This article describes the ACE architecture and how data flows into, gets processed, and flows out of the ACE. It provides a basic understanding of these concepts to assist you in troubleshooting the ACE.

Guide Contents
Main Article
Overview of ACE Troubleshooting
Understanding the ACE Module Architecture and Traffic Flow
Preliminary ACE Troubleshooting
Troubleshooting ACE Boot Issues
Troubleshooting with ACE Logging
Troubleshooting Connectivity
Troubleshooting ACE Appliance Ethernet Ports
Troubleshooting Remote Access
Troubleshooting Access Control Lists
Troubleshooting Network Address Translation
Troubleshooting ACE Health Monitoring
Troubleshooting Layer 4 Load Balancing
Troubleshooting Layer 7 Load Balancing
Troubleshooting Redundancy
Troubleshooting SSL
Troubleshooting Compression
Troubleshooting Performance Issues
ACE Resource Limits
Managing ACE Resources
Show Counter Reference

Contents

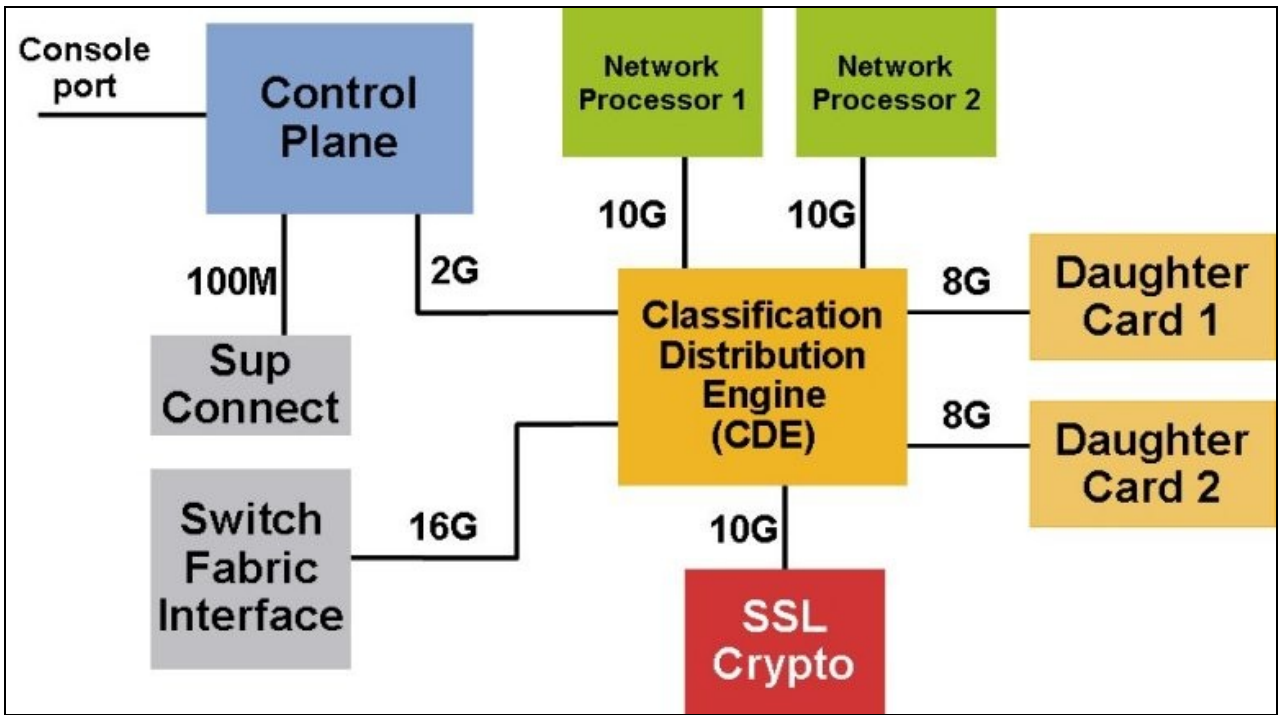
Understanding the ACE Architecture

Having a basic understanding of the ACE architecture and data flow can help to make troubleshooting the ACE easier. This section describes the major functional areas of the ACE and how they work together.

Overview of the ACE Hardware Architecture

The ACE hardware architecture is divided into a series of functional areas or subsystems that are defined by processors or groups of processors and interfaces as shown in Figure 1.

Figure 1. ACE Module Architecture



A console connection allows direct access to the ACE control plane (CP) for initial configuration, management, and troubleshooting. The supervisor engine connection allows you to determine the status of the ACE, to load images into the ACE, to reboot the ACE, and to provide remote access to the ACE from the Catalyst 6500 series switch or Cisco 7600 series router when you use the **session** command. Because the ACE has no external ports, packets enter the ACE through the Switch Fabric Interface (SFI) connected to the Catalyst 6500 series switch or Cisco 7600 series router back plane. The two major functional areas of the ACE are as follows:

- Control plane
- Data plane

Control Plane

The control plane (CP) is used to configure the ACE and for management traffic, syslogs, ARP, DHCP, and so on. You can access the CP directly by using the console port. For remote management, you must configure a management interface and enable remote access using a management policy to permit Telnet or SSH access, for example. The CP is responsible for the following ACE functions:

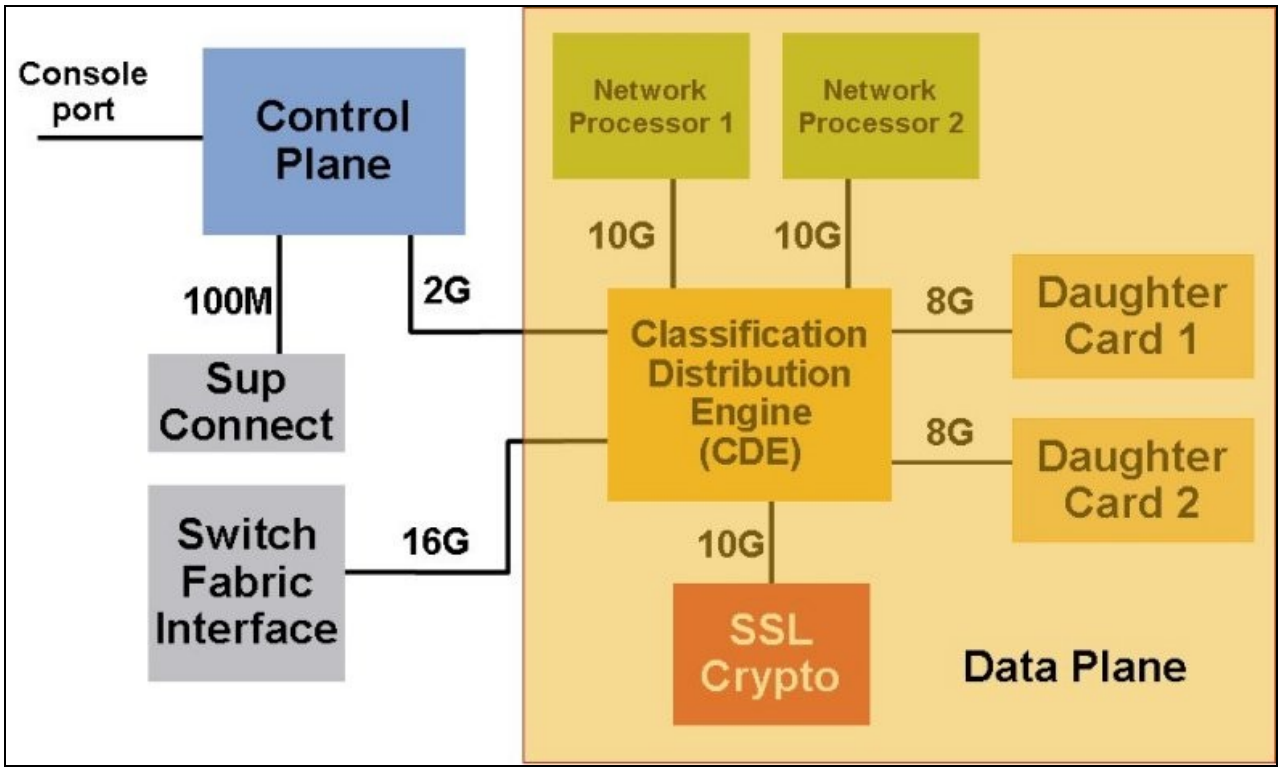
- Device management and control
- Configuration management (CLI or XML interface)
- Server health monitoring
- syslogs
- SNMP
- Address Resolution Protocol (ARP)
- DHCP relay
- Redundancy (also known as high availability or fault tolerance)
- Access control list (ACL) compilation

Data Plane

The data plane (DP) is responsible for distributing and processing packets and connections that do not match a management policy.

In the ACE, the CP and the DP are separated and run on different processors for maximum performance. See Figure 2.

Figure 2. ACE Data Plane



The DP is responsible for the following ACE functions:

- Access control lists (ACLs)
- Connection management
- TCP termination
- Network address translation (NAT)
- SSL processing (termination, initiation, encryption, and decryption)
- Regular expression matching
- Load balancing and forwarding
- Application protocol inspection

The DP consists of the following functional areas:

- Classification distribution engine (CDE)
- Network processors (NPs)
- SSL Crypto Module
- Daughter card interfaces (for future feature expansion)

Classification and Distribution Engine

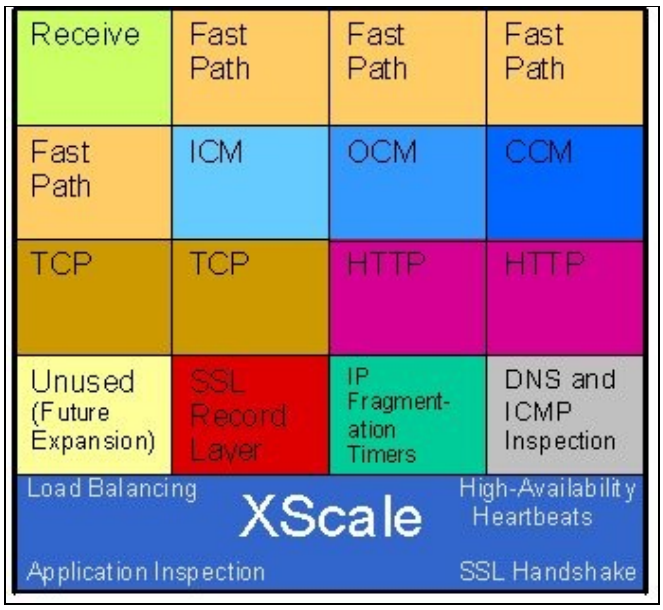
The Classification and Distribution Engine (CDE) is the traffic controller for the ACE. Its main purpose is to forward packets that it receives from the SFI to the two network processors (NPs). It also acts as the central point of contact among all the major subsystems within the ACE. The CDE computes, and if necessary, adjusts the IP, TCP, and UDP checksums of every packet that it receives.

The CDE appends a special header known as the IMPH header to each packet before sending it to the fast path. The IMPH header is 18 bytes long and contains information from the DBUS header (the header sent to the ACE Module by the Catalyst 6500 series switch or Cisco 7600 series router) as well as special messaging directly understood by the fast path. Fields in the IMPH header can include notification of a checksum error, Layer 3 or Layer 4 offsets, source and destination ports of the CDE, the VLAN for determining the interface that the fast path will use, and so on.

Network Processors

The ACE has two network processors (NP1 and NP2) that perform most of the packet processing in the ACE. All traffic entering the ACE must traverse one or both NPs after being forwarded by the CDE. Each NP contains a CPU (XScale) and several components called microengines (MEs). See Figure 3.

Figure 3. Network Processor Micorengines



Each microengine can handle eight simultaneous threads or processes and performs a specific function for the NP as follows:

- Receive - One ME for receiving incoming packets
- Fast Path - Four MEs for the hardware accelerated data path that is used for MAC rewrite, NAT, TCP normalization, and so on (essentially all operations performed on a per-packet basis)
- ICM - One ME for the inbound connection manager
- OCM - One ME for the outbound connection manager
- CCM - One ME for the connection close manager
- TCP - Two MEs for TCP termination with a full TCP stack
- HTTP - Two MEs for HTTP parsing
- Unused (future expansion) - One ME
- SSL Record Layer - One ME for the SSL record layer
- IP fragmentation timers - One ME for IP fragmentation reassembly and timer management
- DNS and ICMP Inspection - One ME for DNS and ICMP packet inspection

The XScale microprocessor is programmed to handle the following features:

- Load-balancing algorithms
- SSL handshake
- FTP and Real-Time Streaming Protocol (RTSP) inspection
- HTTP inspection (although a considerable part is performed by the microengines)
- High-availability heartbeat generation
- Returned statistics for most connection-related commands

Each network processor has RDRAM memory to store ACL entries, routing table entries, ARP entries, and inspection policies. Additional SRAM memory provides faster access times and is used to store regular expressions and statistics on a per?virtual system basis, among other things.

SSL Crypto Module

The SSL Crypto Module is responsible for SSL record layer processing. This processing includes encrypting and decrypting data for SSL flows.

Understanding the ACE Traffic Flow

Because the ACE has no native ports, it relies on the switch fabric in the Catalyst 6500 series switch or the Cisco 7600 series router back plane to send and receive packets to and from the network. Packets that are marked with a destination VLAN and Layer 2 information enter the ACE through the SFI on the 10 Gbps Ethernet link. Packets entering or leaving the ACE traverse this link using VLAN tagging. The switch fabric interface (SFI) forwards to the CDE all packets that are destined to the ACE. See Figure 1.

The CDE classifies the packets based on the configured traffic policies, fills out the IMPH header information, and forwards the traffic to one of the NPs. To determine which NP to forward the traffic to, the CDE hashes incoming packets based on the traffic type as follows:

- TCP/UDP - Hash of source/destination port
- Non-TCP/UDP IP - Hash of source/destination IP address
- Non-IP - Hash of source/destination Layer 2 MAC address

The NPs process the traffic and forward it back through the CDE to either the control plane or the SSL Crypto Module for further processing.

To-the-ACE Traffic

To-the-ACE traffic is traffic that is destined to an interface VLAN IP address on the ACE. This traffic must match a class map of type management, which is associated with a policy map and applied as a service policy on an interface VLAN. The management class map supports the following protocols:

- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- Internet Control Message Protocol (ICMP)
- Keepalive Application Protocol (KAL-AP)
- User Datagram Protocol (UDP)
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH) Protocol
- Telnet

This management traffic is called control plane traffic because it is destined to the CP. Because of the separation of the CP traffic from the data plane traffic on different processors, the control plane traffic will never interfere with data plane traffic, even if the control plane is oversubscribed.

Through-the-ACE Traffic

The CDE sends traffic that requires load balancing, forwarding, routing, or other processing by the ACE to one of the NPs.

The NPs comprise two parallel forwarding paths that maintain their own connection state information and forward traffic independently.