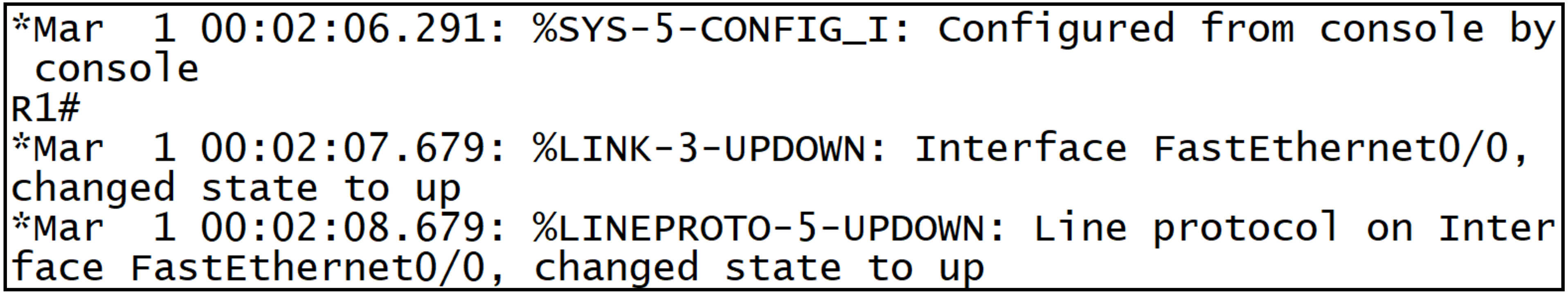
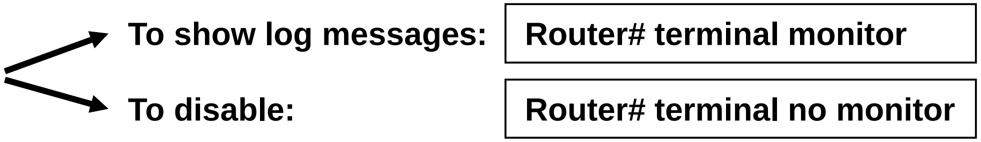
# Syslog – SNMP – NTP

# Implementing Log Messaging



```
*Mar  1 00:02:06.291: %SYS-5-CONFIG_I: Configured from console by
 console
R1#
*Mar  1 00:02:07.679: %LINK-3-UPDOWN: Interface FastEthernet0/0,
changed state to up
*Mar  1 00:02:08.679: %LINEPROTO-5-UPDOWN: Line protocol on Inter
face FastEthernet0/0, changed state to up
```

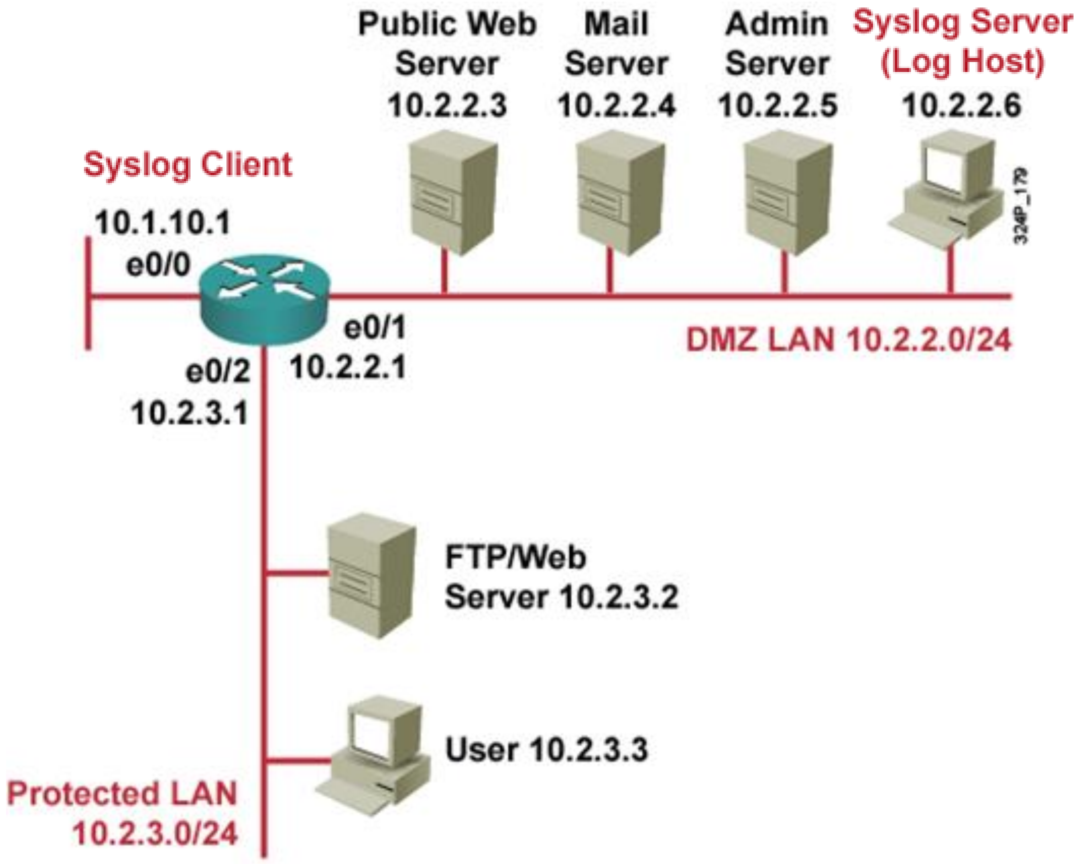
- **Routers should be configured to send log messages to one or more of these:**
  - Console
  - Terminal lines
  - Memory buffer
  - SNMP traps
  - Syslog
- **Syslog logging is a key security policy component.**



**To show log messages:** `Router# terminal monitor`

**To disable:** `Router# terminal no monitor`

# Syslog Systems

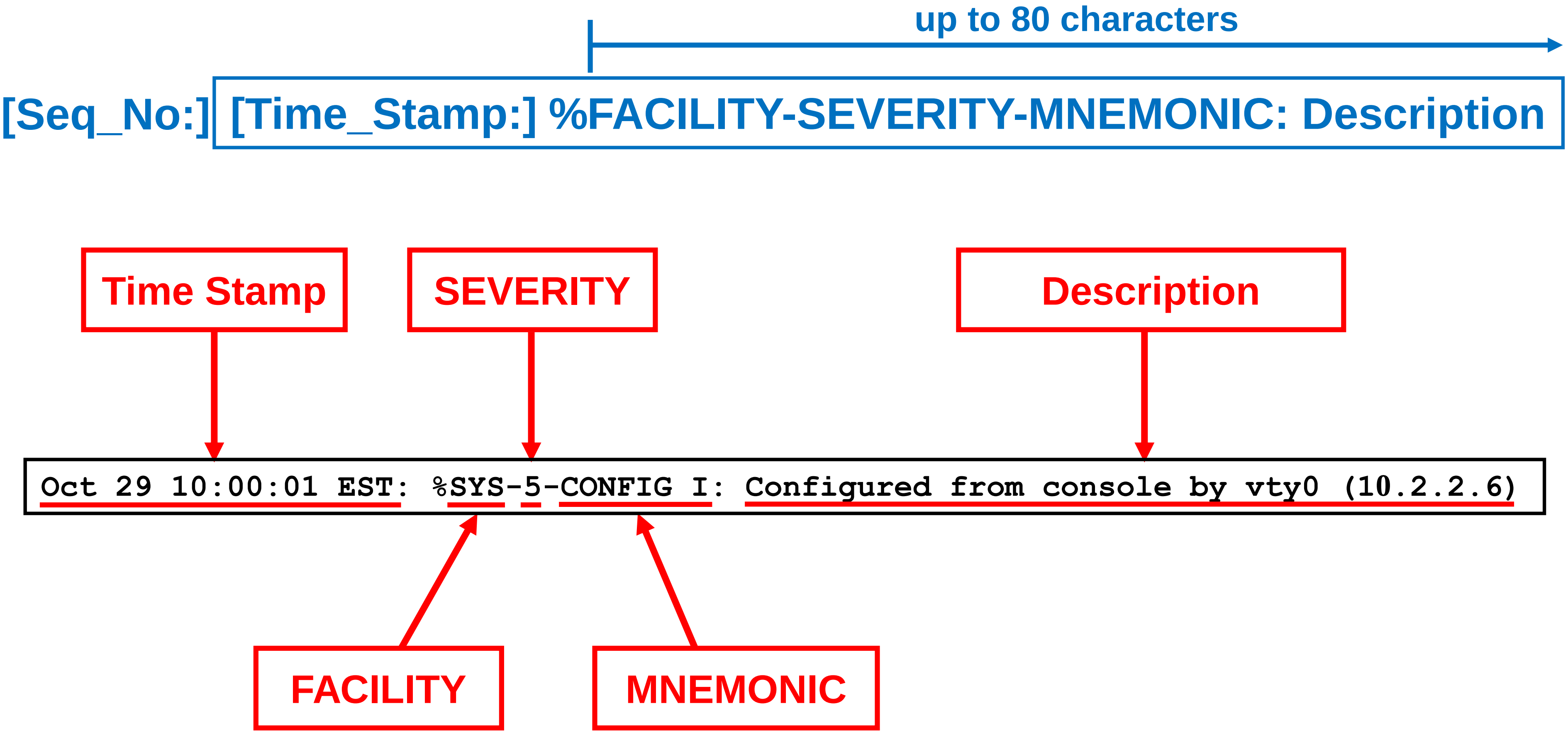


- **Syslog server:** A host that accepts and processes log messages from one or more syslog clients.
- **Syslog client:** A host that generates log messages and forwards them to a syslog server. ⟶ UDP port 514

# Cisco Log Severity Levels

| Level | Name | Description |
|---|---|---|
| 0 (Highest) | Emergencies | System unusable |
| 1 | Alerts | Immediate action required |
| 2 | Critical | Critical Conditions |
| 3 | Errors | Error conditions |
| 4 | Warnings | Warning conditions |
| 5 | Notifications | Normal but significant condition |
| 6 | Informational | Informational messages |
| 7 (Lowest) | Debugging | Debugging messages |

# Log Message Format



up to 80 characters

[Seq_No:] [Time_Stamp:] %FACILITY-SEVERITY-MNEMONIC: Description

```
Oct 29 10:00:01 EST: %SYS-5-CONFIG_I: Configured from console by vty0 (10.2.2.6)
```

**SYS: system events**
**LINK: Interface status**
**LINEPROTO: line protocol status**
**.....**

# Configuring Syslog Logging

# Configuring Syslog Client

```
Router(config)#
logging [host-name | ip-address]
```

1. Sets the destination logging host

```
Router(config)#
logging trap level
```

2. (Optional) Sets the log severity (trap) level

```
Router(config)#
logging facility facility-type
```

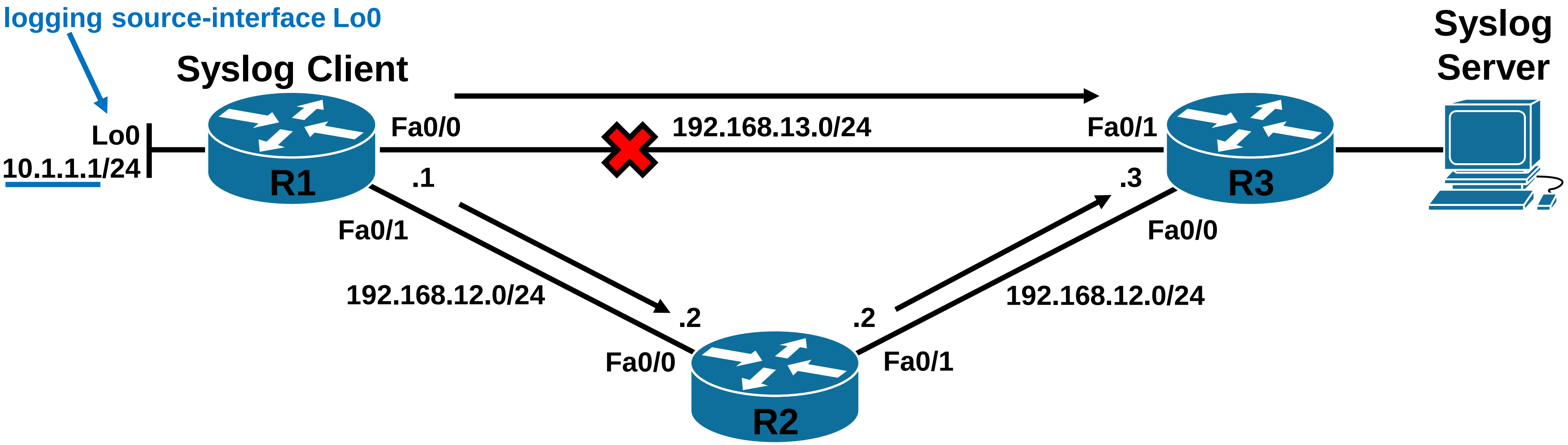
3. (Optional) Sets the syslog facility

# Configuring Syslog Client (Cont.)

```
Router(config)#
```

```
logging source-interface interface-type interface-number
```

4. (Optional) Sets the source interface

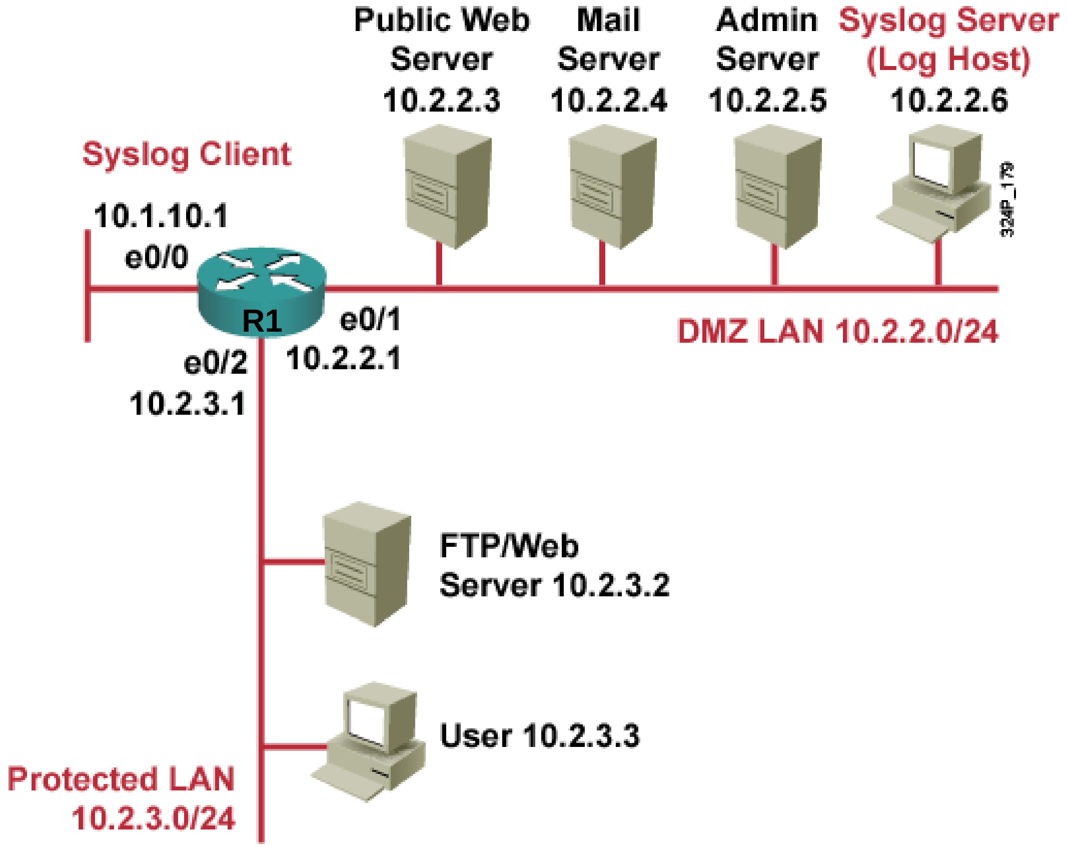


```
Router(config)#
```

```
logging on
```

5. Enables logging

# Syslog Implementation Example



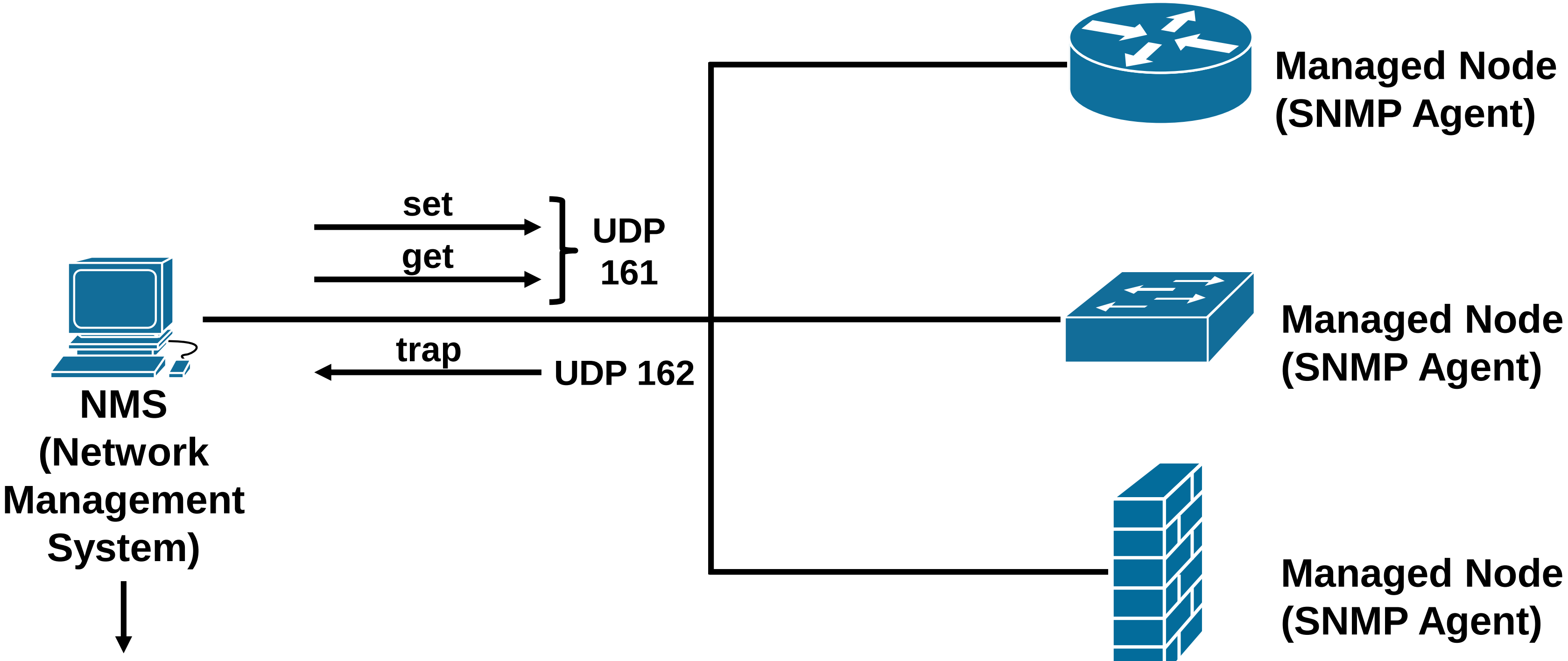
```
R1(config)#logging 10.2.2.6
R1(config)#logging trap informational
R1(config)#logging source-interface loopback 0
R1(config)#logging on
```

# SNMP

# (Simple Network Management Protocol)

# SNMPv1 and SNMPv2 Architecture

- The SNMP NMS asks agents embedded in network devices for information, or tells the agents to do something.



Network Monitoring Software:
SolarWinds, PRTG Network Monitor,
WhatsUp Gold, OpManager, Riverbed,
Tivoli Monotoring (IBM), ...

# Community Strings

**Used to authenticate messages between a management station, and an SNMPv1 or SNMPv2c engine:**

- **Read only community strings can get information, but can not set information in an agent.**
- **Read-write community strings can get and set information in the agent.**
- **Having read-write access is like having the enable password for the device.**

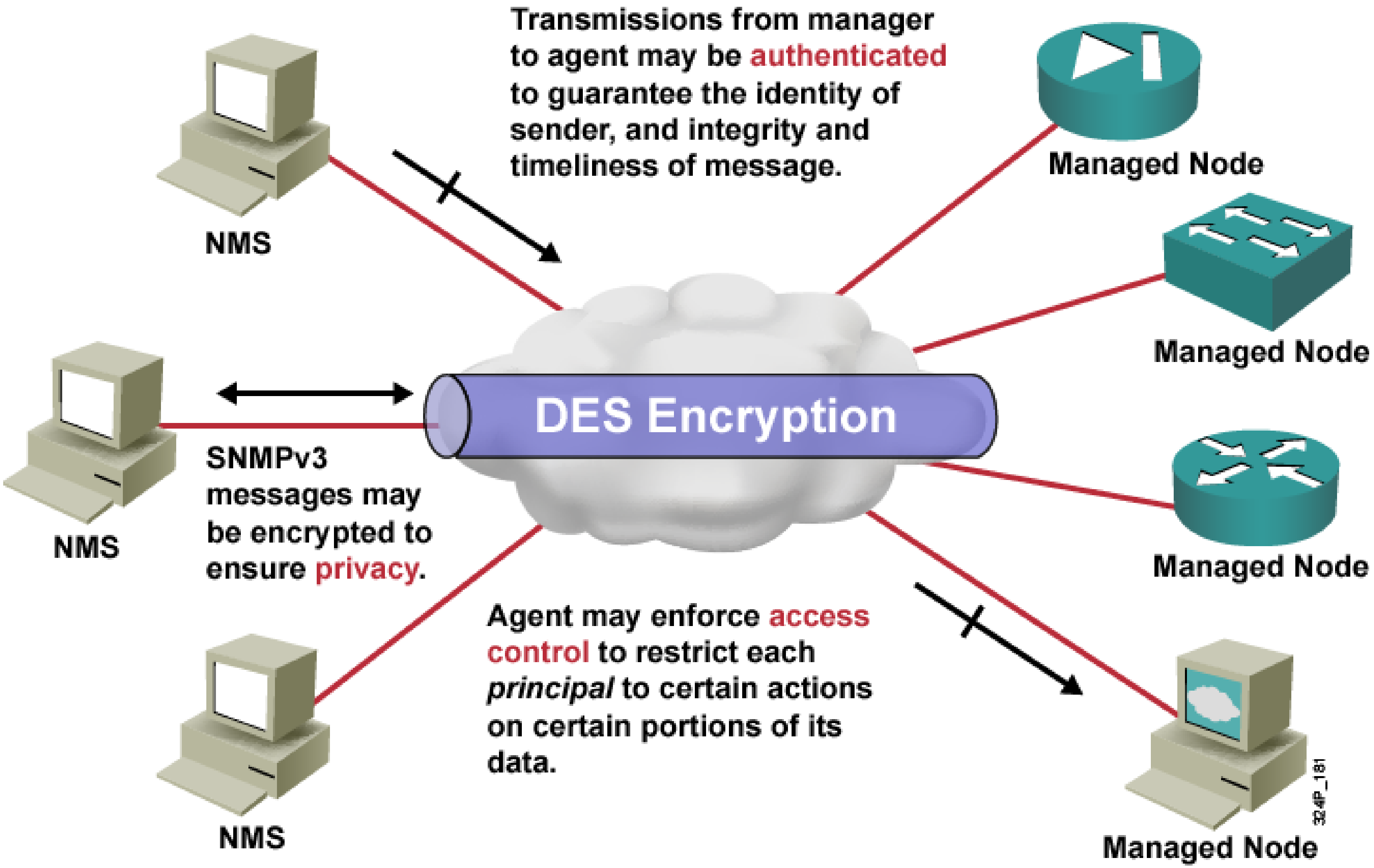
# SNMP Security Models and Levels

## Definitions:

- Security model is a security strategy used by the SNMP agent
- Security level is the permitted level of security within a security model

| Model | Level | Authentication | Encryption | What Happens |
|---|---|---|---|---|
| v1 | noAuthNoPriv | Community String | No | • Authenticates with a community string match |
| v2 | noAuthNoPriv | Community String | No | • Authenticates with a community string match |
| v3 | noAuthNoPriv | Username | No | • Authenticates with a username |
|  | authNoPriv | MD5 or SHA | No | • Provides HMAC MD5 or SHA algorithms for authentication |
|  | authPriv | MD5 or SHA | DES<br>3-DES<br>AES | • Provides HMAC MD5 or SHA algorithms for authentication<br>• Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard |

# SNMPv3 Architecture



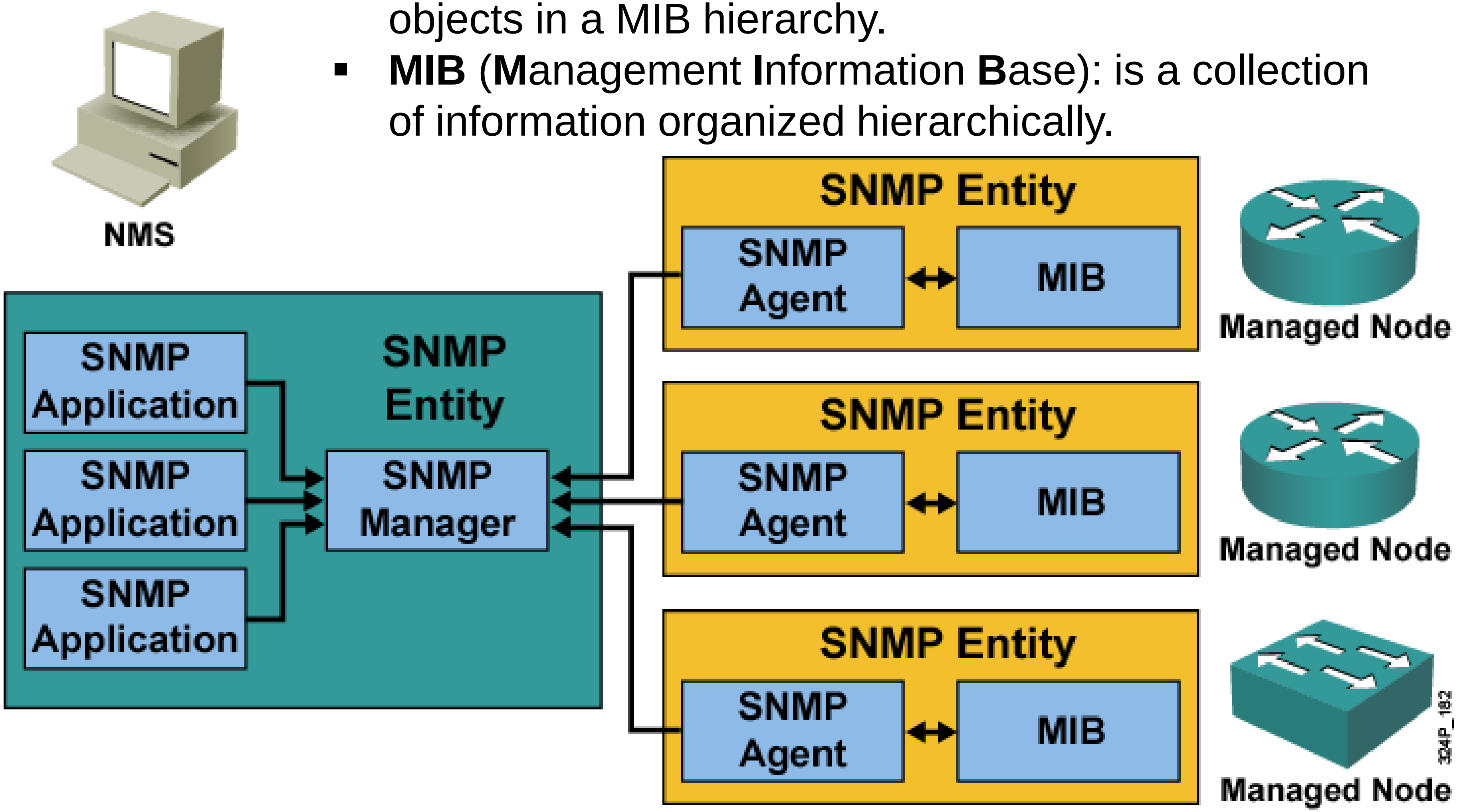
Transmissions from manager to agent may be authenticated to guarantee the identity of sender, and integrity and timeliness of message.

SNMPv3 messages may be encrypted to ensure privacy.

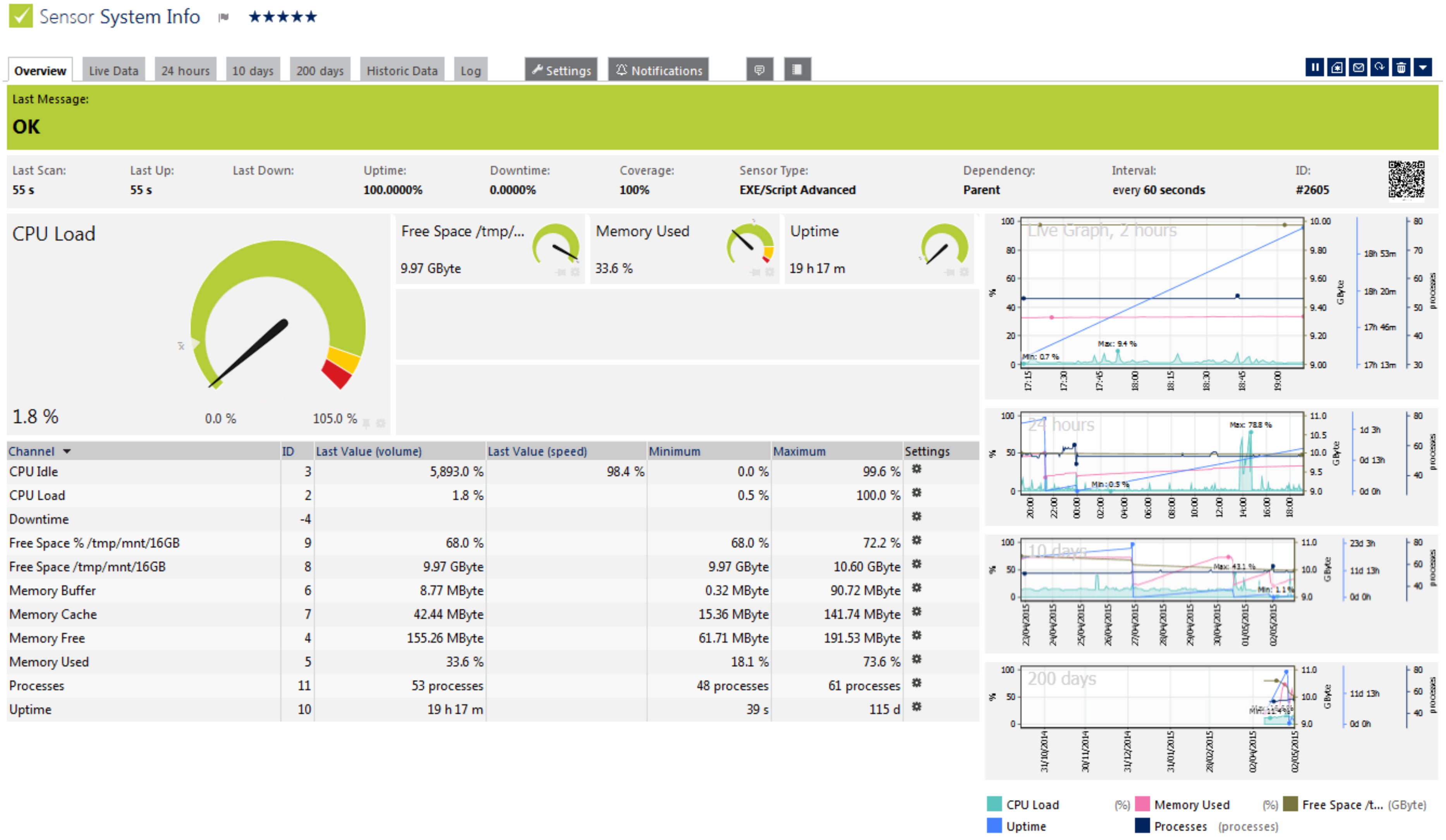
Agent may enforce access control to restrict each *principal* to certain actions on certain portions of its data.

# SNMP Operational Model

- **OID (O**bject **Id**entifiers): uniquely identify managed objects in a MIB hierarchy.
- **MIB** (**M**anagement **I**nformation **B**ase): is a collection of information organized hierarchically.



# Example



Sensor System Info ★★★★★

Last Message:

**OK**

| Last Scan: | Last Up: | Last Down: | Uptime: | Downtime: | Coverage: | Sensor Type: | Dependency: | Interval: | ID: |
|---|---|---|---|---|---|---|---|---|---|
| 55 s | 55 s | | 100.0000% | 0.0000% | 100% | EXE/Script Advanced | Parent | every 60 seconds | #2605 |

CPU Load

1.8 %

0.0 % 105.0 %

Free Space /tmp/...

9.97 GByte

Memory Used

33.6 %

Uptime

19 h 17 m

| Channel | ID | Last Value (volume) | Last Value (speed) | Minimum | Maximum | Settings |
|---|---|---|---|---|---|---|
| CPU Idle | 3 | 5,893.0 % | 98.4 % | 0.0 % | 99.6 % | ⚙ |
| CPU Load | 2 | 1.8 % | | 0.5 % | 100.0 % | ⚙ |
| Downtime | -4 | | | | | ⚙ |
| Free Space % /tmp/mnt/16GB | 9 | 68.0 % | | 68.0 % | 72.2 % | ⚙ |
| Free Space /tmp/mnt/16GB | 8 | 9.97 GByte | | 9.97 GByte | 10.60 GByte | ⚙ |
| Memory Buffer | 6 | 8.77 MByte | | 0.32 MByte | 90.72 MByte | ⚙ |
| Memory Cache | 7 | 42.44 MByte | | 15.36 MByte | 141.74 MByte | ⚙ |
| Memory Free | 4 | 155.26 MByte | | 61.71 MByte | 191.53 MByte | ⚙ |
| Memory Used | 5 | 33.6 % | | 18.1 % | 73.6 % | ⚙ |
| Processes | 11 | 53 processes | | 48 processes | 61 processes | ⚙ |
| Uptime | 10 | 19 h 17 m | | 39 s | 115 d | ⚙ |

# Configuring NTP Client

# Understanding NTP

- NTP is used to synchronize the clocks in the entire network.
- System clock is set by the battery system calendar during bootup.
- System clock can then be modified manually or via NTP.
- NTP runs over UDP port 123; current version is 4.
- Only NTP up to version 3 has been documented in RFCs.
- Stratum describes how many “NTP hops” away a machine is from authoritative time source.
- NTP establishes associations to synchronize time.

# Configuring NTP Associations

```
Router(config)#
```

```
ntp server {ip-address | hostname} [version number] [key
keyid] [source interface] [prefer]
```

- Forms a server association with another system

CISCO