

第10章

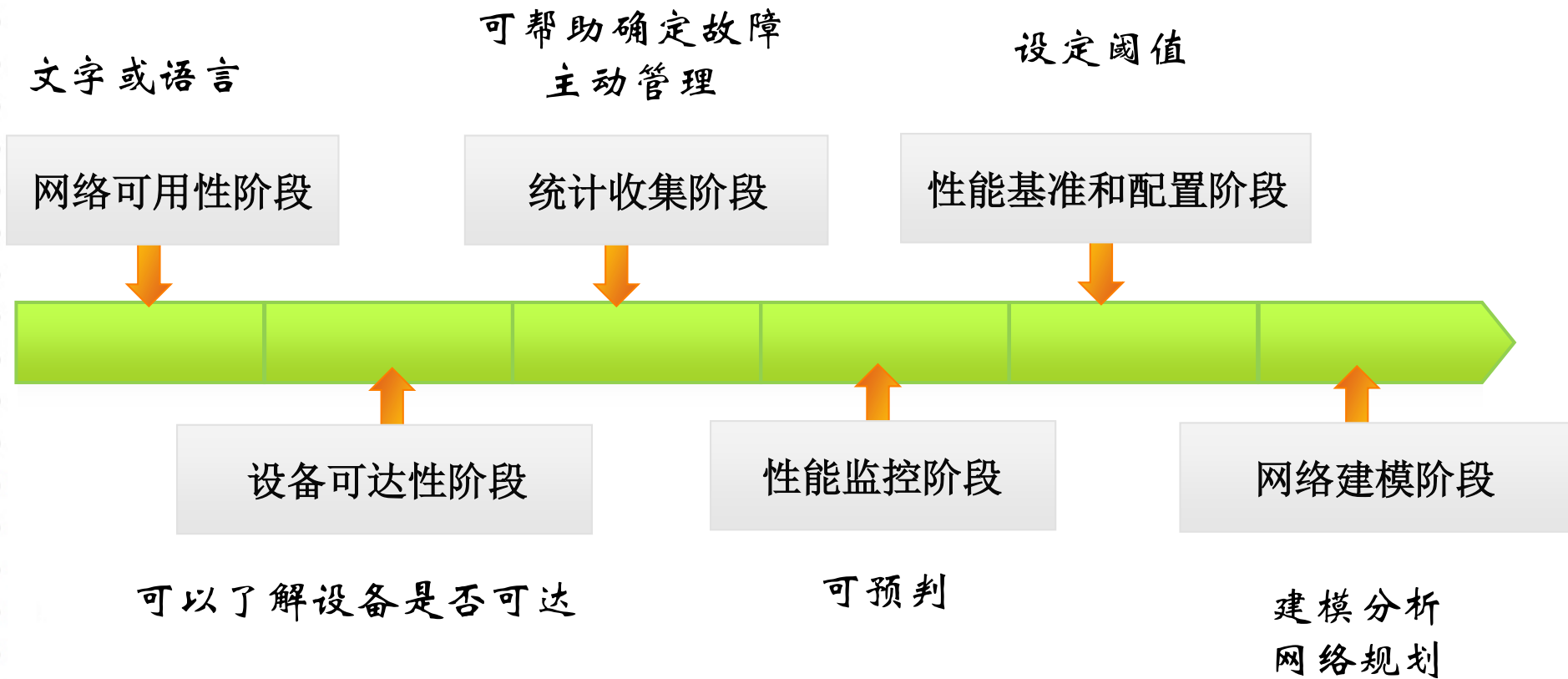
网络管理服务

服务支持



网络管理服务

网络管理



网络管理功能FCAPS

■ 目前，网络管理已涵盖了FCAPS：

◆ Fault,

◆ Configuration,

◆ Accounting,

◆ Performance

◆ Security

■ FCAPS：故障、配置、计费、性能和安全等5大网络管理功能。

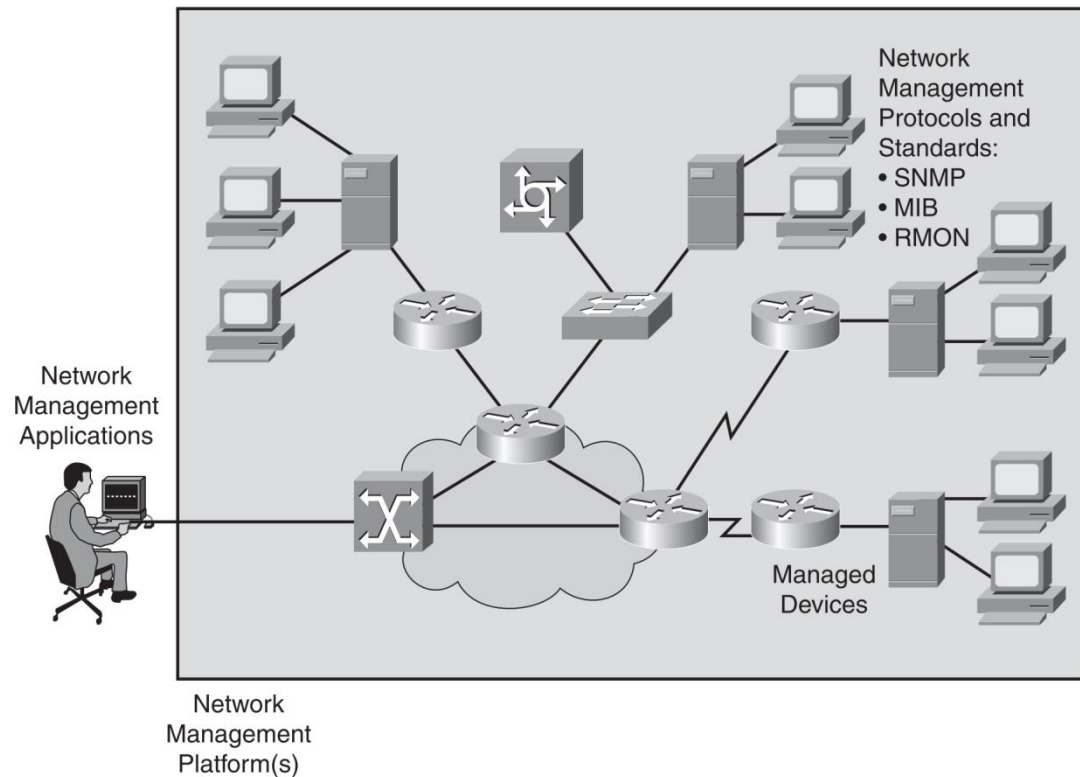
网络管理功能FCAPS

■ FCAPS 管理功能：

- ◆ **故障管理**：负责检测、隔离、通告、纠正网络中出现的故障情况。
- ◆ **配置管理**：负责跟踪和维护网络中的设备配置情况，包括配置文件、设备目录和软件的管理等功能。
- ◆ **计费管理**：负责跟踪网络设备和网络资源的使用状况，跟踪网络硬件和软件的目录信息，并提供变更控制功能。
- ◆ **性能管理**：负责收集并分析网络的性能信息，确定网络链路和网络设备的性能级别，通过收集到的网络性能信息，主动发现并纠正网络中的性能问题。
- ◆ **安全管理**：负责限制并记录用户对网络资源的访问，以防止网络遭受恶意攻击，并追踪用户对网络资源的未授权访问。

网络管理体系架构★

e 3-25 Network Management Architecture



■ 网络管理体系架构:

- ◆ **网络管理系统:**
Network management system (NMS)
- ◆ **网络管理协议:**
Network management protocol
- ◆ **被管设备:**
Managed devices
- ◆ **管理代理:**
Management agents
- ◆ **管理信息:**
Management information

remote monitoring (RMON)
Management Information Bases (MIB)
Simple Network Management Protocol [SNMP]

帶內/帶外管理

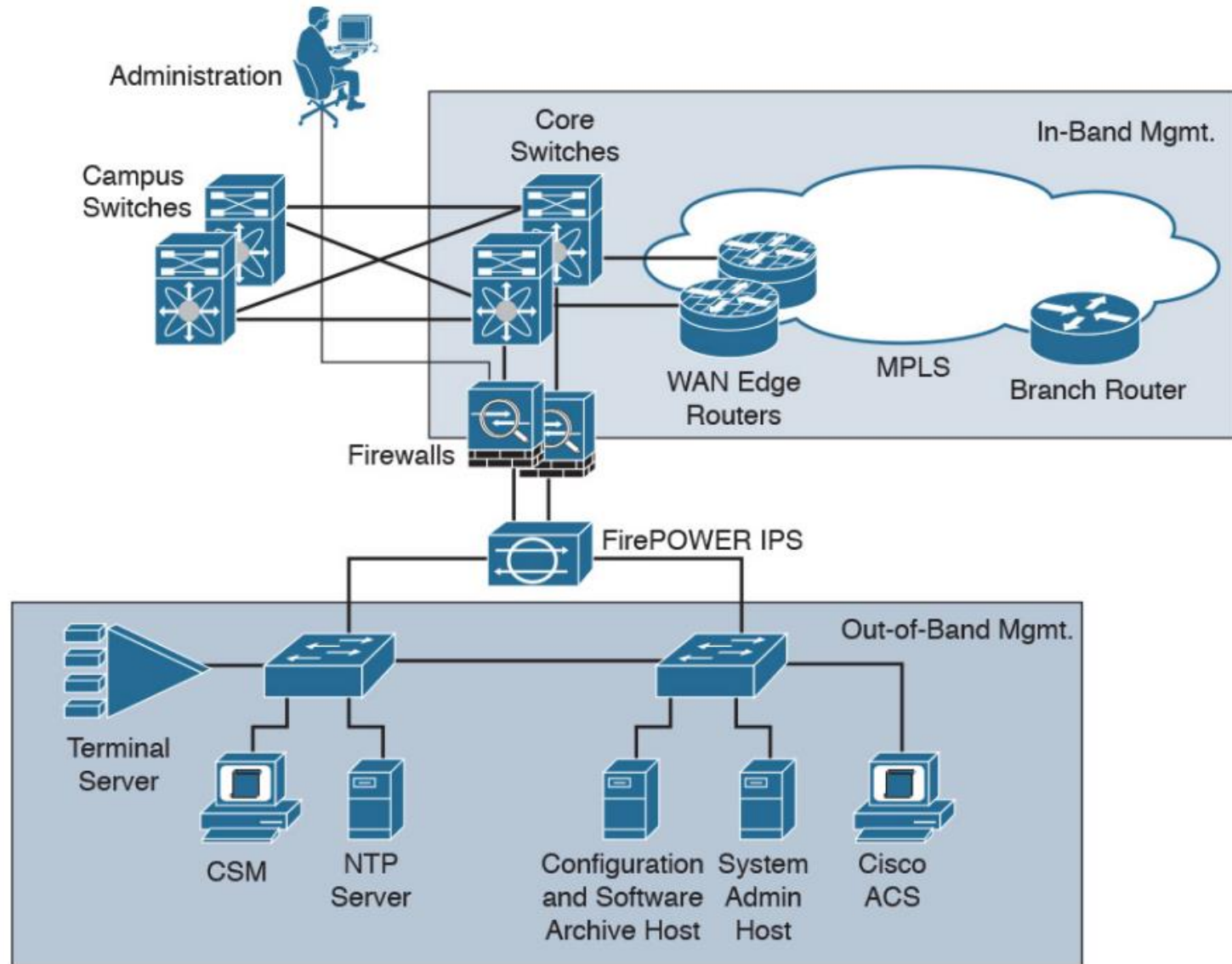
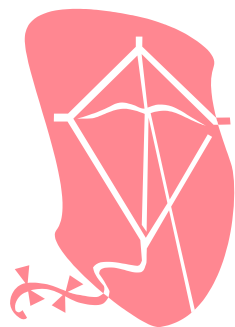


Figure 13-8 Security management network: in-band and out-of-band

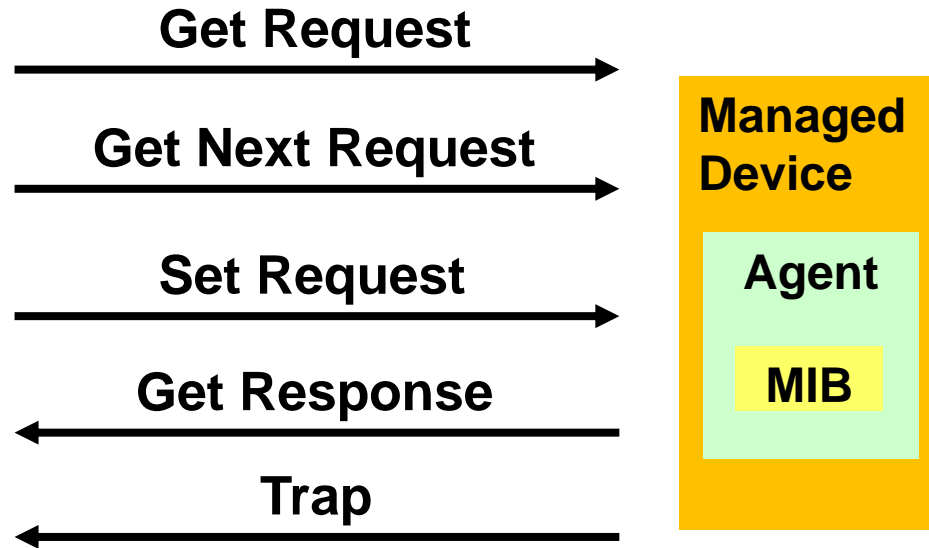
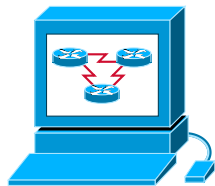
网络管理



SNMP

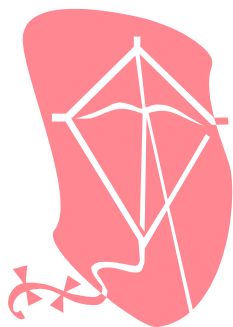
Simple Network Management Protocol [SNMP]

SNMP协议



- **SNMPv1 消息**
- **SNMPv2 增加两条新消息**
 - ◆ **GetBulk** , 批量读
 - ◆ **InformRequest**, 带确认功能的报警
- **SNMPv3 增加认证和加密功能**

网络管理



MIB

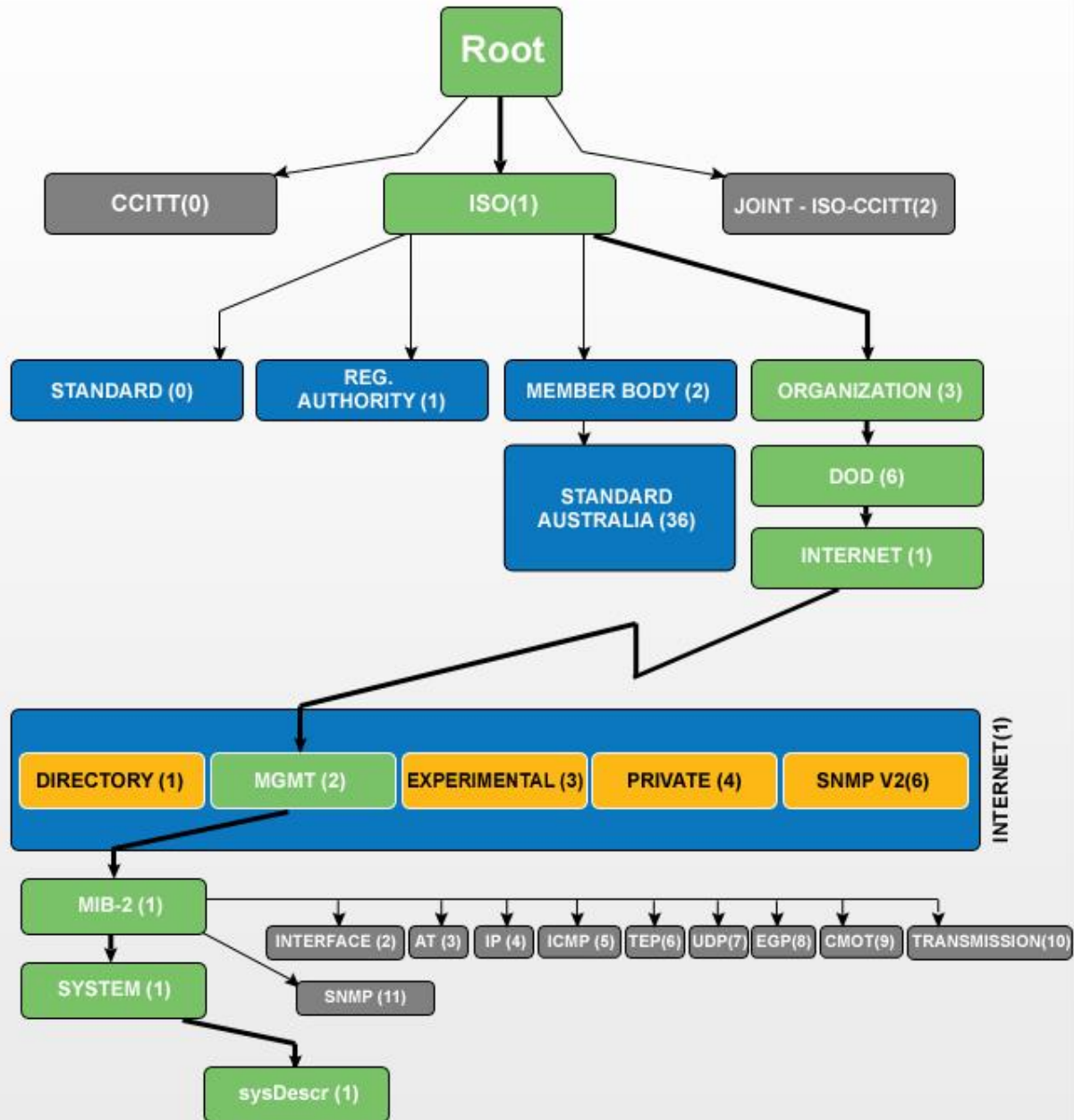
Management Information Bases (MIB)

MIB

- MIB是Management Information Base的缩写，中文名字叫“管理信息库”，它是网络管理数据的标准。
 - ◆在这个标准里规定了网络代理设备必须保存的**数据项目**，**数据类型**，以及允许在每个数据项目中的**操作**。
 - ◆通过对这些数据项目的存取访问，就可以得到该网关的所有**统计**内容。
 - ◆再通过对多个网关统计内容的综合分析即可实现基本的网络**管理**。

MIB

The Registered Tree



MIB示例

三属性:

Name

Type and syntax

Encoding

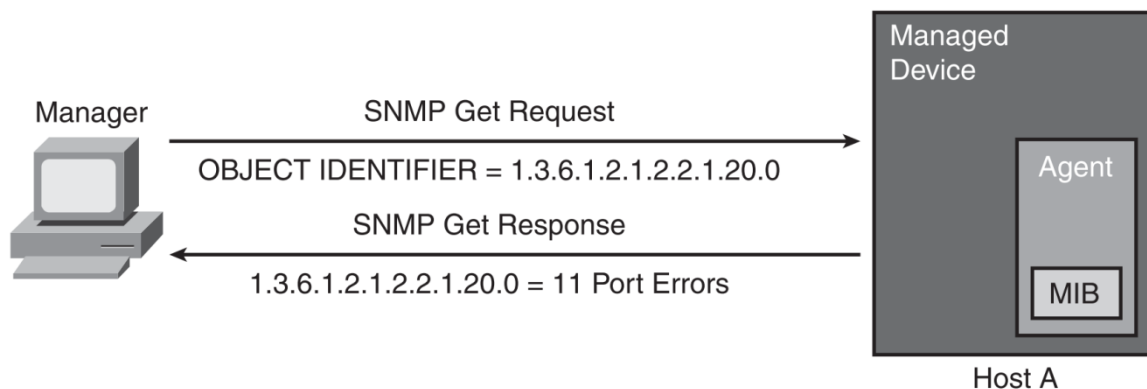
Figure 3-29 *SNMP MIB Variable Retrieval*

- Base format to retrieve the number of errors on an interface

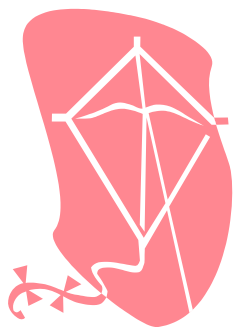
```
iso org dod internet mgmt mib interface ifTable ifEntry ifOutErrors
1 3 6 1 2 1 2 2 1 20
```

- Specific format to retrieve the number of errors on first interface

```
iso org dod internet mgmt mib interface ifTable ifEntry ifOutErrors Instance
1 3 6 1 2 1 2 2 1 20 0
```



网络管理



RMON

remote monitoring (RMON)

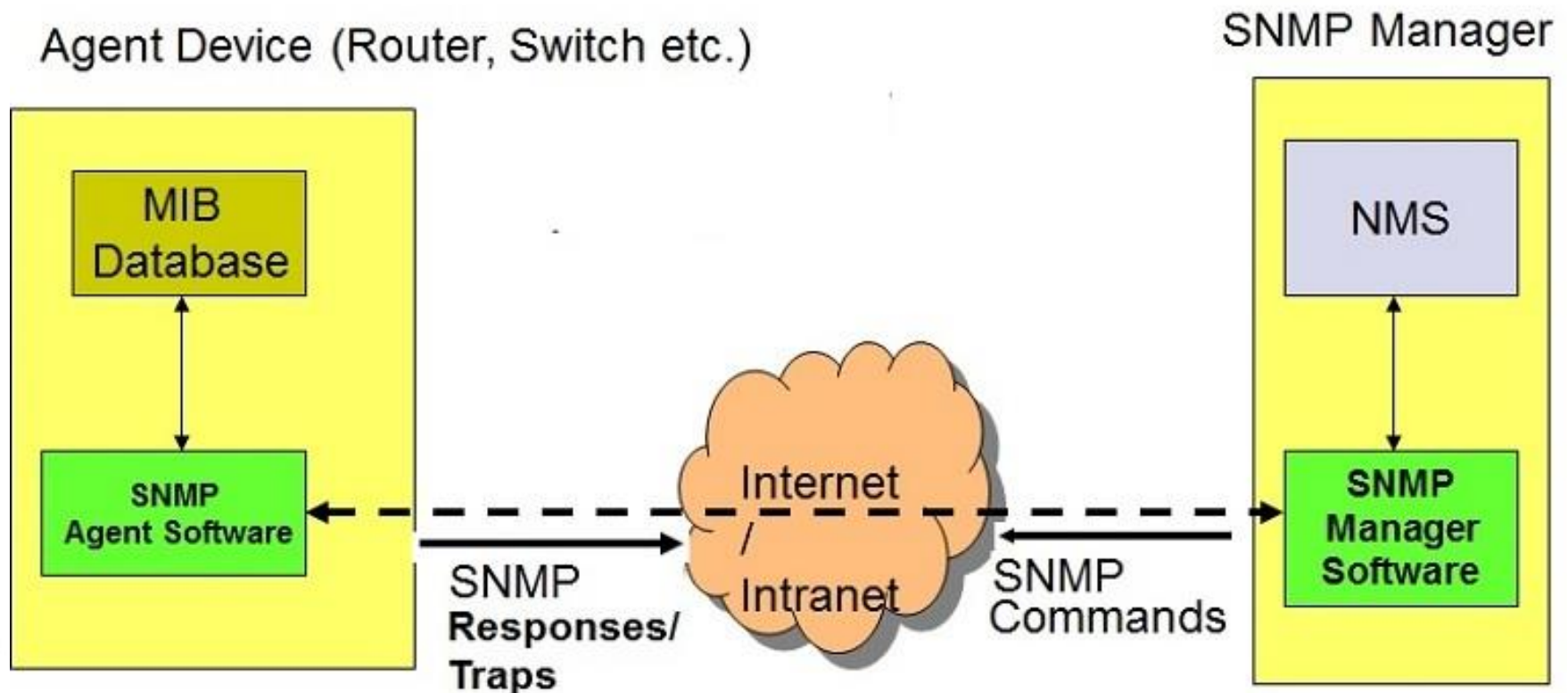
RMON与MIB ★

■ RMON 规范是由 SNMP MIB 扩展而来。

- ◆ 不使用RMON，可直接使用MIB来获取网络性能指标，但是管理流量会占用大量的带宽。
- ◆ 使用RMON，被管理设备利用RMON代理，收集和存储原来需要不断从MIB中获取的数据。

SNMP

SNMP Architecture



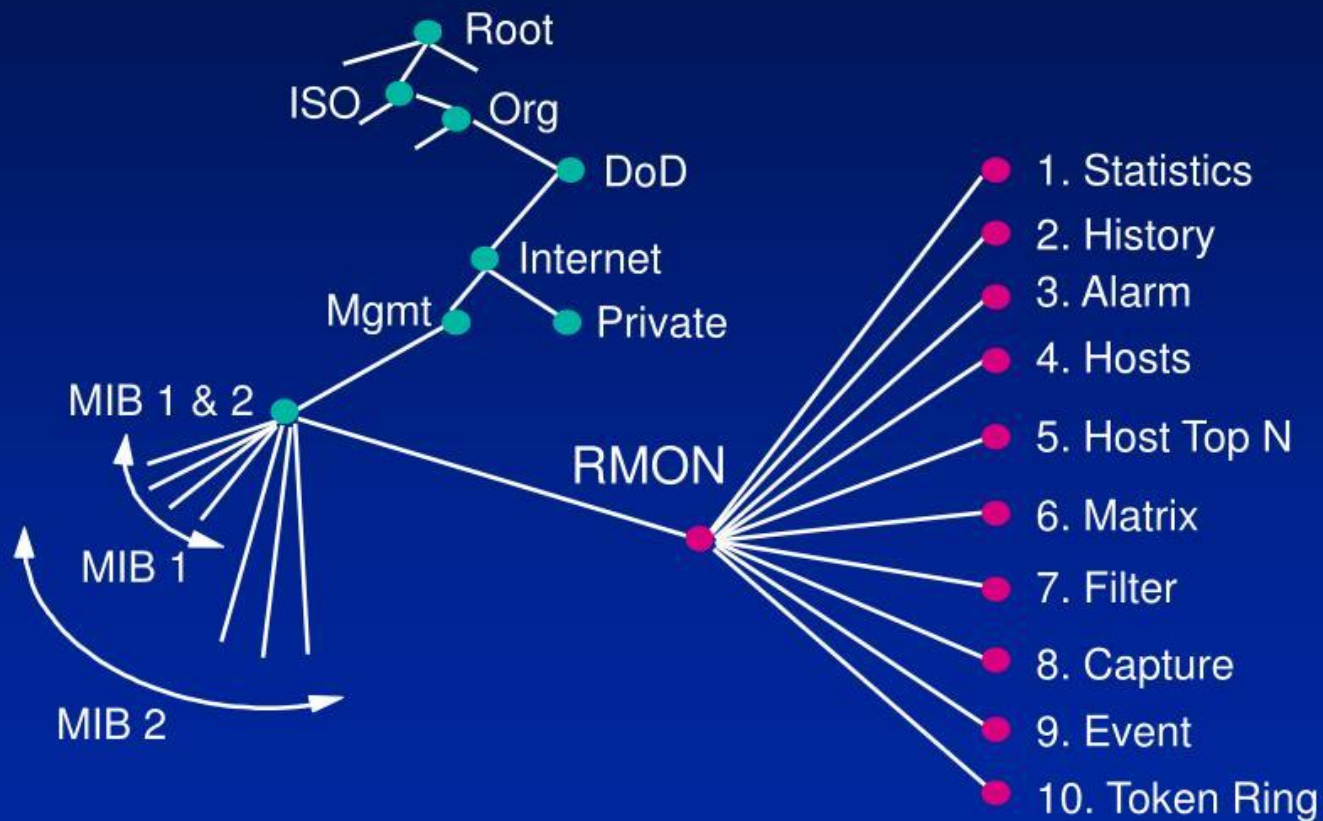
RMON

■ RMON 跟踪以下内容:

- ◆ Number of packets
- ◆ Packet sizes
- ◆ Broadcasts
- ◆ Network utilization
- ◆ Errors and conditions, such as Ethernet collisions
- ◆ Statistics for hosts, including errors generated by hosts, busiest hosts, and which hosts communicate with each other

RMON

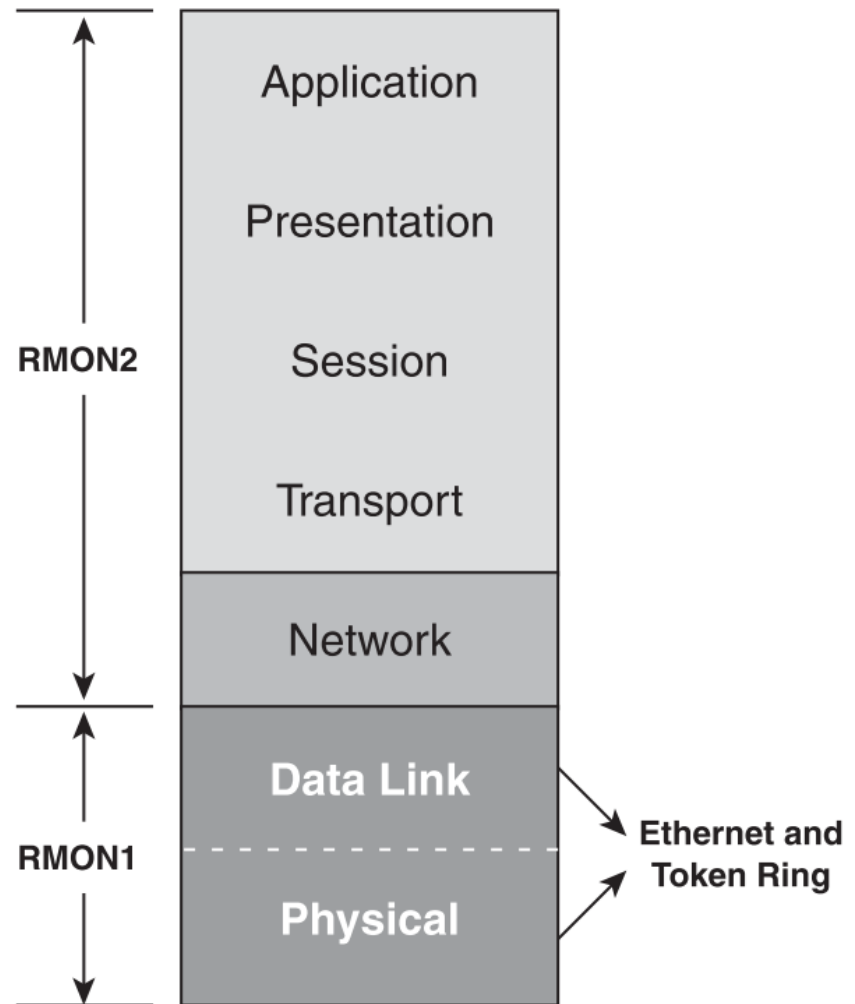
Diagram of RMON MIB



RMON版本

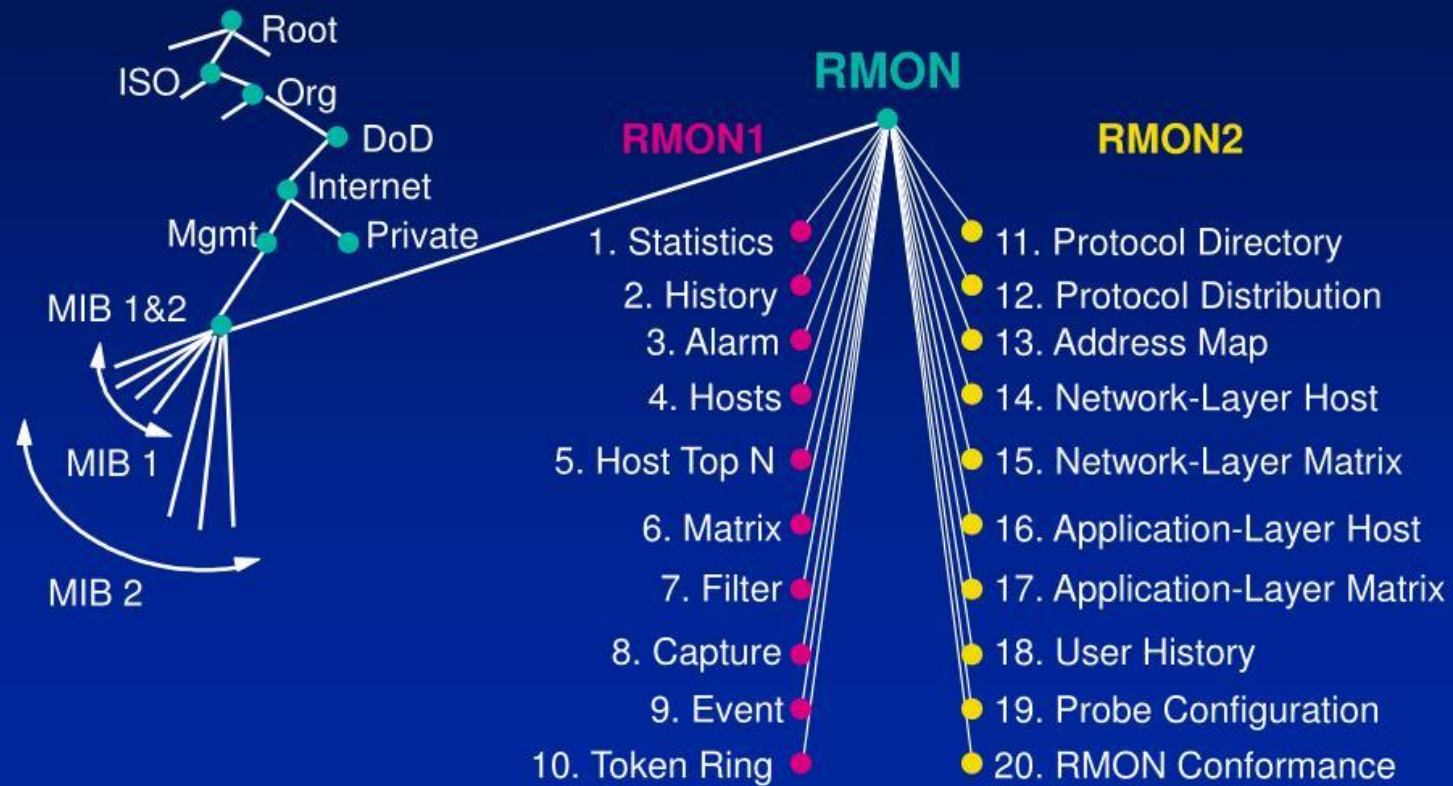
Figure 3-31 *RMON2 Is an Extension of RMON1*

- RMON2增加了更多的上层协议支持

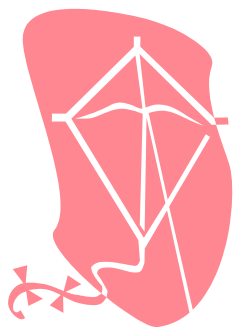


RMON2

Diagram of the RMON2 MIB



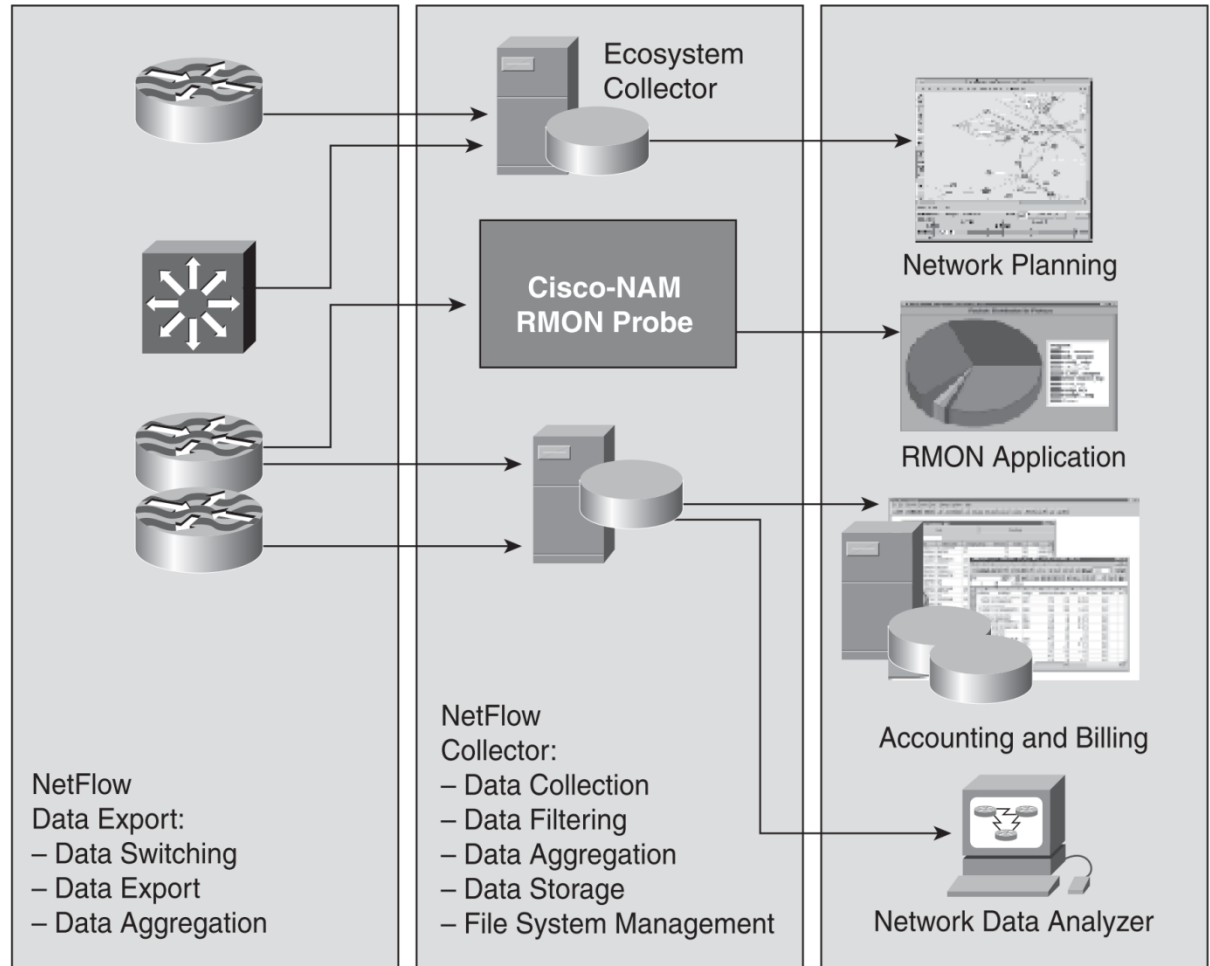
网络管理



Netflow

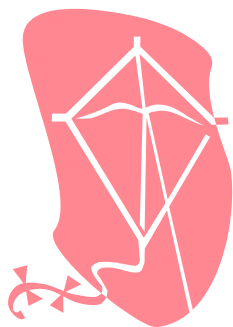
Netflow

Figure 3-33 *NetFlow Infrastructure*



Netflow, CISCO
软件。用来测量流
经**CISCO**设备的流
量，并用图表方式
进行数据呈现和分
析。

网络管理



CDP

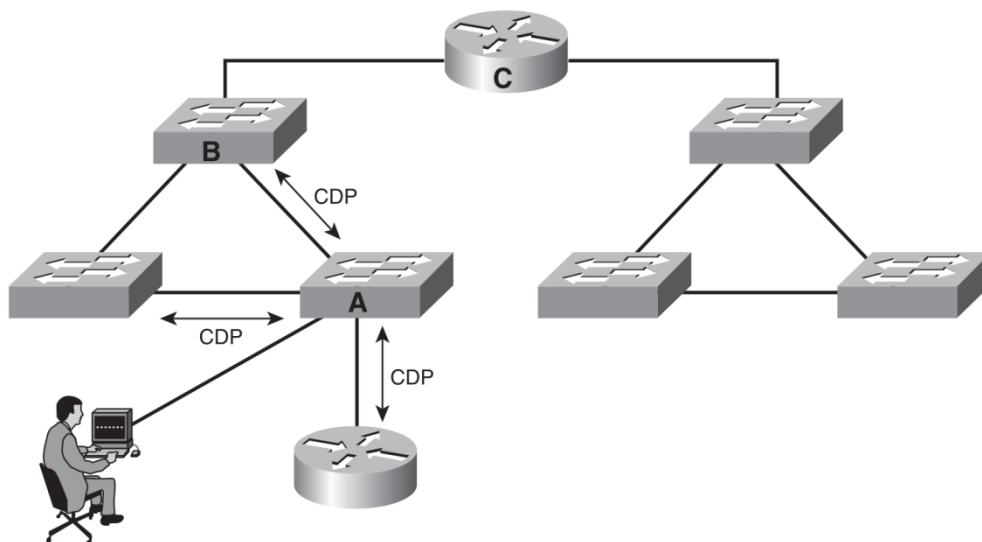
Cisco Discovery Protocol: Cisco发现协议

CDP

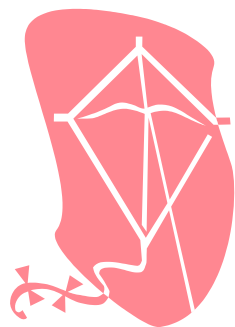
Figure 3-34 *CDP Runs at the Data Link Layer and Enables the Discovery of Directly Connected Cisco Devices*

Upper-Layer Addresses	TCP/IP	Novell IPX	AppleTalk	Others
Cisco Proprietary Data-Link Protocol	CDP discovers and shows information about directly connected Cisco devices			
Media Supporting SNAP	LANs	Frame Relay	ATM	Others

Figure 3-35 *CDP Provides Information About Neighboring Cisco Devices*



网络管理



Syslog

系统日志

syslog

Example 3-1 Syslog Messages

```
20:11:31: %SYS-5- CONFIG I: Configured from console by console

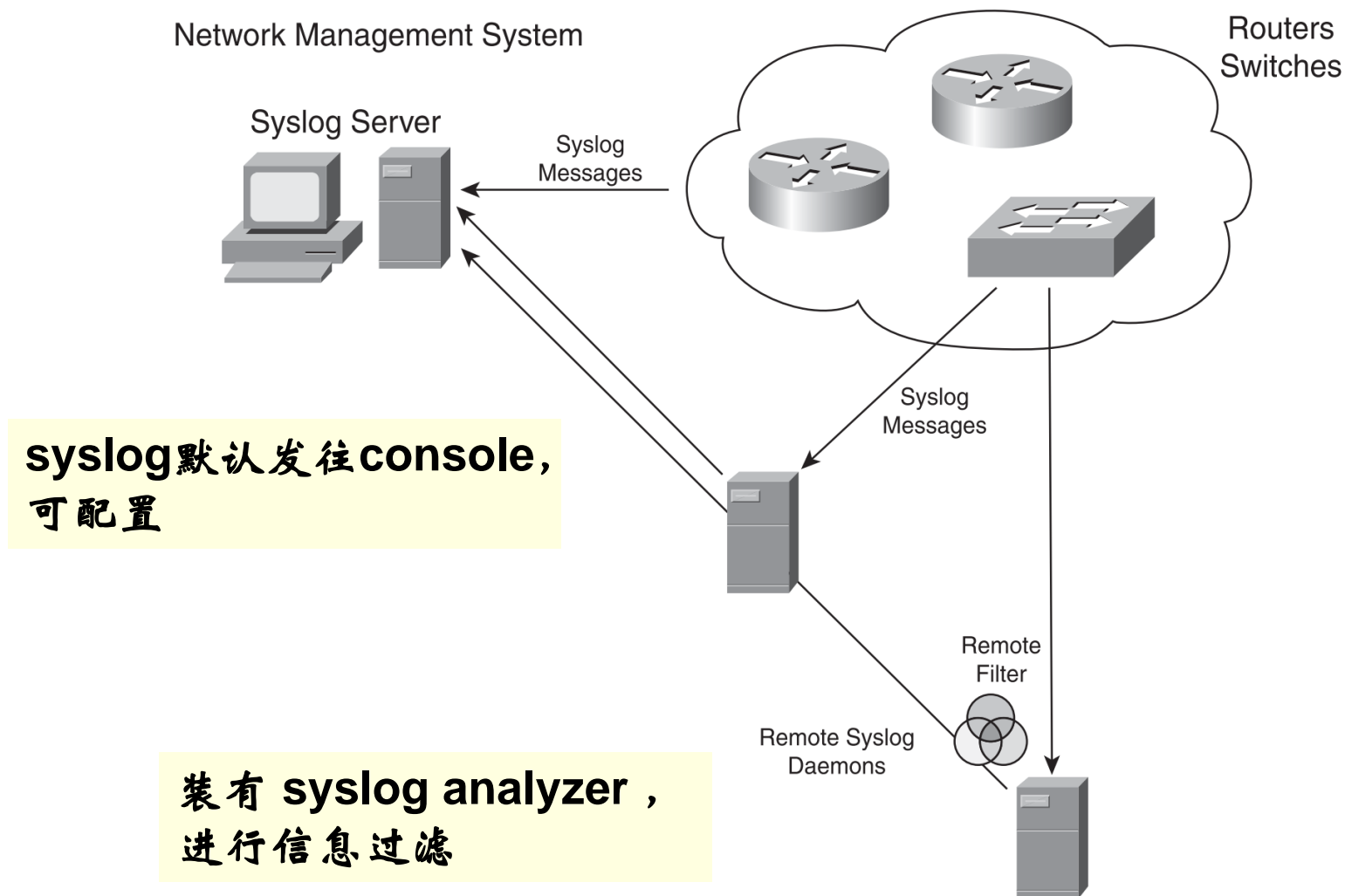
20:11:57: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively
down
20:11:58: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
to down

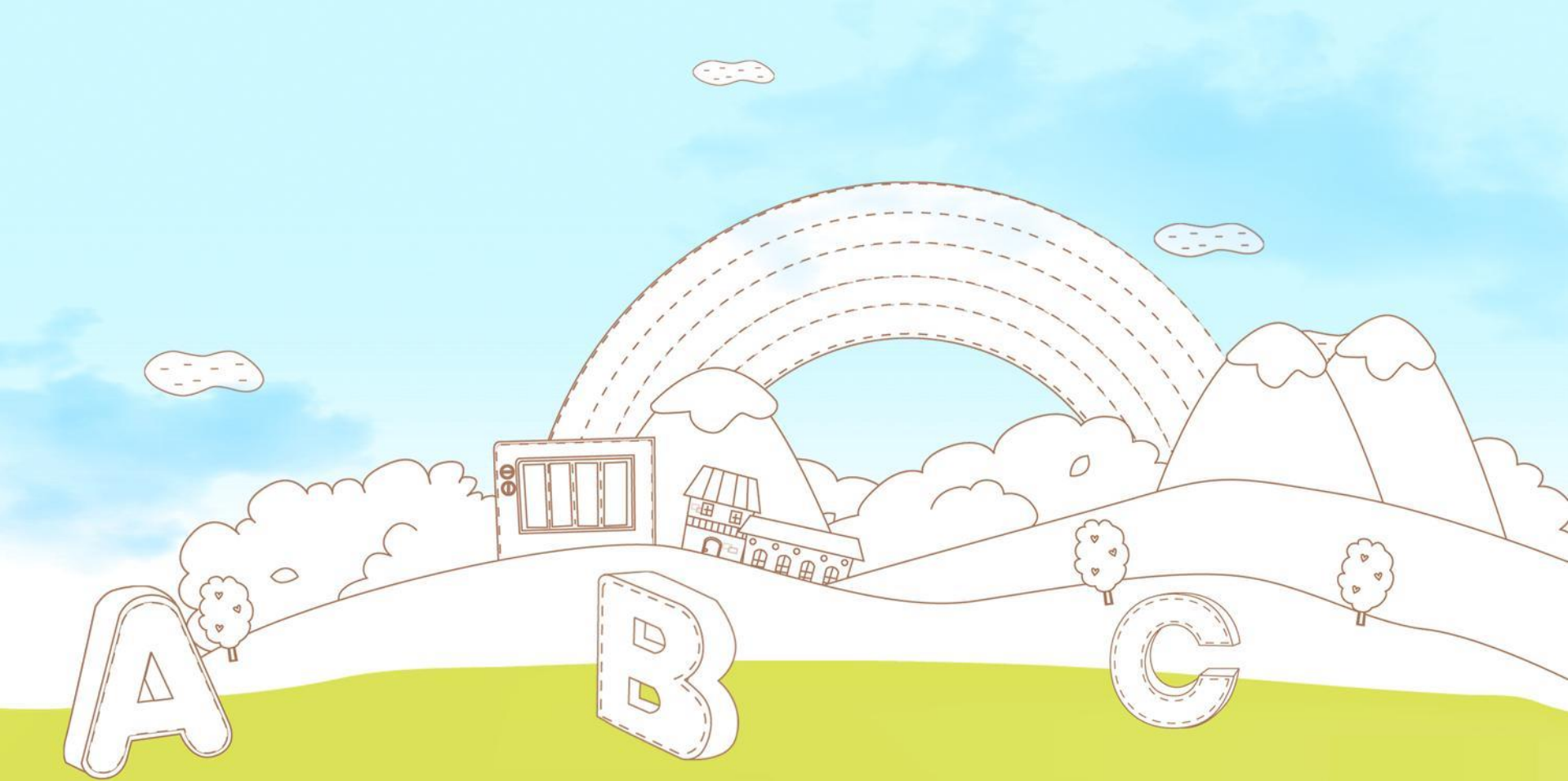
20:12:04: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
20:12:06: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
to up
20:13:53: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -
> 63.78.199.4(161), 1 packet
20:14:26: %MLS-5-MLSENABLED:IP Multilayer switching is enabled
20:14:26: %MLS-5-NDEDISABLED: Netflow Data Export disabled
20:14:26: %SYS-5-MOD_OK:Module 1 is online
20:15:47: %SYS-5-MOD_OK:Module 3 is online
20:15:42: %SYS-5-MOD_OK:Module 6 is online
20:16:27: %PAGP-5-PORTTOSTP:Port 3/1 joined bridge port 3/1
20:16:28: %PAGP-5-PORTTOSTP:Port 3/2 joined bridge port 3/2
```

seq no:timestamp: %facility-severity-MNEMONIC:description

Syslog 架构

Figure 3-36 Syslog Distributed Architecture





Thank You !