Praktické IOS nástroje pro (nejen) každodenní úkoly

T-SDN3 / L2

Radek Boch, CCIE# 7095, Systems Engineer, Cisco
rboch@cisco.com
Cisco Open Network Environment – ONE

Preserve What is Working
- Resilience, Scale, Security
- Functionality and Rich Features
- Instrumentation

Evolve for New Requirements
- Operational Simplicity and Automations
- Programmability and Network-Awareness
- Upcoming Innovations

Open and Integrated Framework
- Software Defined Network concepts are a component of the Open Network Environment
- Existing APIs, Agents, Controllers and Infrastructure contribute

Open Network Environment

<table>
<thead>
<tr>
<th>Network Programming</th>
<th>(Software) Architectures and Patterns</th>
<th>Deployment and Virtualization</th>
</tr>
</thead>
<tbody>
<tr>
<td>onePK</td>
<td>Controllers (ONE/Openflow PoC)</td>
<td>Nexus 1000v</td>
</tr>
<tr>
<td>developer.cisco.com, CDN, Training, Certification, Partners, EEM, EASy</td>
<td>(SBC, WLC, ++++)</td>
<td>CSR 1000v</td>
</tr>
<tr>
<td></td>
<td>CIN, CloudConnect, Sentinels, Agents</td>
<td>VSG and vFW/ASA, vWAAS, vNAM, ...</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco Openstack Ed</td>
</tr>
</tbody>
</table>

Blade Hosting (UCS-E, ...), Virtual Containers (AirVision, Cat, ISR, ASR, ...)

Scenarios and Motivations
### Device Manageability Instrumentation

#### Fault
- IP OAM—Ping, Trace, BFD, ISG per session
- 802.3ah—Link monitoring and remote fault indication
- 802.1ag—Continuity check, L2 ping, trace, AIS
- MPLS OAM—LSP ping, LSP trace, VCCV
- EEM—Embedded Event Manager
- EVENT-MIB—OID-based triggers, events, or SNMP Set, IETF DISMON
- EXPRESSION-MIB—OID expression-based triggers, IETF DISMON
- ...

#### Configuration
- Config CLI—diff, logging, lock, replace, rollback
- E-LMI—parameter and status signaling
- E-DI—Enhanced Device Interface, CLI, Perl, IETF Netconf
- EMM—Embedded Menu Manager
- NETCONF—IETF NETCONF XML PI
- CNS and WSMA
- TR-069
- KRON—command scheduler
- AutoInstall—bootstrapping
- IOS.sh—IOS Shell
- SmartInstall
- Auto SmartPorts
- ...

#### Performance
- Auto IP SLA—delay, jitter, loss probability
- CBQoS MIB—class-based QoS
- NBAR
- RMON
- EPC—Embedded Packet Capture
- ERM—Embedded Resource Manager
- GOLD—Generic Online Diagnosis
- Smart Call Home—preventive maintenance
- VidMon—Video Monitoring
- ...

#### Accounting
- Flexible NetFlow—IETF IPFIX
- BGP policy accounting—includes AS information
- Periodic MIB bulk data collection and transfer
- ...

#### Security
- Auto Secure—one-touch device hardening
- LDP Auth—message authentication
- Routing Auth—MD5 authentication, BGP, OSPF
- ...

---

Cisco IOS® Device Manageability Instrumentation (DMI)

Device Manageability Instrumentation Has Evolved Significantly

© 2013 Cisco and/or its affiliates. All rights reserved.
Embedded Event Manager (EEM)

**Actions**

- Syslog
- email notification
- SNMP set Counter
- SNMP get
- SNMP notification
- Reload or switch-over
- Application specific
- CLI Applets
- IOS.sh Policies
- TCL Policies

**EEM Applets**

- multi-event-correlation

**Event Detectors**

- Syslog ED
- SNMP EDs
- Timer EDs
- none ED
- HW EDs
- Watchdog ED
- Interface Counter ED
- XML RPC ED
- CLI ED
- OIR ED
- ERM ED
- EOT ED
- RF ED
- GOLD ED
- NetFlow ED
- IPSLA ED
- Route ED
- CDP LLDP ED
- 802.1x ED
- MAC ED

**Syslog Event**

- Remote:
  - Notification
  - Local:
  - Notification
  - Get/Set
- Cron
- Count down

**Event Detectors**

- Fan
- Temp
- Env
- ...
Packaging Embedded Automations

**Problem:** Cisco IOS Embedded Automation Systems often include multiple configuration items, files, checks and procedures.

**Solution:** Cisco EASy provides a simple packaging mechanism and open-source EASy Installer. A developer guide is available online to assist with the creation of EASy packages.

- Package Description
- Pre-Requisite Verification
- Pre-Installation Config
- Pre-Installation Exec
- Environment Variables
- Configuration
- Files
- Post-Requisite Verification
- Post-Installation Config
- Post-Installation Exec
- Uninstall

```
EASy Installer + MyPackage.tar
```

```
Router# easy-installer tftp://10.1.1.1/mypackage.tar flash:/easy
Configure and Install EASy Package 'mypackage-1.03'

1. Display Package Description
2. Configure Package Parameters
3. Deploy Package Policies
4. Exit

Enter option: 2
```

See: [http://www.cisco.com/go/easy](http://www.cisco.com/go/easy)
Monitoring
Troubleshooting
Configuration
Getting Started with MIBs
Where to start with MIBs?

MIB Locator: http://www.cisco.com/go/mibs

SNMP Object Navigator: http://www.cisco.com/go/mibs
Which OIDs are actually being used?

Example: CiscoView polling

```
Router#show snmp statistics oid

time-stamp         #of times requested  OID
16:16:50 CET Jan 12 2005  97  sysUpTime
16:16:50 CET Jan 12 2005  9  cardTableEntry.7
16:16:50 CET Jan 12 2005  9  cardTableEntry.1
16:16:50 CET Jan 12 2005  4  cardTableEntry.9
16:16:50 CET Jan 12 2005  16  ifAdminStatus
16:16:50 CET Jan 12 2005  16  ifOperStatus
16:16:50 CET Jan 12 2005  6  ciscoEnvMonSupplyStatusEntry.3
16:16:50 CET Jan 12 2005  17  ciscoFlashDeviceEntry.2
16:16:50 CET Jan 12 2005  8  ciscoFlashDeviceEntry.10
16:16:50 CET Jan 12 2005  2  ltsLineEntry.1
16:16:50 CET Jan 12 2005  2  chassis.15
16:16:27 CET Jan 12 2005  11  ciscoFlashDeviceEntry.7
16:16:27 CET Jan 12 2005  2  cardIfIndexEntry.5
16:16:24 CET Jan 12 2005  1  ciscoFlashDevice.1
```

Available from: IOS 12.0(22)S, 12.4(20)T
MIB Persistence

Now there is a show command:

```bash
Router# show snmp mib ifmib ifindex
    Ethernet0/0: Ifindex = 1
    Loopback0: Ifindex = 39
    Null0: Ifindex = 6
    :

Router# snmp mib ifmib ifindex loopback 0
    Loopback0: Ifindex = 39
```

Introduced in 12.0(7)S, 12.2(2)T

If only the wrong OIDs exist – Event and Expression MIB
Example: Expression- & Event-MIB

- Simple capacity planning example: if my link utilization is above 50% for an hour, it’s time to upgrade the link
- Steps:
  1. Create an Expression
     Utilization = (Δ ifInOctets + Δ ifOutOctets) * 8 * 100 / hour / ifSpeed
  2. Create an Event
     If utilization > 50% → generate an Event
Example: Expression- & Event-MIB

- Simple capacity planning example: Calculate link utilization on all the interfaces in the router

```plaintext
Router# show running | beg expression
snmp mib expression owner administrator name exp3
  expression ($1*800)/$2
  enable
  object 1
    id ifInOctets
    wildcard
  object 2
    id ifSpeed
    wildcard

NMS% snmpwalk -c public -v 2c <router> expValueCounter32Val
SNMPv2-SMI:: expValueCounter32Val.7.109.97.114.105.115.111.108.4.101.120.112.51.0.0.1 = Counter32: 214800
SNMPv2-SMI:: expValueCounter32Val.7.109.97.114.105.115.111.108.4.101.120.112.51.0.0.2 = Counter32: 0
SNMPv2-SMI:: expValueCounter32Val.7.109.97.114.105.111.108.4.101.120.112.51.0.0.4 = Counter32: 0
SNMPv2-SMI:: expValueCounter32Val.7.109.97.114.105.111.108.4.101.120.112.51.0.0.5 = Counter32: 0
```
If the OID doesn’t exist – Custom MIB
Problem: Sometimes there is a show command – but no MIB support. What if we still want to collect the Information via SNMP?

Solution: Automate Custom MIB Polling via EEM and Expression-MIB or RFC2982-MIB depending on Cisco IOS Version

See: Available as an EASy Package: http://www.cisco.com/go/easy
Scripts for ASR available from CiscoBeyond
Verifying the Monitoring Config – EASy NMS Tester Package
Is Monitoring Actually Working?

**Problem:** Monitoring relies on a number of protocols to be configured and functional end-to-end, not just on the local node.

**Solution:** Use the EASy NMS Tester Package – which generates test messages for each configured monitoring protocol

1) Install and Configure EASy NMS Tester Package

2) NMS Tester Package will generate Test Messages

3) Verify Test Messages

Monitoring Remote Information
Receive Remote Information

**Problem:** Sometimes we want to receive remote information on a Router / Switch and be able to react to it locally – for example a notification from a UPS System.

**Solution:** Use Network Automation based on Cisco IOS Embedded Event Manager leveraging the EEM SNMP Notification Event Detector

- Router / Switch can received SNMP Notifications
- Execute (trigger) EEM Policy to take local action
- Policy can query varbind info
- Supports Incoming or Outgoing Notifications
- Outgoing only for locally generated Notifications

```bash
Router(config)# event manager applet catch-a-trap
router(config-applet)# description test snmp notification unmanaged service
router(config-applet)# event snmp-notification oid 1.3.6.1.6.3.1.1.4.1.0
             oid-val "1.3.6.1.6.3.1.1.5.3" op eq src-ip-address 10.51.89.176
direction incoming
router(config-applet)# action 010 ...
routing(config-applet)# action 020 ...
```
Format and Share Information
Format and Share Remote Information

**Problem:** How to actively gather and share information from a router and from a few devices behind the router – across organizational and technical borders?

**Solution 1:** Initiate a project to make use of SNMP, Syslog, Event Management Software, Reporting, Provisioning and CRM Systems ...

**Solution 2:** Use Cisco IOS Network Automation to collect and post the information

Using Cisco IOS Embedded Event Manager and Tcl:

1. Import the http package into EEM policy
   ```tcl
   namespace import ::http::*
   ```

2. Collect the information required

3. Build a query for the http POST operation
   ```tcl
   set my_query [::http::formatQuery "status" $my_info]
   ```

4. POST the information to a website
   ```tcl
   set my_reply [::http::geturl $my_server_url -query $my_query]
   ```
Traffic Flows – Flexible Netflow and EEM
Flexible NetFlow (FNF) – Recap

- Top N talkers
- MAC, interface, VLAN
- 80+ Key Fields
- 14 Non-Key fields

Key Fields
- Packet 1
  - Source IP: 3.3.3.3
  - Destination IP: 2.2.2.2
  - Source Port: 23
  - Destination Port: 22078
  - Layer 3 Protocol: TCP - 6
  - TOS Byte: 0
  - Input Interface: Ethernet 0

Non-Key Fields
- Packet 1
  - Source IP: 3.3.3.3
  - Destination IP: 2.2.2.2
  - Source Port: 23
  - Destination Port: 22078
  - Layer 3 Protocol: TCP - 6
  - TOS Byte: 0
  - Input Interface: Ethernet 0

Traffic Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Source Port</th>
<th>Dest. Port</th>
<th>Protocol</th>
<th>TOS</th>
<th>Input I/F</th>
<th>...</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>23</td>
<td>22078</td>
<td>6</td>
<td>0</td>
<td>E0</td>
<td></td>
<td>1100</td>
</tr>
</tbody>
</table>

Security Analysis Cache

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>Input I/F</th>
<th>Flag</th>
<th>...</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.3</td>
<td>2.2.2.2</td>
<td>E0</td>
<td>0</td>
<td></td>
<td>11000</td>
</tr>
</tbody>
</table>
## Flexible NetFlow (FNF) – Key Fields – 1/2

<table>
<thead>
<tr>
<th>Flow</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampler ID</td>
<td>IP (Source or Destination)</td>
<td>IP (Source or Destination)</td>
</tr>
<tr>
<td>Direction</td>
<td>Payload Size</td>
<td>Payload Size</td>
</tr>
<tr>
<td>Interface</td>
<td>Prefix (Source or Destination)</td>
<td>Prefix (Source or Destination)</td>
</tr>
<tr>
<td>Input</td>
<td>Packet Section (Header)</td>
<td>Packet Section (Header)</td>
</tr>
<tr>
<td>Output</td>
<td>Mask (Source or Destination)</td>
<td>Mask (Source or Destination)</td>
</tr>
<tr>
<td>Payload Section (Payload)</td>
<td>Packet Section (Payload)</td>
<td>Packet Section (Payload)</td>
</tr>
<tr>
<td>Minimum-Mask (Source or Destination)</td>
<td>TTL</td>
<td>DSCP</td>
</tr>
<tr>
<td>Source VLAN</td>
<td>Protocol</td>
<td>Protocol</td>
</tr>
<tr>
<td>Dest VLAN</td>
<td>Options bitmap</td>
<td>Extension Headers</td>
</tr>
<tr>
<td>Dot1q VLAN</td>
<td>Version</td>
<td>Traffic Class</td>
</tr>
<tr>
<td>Dot1q priority</td>
<td>Precedence</td>
<td>Hop-Limit</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>Identification</td>
<td>Flow Label</td>
</tr>
<tr>
<td>Dest VLAN</td>
<td>DSCP</td>
<td>Length</td>
</tr>
<tr>
<td>Dot1q VLAN</td>
<td>Header Length</td>
<td>Option Header</td>
</tr>
<tr>
<td>Source MAC address</td>
<td>TOS</td>
<td>Next-header</td>
</tr>
<tr>
<td>Destination MAC address</td>
<td>Payload Length</td>
<td>Header Length</td>
</tr>
<tr>
<td>Total Length</td>
<td>Version</td>
<td>payload Length</td>
</tr>
</tbody>
</table>
## Flexible NetFlow (FNF) – Key Fields – 2/2

<table>
<thead>
<tr>
<th><strong>Routing</strong></th>
<th><strong>Transport</strong></th>
<th><strong>Application</strong></th>
<th><strong>Multicast</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>src or dest AS</td>
<td>Destination Port</td>
<td>TCP Flag: ACK</td>
<td>Replication Factor*</td>
</tr>
<tr>
<td>Peer AS</td>
<td>Source Port</td>
<td>TCP Flag: CWR</td>
<td>RPF Check Drop*</td>
</tr>
<tr>
<td>Traffic Index</td>
<td>ICMP Code</td>
<td>TCP Flag: ECE</td>
<td>Is-Multicast</td>
</tr>
<tr>
<td>Forwarding Status</td>
<td>ICMP Type</td>
<td>TCP Flag: FIN</td>
<td></td>
</tr>
<tr>
<td>IGP Next Hop</td>
<td>IGMP Type*</td>
<td>TCP Flag: PSH</td>
<td></td>
</tr>
<tr>
<td>BGP Next Hop</td>
<td>TCP ACK Number</td>
<td>TCP Flag: RST</td>
<td></td>
</tr>
<tr>
<td><strong>Input VRF Name</strong></td>
<td>TCP Header Length</td>
<td>TCP Flag: SYN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Sequence Number</td>
<td>TCP Flag: URG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Window-Size</td>
<td>UDP Message Length</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Source Port</td>
<td>UDP Source Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Destination Port</td>
<td>UDP Destination Port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP Urgent Pointer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* IPv4 Flow only
Flexible NetFlow (FNF) – Configuration

1. Configure the Exporter

   Router(config)# flow exporter my-exporter

   Router(config-flow-exporter)# destination 1.1.1.1

2. Configure the Flow Record

   Router(config)# flow record my-record

   Router(config-flow-record)# match ipv4 destination address

   Router(config-flow-record)# match ipv4 source address

   Router(config-flow-record)# collect counter bytes

3. Configure the Flow Monitor

   Router(config)# flow monitor my-monitor

   Router(config-flow-monitor)# exporter my-exporter

   Router(config-flow-monitor)# record my-record

4. Apply to an Interface

   Router(config)# interface s3/0

   Router(config-if)# ip flow monitor my-monitor input
**Flexible NetFlow (FNF) – Top Talkers**

- Top ten IP addresses that are sending the most packets
  
  ```
  Router# show flow monitor <monitor> cache
  aggregate ipv4 source address
  sort highest counter bytes top 10
  ```

- Top five destination addresses to which we're routing most traffic from the 10.10.10.0/24 prefix
  
  ```
  Router# show flow monitor <monitor> cache
  filter ipv4 destination address 10.10.10.0/24
  aggregate ipv4 destination address
  sort highest counter bytes top 5
  ```

- 5 VLAN's that we're sending the least bytes to:
  
  ```
  Router# show flow monitor <monitor> cache
  aggregate datalink dot1q vlan output
  sort lowest counter bytes top 5
  ```

- Top 20 sources of 1-packet flows:
  
  ```
  Router# show flow monitor <monitor> cache
  filter counter packet 1
  aggregate ipv4 source address
  sort highest flow packet top 20
  ```
Problem: We want to know about low-TTL traffic

Solution: Use Flexible Netflow and Embedded Event Manager 3.0 to detect traffic flows with TTL < 5

1. Configure flexible Netflow to match on TTL, Source- and Destination Address

```
flow record <my-record>
match ipv4 ttl
match ipv4 source address
match ipv4 destination address
:
flow monitor <my-monitor>
record <my-record>
:
```

2. Configure the Netflow Event Detector in EEM to notify upon a new flow record

```
event manager applet my-ttl-applet
  event nf monitor-name "my-ttl-monitor" event-type create event1
  entry-value "5" field ipv4 ttl entry-op lt
  action 1.0 syslog msg "Low-TTL flow from $_nf_source_address"
```

3. Syslog message and/or use show flow monitor <my-monitor> cache command

```
```
Dynamic SLAs – Using IPSLA and EEM
Dynamic SLAs and Custom High Availability

**Problem:** Define – Monitor – Alert was yesterday. Today’s SLAs often require preventive, mitigating or optimizing actions to happen automatically.

**Solution I:** Use configurable point features where available

**Solution II:** Use EEM with a generic Event Detector

**Solution III:** Use EEM with a specific Event Detector

**Solution IV:** Use onePK to program for external dynamic metrics and/or algorithms
**Example: Custom Failover Scenarios**

**Problem:** Upon a standby ASA deciding to become active, we want to force full cluster failover by shutting down all ASA-facing interfaces on the other cluster’s switch.

**Solution:** use EEM SNMP Event Detector

```
::cisco::eem::event_register_snmp_notification oid 1.3.6.1.4.1.9.9.41.1.2.3.1.5.0 oid_val 0 op ne
```

On active cluster switches
If we are in HSRP 'Active' state && sender is a secondary ASA going to active {
    For each ASA-facing interface {
        shut
    }
}
Custom HA – EASy Package

Embedded Automation Systems (EASy)

Custom HA EASy Package provides:

• Primary/Backup Link Failover
• Based on IP SLA Metric
• Open Source Tutorial/Framework

To use the Package:

1. Browse and Download EASy Package
   www.cisco.com/go/easy
2. Make Sure to also download EASy Installer
3. Watch VOD and/or read documentation
   www.cisco.com/go/easy
4. Customize and tailor to your needs
5. Install and Use
Monitoring

Troubleshooting

Configuration
“Troubleshooting starts before Troubleshooting starts “

Source unknown
Reliable Delivery and Filtering of Syslog
Reliable Delivery and Filtering of Syslog

**Problem:** Syslog uses UDP, rate-limiting is recommended practice – according to Murphy – which messages will you lose first?

**Solution:** Make use of Reliable Delivery and Filtering

- RFC 3195: **Reliable** and **secure** delivery for syslog messages via Blocks Extensible Exchange Protocol (BEEP)
- IOS provides a **filtering** mechanism per syslog session, called a message discriminator as well as a **rate-limiter** per syslog session
- Integrated in 12.4(11)T, even if the BEEP framework was supported for quite some time, 12.4(2)T

```plaintext
Router(config)# logging discriminator filter1 severity includes 0,1,2,3 rate-limit 10000
Router(config)# logging discriminator filter2 severity includes 4,5,6,7 rate-limit 100
Router(config)# logging discriminator filter3 msg-body includes debug includes facility OSPF
Router(config)# logging trap debugging
Router(config)# logging host <production> transport beep discriminator filter1
Router(config)# logging host <production> transport udp port 1471 discriminator filter2
Router(config)# logging host <troubleshooting> discriminator filter3
```

BEEP capable Syslog servers: [http://www.syslog.cc/ietf/rfc3195.html](http://www.syslog.cc/ietf/rfc3195.html)
ACL Syslog Correlation

Problem: ACL hits can produce a Syslog message – but often in the NOC or SOC we want to know which specific line of an ACL (i.e., ACE – Access Control Entry) was kicking-in ...

Solution: Make use of IOS ACL Tags and Syslog Correlation

1. Define Tags for your ACEs:
   ```
   ip access-list extended access-control
   permit ip any host 10.10.10.100 log red-server
   permit ip any host 10.10.10.200 log blue-server
   permit ip any any
   ```

2. Tags will be appended to Syslog Messages:
   ```
   *Apr 13 16:31:18.958: %SEC-6-IPACCESSLOGDP: list access-control permitted
   icmp 192.168.1.100 -> 10.10.10.100 (0/0), 11 packets [ red-server ]
   *Apr 13 16:32:18.953: %SEC-6-IPACCESSLOGDP: list access-control permitted
   icmp 192.168.1.100 -> 10.10.10.200 (0/0), 3 packets [ blue-server ]
   ```

Available from: IOS 12.4(22)T
Platforms: 18xx, 28xx, 38xx, 72xx, 73xx, 76xx
ACL Syslog Correlation and EEM

**Problem:** Let's assume we not only need a syslog message, but also want to take specific actions...

**Solution:** Combine ACL Syslog Correlation with EEM

1. Define Tags for your ACEs:

   ```
   access-list 100
   deny tcp host 10.0.2.2 host 10.0.2.181 eq 9000 log ThisIsBlocked
   permit ip any any
   ```

2. Define an EEM Applet to match the Tag and take action:

   ```
   event manager applet catch-an-ace-tag
   event syslog pattern "ThisIsBlocked"
   action 1.0 syslog priority emergencies msg "Start... "
   Your Actions Here
   action 9.0 syslog priority emergencies msg "... done"
   ```

3. A matching packet will generate a syslog message, which will in turn trigger EEM:

   ```
   *Apr 13 16:58:06.386: %SEC-6-IPACCESSLOGDP: list 100 denied tcp
   10.0.2.2(56273) 10.0.2.181(9000), 1 packet [ThisIsBlocked]
   *Apr 13 16:58:06.394 UTC: %HA_EM-0-LOG: catch-an-ace-tag: Start ...
   *Apr 13 16:58:07.025 UTC: %HA_EM-0-LOG: catch-an-ace-tag: ... done
   ```
Quickly export SNMP Statistics – using Bulk File MIB
Quickly export SNMP Statistics?

**Problem:** Sometimes we need data from one or multiple MIBs, but
- we may not want to (re-)configure an NMS
- don’t want to constantly poll
- need to gather data during temporary loss of connectivity

**Solution:** Use Bulk File MIB to define the data we need and periodically transfer it to a convenient location
- group data from multiple MIBs
- single, common polling interval
- buffer data
- transfer using RCP, FTP, TFTP
- format ASCII or Binary

Feature Name: Periodic MIB Data Collection and Transfer Mechanism

**Available from:** IOS 12.0(24)S, 12.2(25)S, 12.3(2)T, IOS XE 2.1, IOS XR 3.2
**Platforms:** ASR1k, x8xx ISR, x900x ISR, 72xx, 73xx, 76xx, 10xxx, ME3400, C4k, C6k, ...
**See:** [http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.2.1.2](http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.2.1.2)
Configuration – Example

1. Define Lists of relevant OIDs (Names for IF-MIB, ASN.1 for all others)

   ```
   Router(config)# snmp mib bulkstat object-list my-if-data
   Router(config-bulk-objects)# add ifIndex
   Router(config-bulk-objects)# add ifDescr
   Router(config-bulk-objects)# add ifAdminStatus
   Router(config-bulk-objects)# add ifOperStatus
   Router(config-bulk-objects)# exit
   ```

2. Specify Polling Schema

   ```
   Router(config)# snmp mib bulkstat schema my-if-schema
   Router(config-bulk-sc)# object-list my-if-data
   Router(config-bulk-sc)# poll-interval 1
   Router(config-bulk-sc)# instance exact interface FastEthernet0
   Router(config-bulk-sc)# exit
   ```

3. Configure the Transfer Mechanism – and enable it!

   ```
   Router(config)# snmp mib bulkstat transfer my-fa0-transfer
   Router(config-bulk-tr)# schema my-if-schema
   Router(config-bulk-tr)# transfer-interval 5
   Router(config-bulk-tr)# url primary tftp://10.10.10.10/folder/
   Router(config-bulk-tr)# retain 30
   Router(config-bulk-tr)# buffer-size 4096
   Router(config-bulk-tr)# enable
   ```
Local Logging for Syslog and SNMP
Local Logging

Problem: When an NMS is not available, we may need to log events locally on the IOS node. Syslog provides several options to do this:

logging buffered [discriminator descr-name] [buffer-size] [severity-level]
logging history [severity-level-name | severity-level-number]
logging persistent [batch batch-size] [filesize logging-file-size] ...

But what about SNMP?

Solution: Use the EASy Trap Logger Package – which enables SNMP logging into a local ASCII file

c1812-easy#more flash:/traplog

Thu Sep 23 13:54:16 UTC 2010: OID: 1.3.6.1.4.1.9.9.43.2.0.1 VARBINDS:
1.3.6.1.4.1.9.9.43.1.1.6.1.4.10=2, 1.3.6.1.6.3.1.1.4.1.0=ciscoConfigManMIB.2.0.1,
1.3.6.1.4.1.9.9.43.1.1.6.1.3.10=1, 1.3.6.1.4.1.9.9.43.1.1.6.1.5.10=3, 1.3.6.1.2.1.1.3.0=90317

Thu Sep 23 13:54:16 UTC 2010: OID: 1.3.6.1.4.1.9.9.43.2.0.1 VARBINDS:
1.3.6.1.4.1.9.9.43.1.1.6.1.4.10=2, 1.3.6.1.6.3.1.1.4.1.0=ciscoConfigManMIB.2.0.1,
1.3.6.1.4.1.9.9.43.1.1.6.1.3.10=1, 1.3.6.1.4.1.9.9.43.1.1.6.1.5.10=3, 1.3.6.1.2.1.1.3.0=90317

See: Available as an EASy Package:
http://www.cisco.com/go/easy
Verify Resource Utilization – using ERM
Embedded Resource Manager (ERM)

- The ERM framework tracks resource depletion and resource dependencies across processes and within a system
- Monitor thresholds for CPU, buffer, and/or memory
- For system or line card
- ERM can define “group”, i.e. group of different CPU processes
- CISCO-ERM-MIB
- Interface into EEM

Available from: IOS 12.2(33)SRB, 12.4(15)T
Platforms: UC520, 800, x8xx ISR, x900x ISR, 65xx, 72xx, 73xx, 75xx, 76xx, 10xxx
Monitoring Multiple Processes

Problem: In order to detect resource consumption caused by brute force login attempts, we want to keep an eye on CPU utilization by the login processes.

Solution: Define an ERM policy to notify upon critical / suspicious levels.

```
resource policy
  policy my-login-policy type iosprocess
  system
    cpu process
      critical rising 30 interval 10 falling 20 interval 10
      major rising 20 interval 10 falling 10 interval 10
      minor rising 10 interval 10 falling 5 interval 10
  user group my-login-group type iosprocess
    instance "SSH Process"
    instance "SSH Event handler"

  : policy my-login-policy
```

→ Syslog if Group CPU Usage Count Rises Above 10% at an Interval of 10s

*Aug 25 12:56:26.089: %SYS-4-CPURESISING: Resource group my-login-group is seeing local cpu util 16% at process level more than the configured minor limit 10%

*Aug 25 12:56:41.089: %SYS-6-CPURESFALLING: Resource group my-login-group is no longer seeing local high cpu at process level for the configured minor limit 10%, current value 0%
Verify Resource Utilization – using ERM, EEM and onePK
Managed Network Use Case – Monitor Memory Usage

- **Problem**: What if we need to dynamically investigate further upon a resource symptom?
- **Solution**: Use the integration of EEM + ERM to trigger an EEM event when processor memory is greater than 80%.

```resource policy
policy critmem global
  system
  memory processor
critical rising 80 interval 5
user global critmem
```

```event manager applet totmemcheck
  event resource policy critmem
  action 100 mail server "<server>" to "<to>" from "<from>" subject "Warning: proc memory spike"
```
A Network “Top”

- Use onePK to build a live process monitor similar to UNIX *top*
- The same app can connect to multiple devices to display the top processes across the entire network
Capturing Packets – EPC
### Embedded Packet Capture (EPC)

**Problem:** Sometimes a Packet Capture would be useful for Troubleshooting, BUT: deploying Packet Sniffers is slow, expensive and requires local skills and equipment ...

**Solution:** Make use of IOS Embedded Packet Capture to capture PCAP format data and/or analyze on the device

1. Defining a capture buffer on the device
   ```
   Router# monitor capture buffer ...
   ```

2. Defining a capture point
   ```
   Router# monitor capture point ...
   ```

3. Associate capture point to buffer
   ```
   Router# monitor capture point associate ...
   ```

4. Start / Stop capture points
   ```
   Router# monitor capture point start ...
   ```

5. Show and/or Export the content of the buffer
   ```
   Router# monitor capture buffer <tracename> export
   ```

See: [http://www.cisco.com/go/epc](http://www.cisco.com/go/epc)
Available from: IOS 12.4(20)T
Platforms: 8xx, 18xx, 28xx, 38xx ISRs, ISR G2s, 72xx
Capturing Packets – EPC and EEM
EPC and Transient Issues

**Problem:** You Are Seeing VPN Tunnel Drops on Your VPN Head-End Router at 3:00 AM Every Day. You Need to Analyze the Traffic on the Wire at That Time.

**Solution:** Combine EPC and Embedded Event Manager (EEM)

1) Define EPC with a circular buffer

```
Router# monitor capture point ip cef cappnt Serial2/0 both
Router# monitor capture buffer capbuf size 512 max-size 1518 circular
Router# monitor capture point associate cappnt capbuf
```

2) Use EEM Timer Event Detector to automatically start capturing at 2:55 AM

```
::cisco::eem::event_register_timer cron cron_entry "55 2 * * *"
namespace import ::cisco::eem::*
namespace import ::cisco::lib::*
if { [catch {cli_open} result] } {
    error "Failed to open CLI session: '$result'" $errorInfo
} 
array set cliarr $result
if { [catch {cli_exec $cliarr(fd) "enable"} result] } {
    error "Failed to enable CLI session: '$result'" $errorInfo
}
if { [catch{cli_exec $cliarr(fd) "monitor capture point start cappnt"} result]}{
    error "Failed to start packet capture: '$result'" $errorInfo
}
catch {cli_close $cliarr(fd) $cliarr(tty_id)} result
```

3) Use EEM Syslog Event Detector to stop capturing upon transient issue

```
::cisco::eem::event_register_syslog pattern "\%CRYPTO-4-RECVD_PKT_MAC_ERR:"
if { [catch {cli_exec $cliarr(fd)"monitor capture point stop cappnt"} result]}{
    error "Failed to stop packet capture: '$result'" $errorInfo
}
```

Capturing Packets – Packet Analysis
EPC – Capture Analysis on the CLI

IOS natively does NOT provide further Capture Analysis

However, it is possible to decode PCAP headers on the CLI

- Using the enhanced EEM CLI Event Detector, you can extend the built-in EPC CLI to decode captures directly on the device


```
Router# show monitor capture buffer capbuf decode
01:27:54.285 EDT Oct 11 2010 : IPv6 CEF : Fa0/0 None
IPv6:
  Dest MAC : 00:10:14:33:D4:00    Src MAC : 00:17:08:5A:1B:16
  Dest IP  : 2003:a00::2          Src IP  : 2003:a00::1

01:27:54.285 EDT Oct 11 2010 : IPv6 CEF : Fa0/0 None
IPv6:
  Dest MAC : 00:10:14:33:D4:00    Src MAC : 00:17:08:5A:1B:16
  Dest IP  : 2003:a00::2          Src IP  : 2003:a00::1
```
EPC – Capture Export

- EPC Capture Buffer is just a normal .pcap format file
- EPC provides an export command
  ```
  Router# monitor capture buffer my-buffer export tftp://10.10.10.10/mypcap
  ```
- Alternatively: combine with EEM to email, copy, export automatically

NAM 5.0 and later provides:
- Packet trace analysis highlighting observed protocol/packet level anomalies
- One-click targeted packet captures
- Smart analysis of packet capture
- Combined application visibility, traffic analysis
Early Detection – GOLD
POST (Power-On Self-Test) is great ...

... but some errors you prefer to know while the system is up and running ...

... and: can you afford to power-cycle after OIR just for POST to run?
Generic Online Diagnostics (GOLD) – 1/3

**Problem:** How to detect wear and tear issues before they cause an outage? Hardware aging as well as repeated insertion and removal of modules can lead to wear and tear damage on connectors. This can cause failures – how do you find out during operation, without power-cycling the box?

**Solution:** Use GOLD to verify functionality of a mis-behaving module

- Bootup Diagnostics (upon bootup and OIR)
- Periodic Health Monitoring (during operation)
- OnDemand (from CLI)
- Scheduled Testing (from CLI)
- Test Types include:
  - Packet switching tests
  - Memory Tests
  - Error Correlation Tests
- Complementary to POST

**Available from:** CatOS 8.5(1), IOS 12.2(14)SX

**Platforms:** CBS 3xxx, Cat 3560, 3750, 6500, ME6524, 72xx, 10k, CRS
1) Let’s see which GOLD tests are available and scheduled for our Module:

```
Router# show diagnostic content module 3
Module 3:

Diagnostics test suite attributes:
  M/C/* - Minimal level test / Complete level test / Not applicable
  B/* - Bypass bootup test / Not applicable
  P/* - Per port test / Not applicable
  D/N/* - Disruptive test / Non-disruptive test/ Not applicable
  S/* - Only applicable to standby unit / Not applicable
  X/* - Not a health monitoring test / Not applicable
  F/* - Fixed monitoring interval test / Not applicable
  E/* - Always enabled monitoring test / Not applicable
  A/I - Monitoring is active / Monitoring is inactive

<table>
<thead>
<tr>
<th>ID</th>
<th>Test Name</th>
<th>Attributes</th>
<th>(day hh:mm:ss.ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TestScratchRegister</td>
<td><em>B</em>N****A</td>
<td>000 00:00:30.00</td>
</tr>
<tr>
<td>2</td>
<td>TestSPRPInbandPing</td>
<td><em>B</em>N****A</td>
<td>000 00:00:15.00</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>TestL3VlanMet</td>
<td>M**N****I</td>
<td>not configured</td>
</tr>
</tbody>
</table>
```
2) Now let's run TestL3VlanMet on-demand for Module 3:

```
Router# diagnostic start module 3 test 18
00:09:59: %DIAG-SP-3-MINOR: Module 3: Online Diagnostics detected a Minor Error. Please use 'show diagnostic result <target>' to see test results.
```

3) Then check the test results:

```
Router# show diagnostic result module 3
Module 3: CEF720 48 port 1000mb SFP SerialNo : xxxxxxxx

Overall Diagnostic Result for Module 3 : MINOR ERROR
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)
1) TestTransceiverIntegrity:
   Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
   --------------------------------------------------
      U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U

   Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
   --------------------------------------------------
      U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U

: :
18) TestL3VlanMet ------------------------> F
```
Early Detection and Mitigation – using GOLD and EEM
Problem: How to initiate preventive Maintenance in a HA Environment?

Solution 1: Manually change topology after a low priority Syslog warning has been seen (and understood)

Solution 2: Use Cisco IOS Network Automation to schedule a HSRP failover upon GOLD hardware diagnostics result

1. Cisco IOS Generic Online Diagnostics (GOLD) detects a potential hardware problem

2. GOLD Event is detected by Embedded Event Manager (EEM) – which schedules an HSRP Failover upon next maintenance window

3. HSRP Failover to Standby node

4. Preventive maintenance / replacement activity can now take place on Primary node
CLI ‘Safety’ and Quality Features

- **Contextual configuration diff utility** (from 12.3(4)T, 12.2(25)S)
  - Easily show differences between running and startup configuration
  - Compare any two configuration files

- **Config change logging and notification** (from 12.3(4)T, 12.2(25)S)
  - Tracks config commands entered per user, per session
  - Notification sent indicating config change has taken place—changes can be retrieved via SNMP

- **Configuration replace and rollback** (from 12.3(7)T, 12.2(25)S)
  - Replace running config with any saved configuration (only the diffs are applied) to return to previous state
  - Automatically save configs locally or off box
  - Config Rollback Confirmed Change (from 12.4(23)T, 12.2(33)S)

- **Configuration locking** (from 12.3(14)T, 12.2(25)S)
  - Ensures exclusive configuration change access
Example: Config Revert

**Problem:** critical config change to a remote router may result in loss of connectivity, requiring a reload.

**Solution:** revert the running configuration after two minutes – unless the change made is confirmed.

```
router# config terminal revert time 2
Rollback Confirmed Change: Backing up current running config to flash:bk-2

Enter configuration commands, one per line. End with CNTL/Z.
...
... your Config Change work here ...
...
router# hostname oops
oops(config)# end

oops# Rollback Confirmed Change: Rollback will begin in one minute. Enter "configure confirm" if you wish to keep what you've configured
```

```
oops# Rollback Confirmed Change: rolling to: flash:bk-2
Total number of passes: 1
Rollback Done
```

```
or
oops# config confirm
oops#
```

Available from: IOS 12.4(23)T, 12.2(33)S
Switch Deployment

Switch Replacement

Aggregation Layer
Access Layer
Smart Install

- Central DHCP / TFTP Servers
- Smart Install Director on Aggregation Switch or Router
- Smart Install Client Switches
- Grouping for ease of management
How Smart Install Works

Simplified New Install Example

1. New switch connected
2. Director discovers client via CDP
3. New switch issues DHCP discover
4. Director adds options to DHCP offer
   (Director MUST be first L3 hop between client and DHCP server)
5. Client retrieves image, config via TFTP
6. Client reboots with new configuration and image

~20 Minutes
How to Configure 200 Switches in One Day: Cisco Live Europe 2012 NOC Case Study

- Director device configured by Network Admin
  - Approx 30 lines of config

- Brand-new client switches connected in batches of 20

- Successful configuration of each batch verified with “show vstack status”

- External TFTP server used to maximize transfer performance

- 20-30 minutes start-to-finish for each batch
Event-Based Configurations – Beyond ASP

**Problem:** How to trigger custom event-based port configurations

**Solutions:** Use Embedded Event Manager (EEM)

- Auto Smart Ports are powered by EEM
- Pre-built port configuration templates for simplify user experience and minimize configuration error
- Automatic event detection (CDP/LLDP/MAC) triggers auto configuration
- Authentication (802.1x, MAB) and authorization can be conducted before port configuration applied
- Automatic notification can be sent to NMS system to help with asset tracking
- Plug-n-play device deployment lowers overall management cost
Example: When a printer is added to the network, use an EEM applet to create a new ASP event

```
event manager applet detect-printer
  event neighbor-discovery interface regexp FastEthernet.* cdp add
  action 001 regexp ".*LasterJet.*" "$_nd_cdp_platform"
  action 002 if $_regexp_result eq 1
  action 003 cli command "enable"
  action 004 cli command "config t"
  action 005 cli command "interface $_nd_local_intf_name"
  action 006 cli command "switchport access vlan $printer_vlan"
  action 007 cli command "switchport mode access"
  action 008 cli command "switchport port-security"
  action 009 cli command "switchport port-security violation restrict"
  action 010 cli command "switchport port-security aging time 2"
  action 011 cli command "switchport port-security aging type inactivity"
  action 012 cli command "spanning-tree portfast"
  action 013 cli command "spanning-tree bpduguard enable"
  action 014 cli command "end"
  action 015 syslog msg "New printer added: $_nd_cdp_entry_name , type: $_nd_cdp_platform"
  action 016 end
```
Summary, References
References – Programming and Cloud-Intelligent

  (Note: local SE champion to nominate/follow-up via api-marketing@cisco.com)
- Cisco Scripting Community: [www.cisco.com/go/ciscobeyond](http://www.cisco.com/go/ciscobeyond)
References – Instrumentation and Automation

**Device Manageability Instrumentation (DMI)** [www.cisco.com/go/instrumentation](www.cisco.com/go/instrumentation)
- Cisco Beyond – EEM Community: [www.cisco.com/go/ciscobeyond](www.cisco.com/go/ciscobeyond)
- Embedded Packet Capture (EPC): [www.cisco.com/go/epc](www.cisco.com/go/epc)
- Network Based Application Recognition (NBAR): [www.cisco.com/go/nbar](www.cisco.com/go/nbar)
- Smart Call Home: [www.cisco.com/go/smartcall](www.cisco.com/go/smartcall)

- **Feature Navigator:** [www.cisco.com/go/fn](www.cisco.com/go/fn)
- **MIB Locator:** [www.cisco.com/go/mibs](www.cisco.com/go/mibs)
Embedded Automation Systems (EASy)

1. Browse and Download EASy Packages
   www.cisco.com/go/easy

2. Make Sure to also download EASy Installer

3. Browse Other Embedded Automations
   www.cisco.com/go/ciscobeyond

4. Learn About The Technology Under The Hood
   www.cisco.com/go/instrumentation
   www.cisco.com/go/eem
   www.cisco.com/go/pec

5. Discuss, Ask Questions, Suggest Answers
   supportforums.cisco.com
   supportforums.cisco.mobi

6. Upload your own Examples to CiscoBeyond
   www.cisco.com/go/ciscobeyond

7. Engage via ask-easy@cisco.com
Otázky a odpovědi

Zodpovíme též v “Ptali jste se” v sále LEO v 17:45 – 18:30
e-mail: connect-cz@cisco.com
Prosíme, ohodnoťte tuto přednášku.
Děkujeme za pozornost.