Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders

Common Criteria Operational User Guidance and Preparative Procedures

Version 1.0

14 January 2021

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

List of Acronyms

The following acronyms and abbreviations are common and may be used in this Administrators Guidance.

Table 1 Acronyms

Acronyms / Abbreviations	Definitions
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
APIC	Application Policy Infrastructure Controller
BRI	Basic Rate Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
CSU	Channel Service Unit
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
GE	Gigabit Ethernet port
GUI	Graphical User Interface
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Information Technology
LLDP	Link Layer Discovery Protocol
NTP	Network Time Protocol
OS	Operating System
PoE	Power over Ethernet
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SSHv2	Secure Shell protocol version 2
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEP	Tunnel End Point
TLS	Transport Layer Security
TOE	Target of Evaluation

Acronyms / Abbreviations	Definitions
ToR	Top of Rack
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
vPC	virtual Port Channels
VRF	Virtual Routing and Forwarding

Terminology

The following terms are common and may be used in this Administrators Guidance.

Table 2 Terminology

Term	Definition
Application Profile	An application profile (fvAp) defines the policies, services and relationships between endpoint groups (EPGs).
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF related functions.
Endpoint Groups	The endpoint group (EPG) is the most important object in the policy model. An EPG is a managed object that is a named logical entity that contains a collection of endpoints. Endpoints are devices that are connected to the network directly or indirectly.
Line Cards	The line cards of the Cisco Nexus 9500 Series are equipped with multiple network forwarding engines (NFE) that perform packet lookup, processing and forwarding functions.
Peer switch	Another switch on the network that the TOE interfaces with.
Privilege level	The Authorized Administrator assigns administrative users to specific privilege levels to manage various aspects of the TOE. The privilege levels are from 1-15 with 15 having full administrator access to the TOE whereas privilege level 1 has the most limited access to the TOE. At this level, the Administrator has access to some information about the TOE, such as the status of interfaces and they can view routes in the routing table. However, the Administrator cannot make any changes or view the running configuration file.
Role	A role gives an Authorized Administrator varying access to the management of the TOE. For the purposes of this evaluation the privilege level of an Administrator is synonymous with the assigned role.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
System Controller	The System Controllers of Cisco Nexus 9500 Series are used to offload the internal non-data-path switching and management functions from the supervisor engines. It also provides the pathway for access to the power supplies and fan trays.
Tenant	A tenant (fvTenant) is a logical container for application policies that enable an administrator to exercise domain-based access control. A tenant represents a unit of

Term	Definition
	isolation from a policy perspective, but it does not represent a private network. Tenants can represent a customer in a service provider setting, an organization or domain in an enterprise setting, or just a convenient grouping of policies.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
VRF	A Virtual Routing and Forwarding (VRF) object (fvCtx) or context are a tenant network (called a private network in the APIC GUI). A tenant can have multiple VRFs. A VRF is a unique Layer 3 forwarding and application policy domain.
Vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).
VXLAN	VXLAN is a tunneling protocol that encapsulates Layer 2 Ethernet frames in Layer 3 UDP packets, enabling you to create virtualized Layer 2 subnets, or segments, that span physical Layer 3 networks

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and Security Administrators in this document.

1 Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders (FEX), the TOE, as it was certified under Common Criteria. The Cisco Nexus 9000 Switch may be referenced below by the model number series related acronym 9K, TOE, Nexus 9000 Series or simply switch. All the instructions pertain specifically to the switch except for the instructions specifically noted for APIC. The APIC and ACI mode switches as well as the FEX and network connections that make up the ACI fabric must be installed in one physically protected data center.

1.1 Audience

This document is written for administrators configuring and maintaining the TOE, specially the Cisco NX-OS System Software-ACI 14.2, APIC 4.2. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, understand your network topology, the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running on your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the Security Target (ST). This document covers all the security functional requirements specified in the ST and as summarized in Section 3 of this document. This document does not mandate configuration settings for the features of the TOE that are outside the evaluation scope, such as such as the type or quantity of switches, fabric extenders or the number of Authorized Administrators all of which should be set according to your organizational security policies.

This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining the TOE operations. It is recommended that you read all instructions in this document and any references before performing steps outlined and entering commands. Section 7 of this document provides information for obtaining assistance in using Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders. The use of the Fabric Extender is optional. The Nexus 2000 Fabric Extender functions essentially as a remote line card and is optional to the deployment of the Nexus 9000 with APIC/ACI to add additional ports if needed.

1.3 Document References

This document refers to several Cisco Systems product documents. The documents used are listed below in Table 3. Throughout this document, the guides will be referred to by the "#", such as **[1]**.

As a note, the guides below that reference 14.2 and 4.2 also apply to the Nexus 9k in ACI mode. Only a subset of the Nexus commands for Nexus stand-alone mode are in the Nexus ACI mode. Therefore, commands in the Nexus command reference guides which are not specific to ACI mode may not work. See the APIC specific guides for APIC and ACI mode for specific commands. These guides are listed for completeness.

Table 3 Cisco Documentation

#	Title	Link
[1]	Cisco Nexus 900 Switch Series with ACI mode, APIC and Nexus 200 Fabric Extenders Common Criteria Security Target, (Current Version)	https://www.commoncriteriaportal.org/products/ https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html?dtid=osscdc000283
[2]	Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system-management/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x.html
[3]	Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x.html
[4]	Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/fundamentals/configuration/guide/b-cisco-nexus-9000-nx-os-fundamentals-configuration-guide-93x.html
[5]	Cisco Nexus 9000 Series NX-OS Command Reference (Configuration Commands), Release 9.3(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/command/reference/config/b_N9K_Config_Commands_93x.html
[6]	Cisco Nexus 9000 Series NX-OS Command Reference (Show Commands), Release 9.3(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/command/reference/show/b_N9K_Show_Commands_93x.html
[7]	Cisco Nexus Mode Switch Hardware Installation Guides	93108LC-FX https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_93180lcex_hig/guide/b_c93180lcex_aci_mode_hardware_install_guide.html 93108TC-FX - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_93108tcex_hig/guide/b_c93108tcex_aci_mode_hardware_install_guide.html 9348GC-FXP - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nex

#	Title	Link
		us9000/hw/aci_9348gcfxp_hig/guide/b_c9348gc_fxp_aci_mode_hardware_install_guide.html 93216TC-FX2 - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci-93216tc-fx2-hig/b_c93216TC-FX2-aci-mode-hardware-installation-guide.html 93180YC-EX - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_93180YCex_hig/guide/b_n93180ycex_aci_mode_hardware_install_guide.html 93180YC-FX - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_93180ycfx_hig/guide/b_n93180ycFX_aci_hardware_installation_guide.html 93240YC-FX2 - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_93240ycfx2_hig/b_n93240YC-FX2_aci_hardware_installation_guide.html 93360YC-FX2 - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci-93360yc-fx2-hig/b_c93360yc-fx2-aci-mode-hardware-installation-guide.html 9336C-FX2 - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_9336cfx2_hig/guide/b_n9336cFX2_aci_hardware_installation_guide.html 9364C-GX - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci-9364c-gx-hig/b_c9364c-gx-aci-mode-hardware-installation-guide.html 9316D-GX - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_9316D-GX_hig/guide/b_C9316D-GX_aci_hardware_installation_guide.html 93600CD-GX - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci-93600cd-gx/guide/b_c93600CD-GX-aci-mode-hardware-installation-guide.html 9332C - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_9332c_hig/guid/b_n9332C-aci-mode-hardware-installation-guide.html 9364C - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nex

#	Title	Link
		us9000/hw/aci_9364c_hig/guide/b_c9364c_ACI_mode_hardware_install_guide.html 9504 - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_9504_hig/guide/b_n9504_aci-mode_hardware_install_guide.html 9508 - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_9508_hig/guide/b_n9508_aci-mode_hardware_install_guide.html 9516 - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_9516_hig/guide/b_n9516_aci-mode_hardware_install_guide.html 20000 Series - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/hw/installation/guide/nexus_2000_hig.html APIC - https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/hw/aci_hig/guide/b_aci_hardware_install_guide.html UCS C220 M5 - https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C220M5/install/C220M5.html UCS C240 M5 – https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M5/install/C240M5.html
[8]	Cisco ACI System Messages Reference Guide	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/all/syslog/guide/b_ACI_System_Messages_Guide/b_ACI_System_Messages_Guide_preface_00.html
[9]	Cisco APIC Security Configuration Guide, Release 4.2(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/b-Cisco-APIC-Security-Configuration-Guide-421/.html
[10]	Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/unicast/configuration/guide/l3_cli_nxos.pdf
[11]	Cisco APIC Getting Started Guide, Release 4.2(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/getting-started/Cisco-APIC-Getting-Started-Guide-421.html
[12]	Operating Cisco Application Centric Infrastructure	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/Operating_ACI/guide/b_Cisco_Operating_ACI.html
[13]	Cisco APIC Layer 4 to Layer 7 Services Deployment Guide	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/L4-L7-services/Cisco-APIC-Layer-4-to-Layer-7-Services-Deployment-Guide-42x.html

#	Title	Link
[14]	Cisco Application Centric Infrastructure Fundamentals, Release 4.2(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/aci-fundamentals/Cisco-ACI-Fundamentals-42x.html
[15]	Cisco APIC NX-OS Style CLI Configuration Guide, Release 4.2(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/cli-configuration/Cisco-APIC-NX-OS-Style-CLI-Configuration-Guide-42x.pdf
[16]	Cisco ACI Switch Command Reference, NX-OS Release 13.x	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/cli/inxos/13x/b_ACI_Switch_Command_Ref_13x.html
[17]	Cisco APIC REST API Configuration Guide, Release 4.2(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/rest-api-config/Cisco-APIC-REST-API-Configuration-Guide-42x.html
[18]	Cisco APIC Basic Configuration Guide, Release 4.2(x)	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/basic-configuration/Cisco-APIC-Basic-Configuration-Guide-42x.html
[19]	Cisco Application Centric Infrastructure Best Practices Guide	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/ACI_Best_Practices/b_ACI_Best_Practices.html
[20]	Cisco Application Centric Infrastructure Design Guide White Paper	https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737909.html
[21]	(a) Cisco APIC Troubleshooting Guide, Release 4.2(x) (b) Cisco APIC Faults, Events, and System Messages Management Guide (c) Cisco ACI System Messages Reference Guide	https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/troubleshooting/Cisco-APIC-Troubleshooting-Guide-42x.html https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/all/faults/guide/b_APIC_Faults_Errors.html https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/all/syslog/guide/b_ACI_System_Messages_Guide.html

1.4 Supported Hardware and Software

Only the following hardware and software listed below is compliant with the Common Criteria Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders running Cisco NX-OS System Software-ACI 14.2, APIC 4.2 EAL2 evaluation. Using hardware not specified invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed below will invalidate the secure configuration.

1.4.1 Supported Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders and Software

The Cisco ACI fabric is composed of the APIC and the Cisco Nexus 9000 Series with ACI mode leaf and spine switches. The Cisco APIC provides centralized access to all fabric

information and supports flexible application provisioning across physical and virtual resources. Cisco ACI consists of:

- APIC
- Nexus 9000 Series Switches in ACI spine and leaf configuration

When the Nexus 9000 Series Switches are configured for ACI mode, which identifies the APIC for remote management and configuration. The APIC is the Authorized Administrator's centralized management interface for all devices in the fabric. From the APIC, the Authorized Administrator can attach to the switch CLI over SSHv2 or the GUI over HTTPS/TLSv1.2 to make specific configuration changes.

Typically, the APIC will be deployed in a cluster with a minimum of three controllers for scalability and redundancy purposes, though is not required. Any controller in the cluster can service any user for any operation, and a controller can be transparently added to or removed from the Cisco APIC cluster. The minimum deployment configuration is 1 spine, 2 leafs and 1 APIC.

The Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders that comprises the TOE are listed in Table 4 Hardware Models and Specification below.

Table 4 Hardware Models and Specification

Model	Description	Interfaces
Cisco 9300 ACI Leaf Models		
93180LC-EX	32 x 40/50-Gbps QSFP+ ports OR 18 x 100-Gbps QSFP28 ports, 4 cores CPU, 24 GB system memory, 64 GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93108TC-EX	48 x 10GBASE-T and 6 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 64GB SSD, Power supplies (up to 2) 500W AC, 650W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93108TC-FX	48 x 100M/1/10GBASE-T ports and 6 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9348GC-FXP	48 x 100M/1G BASE-T ports, 4 x 1/10/25-Gbps SFP28 ports and 2 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1200W AC or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93216TC-FX2	96 x 100M/1/10GBASE-T ports and 12 x 40/100-Gigabit QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port

Model	Description	Interfaces
93180YC-EX	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports, 6 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 port - (L1 and L2 ports are unused) 1 USB port 1 RS-232 serial port
93180YC-FX	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports, 6 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 port - (L1 and L2 ports are unused) 1 USB port 1 RS-232 serial port
93240YC-FX2	48 x 1/10/25-Gbps fiber ports and 12 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93360YC-FX2	96 x 1/10/25-Gbps and 12 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1200W AC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9336C-FX2	36 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9364C-GX	64 x 100/40-Gbps QSFP28 ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9316D-GX	16 x 400/100/40-Gbps QSFP-DD ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93600CD-GX	28 x 100/40-Gbps QSFP28 ports and 8 x 400/100-Gbps QSFP-DD ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
Cisco 9300 and 9500 ACI Spine Models		
9332C	32-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports, 4 core CPU, 16GB system memory, 128GB SSD, Power supplies 1100W AC, 1100W DC, or 2000W HVAC/HVDC	Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP) 1 USB port 1 RS-232 serial port
9364C	64-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies 1200W AC, 93000W DC, or 1100W HVAC/HVDC	Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP) 1 USB port 1 RS-232 serial port
9504	Chassis: 4-slot, up to 4 line cards, up to 4 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays	Based on Supervisor and ACI compatible I/O modules installed. Each line card should be ACI compatible

Model	Description	Interfaces
9508	Chassis: 8-slot, up to 8 line cards, up to 8 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays	Based on Supervisor and ACI compatible I/O modules I/O modules installed
9516	Chassis: 16-slot, up to 16 line cards, up to 10 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays	Based on Supervisor and ACI compatible I/O modules I/O modules installed
Cisco 9500 Model Components		
Supervisor A/A+	4 core cpu, 16 GB of memory and 64 GB of SSD (N9K-SUP-A/A+)	Two USB ports, a serial port, and a 10/100/1000-Mbps Ethernet port
Supervisor B /B+	6 core cpu, 24 GB of memory and 256 GB of SSD (N9K-SUP-B/B+)	Two USB ports, a serial port, and a 10/100/1000-Mbps Ethernet port
Cisco 2000 Series Fabric Extenders		
2248TP-E	48 x 100/1000BASE-T host interfaces and 4 x 10 Gigabit Ethernet fabric interfaces (SFP+)	As described
2232PP-10GE	32 x 1/10 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) host interfaces (SFP+) and 8 x 10 Gigabit Ethernet and FCoE fabric interfaces (SFP+)	As described
2232TM-E	32 x 100M, 1/10GBASE-T host interfaces and uplink modules (8 x 10 Gigabit Ethernet fabric interfaces [SFP+]); FCoE support up to 30m with Category 6a and 7 cables	As described
2348TQ-E	48 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables	As described
2332TQ	32 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 4 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables	As described
2348TQ	48 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables	As described
2348UPQ	48 x 1/10 Gigabit Ethernet and unified port host interfaces (SFP+) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces	As described
APIC		

Model	Description	Interfaces
APIC (Medium - Large) and clustered (cluster requires at least three appliances)	APIC with medium-size CPU, hard drive, and memory configurations (up to 1200 edge ports) (APIC-SERVER - M3) APIC with large CPU, hard drive, and memory configurations (more than 1200 edge ports) (APIC-SERVER -L3) The type of virtual interface card (VIC) installed on the APIC determines the types of interface cables that can be used to connect the leaf switches to the APIC. • The VIC 1225T module supports copper connectors, copper cables, and switches with copper downlink ports (such as: Cisco Nexus 93108TC-EX, 93108TC-FX, 93120TX, 93128TX, 9372TX, 9372TX-E, and 9396TX switches). • The VIC 1225 module supports optical transceivers, optical cables, and switches with optical downlink ports (such as: Cisco Nexus 93180LC-EX, 93180YC-EX, 93180YC-FX, 9332PQ, 9336C-FX2, 9348GC-FXP, 9372PX, 9372PX-E, 9396PX, and 93600CD-GC switches). • The VIC 1455 module supports optical transceivers, optical cables, and switches with optical downlink ports (such as: Cisco Nexus 9336C-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC=FX2, and 93600CD-GC switches).	Dual 1-Gb/10-Gb Ethernet ports (LAN1 and LAN2) - The dual LAN ports can support 1 Gbps and 10 Gbps, depending on the link partner capability. 1-Gb Ethernet dedicated management port Serial port (RJ-45 connector) USB 3.0 ports (two)

The Cisco the NX-OS System Software-ACI 14.2, APIC 4.2 is a Cisco-developed highly configurable proprietary operating system that provides for a network that is deployed, monitored, and managed in a fashion that supports rapid application change. The TOE provides security and performance while maintaining complete visibility into application health on both virtual and physical resources.

Although Cisco NX-OS Software performs many networking functions, this TOE only addresses the functions that satisfy the requirements as claimed in the Security Target (ST) and defined in this document. For example:

- Security audit – The TOE generates audit records to assist the Authorized Administrator in monitoring the security of the TOE as well as trouble shooting various problems that may arise throughout the operation in its evaluated configuration.

- Full Residual Information Protection –The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic.
- Identification and authentication – The TOE require all Authorized Administrators to be successfully identified and authenticated prior to gaining access to the TOE. The TOE also enforces a minimum password length as well as mandatory password complexity rules. The TOE can optionally be configured to support IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.
- Information Flow Control – The TOE provides the ability to control traffic flow into and out of the TOE. The traffic flows are controlled for both IPv4 and IPv6 traffic.
- Secure Management – The TOE provides secure administrative services for management of the TOE configuration and the security functionality that is provided by the TOE. All TOE administration occurs through the CLI over SSHv2 secure connection and/or the GUI over HTTPS/TLSv12 secure connection. All the TOE management functions are restricted to Authorized Administrator. The term "Authorized Administrator" is used in this document to refer to any user account that has been assigned the privileges to perform the relevant action. The TOE provides the ability to perform the following actions:
    - Administer the TOE locally and remotely
    - Manage information flow control attributes
    - Manage Authorized Administrator's security attributes, noting the TOE allows for more than one administrator account to be configured. Each Authorized Administrator must be assigned a unique username and password
    - Review audit record logs
    - Configure and manage the system time
- Protection of the TSF - The TOE protects against interference and tampering by untrusted subjects by implementing identification and authentication, data flow controls to/through the TOE runs a suite of self-tests to ensure the TOE is operating correctly and limits configuration options to the Authorized Administrator. Additionally, TOE is not a general-purpose operating system and access to the Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders memory space is restricted to only the Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders functions. Finally, the TOE internally maintains the date and time. This date and time are used as the timestamp that is applied to audit records generated by the TOE. Authorized Administrator can update the TOE's clock manually or configure the TOE to use NTP to synchronize the TOE's clock. In the evaluated configuration NTP is used to

sync time across the entire site. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

- TOE Access – Prior to the Authorized Administrator logging in, the TOE displays a warning and consent of use banner. The TOE also provides the ability for the Authorized Administrator to terminate their own sessions. Once a session has been terminated, the TOE requires the Authorized Administrator to re-authenticate to establish a new session.
- Trusted Path/Channel – Allows a trusted path to be established between the TOE and the CLI using SSHv2 and for the GUI using HTTPS/TLSv1.2.

The following figure provides a visual depiction of the TOE deployment, including environment components.

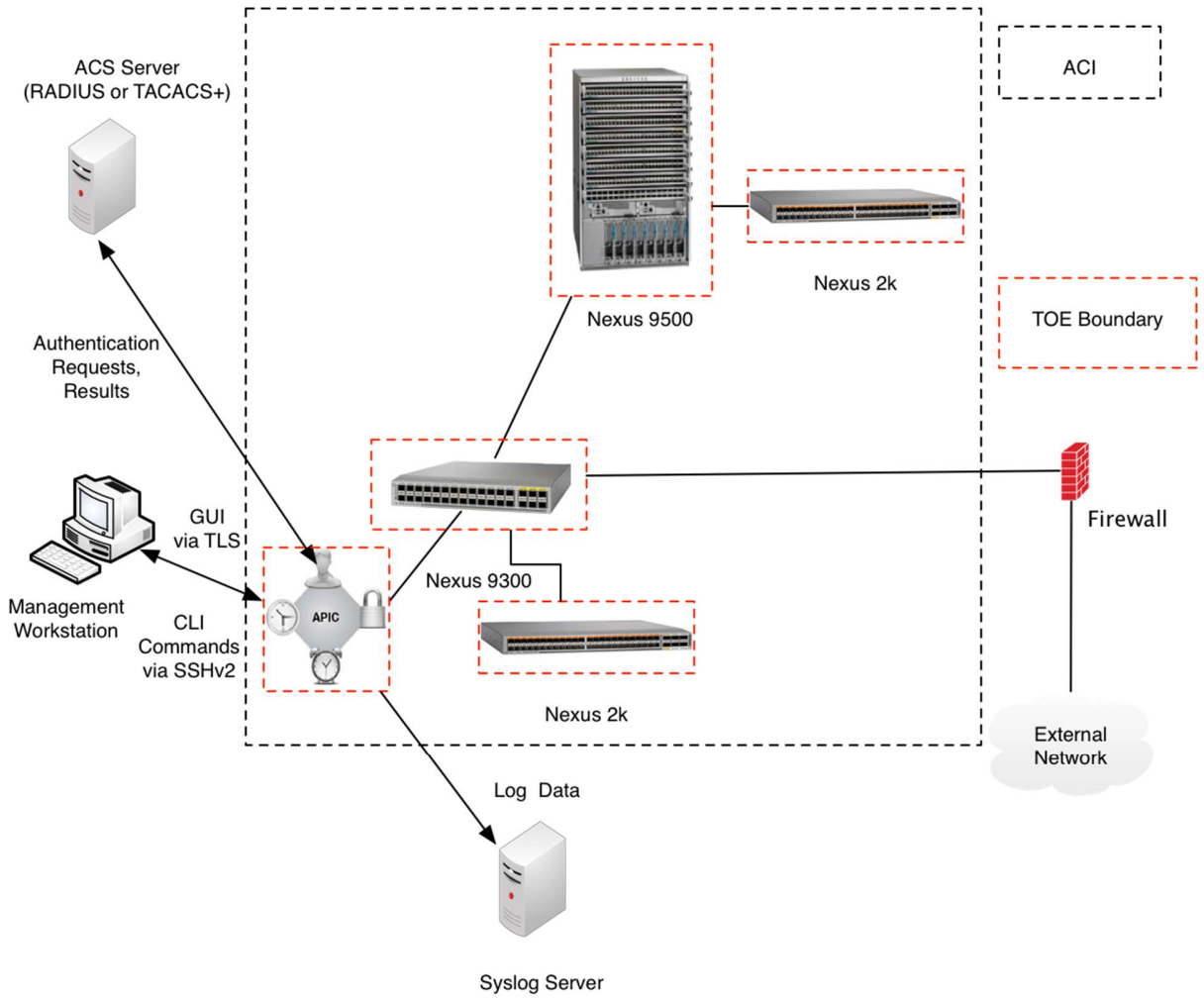

Figure 1 TOE and Environment Components

1.5 Operational Environment

1.5.1 Required components and software for the operational environment

Following is the list of environment components, in some cases optionally for the secure and functional operation of the TOE in its evaluated configuration. It is recommended the operational environment components be installed in a controlled environment where implementation of security policies can be enforced, and access controlled. The Authorized Administrator is responsible for the secure operation of the TOE. While the Authorized Administrator may be assigned responsibility of some or all the operational environment components that responsibility is not covered by this document unless specifically document within.

Table 5 Operational Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the Authorized Administrator to support TOE administration.
Firewall	Yes	This includes a firewall that must be placed between the ACI fabric and an external network.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation using web browser for HTTPS	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE Authorized Administrator to support TOE administration through HTTPS/TLSv1.2 protected channels. Any web browser that supports HTTPS/TLSv1.2 may be used.
NTP Serve	Yes	The TOE supports communications with an NTP server..
Syslog Server	No	This includes any syslog server to which the TOE would transmit syslog messages.
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. The TOE correctly leverages the services provided by this RADIUS or TACACS+ AAA server to provide single-use authentication to administrators.

1.6 Excluded Functionality

Following is the functionality that is excluded from the evaluated configuration. Not including this functionality does not affect the requirements being claimed.

Table 6 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Telnet	Telnet sends authentication data in plain text. This feature is disabled by default and must remain disabled in the evaluated configuration.
SNMP	SNMP may allow an unauthorized third party to gain access to a network device. This feature will be disabled in the evaluated configuration

2 Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on

the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). To further ensure proper and secure delivery of the TOE, the recipient must check the models received against the list of TOE component hardware models listed in Table 4 Hardware Models and Specification of this document. For APIC-SERVER-L3 or APIC-SERVER-M3, verify that the label displayed on the top of the device matches Table 4 Hardware Models and Specification of this document. Once the TOE has been inspected and external identification has been verified the unit(s) have the external identification as listed in Table 4 Hardware Models and Specification, follow the installation prerequisites for the environmental requirements in **[7]** for the platform models.

Step 7 After the TOE hardware has been installed and setup, follow the steps below for the approved methods for obtaining a Common Criteria evaluated software image:

Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. Software images are available from Cisco.com at the following: https://software.cisco.com [Login to CCO is required to download, but not to search.]

- The TOE ships with the correct software images installed. When a new software version is released, refer to **[2]** Performing Software Maintenance Upgrades.

Step 8 Once the file is downloaded, the Authorized Administrator verifies that it was not tampered with by either using a hash utility to verify the SHA512 hash by comparing the SHA512 hash that is listed on the Cisco web site and in Table 7 Evaluated Software Images or by using the show file command.

The "show file *filename* cksum" command on the Nexus 9K can be used to verify the SHA512 hash. Refer to section "Displaying File Checksums" in **[4]**.

If the SHA512 hashes do not match, contact Cisco Technical Assistance Center (TAC) https://mycase.cloudapps.cisco.com/case.

Step 9 Install the downloaded and verified software image onto your APIC as described in section "Setting Up the APIC" of chapter Initial Setup and in chapter "Fabric Initialization and Switch Discovery" in the *Cisco APIC Getting Started Guide* **[11]**. Start your APIC as described in **[11]**. Confirm that your APIC loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console. The APIC has the images for the ACI mode switches in the fabric also. First you will bring up the APIC and then the ACI switches.

Table 7 Evaluated Software Images

Software Version	Filename	Description	SHA 512
Cisco NX-OS System Software-ACI 14.2(4o)	aci-n9000-dk9.14.2.4o.bin	Cisco Nexus 9000 Series ACI Mode Switch Software 14.2(4o)	3c6a3bc5f8203570d32e1cc16807008521d94e0d4e91e435c98ed3524985349ceccb48b85e3282377e0c95577b584e87df998fad58f0c6cf9f648e885d6e5f0f
Cisco APIC 4.2(4o)	aci-apic-dk9.4.2.4o.iso	APIC Image for 4.2(4o) Release	6ff044de0bbcc3dc76ae01dc8bf8e87ca7cc4ee291162c77c7256a008bf2ef9d9ad7e2a00c856b62e900a80f1af7b08ff6cb6c83a8b4e6dd54c03676b023d4d3

3 Secure Installation and Configuration

3.1 Physical Installation

Follow the Cisco Nexus 9000 Series Hardware Installation and Reference Guides **[7]** for hardware installation instructions. Follow these directions for connecting all Nexus 9k models. All the Nexus 9k APIC and ACI models installed to make up the ACI fabric must be installed in a single datacenter within a physically secure facility. For example, a raised floor that has badge readers for access that is located within a secured building with external door badge readers and building security.

3.2 Initial Setup via Direct Console Connection

Once the Nexus 9K switches and APIC have been setup and powered-on, the APIC needs to be configured given that it acts as the central management interface for the switches and the entire ACI. Refer to **[11]** Cisco APIC Getting Started Guide, "Setting up the APIC" section. A console and keyboard can be directly connected into the APIC.

The APIC controller ships with a default BIOS password. The default password is 'password'. When the boot process starts, the boot screen displays the BIOS information on the console server.

To change the default BIOS password, follow the steps in **[11]** Initial Setup -> Changing the BIOS Default Password

3.2.1 Initial Set-up the APIC

When the Cisco Application Policy Infrastructure Controller (Cisco APIC) is launched for the first time, the Cisco APIC console presents a series of initial setup options. For many options, you can press Enter to choose the default setting that is displayed in brackets. At any point in the setup dialog, you can restart the dialog from the beginning by pressing Ctrl-C.

Following are some of the initial options that are presented:

Fabric Name:
This is the first entry request for information. If there are multiple ACI fabrics, it is recommended that each fabric has a unique name.

Number of Controllers:
It is recommended to have multiple controllers for redundancy, as well as multiple APICs.

Controller ID:

Each APIC must be configured in order, for example the first APIC must be configured with a Controller ID of 1. The Authorized Administrator cannot configure the APICs out of order for the first time. The Authorized Administrator must boot them and set them up in order. After they are all set up it does not matter what boot order is used later.

Controller Name:
This is the name that will identify each APIC. The Authorized Administrator may want to specify that it's APIC_1 indicating that it's the first controller to match the controller ID configured above.

TEP Address Pool:
A TEP is a Tunnel End Point that is used for VXLAN traffic and the Authorized Administrator must have TEPs to send traffic over the VXLANs. The ACI fabric uses VXLAN exclusively within the infrastructure space, or the space between the spine and leaf switches. This pool will assign each TEP an IP address on the leaf and spine switches.

VLAN ID for Infra Network:
The Infra Network (or Infrastructure Network) is the space between the leaf and spine switches. Will only need to use one VLAN ID since VXLAN will be used to allow it to scale. In the setup screen example above, it uses 4093 since 4094 is reserved for other communication. However, if using UCS within your environment, may want to take care not to use VLANs 3968-4047 as this range of VLANs is also reserved.

Authorized Administrator User Configuration:
Choose 'Y 'for Yes to enable strong passwords. When entering the new Authorized Administrator password, the Authorized Administrator will be required to choose a strong password according to the guidelines in section 4.3 Passwords

Following is a sample of the initial setup dialog as displayed on the console:

```
Cluster configuration ...
  Enter the fabric name [ACI Fabric1]:
  Enter the fabric ID (1-128) [1]:
  Enter the number of active controllers in the fabric (1-9) [3]:
  Enter the POD ID (1-9) [1]:
  Is this a standby controller? [NO]:

  Enter the controller ID (1-3) [1]:
  Enter the controller name [apic1]: sec-ifc5
  Enter address pool for TEP addresses [10.0.0.0/16]:
  Note: The infra VLAN ID should not be used elsewhere in your environment
      and should not overlap with any other reserved VLANs on other platforms.
  Enter the VLAN ID for infra network (2-4094): 3967
```

```
  Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
  Enable IPv6 for Out of Band Mgmt Interface? [N]:
  Enter the IPv4 address [192.168.10.1/24]: 172.23.142.29/21
  Enter the IPv4 address of the default gateway [None]: 172.23.136.1
  Enter the interface speed/duplex mode [auto]:

admin user configuration ...
  Enable strong passwords? [Y]:
  Enter the password for admin:

  Re-enter the password for admin:

Cluster configuration ...
  Fabric name: ACI Fabric1
  Fabric ID: 1
  Number of controllers: 3
  Controller name: sec-ifc5
  POD ID: 1
  Controller ID: 1
  TEP address pool: 10.0.0.0/16
  Infra VLAN ID: 3967
  Multicast address pool: 225.0.0.0/15

Out-of-band management configuration ...
  Management IP address: 172.23.142.29/21
  Default gateway: 172.23.136.1
  Interface speed/duplex mode: auto

admin user configuration ...
  Strong Passwords: Y
  User name: admin
  Password: ********

The above configuration will be applied ...

Warning: TEP address pool, Infra VLAN ID and Multicast address pool
         cannot be changed later, these are permanent until the
         fabric is wiped.

Would you like to edit the configuration? (y/n) [n]:
```

3.2.2 Switch Discovery and Setup of the ACI Fabric

The APIC is a central point of automated provisioning and management for all the switches that are part of the ACI fabric. To ensure that a switch is managed only by a single APIC cluster, each switch must be registered with that specific APIC cluster that manages the fabric.

Note: Before you begin registering a switch, make sure that all switches in the fabric are physically connected and booted in the desired configuration

Note: There are two methods for configuring the Fabric access policy either through the wizard or manually. An authorised Administrator should select and use only one of these methods when setting up a policy.

The APIC discovers new switches that are directly connected to any switch it currently manages. For example, each APIC instance in the cluster will firstly discover only the leaf switch to which it is directly connected. After that leaf switch is registered with the APIC, the APIC will discover all spine switches that are directly connected to the leaf switch. As each spine switch is registered, that APIC discovers all the leaf switches that are connected to that spine switch. This cascaded discovery allows the APIC to discover the entire fabric topology in a few simple steps. However, the Authorized Administrator must still register/authorize the switches with the APIC.

After a switch is registered with the APIC, the switch is part of the APIC-managed fabric inventory. With the Application Centric Infrastructure fabric (ACI fabric), the APIC is the single point of provisioning, management, and monitoring for switches in the infrastructure.

Once the first fabric switch is registered then the other leaf switches and then spine switches in the fabric will be discovered. Use the same naming conventions as described above in Figures 2 and 3 above and click Update.

You may have to click the refresh button to see the other switches that are registered.

After all the switches are registered with the APIC cluster, the APIC automatically discovers all the links and connectivity in the fabric and discovers the entire topology as a result. Once this is complete, the Authorized Administrator will need to validate the fabric topology. Refer to Validating the Fabric Topology in **[4]** for the steps using the GUI.

To validate the registered switches using the GUI, perform the following steps using the GUI.

Step 1 – On the menu bar, choose **Fabric** -> **Inventory**
Step 2 – In the Navigation pane, expand **Fabric Membership**
The switches in the fabric are displayed with their node IDs. In the Workpane, all the registered switches are displayed with the IP addresses that are assigned to them.

To validate the fabric topology using the GUI, perform the following steps:

Step1 - On the menu bar, choose **Fabric** -> **Inventory**

Step2 - In the Navigation pane, click **Topology**. The displayed summary shows the quantity and health of all pods, switches, APIC instances,and EPGs.

Step3 - In the **Work** pane, click the **Topology** tab. If an Inter-Pod Network block diagram is displayed, click **View Pod** in the desired pod. The displayed diagram shows all attached switches, APIC instances, and links.

Step4 (Optional) Hover over any component to view its health, status, and inventory information.

Step5 (Optional) To view the port-level connectivity of a leaf switch or spine switch, double-click its **icon** in the topology diagram.

Step6 (Optional) To refresh the topology diagram, click the **icon** in the upper right corner of the Workpane.

3.2.3 Tenant Setup

Once the Fabric nodes are setup, the Authorized Administrator use the **Tenants** tab in the menu bar to perform tenant management. Refer to Tenants chapter in **[12]**

A Tenant is a logical container or a folder for application policies. The Tenant can represent an actual tenant, an organization, a domain or can be used for the convenience of organizing information. A normal tenant represents a unit of isolation from a policy perspective, but it does not represent a private network. A special tenant named "**common**" has sharable policies that can be used by all tenants. Whereas the **infra** tenant is preconfigured for configuration related to the fabric infrastructure and the **mgmt** tenant is preconfigured for in-band and out-of-band connectivity configurations of hosts and fabric nodes (leafs, spines, and controllers).

A Private Network is also referred to as a Virtual Routing and Forwarding (VRF), private Layer 3 network, or context. It is a unique Layer 3 forwarding and application policy domain. Private networks are a child of the Tenant object. Private networks created in the common tenant are shared globally within the fabric. However, a private network that is intended to be used by multiple tenants and is not created in the common tenant requires explicit configuration to be shared. Refer to **[10]**, Configuring Layer 3 Virtualization -> Configuring VRFs.

A Context is a representation of a private Layer 3 network such as a VRF. It is a unit of isolation in the Cisco ACI framework. A Tenant can be configured with several contexts or VRFs to provide private layer 3 networks. Contexts can be configured within a single tenant (contained by the tenant) or can be shared across multiple tenants in the "common" tenant. This approach provides both multiple private Layer 3 networks per tenant and shared Layer 3 networks used by multiple tenants.

A Bridge Domain is the logical representation of a Layer 2 forwarding domain within the fabric. A Bridge Domain is a child of the tenant object and must be linked to a private network. Bridge domains will span all switches in which associated endpoint groups are configured. A bridge domain can have multiple subnets. However, a subnet is contained within a single bridge domain.

Application Profile is a convenient logical container for multiple hosts (physical or virtual). You can create application profile containers based on a variety of criteria, such as what function the application provides, how the application looks from the end-user perspective, where they are located within the context of the data center, or any other logical grouping relative to the implementation. Application profile servers are grouped in endpoint groups depending on the use of common policies. An application profile is a child object of the Tenant and a single Tenant can contain multiple application profiles. Refer to **[12]** Tenants -> Application Profile.

Endpoint groups (EPGs) are used to create logical groupings of devices (hosts or servers) that perform similar functions within the fabric and that will share similar policies. The endpoints devices are devices that are connected to the network either directly or indirectly. Endpoint devices have an address (identity), a location, and attributes, and can be either virtual or physical. Refer to **[12]** Tenants -> Application Profile -> Endpoint Group.

Following is a graphical overview of Tenants Logical Model that includes Tenant Policy, Endpoint Groups, Bridge Domains and Subgroups.

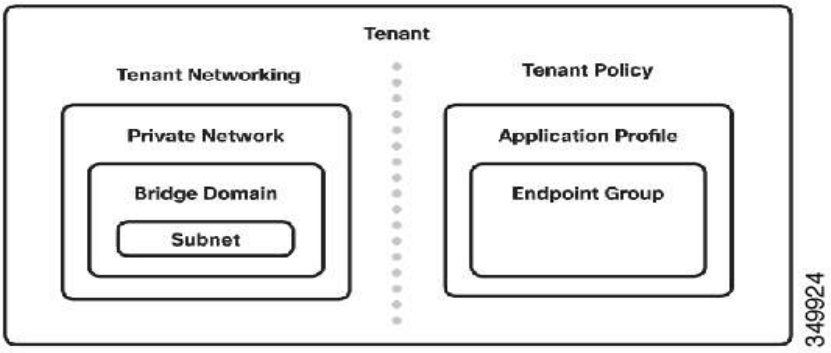

Figure 2 Logical Model Overview

The following image provides an example of a tenant to show how bridge domains are contained inside of private networks and how they are linked to endpoint groups and the other elements.

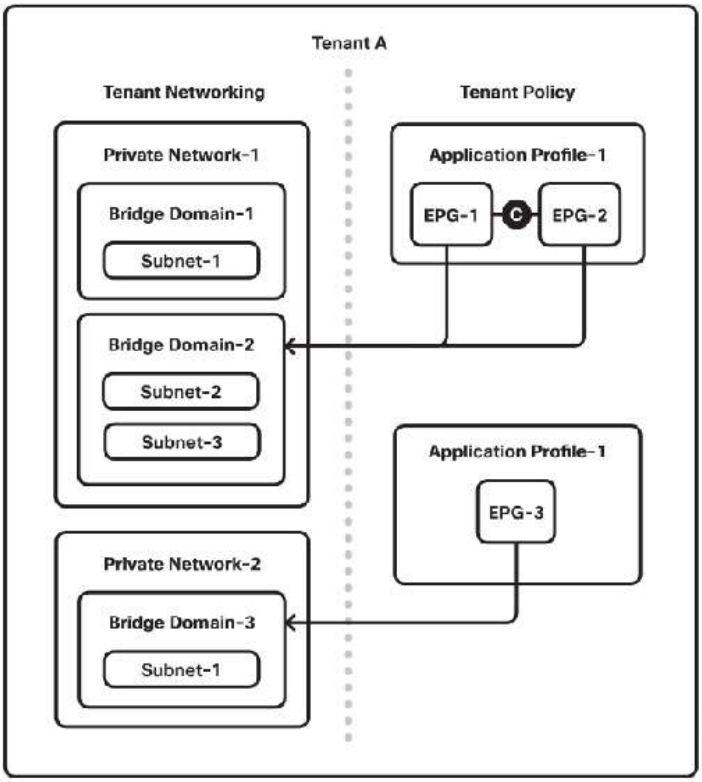

Figure 3 End Point Group as part of the Tenant Application Profile

The Authorized Administrator can verify and monitor the status and health of the components and policies by clicking on the **Stats** tab in the GUI to display on-demand statistics. The Authorized Administrator can also create policies to monitor Tenants and, diagnostic policies using the GUI. Refer to **[14]** Monitoring.

3.3 Remote Administration Protocols

3.3.1 Nexus CLI

The TOE supports a command line interface (CLI) that is used by the Authorized Administrator to manage the TOE. The CLI sessions are secured using SSHv2. By default, the Secure Shell (SSHv2) server is enabled and configured during the initial setup of the TOE.

To edit the SSHv2 configuration, refer to **[3]**, Configuring SSH and Telnet. Note, Telnet server is disabled by default on the Cisco NX-OS device and should not be used for TOE management in the evaluated configuration as sensitive information may be transmitted in the clear.

To configure hmac-sha1, hmac-sha2-256, hmac-sha-512, aes128-cbc,aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, aes256-gcm@openssh.com, aes128-gcm@openssh.com, enter the following commands:

apic1# configure terminal
apic1(config)#**ssh macs all**
apic1(config)#**ssh ciphers all**
apic1(config)# **ssh kexalgos curve25519-sha256 diffie-hellman-group-exchange-sha256 diffie-hellman-group14-sha1 ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521**
apic1(config)# **exit**

To configure SSHv2 on the APIC management port (mgmt0), enter the following commands, refer to **[18]** for additional information:

apic1# configure
apic1(config)# **switch 101**
apic1(config-switch)# **interface inband-mgmt0**
apic1(config-switch-if)# ip address 10.13.1.1/24 gateway 10.13.1.254
apic1(config-switch-if)# **exit**
apic1(config-switch)# **exit**

3.3.2 Nexus APIC GUI

The TOE supports a graphical user interface (GUI) that may be used by the Authorized Administrator to manage the TOE. The GUI sessions are secured using over HTTPS/TLSv1.2.

The TOE supports the following browsers:
Chrome version 59 (at minimum)
Firefox version 54 (at minimum)
Internet Explorer version 11 (at minimum)

Step 1 - Open with one of the browsers, enter the URL: https:// mgmt_ip-address. Use the out-of-band management IP address that you configured during the initial setup. For example, https://192.168.10.1.

Note, HTTPS is enabled by default. In addition, by default, http and http-to-https redirection are disabled.

Step 2 - When the login screen appears, enter the administrator name and password that you configured during the initial setup.

Step 3 - In the **Domain** field, from the drop-down list, choose the appropriate domain that is defined. If multiple login domains are defined, the **Domain** field is displayed. If the user does not choose a domain, the DefaultAuth login domain is used for authentication by default. This may result in login failure if the username is not in the DefaultAuth login domain.
Refer to **[11]** Accessing the GUI

In the GUI to configure hmac-sha1, hmac-sha2-256, hmac-sha-512, aes128-cbc,aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, aes256-gcm@openssh.com, aes128-gcm@openssh.com go to Fabric>Protocols>Pod>Management Access>Default>Policy. Under SSH complete the Ciphers and Macs.

3.3.3 Nexus REST API

The Application Policy Infrastructure Controller (APIC) REST API is a programmatic interface that uses REST architecture. The API accepts and returns HTTP (not enabled by default) or HTTPS messages that contain JavaScript Object Notation (JSON) or Extensible Markup Language (XML) documents.
The REST API is the interface into the management information tree (MIT) and allows manipulation of the object model state. The same REST interface is used by the APIC CLI and GUI, so that whenever information is displayed, it is read through the REST API, and when configuration changes are made, they are written through the REST API.

The REST API is not directly used by the Authorized Administrator to manage the TOE in the evaluated configuration.

3.4 Audit Logging Configuration

The TOE generates and logs system messages to the console and the log file by default. The following table lists the default settings for the system logging parameters.

Table 8 Default System Message Logging Parameters

Parameters	Default
Console Logging	Enabled at severity level 2
Monitor Logging	Enabled at severity level 5

Parameters	Default
Log file Logging	Enabled to log messages at severity level 5
Module Logging	Enabled at severity level 5
Facility logging	Enabled
Time-stamp units	Seconds
Syslog server logging	Disabled
Syslog server configuration distribution	Disabled

Each new event record Managed Object (MO) is added to one of three separate event logs, depending on the cause of the event:

- Audit log—Holds objects that are records of user-initiated events such as logins and logouts (aaa:SessionLR) or configuration changes (aaa:ModLR) that are required to be auditable.
- Health score log—Holds records of changes in the health score (health:Record) of the system or components.
- Event log—Holds records of other system-generated events (event:Record) such as link state transitions.

Table 9 Event Properties

Property	Description
Code	The event code
ID	The unique identifier assigned to the event
Affected	The MO associated with the event
Trigger	The probable cause category (example, transition)
Severity	The severity level of the event. Events are of severity level 'info'
Created	The day and tine when the event occurred
Descr	The description of the event

Each log collects and retains event records. An event MO remains in the log until it is purged when the log reaches capacity and space is needed for new event records. The retention and purge behaviour for each log is specified in a record retention policy (event:ARetP) object associated with each log.

The Authorized Administrator can configure the TOE to send the log files to a remote syslog server. It is recommended if configuring a syslog server, to use the management virtual routing and forwarding (VRF) instance. This will provide a protected transmission. Refer to **[2]** Configuring System Message Logging -> Configuring Syslog Servers and **[10]** Configuring Layer 3 Virtualization -> Configuring VRFs

3.4.1 ACI Mode

During the operation of the ACI, the TOE generates system messages to the console to be viewed by the Authorized Administrator. A system message typically contains a subset of information about the fault or event. Many system messages are specific to the action that a user is performing or the object that a user is configuring or administering. System messages are created by various sources, such as the Application Policy Infrastructure Controller (APIC) or the spine and leaf switches in the ACI fabric. Refer to **NX-OS System Messages [22C]**.

The TOE supports local logging of events which are referred to as system messages in **Monitoring** -> **Faults, Errors, Events, Audit Logs [14]** and **NX-OS System Messages [22C]**. The logs are written to a circular file and remains in the log until it is purged (overwritten) when the log reaches capacity and space is needed for new events. The Authorized Administrator can optionally configure the log files to be sent to a remote URL in the GUI by selecting **Start Remote Logging**, that is set in **Management Tools** -> **User Login Menu Options**, click on **Start Remote Logging**. The log files are then forwarded to a remote URL. Refer to **[14].**

The System Messages contain a timestamp that includes the date and time of the event, the facility code that consists of wo or more uppercase letters that indicate the facility to which the message refers. A facility can be a hardware device, a protocol, or a module of the system software. The final field is the severity level that is a single-digit code from 0-7, as follows, noting the lower the number, the more serious the event:

Table 10 NX-OS Message Severity Levels

Level	Severity Level (NX-OS)	ITU Level (ACI)	Description
0	Emergency		System is unusable
1	Alert	Critical	Immediate action is required
2	Critical	Major	Critical condition
3	Error	Minor	Error condition
4	Warning	Warning	Warning condition
5	Notification	Cleared	Normal but significant condition
6	Informational		Informational message only
7	Debugging		Messages that appears during debugging only

To view the logs, refer to [22C], Events and Audit Logs -> Viewing Events.

3.4.2 APIC

The APIC maintains a comprehensive, up-to-date run-time representation of the administrative and operational state of the Cisco Application Centric Infrastructure (ACI) fabric system in a collection of managed objects (MOs). Any configuration or state change in any MO is considered an event. Each of the events is specified in the log records in enough detail to identify the user or object for which the event is associated, when the event occurred, where the event occurred, the type of event that occurred and the outcome of the event.

For a list of syslog messages that the APIC can generate, refer to **[22b]**.

3.4.3 Required Auditable Events

To ensure audit records are generated for the required auditable events, the TOE must be configured in its evaluated configuration as specified in this document. This is to ensure that auditing is enabled, and the audit records are being generated for the required auditable events.

Below are the required auditable events.

Table 11 Required Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU.2	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UID.2	All use of the identification mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	None
FMT_MTD.1	All modifications to the values of TSF data	The identity of the authorized administrator performing the operation.
FMT_SMF.1	Use of the management functions	The identity of the authorized administrator performing the operation.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.
FPT_TST.1	Execution of the TSF self tests and the results of the tests	None

Requirement	Auditable Events	Additional Audit Record Contents
FTA_SSL.4	Termination of an interactive session by a user.	None
FTP_TRP.1	Attempts to use the trusted path functions.	Identification of the user associated with all trusted path invocations including failures, if available.

3.4.4 Viewing Audit Records

The Authorized Administrator can view the logged events using the GUI. The events that are showed are only those events that are relevant to the current GUI context. The **History** tab appears in the GUI Work pane for the relevant log entries in the event log, health log and the audit log. To view the events, perform the following steps:

- Step 1 - In the menu bar, click **Admin**.
- Step 2 - In the submenu bar, click **AAA**.
- Step 3 - In the Navigation pane, choose **AAA Authentication**.
- Step 4 - In the Work pane, click the **History tab**.
- Step 5 - Under the History tab, click the **Events subtab** to view the event log.
- Step 6 - Under the History tab, click the **Audit Log subtab** to view the audit log.
- Step 7 - Double-click a **log entry** to view additional details about the event.

Refer to **[22b]** for additional details

3.4.5 Deleting Audit Records

The TOE provides the Authorized Administrator the ability to delete audit records stored within the TOE. However, there is no interface available to modify the audit records.

To delete the audit records, use the **clear logging** command.

TOE-common-criteria# **clear logging**
Clear logging buffer [confirm] <**ENTER**>
TOE-common-criteria# **clear logging nvram**

The Authorized Administrator can configure the following settings:

- Maximum Size—The maximum number of records to be maintained in the log. The range is 1000 to 500000 records; the default is 100000 records.
- Purge Window Size— The maximum number of records to be deleted in a single swipe. Record deletion is performed periodically (every 30 seconds) in batches.

The maximum size of a batch should be chosen to avoid spikes in I/O and CPU utilization. The range is 100 to 1000 records; the default is 250 records.

Refer to **[22b]** Logs and Retention Policies for details and GUI configuration options.

4 Secure Management

4.1 User Roles

The TOE maintains an Authorized Administrator role to administer the TOE locally and remotely. During the installation of the TOE, the Authorized Administrator user is created and has all the required permissions to manage and administer the TOE in the evaluated configuration as defined in this document. Additional Authorized Administrator users may be created, noting that each Authorized Administrator user must be assigned a unique user name and password.

All users of the TOE are considered Authorized Administrators. It is assumed all administrators are trusted, trained and knowledgeable and will follow the guidance to ensure the TOE is properly monitored and operated in a secure manner. The TOE includes a set of Administrator roles that include a defined set of privileges, privilege types and security tags that identify the portion of the management structure of the TOE they can access. Configuring additional Administrator roles, such as a 'Tenant-admin' can only have access to the tenant to which they're associated. Creating additional Administrator roles does not impact the traffic flow, it simply appoints additional Administrators verse a single Administrator to manage functions of the TOE See **[12]** Management -> Role-Based Access Control

4.2 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the Authorized Administrator.

Each Authorized Administrator of the TOE must have a unique username and password.

By default, the TOE uses local authentication and authorization. The Authorized Administrator must be successfully identified and authenticated prior to gaining access to the TOE and the TOE security management functions.

The TOE can optionally be configured to support IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced. See **[3]** Configuring AAA, Configuring RADIUS, Configuring TACACS+

4.3 Passwords

By default, the TOE is set to check for password-strength which prevents the user from choosing weak passwords. The password must be at least eight characters, include both

upper and lower alpha characters, numeric characters and may include the following special charters:
"+","=", ".","_","\","-",

The following are recommendations for a strong password to have the following characteristics in addition to the required elements listed above:

- Does not contain many consecutive characters (such as abcd)
- Does not contain many repeating characters (such as aaabbb)
- Does not contain dictionary words
- Does not contain proper names

Refer to **[3]** Configuring User Accounts and RBAC -> Enabling Password-Strength Checking for details.

4.4 Login Banners

The TOE provides the Authorized Administrator the ability to configure a banner that is displayed before the username and password prompts.

Banners are required to be displayed when the user is prompted to log in to the CLI or GUI. The CLI banner is a simple text string to be printed at the terminal before the password prompt. You can define a banner for the APIC CLI and a separate banner for the switch CLI. The GUI banner displays at the APIC URL before user login authentication.

To create the banner, perform the following steps:

Step 1 - On the APIC menu bar, choose **System > System Settings**.
Step 2 - In the Navigation pane, click APIC Identification Preferences.
Step 3 - In the work pane, complete the following fields as desired:

- To configure an APIC CLI banner, type the banner text into the **Controller CLI Banner** textbox.
- To configure a switch CLI banner, type the banner text into the **Switch CLI Banner** textbox.
- To configure an APIC GUI banner, type the URL of a site hosting the desired HTML into the **GUI Banner (URL)** textbox.

Note: The URL site owner must allow the site to be placed in an iFrame to display the informational banner. If the owner of the site sets the x-frame-option to deny or same origin, the site the URL points to will not appear.
Step 4 - Click Submit.

Refer to APIC GUI Overview -> Personalizing the Interface -> Adding a Login Banner to the CLI or GUI **[11]**

4.5 Clock Management

The TOE provides the Authorized Administrator the ability to set the time for the TOE. The TOE also provides the ability to set the local (hardware clock) as well as setting the clock protocol. The TOE also provides the options to set a 12 hour or 24-hour time clock, to show the time zone and to set summer (daylight savings) time.

To set the local time, use the **clock set** command.

clock set < HH:MM:SS Current Time> < Day of the month> < Month of the year>

clock set <06:45:10><Sunday><May>

Refer to **[5]** Chapter: C Commands

In the evaluated configuration Network Time Protocol (NTP), a time synchronization protocol for nodes distributed across a network. The clocks are organized into a master-member synchronization hierarchy with the grandmaster clock, the clock at the top of the hierarchy, determining the reference time for the entire system. When NTP is enabled, a spine is automatically chosen as a master to which the entire site gets synced.

For instructions on how to configure NTP Server, refer to the following sections in **[18]**

- First Time setup Wizard - > NTP and
- Provisioning Core ACI Fabric services > Time Sychronization and NTP > Configuring NTP Using the GUI

4.6 Configuring Administrator Management Access to APIC

The APIC controller has two routes to reach the management network, one is by using the in-band management interface and the other is by using the out-of-band management interface. In the evaluated configuration, the TOE will be configured for in-band management. A management EPG will be configured to ensure that only In-Bound Management Access is allowed within the ACI Fabric.

The APIC management interface does not support an IPv6 address and therefore cannot connect to an external IPv6 server through this interface.

Configuring the external management instance profile under the management tenant for in-band or out-of-band has no effect on the protocols that are configured under the fabric-wide communication policies. The subnets and contracts specified under the external management instance profile do not affect HTTP/HTTPS or SSH. Refer to Remote Administration Protocols in **Section 3.3** of this document.

Following is an example of assigning a VLAN for the APIC in-band management using the CLI:

Step 1 Assign a VLAN for the APIC inband management, as shown in the following example:

Example:
apic1(config)#
apic1(config)# vlan-domain inband-mgmt
apic1(config-vlan) **vlan 10**
apic1(config-vlan) **exit**

Step 2 Provide external connectivity to the inband management ports, as shown in the following example:

Example:
Note In this step, the controller is connected to a port on a leaf switch. You must add a VLAN domain member on that port. In this example, in leaf 101, the port ethernet 1/2 is connected to controller 1. You are configuring the VLAN domain member "in-band management". This is one part of the connection. The other part is that the management station is connected to leaf 102, interface ethernet 1/3. A controller is one machine connected to one port on the leaf switch, which in this case is leaf 102. The machine is trying to connect to the controller from the outside (ethernet 1/3).

apic1(config)#
apic1(config)# **leaf 101**
apic1(config-leaf) internet ethernet 1/2
apic1(config-leaf-if)# vlan-domain member inband-mgmt
apic1(config-leaf-if)# **exit**
apic1(config)# **leaf 102**
apic1(config-leaf) internet ethernet 1/3
apic1(config-leaf-if)# vlan-domain member inband-mgmt
apic1(config-leaf-if)# switchport trunk allowed vlan
apic1(config-leaf-if)# **exit**

Refer to Configuring In-Band Management Access Using the NX-OS Style CLI **[18]**.

To configure in-band management access using the GUI, refer to Configuring In-Band Management Access Using the Advanced GUI **[18]**

4.6.1 Management Tenants

The management [**mgmt**] tenant provides convenient means to configure access policies for fabric nodes. While fabric nodes are accessible and configurable through the APIC,

they can also be accessed directly using in-band and out-of band connections. In-band and out-of-band policies are configured under the **mgmt** tenant.

Using the following example, the management profile includes the in-band EPG MO that provides access to management functions via the in-band contract (*vzBrCP*). The *vzBrCP* enables *fvAEPg*, *l2extInstP*, and *l3extInstP* EPGs to consume the in-band EPG. This exposes the fabric management to locally connected devices, as well as devices connected over Layer 2 bridged external networks, and Layer 3 routed external networks. If the consumer and provider EPGs are in different tenants, they can use a bridge domain and VRF from the common tenant. Authentication, access, and audit logging apply to these connections; any user attempting to access management functions through the in-band EPG must have the appropriate access privileges.

The figure below shows an in-band management access scenario.

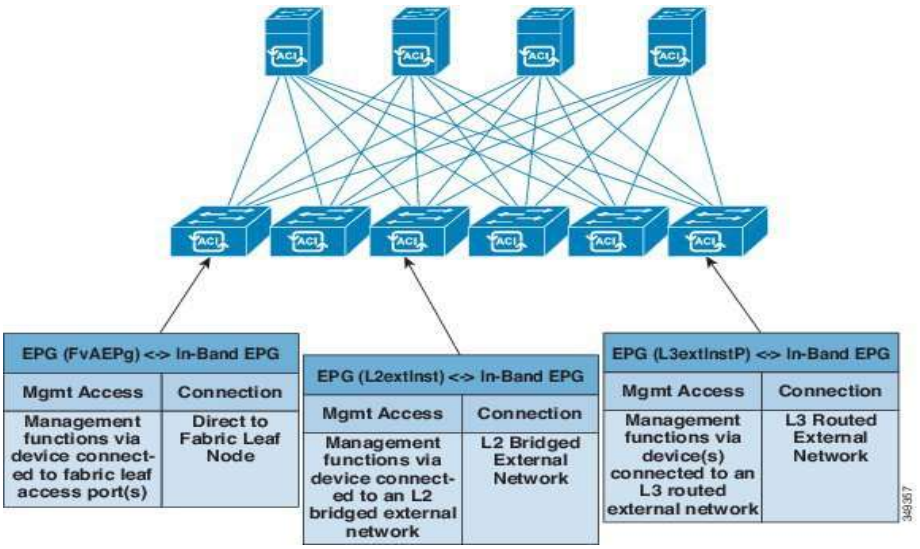

Figure 4 In-Band Tenant Management

As shown above in Figure 4, separate tenants ensure traffic is isolated for a specific tenant. Traffic can only flow between different EPGs once a specific contract is configured for which the traffic is allowed to flow. The in-band EPG MO ensures the management traffic will be separate from the regular user data traffic. This configuration settings will have to be done before assigning the static addresses for the APIC, Leaves, and Spines to ensure the traffic flow policies are enforced.

4.7 Information Flow Policies

The TOE enforces information flow policies on network packets that are receive by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, permit the traffic, drop the traffic or ignore the traffic.

The Cisco APIC policy model is built on a series of one or more tenants that allow segregation of the network infrastructure administration and data flows. These tenants can be used for customers, business units, or groups, depending on organizational needs as described in section 3.2.3 .

The Authorized Administrator configures the information flow control using the APIC policies. The traffic rules that can be configured include permit the traffic to flow, drop the traffic or ignore the traffic. This is set within the contracts that specify the subjects, filters, and actions of the policy rules applied to Endpoint Groups (EPGs).

The network traffic is mediated via the I/O network module ports. Refer to ACI Policy Model, Tenants, VRFs, Endpoint Groups, Contracts **[14]**.

4.7.1 Tenants

A tenant (fvTenant) is a logical container for application policies that enable an administrator to exercise domain-based flow control. A tenant represents a unit of isolation from a policy perspective, but it does not represent a private network.

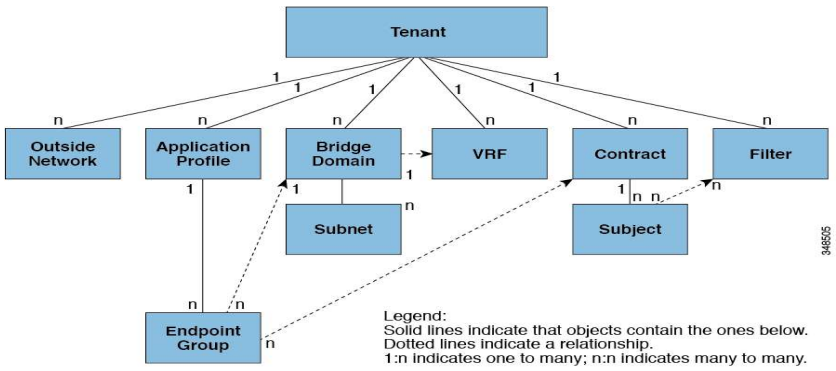

Figure 5 Tenants

4.7.1.1 EPGs

An endpoint group (EPG) is a managed object that is a named logical entity that contains a collection of endpoints. Endpoints are devices that are connected to the network directly or indirectly.

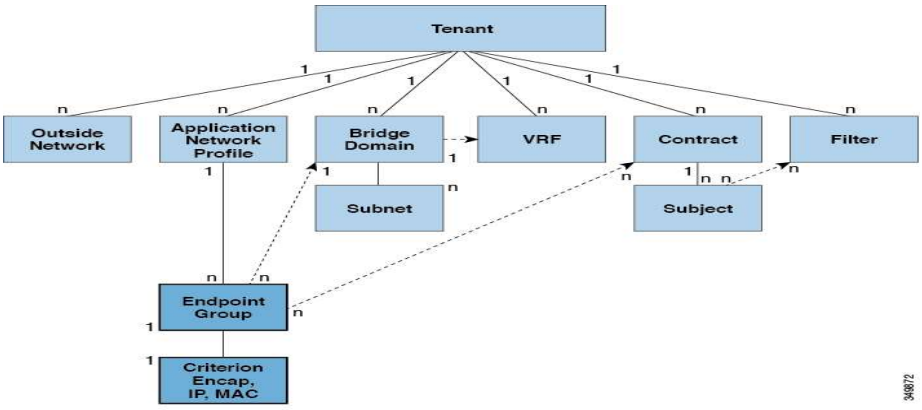

Figure 6 Endpoint Group (EPG)

The ACI fabric can contain the following types of EPGs:

- Application endpoint group (fvAEPg)
- Layer 2 external outside network instance endpoint group (l2extInstP)
- Layer 3 external outside network instance endpoint group (l3extInstP)
- Management endpoint groups for out-of-band (mgmtOoB) or in-band (mgmtInB) access

EPGs contain endpoints that have common policy requirements such as security, virtual machine mobility (VMM), QoS, or Layer 4 to Layer 7 services. Rather than configure and manage endpoints individually, they are placed in an EPG and are managed as a group.

Policies apply to EPGs, never to individual endpoints. An EPG can be statically configured by the Authorized Administrator in the APIC.

4.7.1.2 Contracts

In addition to EPGs, contracts (*vzBrCP*) are key objects in the policy model. EPGs can only communicate with other EPGs according to contract rules. The following figure shows the location of contracts in the management information tree (MIT) and their relation to other objects in the tenant.

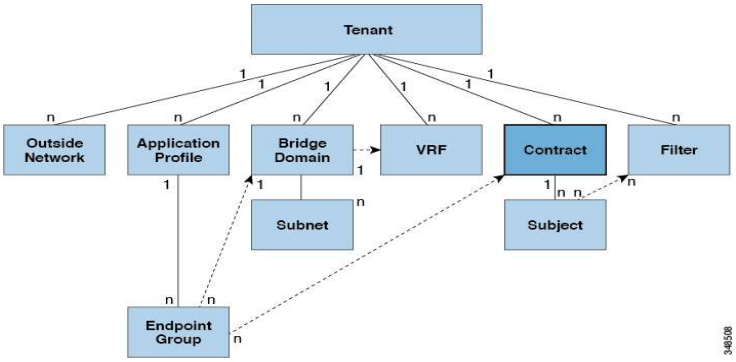

Figure 7 Contracts

The Authorized Administrator uses a contract to select the type(s) of traffic that can pass between EPGs, including the protocols and ports allowed. If there is no contract, inter-EPG communication is disabled by default. There is no contract required for intra-EPG communication; intra-EPG communication is always implicitly allowed. The following lists the types of endpoint group communications governed by contracts:

- Between ACI fabric application EPGs (*fvAEPg*), both intra-tenant and inter-tenant
- Between ACI fabric application EPGs and Layer 2 external outside network instance EPGs (*l2extInstP*)
- Between ACI fabric application EPGs and Layer 3 external outside network instance EPGs (*l3extInstP*)
- Between ACI fabric out-of-band (mgmtOoB) or in-band (mgmtInB) management EPGs

Contracts can contain multiple communication rules and multiple EPGs can both consume and provide multiple contracts.

Refer to Contract Scope Examples in **[14]** to see how contracts use labels to classify which objects can and cannot communicate with each other, how aliases (alternative names) can be applied to objects and how filters for layer 2 to layer 4 fields that can dictate the protocols and ports in both the in and out directions.

5 Modes of Operation

The TOE has several modes of operation, these modes are as follows:

System BIOS Setup – This is an interactive text-based program for configuring low-level switch hardware and boot options. When this program is exited, the switch transitions to Booting mode. In this mode the switch has no IP address and therefore does not handle network traffic, thus preventing an insecure state.

Booting – while booting, the switches drop all network traffic until the APIC and ACI mode image and configuration has loaded. The boot mode transitions to the following modes:

BIOS Loader Prompt – When the APIC and supervisor modules power up, a specialized BIOS image automatically loads and tries to locate a valid kickstart image for booting the system. If a valid ACI or APIC image is not found, the following BIOS loader prompt displays:
loader>

Loader Prompt – This mode allows the Authorized Administrator to enter into the console port to specify the TFTP server to load the APIC and ACI mode image. No authentication before interacting with the loader is required. In this mode the switch does not handle any network traffic, apart from what is required to perform the TFTP boot, thus preventing an insecure state.

Setup – The APIC and ACI switch enters this mode after booting if no configuration exists (e.g. First boot). In this mode the switch has no IP address and therefore does not handle network traffic, thus preventing an insecure state.

The APIC and ACI switch starts an interactive setup program to allow the Authorized Administrator to enter basic configuration data, such as the switch's IP address, administrator password, and management channels. When the setup program is exited, the switch transitions to the Normal mode.

Fabric Discovery – During the setup there is a Fabric discovery of all ACI switches. The ACI fabric uses an infrastructure space, which is securely isolated in the fabric and is where all the topology discovery, fabric management, and infrastructure addressing is performed. ACI fabric management communication within the fabric takes place in the infrastructure space through internal private IP addresses.

This addressing scheme allows the APIC to communicate with fabric nodes and other Cisco APIC controllers in the cluster. The APIC discovers the IP address and node

information of other Cisco APIC controllers in the cluster using the Link Layer Discovery Protocol (LLDP)-based discovery process.

The following describes the APIC cluster discovery process:

- Each APIC in the Cisco ACI uses an internal private IP address to communicate with the ACI nodes and other APICs in the cluster. The APIC discovers the IP address of other APIC controllers in the cluster through the LLDP-based discovery process.
- APICs maintain an appliance vector (AV), which provides a mapping from an APIC ID to an APIC IP address and a universally unique identifier (UUID) of the APIC. Initially, each APIC starts with an AV filled with its local IP address, and all other APIC slots are marked as unknown.
- When a switch reboots, the policy element (PE) on the leaf gets its AV from the APIC. The switch then advertises this AV to all of its neighbours and reports any discrepancies between its local AV and neighbours' AVs to all the APICs in its local AV.
- Using this process, the APIC learns about the other APIC controllers in the ACI through switches. After validating these newly discovered APIC controllers in the cluster, the APIC controllers update their local AV and program the switches with the new AV. Switches then start advertising this new AV. This process continues until all the switches have the identical AV and all APIC controllers know the IP address of all the other APIC controllers.

Normal - The APIC and ACI mode images and configuration is loaded and the switch is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all TOE security functions are operating as configured.

Graceful Insertion and Removal (GIR) Mode - The Graceful Insertion and Removal (GIR) mode, or maintenance mode, allows you to isolate a switch from the network with minimum service disruption. In the GIR mode you can perform real-time debugging without affecting traffic.

You can use graceful insertion and removal to gracefully remove a switch and isolate it from the network in order to perform debugging operations. The switch is removed from the regular forwarding path with minimal traffic disruption.

In graceful removal, all external protocols are gracefully brought down except the fabric protocol (IS-IS) and the switch is isolated from the network. During maintenance mode, the maximum metric is advertised in IS-IS within the Cisco Application Centric Infrastructure (Cisco ACI) fabric and therefore the leaf switch in maintenance mode does not attract traffic from the spine switches. In addition, all front-panel interfaces on the

switch are shutdown except for the fabric interfaces. To return the switch to its fully operational (normal) mode after the debugging operations, you must recommission the switch. This operation will trigger a stateless reload of the switch.

In graceful insertion, the switch is automatically decommissioned, rebooted, and recommissioned. When recommissioning is completed, all external protocols are restored and maximum metric in IS-IS is reset after 10 minutes.

5.1 Module States

The Nexus switches can be deployed with a single or redundant pair of supervisors. The supervisor modules have some additional module states. The '**show module**' command shows the status of the supervisor or I/O cards.

Table 12 Module States[1]

Show Module Command Status Output	Description
Powered Up	The hardware has electrical power. When the hardware is powered up, the software begins booting
Testing	The switch module has established connection with the supervisor and the switching module is performing bootup diagnostics.
Initializing	The diagnostics have completed successfully and the configuration us being downloaded.
Failure	The switch detects a switching module failure upon initialization and automatically attempts to power-cycle the module three times. After the third attempt, the module power downs.
OK	The switch is ready to be configured.
Power-denied	The switch detects insufficient power for switching module power-up.
Active	This module is the active supervisor module and the switch is ready to be configured.
HA-standby	The HA switchover mechanism is enabled on the standby supervisor module.

The following table shows the status of the supervisor cards when set in redundancy mode.

Table 13 Redundancy Modes for Supervisor Cards

Redundancy Mode	Description
Not present	The supervisor module is not present or is not plugged into the chassis.
Initializing	The diagnostics have passed, and the configuration is being downloaded.
Active	The active supervisor module and the switch are ready to be configured.
Standby	A switchover is possible.
Failed	The switch detects a supervisor module failure on initialization and automatically attempts to power-cycle the module three (3) times. After the third attempt it continues to display a failed state.
Offline	The supervisor module is intentionally shut down for debugging purposes.
At BIOS	The switch has established connection with the supervisor and the supervisor module is performing diagnostics.

[1] Section "Displaying the Current Status of a Module" **[7]**

Redundancy Mode	Description
Unknown	The switch is in an invalid state. If it persists, call Cisco TAC.

5.2 Self-Tests

During the initial start-up of the TOE, the TOE runs a suite of self-tests to verify its correct operation. The TOE also runs the suite of tests during reboots. All ports are blocked from moving to a forwarding state during the self tests. Only when all components of all tests pass, is the system placed in an operational state and ports are allowed to forward data traffic.

The power-up self-tests run on the supervisor and line cards. If any of the self-tests fail, the TOE will transition into an error state. In the error state all data transmission is halted and the TOE outputs status information indicating the failure.

If any of the tests fail, the following actions should be taken:

Use the **system cores** command to set up core dumps on the system. This will provide additional information on the cause of the crash:

switch# configure terminal
switch(config)# system cores slot0:core_file
Example:
switch# system cores tftp://x.x.x.x/filename
switch# show system cores

Note, the filename (indicated by filename) must exist in the TFTP server directory. Restart the TOE to [re]run the self tests and determine if normal operation can be resumed. If the problem persists, contact Cisco TAC.

6 Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized users of the TOE to ensure that the TOE environment provides the necessary functions. The following identifies the requirements and the associated security measures of the authorized users.

Table 14 Operational Environment Security Measures

Security Objective for the Operational Environment (from the Security Target)	Definition of the Security Objective (from the Security Target)	Responsibility of the Administrators
OE.ADMIN	The Authorized Administrator is well trained and trusted to manage the TOE, to configure the IT environment and required non-TOE devices for the proper network support.	Authorized Administrators must be trained and must read, understand and follow the guidance in this document to securely install and operate the TOE.
OE.CONNECTION	The operational environment will have the required protected network support for the operation of the TOE to prevent unauthorized access to the TOE.	Authorized Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE.
OE.FIREWALL	The operational environment of the TOE shall provide a firewall located between the ACI fabric and external networks to protect against malicious or unauthorized traffic from entering the ACI fabric.	The Authorized Administrator of the TOE must ensure that the Operational Environment provides a properly configured firewall between the TOE (ACI fabric) and external networks.
OE.LOCATE	The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access.	The TOE and the operational environment components are required to be installed in a controlled environment where access is controlled. The Authorized Administrator is responsible for the secure operation of the TOE. While the Authorized Administrator may be assigned responsibility of some or all of the operational environment components that responsibility is not covered by this document unless specifically document within. The operational environment components include the following:

Security Objective for the Operational Environment (from the Security Target)	Definition of the Security Objective (from the Security Target)	Responsibility of the Administrators
		A local console that is directly connected to the TOE for TOE administration, Remote administration of the TOE using the CLI, this remote connection is secured with SSHv2, Remote administration of the TOE using the GUI, this remote connection is secured with HTTPS, and Firewall that is placed between the ACI fabric and the external network

7 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation at:

With CCO login:
http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com

7.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

7.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com