Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Implementing Network Automations – Power Tools for Catalyst Switching Network Operations

BRKCRS-3090

Agenda

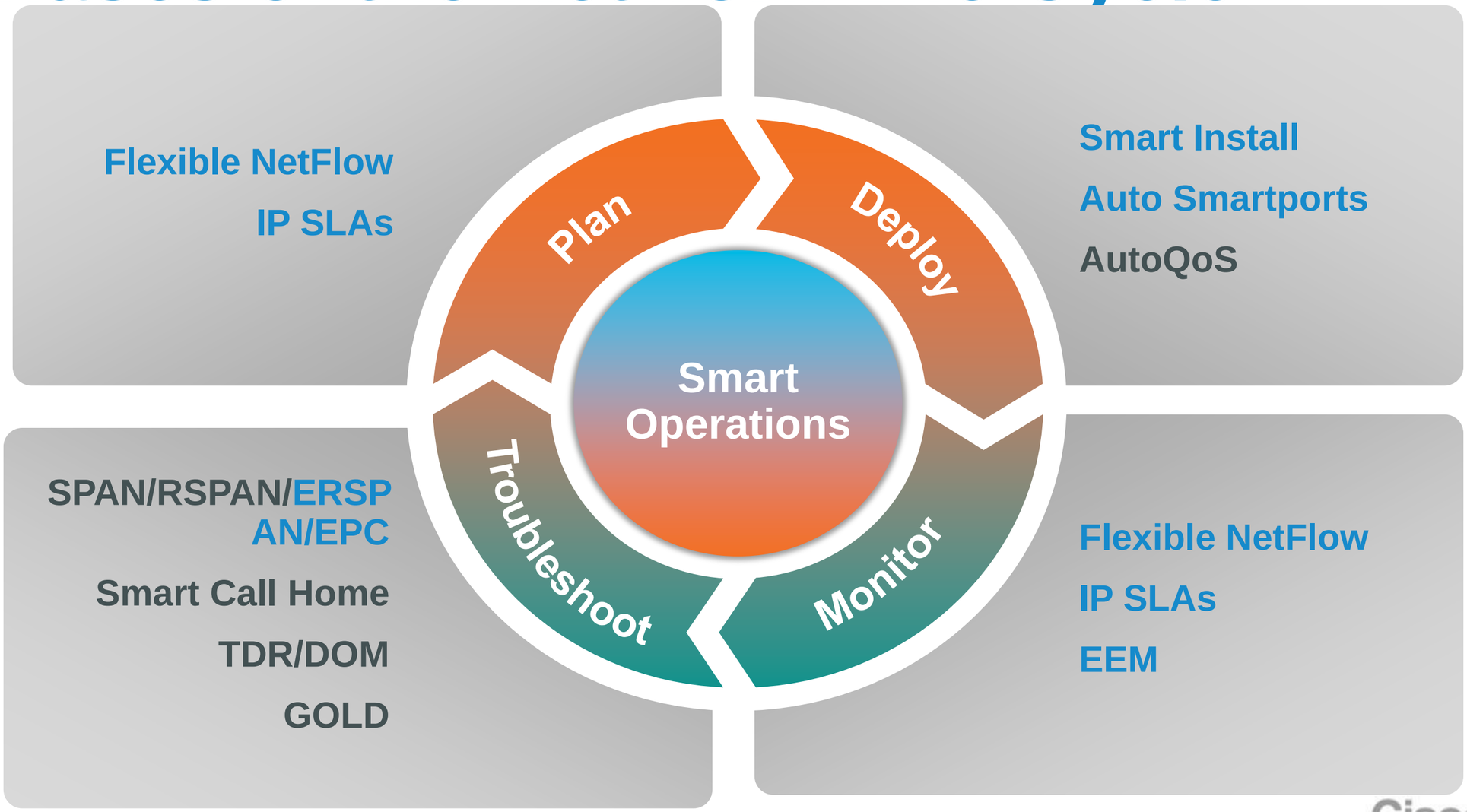
- What is Smart Operations?
- Smart Install
- Auto Smartports
- Other Gems
- EEM
- TCL

Smart Operations is:

Time-saving	LAN-focused	Free
▪ Tools that **automate** and **simplify** network administration	▪ Focused on **branch and campus** switch network operations	▪ **Included in IOS** on the Catalyst 2K, 3K, 4K and 6K

- Reducing Total cost of Ownership is an ongoing priority.

Smart Operations Includes Tools for all Phases of the Network Life Cycle



Smart Operations Feature Support

FYI

Jan 2013

Tool	Catalyst 6500	Catalyst 4500	Catalyst 3xx0	Catalyst 2xx0
Smart Install (Director)	●	●	●	○
Auto Smartports	○	●	●	●
AutoQoS	●	●	●	●
Flexible NetFlow	●	●	● *	○
IP SLAs	●	●	●	◑ Responder only
EEM	●	●	●	○
Smart Call Home	●	●	●	●
GOLD	●	●	●	○
SPAN/RSPAN	●	●	●	●
ERSPAN	●	○	○	○
Protocol analyser/Wireshark	●	●	○	○
TDR	●	●	●	●

* Specific hardware required C3KX-SM-10G

Agenda

- What is Smart Operations?
- Smart Install
- Auto Smartports
- Other Gems
- EEM
- TCL

Even been hit by this?

```
BNE-6500#192.168.4.2
Trying 192.168.4.2 ... Open


Password required, but none set

[Connection to 192.168.4.2 closed by foreign host]
BNE-6500#
```

Or this?

Good News!!!

Refresh Switches have arrived

Bad News

You are the racker and stacker

What is Smart Install?

- Hands-off IOS installation
- Hands-off device configuration
- Plug and Play
- Around since 12.2(55)SE
- Can either
  - Be entirely handled by switch infrastructure, or
  - Use external TFTP/DHCP server

Smart Install Benefits

Zero-touch Deployment and Maintenance

Zero-touch Installation

- **Anyone can install a switch:**
  - Reduce travel
  - Less skilled labor
- **Speeds up deployment for large installs:**
  - Network does IOS SW install

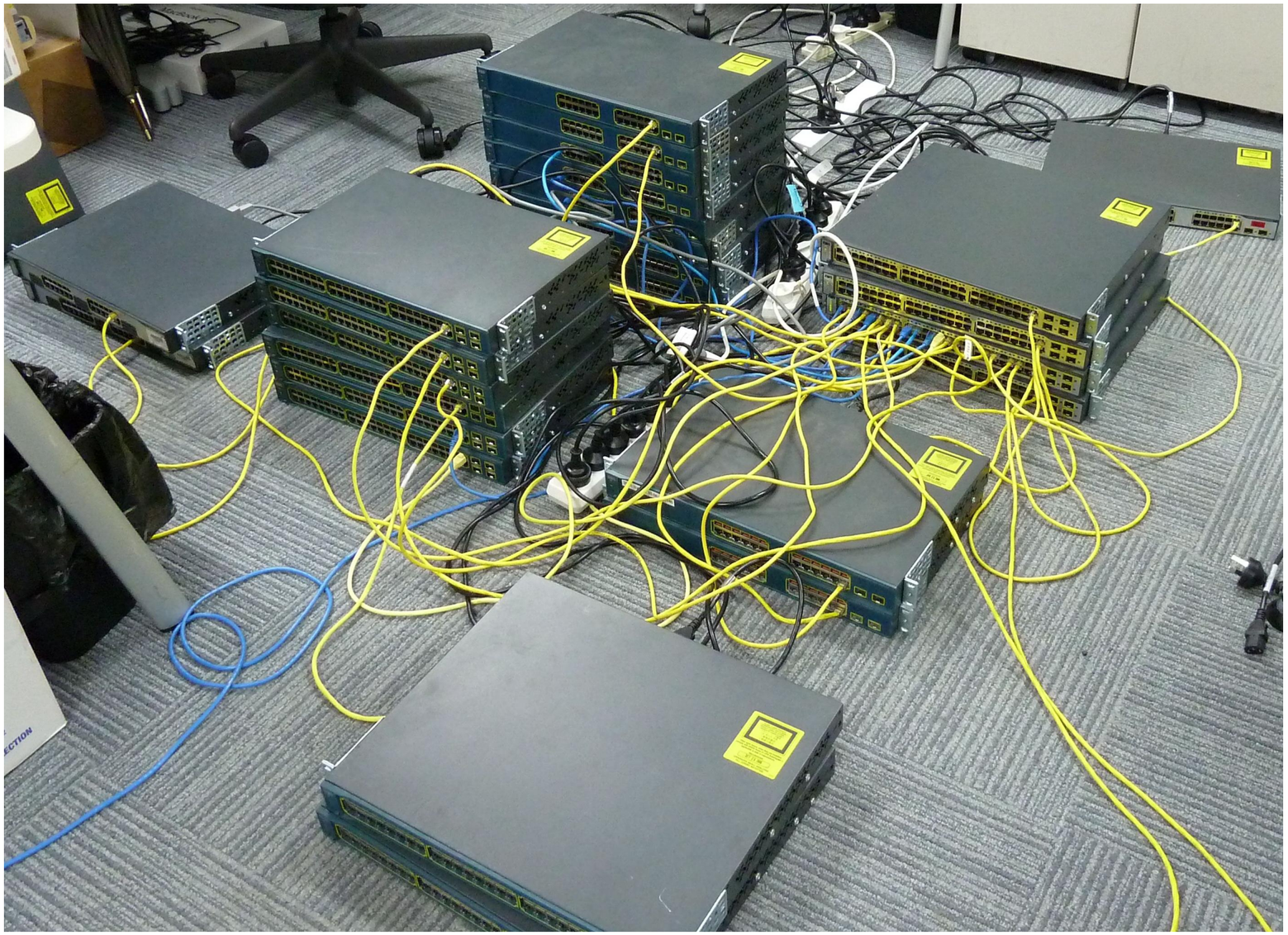
Centralised Image and Config Management

- **Catalyst switch update** from a **single point of control (vstack)**
- Ensure Configuration **consistency** across Catalyst switches
- **Prevents manual configuration errors**

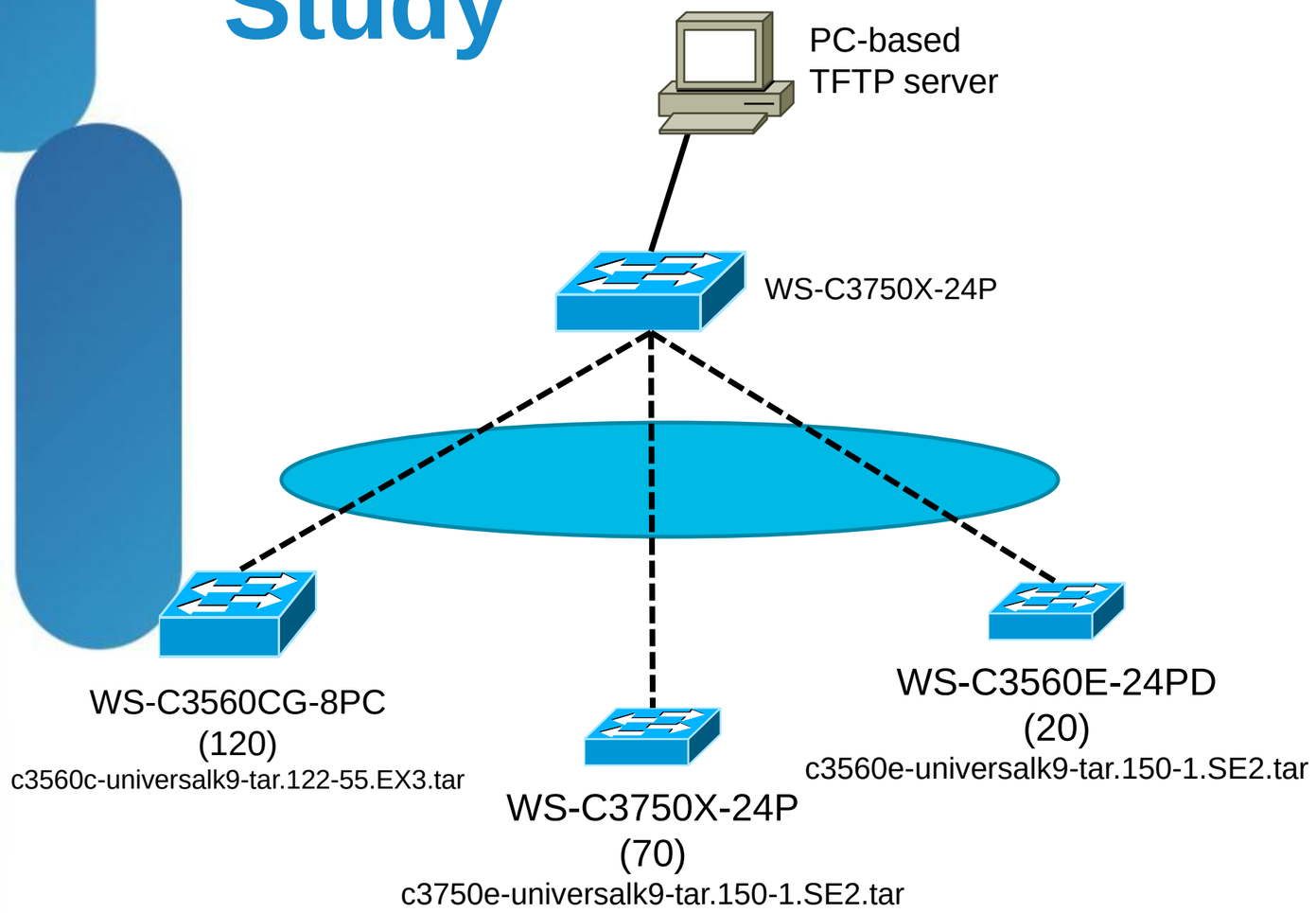
Automated Replacement

- **Configurations** automatically **backed up**
- RMA supported:
  - New Switch **automatically configured** same as old.

Flood Activities



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

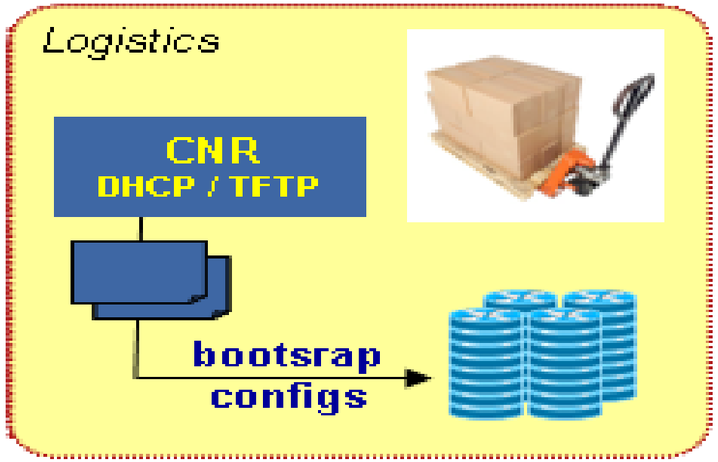


- Director device configured by Network Admin
  - Approx 30 lines of config
- Brand-new client switches connected in batches of 20
- Successful configuration of each batch verified with "*show vstack status*"
- External TFTP server used to maximise transfer performance
- 20-30 minutes start-to-finish for each batch

Smart Install the Beginnings – Auto Install

IOS Auto Install Feature consists of:

- Ethernet Interface up
- DHCP Client + Option 150



Combined with external

- DHCP and TFTP Server

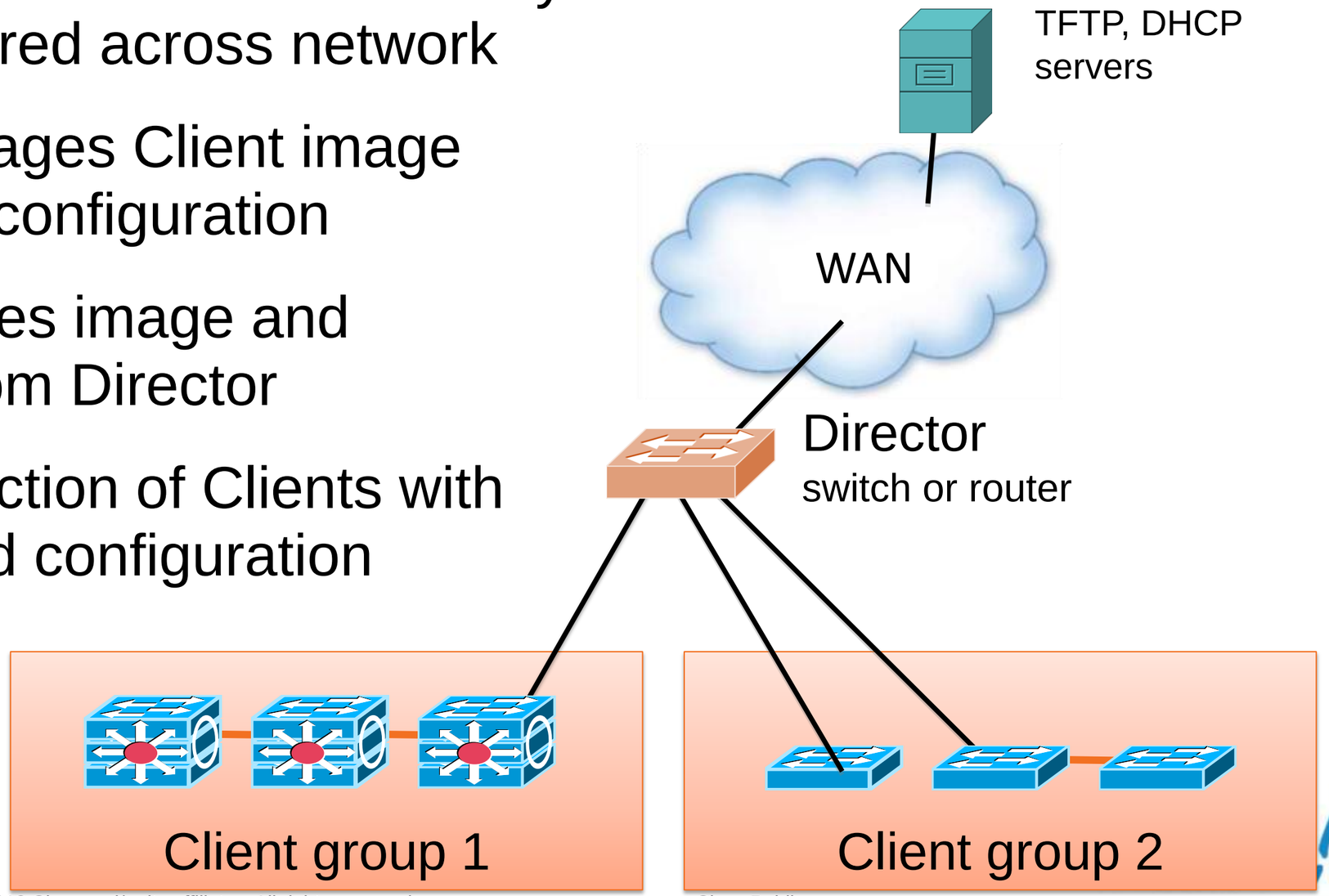
this enables a new router to

- automatically retrieve a default configuration
- without manual interaction via console cable or telnet

*Mar 1 00:02:21.985: AUTOINSTALL: Vlan1 is assigned 192.168.251.53

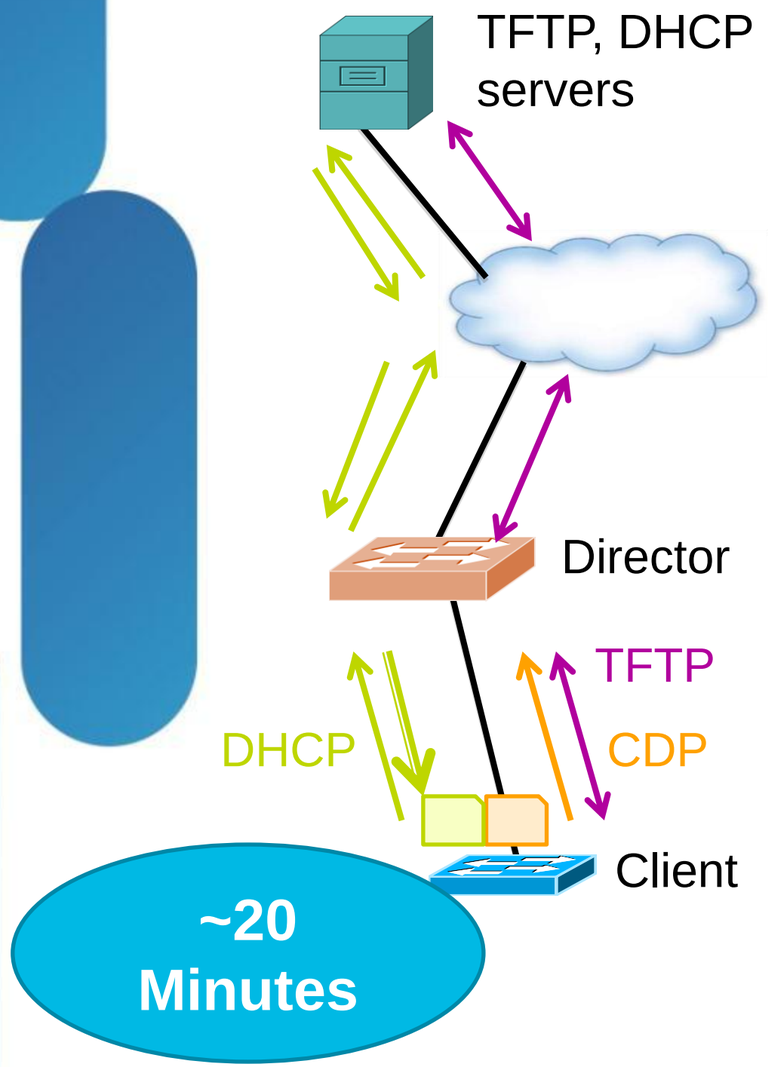
Smart Install Components

- **DHCP and TFTP Servers –** Centrally located and shared across network
- **Director –** manages Client image installation and configuration
- **Client -** Receives image and configuration from Director
- **Groups -** Collection of Clients with same image and configuration



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
5. Client retrieves image, config via TFTP
6. Client reboots with new configuration and image

Smart Install (SI) – Considerations

- The Director must be first L3 hop in-between SI clients and the DHCP server
- Director Scaling considerations:
  - 3K / 4K supports 64 clients
  - 6500 supports 32 clients
  - ISR supports 36 clients
- No redundancy for the Smart Install Director

Smart Install Supported Platforms

Smart Install Directors

ISR Branch Router

G1: 1841, 2801, 2811, 2821, 2851, 3825, 3845
G2: 1921, 1941, 2901, 2911, 2921, 2951, 3925, 3945, 3925E, 3945E,
Min release: : 15.1.(3)T1

Catalyst 3K

3750, 3750G, 3750v2, 3750E, 3560, 3560v2, 3560E, 3560G 3750X, 3560X
Min Recommended: 12.2.(58)SE2

Catalyst 4500
Catalyst 6500

Smart Install Clients

Catalyst 3K

3750, 3750v2, 3750E, 3750G, 3750X,
3560, 3560v2 3560E, 3560G, 3560X

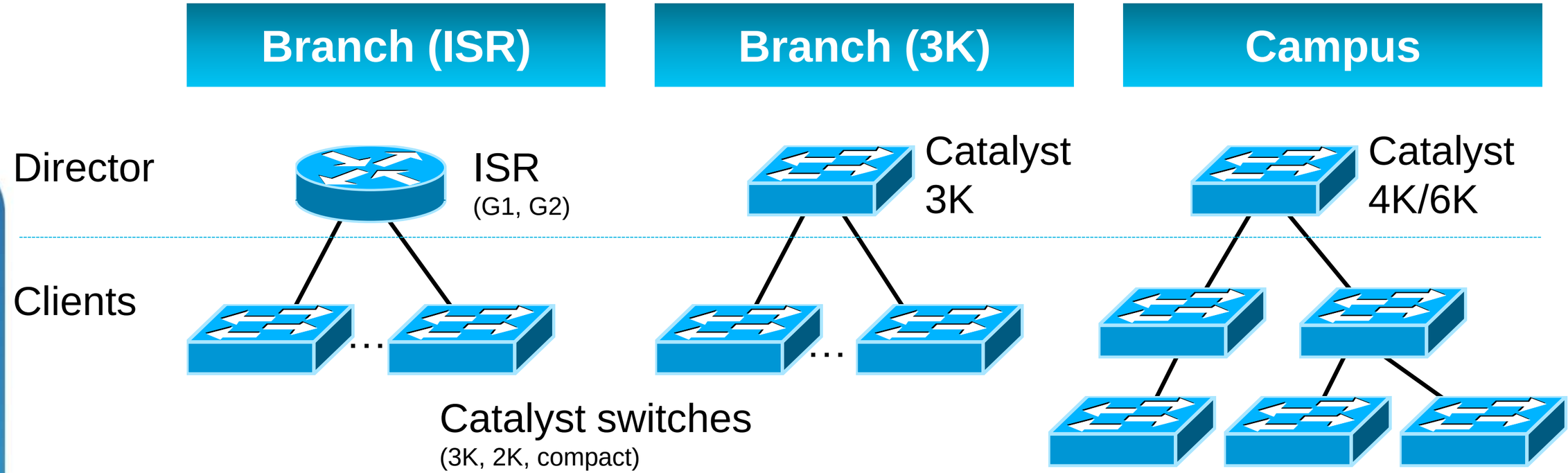
Catalyst 2K

2960, 2960S, 2960G

Catalyst 2K/3K Compact

2960C, 3560C

Common Deployment Scenarios



Also: central staging before deployment

Step by Step on the Director

- Int lo 0

  ip address 10.66.236.245 255.255.255.255

- interface Vlan1

  ip address 192.168.7.1 255.255.255.0

  ip helper-address 10.66.236.245

- vstack dhcp-localserver pool1

  address-pool 192.168.7.0 255.255.255.0

  default-router 192.168.7.1

- Copy client_cfg and image tar to flash

- vstack director 10.66.236.245
- vstack hostname-prefix CL2013-Lab

- vstack group built-in 3560 8poe

  image bootflash:c3560-ipservicesk9-tar.150-1.SE3.tar

  config bootflash:cl2013_client_cfg.txt

Sample Client Config (cl2013_client_cfg.txt)

```
vtp mode transparent
clock timezone Brisban 10 0
ntp server 10.66.236.1
macro auto device phone
   VOICE_VLAN=2
macro auto global processing
enable secret 5 $1$KtA
username admin secret 5 $1$ati
int vlan 1
    ip address dhcp
int vlan 2
    no shut
    exit
line vty 0 4
    login local
logging 10.66.236.46
snmp-server community public RO
snmp-server community private RW
end
```

Smart Install – Considerations

- Not all clients are “built-in” but can create custom-groups

```
BNELAB-4507-R(config)#vstack group custom NewModelSwitch product-id
BNELAB-4507-R(config-vstack-group)#match ?
  WORD  Product-ID: (a few examples are shown below)
          WS-C2960-48TC-L, WS-C3560E-12SD
          NME-16ES-1G-P, NME-X-23ES-1G, NME-XD-48ES-2S-P
          SM-ES3G-24-P, SM-ES3-16-P, SM-ES2-48
```

- Take care with director tftp, if you are logged in and change directory, the IOS tftp server will change its directory
- Watch out for 15.0(2) SE prior to Jan 2013, SI clients fails to reload if new image is the same as existing.

Smart Install – Getting Started

- Be Patient
  - Download starts after client gets IP Address (DHCP scope)
  - Smart Install is Hands-off
  - Image is downloaded to flash
  - ‘Show vstack status’ or ‘Show Archive Status’ if in doubt

```
BNELAB-4507-R#show vstack download-status
SmartInstall:  ENABLED
Total no of entries : 1
No   client-IP        client-MAC      Method          Image-status  Config-status
===  ===============  ==============  ==============  ============  =============
1    192.168.7.44     0022.be51.4500  zero-touch      UPGRADING     UPGRADED

BNELAB-4507-R#
```

Smart Install – Lab Notes

- Apply KISS principle for lab – use director for DHCP and TFTP
- Then move to external TFTP
- SI supports auto replacement of switches

```
CL2103-Lab-51.4540#
*Mar  1 00:04:54.347: %SMI-6-SMI_CLIENT_BACKUP_SUCCESS:
    Client Device startup configuration backup successful on repository
```

- If testing fresh install
  - Wri-erase client
  - Remove client from director database (clear vstack director-db entry)
  - Remove client back-up config files from director

What Else Does Smart Install Bring?

Simplified Ongoing Operations

- Monitor the entire vstack from director
- Can also attach to client switches (e.g. vstack attach 5)

```
3750-HQD#sho vstack status
SmartInstall:  ENABLED

Status: Device_type Health_status Join-window_status Upgrade_status
Device_type:  S - Smart install N - Non smart install P - Pending
Health_status:  A - Active I - Inactive
Join-window_Status:  a - Allowed  h - On-hold   d - Denied
Image Upgrade:   i - in progress     I - done           X - failed
Config Upgrade:  c - in progress     C - done           x - failed
Director Database:
DevNo  MAC Address     Product-ID          IP_addr           Hostname    Status
=====  ==============  ==================  ================  ==========  =========
0      0025.45d2.1900  WS-C3750E-48PD      10.66.236.241     3750-HQD    Director
4      0025.45e4.8000  WS-C3750E-48PD      192.168.251.52    BNE-HQ-e4.  S A a
5      0025.45d2.4000  WS-C3750E-48PD      192.168.251.53    BNE-HQ-d2.  S A a
9      0011.5cd8.8e00  WS-C6506            192.168.250.1     BNE-6500.b  N A a
11     70ca.9be3.ac80  WS-C3750X-24        192.168.251.55    PeterWasHE  S I a I C
```

Visibilty of the Clients

```
BNELAB-4507-R#sho vstack status detail
SmartInstall:  ENABLED

Device Num      : 2
Device ID       : CL2013-Lab-51.4540.bnelab.cisco.com
MAC Address     : 0022.be51.4500
IP Addr         : 192.168.4.2
Hop value       : 1
Serial          : FOC1232V136
Product-ID      : WS-C3560-8PC
Version         : 15.0(2)SE
Image           : C3560-IPSERVICESK9-M
Entry Role      : IBC Entry
(N-1)HOP Entry : c471.fe71.ce80
Backup done     :  Yes
Latest backup file: bootflash:/vstack/CL2013-Lab-51.4540-0022.be51.4500.REV2
Latest backup client name: CL2013-Lab-51.4540
File checksum      : EFFBE13CAAD8CCA6507C26BF9054597B
Switch replace type: Same Switch
Switch version      : 1
Status             : S A a X C
Capability      : Network derived SMI management VLAN supported
```

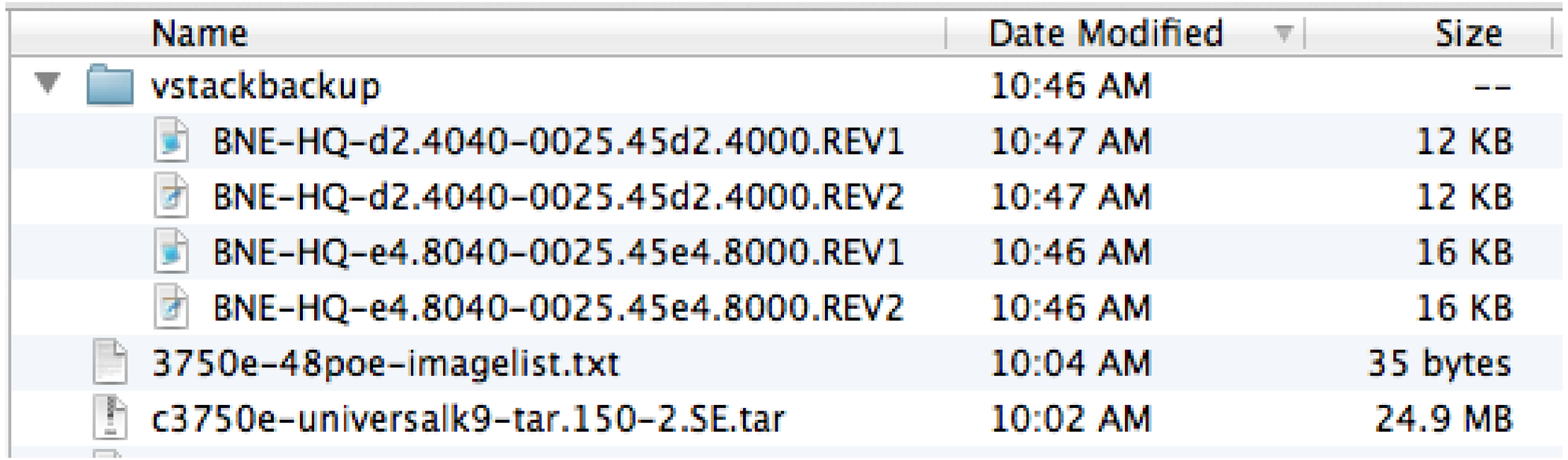
Upgrading Multiple Switches

```
3750-HQD#sho vstack status  detail | inc Version
Version         : 15.0(1)SE1
Version         : 15.0(1)SE1
Version         : 15.0(1)SE1
Version         : 12.2(33)SXI3

3750-HQD#sho run | beg vstack
.....
vstack group built-in 3750e 48poe
 image tftp://192.168.2.20/c3750e-universalk9-mz.150-2.SE.bin
 config tftp://192.168.2.20/ips_config.txt
.....

3750-HQD#vstack download-image built-in 3750e 48poe cisco,123 override reload in 00:30
Existing image on Clients can be replaced and Clients will be reloaded. proceed?[confirm]

3750-HQD#sho vstack download-status
SmartInstall:  ENABLED
Total no of entries : 4
No   client-IP        client-MAC      Method           Image-status  Config-status
===  ==============  ==============  ===============  ============  =============
1    192.168.251.54   7081.0529.dc80  zero-touch       UPGRADED      UPGRADED
2    192.168.251.55   70ca.9be3.ac80  zero-touch       UPGRADED      UPGRADED
3    192.168.251.52   0025.45e4.8000  image-upgrade    UPGRADING     **
4    192.168.251.53   0025.45d2.4000  image-upgrade    UPGRADING     **
```

What Else Does it Bring?

Centralised configuration back-ups.

```
vstack backup file-server tftp://192.168.2.20/vstackbackup
```



Name	Date Modified	Size
vstackbackup	10:46 AM	--
BNE-HQ-d2.4040-0025.45d2.4000.REV1	10:47 AM	12 KB
BNE-HQ-d2.4040-0025.45d2.4000.REV2	10:47 AM	12 KB
BNE-HQ-e4.8040-0025.45e4.8000.REV1	10:46 AM	16 KB
BNE-HQ-e4.8040-0025.45e4.8000.REV2	10:46 AM	16 KB
3750e-48poe-imagelist.txt	10:04 AM	35 bytes
c3750e-universalk9-tar.150-2.SE.tar	10:02 AM	24.9 MB

Smart Install – VLAN 1 Requirement

Problem: Smart Install Client assumes VLAN 1 for initial connectivity, however best practice is to NOT use VLAN 1 for management.

Workaround: Reconfigure access port on Smart Install Director:

```
interface Port-channel101
description Connected to clientsw123
switchport
switchport trunk encapsulation dot1q

switchport trunk native vlan 4001
switchport trunk allowed vlan 2-17,4093
switchport mode trunk
logging event link-status
logging event bundle-status
load-interval 30
carrier-delay msec 0
mls qos trust dscp
hold-queue 2000 out
```

```
interface Port-channel101
description Connected to clientsw123
switchport
switchport trunk encapsulation dot1q
switchport access vlan 4093
switchport trunk native vlan 4001
switchport trunk allowed vlan 2-17,4093
~~switchport mode trunk~~
logging event link-status
logging event bundle-status
load-interval 30
carrier-delay msec 0
mls qos trust dscp
hold-queue 2000 out
```

Smart Install – Best Practices

- Use external TFTP if possible
  - Higher performance for concurrent downloads
  - Plenty of disk space (flash space on 3K switches is limited)
  - Less points of management
- For Remote Sites
  - If link slow or lossy consider using ISR as TFTP server

Smart Install Summary

Smart Install : Automates Device Deployment and Replacement

- Accelerated deployment, upgrades and replacement
- Use for staging in the lab, or installation in remote locations
- Requires the director in DHCP Path
- Questions???

- To learn more (case studies, white papers, documentation):

  http://cisco.com/go/smartoperations

Agenda

- What is Smart Operations?
- Smart Install
- Auto Smartports
- Other Gems
- EEM
- TCL

Automation is Good

Postal Service can not operate without Automation

Now Sort the mail Manually

Auto Smartports (ASP) – What is it?

Dynamically Configures Ethernet Port Based on the Device Type

Existing Challenges	ASP addresses by
Manual configuration of every port - Devices move	Configuration moves with device
Wasted Ports – pre-configured dedicated interfaces and no device	Interfaces in ready state waiting for a device to attach. - More efficient use of valuable ports
Unsure how to mix multiple features together	Cisco Best Practices for mixing interface level configurations
Not knowing what is connected -Which interface has the printer?	Device classification. What is attached on every interface

Auto Smartports – History

- Enhancement to “Smart Ports”
- Originally released in 12.2(50)SE on Catalyst 2960, 3560, 3750
- Summer of 2011 15.0.1SE enhanced device classification
  - Adds profiles for MAC OUI, and DHCP options to identify device.
  - Easier to find the printer now.

Auto Smart Ports – How it Works

1. ASP snoops incoming packets for
   - Source MAC Address
   - CDP – Cisco Discovery Protocol
   - LLDP – Link Layer Discovery Protocol
   - DHCP Discover from end device
2. Uses Above to determine Device Type
3. Applies Macro to interface based on Device Type
   - Macro = set of interface level CLI commands.
   - Built-in Macro's for well known devices using best practices

Auto Smart Ports – Cisco IP Phone

Order of events for IP Phone attachment, and configuration applied

POE

CDP/LLDP

Attach IP Phone to interface Gig 1/0/4
Power up via POE
Exchange CDP/LLDP with switch
Get Voice vlan config
Register with Call manager

Attach IP Phone to interface Gig 1/0/4
Apply Power to Gig 1/0/4
Exchange CDP/LLDP with device
Detects Device is IP Phone
Apply CISCO_IP_PHONE_MACRO to Gig 1/0/4
Contents of MACRO
- Voice and data vlan applied
- QOS applied
- Cisco best practice security applied to IP Phone interface

Auto Smart Ports – Built-in Device Macros

Switch# show macro auto device ?

```
BNELAB-4507-R#sho macro auto device ?
  access-point    Display auto configuration information for the autonomous
                  access point
  ip-camera       Display auto configuration information for the video
                  surveillance camera
  lightweight-ap  Display auto configuration information for the light weight
                  access point
  media-player    Display auto configuration information for the digital media
                  player
  phone           Display auto configuration information for the phone device
  router          Display auto configuration information for the router device
  switch          Display auto configuration information for the switch device
  |               Output modifiers
  <cr>
```

Macro Contents – IP PHONE

Interface Configuration of CISCO_PHONE_AUTO_SMARTPORT

Switch# show run interface Gig 1/0/6

```
interface GigabitEthernet1/0/6
 switchport access vlan 10
 switchport mode access
 switchport block unicast
 switchport voice vlan 11
 switchport port-security maximum 3
 switchport port-security maximum 2 vlan access
 switchport port-security
 switchport port-security aging time 1
 switchport port-security violation restrict
 switchport port-security aging type inactivity
 load-interval 30
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 macro description CISCO_PHONE_EVENT
 auto qos voip cisco-phone
```

Cisco Best Practices for IP Phone

…. Continued

```
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 spanning-tree portfast
 spanning-tree bpduguard enable
 service-policy input AutoQoS-Police-CiscoPhone
 ip dhcp snooping limit rate 15
!
```

Auto Smart Ports – Macro Contents sample

Switch# show shell functions CISCO_AP_AUTO_SMARTPORT

```
function CISCO_AP_AUTO_SMARTPORT () {
 if [[ $LINKUP -eq YES ]]; then
   conf t
     interface  $INTERFACE
       macro description $TRIGGER
       switchport trunk encapsulation dot1q
       switchport trunk native vlan $NATIVE_VLAN
       switchport trunk allowed vlan ALL
       switchport mode trunk
       switchport nonegotiate
       auto qos voip trust
       mls qos trust cos
       exit
     end
 fi
```

…Continued

```
if [[ $LINKUP -eq NO ]]; then
  conf t
    interface  $INTERFACE
      no macro description
      no switchport nonegotiate
      no switchport trunk native vlan $NATIVE_VLAN
      no switchport trunk allowed vlan ALL
      no auto qos voip trust
      no mls qos trust cos
      if [[ $AUTH_ENABLED -eq NO ]]; then
        no switchport mode
        no switchport trunk encapsulation
      fi
      exit
    end
fi
```

Macro definition includes anti-macro configuration as well

Auto Smart Ports - Timing

- Time for IP Phone to power on and configure

```
May  4 01:55:05.645: %ILPOWER-7-DETECT: Interface Gi1/0/11: Power Device detected: IEEE PD (Stack-1)
May  4 01:55:06.836: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/11, changed state to down
May  4 01:55:06.710: %ILPOWER-5-POWER_GRANTED: Interface Gi1/0/11: Power granted (Stack-1)
May  4 01:55:13.371: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/11, changed state to up
May  4 01:55:14.377: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/11, changed state to up
May  4 01:55:29.536: %AUTOSMARTPORT-5-INSERT: Device Cisco-IP-Phone detected on interface GigabitEthernet1/0/11,
executed CISCO_PHONE_EVENT
```

- PoE Device Detect: 0 – starts the process
- Power granted: 1 second
- Interface up: 7.7 seconds
- Protocol up: 8.7 seconds
- ASP configures interface: 23.8 seconds

Auto Smart Ports – Device Support

- Cisco Endpoint devices auto detected via CDP
  - IP Phones, IP Cameras, Digital Media Players, Access Points, Lightweight access points
  - Cisco Routers and Switches
  - All have built-in MACROs ready to use
- Support for LLDP, & MAC OUI
  - 3rd Party: IP phone, switch, router, Access Point, Printer, …
  - MAC OUI – first 3 bytes of MAC Address
  - List of OUIs - http://standards.ieee.org/develop/regauth/oui/oui.txt

Auto Smart Ports- the Basics

- Built-in Macros have default vlan id.
  - –Change vlan id for built-in macros

```
Switch(config)#macro auto execute CISCO_PHONE_EVENT builtin \
        CISCO_PHONE_AUTO_SMARTPORT VOICE_VLAN=10 ACCESS_VLAN=3

(repeat for all devices or builtin macros)
```

- Use LAST_RESORT MACRO for Unclassified Devices
  - – Applied to interface that has no matches (eg: laptops)

```
Switch(config)# macro auto execute CISCO_LAST_RESORT_EVENT builtin \
     CISCO_LAST_RESORT_SMARTPORT ACCESS_VLAN=data_vlan
```

- Enable Auto Smart Ports – Last step

```
Switch(config)# macro auto global processing
```

Auto Smart Ports – Advanced Features

- Exclude specific Ethernet Interfaces from ASP

```
Switch(config)# interface Gi3/1/1
Switch(config-if)# no macro auto processing
```

- Make Macros “sticky”
  - stick to interface regardless of port operational state, disabled by default

```
Switch(config)# macro auto sticky
```

- Use vlan names instead of numbers for Macro parameter substitution

```
macro auto device phone ACCESS_VLAN=data_vlan VOICE_VLAN=voice_vlan
```

Auto Smart Ports
– What Macro has been Applied

```
Switch# show macro auto interface
```

```
Global Auto Smart Port Status
 Auto Smart Ports Enabled
 Fallback : CDP  Disabled
Interface      Auto Smart Port   Fallback    Macro Description(s)
-----------------------------------------------------------------
Vl1            TRUE              None        No Macro Applied
Vl10           TRUE              None        No Macro Applied
Fa0            TRUE              None        No Macro Applied
Gi1/0/1        TRUE              None        No Macro Applied
Gi1/0/2        TRUE              None        CISCO_WIRELESS_AP_EVENT
Gi1/0/3        TRUE              None        No Macro Applied
Gi1/0/4        TRUE              None        CISCO_LAST_RESORT_EVENT
Gi1/0/5        TRUE              None        HP_printer_OUI macro
Gi1/0/6        TRUE              None        CISCO_CUSTOM_EVENT
Gi1/0/7        TRUE              None        CISCO_PHONE_EVENT
.
.
.
```

laptop

Auto Smart Ports – Custom Device

- Custom Macro (eg: MAC OUI) for devices without built-in Macro

```
Switch(config)# macro auto mac-address-group Xerox_printer_OUI
 oui list 0000AA
 exit

Switch(config)#macro auto execute Xerox_printer_OUI  {
 if [[ $LINKUP -eq YES ]]
  then conf t
  interface $INTERFACE
  <snip>
 fi
 if [[ $LINKUP -eq NO ]]
  then conf t
  interface $INTERFACE
   <snip>
 fi
}
```

Appending In-built Macros

- Lets not leave ports sitting in VLAN 1

```
BNE-HQ-e4.8040#sho shell functions CISCO_CUSTOM_AUTOSMARTPORT
function CISCO_CUSTOM_AUTOSMARTPORT () {
    if [[ $LINKUP -eq YES ]]; then
        conf t
            interface $INTERFACE
            exit
        end
    fi
    if [[ $LINKUP -eq NO ]]; then
        conf t
            interface $INTERFACE
            exit
        end
    fi
}
```

```
macro auto execute CISCO_CUSTOM_EVENT {
    if [[ $LINKUP -eq YES ]]; then
        conf t
            interface $INTERFACE
            exit
        end
    fi
    if [[ $LINKUP -eq NO ]]; then
        conf t
            interface $INTERFACE
            no macro description
            switchport access vlan 2
            exit
        end
    fi
}
```

Auto Smart Port – Best Practices

- Change the Vlan IDs in the Macros that will be used.
- EtherChannels can be tricky, don't use with Auto Smart Ports
- Devices that do not move, don't use with Auto Smart Ports
  - Routers and Switches don't change interfaces

```
Switch(config-if)#  !!! Disable auto smart processing on the interface
Switch(config-if)# no macro auto processing
```

- Complete configuration before globally enabling Auto Smart Ports

Device Classifier

Identifies Directly Attached Devices

- Uses CDP/LLDP, DHCP, and MAC OUI to analyse device types
- Enabled by Default
  - 15.0.1SE (C3750, C3560, C2960) & 3.3.0SG (4500E Sup7)

```
BNELAB-4507-R#sho macro auto monitor device
Summary:

MAC_Address       Port_Id       Profile Name                      Device Name
==============    ==========    ==============================    ======================
0022.be51.4540    Gi1/47        Cisco-Device                      CISCO SYSTEMS
001c.58d6.435c    Gi1/35        Cisco-IP-Phone-7961               Cisco IP Phone 7961
c84c.7520.8dae    Gi1/39        Cisco-Device                      CISCO SYSTEMS
0022.be51.4501    Gi1/47        Cisco-Switch                      cisco WS-C3560-8PC
a40c.c394.5027    Gi1/41        Cisco-IP-Phone-7962               Cisco IP Phone 7962
0011.5cd8.8ef7    Gi6/6         Cisco-Switch                      cisco WS-C6506
649e.f346.ceb0    Gi1/48        Cisco-Switch                      cisco WS-C3560X-48
406c.8f1d.72fa    Gi1/35        Apple-Device                      APPLE, INC.
0080.9f6f.a649    Gi1/45        Un-Classified Device              alcatel.noe.0
1cdf.0f95.33c4    Gi1/46        Cisco-AIR-LAP                     cisco AIR-CAP3502I-N-K9
```

Automation Taken it to the Next Level - 1

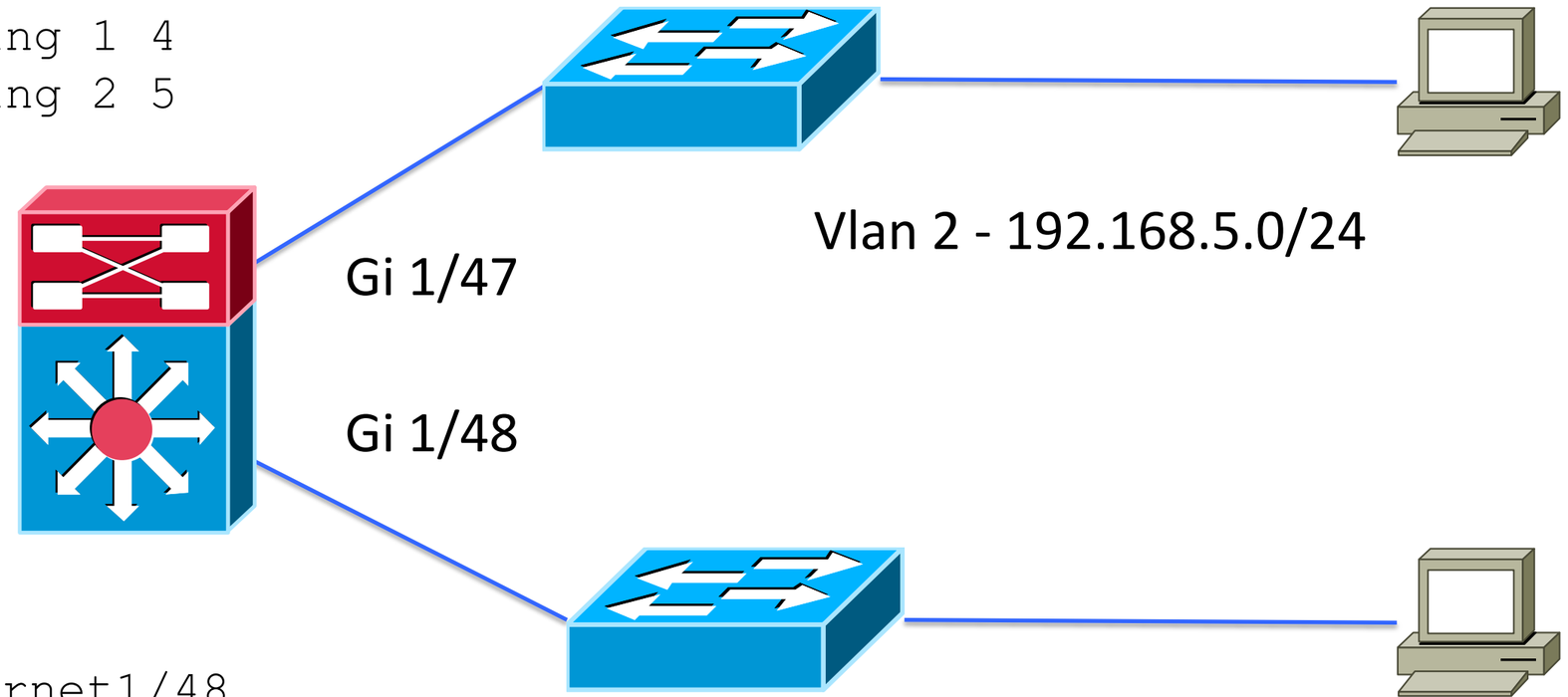
Solving the Consistency Problem

- Automation likes consistency
  - VLAN numbers used in Auto SmartPort Macros
  - Traditionally have trunked different VLAN numbers to different floors
- Security Likes consistency
  - Able to return vlan number in radius responses
- Humans like consistency
  - Eases troubleshooting
- Addressed by VLAN Remapping
  - 6500 Sup2T and 4500 Sup7 support VLAN remapping
  - A little extra effort at Core/Distribution layer but saves effort at the edge

Automation Taken it to the Next Level - 2

Solving the Consistency Problem

```
interface GigabitEthernet1/47
 switchport mode trunk
 switchport vlan mapping 1  4
 switchport vlan mapping 2  5
```




```
interface GigabitEthernet1/48
 switchport mode trunk
 switchport vlan mapping 1  6
 switchport vlan mapping 2  7
```

Automation Taken it to the Next Level - 3

Solving the Consistency Problem

- VLAN Remapping – remaps internal VLAN number to that of the trunk

```
interface Vlan4
 ip address 192.168.4.1 255.255.255.0
!
interface Vlan5
 ip address 192.168.5.1 255.255.255.0
!
interface Vlan6
 ip address 192.168.6.1 255.255.255.0
!
interface Vlan7
 ip address 192.168.7.1 255.255.255.0
```

```
interface GigabitEthernet1/47
 switchport mode trunk
 switchport vlan mapping 1 4
 switchport vlan mapping 2 5
!
interface GigabitEthernet1/48
 switchport mode trunk
 switchport vlan mapping 1 6
 switchport vlan mapping 2 7
```

ASP – The Next Generation

How Do We Make It Better? Current Challenges

1. Configurations can get large and complex as you introduce security
2. And larger as you add safety features associated with security
3. IPv6 means configurations will grow further
4. Configurations constantly changing as port change states, makes version control difficult
5. Configuration Residue
6. Management Access Collision

SaNet – Session Aware Networking

1. New Identity Policy Engine for Trustsec
2. Able to tie Any Authentication Method with Any Authorisation Feature for both wired and wireless
3. Leverages Templates for Sessions and Interfaces
4. Smaller configurations - define once use many times (like Port Profiles in NX-OS)
5. Configurations not constantly changing - Policy is visible via CLI
6. Enabler to simplify and extend the definition and delivery of policy (Identity, MediaNet, Energywise)

3850 at FCS and 2HCY13 on 2k / 3k / 4k

Auto Smart Ports – Summary

- ASP uses Device MAC, CDP/LLDP, DHCP options to detect device type
- Built-In Macros for known devices
  - Based on best practices
- Extendable for more devices
- Questions???

Agenda

- What is Smart Operations?
- Smart Install
- Auto Smartports
- Other Gems
- EEM
- TCL

Other Gems

- Embedded Packet Capture
- ERSPAN
- Config Management
  - Archive
  - Restore – diff

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 analyse 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

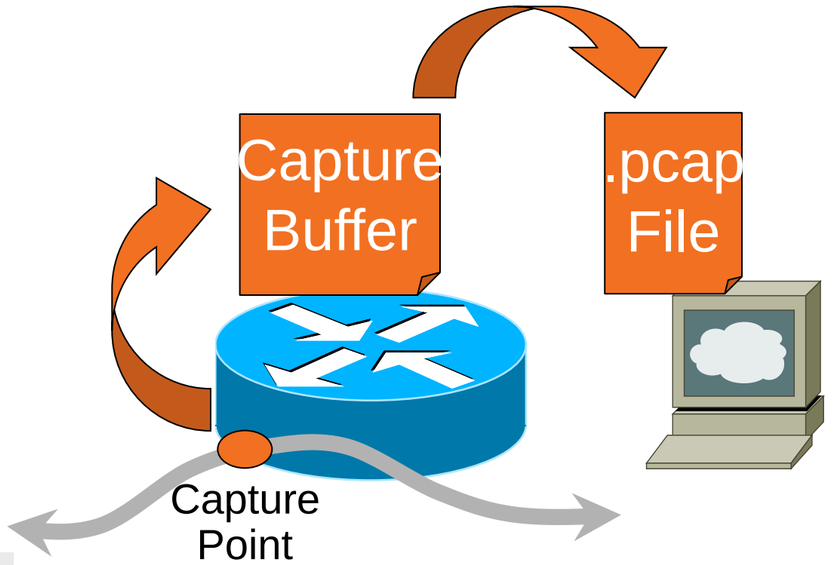
```
Router# monitor capture point associate …
```

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
Available from: IOS 12.4(20)T
Platforms: 8xx, 18xx, 28xx, 38xx ISRs, ISR G2s, 72xx

EPC – Configuration

1-3. Define a capture buffer, capture point and associate the two

```
Router# monitor capture buffer my-buffer size 100 max-size 1000 circular
Router# monitor capture point ip process-switched my-capture in
Router# monitor capture point associate my-capture my-buffer
```

4. Start capturing traffic

```
Router# monitor capture point start all
*Nov 25 10:00:58.990: %BUFCAP-6-ENABLE: Capture Point my-capture enabled.
```

5. Show / Analyse on the router …

```
Router# show monitor capture buffer all parameters
  Capture buffer my-buffer (circular buffer)
  Buffer Size : 102400 bytes, Max Element Size : 1000 bytes, Packets : 28
  Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
  Associated Capture Points:
  Name : my-capture, Status : Active
  Configuration:
  monitor capture buffer my-buffer size 100 max-size 1000 circular
  monitor capture point associate my-capture my-buffer
```

We have some traffic

```
Router# show monitor capture buffer my-buffer dump
  10:14:05.914 UTC Nov 25 2008 : IPv4 Process    : Fa0/0 None
  66A3C5B0:          FFFFFFFF FFFF0001 64FF4C01      ........d.L.
  66A3C5C0: 080045C0 00300000 00000111 0B5AACA1  ..E@.0.......Z,!
  66A3C5D0: 0103FFFF FFFF02C7 02C7001C 85F60001  .......G.G...v..
  66A3C5E0: 0010AC12 01020000 5D4C0F03 0004AC12  ..,.....]L....,.
```

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
- Policy available from https://supportforums.cisco.com/docs/DOC-19371

```
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
```

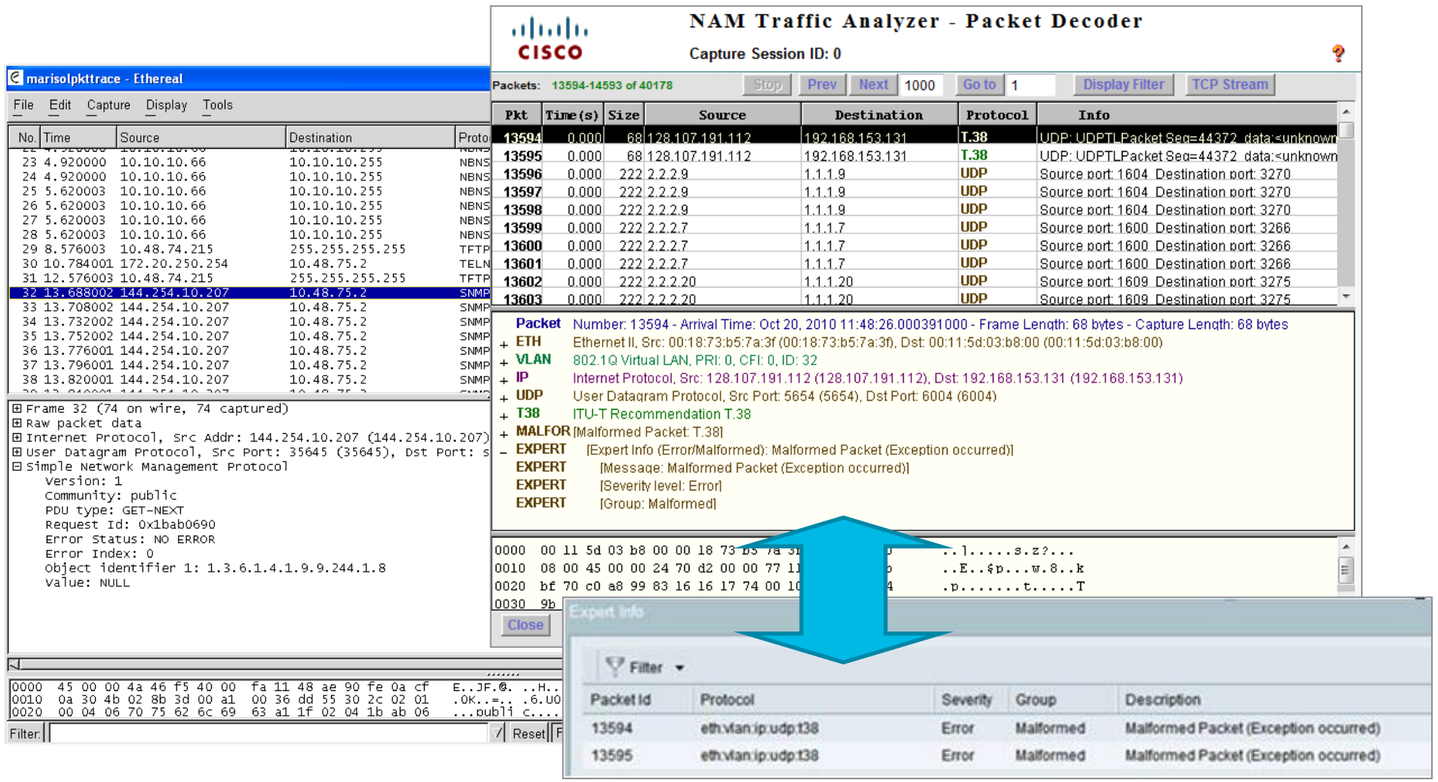
decode keyword triggers policy

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

EPC for the 4500

Configuration Very Similar to Routers

```
Monitor capture MyCaptur buffer circular size 50 access-list MyCaptureACL
monitor capture MyCaptur buffer size 10 int gi 1/35 both

monitor capture MyCaptur start
monitor capture MyCaptur stop

monitor capture MyCaptur export bootflash:phoneme.cap
```

EPC 4500 Config and Output

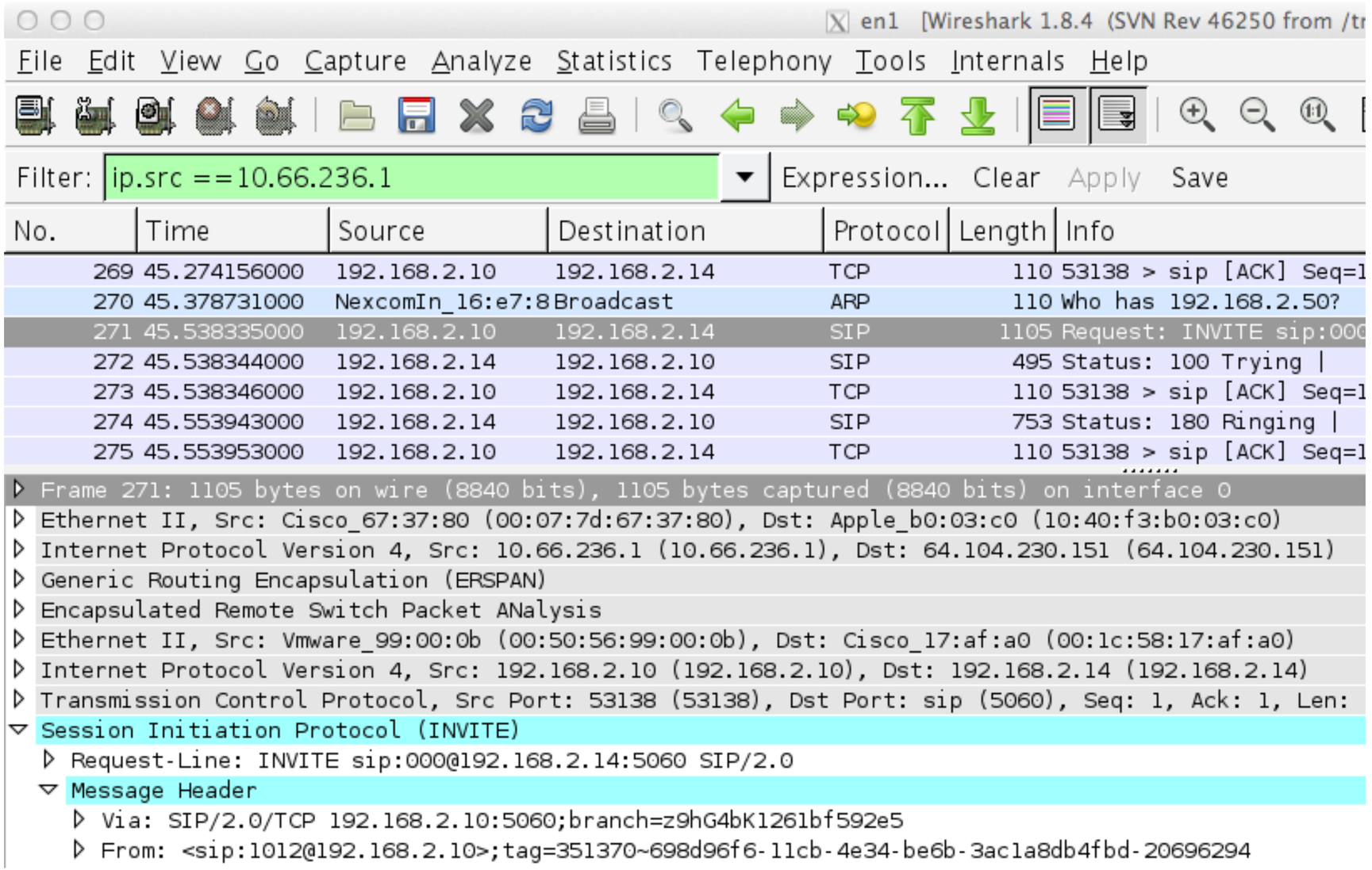
```
BNELAB-4507-R#show monitor capture MyCaptur

Status Information for Capture MyCaptur

  Target Type:

   Interface: GigabitEthernet1/35, Direction: both

   BNELAB-4507-R#sho monitor capture MyCaptur buffer

   ….

   110.078991 192.168.6.50 -> 192.168.2.20 DNS Standard query AAAA bnecucm9-P2.bnelab.cisco.com
   110.116999 192.168.6.50 -> 192.168.2.20 DNS Standard query A bnecucm9-P2.bnelab.cisco.com
   110.206990 192.168.6.50 -> 192.168.2.20 DNS Standard query AAAA bnecucm9-P2.bnelab.cisco.com
   111.100993 192.168.6.50 -> 10.66.238.80 TCP 53079 > 6970 [SYN] Seq=0 Win=8192 Len=0 MSS=1340
   111.100993 192.168.6.50 -> 10.66.238.80 TCP 53079 > 6970 [ACK] Seq=1 Ack=1 Win=8192 Len=0
   111.103999 192.168.6.50 -> 10.66.238.80 TCP 53079 > 6970 [PSH, ACK] Seq=1 Ack=1 Win=8192 Len=67
   111.109004 192.168.6.50 -> 10.66.238.80 TCP 53079 > 6970 [FIN, ACK] Seq=68 Ack=66 Win=8192 Len=0

…
```

ERSPAN – Span Over Layer 3 Transport

- Currently only available in the 6500
- Wraps all traffic into a GRE tunnel
- Can land on another 6500, NAM, or PC/Mac running wireshark

```
monitor session 1 type erspan-source
 source interface Gi3/4
 destination
  erspan-id 1
  ip address X.X.X.X (address of PC or Mac running Wireshark)
  origin ip address 10.66.236.1
```

ERSPAN



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

Config Management

Show Archive

```
BNELAB-4507-R#sho archive
The maximum archive configurations allowed is 14.
There are currently 8 archive configurations saved.
The next archive file will be named bootflash:/configs/-<timestamp>-
8
 Archive #  Name
   1        bootflash:/configs/-Jan--3-21-44-44.863-0
   2        bootflash:/configs/-Jan--3-21-49-22.526-1
   3        bootflash:/configs/-Jan--3-21-53-04.400-2
   4        bootflash:/configs/Jan--4-04-47-21.617-3
   5        bootflash:/configs/Jan--4-04-49-01.105-4
   6        bootflash:/configs/Jan--4-04-50-48.437-5
   7        bootflash:/configs/Jan--4-04-51-45.205-6
   8        bootflash:/configs/Jan--4-04-53-06.706-7 <- Most Recent
   9
   10
```

Config Management

Show archive config diff

```
BNELAB-4507-R#sho arch config dif  bootflash:/configs/Jan--4-04-49-01.105-4
!Contextual Config Diffs:
interface GigabitEthernet1/1
 +ip policy route-map Texas
interface Loopback0
 -description Management Address
interface GigabitEthernet1/1
 -ip policy route-map texas

BNELAB-4507-R#
```

Config Management

Config replace

```
BNELAB-4507-R#configure replace bootflash:/configs/Jan--4-04-49-01.105-4
This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. Enter Y if you are sure you want to proceed. ? [no]: y
Total number of passes: 1
Rollback Done
```

Config Management

Config Lock – Managing Contention

- Config Lock

```
BNELAB-4507-R#configure terminal lock
Configuration session is locked. The lock will be cleared once you exit out \
          of configuration mode.
```

```
BNELAB-4507-R#conf t
Configuration mode is locked by process '140' user 'unknown' from terminal '1'. \
          Please try later.


BNELAB-4507-R#clear config lock
Process <140> is holding the config session lock !
Do you want to clear the lock?[confirm]
BNELAB-4507-R#
```

Config Management

Local Logging of Config Activity

```
archive
 log config
  logging enable
  logging persistent auto
```

```
BNELAB-4507-R#sho archive log config all
 idx   sess           user@line      Logged command
..
  165    34           vty1@vty1     |username admin privilege 15
  166    34           vty1@vty1     |!config: USER TABLE MODIFIED
  167    34           vty1@vty1     |username pethomas privilege
  168    34           vty1@vty1     |!config: USER TABLE MODIFIED
  169    34           vty1@vty1     |line vty 0 4
  170    34           vty1@vty1     | login local
  171     0   unknown user@vty2     |!exec: enable
  172    35       pethomas@vty1     |interface GigabitEthernet1/35
  173    35       pethomas@vty1     | description test
  174     0   unknown user@vty2     |!exec: enable

BNELAB-4507-R#
```

Agenda

- What is Smart Operations?
- Smart Install
- Auto Smartports
- Other Gems
- EEM
- TCL

What is Embedded Event Manager (EEM)?

- Flexible and Powerful tool within Cisco IOS Software
- Takes action on user enabled system events
- Events trigger the execution of user defined set of actions
  - User defined actions written in CLI or Tool Command Language (Tcl)
- Consistent behaviour across Catalyst switches and Cisco Routers
- EEM: Catalyst switches with IP Base feature set and above

Embedded Event Manager Benefits

- Automate operational activities done manually
- Change the behaviour of Catalyst Switch or Cisco Router
  - –Customise switch or router behaviour
  - –Change configuration dynamically
- Notify network admin on event
  - –Eg: Send email on temperature threshold crossing

Network Automation

Example: Rural Road Monitoring

Problem: Rural Roads Subject to Flooding Need to be Centrally Monitored from Traffic Operations Centre (TOC)

Solution: Use Network Automation on a DC Powered ISR to Detect Raising Water Levels and Alert the TOC via 3G.

1. Deploy DC-powered ISR, pole-mounted with solar panel, battery pack and rugged housing
2. Connect ‘unused’ switchports to custom water detectors
3. EEM triggers upon interface loopback / error-disable state changes
4. EEM sends alert/clear messages to TOC

Why use Embedded Event Manager

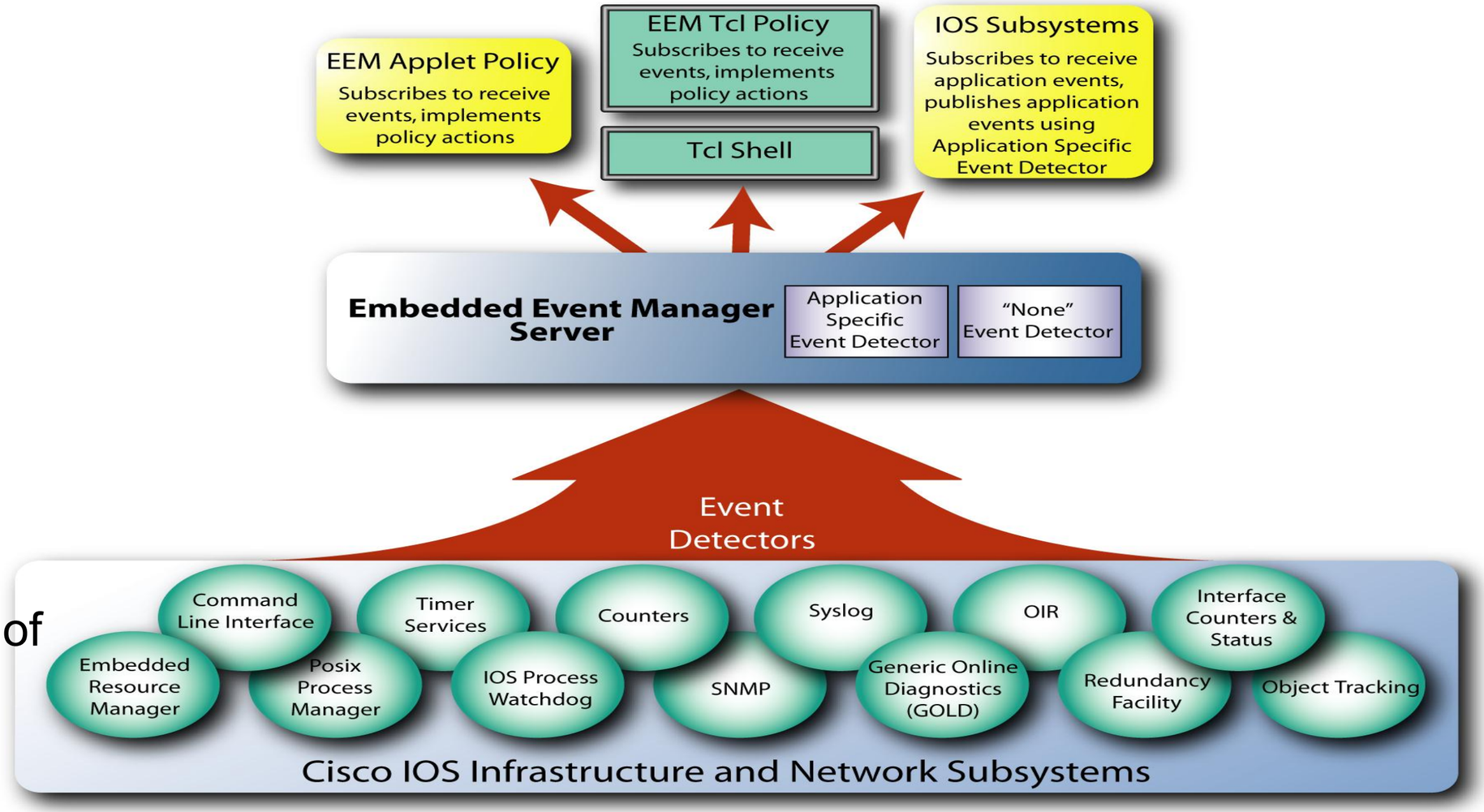
Do You Read syslog msgs Regularly???

- EEM can read syslog msgs for you.
- EEM can perform actions for you
- You don’t have to read syslogs!

EEM Basic Architecture

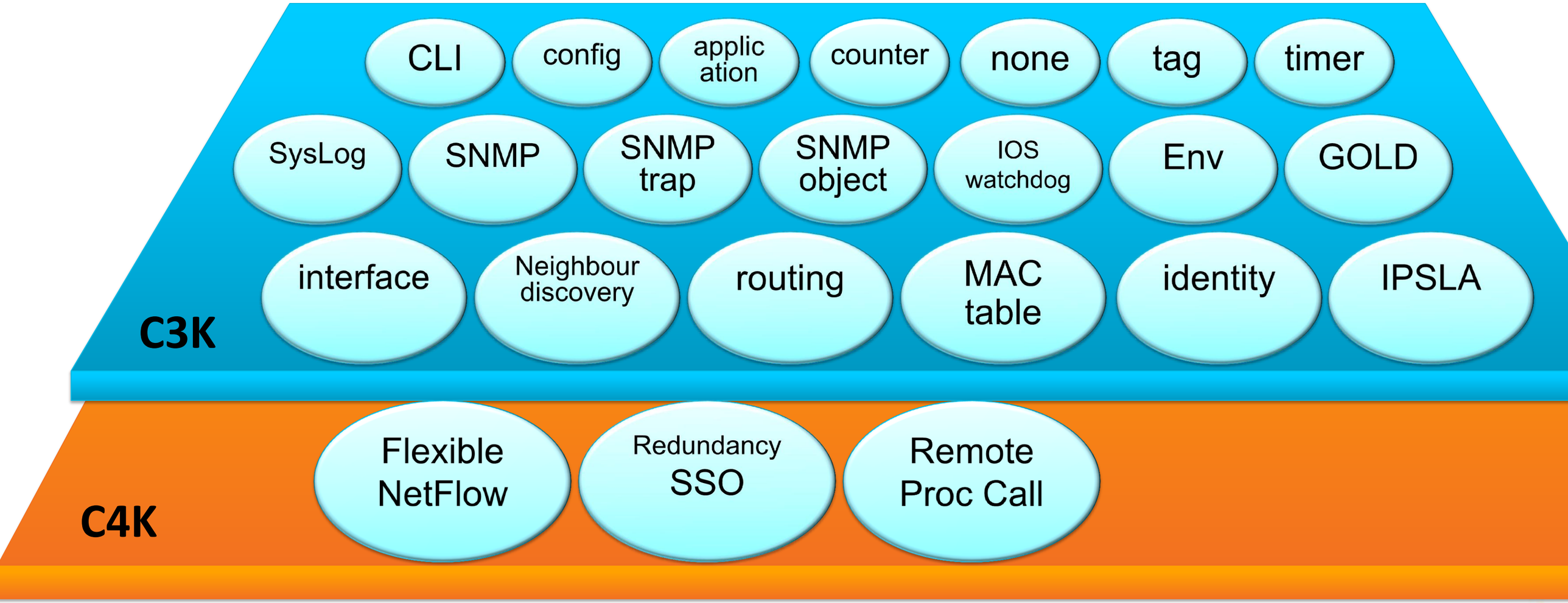
- Policies (scripts)
  - –Applets
  - –Tcl-based
  - –IOS.sh
- EEM Server
  - –The “brain” of the system
- Event Detectors
  - –“watch for events of interest”

All within Cisco IOS



Embedded Event Manager

Event Detectors Supported



Embedded Event Manager

Event Detectors supported

REFERENCE

```
4500E(config)#event manager applet test
4500E(config-applet)#event ?
 application          Application specific event
  cli                  CLI event
  config               Configuration policy event
  counter              Counter event
  env                  Environmental event
  gold                 GOLD event
  identity             Identity event
  interface            Interface event
  ioswdsysmon          IOS WDSysMon event
  ipsla                IPSLA Event
  mat                  MAC address table event
  neighbor-discovery   Neighbor Discovery event
  nf                   NF Event
  none                 Manually run policy event
  oir                  OIR event
  rf                   Redundancy Facility event
  routing              Routing event
  rpc                  Remote Procedure Call event
  snmp                 SNMP event
  snmp-notification    SNMP Notification Event
  snmp-object          SNMP object event
  syslog               Syslog event
  tag                  event tag identifier
  timer                Timer event
```

```
3750X(config)#event manager applet test
3750X(config-applet)#event ?
  application          Application specific event
  cli                  CLI event
  config               Configuration policy event
  counter              Counter event
  env                  Environmental event
  gold                 GOLD event
  identity             Identity event
  interface            Interface event
  ioswdsysmon          IOS WDSysMon event
  ipsla                IPSLA Event
  mat                  MAC address table event
  neighbor-discovery   Neighbor Discovery event
  none                 Manually run policy event
  oir                  OIR event
  routing              Routing event
  snmp                 SNMP event
  snmp-notification    SNMP Notification Event
  snmp-object          SNMP object event
  syslog               Syslog event
  tag                  event tag identifier
  timer                Timer event
```

Using Syslog to Extend Archive

- Archive infrastructure normally manually triggered
- Automate archive (just like Cisco Prime)
- Look for Syslog Msg (%SYS-5-CONFIG_I: Configured from console)

```
event manager applet ArchiveAllConfigChanges
 description Captures any sneaky changes
 event syslog pattern "SYS-5-CONFIG_I"
 action 2.0 cli command "enable"
 action 3.0 cli command "archive config"
```

EEM with Flexible NetFlow

REFERENCE

Problem: CPU processing required to respond to packets with TTL values of one or less.

- (using TTL-exceeded packets)

Cannot forward a packet with a TTL value Less than one.

Results in a Denial of Service attack

Packet TTL=1

Flexible NetFlow Configuration

```
flow record ttl
 match ipv4 ttl
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes
 collect counter packets
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
flow monitor ttl
 record ttl
 cache timeout inactive 20
 cache timeout active 30
interface GigabitEthernet8/47
 switchport access vlan 50
 switchport mode access
  ip flow monitor ttl input
```

EEM Configuration

- NetFlow Counters available for EEM
- E.g. look for packets with Time To Live (TTL) less than or equal to 1.
- EEM can also be configured to start a wireshark capture

```
event manager applet ttl
 event nf monitor-name "ttl" event-type create event1 entry-value "2" field ipv4 ttl entry-op lt

 action 1.0 syslog msg "TTL=1 frames from $_nf_source_address to $_nf_dest_address detected."

action 2.6 cli command "conf t"
 action 2.7 cli command "int gi 2/2"
 action 2.8 cli command "shut"
```

EEM CLI Trigger

```
3845-Rack5#reload reason
% Incomplete command.

3845-Rack5#reload reason ?
Please enter reload reason

3845-Rack5#reload reason The Boss is looking ?
  <cr>

3845-Rack5#reload reason The Boss is looking

Proceed with reload? [confirm]n
```

```
event manager applet cli-sync
 event cli pattern "^debug all" sync yes
 action 1.0 puts "Do you have your resume up to date[y|n]:"
 action 2.0 gets response
 action 3.0 if $response eq y goto 5.0
 action 4.0 puts "Not debugging your job is safe"
 action 4.1 exit 0
 action 5.0 puts "Start looking for a new job"
 action 5.1 exit 1
```

Regex Tester http://www.regextester.com/

Reload Reason

```
event manager applet GetReloadReason
 event cli pattern "^reload" sync yes
 action 1.0 comment Check to see if the Reason command line option was used
 action 1.2 regexp "reason" "$_cli_msg"
 action 2.0 if $_regexp_result ne 1
 action 2.2  puts "Please enter reason for reload"
 action 2.4  gets response
 action 2.6  syslog priority emergencies msg "Reload initiatated - reason $response"
 action 2.8  cli command "enable"
 action 3.0  cli command "reload reason $response"
 action 3.2  exit 0
 action 4.0 else
 action 4.2  comment A reason was included on command line continue
 action 4.4  exit 1
 action 5.0 end
end
```

Monitoring Failed SLAs

Use Standard IP SLA infrastructure

```
ip sla 10
 icmp-echo 192.168.55.1
 frequency 30
ip sla schedule 10 life forever start-time now
```

```
track 10 ip sla 10 reachability
 delay down 10 up 20
```

```
event manager applet email_loopback_unreachable
 event track 10 state down
 action 1.00 syslog msg "Ping has failed to loopback”
 ……
```

EEM Working Files and Email - 1

Define the Environment Variables

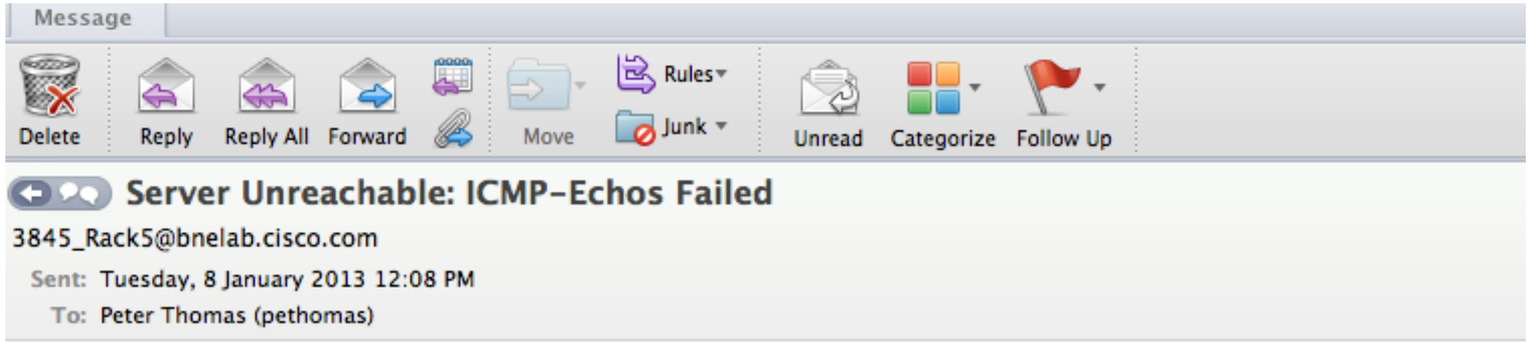
- These variables accessing with $ Prefix in script

```
event manager environment _email_to pethomas@cisco.com
event manager environment _email_from 3845_Rack5@bnelab.cisco.com
event manager environment _email_server ItsASecret.cisco.com
event manager environment traceroute_ip 10.66.236.1
```

EEM Working Files and Email - 2

```
event manager applet email_loopback_unreachable
 event track 10 state down
 action 1.00 syslog msg "Ping has failed to loopback"
 action 1.20 comment Spawn off trace
 action 1.22 policy tcltrace.tcl
 action 2.00 comment Send brief email alert while traceroute is completing
 action 2.20 mail server "$_email_server" to "$_email_to" from  \
          "$_email_from" subject "Loopback Down" body "Connectivity Lost to $traceroute_ip"
 action 3.20 cli command "enable"
 action 3.22 cli command "del /force flash:server_unreachable"
 action 3.24 cli command "show clock | append server_unreachable"
 action 3.26 cli command "show ip route | append server_unreachable"
 action 3.30 comment Wait for Traceroute to complete
 action 3.32 wait 20
 action 4.00 comment Append info and email off
 action 4.20 cli command "more flash:/TraceResults.txt | append server_unreachable"
 action 4.22 cli command "more flash:server_unreachable"
 action 4.24 mail server "$_email_server" to "$_email_to" from
          "$_email_from" subject "Server Unreachable: ICMP-Echos Failed" body "$_cli_result"
end
```

You've Got Mail




```
12:07:56.790 aest Tue Jan 8 2013

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is 192.168.2.1 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/28928] via 192.168.2.1, 00:34:10, GigabitEthernet0/0
                [170/28928] via 10.66.238.65, 00:34:10, GigabitEthernet0/1
      10.0.0.0/8 is variably subnetted, 35 subnets, 7 masks
D        10.1.103.0/24 [90/3072] via 192.168.2.1, 00:34:10, GigabitEthernet0/0
                       [90/3072] via 10.66.238.65, 00:34:10, GigabitEthernet0/1
D        10.3.3.0/24
           [90/26880256] via 192.168.2.1, 00:34:10, GigabitEthernet0/0
           [90/26880256] via 10.66.238.65, 00:34:10, GigabitEthernet0/1
D        10.8.254.21/32
           [90/130816] via 192.168.2.1, 00:34:10, GigabitEthernet0/0
           [90/130816] via 10.66.238.65, 00:34:10, GigabitEthernet0/1
```

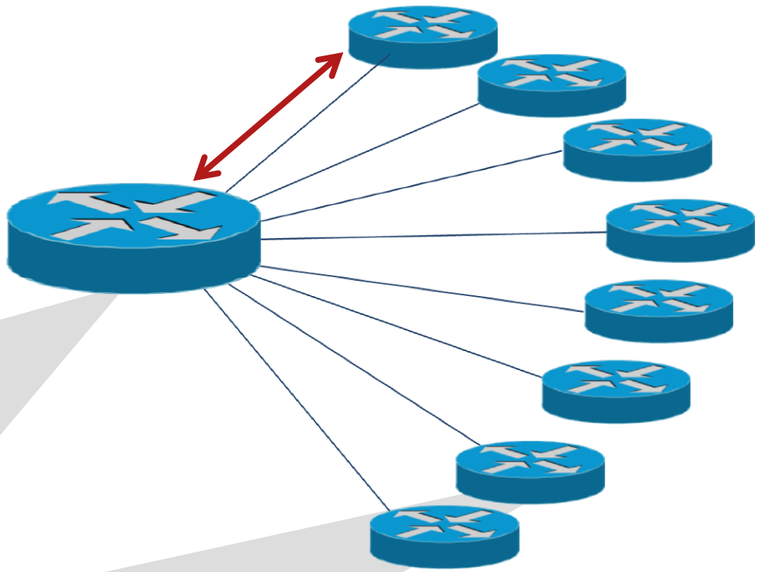
Auto IP SLA – Don't Touch Your Hub

Some IP SLA Topologies …

- … are naturally Hub and Spoke
- … have a large number of Spokes with similar IP SLA requirements
- … consist of dynamically joining / disappearing Spokes

New 15.1T

```
ip sla auto template type ip udp-jitter my-ipsla-template
  parameters
    request-data-size 64
    num-packets 1000
ip sla auto schedule my-ipsla-schedule
  frequency 45
  start-time now
ip sla auto endpoint-list type ip my-ipsla-endpoints
  discover
    ageout 36000
ip sla auto group type ip my-ipsla-group
  schedule my-ipsla-schedule
  template udp-jitter my-ipsla-template
  destination my-ipsla-endpoints
```



```
ip sla responder auto-register 10.10.10.2 endpoint-list my-ipsla-endpoints
```

EMM – What is there isn't a Syslog Msg

Use Watchdog timer

```
event manager applet EmergencyCallCheck
 event timer watchdog name EmergencyTimer time 20 maxrun 5000
 action 1.0 puts "Executing Emergency check"
 action 1.1 cli command "enable"
 action 2.0 cli command "show call active voice compact | inc P000"
 action 2.2 regexp "P000" "$_cli_result"
 action 3.0 comment Check if any lines contain P000 if not exit
 action 3.2 if $_regexp_result eq 1
 action 3.4  syslog msg "Emergency Services Called"
 action 3.6  mail server "$_email_server" to "$_email_to" from  \
        "$_email_from" subject "Emergency Services Called" \
        body "$_cli_result"
 action 4.0  comment Collect More information to send a second email
 action 4.2  cli command "sho sip calls"
 action 4.4  mail server "$_email_server" to "$_email_to" from \
        "$_email_from" subject "Emergency Services Called - Detail" \
        body "$_cli_result"
 action 5.0 end
```

EMM History

```
3845-Rack5#sho event manager history events
No.   Job Id  Proc  Status    Time    Event Type          Name
1     38023   Actv  success   Tue ..  timer watchdog      applet: EmergencyCallCheck
2     38024   Actv  success   Tue ..  timer watchdog      applet: EmergencyCallCheck
3     38025   Actv  success   Tue ..  timer watchdog      applet: EmergencyCallCheck
4     38026   Actv  success   Tue ..  timer watchdog      applet: EmergencyCallCheck
5     38027   Actv  success   Tue ..  timer watchdog      applet: EmergencyCallCheck
6     38028   Actv  success   Tue ..  timer watchdog      applet: EmergencyCallCheck
7     38029   Actv  success   Tue ..  syslog              applet: ArchiveAllConfigChanges
8     38031   Actv  success   Tue ..  none                script: tcltrace.tcl
9     38032   Actv  success   Tue ..  timer watchdog      applet: EmergencyCallCheck
10    38030   Actv  success   Tue ..  track               applet: email_loopback_unreachable
```

EMM Real Time Captures While You Sleep

- Performance Monitor – ISR-G2
- Real time monitoring of traffic flows
- Ability to alert on traffic behaviours such as loss/jitter
- Use existing building blocks – EPC and Performance Monitor
- What about system restart?

Performance Monitor - 1

Define the Traffic to Monitor

```
class-map match-all AudioRTP
 match protocol rtp audio
policy-map type performance-monitor pm-RTP-Audio
 class AudioRTP
   flow monitor PerfMon
   monitor parameters
    interval duration 15
    flows 100
   react 1 transport-packets-lost-rate
    threshold value gt 0.05
    alarm severity alert
    action syslog
```

Performance Monitor - 2

Apply Performance Policy to Interface

```
interface GigabitEthernet0/1
 description link to bne-2951-local
 ip address 10.66.236.218 255.255.255.252
 ip wccp 62 redirect in
 ip flow ingress
 ip flow egress
 duplex auto
 speed auto
 service-policy type performance-monitor input pm-RTP-Audio
 service-policy type performance-monitor output pm-RTP-Audio
 mace enable
```

Performance Monitor - 3

Monitoring via the CLI

```
2951-HQ#sho policy-map type performance-monitor  int gi 0/1 \
        input class AudioRTP

GigabitEthernet0/1

  Service-policy performance-monitor input: pm-RTP-Audio

    Class-map: AudioRTP (match-all)
      9820 packets, 2101480 bytes
      5 minute offered rate 44000 bps, drop rate 0000 bps
      Match: protocol rtp audio
      media-monitoring:
       flow monitor PerfMon
```

Performance Monitor - 4

The Syslog Alerts

```
Jan  8 03:45:15.082: %PERF_TRAFFIC_REACT-1-ALERTSET: TCA RAISE.
Detailed info: Threshold value crossed - current value 0.26%
Flow info: ipv4 source address 10.66.236.212, ipv4 destination address 192.168.2.14,\
          transport source-port 20544, transport destination-port 18282, ip protocol 17,
Policy info: Policy-map pm-RTP-Audio, Class AudioRTP
React info: id 1, criteria transport-packets-lost-rate, severity alert,
          alarm type discrete, threshold range (0.05%, 100.00%]
```

```
Jan  8 03:45:30.124: %PERF_TRAFFIC_REACT-1-ALERTCLEAR: TCA CLEAR.
Detailed info: Threshold value crossed - current value 0.00%
Flow info: ipv4 source address 10.66.236.212, ipv4 destination address 192.168.2.14, \
          transport source-port 20544, transport destination-port 18282, ip protocol 17,
Policy info: Policy-map pm-RTP-Audio, Class AudioRTP
React info: id 1, criteria transport-packets-lost-rate, severity alert,
          alarm type discrete, threshold range (0.05%, 100.00%]
```

EMM Tying it all Together

```
event manager applet StopCaptureOnAlert
 event syslog pattern "PERF_TRAFFIC_REACT-1-ALERTSET: TCA RAISE" maxrun 240
 action 1.0 puts "High traffic loss encountered, sending capture to NOC"
 action 2.0 cli command "enable"
 action 3.0 cli command "monitor capture point stop cp-Wan"
 action 3.5 cli command "monitor capture buffer Capture-It-All \
        export tftp://192.168.2.20/HQ_Wan.pcap"
 action 4.0 cli command "monitor capture point start cp-Wan"
 action 5.0 puts "Upload Completed - capture restarted"
```

EMM – Dealing with a System Reload

Use Syslog Detector

```
event manager applet StartCaptureOnBoot
 event syslog pattern "SYS-5-RESTART" maxrun 90
 action 1.0 puts "Waiting for things to settle after boot"
 action 1.2 wait 60
 action 1.4 cli command "enable"
 action 2.0 puts "Creating Capture Buffer"
 action 2.2 cli command "monitor capture buffer Capture-It-All"
 action 3.0 cli command "monitor capture buffer Capture-It-All size 40000  \
                 max-size 1500 circular "
 action 4.0 cli command "monitor capture buffer Capture-It-All filter access-list 100"
 action 5.0 cli command "monitor capture point ip cef cp-Wan gi 0/1 both"
 action 6.0 cli command "monitor capture point associate cp-Wan Capture-It-All"
 action 7.0 cli command "monitor capture point start cp-Wan"
 action 7.2 puts "Capture Started"
```

Embedded Event Manager

Applet vs. Tcl Policy

EEM Applet

- EEM Applet
- Easier programming language
- Can be seen as part of the switch config and modified/tweaked online
- Limited regexp capabilities
- If goal is too complex can become cumbersome

EEM Tcl Policy

- All Tcl built-in powerful functionalities
- Expandable with existing libraries
- Better for complex solutions

TCL (Tools Command Language)

- Around for while
- Multi-platform (IOS, PC, Mac)
- Extends EMM capabilities.
  - Create TCL Script
  - Copy to Router (or distribution point)
  - Register
  - Call via Policy Step

TCL Create the Script

- Create file – WordPad isn't cool, leads to head scratching

```
::cisco::eem::event_register_none maxrun 90

namespace import ::cisco::eem::*
namespace import ::cisco::lib::*

if { [catch {cli_open} result] } {
   error $result $errorInfo
}


array set cli $result

if { [catch {cli_exec $cli(fd) "traceroute $traceroute_ip"} result] } {
  error $result $errorInfo
}

puts $result
set fd [open "flash:/TraceResults.txt" "w"]
puts $fd $result
close $fd


catch {cli_close $cli(fd) $cli(tty_id)}
}
```

EEM Registration

LinkUpApplyConfig

EEM Tcl Policy

- Step 1 – Register User Directories
  - Register user policy directory and user library directory
- Step 2 – Code Policies Offline
  - No online editor available, but tclsh for test
- Step 3 – Download Policy
  - Download TCL policies using standard IOS file transfer mechanisms
  - Copy policy to all stack members
  - Support script auto refresh from remote location
- Step 4 – EEM Environment Variable Configuration
- Step 5 – Register Policy
  - Register policy to TCL policy engine

```
mkdir flash:/eem
event manager directory user policy flash:/eem
event manager directory user library flash:/eemlib
```

```
copy tftp flash1:/eem
Address or name of remote host []? 10.1.88.9
Source filename []? LinkUpApplyConfig.tcl
Destination filename [LinkUpApplyConfig.tcl]?
eem/LinkUpApplyConfig.tcl
Accessing tftp://10.1.88.9/LinkUpApplyConfigT.tcl...!
1232 bytes copied in 0.620 secs (1987 bytes/sec)

mkdir flash2:/eem
copy flash1:/eem/LinkUpApplyConfig.tcl flash2:/eem/

event manager update user policy group “*.tcl” repository
tftp://2.2.2.2/users/mpessi/eem_1
```

```
event manager environment _ConfigCommands speed duplex
event manager environment _IfSFP 1000BaseTX 100BaseFX
```

```
event manager policy LinkUpApplyConfig.tcl type user
```

TCL Library and Script Load

```
mkdir flash:/eem
event manager directory user policy flash:/eem
event manager directory user library flash:/eemlib
```

```
Copy tftp flash:
```

Registering and Calling TCL Script

```
event manager policy tcltrace.tcl type user
……
event manager applet email_loopback_unreachable
 event track 10 state down
 action 1.00 syslog msg "Ping has failed to loopback"
 action 1.20 comment Spawn off trace
 action 1.22 policy tcltrace.tcl
```

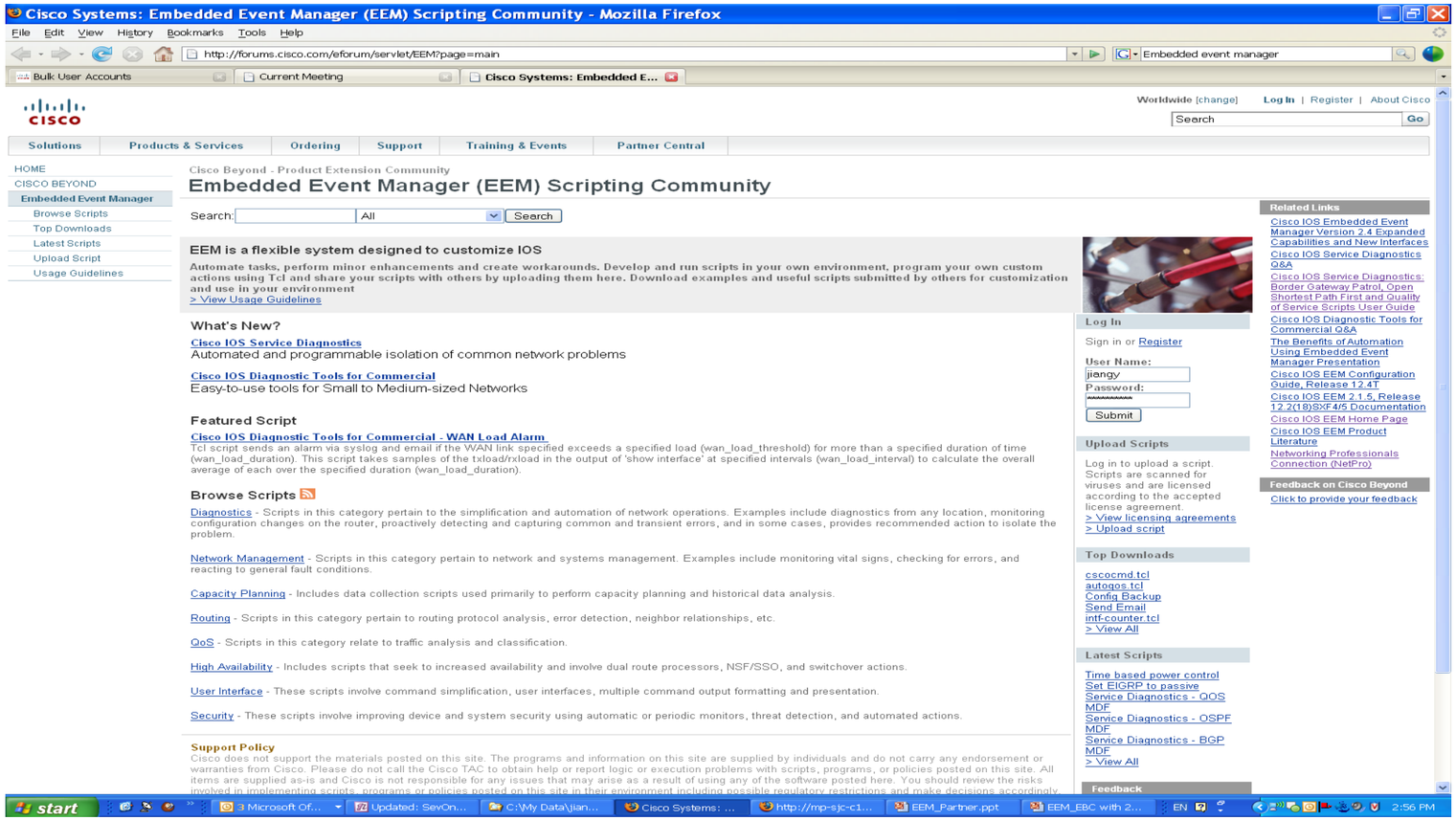
Updating TCL Scripts

```
3845-Rack5#event manager update user policy name "tcltrace.tcl"  \
        repository tftp://192.168.2.20/eem

%EEM: Update will use the repository path: tftp://192.168.2.20/eem
%EEM: Attempting to copy tftp://192.168.2.20/eem/tcltrace.tcl to \
        flash:/eem/tcltrace.tcl
Loading eem/tcltrace.tcl from 192.168.2.20 (via GigabitEthernet0/0): !
[OK - 450 bytes]

%EEM: Copied 450 bytes from tftp://192.168.2.20/eem/tcltrace.tcl to \
        flash:/eem/tcltrace.tcl
%EEM: Policy tcltrace.tcl has been successfully copied and re-registered
3845-Rack5#
```

Cisco Beyond - Product Extension Community

EEM Scripting Community

- Open source scripts, share, upload, download, learn by example
- Categories include: Ntwk mgmt., Diagnostics, Routing, QoS, High availability, User interface, Security etc.
- Comments, ratings, community managed forum



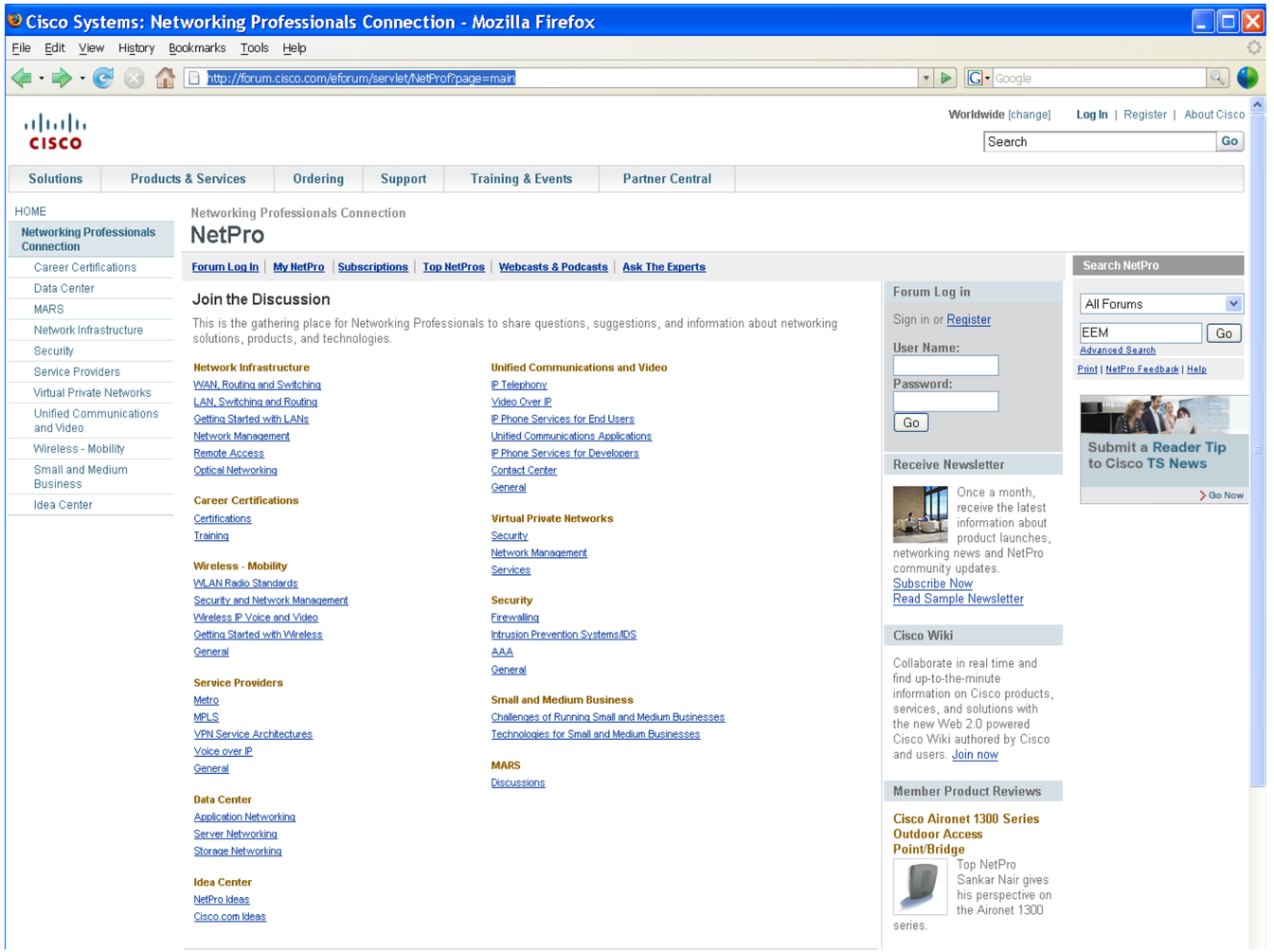
http://cisco.com/go/ciscobeyond

Other EEM Support Resources

- EEM Cisco.com web site: http://www.cisco.com/go/eem
- NetPro Forum (http://forum.cisco.com/eforum/servlet/NetProf?page=main)

  -- Search the forum for EEM related discussions

  -- Post your question to get answer from EEM experts
- Email askabouteem@cisco.com



Embedded Event Manager – Summary

- Built-in in IOS
- Dynamic problem solving
- Manageable Learning Curve – Support and Examples online
- Different Scripting Options, not just for nerds
- Questions ???

Smart Operations Summary

- Smart Operations –tools available in IOS today
- Smart Install – automate the process of installing switches
- Auto Smartports – Device based automated configuration
- The Hidden Gems – continued innovation in the platform
- EEM –event based dynamic network configuration

- Questions?

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww

Cisco live!