Cisco Embedded Automation Systems - EASy
Embedded Packet Capture

January 2010

Objective

Objective

- **Problem:** A certain traffic pattern is causing problems on the network, and the packets must be captured and analyzed in order to determine the cause
- **Solution:** Use the Embedded Packet Capture (EPC) feature in Cisco IOS® Software Release 12.4(20)T and higher to capture the network traffic into an internal capture buffer; then, using the Embedded Event Manager (EEM), the capture can be automatically started and stopped as required—once the required network traffic has been captured, tools such as Wireshark can be used to analyze the packets

See: http://www.cisco.com/en/US/prod/collateral/losswrel/ps6537/ps6555/ps9913/datasheet_c78-502727.html

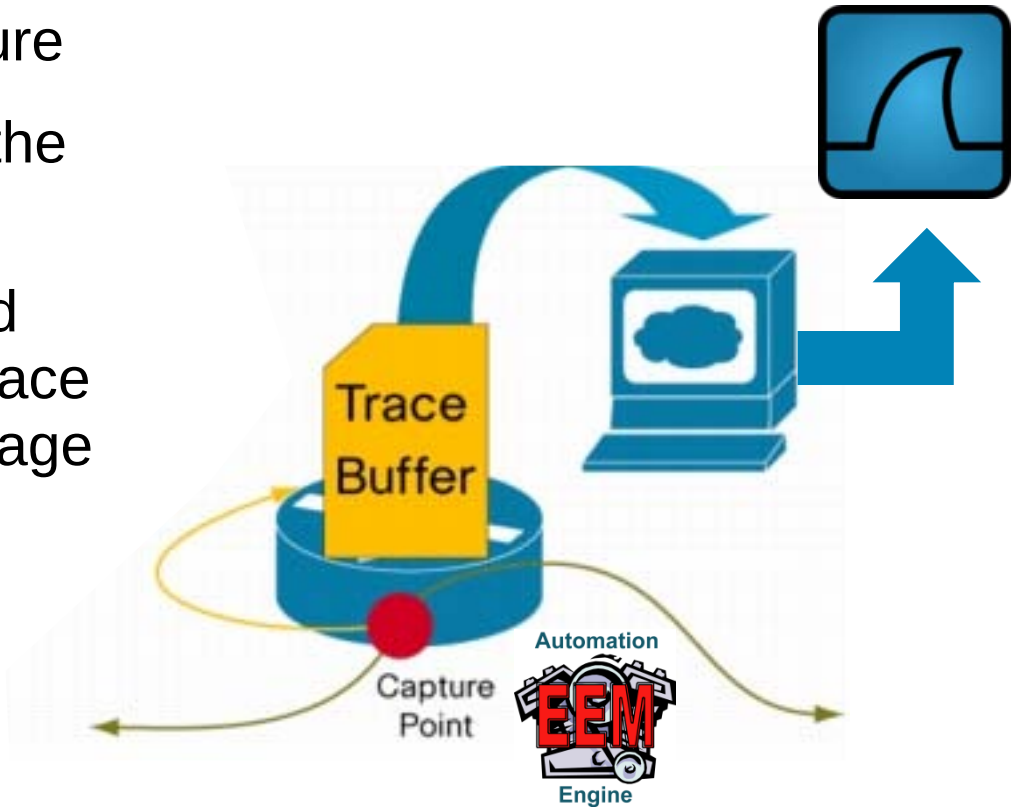
Overview

Application or Service	Troubleshooting
Technology	Embedded Packet Capture
Problem	Certain network traffic is causing problems, either on the local device or on the network as a whole. Troubleshooting the issue involves capturing and analyzing the problematic traffic.
Impact	The network may become unstable, performance may suffer, certain users may not be able to connect to certain services, and so on.
Non-EASy Solution	An external sniffer would need to be set up and started at the required time. Additionally, if EPC were used without EASy, one would have to monitor the capture buffer and export the files by hand when the buffer is full.
Benefit of EASy Solution	EASy allows an administrator to automate the start of the EPC session as well as have EEM watch for a “buffer full” condition. When that condition occurs, the capture files are automatically exported for analysis.
Category	Diagnostics

Background

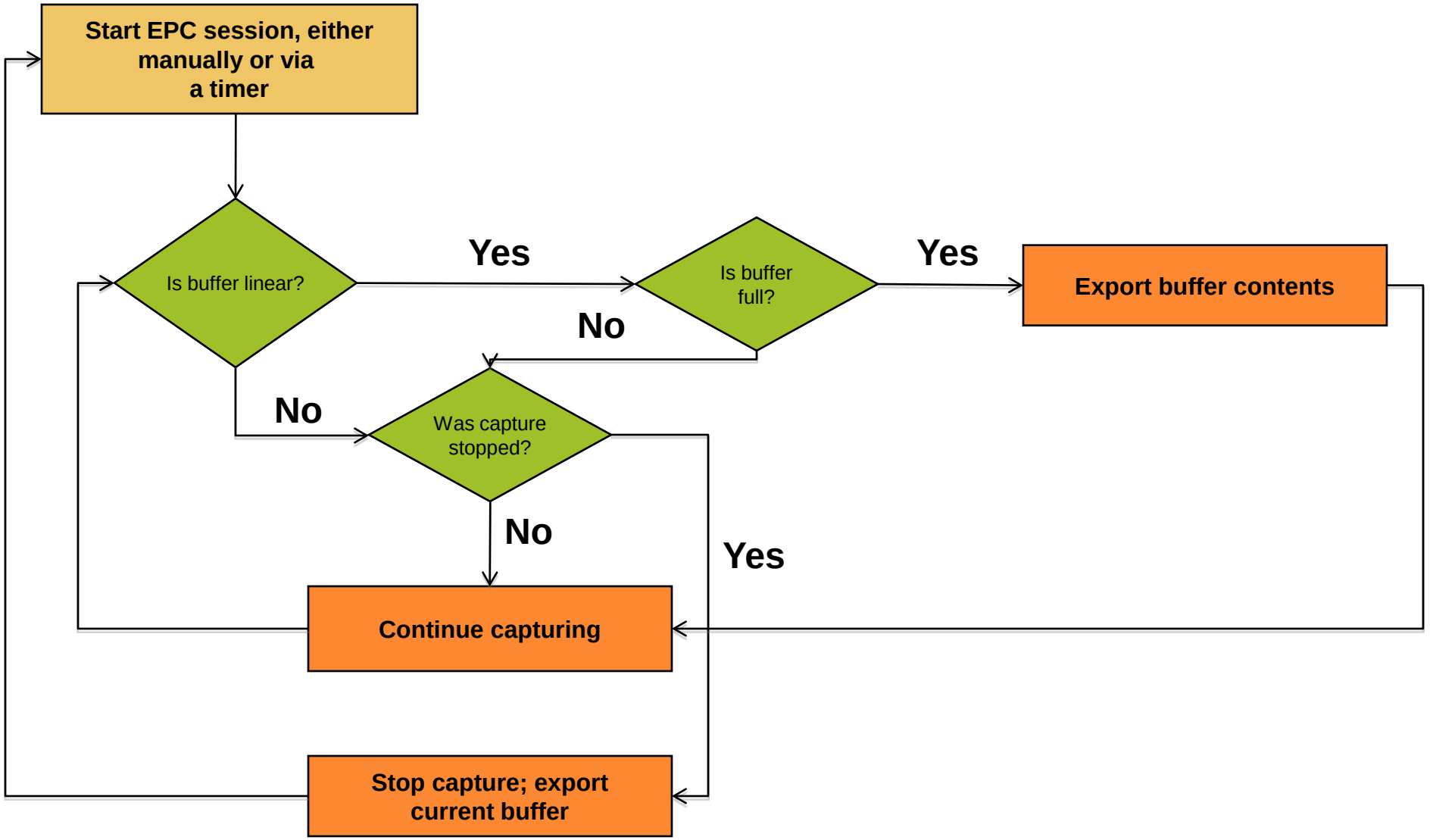
Background

- Use EEM to start the capture
- EEM checks to see when the buffer is full
- EEM stops the capture and informs the user that the trace is ready via a syslog message
- The resulting trace can be analyzed in Wireshark



Pseudo Code

Solution Flowchart



Pseudo Code: Core Script

The main script listens for an EEM application event sent from either a stop or a buffer full event.
Then it will export the capture buffer to the configured location.

```
set pcap_timername   "pcap_timer"
set pcap_cleanup      0
set pcap_timer_id    -1
set mytrigger        $arr_einfo(data1)

if { [catch { foreach {var value} [context_retrieve PCAP] {set $var $value;
#puts "\n\n*** DEBUG context_retrieve var = $var  value = $value"; } }
result]} {
   error "*** ERROR: no context PCAP was retrieved!" $errorInfo
}

#puts "*** DEBUG *** Exporting capture buffer $pcap_var_capbuf1 ..."
if {[catch { ExportCapBuffer $pcap_var_capbuf1 $pcap_var_export_url $pcap_ctr
} result]} {
   error "*** ERROR: $result" $errorInfo
}

set export_file $result

#puts "*** DEBUG *** Clearing capture buffer $pcap_var_capbuf1..."
if {[catch { ClearCapBuffer $pcap_var_capbuf1 } result]} {
   error "*** ERROR: $result" $errorInfo
}
```

Retrieve previously saved state.

Export the capture buffer to the desired URL (this URL can be a local flash destination or a network server such as TFTP).

Empty the capture buffer so more data can be captured (if the buffer type is linear).

Pseudo Code: Core Script

```
if { $pcap_ctr < $pcap_var_max_capnum && $pcap_cleanup == 0 } {
   #puts "*** DEBUG *** Num Capture Buffers Exported = $pcap_ctr"
   if {[catch { StartCapPoint $pcap_var_cappnt1 } result]} {
      error "*** ERROR: $result" $errorInfo
   }
   incr pcap_ctr 1

   if {[catch {context_save PCAP "pcap_*"} result]} {
      error "*** ERROR: $result" $errorInfo
   }
} else {
   #puts "*** DEBUG *** Stopping capture point $pcap_var_cappnt1 ..."
   if {[catch { StopCapPoint $pcap_var_cappnt1 } result]} {
      error "*** ERROR: $result" $errorInfo
   }

   set timer_trigger "triggered by expired timer"

   if {![string equal $mytrigger $timer_trigger]} {
      #puts "*** DEBUG *** Canceling timer $pcap_timername"
      array set time_remaining [timer_cancel event_id $pcap_timer_id]
   }
}

action_syslog msg "Successfully exported capture buffer for $pcap_var_cappnt1 to
$export_file"
```

If the number of captures does not exceed the configured maximum, restart the capture point.

Else, stop the capture point...

...and stop the max run timer.

Finally, send a syslog message informing the user where to find the exported capture file.

Overview

Components

Components

- **Hardware:** This package has been tested on a Cisco® 7200 Series Router running 12.4(24)T and a Cisco 2821 Integrated Services Router running 15.0(1)M; all platforms that support Embedded Packet Capture and Embedded Event Manager are supported
- **Topology:** This package runs on the device that supports EPC—such a device can exist anywhere in the network
- **Configurations:** The EASy package will walk the user through setting up an EPC capture point and capture buffer—it can optionally walk the user through creating an access list to filter what traffic is captured; all configuration changes will be presented to the user before committing them to the device

Components: EEM Policies

This package installs the following EEM policies:

ap_easy_epc_export.tcl	Script that exports the current capture buffer contents
no_easy_epc_start.tcl	Script to manually start the EPC packet capture; this script can be run from Cisco IOS® Software EXEC mode with the command “event manager run no_easy_epc_start.tcl”
no_easy_epc_stop.tcl	Script to manually stop the running EPC packet capture; this script can be run from Cisco IOS Software EXEC mode with the command “event manager run no_easy_epc_stop.tcl”
sl_easy_epc_fullbuffer.tcl	Script that watches for a BUFCAP-5-BUFFER_FULL syslog message, then calls ap_easy_epc_export.tcl to export the current buffer contents
tm_easy_epc_start.tcl	Optional script that allows one to start the EPC session at a specified time (or even periodically) using a cron entry; if enabled, the EASy Installer will prompt for the required cron entry
ts_easy_epc_stop.tcl	Script that waits until the maximum run timer for the EPC session (as specified by the user) expires; when it does, the capture will automatically be stopped and the buffer contents exported

Installation

EASy Installer

Preparing for Installation

- **Prerequisites**

  Cisco IOS® Software device capable of supporting EEM 2.1

  A device that supports the Embedded Packet Capture feature

  Typically, any device running Cisco IOS Software Release 12.4(20)T or higher is supported

- **Configuration:** No preconfiguration is required; the EASy Installer will guide the user through all configuration steps
- **EASy Installer:** Ensure that the EASy Installer is available:

```
Router#sh run | inc easy
alias exec easy_installer tclsh flash:/easy/easy_installer.tcl
```

Installing the Package

- If using the EASy Installer:

--debug option will add debugging information when executing

```
Router# easy_installer tftp://x.x.x.x/easy-packet-capture.tar flash:/easy
```

Installing the Package, cont.

```
Router# easy-installer tftp://172.18.123.33/easy/easy-packet-capture.tar

------------------------------------------------------------------------------
Configure and Install EASy Package 'easy-packet-capture-1.0'
------------------------------------------------------------------------------

1. Display Package Description
2. Configure Package Parameters
3. Deploy Package Policies
4. Configure Embedded Packet Capture
5. Exit

Enter option:
```

Enter option 2 to configure package parameters.

Installing the Package, cont.

```
Embedded Packet Capture Configuration:

Capture Point Name   : cappnt
Capture Buffer Name  : capbuf
Capture Protocol     : ip
Capture Method       : cef
Capture Interface    : all
Capture Direction    : both
Capture Buffer type  : linear
Capture Buffer Size  : 256
Maximum Element Size : 1024

CLI to be configured:

monitor capture point ip cef cappnt all both
monitor capture buffer capbuf size 256 max-size 1024 linear
monitor capture point associate cappnt capbuf

Are you satisfied with these settings? (y/n) [y]:
```

The EASy Installer walks the user through setting up each EPC parameter. Once done, the user can see the command to be deployed and confirm the changes.

Installing the Package, cont.

```
easy-packet-capture EEM Environment Variable Configuration:

pcap_var_export_url  : flash:/
pcap_var_max_captime : 3600
pcap_var_max_capnum  : 20
easy_epc_cron_entry  : 0 0 * * *

Are you satisfied with these settings? (y/n) [y]:
```

Next, the EASy Installer prompts for the required EEM environment variable configuration, which controls how long to run the packet capture and whether or not to start it automatically at a specified time.

Installing the Package, cont.

```
Router# easy-installer tftp://172.18.123.33/easy/easy-packet-capture.tar

------------------------------------------------------------------------------
Configure and Install EASy Package 'easy-packet-capture-1.0'
------------------------------------------------------------------------------

1. Display Package Description
2. Configure Package Parameters
3. Deploy Package Policies
4. Configure Embedded Packet Capture
5. Exit

Enter option:
```

Enter option 3 to install the package.

Installing the Package, cont.

```
Installation is complete!

To start the Embedded Packet Capture setting, run the following command
from enable mode:

event manager run no_easy_epc_start.tcl

The capture will stop automatically based on your configured parameters.
However, if you would like to stop it manually, run the following command
from enable mode:

event manager run no_easy_epc_stop.tcl

Hit Enter to continue...
```

The package is installed.

Verifying the Installation

```
------------------------------------------------------------------------------

Configure and Install EASy Package 'easy-packet-capture-1.0'

------------------------------------------------------------------------------

1. Display Package Description
2. Configure Package Parameters
3. Deploy Package Policies
4. Configure Embedded Packet Capture
5. Verify Installed Package
6. Exit

Enter option:5

INFO: Package easy-packet-capture-1.0 is properly installed.

Hit Enter to continue...
```

Enter option 5 to verify that the package was installed properly.

Deinstallation

- The EASy Installer can be used to remove the Embedded Packet Capture package

```
Router#easy_installer --uninstall --pkgname packagename
Uninstalling easy-packet-capture...DONE!

INFO: Uninstall of easy-packet-capture completed successfully.
Configuration was changed, do you want to save the running config to
startup? (y/n) [y]
```

Manual Installation

Manual Installation

- If not using the EASy Installer, extract the contents of the easy-packet-capture.tar file:

```
tar xvf easy-packet-capture.tar
```

- Transfer all of the *.tcl files to the device's EEM policy directory

  See slide 12 for a complete list of Tcl policies

Manual Installation, cont.

Configure the following EEM environment variables, using the “event manager environment VARIABLE VALUE” config command:

- **pcap_var_capbuf1** Capture point name (e.g., “cappnt”)
- **pcap_var_cappnt1** Capture buffer name (e.g., “capbuf”)
- **pcap_var_intf_name** Interface name on which to capture traffic, or “all” for all interfaces (e.g., “FastEthernet0/1”)
- **pcap_var_export_url** URL to which exported captures will be written; the location must already exist (e.g., “flash:/”)
- **pcap_var_max_captime** Maximum time (in seconds) for which the capture will remain active (e.g., “3600” for one hour)
- **pcap_var_max_capnum** Maximum number of capture files to export (e.g., “20”)
- **easy_epc_cron_entry** (Optional) cron entry for when to automatically start the capture session (e.g., “0 0 * * *” to start the capture at 12:00 a.m. every day)

Manual Installation, cont.

- Configure the Embedded Packet Capture capture point and buffer:

```
monitor capture point ip cef CAPPNT all both
```

where CAPPNT is the value used for the environment variable pcap_var_cappnt1

```
monitor capture buffer CAPBUF size 256 max-size 1024 linear
```

where CAPBUF is the value used for the environment variable pcap_var_capbuf1

```
monitor capture point associate CAPPNT CAPBUF
```

- An access list can also be specified to filter the network traffic captured by the EPC session
- See https://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_packet_capture_ps6441_TSD_Products_Configuration_Guide_Chapter.html for more on configuring EPC

Manual Installation, cont.

- Register all of the EEM policies, using the “event manager policy POLICY” config command

  Note: The tm_easy_epc_start.tcl policy should **not** be registered unless the easy_epc_cron_entry environment variable was set

- Start the capture session with the following Cisco IOS® Software EXEC command:

```
event manager run no_easy_epc_start.tcl
```

- If the tm_easy_epc_start.tcl policy is registered, the packet capture will also start automatically, based on the configured cron entry

Verifying Manual Installation

Verifying the Install: Manual Process

- Check the output of “show event manager policy registered” to make sure the required Tcl policies are registered:

```
4    script    user    timer countdown     Off   Wed Oct 7 17:26:22 2009   2048
    ts_easy_epc_stop.tcl
 name {pcap_timer} time 0.000
 nice 0 queue-priority normal maxrun 300.000 scheduler rp_primary
5    script    user    syslog              Off   Wed Oct 7 17:26:22 2009   2048
    sl_easy_epc_fullbuffer.tcl
 occurs 1 pattern {.*BUFCAP-5-BUFFER_FULL.*}
 nice 0 queue-priority normal maxrun 300.000 scheduler rp_primary
6    script    user    none                Off   Wed Oct 7 17:26:22 2009   2048
    no_easy_epc_start.tcl
 policyname {no_easy_epc_start.tcl} sync {yes}
 nice 1 queue-priority low maxrun 600.000 scheduler rp_primary
7    script    user    none                Off   Wed Oct 7 17:26:22 2009   2048
    no_easy_epc_stop.tcl
 policyname {no_easy_epc_stop.tcl} sync {yes}
 nice 1 queue-priority low maxrun 600.000 scheduler rp_primary
8    script    user    application         Off   Wed Oct 7 17:26:23 2009   2048
    ap_easy_epc_export.tcl
 sub_system 798 type 217
 nice 0 queue-priority normal maxrun 600.000 scheduler rp_primary
```

Verifying the Install: Manual Process, cont.

- Check the output of “show monitor capture point CAPPNT” to verify that the capture point is configured:

```
Router#show monitor capture point cappnt
Status Information for Capture Point cappnt
IPv4 CEF
Switch Path: IPv4 CEF            , Capture Buffer: capbuf
Status : Inactive

Configuration:
monitor capture point ip cef cappnt all both
```

- Check the output of “show monitor capture buffer CAPBUF parameters” to verify that the capture buffer is configured:

```
Buffer Size : 262144 bytes, Max Element Size : 1024 bytes, Packets : 0
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
Associated Capture Points:
Name : cappnt, Status : Inactive
Configuration:
monitor capture buffer capbuf size 256 max-size 1024 linear
monitor capture point associate cappnt capbuf
```

Uninstalling Manual Process

Uninstalling: Manual Process

- Unregister all of the installed policies:

  See slide 12 for a complete list of policies

```
Router(config)#no event manager policy no_easy_epc_start.tcl
Router(config)#no event manager policy no_easy_epc_stop.tcl
…
```

- Delete the policies from the EEM policy directory:

  See slide 12 for a complete list of policies

```
Router#delete /force flash:/policies/no_easy_epc_start.tcl
Router#delete /force flash:/policies/no_easy_epc_stop.tcl
…
```

- Remove the EPC configuration:

```
Router#no monitor capture buffer
Router#no monitor capture point ip cef all cappnt
```

Operation

Operation

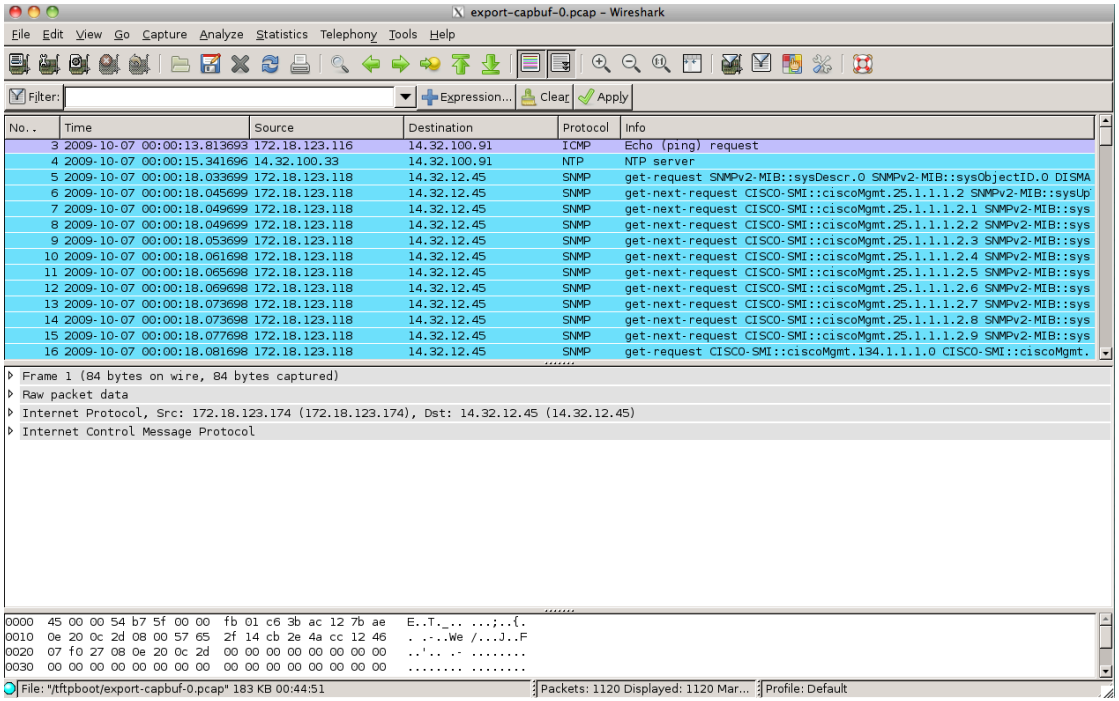
- To start a packet capture, run the command “event manager run no_easy_epc_start.tcl”
- If the package was configured to start at a specified time (during configure time), the packet capture will also start automatically
- Once the package is started, the status of the capture point will move to “Active”

```
Router#show monitor capture point cappnt
Status Information for Capture Point cappnt
IPv4 CEF
Switch Path: IPv4 CEF            , Capture Buffer: capbuf
Status : Active

Configuration:
monitor capture point ip cef cappnt all both
```

Operation, cont.

- If the buffer is configured to be linear (the default), capture files will be exported to the export URL with the name export-CAPBUF-X.pcap, where CAPBUF is the capture buffer name and X is a number from 0 to the maximum number of capture files
- Those files can be opened in Wireshark:



Operation, cont.

- To stop the packet capture, run the command “event manager run no_easy_epc_stop.tcl”
- The packet capture will also stop automatically when the maximum number of capture files have been exported, or after the maximum run time has expired

Future Enhancements and References

Enhancements

- The packet capture can currently be started either manually or at a set time; future enhancements could allow for other triggers
- A future release of Cisco IOS® Software may allow for using NBAR data to trigger a packet capture
- Other suggestions for improvement are welcome; send to ask-easy@cisco.com

References

Cisco Embedded Automation Systems: www.cisco.com/go/easy

Device Manageability Instrumentation (DMI): www.cisco.com/go/instrumentation

- Embedded Event Manager (EEM): www.cisco.com/go/eem
- Cisco® Beyond—EEM Community: www.cisco.com/go/ciscobeyond
- Embedded Packet Capture (EPC): www.cisco.com/go/epc
- GOLD: http://www.cisco.com/en/US/products/ps7081/products_ios_protocol_group_home.html
- Flexible NetFlow: www.cisco.com/go/netflow and www.cisco.com/go/fnf
- IP SLA (aka SAA, aka RTR): www.cisco.com/go/ipsla
- Network Analysis Module: http://www.cisco.com/go/nam
- NBAR: www.cisco.com/go/nbar
- Security Device Manager (SDM): http://www.cisco.com/go/sdm
- Smart Call Home: www.cisco.com/go/smartcall
- Feature Navigator: www.cisco.com/go/fn
- MIB Locator: www.cisco.com/go/mibs

Software Application Support Services

- www.cisco.com/go/services/applicationsupport

Network Management Applications

- www.cisco.com/go/nms

News—Podcast Series

- Cisco Network Management Podcasts: www.cisco.com/go/nmpodcasts