Network Monitoring With SNMP & Syslog

ine.com

Keith Bogart

CCIE #4923

✉ kbogart@ine.com

@keithbogart1

linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Course Prerequisites

- High-level understanding of the function of network devices
- Understanding of the Internet Protocol (IP)

Course Objectives

- To introduce you to SNMP, its purpose, message types, versions and configuration on Cisco IOS devices
- To introduce you to Syslog, its purpose, and configuration on Cisco IOS devices

INE

Introduction To SNMP

ine.com

Topic Overview

- Network Management Fundamentals
- SNMP Overview
- SNMP Components & Architecture
- SNMP Message Types

Network Management Fundamentals

- Mid-to-large size networks could be composed of hundreds of network devices.
- All of these devices need to be monitored for;
  - Environmental conditions (HVAC in Datacenter goes out)
  - Capacity warnings (CPU on router reaching 95%)
  - Capacity planning/forecasting
  - Infrastructure changes (routes being lost, interface changes, etc)
- Network Management protocols and software streamline this process.

Common Network Management Protocols

- SNMP
- NetFlow
- System Message Logging (Syslog)

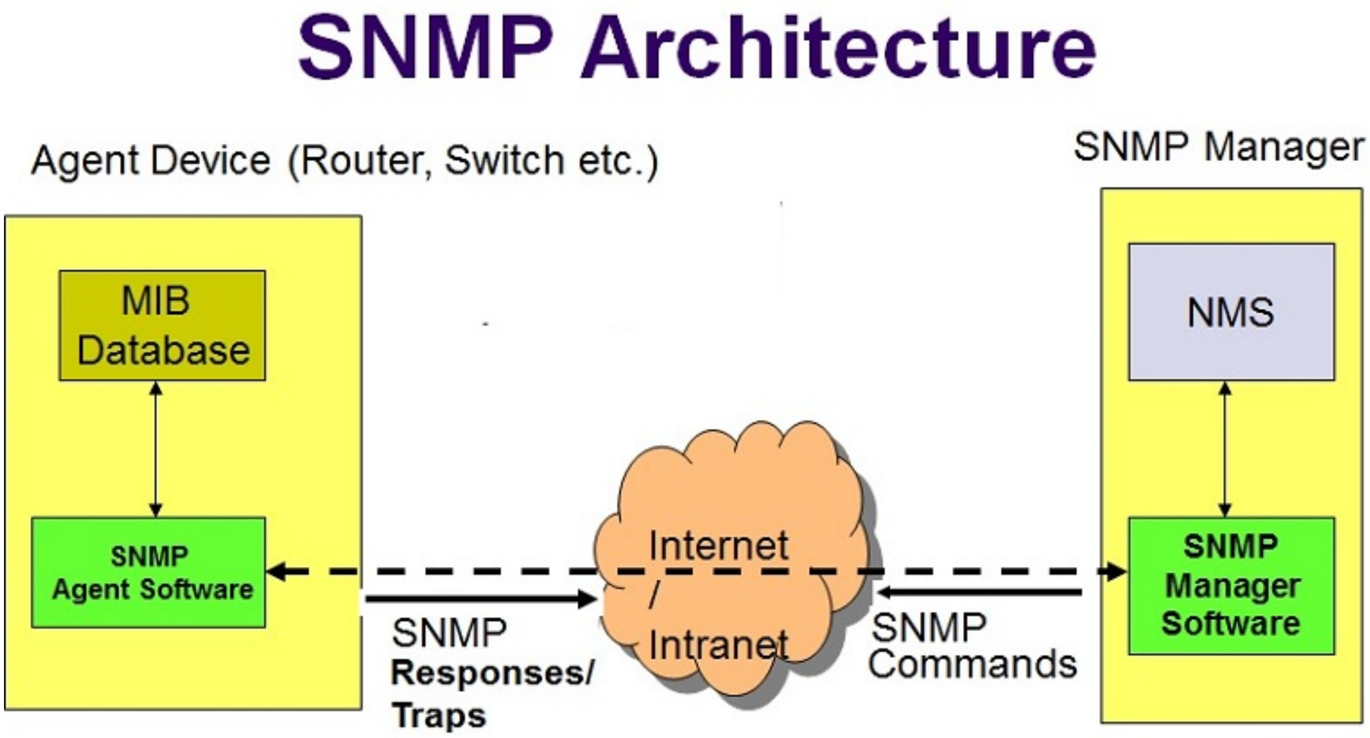
What Is SNMP?

- Simple Network Management Protocol
- Application-Layer Protocol
- First conceptualized in 1988 with RFC 1065
- Utilizes UDP Ports 161 and 162
- Three main versions of the protocol;
  - SNMPv1
  - SNMPv2c
  - SNMPv3

SNMP Components

- SNMP Manager
  - SNMP Server
  - Also called the NMS (Network Management Station)
  - Software purchased and installed onto a PC/Server
- SNMP Agents (SNMP software residing on devices that are being monitored, like a Router)
- MIB = Management Information Base (datastructure where variables are stored on the Agent)

SNMP Architecture

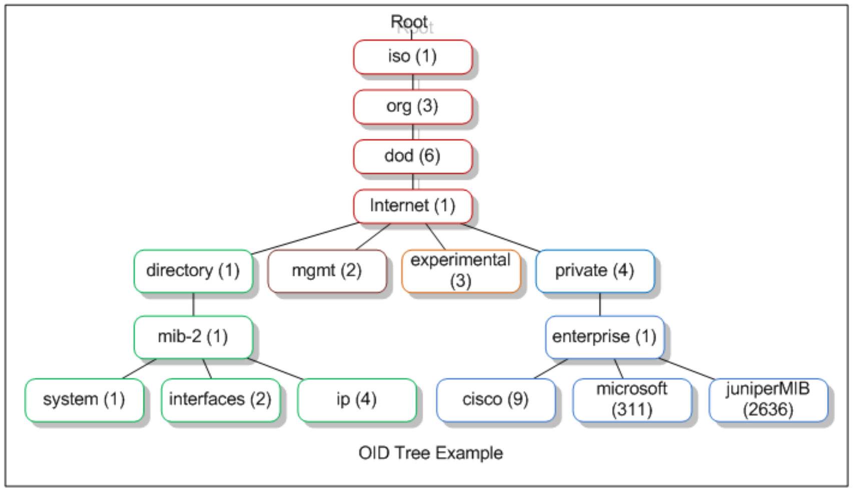


SNMP Components: Agent

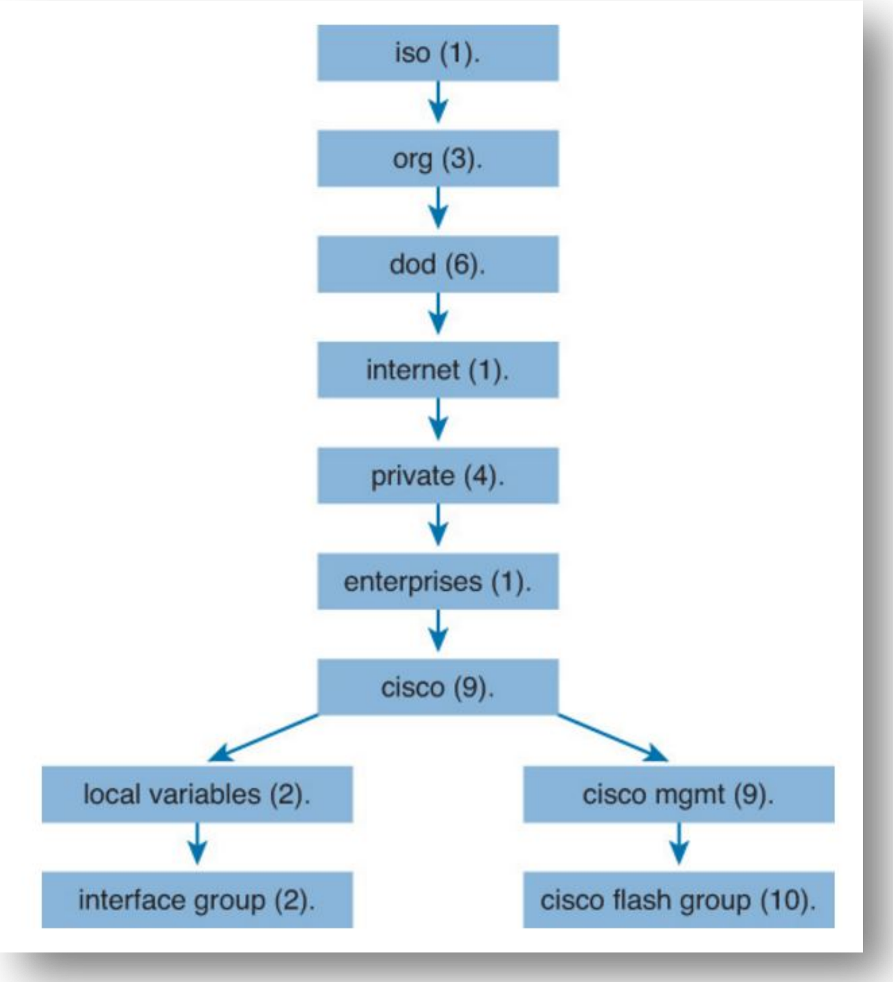
- SNMP Agent
  - A device (Router, Switch, Firewall, Printer, etc) running SNMP software that contains a MIB.
  - Software module that translates device information into an SNMP-compatible format in order to make the device information available for monitoring with SNMP.
- Cisco devices must be configured with commands to activate the SNMP Agent functionality.

SNMP Components: MIB

- SNMP MIB (Management Information Base)
  - Database of managed data called, “variables” or “objects” stored in a hierarchical fashion.
  - Each object called/referenced by an Object-ID (OID)

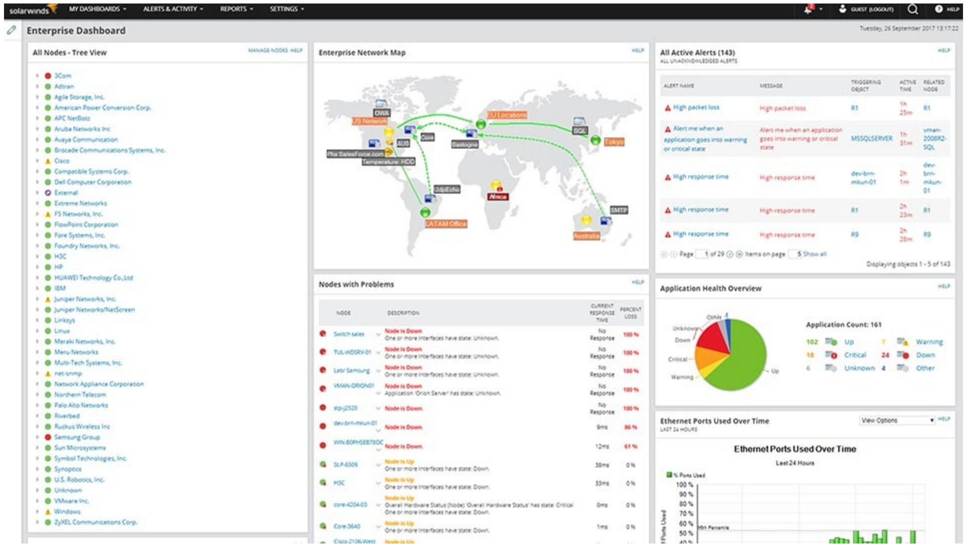


MIB Structure



SNMP Components: NMS

- SNMP NMS (Network Management Station)
  - Typically a server running SNMP NMS software.
  - Server can either periodically poll the SNMP Agents for MIB data, or receive that data in an unsolicited form when the agent is triggered to do so.



Enterprise Dashboard

Tuesday, 26 September 2017 13:17:22

All Nodes - Tree View

- 3Com
- Adtran
- Agile Storage, Inc.
- American Power Conversion Corp.
- APC NetBotz
- Aruba Networks Inc
- Avaya Communication
- Brocade Communications Systems, Inc.
- Cisco
- Compatible Systems Corp.
- Dell Computer Corporation
- External
- Extreme Networks
- F5 Networks, Inc.
- FlowPoint Corporation
- Fore Systems, Inc.
- Foundry Networks, Inc.
- H3C
- HP
- HUAWEI Technology Co.,Ltd
- IBM
- Juniper Networks, Inc.
- Juniper Networks/NetScreen
- Linksys
- Linux
- Meraki Networks, Inc.
- Meru Networks
- Multi-Tech Systems, Inc.
- net-snmp
- Network Appliance Corporation
- Northern Telecom
- Palo Alto Networks
- Riverbed
- Ruckus Wireless Inc
- Samsung Group
- Sun Microsystems
- Symbol Technologies, Inc.
- Synoptics
- U.S. Robotics, Inc.
- Unknown
- VMware Inc.
- Windows
- ZyXEL Communications Corp.

Nodes with Problems

NODE	DESCRIPTION	CURRENT RESPONSE TIME	PERCENT LOSS
Switch sales	Node is Down One or more interfaces have state: Unknown.	No Response	100 %
TUL-WDSRV-01	Node is Down One or more interfaces have state: Unknown.	No Response	100 %
Lab/ Samsung	Node is Down One or more interfaces have state: Unknown.	No Response	100 %
VMAN-ORION01	Node is Down Application 'Orion Server' has state: Unknown.	No Response	100 %
stp-j2320	Node is Down.	No Response	100 %
dev-brn-mkun-01	Node is Down.	9ms	86 %
WIN-B0PHSEB70OC	Node is Down.	12ms	61 %
St.P-6509	Node is Up One or more interfaces have state: Down.	38ms	0 %
H3C	Node is Up One or more interfaces have state: Down.	33ms	0 %
core-4204-03	Node is Up Overall Hardware Status (Node) 'Overall Hardware Status' has state: Critical One or more interfaces have state: Down.	0ms	0 %
Core-3640	Node is Up One or more interfaces have state: Down.	1ms	0 %
Cisco-2106-West	Node is Up		

All Active Alerts (143)

ALL UNACKNOWLEDGED ALERTS

ALERT NAME	MESSAGE	TRIGGERING OBJECT	ACTIVE TIME	RELATED NODE
High packet loss	High packet loss	R1	1h 25m	R1
Alert me when an application goes into warning or critical state	Alert me when an application goes into warning or critical state	MSSQLSERVER	1h 31m	vman-2008R2-SQL
High response time	High response time	dev-brn-mkun-01	2h 1m	dev-brn-mkun-01
High response time	High response time	R1	2h 23m	R1
High response time	High response time	R9	2h 28m	R9

Page 1 of 29 Items on page 5 Show all

Displaying objects 1 - 5 of 143

Application Health Overview

Application Count: 161

102	Up	7	Warning
18	Critical	24	Down
6	Unknown	4	Other

Ethernet Ports Used Over Time

LAST 24 HOURS

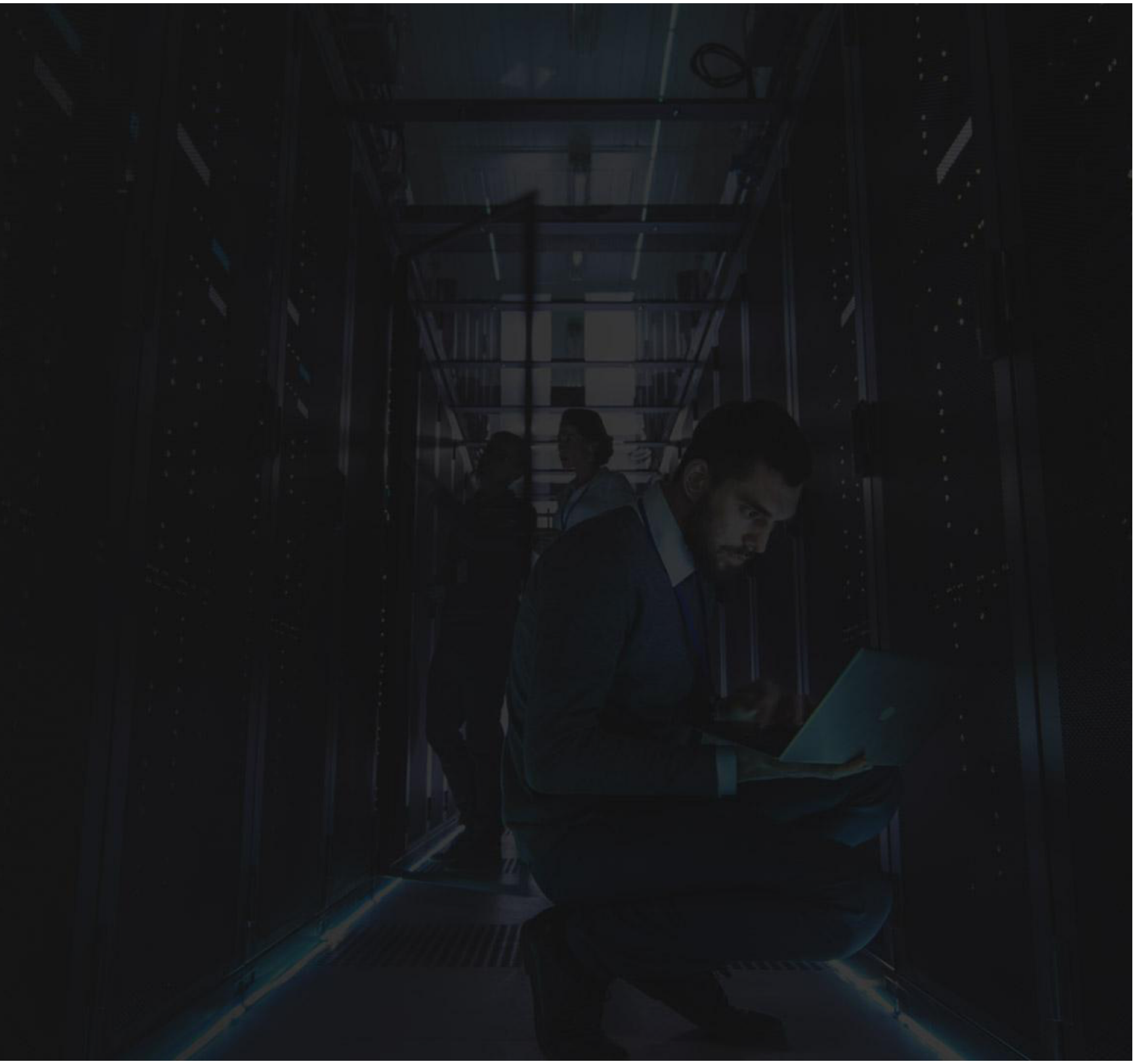
SNMP Message Types

- SNMP Get
  - Polling the MIB to retrieve data
  - Typically automated to occur at predefined intervals.
- SNMP Set
  - Modifying the MIB which, in turn, modifies device configuration.
- SNMP Response
  - PDU sent from Agent in reply to SNMP Get or SNMP Set message

SNMP Message Types

- SNMP Trap
  - Generated by SNMP Agent when threshold or error conditions occur.
  - Transmitted to NMS (SNMP Manager)
  - Agent does not receive an acknowledgement.
- SNMP Inform
  - Similar to an SNMP Trap
  - Only supported in SNMP version 3
  - Agent receives acknowledgement from NMS.

SNMP Versions



ine.com

Topic Overview

- Comparing SNMP versions
- SNMP Community Strings
- Configuring SNMP Community Strings
- Overview of SNMPv3

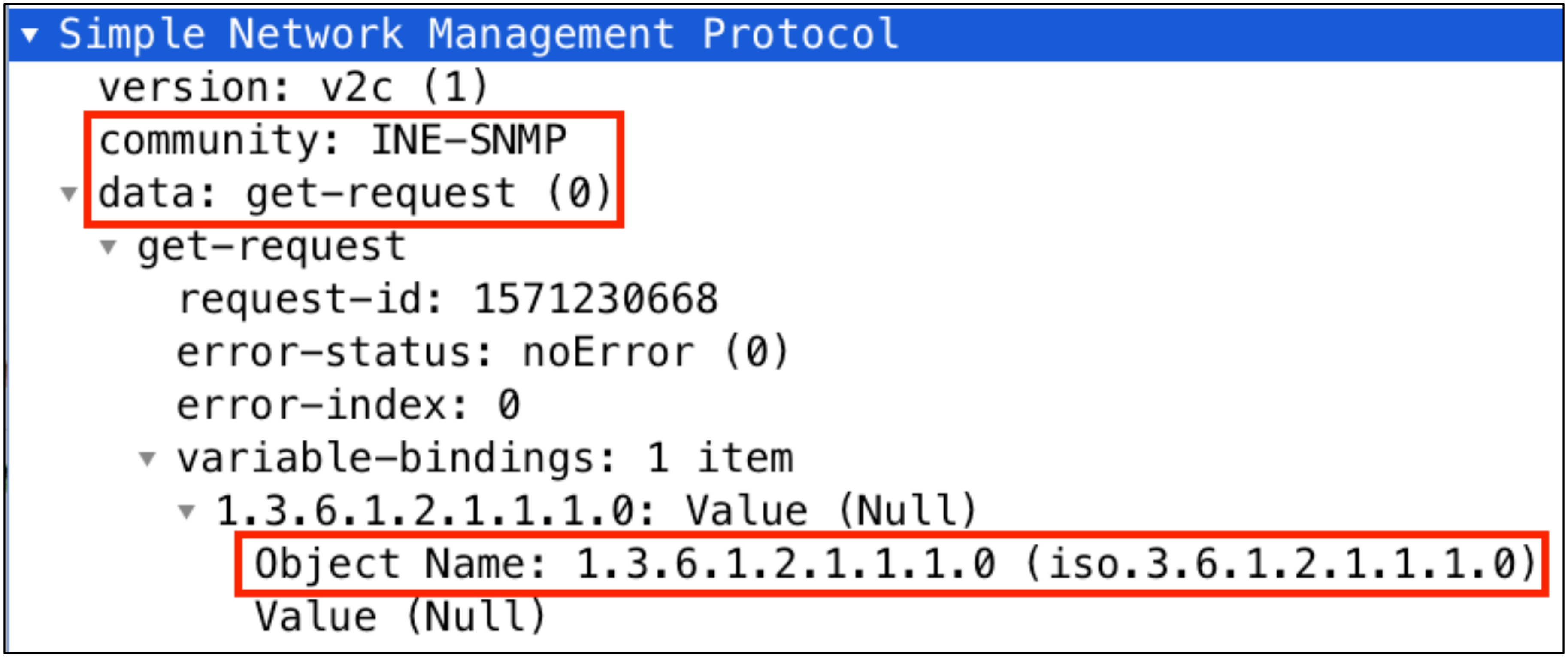
SNMP Versions (1 and 2c)

- SNMP Version-1 (very old…not used much)
- SNMP Version 2c
  - Extended capabilities of SNMP (new MIB support, new SNMP PDUs, GetBulkRequest, Inform)
  - Solved some performance deficiencies of SNMPv1 (64-bit variable counters vs. 32-bit counters in SNMPv1)
  - Still utilized SNMP Community Strings
  - Not compatible with SNMPv1 (different message formats and protocol operations)

Community Strings

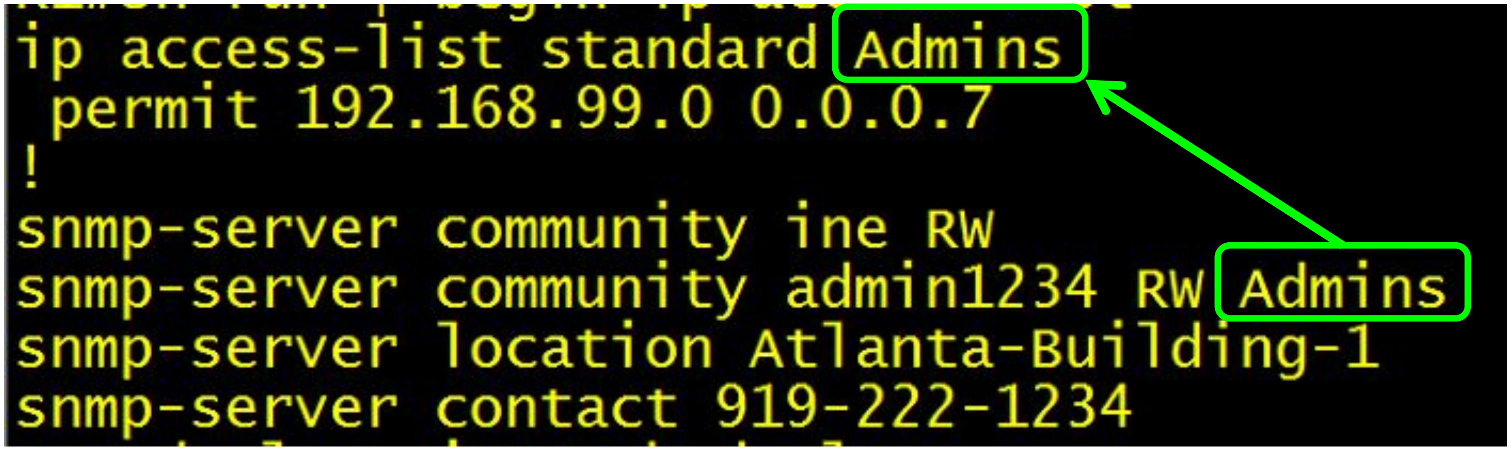
- Two types of Community Strings
- RO = Read-Only
  - Provides access to MIB variables for reading only.
- RW = Read-Write
  - Provides access to MIB variables for both reading, and modifying (writing).

Capture Of An OID



```
▾ Simple Network Management Protocol
    version: v2c (1)
    community: INE-SNMP
  ▾ data: get-request (0)
    ▾ get-request
        request-id: 1571230668
        error-status: noError (0)
        error-index: 0
      ▾ variable-bindings: 1 item
        ▾ 1.3.6.1.2.1.1.1.0: Value (Null)
            Object Name: 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0)
            Value (Null)
```

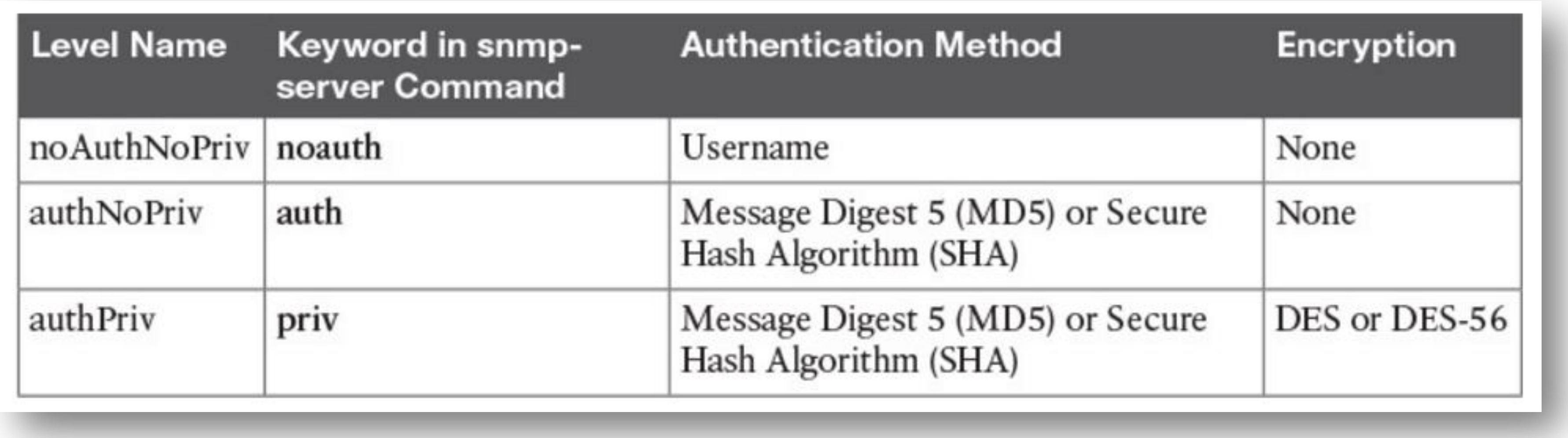
Configuring SNMP Community Strings



```
ip access-list standard Admins
 permit 192.168.99.0 0.0.0.7
!
snmp-server community ine RW
snmp-server community admin1234 RW Admins
snmp-server location Atlanta-Building-1
snmp-server contact 919-222-1234
```

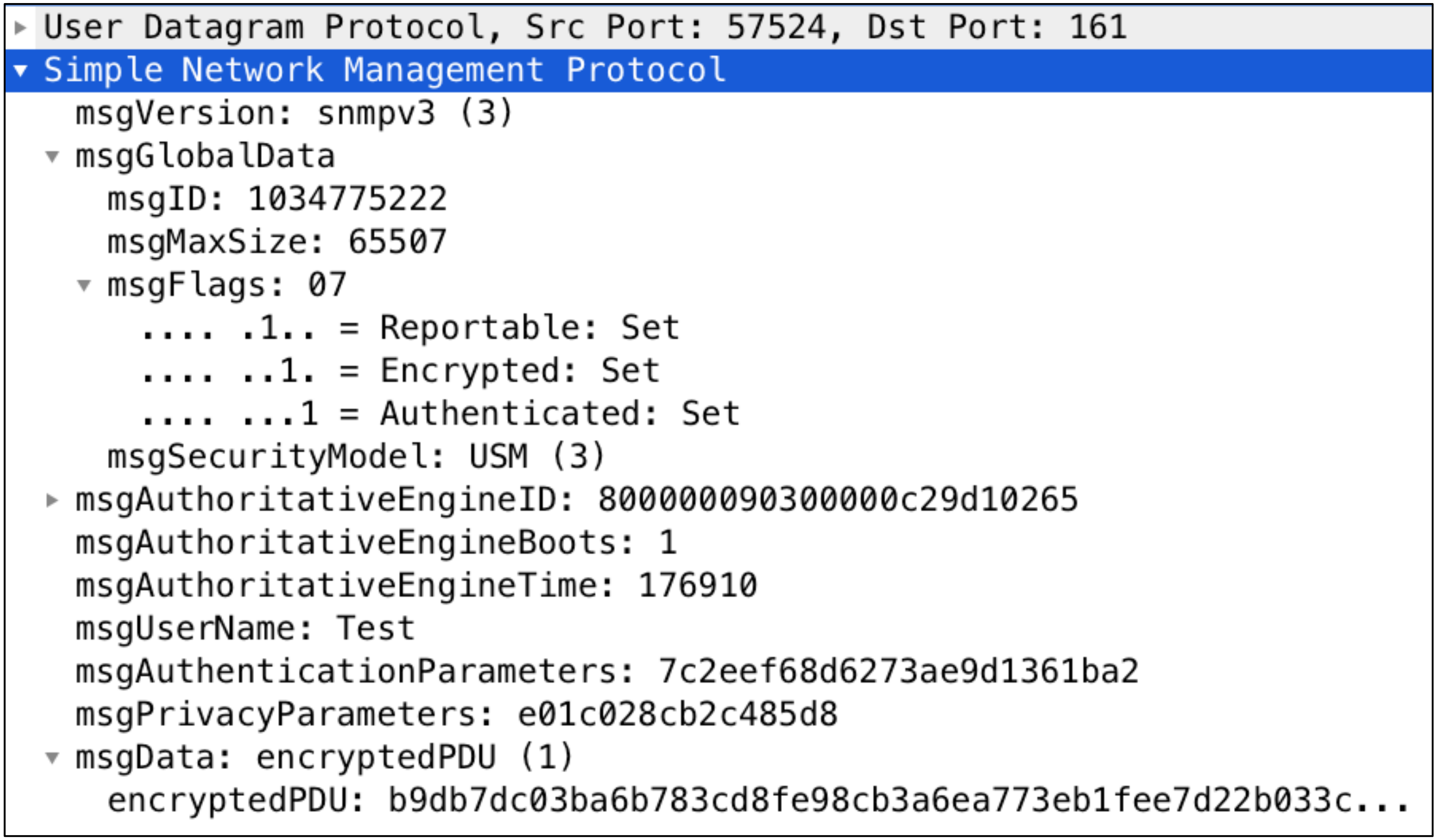
SNMP Version 3

- Provided the following added security benefits:
  - Message Integrity
  - Authentication
  - Encryption



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

SNMPv3 PDU Example



```
▸ User Datagram Protocol, Src Port: 57524, Dst Port: 161
▾ Simple Network Management Protocol
    msgVersion: snmpv3 (3)
  ▾ msgGlobalData
      msgID: 1034775222
      msgMaxSize: 65507
    ▾ msgFlags: 07
        .... .1.. = Reportable: Set
        .... ..1. = Encrypted: Set
        .... ...1 = Authenticated: Set
      msgSecurityModel: USM (3)
  ▸ msgAuthoritativeEngineID: 800000090300000c29d10265
    msgAuthoritativeEngineBoots: 1
    msgAuthoritativeEngineTime: 176910
    msgUserName: Test
    msgAuthenticationParameters: 7c2eef68d6273ae9d1361ba2
    msgPrivacyParameters: e01c028cb2c485d8
  ▾ msgData: encryptedPDU (1)
      encryptedPDU: b9db7dc03ba6b783cd8fe98cb3a6ea773eb1fee7d22b033c...
```

Thanks for Watching!

Configuring SNMPv1/v2c

ine.com

Topic Overview

- SNMPv1/v2c Configuration in Cisco IOS

SNMPv1/v2c Router Configuration

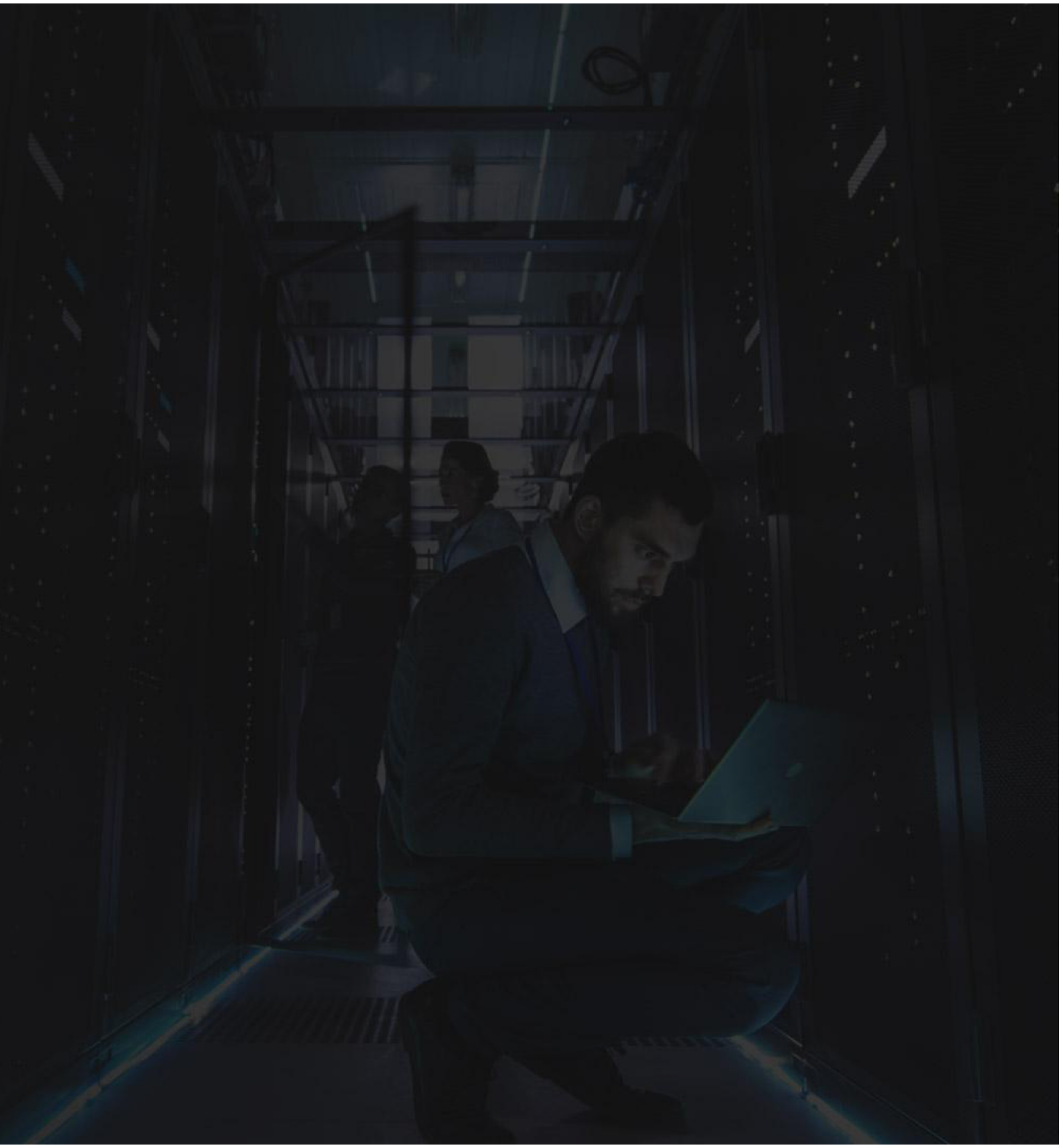
- Step-1: Create Access-List specifying authorized SNMP Management Stations.
  - Access-list 1 permit 1.1.1.0 0.0.0.255
  - Access-list 2 permit host 2.2.2.2
- Step-2: Define Community Lists (i.e. passwords) that will allow Read and/or Read-Write access to the Agent.
  - Snmp-server community Monitors ro 1
  - Snmp-server community Admins rw 2

SNMPv1/v2c Router Configuration

- Step-3: Configure Agent to know where to send SNMP Traps/Informs.
  - Snmp-server host 2.2.2.2 Admins SNMPv1 or v2c
  - …or…
  - Snmp-server host 2.2.2.2 informs v2c Admins SNMPv2c

Thanks for Watching!

Configuring SNMPv3



ine.com

Topic Overview

- Views, Groups & Users
- Configuring SNMPv3 Views
- Configuring SNMPv3 Groups & Users
- Configuring SNMPv3 Traps & Informs

Views, Groups & Users

- SNMPv3 Configuration involves two mandatory, and two optional steps.
  - Step-1 (optional): Define one-or-more SNMP Views
  - Step-2 (**required**): Define one-or-more SNMP Groups as well as the Security Model associated with that group.
  - Step-3 (**required**): Define one-or-more SNMP Users as well as the Security Model associated with that user.
  - Step-4 (optional): Define an SNMP-Host statement if Traps/Informs will be sent by the Agent.

Configuring SNMPv3 Views

- Configure an Access-List of authorized NMS addresses

```
access-list 1 permit 1.1.1.0 0.0.0.255
```

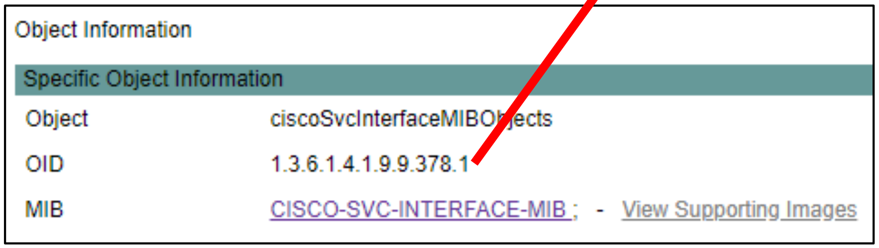
- Configure an SNMP View (optional)

```
snmp-server view Interfaces 1.3.6.1.4.1.9.9.378.1 included
```

Descriptive Name of View

Specific Object ID or MIB name

Include (or exclude) this MIB from the View

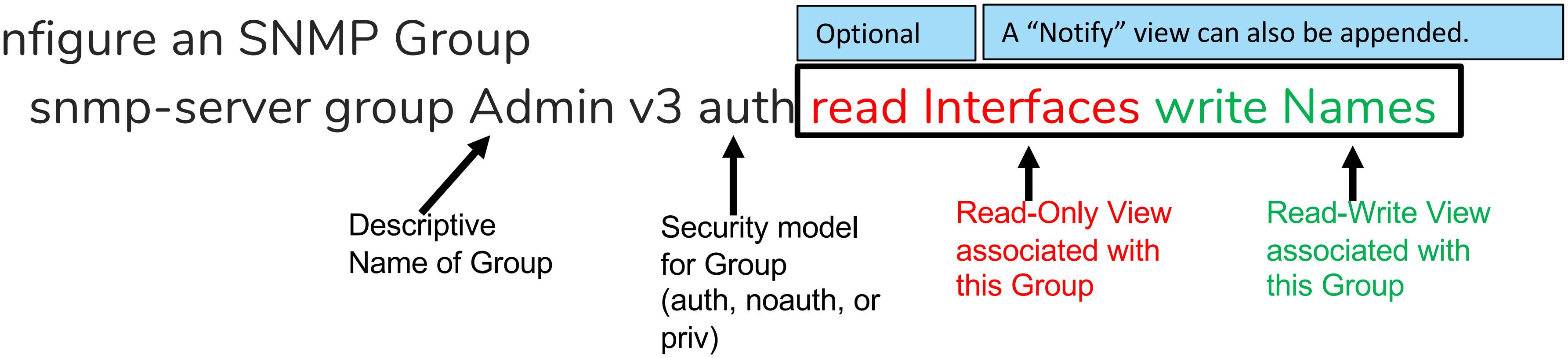


Object Information

Specific Object Information	
Object	ciscoSvcInterfaceMIBObjects
OID	1.3.6.1.4.1.9.9.378.1
MIB	CISCO-SVC-INTERFACE-MIB ; - View Supporting Images

Configuring SNMPv3 Groups & Users

- Configure an SNMP Group



Optional

A “Notify” view can also be appended.

```
snmp-server group Admin v3 auth read Interfaces write Names
```

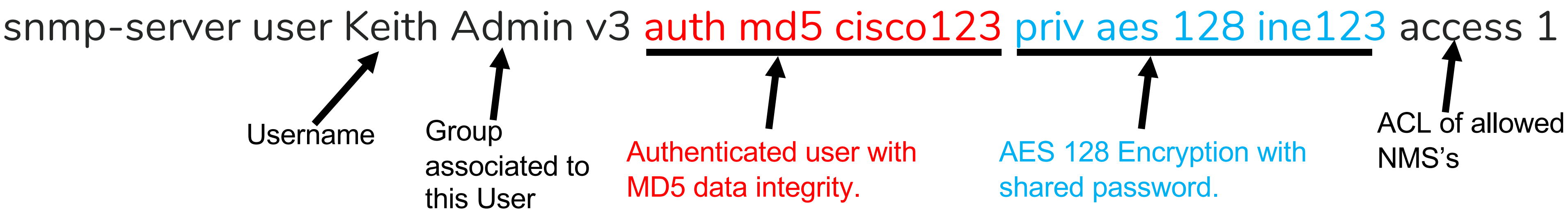
Descriptive Name of Group

Security model for Group (auth, noauth, or priv)

Read-Only View associated with this Group

Read-Write View associated with this Group

- Configure an SNMP User



```
snmp-server user Keith Admin v3 auth md5 cisco123 priv aes 128 ine123 access 1
```

Username

Group associated to this User

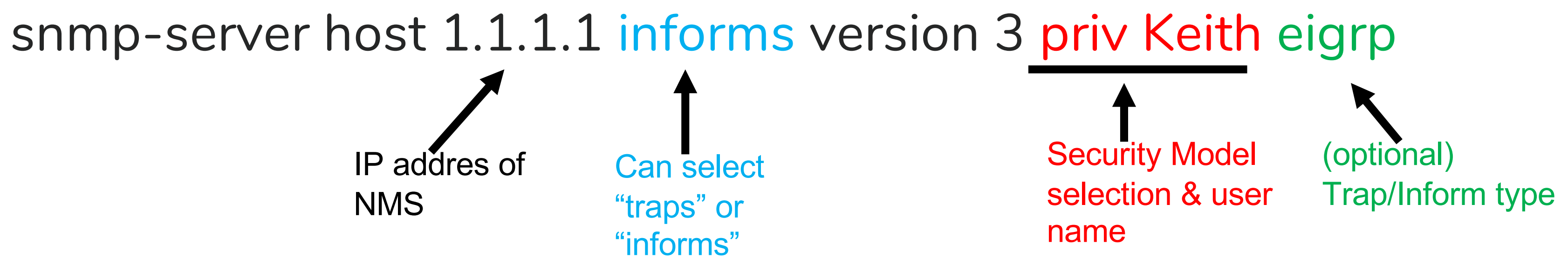
Authenticated user with MD5 data integrity.

AES 128 Encryption with shared password.

ACL of allowed NMS’s

Configuring SNMPv3 Traps & Informs

- Configure Router/Switch to send SNMP Traps (or Informs)



```
snmp-server host 1.1.1.1 informs version 3 priv Keith eigrp
```

IP addres of NMS

Can select “traps” or “informs”

Security Model selection & user name

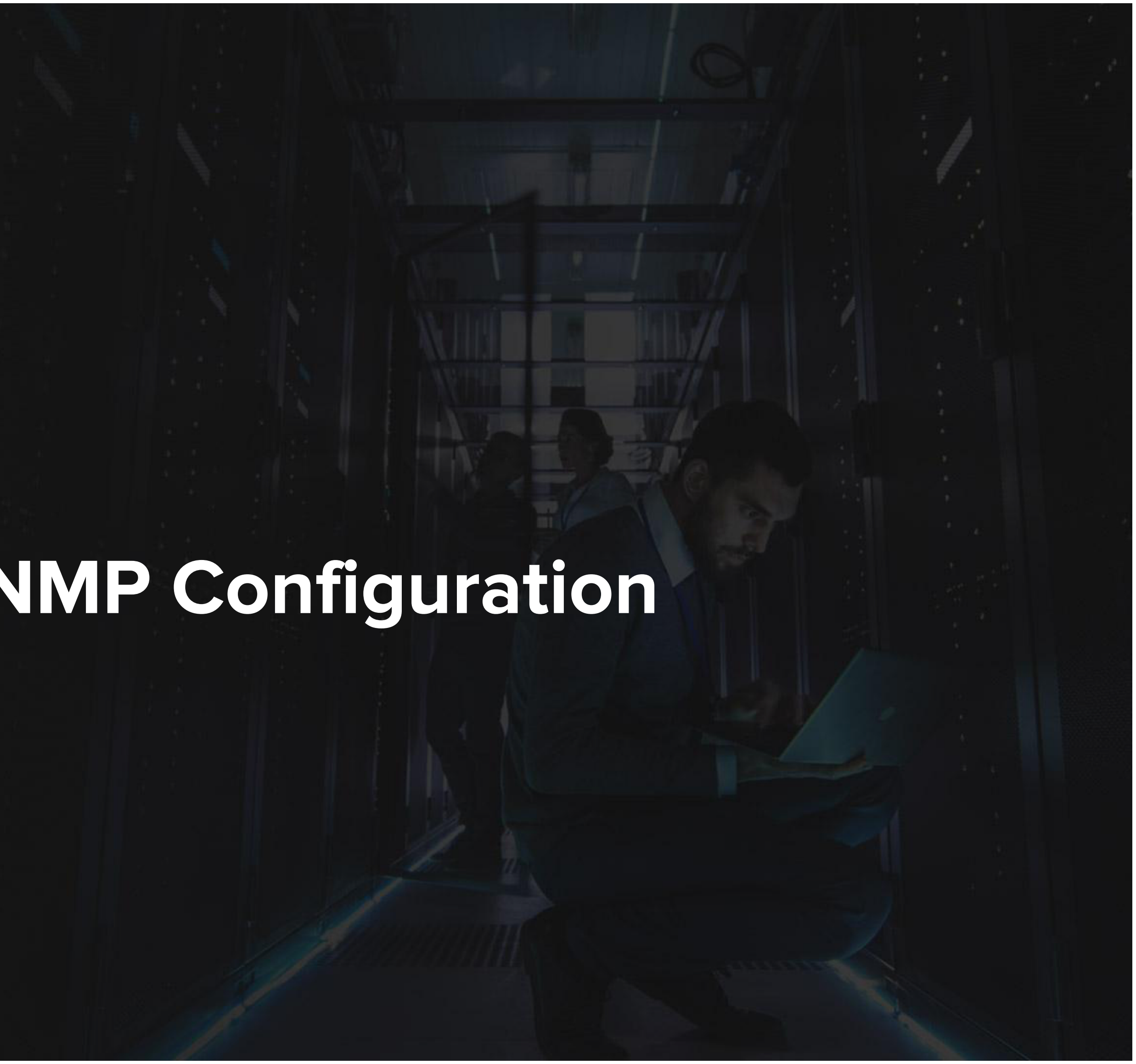
(optional) Trap/Inform type

- Specify interface for sending of SNMP Traps (or Informs)

```
snmp-server trap-source FastEthernet0/1
```

Thanks for Watching!

Verifying Your SNMP Configuration



ine.com

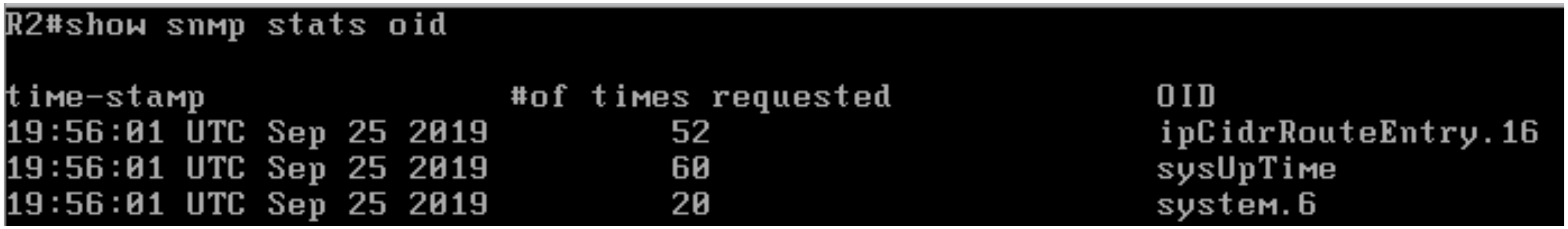
Topic Overview

- Verifying SNMP in IOS

Verifying SNMP In IOS

- The best way to confirm your SNMP configuration is by viewing output displayed on the NMS
- But what if the NMS is unavailable?
- Various IOS commands can verify communications between NMS and SNMP Agent

  - **show snmp stats oid**

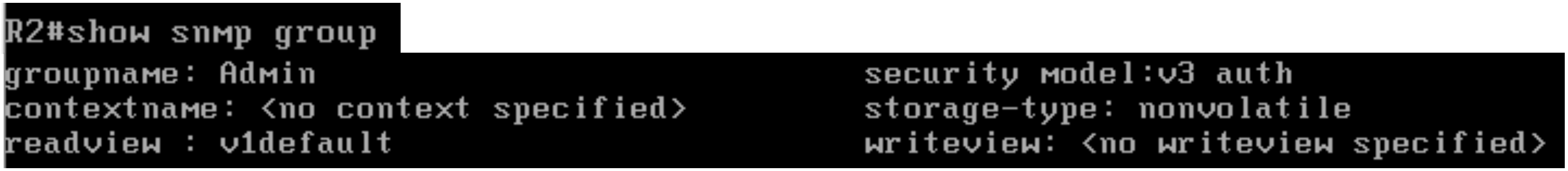


```
R2#show snmp stats oid

time-stamp                   #of times requested            OID
19:56:01 UTC Sep 25 2019              52                    ipCidrRouteEntry.16
19:56:01 UTC Sep 25 2019              60                    sysUpTime
19:56:01 UTC Sep 25 2019              20                    system.6
```

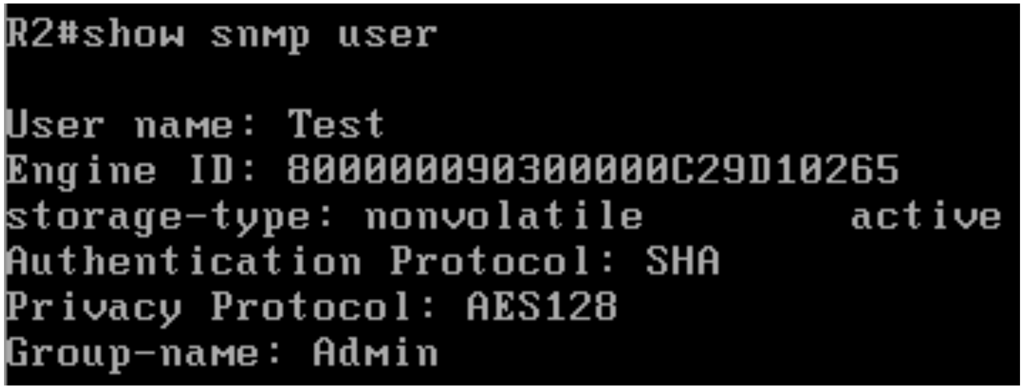
Other IOS Verification Commands

- Show snmp group



```
R2#show snmp group
groupname: Admin                            security model:v3 auth
contextname: <no context specified>         storage-type: nonvolatile
readview : v1default                        writeview: <no writeview specified>
```

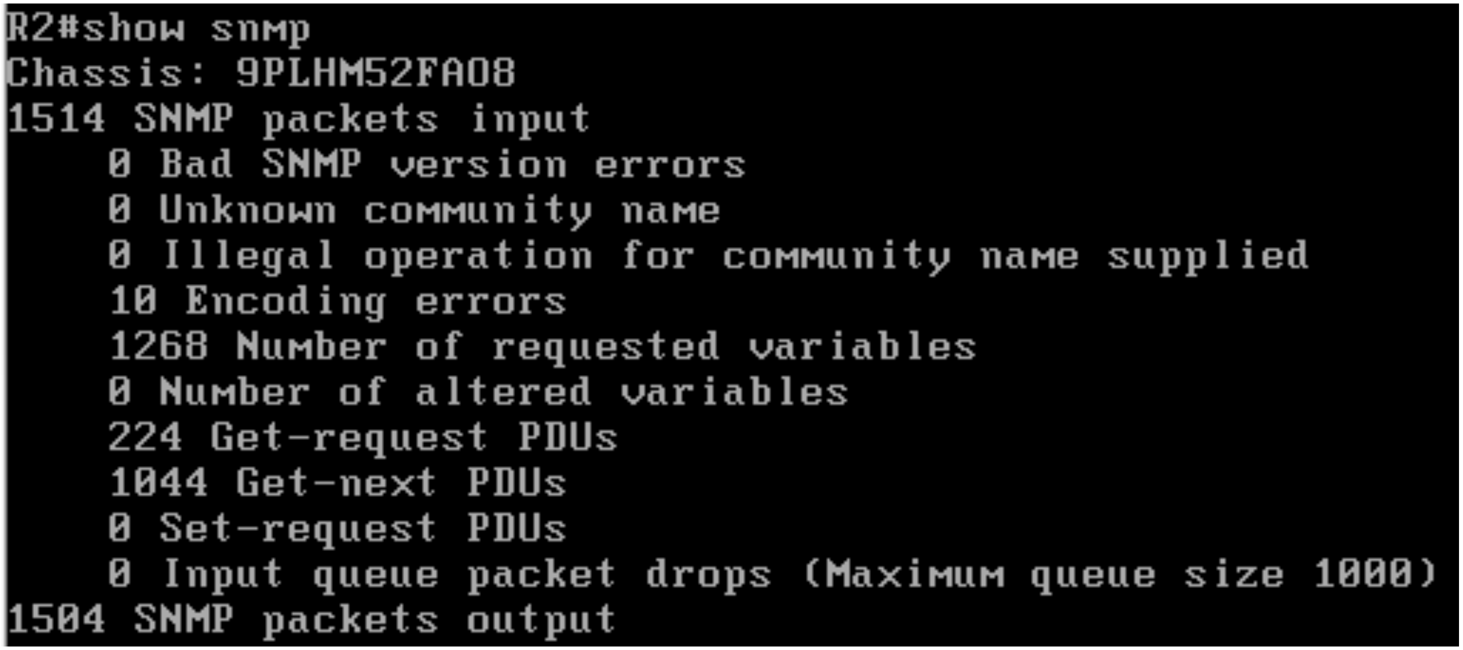
- Show snmp user



```
R2#show snmp user

User name: Test
Engine ID: 800000090300000C29D10265
storage-type: nonvolatile        active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: Admin
```

Show SNMP



```
R2#show snmp
Chassis: 9PLHM52FA08
1514 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    10 Encoding errors
    1268 Number of requested variables
    0 Number of altered variables
    224 Get-request PDUs
    1044 Get-next PDUs
    0 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
1504 SNMP packets output
```

INE

Thanks for Watching!

Introduction To Syslog

ine.com

Topic Overview

- Introduction To Syslog
- Messages & Transport
- Syslog Message Format
- Syslog Facility Levels
- Syslog Severity Levels
- Cisco IOS Basic Syslog Configuration

Introduction To Syslog

- Why do we need logging?
  - Reduce the quantity of trouble tickets by getting notifications of problems as they occur
  - Reduce downtime
  - Decrease the volume of business interruptions
  - Promotes preventative troubleshooting
- SYSLOG = **Sys**tem **log**ging
- A tool/protocol for system logging
- Standardized in RFC 5424
  - Originally defined in RFC 3164

Syslog Messages & Transport

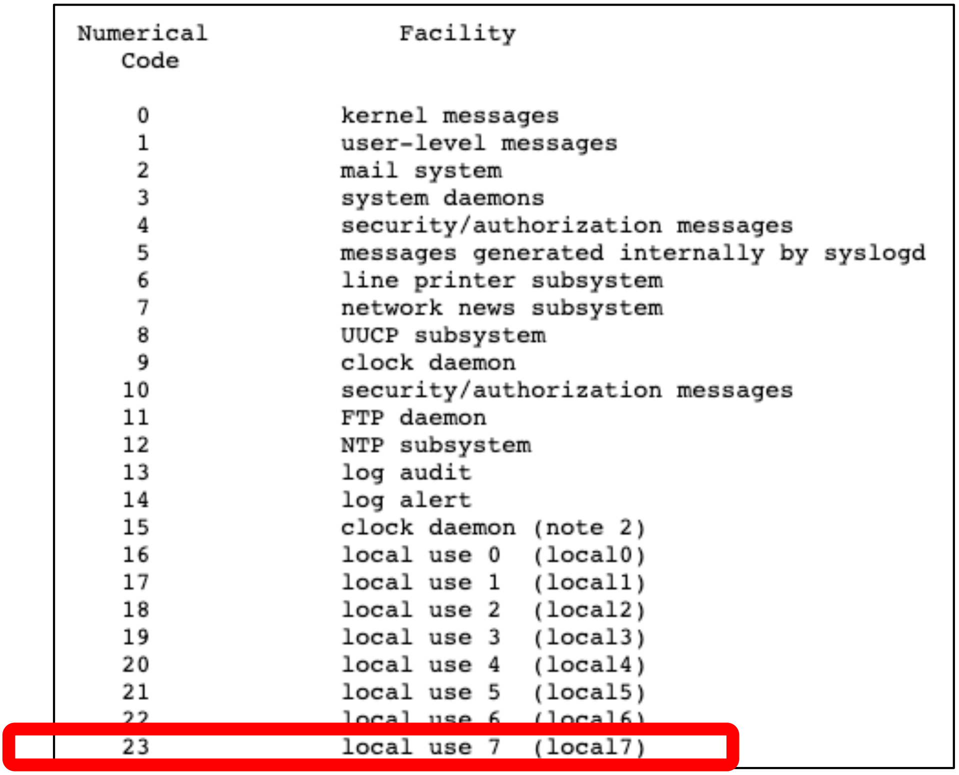
- Syslog Messages include several things:
  - Timestamps
  - Event message
  - Severity
  - Host IP address
  - Diagnostics
  - Etc
- Utilizes UDP (port 514) and IP to transport notification messages from device to Syslog server (a.k.a. Event Message Collector)

Syslog Message Format

- Syslog has a standard definition and format of the log message defined by RFC 5424
- Every Syslog message is composed of three pieces:
  - Header
  - Structured Data
  - Message
- Header consists of a Syslog priority value and a version
  - The priority value is calculated using the formula (Priority = Facility * 8 + Level)
  - Version is similar to a simple counter

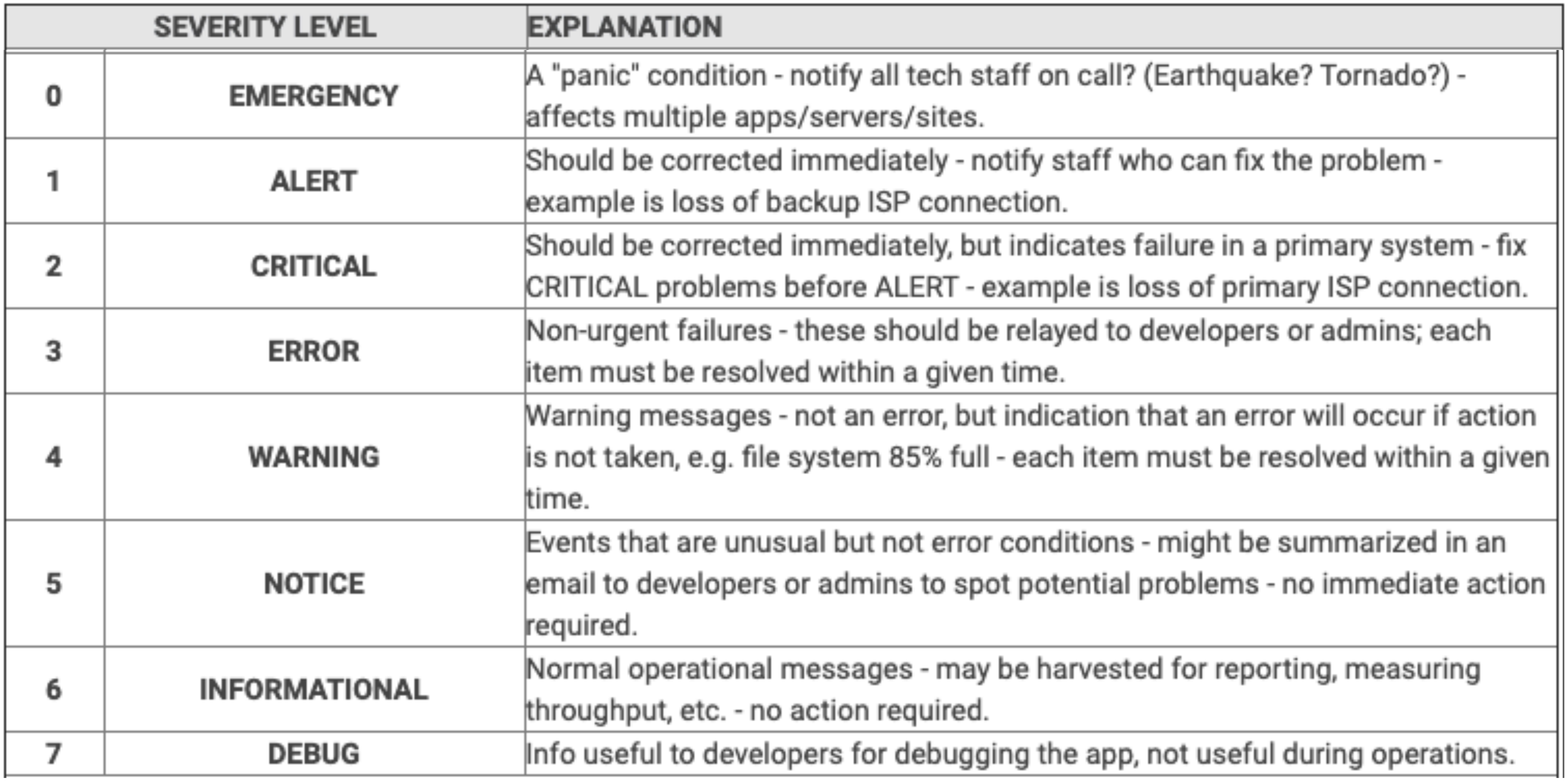
SYSLOG Facility Levels

- The facility represents the machine process that created the syslog event.
- A value that represents a way of determining which process of the machine created the message



Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

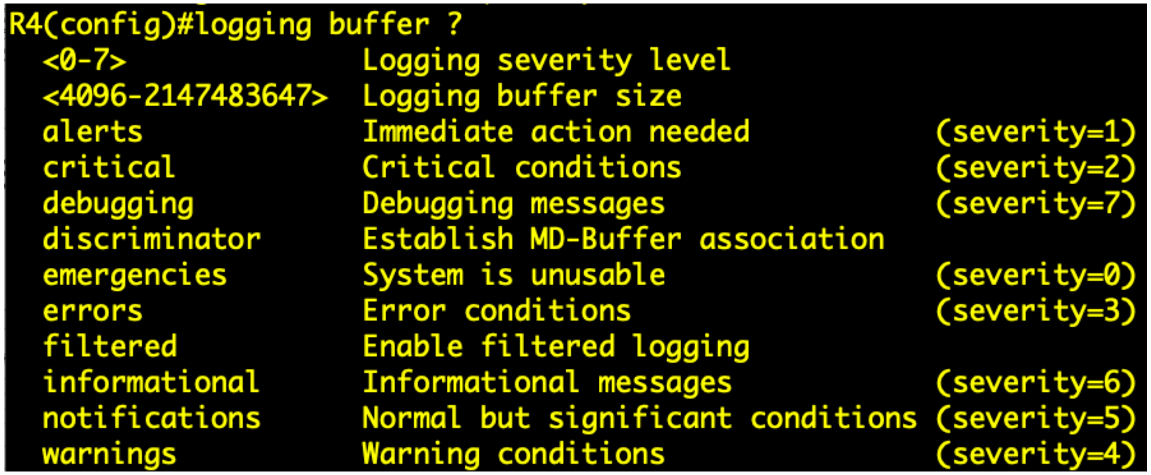
SYSLOG Priority/Severity Levels



SEVERITY LEVEL		EXPLANATION
0	EMERGENCY	A "panic" condition - notify all tech staff on call? (Earthquake? Tornado?) - affects multiple apps/servers/sites.
1	ALERT	Should be corrected immediately - notify staff who can fix the problem - example is loss of backup ISP connection.
2	CRITICAL	Should be corrected immediately, but indicates failure in a primary system - fix CRITICAL problems before ALERT - example is loss of primary ISP connection.
3	ERROR	Non-urgent failures - these should be relayed to developers or admins; each item must be resolved within a given time.
4	WARNING	Warning messages - not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time.
5	NOTICE	Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required.
6	INFORMATIONAL	Normal operational messages - may be harvested for reporting, measuring throughput, etc. - no action required.
7	DEBUG	Info useful to developers for debugging the app, not useful during operations.

Sending Syslog Messages

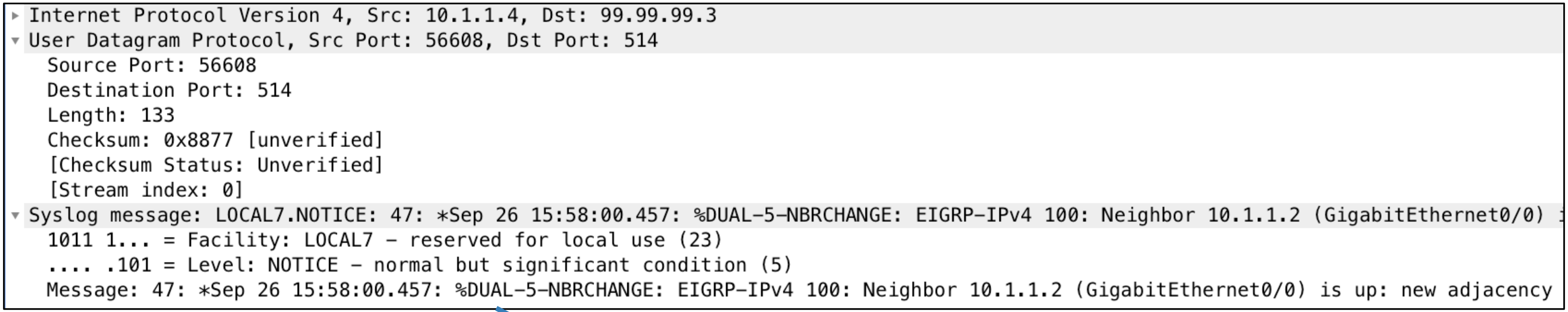
- Syslog messages can be stored internally in the system buffer



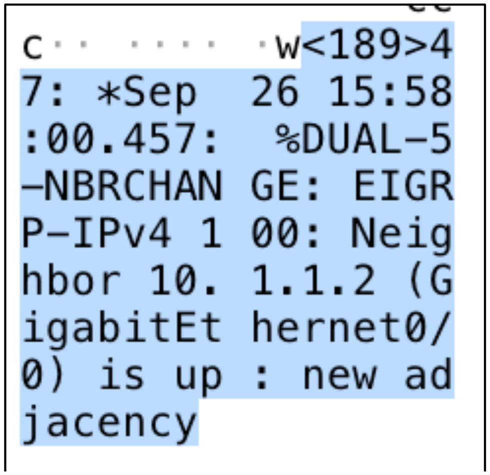
```
R4(config)#logging buffer ?
  <0-7>               Logging severity level
  <4096-2147483647>   Logging buffer size
  alerts              Immediate action needed             (severity=1)
  critical            Critical conditions                 (severity=2)
  debugging           Debugging messages                  (severity=7)
  discriminator       Establish MD-Buffer association
  emergencies         System is unusable                  (severity=0)
  errors              Error conditions                    (severity=3)
  filtered            Enable filtered logging
  informational       Informational messages              (severity=6)
  notifications       Normal but significant conditions (severity=5)
  warnings            Warning conditions                  (severity=4)
```

- Syslog messages can also be sent to an external syslog server
  - Device(config)#**logging host <ip-address>**

Example Syslog Message



```
▸ Internet Protocol Version 4, Src: 10.1.1.4, Dst: 99.99.99.3
▾ User Datagram Protocol, Src Port: 56608, Dst Port: 514
    Source Port: 56608
    Destination Port: 514
    Length: 133
    Checksum: 0x8877 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
▾ Syslog message: LOCAL7.NOTICE: 47: *Sep 26 15:58:00.457: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.2 (GigabitEthernet0/0) i
    1011 1... = Facility: LOCAL7 - reserved for local use (23)
    .... .101 = Level: NOTICE - normal but significant condition (5)
    Message: 47: *Sep 26 15:58:00.457: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.1.1.2 (GigabitEthernet0/0) is up: new adjacency
```



```
c··  ····· ·w<189>4
7: *Sep  26 15:58
:00.457:  %DUAL-5
-NBRCHAN GE: EIGR
P-IPv4 1 00: Neig
hbor 10. 1.1.2 (G
igabitEt hernet0/
0) is up : new ad
jacency
```

Thanks for Watching!