Let's go

The bridge to possible

Learning DCN Solutions with Real-World Cases

BGP EVPN VXLAN w/ NDFC
Security(MACSEC, CLOUDSEC)
Nexus Data Broker

Kyuhyun(Kai) Lim, Technical Solutions Architect
@CCIE55998

BRKDCN-2505

Who am I?

CCIE#55998

- 6 Years @ Cisco systems (2 Years @ Internet Service Provider)
- Responsible for DC Network (Nexus, MDS)
- Covered : Public, Commercial and Enterprise (Finance, Manufacture) customer
- Covering : Largest global customer (Manufacture and CSP)
- Trying to make proposal depending on requirement and situation from Customer

Session goal

- Various technical situation from various industry
- Sharing resolution w/ Cisco DC Network product

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Webex App

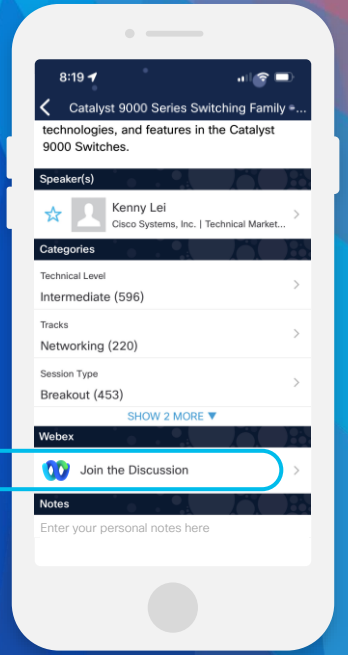
Questions?

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 December 22, 2023.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKDCN-2505

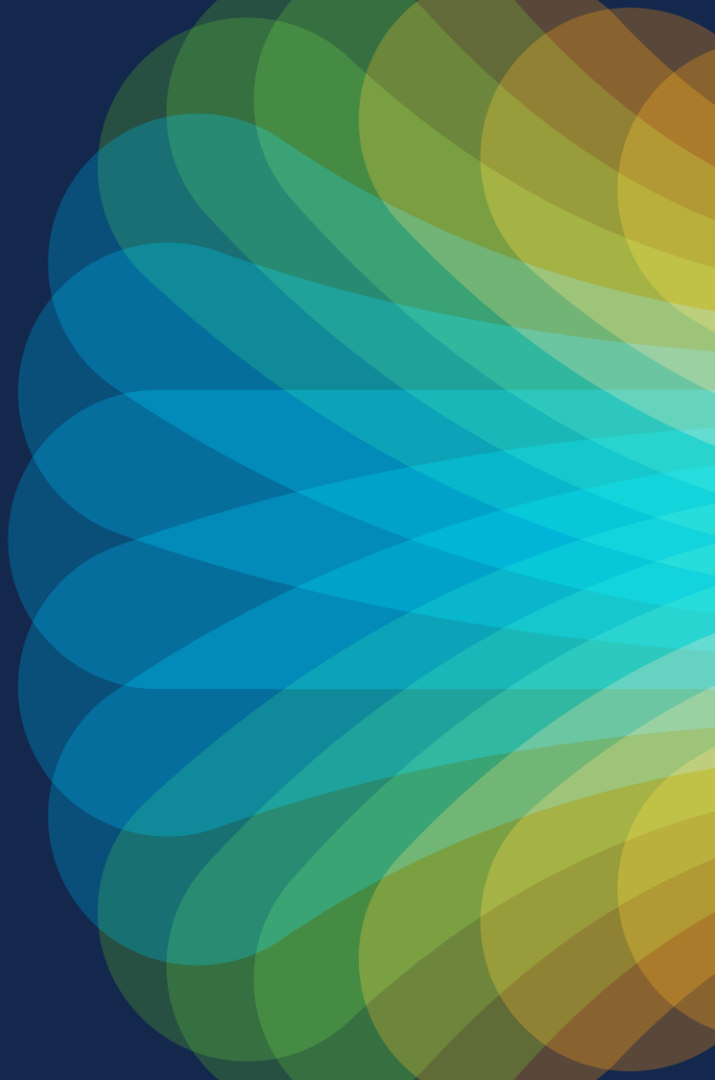
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

- Nexus Dashboard for Data Center Operation
- How to use VXLAN EVPN and NDFC?
- How to ensure secure communication between data centers?
- How to make money from your Network?
- Summary

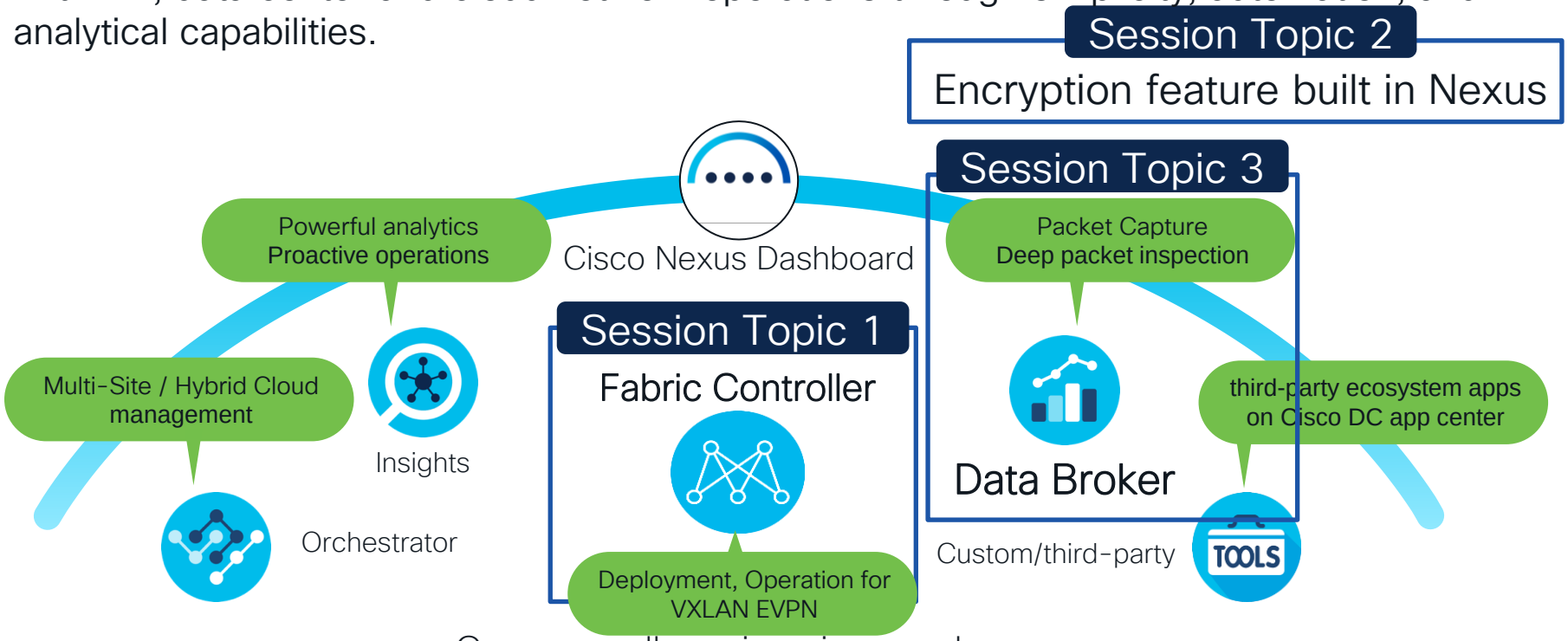
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Nexus Dashboard for Data Center operation



What is Nexus Dashboard?

With ND, data center and cloud network operations through simplicity, automation, and analytical capabilities.

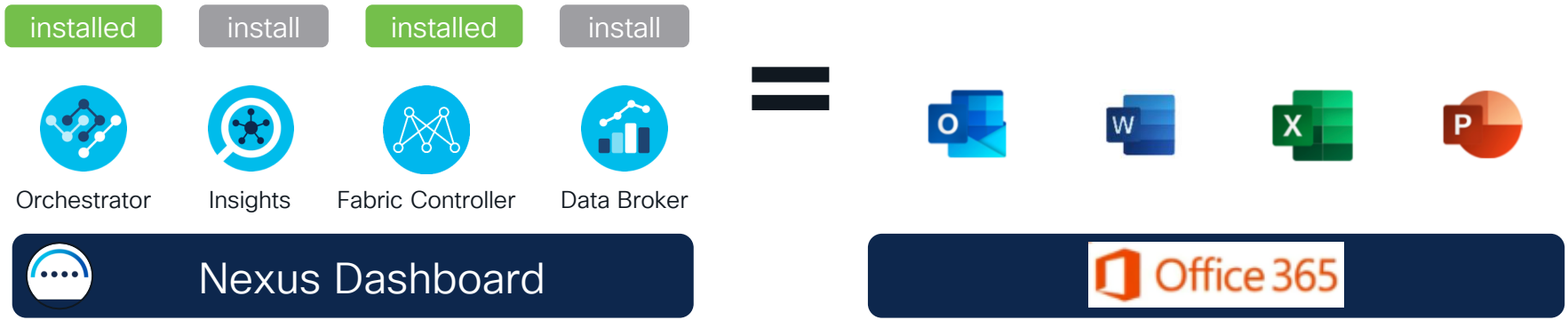


Consume all services in one place

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Nexus Dashboard hosts Apps for operations.

With ND, data center and cloud network operations through simplicity, automation, and analytical capabilities.



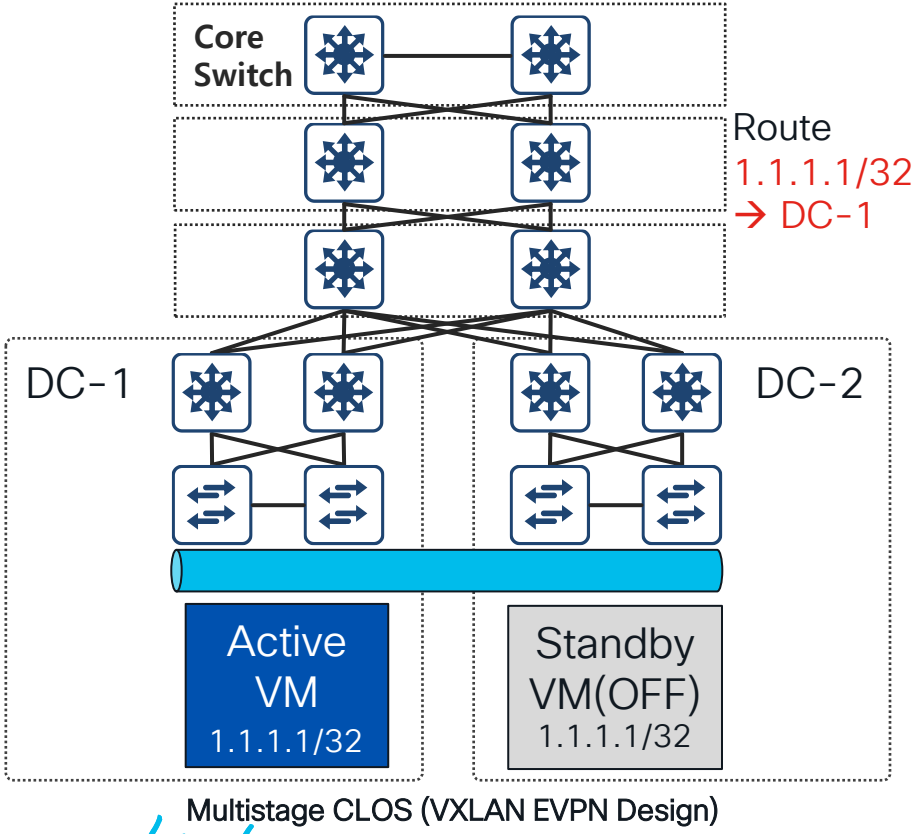
Nexus dashboard is the hosting Apps

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

How to use VXLAN EVPN and NDFC?

- Keep network service on any situation
- Separate network on shared network

Case 1-1. Requirement for fast disaster recovery

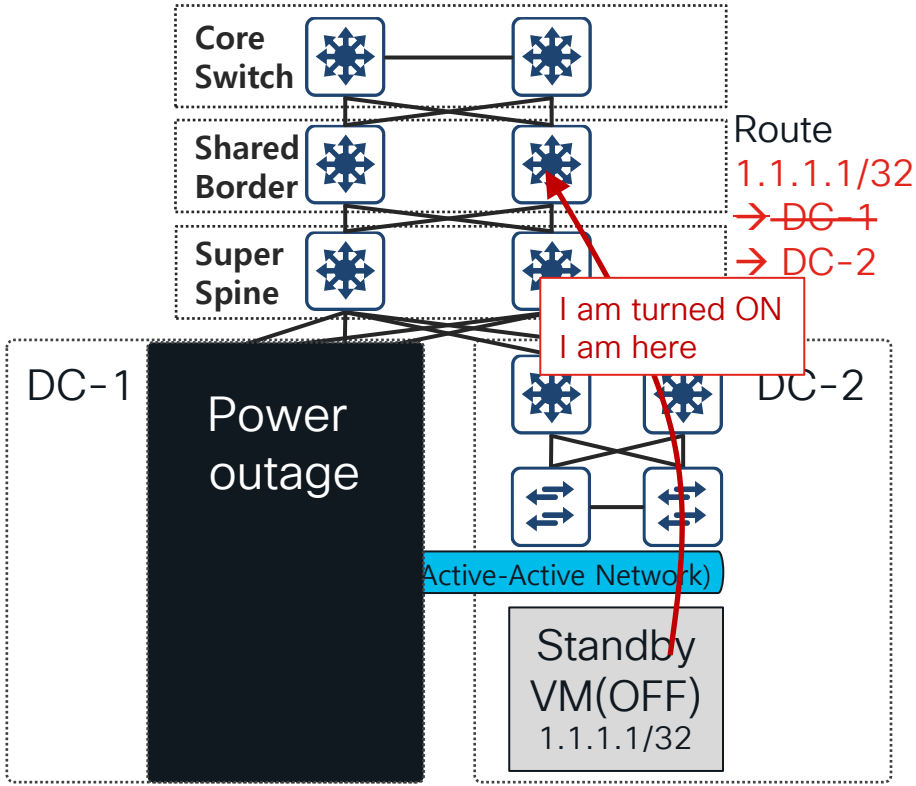


Requirement for fast disaster recovery

- Eliminating manual network configuration task during disaster
- Multiple Data Center within a campus
- Running important application
- Has enough space within campus
- Preparing additional surfaces to protect pause of application

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Case 1-2. Multi CLOS EVPN Design for fast recovery



What technical benefits in disaster situation?

- Provide automatic change of next-hop per particular end-point
- ARP used for type-2 information update

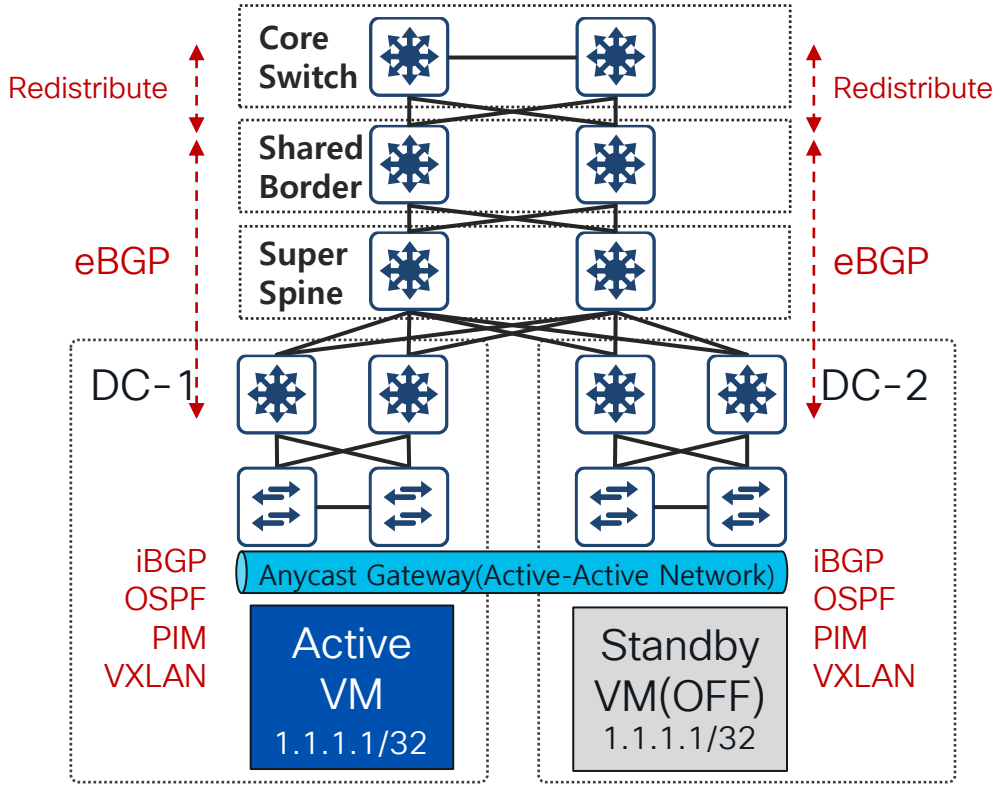
Advantages of Network operator

→ Just turn on power of Virtual Machine

- No network change tasks based on the changed location of the VM
- No need to change the IP of the VM

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Case 1-3. Considering automation of Multi CLOS



Considering multi protocol operation

- MP-iBGP for overlay of intra site
- MP-eBGP for overlay of inter site
- OSPF for Underlay of site intra
- Multicast, Ingress replication for flooding
- VXLAN to expand Layer 2 network

Needs automation

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Case 1-3. Considering automation w/ NDFC

Building Multi Fabric

Data Center VXLAN EVPN
Fabric for a VXLAN EVPN deployment with Nexus 9000 and 3000 switches.

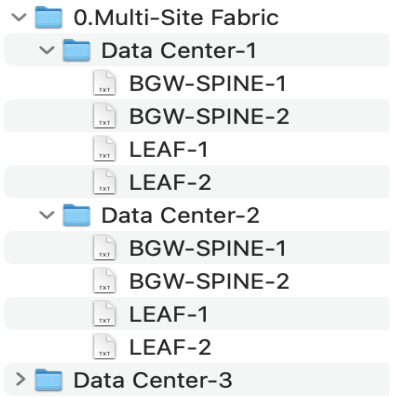
VXLAN EVPN Multi-Site
Domain that can contain multiple VXLAN EVPN Fabrics with Layer-2/Layer-3 Overlay Extensions and other Fabric Types.

Multi-Site Interconnect Network
Fabric to interconnect VXLAN EVPN fabrics for Multi-Site deployments with a mix of Nexus and Non-Nexus devices.

Fabric Hierarchy

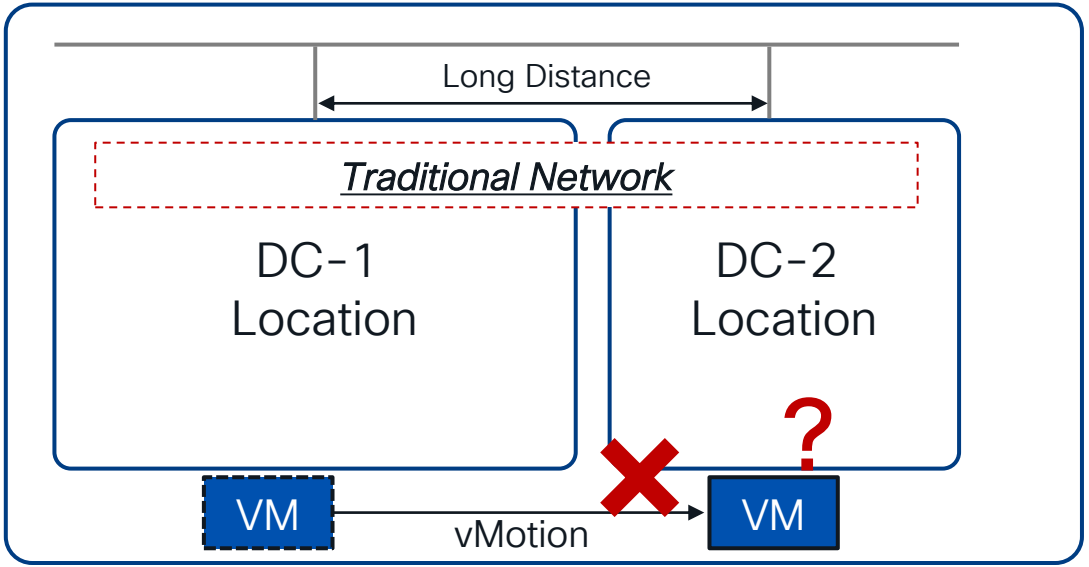
Parent Fabric : VXLAN EVPN Multi-Site

- Child Fabric – Data Center VXLAN EVPN
- Child Fabric - Campus VXLAN EVPN
- Child Fabric – Data Center VXLAN EVPN
- ⋮
- Child Fabric – Data Center VXLAN EVPN



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-1. Requirement for VM Mobility



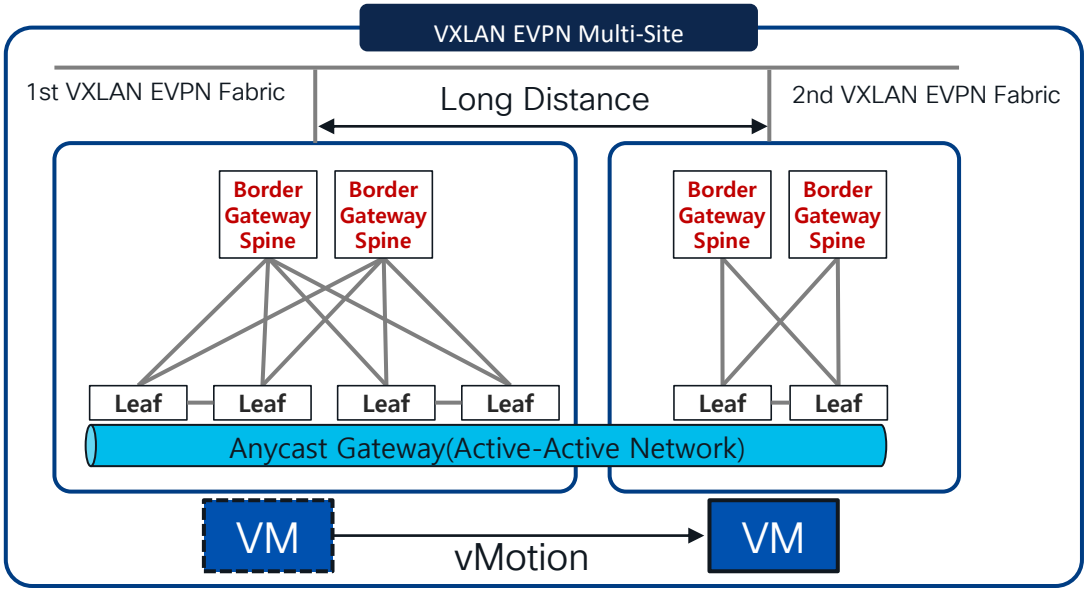
Requirement for VM Mobility

- Eliminating limitation of subnet duplication between Data Center
- Need to ensure VM mobility between Data Center
- vMotion schedular adjusting usage
  - ✓ To ensure equal use of Power/Temperature of Server
  - ✓ To protect resource of Server

vMotion is impossible with Traditional network.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-2. Multi-Site VXLAN EVPN for VM mobility



What technical benefits?

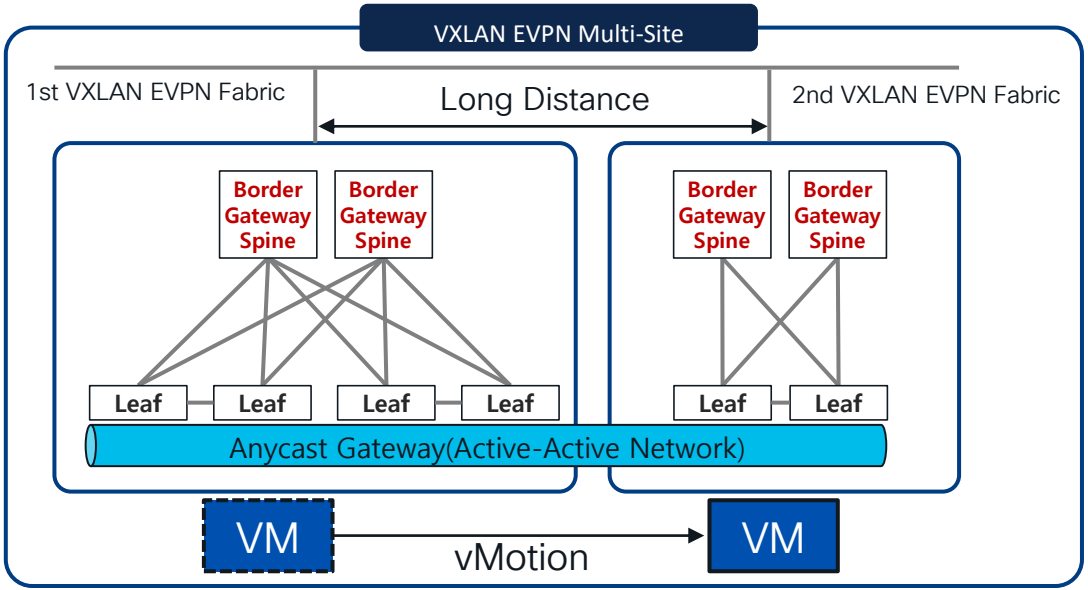
- Spreading Layer 2 network across Multi data centers
- Anycast gateway provide same IP address / MAC address across Multi data centers

Advantages for operator

- No Gateway IP address configuration of VM whenever vMotion.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-3. Considering tracking VM on mobility Env



Where is my VM
which was located in Fabric-1?

Deploying VXLAN EVPN is meaning VM can move to anywhere,
But Operator should track VM location in real time

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-3. Considering tracking VM on mobility Env

Endpoint Search

IP == 192.168.11.50

① Timesta...	Fabric Id	② IP	MAC	L2 VNI	L3 VNI	③ Switch Name	Switch Type	Switch IP	Origin IP	Switch NextHop IP	④ Port	VLAN	L3 INT	⑤ Operation	Endpoint Type	⑥ Sequence Number	VRF
September 20 2023, 03:31:28	12:l2vpn	192.168.11.50	12:34:12:34:a	30000	50000	F1-Leaf-2	N9K	10.70.137.15	10.2.1.2 0.0.0.0 0.0.0.0 0.0.0.0	10.3.1.5	Po1	11	11	DELETE		2	service-1
September 20 2023, 03:31:28	12:l2vpn	192.168.11.50	12:34:12:34:a	30000	50000	F1-Leaf-2	N9K	10.70.137.15	10.2.1.3 0.0.0.0 0.0.0.0 0.0.0.0	10.3.1.5	Po1	11	11	DELETE		2	service-1
September 20 2023, 03:31:28	12:l2vpn	192.168.11.50	12:34:12:34:a	30000	50000	F1-Leaf-1	N9K	10.70.137.15	10.2.1.3 0.0.0.0 0.0.0.0 0.0.0.0	10.3.1.5	Po1	11	11	DELETE	DA	2	service-1
September 20 2023, 03:31:28	12:l2vpn	192.168.11.50	12:34:12:34:a	30000	50000	F1-Leaf-1	N9K	10.70.137.15	10.2.1.2 0.0.0.0 0.0.0.0 0.0.0.0	10.3.1.5	Po1	11	11	DELETE	DA	2	service-1
September 20 2023,	12:l2vpn	192.168.11.50	12:34:12:34:a	30000	50000	F1-	N9K	10.70.137.15	10.2.1.3 0.0.0.0 0.0.0.0	10.3.1.5	Po1	11	11	ADD	DA	2	service-1

① : Endpoint event timestamp

② : IP/MAC lookup

③ : the Endpoint attached Switch

④ : the Endpoint attached Port

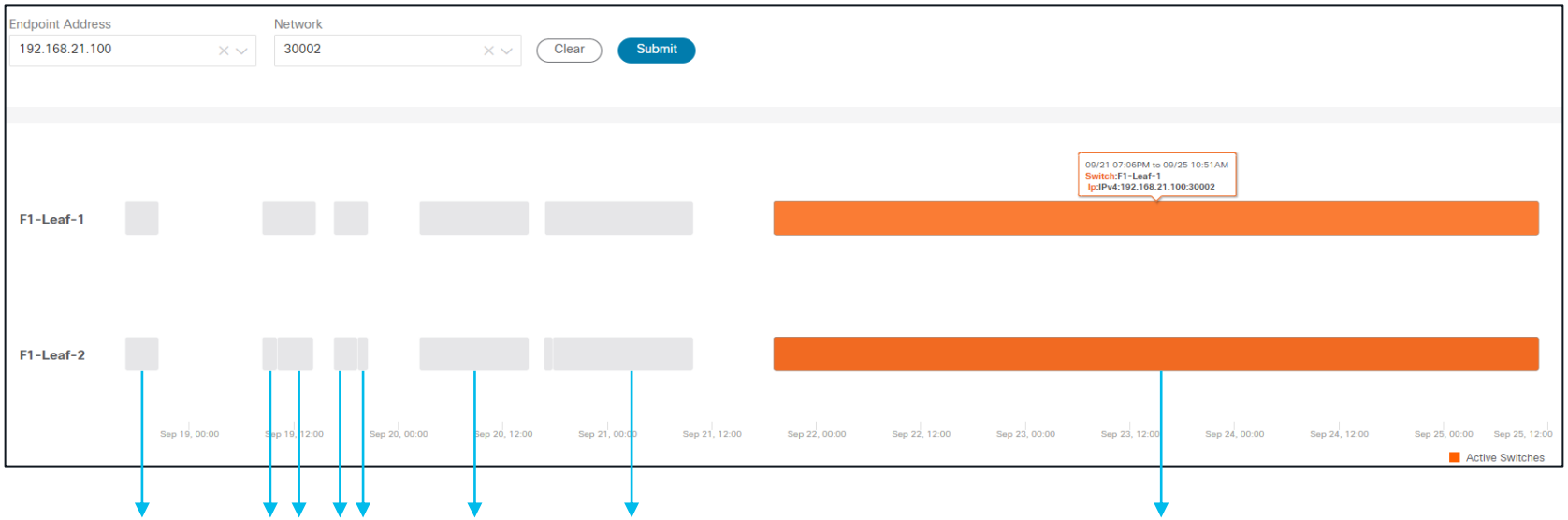
⑤ : attached or deleted

⑥ : IP/MAC move or dup count

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-3. Considering tracking VM on mobility Env

Endpoint Lifetime from Endpoint Locator(EPL)



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Summary of BGP EVPN VXLAN w/ NDFC

NDFC provide automation for complicated Network infrastructure.

Deploy, manage and operate VXLAN EVPN Single to Multi-Data center w/ NDFC

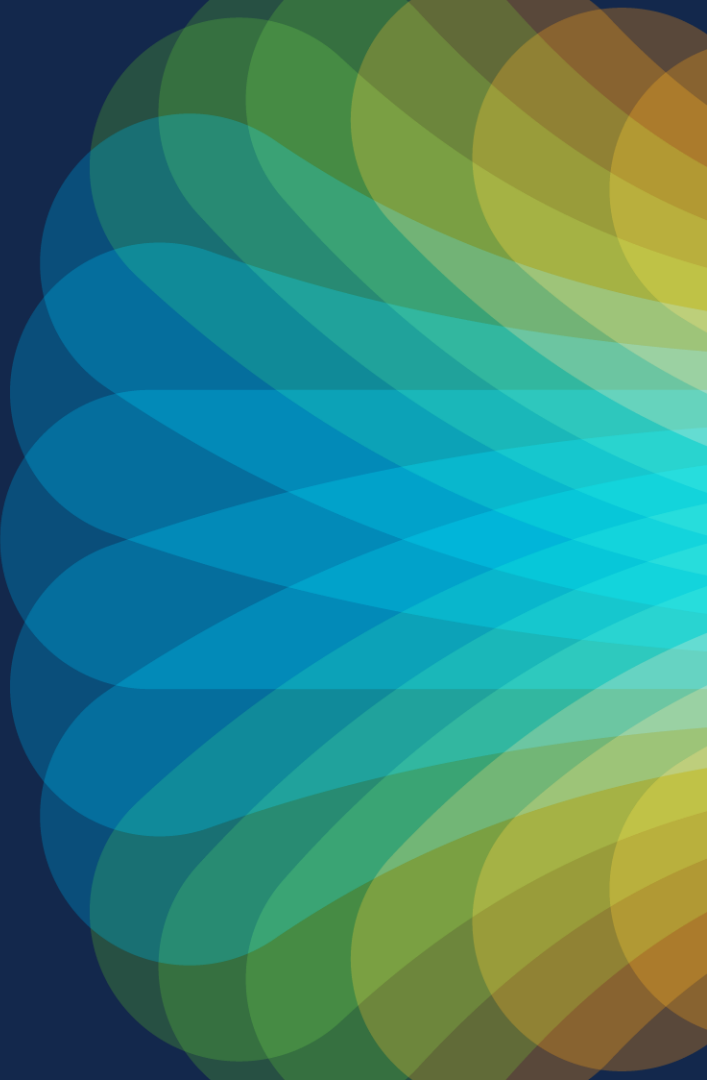
- Active-Active Data Center Network for High availability from Disaster and IP mobility
- Network Separation configuring VRF to fabric wide

VXLAN EVPN can provide Active Active Data center network, But need to track VM location in real time

- End point locator(EPL)

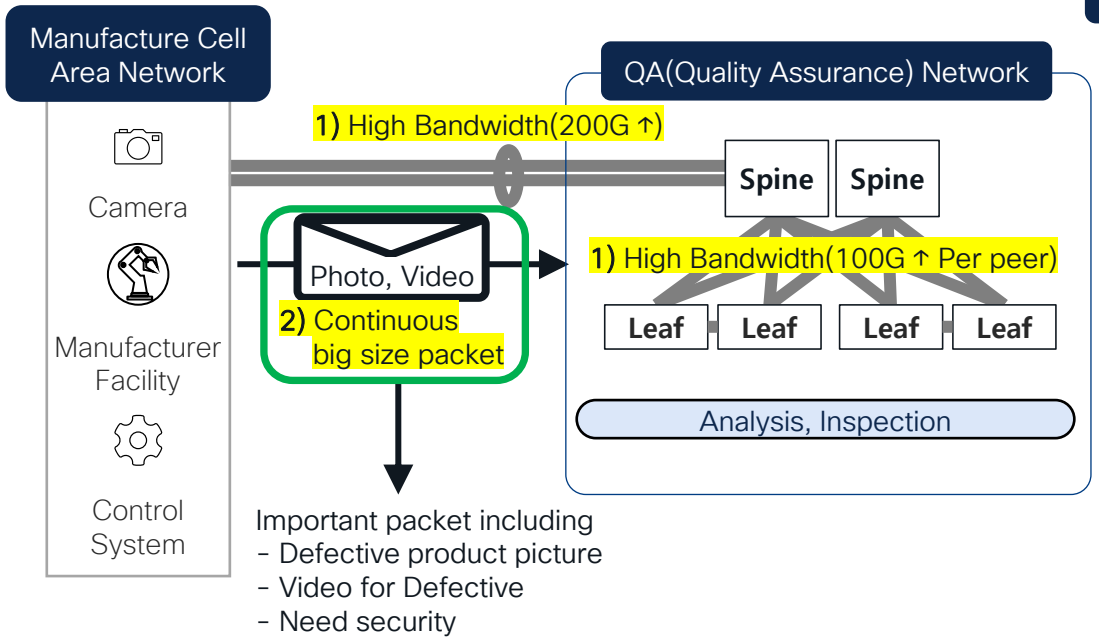
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

How to ensure secure communication between data centers?



1-1. Requirement for Encryption between networks

Requirement & Environment



Requirement for encryption. why?

National and Company Policies needs encryption between particular network

Environment analysis

1) High bandwidth

- Aggregation bandwidth(more 200G)
- Accommodation of Continuous large packets

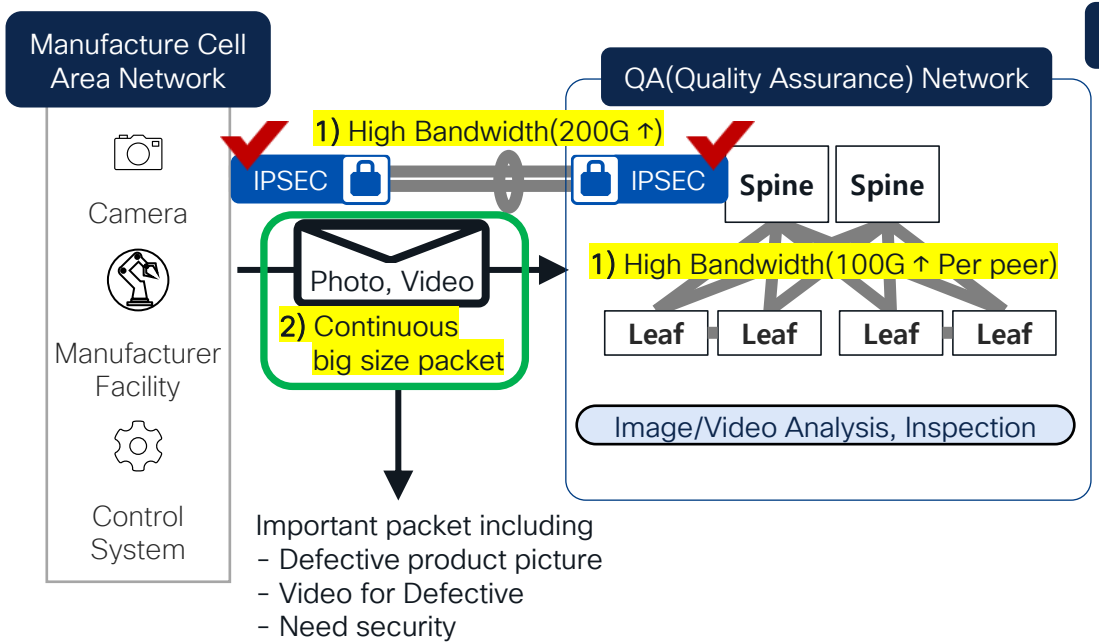
2) Continuous big size packets

- High-definition photo/video
  Ex) 1 photo size : more 4MByte
- Jumbo Frame
- Constant high bandwidth needed

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

1-2. Consider suitable way for encryption

If with IPSEC



Consider some way for encryption

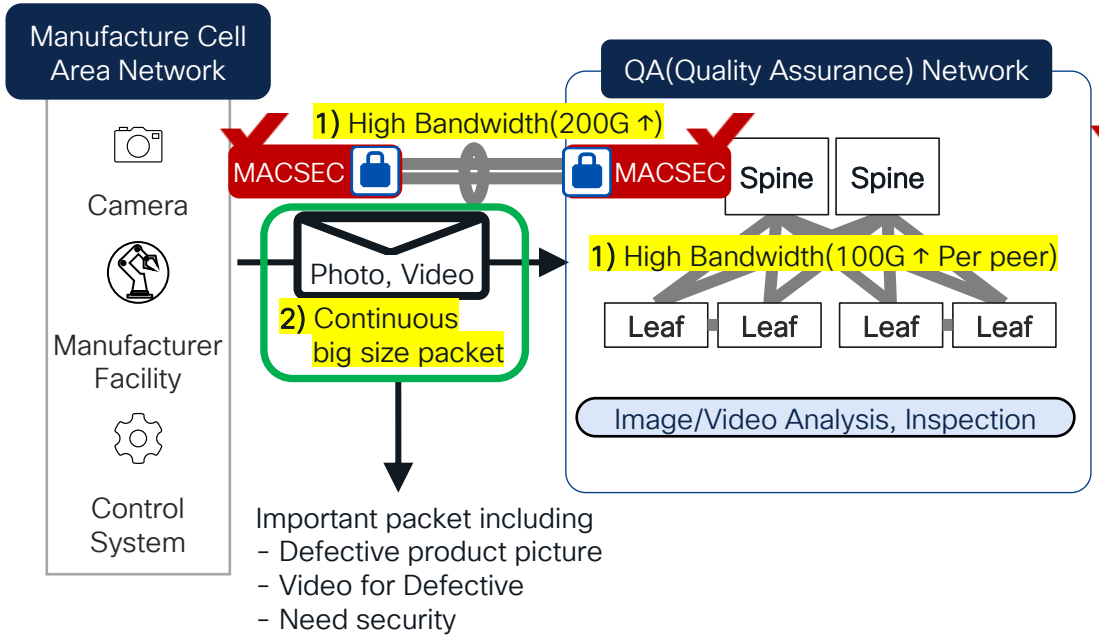
What if we use IPSec in such an environment?

Env	IPSEC
1)	Investing 200G VPN Device Changing design
2)	Performance Degradation
	Over-investment

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

1-3. MACSEC for Direct connected Environment

MACSEC for Direct connected



MACSEC Meets requirement immediately

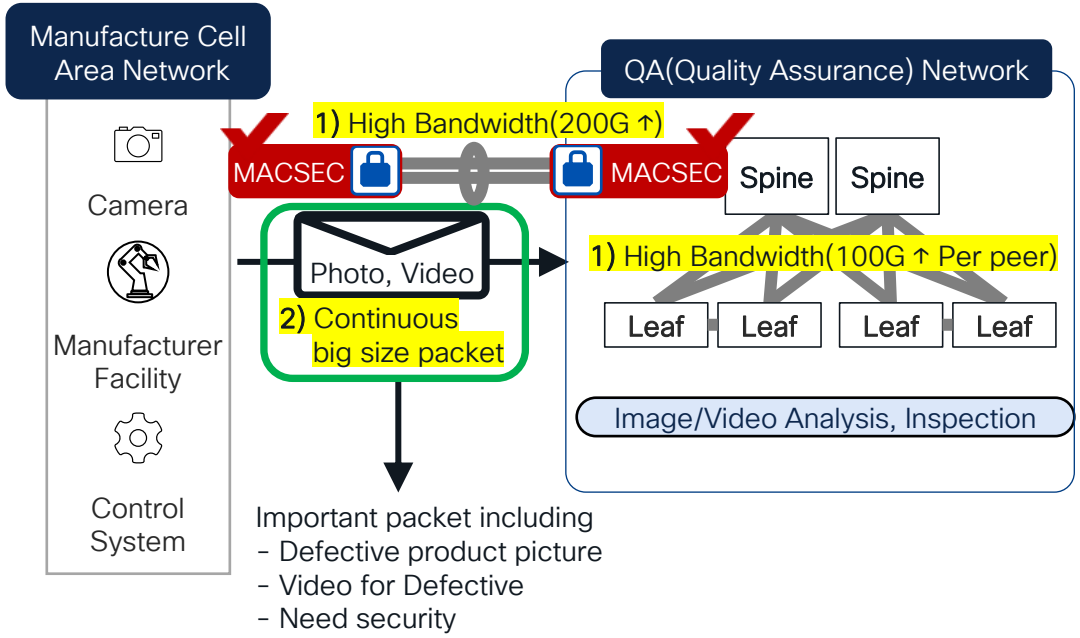
✔ Use MACSEC in such an environment.

Env	MACSEC	IPSEC
1)	Just Configuring MACSEC	Investing 200G VPN Device Changing design
2)	Line-Rate Encrypt/Decrypt	Performance Degradation
	No device investment	Over-investment

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

1-3. MACSEC for Direct connected Environment

MACSEC for Direct connected



MACSEC Meets requirement immediately

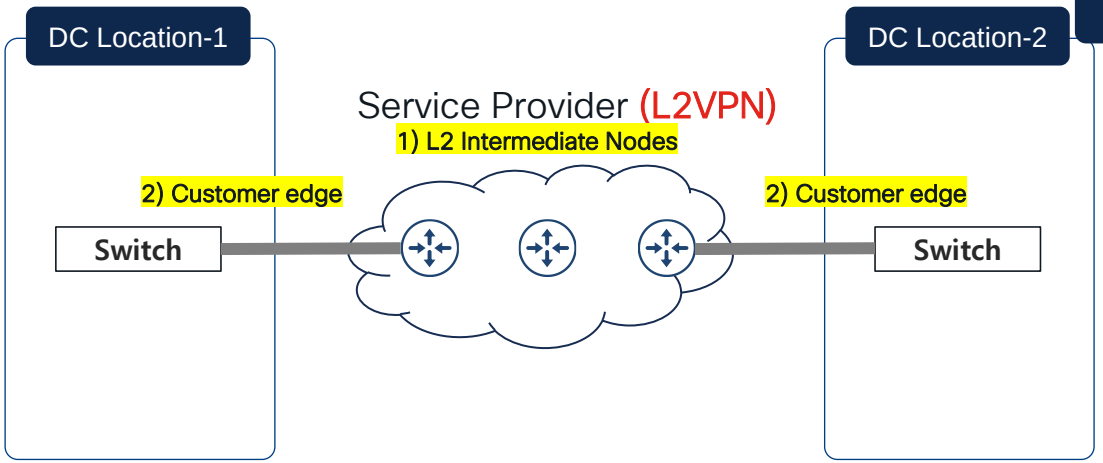
✔ Use MACSEC
in L2 Direct connection environment.

- Minimum cost, maximum effect
- No additional equipment investment
- Line rate encryption
- Simple Configuration

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-1. Encryption over other company L2 transit

Environment analysis



Requirement for encryption. why?

As Two sites is connected via other company's line
Encryption is necessary between DCs

Environment analysis

1) L2 Intermediate
- Not dark fiber
- There are many intermediate nodes

2) Customer edge
- Customer edge couldn't see intermediate node
- need to establish security session

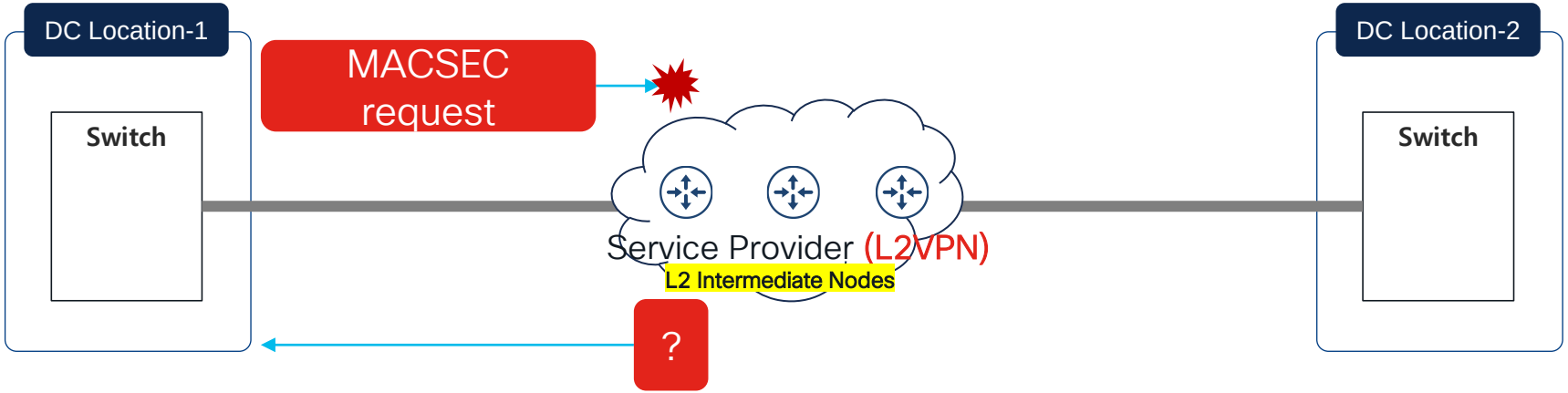
Is MACSEC suitable? No...

MACSEC cannot be used in a Layer 2 environment where there is a node in the middle.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-2. Why need to use WAN MACSEC over Layer2

Environment analysis

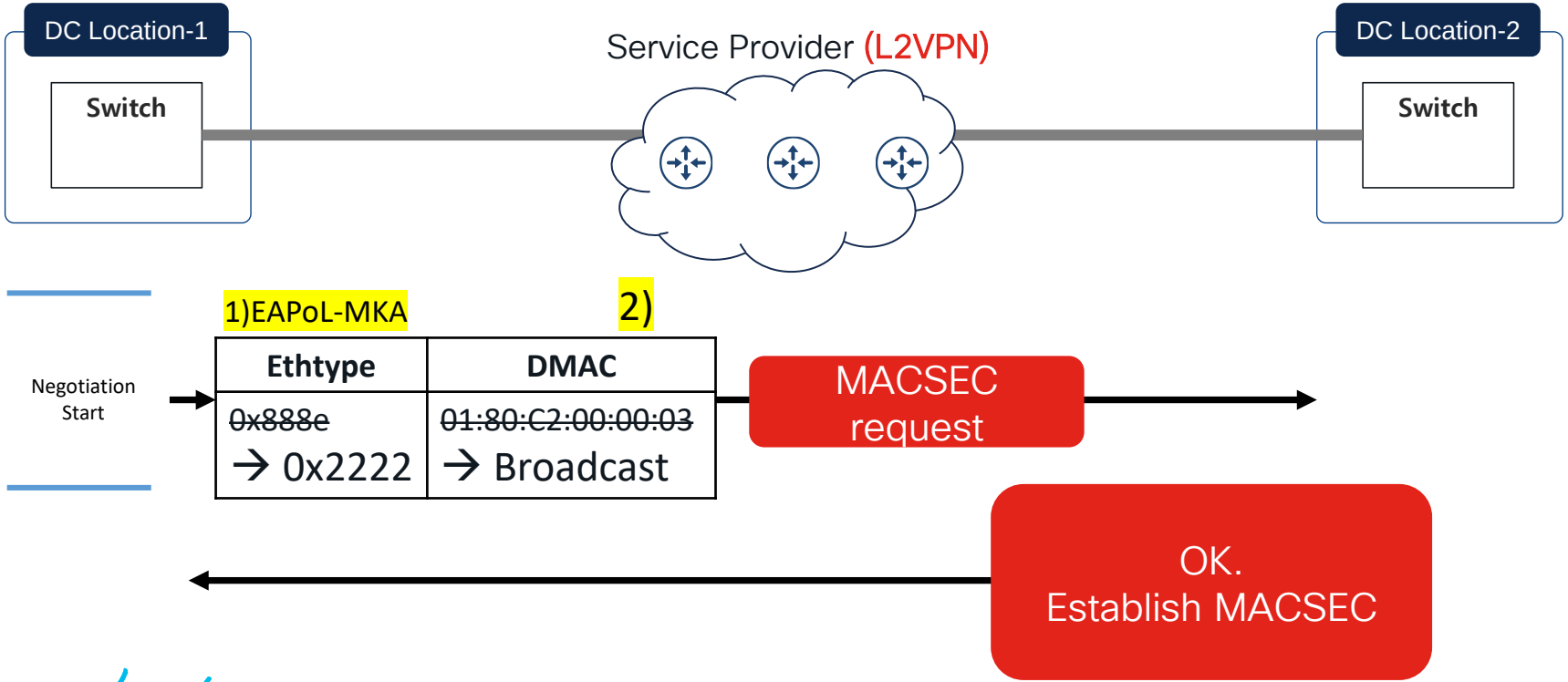


Why are MACSEC negotiation packets lost in the middle?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-2. Why need to use WAN MACSEC over Layer2

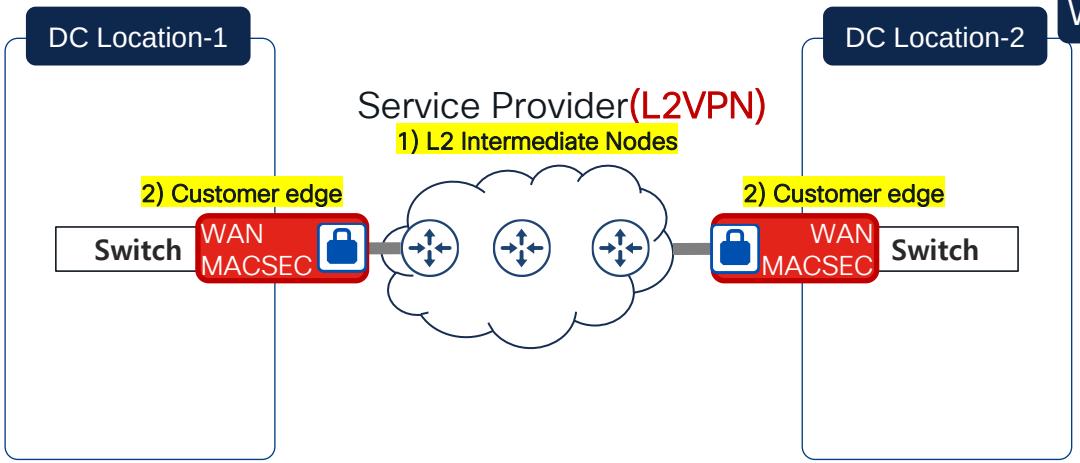
MACSEC for over Layer 2 WAN



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

2-3. Encryption over other company L2 transit

Environment analysis



WAN MACSEC is proper way via L2 Transit

Communication via other company's line
Encryption is necessary between DCs

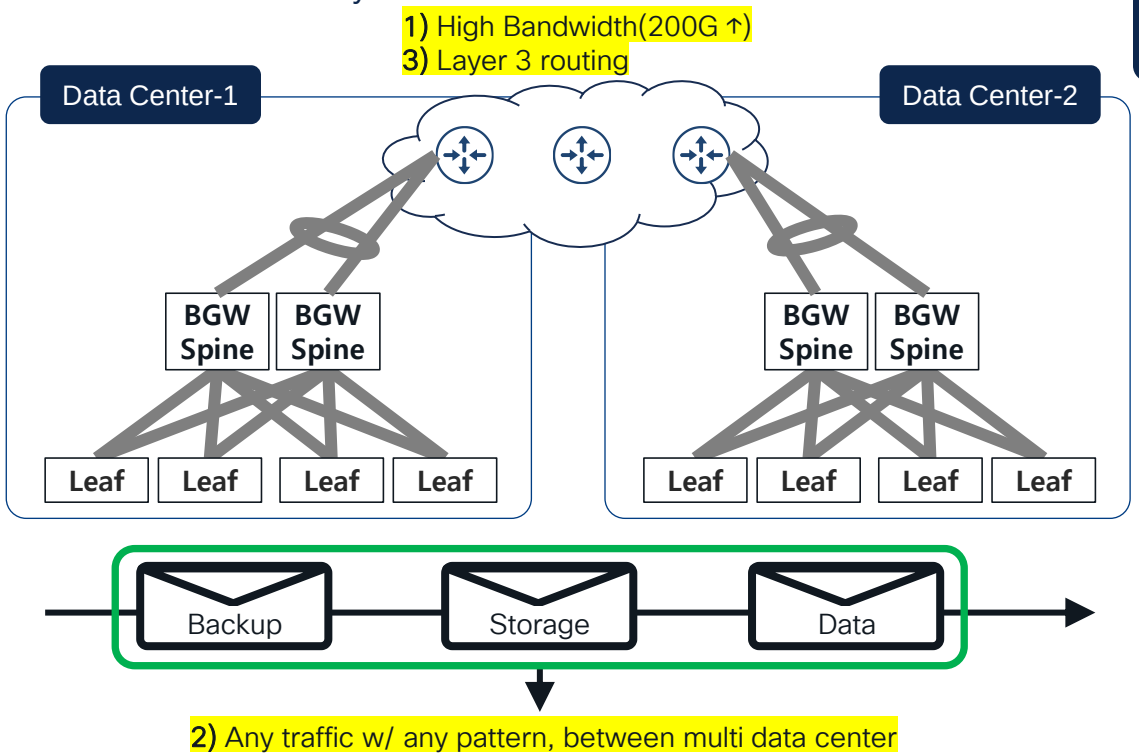
✔ Use WAN MACSEC,
If there is intermediate node

- Secure Channel over Layer 2 multi hop
- Line-rate encryption

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

3-1. Encryption over L3 WAN

Environment analysis



Encryption between 2 DCs connected w/ Layer 3 routing

Two sites connected via L3 Network
: Encryption is needed for L3 communication

Muti Data Center w/ VXLAN EVPN

1) Any traffic
- From small to big traffic
- Backup traffic between multi Data Center
- High performance

2) High bandwidth
- Accommodate all business traffic

3) L3 Interconnect over L3 intermediate
- Communication between DCIs via routing

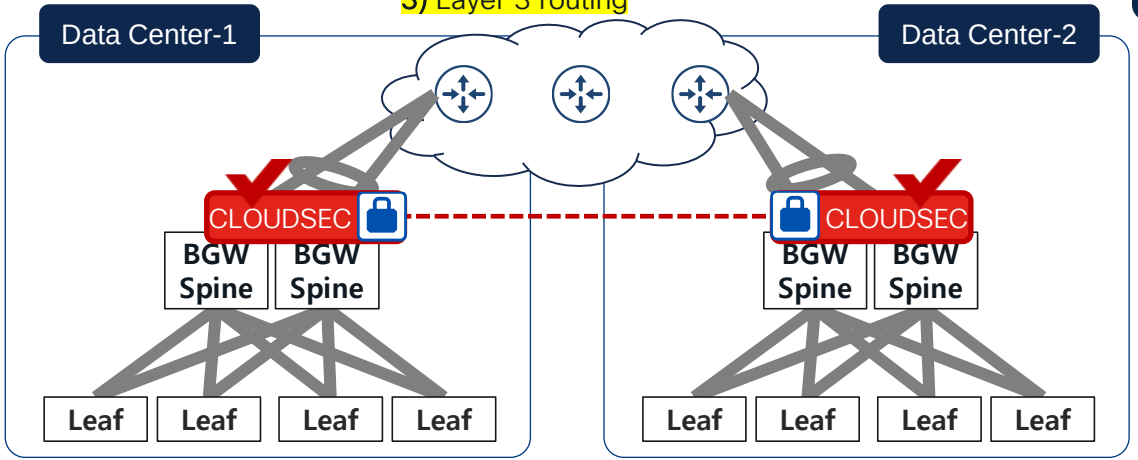
CloudSec needed

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

3-1. Encryption over L3 WAN

Cloudsec for Layer 3 WAN

1) High Bandwidth(200G ↑)
3) Layer 3 routing



Physical = Multi-hop

Logical = Back to Back Secure Channel

Encryption between 2 DCs connected w/ Layer 3 routing

Two sites connected via L3 Network
: Encryption is needed for L3 communication

Muti Data Center w/ VXLAN EVPN

1) Any traffic
- From small to big traffic
- Backup traffic between multi Data Center
- High performance

2) High bandwidth
- Accommodate all business traffic

→ resolve Line-rate encryption

3) L3 Interconnect over L3 intermediate
- Communication between DCIs via routing

→ resolve it except IP Header Encryption

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

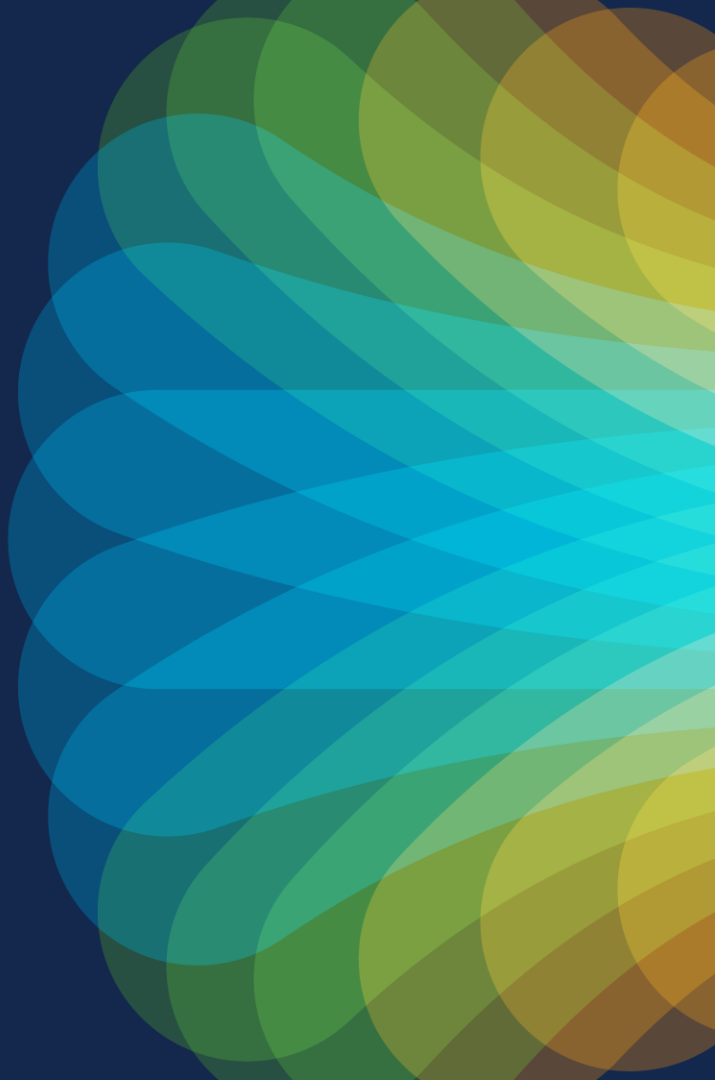
Conclusion

MACSEC/ WAN MACSEC/ CLOUDSEC

- Secure channel besides IPSec.
- High Bandwidth : Most of Nexus 9K provides services of high-bandwidth MACSEC, WAN MACSEC, and CLOUDSEC.
- Line rate : encryption/decryption is performed at Nexus 9K Cloudscale ASIC.
- Choose and apply technology depending on your network design
  - Direct Secure Connectivity = MACSEC
  - Secure Connectivity over L2 WAN = WAN MACSEC
  - Secure Connectivity over L3 WAN = CloudSEC

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

How to make money from your network?



Use case : Revenue w/ network infrastructure

Network administrator where utilizing network infrastructure was necessary for revenue generation within an organization.

Need Revenue..

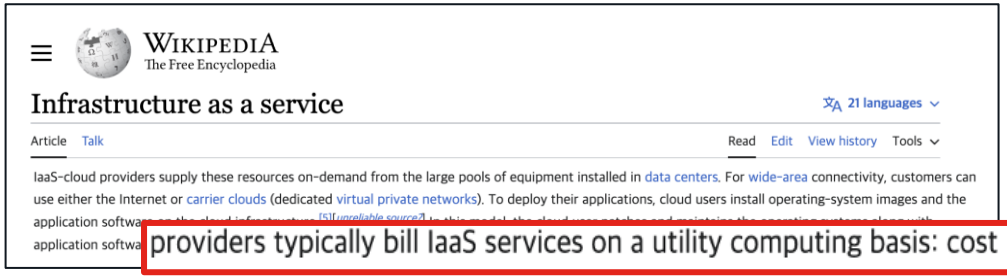
Situation : **Necessary to generate revenue within the organization by utilizing the network infrastructure.**

Typically : **Network organization is not a profit-driven organization**
(For Use case, only investing in new equipment than revenue generation)

Generating revenue solely through network equipment is challenging.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Idea by redefining Infrastructure as a Service(IaaS)



WIKIPEDIA
The Free Encyclopedia

Infrastructure as a service

21 languages

Article Talk Read Edit View history Tools

IaaS–cloud providers supply these resources on–demand from the large pools of equipment installed in data centers. For wide–area connectivity, customers can use either the Internet or carrier clouds (dedicated virtual private networks). To deploy their applications, cloud users install operating–system images and the application softwa

application softwa providers typically bill IaaS services on a utility computing basis: cost reflects the number of resources allocated and consumed.

providers typically bill IaaS services on a utility basis
: cost reflects the number of ..... consumed.

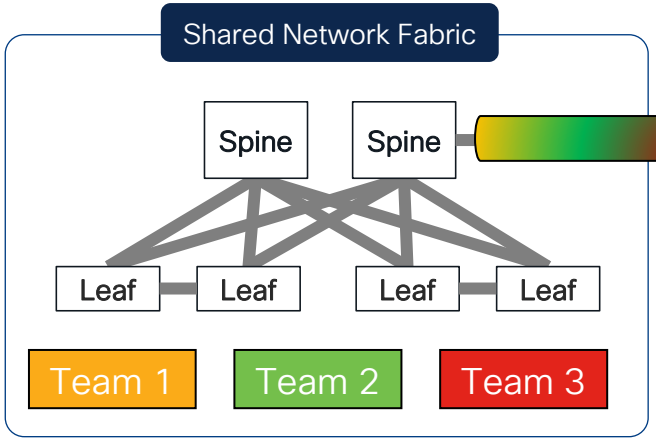
The amount of **traffic** generated on the rented network **equals** **the revenue** generated by the network organization.

ex) 1923891bytes x $ = Revenue

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Usage-Based Metered Service (Packet Amount)

With Nexus Data Broker



Nexus Data Broker

Team	Traffic Amount(Bytes)
Team 1	42,714,819
Team 2	18,712,838,127
Team 3	627,381

Traffic amount per each team as for billing data

For Revenue Generation of Network Operations Team

- Precise Packet Amount Collection
- Distinguishing Network Traffic by Organizational Units Within the Company
- Periodic Billing Based on Organizational Traffic Usage Collection

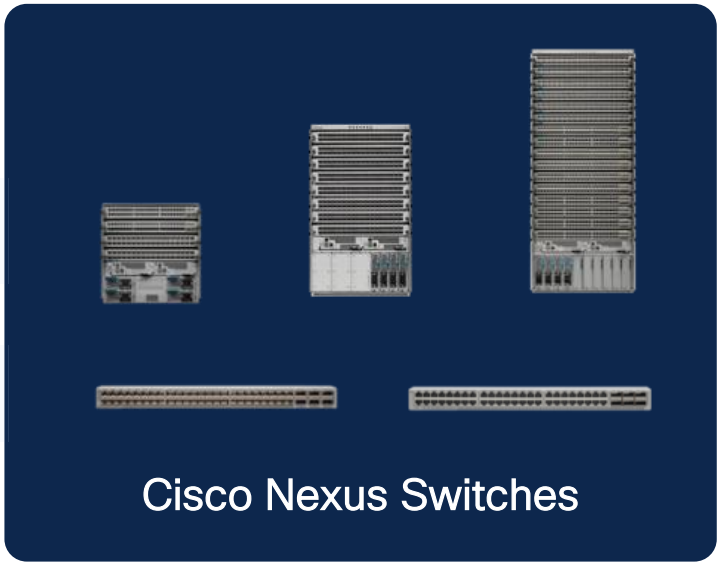
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

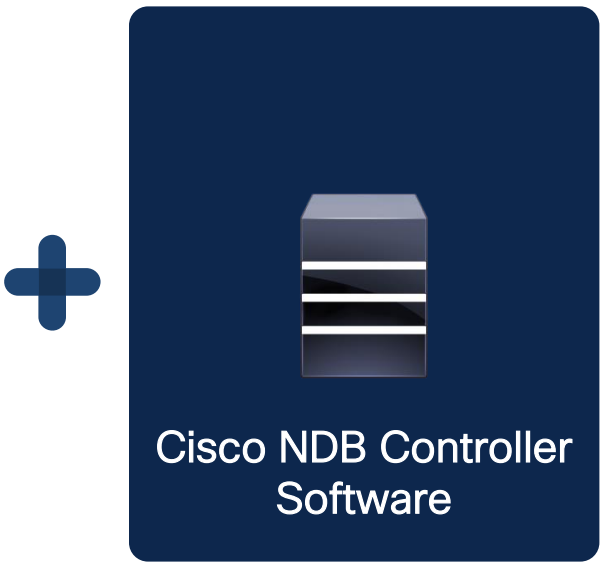
Cisco Nexus Data Broker

Objective: Build scalable packet broker network that is easy to operate
+ Cost effective TAP Aggregation Switch

9000 Series

3000 Series

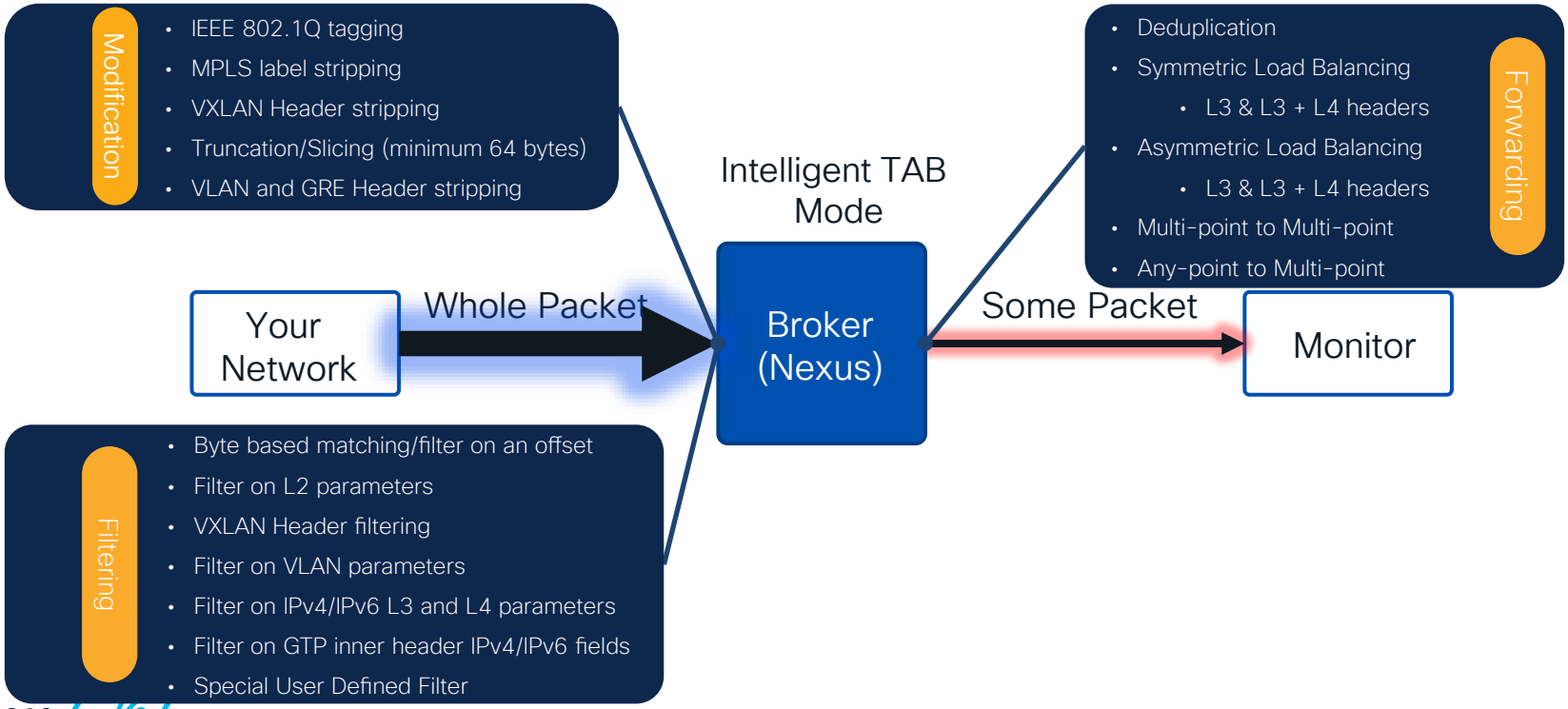




© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is DATA BROKER?

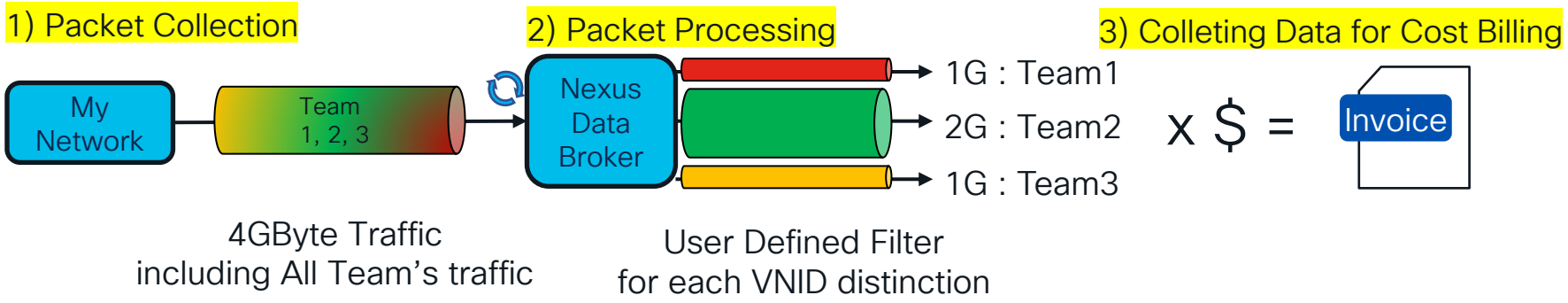
Ingress : Packet Filter & Modification → Egress : Forwarding



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Considerations for Billing through Traffic Measurement

Concept & Flow



1) Packet Collection
Accurate Traffic Amount Collection

2) Packet Processing
Precision Organizational Distinction of Traffic Based on Packet Types

3) Colleting Data for bill
Billing
Earning Revenue

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

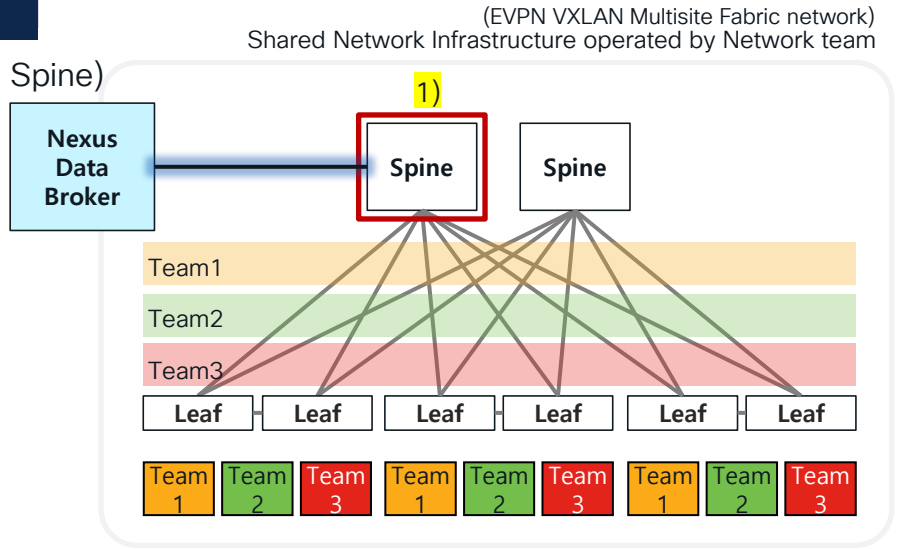
Use case : Traffic Measure

w/ DATA BROKER for Private Cloud

1) Select Production Device to Integrate with NDB

Recommendation: Intermediate node receiving All Traffic (ex. Spine)
→ To Save Leaf Ports and NDB Investment

Key : Mirroring the Leaf-Port Traffic to NDB Interface



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use case : Traffic Measure

w/ DATA BROKER for Private Cloud

1) Select Production Device to Integrate with NDB

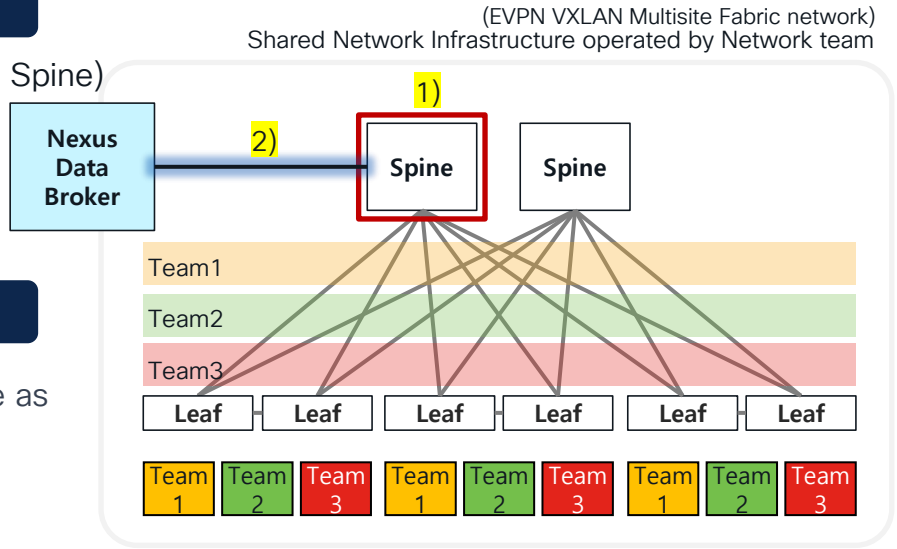
Recommendation: Intermediate node receiving All Traffic (ex. Spine)
→ To Save Leaf Ports and NDB Investment

Key : Mirroring the Leaf-Port Traffic to NDB Interface

2) Connecting NDB to High Bandwidth(to receive mirror packet)

Recommendation: Utilize 2 High-Bandwidth Links as possible as you can to defend packet drop

Key : No negotiation when receiving SPAN(Mirror data)
→ Missing Out On Money



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use case : Traffic Measure

w/ DATA BROKER for Private Cloud

3) Received packet format

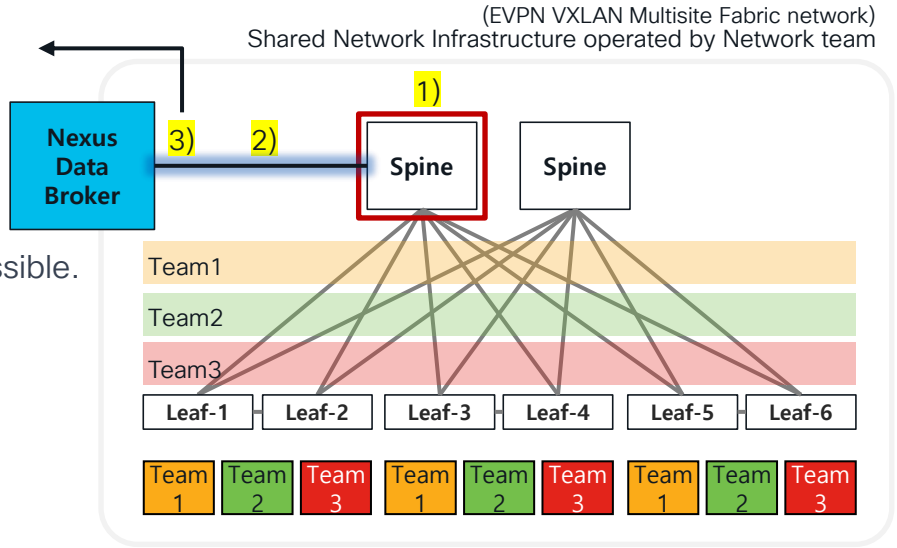
NDB is receiving mirrored packet from production network

With 5-Tuple, Distinguishing Organizations is Impossible.
Due to this packet format, with NetFlow and sFlow,
Obtaining Organizational Packet Volume Information is Impossible.

The Section of Netflow/sFlow

LEAF-1 VTEP	LEAF-3 VTEP	UDP	VXLAN	Team-1 Packet

Needed Areas for Billing

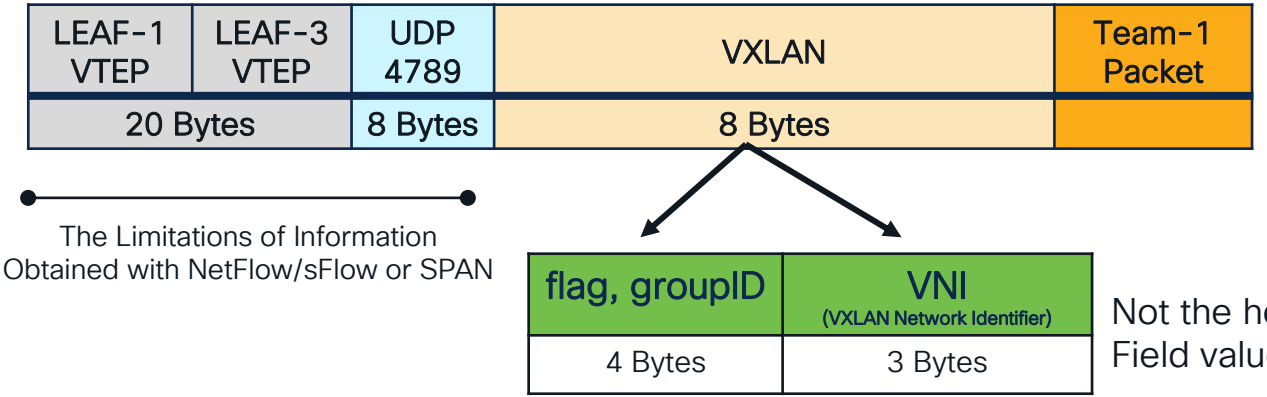


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Use case : Traffic Measure

with DATA BROKER for Private Cloud

Understanding of receiving VXLAN Header



30000 = Team A

30001 = Team B

30002 = Team C

With Filter : Extracting VNI Packet Usage

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

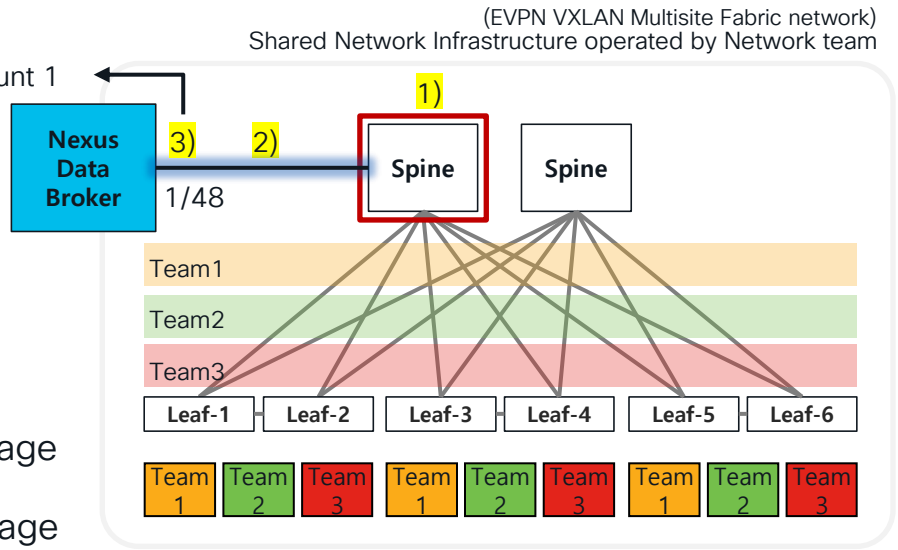
Use case : Traffic measure

with DATA BROKER for Private Cloud

Extract result from NDB

NDB# show system internal access-list tcam ingress start-idx fitler-index count 1

pkts: 84812, bytes: 118101231



Python Output

VNI	Packets	Bytes	
30001	84812	118101231	Team1 packet usage
30002	169624	236202462	Team2 packet usage
30003	254436	354303693	Team3 packet usage

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conclusion : Nexus Data Broker

Make money from your Network with Nexus data broker

NDB is the cost-effective tap switch.

Extract the packet information you want without restrictions.

- UDF Feature: More than header, need deeper w/ filter
- OFM, Truncation Feature : Overlay aware strip, modify and Forward

→ accurately extract only the desired information

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Summary for 3 subjects

BGP EVPN VXLAN w/ NDFC : Provide deployment, operation and management

- Active-Active Data Center for service high availability
- Provide network separation for hosting service

DC Network Security : Analyze network design and turn on proper security feature

- MACSEC : Layer 2 Direct connected
- WAN MACSEC : Connectivity via Layer 2 Intermediate Node
- CLOUDSEC : Layer 3 routing communication

Nexus Data Broker : Make money with various feature.

- User Defined Filter(UDF) : Filtering field within header
- Overlay Forwarding Manager : Stripping Overlay header for inner header

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco Live!

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.

Meet the Expert Opening Hours:

Tuesday	**3:00pm – 7:00pm**
Wednesday	**11:15am – 7:00pm**
Thursday	**9:30am – 4:00pm**
Friday	**10:30am – 1:30pm**

Session Surveys

We would love to know your feedback on this session!

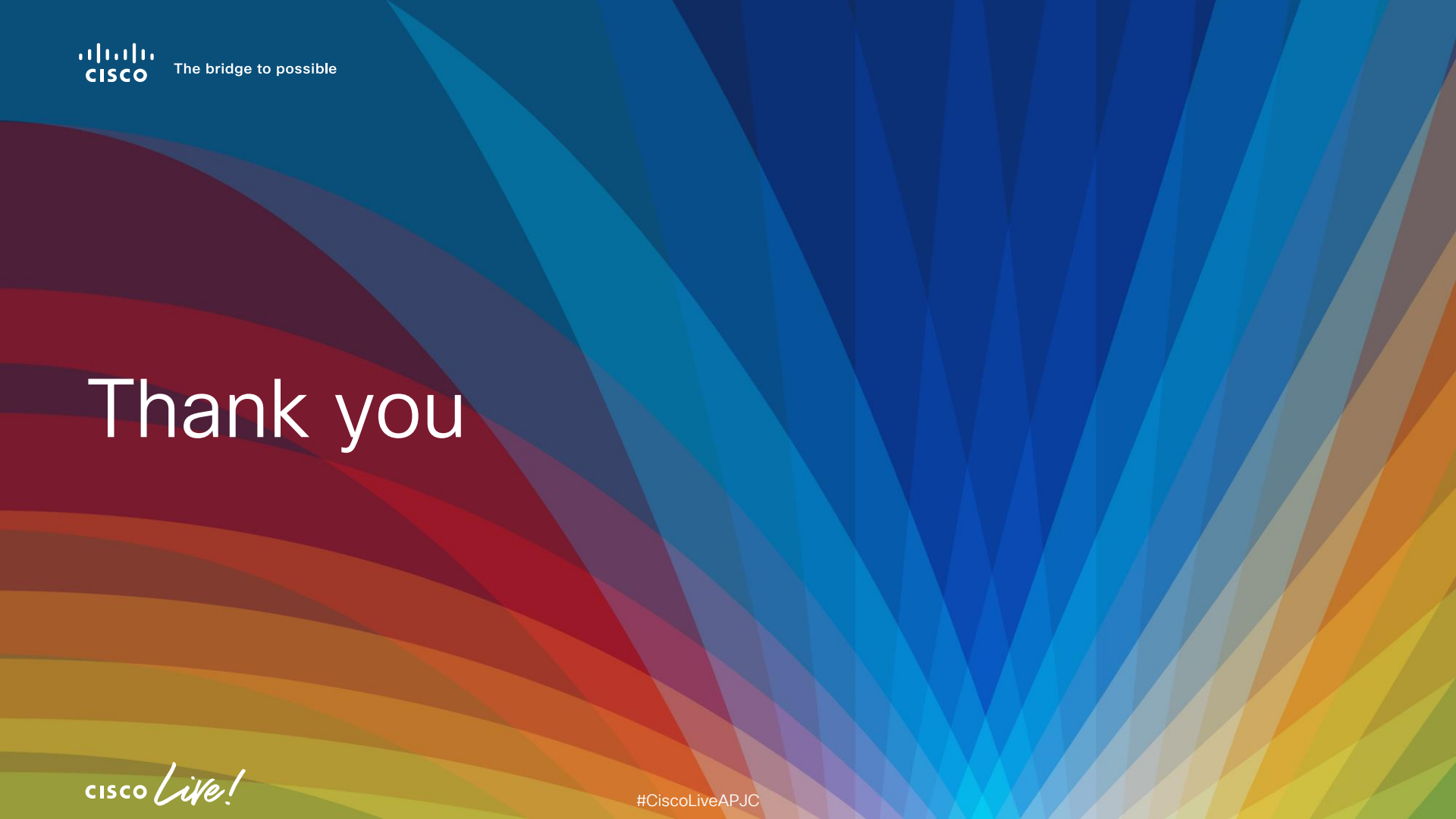
- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public


cisco
The bridge to possible
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
Let's go
#CiscoLiveAPJC