Contents

Introduction

This document describes what Embedded Logic Analyzer Module (ELAM) is, its drawbacks, and how to best use it.

Backgound Information

With the increased complexity of networking devices and protocols, it can be extremely difficult to discover the source of a networking problem. Often, you must determine if a frame is received and forwarded correctly on a particular device. There are several capture tools, debugs, and tricks available in order to help answer this question. However, not all are feasible or available to run on a production network.

ELAM is an engineering tool that gives you the ability to look inside Cisco ASICs and understand how a packet is forwarded. It is *embedded* within the forwarding pipeline, and it can capture a packet in real-time without disruptions to performance or control-plane resources. It helps to answer questions such as:

- Did the packet reach the Forwarding Engine (FE)?
- On what port and VLAN is the packet received?
- How does the packet appear (Layer 2 (L2) – Layer 4 (L4) data)?
- How is the packet altered, and where is it sent?

ELAM is extremely powerful, granular, and non-intrusive. It is a valuable troubleshooting tool for Cisco Technical Assistance Center (TAC) engineers who work on hardware-switching platforms.

ELAM Challenges

ELAM was designed as a diagnostic tool for internal use. The CLI syntax uses internal code names for Cisco ASICs, so interpretion of the ELAM data requires hardware-specific architecture and forwarding knowledge. Many of these details cannot be explained because they expose the internal Cisco proprietary features that make Cisco devices best-in-class.

For these reasons, ELAM is not a customer-supported feature, and has remained a diagnostic tool for internal use. There are no external configuration guides, and the syntax and operation might change from version to version without any notice.

Given these challenges and the disclaimer, here are the reasons that ELAM is described now:

- First, it is very common for a TAC engineer to use ELAM in order to isolate an issue. TAC might request that you perform ELAM if the issue is intermittent. It is important to understand that these steps are non-intrusive, and how they can help provide a root-cause analysis.

- Also, sometimes there are no other available tools that can help isolate an issue. For example, when no configuration changes are allowed during production hours for SPAN, ACL hits, or intrusive debugs. There might not be time to reach TAC, and ELAM can be an extremely helpful tool to have as a last resort.

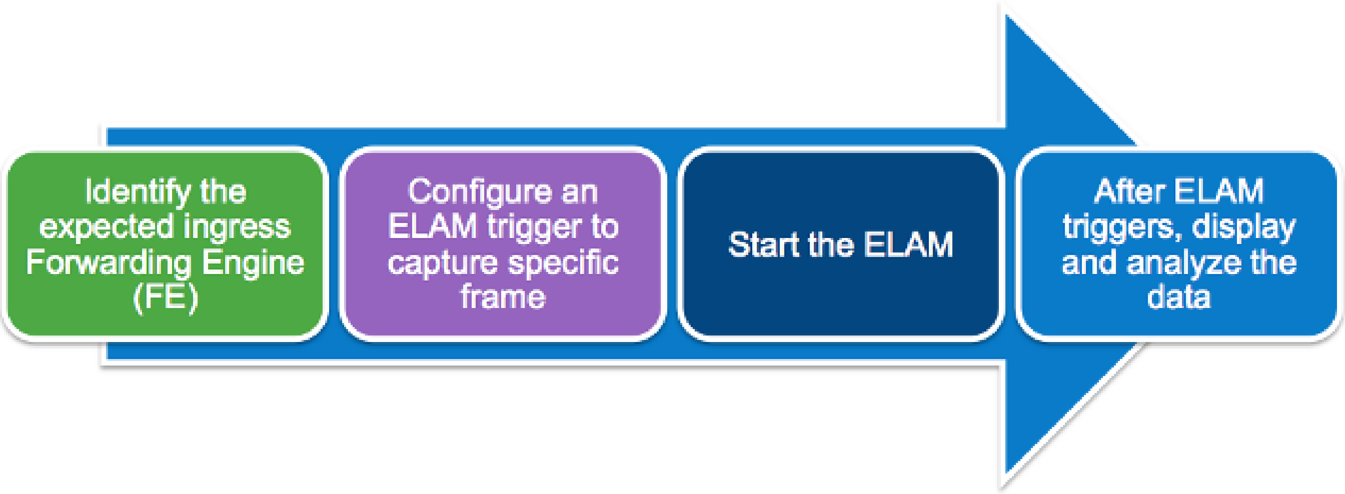
ELAM Basics

ELAM can be performed without full architectural knowledge of each platform. This section describes the basics needed in order to perform an ELAM on the Cisco Catalyst 6500 and 7600 Series switch platforms (referred to as simply *6500* and *7600*, respectively), along with the Nexus 7000 Series switch platform.

ELAM Workflow

As previously mentioned, ELAM is dependent on the underlying hardware; therefore, the CLI syntax is dependent on the hardware in use. However, each platform follows a similar workflow, as shown in this image:

> **Note**: Refer to the ELAM Examples section in order to see how this workflow is applied on different platforms.


Identify the expected ingress Forwarding Engine (FE)
Configure an ELAM trigger to capture specific frame
Start the ELAM
After ELAM triggers, display and analyze the data

These four steps, which are further detailed later in this section, describe the workflow:

1. Identify the expected ingress FE. When platforms have more than one FE, it is critical to identify the FE that makes the forwarding decision for the packet you want to capture. Configure the ELAM on the correct FE.

2. Configure the ELAM trigger. You must configure a trigger with details specific to the packet that you want to capture. Common triggers include a source and destination IP address or L4 port numbers. ELAM allows multiple fields to be specified, and performs a logical AND on all fields configured.

3. Start the ELAM.

4. Wait for the ELAM to trigger and display the result.

Centralized Versus Distributed Forwarding

The first step that you must complete in order to perform an ELAM is to identify the correct FE. A 6500 with classical or Centralized Forwarding (CFC) linecards uses centralized forwarding, where the active supervisor makes the forwarding decision. For packets that ingress on classical or CFC linecards, you must perform the ELAM on the active supervisor.

With Distributed Forwarding (DFC)-enabled linecards, the forwarding decision is made locally by an FE on the linecard without the supervisor. For packets that ingress DFC linecards, you must perform the ELAM on the linecard itself.

For the Nexus 7000 Series switch platform, all linecards are fully-distributed. Additionally, most linecards have multiple FEs. When you set up the ELAM, you must know the port on which the packet is received, and determine the FE that maps to that port.

For additional information on hardware and forwarding architecture, reference these Cisco Live 365 articles:

- BRKARC-3465 Cisco Catalyst 6500 Switch Architecture

- BRKARC-3470 - Cisco Nexus 7000 Switch Architecture

Data Bus (DBUS) and Result Bus (RBUS)

The DBUS contains information that is used by the FE in order to make a forwarding decision. It contains several platform-specific internal fields, along with the header information for a frame. View the DBUS in order to help determine where the packet is received, and the packet L2-L4 information.

The RBUS contains the forwarding decision made by the FE. View the RBUS in order to help determine if the frame is altered, and where it is sent.

Local Target Logic (LTL)

The LTL is an index used in order to represent a port or group of ports. The source LTL index and the destination LTL index shows you where the frame is received, and where it is sent.

> **Note**: Different platforms and supervisors use different commands in order to decode the LTL values.

Flood Bit

LTL values are displayed as five or less hex numbers (0xa2c, for example). The flood bit is the 16th bit in the LTL result. Often, the RBUS displays a field with the destination LTL index, and has a separate field for the flood bit. It is important to merge these results for the correct LTL. For example:

```
RBUS:

FLOOD ........................... [1] = 1
DEST_INDEX ...................... [19] = 0x48
```

In this example, the destination LTL index is **0x48**. Since the flood bit is **1**, you must set the 16th bit in the LTL to **1**:

```
0x00048 = 0000 0000 0000 0100 1000
               |
               +---- Flood bit, set to 1 = 0x08048
```

After you account for the flood bit, the destination index has become **0x8048**.

ELAM Examples

The purpose of these examples is to illustrate how ELAM is used in order to validate basic IPv4 or IPV6 unicast flows. As described in the ELAM Challenges section of this document, it is not practical to explain all internal fields or packet types, such as recirculation for multicast, tunnels, and MPLS.

Follow these links for examples of ELAM use with different devices:

- Catalyst 6500 Series Switches with Supervisor Engine 720 ELAM Procedure
- Catalyst 6500 Series Switches with Supervisor Engine 2T ELAM Procedure
- Nexus 7000 M-Series Module ELAM Procedure
- Nexus 7000 M3 Module ELAM Procedure
- Nexus 7000 F1 Module ELAM Procedure
- Nexus 7000 F2 Module ELAM Procedure
- Nexus 6000 Switch ELAM Overview

Internal ASIC Names

As a reference, the internal ASIC name that is assigned to ELAM for each module type is listed in this table:

Platform	Module Type	Internal ASIC Name
Catalyst 6500/ Cisco 7600	Sup720 (PFC3, DFC3)	Superman
Catalyst 6500	Sup2T (PFC4, DFC4)	Eureka
Nexus 7000	M-Series (M1 and M2)	Eureka

Nexus 7000	M3 Module	F4
Nexus 7000	F1	Orion
Nexus 7000	F2	Clipper
Nexus 7000	F3	Flanker
Nexus 6000	N/A	Bigsur

Additional Ways to Use ELAM

There is a more customer-friendly way to use ELAM. With Cisco IOS® Releases 12.2(50)SY and later, Cisco added the **show platform datapath** command for the 6500s that run Supervisor Engine 2T (Sup2T). This command uses ELAM in order to capture and display the forwarding result of a specific packet.

For Nexus 7000 Series switch platforms, an easy-to-use script, **elame**, was added in Cisco IOS Release 6.2(2) in order to leverage ELAM:

```
N7KA# source sys/elame
elam helper, version 1.015

Usage:
elame [<src>] <dest> [vlan <vlan#>] [vrf <vrf_name>] [int <interface> | vdc] [trace]
```

In the output:

- The **<src>** and **<dest>** are IPV4 addresses in the form **1.2.3.4**.
- The **<vlan>** and **<interface>** indicate the ingress VLAN/interface.
- The **vdc** indicates that all ELAMs in the current Virtual Device Contexts (VDC) are used.
- The **[trace]** indicates that the system keeps record of all outputs in the volatile (elame.log).

Note that the elame script is not supported on F3 modules and other N77xx linecards at this point. A few enhancement bugs have been filed in order to improve the Elame script and it is still being looked at by the business unit.

- Cisco bug ID CSCuy42559
- Cisco bug ID CSCuw60869

Note: Elam is an internal tool and it has to be used only under TAC/BU supervision.

Related Information

- **BRKARC-2011 - Overview of Troubleshooting Tools in Cisco Switches and Routers - Cisco Live 365**
- **Technical Support & Documentation - Cisco Systems**