
cisco Live!
TURN
IT
UP
#CiscoLive

The bridge to possible

SDA for everyone – now even ready for YOUR network!

Patrick Mosimann, Technical Solutions Architect Cisco Switzerland
Peter Fuchs, Technical Solutions Architect Cisco Austria
Ivan Caduff, Technical Solutions Architect Cisco Switzerland

BRKEMT-2102

The bridge to possible

Patrick Mosimann

Technical Solutions Architect
Cisco Switzerland

Ivan Caduff

Technical Solutions Architect
Cisco Switzerland

The bridge to possible

Thank you

Peter Fuchs

Technical Solutions Architect
Cisco Austria

SDA for everyone – now even ready for YOUR network!

Agenda

- Introduction
- Onboard the Border
- Demystify Wake-on-LAN & Silent hosts
- Conclusion

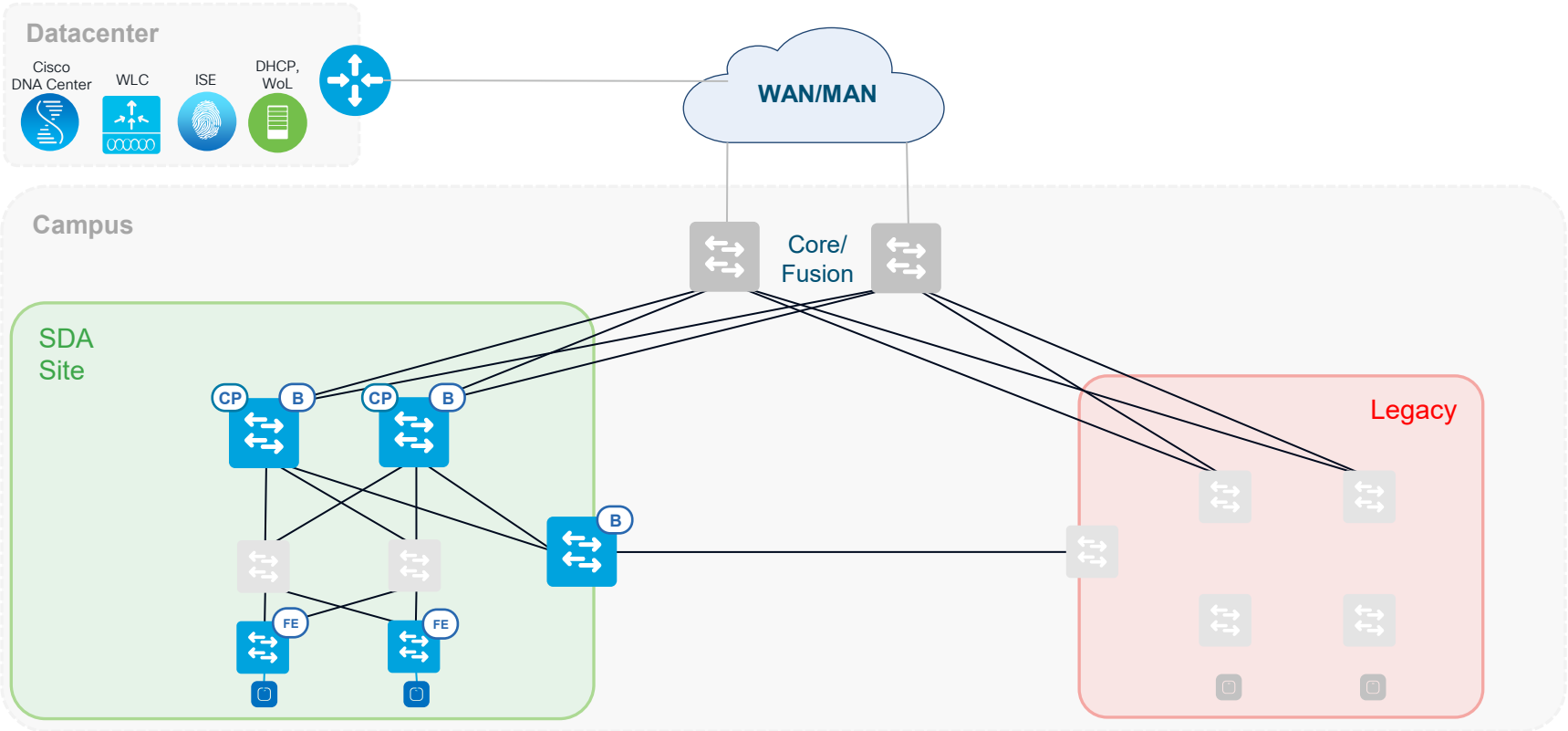
Introduction

ITs-Best Corp Introduction

- As-IS
  - Existing | traditional Layer-2 based network in the campus
  - Datacenter hosts applications and tools

- To-BE
  - New SDA-Environment in the campus
  - Layer-2 interconnect between existing network and new SDA network for migration purpose

ITs-Best Corp
High Level Layout



ITs-Best Corp Challenges

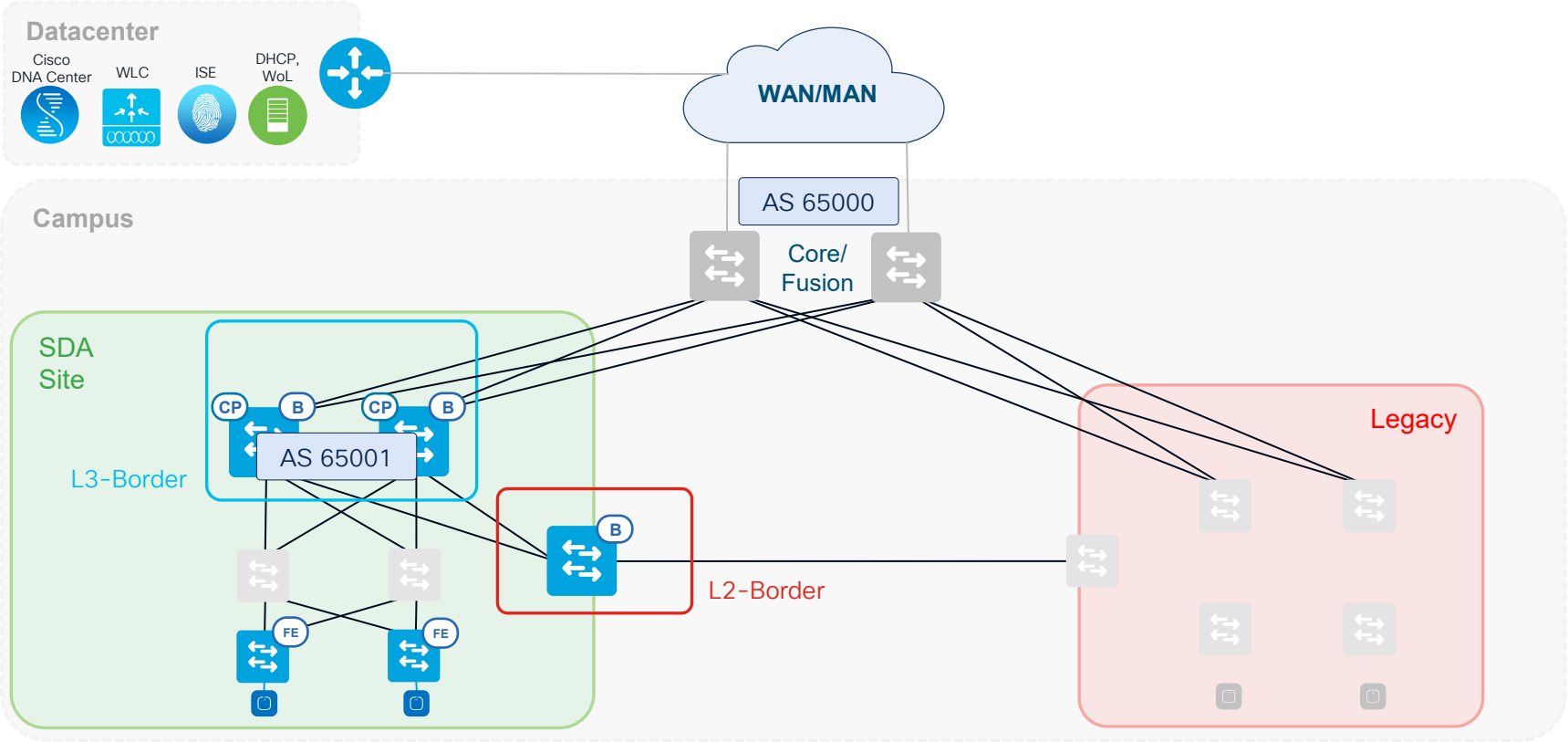
- Day-0
  - L2-Border vs. L3-Border
  - Deployment of the L3-Border and starting the SDA setup
  - How to interconnect existing environment for migration purpose
  - Onboard the border

- Day-1
  - What about my Wake-on-LAN?
  - What about my Silent Hosts?
  - Demystify Wake-on-LAN | Silent hosts

Onboard the Border

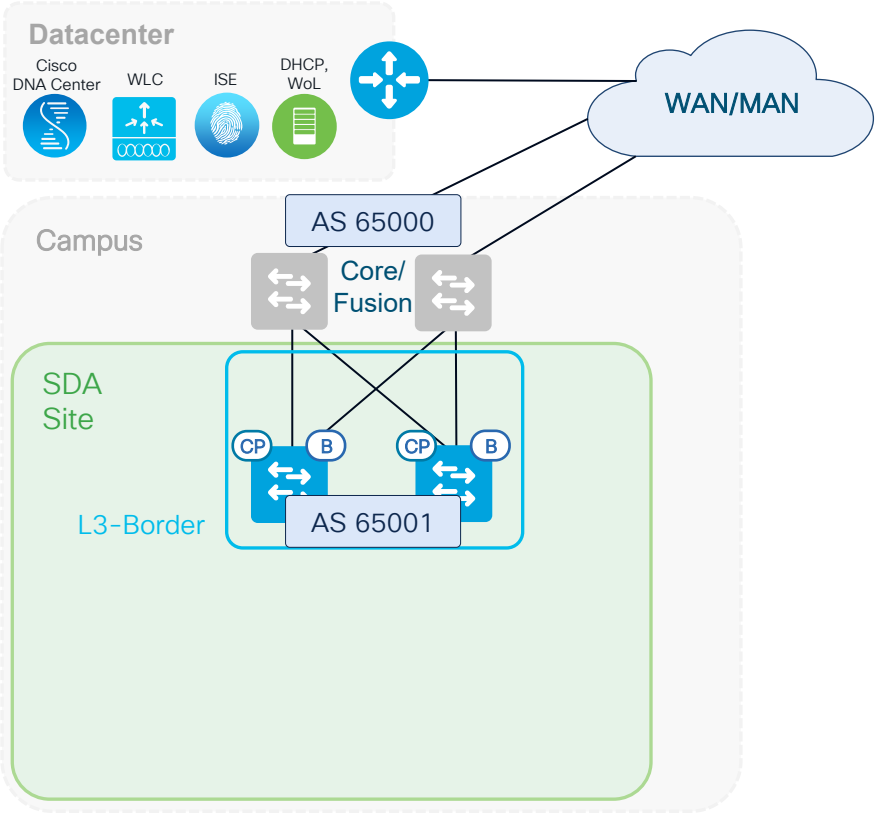
Onboard the Border

High Level Design



Onboard the Border

Introduction L3-Border



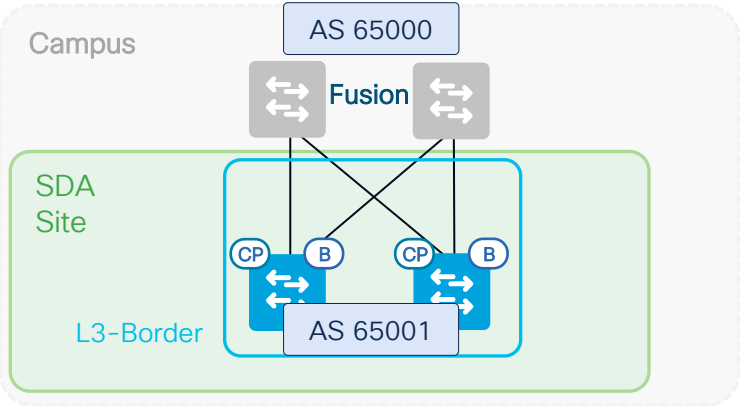
- Connects the Fabric to the outside
- Type:
  - Internal
  - External
  - Internal & External
  - -> BRKCRS-2811

Reference

Onboard the Border

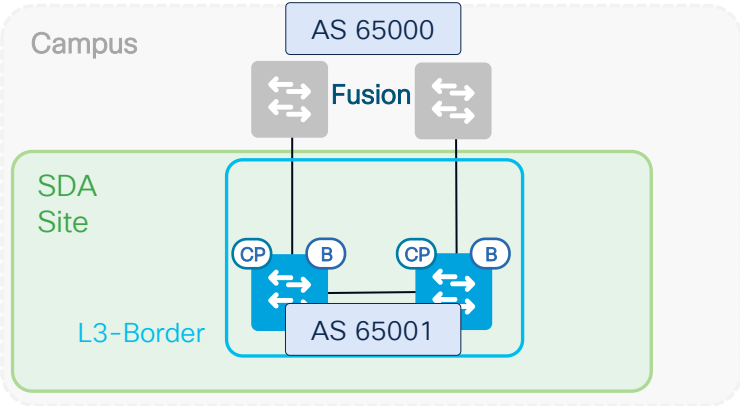
Design Options

X-Shape



Fully automated

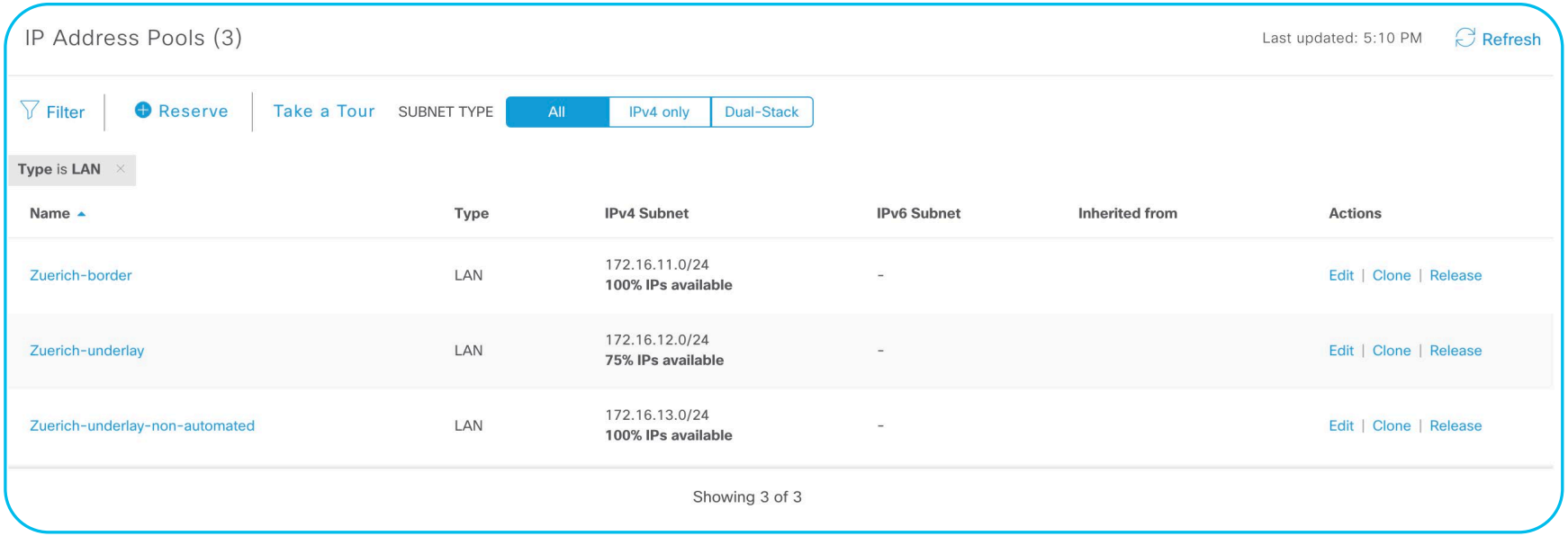
U-Shape



Manual config of B2B-link & iBGP
Less uplinks required

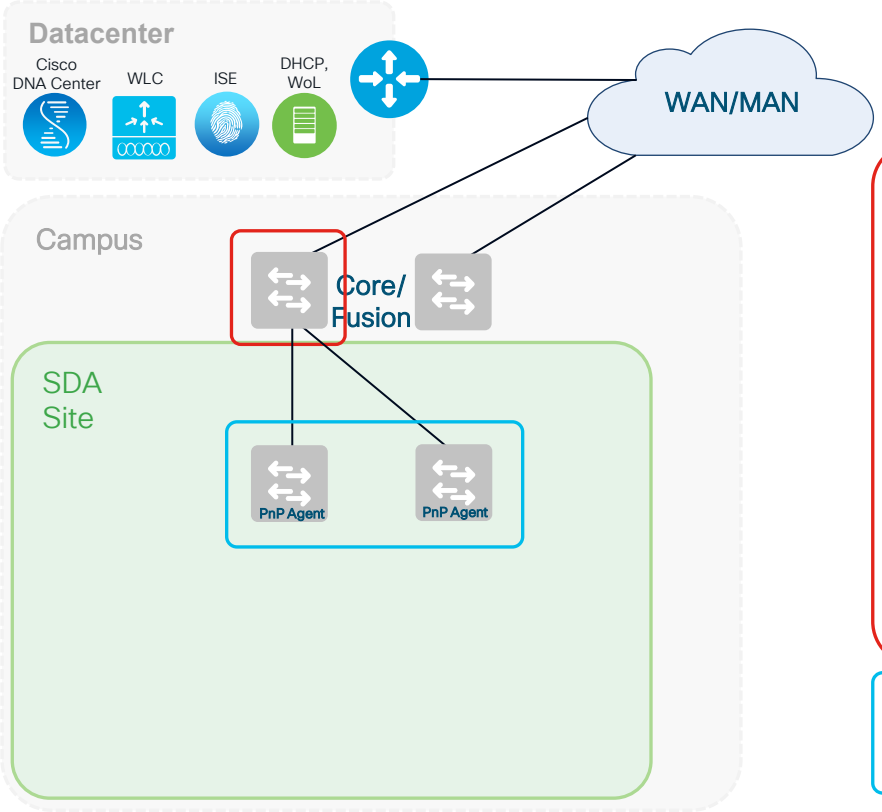
Onboard the Border

Step 1: Reserve IP Address Pools



Onboard the Border

Step 2: Plug and Play (PnP) for the two L3-Border



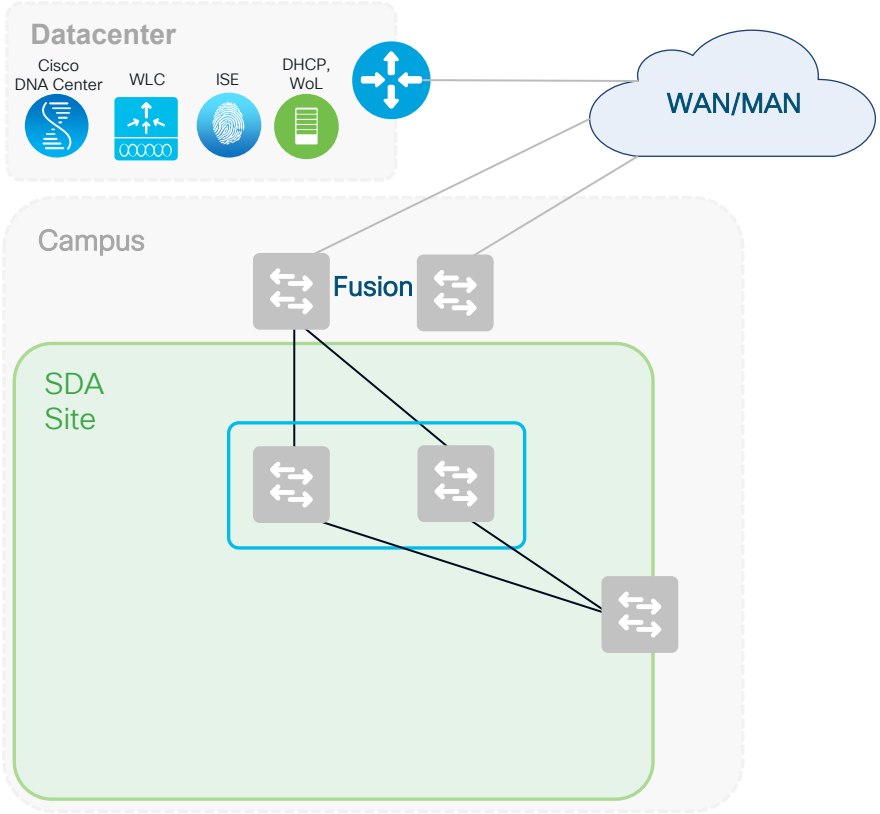
On the Fusion add:

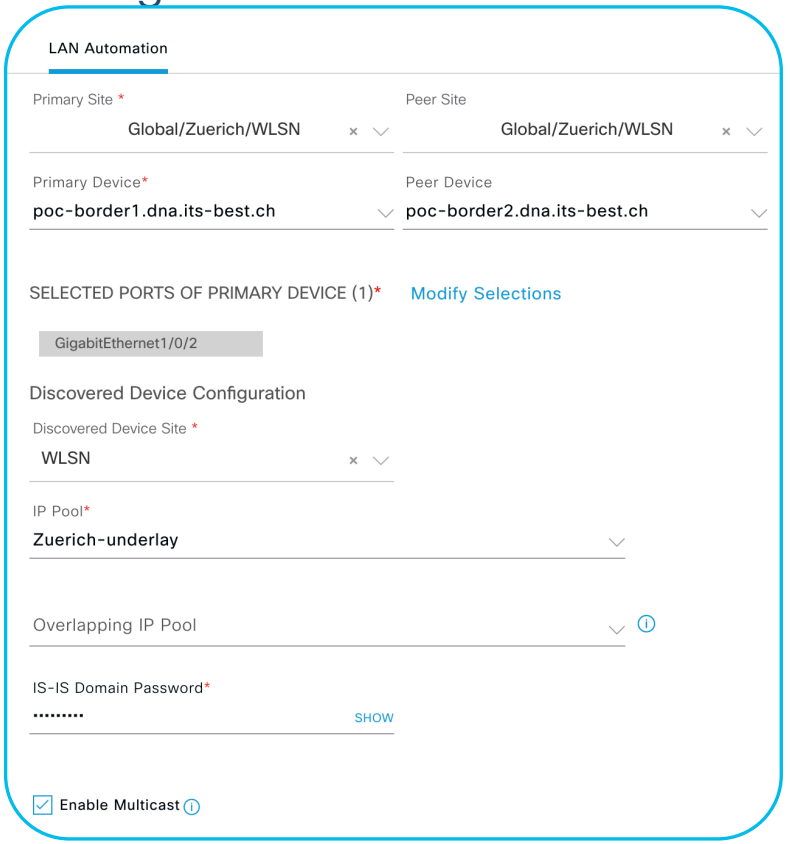
```
ip dhcp excluded-address 172.16.13.1
ip dhcp pool nw_orchestration_pool
  network 172.16.13.0 255.255.255.192
  option 43 ascii 5A1D;B2;K4;I192.168.99.10;J80;
  default-router 172.16.13.1
  class ciscopnp
    address range 172.16.13.2 172.16.13.62
ip dhcp class ciscopnp
  option 60 ^ciscopnp
vlan 13
  name PnP_OnboardTheBorder
interface Vlan13
  ip address 172.16.13.1 255.255.255.192
pnp startup-vlan 13
static route 172.16.12.0 255.255.255.0 172.16.13.2
```

Border gets initial config template (Appendix)

Onboard the Border

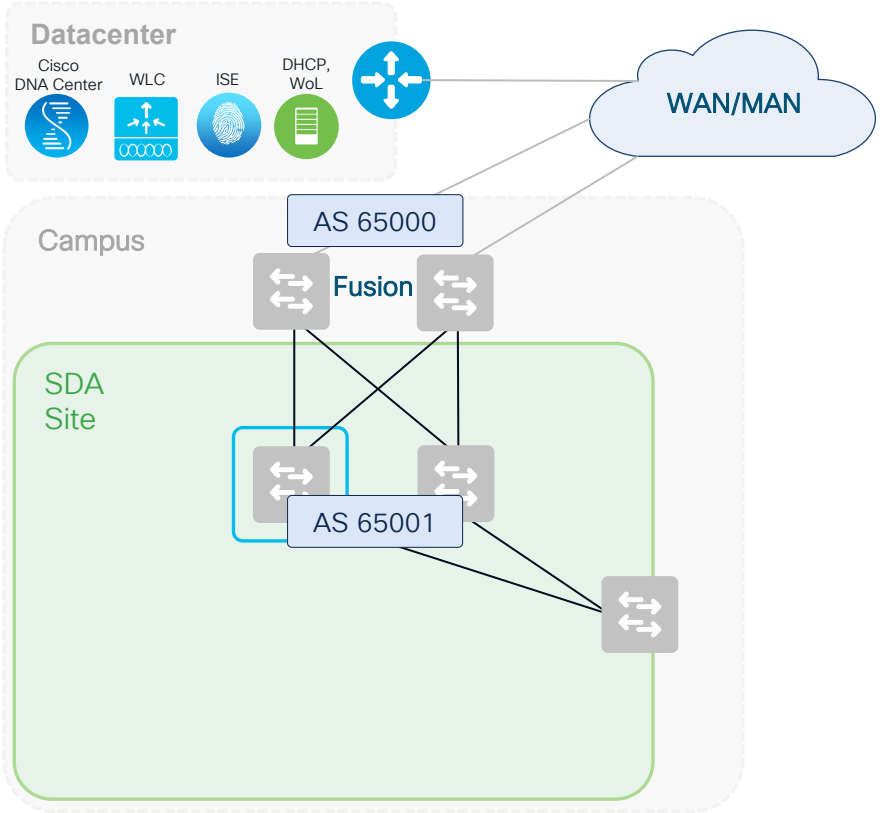
Step 3: LAN Automation for IS-IS & Multicast Config

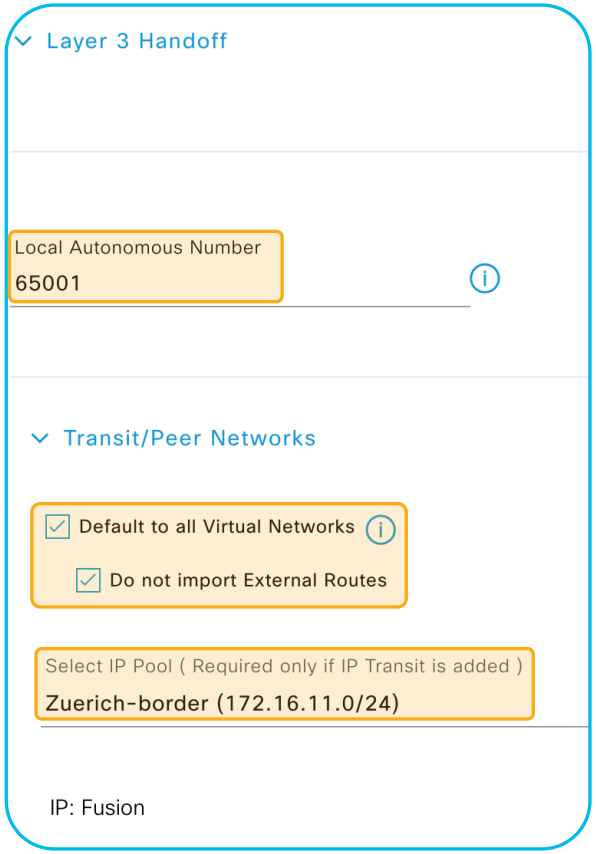




Onboard the Border

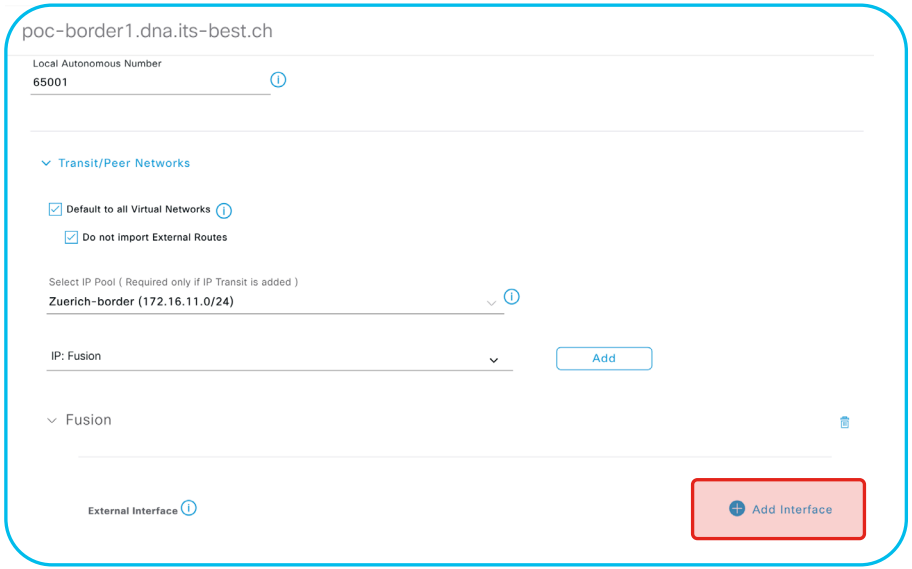
Step 4: L3-Border Handoff (1/2)

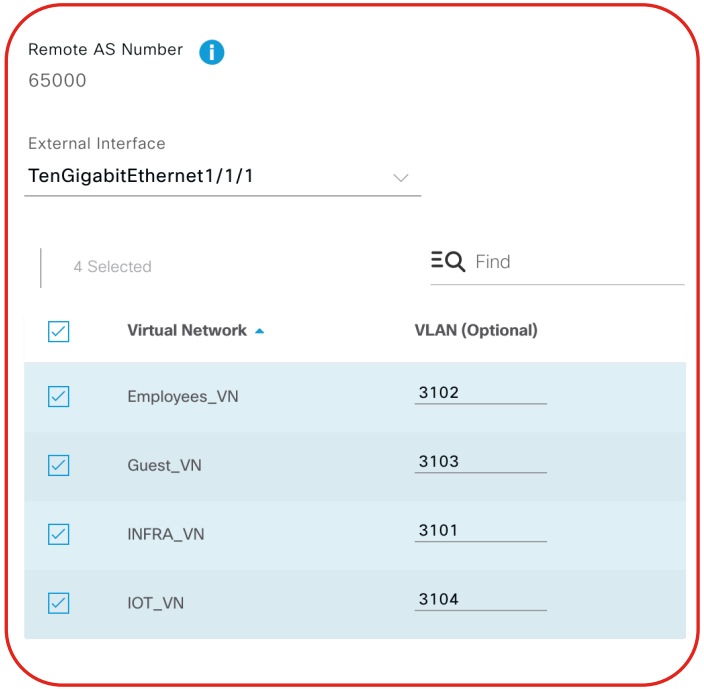




Onboard the Border

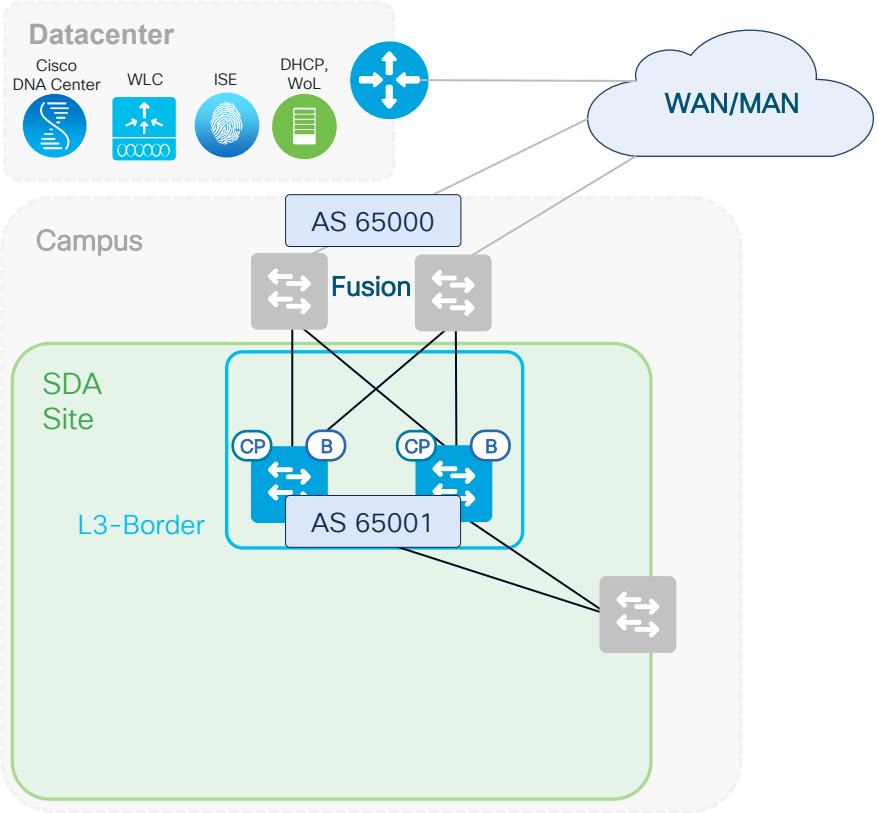
Step 4: L3-Border Handoff (2/2)





Onboard the Border

Conclusion L3-Border



Add DHCP and PnP startup VLAN config to Fusion

Use trunk interface between Fusion and Border

Run LAN Automation for IS-IS & Multicast Config

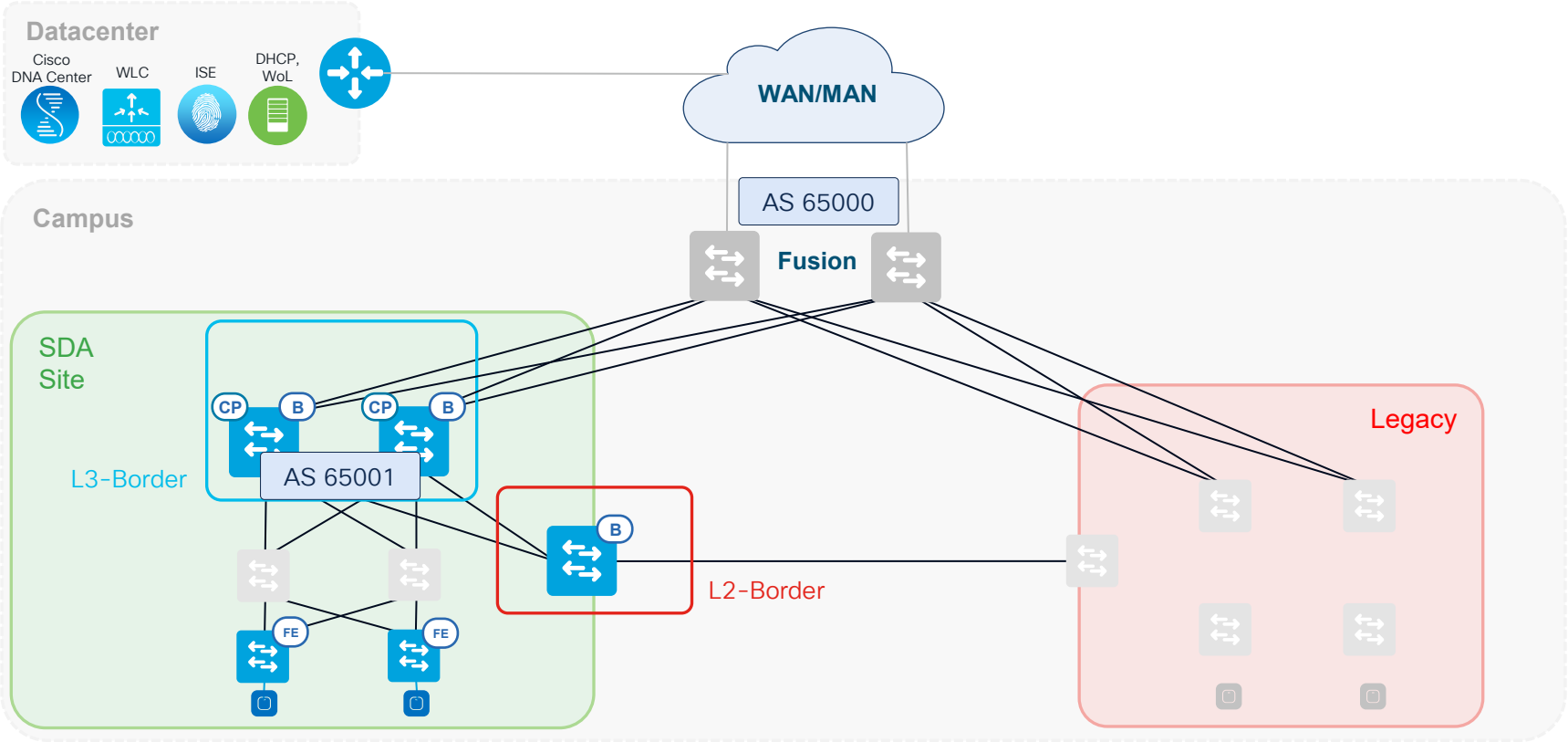
Layer 3 Handoff for all VN's

- Incl. INFRA_VN = underlay
- Add redistribute IS-IS for underlay

Add BGP config on Fusion and remove temporary config (VLAN13, DHCP & static route)

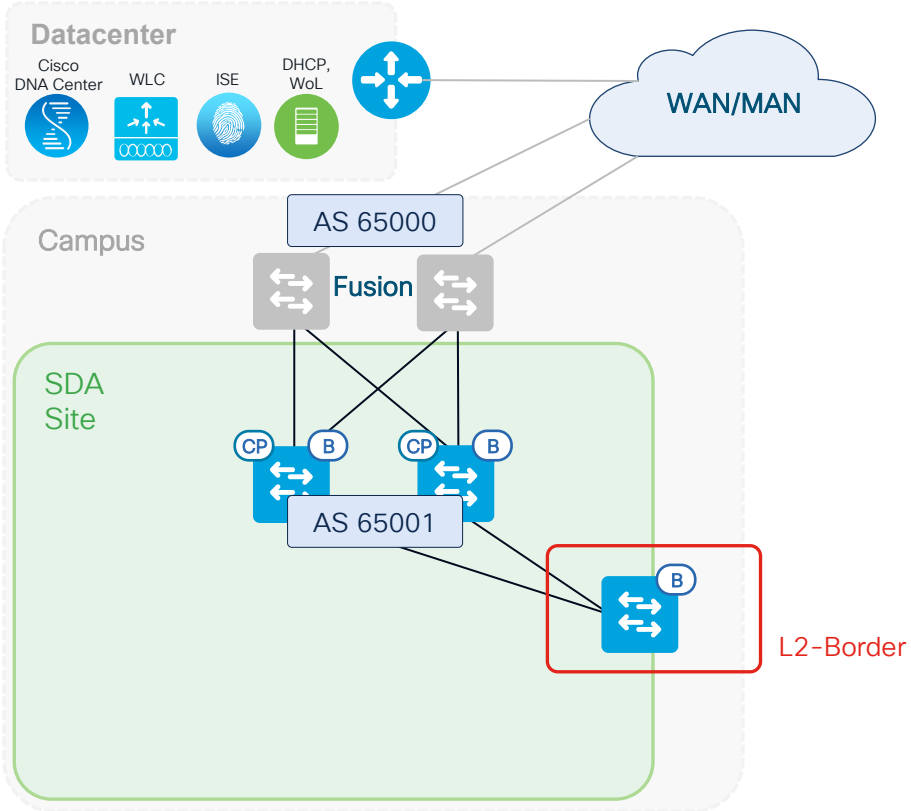
Onboard the Border

High Level Design



Onboard the Border

Introduction L2-Border



Connects your Legacy network via Layer 2 connectivity with the Fabric

Use dedicated L2-Border For Redundancy

- StackWise-480 or
- StackWise Virtual (2.1.2.x+)

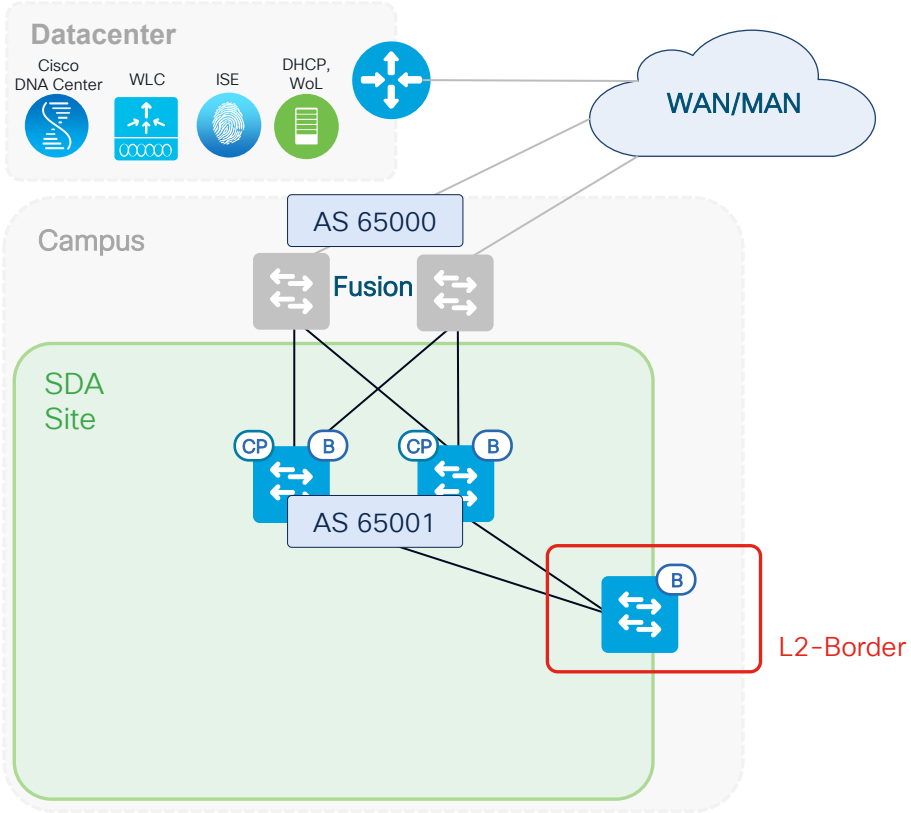
L3 Gateway

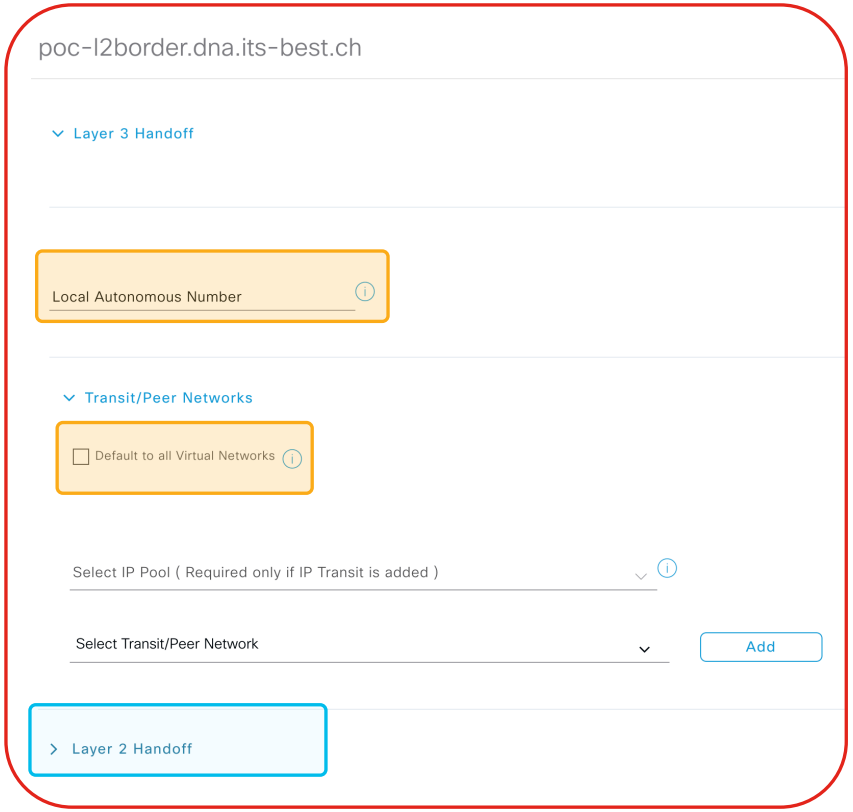
- Move inside the Fabric
- Outside the Fabric (2.1.2.x+)

Reference

Onboard the Border

Step 1: L2-Border configure Local AS





Onboard the Border

Step 2: L2-Border Handoff (1/2)

poc-l2border.dna.its-best.ch

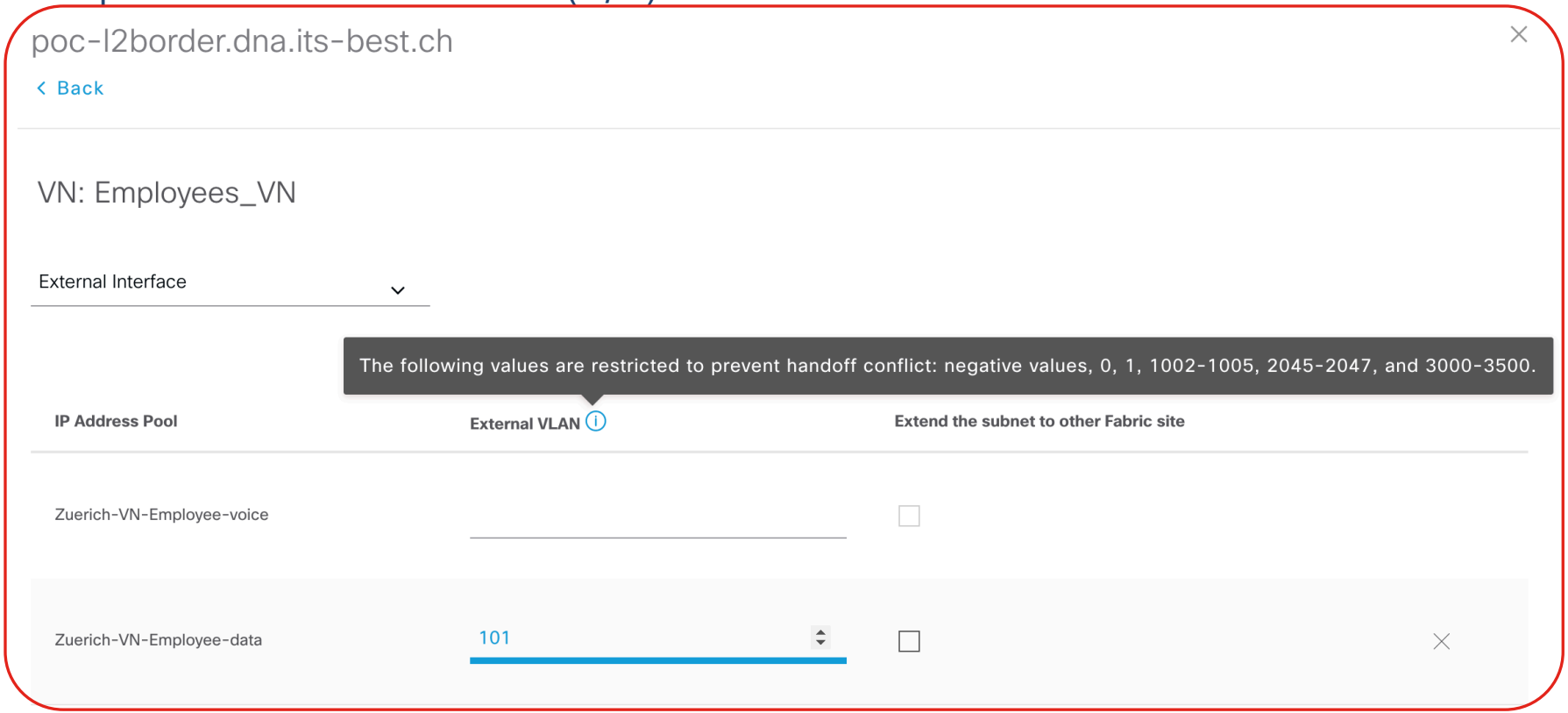
> Layer 3 Handoff

v Layer 2 Handoff

	Virtual Network	IP Pools
☐	IOT_VN	1
☐	Guest_VN	1
☐	Employees_VN	2

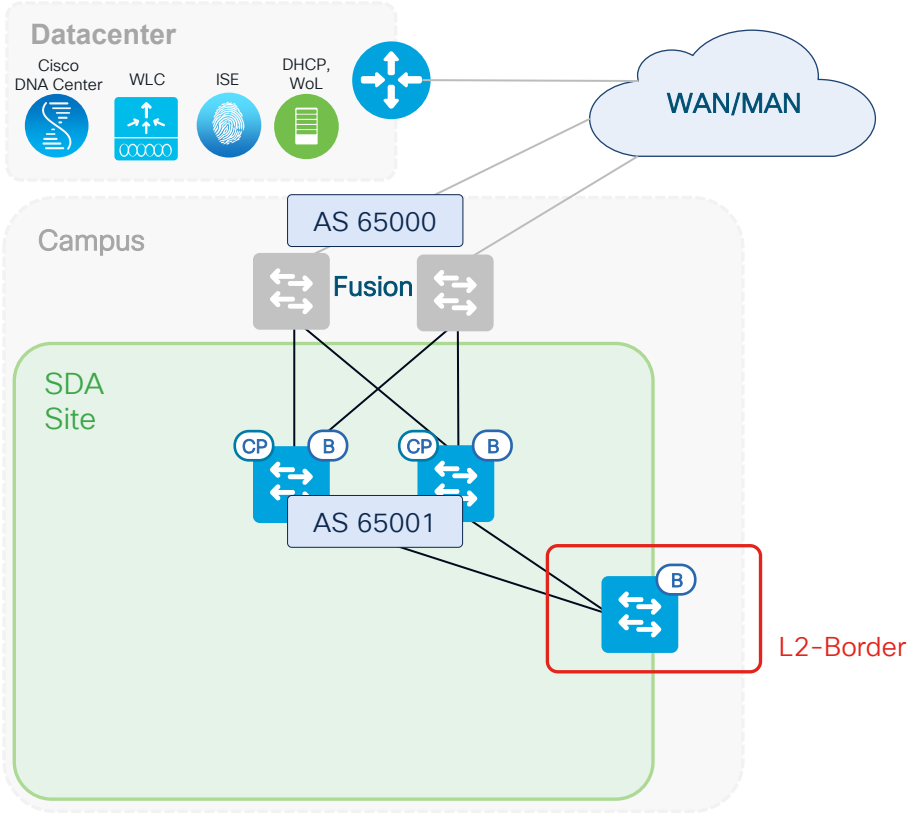
Onboard the Border

Step 2: L2-Border Handoff (2/2)



Onboard the Border

Conclusion L2-Border



- Use dedicated Border for L2 Handoff
- L3 Gateway
  - Move inside the Fabric -> Route IP Pool to External Borders
  - Outside the Fabric -> enable L2 flooding to use external gateway (2.1.2.x+)

SDA for everyone – now even ready for YOUR network!

Demystify Wake-on-LAN & Silent hosts

cisco Live!

What is Wake-on-LAN

Reference

- Wake-on-LAN wakes up a client that is in sleep mode
- A client that is in sleep mode does:
  - usually require less power
  - goes through a state change when moving from active to sleep
  - not respond to normal ethernet frames
  - if it supports WoL and is correctly configured, it wakes up if it is the target of a Wake-on-LAN magic packet

Why do you need Wake-on-LAN

Reference

- you want to patch windows endpoints during not operational times
- you want to wake up sleeping clients before an event/session starts
- you want to make endpoints react as they are very silent otherwise

IP-Directed Broadcast – Wake-on-LAN (WoL) Introduction

Reference

WoL Ethernet Broadcast

- The source and destination are both in the **same** subnet.
- This feature is supported today with the Layer 2 Flooding features introduced in Cisco DNA Center 1.2.5/6.

WoL Subnet Broadcast

- The source and destination are both in **different** subnet.
- Referred to as *Subnet-directed broadcast* or *IP-directed broadcast.*

WoL Magic Packet

- A Broadcast frame that can be sent as an Ethernet Broadcast or Subnet Broadcast.
- Typically sent to UDP destination port 7 or port 9.
- Payload contains *FF FF FF FF FF FF* in hexadecimal followed by sixteen (16) repetitions of the target machine's MAC address.

The magic packet Header – using Ethernet Broadcast

Reference

No.	Time	Source	Destination	Protocol	Info
40	2020-10-21 16:50:10.961631	10.2.17.14	10.2.17.127	WOL	MagicPacket for 98:fa:9b:8c:62:51

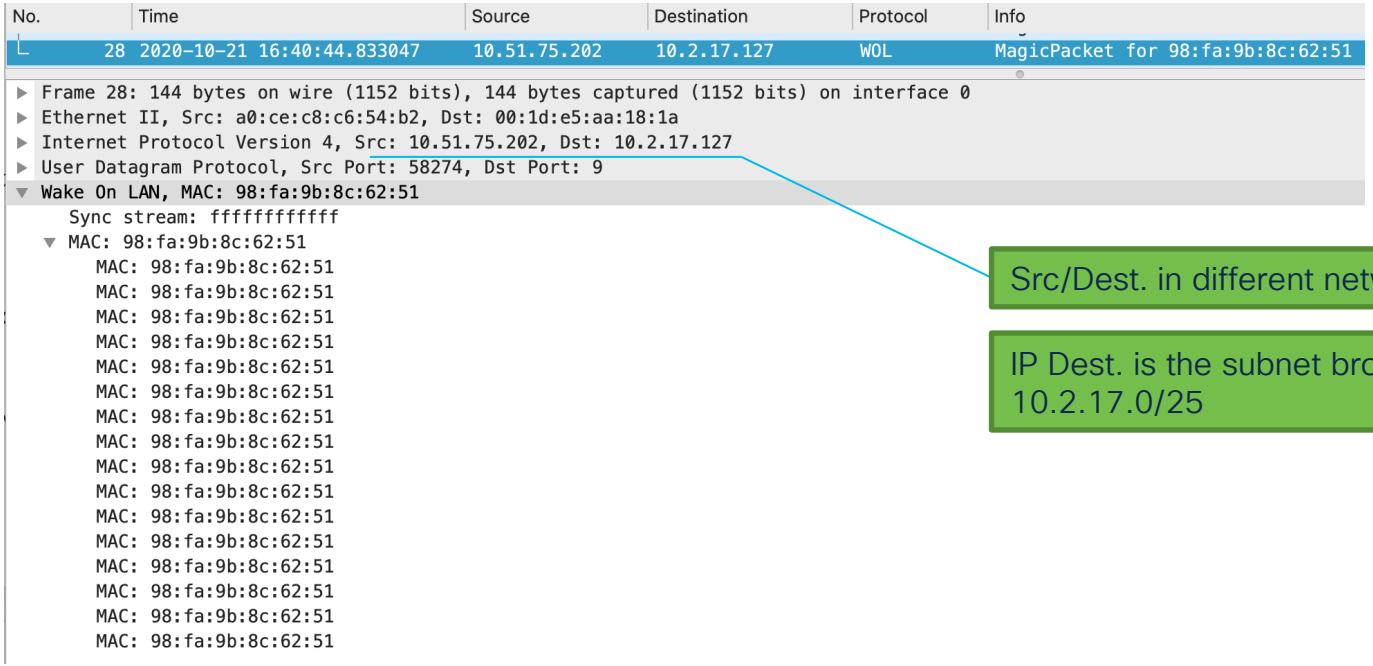
```
▶ Frame 40: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits) on interface 0
▶ Ethernet II, Src: a0:ce:c8:c6:54:b2, Dst: ff:ff:ff:ff:ff:ff
▶ Internet Protocol Version 4, Src: 10.2.17.14, Dst: 10.2.17.127
▶ User Datagram Protocol, Src Port: 64530, Dst Port: 9
▼ Wake On LAN, MAC: 98:fa:9b:8c:62:51
    Sync stream: ffffffffffff
  ▼ MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
      MAC: 98:fa:9b:8c:62:51
```

L2 Broadcast

Src/Dest. on same subnet
IP Dest. Address is the broadcast address of 10.2.17.0/25

The magic packet Header – using IP directed Broadcast

Reference

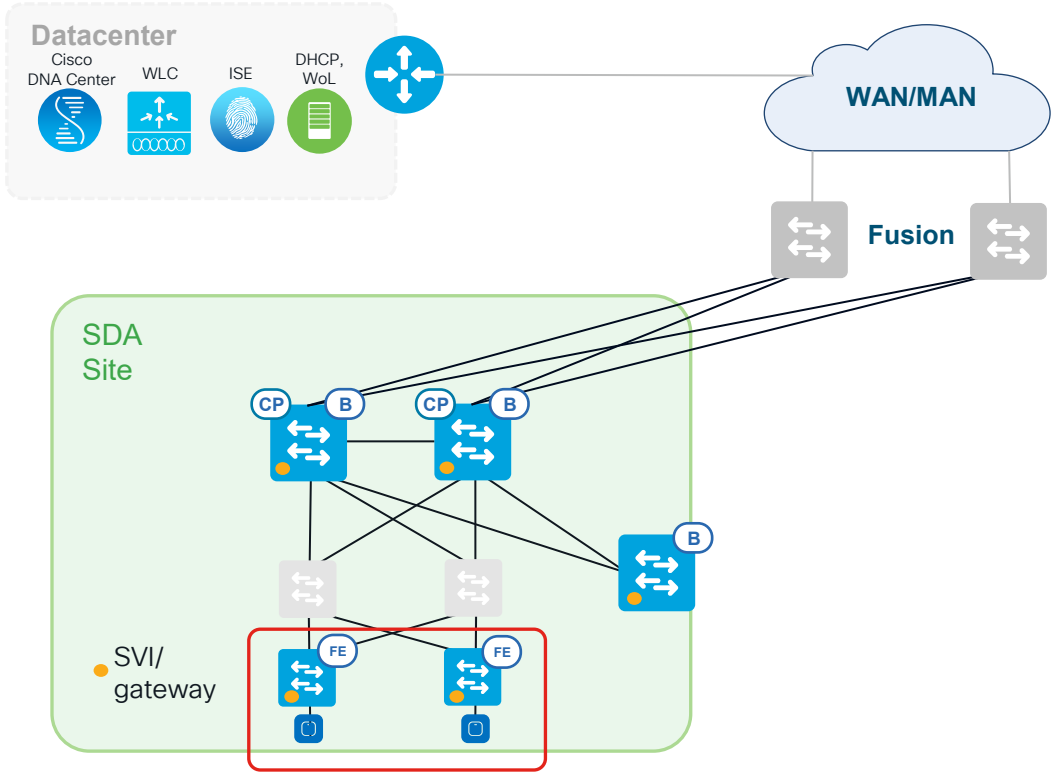


Src/Dest. in different networks

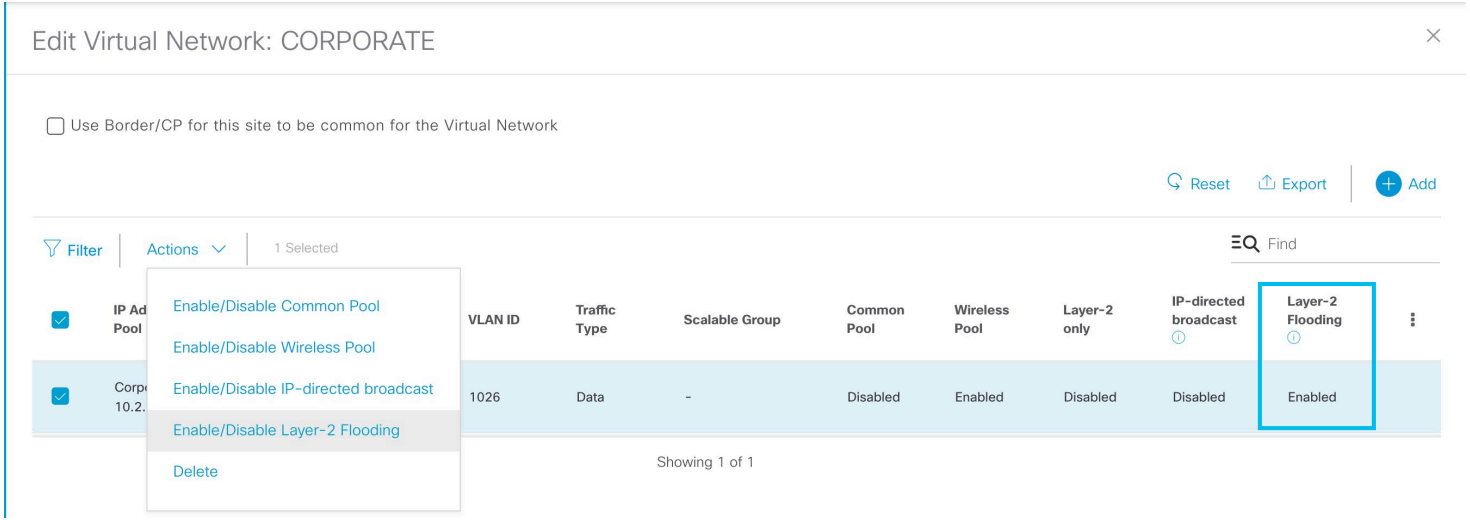
IP Dest. is the subnet broadcast address of 10.2.17.0/25

Challenge #1: Gateway function in SDA

- Without any “tuning” SDA terminates broadcasts on the Edge switch
- Each Edge switch is the gateway – same SVI, same IP, same MAC -> Anycast Gateway



How to solve it – Ethernet Broadcast



Use cases and best practices for subnet broadcast

- L2 flooding might be required if you have BAC NET running in your network – e.g for PLC and building automation installations
- WoL Server and Clients are both part of the same IP address segment in SDA

- Best practice:
- Keep your broadcast segments small – it broadcasts ☺

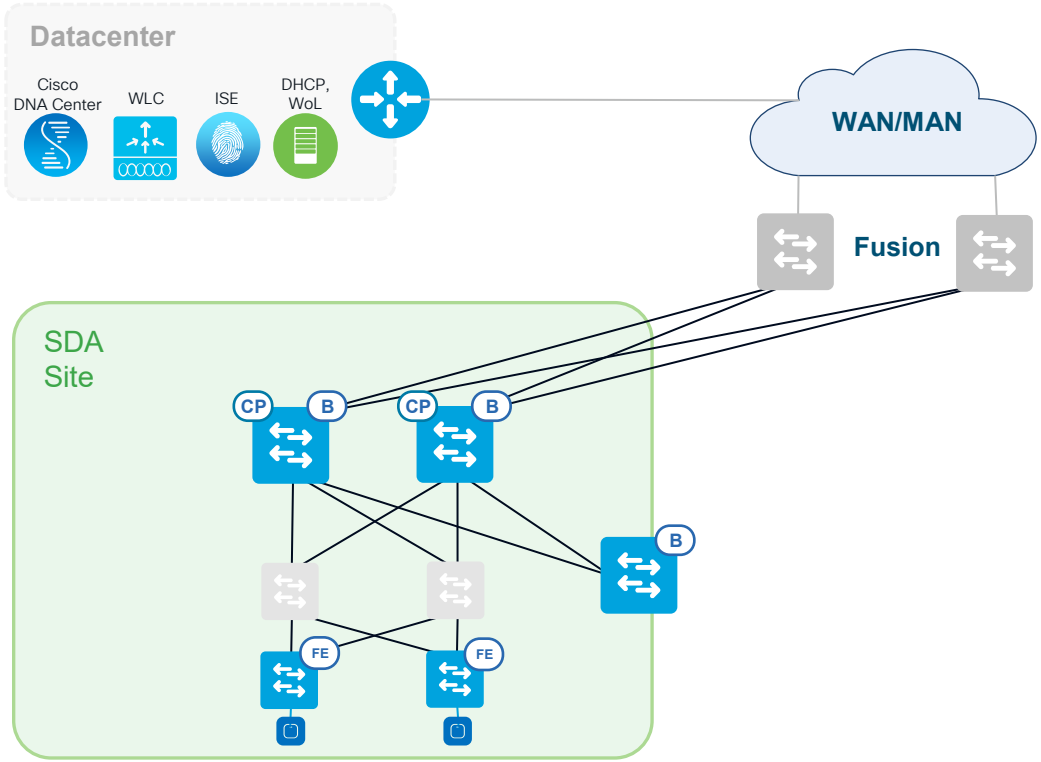
Challenge #2: 802.1x and dynamic vlan assignment

Situation:

Interfaces of Edge switches are in closed Authentication mode

VN / IP Pool assignment happens via ISE

No static assignment applied on interfaces

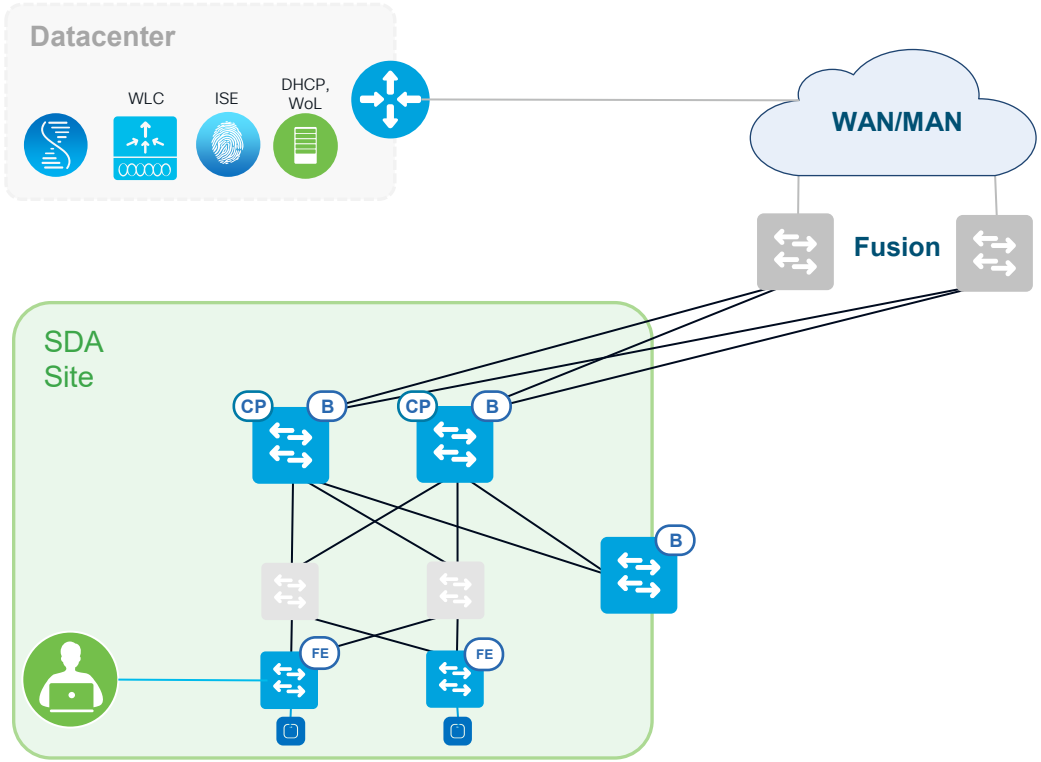


Challenge #2: 802.1x and dynamic vlan assignment

Situation:

User is authenticated/authorized

ISE assigned the User to VN/Pool CORPORATE



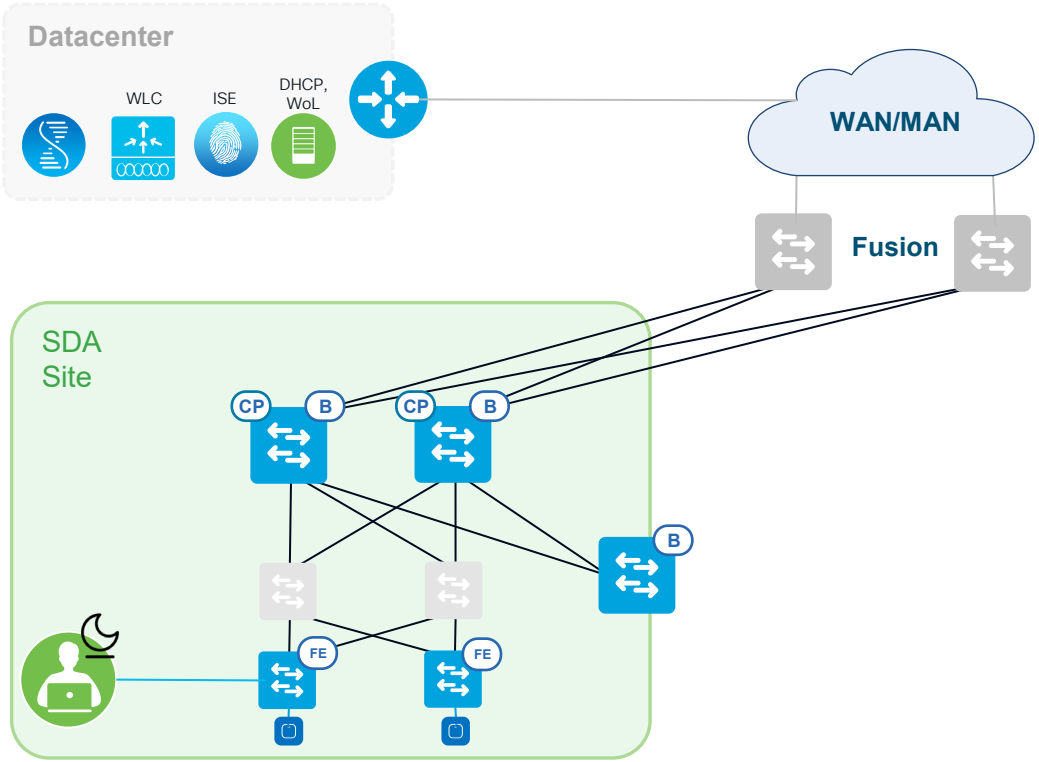
Challenge #2: 802.1x and dynamic vlan assignment

Situation:

Client changes to sleep mode

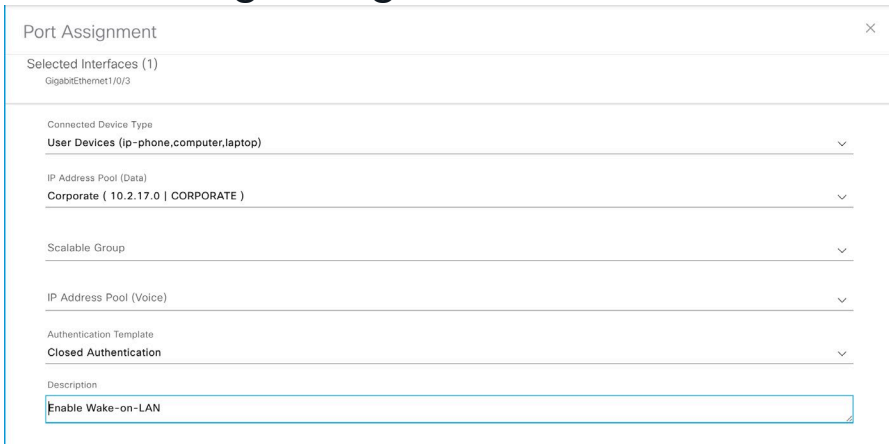
Client executes state change on interface from GE to 100/half

Therefore client is moved to default port setting (Vlan1)



How to solve it – port configuration

- #1: use a static port configuration, ISE authorization has higher priority
  - Drawback: it depends how many ports you need to configure
  - Your WOL segment might differ from the target segment



How to solve it – port configuration

- #2: use an event manager applet that dynamically configures your switch ports
- Configure: `authentication logging verbose`

→ Use DNAC template engine to push it to your edge switches

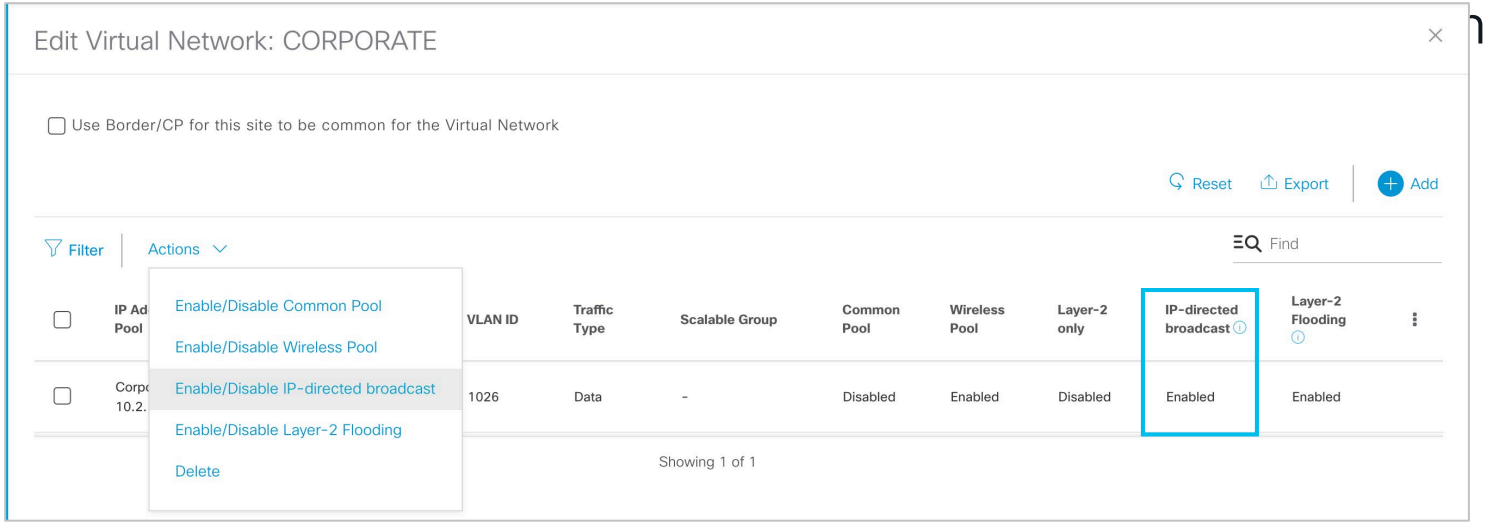
```
event manager applet
Copy_Dynamic_VLAN_Assigned_from_ISE_to_native_vlan
event syslog pattern "%SESSION_MGR-5-SUCCESS:"
action 0.1 regexp "Interface ([^ ]+)" "$_syslog_msg"
match intf
action 0.2 cli command "enable"
action 0.3 cli command "show interface $intf
switchport | include Access Mode VLAN"
action 0.4 regexp "Access Mode VLAN: ([0-9]+)"
"$_cli_result" match OPER_VLAN
action 0.5 syslog msg "Dynamically set vlan is
$OPER_VLAN"
action 0.6 cli command "config terminal"
action 0.7 cli command "interface $intf"
action 0.8 cli command "switchport access vlan
$OPER_VLAN"
action 0.9 cli command "exit"
```

Wake-on-LAN from outside of the fabric

- If your Wake-on-LAN server is located in a Datacenter outside of the fabric, directed Broadcast usually doesn't go through
  - Your Default gateway configuration in the server segment will block it
  - The Border will not translate it to vxlan

How to solve it – IP directed Broadcast

- Step 1: enable ip directed-broadcast on your Server Gateway
- Step 2: enable L2-Flooding for the segment



Use cases and best practices – IP directed broadcast

- use cases:
- WoL Server is outside of the fabric, your WoL Clients are part of the fabric
- Wake up sleepy clients that don't talk regulary
- Best practice:
- Keep your broadcast segments small – it broadcasts ☺

- Device Support:
- DNAC 1.2.5/6 for L2-Broadcast
- DNAC 2.1.2.4 for directed-Broadcast
- Routers, Nexus 7700 are not supported
- Edge and Border require ≥ 17.3.1

SDA for everyone – now even ready for YOUR network!

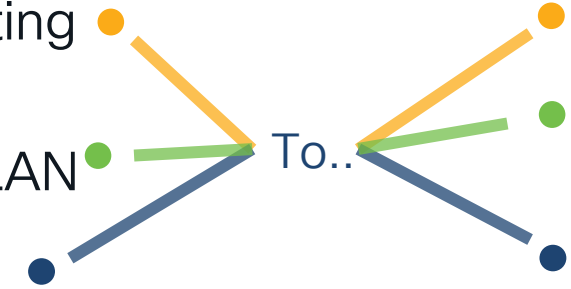
Conclusion

... there is a way ...

to migrate an existing network

to use Wake-on-LAN

to get Silent Host



participate in an SDA network

Wake-Up Hosts in an SDA network

Integrated in an SDA network

Where to go next....

- BRKCSR-2811 Connecting the Fabric to External Networks
- BRKCRS-2810 Cisco SD-Access Fundamentals
- BRKSDN-2500 Real World Use Cases for Deploying and Operating Cisco SD-Access Using Cisco DNA Center

SDA for everyone – now even ready for YOUR network!

The bridge to possible

Thank you


cisco Live!
TURN
IT
UP
#CiscoLive

Appendix


cisco Live!
TURN
IT
UP
#CiscoLive