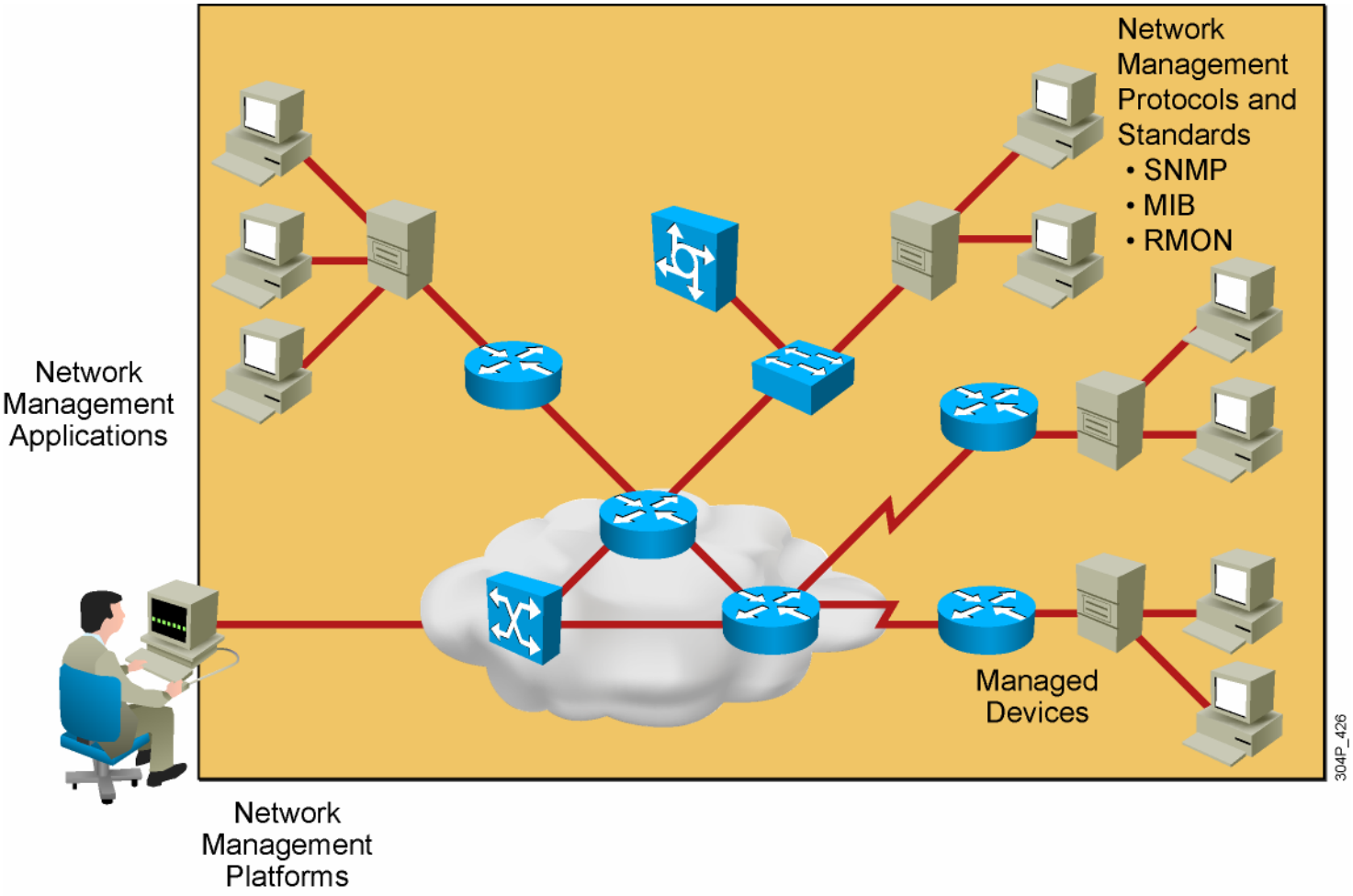
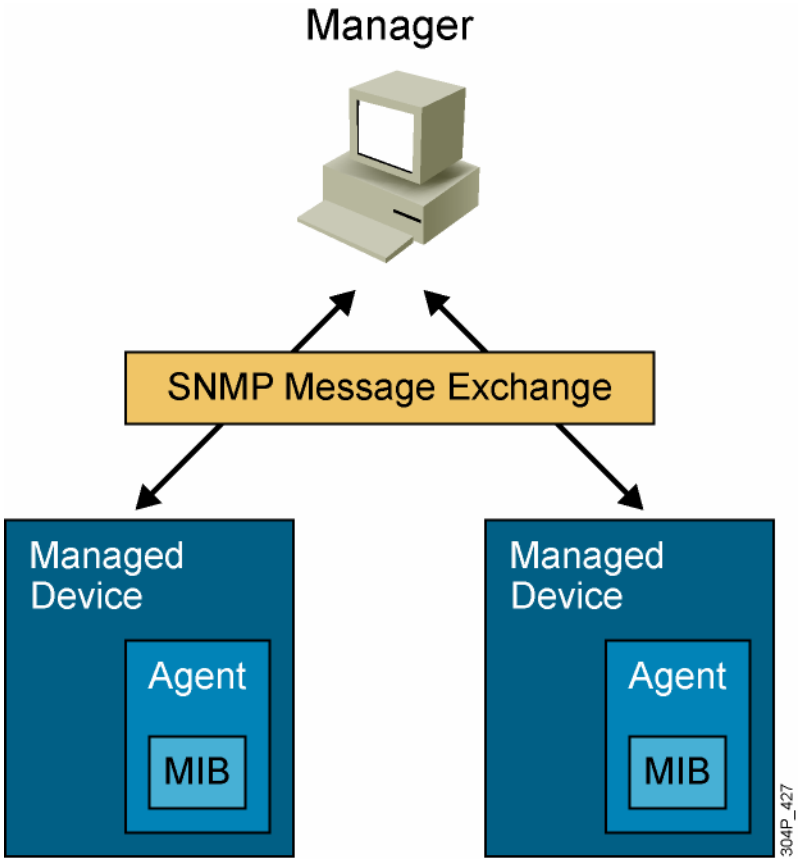
Identifying Network Management Protocols and Features

Structuring and Modularizing the Network

Network Management Overview



SNMP Overview



Manager:

- Polls agents on the network
- Correlates and displays information

SNMP:

- Supports message exchange
- Runs on IP

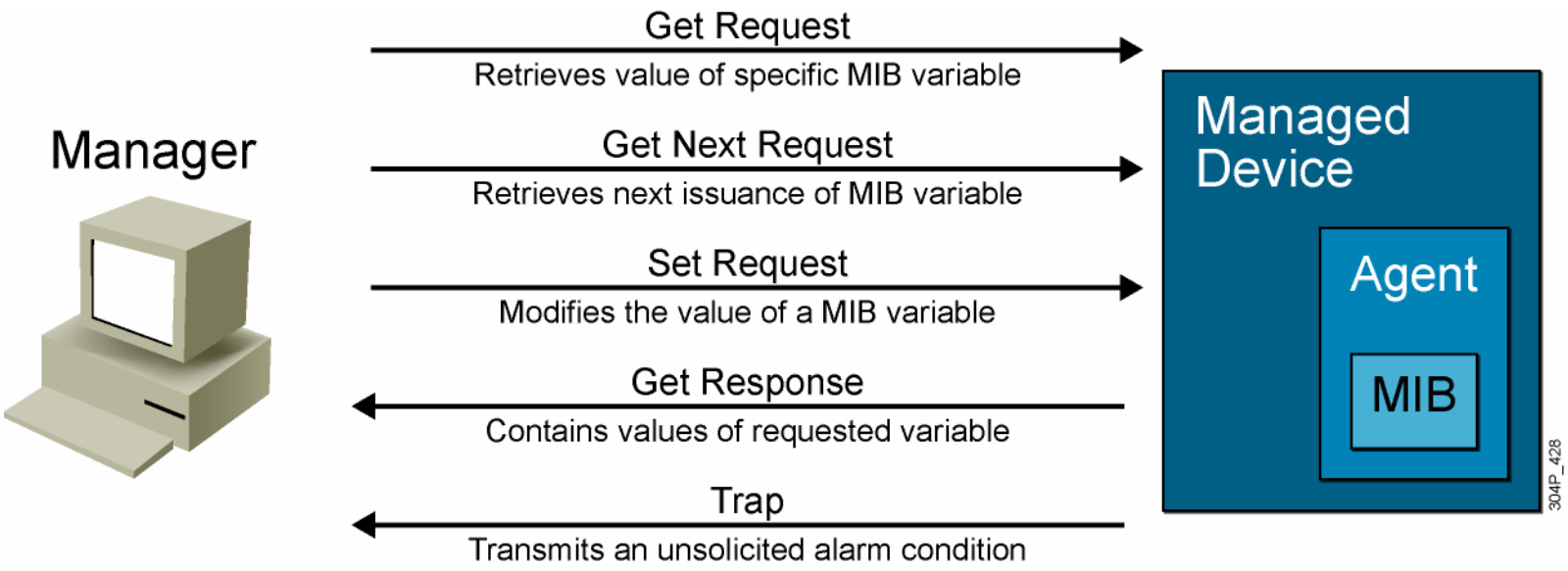
Agent:

- Collects and stores information
- Responds to manager requests for information
- Generates traps

MIB:

- Database of objects (information variables)
- Read and write community strings for controlling access

SNMPv1 Message Types



SNMP Version 2

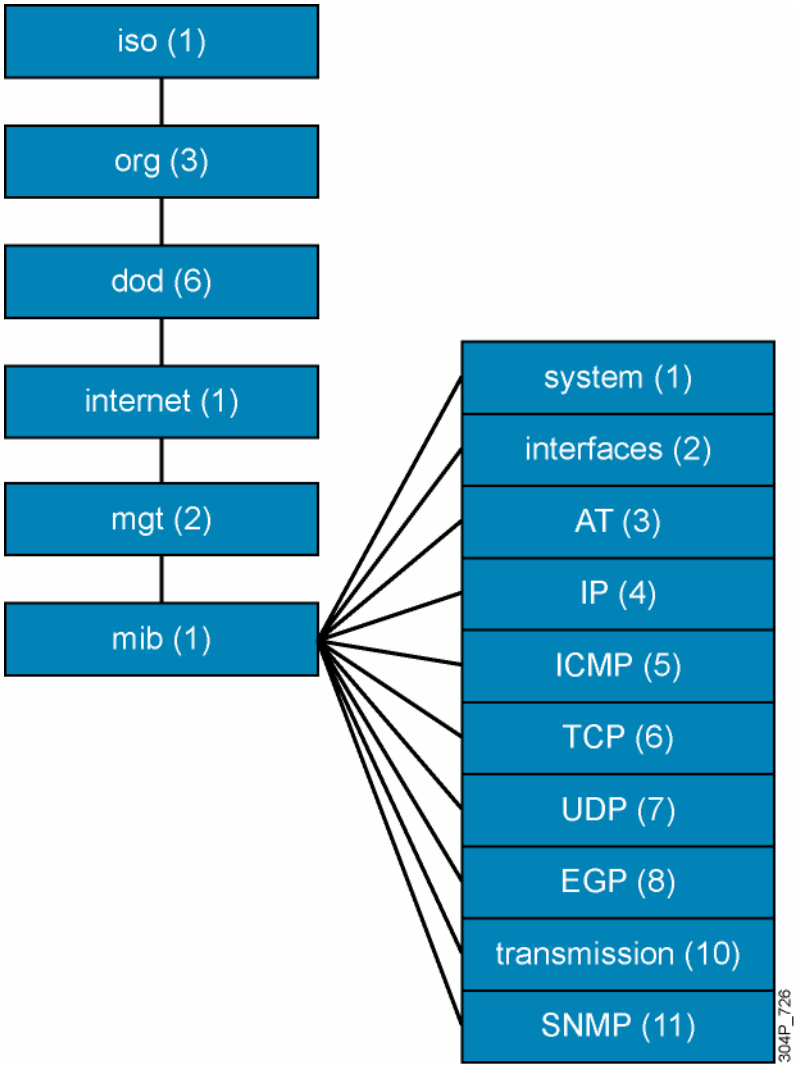
- SNMPv2 introduced in RFC 1441
- SNMPv2C defined in RFC 1901
- SNMPv2 new features:
  - Get Bulk Request
  - Inform Request
  - Data types with 64-bit values

SNMP Version 3

- RFCs 3410 through 3415
- Authentication and privacy
- Authorization and access control
- Usernames and key management
- Remotely configurable via SNMP operations
- Available since Cisco IOS Software Release 12.0

MIB Definition

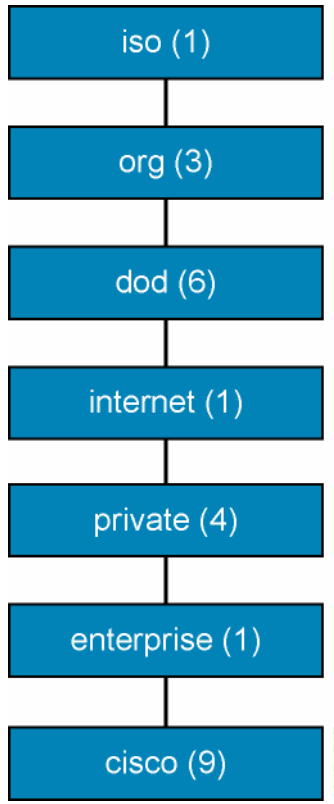
- Collection of managed objects
- Each object has a unique identifier
- Objects are grouped into a “tree”
- Standard MIBs = RFC xxxx
- Private MIBs



Example: Cisco Router MIB

- Standard managed objects:
  - Interfaces
  - Buffers
  - Memory
  - Standard protocols
- Private managed objects:
  - Small, medium, large, and huge buffers
  - Primary and secondary memory
  - Proprietary protocols
- Private extensions to MIB-II:
  - 1.3.6.1.4.1.9

    or
  - iso.org.dod.internet.private.enterprise.cisco
- Definitions available at http://www.cisco.com/public/mibs



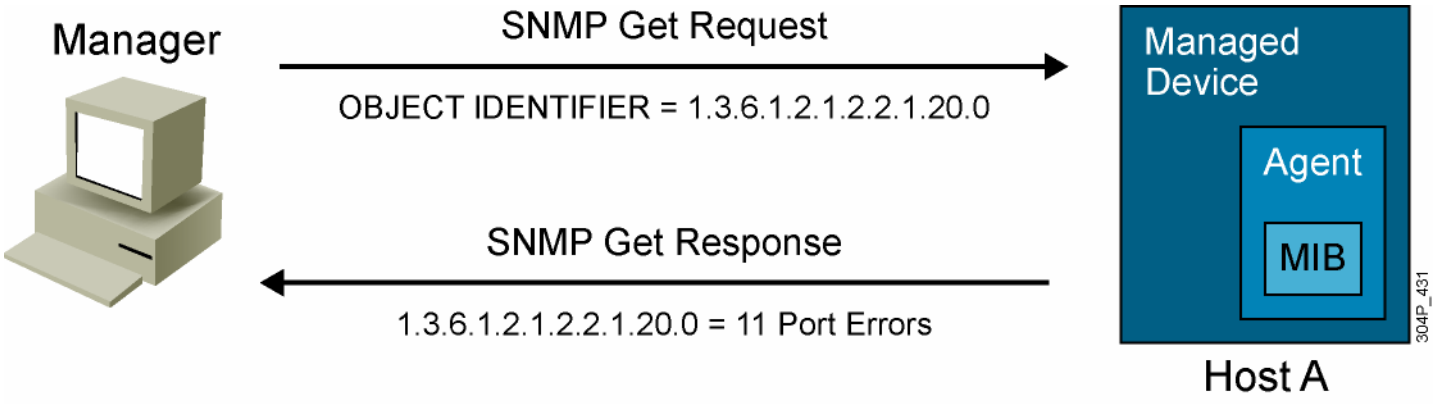
Example: Variable Retrieval

- 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

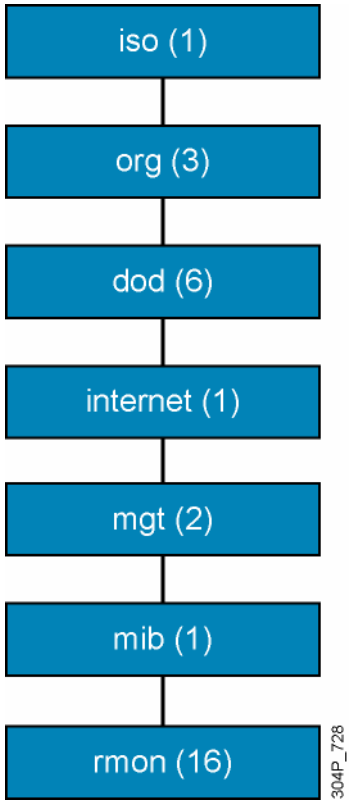
- Specific format to retrieve the number of errors on first interface

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



RMON1

- Supports proactive monitoring of LAN traffic:
  - Network fault diagnosis
  - Planning
  - Performance tuning
- Works on MAC layer data:
  - Monitors only the aggregate LAN traffic for remote LAN segments
  - Traffic statistics and analysis
- Implemented on agents:
  - Routers, switches, hubs, servers, hosts, and dedicated probes

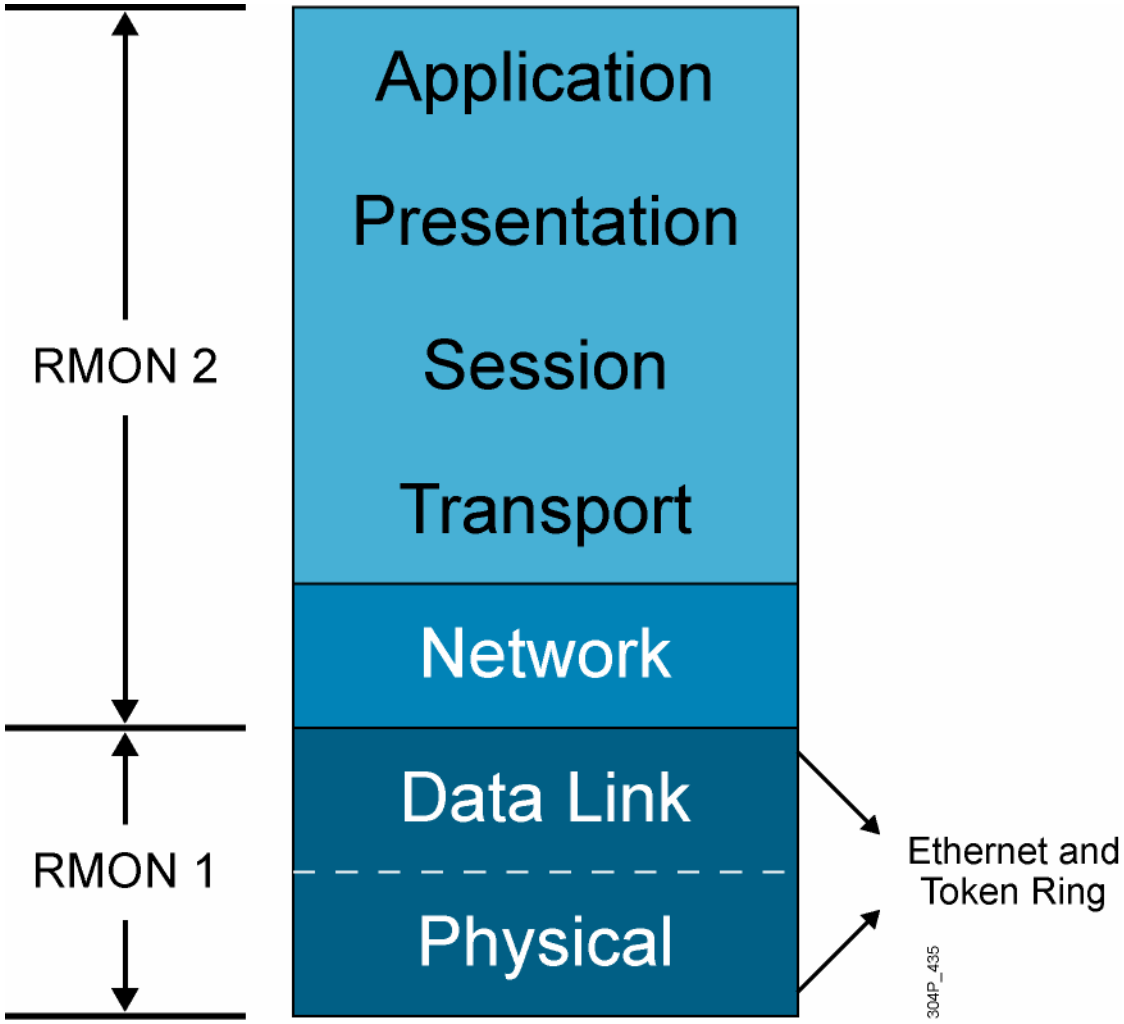


RMON1 Groups (RFC 1513 and 2819)

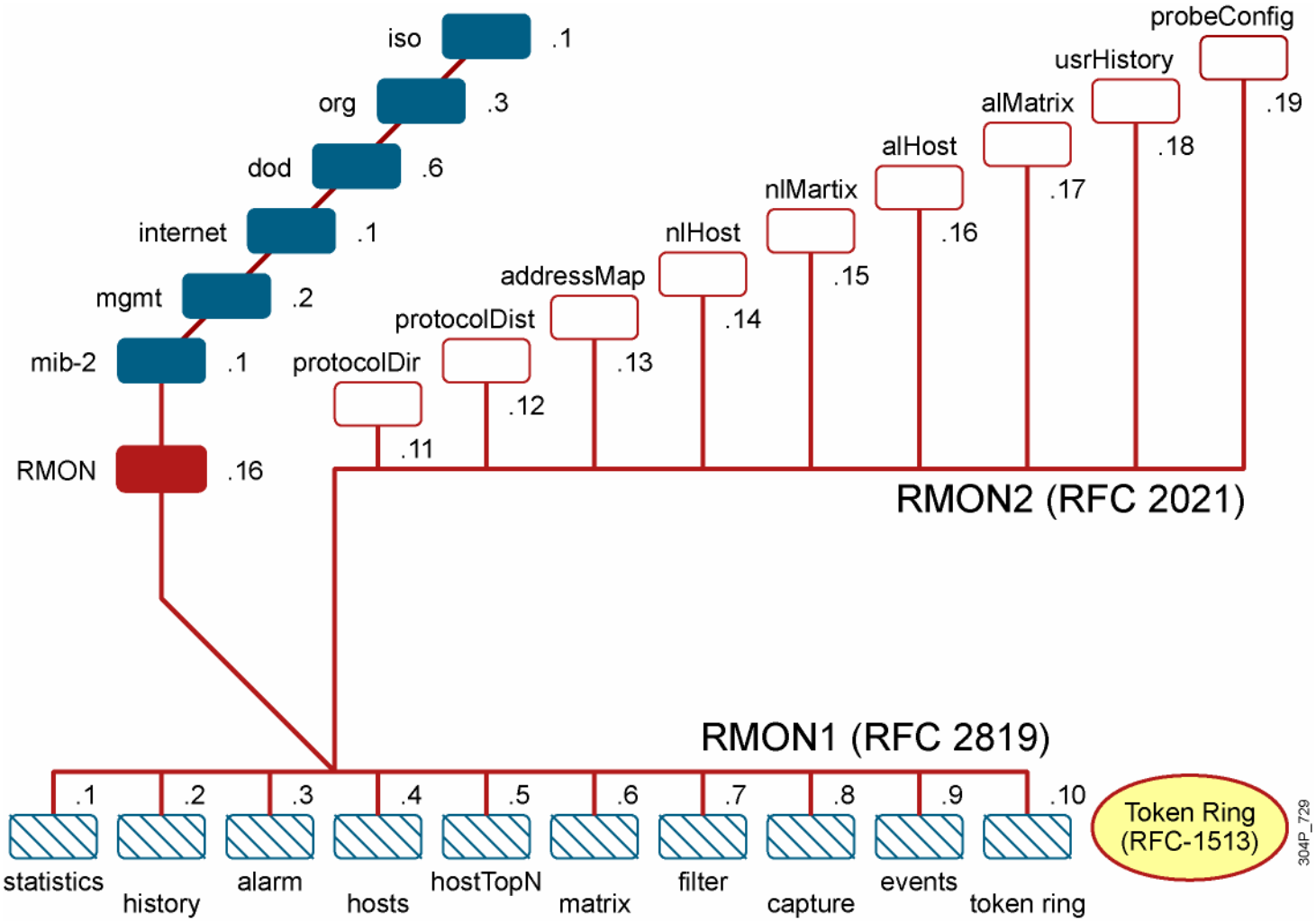
1	statistics	Real Time—Current Statistics
2	history	Statistics over Time
3	alarm	Predetermined Threshold Watch
4	host	Individual Host Statistics Tracking
5	hostTopN	"N" Statistically Most Active Hosts
6	matrix	A < > B—Conversation Statistics
7	filters	Packet Structure and Content Matching
8	packet capture	Collection for Subsequent Analysis
9	events	Reaction to Predetermined Conditions
10	Token Ring	Token Ring—RMON Extensions

304P_433

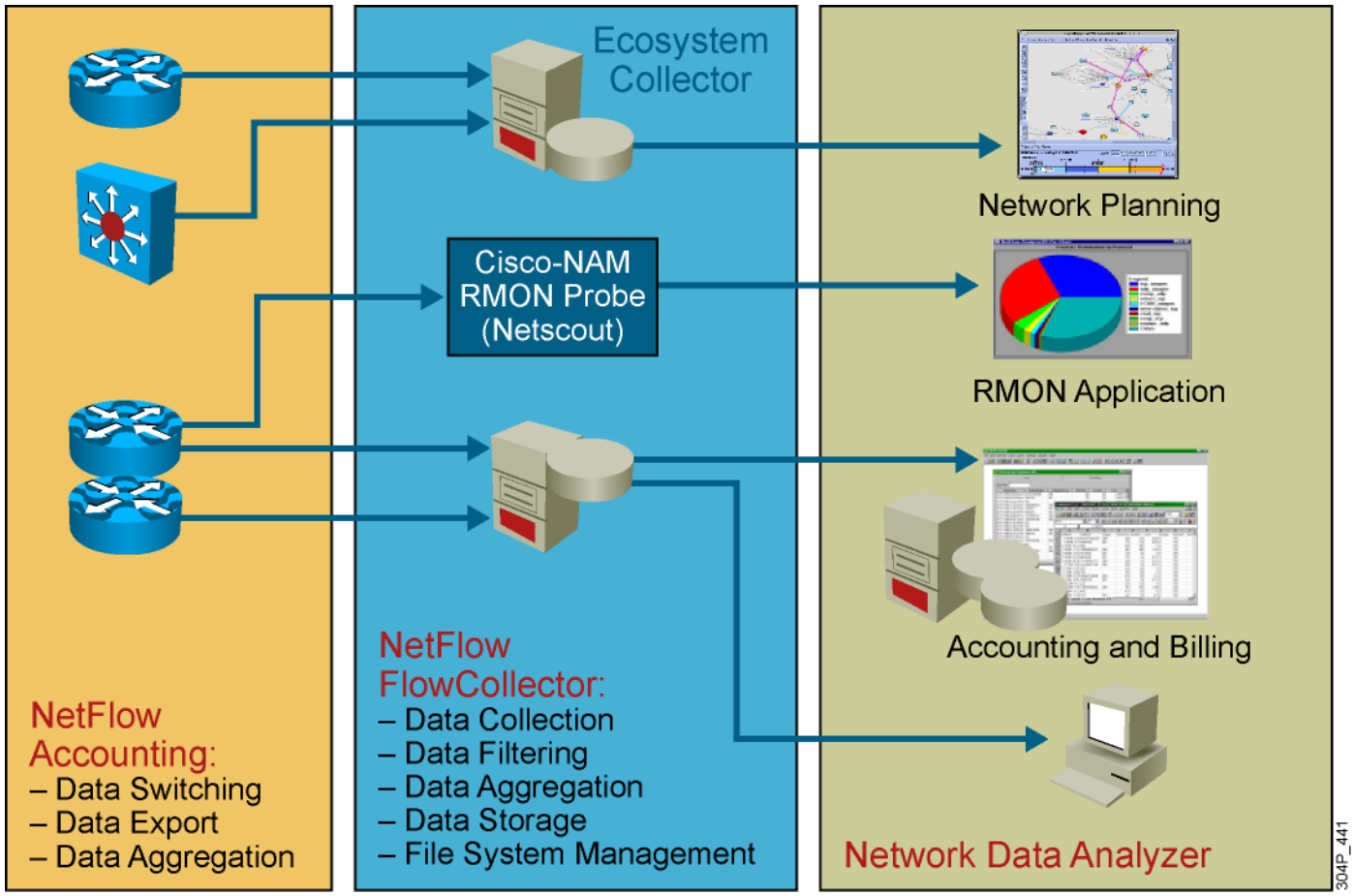
RMON2



RMON2 (RFC 2021)



NetFlow Infrastructure



NetFlow vs. RMON Information Gathering

- NetFlow can be configured on individual interfaces.
- NetFlow gathers more detailed information:
  - Source and destination interface numbers
  - Source and destination IP addresses
  - TCP/UDP source port and destination ports
  - Number of bytes and packets in the flow
  - Source and destination autonomous system (AS) numbers
  - IP type of service
- NetFlow provides greater scalability, customized data collection, and a lower performance impact.

Applications Using NetFlow

- Accounting and billing
- Network planning and analysis
- Network and security monitoring
- Application monitoring and profiling
- User monitoring and profiling
- NetFlow data warehousing and mining

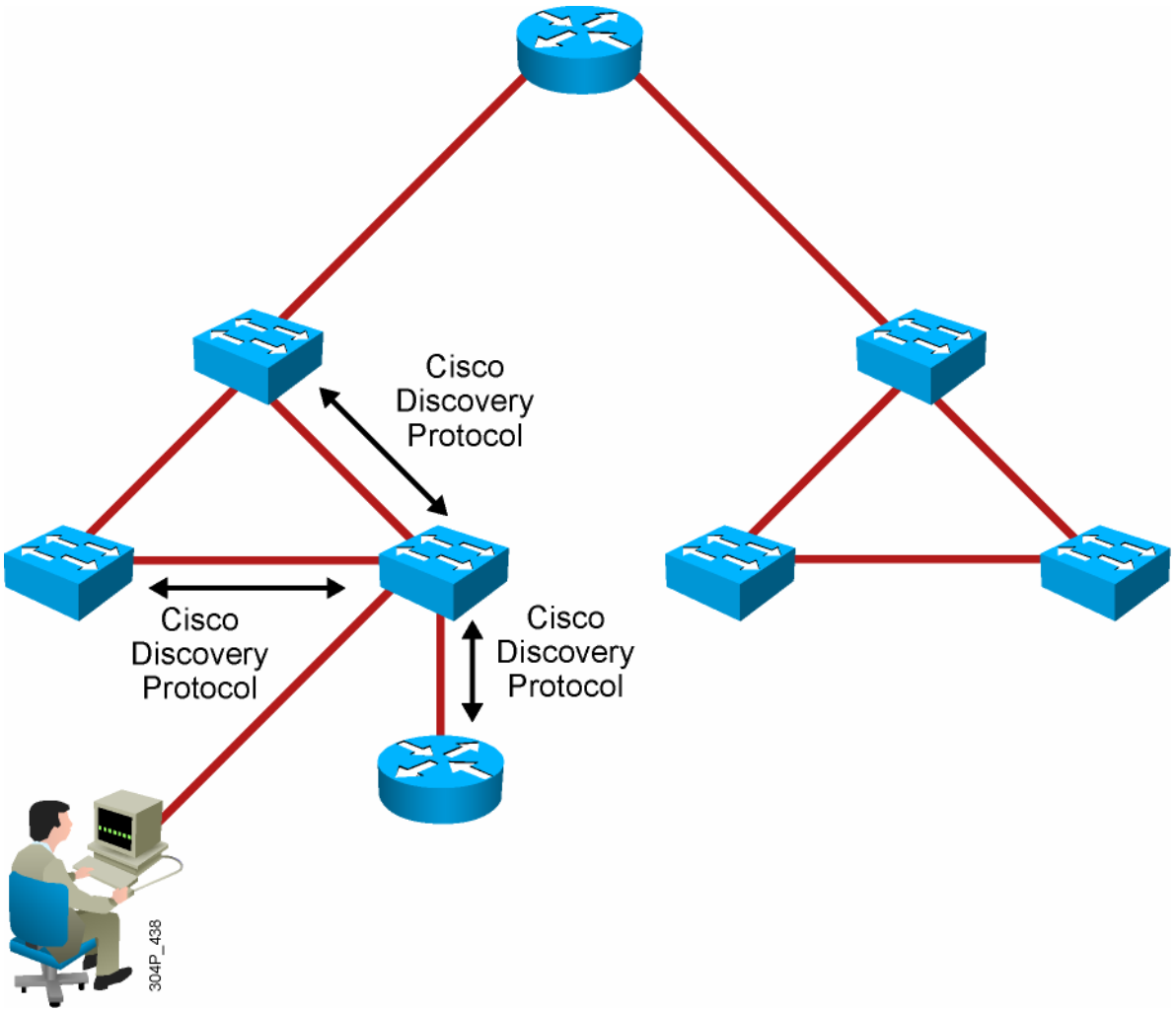
Cisco Discovery Protocol

Upper-Layer Entry Addresses	TCP/IP	Novell IPX	AppleTalk	Others
Cisco Proprietary Data Link Protocol	CDP	CDP	CDP	CDP
Media Supporting SNAP	LANs	Frame Relay	ATM	Others

CDP = Cisco Discovery Protocol

- Provides a summary of directly connected switches, routers, and other Cisco devices
- Discovers neighbor devices regardless of which protocol suite they are running
- Requires that physical media support SNAP encapsulation

Discovering Neighbors with Cisco Discovery Protocol

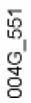


Syslog Features

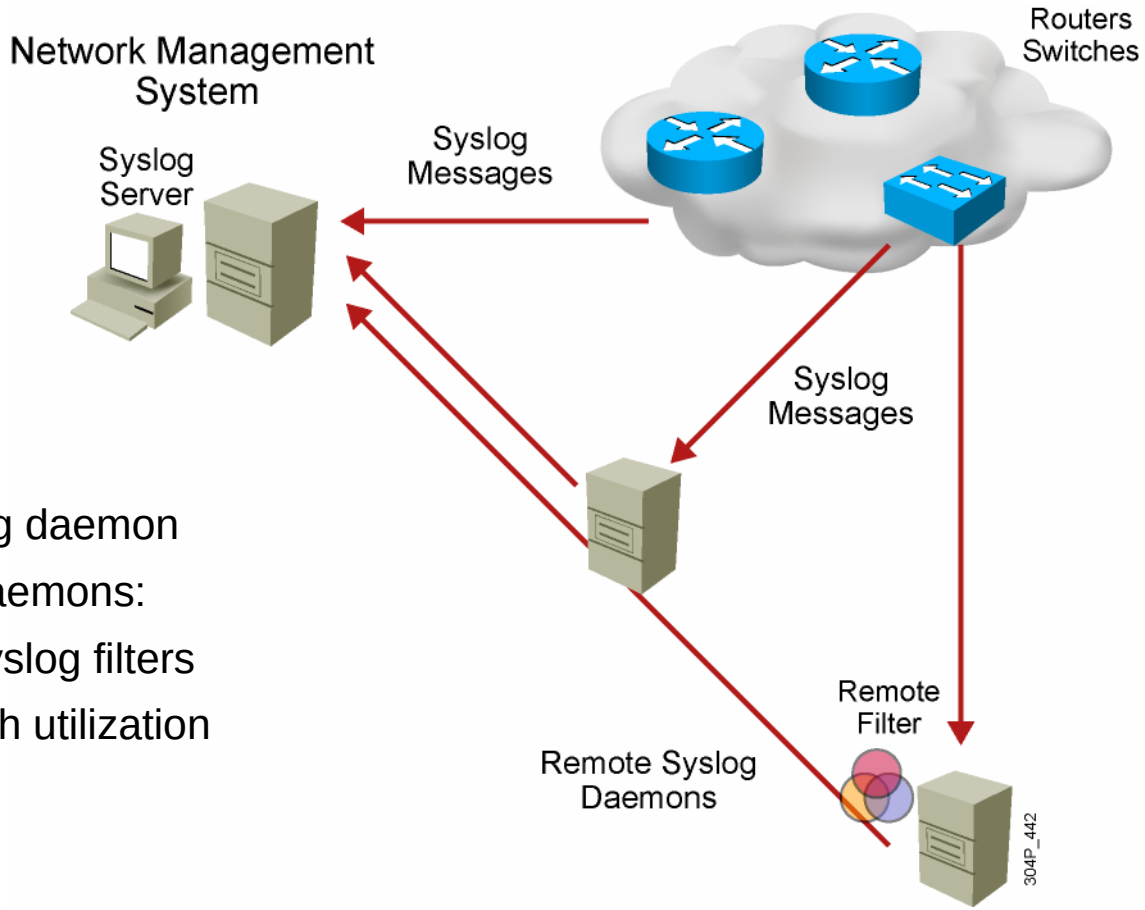
- Devices produce syslog messages.
- Syslog messages contain level and facility.
- Common syslog facilities:
  - IP
  - OSPF protocol
  - SYS operating system
  - IP Security (IPsec)
  - Route Switch Processor (RSP)
  - Interface (IF)
- Syslog levels:
  - Emergency (level 0, highest level)
  - Alert (level 1)
  - Critical (level 2)
  - Error (level 3)
  - Warning (level 4)
  - Notice (level 5)
  - Informational (level 6)
  - Debugging (level 7)

Example: 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
```



Syslog Architecture



- Centralized syslog daemon
- Remote syslog daemons:
  - Support for syslog filters
  - Low bandwidth utilization

Summary

- Network management is supported with various devices and servers that use network management protocols and standards.
- SNMP is a simple network management protocol that is the foundation of a network management architecture.
- A MIB stores local management agent information on a managed device.
- RMON is a MIB that supports proactive management of remote networks.
- NetFlow collects network flow data to support network accounting, usage-based billing, planning, performance monitoring, and QoS applications.
- Cisco Discovery Protocol is a Cisco proprietary protocol that enables you to discover Cisco devices on the network.
- Syslog reports system state information based on preset facilities and severity levels.