CISCO The bridge to possible

Cisco SD-Access – Connecting Multiple Sites in a Single Fabric Domain

Scott Hodgdon, Technical Marketing Engineer technical Leader

CISCO Live!

BRKENS-2815

Cisco Webex App

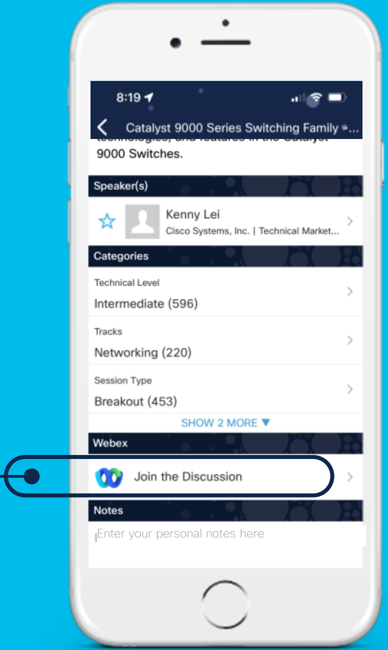
Questions?

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
until February 24, 2023.**



8:19

Catalyst 9000 Series Switching Family •...

9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Who is Scott ?

Personal

- Based in Raleigh, NC (US)
- 22-year-old daughter in university (she's smarter than I)

Career

- 22 years as a Technical Marketing Engineer
- 13 Years focused on just Catalyst 6K Family
- 15+ years as a Cisco Live Speaker
- 10 years as Cisco Live Session Group Manager for US and EMEA
- 2 Years as a Cisco Partner SE
- 2 Years Lead Network Engineer for 15-site Health Care network in North Carolina
- No formal technology schooling … I have a Business Degree with a Finance Concentration

Current Focus

- Cisco SDA Network Design and Partner Enablement

Agenda

Cisco SD-Access Basic Concepts

Cisco SD-Access Transit Types

- IP as Transit/Peer Network
- SD-Access as Transit

Cisco SD-Access Policy across Distributed Campus

SD-Access Transit LISP Pub/Sub

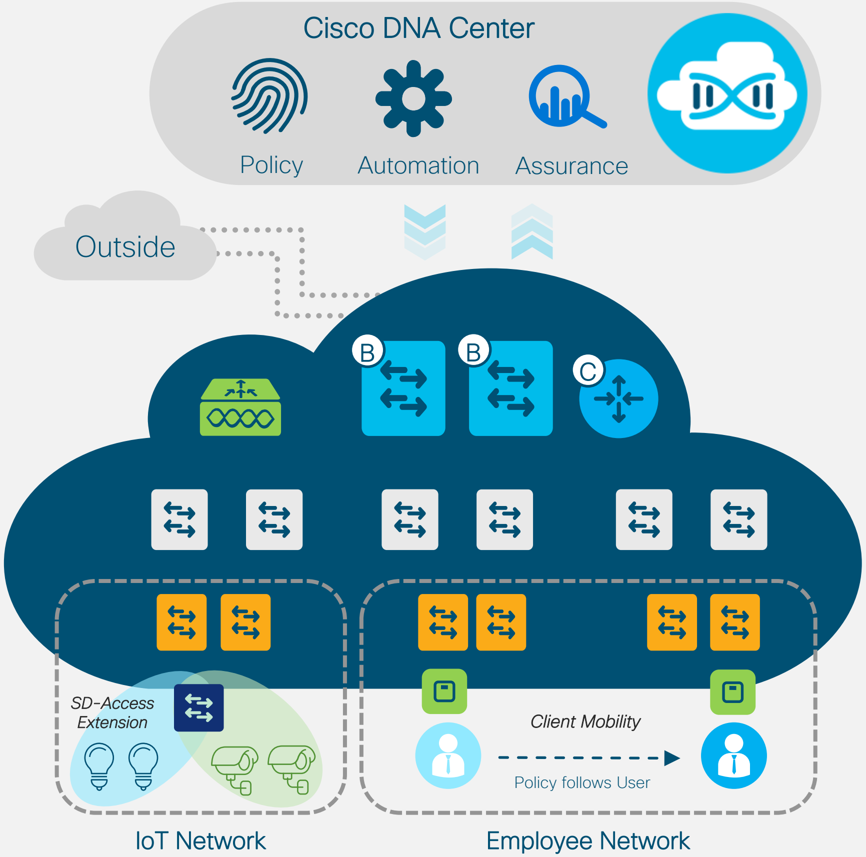
- Registration
- Packet Walk
- Remote Internet
- Backup Internet

SD-Access Basic Concepts

RECAP

Cisco Software Defined Access

The Foundation for Cisco's Intent Based Network



One Automated Network Fabric

Single fabric for Wired and Wireless with full automation

Identity-Based Policy and Segmentation

Policy definition decoupled from VLAN and IP address

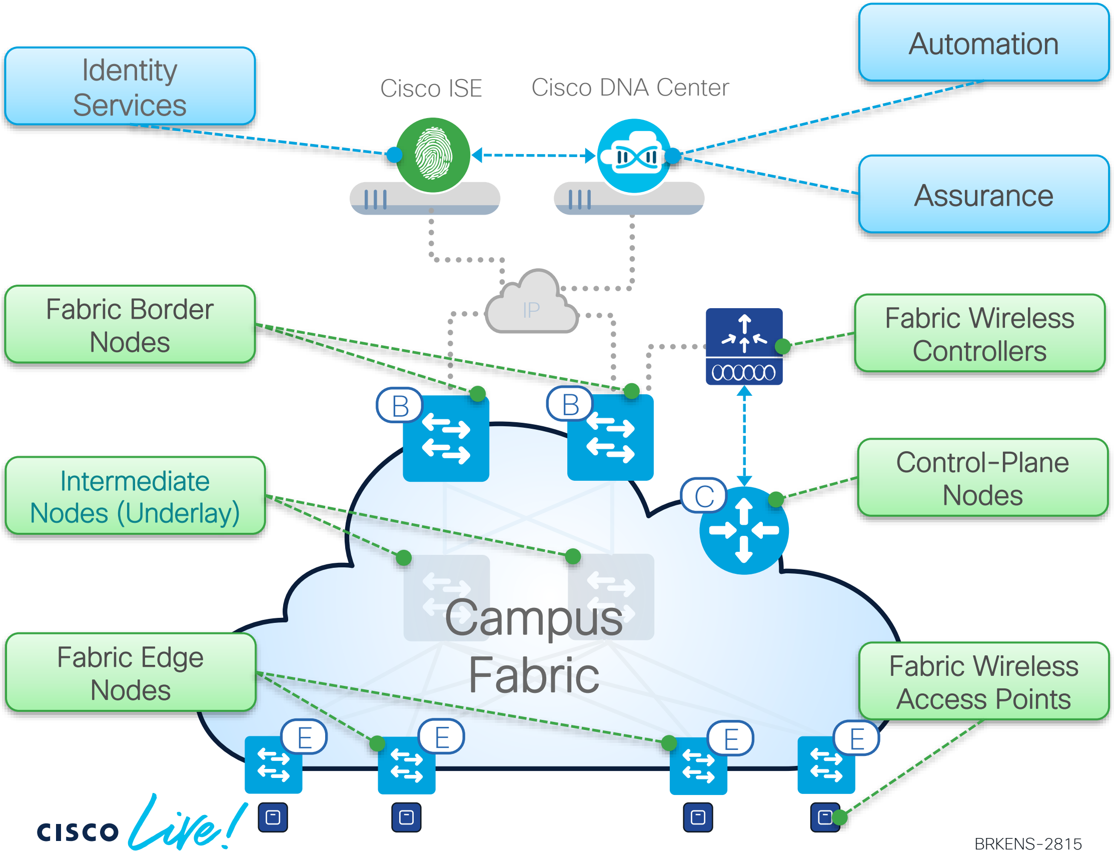
AI-Driven Insights and Telemetry

Analytics and visibility into User and Application experience

RECAP

Cisco SD-Access

Fabric Roles and Terminology



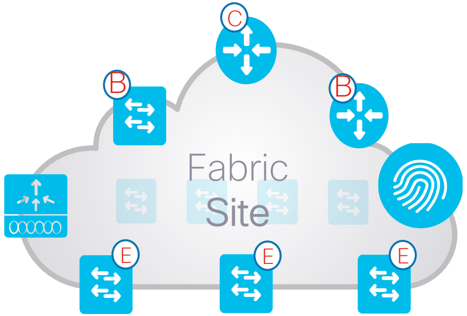
- Network Automation – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- Network Assurance – Data Collectors analyze Endpoint to Application flows and monitor fabric network status
- Identity Services – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition

- Control-Plane Nodes – Map System that manages Endpoint to Device relationships
- Fabric Border Nodes – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- Fabric Edge Nodes – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- Fabric Wireless Controller – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

Fabric Sites:
Single or Multiple

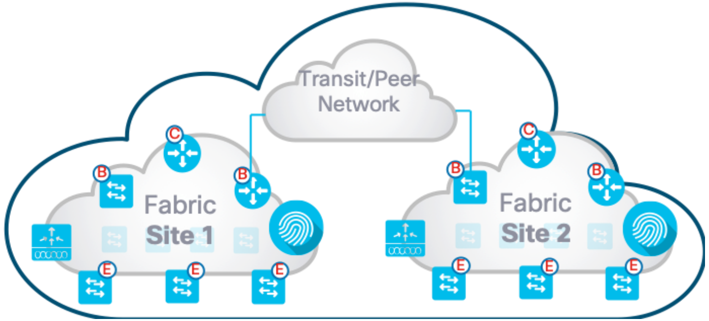
Fabric Sites : Single vs Multiple

Single Site



- Includes CP,B,FE, Fabric WLC and ISE PSN
- Benefits
  - Scalability
  - Resiliency
  - Survivability
- Fabric Site may cover a single physical location, multiple locations, or just a subset of a location

Multiple Sites



- Includes One or more Fabric sites with Transit network (IP or SD-Access)
- Managed by Single DNAC cluster
- End to End Segmentation between Fabric Sites needs to be considered

Cisco DNAC System Scale

Rel:2.3.3.x

Parameters	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
No of Devices (Switch/Router/WLC)	1000	2000	5000 / 10,000*
No of Access Points	4000	6000	12000
No of Endpoints (Concurrent)	25,000	40,000	100,000 / 300,000*
No of Endpoints (Transient)	75,000	120,000	250,000 / 750,000*
No of endpoints – wired: wireless ratio	Any	Any	Any
No of Fabric Sites	500	1000	2000
No of Virtual Networks per Fabric Site	64/Site	64/site	256/site
No of Fabric Devices per Fabric/site	500/site	600/site	1200/site
No if IP Pools	100/site	300/site	1000/site

* With 3-Node Cluster

Cisco SD-Access Transit Types

Transit/Peer Network Types

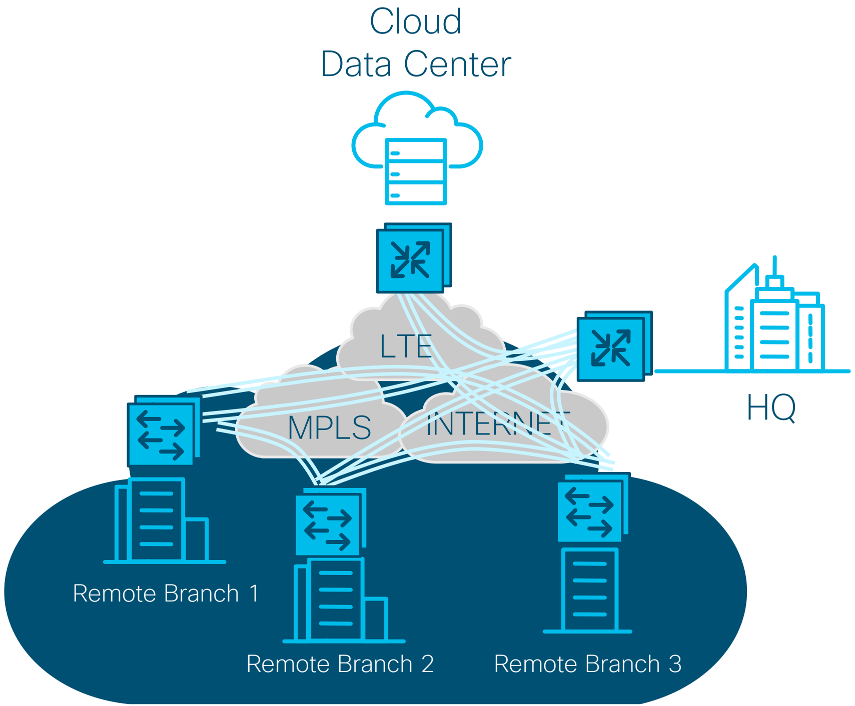
Transit/Peer Network type include

- IP-Based Transit – Leverages a traditional IP-based (VRF-LITE, MPLS) network, which requires remapping of VRFs and SGTs between sites.

- Cisco SD-Access Transit - Enables a native Cisco SD-Access (VXLAN,SGT) fabric, with Transit Control Plane Nodes for inter-site communication.

Transit Connectivity

Why IP Based Transit?



✓ Customers already using existing WAN or have adopted SD-WAN

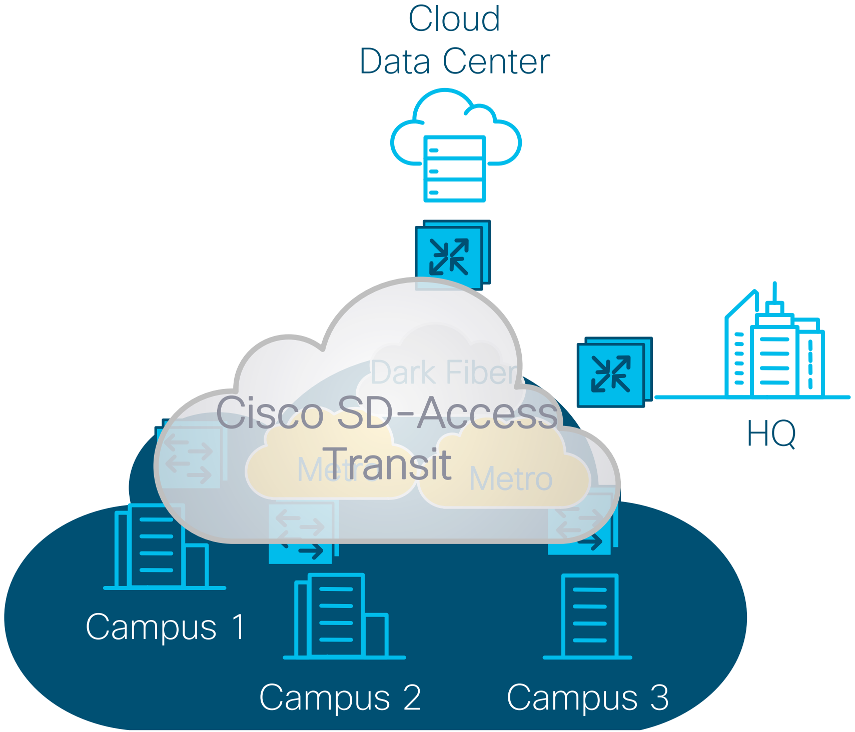
✓ Unable to carry VXLAN header in WAN

Typical use cases

- Internet Handoff
- P2P IPSEC encryption
- Policy Based Routing
- WAN Accelerators
- Traffic engineering
- Mobile Backhaul LTE

Cisco SD-Access Multi-Site Fabric

When to use Cisco SD-Access Transit? – Distributed Campus/Metro Deployments



✓ Higher MTU support

Typical use cases

- Native unified policy across the locations and end-to-end segmentation using VNs and SGTs
- Smaller and Isolated fault domains
- Resiliency and Scalability

IP as Transit/Peer Network

IP Transit / Peer Network

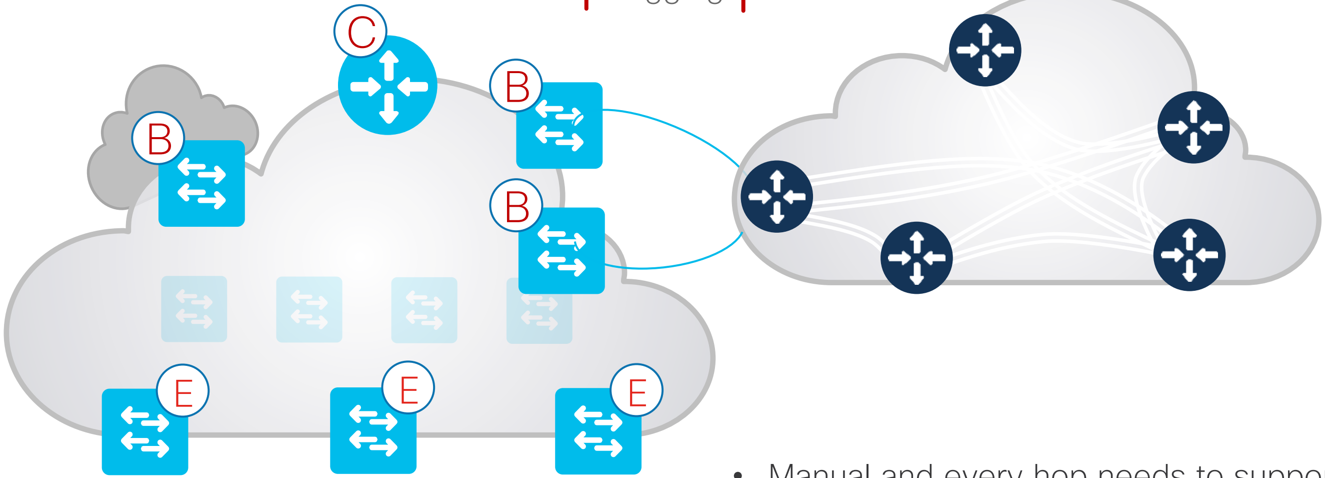
Network Plane Analysis Perspectives

1. Control-Plane: How routes / prefixes are communicated
2. Data-Plane: Which encapsulation method is used to carry data
3. Policy Plane: How group and segmentation information is communicated
4. Management Plane: How Management Infrastructure is Integrated

Communicating to Peer Network – IP

Control/Data/Policy Plane

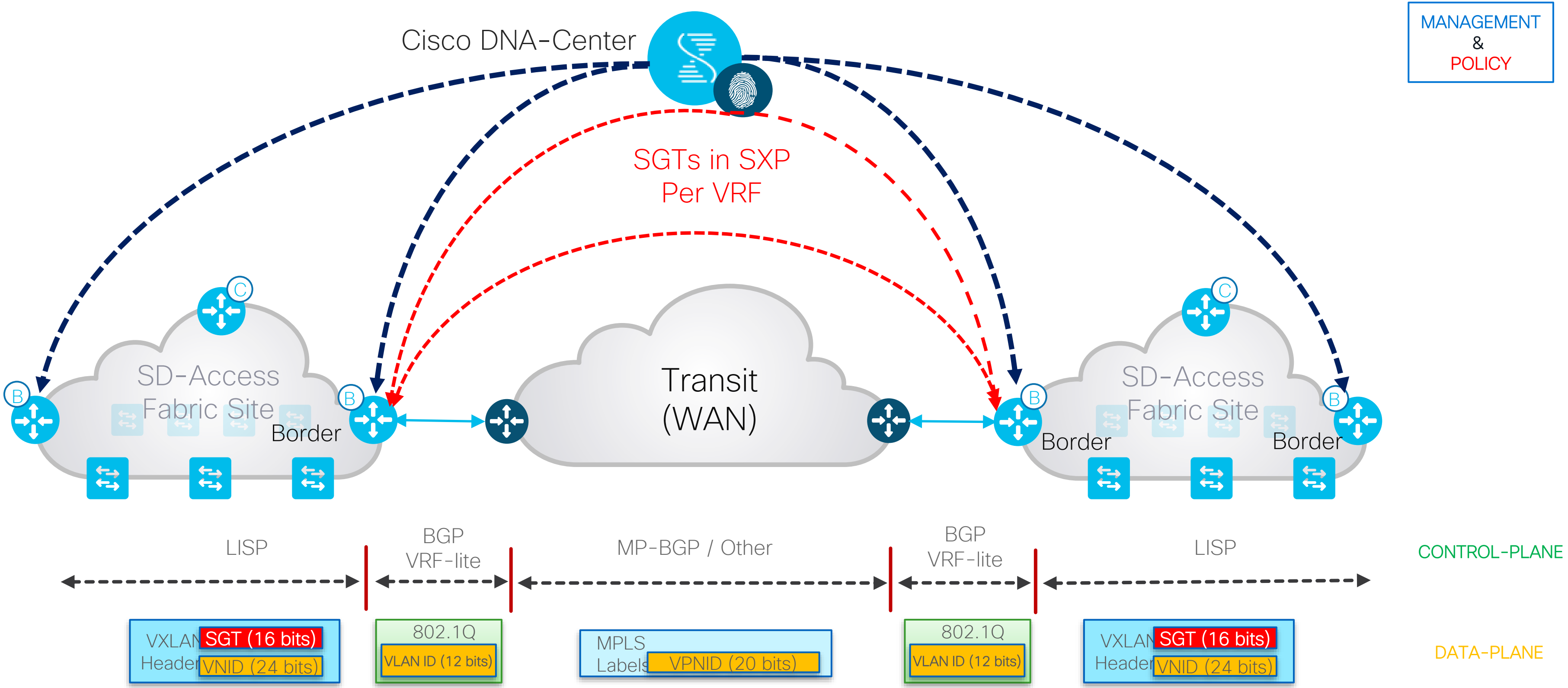
CONTROL-PLANE	LISP	eBGP	External Domain(BGP/IGP)
DATA-PLANE	VXLAN	VRF-LITE	External Domain(IP/MPLS/VXLAN
POLICY-PLANE	SGT in VXLAN	SGT* Tagging	External Domain (IP ACL/SGT)



- Manual and every hop needs to support SGT propagation

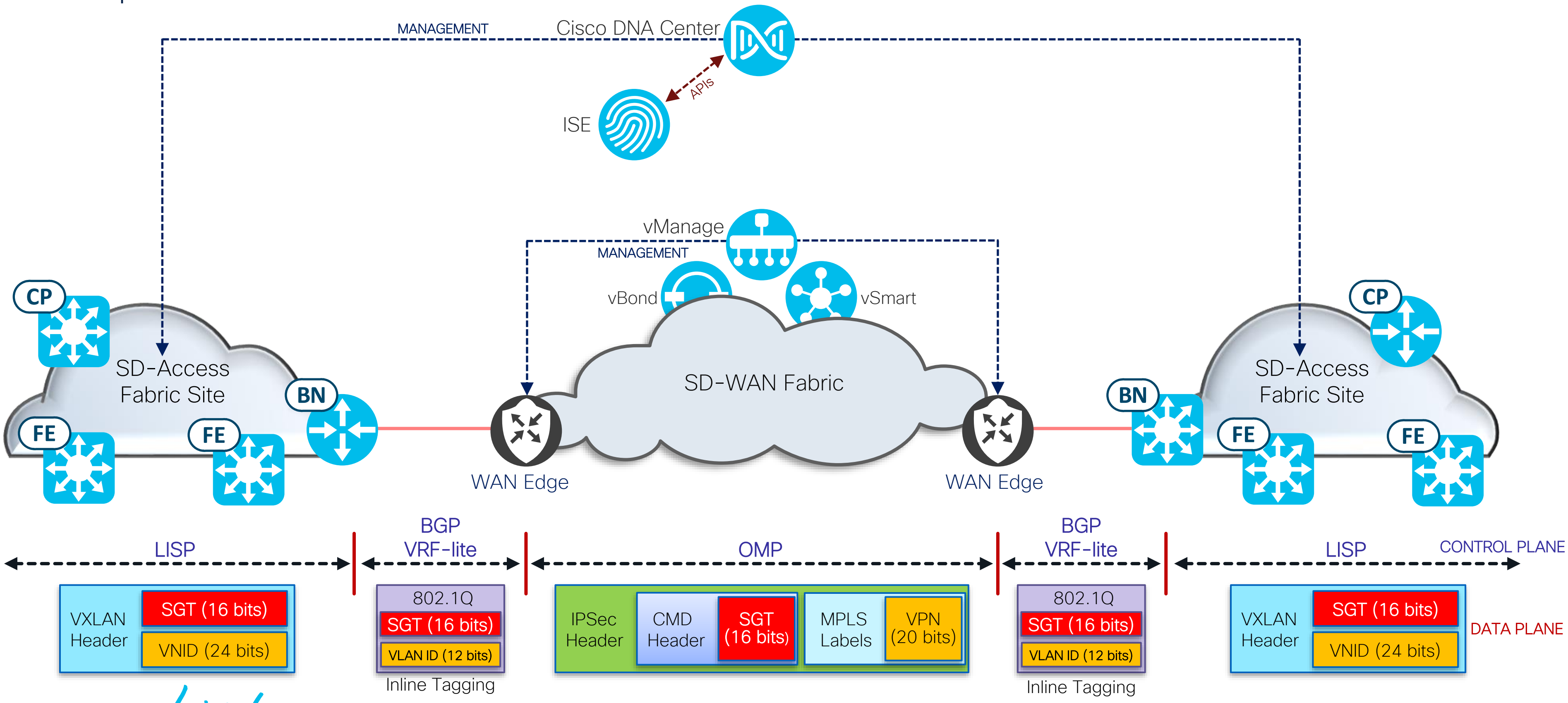
Inter-Connecting Fabrics/Sites

IP-Based WAN



Inter-Connecting Fabrics/Sites

Viptella SD-WAN



MANAGEMENT

Cisco DNA Center

APIs

ISE

vManage

MANAGEMENT

vBond

vSmart

CP

SD-Access Fabric Site

BN

FE

FE

SD-WAN Fabric

WAN Edge

WAN Edge

BN

CP

SD-Access Fabric Site

FE

FE

LISP

BGP VRF-lite

OMP

BGP VRF-lite

LISP

CONTROL PLANE

VXLAN Header | SGT (16 bits) | VNID (24 bits)

802.1Q | SGT (16 bits) | VLAN ID (12 bits)

Inline Tagging

IPSec Header | CMD Header | SGT (16 bits) | MPLS Labels | VPN (20 bits)

802.1Q | SGT (16 bits) | VLAN ID (12 bits)

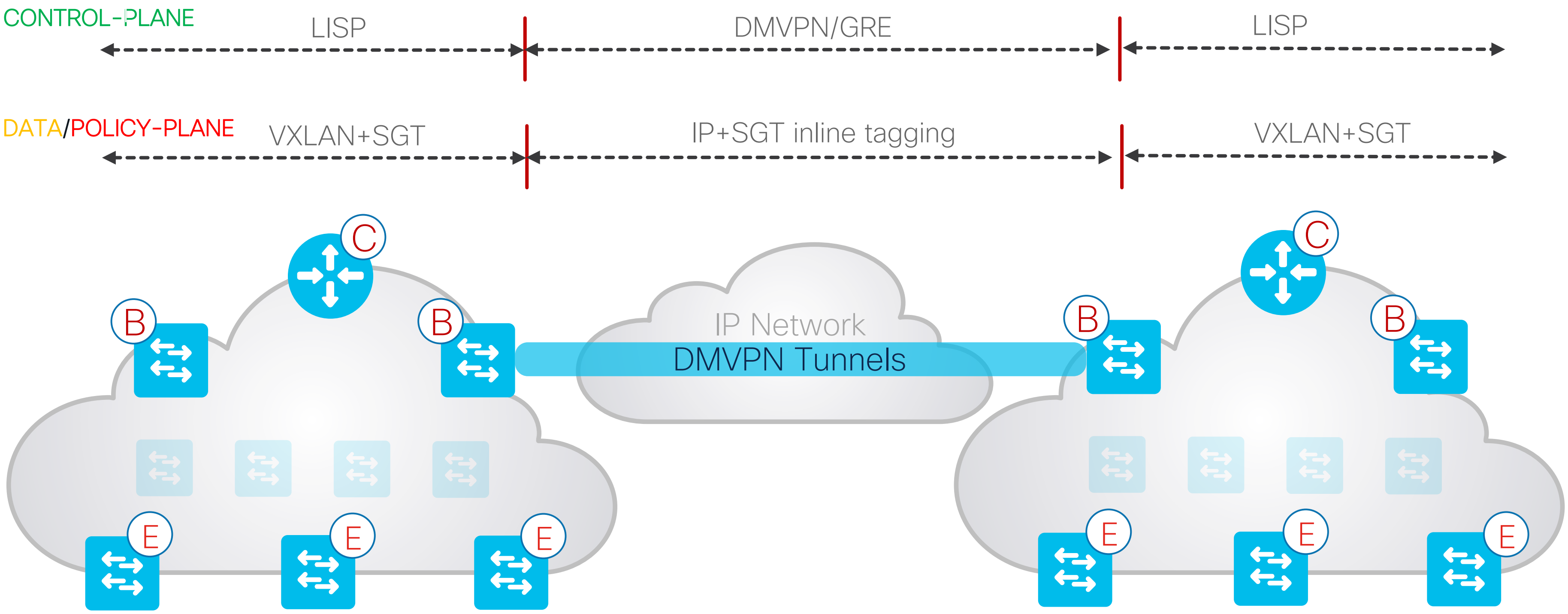
Inline Tagging

VXLAN Header | SGT (16 bits) | VNID (24 bits)

DATA PLANE

Inter-Connecting Fabrics/Sites

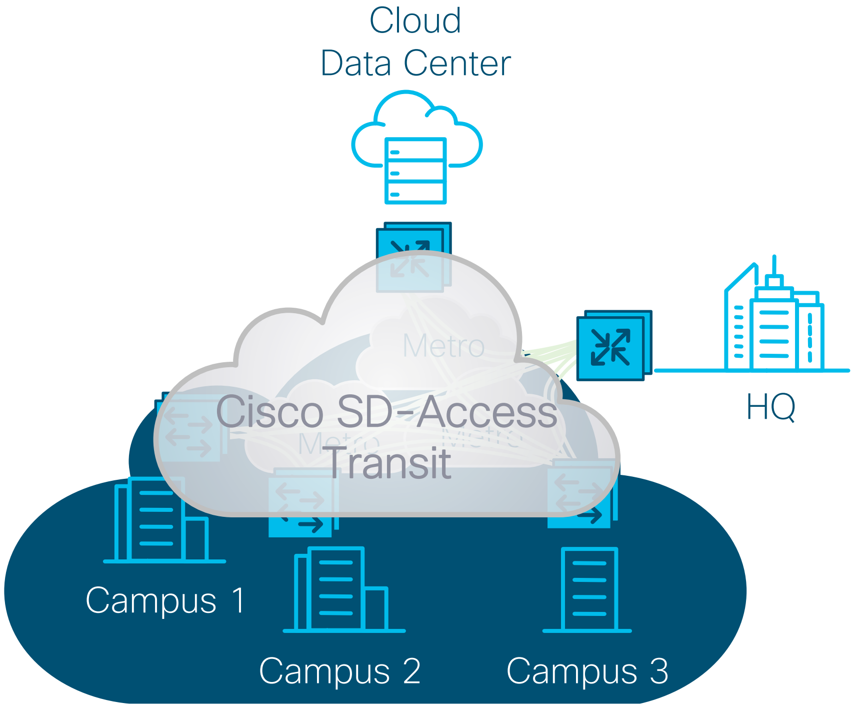
DMVPN



SD-Access as Transit

Cisco SD-Access Transit Multi-Site

Consistent Segmentation and Policy across sites

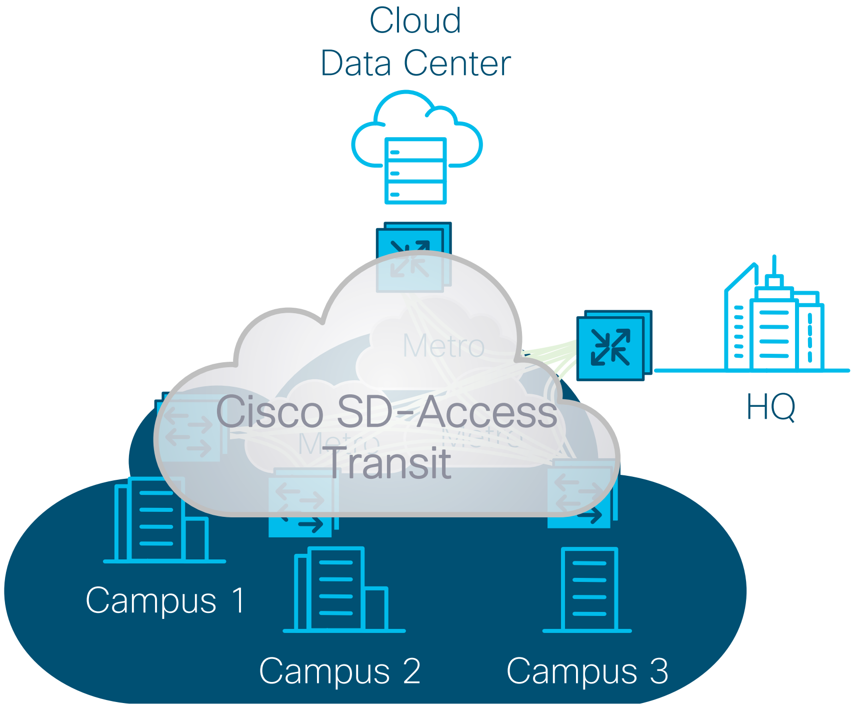


Cisco SD-Access Transit Multi-Site Advantages:

- End-to-end Segmentation and policy
- Smaller or isolated Failure Domains
- Horizontally scaled networks
- Single view of Entire Network
- Elimination of Per Deviceat every site*

Cisco SD-Access Multi-Site

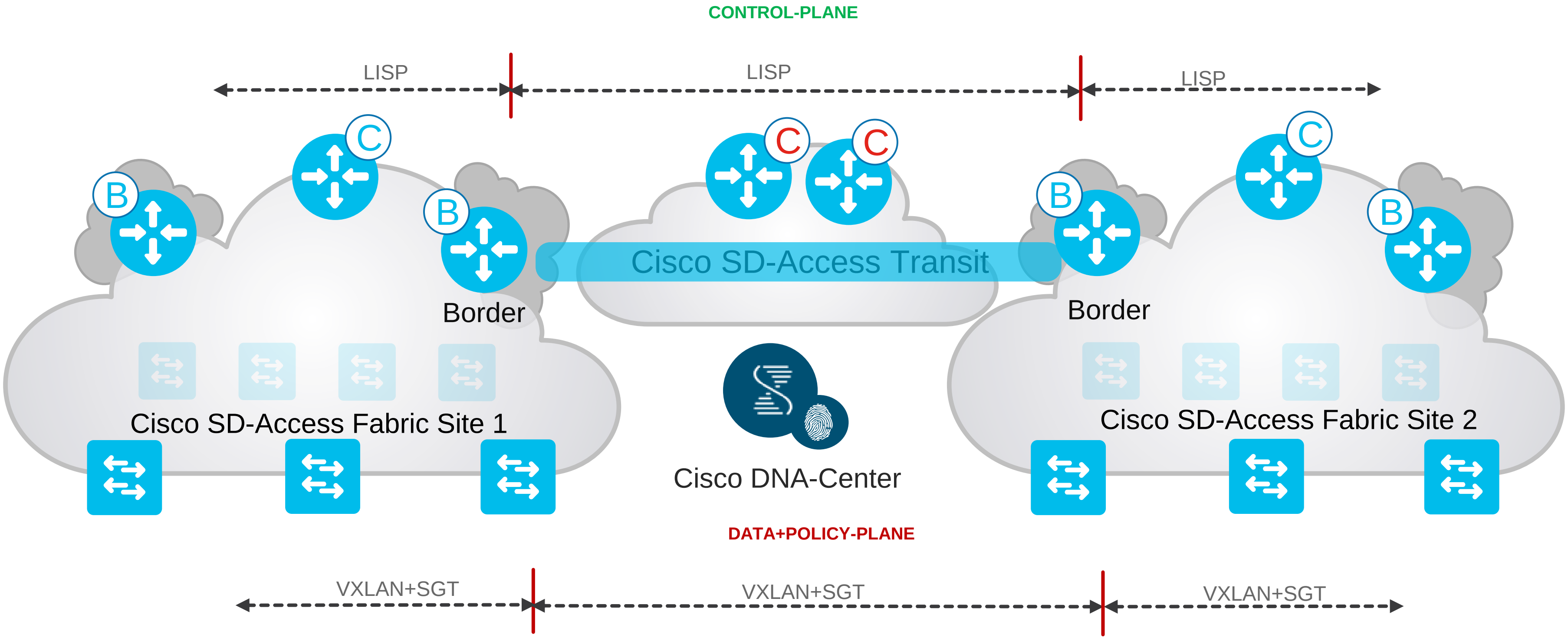
Key Considerations



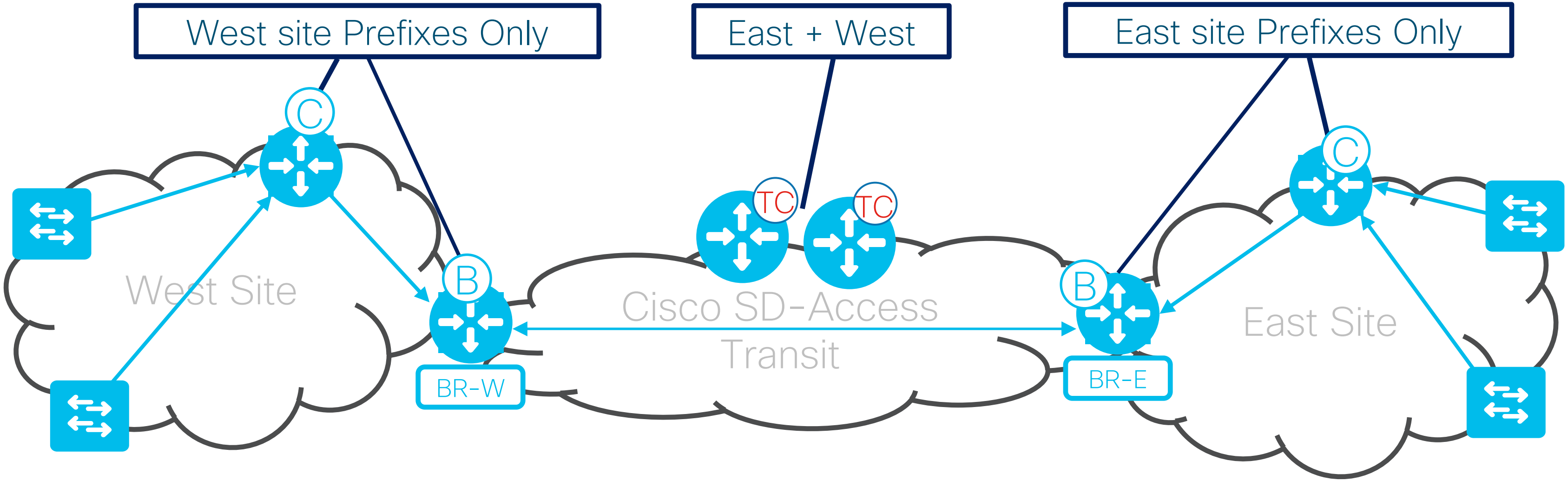
Cisco SD-Access Transit Multi-Site Key Considerations:

- ➢ Should accommodate the MTU setting used for SD-Access in the campus network

Cisco SD-Access Multi-Site - SD-Access Transit



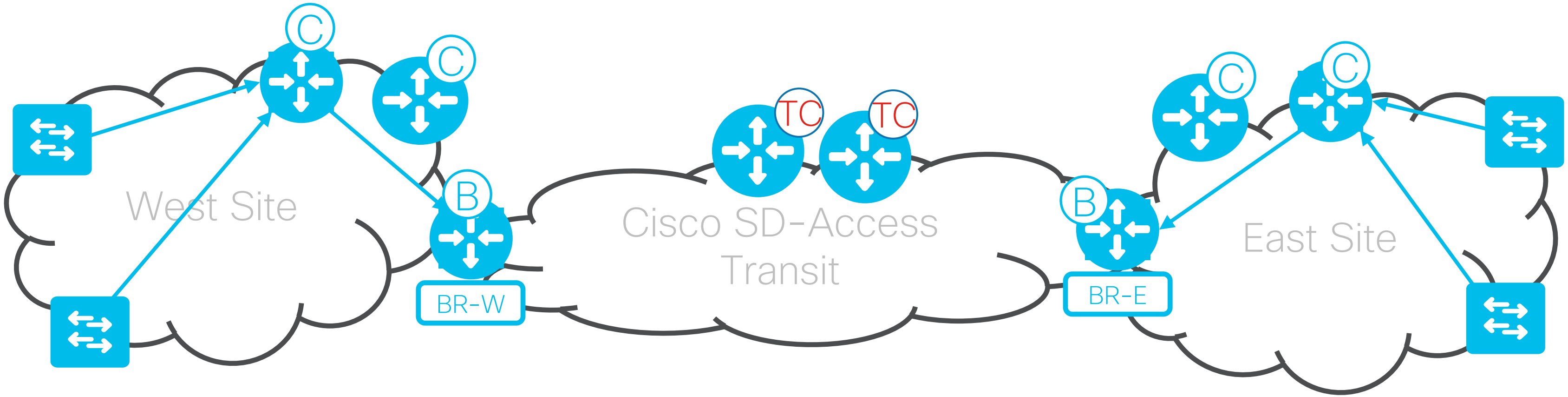
Cisco SD-Access Transit Control Plane for Global Scale



- Each site only maintains state for in-site end-points.
- Off site traffic follows default to transit.
- Survivability, each site is a fully autonomous resiliency domain
- Each Site has its own unique subnets

Cisco SD-Access Multi-Site

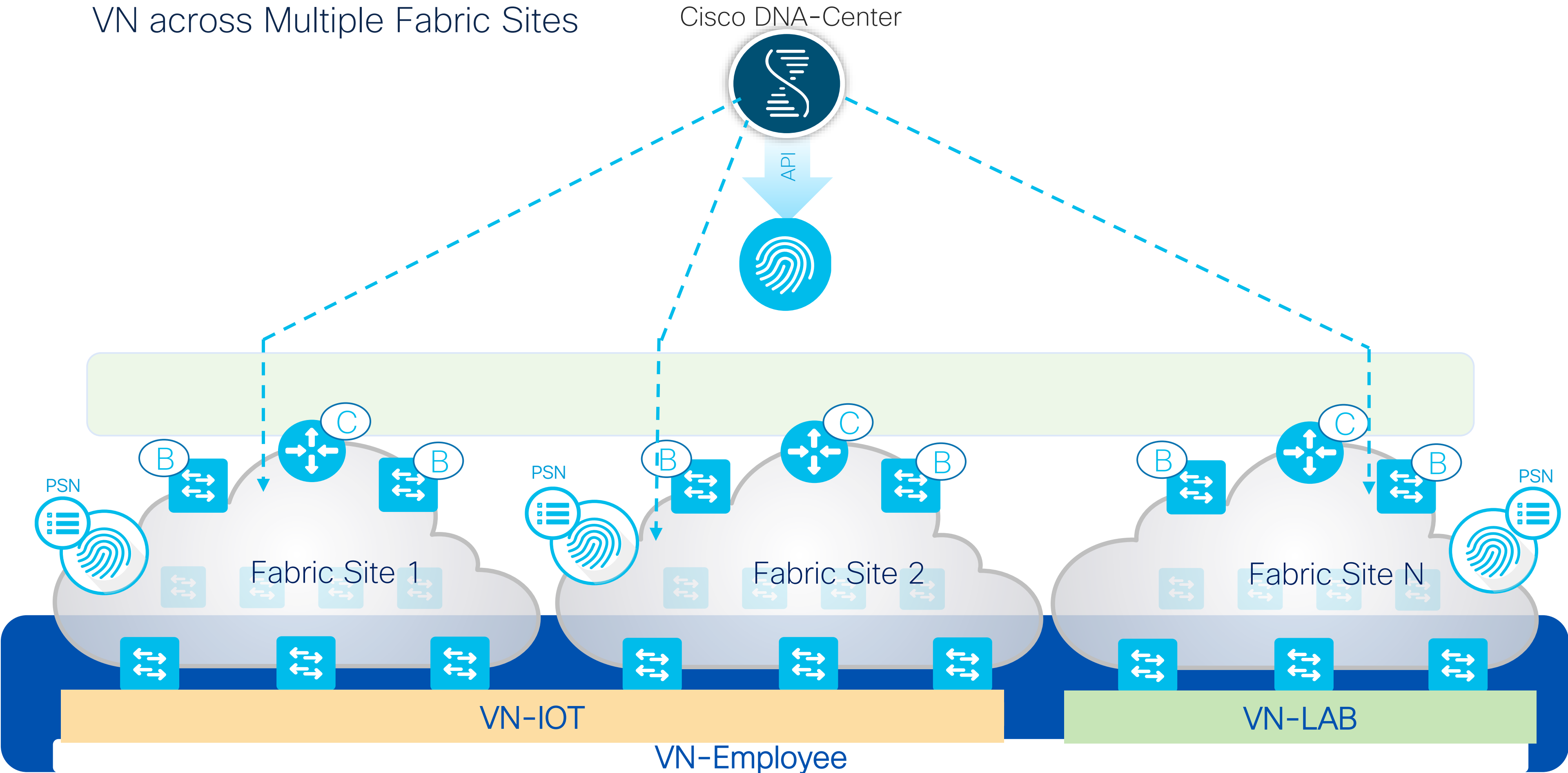
Transit Control Plane Deployment Location



- ➢ Device must be dedicated to the transit control plane node role.
- ➢ Doesn’t have to be physically deployed in Transit Area
- ➢ Ideally, device should not be in the data forwarding (transit path) between sites.
- ➢ Requires IP connectivity in the underlay from site borders at all fabric sites
- ➢ Deploy 2 Transit Control Plane nodes for redundancy and load balancing.

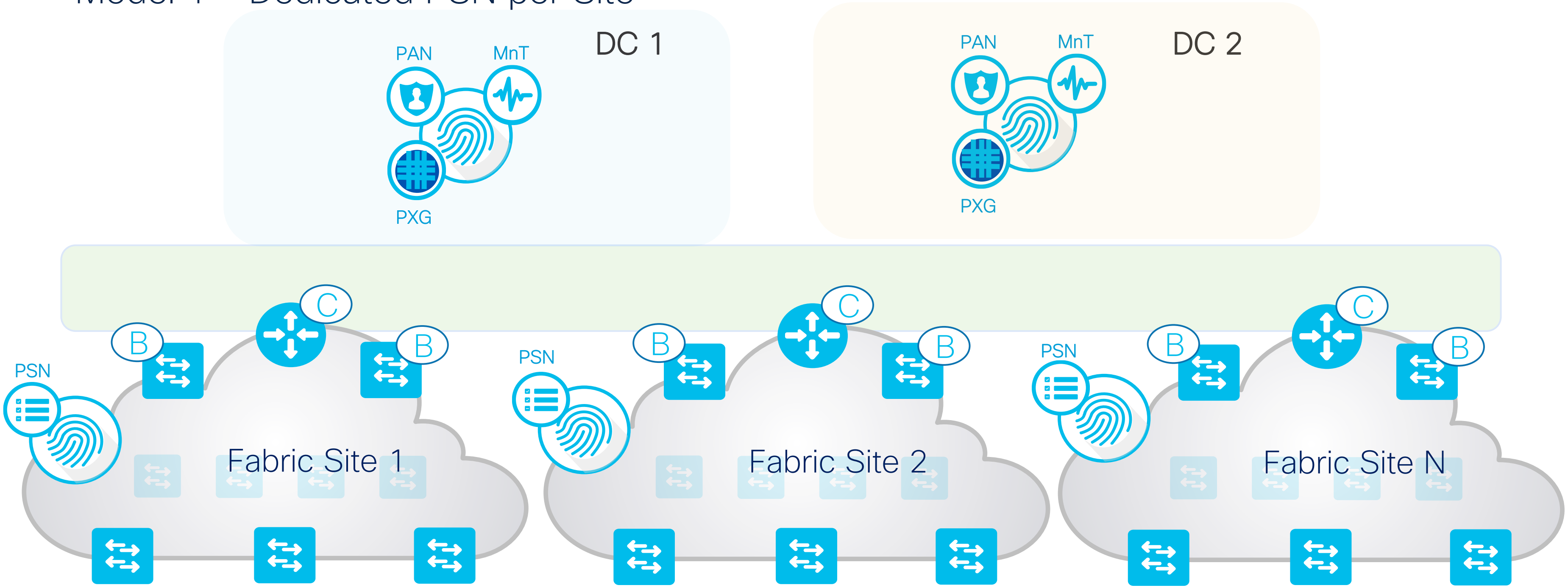
Cisco SD-Access Multi-Site

VN across Multiple Fabric Sites



ISE Distributed Deployment

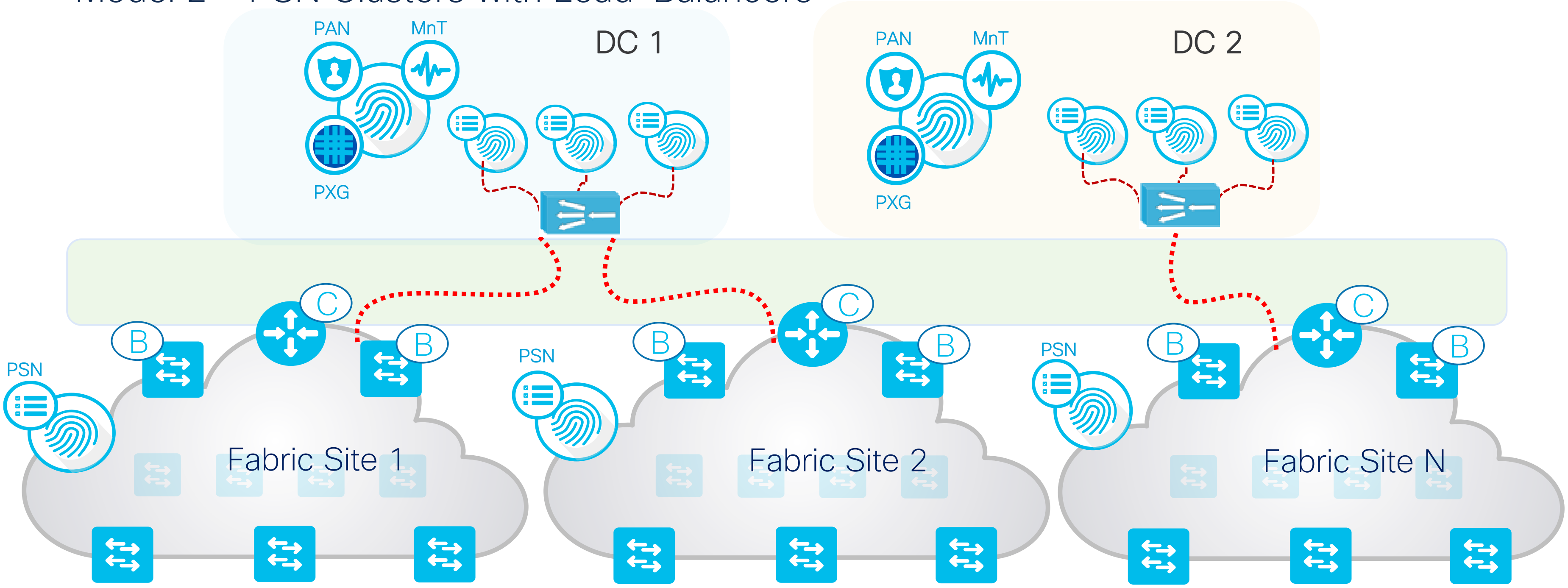
Model 1 - Dedicated PSN per Site



- PSN Nodes dedicated to every site
- Maximum of 2 PSN's per site
- PAN's are centralized in Data Center

ISE Distributed Deployment

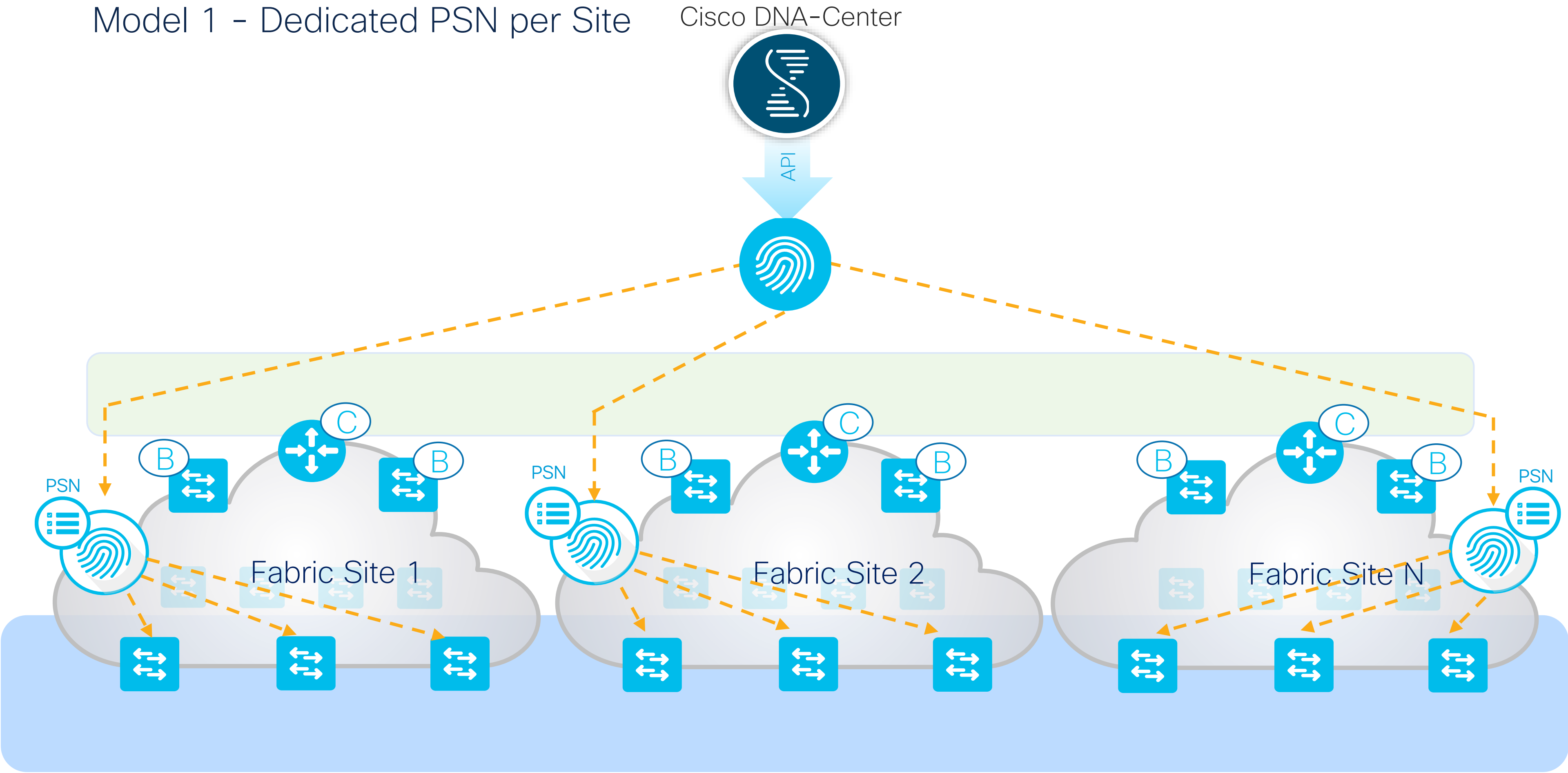
Model 2 - PSN Clusters with Load-Balancers



- PSN's are behind a dedicated Load Balancer
- DNAC site settings point to Load Balancer IP

ISE Distributed Deployment

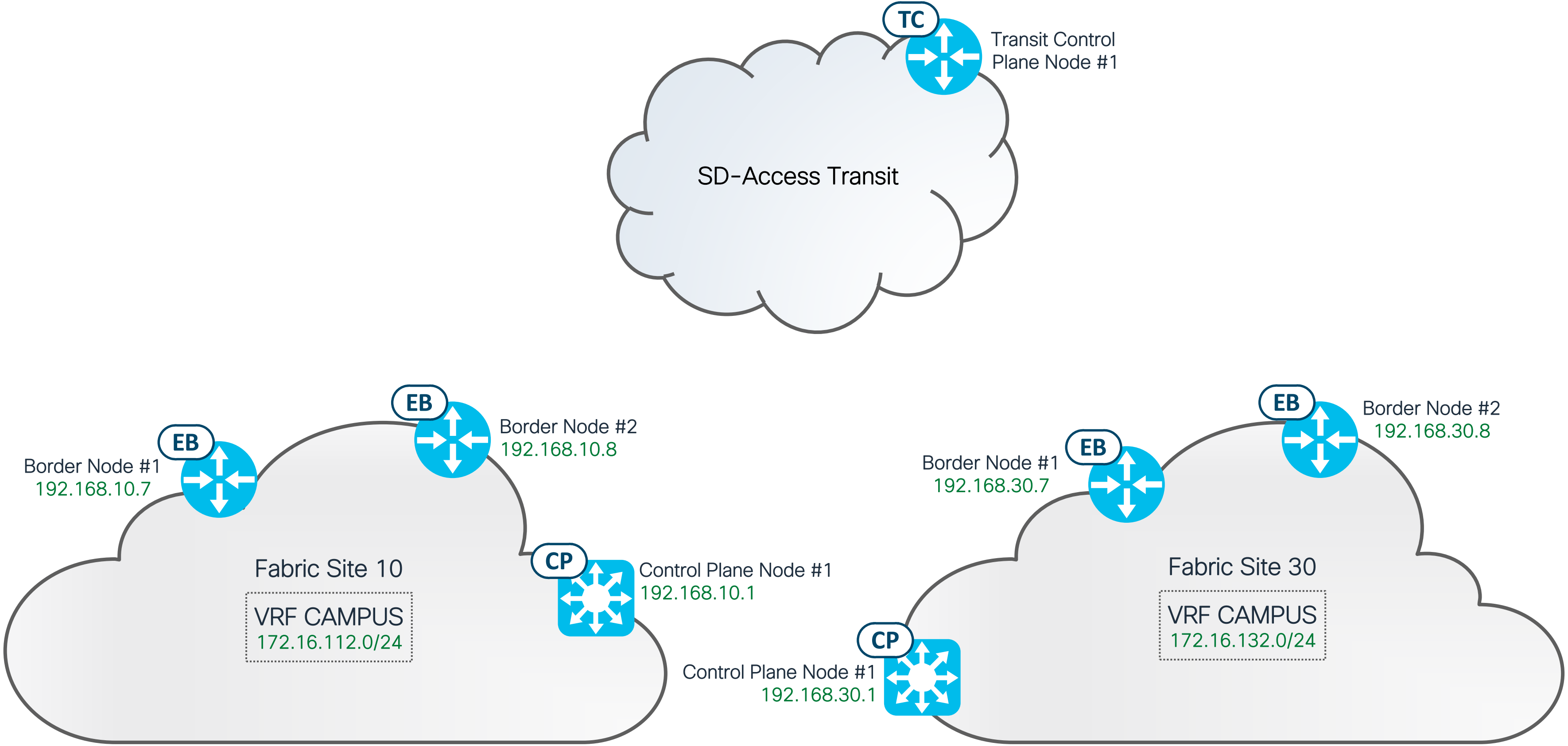
Model 1 - Dedicated PSN per Site



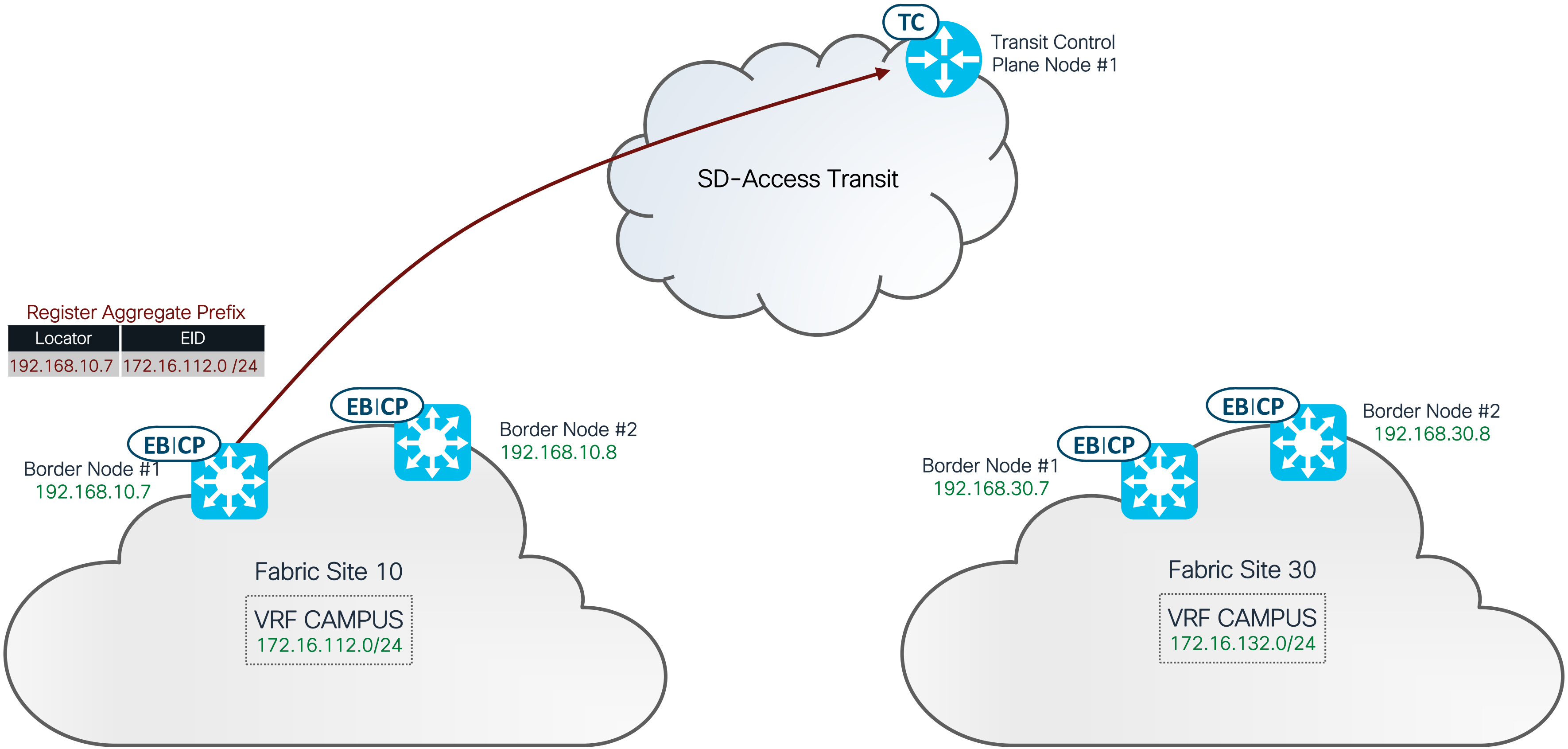
SD-Access Transit LISP Pub/Sub Registration

LISP Pub/Sub Registration and Publication in SD-Access Transit

Simplified Topology For this Section



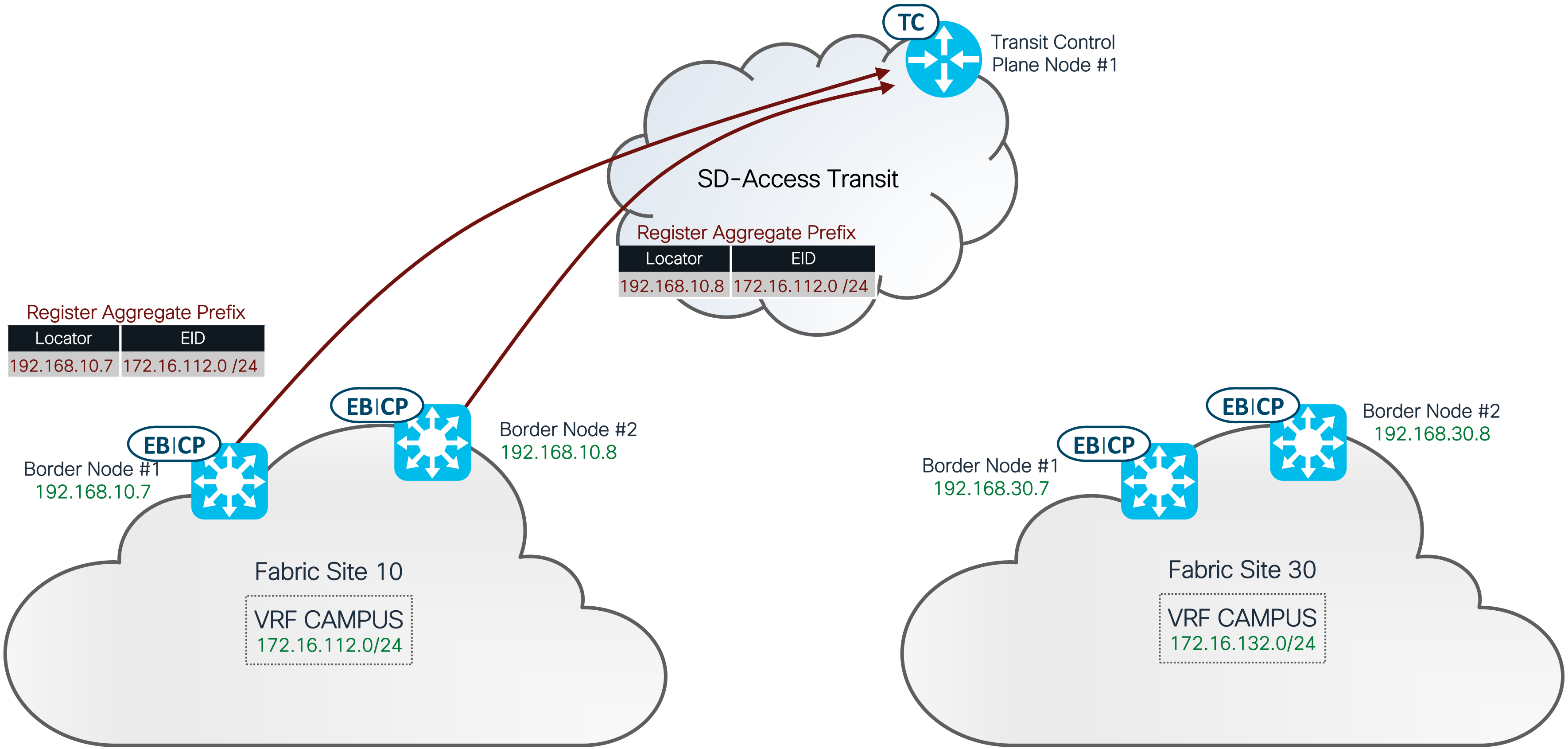
LISP Pub/Sub Registration and Publication in SD-Access Transit



Register Aggregate Prefix

Locator	EID
192.168.10.7	172.16.112.0 /24

LISP Pub/Sub Registration and Publication in SD-Access Transit



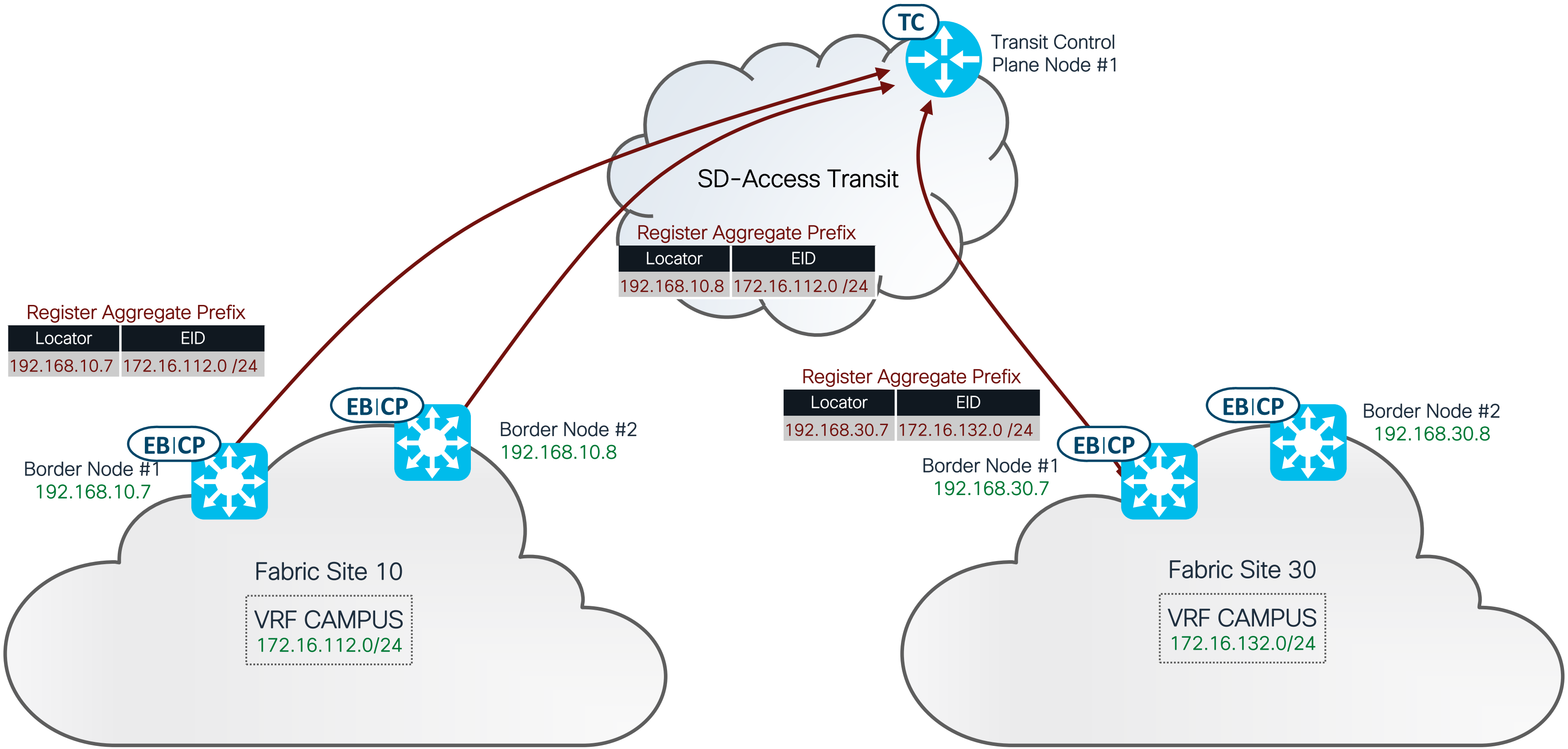
Register Aggregate Prefix

Locator	EID
192.168.10.7	172.16.112.0 /24

Register Aggregate Prefix

Locator	EID
192.168.10.8	172.16.112.0 /24

LISP Pub/Sub Registration and Publication in SD-Access Transit



Register Aggregate Prefix

Locator	EID
192.168.10.7	172.16.112.0 /24

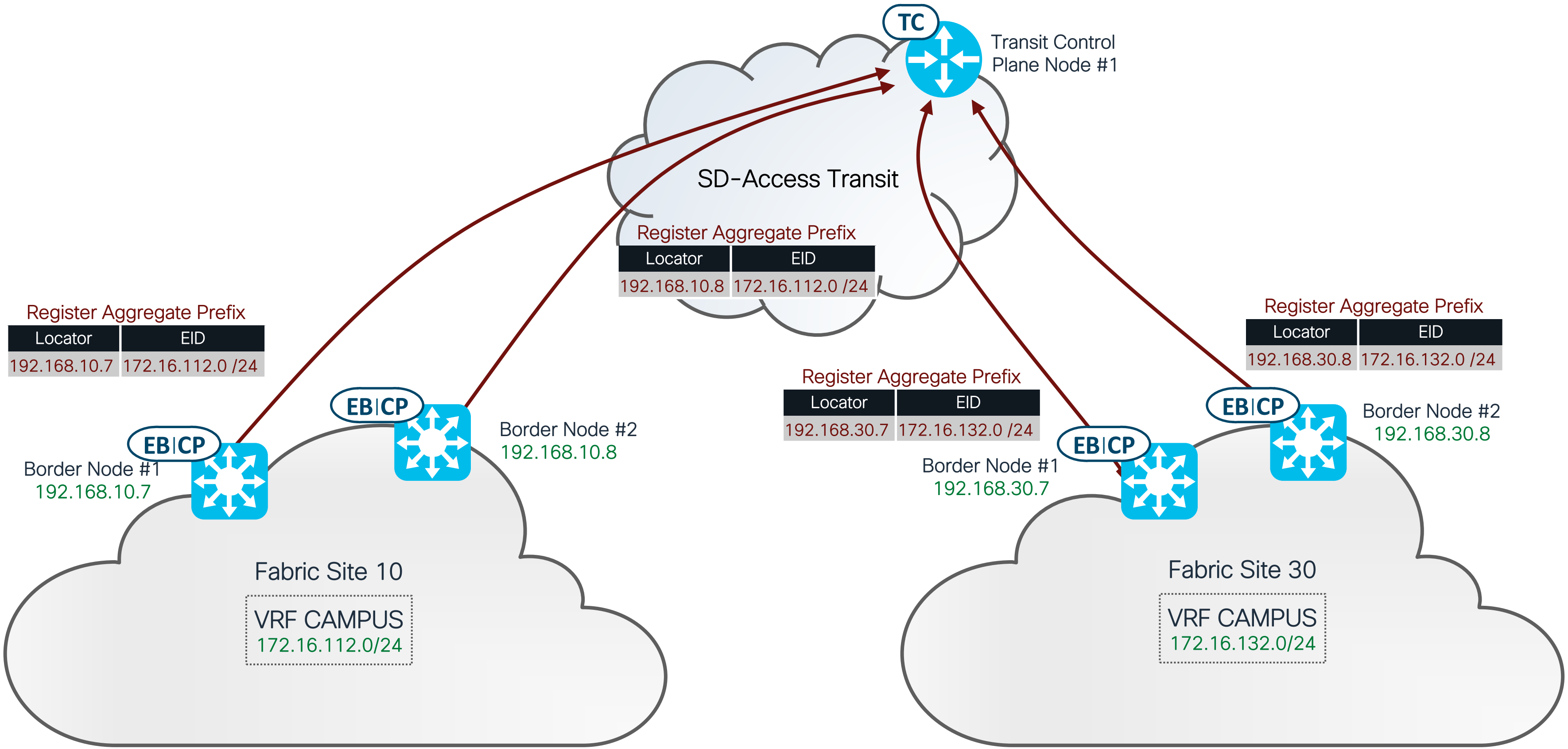
Register Aggregate Prefix

Locator	EID
192.168.10.8	172.16.112.0 /24

Register Aggregate Prefix

Locator	EID
192.168.30.7	172.16.132.0 /24

LISP Pub/Sub Registration and Publication in SD-Access Transit



Register Aggregate Prefix

Locator	EID
192.168.10.7	172.16.112.0 /24

Register Aggregate Prefix

Locator	EID
192.168.10.8	172.16.112.0 /24

Register Aggregate Prefix

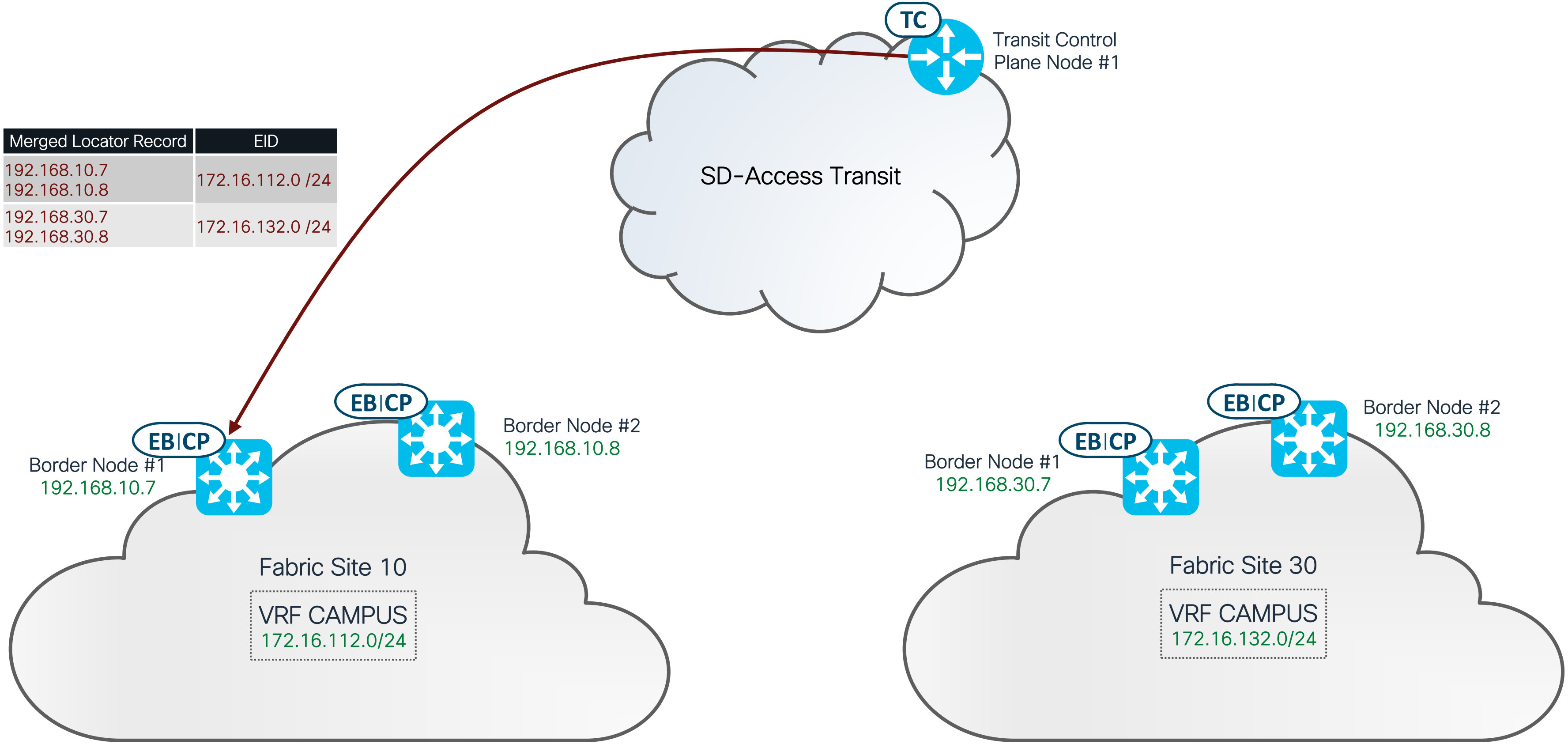
Locator	EID
192.168.30.7	172.16.132.0 /24

Register Aggregate Prefix

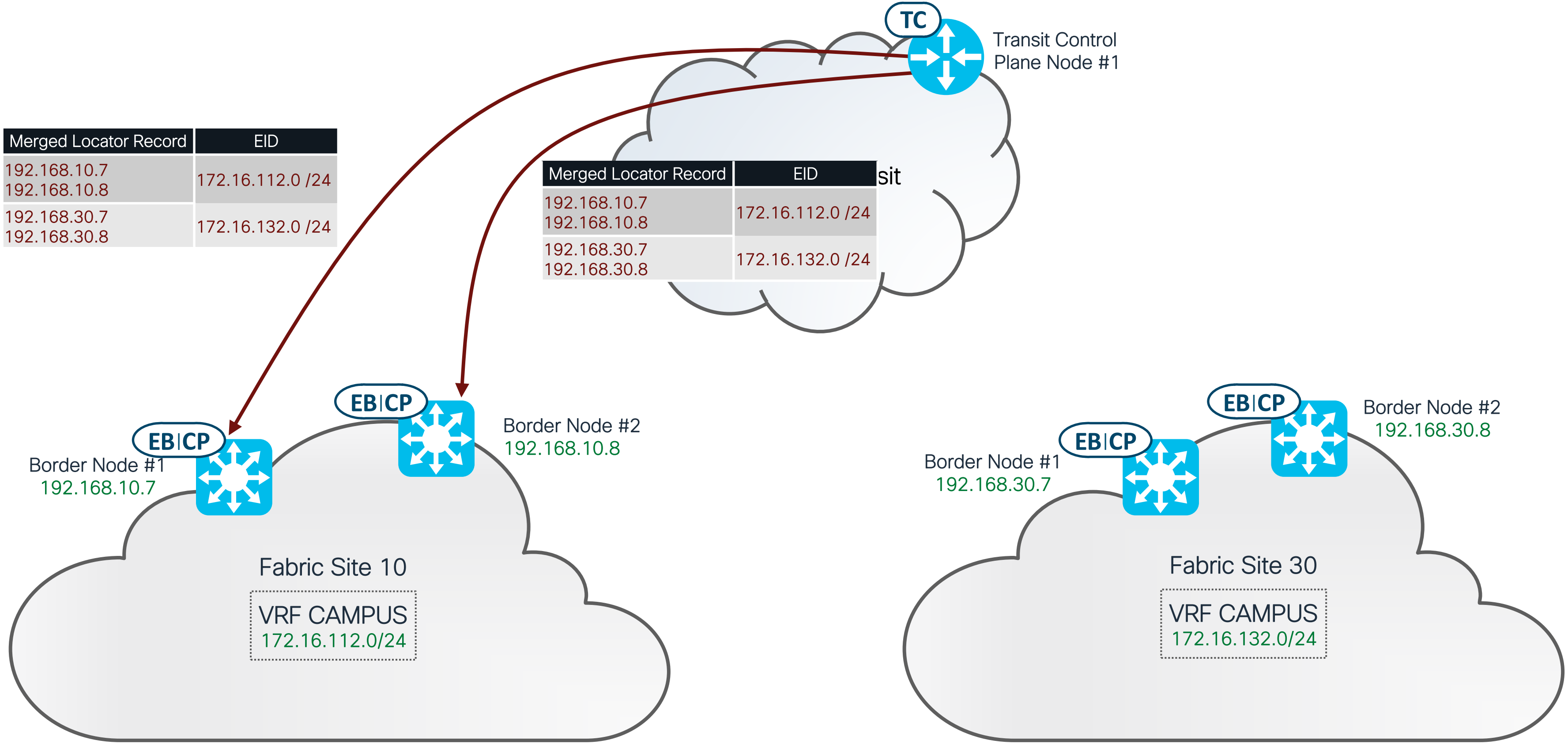
Locator	EID
192.168.30.8	172.16.132.0 /24

LISP Pub/Sub Registration and Publication in SD-Access Transit

Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24



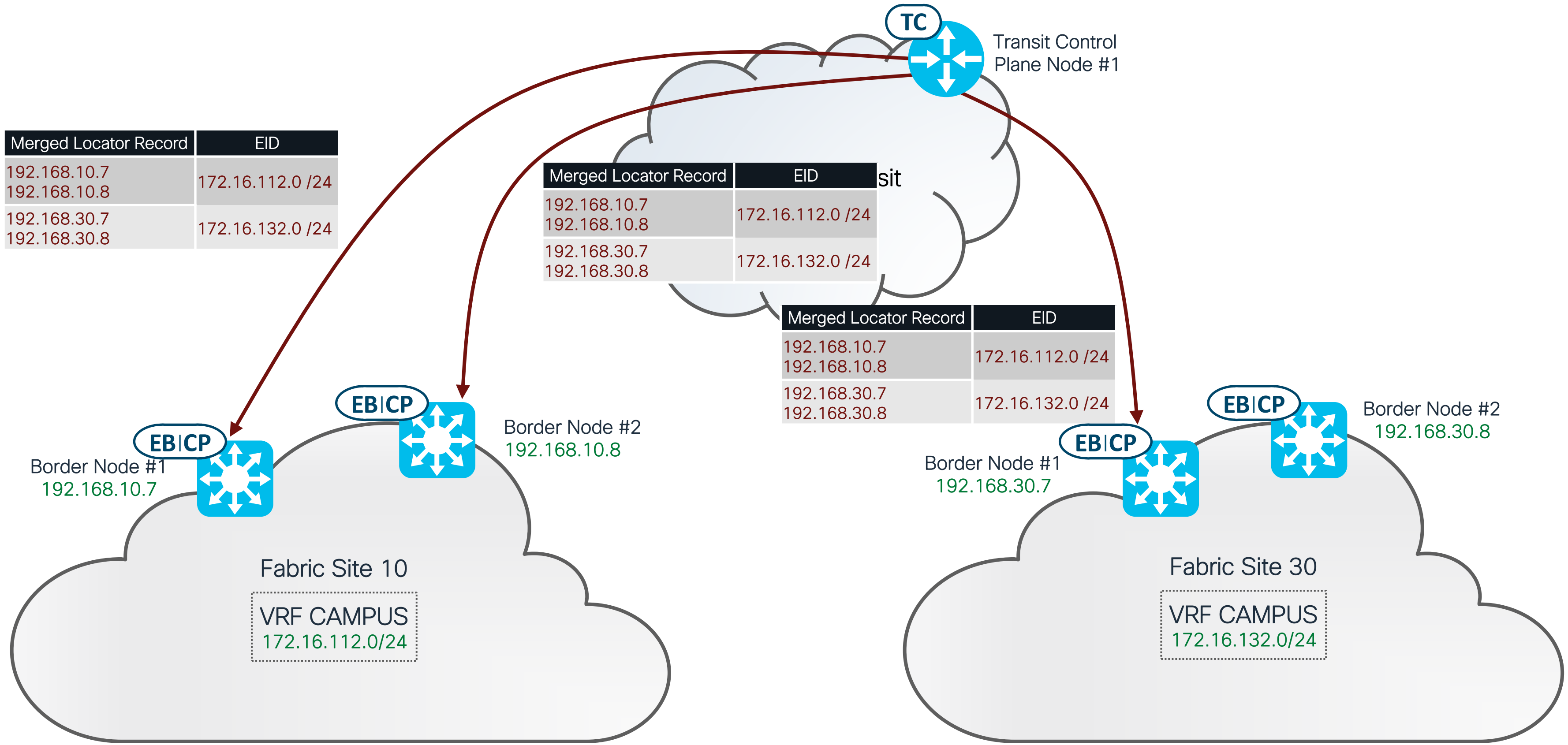
LISP Pub/Sub Registration and Publication in SD-Access Transit



Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

LISP Pub/Sub Registration and Publication in SD-Access Transit

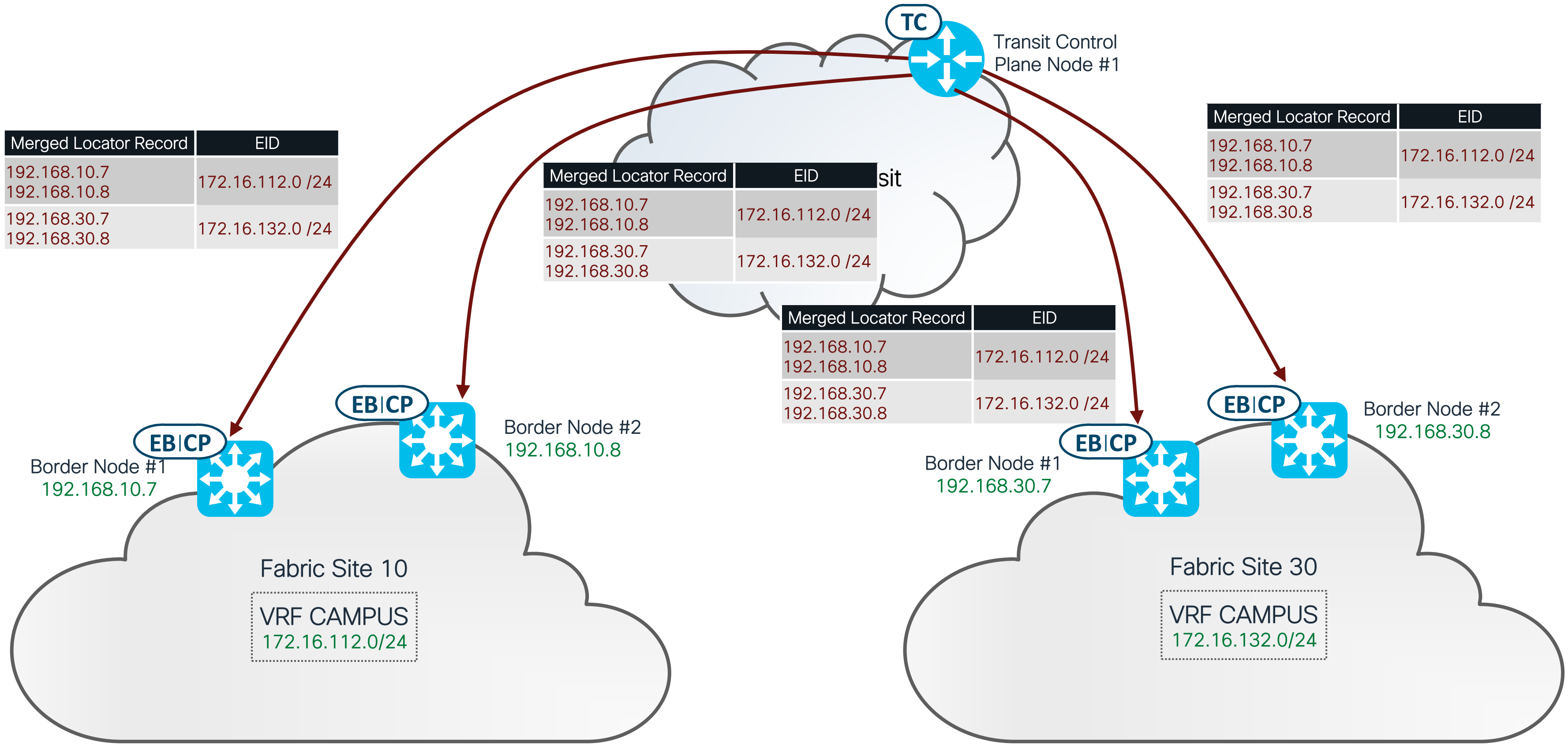


Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

LISP Pub/Sub Registration and Publication in SD-Access Transit



Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

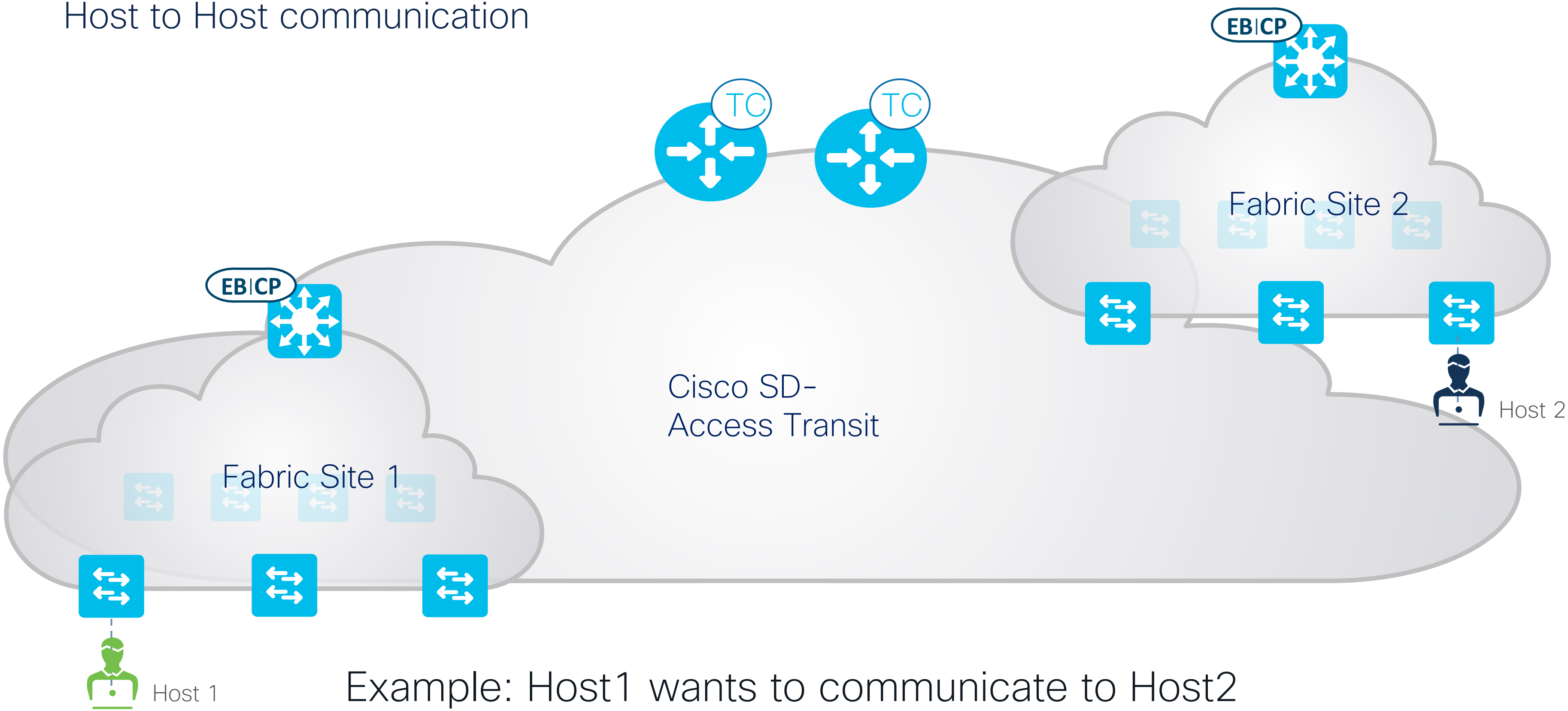
Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

Merged Locator Record	EID
192.168.10.7 192.168.10.8	172.16.112.0 /24
192.168.30.7 192.168.30.8	172.16.132.0 /24

SD-Access Transit Packet Walk with LISP Pub/Sub

SD-Access Transit Forwarding with LISP Pub/Sub

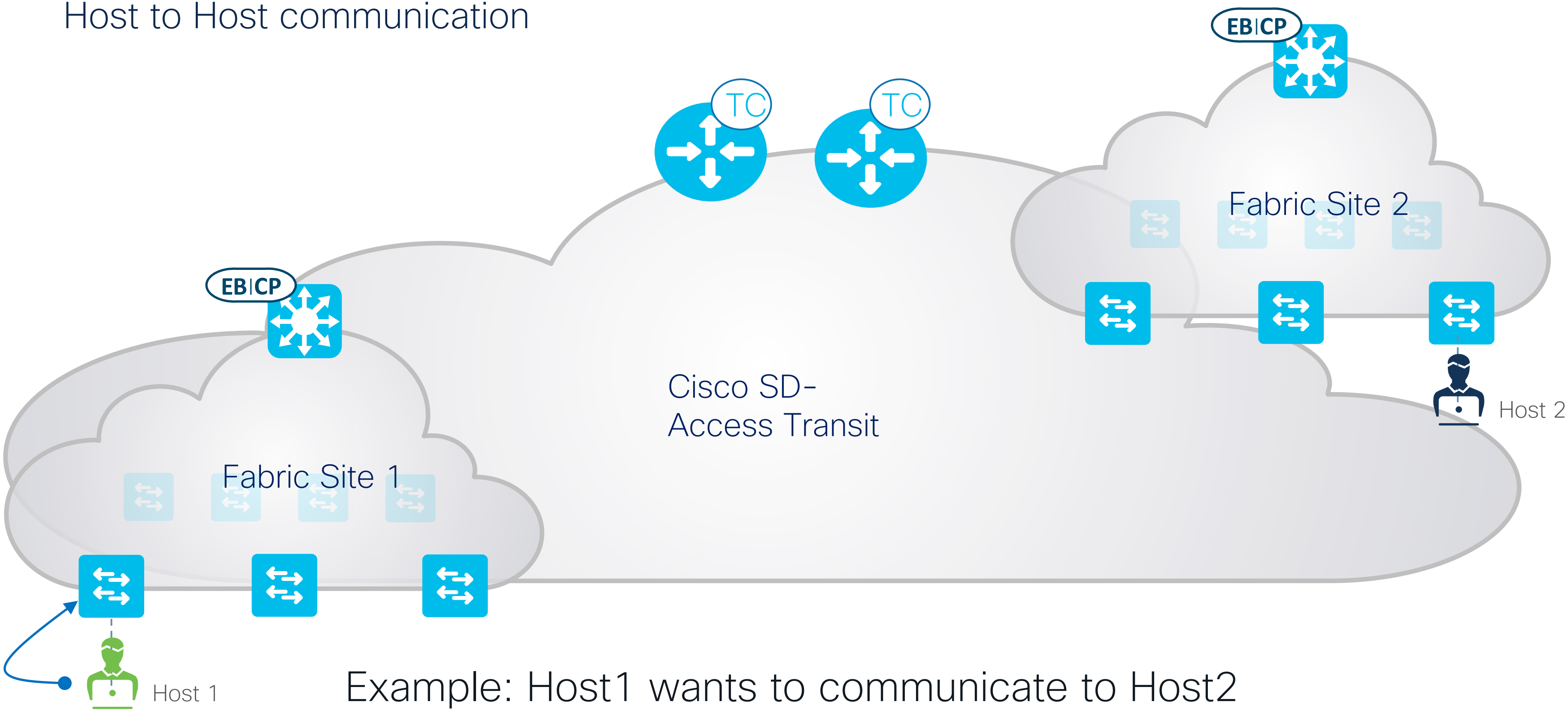
Host to Host communication



Example: Host1 wants to communicate to Host2

SD-Access Transit Forwarding with LISP Pub/Sub

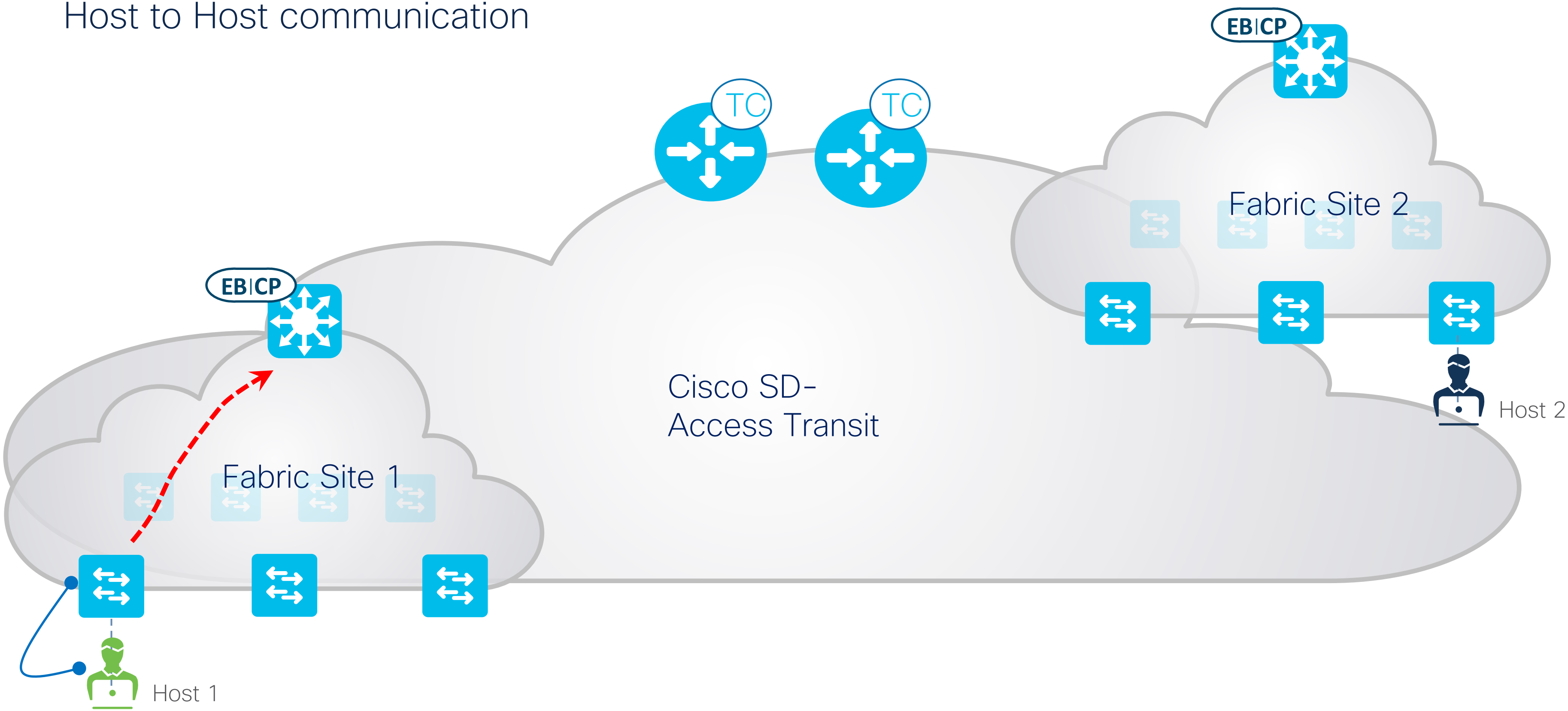
Host to Host communication



Example: Host1 wants to communicate to Host2

SD-Access Transit Forwarding with LISP Pub/Sub

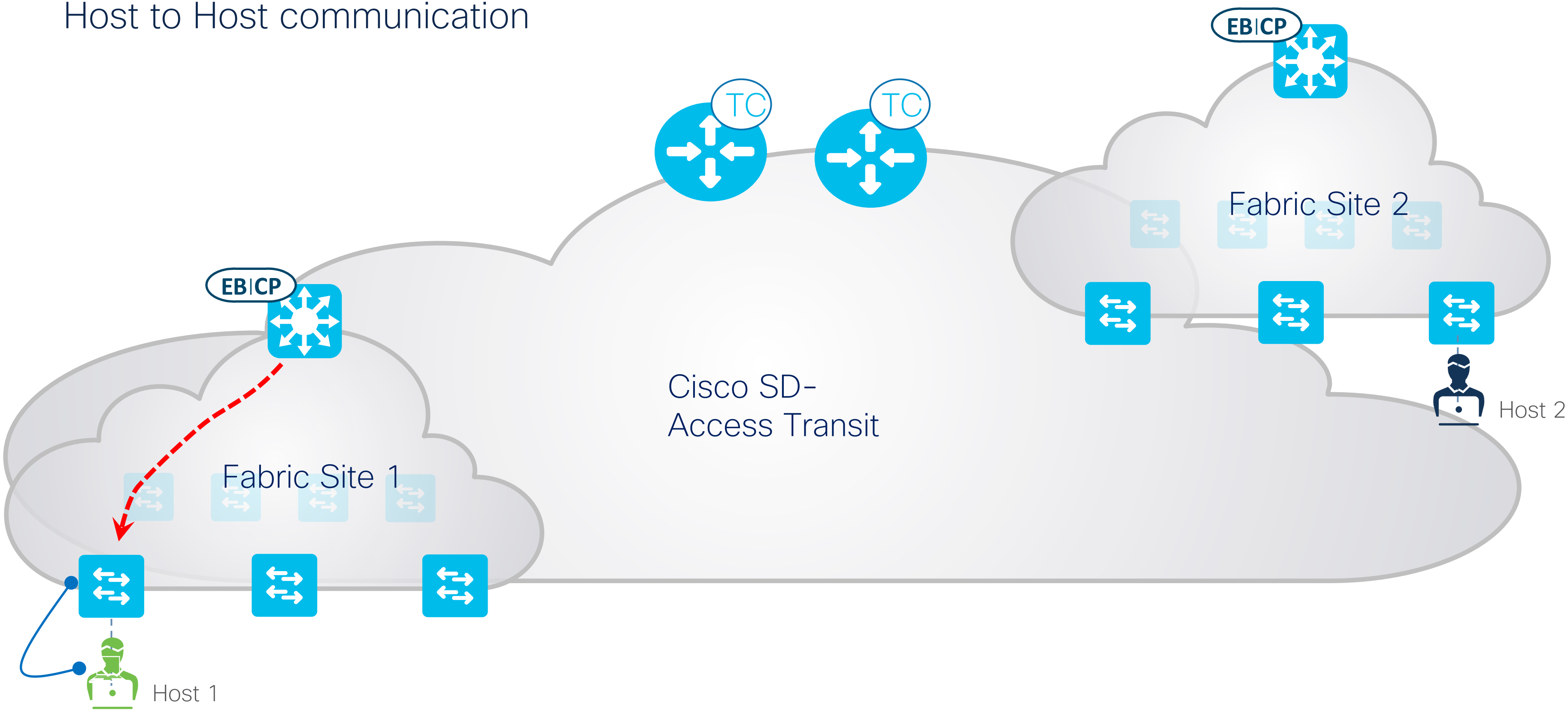
Host to Host communication



Edge Node in Fabric Site 1 sends a map-request to local Control Plane Node for host 2 IP in Fabric Site 2

SD-Access Transit Forwarding with LISP Pub/Sub

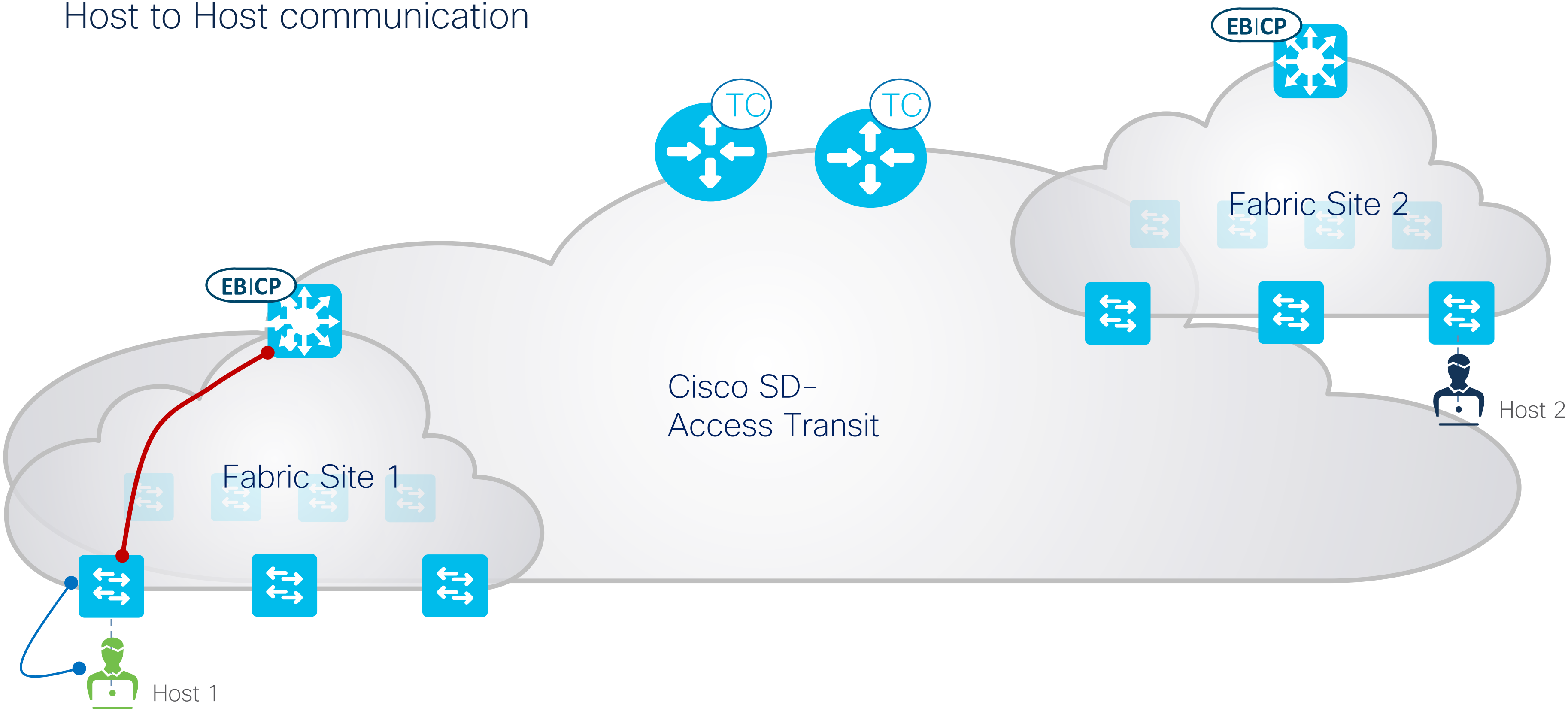
Host to Host communication



Fabric Control Plane Node in Fabric Site 1 sends a Negative map-reply(NMR) informing the Edge Node that it does not have information about Host 2

SD-Access Transit Forwarding with LISP Pub/Sub

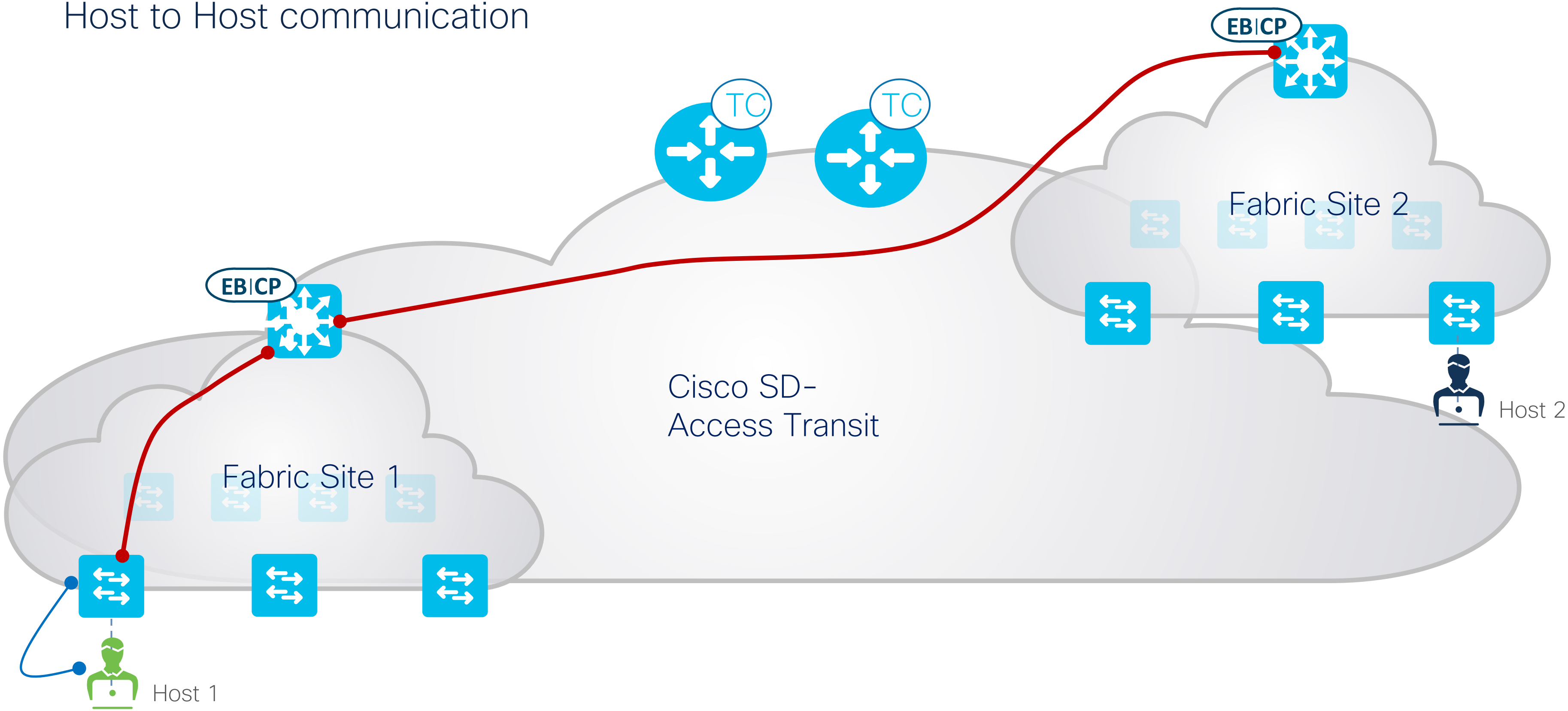
Host to Host communication



Traffic is VxLAN encapsulated from the Edge Node in Fabric Site 1 to the Site-local Border Node.

SD-Access Transit Forwarding with LISP Pub/Sub

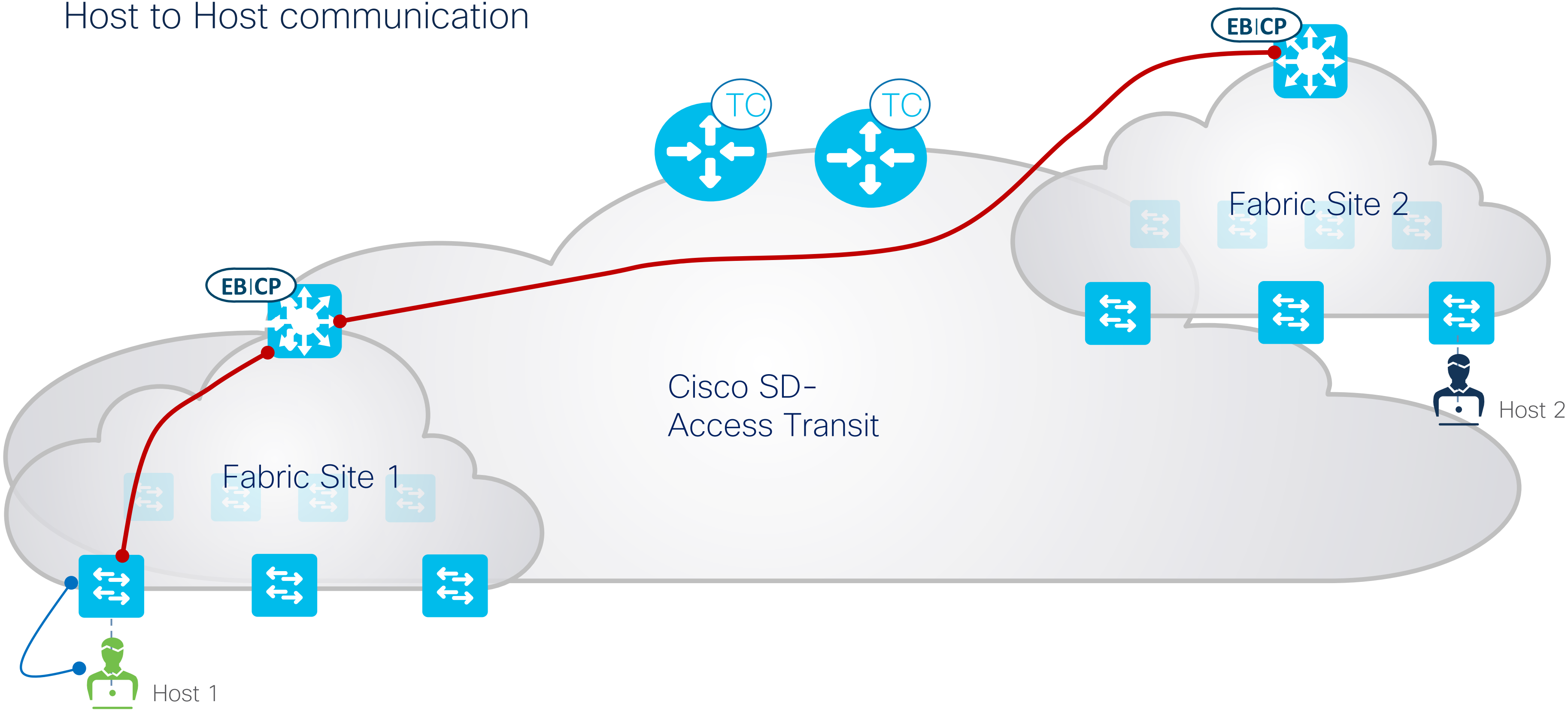
Host to Host communication



Traffic is forwarded from the Border Node in Fabric Site 1 to Fabric Site 2 using VXLAN encapsulation with SGT tags encoded.

SD-Access Transit Forwarding with LISP Pub/Sub

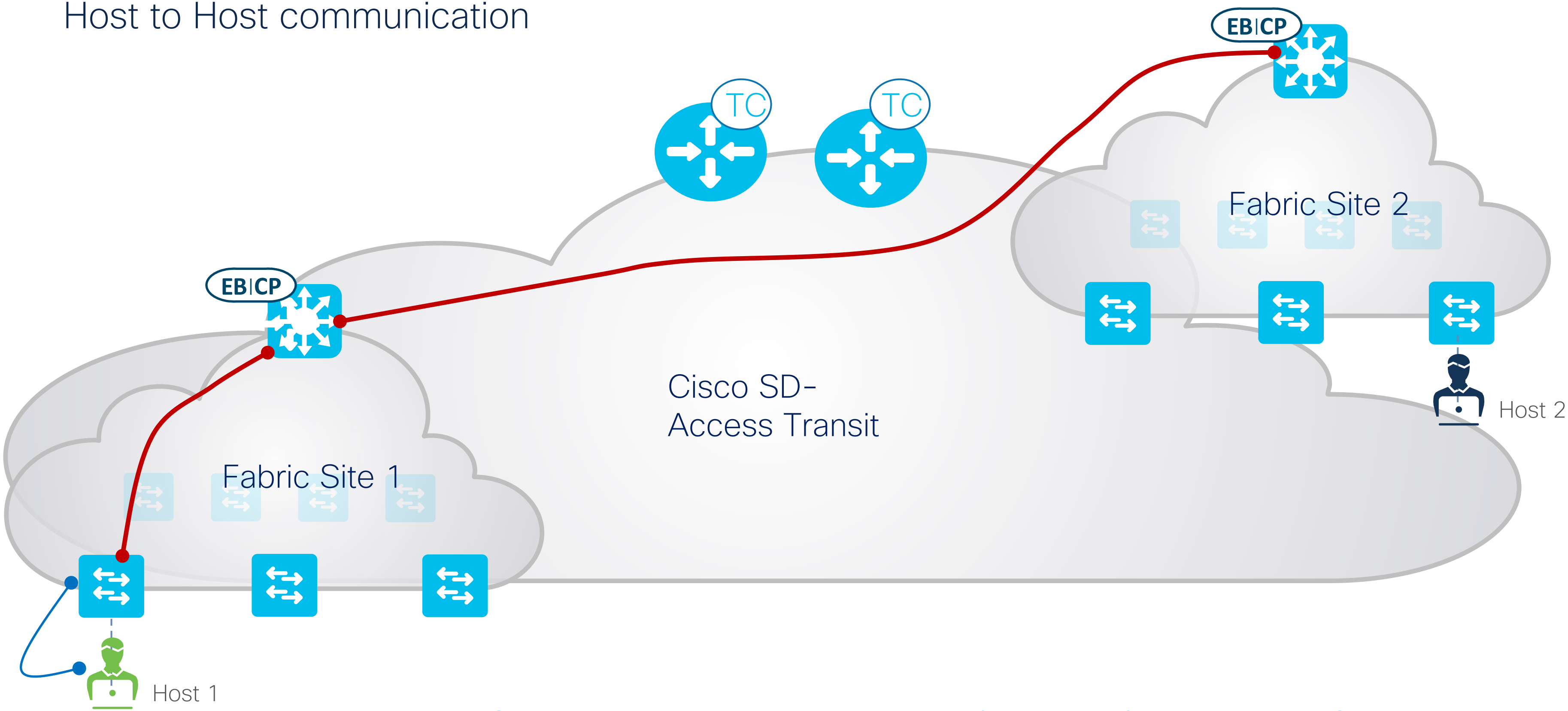
Host to Host communication



The Border Node in Fabric Site 2 will query the local Control Plane Node for the destination host.

SD-Access Transit Forwarding with LISP Pub/Sub

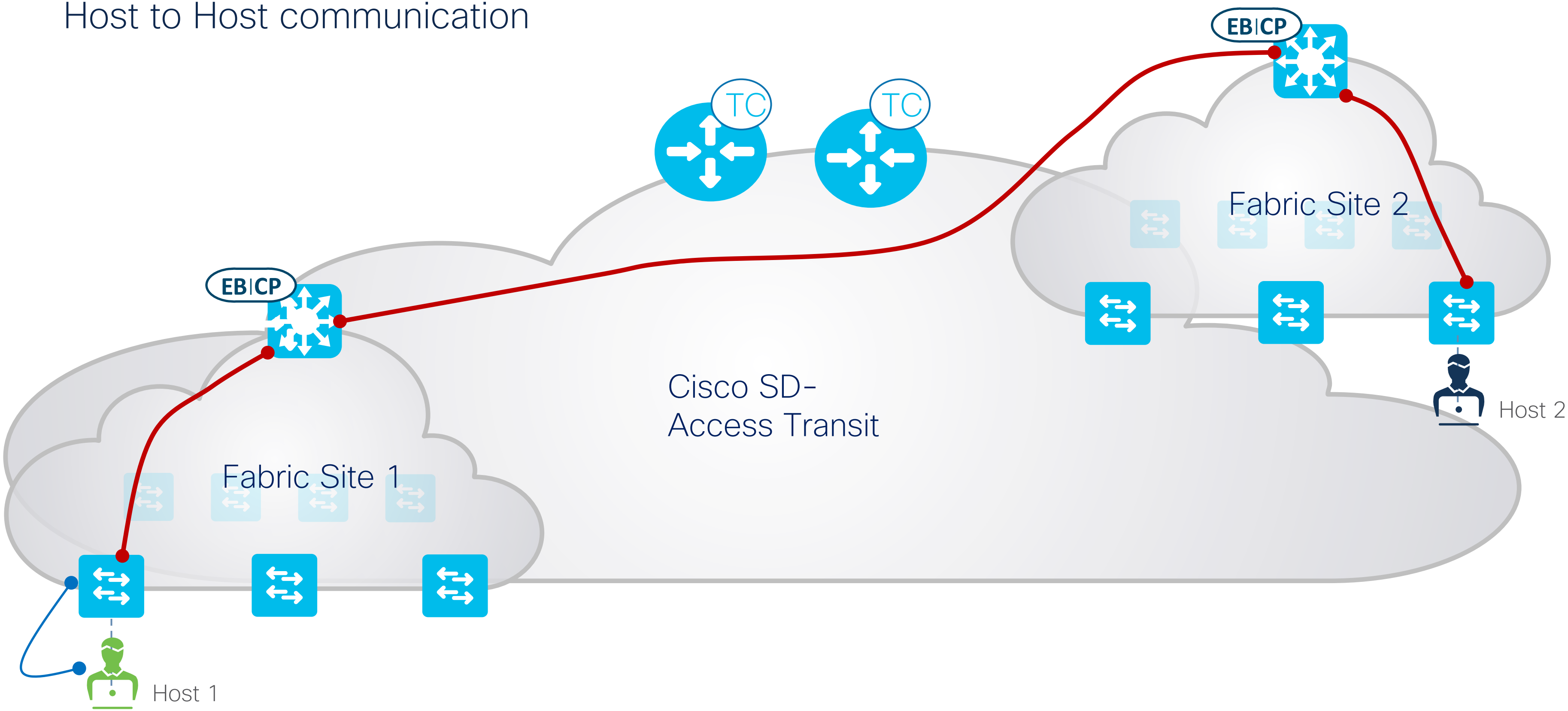
Host to Host communication



The Border Node in Fabric Site 2 will receive the mapping information from the local Control Plane Node with the destination address of the Edge Node in Fabric Site 2

SD-Access Transit Forwarding with LISP Pub/Sub

Host to Host communication

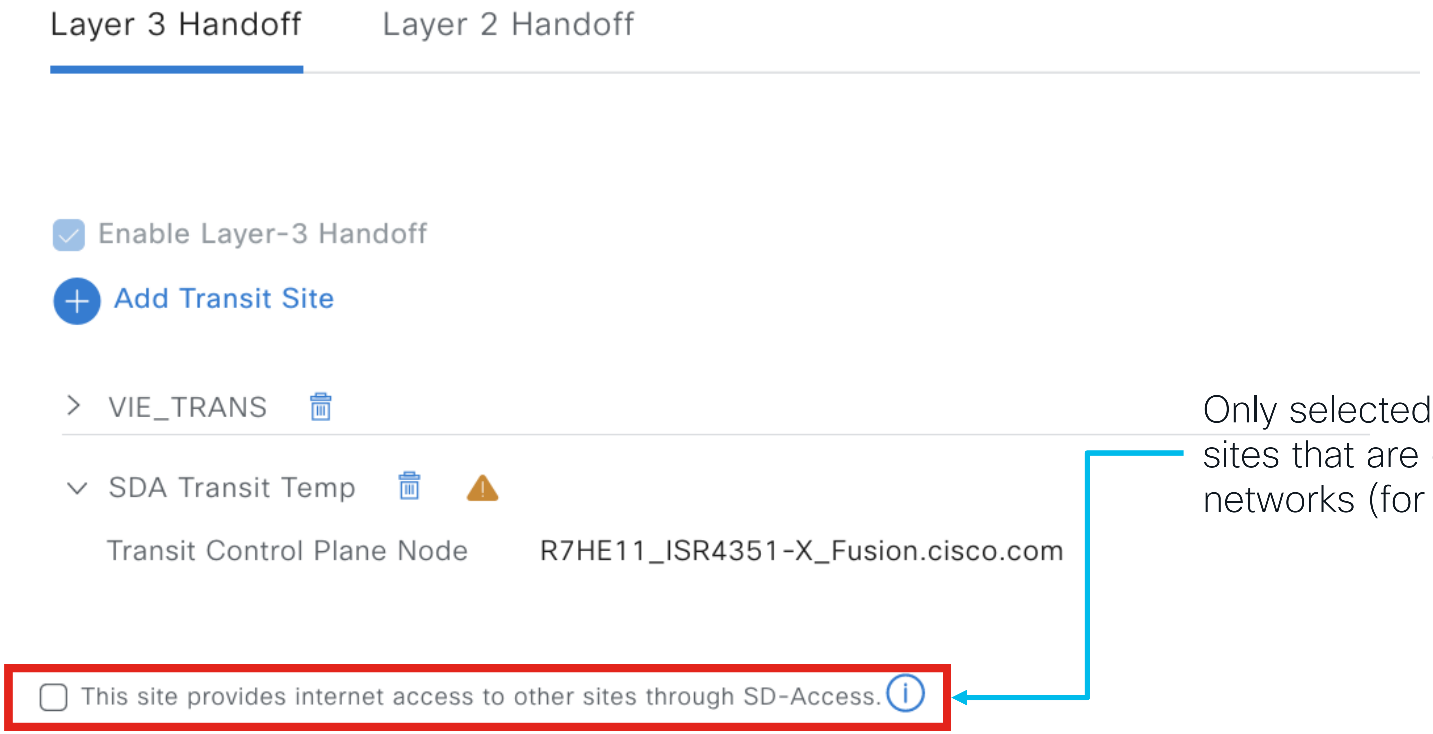


Traffic is forwarded from fabric border node in fabric site 2 to the fabric edge node in fabric site 2 using VXLAN encap with SGT tags encoded

SD-Access Transit Remote Internet with LISP Pub/Sub

SD-Access Transit Remote Internet with LISP Pub/Sub

Designating the Border(s) Connected to the Internet



Layer 3 Handoff | Layer 2 Handoff

☑ Enable Layer-3 Handoff

⊕ Add Transit Site

> VIE_TRANS

⌄ SDA Transit Temp

Transit Control Plane Node R7HE11_ISR4351-X_Fusion.cisco.com

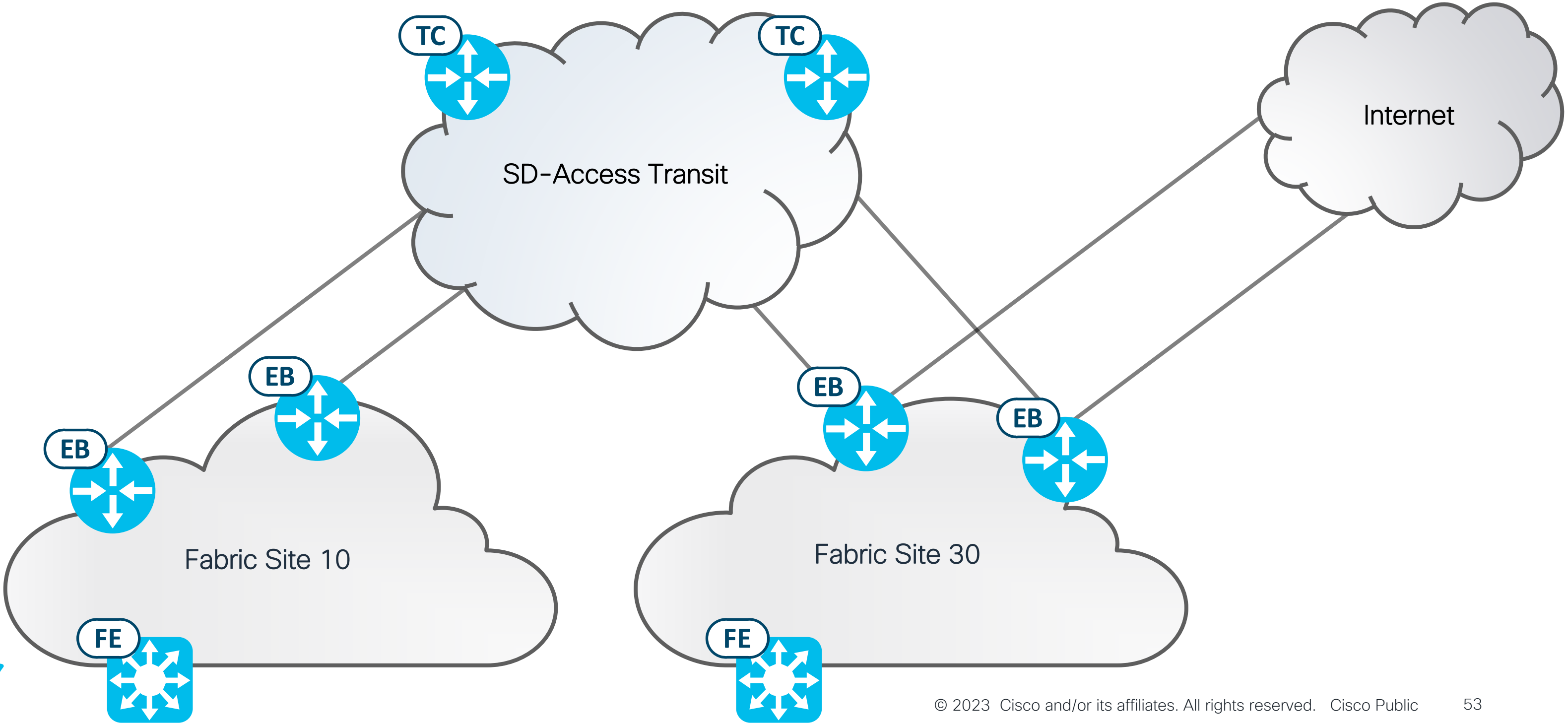
□ This site provides internet access to other sites through SD-Access. ⓘ

Only selected for SD-Access Transit sites that are connected to unknown networks (for example, Internet)

SD-Access Transit Remote Internet with LISP Pub/Sub

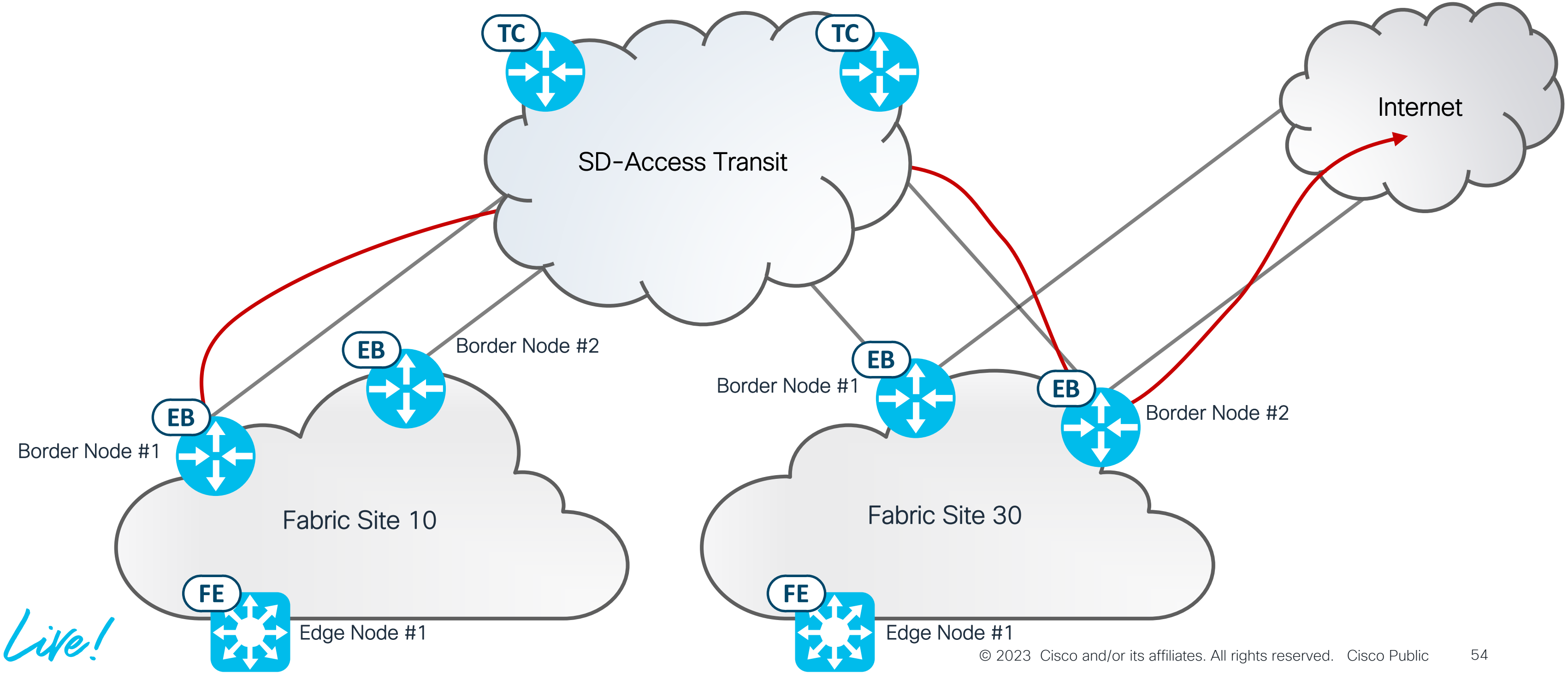
Topology and Description

- Two Fabric Sites connected to an SD-Access Transit.
- Fabric Site 30 local Internet.
- Fabric Site 30 is sharing Internet access with the deployment.



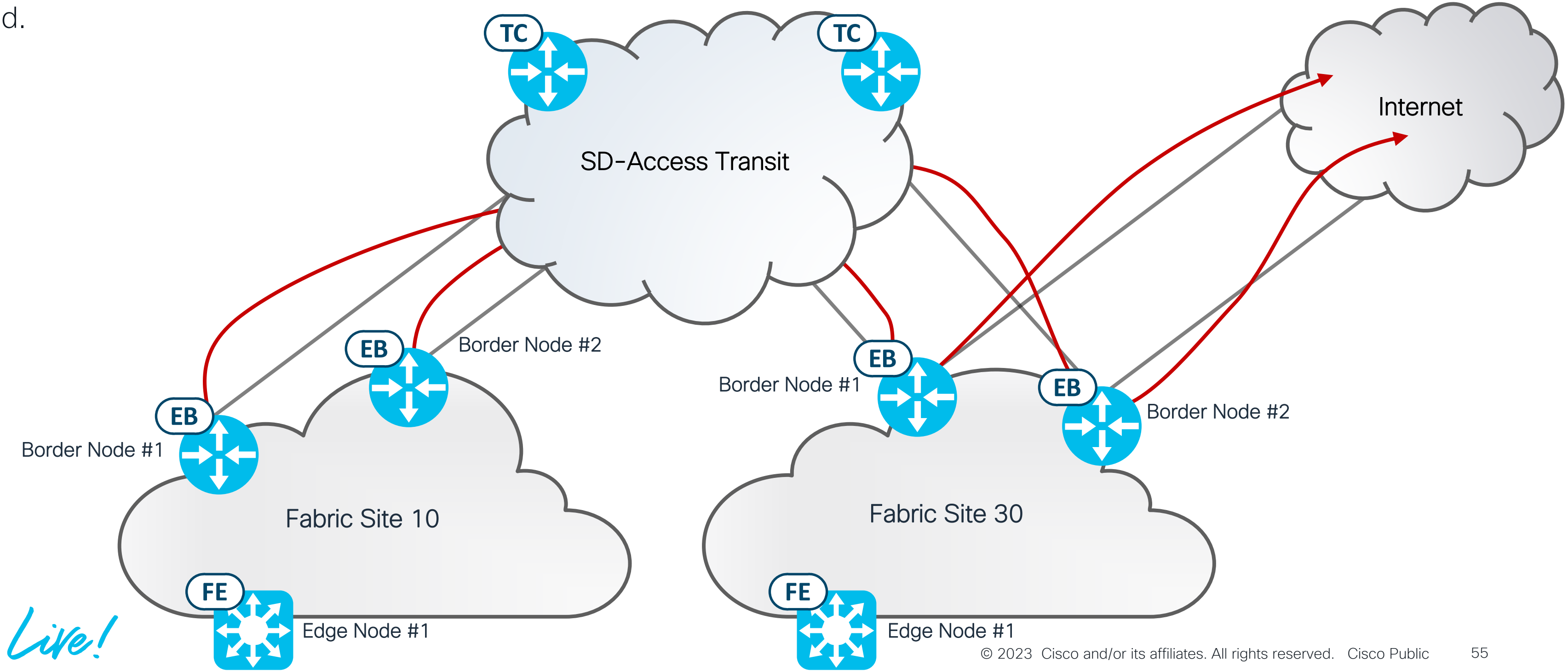
LISP Remote Internet with Border Convergence

- Border Node #1 uses Internet available through Fabric Site 30. Either of the Border Nodes in Fabric Site 30 will be used.



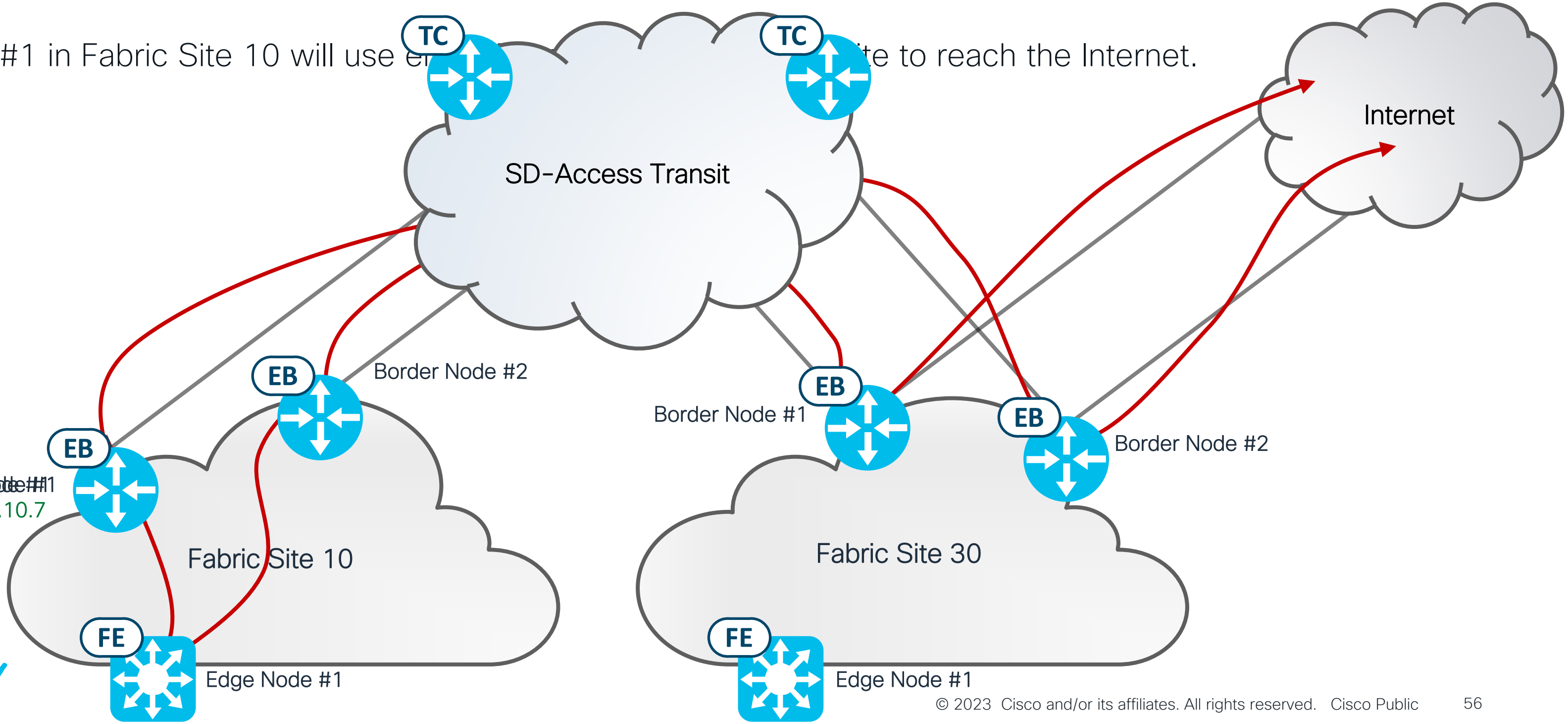
LISP Remote Internet with Border Convergence

- Border Node #1 uses Internet available through Fabric Site 30. Either of the Border Nodes in Fabric Site 30 will be used.
- Border Node #2 uses Internet available through Fabric Site 30. Either of the Border Nodes in Fabric Site 30 will be used.



LISP Remote Internet with Border Convergence

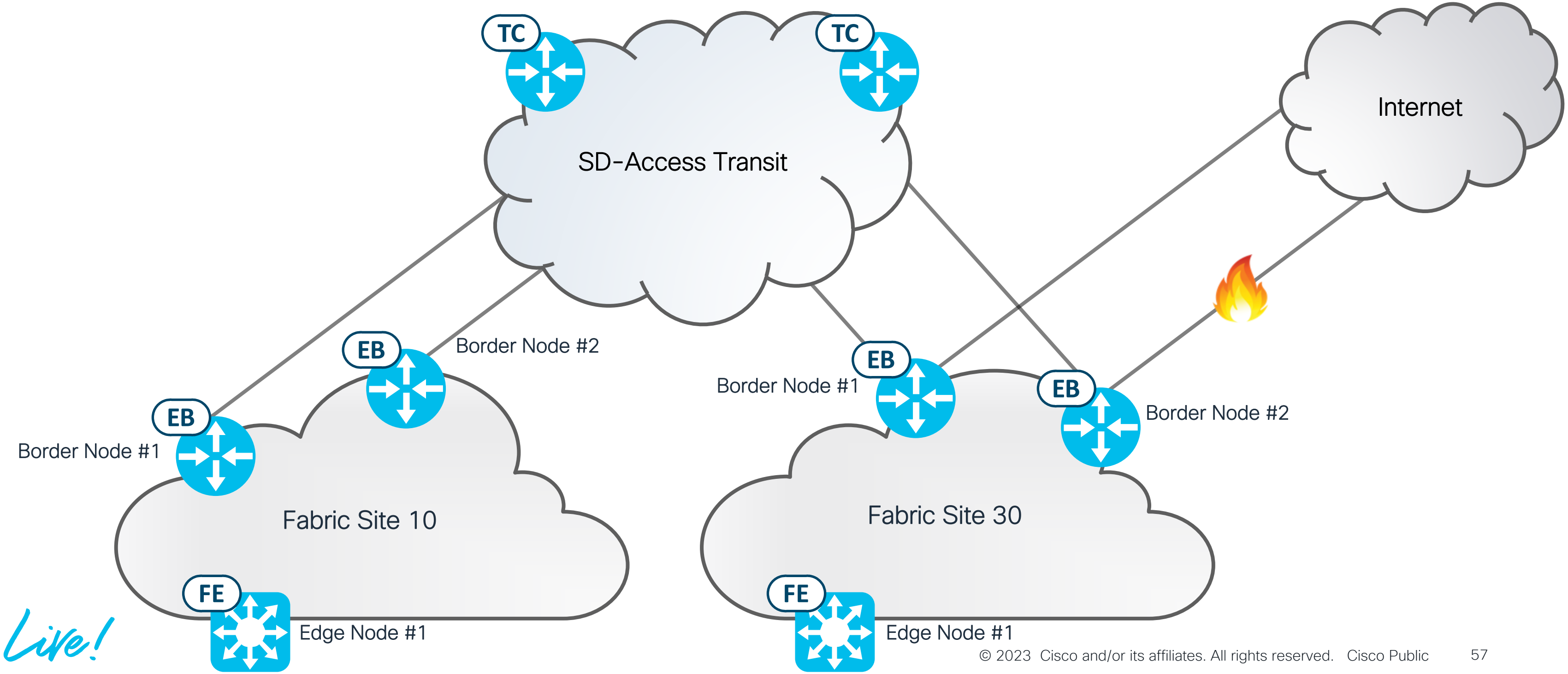
- Border Node #1 uses Internet available through Fabric Site 30. Either of the Border Nodes in Fabric Site 30 will be used.
- Border Node #2 uses Internet available through Fabric Site 30. Either of the Border Node in Fabric Site 30 will be used.
- Edge Node #1 in Fabric Site 10 will use ei te to reach the Internet.



cisco Live!

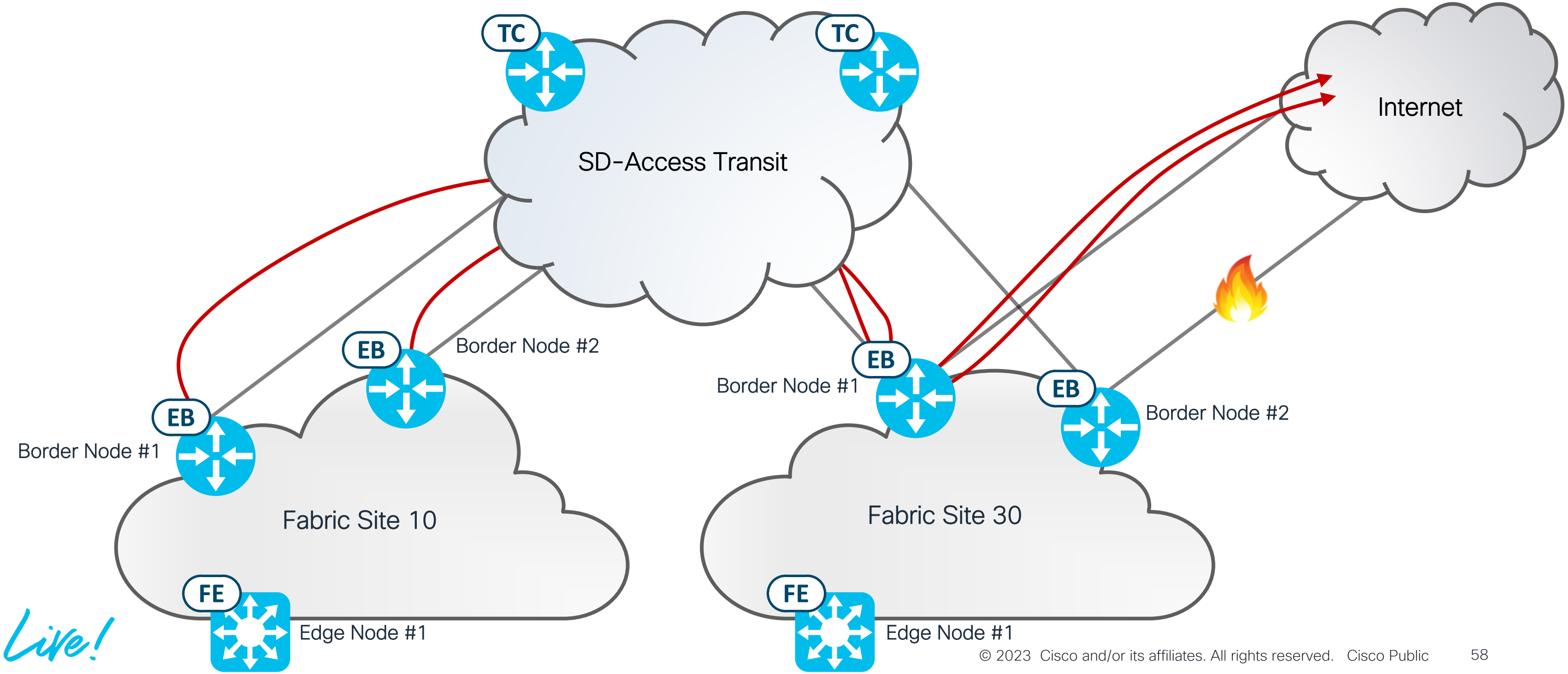
LISP Remote Internet with Border Convergence

- Border Node #2 in Fabric Site 30 loses the default route.



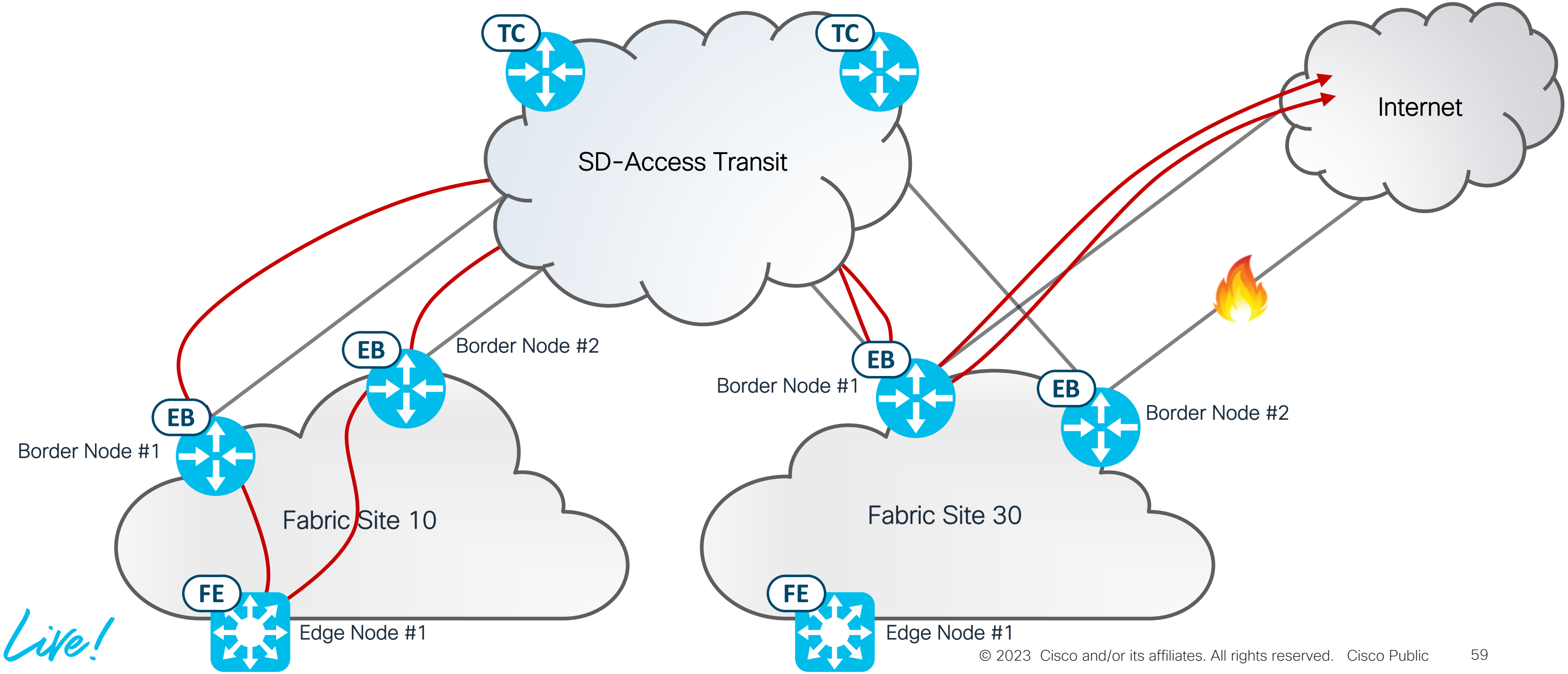
LISP Remote Internet with Border Convergence

- Both Border Nodes in Fabric Site 10 will use Border Node #1 in Fabric Site 30 to reach the Internet.



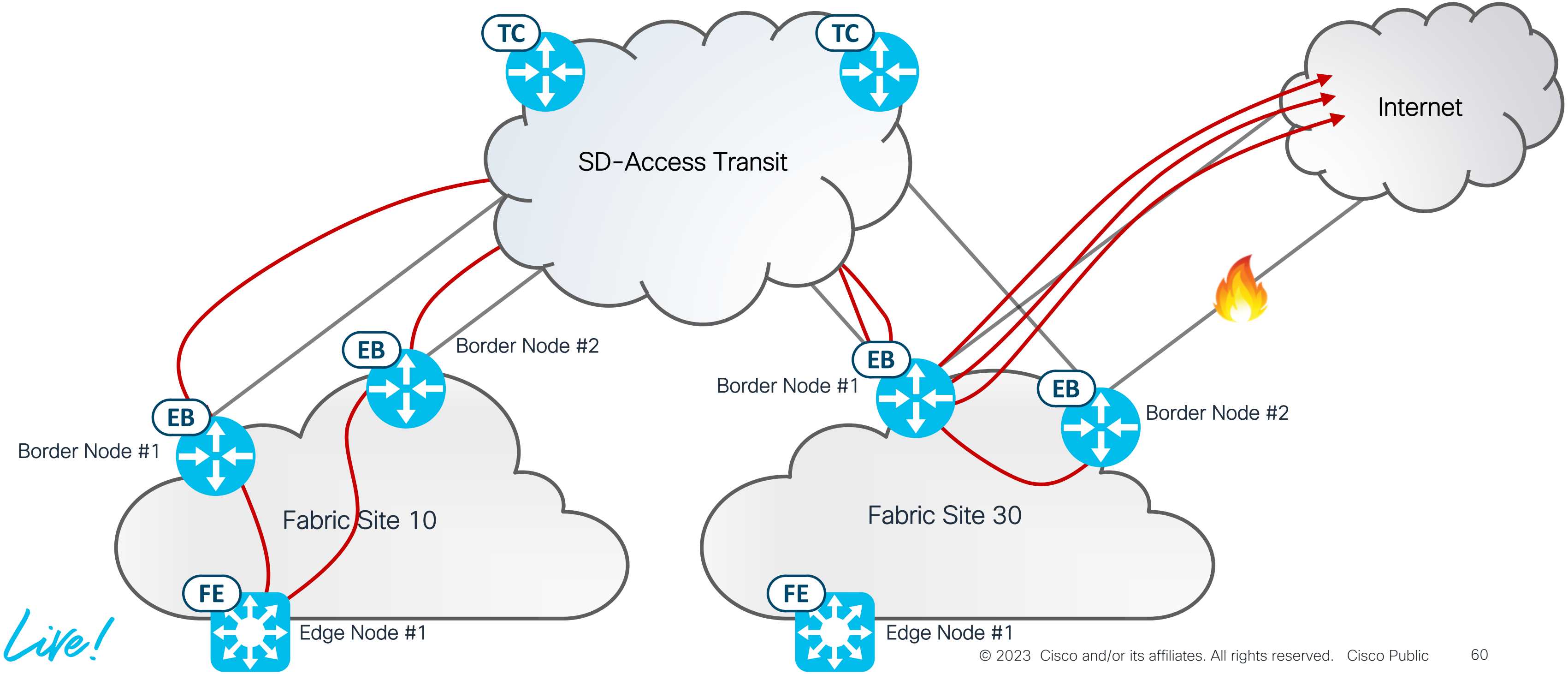
LISP Remote Internet with Border Convergence

- Edge Node #1 in Fabric Site 10 will continue to use either site-local Border Node to reach the Internet.



LISP Remote Internet with Border Convergence

- Border Node #2 in Fabric Site 30 will use Border Node #1 in Fabric Site 30 to reach the Internet.

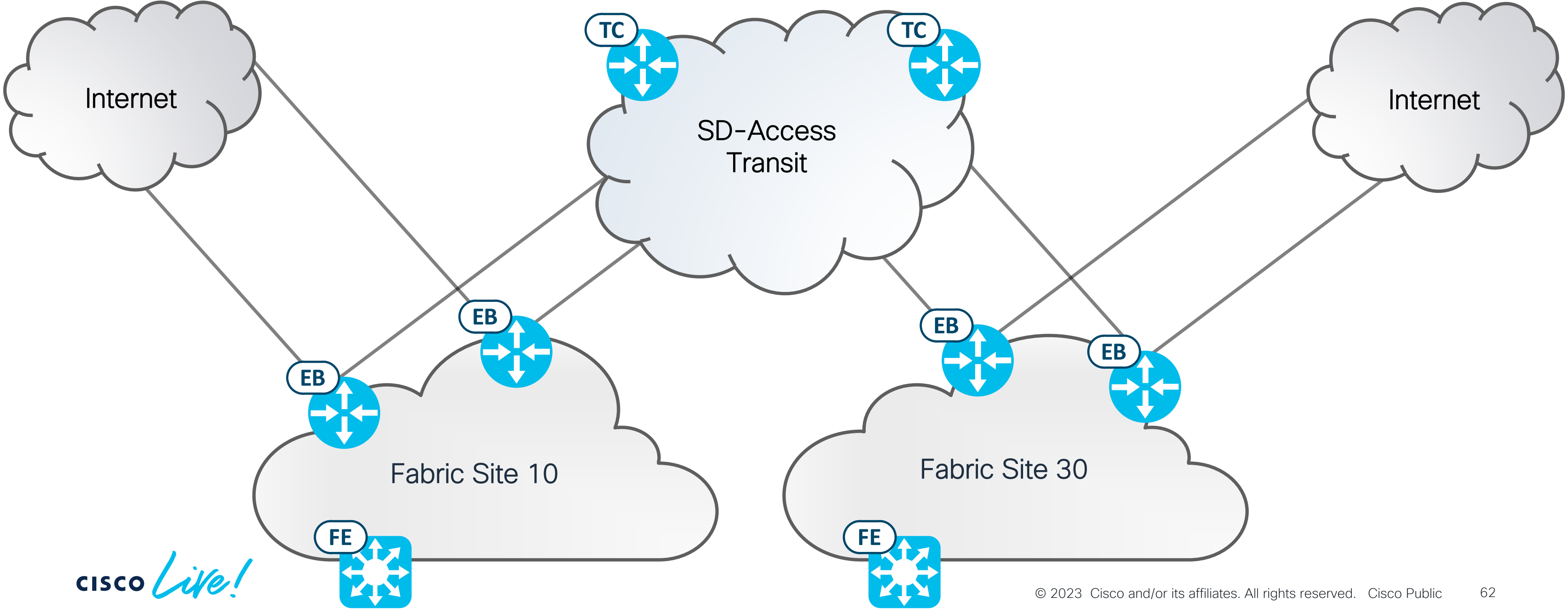


SD-Access Transit Backup Internet Access with LISP Pub/Sub

LISP Backup Internet with Border Convergence

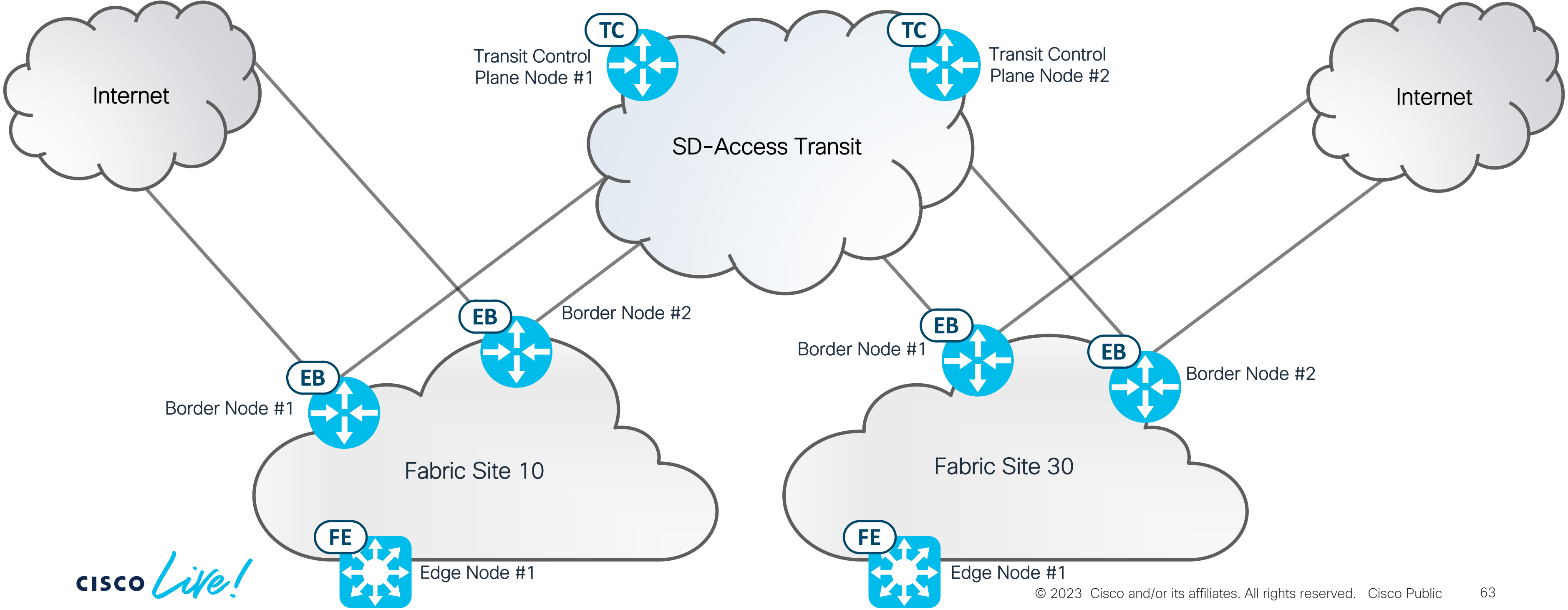
Topology and Description

- Two Fabric Sites connected to an SD-Access Transit.
- Both Fabric Sites have local Internet.
- Both Sites are sharing Internet access.



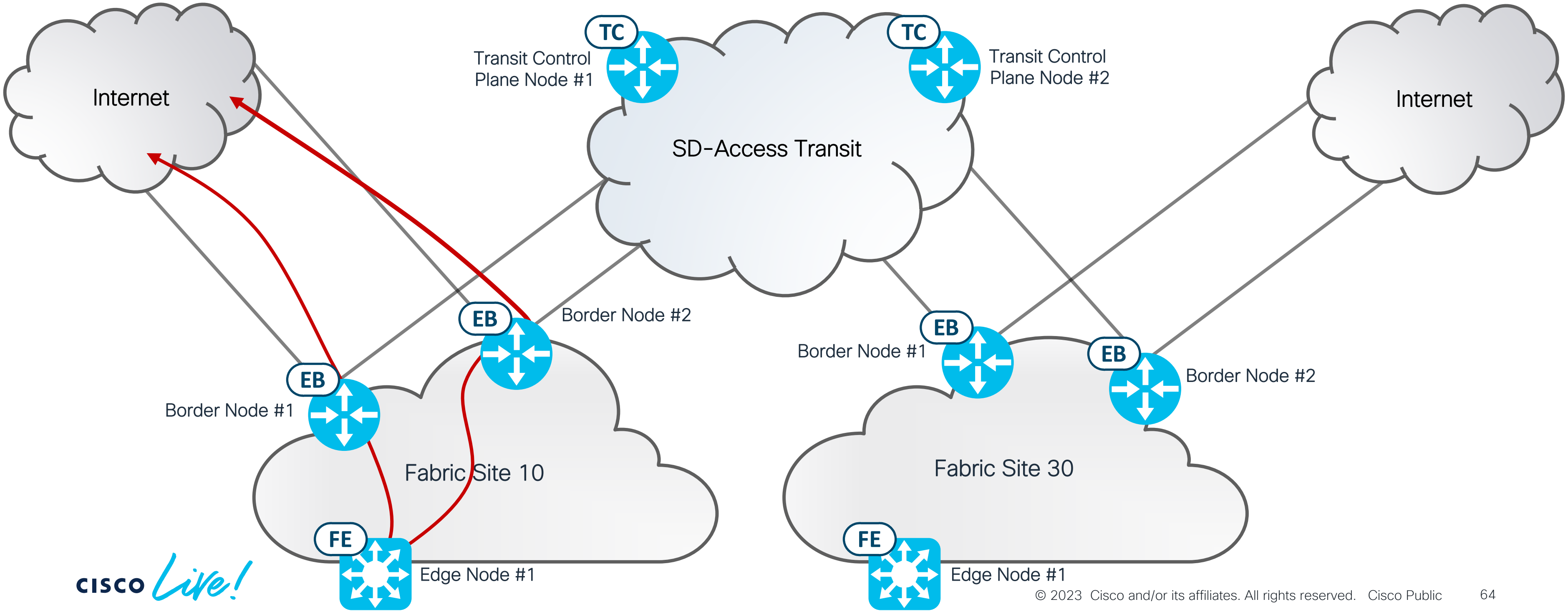
LISP Backup Internet with Border Convergence

- Two Fabric Sites connected to an SD-Access Transit.
- Both Fabric Sites have local Internet.
- Both Sites are sharing Internet access.



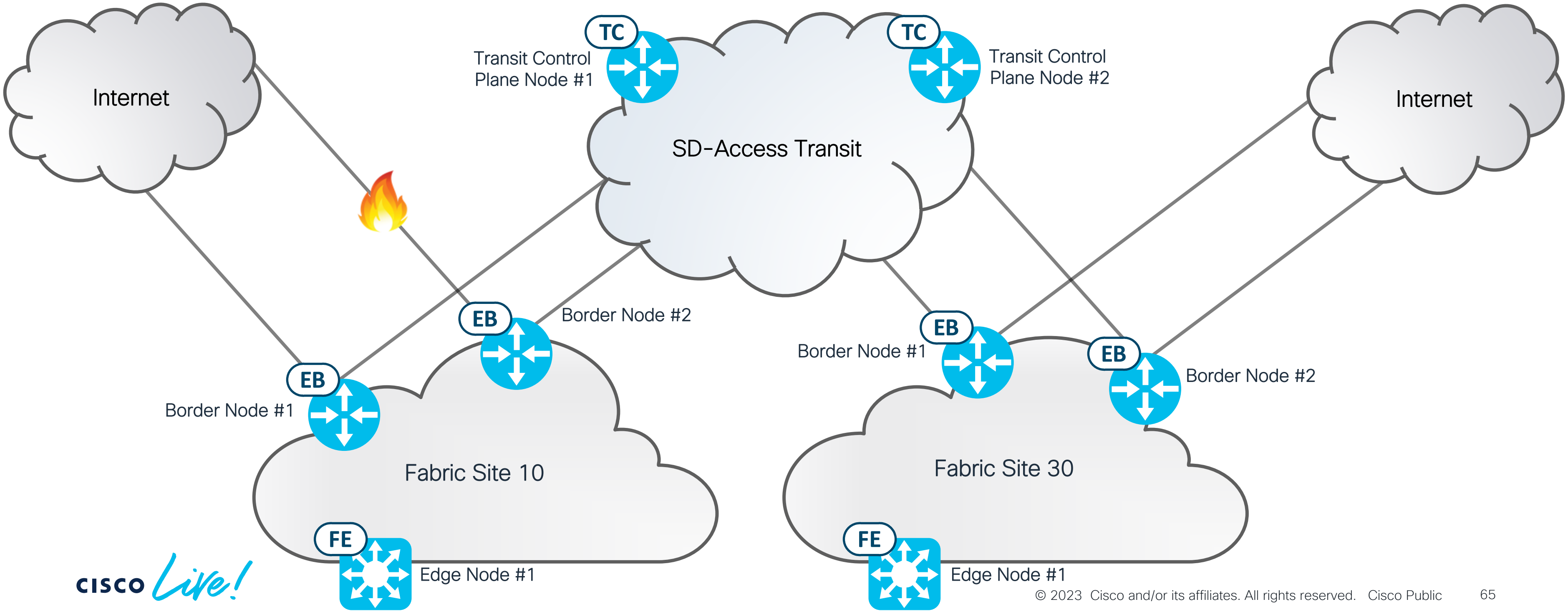
LISP Backup Internet with Border Convergence

- Edge Node #1 will initially use either site-local Border Node to reach the Internet.



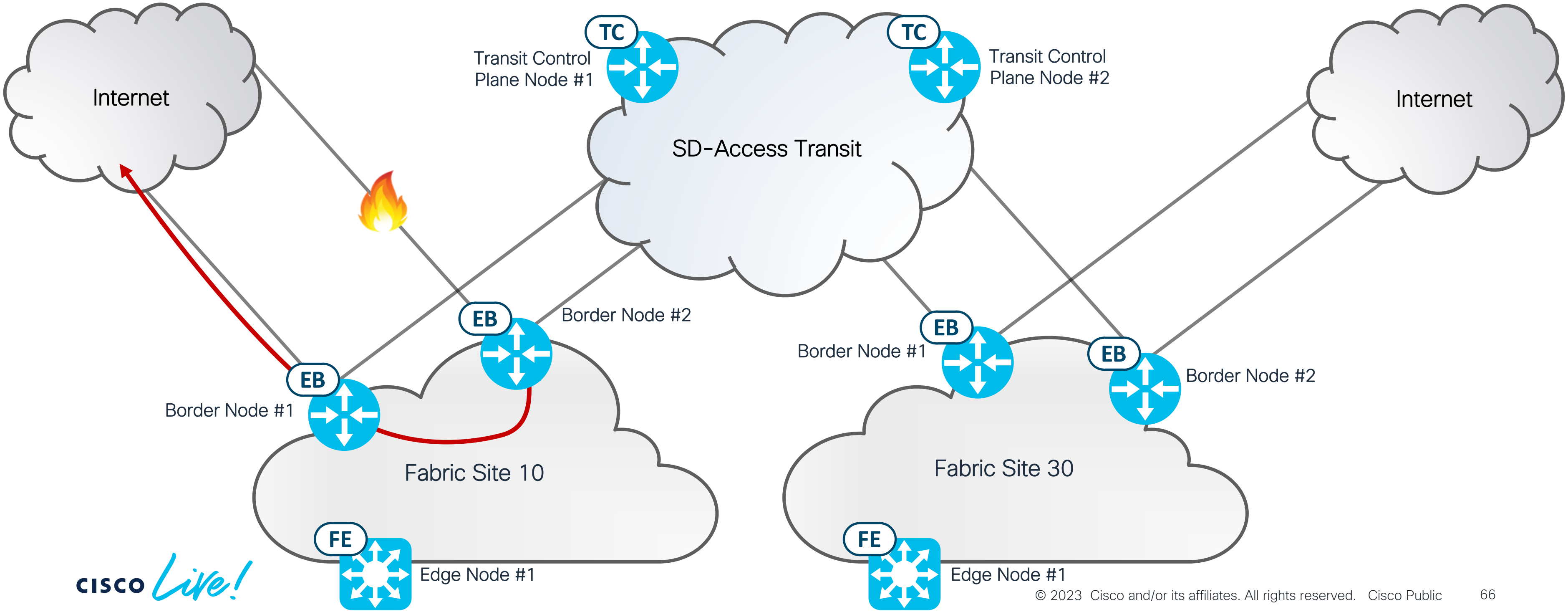
LISP Backup Internet with Border Convergence

- Border Node #2 in Fabric Site 10 loses the default route.



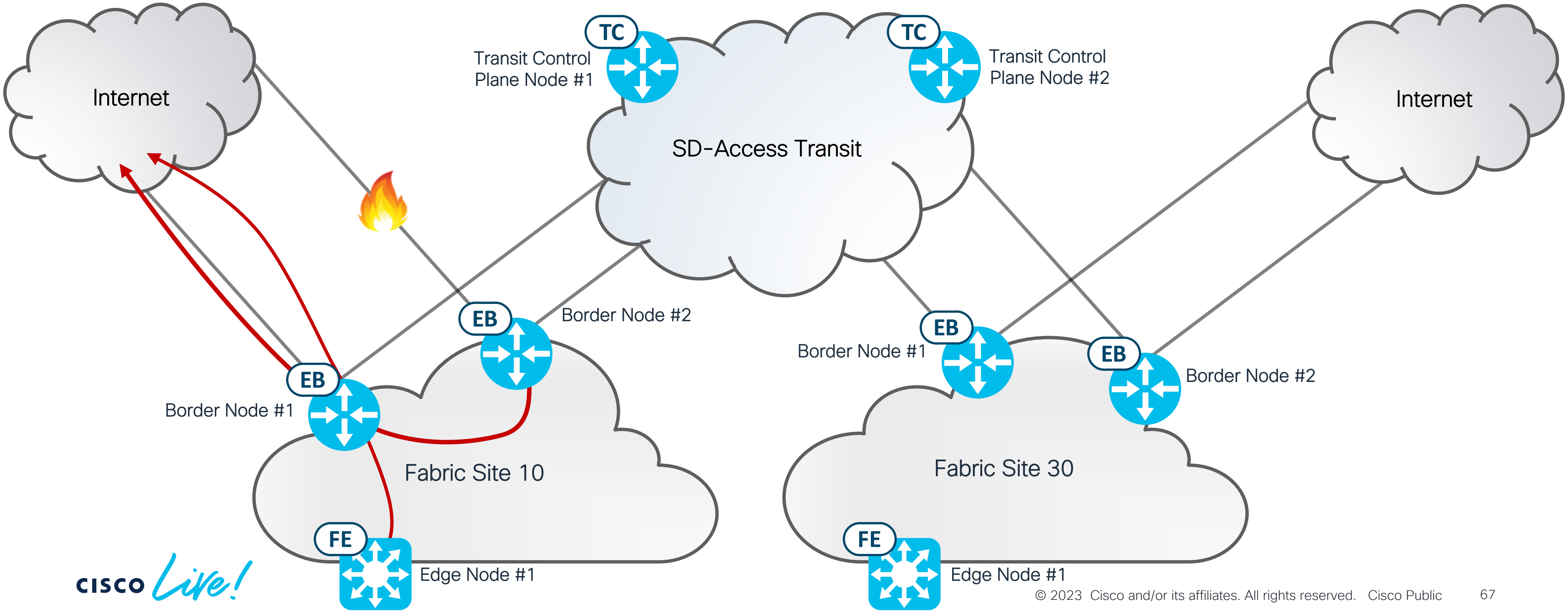
LISP Backup Internet with Border Convergence

- Border Node #2 will use Border Node #1 in Fabric Site 10 to reach the Internet.



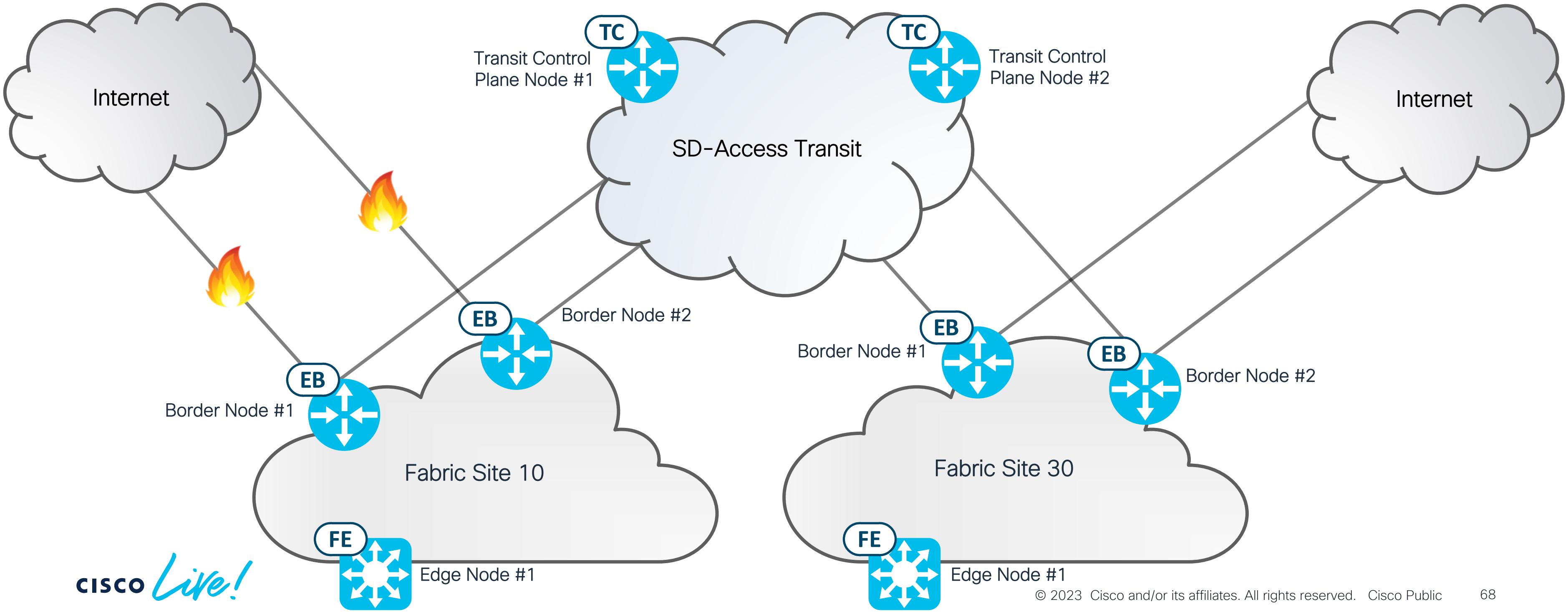
LISP Backup Internet with Border Convergence

- Edge Node #1 will only use Border Node #1 in in Fabric Site 10 to reach the Internet.



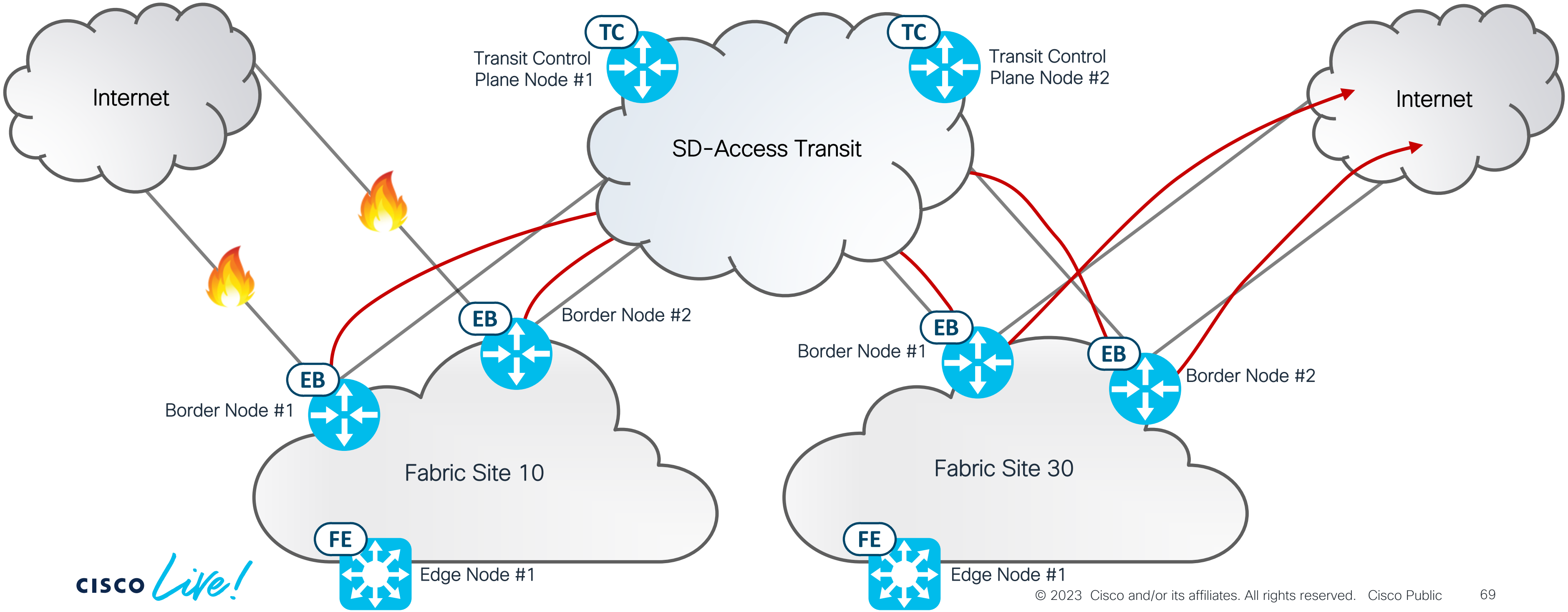
LISP Backup Internet with Border Convergence

- Border Node #2 in Fabric Site 10 loses the default route.
- Border Node #1 in Fabric Site 10 also loses the default route.



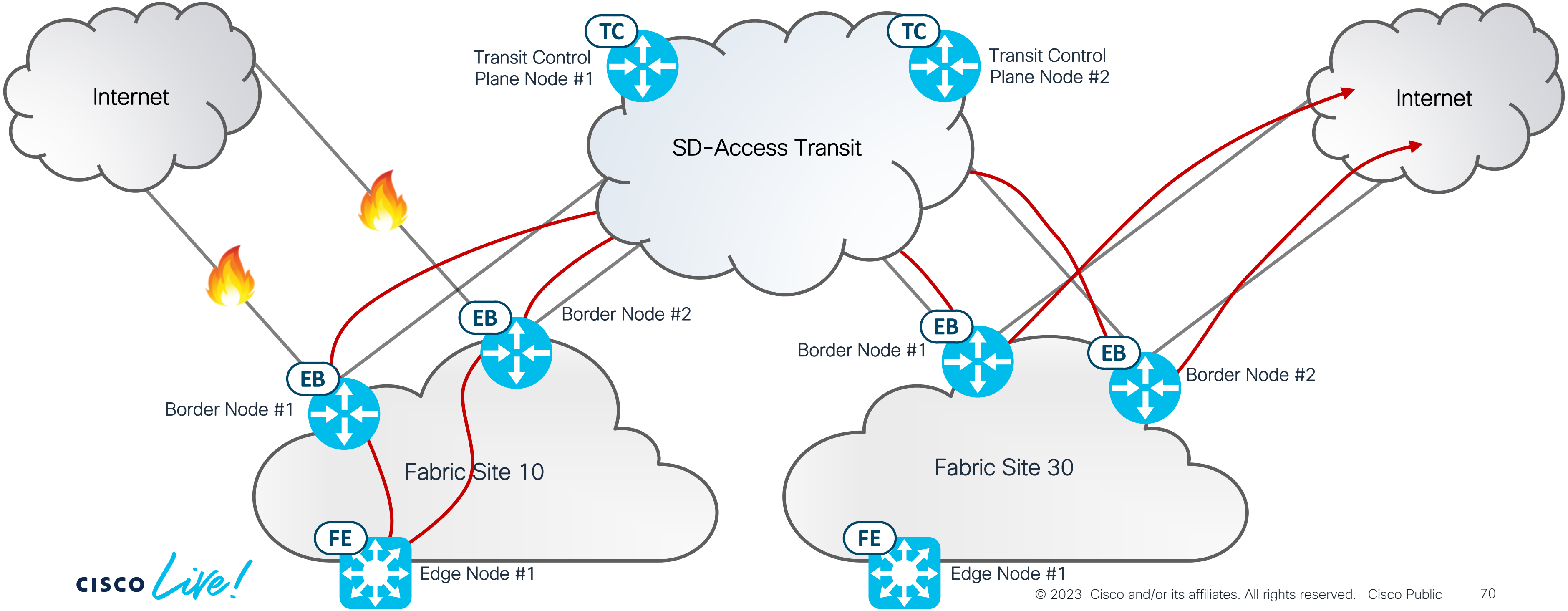
LISP Backup Internet with Border Convergence

- The Border Nodes in Fabric Site 10 will use the Border Nodes in Site 30 for Internet Access.
- Either of the Border Nodes in Fabric Site 30 will be used.



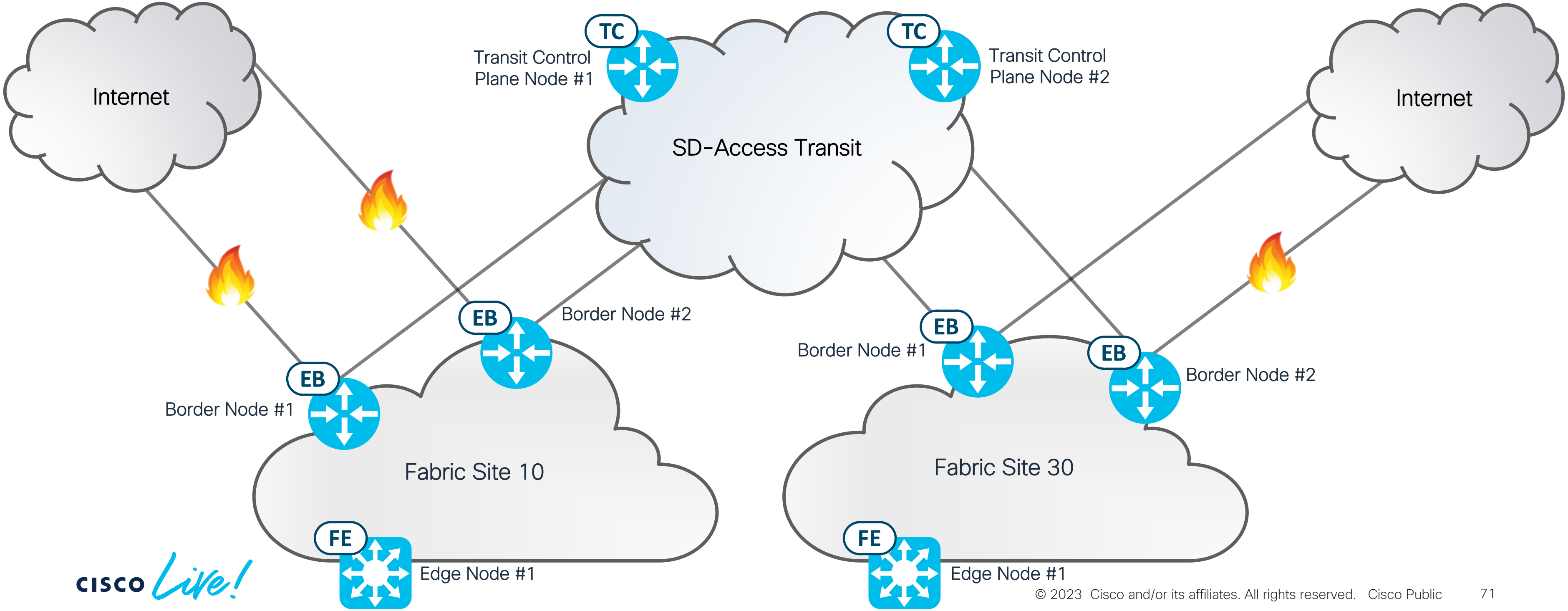
LISP Backup Internet with Border Convergence

- Edge Node #1 in Fabric Site 10 will both site-local Border Nodes for Internet Access.



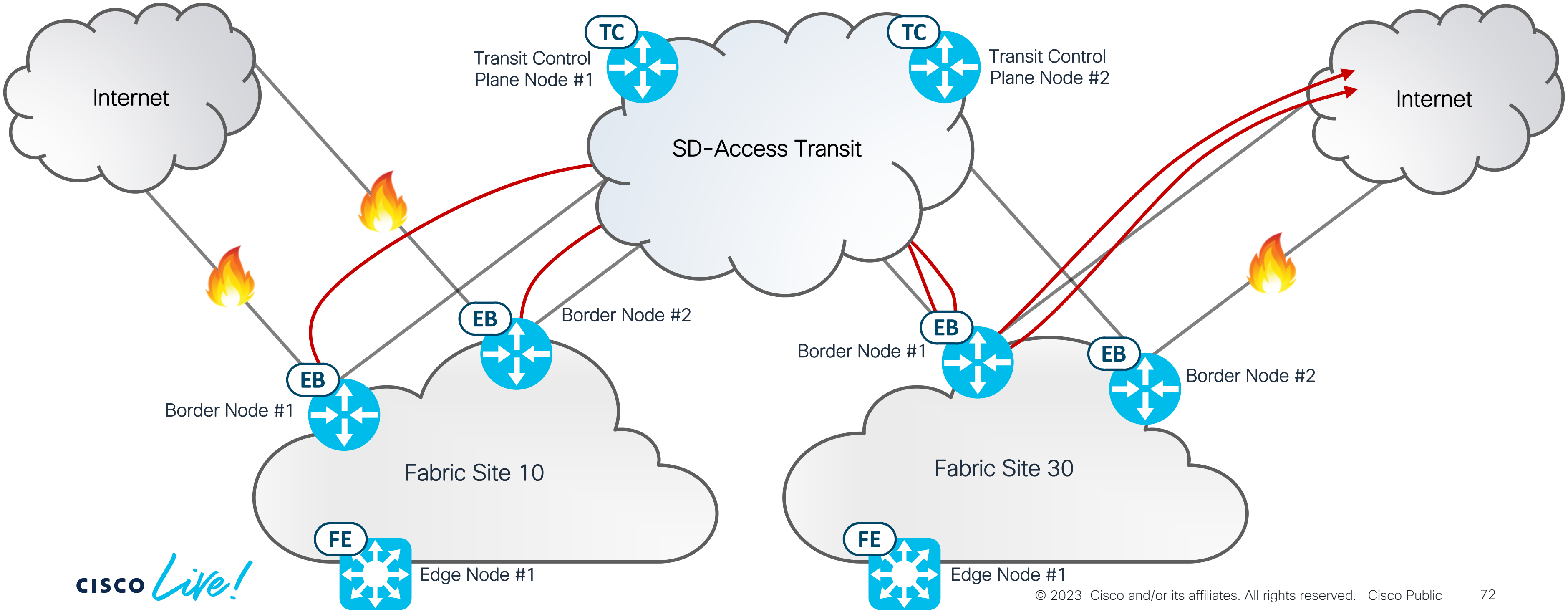
LISP Backup Internet with Border Convergence

- Border Node #2 in Fabric Site 30 loses the default route.



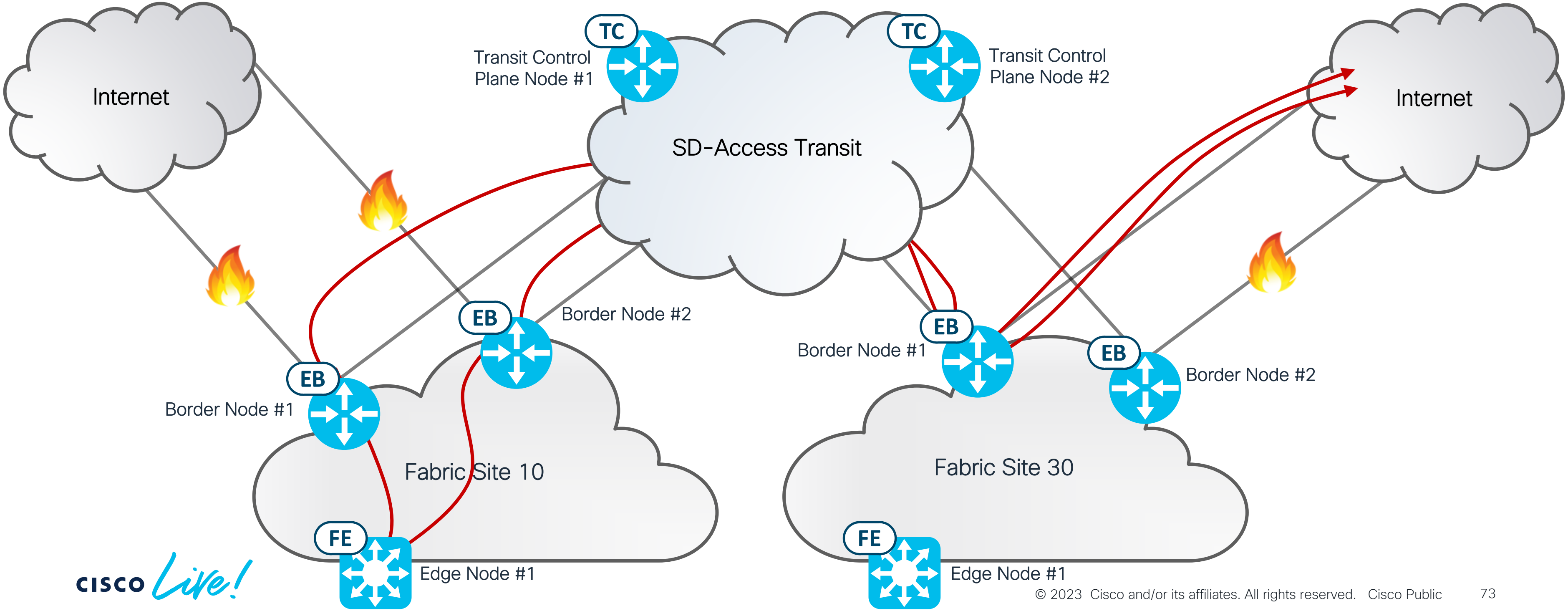
LISP Backup Internet with Border Convergence

- Border Nodes in Fabric Site 10 will use Border Node #1 in Fabric Site 30 to reach the Internet.



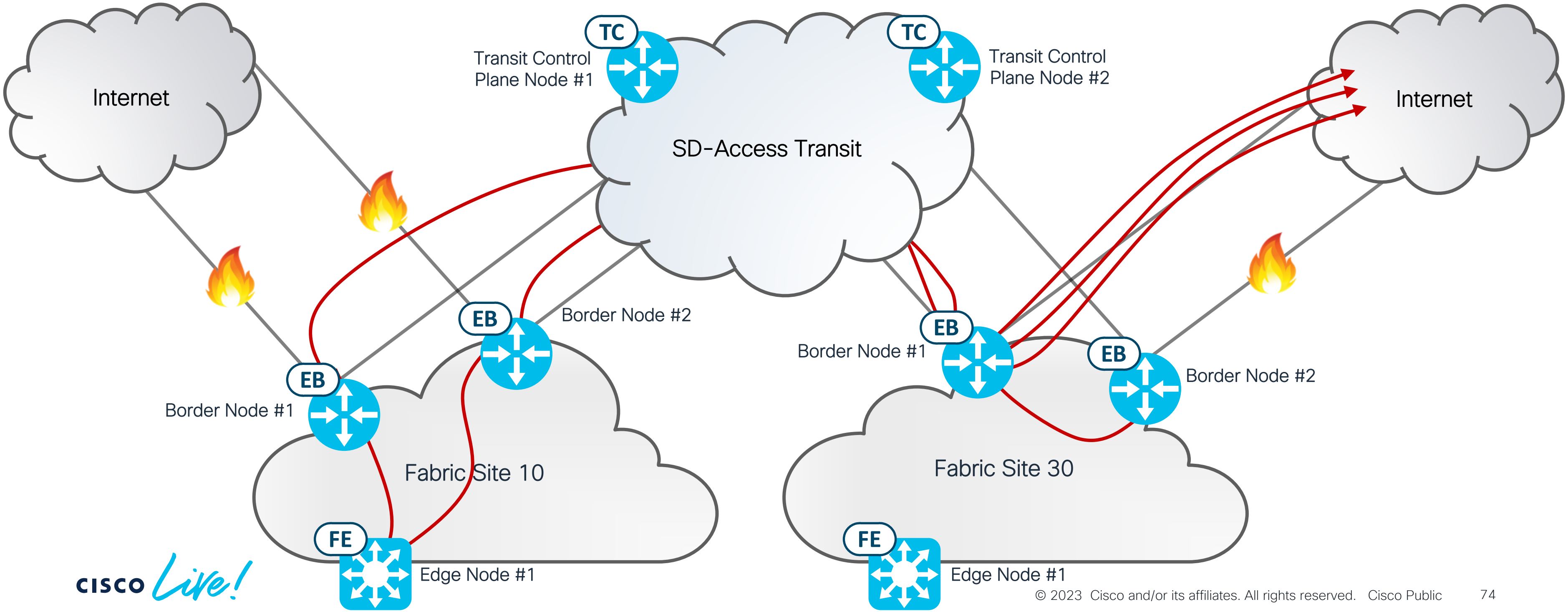
LISP Backup Internet with Border Convergence

- Edge Node #1 in Fabric Site 10 will continue to use either site-local Border Node to reach the Internet.



LISP Backup Internet with Border Convergence

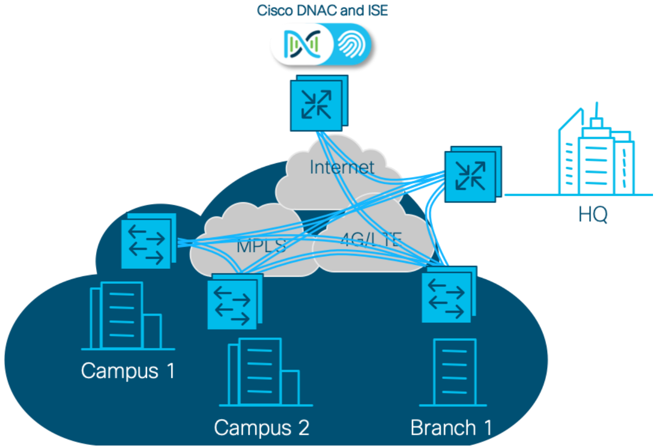
- Border Node #2 in Fabric Site 30 will use Border Node #1 in Fabric Site 30 to reach the Internet.

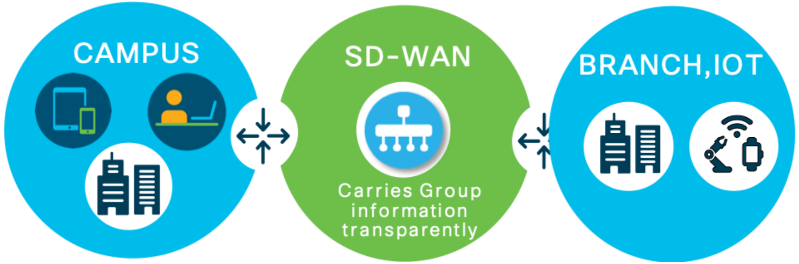


Summary

Summary

Cisco SD-Access Multi-Site fabric





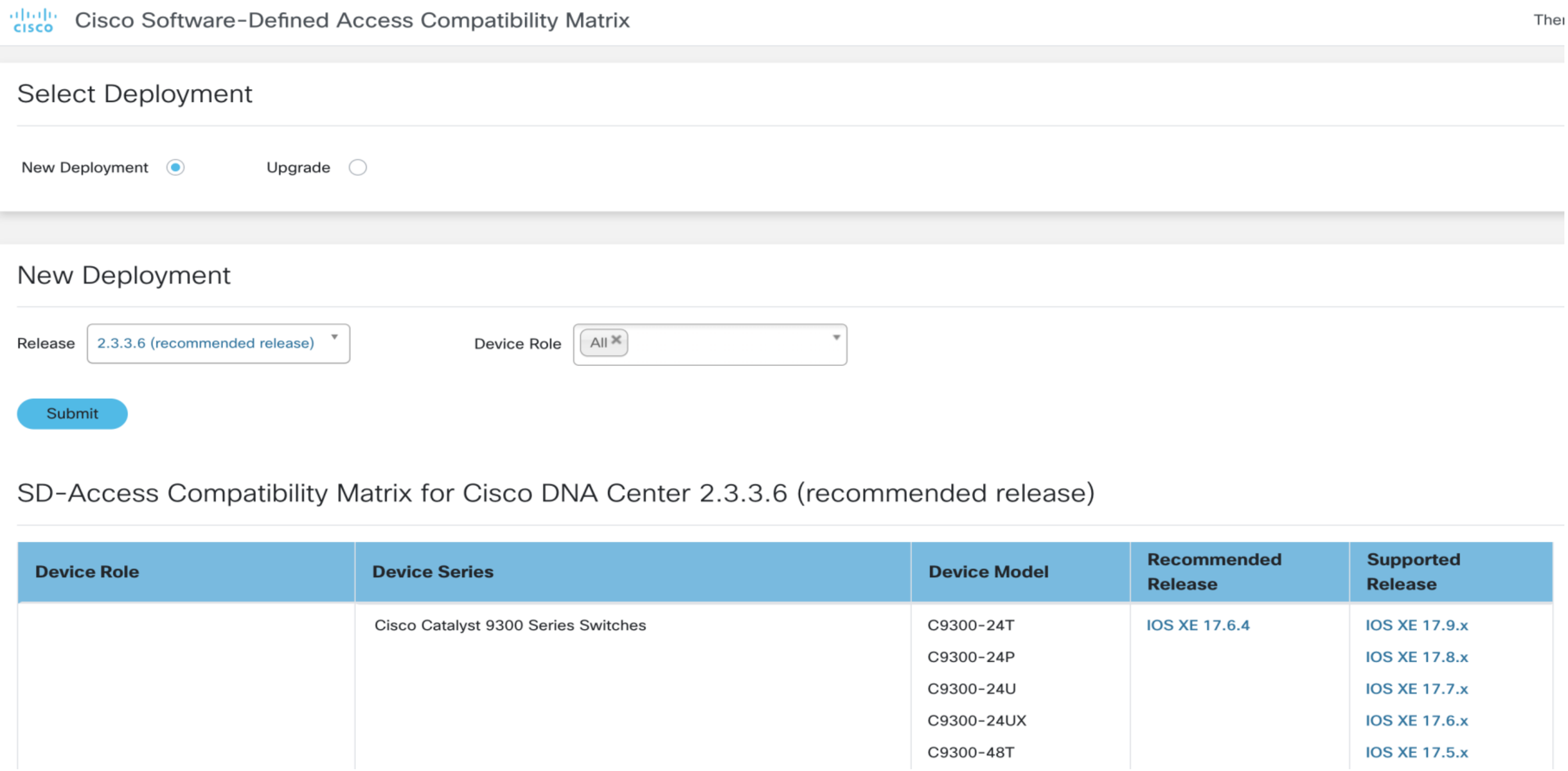
- ✓ Automated Inter-Site Connectivity
- ✓ E2E Segmentation, Policy and Assurance
- ✓ Flexible and Scalable

- ✓ LISP Pub/Sub Enhanced Capabilities
- ✓ Flexible Group to VPN Mapping
- ✓ Flexible WAN options

For more details: cs.co/sda-compatibility-matrix

SD-Access Support

Digital Platforms for your Cisco Digital Network Architecture



Cisco Software-Defined Access Compatibility Matrix

Thei

Select Deployment

New Deployment ● Upgrade ○

New Deployment

Release: 2.3.3.6 (recommended release)

Device Role: All ×

SD-Access Compatibility Matrix for Cisco DNA Center 2.3.3.6 (recommended release)

Device Role	Device Series	Device Model	Recommended Release	Supported Release
	Cisco Catalyst 9300 Series Switches	C9300-24T C9300-24P C9300-24U C9300-24UX C9300-48T	IOS XE 17.6.4	IOS XE 17.9.x IOS XE 17.8.x IOS XE 17.7.x IOS XE 17.6.x IOS XE 17.5.x

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.

- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard” at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

cisco The bridge to possible

Thank you

cisco Live!

cisco Live!