LET'S
BUILD
TOMORROW
TODAY

Securely Managing Your Networks With SNMPv3

Gilbert Bollinger

BRKNMS-2658

Cisco live!

Housekeeping

- Please remember this is a 'non-smoking' venue!
- Please mute your mobile devices
- Please make use of the recycling bins provided
- Please remember to wear your badge at all times

Agenda

- Introduction
- Balancing Security with Manageability
- SNMP Security
- Securing SNMP
- SNMP on the Network
- Configuration Best Practices
- Conclusion

Abstract

- This technical session explains the concepts, issues, and current capabilities in network management with Simple Network Management Protocol (SNMP) v3. We will compare and contrast the functionality of SNMP v1, v2c, and v3. A considerable amount of time will be spent covering SNMPv3 and understanding how to configure its usage. We'll discuss the benefits and challenges with its implementation, along with application, device support and instrumentation.
- And finally, you'll learn what to look for when considering network management tools and applications that use SNMPv3 to ensure proper and efficient functionality.
- Target Audience - All network administrators

What Are We Not Covering?

- How to manage VPNs
- How to manage IDS
- How to manage firewalls/FWSM/PIX®
- Security management applications [ASDM, IronPort, CMC, etc]
- Other Security features – AAA, SSH, ACLs, etc.
  [Note: Some of these concepts are covered in the Extra Slides at the end of the preso!]

Network Management Goals

- Fault, Configuration, Accounting, Performance, Security (FCAPS)
- Inventory—discover/identify all devices for asset management, configuration management, software image management, etc.
- Performance Monitoring—poll statistics and get results; trending
- Fault Management—get asynchronous alerts to system issues

Network Security Goals

- Traditional categories:
  - Data confidentiality
  - Data integrity
  - Data availability
- Traditional approaches:
  - Restrict access to authorized users
  - Obscure devices from attackers
  - Identify/locate vulnerabilities
  - Identify network threats

Security Things that Bother Security Folks

- Configuration management applications that use Telnet session (clear-text) over public networks
- Default passwords and community strings
- Difficult-to-control port usage (NMS, device and client issues)
- Ability to reboot a router via SNMP
- DNS is usually required (information is power)

- SNMP community strings (clear-text)
- SNMP tools use of port scanning methods for network discovery
- CDP
- Ping sweeps

Security Things that Bother NM Folks

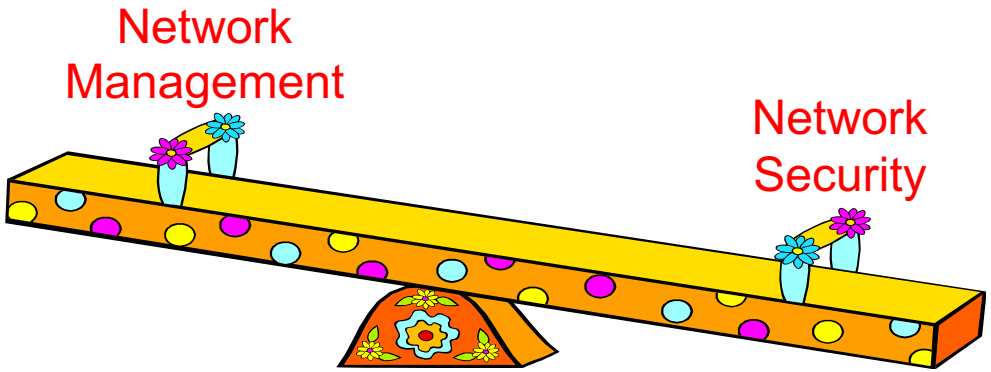
- “No CDP” policies
- “No SNMP” policies
- Security appliances that ID legitimate NM traffic as rogue activity
- Firewalls blocking NM traffic
- Overly sensitive IDS monitoring solutions that flood event monitoring tools with needless alarms

Conflict? Or…

Intersection of Network Management and Security?

Compromise?

- Identify and Define Your Policies
- Understand Business Requirements
- Government/political/legal requirements
  - HIPAA
  - S-Ox
  - FIPS
  - DPA
  - PCI DSS
- Resource requirements and constraints
- Risk assessment



Compromise!

- Balance the business needs of NM & Security
- Encourage joint team meetings to share needs and concerns
- Recognize that each team has a different perspective
- Reasonable compromises may be possible as we understand each other's needs/concerns
- Don't empower an environment of 'Security guys get whatever they want' – NM is just as important
- Encourage pilots of new techniques and features with tangible metrics to remove the 'feelings'

Simple Network Management Protocol (SNMP)

SNMP v1/2c and ~~Security~~ Insecurity

- Community strings define which management domain a device is in
- There are separate Read-Only and Read-Write strings
  (CatOS switches also have Read-Write-All)
- Community strings are passed as clear-text in packets—easily sniffed and therefore not considered secure
- Use access-lists and SNMP views against community definitions to reduce security exposures

NM → Device

SNMP v1/2c Sniffer Example

- NMS requests data from the router
- "snmpget –v2c –cpublic lab-router system.sysContact.0"
- Sniffer capture reveals the community string is "public"

```
⊞ User Datagram Protocol, Src Port: 36431 (36431), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    Version: 2C
    Community: public
    PDU type: GET
    Request Id: 0x697c3085
    Error Status: NO ERROR
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.4.0 (SNMPv2-MIB::sysContact.0)
    Value: NULL

0000  00 01 97 37 64 00 08 00  20 a8 8a ba 08 00 45 00   ...7d...  .....E.
0010  00 47 1f 61 40 00 ff 11  4e 30 ac 12 56 4a 0b 84   .G.a@...  NO..VJ..
0020  00 34 8e 4f 00 a1 00 33  93 3d 30 29 02 01 01 04   .4.O...3  .=0)....
0030  06 70 75 62 6c 69 63 a0  1c 02 04 69 7c 30 85 02   .public.  ...i|0..
0040  01 00 02 01 00 30 0e 30  0c 06 08 2b 06 01 02 01   .....0.0  ...+....
0050  01 04 00 05 00                                      .....
```

NM ⟵ Device

SNMP v1/2c Sniffing Example

- Device returns an SNMP get response
- Sniffer capture reveals the community string is “public”
- The value of sysContact.0 is

  “Cisco NOC / 888-555-1234”

```
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: 36431 (36431)
⊟ Simple Network Management Protocol
    Version: 2C
    Community: public
    PDU type: RESPONSE
    Request Id: 0x697c3085
    Error Status: NO ERROR
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.4.0 (SNMPv2-MIB::sysContact.0)
    Value: STRING: "Cisco NOC / 888-555-1234"

0000  08 00 20 a8 8a ba 00 01  97 37 64 00 08 00 45 00   .. ..... .7d...E.
0010  00 61 18 f1 00 00 fe 11  95 86 0b 84 00 34 ac 12   .a...... .....4..
0020  56 4a 00 a1 8e 4f 00 4d  e3 20 30 43 02 01 01 04   VJ....O.M. 0C....
0030  06 70 75 62 6c 69 63 a2  36 02 04 69 7c 30 85 02   .public. 6..i|0..
0040  01 00 02 01 00 30 28 30  26 06 08 2b 06 01 02 01   ......(0 &..+....
0050  01 04 00 04 1a 22 43 69  73 63 6f 20 4e 4f 43 20   ....."Ci sco NOC
0060  2f 20 38 38 38 2d 35 35  35 2d 31 32 33 34 22      / 888-55 5-1234"
```

Locking Down SNMP v1/2c

- ACL applied to SNMP community strings
- Define a Read-only ACL and a Read-Write ACL
- Only devices on 192.168.1.0/24 can do snmpgets with the correct community string
- Only specific .10 and .13 NMS servers can do snmpsets with the correct community string

```
access-list 10 permit 192.168.1.0 0.0.0.255
!
access-list 20 permit 192.168.1.10
access-list 20 permit 192.168.1.13
access-list 20 deny any log
!
snmp-server community dontusepublic ro 10
snmp-server community dontuseprivate rw 20
```

Locking Down SNMP v1/2c

SNMP – IOS-XR

```
ipv4 access-list SNMP_READ
  10 permit ipv4 192.168.1.0/24
!
ipv4 access-list SNMP_WRITE
  10 permit ipv4 192.168.1.10
  20 permit ipv4 192.168.1.13
  30 deny any log
!
snmp-server community dontusepublic RO SNMP_READ
snmp-server community dontuseprivate RW SNMP_WRITE
```

SNMP – NXOS

```
ip access-list SNMP_READ
  10 permit ip 192.168.1.0/24 any
!
ip access-list SNMP_WRITE
  10 permit ip 192.168.1.10/32 any
  20 permit ip 192.168.1.13/32 any
  30 deny any log
!!
snmp-server community dontusepublic ro
snmp-server community dontusepublic use-acl SNMP_READ
snmp-server community dontuseprivate rw
snmp-server community dontuseprivate use-acl SNMP_WRITE
```

Authentication Failure Notifications

- An SNMP authenticationFailure trap can be generated and sent to the NMS console

```
131 days 10h:8m:0.69s Tue Apr 20 19:41:16 2011 0 public 4 0 1135488069
10.20.30.1
```

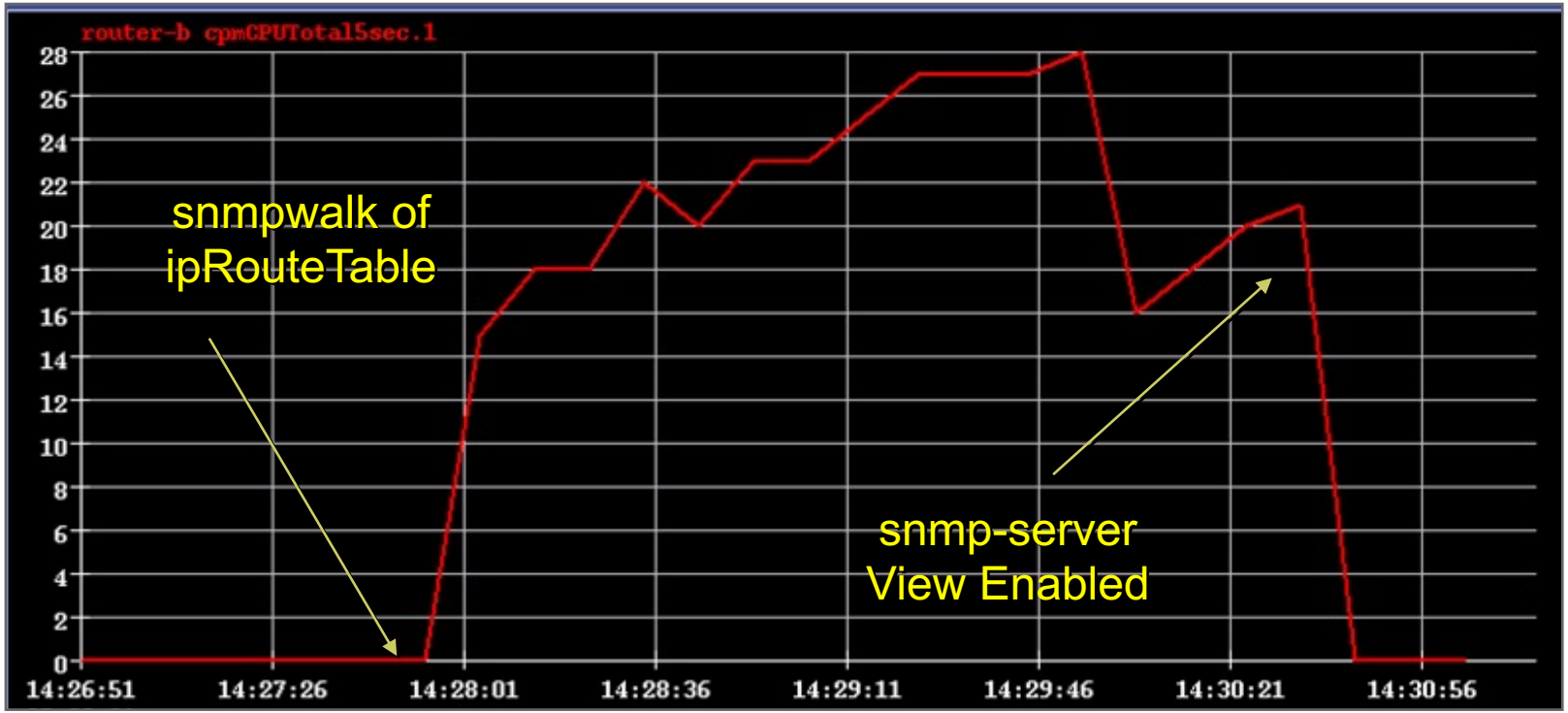
- Syslog events can also be generated

```
Apr 20 19:41:16 EDT: %SNMP-3-AUTHFAIL: Authentication failure for SNMP req
from host 10.20.30.1

Apr 20 19:45:19 EDT: %SEC-6-IPACCESSLOGS: list 10 denied 10.20.30.1 1
packet
```

- Sometime we need to permit polling access, but restrict access to certain MIBs
- Some NM apps poll IP route tables and ARP caches—this can cause high CPU load on low-end routers with many route entries
- Use SNMP Views (“snmp-server views” configuration)
  – like ACLs for MIBs

SNMP View Application



Cisco 2621 w/64MB RAM and 4000 Routes (EIGRP)
snmpwalk Would Have Run for 25½ Minutes Unrestricted

Locking Down SNMP Access – SNMP Views

- Cisco IOS
- ‘snmp-server view’ example
- If the router doesn’t accept the ipRouteTable MIB tree descriptor use ‘ip.21’. Use ‘ip.22’ for ipNetToMediaTable.

```
snmp-server view nopoll internet included
snmp-server view nopoll ipRouteTable excluded
snmp-server view nopoll at excluded
snmp-server view nopoll ipNetToMediaTable excluded
!
snmp-server community public view nopoll ro
```

Locking Down SNMP Access – SNMP Views

Cisco IOS XR

```
Same as IOS
```

Cisco NX-OS

```
Dependent on RBAC and DDTS CSCtc86349
```

SNMPv3

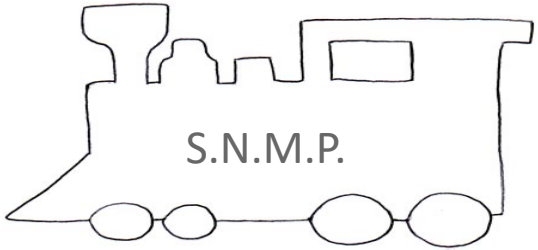
- What is it?
- What are the three levels?
- Sniffer caps
- Configuration examples
- How can I use it? Which Cisco applications use it? Which partner applications use it?

SNMPv3

- An interoperable standards-based protocol for network management
- Defined by RFCs 3410 to 3418 and 3826 (Advanced Encryption)
- Provides secure access to devices by a combination of authenticating and encrypting packets
- The security features provided in SNMPv3 are:
  - Message integrity—Ensuring that a packet has not been tampered with in-transit
  - Authentication—Determining the message is from a valid source
  - Encryption (optional)—Obscuring the contents of a packet prevent it from being seen by an unauthorized source

SNMPv3

- In SNMPv1/2c “Community Strings” are required to poll/set a device’s MIB variables
- In SNMPv3 user/group assignments with an authentication password permit authentication
- Every SNMPv3 sender/receiver has an snmpEngineID that uniquely identifies itself in the network
  - A key principal is “authoritative engine ID” - the device WITH the needed information is ‘authoritative’
- Any poll/set done with an invalid snmpEngineID is rejected and a REPORT packet is generated
- Each device can have multiple ‘identities’ called a context
  - Essentially a separate MIB environment or partitioned space
    Used with BRIDGE-MIB/VLAN polling



SNMP Versions and Capabilities

	Level	Auth	Encryption	What Happens
SNMPv1	noAuthNoPriv	Community String		Uses a Community String Match for Authentication
SNMPv2c	noAuthNoPriv	Community String		Uses a Community String Match for Authentication
SNMPv3	noAuthNoPriv	Username		Uses a Username Match for Authentication
SNMPv3	authNoPriv	MD5 or SHA		Provides Authentication Based on HMAC-MD5 or HMAC-SHA Algorithms
SNMPv3	authPriv	MD5 or SHA	CBC-DES	Adds DES 56-Bit Encryption in Addition to Authentication Based on DES-56

128/192/256-Bit AES and 168-Bit 3DES Available in 12.4(2)T
Other Supported Images in Backup Slides

The User-Based Security Model (USM)

- Uses Message-Digest algorithm 5 (MD5) or Secure Hash Algorithm (SHA) for digest computation.
- Provides data integrity against data modification attacks, indirectly provides data origin authentication, and defends against masquerade attacks.
- Time indicators defend against message stream modification attacks.
- Data Encryption Standard (DES) in cipher block chaining mode (CBC) optionally protects against disclosure [provides encryption]

User-Based Security Model (USM)

- Each user has a unique password/non-localized key – Two are needed
  - authentication (authKey)
  - encryption/privacy (privKey)

- Keys are not stored in device MIB.
- RFC does not allow for user passwords or keys to be stored in user-accessible config
  - [Cisco obscures in non-accessible NVRAM]

> …a user's password or non-localized key MUST NOT be stored on a managed device/node. Instead the localized key SHALL be stored (if at all), so that, in case a device does get compromised, no other managed or managing devices get compromised.
>
> RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) Section 11.2, Defining Users

Security with One Password

- Users want one domain-wide authentication and encryption password to remember instead of one per device…
- ...But for security we need each SNMP Engine to have their secrets cryptographically unique
- A key localization algorithm converts a user password and an snmpEngineID into an exclusive secret uniquely associated to each managed device
- If an SNMP Engine is compromised, only communication with that engine is compromised. All communication with the user and other engines are still secure.

Non-Localized Keys

How Are They Created

When You Declare a User in the System Config the SNMP Sub-System Takes the User's Password and Concatenates Over and Over

myauthpassword**myauthpassword**myauthpassword

Until a 1 MB String in Size

↓

MD5/SHA (One Way Hash)

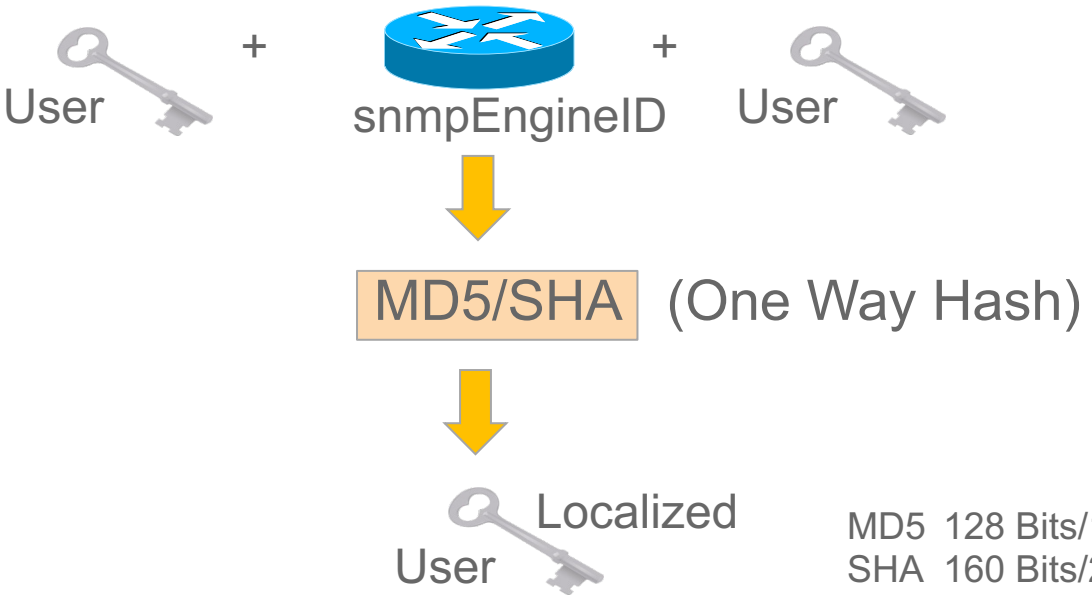
↓

User

MD5 128 Bits/16 Byte Key
SHA 160 Bits/20 Byte Key

Localized Keys

Localized to a Specific Device



MD5 128 Bits/16 Byte Key
SHA 160 Bits/20 Byte Key

Since Every Managed Device's snmpEngineID Is Unique, Every Localized User Key Will Be Unique

Timeliness Verification

- Timeliness is based on
  - snmpEngineBoots – how often the engine has reset
  - snmpEngineTime – the ‘uptime’ of the agent
- The receiving management agent’s snmpEngine determines if incoming message is within 150 second time window.
- Polls outside of window are rejected and a REPORT packet is generated

View-Based Access Control (VACM)

- Restricts users right to view or alter specific MIBs.
- VACM is specified at a per group basis. Each may have different privileges.
  - Who – user/subject of the operation
  - What – object of the SNMP operation (MIB)
  - Where – Context (contextName)
  - Why – type of request – read, write, notify

snmp-server group [*groupname* {**v1** | **v2c** | **v3**{**auth** | **noauth** | **priv**}}] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]

```
Router#show snmp view
*ilmi system - included permanent active
*ilmi atmForumUni - included permanent active
readview internet - included nonvolatile active
v1default iso - included permanent active
v1default internet.6.3.15 - excluded permanent active
v1default internet.6.3.16 - excluded permanent active
v1default internet.6.3.18 - excluded permanent active
v1default ciscoMgmt.394 - excluded permanent active
v1default ciscoMgmt.395 - excluded permanent active
v1default ciscoMgmt.399 - excluded permanent active
v1default ciscoMgmt.400 - excluded permanent active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF7F ieee802dot11 - included volatile active
*tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.FFFFFFFF7F internet - included volatile active
```

snmpUsmMIB
snmpVacmMIB
snmpCommunityMIB
ciscoIpTapMIB
cisco802TapMIB
ciscoTap2MIB
ciscoUserConnectionTapMIB

SNMPv3 Configuration

- SNMPv3 authNoPriv
- Cisco IOS 12.0 example
- Note: The “snmp-server user” config disappears (required in RFC 3414) so a user’s password is not viewable from the config
- To see configured users — “show snmp user”
- EngineID is “Pre-generated”; if engineID is changed all user accounts must be reconfigured
- Store the ‘snmp-server user’ line, securely, off-line for config restore

```
snmp-server engineID local 00000009020000049AC87300
snmp-server group NMCons v3 auth write v1default
snmp-server user CSCOJason NMCons v3 auth md5 password1
```

SNMPv3 Configuration

- SNMPv3 authNoPriv
- Cisco IOS-XR 3.2 example

```
snmp-server engineID local 00:00:00:09:00:00:00:ab:cd:ef:01:23
snmp-server group NMCons v3 auth write v1default
snmp-server user CSCOJason NMCons v3 auth md5 clear password1
[SystemOwner]
```

- Cisco NX-OS 4.0 example

```
snmp-server user CSCOJason network-admin v3 auth md5 password1
```

SNMPv3 Configuration

SNMPv3 authNoPriv Polling Example with Net-SNMP Tools

http://www.net-snmp.org

```
nms% snmpget -v 3 -u CSCOJason -l authNoPriv -a MD5 -A password1
192.168.100.2 system.sysContact.0

system.sysContact.0 = "Cisco NOC / 888-555-1234"
```

NM → Device

SNMPv3 Sniffing

authNoPriv (1 of 4)

- SNMPv3 get request
- This is the first step in SNMPv3 polling (authentication)—note this is not “authPriv” level
- You don’t know the user’s authentication password used and can’t poll the device

```
⊞ User Datagram Protocol, Src Port: 37155 (37155), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    Version: 3
  ⊟ Message Global Header
      Message Global Header Length: 17
      Message ID: 1332247940
      Message Max Size: 65507
    ⊟ Flags: 0x04
        .... .1.. = Reportable: Set
        .... ..0. = Encrypted: Not set
        .... ...0 = Authenticated: Not set
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 16
      Authoritative Engine ID:
      Engine Boots: 0
      Engine Time: 0
      User Name:
      Authentication Parameter:
      Privacy Parameter:
    Context Engine ID:
    Context Name:
    PDU type: GET
    Request Id: 0x64d17993
    Error Status: NO ERROR
    Error Index: 0

0000  00 01 97 37 64 00 08 00  20 a8 8a ba 08 00 45 00   ...7d...  .....E.
0010  00 5c 2e e3 40 00 ff 11  3e 99 ac 12 56 4a 0b 84   .\..@...  >...VJ..
0020  00 34 91 23 00 a1 00 48  e9 aa 30 3e 02 01 03 30   .4.#...H  ..0>...0
0030  11 02 04 4f 68 7d 84 02  03 00 ff e3 04 01 04 02   ...oh}..  ........
0040  01 03 04 10 30 0e 04 00  02 01 00 02 01 00 04 00   ....0...  ........
0050  04 00 04 00 30 14 04 00  04 00 a0 0e 02 04 64 d1   ....0...  ......d.
0060  79 93 02 01 00 02 01 00  30 00                     y.......  0.
```

NM ⟸ Device

SNMPv3 Sniffing

authNoPriv (2 of 4)

- SNMPv3 get <u>response</u> (as a '*<u>report</u>*')
- REPORT packets are a new SNMPv3 concept
- This is done if we are missing authentication information
- You don't know the user's authentication password used and can't poll the device
- We're now doing 'SNMP Engine Discovery' (more on this later)

```
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: 37155 (37155)
⊟ Simple Network Management Protocol
    Version: 3
  ⊟ Message Global Header
      Message Global Header Length: 16
      Message ID: 1332247940
      Message Max Size: 2048
    ⊟ Flags: 0x08
        .... .0.. = Reportable: Not set
        .... ..0. = Encrypted: Not set
        .... ...0 = Authenticated: Not set
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 30
      Authoritative Engine ID: 0000000902000001960F12C0
      Engine Boots: 2
      Engine Time: 1656215
      User Name:
      Authentication Parameter:
      Privacy Parameter:
    Context Engine ID: 0000000902000001960F12C0
    Context Name:
    PDU type: REPORT
    Request Id: 0x64d17993
    Error Status: NO ERROR
    Error Index: 0
    Object identifier 1: 1.3.6.1.6.3.15.1.1.4.0 (SNMP-USER-BASED-SM-MIB::usmStatsUnknownEngineIDs.0)
    Value: Counter32: 5

0000  08 00 20 a8 8a ba 00 01  97 37 64 00 08 00 45 00   .. ..... .7d...E.
0010  00 86 18 fd 00 00 fe 11  95 55 0b 84 00 34 ac 12   ........ .U...4..
0020  56 4a 00 a1 91 23 00 72  63 27 30 68 02 01 03 30   VJ...#.r c'0h...0
0030  10 02 04 4f 68 7d 84 02  02 08 00 04 01 08 02 01   ...oh}.. ........
0040  03 04 1e 30 1c 04 0c 00  00 00 09 02 00 00 01 96   ...0.... ........
0050  0f 12 c0 02 01 02 02 03  19 45 97 04 00 04 00 04   ........ .E......
0060  00 30 31 04 0c 00 00 00  09 02 00 00 01 96 0f 12   .01..... ........
0070  c0 04 00 a8 1f 02 04 64  d1 79 93 02 01 00 02 01   .......d .y......
0080  00 30 11 30 0f 06 0a 2b  06 01 06 03 0f 01 01 04   .0.0...+ ........
0090  00 41 01 05                                        .A..
```

NM → Device

SNMPv3 Sniffing

authNoPriv (3 of 4)

- SNMPv3 get request (now the actual request)
- This is the third step in SNMPv3 polling for scenarios missing some authentication
- **But** it can be the **first** step for scenarios where all authentication information is known up-front
- You can see the Requesting user name and the OID
- You don't know the password used and can't poll the device

```
⊞ User Datagram Protocol, Src Port: 37155 (37155), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    Version: 3
  ⊟ Message Global Header
      Message Global Header Length: 17
      Message ID: 1332247941
      Message Max Size: 65507
    ⊟ Flags: 0x05
        .... .1.. = Reportable: Set
        .... ..0. = Encrypted: Not set
        .... ...1 = Authenticated: Set
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 51
      Authoritative Engine ID: 0000000902000001960F12C0
      Engine Boots: 2
      Engine Time: 1656215
      User Name: CSCOJason
      Authentication Parameter: 746B1B52E514548FDD434E7B
      Privacy Parameter:
    Context Engine ID: 0000000902000001960F12C0
    Context Name:
    PDU type: GET
    Request Id: 0x64d17994
    Error Status: NO ERROR
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.4.0 (SNMPv2-MIB::sysContact.0)
    Value: NULL
```

```
0000  00 01 97 37 64 00 08 00  20 a8 8a ba 08 00 45 00   ...7d... .....E.
0010  00 99 2e e4 40 00 ff 11  3e 5b ac 12 56 4a 0b 84   ....@... >[..VJ..
0020  00 34 91 23 00 a1 00 85  3d 2a 30 7b 02 01 03 30   .4.#.... =*0{...0
0030  11 02 04 4f 68 7d 85 02  03 00 ff e3 04 01 05 02   ...Oh}.. ........
0040  01 03 04 33 30 31 04 0c  00 00 00 09 02 00 00 01   ...301.. ........
0050  96 0f 12 c0 02 01 02 02  03 19 45 97 04 09 43 53   ........ ..E...CS
0060  43 4f 4a 61 73 6f 6e 04  0c 74 6b 1b 52 e5 14 54   COJason. .tk.R..T
0070  8f dd 43 4e 7b 04 00 30  2e 04 0c 00 00 00 09 02   ..CN{..0 ........
0080  00 00 01 96 0f 12 c0 04  00 a0 1c 02 04 64 d1 79   ........ .....d.y
0090  94 02 01 00 02 01 00 30  0e 30 0c 06 08 2b 06 01   .......0 .0...+..
00a0  02 01 01 04 00 05 00                               .......
```

NM ⟸ Device

SNMPv3 Sniffing

authNoPriv (4 of 4)

- SNMPv3 get response
- This is the fourth Step in SNMPv3 Polling (data response)
- You can see the requesting user name, the OID, and the value
- You don't know the user's authentication password and can't poll the device

```
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: 37155 (37155)
⊟ Simple Network Management Protocol
    Version: 3
  ⊟ Message Global Header
      Message Global Header Length: 16
      Message ID: 1332247941
      Message Max Size: 2048
    ⊟ Flags: 0x01
        .... .0.. = Reportable: Not set
        .... ..0. = Encrypted: Not set
        .... ...1 = Authenticated: Set
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 51
      Authoritative Engine ID: 0000000902000001960F12C0
      Engine Boots: 2
      Engine Time: [illegible]
      User Name: CSCOJason
      Authentication Parameter: 55769D2E0713BE94DBDC3855
      Privacy Parameter:
    Context Engine ID: 0000000902000001960F12C0
    Context Name:
    PDU type: RESPONSE
    Request Id: 0x64d17994
    Error Status: NO ERROR
    Error Index: 0
    Object identifier 1: 1.3.6.1.2.1.1.4.0 (SNMPv2-MIB::sysContact.0)
    Value: STRING: "Cisco NOC / 888-555-1234"
```

```
0010  00 b3 18 fe 00 00 fe 11  95 27 0b 84 00 34 ac 12   ........ .'....4..
0020  56 4a 00 a1 91 23 00 9f  86 26 30 81 94 02 01 03   VJ...#.. .&0.....
0030  30 10 02 04 4f 68 7d 85  02 02 08 00 04 01 01 02   0...oh}. ........
0040  01 03 04 33 30 31 04 0c  00 00 00 09 02 00 00 01   ...301.. ........
0050  96 0f 12 c0 02 01 02 02  03 19 45 97 04 09 43 53   ........ ..E...CS
0060  43 4f 4a 61 73 6f 6e 04  0c 55 76 9d 2e 07 13 be   COJason. .Uv.....
0070  94 db dc 38 55 04 00 30  48 04 0c 00 00 00 09 02   ...8U..0 H.......
0080  00 00 01 96 0f 12 c0 04  00 a2 36 02 04 64 d1 79   ........ ..6..d.y
0090  94 02 01 00 02 01 00 30  28 30 26 06 08 2b 06 01   .......0 (0&..+..
00a0  02 01 01 04 00 04 1a 22  43 69 73 63 6f 20 4e 4f   ........ "Cisco NO
00b0  43 20 2f 20 38 38 38 2d  35 35 35 2d 31 32 33 34   C / 888- 555-1234
00c0  22                                                 "
```

SNMPv3 Configuration

authPriv

- Cisco IOS 12.0 example – requires K8/K9 image, like SSH
- Note: The “snmp-server user” config disappears (required in RFC 3414) so a user’s password is not viewable from the config
- To see configured users — “show snmp user”
- EngineID is “Pre-generated”; if engineID is changed all user accounts must be reconfigured
- Store the ‘snmp-server user’ line, securely, off-line for config restore

```
snmp-server engineID local 00000009020000049AC87300
snmp-server group NMCons v3 priv write v1default
snmp-server user CSCOJason NMCons v3 auth md5 password1 priv des56
password2
```

SNMPv3 Configuration

authPriv

- Cisco IOS-XR 3.2 example

```
snmp-server engineID local 00:00:00:09:00:00:00:ab:cd:ef:01:23
snmp-server group NMCons v3 priv write v1default
snmp-server user CSCOJason NMCons v3 auth md5 clear password1
 priv des56 clear password2 [SystemOwner]
```

- Cisco NX-OS 4.0 example

```
snmp-server user CSCOJason network-admin v3 auth md5 password1
 priv password2
```

SNMPv3 Configuration

Enhanced Encryption Capabilities

Since IOS 12.4(2)T and 12.2(33)SRE and IOS-XR 3.9 the options for ‘priv’ can be

3des	Use 168-Bit 3DES Algorithm for Encryption
aes {128 | 192 | 256}	Use AES Algorithm for Encryption
des	Use 56-Bit DES Algorithm for Encryption

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/snmpv3ae.html

```
snmp-server engineID local 00000009020000049AC87300
snmp-server group NMCons v3 auth write v1default
snmp-server user CSCOJason NMCons v3 auth md5 password1 priv aes 256
password2
```

NX-OS supports up to AES-128

NM → Device

SNMPv3 authPriv Sniffing

authPriv (1 of 4)

- NMS to router
- SNMPv3 get request
- With DES encrypted PDU
- You tell me - What was I polling !?!?

```
⊞ User Datagram Protocol, Src Port: 37313 (37313), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    Version: 3
  ⊟ Message Global Header
      Message Global Header Length: 17
      Message ID: 2019475258
      Message Max Size: 65507
    ⊟ Flags: 0x04
        .... .1.. = Reportable: Set
        .... ..0. = Encrypted: Not set
        .... ...0 = Authenticated: Not set
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 16
      Authoritative Engine ID:
      Engine Boots: 0
      Engine Time: 0
      User Name:
      Authentication Parameter:
      Privacy Parameter:
    Context Engine ID:
    Context Name:
    PDU type: GET
    Request Id: 0x5472c1a6
    Error Status: NO ERROR
    Error Index: 0
```

```
0000  00 01 97 37 64 00 08 00  20 a8 8a ba 08 00 45 00   ...7d...  .....E.
0010  00 5c a7 a1 40 00 ff 11  c5 da ac 12 56 4a 0b 84   .\..@...  ....VJ..
0020  00 34 91 c1 00 a1 00 48  04 ee 30 3e 02 01 03 30   .4.....H  ..0>...0
0030  11 02 04 78 5e bf 3a 02  03 00 ff e3 04 01 04 02   ...x^.:.  ........
0040  01 03 04 10 30 0e 04 00  02 01 00 02 01 00 04 00   ....0...  ........
0050  04 00 04 00 30 14 04 00  04 00 a0 0e 02 04 54 72   ....0...  ......Tr
0060  c1 a6 02 01 00 02 01 00  30 00                     ........  0.
```

Cisco Live!

NM ⟸ Device

SNMPv3 authPriv Sniffing

authPriv (2 of 4)

- Router to NMS
- SNMPv3 get/report response
- This one is telling me the total number of packets received by the SNMP engine dropped because they referenced an snmpEngineID that was not known to the SNMP engine

```
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: 37313 (37313)
⊟ Simple Network Management Protocol
    Version: 3
  ⊟ Message Global Header
      Message Global Header Length: 16
      Message ID: 2019475258
      Message Max Size: 2048
    ⊟ Flags: 0x08
        .... .0.. = Reportable: Not set
        .... ..0. = Encrypted: Not set
        .... ...0 = Authenticated: Not set
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 30
      Authoritative Engine ID: 0000000902000001960F12C0
      Engine Boots: 2
      Engine Time: 1659676
      User Name:
      Authentication Parameter:
      Privacy Parameter:
    Context Engine ID: 0000000902000001960F12C0
    Context Name:
    PDU type: REPORT
    Request Id: 0x5472c1a6
    Error Status: NO ERROR
    Error Index: 0
    Object identifier 1: 1.3.6.1.6.3.15.1.1.4.0 (SNMP-USER-BASED-SM-MIB::usmStatsUnknownEngineIDs.0)
    Value: Counter32: 9

0000  08 00 20 a8 8a ba 00 01  97 37 64 00 08 00 45 00   .. ..... .7d...E.
0010  00 86 19 05 00 00 fe 11  95 4d 0b 84 00 34 ac 12   ........ .M...4..
0020  56 4a 00 a1 91 c1 00 72  7c d5 30 68 02 01 03 30   VJ.....r |.0h...0
0030  10 02 04 78 5e bf 3a 02  02 08 00 04 01 08 02 01   ...x^.:. ........
0040  03 04 1e 30 1c 04 0c 00  00 00 09 02 00 00 01 96   ...0.... ........
0050  0f 12 c0 02 01 02 02 03  19 53 1c 04 00 04 00 04   ........ .S......
0060  00 30 31 04 0c 00 00 00  09 02 00 00 01 96 0f 12   .01..... ........
0070  c0 04 00 a8 1f 02 04 54  72 c1 a6 02 01 00 02 01   .......T r.......
0080  00 30 11 30 0f 06 0a 2b  06 01 06 03 0f 01 01 04   .0.0...+ ........
0090  00 41 01 09                                        .A..
```

Cisco live!

NM → Device

SNMPv3 authPriv Sniffing

authPriv (3 of 4)

- NMS to router
- SNMPv3 get request with all necessary data
- You can tell what **user** polled, but still no clue as to **what** object was polled!

```
⊞ User Datagram Protocol, Src Port: 37313 (37313), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    Version: 3
  ⊟ Message Global Header
      Message Global Header Length: 17
      Message ID: 2019475259
      Message Max Size: 65507
    ⊟ Flags: 0x07
        .... .1.. = Reportable: Set
        .... ..1. = Encrypted: Set
        .... ...1 = Authenticated: Set
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 59
      Authoritative Engine ID: 0000000902000001960F12C0
      Engine Boots: 2
      Engine Time: 1659676
      User Name: CSCOJason
      Authentication Parameter: 1F8638FE30F24C50F3066684
      Privacy Parameter: 0000000107036F6D
    Encrypted PDU (50 bytes)

0000  00 01 97 37 64 00 08 00  20 a8 8a ba 08 00 45 00   ...7d...  .....E.
0010  00 a4 a7 a2 40 00 ff 11  c5 91 ac 12 56 4a 0b 84   ....@...  ....VJ..
0020  00 34 91 c1 00 a1 00 90  6c 68 30 81 85 02 01 03   .4......  lh0.....
0030  30 11 02 04 78 5e bf 3b  02 03 00 ff e3 04 01 07   0...x^.;  ........
0040  02 01 03 04 3b 30 39 04  0c 00 00 00 09 02 00 00   ....;09.  ........
0050  01 96 0f 12 c0 02 01 02  02 03 19 53 1c 04 09 43   ........  ...S...C
0060  53 43 4f 4a 61 73 6f 6e  04 0c 1f 86 38 fe 30 f2   SCOJason  ....8.0.
0070  4c 50 f3 06 66 84 04 08  00 00 00 01 07 03 6f 6d   LP..f...  ......om
0080  04 30 9c 94 f9 e7 e6 a3  4f 13 61 2f 76 59 7d ab   .0......  O.a/vY}.
0090  88 6e a9 fa 29 27 62 a3  a0 f3 43 45 53 ff 1f d1   .n..)'b.  ..CES...
00a0  8c 37 d4 55 ed 59 d7 c3  5e fa 52 29 f7 95 9d 90   .7.U.Y..  ^.R)....
00b0  81 13                                              ..
```

Cisco live!

NM ⟸ Device

SNMPv3 authPriv Sniffing

authPriv (4 of 4)

- Router to NMS
- SNMPv3 get response
- Here's the final reply, but no clue as to what was polled or what the return value was!

```
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: 37313 (37313)
⊟ Simple Network Management Protocol
    Version: 3
  ⊟ Message Global Header
      Message Global Header Length: 16
      Message ID: 2019475259
      Message Max Size: 2048
    ⊟ Flags: 0x03
        .... .0.. = Reportable: Not set
        .... ..1. = Encrypted: Set
        .... ...1 = Authenticated: Set
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 59
      Authoritative Engine ID: 0000000902000001960F12C0
      Engine Boots: 2
      Engine Time: 1659676
      User Name: CSCOJason
      Authentication Parameter: 5CCC7F958A56D8A391824EB7
      Privacy Parameter: 000000026B43A803
    Encrypted PDU (58 bytes)

0000  08 00 20 a8 8a ba 00 01  97 37 64 00 08 00 45 00   .. ..... .7d...E.
0010  00 ab 19 06 00 00 fe 11  95 27 0b 84 00 34 ac 12   ........ .'...4..
0020  56 4a 00 a1 91 c1 00 97  a7 ef 30 81 8c 02 01 03   VJ...... ..0.....
0030  30 10 02 04 78 5e bf 3b  02 02 08 00 04 01 03 02   0...x^.; ........
0040  01 03 04 3b 30 39 04 0c  00 00 00 09 02 00 00 01   ...;09.. ........
0050  96 0f 12 c0 02 01 02 02  03 19 53 1c 04 09 43 53   ........ ..S...CS
0060  43 4f 4a 61 73 6f 6e 04  0c 5c cc 7f 95 8a 56 d8   COJason. .\.▯..V.
0070  a3 91 82 4e b7 04 08 00  00 00 02 6b 43 a8 03 04   ...N.... ...kC..▯
0080  38 be ad ad 32 0b 74 dd  5c ef 57 49 ab b7 07 55   8...2.t. \.WI...U
0090  f4 ac 0a 34 e2 ca 1a b2  2b c5 39 ca 19 63 e1 c0   ...4.... +.9..c..
00a0  78 74 a9 1d ac bd 42 e6  a9 ce 4d 4a f9 37 86 aa   xt....B. ..MJ.7..
00b0  3d 14 d4 11 a1 1f a5 ab  64                        =....... d
```

Cisco live!

SNMPv3 authPriv Polling Results

- Using Net-SNMP tools, here's what I polled and the returned value
- Note: I specified an MD5 password for authentication AND a DES (-X option) password for encryption

```
nms% snmpget -v 3 -u CSCOJason -l authPriv -a MD5 -A password1 -X
password2 192.168.100.2 sysUpTime.0

system.sysUpTime.sysUpTimeInstance = Timeticks: (165967680) 19 days,
5:01:16.80
```

SNMPv3 snmpEngineID Discovery

Very Important Consideration!

- Remember the report packets?
- SNMPv3 requests need to be authenticated;
  snmpEngineID must be explicitly defined along with snmpEngineBoot and snmpEngineTime
- The device being polled has the “Authoritative Engine ID”
- If all components aren’t correct (and within 150s for snmpEngineTime) you will incur extra packets to get the correct information
- Note the following slides

NM → Device

Example 1:

- First Packet---No Engine Info Provided

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.86.74	172.18.86.111	SNMP	GET
2	0.021764	172.18.86.111	172.18.86.74	SNMP	REPORT SNMP-USER-BASED-SM-MIB::usmStatsUnknownEngineIDs.0
3	0.023296	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
4	0.060090	172.18.86.111	172.18.86.74	SNMP	Encrypted PDU

```
▷ Frame 1 (106 bytes on wire, 106 bytes captured)
▷ Ethernet II, Src: 08:00:20:a8:8a:ba, Dst: 00:10:36:40:00:01
▷ Internet Protocol, Src Addr: 172.18.86.74 (172.18.86.74), Dst Addr: 172.18.86.111 (172.18.86.111)
▷ User Datagram Protocol, Src Port: 51208 (51208), Dst Port: snmp (161)
▽ Simple Network Management Protocol
    Version: 3 (3)
  ▷ Message Global Header
  ▽ Message Security Parameters
      Message Security Parameters Length: 16
      Authoritative Engine ID:
      Engine Boots: 0
      Engine Time: 0
      User Name:
      Authentication Parameter:
      Privacy Parameter:
    Context Engine ID:
    Context Name:
    PDU type: GET (0)
    Request Id: 0x30fcbc70
    Error Status: NO ERROR (0)
    Error Index: 0
```

```
0000  00 10 36 40 00 01 08 00  20 a8 8a ba 08 00 45 00   ..6@.... .....E.
0010  00 5c 0c 79 40 00 ff 11  6a 39 ac 12 56 4a ac 12   .\.y@... j9..VJ..
0020  56 6f c8 08 00 a1 00 48  13 24 30 3e 02 01 03 30   Vo.....H .$0>...0
0030  11 02 04 70 bf 2b c7 02  03 00 ff e3 04 01 04 02   ...p.+.. ........
0040  01 03 04 10 30 0e 04 00  02 01 00 02 01 00 04 00   ....0... ........
0050  04 00 04 00 30 14 04 00  04 00 a0 0e 02 04 30 fc   ....0... ......0.
0060  bc 70 02 01 00 02 01 00  30 00                     .p...... 0.
```

Second Packet—Report from Device for Lack of Engine Information

snmpv3-1-engineiddisc - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.86.74	172.18.86.111	SNMP	GET
2	0.021764	172.18.86.111	172.18.86.74	SNMP	REPORT SNMP-USER-BASED-SM-MIB::usmStatsUnknownEngineIDs.0
3	0.023296	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
4	0.060090	172.18.86.111	172.18.86.74	SNMP	Encrypted PDU

```
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: 51208 (51208)
⊟ Simple Network Management Protocol
    Version: 3 (3)
  ⊟ Message Global Header
      Message Global Header Length: 16
      Message ID: 1891576775
      Message Max Size: 1500
    ⊞ Flags: 0x00
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 31
      Authoritative Engine ID: 80000009030000D0BAF46480
      Engine Boots: 1
      Engine Time: 11364837
      User Name:
      Authentication Parameter:
      Privacy Parameter:
    Context Engine ID: 80000009030000D0BAF46480
    Context Name:
    PDU type: REPORT (8)
    Request Id: 0x30fcbc70
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.6.3.15.1.1.4.0 (SNMP-USER-BASED-SM-MIB::usmStatsUnknownEngineIDs.0)
    Value: Counter32: 2
```

```
0000  08 00 20 a8 8a ba 00 10  36 40 00 01 08 00 45 00   .. ..... 6@....E.
0010  00 87 3f 3b 00 00 ff 11  77 4c ac 12 56 6f ac 12   ..?;.... wL..Vo..
0020  56 4a 00 a1 c8 08 00 73  19 5e 30 69 02 01 03 30   VJ.....s .^0i...0
0030  10 02 04 70 bf 2b c7 02  02 05 dc 04 01 00 02 01   ...p.+.. ........
0040  03 04 1f 30 1d 04 0c 80  00 00 09 03 00 00 d0 ba   ...0.... ........
0050  f4 64 80 02 01 01 02 04  00 ad 69 e5 04 00 04 00   .d...... ..i.....
0060  04 00 30 31 04 0c 80 00  00 09 03 00 00 d0 ba f4   ..01.... ........
0070  64 80 04 00 a8 1f 02 04  30 fc bc 70 02 01 00 02   d....... 0..p....
0080  01 00 30 11 30 0f 06 0a  2b 06 01 06 03 0f 01 01   ..0.0... +.......
0090  04 00 41 01 02                                     ..A..
```

Filter: Reset Apply File: snmpv3-1-engineiddisc

Third Packet—Poller Tries Again, now with All Required Information

snmpv3-1-engineiddisc - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.86.74	172.18.86.111	SNMP	GET
2	0.021764	172.18.86.111	172.18.86.74	SNMP	REPORT SNMP-USER-BASED-SM-MIB::usmStatsUnknownEngineIDs.0
3	0.023296	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
4	0.060090	172.18.86.111	172.18.86.74	SNMP	Encrypted PDU

```
⊞ Frame 3 (179 bytes on wire, 179 bytes captured)
⊞ Ethernet II, Src: 08:00:20:a8:8a:ba, Dst: 00:10:36:40:00:01
⊞ Internet Protocol, Src Addr: 172.18.86.74 (172.18.86.74), Dst Addr: 172.18.86.111 (172.18.86.111)
⊞ User Datagram Protocol, Src Port: 51208 (51208), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    Version: 3 (3)
  ⊟ Message Global Header
      Message Global Header Length: 17
      Message ID: 1891576776
      Message Max Size: 65507
    ⊞ Flags: 0x07
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 60
      Authoritative Engine ID: 80000009030000D0BAF46480
      Engine Boots: 1
      Engine Time: 11364837
      User Name: CSCOJason
      Authentication Parameter: 0E2F9653495188DEE51A5228
      Privacy Parameter: 00000001A5C2B995
  Encrypted PDU (50 bytes)
```

```
0000  00 10 36 40 00 01 08 00  20 a8 8a ba 08 00 45 00   ..6@.... .....E.
0010  00 a5 0c 7a 40 00 ff 11  69 ef ac 12 56 4a ac 12   ...z@... i...VJ..
0020  56 6f c8 08 00 a1 00 91  1b 2b 30 81 86 02 01 03   Vo...... .+0.....
0030  30 11 02 04 70 bf 2b c8  02 03 00 ff e3 04 01 07   0...p.+. ........
0040  02 01 03 04 3c 30 3a 04  0c 80 00 00 09 03 00 00   ....<0:. ........
0050  d0 ba f4 64 80 02 01 01  02 04 00 ad 69 e5 04 09   ...d.... ....i...
0060  43 53 43 4f 4a 61 73 6f  6e 04 0c 0e 2f 96 53 49   CSCOJaso n.../.SI
0070  51 88 de e5 1a 52 28 04  08 00 00 00 01 a5 c2 b9   Q....R(. ........
0080  95 04 30 5d 49 c2 81 73  01 ed 78 bd ec 81 04 fa   ..0]I..s ..x.....
0090  37 ef c3 bf ae 03 eb ba  1e 4c cc 64 db d8 94 27   7....... .L.d...'
00a0  6f 22 2a 21 90 5e 16 9c  52 95 d6 41 ec 25 75 21   o"*!.^.. R..A.%u!
00b0  89 a5 a0                                           ...
```

Filter: / Reset Apply File: snmpv3-1-engineiddisc

Fourth Packet—All Information Good, Device Gives Final Response

snmpv3-1-engineiddisc - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.86.74	172.18.86.111	SNMP	GET
2	0.021764	172.18.86.111	172.18.86.74	SNMP	REPORT SNMP-USER-BASED-SM-MIB::usmStatsUnknownEngineIDs.0
3	0.023296	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
4	0.060090	172.18.86.111	172.18.86.74	SNMP	Encrypted PDU

```
⊟ Simple Network Management Protocol
    Version: 3 (3)
  ⊟ Message Global Header
      Message Global Header Length: 16
      Message ID: 1891576776
      Message Max Size: 1500
    ⊞ Flags: 0x03
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 60
      Authoritative Engine ID: 800000090300000D0BAF46480
      Engine Boots: 1
      Engine Time: 11364837
      User Name: CSCOJason
      Authentication Parameter: B0D9C86B00915A0E61DD5FFE
      Privacy Parameter: 000000014ECE71E1
    Encrypted PDU (276 bytes)
```

```
0000  08 00 20 a8 8a ba 00 10  36 40 00 01 08 00 45 00   .. ..... 6@....E.
0010  01 87 3f 3c 00 00 ff 11  76 4b ac 12 56 6f ac 12   ..?<.... vK..Vo..
0020  56 4a 00 a1 c8 08 01 73  45 22 30 82 01 67 02 01   VJ.....s E"0..g..
0030  03 30 10 02 04 70 bf 2b  c8 02 02 05 dc 04 01 03   .0...p.+ ........
0040  02 01 03 04 3c 30 3a 04  0c 80 00 00 09 03 00 00   ....<0:. ........
0050  d0 ba f4 64 80 02 01 01  02 04 00 ad 69 e5 04 09   ...d.... ....i...
0060  43 53 43 4f 4a 61 73 6f  6e 04 0c b0 d9 c8 6b 00   CSCOJaso n.....k.
0070  91 5a 0e 61 dd 5f fe 04  08 00 00 00 01 4e ce 71   .Z.a._.. .....N.q
0080  e1 04 82 01 10 07 9d b0  9c 97 35 dd 15 86 ae 5f   ........ ..5....
0090  1b e8 d2 6c 79 95 fb bc  82 5e eb 84 36 61 a4 e5   ...ly... .^..6a..
00a0  61 14 a1 ea 7d cd a3 b1  c3 9a 2c b6 0a f4 38 d0   a...}... ......8.
00b0  3f ff 74 37 10 64 c7 c7  e7 85 c3 90 03 be 55 b4   ?.t7.d.. ......U.
00c0  92 9b 83 79 82 ca f7 f6  5b d4 ae 15 68 cb 12 12   ...y.... [...h...
00d0  4e ee 7f 2f d2 7e 92 60  8f b7 fe fd 06 c7 e1 3e   N./.~.` .......>
00e0  27 70 ee 71 5a ab 12 0c  bc b2 30 af 48 df d9 74   'p.qZ... ..0.H..t
00f0  76 b1 35 d9 e7 26 e4 cf  50 eb 49 7c 57 4f c4 a5   v.5..&.. P.I|WO..
0100  ea d6 65 f3 2d 7c 8d 00  aa 0f 17 ff 53 92 89 c5   ..e.-|.. ....S...
0110  0b d5 d5 bf ec b1 e9 fa  27 58 07 27 52 12 d8 a8   ........ 'X.'R...
```

NM → Device

Example 2:

Polling with Correct snmpEngineID and snmpEngineBoot, But snmpEngineTime Is Off

snmpv3-3-engineid-engineboot - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
2	0.018335	172.18.86.111	172.18.86.74	SNMP	REPORT SNMP-USER-BASED-SM-MIB::usmStatsNotInTimewindows.0
3	0.019144	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
4	0.056897	172.18.86.111	172.18.86.74	SNMP	Encrypted PDU

```
⊞ Frame 1 (176 bytes on wire, 176 bytes captured)
⊞ Ethernet II, Src: 08:00:20:a8:8a:ba, Dst: 00:10:36:40:00:01
⊞ Internet Protocol, Src Addr: 172.18.86.74 (172.18.86.74), Dst Addr: 172.18.86.111 (172.18.86.111)
⊞ User Datagram Protocol, Src Port: 51336 (51336), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    Version: 3 (3)
  ⊟ Message Global Header
      Message Global Header Length: 17
      Message ID: 65828980
      Message Max Size: 65507
    ⊞ Flags: 0x07
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 57
      Authoritative Engine ID: 8000000903000D0BAF46480
      Engine Boots: 1
      Engine Time: 1
      User Name: CSCOJason
      Authentication Parameter: F9087B7CB094F728170A1630
      Privacy Parameter: 0000000180986782
    Encrypted PDU (50 bytes)
```

```
0000  00 10 36 40 00 01 08 00  20 a8 8a ba 08 00 45 00   ..6@.... .....E.
0010  00 a2 0c 91 40 00 ff 11  69 db ac 12 56 4a ac 12   ....@... i...VJ..
0020  56 6f c8 88 00 a1 00 8e  88 fb 30 81 83 02 01 03   Vo...... ..0.....
0030  30 11 02 04 03 ec 78 74  02 03 00 ff e3 04 01 07   0.....xt ........
0040  02 01 03 04 39 30 37 04  0c 80 00 00 09 03 00 00   ....907. ........
0050  d0 ba f4 64 80 02 01 01  02 01 01 04 09 43 53 43   ...d.... .....CSC
0060  4f 4a 61 73 6f 6e 04 0c  f9 08 7b 7c b0 94 f7 28   OJason.. ..{|...(
0070  17 0a 16 30 04 08 00 00  00 01 b0 98 67 82 04 30   ...0.... ....g..0
0080  13 47 f0 85 e8 2d d7 26  c2 91 8a 9a b4 ec 8d 55   .G...-.& .......U
0090  16 12 58 ff b2 3d a7 6b  59 e2 8a 66 10 09 18 d8   ..X..=.k Y..f....
00a0  76 6d 61 2d 91 c0 0b 2d  d5 2d 21 67 6e 0e 9d ae   vma-...- .-!gn...
```

Filter: Reset Apply File: snmpv3-3-engineid-engineboot

Device Reports Back Out of Time Sync, Provides Correct Information (Last Two Packets Like Example 1)

NM ⟵ Device

snmpv3-3-engineid-engineboot - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
2	0.018335	172.18.86.111	172.18.86.74	SNMP	REPORT SNMP-USER-BASED-SM-MIB::usmStatsNotInTimewindows.0
3	0.019144	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
4	0.056897	172.18.86.111	172.18.86.74	SNMP	Encrypted PDU

```
⊞ User Datagram Protocol, Src Port: snmp (161), D
⊟ Simple Network Management Protocol
    Version: 3 (3)
  ⊟ Message Global Header
      Message Global Header Length: 16
      Message ID: 65828980
      Message Max Size: 1500
    ⊞ Flags: 0x01
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 52
      Authoritative Engine ID: 800000090300000D0BAF46480
      Engine Boots: 1
      Engine Time: 11366016
      User Name: CSCOJason
      Authentication Parameter: B26203522DCF180D6F36EBB1
      Privacy Parameter:
    Context Engine ID: 800000090300000D0BAF46480
    Context Name:
    PDU type: REPORT (8)
    Request Id: 0x7fffffff
    Error Status: NO ERROR (0)
    Error Index: 0
    Object identifier 1: 1.3.6.1.6.3.15.1.1.2.0 (SNMP-USER-BASED-SM-MIB::usmStatsNotInTimewindows.0)
    Value: Counter32: 2
```

```
0000  08 00 20 a8 8a ba 00 10  36 40 00 01 08 00 45 00   .. ..... 6@....E.
0010  00 9c 40 10 00 00 ff 11  76 62 ac 12 56 6f ac 12   ..@..... vb..Vo..
0020  56 4a 00 a1 c8 88 00 88  39 cb 30 7e 02 01 03 30   VJ...... 9.0~...0
0030  10 02 04 03 ec 78 74 02  02 05 dc 04 01 01 02 01   .....xt. ........
0040  03 04 34 30 32 04 0c 80  00 00 09 03 00 00 d0 ba   ..402... ........
0050  f4 64 80 02 01 01 02 04  00 ad 6e 80 04 09 43 53   .d...... ..n...CS
0060  43 4f 4a 61 73 6f 6e 04  0c b2 62 03 52 2d cf 18   COJason. ..b.R-..
0070  0d 6f 36 eb b1 04 00 30  31 04 0c 80 00 00 09 03   .o6....0 1.......
0080  00 00 d0 ba f4 64 80 04  00 a8 1f 02 04 7f ff ff   .....d.. .....¤..
0090  ff 02 01 00 02 01 00 30  11 30 0f 06 0a 2b 06 01   .......0 .0...+..
00a0  06 03 0f 01 01 02 00 41  01 02                     .......A ..
```

Filter: Reset Apply File: snmpv3-3-engineid-engineboot

We Must Be Within 150 Seconds of Time Sync
This Protects Against 'Replay' Attacks

NM → Device

Example 3:

Polling with All the Required Information First Time

snmpv3-4-alldiscinfo - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
2	0.026425	172.18.86.111	172.18.86.74	SNMP	Encrypted PDU

```
⊞ Frame 1 (179 bytes on wire, 179 bytes captured)
⊞ Ethernet II, Src: 08:00:20:a8:8a:ba, Dst: 00:10:36:40:00:01
⊞ Internet Protocol, Src Addr: 172.18.86.74 (172.18.86.74), Dst Addr: 172.18.86.111 (172.18.86.111)
⊞ User Datagram Protocol, Src Port: 51333 (51333), Dst Port: snmp (161)
⊟ Simple Network Management Protocol
    Version: 3 (3)
  ⊟ Message Global Header
      Message Global Header Length: 17
      Message ID: 1809289963
      Message Max Size: 65507
    ⊞ Flags: 0x07
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 60
      Authoritative Engine ID: 800000090300000D0BAF46480
      Engine Boots: 1
      Engine Time: 11365910
      User Name: CSCOJason
      Authentication Parameter: D18F1BDC2F5F41F68D87105C
      Privacy Parameter: 0000000145DEA0A1
    Encrypted PDU (50 bytes)
```

```
0000  00 10 36 40 00 01 08 00  20 a8 8a ba 08 00 45 00   ..6@.... .....E.
0010  00 a5 0c 90 40 00 ff 11  69 d9 ac 12 56 4a ac 12   ....@... i...VJ..
0020  56 6f c8 85 00 a1 00 91  8d a0 30 81 86 02 01 03   Vo...... ..0.....
0030  30 11 02 04 6b d7 92 eb  02 03 00 ff e3 04 01 07   0...k... ........
0040  02 01 03 04 3c 30 3a 04  0c 80 00 00 09 03 00 00   ....<0:. ........
0050  d0 ba f4 64 80 02 01 01  02 04 00 ad 6e 16 04 09   ...d.... ....n...
0060  43 53 43 4f 4a 61 73 6f  6e 04 0c d1 8f 1b dc 2f   CSCOJaso n...../
0070  5f 41 f6 8d 87 10 5c 04  08 00 00 00 01 45 de a0   _A....\. .....E..
0080  a1 04 30 b6 b4 7c 9e a5  c0 05 6c 51 b0 d9 a6 ac   ..0..|.. ..lQ....
0090  89 13 73 59 a5 35 85 5c  f3 32 a0 d1 b8 93 bc 03   ..sY.5.\ .2......
```

Device Responds Back—
Only Two Packets Required!

NM ⟵ Device

snmpv3-4-alldiscinfo - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000000	172.18.86.74	172.18.86.111	SNMP	Encrypted PDU
2	0.026425	172.18.86.111	172.18.86.74	SNMP	Encrypted PDU

```
⊞ Frame 2 (405 bytes on wire, 405 bytes captured)
⊞ Ethernet II, Src: 00:10:36:40:00:01, Dst: 08:00:20:a8:8a:ba
⊞ Internet Protocol, Src Addr: 172.18.86.111 (172.18.86.111), Dst Addr: 172.18.86.74 (172.18.86.74)
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: 51333 (51333)
⊟ Simple Network Management Protocol
    Version: 3 (3)
  ⊟ Message Global Header
      Message Global Header Length: 16
      Message ID: 1809289963
      Message Max Size: 1500
    ⊞ Flags: 0x03
      Message Security Model: USM
  ⊟ Message Security Parameters
      Message Security Parameters Length: 60
      Authoritative Engine ID: 800000090300000D0BAF46480
      Engine Boots: 1
      Engine Time: 11365948
      User Name: CSCOJason
      Authentication Parameter: 4BA2B36875137F7409214122
      Privacy Parameter: 000000014ECE71EC
    Encrypted PDU (276 bytes)
```

```
0000  08 00 20 a8 8a ba 00 10  36 40 00 01 08 00 45 00   .. ..... 6@....E.
0010  01 87 40 0f 00 00 ff 11  75 78 ac 12 56 6f ac 12   ..@..... ux..Vo..
0020  56 4a 00 a1 c8 85 01 73  24 13 30 82 01 67 02 01   VJ.....s $.0..g..
0030  03 30 10 02 04 6b d7 92  eb 02 02 05 dc 04 01 03   .0...k.. ........
0040  02 01 03 04 3c 30 3a 04  0c 80 00 00 09 03 00 00   ....<0:. ........
0050  d0 ba f4 64 80 02 01 01  02 04 00 ad 6e 3c 04 09   ...d.... ....n<..
0060  43 53 43 4f 4a 61 73 6f  6e 04 0c 48 a2 b3 68 75   CSCOJaso n..H..hu
0070  13 7f 74 09 21 41 22 04  08 00 00 00 01 4e ce 71   .Bt.!A". .....N.q
0080  ec 04 82 01 10 9e 24 67  37 10 3e 95 4e 8b 6b ad   ......$g 7.>.N.k.
0090  be 9f e3 45 19 28 2c 2a  7e 03 2f 89 20 f5 9c e7   ...E.(,* ~./. ...
00a0  7a b1 2e ef 04 c1 9e eb  ff 51 30 21 91 96 1e 90   z....... .Q0!....
00b0  f0 08 0f 4a f1 27 8c 47  2a 2b 49 5a c1 23 ce de   ...J.'.G *+IZ.#..
00c0  07 b7 2e 2a 29 11 ee 8d  ee 97 88 37 04 e7 2a a7   ...*).... ...7..*.
```

Filter: / Reset Apply File: snmpv3-4-alldiscinfo

SNMPv3 snmpEngineID Discovery

Very Important Consideration!

- What does this tell us?
- If we don't store a lot of information about the device and keep within 150s of the polled device's clock,
  we'll do double the SNMP packets of SNMPv1/2c!
- NTP is crucial
- Ensure your SNMPv3 NM application vendors are *persisting* snmpEngineID, snmpEngineBoot and snmpEngineTime
- If you poll every 5 minutes, why do an engine discovery every time?
  Just increment the 'polling clock' by 300 seconds!

SNMPv3 and Contexts

- Some standard MIBs assume that a particular SNMP entity contains only one instance of the MIB.
- In SNMPv1 and 2c we used ‘Community String Indexing’ to access the alternate instances
- Commonly used with BRIDGE-MIB to extract MAC address info from each VLAN
  - [Community String]@[VLAN_Instance]
  - SNMP_READ@10
- Also used with SNMP-REPEATER-MIB
  - [Community String]@[Module/Port]
  - SNMP_READ@1/1
- With SNMPv3, we have no Community String, so nothing to index with…
  We use Contexts instead

This Explains Why You Shouldn’t Use “@” in Your Community Strings

SNMPv3 and Contexts

- Ensure your device/code can see the contexts with ‘show snmp context’ [Note: Not supported in Cat2950]

```
Switch# sh snmp context
vlan-1
vlan-30
vlan-32
vlan-200
vlan-1002
vlan-1003
vlan-1004
vlan-1005
```

- You also need to add contexts for each vlan with:

  snmp-server group v3group v3 auth context vlan-# write v1default

- After 12.4(20)T it can be one line for ALL vlans

  snmp-server group v3group v3 auth context vlan- match prefix write v1default

SNMPv3 and Contexts

If supported, you can manually poll a VLAN (context) using Net-SNMP with this example:

```
nms$ snmpwalk -v 3 -Ob -u CSCOJason -l authNoPriv -a MD5 -A password1 -n vlan-32
172.18.86.248 dot1dTpFdbAddress

BRIDGE-MIB::dot1dTpFdbAddress.0.0.0.77.0.50 = Hex-STRING: 00 00 00 4D 00 32
BRIDGE-MIB::dot1dTpFdbAddress.0.0.12.7.172.0 = Hex-STRING: 00 00 0C 07 AC 00
BRIDGE-MIB::dot1dTpFdbAddress.0.5.155.113.172.64 = Hex-STRING: 00 05 9B 71 AC 40
BRIDGE-MIB::dot1dTpFdbAddress.0.12.41.25.71.62 = Hex-STRING: 00 0C 29 19 47 3E
BRIDGE-MIB::dot1dTpFdbAddress.0.12.41.143.181.120 = Hex-STRING: 00 0C 29 8F B5 78
BRIDGE-MIB::dot1dTpFdbAddress.0.12.41.217.229.136 = Hex-STRING: 00 0C 29 D9 E5 88
BRIDGE-MIB::dot1dTpFdbAddress.0.20.79.149.163.219 = Hex-STRING: 00 14 4F 95 A3 DB
BRIDGE-MIB::dot1dTpFdbAddress.0.20.169.204.119.0 = Hex-STRING: 00 14 A9 CC 77 00
BRIDGE-MIB::dot1dTpFdbAddress.0.21.23.194.252.100 = Hex-STRING: 00 15 17 C2 FC 64
BRIDGE-MIB::dot1dTpFdbAddress.0.25.6.102.104.112 = Hex-STRING: 00 19 06 66 68 70
. . .
```

SNMPv3

Application Support

Application	SNMPv3 Support
Cisco Prime Infrastructure 1.2 to 2.0	Yes – authPriv (w/ advanced encryption)
CiscoWorks LMS 2.5 to 4.0	Yes – authPriv
Cisco Prime LMS 4.1 and 4.2	Yes – authPriv (w/ advanced encryption)
CiscoWorks NCM 1.1 and higher	Yes – authPriv
CiscoWorks QoS Policy Manager 4.1+	Yes – authPriv
EMC Ionix Network Configuration Manager	Yes
CA eHealth	Yes
CA NetQoS SuperAgent and Performance Center	Yes – authPriv (w/ advanced encryption)
InfoVista VistaInsight for Networks	Yes
ScienceLogic EM7	Yes
Cacti (Open-Source)	Yes
Solarwinds Orion	Yes

SNMPv3 Adoption

- Based on Cisco Advanced Services data from May 2013
- Scope: 916 collectors
  1,724,827 device/configs

- SNMP adoption: 98.5% customers 88.2% devices [up 9% from 2012]
- SNMPv3 adoption: 34.6% customers 10.4% devices [up 4% from 2012]

SNMPv3 with Cisco Prime LMS

Admin > Network > Device Credential Settings > Default Credential Sets

Navigator

- Current DCR Settings
- **Default Credential Sets**
- Default Credential Sets Policy Configuration
- Device Poll Settings
- Device Polling
- Mode Settings
- User Defined Fields
- Verification Settings

Default Credential Sets

Default Credential Set

Default Credentials

- **Credential Sets**
  - Credentials Set Name
  - Standard Credentials
  - SNMP Credentials
  - HTTP Credentials
  - Auto Update Server Managed Device Credentials
  - Rx-Boot Mode Credential

SNMPv2c/SNMPv1

RO Community String: Verify:

RW Community String: Verify:

SNMPv3

Mode: NoAuthNoPriv AuthNoPriv AuthPriv

Username: CSCOjason

Auth Password: ********** Verify: **********

Auth Algorithm : None

Privacy Password: Verify:

Privacy Algorithm : None

Note: * - Required Field

Apply Cancel Remove

None
DES
3DES
AES128
AES192
AES256

SNMPv3 with Cisco Prime Infrastructure

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | jadavis ▾ Search Menu/Prime Data

Home Design ▾ Deploy ▾ Operate ▾ Report ▾ Administration ▾ Workflows ▾

System Settings

Data Sources Appliance Background Tasks High Availability System Audit

- Alarms and Events
- Audit
- Audit Log Purge Settings
- Change Audit Notification
- CLI Session
- Client
- Configuration
- Configuration Archive
- Controller Upgrade Settings
- Data Deduplication
- Data Retention
- Grouping
- Guest Account Settings
- Image Management
- Inventory
- Job Approval Settings
- Known Ethernet MAC Address List
- Login Disclaimer
- Mail Server Configuration
- Notification Receivers

SNMP Credentials

Administration > System Settings > **SNMP Credentials**

-- Select a Command -- Go

The SNMP credentials listed in this page will be used only for tracing the Rogue APs Switch Port.

	Network Address
	0.0.0.0

Workflow Status 0 0 0 | Support Cases | Alarm Browser | Alarm Summary 324 0 173

Go to Administration / System Settings,
Then scroll down to SNMP Credentials

Create new SNMP Credential sets to suite

SNMPv3 with Cisco Prime Infrastructure

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | jadavis ▾ Search Menu/Prime

Home Design ▾ Deploy ▾ Operate ▾ Report ▾ Administration ▾ Workflows ▾

System Settings

Data Sources Appliance Background Tasks High Availability

- Alarms and Events
- Audit
- Audit Log Purge Settings
- Change Audit Notification
- CLI Session
- Client
- Configuration
- Configuration Archive
- Controller Upgrade Settings
- Data Deduplication
- Data Retention
- Grouping
- Guest Account Settings
- Image Management
- Inventory
- Job Approval Settings
- Known Ethernet MAC Address List
- Login Disclaimer
- Mail Server Configuration
- Notification Receivers

SNMP Credential Details '0.0.0.0'

Administration > System Settings > SNMP Credentials > **SNMP Credential Details**

General Parameters

Add Format Type	**SNMP Credential Info**
*Network Address	0.0.0.0 (comma-separated Network Addresses)
Network Mask	255.255.255.0

SNMP Parameters

* Retries	3
* Timeout	4
SNMP v1 Parameters	☐
SNMP v2 Parameters	☑
*Community	•••••••
SNMP v3 Parameters	☑
*Username	admin
Auth. Type	None
*Auth. Password	•••••
Privacy Type	None
*Privacy Password	•••••

OK Cancel

Note: Selecting any one of the SNMP versions is mandatory

Auth. Type None
*Auth. Password
Privacy Type
None
HMAC-MD5
HMAC-SHA

Privacy Type None
*Privacy Password
OK Cancel
Note: Selecting any one of the
None
CBC-DES
CFB-AES-128
CFB-AES-192
CFB-AES-256

Workflow Status 0 0 0 | Support Cases | Alarm Browser | Alarm Summary 324 0 171

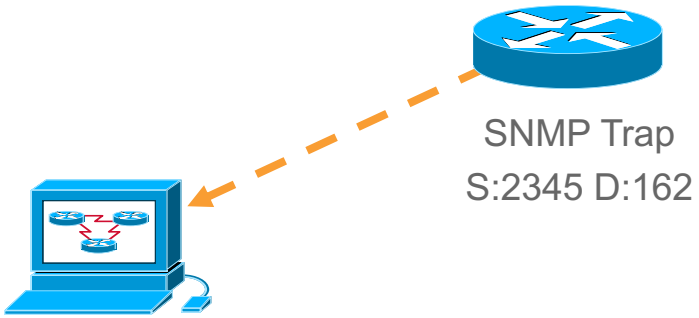
SNMPv3 Support and Issues

- How many devices support it? What does it take to implement?
  - Any that can run a k8/k9 image—most do! Look for devices that can also do SSH—they have similar requirements
  - See the previous configurations for how to implement
- What are the issues with running SNMPv3?
  - Managing the local usernames/passwords—not stored in configuration, can't be restored through an upload of old configuration
  - No current options for localized key management—a la AAA
  - Older model devices may not have high performance CPU for encryption and/or key generation
  - Some tools are inefficient and spawn SNMP EngineID Discovery too often

Note Your Use of MIBs Is the Same – snmpget, snmpwalk, getbulk, 64-Bit HC
SNMPv3 Is Mostly a Transport Change

SNMP Traps/Notifications and Informs

- SNMP Traps are unsolicited events from a device to the NMS
- Traps are sent from device and received by the NMS on well known UDP port 162
- Informs are ‘acknowledged’ traps



SNMP Traps/Notifications and Informs

Cisco IOS SNMP Trap Receiver Configuration Example

Syntax:

snmp-server enable traps [notification-type] [notification-option]

snmp-server host host [traps | informs] [version {1 | 2c}] community-string [udp-port port] [notification-type]

NOTE: NOT the Same as Your Polling/Setting SNMP Community String And We Don't Want It to Be!

```
snmp-server enable traps
snmp-server host 192.168.1.25 notpublic
```

SNMPv3 Notifications

What About Traps/Informs as in v1/v2c?

- SNMPv3 also supports notifications from a device to a NMS
- Decide if doing noauth, auth or with priv traps
- Also decide if doing traps or informs
- For SNMPv3 traps the device sending the trap is authoritative
- Example: Trap / auth

```
! Enables all traps
snmp-server enable traps
!
! …or do selective ones
snmp-server enable traps cpu snmp ospf …
!
snmp-server group notifgroup v3 auth
snmp-server user notifuser notifgroup v3 auth sha AuthPassword
snmp-server host 192.168.1.11 traps version 3 auth notifuser
```

Note: Trap receiver must also have notifuser and password defined locally

SNMPv3 Notifications

What About Traps/Informs as in v1/v2c?

- Example: Trap / priv

  [Main differences highlighted]

```
! Enables all traps
snmp-server enable traps
!
! …or do selective ones
snmp-server enable traps cpu snmp ospf …
!
snmp-server group notifgroup v3 priv
snmp-server user notifuser notifgroup v3 auth sha AuthPassword priv 3des PrivPassword
snmp-server host 192.168.1.11 traps version 3 priv notifuser
```

Note: Trap receiver must also have notifuser and password defined locally

SNMPv3 Notifications

What About Traps/Informs as in v1/v2c?

- Example: Inform / priv
- Receiver (NMS) is authoritative – must add remote engineID
  [Main differences highlighted]

```
! Enables all traps
snmp-server enable traps
!
! …or do selective ones
snmp-server enable traps cpu snmp ospf …
!
snmp-server engineID remote 192.168.1.11 800007E580764D0FFC4265C1C6
snmp-server group notifgroup v3 priv
snmp-server user informuser notifgroup remote 192.168.1.11 v3 auth sha AuthPassword
priv 3des PrivPassword
snmp-server host 192.168.1.11 informs version 3 priv informuser
```

Note: Trap receiver must also have informuser and password defined locally

SNMPv3 and IPv6 Considerations

- IPv6 as a transport - Possible on many products
  IOS XE 2.1.1+
  NX-OS 4.2(1)+
  IOS 12.0S, 12.2SE, 12.3T, 12.4
- Management Application use of IPv6 native – Many only support dual-stack
  - awareness of IPv6 interfaces/IPs, but rely on IPv4 transport
- MIBS / Instrumentation
  - CISCO-CONFIG-COPY-MIB, CISCO-CONFIG-MAN-MIB, CISCO-DATA-COLLECTION-MIB, CISCO-FLASH-MIB, CISCO-IETF-IP-FORWARDING-MIB, CISCO-IETF-IP-MIB, IP-FORWARD-MIB, IP-MIB, ENTITY-MIB, NOTIFICATION-LOG-MIB, SNMP-TARGET-MIB
  - For IPv6 over SNMP: CISCO-SNMP-TARGET-EXT-MIB

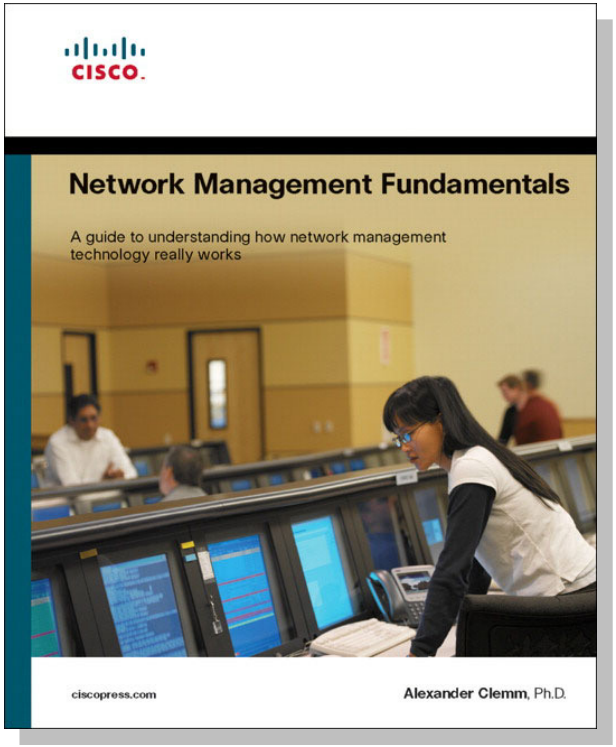
http://www.cisco.com/web/about/security/intelligence/ipv6_mib.html

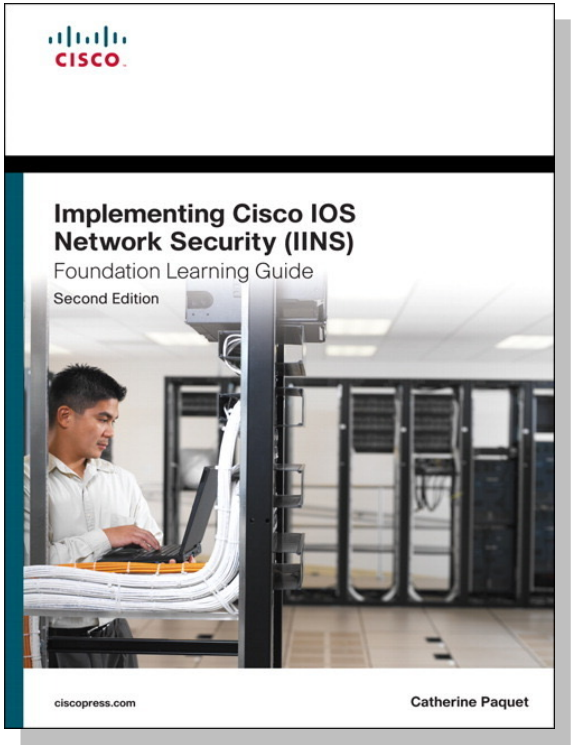
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-mng_apps.html#wp1055171

Conclusion/Summary

- Use the Network Management configuration examples/leading practices we've discussed
- Communicate with your security team to bolster NM security
- Consider—what are the **real** risks? Engineer & Implement Appropriately
- Consider the impact to devices and network management to implement new security features

Recommended Reading for BRKNMS-2658





Q and A

Call to Action…

Visit the World of Solutions:-

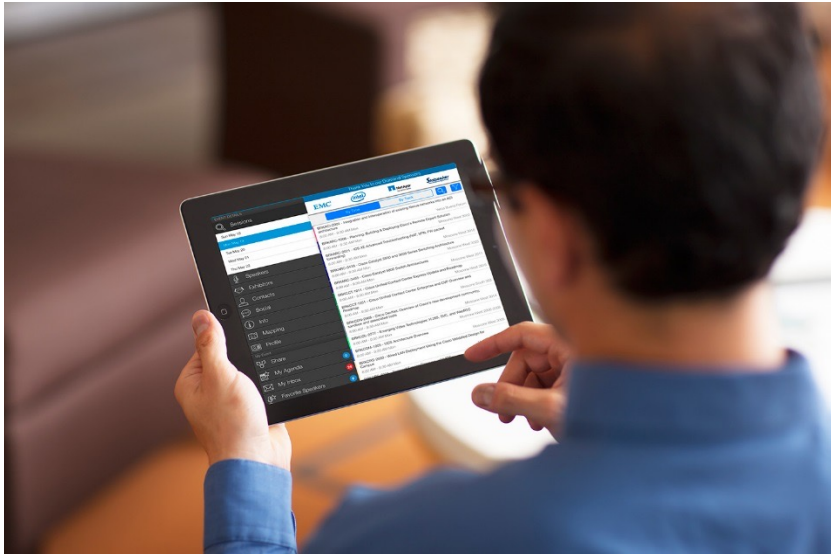
- **Cisco Campus**
- **Walk-in Labs**
- **Technical Solutions Clinics**

- **Meet the Engineer**

- **Lunch Time Table Topics**, held in the main Catering Hall
- **Recommended Reading**: For reading material and further resources for this session, please visit www.pearson-books.com/CLMilan2014

Complete Your Online Session Evaluation

- Complete your feedback surveys through the Cisco Live mobile app or your computer on Cisco Live Connect.
- Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.



Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Continue Your Education

- Demos in the Cisco campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

CISCO

TOMORROW starts here.

Backup/Reference Slides

… and Musings About Other Security Methods
You Should Use When Managing Your Network ☺

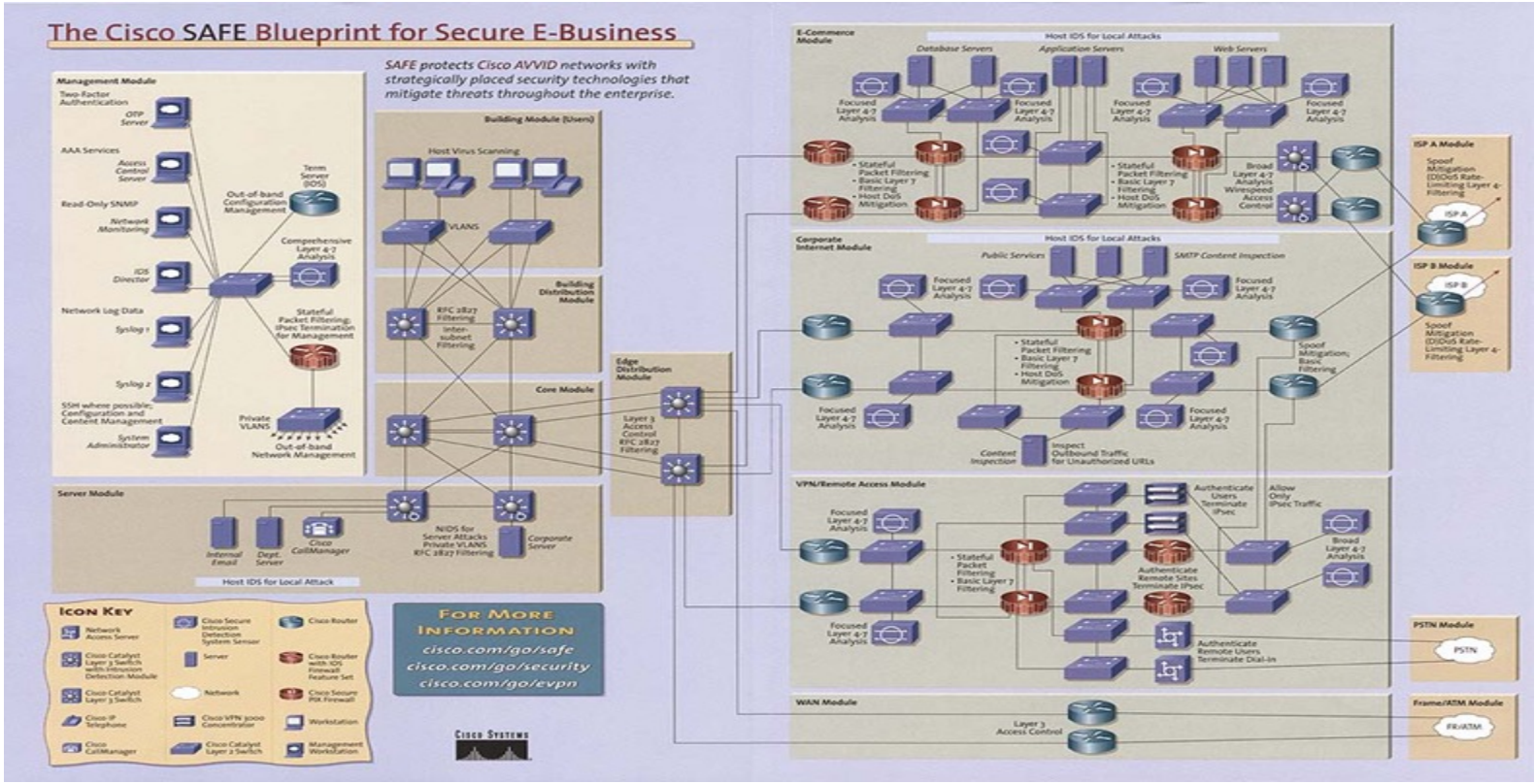
SNMPv3 Advanced Encryption Support in Software

--- IOS XE ---	--- IOS ---	12.4(22)XR3	12.4(15)T7	12.4(9)T1	12.4(4)XC7	12.2(53)SG2	12.2(33)SRD2
2.1.2	15.1(4)M	12.4(22)XR2	12.4(15)T6	12.4(9)T	12.4(4)XC6	12.2(53)SG1	12.2(33)SRD1
2.1.1	15.1(3)T	12.4(22)XR1	12.4(15)T5	12.4(6)XT2	12.4(4)XC5	12.2(53)SG	12.2(33)SRD
2.1.0	15.1(2)T	12.4(22)T4	12.4(15)T4	12.4(6)XT1	12.4(4)XC4	12.2(53)SE2	12.2(33)SRC6
2.2.3	15.1(2)S	12.4(22)T3	12.4(15)T3	12.4(6)XT	12.4(4)XC3	12.2(53)SE1	12.2(33)SRC5
2.2.2	15.1(2)GC	12.4(22)T2	12.4(15)T2	12.4(6)XP	12.4(4)XC2	12.2(53)SE	12.2(33)SRC4
2.2.1	15.1(1)XB	12.4(22)T1	12.4(15)T1	12.4(6)XE3	12.4(4)XC1	12.2(52)XO	12.2(33)SRC3
2.3.2	15.1(1)T	12.4(22)T	12.4(15)T	12.4(6)XE2	12.4(4)XC	12.2(52)SG	12.2(33)SRC2
2.3.1t	15.1(1)S1	12.4(20)T5	12.4(14)XK	12.4(6)XE1	12.4(4)T7	12.2(52)SE1	12.2(33)SRC1
2.3.1	15.1(1)S	12.4(20)T4	12.4(11)XW10	12.4(6)XE	12.4(4)T6	12.2(50)SG8	12.2(33)SRC
2.3.0t	15.0(1)S3a	12.4(20)T3	12.4(11)XW9	12.4(6)T11	12.4(4)T5	12.2(50)SG7	12.2(33)SRB7
2.3.0	15.0(1)S2	12.4(20)T2	12.4(11)XW7	12.4(6)T10	12.4(4)T4	12.2(50)SG6	12.2(33)SRB6
2.4.4	15.0(1)S1	12.4(20)T1	12.4(11)XW6	12.4(6)T9	12.4(4)T3	12.2(50)SG4	12.2(33)SRB5a
2.4.3	15.0(1)S	12.4(20)T	12.4(11)XW5	12.4(6)T8	12.4(4)T2	12.2(50)SG3	12.2(33)SRB5
2.4.2	15.0(1)M5	12.4(15)XY5	12.4(11)XW4	12.4(6)T7	12.4(4)T1	12.2(50)SG2	12.2(33)SRB4
2.4.1	15.0(1)M4	12.4(15)XY4	12.4(11)XW3	12.4(6)T6	12.4(4)T	12.2(50)SG1	12.2(33)SRB3
2.4.0	15.0(1)M3	12.4(15)XY3	12.4(11)XW2	12.4(6)T5	12.4(2)XA2	12.2(50)SG	12.2(33)SRB2
2.5.2	15.0(1)M2	12.4(15)XR8	12.4(11)XW	12.4(6)T4	12.4(2)XA1	12.2(46)SG	12.2(33)SRB1
2.5.1	15.0(1)M1	12.4(15)XR7	12.4(11)XJ4	12.4(6)T3	12.4(2)XA	12.2(33)SXJ	12.2(33)SRB
2.5.0	15.0(1)M	12.4(15)XR6	12.4(11)XJ3	12.4(6)T2	12.4(2)T6	12.2(33)SXI4	12.2(33)SCB6
2.6.2	12.4(24)T3	12.4(15)XR5	12.4(11)XJ2	12.4(6)T1	12.4(2)T5	12.2(33)SXI3	12.2(33)SCB5
2.6.1	12.4(24)T2	12.4(15)XR4	12.4(11)XJ	12.4(6)T	12.4(2)T4	12.2(33)SXI2a	12.2(33)SCB4
2.6.0	12.4(24)T1	12.4(15)XR3	12.4(11)T4	12.4(4)XD12	12.4(2)T3	12.2(33)SXI2	12.2(33)SB8
3.1.2S	12.4(24)T	12.4(15)XR2	12.4(11)T3	12.4(4)XD11	12.4(2)T2	12.2(33)SXI1	12.2(33)SB7
3.1.1S	12.4(22)YB8	12.4(15)XR1	12.4(11)T2	12.4(4)XD10	12.4(2)T1	12.2(33)SXI	12.2(33)SB6
3.1.0S	12.4(22)YB7	12.4(15)XR	12.4(11)T1	12.4(4)XD9	12.4(2)T	12.2(33)SRE3	12.2(33)SB5
3.1.1SG	12.4(22)YB6	12.4(15)XF	12.4(11)T	12.4(4)XD8	12.2(55)SE	12.2(33)SRE2	12.2(33)SB4
3.2.1S	12.4(22)YB5	12.4(15)T13	12.4(9)T7	12.4(4)XD7	12.2(54)XO	12.2(33)SRE1	12.2(33)SB3
3.2.0S	12.4(22)YB4	12.4(15)T12	12.4(9)T6	12.4(4)XD5	12.2(54)WO	12.2(33)SRE0a	12.2(33)SB2
3.3.0S	12.4(22)YB1	12.4(15)T11	12.4(9)T5	12.4(4)XD4	12.2(54)SG1	12.2(33)SRE	12.2(33)SB1
	12.4(22)YB	12.4(15)T10	12.4(9)T4	12.4(4)XD3	12.2(54)SG	12.2(33)SRD4	12.2(33)SB

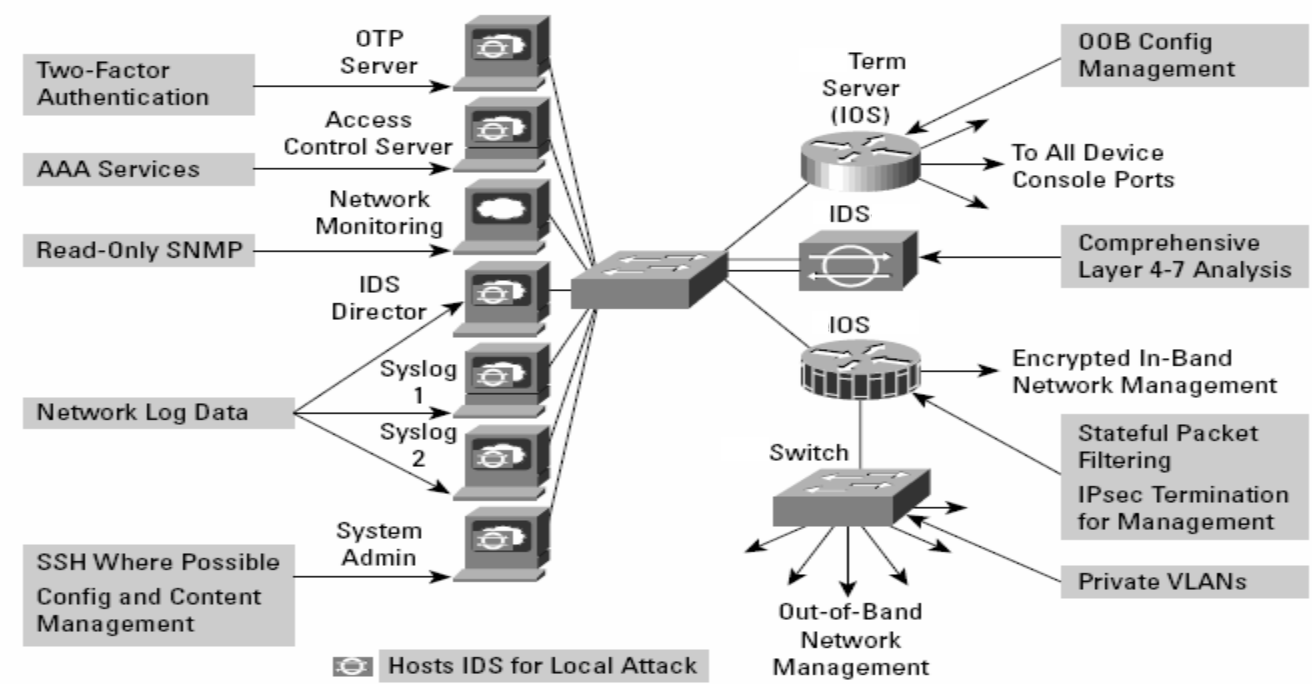
SNMPv3 Advanced Encryption Support in Hardware

--- IOS XE ---
ASR1000-RP1
ASR1000-RP2
ASR1001
CAT4500E-SUP7E
--- IOS ---
10000-PRE2
10000-PRE3
10000-PRE4
1701
1711
1712
1721
1751
1751-V
1760
1801
1802
1803
1805
1811
1812
1841
1841C
1861
1861E
1905
1921
1941
1941W
2610XM-2611XM
2620XM-2621XM
2650XM-2651XM
2691
2801
2801C
2811
2811C
2821
2821C
2851
2901
2911
2921
2951
3220
3250
3270
3660
3725
3745
3825
3825-NOVPN
3845
3845-NOVPN
3925
3925E
3945
3945E
7200
7200-NPE-G2
7201
7301
7304-NPE-G100
7304-NSE-100
7304-NSE-150
7400
7600-CMM
7600-MWAM
7600-RSP720-10GE/MSFC4
7600-RSP720/MSFC4
7600-SAMI
7600-SUP32/MSFC2A
7600-SUP720/MSFC3
815
831
836
837
851
857
861
867
871
876
877
878
881
881SRST
8850RPM-PR
8850RPM-XF
886VA
887
887SRST
887VA
887VA-M
888
888E
888SRST
891
892
AS5350
AS5400
AS5400HPX
AS5850-ERSC
AS5850-RSC
C1841VE
C2811VE
CAT2960-LANLITE
CAT2960S
CAT2975
CAT3560
CAT3560E
CAT3560X
CAT3750
CAT3750-METRO
CAT3750E
CAT3750X
CAT4500-SUP2-PLUS
CAT4500-SUP2-PLUS-10GE
CAT4500-SUP2-PLUS-TS
CAT4500-SUP4
CAT4500-SUP5
CAT4500-SUP5-10GE
CAT4500E-SUP6E
CAT4500E-SUP6L-E
CAT4900M
CAT4928-10GE
CAT4948
CAT4948-10GE
CAT4948-E-F
CAT4948E
CAT6000-CMM
CAT6000-MWAM
CAT6000-SUP32/MSFC2A
CAT6000-SUP720/MSFC3
CAT6000-VS-S720-10G/MSFC3
CBS3012
CBS3020
CBS3030
CBS3032
CBS3040
CBS3110
CBS3120
CBS3130
CGR2010
IAD2430
IAD2431-IAD2432
IAD2801
IAD881
IAD888
IE3000
IGX8400-URM
ME3400
ME3400E
ME4900
ME6524
SLT
SOHO91
SOHO96
SOHO97
UBR10K-PRE4
UC520
VG224
VGD-1T3

Cisco SAFE



NM in the Cisco SAFE Blueprint



Cisco SAFE

SAFE Factors for Network Management

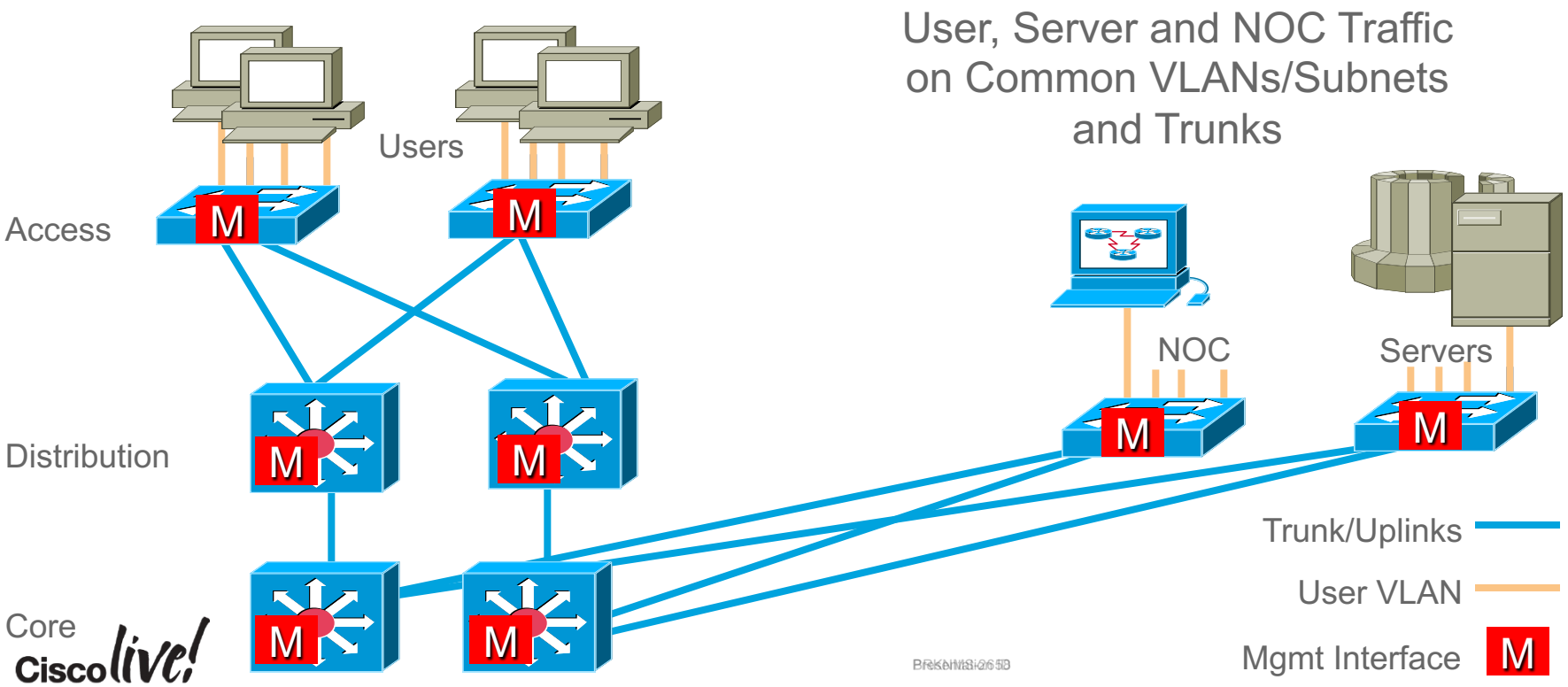
- Appropriate network topology (IB/OOB)
- Restricting access to NM ports
- Locking down Telnet access
- Locking down SNMP access
- Controlling access through the use of TACACS+
- Turning off unneeded services (ports/trunking)
- Logging at appropriate levels
- NM Server and Application Security

In-Band (IB) Network Management

- Network Management traffic runs over common user and server VLANs/subnets
  - SNMP, Telnet, SSH, Syslog, NTP, etc.
- Infrastructure is shared
- Switch management interface (sc0) and router management interfaces (LoopBack0) in common user/data address space

In-Band Network Management

Higher Amount of Risk



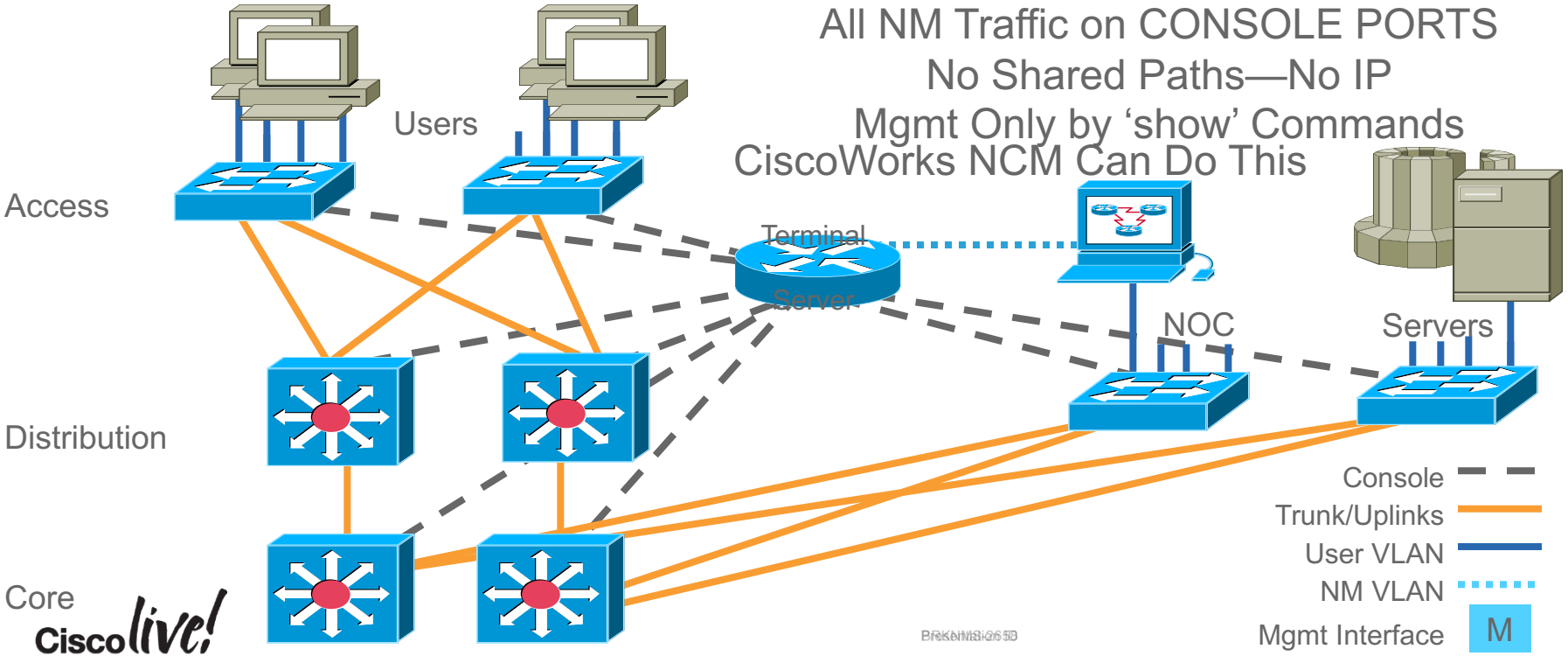
In-Band Network Management

- Pros
  - Easier to implement
  - Lower infrastructure/cabling cost
- Cons
  - Traffic passes on same network path as end-user and server traffic
    - Denial of Service (DoS)
    - Traffic load
    - Device resource constraints (CPU, memory)

REAL OOB Network Management

Least Amount of Risk

User, Server Traffic as Normal;
All NM Traffic on CONSOLE PORTS
No Shared Paths—No IP
Mgmt Only by ‘show’ Commands
CiscoWorks NCM Can Do This



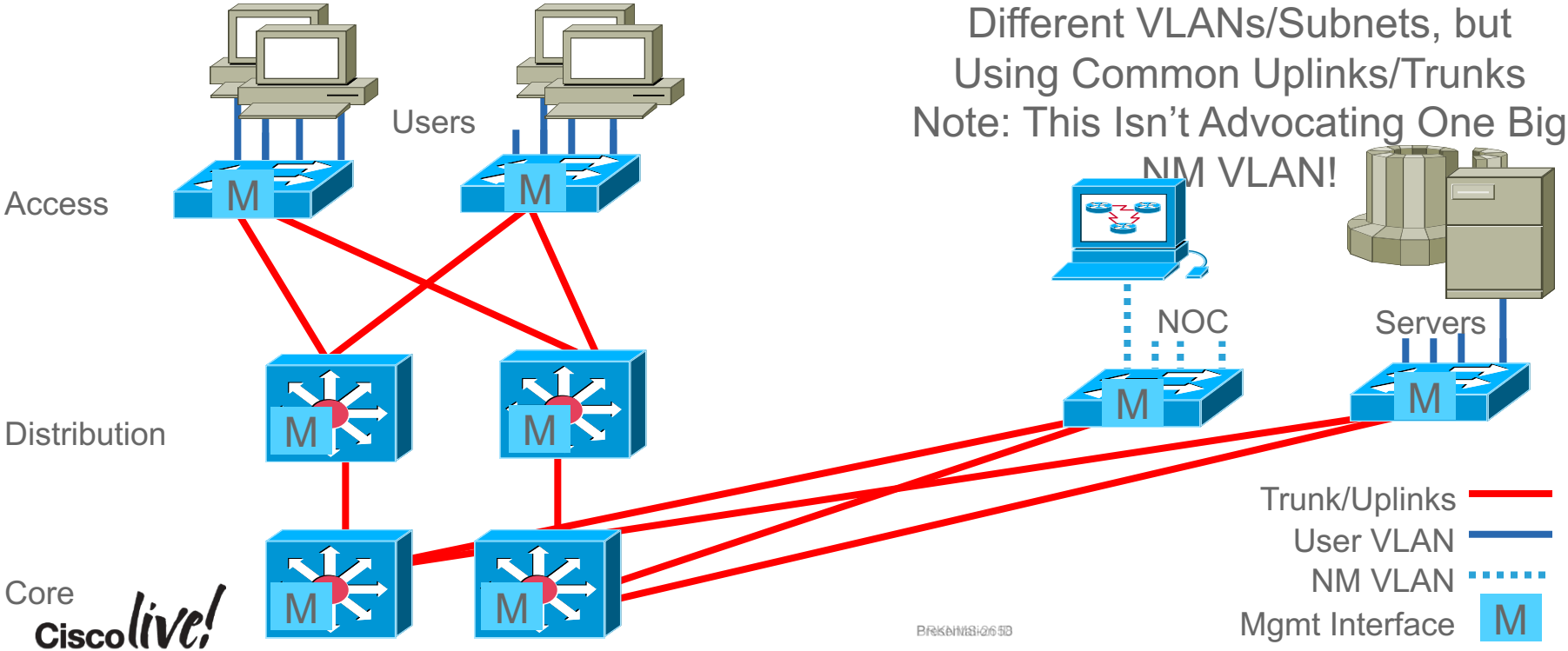
Pseudo Out-of-Band Network Management

- Network management traffic runs over different VLANs/subnets than user and server traffic
  - SNMP, Telnet, SSH, Syslog, NTP, etc.
- Infrastructure is shared (trunks) according to company's level of risk tolerance
- Switch management interface (sc0) and router management interfaces (LoopBack0) in unique address space(s)

Pseudo Out-of-Band Network Management

Lower Amount of Risk—Most Popular

User, Server and NM Traffic on Different VLANs/Subnets, but Using Common Uplinks/Trunks
Note: This Isn't Advocating One Big NM VLAN!



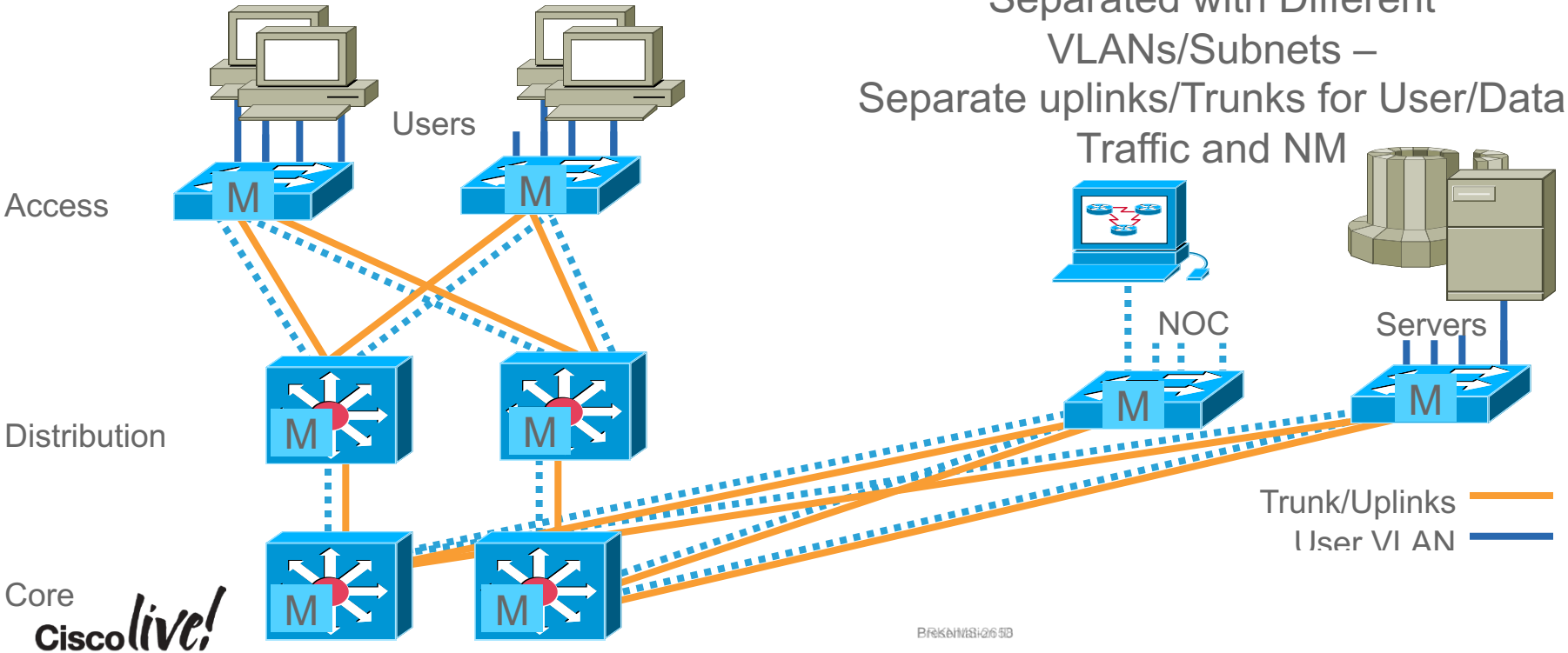
Pseudo Out-of-Band Network Management – Another Version

- Network Management traffic runs over different VLANs/subnets than user and server traffic
  - SNMP, Telnet, SSH, Syslog, NTP, etc.
- Little infrastructure is shared (trunks) according to company's level of risk tolerance—essentially unique uplinks (no shared interfaces/bandwidth)
- Switch management interface (sc0) and router management interfaces (LoopBack0) in unique address space(s)

Pseudo OOB Network Management

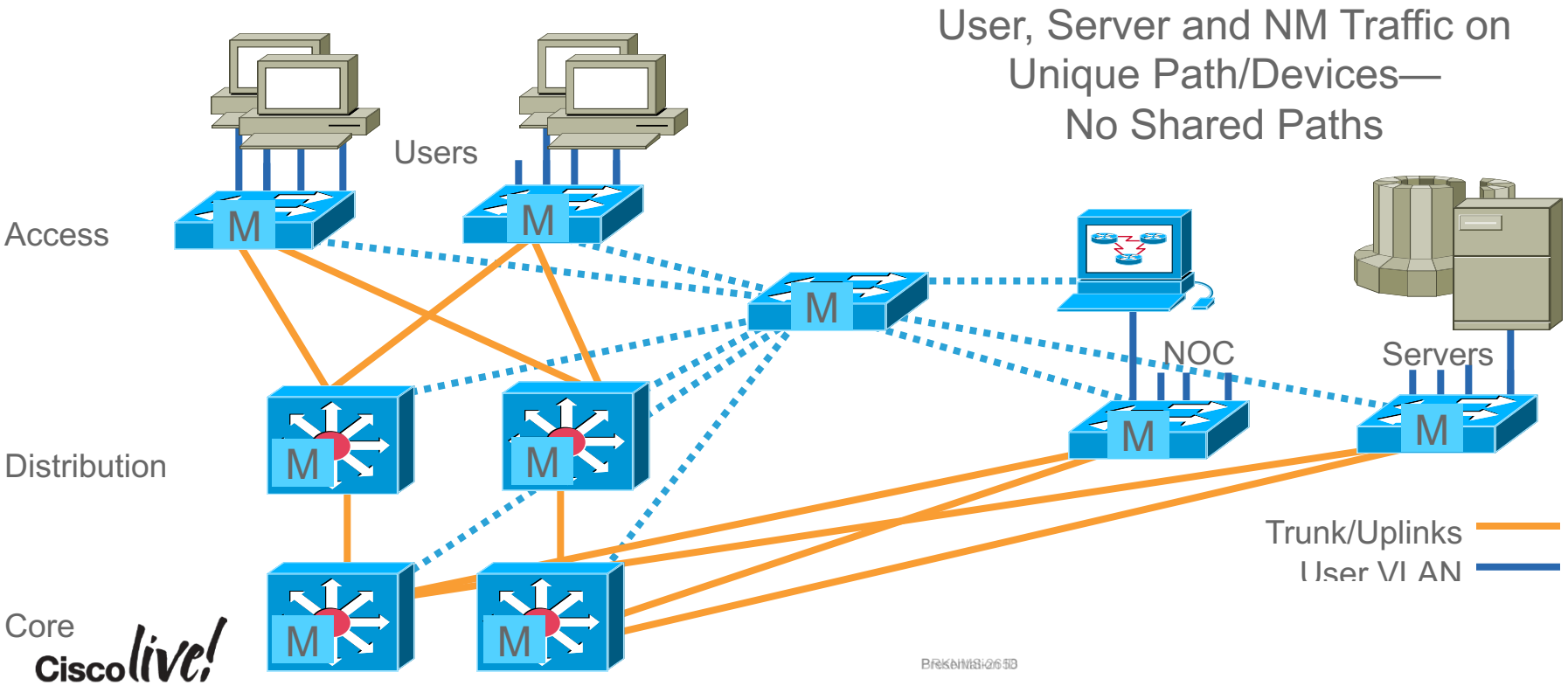
Even Lesser Amount of Risk

User, Server and NM Traffic Are Separated with Different VLANs/Subnets – Separate uplinks/Trunks for User/Data Traffic and NM



OOB Network Management

And an Even Lesser Amount of Risk



Out-of-Band (OOB) Network Management

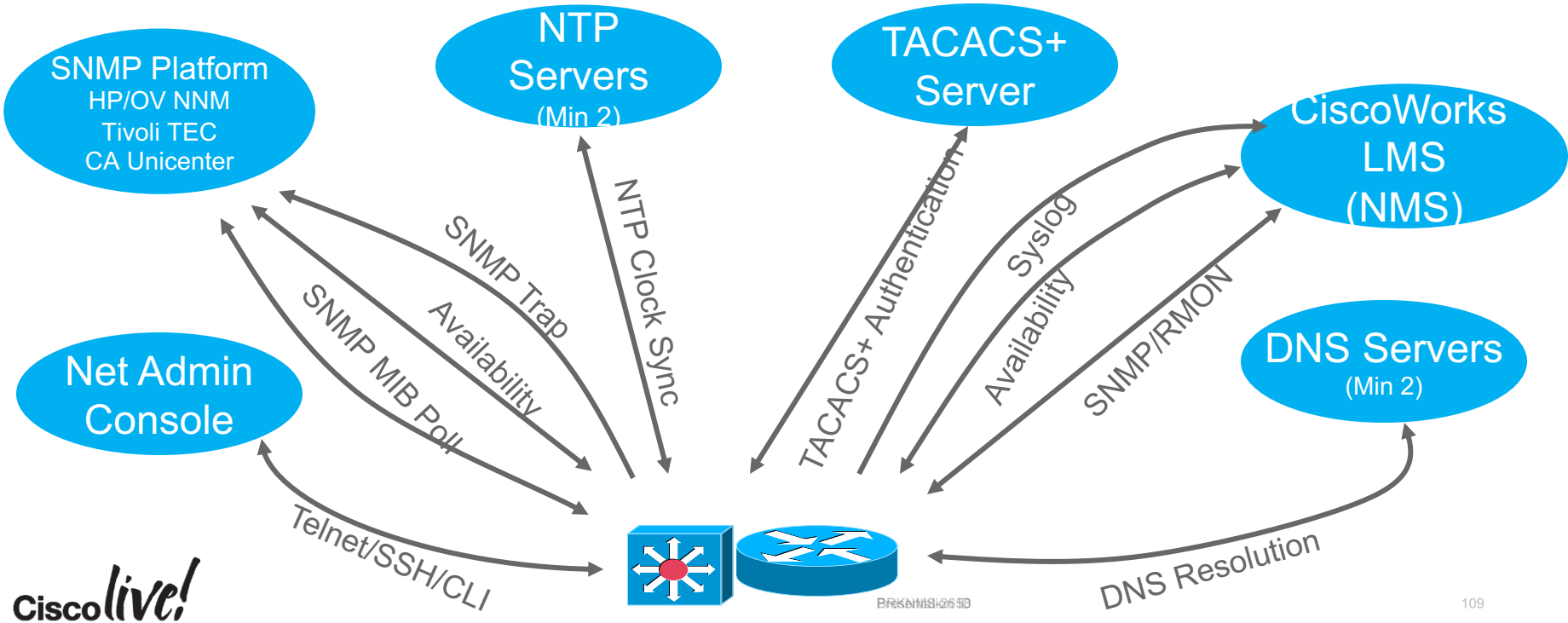
- Pros
  - NM traffic separate from user/server traffic
  - NM processes unimpeded by
    - STP storms
    - Traffic load
    - DoS
- Cons
  - Higher cost—especially if physically separating interfaces and network path
  - More engineering design requirements (a single Layer-2 VLAN for NM spanning a large net is an STP nightmare)

What Is a Private VLAN?

- Like VLANs within a VLAN
- Consists of three port classifications
  - Isolated Ports: Can only communicate with promiscuous ports
  - Promiscuous Ports: Can communicate with all other ports
  - Community Ports: Can communicate with other members of community and all promiscuous ports
- All within the same VLAN (subnet)
- Protected connections
- No ARP discovery by neighbors

Restricting Access to NM Ports

Consider Your Inputs and Outputs



Why SSH?

Telnet Is Insecure for Device Management

```
# snoop admin-pc router-a

Using device /dev/hme (promiscuous mode)

   admin-pc -> router-a  TELNET C port=60534
   router-a -> admin-pc    TELNET R port=60534 \r\n\r\nUser Access
  Verification\r\n\r\nUsername:

   admin-pc -> router-a  TELNET C port=60534 c
   router-a -> admin-pc    TELNET R port=60534 c

   admin-pc -> router-a  TELNET C port=60534 i
   router-a -> admin-pc    TELNET R port=60534 i

   admin-pc -> router-a  TELNET C port=60534 s
   router-a -> admin-pc    TELNET R port=60534 s

   admin-pc -> router-a  TELNET C port=60534 c
   router-a -> admin-pc    TELNET R port=60534 c

   admin-pc -> router-a  TELNET C port=60534 o
   router-a -> admin-pc    TELNET R port=60534 o
```

'snoop' Is a Packet Capture Utility Built into Solaris

Sniffer Capture of Non-Secure Telnet

Why SSH?

Capture of a Clear Telnet Session

```
⊟ Transmission Control Protocol, Src Port: telnet (23), Dst Port: 49440 (49
    Source port: telnet (23)
    Destination port: 49440 (49440)
    Sequence number: 3817725289
    Next sequence number: 3817725331
    Acknowledgement number: 2585398119
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 4104
    Checksum: 0xd750 (correct)
⊟ Telnet
    Data: \r\n
    Data: \r\n
    Data: User Access Verification\r\n
    Data: \r\n
    Data: Username:

0000  08 00 20 a8 8a ba 00 01  97 37 64 00 08 00 45 c0   .. ..... .7d...E.
0010  00 52 00 02 00 00 fe 06  ad cf 0b 84 00 34 ac 12   .R...... .....4..
0020  56 4a 00 17 c1 20 e3 8d  dd 69 9a 1a 0b 67 50 18   VJ... .. .i...gP.
0030  10 08 d7 50 00 00 0d 0a  0d 0a 55 73 65 72 20 41   ...P.... ..User A
0040  63 63 65 73 73 20 56 65  72 69 66 69 63 61 74 69   ccess Ve rificati
0050  6f 6e 0d 0a 0d 0a 55 73  65 72 6e 61 6d 65 3a 20   on....Us ername:
```

Why SSH?

This Freely Available Sniffer Application—Wireshark—Even Has a Nice "Follow TCP Stream" Capability which Made Decoding and Replay a Snap!

Contents of TCP stream

```
........... ..!..".."..'................0
0
User Access Verification0
0
Username: .......P............ ..!..!.....".."..'.......ANSI....$..$cciisscc00.0
Password: cisco1230.0
0
L1-5.2-2611-B>eennaa0.0
Password: cisco1230.0
L1-5.2-2611-B#eexxiitt0.0
..!...
```

Your Passwords!

http://www.wireshark.org

Locking Down Telnet Access—SSH

- An application and protocol that provides a secure, remote connection to a device
- Versions
  - SSH-1 (deprecated as insecure)
  - SSH-1.5 (version 1 with fixes)—introduced in Cisco IOS® 12.1(5)T9
  - SSH-2—introduced in Cisco IOS 12.3(4)T, 12.1(19)E6

Note: v1.99 means compatibility with v1 and v2 (see RFC 4253 Sect5.1)

Locking Down Telnet Access—SSH

- SSH server—Cisco IOS
- SSH v2 introduced in some Cisco IOS platforms/images starting in 12.3(4)T, 12.1(19)E6
- Requires 56-bit DES or 3DES images (k8 or k9)
- Non-trivial memory requirements
- Side note: 12.2 adds an MD5 hash capability for ‘username’ command

```
hostname routera
ip domain-name cisco.com
crypto key generate rsa
aaa new-model
username myuser password 7
2120C5E02144F32555D1D1c08
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
line vty 0 4
  transport input ssh
```

CatOS Example in the Post-Preso Reference Slides

Locking Down Telnet Access—SSH

ssh - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
1	0.000			TCP	49452 > 22 [SYN] Seq=2637627515 Ack=0 Win=8760 Len=0
2	0.001			TCP	22 > 49452 [SYN, ACK] Seq=4226909194 Ack=2637627516 Win=4128
3	0.001			TCP	49452 > 22 [ACK] Seq=2637627516 Ack=4226909195 Win=9112 Len=0
4	0.005			SSH	Server Protocol: SSH
5	0.005			TCP	49452 > 22 [ACK] Seq=2637627516 Ack=4226909214 Win=9112 Len=0
6	0.103			SSH	Client Protocol: SSH
7	0.107			SSH	Server: Public Key
8	0.119			SSH	Client: Session Key
9	0.940			TCP	22 > 49452 [ACK] Seq=4226909490 Ack=2637627694 Win=3950 Len=0
10	2.521			SSH	Server: Encrypted packet len=5
11	2.613			TCP	49452 > 22 [ACK] Seq=2637627694 Ack=4226909502 Win=9112 Len=0
12	2.613			SSH	Client: Encrypted packet len=14
13	2.617			SSH	Server: Encrypted packet len=5
14	2.713			TCP	49452 > 22 [ACK] Seq=2637627714 Ack=4226909514 Win=9112 Len=0
15	5.184			SSH	Client: Encrypted packet len=41
16	5.188			SSH	Server: Encrypted packet len=5
17	5.283			TCP	49452 > 22 [ACK] Seq=2637627766 Ack=4226909526 Win=9112 Len=0

```
⊟ Transmission Control Protocol, Src Port: 49452 (49452), Dst Port: 22 (22), Seq: 2637627714, Ack: 4226909514, Len: 52
    Source port: 49452 (49452)
    Destination port: 22 (22)
    Sequence number: 2637627714
    Next sequence number: 2637627766
    Acknowledgement number: 4226909514
    Header length: 20 bytes
  ⊞ Flags: 0x0018 (PSH, ACK)
    Window size: 9112
    Checksum: 0x7ce4 (correct)
⊟ SSH Protocol
  ⊟ SSH Version 1
      Packet Length: 41
      Padding Length: 7
      Payload: 9D4F3F196348BCBFEC8BD33978F77D4B...
```

```
0000                                              ...7d...  .....E.
0010                                              .\.K@...  .;..VJ..
0020  00 34 c1 2c 00 16 9d 37  01 42 fb f1 85 4a 50 18  .4.,...7 .B...JP.
0030  23 98 7c e4 00 00 00 00  00 29 9d db d1 a8 0f 1f  #.|..... .)......
0040  c7 9d 4f 3f 19 63 48 bc  bf ec 8b d3 39 78 f7 7d  ..O?.cH. ....9x.}
0050  4b 3a 6a f2 84 a2 a4 c6  5b 70 91 d2 13 d7 2c cd  K:j..... [p.....,.
0060  fe 09 5e 08 a5 81 66 29  36 55                   ..^...f) 6U
```

Filter: Reset Apply File: ssh

Sniffer Capture of an SSH Session

Encryption ☺

Locking Down Telnet Access—SSH

Contents of TCP stream

```
.......3..=Y...............J......1...DB.......&...(........Z>..Z.A.......7+...S"<g...9.K...
..j......LgS..<d.M..r.n .J)................o........)..J.D...l'.'U......+Z.(w&...~{'........
#.1...NWPOt..NX........J8<....X....N.
.z.cT9.....[..y.....(%{.DM.qxT..y..zc.......................................3..=Y....U..[M....'*Q7l×
..ix...f...t....B.~L..tg....o*.e.........H...Y......-.8.1&.\j..BA...`).5.Io...n^Y..+.=..T..
.+}.f.D
.........^6:.u,...............$tuk......tv..[|w..y...U......|:O..7.....)..........o?.cH.....9x.
}K:j.....[p....,...^...f)6u.................,.......@9~G.......r.1!B.O..........".O..]........i.~.x{
GD.+...p>].Hxa...,Pl6.D.xr....b.S;a8.K.x...l.%......q....9[.[...J..g.m....".Z..J.....o*.?..
..........|{.O.......ZFz...c)....7.......Js....F....vP&.h.2..O......
..O..u.j..D..&!....
X.1..u.9i.?.)......
..%...*...%.9..9...
..j...z.....3.B....
.E.......bb..,.....
Z-.....%).K.:......
...eK.w.........}........F..E.............m....>1v.."fD.m3.D...>]...
G.....~'#{j...!....
.....D..l-..>......
....u.{U"[.D.N.....
..6...k.qW.u,......
...AI.U.8g..Tt.....
.z...!..4+S_.m@....
OO.?.3..E.D..VA....
O.M..B4..W.........
.('Q....  sqrJ87......v%.."...wU>..'=.]2..EN.....@v.y...
..i.m.La...........
..x.....w...Dv.Y...
..w......a_........
81...^.......I.s...
....&..x.b..%..j...
.
...q..D.W.H..(...
O].q\.ds-..niH.....
.....+.:......5H...
{v...........\......J.z<...1 .....nD....9..{.........a.z............
```

Entire conversation (1425 bytes) | ASCII | EBCDIC | Hex Dump | C Array | Print | Save As | Close

With an SSH Session the “Follow TCP Stream” Feature of Wireshark Shows a Big Mess of Nothin’

Securing NM Client to NM Server SSL—Enabling for CiscoWorks LMS

Admin > Getting Started

CiscoWorks LMS

Faults 33 0 0

jadavis Logout About SiteMap Feedback Help

Search

My Menu Monitor Inventory Configuration Reports Admin Work Centers

Admin > Getting Started

17 Dec 2010, 09:51 EST

System Settings

RCP and SCP Credentials

Browser-Server Security Mode

You can change the security mode for browser-server communication

Current HTTPS setting: **Enabled**

Change HTTPS setting: Enable HTTPS Disable HTTPS

Apply

Backup

Authentication Settings

Proceed to Device Allocation Settings

Skip the rest of the workflow and proceed to Device Status dashboard

Getting Started

- Introduction
- Data Migration
- General System Settings
- Multiserver Configuration
- Other System Settings
  - System Settings
    RCP and SCP credentials, browser-server security mode, backup and authentication settings
- Device Management
- User Management
- Software and Device Updates
- Advanced Configurations

Enables SSL Browser-Server Security

(You Can Also Use Third Party Issued Security Certificates through CLI SSLUtil.pl)

Done

Securing NM Server to Managed Device SSH—Using with CiscoWorks LMS/Config

CiscoWorks LMS

Faults 35 0 0

My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾

Admin > Collection Settings > Config > Config Transport Settings

Navigator

- Config Archive Settings
- Config Collection Settings
- Config compare Exclude Commands Configuration
- Config Job Timeout Settings
- **Config Transport Settings**
- Secondary Credential Settings

Archive Mgmt
- Archive Mgmt
- ConfigEditor
- NetConfig
- NetShow

Transport Settings

Config Transport Settings

Application Name: Archive Mgmt

	Available Protocols		Selected Protocol Order
Config Fetch :	TELNET TFTP SSH RCP HTTPS SCP	> Add >> < Remove <	TELNET TFTP SSH RCP HTTPS
Config Deploy :	TELNET TFTP SSH HTTPS RCP SCP	> Add >> < Remove <	TELNET TFTP SSH HTTPS

Apply Cancel

SSH—Using in CiscoWorks LMS/Admin

CiscoWorks LMS

Faults 33 0 0

My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾

Admin > Network > Device Credential Settings > Default Credential Sets

Navigator

- Current DCR Settings
- **Default Credential Sets**
- Default Credential Sets Policy Configuration
- Device Poll Settings
- Device Polling
- Mode Settings
- User Defined Fields
- Verification Settings

Default Credential Sets

Default Credential Set

Default Credentials

- **Credential Sets**
  - Credentials Set Name
  - Standard Credentials
  - SNMP Credentials
  - HTTP Credentials
  - Auto Update Server Managed Device Credentials
  - Rx-Boot Mode Credential

Information

You can use default credentials to populate newly-added devices in Device Addition flows such as Add and Bulk Import.
Click an item in the left panel and enter the values. Click Apply after you enter all values.
To remove a Default Credential Set and the credentials configured in this Credential Set:

1. Click Credential Set Name in the left panel and select a Default Credential Set name.
2. Click Remove to delete the Default Credential Set and the credentials configured in this Credential Set.

If you delete these credentials, it does not affect the devices that are already added or imported with default credentials.

Note: * - Required Field

Apply Cancel Remove

SSH—Using in CiscoWorks LMS/ Common Services

cisco CiscoWorks LMS

Faults 33 0 0

My Menu ▾ Monitor ▾ Inventory ▾ Configuration ▾ Reports ▾ Admin ▾ Work Centers ▾

Admin > Network > Device Credential Settings > Default Credential Sets

Navigator

- Current DCR Settings
- **Default Credential Sets**
- Default Credential Sets Policy Configuration
- Device Poll Settings
- Device Polling
- Mode Settings
- User Defined Fields
- Verification Settings

Default Credential Sets

Default Credential Set - RTPNML_Default

Default Credentials

- **Credential Sets**
  - Credentials Set Name
  - Standard Credentials
  - SNMP Credentials
  - HTTP Credentials
  - Auto Update Server Managed Device Credentials
  - Rx-Boot Mode Credential

Primary Credential

Username:	netops4lms		
Password:	•••••••••	Verify:	•••••••••
Enable Password:	•••••••••	Verify:	•••••••••

Secondary Credential

Username:			
Password:		Verify:	
Enable Password:		Verify:	

Note: * - Required Field

Apply Cancel Remove

Locking Down Telnet Access—SSH

- SSH Server—
  Cisco Catalyst®
- Introduced in Catalyst 4/5/6K Catalyst OS 6.1 K9 images
- Catalyst 3550—12.1(11)EA1
- Catalyst 85x0—12.1(12c)EY
- No support in Catalyst 1900/2800/2900XL/
  3500XL/4840G/4908

```
set crypto key rsa 1024
set set ip permit enable ssh
set set ip permit enable Telnet
set set ip permit enable snmp
set ip permit 10.1.2.0 255.255.255.0 ssh
set ip permit 10.1.2.0 255.255.255.0 snmp
```

Controlling CLI Access Through AAA/TACACS+

- Authentication, authorization, and accounting
- TACACS+ available in routers and switches—allows for centralized username/password/privilege administration
- Removes the requirement of having to configure hundreds of routers/switches when a user leaves
- Allows for accountability when each user has their own login ID
- Additional capabilities to do authorization and accounting of command usage
- CiscoSecure ACS is a key part of this solution

Controlling CLI Access Through AAA/TACACS+

Cisco IOS 12.0 AAA/TACACS+ Configuration Example

```
username FALLBACK-USERNAME password FALLBACK-PASSWORD
!
aaa new-model
tacacs-server host HOST-IP-ADDR key SECRET-KEY
aaa authentication login consoleport group tacacs+ enable
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
!
aaa authorization exec default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
!
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
!
line con 0
    login authentication consoleport
```

Evaluate Services

- Consider use of CDP to client/server connections (you only need it to other networking gear)
- Explicitly disable auto-negotiation of trunking to client/server connections unless you are using it
- Consider BPDU guard and other STP “safeties”
- Port security (lock down servers to specific ports)
- Consider the use of AutoSecure to quickly lock-down services

AutoSecure cisco.com/go/autosecure

Simplify Securing a Cisco IOS Router and Networks Attached to a Cisco IOS Router

- Built from security audit scripts and security whitepapers that Cisco and others provide
- Global Services Turned Off
  - Finger, PAD, Small Servers, Bootp, HTTP service, CDP, NTP, Source Routing
- Global Services Turned On
  - Password-encryption service, no ip unreachables for NULL0, tcp-synwait-time, tcp-keepalives-in and tcp-keepalives-out
- Services Disabled per Interface
  - Disable icmp unreachables, disable icmp mask reply messages, disable proxy-arp
- Provide Logging for Security
  - Enable sequence numbers and timestamp
- Secure Access to the Router
  - Disables SNMP If not being used; checks and helps configure login banner; re-runs IOS passwords checks (are passwords present, are they the same); checks and sets exec-timeout; enables SSH and SCP (timeout and retries)
- Securing the Forwarding Plane
  - Enable CEF/DCEF, Enable uRPF
  - Block all IANA reserved ip address blocks

Logging

Don’t Stick Your Head in the Sand!

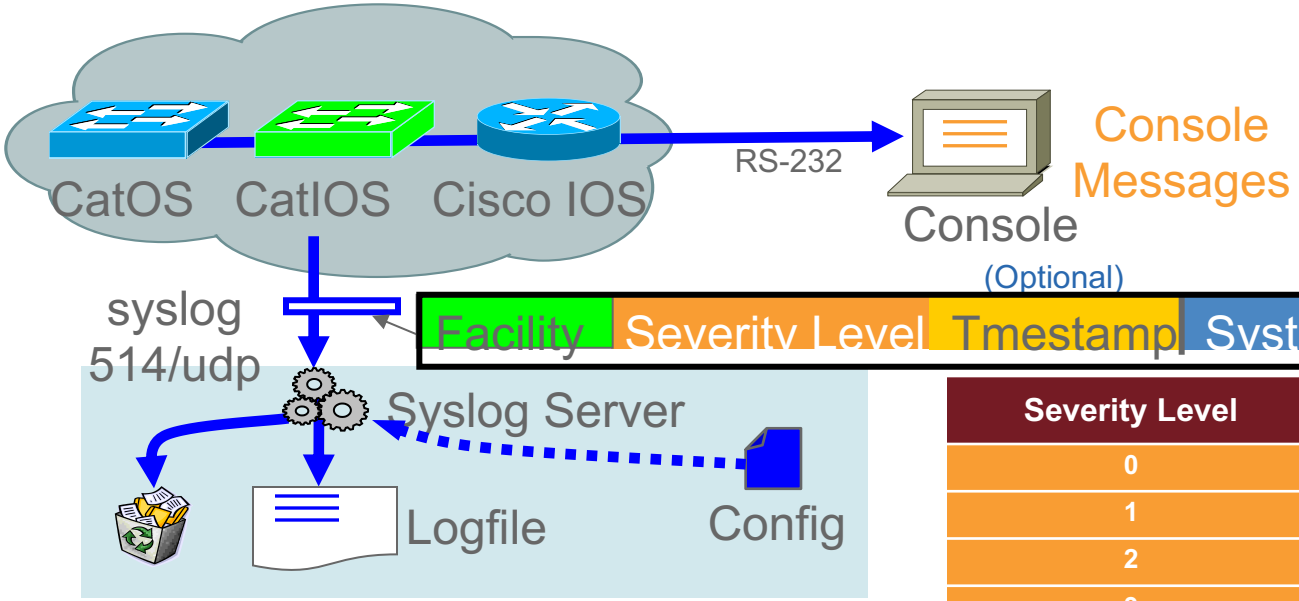
- Managing our network securely goes beyond the use of secure transports and reducing risk
- Logging is necessary for identification and accountability
- If you’re going to log—review them periodically!

Logging—Syslog

Syslog

- Unsolicited notification of an event (like traps)
- Typically more useful than traps alone
  - More information is available
  - Tend to be easier to read, plain English text
  - No variable bindings, no MIBs to load
- Very basic, de facto “standard”, now an Informational RFC 3164
- Sent to a Syslog daemon, on UDP port 514
- Developers seem to define more Syslog messages than traps

Logging—Syslog



Severity Level	Description
0	Emergencies
1	Alerts
2	Critical
3	Errors
4	Warnings
5	Notifications
6	Informational
7	Debugging

CatOS Syslog Default Level → 4

IOS Syslog Default Level → 6

Logging—Syslog

Format

Syslog_Server_Time-Stamp devicename/IP Sequence-Number: [device timestamp] %FACILITY[-SUBFACILITY]-SEVERITY-MNEMONIC: Message-text

```
Apr 26 10:05:15 routera.cisco.com 150905: 14w6d: %GSR_ENV-2-
WARNING: Slot 7 MBUS_5V supply at 4984 mv < 5000 mv

Apr 26 10:07:04 routerb.cisco.com 106052: 12w0d: %BGP-3-
NOTIFICATION: sent to neighbor
10.10.128.200 4/0 (hold time expired) 0 bytes

Apr 26 10:07:10 [10.10.128.129.210.79] 994: 003921: 5d17h: %LINK-3-
UPDOWN: Interface GigabitEthernet1/1, changed state to down
```

Logging—Syslog

- Setting logging history level to “notifications/5” is a good start
- Set lower, to “informational/6” if you aren’t getting the messages you need

IOS:

```
RouterA(config)# logging 192.168.1.25
RouterA(config)# logging 192.168.33.17
RouterA(config)# logging trap notifications
RouterA(config)# logging on
RouterA(config)# service timestamps log datetime msec localtime show-
timezone
RouterA(config)# no logging console
RouterA(config)# no logging monitor
```

NXOS:

```
SwitchA(config)# logging server 192.168.1.25
SwitchA(config)# logging server 192.168.33.17
SwitchA(config)# logging level [facility|all] notifications
SwitchA(config)# logging timestamp milliseconds
SwitchA(config)# no logging console
SwitchA(config)# no logging monitor
```

Logging—Syslog

- ‘Cisco IOS Software System Error Messages’ exists for each Cisco IOS release
  - For Cisco IOS version 12.2:
    - http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_system_message_guide_book09186a008009e73d.html
- ‘System Message Guide’ exists for each CatOS release
  - http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_system_message_guide_chapter09186a00800f2709.html
- Error Message Decoder
  - http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl
- Output Interpreter
  - https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl

Logging—Syslog

- Syslog messages go to a Syslog receiver
  - UNIX server—/var/adm/messages file
  - CiscoWorks LMS server — /var/log/syslog_info
- Trap messages go to a trap receiver
  - HP/OV NNM, Tivoli Netview, CA Spectrum Infrastructure Manager
  - CiscoWorks LMS/Fault Monitor
- Ideally we integrate these into a common event monitor

Locking Down SNMP

SNMP-CatOs

- Setting SNMP read-only, read-write and read-write-all community strings

```
SwitchA> (enable) set snmp community read-only dontusepublic
SwitchA> (enable) set snmp community read-write dontuseprivate
SwitchA> (enable) set snmp community read-write-all dontusesecret
```

- IP Permit list configured
- Only devices on 192.168.1.0/24 can do snmpgets/sets with the correct community string and telnet to th

```
SwitchA> (enable) set ip permit 192.168.1.0 255.255.255.0
SwitchA> (enable) set ip permit enable
```

Locking Down SNMP Access

- Catalyst OS (CatOS) 6.3+
- ‘set snmp view’ example
- Restrict CAM (MAC address) table polling to the BRIDGE-MIB

```
set snmp view nocampoll 1.3.6.1 included nonvolatile
set snmp view nocampoll 1.3.6.1.2.1.17 excluded nonvolatile

set snmp access nocamgroup security-model v1 read nocampoll nonvolatile

set snmp user nocamuser nonvolatile
set snmp group nocamgroup user nocamuser security-model v1 nonvolatile
set snmp community index comm.0 name dontusepublic security nocamuser
  nonvolatile
```

SNMPv3 Configuration

- SNMPv3 authNoPriv
- Catalyst OS 5.4 example (recommend 6.3+)
- Note: The “snmp-server user” config disappears (required in RFC 3414) so a user’s password is not viewable from the config; to see configured users—“show snmp user”
- EngineID is usually “Pre-generated”; if engineID is changed all user accounts must be reconfigured

```
set snmp engineID 00000009020000049AC87300
set snmp access NMCons security-model v3 authentication  set snmp user CSCOJason
authentication md5 password1
set snmp group NMCons user CSCOJason security-model v3
```

SNMPv3 Configuration

- SNMPv3 authPriv
- Catalyst OS 5.4 example (recommend 6.3+)
- Note: The “snmp-server user” statement disappears (required in RFC 3414) so password is not viewable from the Config; to see configured users—“show snmp user”
- EngineID is “Pre-generated”; if engineID is manually changed all user accounts must be reconfigured

```
set snmp engineID 000000090200000049AC87300
set snmp access NMCons security-model v3 privacy
set snmp user CSCOJason authentication md5 password1 privacy password2
set snmp group NMCons user CSCOJason security-model v3
```

Controlling CLI Access Through AAA/TACACS+

Catalyst OS v5.5 AAA/TACACS+ Configuration Example

```
set tacacs server 192.168.1.25 primary
set tacacs key mytacacskey
set authentication login local enable
set authentication login tacacs enable
set authentication enable local enable
set authentication enable tacacs enable
!
set authorization exec enable tacacs+ none both
set authorization commands enable config tacacs none both
!
set accounting exec enable start-stop tacacs+
set accounting system enable start-stop tacacs+
set accounting commands enable all start-stop tacacs+
!
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

SNMP Traps/Notifications and Informs

SNMP Trap Example Without MIB Loaded into NMS

```
988747160 2 Tue May 01 15:59:20 2001 192.168.100.5 - Received event
.1.3.6.1.4.1.9.9.43.2.0.1 (enterprise:.1.3.6.1.4.1.9.9.43.2 generic:6
specific:1),
no format in trapd.conf.   3 args:
 [1] private.enterprises.cisco.ciscoMgmt.43.1.1.6.1.3.60 (Integer): 1;
 [2] private.enterprises.cisco.ciscoMgmt.43.1.1.6.1.4.60 (Integer): 2;
 [3] private.enterprises.cisco.ciscoMgmt.43.1.1.6.1.5.60 (Integer): 3;
1 .1.3.6.1.4.1.9.9.43.2.0.1 0
```

got mibs?

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

SNMP Traps/Notifications and Informs

SNMP Trap Example With MIB Loaded into NMS

A little more clearer!

```
988754041 1 Tue May 01 17:54:01 2001 192.168.100.5
- ciscoConfigManEvent received from enterprise
ciscoConfigManMIBNotificationPrefix with
 3 arguments:
ccmHistoryEventCommandSource=commandLine;
ccmHistoryEventConfigSource=commandSource;
ccmHistoryEventConfigDestination=running;
1 .1.3.6.1.4.1.9.9.43.2.0.1 0
```

Highlighting Added

Logging—SNMP Notifications

Catalyst OS SNMP Trap Receiver Configuration Example

Syntax:

- set snmp trap {enable | disable} [all | auth | bridge | chassis | config | entity | ippermit | module | repeater | stpx | syslog | vmps | vtp]
- set snmp trap rcvr_addr rcvr_community

```
set snmp trap enable all
set snmp trap 192.168.1.25 public
```

SNMPv3 Notifications

What About Traps/Informs as in v1/v2c?

- CatOS (6.3)

```
set snmp user notifyuser authentication md5 authpassword volatile
set snmp group notifygroup user notifyuser security-model v3
 volatile
set snmp access notifygroup security-model v3 notify
 defaultAdminView
set snmp notify snmpV3Trap tag V3Trap trap volatile
set snmp targetparams par1 user notifyuser security-model v3
 message-processing v3 authentication volatile
set snmp targetaddr addr1 param par1 192.168.1.11 udpport 162
 udpmask 0 volatile taglist V3Trap
```

Logging—Syslog

- Setting logging history level to “notifications/5” is a good start
- Set lower, to “informational/6” if you aren’t getting the messages you need

CatOS:

```
SwitchA> (enable) set logging server 192.168.1.25
SwitchA> (enable) set logging server 192.168.33.17
SwitchA> (enable) set logging severity 5
SwitchA> (enable) set logging server enable
SwitchA> (enable) set logging timestamp enable
SwitchA> (enable) set logging console disable
SwitchA) (enable) set logging telnet disable
```

CISCO

TOMORROW starts here.