



CISCO ACI OPERATIONAL BEST PRACTICES

*A technical series and e-book
designed to help get the most out
of your ACI Fabrics*



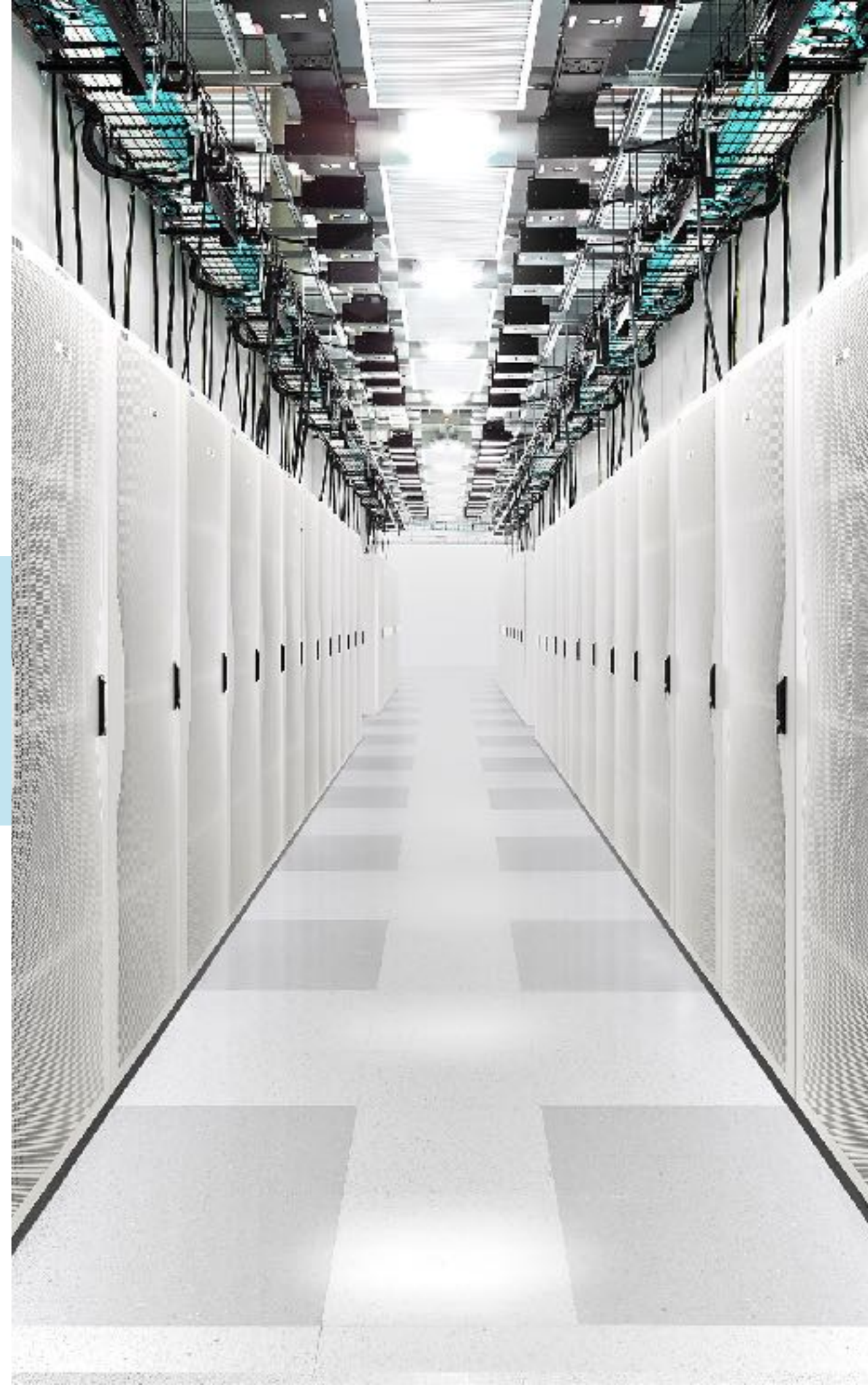
Welcome...

ACI is a modern, powerful, and fully programmable data center fabric. With almost 10 years in production and thousands upon thousands of deployments there is a lot that can be achieved.

For IT Operations Teams, the power of ACI also brings with it an evolution of the processes to design, configure, migrate and troubleshoot.

This e-book is your treasure map to information on various aspects of operating ACI. Its intent is to help you make the most out of your investment in ACI as a solution, avoid common mistakes, and collect various tips and tricks from lessons learned by others.

With anything that dares to call itself “*Best Practices*” we should also make it clear that the information contained within attempts to address the most common designs and situations. We realize that every customer will have unique requirements that require sometimes unique solutions. In any case, it is always best to consult official Cisco documentation and your own Cisco account team to plan for the best results in your own environment.



This Is A Technical Series....

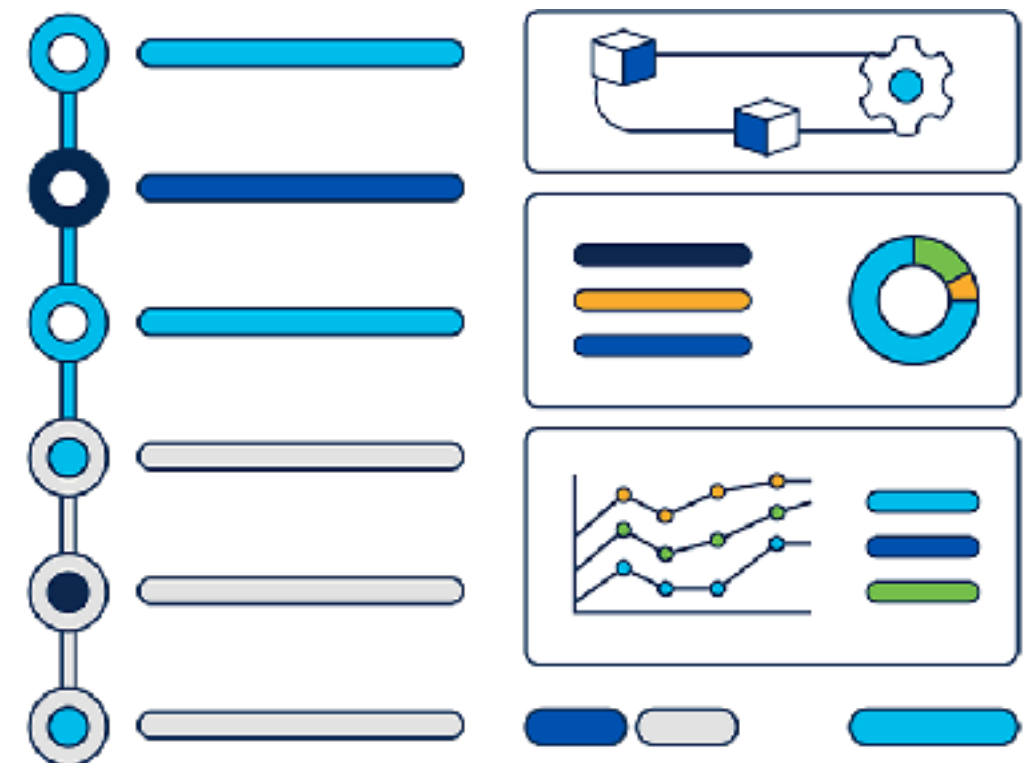
The format of this document is organized by major operational topic. In each topic we will detail the intent and share links to video playback plus where to download the source content for your own further use. In addition, and where possible, we will link and refer you to additional sources that you may find useful.

Each topic is more or less self contained but we present them in the order which we feel is most useful. It is not always necessary to know the contents of a previous module before reviewing a later one.

We assume you have at least introductory level knowledge of ACI and its operations.

Over time, we intend to add more topics and expand this document.

v1.0(1) published November 2023





Who We Are

All the content you find here was created or inspired by a talented and varied team of Data Center Networking Cisco all-stars.

Our extended team includes (Data Center Networking Business Unit) Technical Marketing Engineers, Principal and Distinguished Engineers, Product Managers, Engineering Leaders, plus a generous assist from our brethren in Cisco CX.

We are a passionate bunch who believe in the power and process of ACI. We hope our passion translates to you in the form of successful deployments and outcomes to your own business.

<https://www.cisco.com/go/aci>

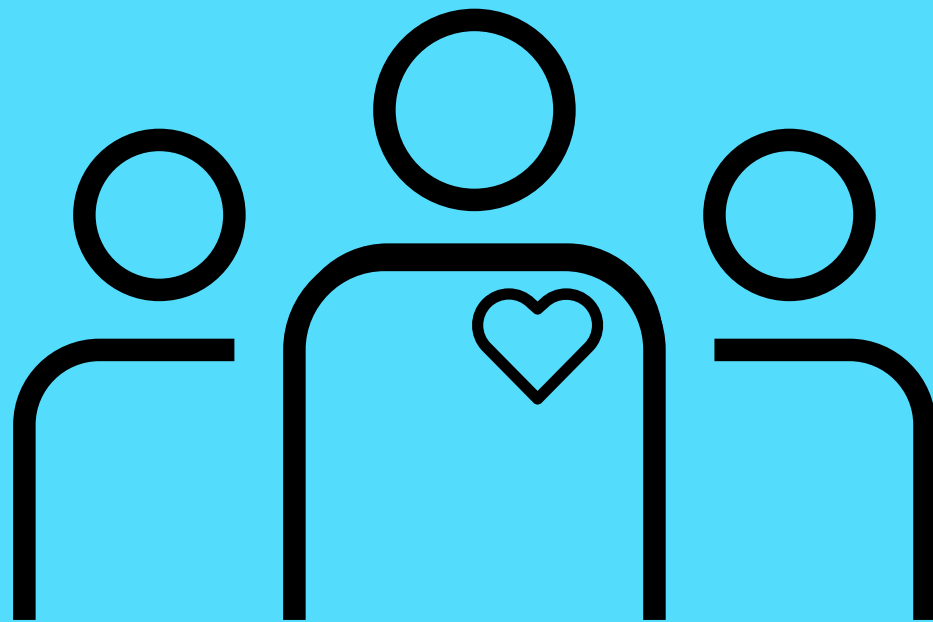


Table Of Contents

Click on any module sub-entry to view content

Module One:

[ACI Access Policies](#)

[Further Reading on Access Policies](#)

Module Two:

[Forwarding and Data Plane Concepts](#)

[Further Reading on Forwarding and Data Plane](#)

Module Three:

[ACI External Connectivity](#)

[Further Reading on External Connectivity](#)

Module Four:

[Segmentation and Contracts](#)

[Further Reading on Segmentation and Contracts](#)

Module Five:

[ACI Software Upgrade Best Practices](#)

[Further Reading in ACI Upgrade Topics](#)



Table Of Contents

Click on any module item to view content

Module Six:

ACI Fabric Hardening

Further Reading for Fabric Hardening

Module Seven:

Policy Based Redirect Best Practices Part One

Further Reading for PBR Topics

Module Eight:

Policy Based Redirect Best Practices Part Two

Further Reading for PBR Topics

Module Nine:

Network Migration: Legacy to ACI

Further Reading on ACI migration Topics

Module Ten:

ACI Multi-Site Best Practices

Further Reading on ACI Multi-Site Topics



ACI Access Policies

version Sept 2021



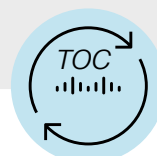
Start Video Replay (Runtime: 1h22m)

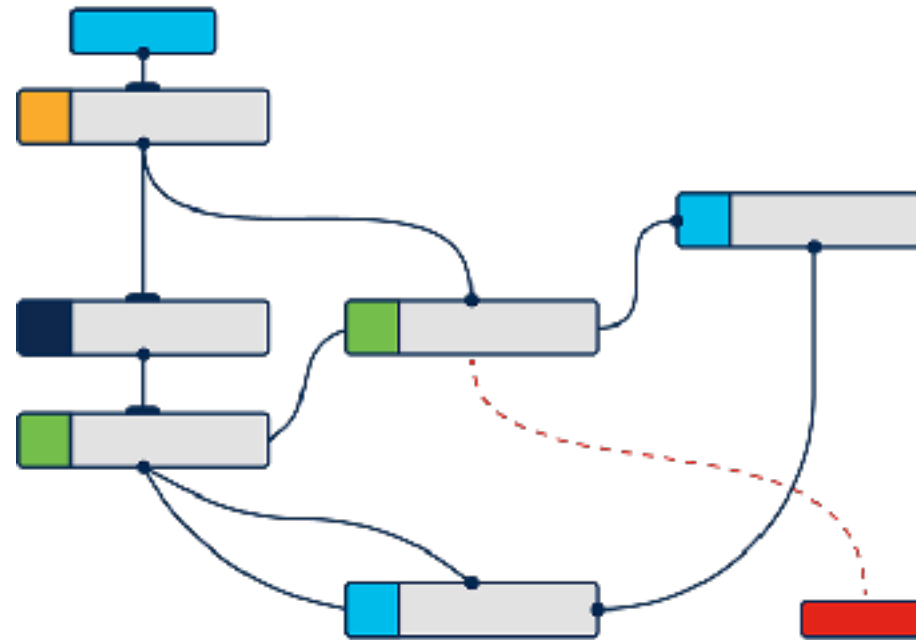
In this video we will review the ins and outs of what we call **Access Policies**. These are the policies you must create whenever you are connecting any type of endpoint (physical or virtual) to the fabric. We will clarify common misconceptions, teach about mistakes to avoid, plus provide some general guidance about how to efficiently configure the necessary objects. We will also demonstrate (where possible) these configurations on a live ACI deployment.

Click on any agenda item below to begin replay at that segment of the video

- Connecting Things to ACI
 - Understanding the AAEP
- Overlapping VLANs
 - Re-using VLANs
- Connecting Servers to ACI
 - NIC Teaming Considerations

- STP and Loop Mitigation





*To acquire knowledge, one must study; but to acquire wisdom, one must observe.
~Marilyn vos Savant*

Access Policies: If you want to know more...

Click on the links below for more details on the topic

- ACI Design Guide (*Complete white paper*)
- *# Access Policies Section*
- Port Tracking Feature (Connecting Servers)
- ACI Virtualization Guide
- VMM and Enhanced LACP
- Design Guidance for Spanning Tree
- Policy Viewer Free App at DC App Center



ACI Forwarding and Data Plane

[Start Video Replay](#)

(Runtime: 1h28m)

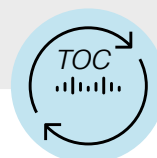
version Jan 2022

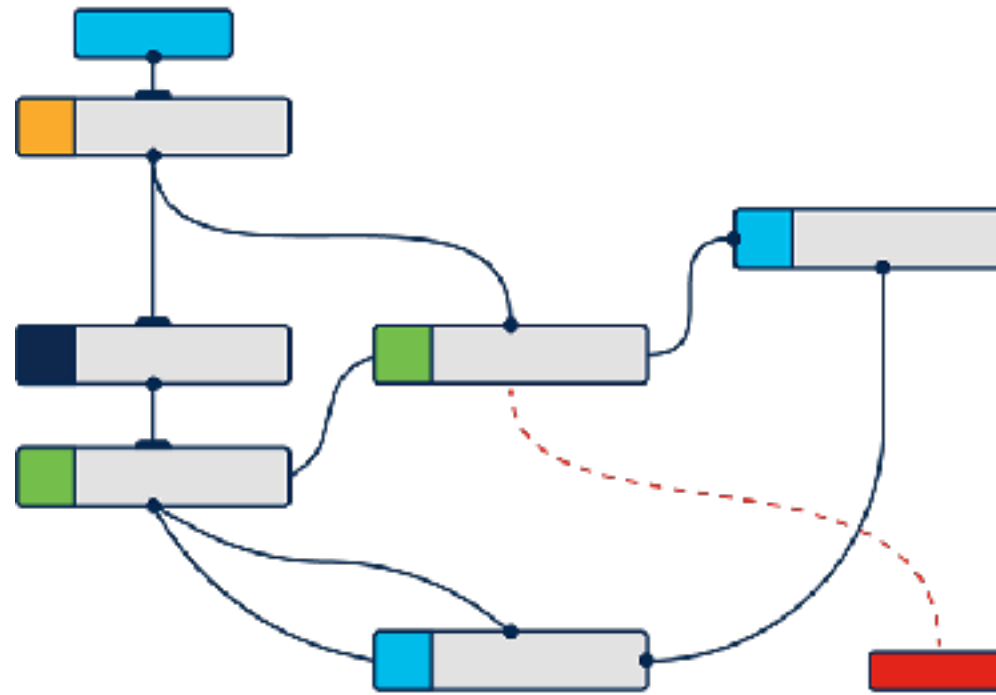


In this video we will review the operation and process of how ACI handles both **Forwarding and Data Planes**. First, we will embark on a review of how ACI processes uses various control plane mechanisms to know where and how to send traffic. We then explain how endpoint learning is handled with some guidance on fine-tuning. We will complete the session with a review and explanation of various Bridge Domain level options. A firm understanding of these concepts is critical to achieving reliable and predication fabric operations.

Click on any agenda item below to begin replay at that segment of the video

- ACI Logical Constructs Recap
- Endpoint Learning Prequel
 - Underlay / Overlay
- Endpoint Learning
 - Endpoint Types
 - Endpoint Fine-Tuning
- Forwarding and Packet Walks
 - Bridge Domain Options Explained
- Additional Helpful Apps
 - *ELAM Assistant*
 - *f-Triage*



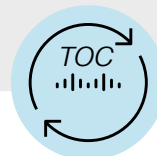


Risk comes from not knowing what you're doing. ~Warren Buffett

Forwarding and Data Plane: If you want to know more...

Click on the links below for more details on the topic

- ACI Endpoint Learning White Paper
- ACI Design Guide White Paper
- CiscoLive BRKACI-3545 - Mastering ACI Forwarding Behavior
- CiscoLive BRKACI-2641 - ACI Troubleshooting Endpoints
- Cisco Press (Free Download):
 - Troubleshooting Cisco Application Centric Infrastructure (2nd Edition)
 - ELAM Assistant Application Download





ACI External Connectivity (L3Out)

version Feb 2022

[Start Video Replay](#)

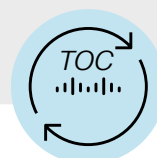
(Runtime: 1h38m)

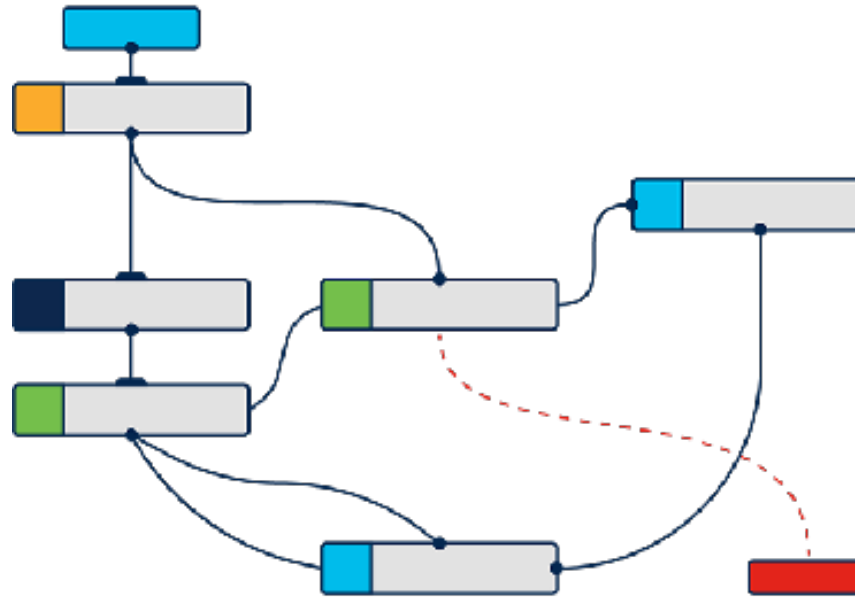


For this video we will focus on what are called **L3 Outs**. They are needed when you want to route traffic in and out of your ACI fabric with the outside world. L3 Outs are also where we configure industry standard routing protocols & options. We will clarify areas that commonly misunderstood and how to avoid the most common mistakes. We will also touch on guidance for transit routing across the fabric as well as designs for sharing L3outs across tenants. We will also demonstrate (where possible) these configurations on a live ACI deployment.

Click on any agenda item below to begin replay at that segment of the video

- Introduction to L3Out
- BD Subnet Advertisement and Methods
 - Method: Under the EPG
 - Method: Export Route Control Subnet
 - Method: Default-export route profile
- External EPG
 - Under the Hood of ExtEPG
- Common Issue: Overlapping Subnets
- Transit Routing
 - Configuring Transit Routing
 - Transit Routing Best Practices
 - Transit Routing and OSPF
- Shared L3Out
- External EPG Flags Summary



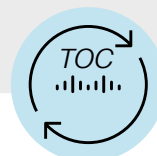


Reading furnishes the mind only with materials of knowledge; it is thinking that makes what we read ours. ~John Locke

External Connectivity: If you want to know more...

Click on the links below for more details on the topic

- [ACI Design Guide White Paper](#)
- [ACI L3Out Config Guide](#)
- [TechNote: Overlapping Subnets on L3Out](#)
- [Cisco ACI L3 Networking Config Guide \(v5.2\)](#)
- [CiscoLive BRCKACI-2642 - Troubleshooting L3Outs](#)

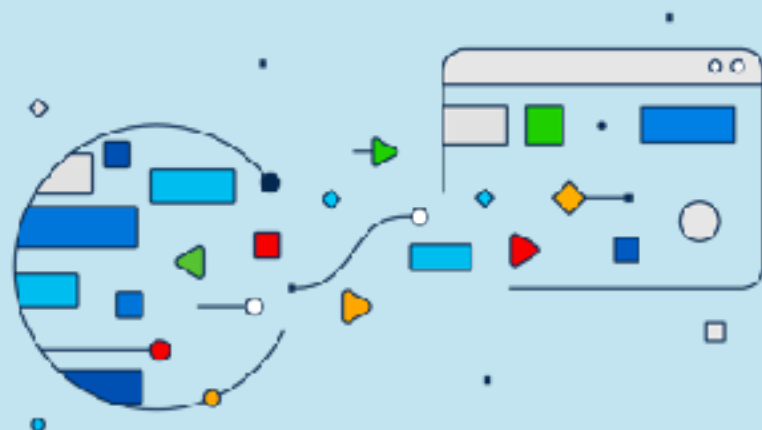


Segmentation and Contracts

version April 2022

[Start Video Replay](#)

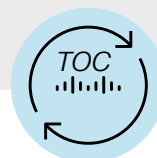
(Runtime: 1h29m)

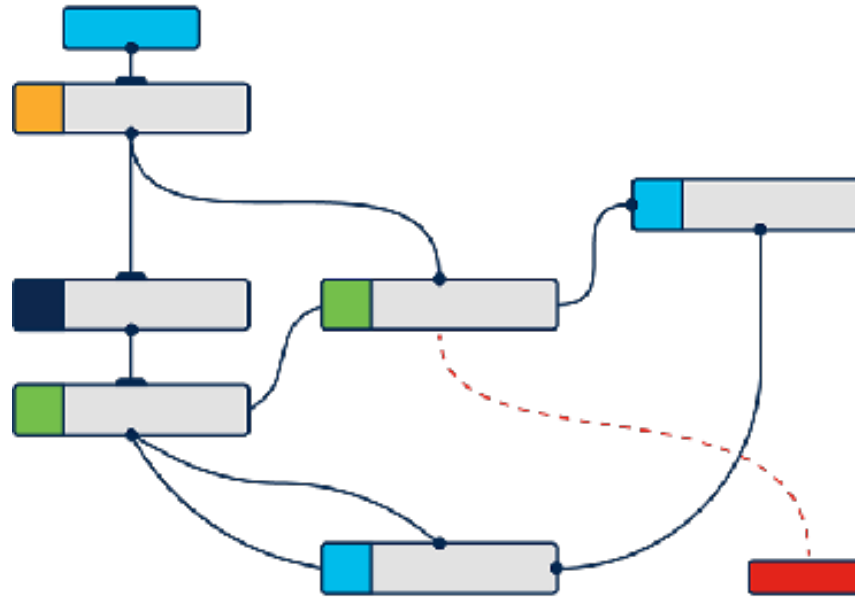


When it comes to Security, ACI is built as a fabric wide stateless firewall. This means security is built-in at a foundational operational level. ACI also takes a cloud based approach in which the default behavior is to deny communication unless it is explicitly permitted. This is where the concepts of **Contracts and Filters** come into being. This video will go in-depth to describe the operational concepts of ACI segmentation, including advice on tuning and optimizing the hardware resources in order to scale to the size of a whole fabric at line rate.

Click on any agenda item below to begin replay at that segment of the video

- Quick Intro on ACI Segmentation
 - Filters
 - Contract Flags / Direction
- Operational Simplifications
 - Preferred Group
 - vzAny (EPG Collection for VRF)
 - EPG Contract Inheritance
- Contracts Verification
- Contract Prioritization
- Contract Scopes
- Scale and TCAM Hardware Optimizations
- Using Policy CAM Analyzer in Nexus Dashboard Insights





It is beyond a doubt that all our knowledge begins with experience. ~Immanuel Kant

Segmentation and Contracts: If you want to know more...

Click on the links below for more details on the topic

- [Cisco ACI Contract Guide](#)
- [TechNote: Verify Contracts and Rules in ACI](#)
- [CiscoLive BRKACI-2301: Practical Applications of Cisco ACI Micro Segmentation](#)





ACI Software Upgrade Best Practices

version Nov 2021

[Start Video Replay](#)

(Runtime: 1h23m)

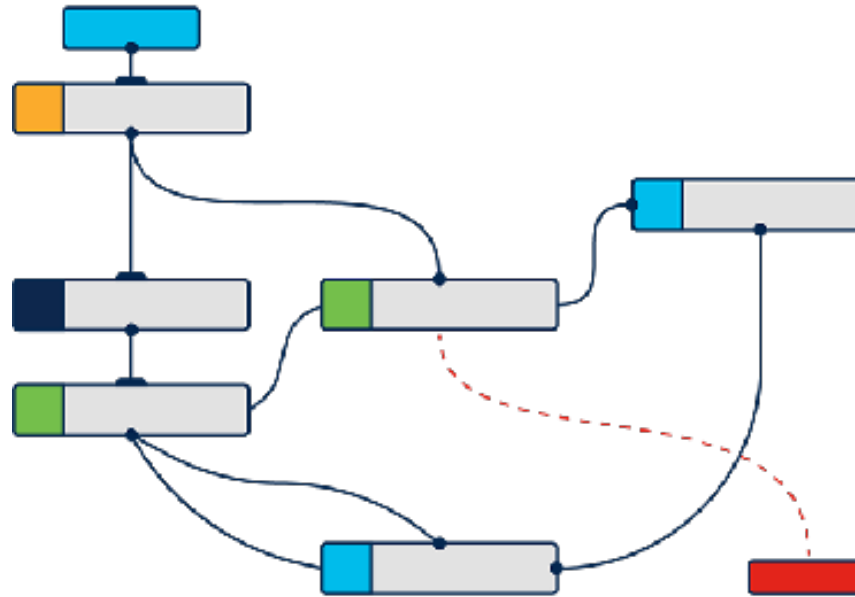


ACI is a sophisticated interworking of leafs and spines, all managed by the APIC controller. Each of these nodes has a software component that requires updating sooner or later. To get the latest features, bug fixes and hardware support we make version recommendations that often trigger an upgrade. In this video we will explore the process of upgrading ACI, gaining an understanding of what happens behind the scenes. We teach how to prep your fabric for a smooth upgrade, and how to avoid those unintended mistakes that can result in longer or failed upgrades.

Click on any agenda item below to begin replay at that segment of the video

- Software Release Guidelines
- Upgrades: Where to Start
- ACI Firmware Upgrade Best Practice Basics
- ACI Firmware Upgrade Flow and Mechanics
- Upgrade Considerations with Multi-X
- Upgrading using the Graceful Option
- ACI Firmware Upgrade Configuration
- ACI Firmware Upgrade Enhancements
 - Upgrade Time Reduction
 - Usability Enhancements
 - Final Tips and Guidance



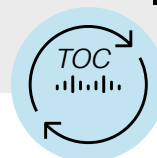


An investment in knowledge pays the best interest. ~Benjamin Franklin

ACI Software Upgrade: If you want to know more...

Click on the links below for more details on the topic

- ACI Upgrade Summary Video Intro
- ACI Upgrade / Downgrade Guide
- ACI Upgrade Handy Checklist
- APIC HW/SW and Compatibility Release Notes
- Bug Note / Guidance on setting IS-IS Policy value
- ACI Pre-upgrade Validation Script (Github)
- TechNote with details on enabling encryption for backups
- Nexus 9000 Switch Release Notes





ACI Fabric Hardening

version Sept 2022

[Start Video Replay](#)

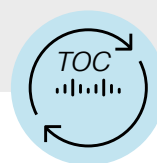
(Runtime: 1h25m)

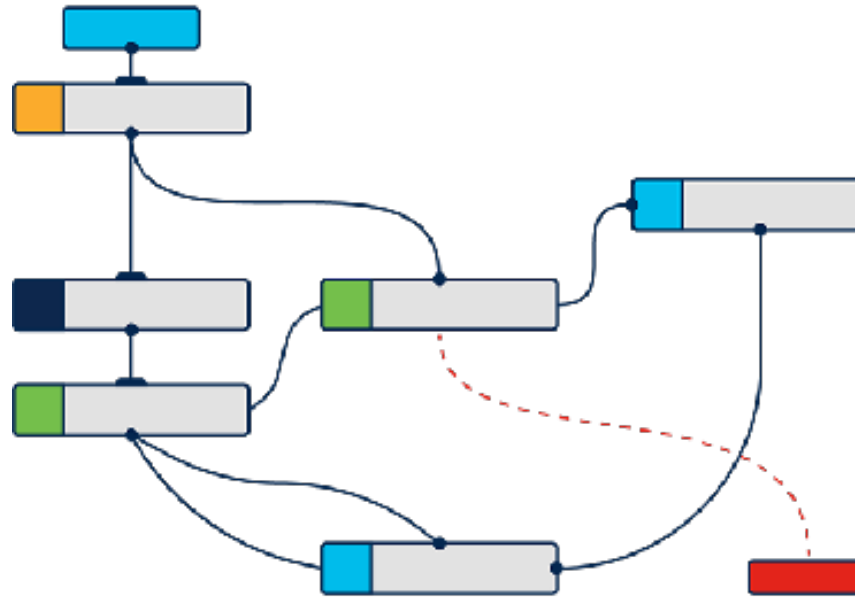


In earlier modules we learned about security and segmentation of endpoint traffic that lives in the tenants of the fabric. It is equally important to also consider a viable security posture for the infrastructure components that make up the fabric itself. In this video we will start with the principles of secure operations. We will then break out to discuss security hardening approaches for each of the Management, Control and Data Planes respectively. As always, we will demonstrate where possible on a live fabric to help you translate these concepts into your own environments.

Click on any agenda item below to begin replay at that segment of the video

- Introduction - Why Hardening is Important
- Principles of Secure Operation
 - Roles Based Access Control (RBAC)
- Securing the Management Plane
 - User Authentication and AAA
 - Disable Unused Services and Protocols
 - Management Contracts
 - CIMC Hardening
- Securing the Control Plane
 - CoPP (Control Plane Policing)
 - Control Plane Authentication
- Securing the Data Plane
 - General Hardening
 - Anti-Spoofing mechanisms
 - Port Security (802.1x) and MACSEC
 - First Hop Security



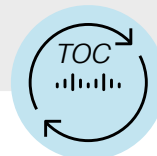


Knowledge is of no value unless you put it into practice. ~Anton Chekhov

ACI Fabric Hardening: If you want to know more...

Click on the links below for more details on the topic

- [Cisco ACI Security Configuration Guide](#)
- [Cisco PSIRT \(Product Security Incident Response Team\)](#)
- [Cisco Security Software Checker](#)
- [Cisco Vulnerability Repository](#)
- [Bug ID Search Tool](#)
- [openVuln API Information](#)





Policy Based Redirect Best Practices (Part 1)

version Jan 2023

[Start Video Replay](#)

(Runtime: 1h28m)



A powerful foundational concept built into ACI is that it is policy driven. This is just a fancy way to say that you have multiple ways to describe to ACI how certain traffic should behave under certain conditions that you define, like re-direct some traffic to a firewall but not other traffic. This is just one example among many possibilities. In this first of a two part video series we will introduce what PBR is and how it works in an ACI fabric. We will present it in the context of common use cases, with configuration guidance, while showing how to avoid common mistakes.

Click on any agenda item below to begin replay at that segment of the video

- Introduction to PBR
 - What is PBR
 - Benefits of PBR
- Use Cases and Deployment Modes
 - East-West Firewall Insertion
 - North-South Firewall Insertion
 - Firewall insertion with NAT
 - Firewall insertion using L1/L2 Option
 - Load Balancer Insertion
 - Symmetric PBR
- PBR Configuration and Demo
- General Best Practices for PBR
- Policy Configuration Best Practices
- PBR Feature Enhancement History





Policy Based Redirect Best Practices (Part 2)

version Feb 2023

[Start Video Replay](#)

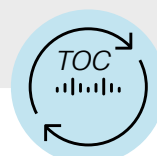
(Runtime: 1h28m)

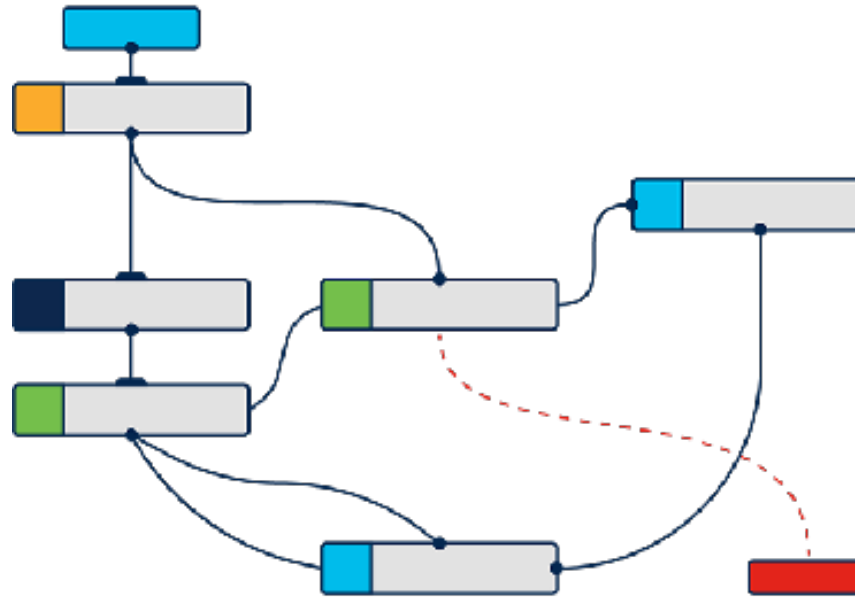


A powerful foundational concept built into ACI is that it is policy driven. This is just a fancy way to say that you have multiple ways to describe to ACI how certain traffic should behave under certain conditions. In this second part of the two part video series, we will go into specific best practices for the various enhancement and options in PBR that cover various use cases. We will talk about using PBR with load balancers, Layer 1 and Layer 2 re-direct options, and using PBR with L3outs. We will close with some guidance around using PBR in a Multi-Pod environment.

Click on any agenda item below to begin replay at that segment of the video

- A quick recap of Part One...
- Demo: Inserting F5 one-arm load balancer with keepalives / health checks
- Continuing Best Practices Topics
 - Using Symmetric PBR
 - PBR with L1/L2 re-direct options
- PBR Destinations in an L3Out
- Best Practices PBR with Multi-Pod



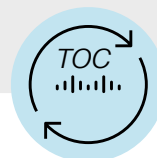


Knowledge speaks, but wisdom listens. ~Jimi Hendrix

Policy Based Redirect: If you want to know more...

Click on the links below for more details on the topic

- White Paper: Service Graph Design
- White Paper: Policy Based Redirect Design
- White Paper: ACI Contract Design
- White Paper: Multi-Pod Service Node Integration
- White Paper: Multi-Site Service Node Integration
- CiscoLive BRKDCN-3610: ACI L4-L7 Policy-Based Redirect (PBR) Deep Dive and Tips

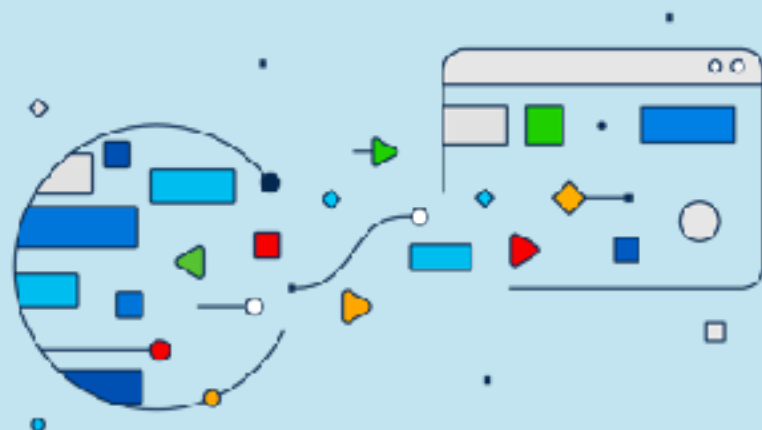


Migrating from Legacy to ACI

version May 2023

[Start Video Replay](#)

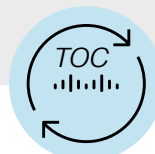
(Runtime: 1h29m)

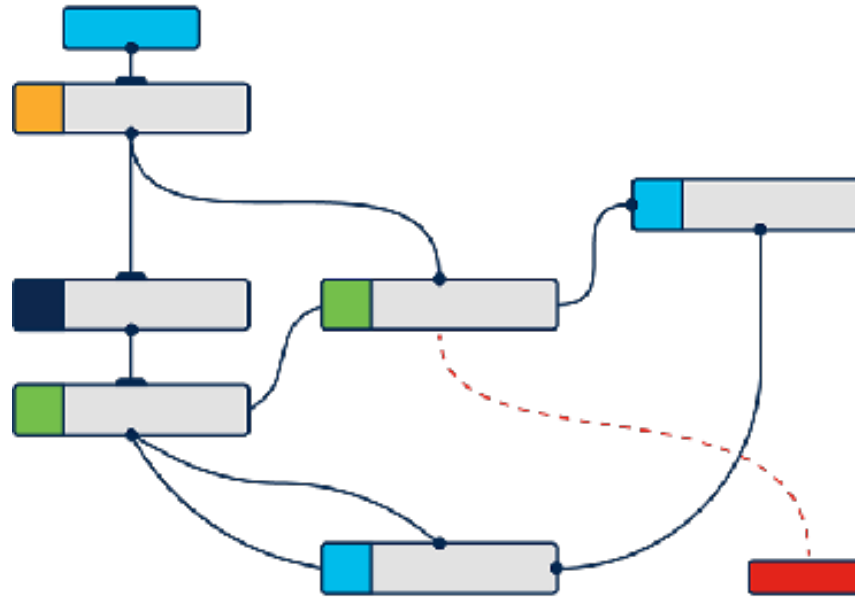


Nearly every customer coming to ACI starts with some sort of existing classic DC infrastructure. It could be from Cisco, or from other vendors. In any case, such customers ask early on about how a migration from existing network to ACI can be done. In this video we talk about securely extending your legacy into ACI, give some design guidance on ways to plan a migration, things to keep track of during the migration of workloads with an eye on minimizing interruption. We will include guidance on how to avoid common mistakes that show up in migration projects.

Click on any agenda item below to begin replay at that segment of the video

- Migration Strategies
- Resource Allocation
- Extending Layer 2 into ACI
 - ACI & Spanning-Tree (Last Resort Guide)
- Extending Layer 3 into ACI
- Workload Migration
 - Gateway Migration
- Network Services Migration
- Multi-X Migration





Life is a traveling to the edge of knowledge, then a leap taken. ~ D.H. Lawrence

ACI Migration: If you want to know more...

Click on the links below for more details on the topic

- White Paper: Migrating Existing Networks to Cisco ACI
- TechNote: ACI Operation with L2 Switches and Spanning Tree Link Types
- APIC Layer 2 Networking Configuration Guide, Release 6.0(x)





Multi-Site Best Practices

version Oct 2023

[Start Video Replay](#)

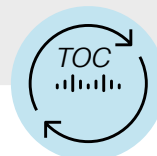
(Runtime: 1h27m)

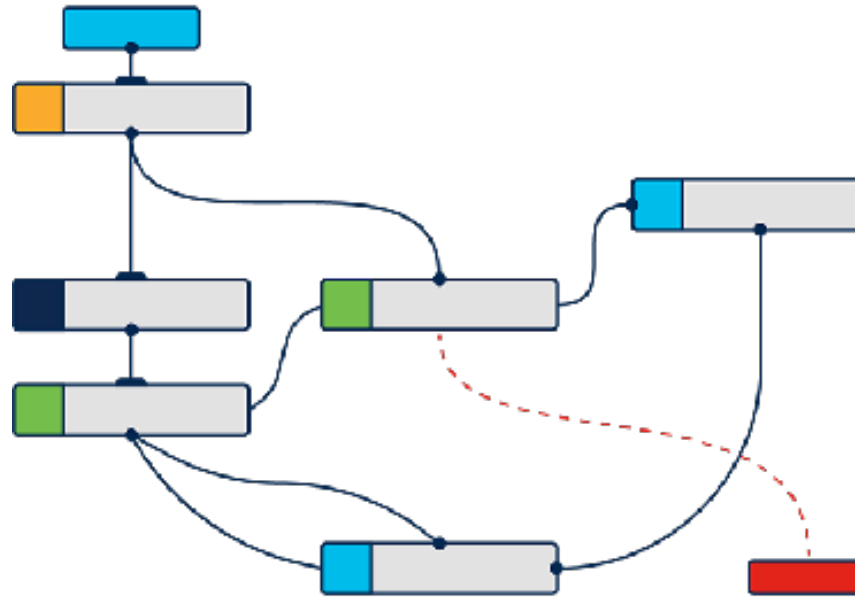


When it comes to expanding the data center fabrics beyond the boundaries of one site, ACI Multi-Site has proven to be a very popular choice. Given the importance of workloads that live, move or are stretched across sites, it becomes important to build from a solid design and implementation plan. In this video we will discuss how to best deploy Nexus Dashboard Orchestrator (including version recommendations), before we move to guidance for creating NDO schemas and templates which are the policy building blocks for ACI Multi-Site operations. We will also include guidance on site to site connectivity, L3outs, and L4-L7 service insertion.

Click on any agenda item below to begin replay at that segment of the video

- Intro to Multi-Site Concepts
- NDO Deployment Best Practices
- NDO Recommended Release
- Schemas and Templates
- Operational Best Practices
- Infrastructure Deployment Best Practices
- Overlay Configuration Best Practices
- External Connectivity (L3Outs)
- L4-L7 Services Insertion



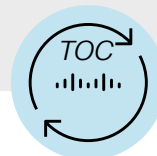


Well done is better than well said. ~Benjamin Franklin

Multi-Site Best Practices: If you want to know more...

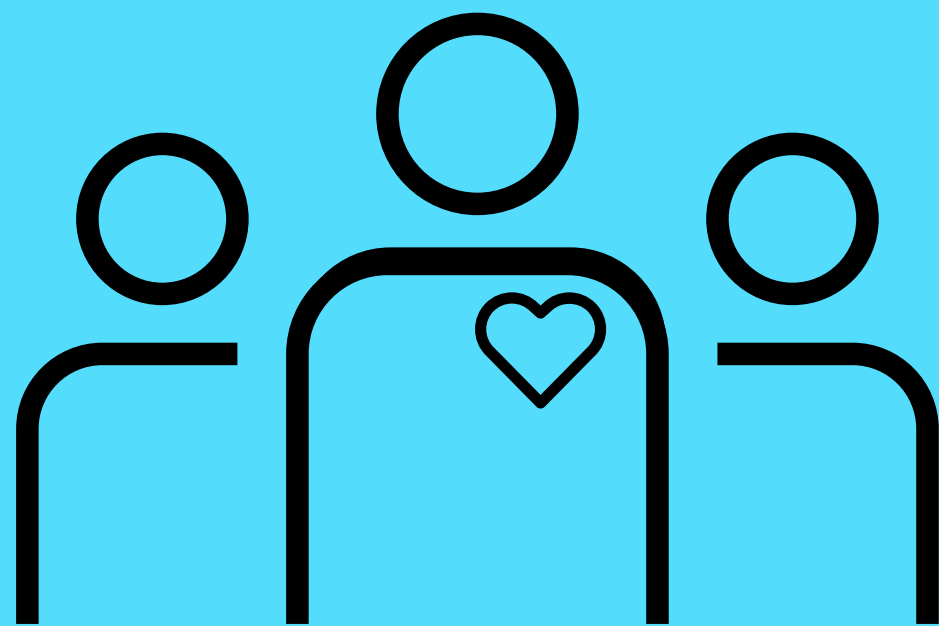
Click on the links below for more details on the topic

- White Paper: ACI Multi-Site Architecture
- White Paper: ACI Multi-Site and L4-L7 Services
- Deployment Guide: NDO 4.2(x)
- Configuration Guide: NDO 4.2(x)
- CiscoLive BRKDCN-2980: ACI Multi-Site Architecture and Deployment
- CiscoLive BRKDCN-2919: How to Setup an ACI Multi-Site with single Pod and Multi-Pod





Final Thoughts and a Thank You



We hope that in the content of this document you have managed to gain some useful knowledge and wisdom about operating your ACI fabric. Getting the most out of your investment is of utmost importance to us. Continue the journey and stay tuned for future best practices content as we evolve alongside you.

<https://www.cisco.com/go/aci>