Syslog, SNMP

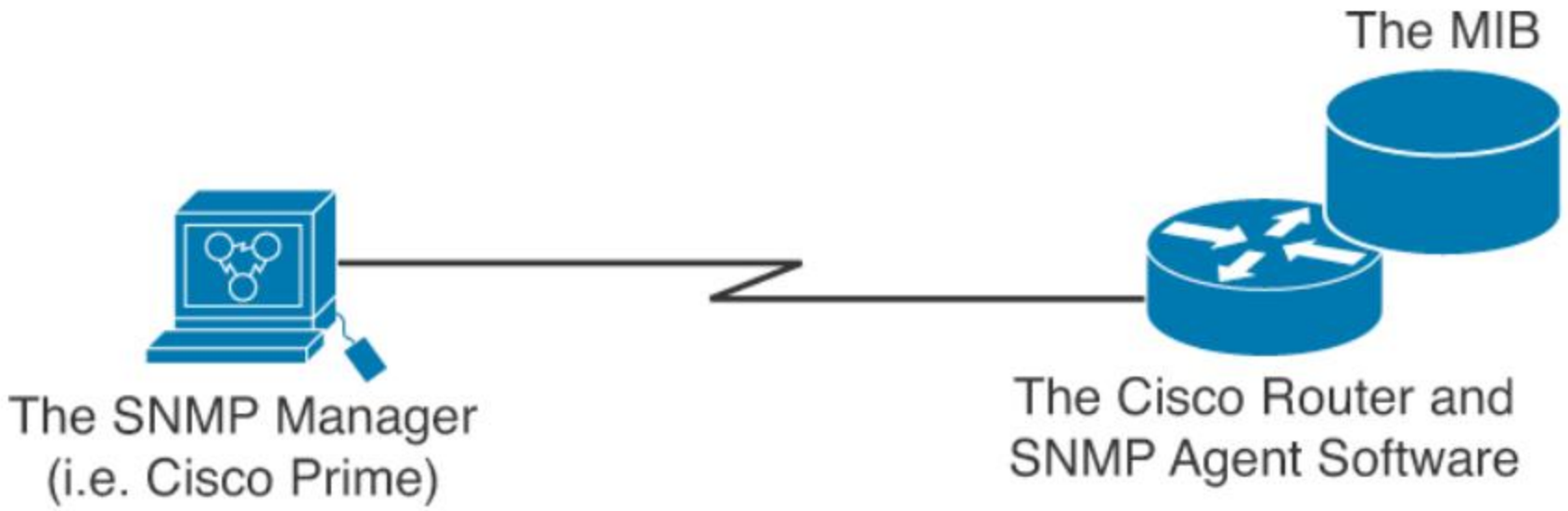
Eng. Maha Jeha

SNMP

- SNMP: هو بروتوكول طبقة التطبيقات الذي يوفر رسائل بين المدير و الوكلاء .
- تتضمن المكونات :

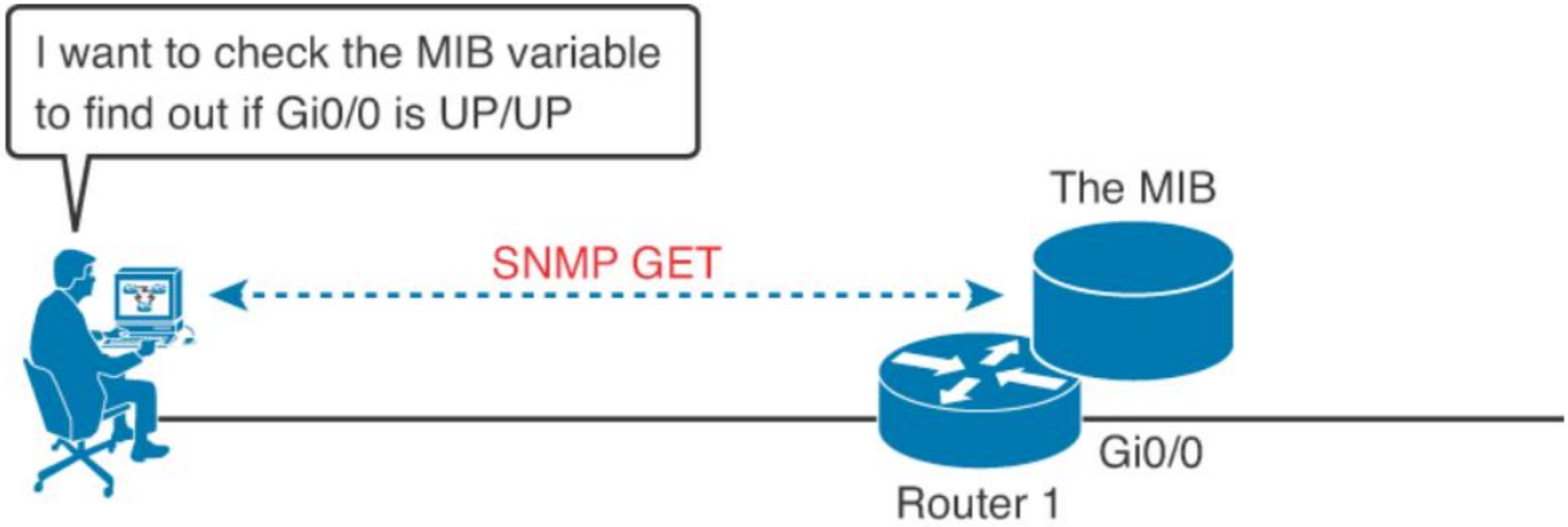
- SNMP manager
- SNMP agent
- Management Information Base

عناصر SNMP



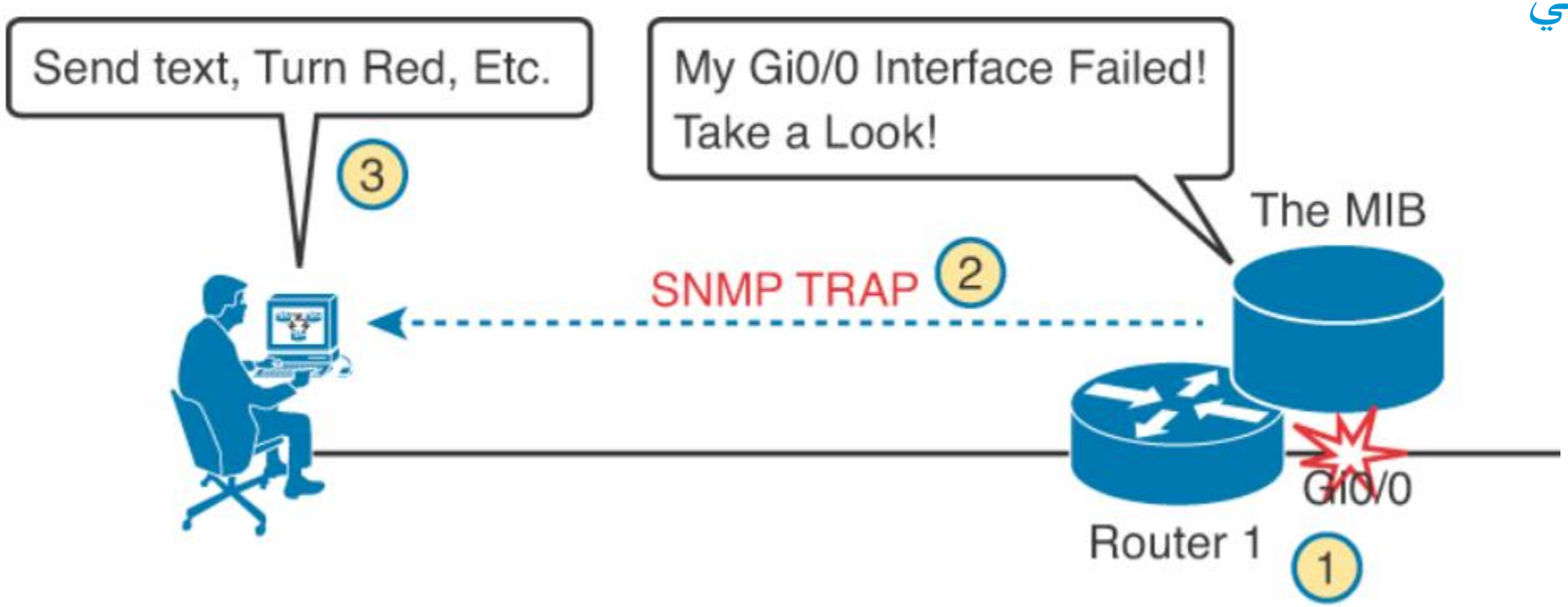
استخدام SNMP لمراقبة الشبكة

- تتم مراقبة الشبكة عن طريق تفحص MIB .



استخدام SNMP لمراقبة الشبكة

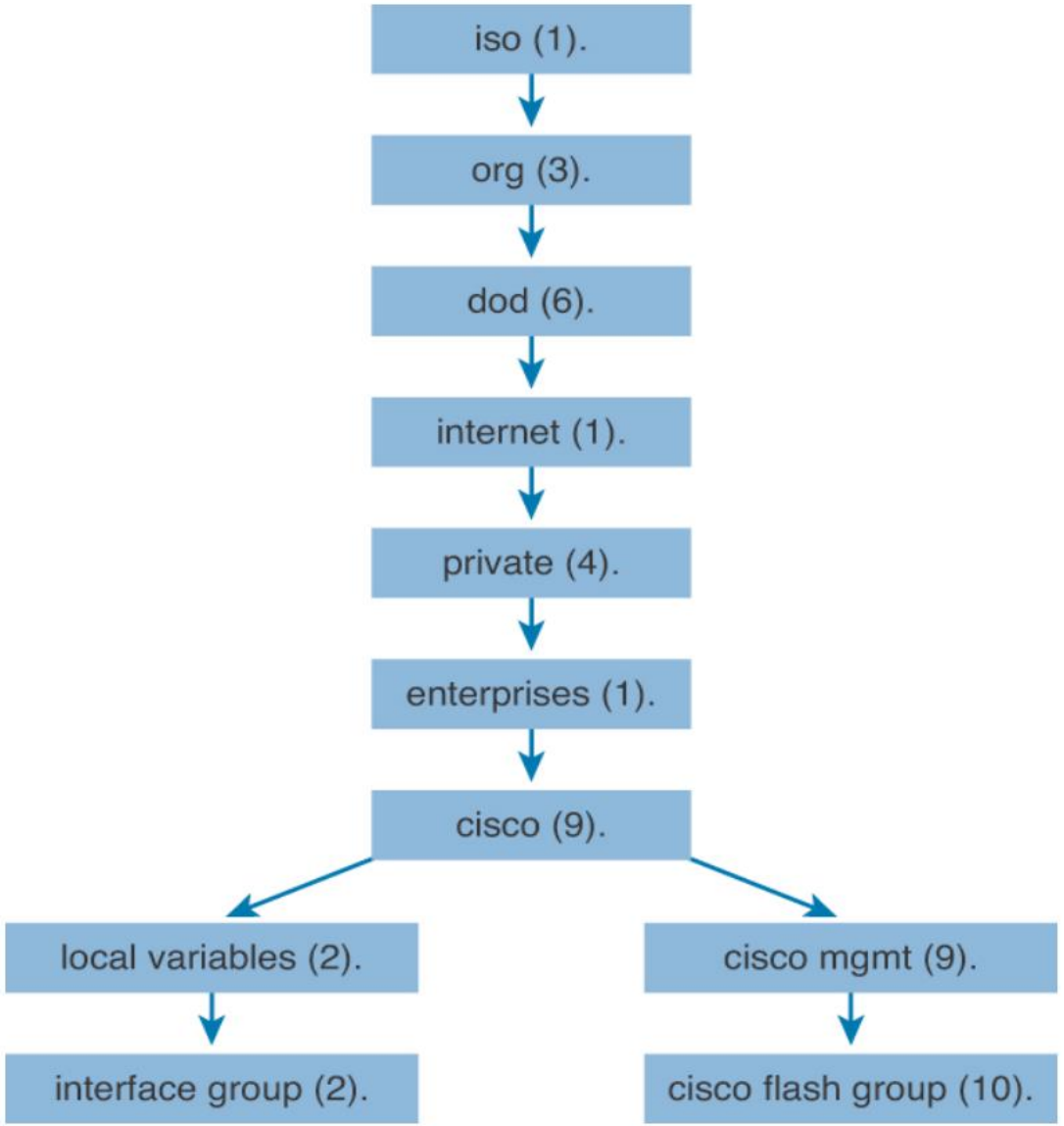
- تتم مراقبة MIB لمنفذ معين حقيقي Real - Interface أو لمنفذ اختبار افتراضي Loopback



The Management Information Base (MIB)

- يعرف MIB كل متحول بما يسمى Object ID أو اختصاراً OID .
- تنظم OIDs بشكل هرمي وغالباً ما تسمى OID – Tree .
- تمثَّل أغصان شجرة OID بمتحولات وهذه المتحولات تتعلق بشكل مباشر بأجهزة الشبكة و التطبيقات الشبكية .
- شركات التجهيزات الشبكية كـ Cisco غالباً ما تبني الشجرة السابقة الخاصة بها .

MIB tree



SNMP-Get باستخدام MIB – Value الحصول على

```
[13:22][cisco@NMS~ ]$ snmpget -v2c -c community 10.250.250.14
1.3.6.1.4.1.9.2.1.58.0
SNMPv2-SMI::enterprises.9.2.1.58.0 = INTEGER: 11
```

`-v2c` The version on SNMP in use

`-c community` The SNMP password, called a community string

`10.250.250.14` The IP address of the monitored device

`1.3.6.1.4.1.9.2.1.58.0` The numeric object identifier (OID) of the MIB variable

إعداد SNMP v2

هناك نوعان من SNMP Community – String المطبقة في الإصدار الثاني :

- **Read-only (RO) :** نستطيع في هذا النوع الوصول إلى متحولات MIB ولكن لا نستطيع التعديل عليها ، وغالباً ما يستخدم هذا النوع في الإصدار الثاني لـ SNMP وذلك لضعف الأمان فيه
- **Read-write (RW) :** نستطيع في هذا النوع الوصول إلى متحولات MIB مع إمكانية التعديل عليها .

إعداد SNMP v2 وذلك لنمط RO

```
R1(config)# ip access-list standard ACL_PROTECTSNMP
R1(config-std-nacl)# permit host 10.10.10.101
R1(config-std-nacl)# exit
R1(config)# snmp-server community V011eyB@11!!! RO ACL_PROTECTSNMP
R1(config)# snmp-server location Tampa
R1(config)# snmp-server contact Anthony Sequeira
R1(config)# end
R1#
```

إعداد SNMP v2 وذلك لنمط RW

```
R2(config)# ip access-list standard ACL_PROTECTSNMP
R2(config-std-nacl)# permit host 10.20.20.201
R2(config-std-nacl)# exit
R2(config)# snmp-server community T3nn1sB@ll RW ACL_PROTECTSNMP
R2(config)# snmp-server location New York
R2(config)# snmp-server contact John Sequeira
R2(config)# end
R2#
```

SNMPv3

من أهم خصائص الإصدار الثالث من SNMP :

- **Message integrity:** This helps ensure that a packet has not been tampered with in transit
- **Authentication:** This helps ensure that the packet came from a known and trusted source
- **Encryption:** This helps to ensure that information cannot be read if the data is captured in transit

Possible Security modes of SNMPv3

Level Name	Keyword in snmp-server Command	Authentication Method	Encryption
noAuthNoPriv	**noauth**	Username	None
authNoPriv	**auth**	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	None
authPriv	**priv**	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	DES or DES-56

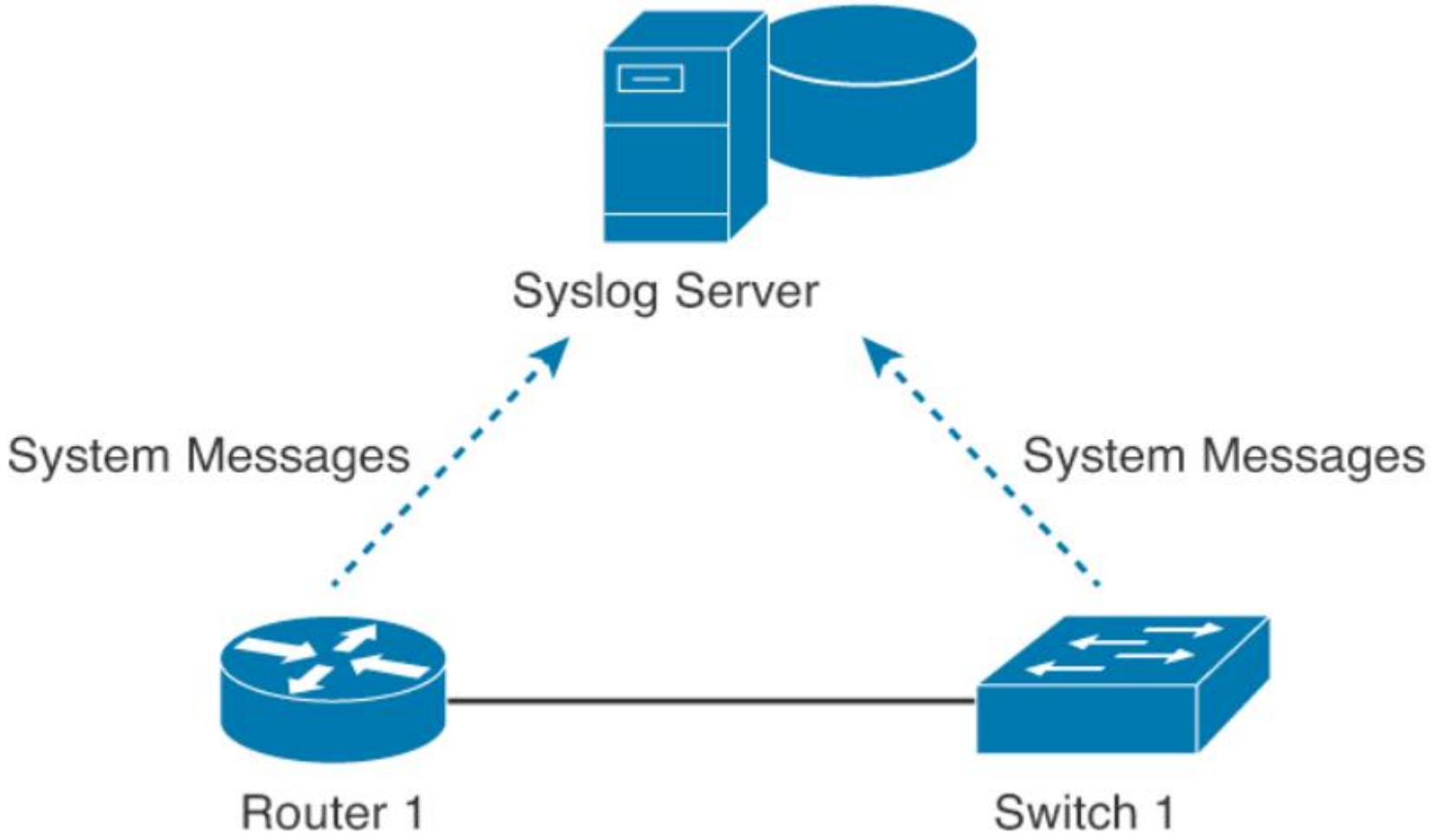
Syslog

- تسمح هذه الرسائل لشركات مزودي تجهيزات الشبكة بإرسال رسائل النظام ضمن الشبكة .
- تخزن هذه الرسائل في مخدمات تدعى Syslog – Servers .
- هناك أنواع عديدة لـ Syslog – Servers تناسب مختلف أنظمة التشغيل كـ Windows – UNIX .

أطراف استقبال رسائل Syslog

- The logging buffer (RAM inside the router or switch)
- The console line
- The terminal lines
- A syslog server

Syslogging in the Network



صيغة رسائل Syslog

```
*Dec 18 17:10:15.079: %LINEPROTO-5-UPDOWN: Line
protocol on Interface FastEthernet0/0, changed state
to down
```

- **A timestamp:** *Dec 18 17:10:15.079
- **The facility on the router that generated the message:** %LINEPROTO
- **The severity level:** 5
- **A mnemonic for the message:** UP/DOWN
- **The description of the message:** Line protocol on Interface FastEthernet0/0, changed state to down

Modifying System Messages

```
R1(config)# no service timestamps
R1(config)# service sequence-numbers
R1(config)# end
R1#
000011: %SYS-5-CONFIG_I: Configured from console by
console
```

System Message Severity Levels

Level	Level Name	Explanation
0	Emergency	The system may be unusable.
1	Alert	Immediate action may be required.
2	Critical	A critical event took place.
3	Error	The router experienced an error.
4	Warning	A condition might warrant attention.
5	Notification	A normal but significant condition occurred.
6	Informational	A normal event occurred.
7	Debugging	The output is a result of a **debug** command.

Configuring and Verifying Syslog

- R1(config)#logging 192.168.1.101
- R1(config)#logging trap 4
- By default, Cisco routers and switches send log messages for all severity levels to the console. On some IOS versions, the device also buffers those log messages by default
  - R1(config)# logging console
  - R1(config)# logging buffered
- R1# show logging

Thank you!