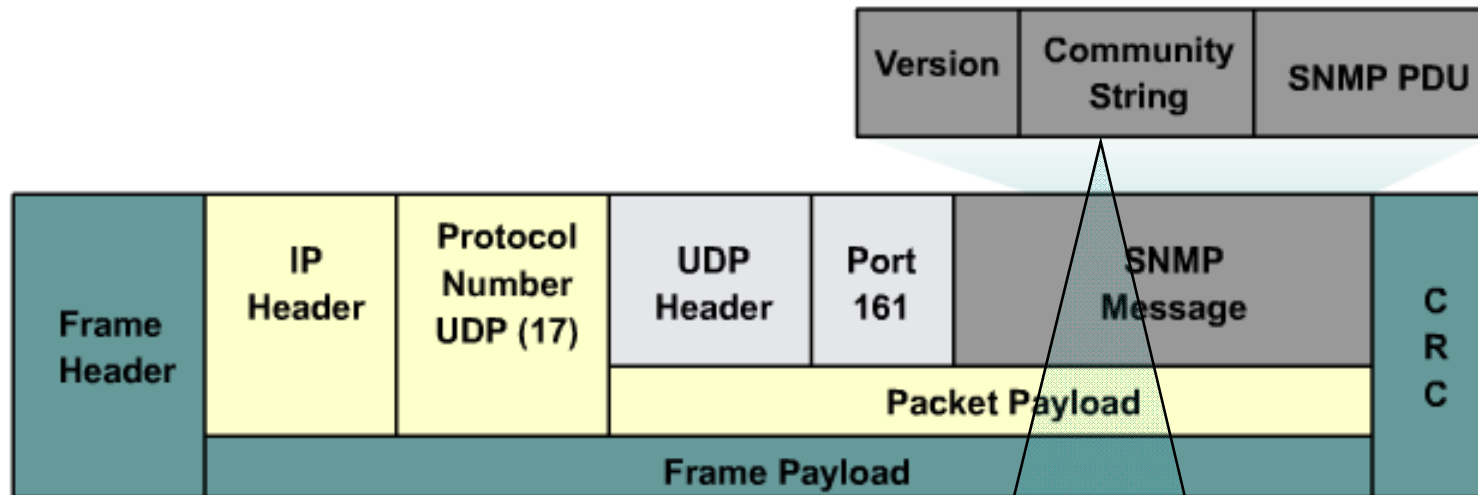
3

4

5

6

7



SNMP Protocol Data Units (PDUs) are processed as per the access policy indicated by the community string

Community strings are cleartext and provide a trivial authentication mechanism (SNMP v1, v2c)

Avoid using the well known default values for community string:

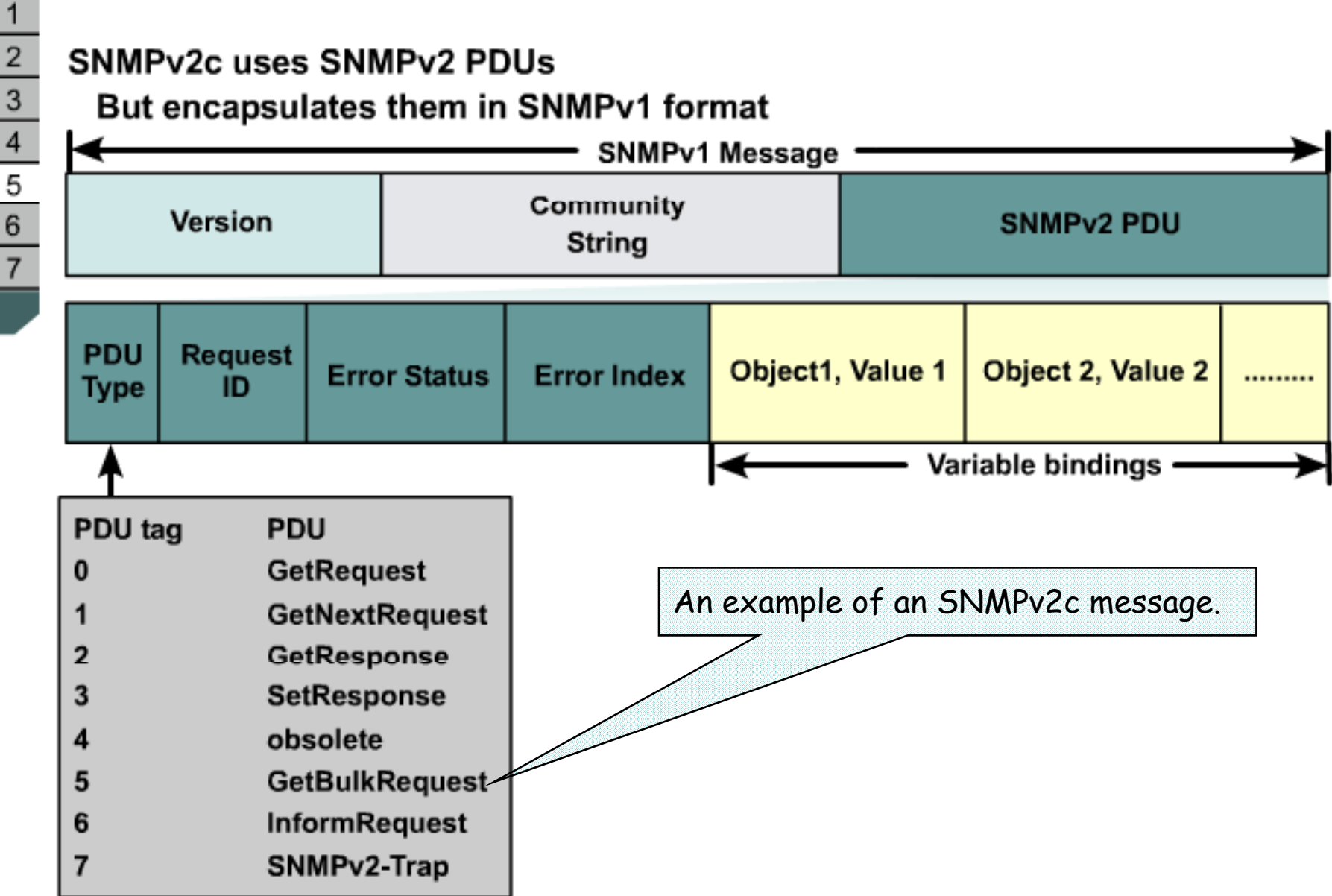
- Read-only agent access: public
- Read-write agent access: private

Each SNMP message contains a clear text string, called a community string. The community string is used like a password to restrict access to managed devices.

SNMPv2c Message Format

FIGURES

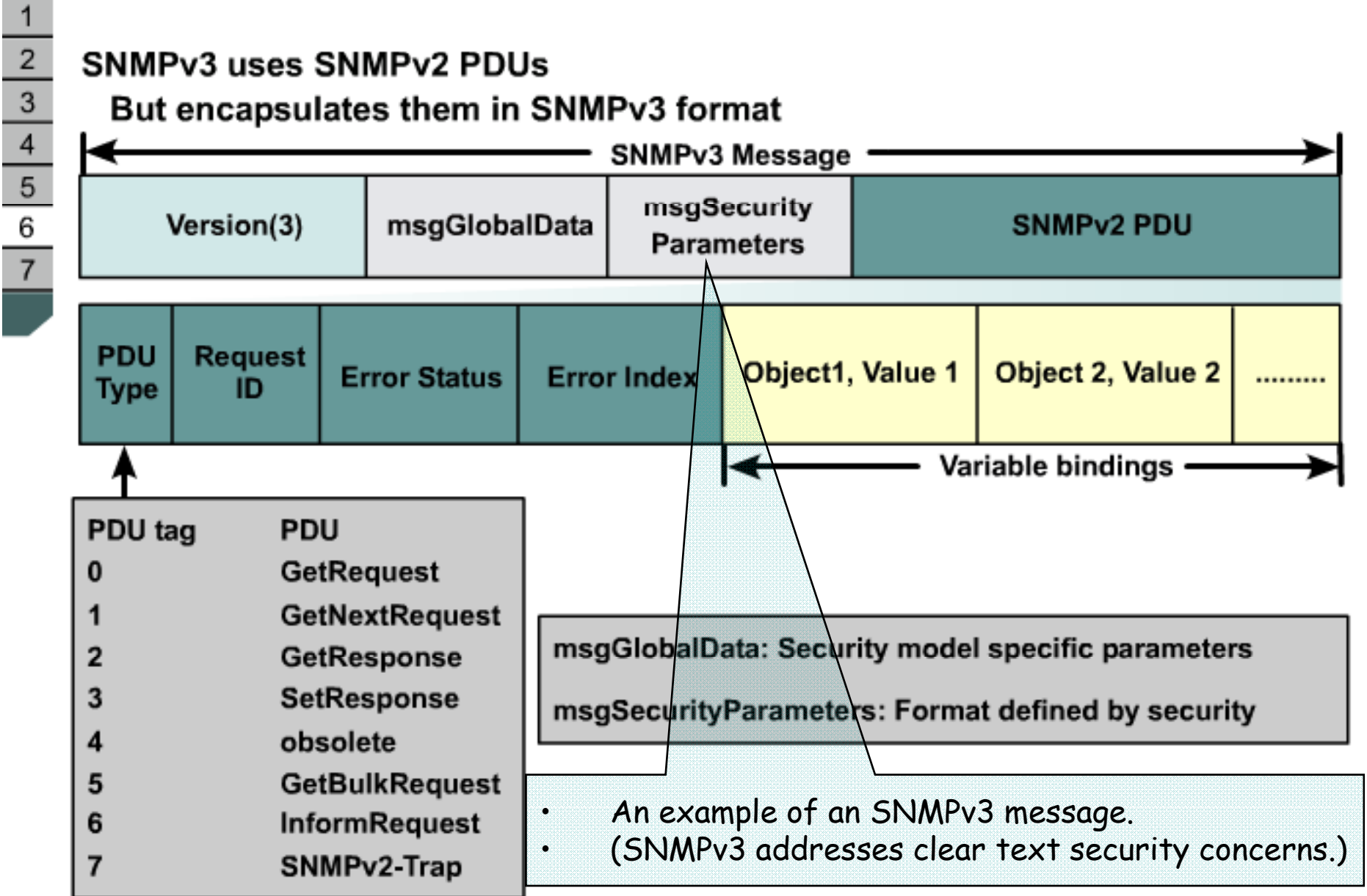
6.2.6 SNMP protocol



SNMPv3 Message Format

FIGURES

6.2.6 SNMP protocol



Management Protocols and Features

FIGURES

6.2.6 SNMP protocol

1

2

3

4

5

6

7

	Level	Auth	Encryption	What Happens
SNMPv1	noAuthNoPriv	Community String		Uses a community string match for authentication
SNMPv2c	noAuthNoPriv	Community String		Uses a community string match for authentication
SNMPv3	noAuthNoPriv	Username		Uses a username string match for authentication
SNMPv3	authNoPriv	MD5 or SHA		Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms
SNMPv3	authPriv	MD5 or SHA	DES	Adds DES 56-bit encryption in addition to authentication based on DES-56

Configuring SNMP

FIGURE

6.2.7 Configuring SNMP

1

ro - (Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.

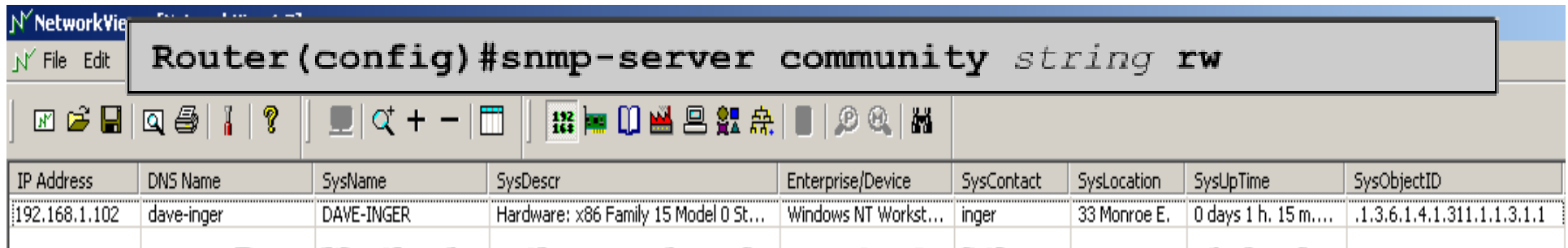
Specify the read-only community string

```
Router(config)#snmp-server community string ro
```

rw - (Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects

Specify the read-write community string

```
Router(config)#snmp-server community string rw
```



IP Address	DNS Name	SysName	SysDescr	Enterprise/Device	SysContact	SysLocation	SysUpTime	SysObjectID
192.168.1.102	dave-inger	DAVE-INGER	Hardware: x86 Family 15 Model 0 St...	Windows NT Workst...	inger	33 Monroe E.	0 days 1 h. 15 m....	.1.3.6.1.4.1.311.1.1.3.1.1

Specify the location and main contact of the managed device

```
Router(config)#snmp-server location text  
Router(config)#snmp-server contact text
```

1

2

3

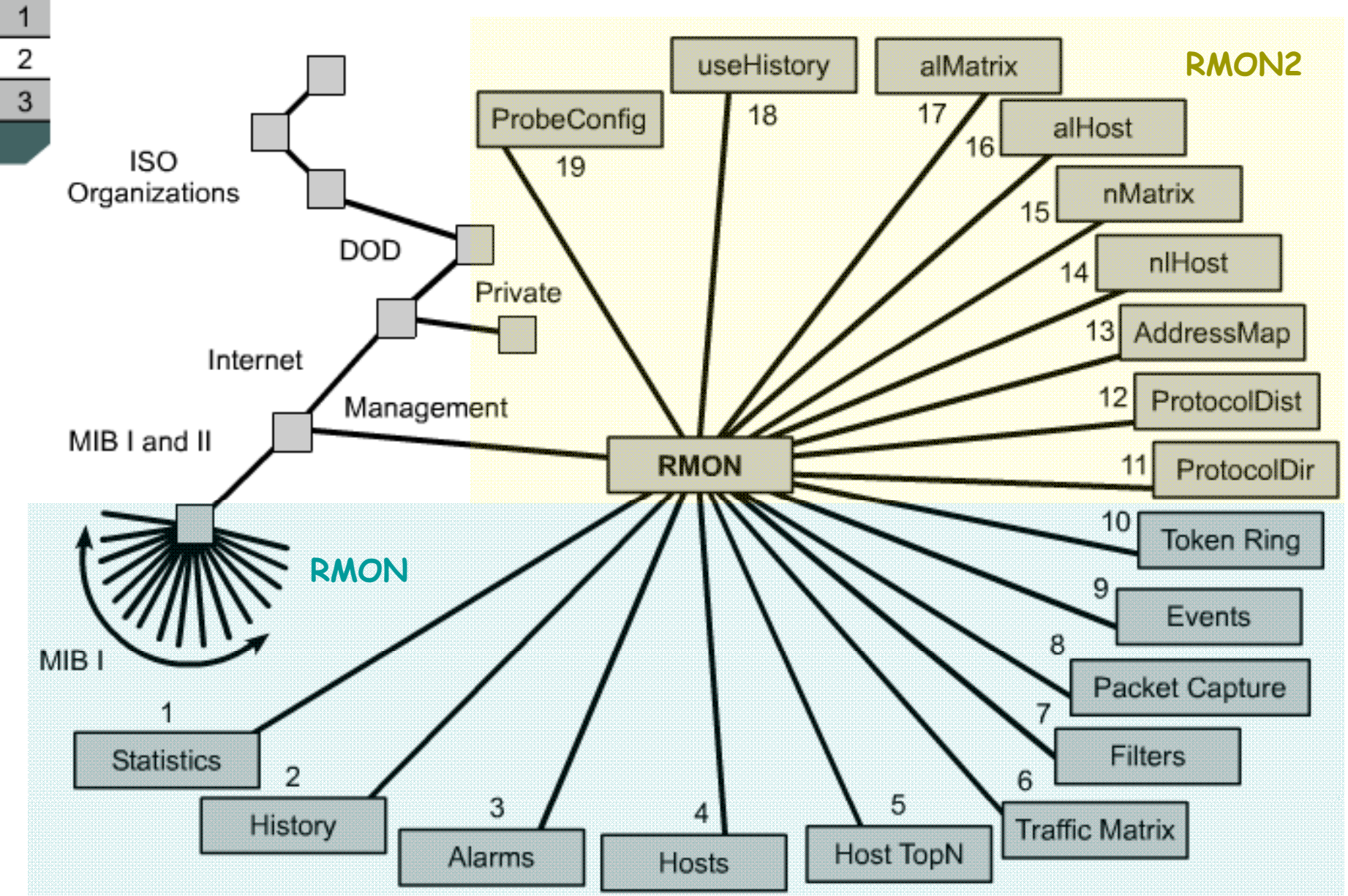
- RMON is a MIB
 - RMON is based on IETF RFCs
 - Gathers statistics by analyzing every frame on a segment
 - RMON1 is for data link layer
 - RMON2 is for the network layer to the application layer
 - Work with an external probe or a Network Analysis Module on the catalyst
-

- RMON was developed to overcome limitations in the capabilities of SNMP. SNMP can store only limited amounts of information (counters for overall traffic, number of errors, etc.), and, as it is a polled system, network loading is high.
 - RMON on the other hand, provides much more detailed information and offers a simplified manner of data collection.
 - RMON makes use of a client (like a Network Management Console, a Protocol Analyzer, or a Network Analyzer like the new Fluke Networks OptiView). The client then gathers the statistics from either one or more agents. These agents can be stand-alone RMON probes (located in strategic spots in the network) and/or embedded RMON agents in routers and switches.
 - In total RMON specifies 10 services called RMON Groups. Not all devices have to support all services as some of the RMON groups require extensive overhead (memory and processor power). Most stand-alone RMON probes will typically support all services, but embedded RMON may be limited to only a few groups.
 - The RMON client communicates directly to the RMON agent. RMON1 only collects data at the MAC level, so you will only get information on the captured packets by decoding them with a Protocol Analyzer. A switch will limit your view of the network.
 - RMON2 has been developed to provide data on higher level protocols such as IP and IPX, and up through the stack to the applications layer.
 - RMON2 provides full information on which protocols are being used on the network and the mix between them, standard RMON host and matrix information also for the network and applications layers, and a customizable history function that can be used for base-lining.
-

RMON MIB

FIGURES

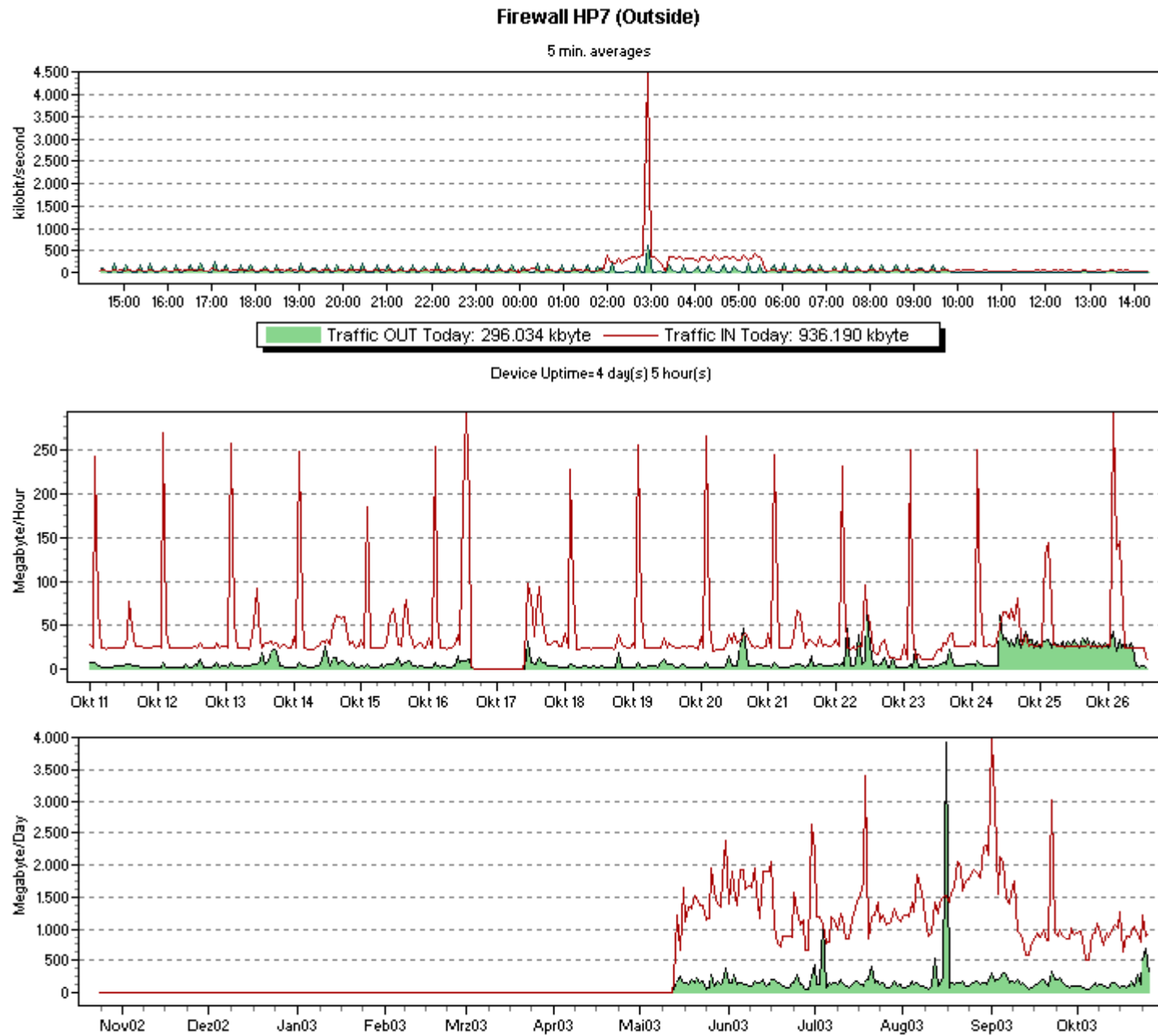
6.2.8 RMON



1. Statistics (OID: 1.3.6.1.2.1.16.1) This group provides basic statistics for the given network interface type on the probe. For example, it will collect a breakdown of packet sizes on the segment over time.
 2. History (OID: 1.3.6.1.2.1.16.2) The history group is responsible for storing periodic samples of the segment for later analysis.
 3. Alarm (OID: 1.3.6.1.2.1.16.3) Using preconfigured thresholds on the probe, this group can generate alarm events when a parameter surpasses a threshold.
 4. Hosts (OID: 1.3.6.1.2.1.16.4) This group keeps track of the MAC addresses of the devices that are communicating on this segment.
 5. HostTopN (OID: 1.3.6.1.2.1.16.5) This group is used to store data regarding the top "talkers" based on some criteria provided by the management station.
 6. Matrix (OID: 1.3.6.1.2.1.16.6) This group holds a table that defines pairs of devices who are talking to one another.
 7. Filter (OID: 1.3.6.1.2.1.16.7) This group allows a Network Manager to define one or more filters, based on a value and offset, for packets that want to be captured. The definition of that filter(s) exists in this group.
 8. Capture Packets (OID: 1.3.6.1.2.1.16.8) This group requires the presence of the Filter group and provides a means of capturing packet flowing through the network interface for later review. This group actually stores the contents of each packet flowing into the interface and meeting the filter criteria.
 9. Event (OID: 1.3.6.1.2.1.16.9) This group provides the mechanism for the device to generate events and alarms. It is basically the holding table for any events that occur on the device, either through configuration or exception.
-

Principles

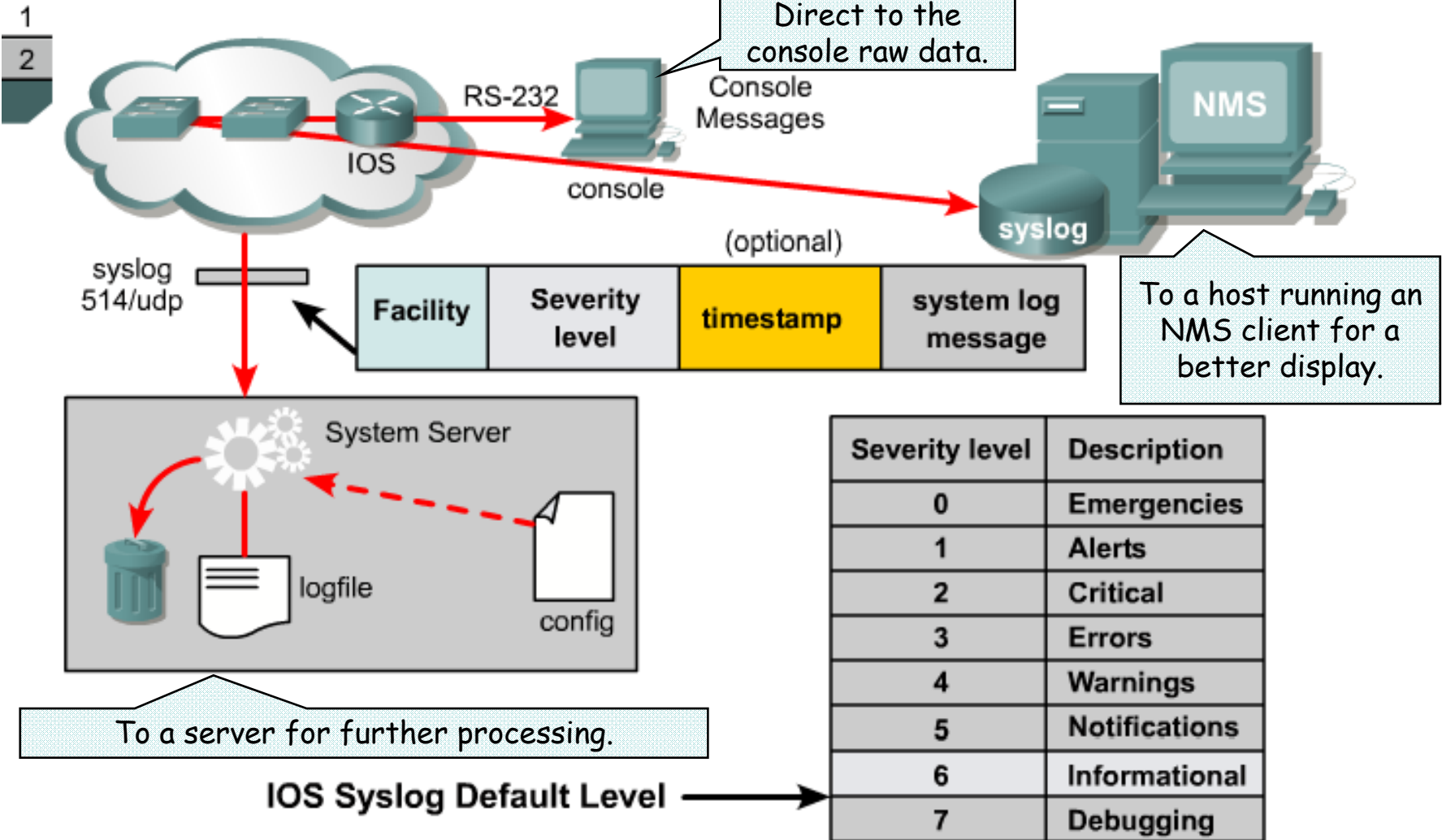
FIGURES



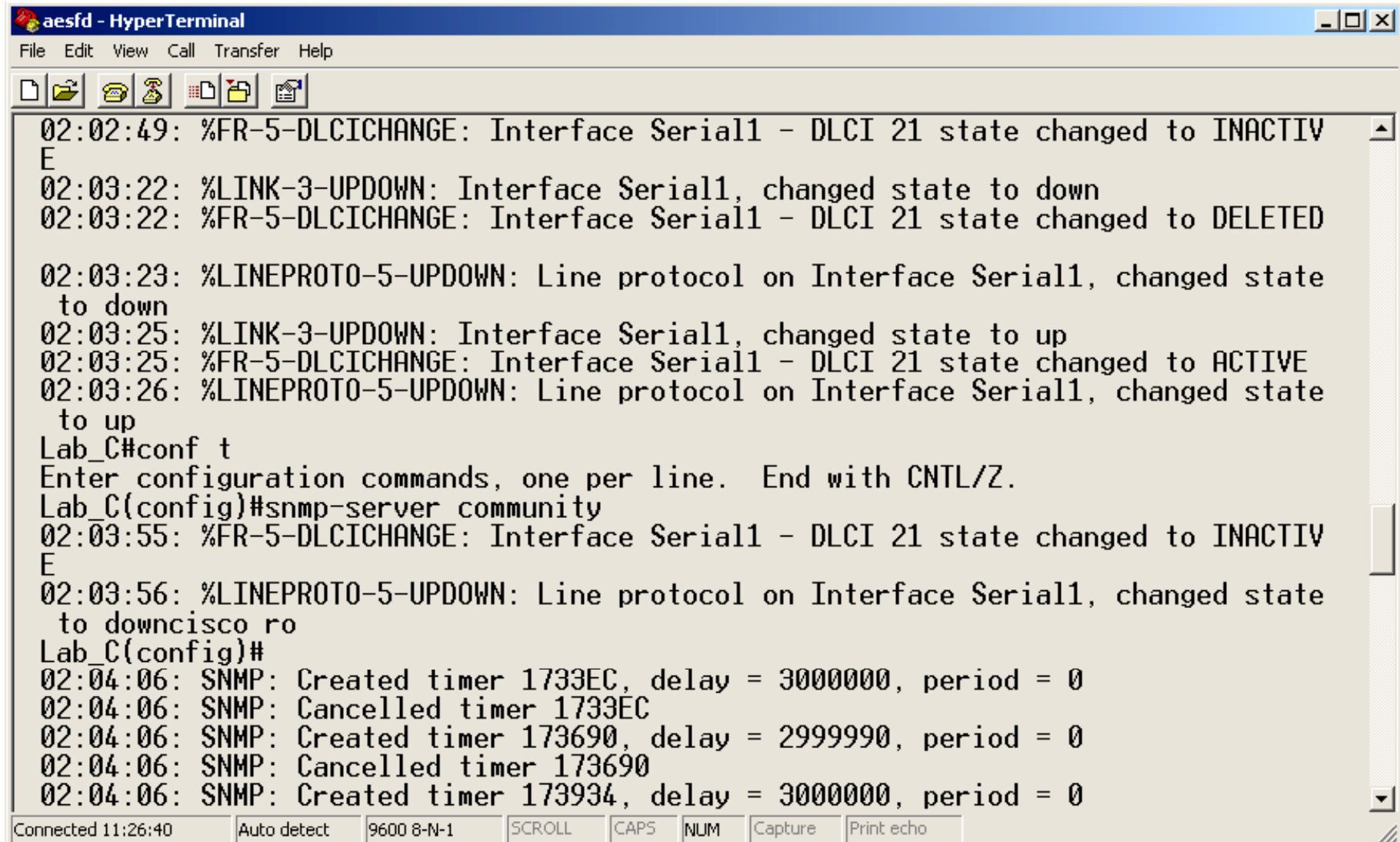
The Syslog Facility

FIGURES

6.2.9 Syslog



- The syslog utility is a mechanism for applications, processes, and the operating system of Cisco devices to report activity and error conditions.
- The syslog protocol is used to allow Cisco devices to issue these unsolicited messages to a network management station.



```
aesfd - HyperTerminal
File Edit View Call Transfer Help

02:02:49: %FR-5-DLCICHANGE: Interface Serial1 - DLCI 21 state changed to INACTIV
E
02:03:22: %LINK-3-UPDOWN: Interface Serial1, changed state to down
02:03:22: %FR-5-DLCICHANGE: Interface Serial1 - DLCI 21 state changed to DELETED

02:03:23: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state
to down
02:03:25: %LINK-3-UPDOWN: Interface Serial1, changed state to up
02:03:25: %FR-5-DLCICHANGE: Interface Serial1 - DLCI 21 state changed to ACTIVE
02:03:26: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state
to up
Lab_C#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Lab_C(config)#snmp-server community
02:03:55: %FR-5-DLCICHANGE: Interface Serial1 - DLCI 21 state changed to INACTIV
E
02:03:56: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed state
to downcisco ro
Lab_C(config)#
02:04:06: SNMP: Created timer 1733EC, delay = 3000000, period = 0
02:04:06: SNMP: Cancelled timer 1733EC
02:04:06: SNMP: Created timer 173690, delay = 2999990, period = 0
02:04:06: SNMP: Cancelled timer 173690
02:04:06: SNMP: Created timer 173934, delay = 3000000, period = 0

Connected 11:26:40 Auto detect 9600 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Configuring Syslog

FIGURES

6.2.9 Syslog

1

2

To enable logging to all supported destinations:
Router(config)#**logging on**

To send log messages to a syslog server host, such as CiscoWorks2000:
Router(config)#**logging** *hostname* | *ip address*

```
logging on
logging <hosting | IP_Addr>
logging facility local7
logging trap informational
logging source-interface loopback0
logging timestamps log datetime
```

1. Emergencies
2. Alerts
3. Critical
4. Errors
5. Warnings
6. **Notifications**
7. Informational
8. Debugging

To set logging severity level to level 6, informational:
Router(config)#**logging trap informational**

To include timestamp with syslog message:
Router(config)#**service timestamps log datetime**

Module 6: Summary

FIGURE

1

1. The functions of a workstation and a server
 2. The roles of various equipment in a client/server environment
 3. The development of Networking Operating Systems (NOS)
 4. An overview of the various Windows platforms
 5. An overview of some of the alternatives to Windows operating systems
 6. Reasons for network management
 7. The layers of OSI and network management model
 8. The type and application of network management tools
 9. The role that SNMP and CMIP play in network monitoring
 10. How management software gathers information and records problems
 11. How to gather reports on network performance
-

FIN

