What's New in SD-Access?

Mahesh Nagireddy
Technical Marketing Engineering, Technical Leader
CCIE R&S

Session ID: BRKENS-2568

Cisco Webex App

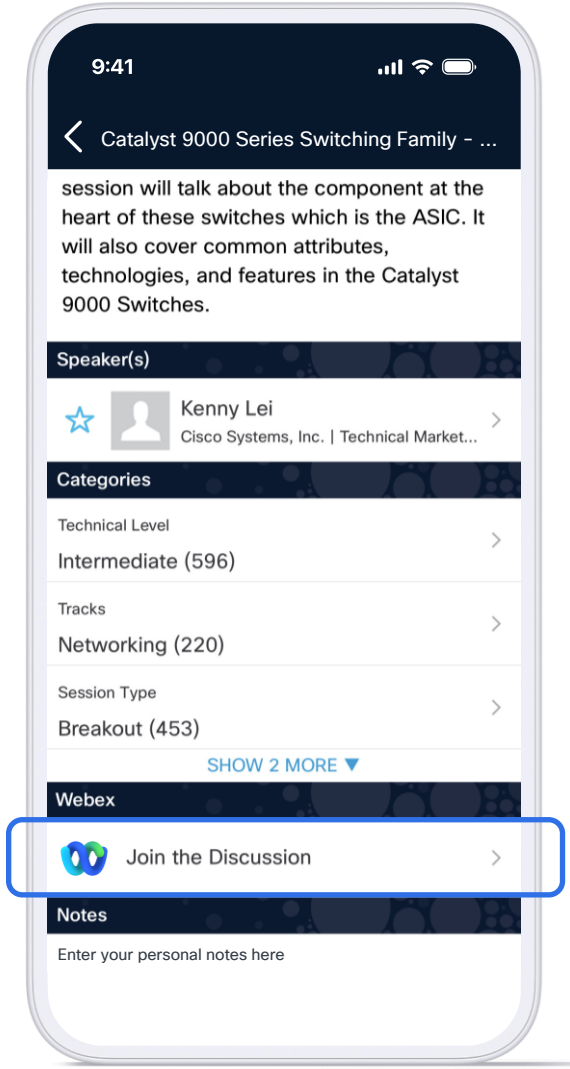
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKENS-2568**

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Lan Automation – OSPF Multi Area

02 LISP Pub/Sub Migration

03 Security Service Insertion

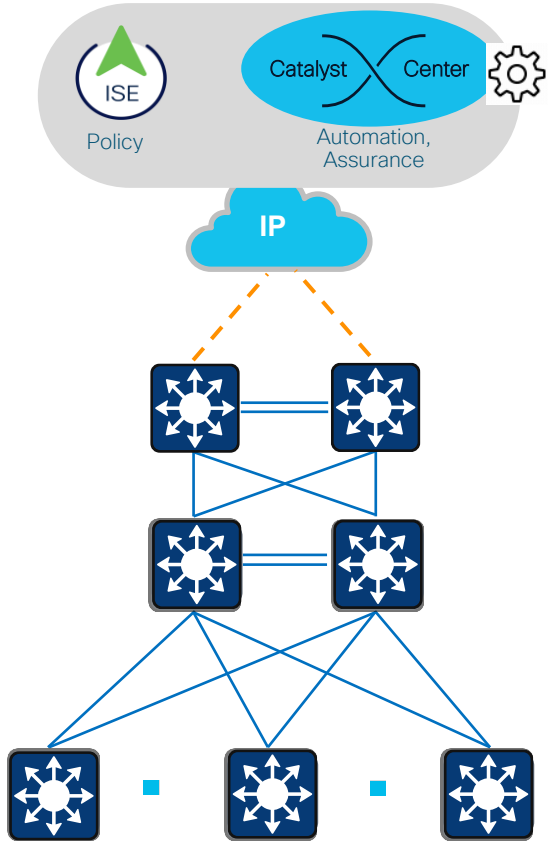
04 SD-Access 2.3.7.x New Features

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

OSPF Multi Area LAN Automation

What is Lan Automation



Lan Automation

- Simplifies network operations
- Frees IT staff from time-consuming, repetitive network configuration tasks
- Creates a standard, error-free underlay network

Lan Automation Benefits

- Zero-touch provisioning
- End-to-end topology
- Resilience
- Security
- Compliance

© 2025 Cisco and/or its affiliates. All rights reserved.

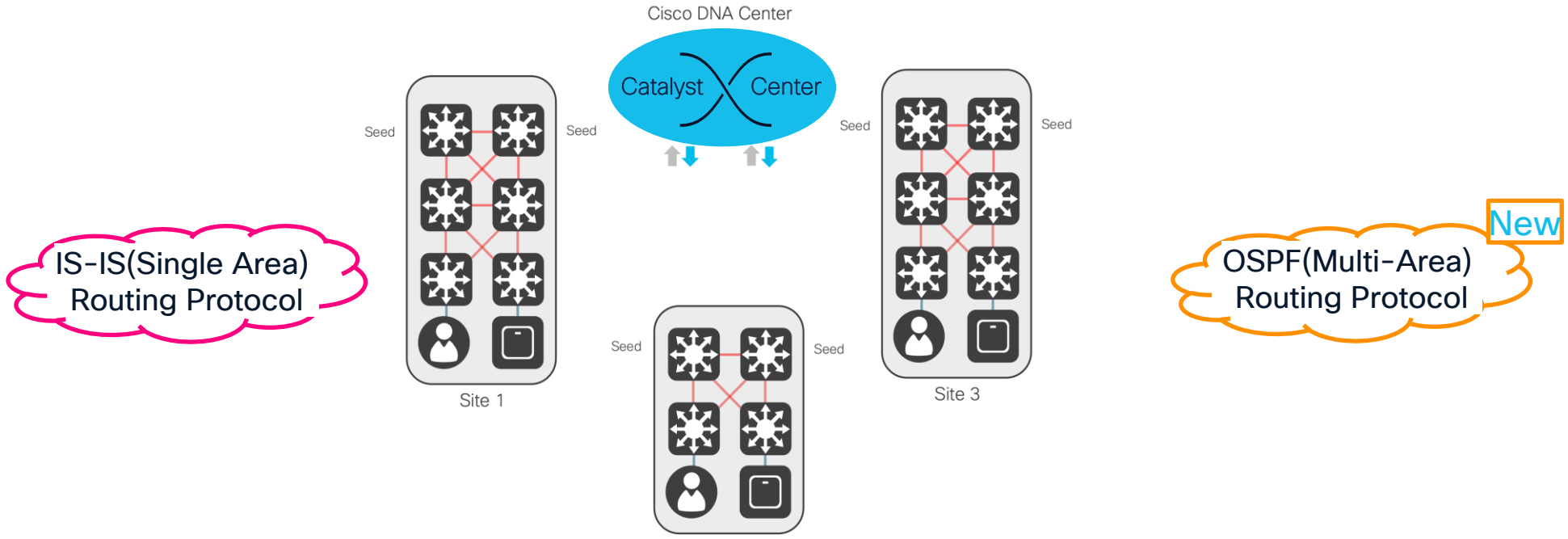
Cisco Catalyst Center
Device Onboarding options

Manual | Semi-Automated Underlay

Device-by-Device onboarding and configuration either manually or through Cisco Plug-and-Play.

Automated Underlay(Lan Automation)

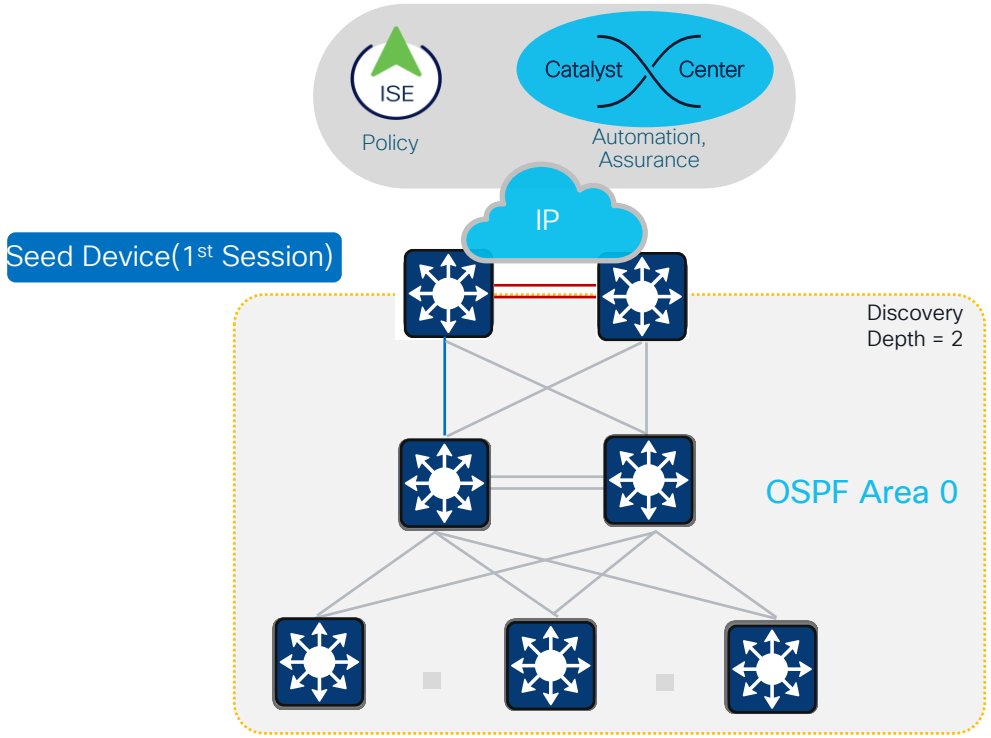
Turnkey solution to onboard multiple switches with image management and best-practices configuration.
Underlay multicast to optimize overlay subnet multicast/broadcast distribution



© 2025 Cisco and/or its affiliates. All rights reserved.

Lan Automation OSPF

Multi-Area OSPF



© 2025 Cisco and/or its affiliates. All rights reserved.

Lan Automation OSPF

Key Chain support

- Key String optional
- Key chain name LAN-AUTO-<variable generated sequential id>
- New Key String won't get pushed if one already exists
- Configs

```
key chain LAN-AUTO-1
 key 1
  key-string 7 070B2F4D4D
  cryptographic-algorithm hmac-sha-512
```

© 2025 Cisco and/or its affiliates. All rights reserved.

Lan Automation Guidelines

- IGP selection:

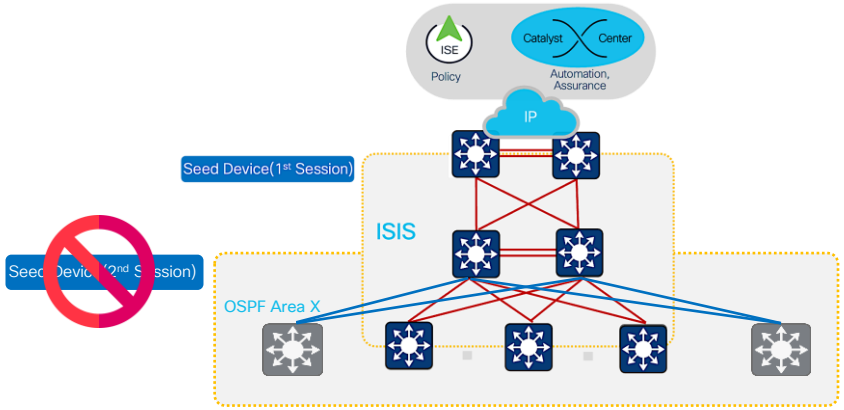
IS-IS(Single Area) Routing Protocol

OR

New

OSPF(Multi-Area) Routing Protocol

- ISIS + OSPF Lan Automation within same site?



- Lan Automated ISIS to OSPF migration?

  No committed Plans

© 2025 Cisco and/or its affiliates. All rights reserved.

DEMO

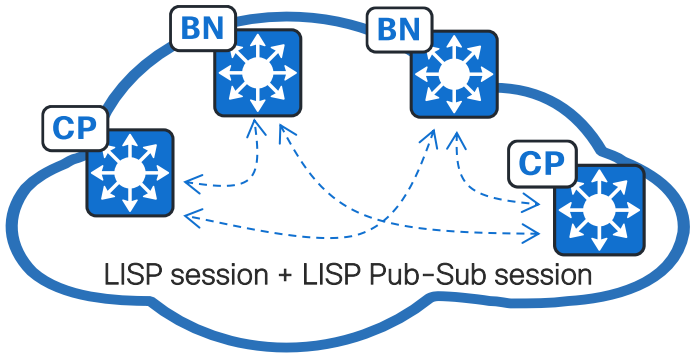
© 2025 Cisco and/or its affiliates. All rights reserved.

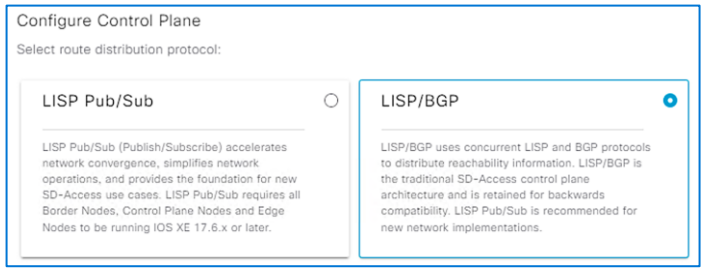
LISP Pub/Sub Migration

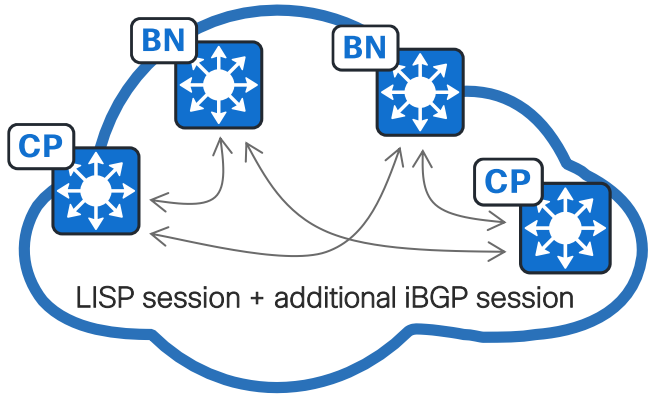
Cisco SD-Access overlay

Starting
Catalyst Center: 2.2.3.x
IOS-XE: ≥ 17.6.2

Fabric control plane enhancements







LISP Pub/Sub

- Publisher-Subscriber model provides LISP Instance-ID table subscription from CP, TCP to Border nodes.
- Faster convergence within fabric site (N-S traffic) and across SD-Access transit.
- LISP Pub/Sub provides backbone for fabric innovations such as **Dynamic-Default Border, Extranet, Active-Backup Internet (with SD–Transit) and more..**
- **4 TCP(Transit Control Plane) Node support**

LISP / BGP

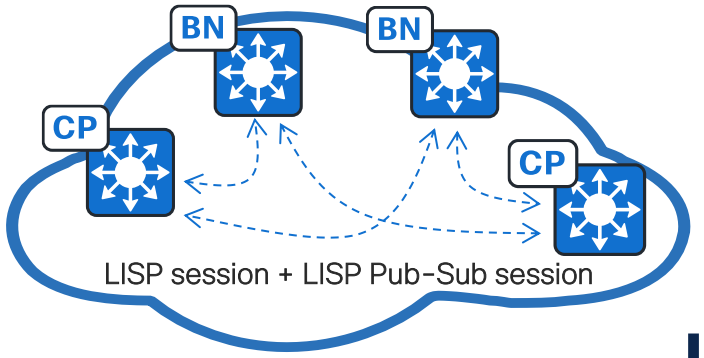
- iBGP session between B – CP and B – TCP node to share prefixes.
- Convergence overhead with additional protocol, redistribution and additional lookups
- Troubleshooting complexity with 2 Control-plane protocols
- Only supported Architecture with SD-WAN Integrated solution
- **Only 2 TCP Node support**

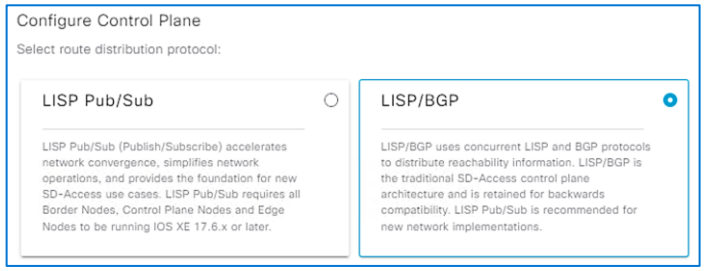
© 2025 Cisco and/or its affiliates. All rights reserved.

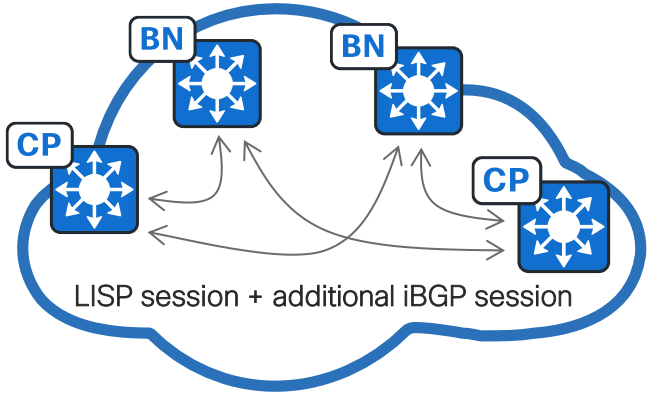
Cisco SD-Access overlay

Starting
Catalyst Center: 2.2.3.x
IOS-XE: ≥ 17.6.2

Fabric control plane enhancements





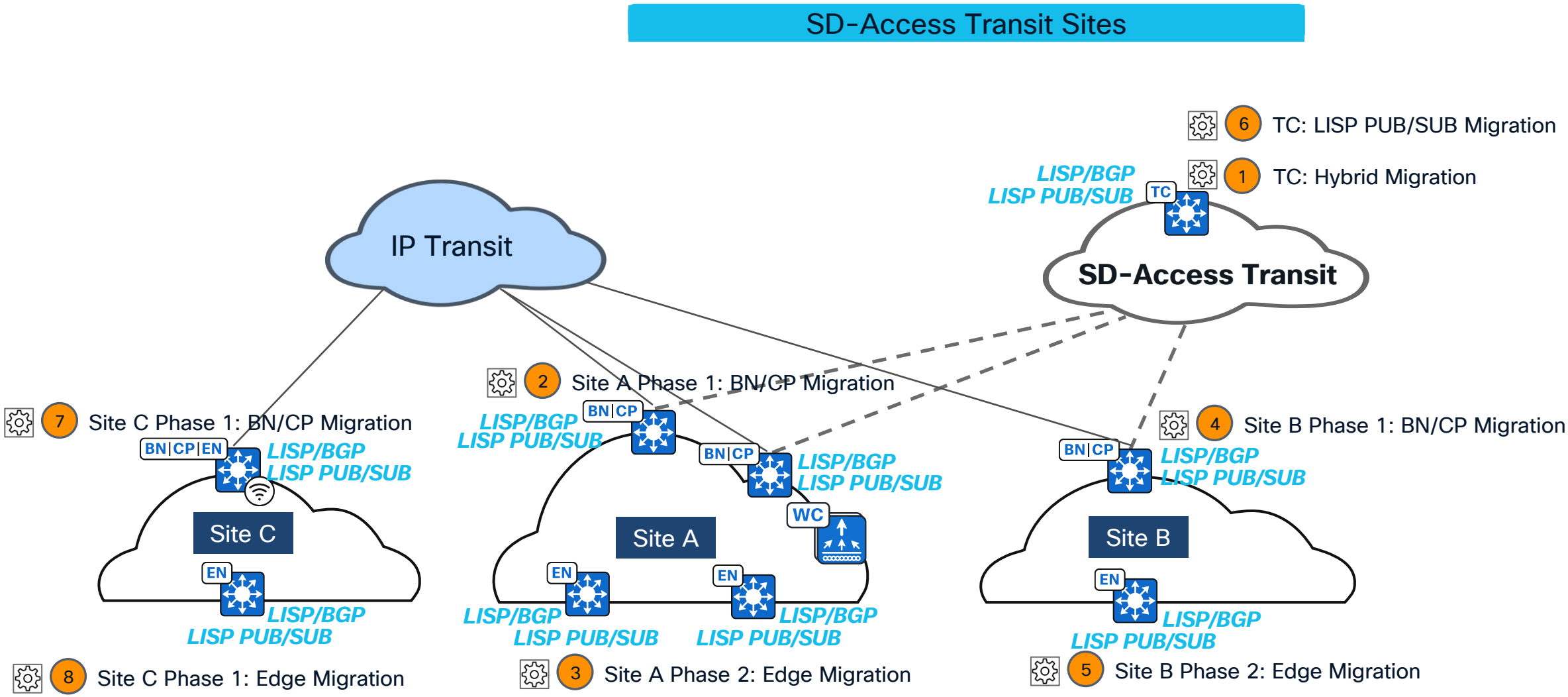


LISP Pub/Sub Benefits

- **Remove dependency on BGP**
- Simplified Border Routing Designs
- **Faster Border Convergence due to faster mapping change updates**
- **Traffic Path Optimization with Dynamic Default Border**
- **Backup Internet Option**
- **Automated route leaking using LISP Extranet**

© 2025 Cisco and/or its affiliates. All rights reserved.

LISP Pub/Sub Migration



© 2025 Cisco and/or its affiliates. All rights reserved.

DEMO

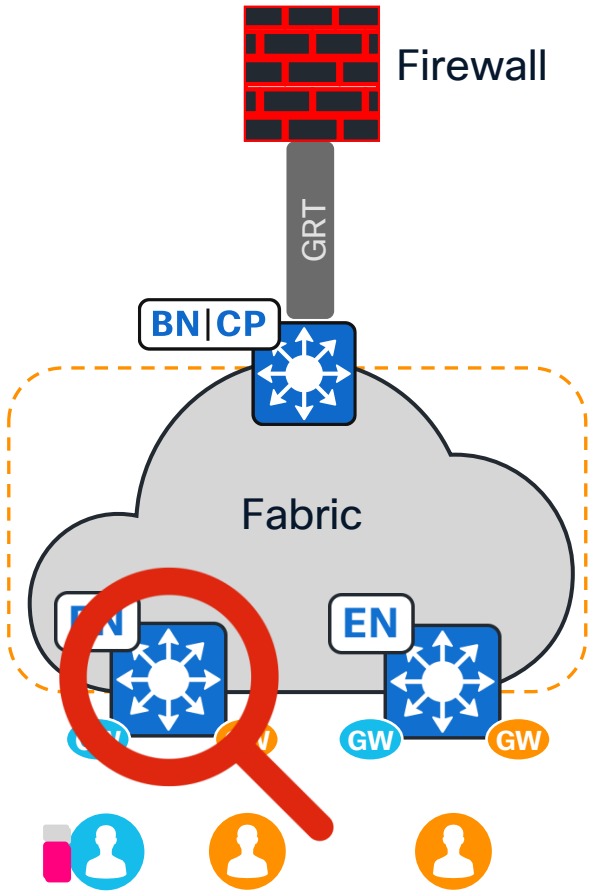
© 2025 Cisco and/or its affiliates. All rights reserved.

Security Service Insertion (SSI)

CISCO Live !

Why Security Service Insertion?

Problem Statement



Primary Objective

- Inspect traffic across untrusted Segments for compliance reasons
- Selective traffic steering for stateful inspection

Method

Rudimentary techniques using hop-by-hop switching/routing changes

Challenges

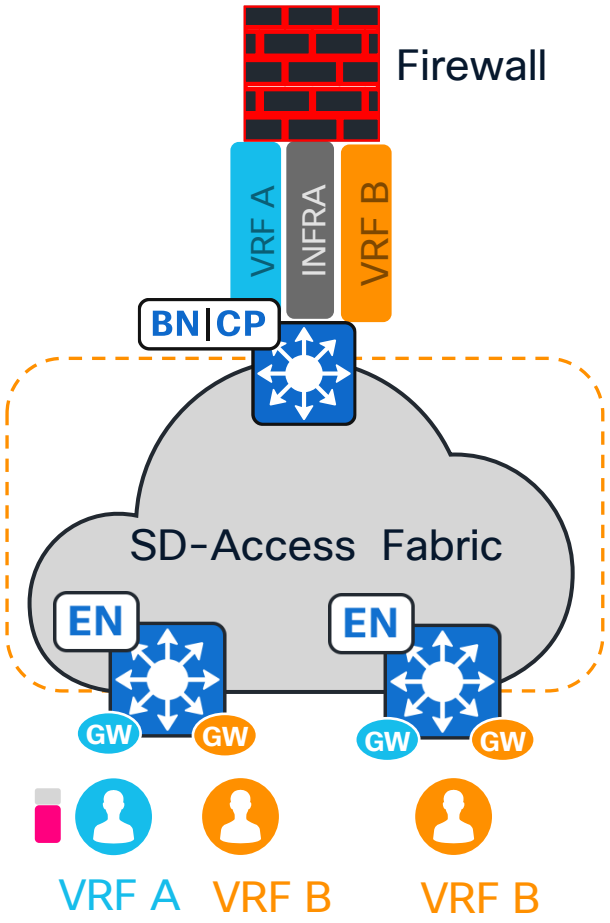
- Static Deployments
- Limited Scalability
- Management Challenges
- Policy based on IP/Subnet/Vlans

© 2025 Cisco and/or its affiliates. All rights reserved.

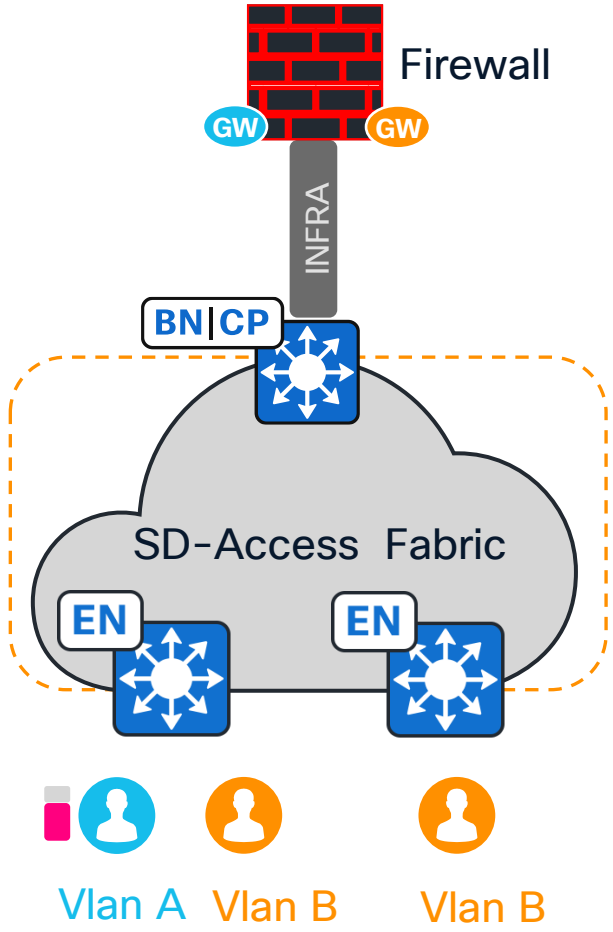
BRKENS-2568

SD-Access Options

Option 1
L3 Overlay



Option 2
L2 Overlay / GWOF



GWOF – Gateway outside Fabric

© 2025 Cisco and/or its affiliates. All rights reserved.

Security Service Insertion(SSI)

Cisco SD-Access LISP Fabric

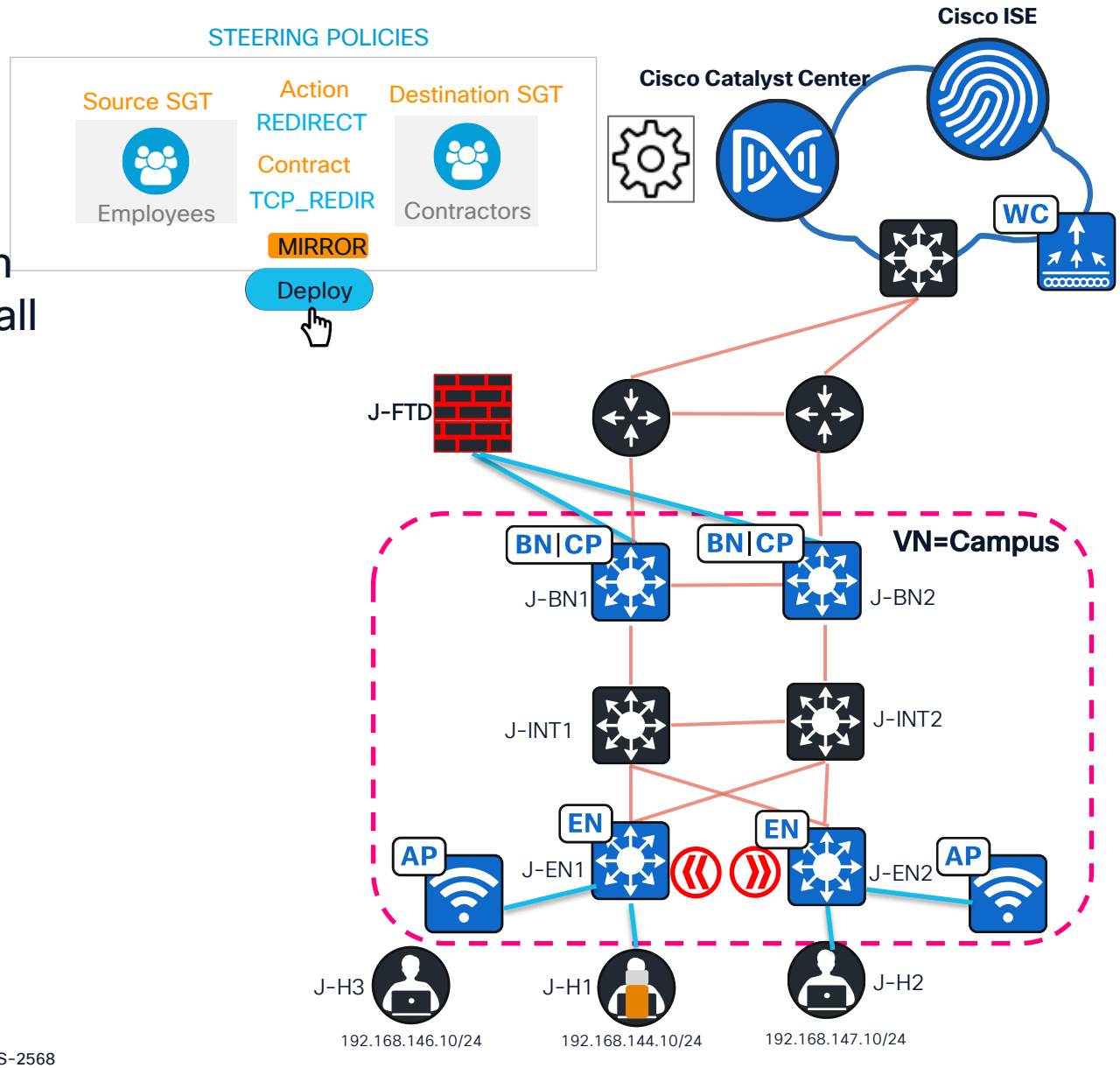
Benefits with SSI

- Fully Orchestrated Workflow on Catalyst Center
- Policy-driven(SGT/DGT based) traffic redirection
- Limit the amount of traffic processed by a Firewall for lower Capex and Opex
- Centralized Firewall Policy

Catalyst Center Workflow Steps

Combined Automation + Policy Workflow

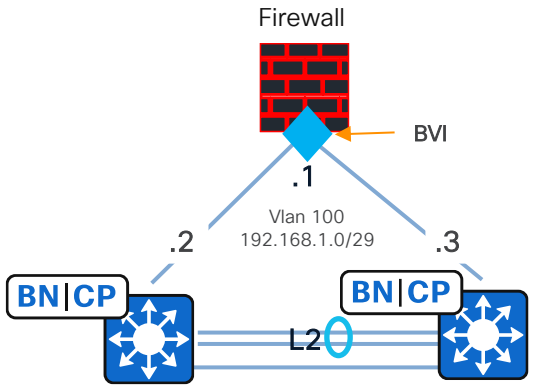
- Run Pre-Check
- Select a Fabric Site
- Map Firewall(s) IPs
- Configure Policy
- Deploy



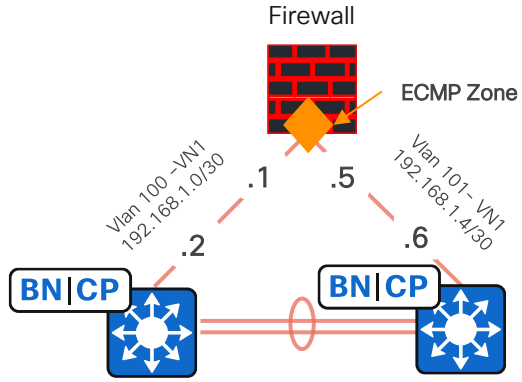
© 2025 Cisco and/or its affiliates. All rights reserved.

Standalone and Redundant FW Topologies

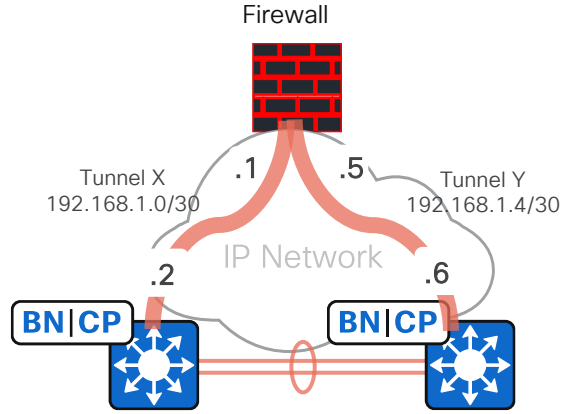
L2 with HSRP & BVI

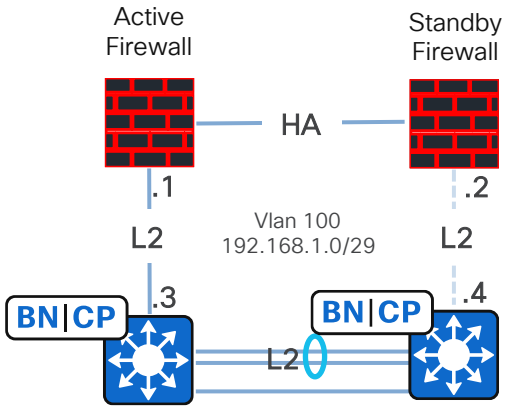


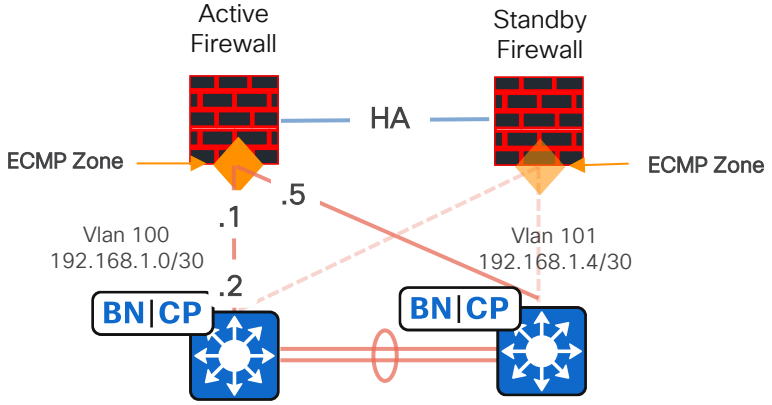
L3 with ECMP



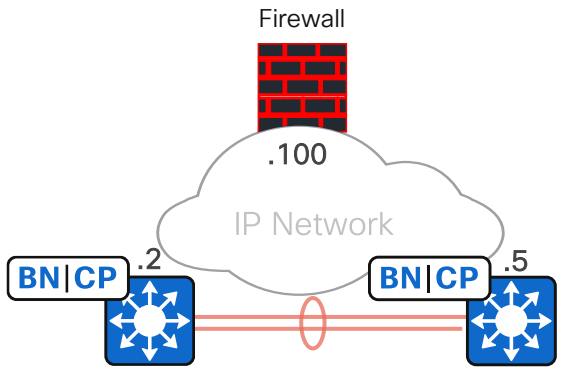
GRE Tunnel







IP Network



© 2025 Cisco and/or its affiliates. All rights reserved.

Security Service Insertion
HW & SW requirements

EFT : 3.1.3- Jun 2025
LA: 3.2.1 – Nov 2025
GA : 3.2.x – CY 2026

Hardware & Software Requirements

- **Cisco Catalyst Center** : DN2 & DN3 Appliance and 3.1.3 or Later releases
- **Cisco ISE :** 3.4 Patch 2 and Later releases
- **Catalyst 9000 series switches(Except 9200,9500X as edge and C9600 Sup2) :** IOS XE 17.17.1 and later releases
- **Firewall:** Cisco FTD & 3rd Party

Prerequisites

- Cisco Catalyst Center and Cisco ISE Integration
- Cisco SD-Access LISP PUB/SUB Control-Plane architecture
- Cisco SD-Access LISP Fabric with Micro-Segmentation enabled

Phase 1 Support

- Wired and Wireless support
- Intra VN with Inter Subnet support
- E-W and N-S Traffic
- Inter SGT support only
- SGT/DGT based steering
- Direct or Indirect Firewall
- Cisco and 3rd Party Firewall support
- Firewall in Routed mode only

© 2025 Cisco and/or its affiliates. All rights reserved.

Phase 1 Scale

Security Service Insertion
Scalability

Feature	DN-SW-APL / DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
Fabric Sites/SSI sites	500	1000/500	2000/500
Virtual Networks	64 / site 4000/Cluster	128 / site 4000/Cluster	256 / site 4000/Cluster
IP Pools	100 / Site 50K/Cluster	300 / site 75K/Cluster	1000 / site 100K/Cluster
All Roles in Fabric	500/site 2,000/Cluster	600/site 4,000/Cluster	1200/site 8,000/Cluster
Control Plane nodes	6	6	6
Border Nodes	4	4	4
Steering Contracts	500	500	500
SGT/DGT Policies	25,000 / Cluster	25,000 / Cluster	25,000 / Cluster

Security Group Tags (SGT)
Destination Group Tags (DGT)

© 2025 Cisco and/or its affiliates. All rights reserved.

DEMO

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco SD-Access 2.3.7.x New Features

Cisco SD-Access 2.3.7.4/5/6/9 Updates

- SD-Access Compatibility Check
- LAN Automation Enhancements
- Telemetry Status in SD-Access Health Dashboard
- Enforcement of Group-Based Policy for VNs
- Cisco SD-Access API Enhancements
- RMA Enhancements in Cisco SD-Access
- Unsupported SD-Access Configuration Detection on Fabric Devices
- Device Refresh of Switch/AP
- In-Service Software Upgrade (ISSU) Support for Catalyst 9400 Fabric Edge Nodes and Catalyst 9800-CL Fabric Wireless Controllers
- Update Fabric Site for Fabric Events

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

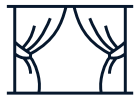
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

CISCO