Cisco live!

6-9 March 2018 · Melbourne, Australia

Cisco SD-Access
Monitoring and Troubleshooting

Parthiv Shah, Technical Leader, Escalation

Derek Huckaby, Technical Marketing Engineer

BRKCRS-2813

Cisco live!

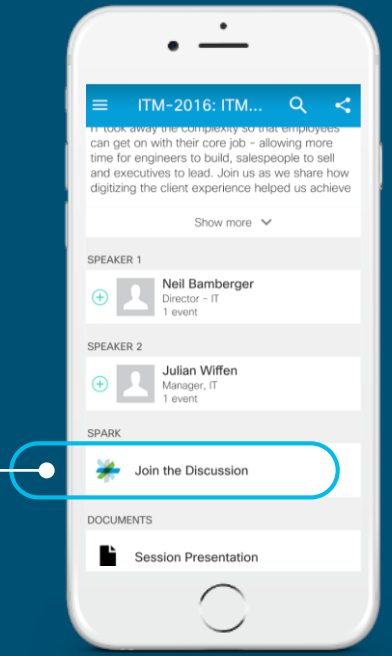
Cisco Spark

Questions?

Use Cisco Spark to communicate with the speaker after the session

How

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



Agenda

- DNA Architecture Overview
- DNA Center Troubleshooting
  - Install / Services Debugging
  - Log Collection
  - ISE and DNA Center Integration
  - Device Discovery
  - Provisioning
- SD-Access Fabric Troubleshooting
  - Host Onboarding
  - DHCP
  - External Connectivity
  - Host Mobility

Objectives and Assumptions

Objectives

After completing this module you will:

- Understand the DNA Center Server Troubleshooting
- Understand SD-Access Fabric Deployment and Troubleshooting
- Understand SD-Access Host Onboarding and Troubleshooting

Assumptions

- Audience must be familiar with ISE deployment scenarios, pxGrid and Cisco TrustSec.
- Working knowledge of APIC-EM and PKI.
- Working knowledge of Routing/Switching and Cisco Fabric architecture.
- This session will not cover CLI based Cisco Fabric or ISE troubleshooting.

DNA Architecture Overview

The DNA Center Appliance

DNA Center Platform

DN1-HW-APL

DNAC 1.1 Scale: Per Node

- 5,000 Nodes (1K Devices + 4K APs)
- 25,000 Clients (Concurrent Hosts)

Fully Integrated Automation & Assurance

- Centralised Deployment - Cloud Tethered
- Built-In Telemetry Collectors (FNF, SNMP, Syslog, etc)
- Built-In Contextual Connectors (ISE/pxGrid, IPAM, etc)
- Multi-Node High Availability (3 Node, Automation)
- RBAC, Backup & Restore, Scheduler, APIs

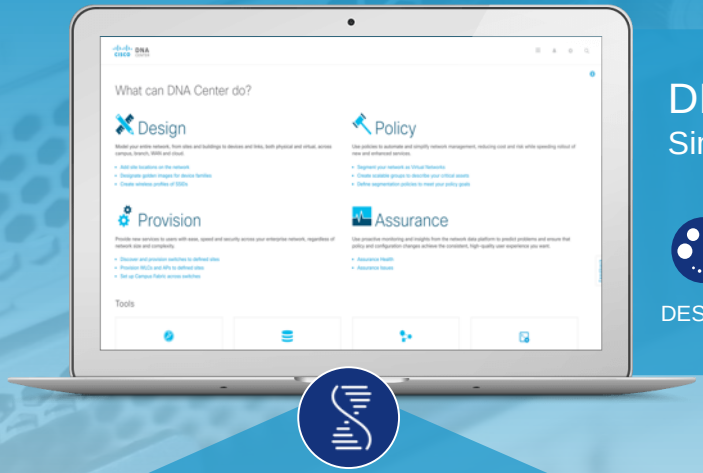
1RU Server (Small form factor)

- UCS 220 M4: 64-bit x86
- vCPU: 44 core (2.2GHz)
- RAM: 256GB DDR4
- Control Disks: 2 x 480GB SSD RAID1
- System Disks: 6 x 1.9TB SSD M-RAID
- Network: 2 x 10GE SFP+
- Power: 2 x 770W AC PSU

Single Appliance for DNAC (Automation + Assurance)

DNA Solution

Cisco Enterprise Portfolio



DNA Center

Simple Workflows

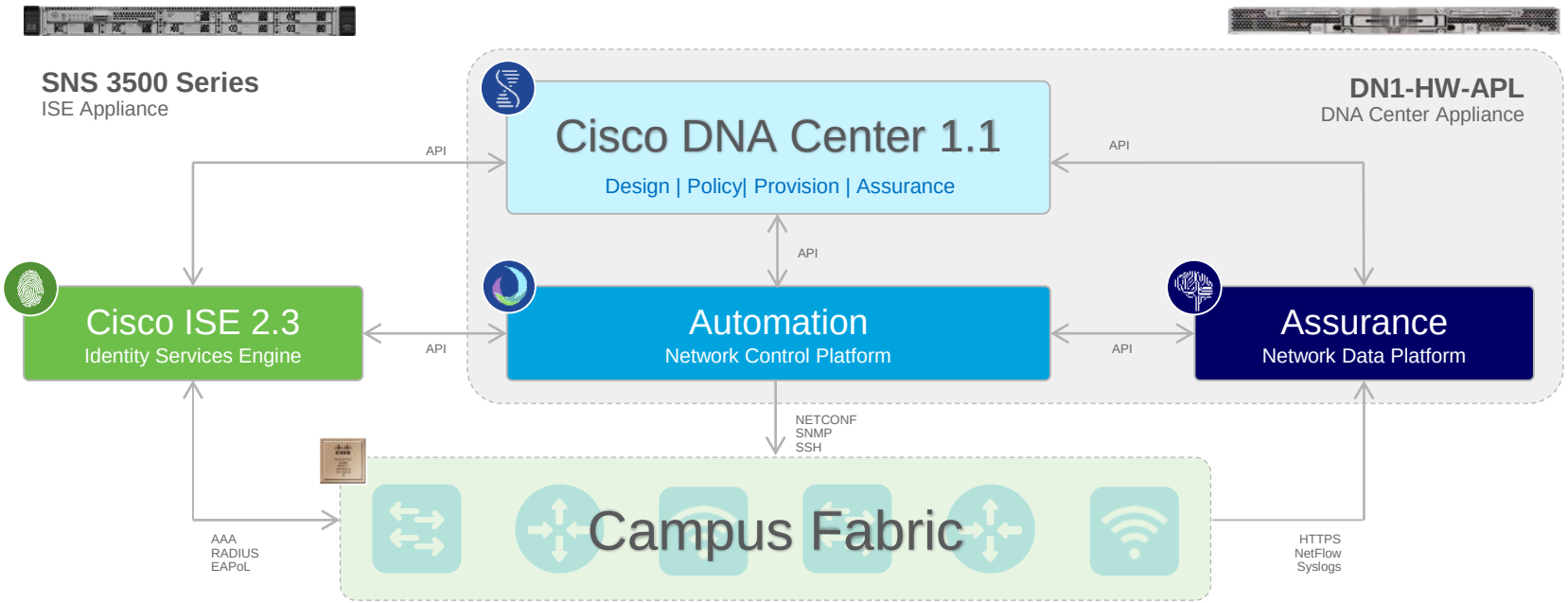
DESIGN — PROVISION — POLICY — ASSURANCE

DNA Center

Identity Services Engine — Network Control Platform — Network Data Platform

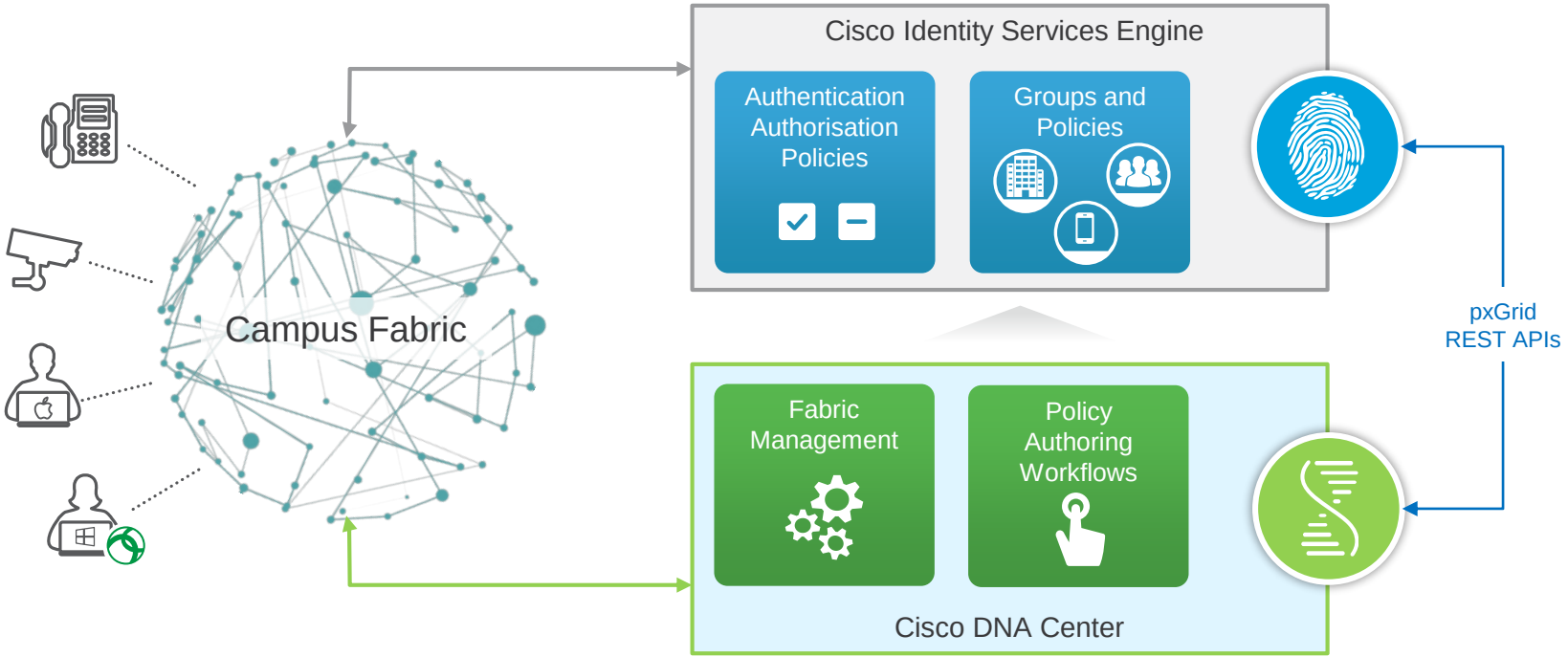
Routers | Switches | Wireless Controllers | Wireless APs

DNA Controller and Service Components



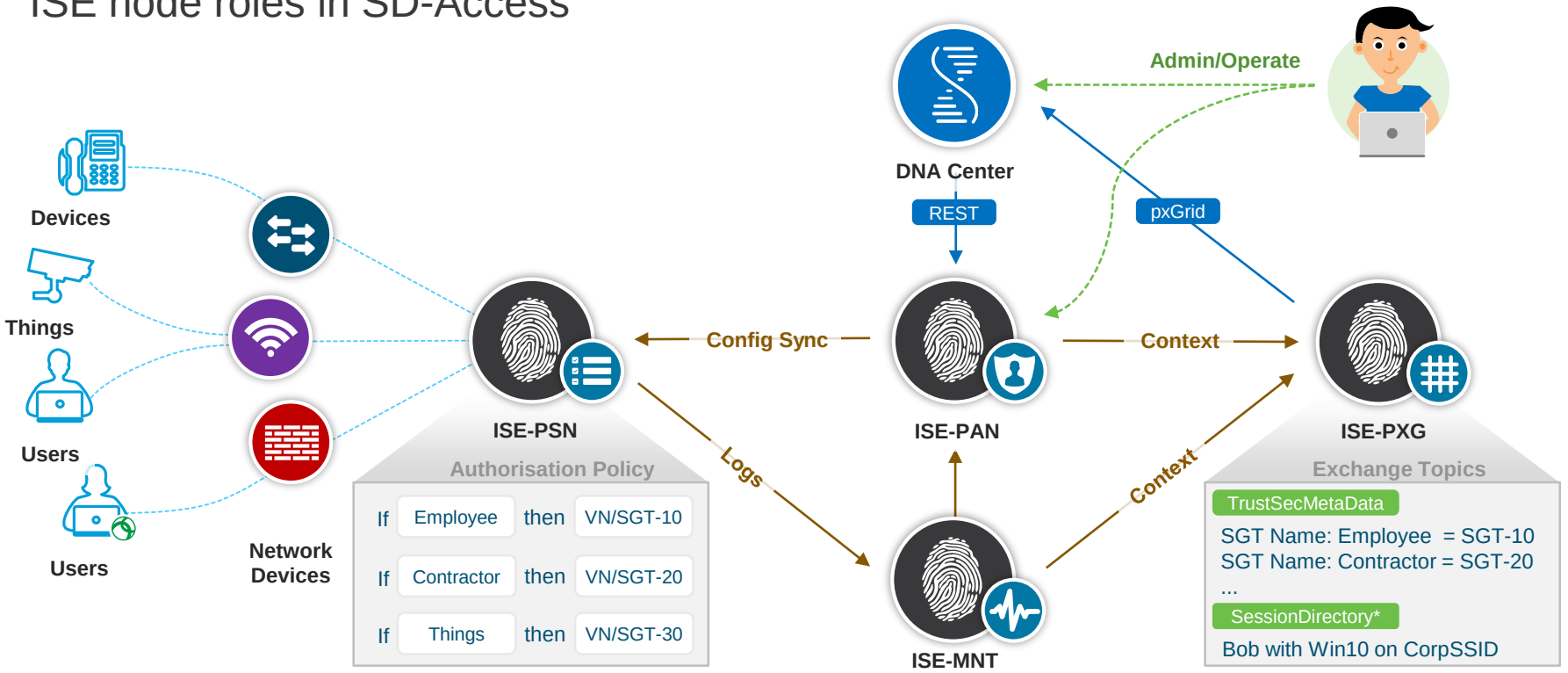
DNA Center and ISE integration

Identity and Policy Automation



DNA Center and ISE integration

ISE node roles in SD-Access



DNA Center Solution Basic Pre-requisite

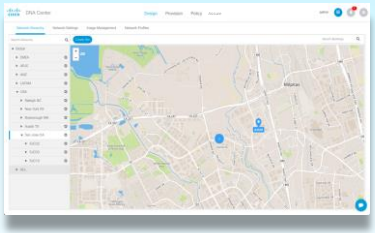
- Hardware
  - Supported DNA Center Appliance (DN1-HW-APL)
  - Supported switch/router/WLC/AP models
- Software
  - Check various platform for recommended IOS-XE software version
  - Check License for planned platforms
  - Recommended ISE and DNA Center software
- Underlay/Overlay
  - IP address plan for DNA Center and ISE
  - Check for underlay network / routing configured correctly and devices are reachable
  - Reachability to Internet – Direct or Proxy connection
  - Access to an NTP server
    - Make sure DNA Center appliance is close to real time using CIMC

DNA Center Troubleshooting

DNA Center

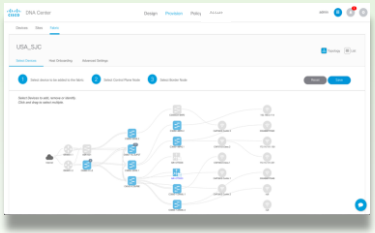
SD-Access 4 Step Workflow

Design



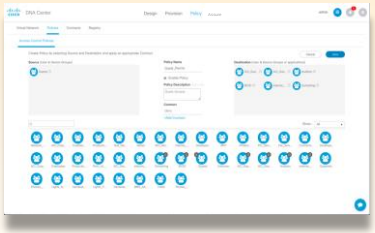
- Global Settings
- Site Profiles
- DDI, SWIM, PNP
- User Access

Provision



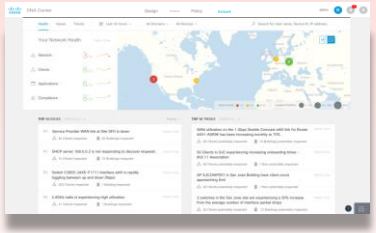
- Fabric Domains
- CP, Border, Edge
- FEW, OTT WLAN
- External Connect

Policy



- Virtual Networks
- ISE, AAA, Radius
- Endpoint Groups
- Group Policies

Assurance

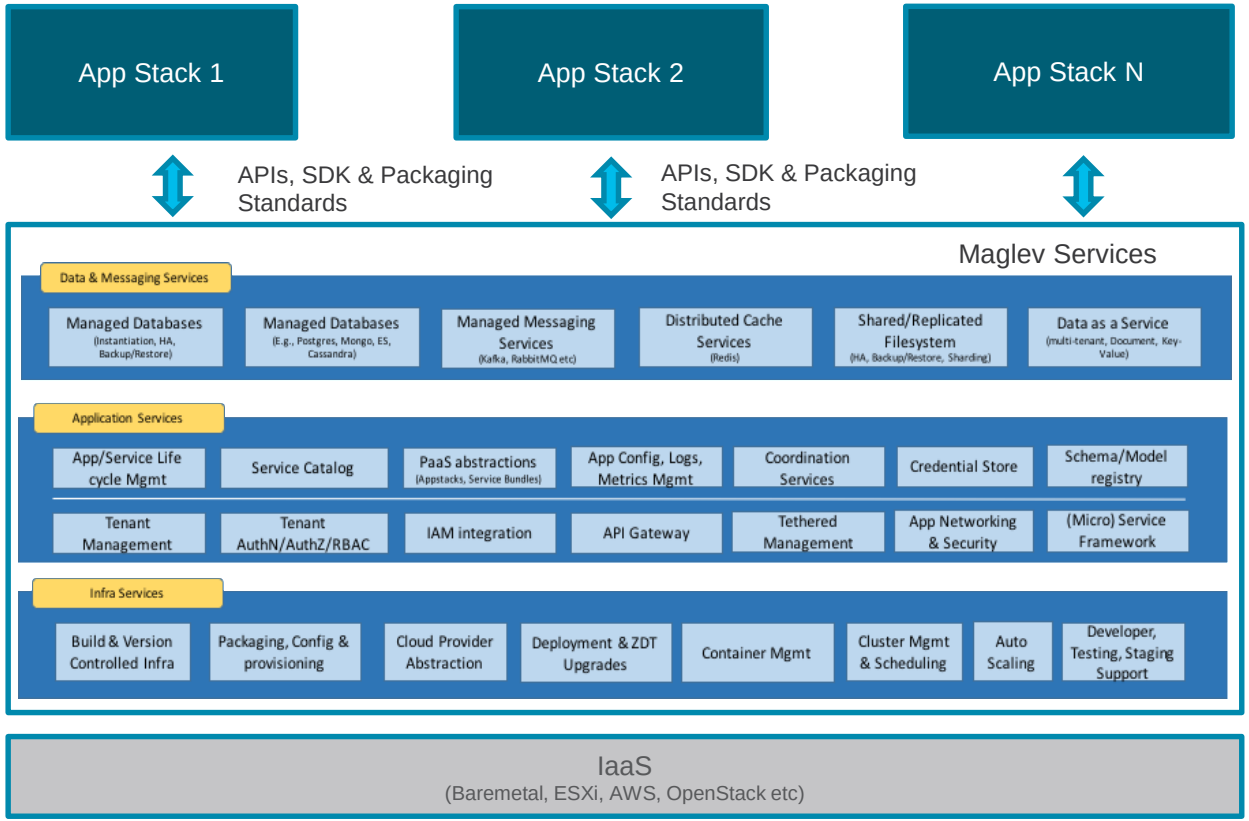


- Health Dashboard
- 360º Views
- FD, Node, Client
- Path Traces

Planning & Preparation

Installation & Integration

DNA Center – Maglev Logical Architecture



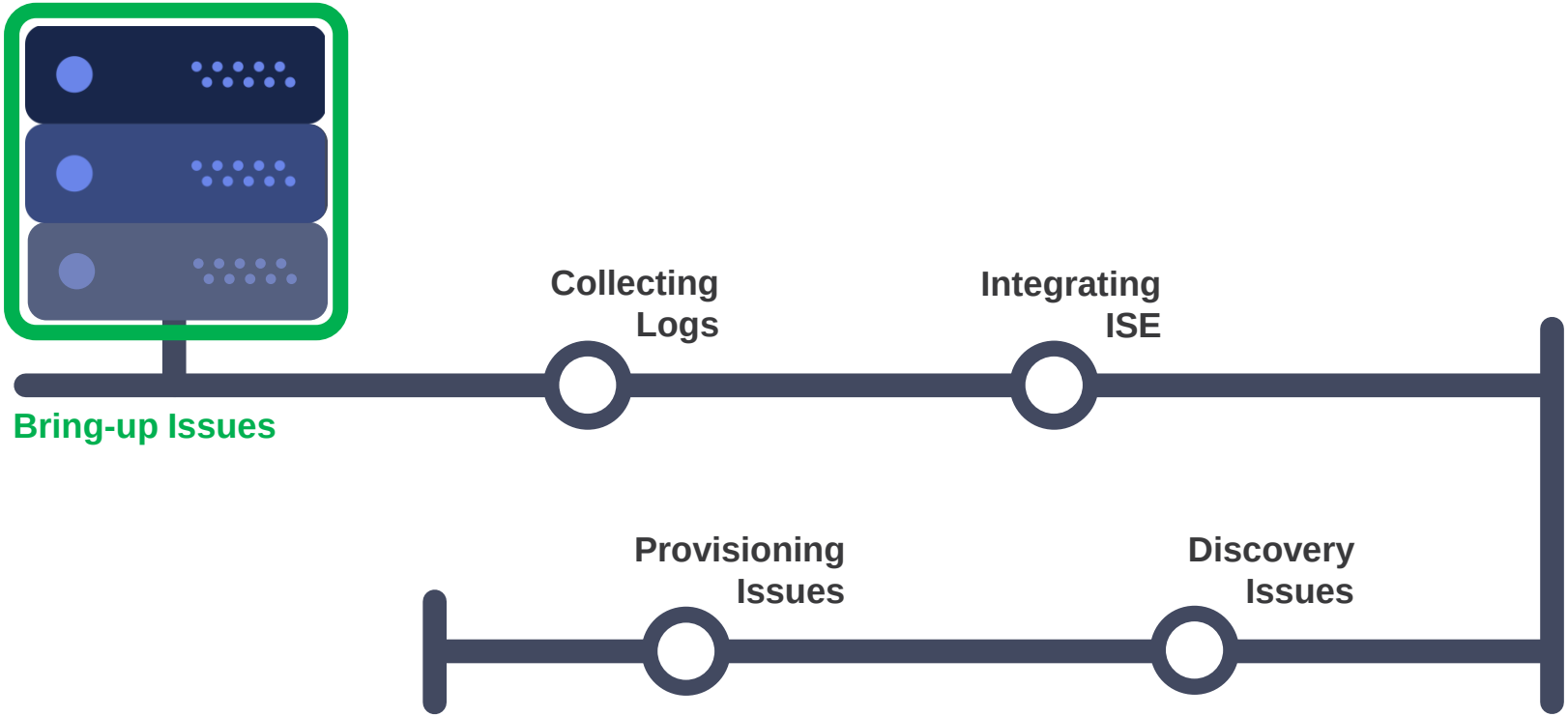
Most Commonly Used Maglev CLI

```
$ maglev
Usage: maglev [OPTIONS] COMMAND [ARGS]...
  Tool to manage a Maglev deployment
Options:
  --version           Show the version and exit.
  -d, --debug         Enable debug logging
  -c, --context TEXT  Override default CLI context
  --help              Show this message and exit.
Commands:
  backup                Cluster backup operations
  catalog               Catalog Server-related management operations
  completion            Install shell completion
  context               Command line context-related operations
  cronjob               Cluster cronjob operations
  job                   Cluster job operations
  login                 Log into the specified CLUSTER
  logout                Log out of the cluster
  maintenance           Cluster maintenance mode operations
  managed_service       Managed-Service related runtime operations
  node                  Node management operations
  package               Package-related runtime operations
  restore               Cluster restore operations
  service               Service-related runtime operations
  system                System-related management operations
  system_update_addon   System update related runtime operations
  system_update_package System update related runtime operations
```

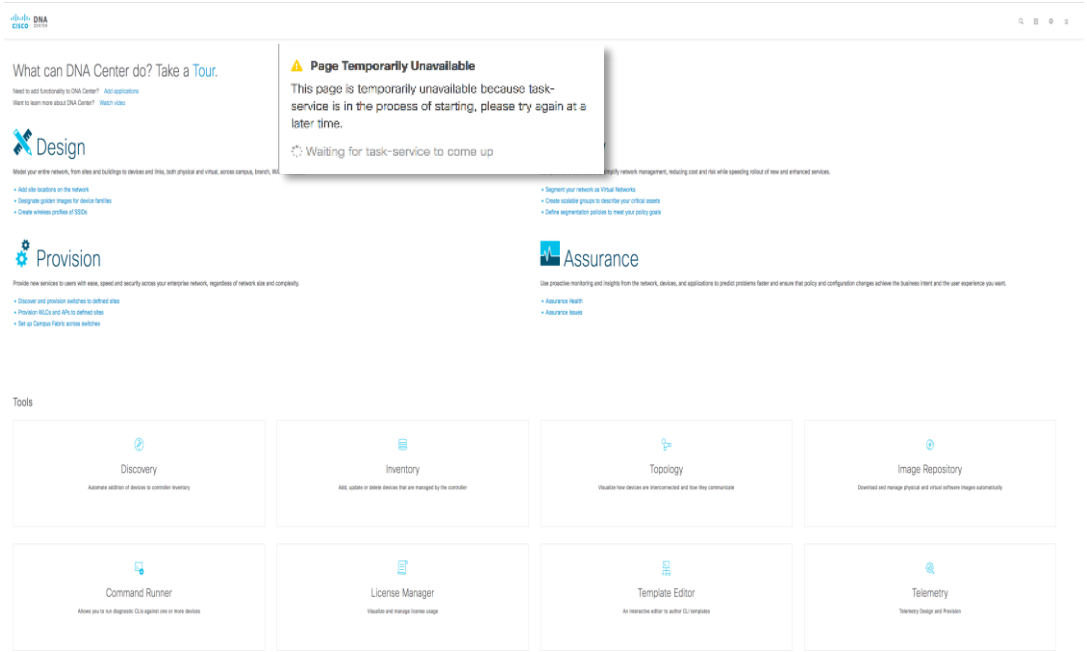
```
$ magctl
Usage: magctl [OPTIONS] COMMAND [ARGS]...
  Tool to manage a Maglev deployment
Options:
  --version    Show the version and exit.
  -d, --debug  Enable debug logging
  --help       Show this message and exit.


Commands:
  api         API related operations
  appstack    AppStack related operations
  completion  Install shell completion
  disk        Disk related operations
  glusterfs   GlusterFS related operations
  iam         Identitymgmt related operations
  job         Job related operations
  logs        Log related operations
  maglev      Maglev related commands
  node        Node related operations
  service     Service related operations
  tenant      Tenant related operations
  token       Token related operations
  user        User related operations
  workflow    Workflow related operations
```

List of Important Fusion Package Services

apic-em-event-service	Trap events, host discovery we leverage snmp traps so they are handled here.
apic-em-inventory-manager-service	Provides communication service between inventory and discovery service
apic-em-jboss-ejbca	Certificate authority and enables controller authority on the DNAC.
apic-em-network-programmer-service	Configure devices. Critical service to check during provisioning.
apic-em-pki-broker-service	PKI Certificate authority
command-runner-service	Responsible for Command Runner related task
distributed-cache-service	Infrastructure
dna-common-service	DNAC-ISE integration task
dna-maps-service	Maps Related services
dna-wireless-service	Wireless
identity-manager-pxgrid-service	DNAC-ISE integration task
ipam-service	IP Address manager
network-orchestration-service	Critical during Provisioning orchestation.
orchestration-engine-service	Orchestration Service
pnp-service	PNP Tasks
policy-analysis-service	Policy related
policy-manager-service	Policy related
postgres	Core database management system
rbac-broker-service	RBAC
sensor-manager	Sensor Related
site-profile-service	Site Profiling
spf-device-manager-service	Core service during Provisioning phase
spf-service-manager-service	Core service during Provisioning phase
swim-service	SWIM



DNA Center Services are not coming up



Have Patience

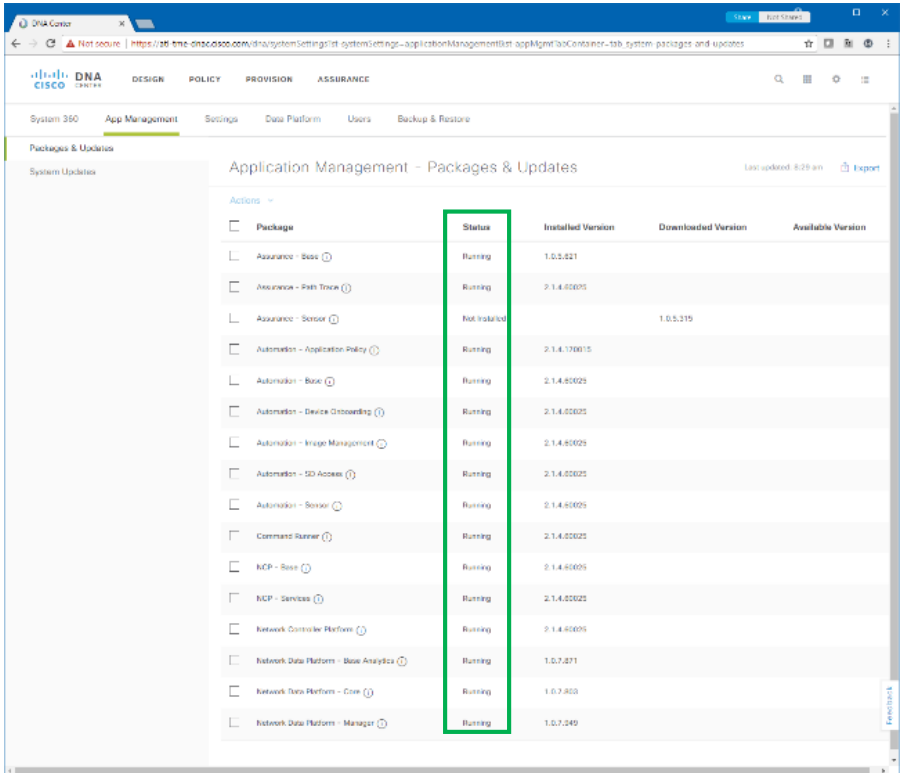
60 to 180 minutes bring-up time

- Make sure supported hardware used
- Check network connectivity
- Check NTP server reachability
- Check any specific service not coming up
- **During install or update use GUI** as much as possible (Avoid console login or don't run any system related commands)

Package Status – GUI v/s CLI

How to Check Package Status from GUI

System Settings → App Management: Packages & Updates



How to Check Package Status from CLI

`maglev package status`

```
$ maglev package status

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]
NAME                          DEPLOYED        AVAILABLE       STATUS
------------------------------------------------------------------------------
application-policy            2.1.1.170016    -               DEPLOYED
assurance                     1.0.5.503       1.0.5.583       DEPLOYED
automation-core               2.1.0.64153     2.1.1.60067     DEPLOYED
base-provision-core           2.1.1.60067     -               DEPLOYED
command-runner                2.1.1.60067     -               DEPLOYED
device-onboarding             2.1.1.60067     -               DEPLOYED
image-management              2.1.1.60067     -               DEPLOYED
ncp-system                    2.1.1.60067     -               DEPLOYED
ndp-base-analytics            1.0.6.342       1.0.7.823       DEPLOYED
ndp-platform                  1.0.6.246       1.0.7.724       DEPLOYED
ndp-ui                        1.0.6.454       1.0.7.919       DEPLOYED
network-visibility            2.1.1.60067     -               UPGRADING
path-trace                    2.1.0.64153     2.1.1.60067     DEPLOYED
sd-access                     2.1.1.60067     -               DEPLOYED
sensor-assurance              -               1.0.5.301       NOT_DEPLOYED
sensor-automation             -               2.1.1.60067     NOT_DEPLOYED
system                        1.0.4.633       1.0.4.661       DEPLOYED
```

Install Failure

If you are unable to run maglev/magctl commands after install:

- Check RAID configuration and install error messages
- USB 3.0 is recommended for installation.
- Avoid KVM and/or USB 2.0 or NFS mount method for installation
- Use Windows 10 or Linux/Mac based system to build burn ISO image.
- Check for Error or Exception in following log files:
  - /var/log/syslog
  - /var/log/maglev_config_wizard.log

Package Mapping – GUI v/s CLI

CLI Package Name	GUI Display Name
application-policy	Automation - Application Policy
assurance	Assurance - Base
automation-core	NCP - Services
base-provisioning-core	Automation - Base
command-runner	Command Runner
core-network-visibility	Network Controller Platform
device-onboarding	Automation - Device Onboarding
image-management	Automation - Image Management
iwan	IWAN
migration-support	
ncp-system	NCP - Base
ndp	Network Data Platform
ndp-base-analytics	Network Data Platform - Base Analytics
ndp-platform	Network Data Platform - Core
Ndp-ui	Network Data Platform - Manager
Network-visibility	Network Controller Platform
path-trace	Assurance - Path Trace
sd-access	Automation - SD Access
system	System Or Infrastructure
waas	Automation - WAAS
sensor-automation	Automation - Sensor
sensor-automation	Assurance - Sensor

GUI Display Name	CLI Package Name
Automation - Application Policy	application-policy
Assurance - Base	assurance
Assurance - Path Trace	path-trace
Assurance - Sensor	sensor-automation
Automation - Base	base-provisioning-core
Automation - Device Onboarding	device-onboarding
Automation - Image Management	image-management
Automation - SD Access	sd-access
Automation - Sensor	sensor-automation
Automation - WAAS	waas
Command Runner	command-runner
IWAN	iwan
NCP - Base	ncp-system
NCP - Services	automation-core
Network Controller Platform	core-network-visibility
Network Controller Platform	Network-visibility
Network Data Platform	ndp
Network Data Platform - Base Analytics	ndp-base-analytics
Network Data Platform - Core	ndp-platform
Network Data Platform - Manager	Ndp-ui
System Or Infrastructure	system
	migration-support

Package Update – GUI v/s CLI

How to get GUI name from CLI

`maglev catalog package display base-provision-core | grep display`

```
$ maglev catalog package display
maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]

NAME                VERSION         STATE      INFO
-------------------------------------------------------------------
application-policy  2.1.1.170016    READY
assurance           1.0.5.583       READY
automation-core     2.1.1.60067     READY
base-provision-core 2.1.1.60067     READY
command-runner      2.1.1.60067     READY
device-onboarding   2.1.1.60067     READY
image-management    2.1.1.60067     READY
ncp-system          2.1.1.60067     READY
ndp-base-analytics  1.0.7.823       PARTIAL    Package needs to
ndp-platform        1.0.7.724       PARTIAL    Package needs to
ndp-ui              1.0.7.919       PARTIAL    Package needs to
network-visibility  2.1.1.60067     READY
path-trace          2.1.1.60067     READY
sd-access           2.1.1.60067     READY
sensor-assurance    1.0.5.301       PARTIAL    Package needs to
sensor-automation   2.1.1.60067     READY
system              1.0.4.661       PARTIAL    Package needs to
```

```
$ maglev catalog package display automation-core | grep display
displayName: NCP - Services

[Fri Jan 19 00:25:39 UTC] maglev@172.27.255.230 (maglev-master-1) ~
$ maglev catalog package display base-provision-core | grep display
displayName: Automation - Base
```

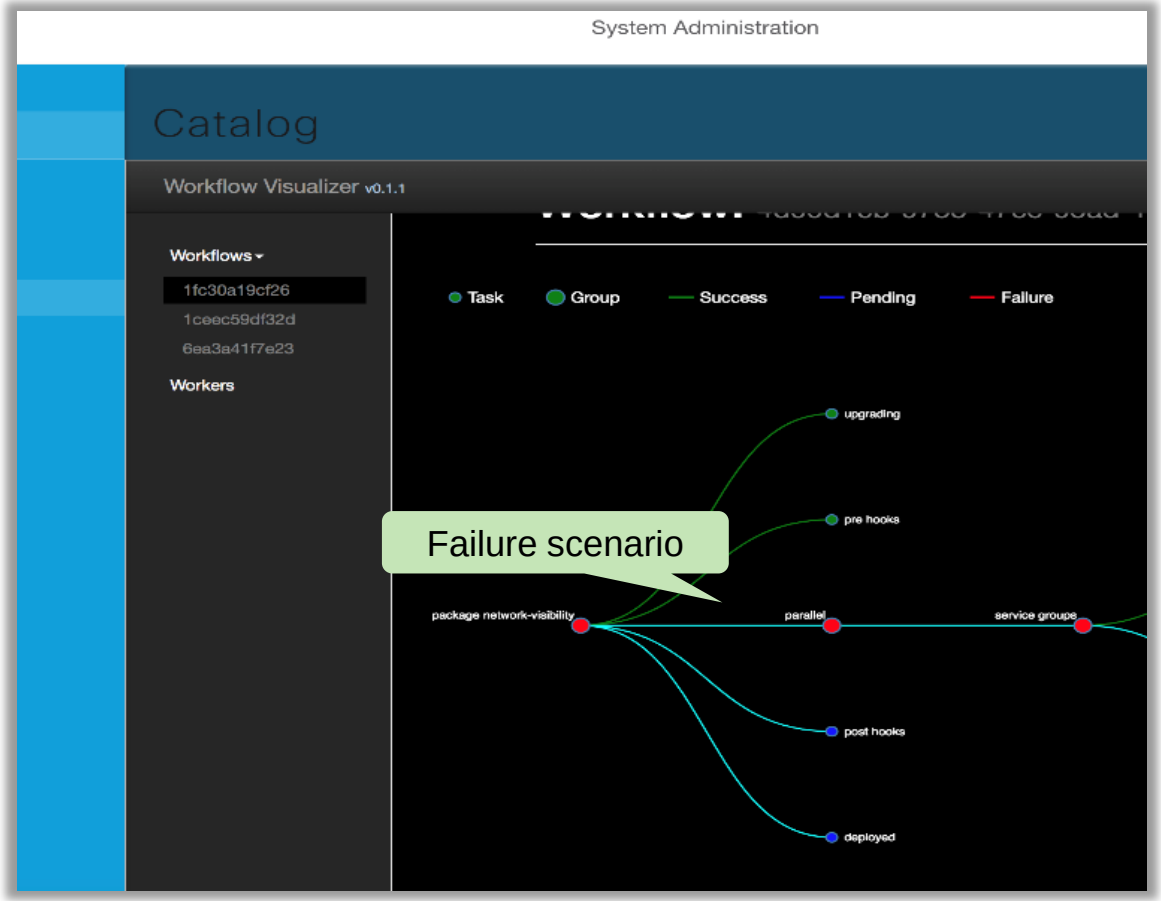
```
$ maglev catalog package status network-visibility
maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]

KIND                RESOURCE                                                                                    STATE      MESSAGE
-------------------------------------------------------------------------------------------------------------------------------
Package             network-visibility:2.1.3.60048                                                              READY
Plugin              fusion/cli-template/devicecontrollability-cli-template-plugin:7.7.3.60048 READY
Plugin              fusion/cli-template/perfmon-cli-template-plugin:7.7.3.60048 READY
Plugin              fusion/cli-template/wlc-dynamic-qos-cli-template-plugin:7.7.3.60048 READY
.
.
.
ServiceBundle       fusion/apic-em-event-service:7.1.3.60048      READY
ServiceBundle       fusion/apic-em-inventory-manager-service:7.1.3.60048 READY
ServiceBundle       fusion/apic-em-jboss-ejbca:7.1.3.60048        READY
.
.
.
ServiceBundleGroup  fusion/apicem-core:2.1.3.60048                READY
ServiceBundleGroup  fusion/dna-maps:2.1.3.60048                   READY
ServiceBundleGroup  maglev-system/apicem-core-ui:2.1.3.60048      READY
ServiceBundleGroup  maglev-system/dna-maps-ui:2.1.3.60048         READY
```

Package Deploy Failure and Recovery

How to Check Workflows from GUI

System Settings → System360: Tools (right-side) → Workflows

https://<dnacenter_ip>/sysadmin/catalog



Package Update Troubleshooting

Fail to Download Packages:

- Check connectivity to Internet
- During update download internet connectivity is mandatory

Fail to install packages:

- During install internet connectivity is mandatory
- Check if there is any failure displayed in GUI
- Check the status from CLI if there is any error

Package Update Ordering

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/rn_release_1_1_2_2/b_dnac_release_notes_1_1_2_2.html#task_nj3_nww_qcb

Proxy Setting check

```
$ maglev catalog settings display
[administration] password for 'admin':

maglev-1 [main - https://172.27.255.230:30443]

SETTING                          VALUE
-------------------------------------------------------------------------
defaultRepository
httpsProxy                       http://proxy.esl.cisco.com:80
parentCatalogServer              https://www.ciscoconnectdna.com:443
parentCatalogServerRepository
```

```
$ curl --proxy http://proxy.esl.cisco.com:80 -s https://raw.githubusercontent.com/sivel/speedtest-cli/master/speedtest.py | python -
Retrieving speedtest.net configuration...
Testing from Cisco Systems (173.36.240.167)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by Mimosa Networks (San Jose, CA) [0.78 km]: 349.224 ms
Testing download speed................................................................................
Download: 92.16 Mbit/s
Testing upload speed................................................................................................
Upload: 51.23 Mbit/s
```

Package Deploy Failure and Recovery

```
$ maglev package status
maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]
NAME                          DEPLOYED        AVAILABLE       STATUS
--------------------------------------------------------------------------------
network-visibility            2.1.1.60067     -               UPGRADE_ERROR - maglev_workflow.workflow.exceptions.TaskCallableExecutionError:
(1516326117.1073043, 1516327147.0490577, 'TimeoutError', 'Timeout of 1020 seconds has expired while watching for k8s changes for apic-em-jboss-
ejbca ')
```

```
$ maglev catalog package display network-visibility | grep fq
fqn: network-visibility:2.1.1.60067
```

Find the package name

```
$ maglev catalog package delete network-visibility:2.1.1.60067
Ok
```

Delete the package

```
$ maglev package undeploy network-visibility.
Undeploying packages 'network-visibility:2.1.1.60067'
Package will start getting undeployed momentarily
```

Undeploy failed package using the –force option only with DE help.

```
$ maglev catalog package pull network-visibility:2.1.1.60067
Package pull initiated
Use "maglev catalog package status network-visibility:2.1.1.60067" to monitor the progress of the operation
```

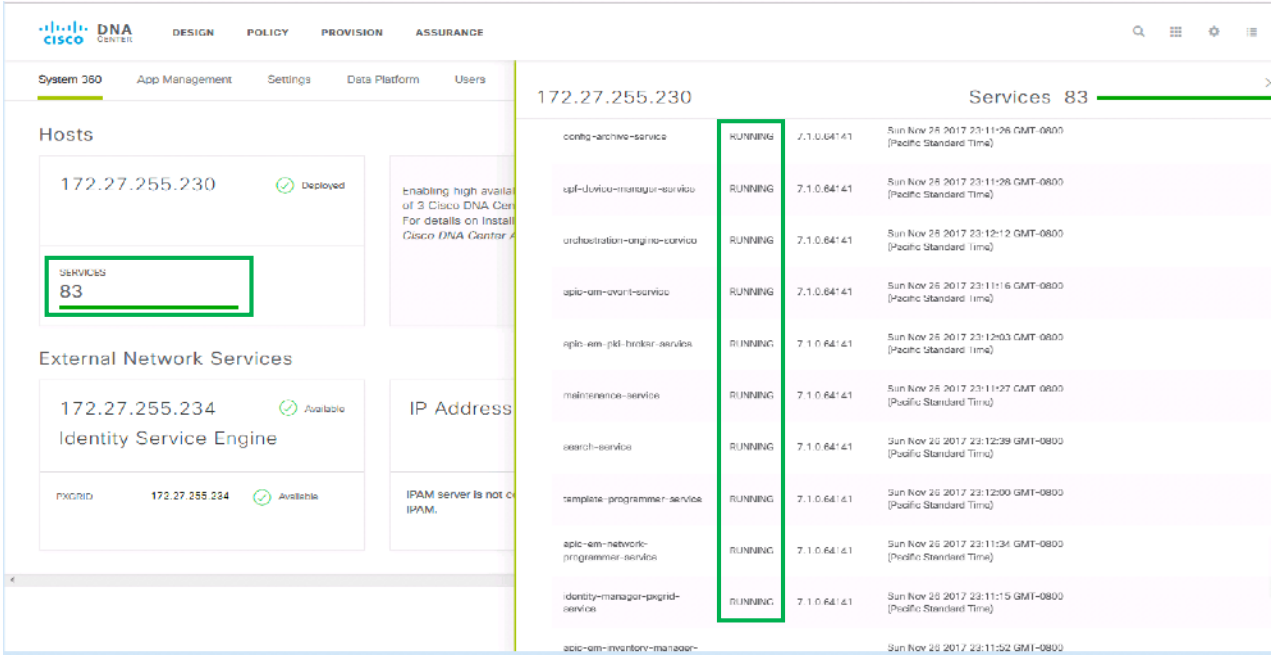
Pull the package again

Once above steps completed, go to GUI and download the package again and install it.
Or you can use “`maglev package deploy <>`”

DNA Center Services not coming up

How to Check Service Status from GUI

System Settings → System360: Services
https://<dnacenter_ip>/dna/systemSettings



DNA Center Services not coming up

How to Check Service Status from CLI

- SSH to DNA Center server
- Check for Service Instance status using "`magctl appstack status` <service>"
- Various States – Running, Terminating, Unresponsive, Error, crashdump, stopped

```
$ magctl appstack status fusion
 NAME                                                READY     STATUS    RESTARTS   AGE       IP              NODE
apic-em-event-service-587097833-j7g75                1/1       Running   1          20h       172.16.243.70   10.90.14.247
apic-em-inventory-manager-service-911522410-ltktp    1/1       Running   1          20h       172.16.243.123  10.90.14.247
apic-em-jboss-ejbca-1435823774-hghz4                 1/1       Running   1          20h       172.16.243.35   10.90.14.247
apic-em-network-programmer-service-1596794817-rrd7j  1/1       Running   1          20h       172.16.243.120  10.90.14.247
apic-em-pki-broker-service-652645917-6xc91           1/1       Running   1          20h       172.16.243.49   10.90.14.247
app-policy-provisioning-service-2960283841-wl982     1/1       Running   1          20h       172.16.243.21   10.90.14.247
command-runner-service-1159149985-5k3sr              1/1       Running   1          20h       172.16.243.104  10.90.14.247
config-archive-service-249636520-88fhl               1/1       Running   1          20h       172.16.243.119  10.90.14.247
distributed-cache-service-2705204688-19d6h           1/1       Running   1          20h       172.16.243.127  10.90.14.247
dna-common-service-2919466290-xbgwx                  1/1       Running   1          20h       172.16.243.84   10.90.14.247
dna-maps-service-3587182290-09csc                    1/1       Running   1          20h       172.16.243.118  10.90.14.247
dna-wireless-service-3203253527-chq6s                1/1       Running   1          20h       172.16.243.28   10.90.14.247
file-service-1297491380-9xfw2                        1/1       Running   2          20h       172.16.243.110  10.90.14.247
grouping-service-1236326915-jjx19                    1/1       Running   1          20h       172.16.243.97   10.90.14.247
heatmap-service-3685073858-01dtf                     1/1       Running   1          20h       172.16.243.126  10.90.14.247
identity-manager-pxgrid-service-697497187-zb688      1/1       Running   1          20h       172.16.243.116  10.90.14.247
integrity-verification-service-537038205-pbmk6       1/1       Running   1          20h       172.16.243.64   10.90.14.247
ipam-service-1593760660-nhjmk                        1/1       Running   1          20h       172.16.243.22   10.90.14.247
licensemanager-334294252-1x7p4                       1/1       Running   2          20h       172.16.243.103  10.90.14.247
maintenance-service-2960437333-pg4v7                 1/1       Running   1          20h       172.16.243.18   10.90.14.247
```

DNA Center Services not coming up

Check for services restarts count / error

- `magctl appstack status | awk '$5 !~ /^0/'`

```
$ magctl appstack status | awk '$5 !~ /^0/'
NAMESPACE           NAME                                                READY     STATUS    RESTARTS   AGE       IP               NODE
assurance-backend   collector-cli-2832156480-gv5bc                       1/1       Running   2          20h       172.16.243.93    10.90.14.247
assurance-backend   nsa-webapp-3650063569-wp9fz                         1/1       Running   2          20h       172.16.243.57    10.90.14.247
assurance-backend   wirelesscollector-107232770-4zwtf                   1/1       Running   2          20h       172.16.243.69    10.90.14.247
fusion              apic-em-event-service-587097833-j7g75               1/1       Running   1          20h       172.16.243.70    10.90.14.247
fusion              apic-em-inventory-manager-service-911522410-ltktp   1/1       Running   1          20h       172.16.243.123   10.90.14.247
fusion              apic-em-jboss-ejbca-1435823774-hghz4                1/1       Running   1          20h       172.16.243.35    10.90.14.247
fusion              apic-em-network-programmer-service-1596794817-rrd7j 1/1       Running   1          20h       172.16.243.120   10.90.14.247
fusion              apic-em-pki-broker-service-652645917-6xc91          1/1       Running   1          20h       172.16.243.49    10.90.14.247
fusion              app-policy-provisioning-service-2960283841-wl982    1/1       Running   1          20h       172.16.243.21    10.90.14.247
fusion              command-runner-service-1159149985-5k3sr             1/1       Running   1          20h       172.16.243.104   10.90.14.247
fusion              config-archive-service-249636520-88fhl              1/1       Running   1          20h       172.16.243.119   10.90.14.247
fusion              distributed-cache-service-2705204688-19d6h          1/1       Running   1          20h       172.16.243.127   10.90.14.247
fusion              dna-common-service-2919466290-xbgwx                 1/1       Running   1          20h       172.16.243.84    10.90.14.247
fusion              dna-maps-service-3587182290-09csc                   1/1       Running   1          20h       172.16.243.118   10.90.14.247
fusion              dna-wireless-service-3203253527-chq6s               1/1       Running   1          20h       172.16.243.28    10.90.14.247
fusion              file-service-1297491380-9xfw2                       1/1       Running   2          20h       172.16.243.110   10.90.14.247
fusion              grouping-service-1236326915-jjx19                   1/1       Running   1          20h       172.16.243.97    10.90.14.247
fusion              heatmap-service-3685073858-01dtf                    1/1       Running   1          20h       172.16.243.126   10.90.14.247
fusion              identity-manager-pxgrid-service-697497187-zb688     1/1       Running   1          20h       172.16.243.116   10.90.14.247
```

DNA Center Services not coming up

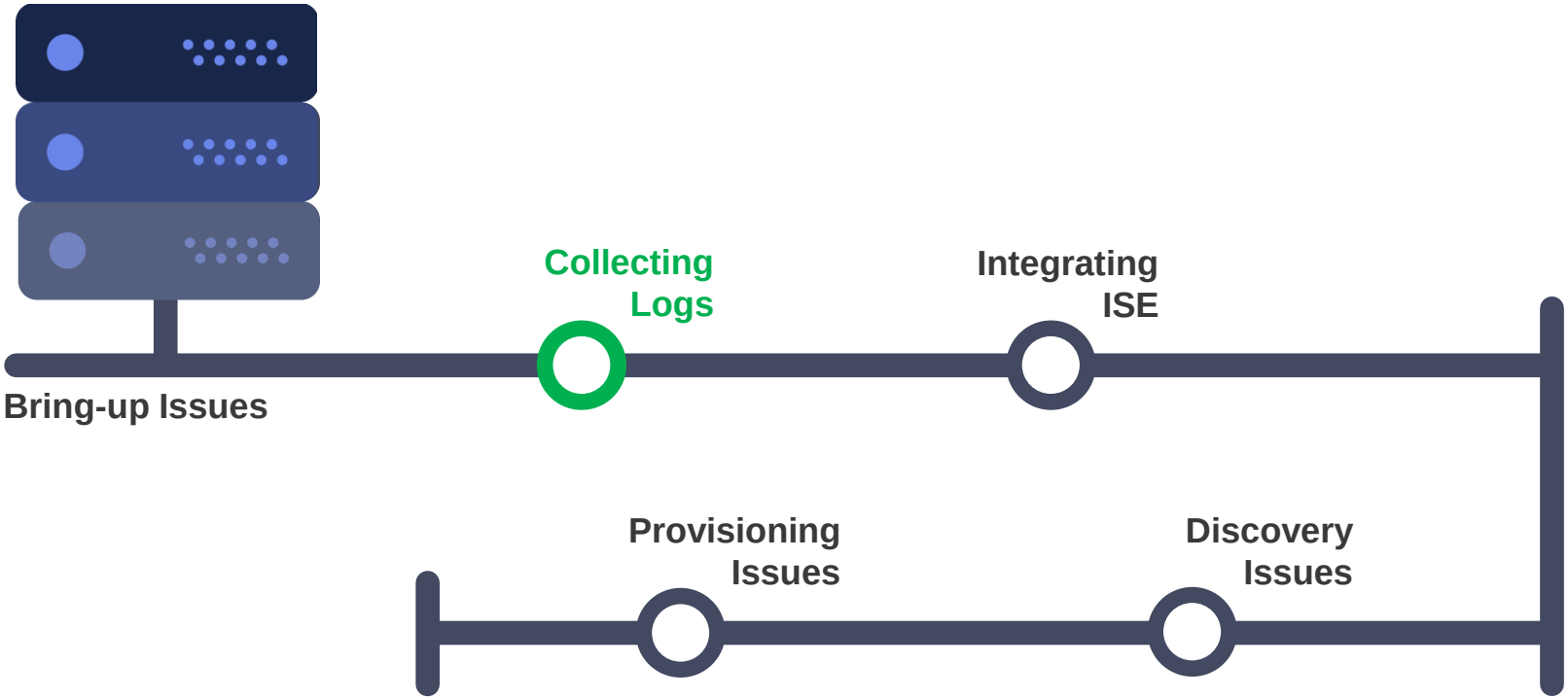
Check DNA Center server resources

- Disk Throughput Check "`iostat`"

```
$ iostat
Linux 4.10.0-40-generic (maglev-master-1)       02/14/2018      _x86_64_

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
           2.61    0.00    1.93    0.10    0.00   95.35

Device:            tps    kB_read/s    kB_wrtn/s    kB_read    kB_wrtn
sda              65.43         3.93       975.84   24216325 6012021312
sdc               4.46         0.16       150.82     962597  929162624
sdd               0.00         0.00         0.00       3127          0
sdb              37.89       719.32      2368.14 4431682506 14589882628
```

- Check CPU usage "`top`"

```
top - 18:53:17 up 71 days,  7:19,  1 user,  load average: 5.55, 6.23, 6.23
Tasks: 1751 total,   1 running, 1748 sleeping,   0 stopped,   2 zombie
%Cpu(s):  3.5 us,  2.6 sy,  0.0 ni, 93.7 id,  0.0 wa,  0.0 hi,  0.2 si,  0.0 st
KiB Mem : 26402937+total,  7768480 free, 16535468+used, 90906192 buff/cache
KiB Swap: 31999996 total, 31999968 free,       28 used. 90897872 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
85885 root      20   0 2135376 149108  43548 S 120.9  0.1   0:03.70 java
 5142 root      20   0 7716288 308636  53148 S  73.9  0.1  57033:54 kubelet
 3268 root      20   0 16.488g 2.507g   7504 S  44.1  1.0  25046:09 docker-containe
 3250 root      20   0 49.144g 542696  27072 S  17.6  0.2  22178:35 dockerd
58433 root      20   0  983268 266204   7760 S   8.5  0.1 198:12.78 fluentd
75641 root      20   0  466300 372156  58428 S   8.5  0.1 454:56.20 kube-apiserver
77905 root      20   0 1953964 866340   7124 S   6.2  0.3  54:57.44 glusterfsd
33700 root      20   0 5506588 2.630g  54504 S   5.2  1.0  56:44.35 java
37116 root      20   0 7104392 4.027g  54724 S   4.9  1.6 112:05.86 java
37871 999       20   0 8722628  45612  42824 S   4.9  0.0  24:52.97 postgres
44313 root      20   0 7041784 3.503g  56860 S   4.9  1.4  71:27.53 java
84005 maglev    20   0 2775132 762052  19988 S   4.9  0.3  58:35.04 java
17347 maglev    20   0 9968864 5.379g  31116 S   4.6  2.1  48:26.20 java
17671 maglev    20   0  9.803g 5.498g  31192 S   4.6  2.2  62:55.75 java
11113 maglev    20   0 22.634g 6.892g  43036 S   4.2  2.7   3900:28 java
13409 root      20   0  792968 364756   6532 S   3.9  0.1 159:37.45 glusterfs
22608 root      20   0 2426960 432952  27016 S   3.9  0.2  45:47.40 java
78527 root      20   0  208880 159244  46780 S   3.9  0.1 232:51.82 kube-controller
86968 root      20   0 2323020 670116   5548 S   3.9  0.3 105:23.30 beam.smp
19649 maglev    20   0 75.606g 6.170g  35700 S   3.3  2.5   1031:24 java
 6690 root      20   0  103032  78812  18584 S   2.9  0.0   4608:53 calico-felix
12859 maglev    20   0   30288   6280   4720 S   2.9  0.0  76:23.02 haproxy
72478 maglev    20   0 15.139g 1.669g 242660 S   2.9  0.7   6661:08 influxd
 4240 root      20   0 10.123g 116064  22828 S   2.6  0.0   1849:41 etcd
25855 maglev    20   0 9818.6m 4.899g  30832 S   2.6  1.9  29:22.43 java
30009 maglev    20   0 9910.0m 5.331g  30864 S   2.6  2.1  35:03.38 java
85770 root      20   0  273792   3732   2492 S   2.6  0.0   0:00.08 docker-containe
86371 root      20   0  406272   3792   2572 S   2.6  0.0   0:00.08 docker-containe
36157 maglev    20   0 9662080 5.070g  31132 S   2.0  2.0  19:26.80 java
78792 maglev    20   0   40084   5248   3060 R   2.0  0.0   0:00.67 top
 6590 maglev    20   0 8288652 4.483g  31464 S   1.3  1.8  19:28.89 java
```

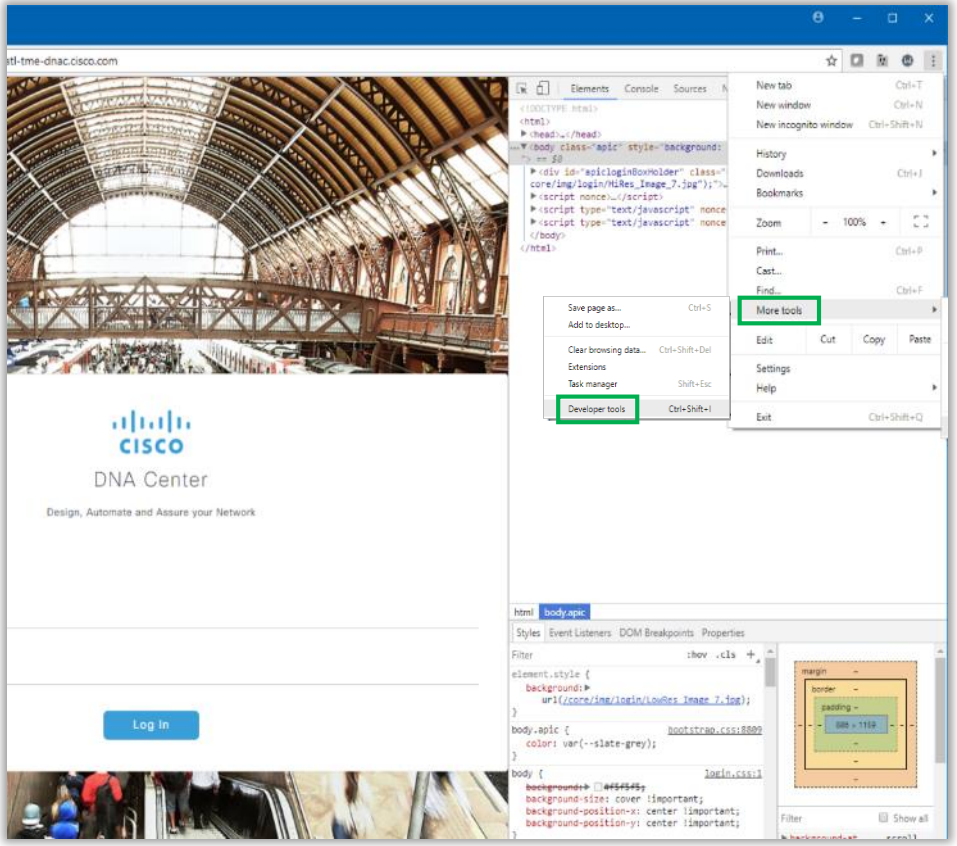


UI Debugging from Browser

Use Browser Debugging mode to find out API or GUI related Errors

For Chrome/Firefox Browsers

- Enable Debugging mode by going to Menu → More Tools → Developer mode
- Select Console from top menu
- For clarity clear existing log.
- Run the task from DNA Center GUI
- Capture the console screenshot to identify API/Error details.

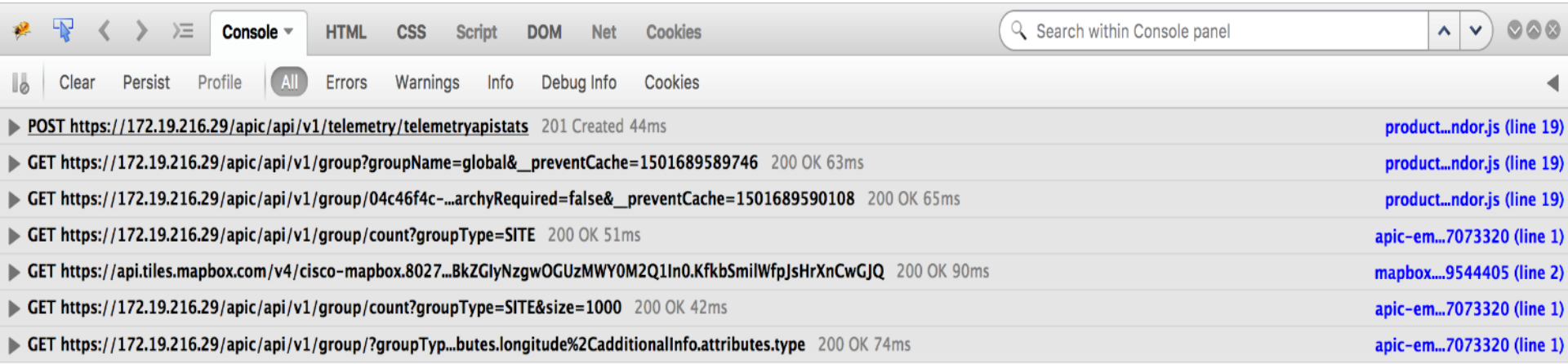


UI Debugging from Browser

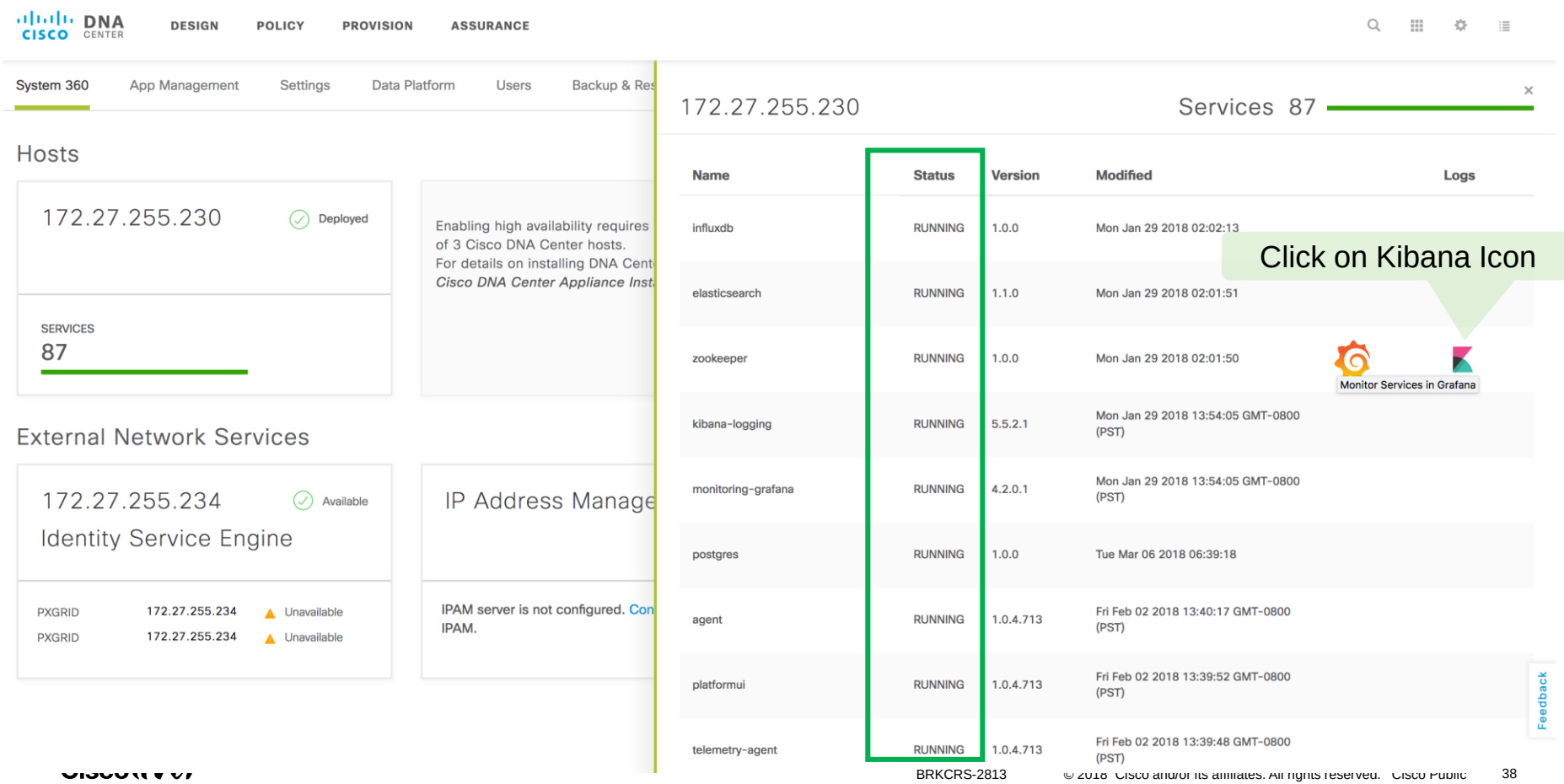
Firebug is another Tool for debugging mode.

For Firefox

- Install Firebug add-on in Firefox Browser
- Enable Firebug add-on
- Launch Firebug and Go to Console
- Run the task and it will capture detailed information



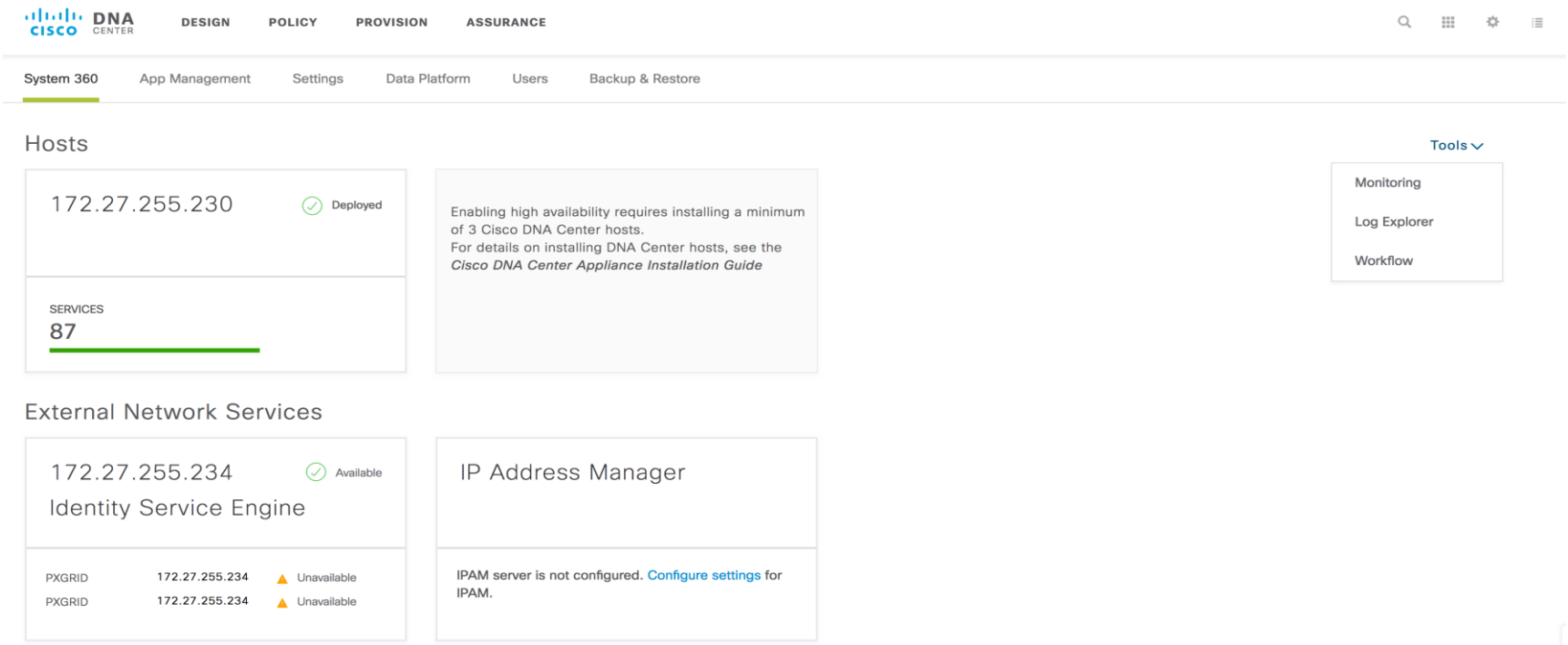
Check Service Log in GUI



Monitoring / Log Explorer / Workflow

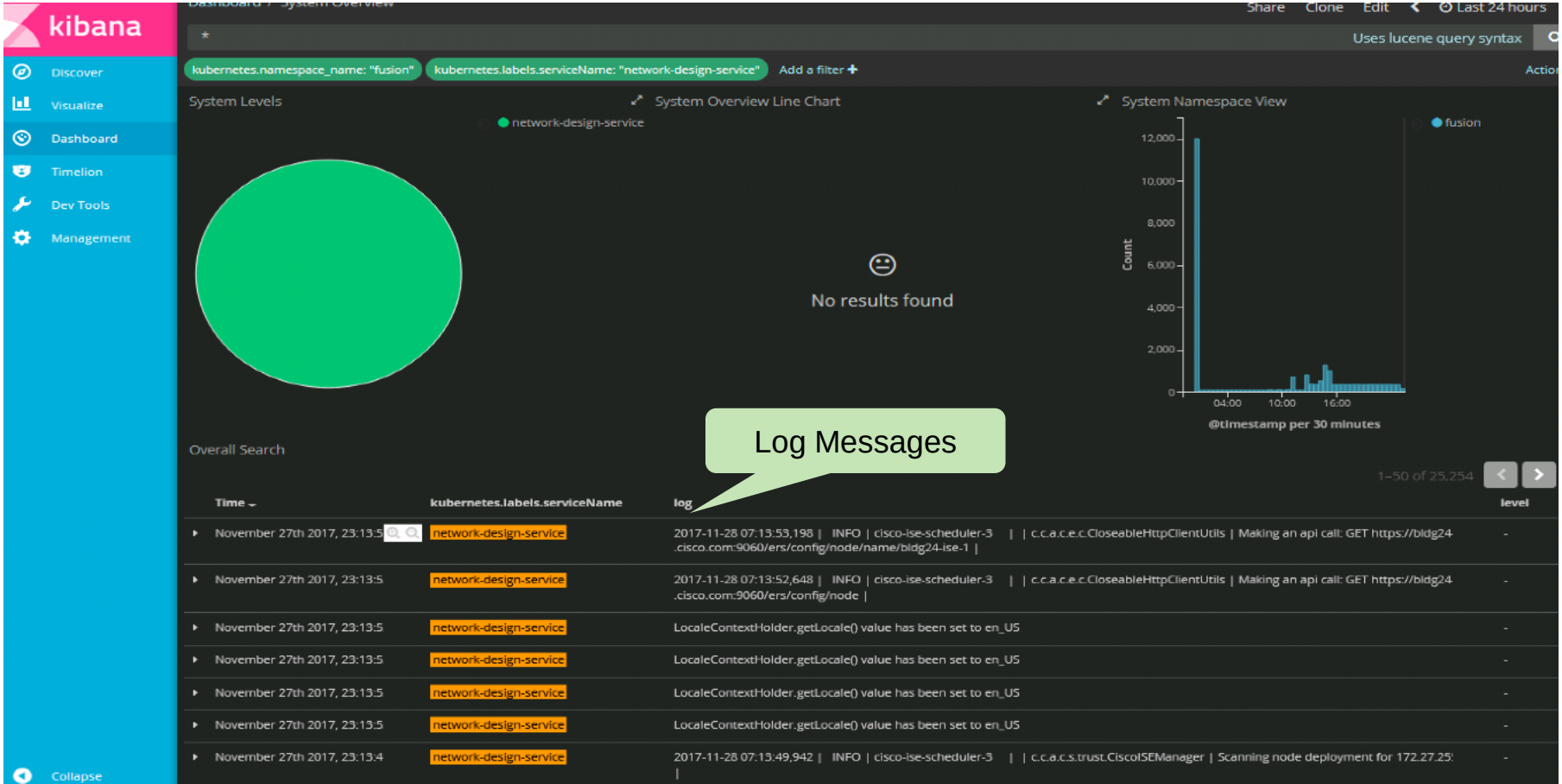
How to Monitor / Log Explorer / Workflow Status from GUI

System Settings → System360: → Tools
https://<dnacenter_ip>/dna/systemSettings

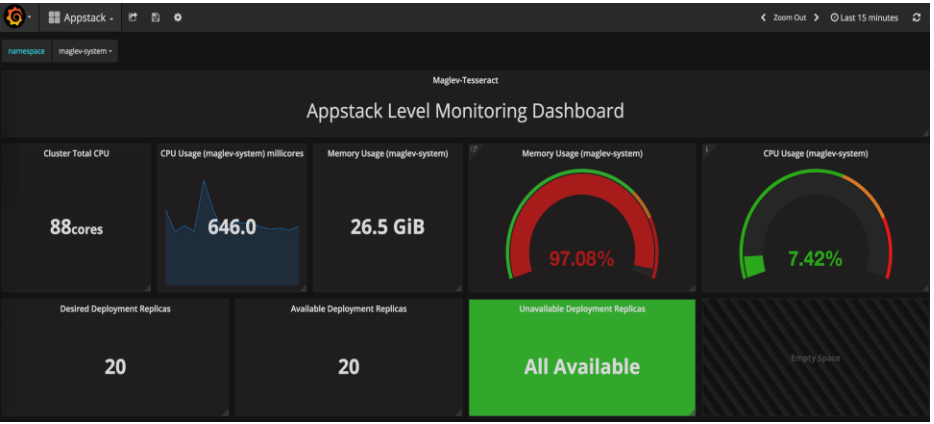


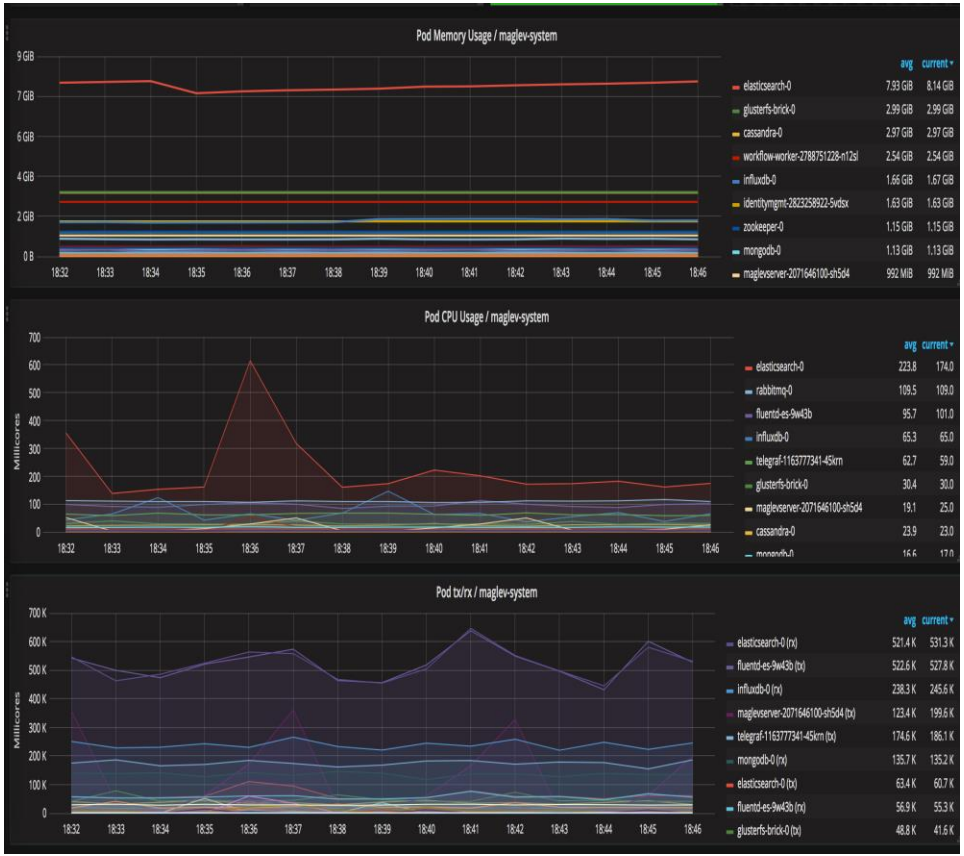
C

Check Service Log using Log Explorer



Resource Monitor Dashboard

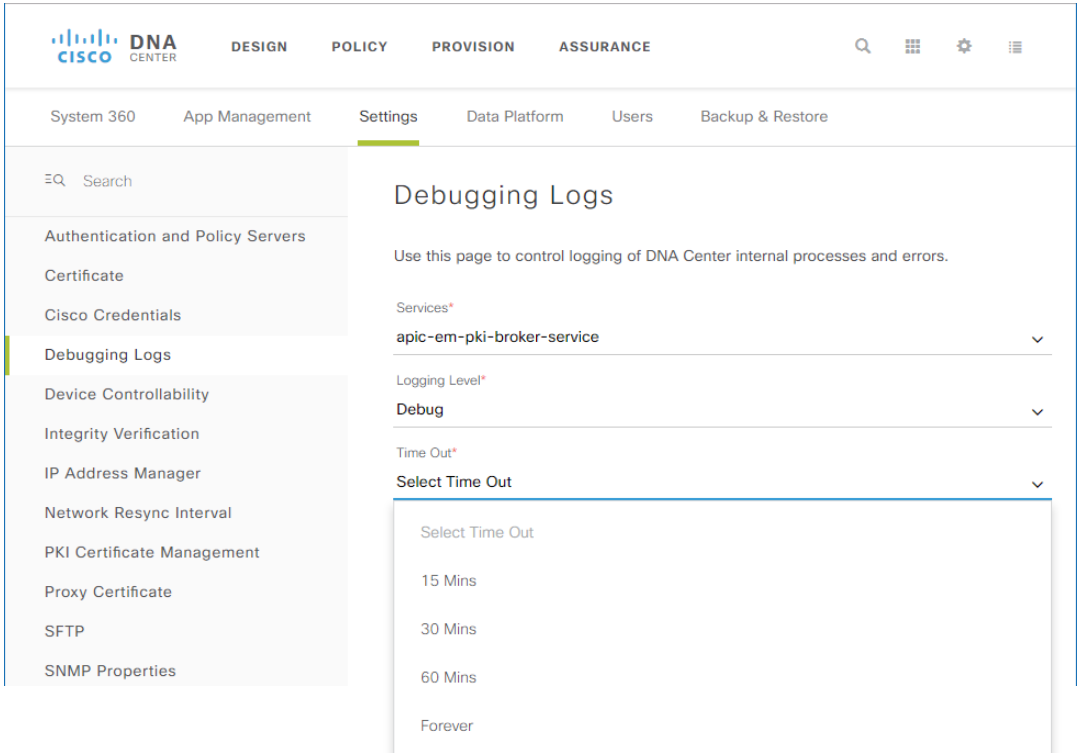




Changing DNA Center Logging Levels

How to Change the Logging Level

- Navigate to the Settings Page: → System Settings → Settings → Debugging Levels
- Select the service of interest
- Select the new Logging Level
- Set the duration DNA Center should keep this logging level change
  - Intervals: 15 / 30 / 60 minutes or forever



Live Log - Service

Find the Service for Which Debug/Log needs to be captured

- `magctl appstack status`

```
$ magctl appstack status | grep network-pro
fusion                    apic-em-network-programmer-service-
4111434980t608v      1/1       Running   0          13d       10.60.3.62       172.27.121.217
```

- `magctl service attach <service-name>`

```
$ magctl service attach apic-em-network-programmer-service

Attaching to 'fusion/apic-em-network-programmer-service-1596794817-rrd7j'
root@apic-em-network-programmer-service-1596794817-rrd7j:/#
```

Live Log - Service

Log Files:

- To get the complete logs of any service:
  - Get the container_id using:

    ```
    docker ps | grep <service-name> | grep -v pause | cut -d' ' -f1
    ```
  - Get logs using: `docker logs <container_id>`

- To follow/tail the current log of any service:

  ```
  magctl service logs –r -f <service-name>
  ```

  EX: `magctl service logs -r -f spf-service-manager-service`

  Note: remove `-f` to display the current logs to the terminal

Required information to report an issue

- RCA file
  - SSH to server using maglev user

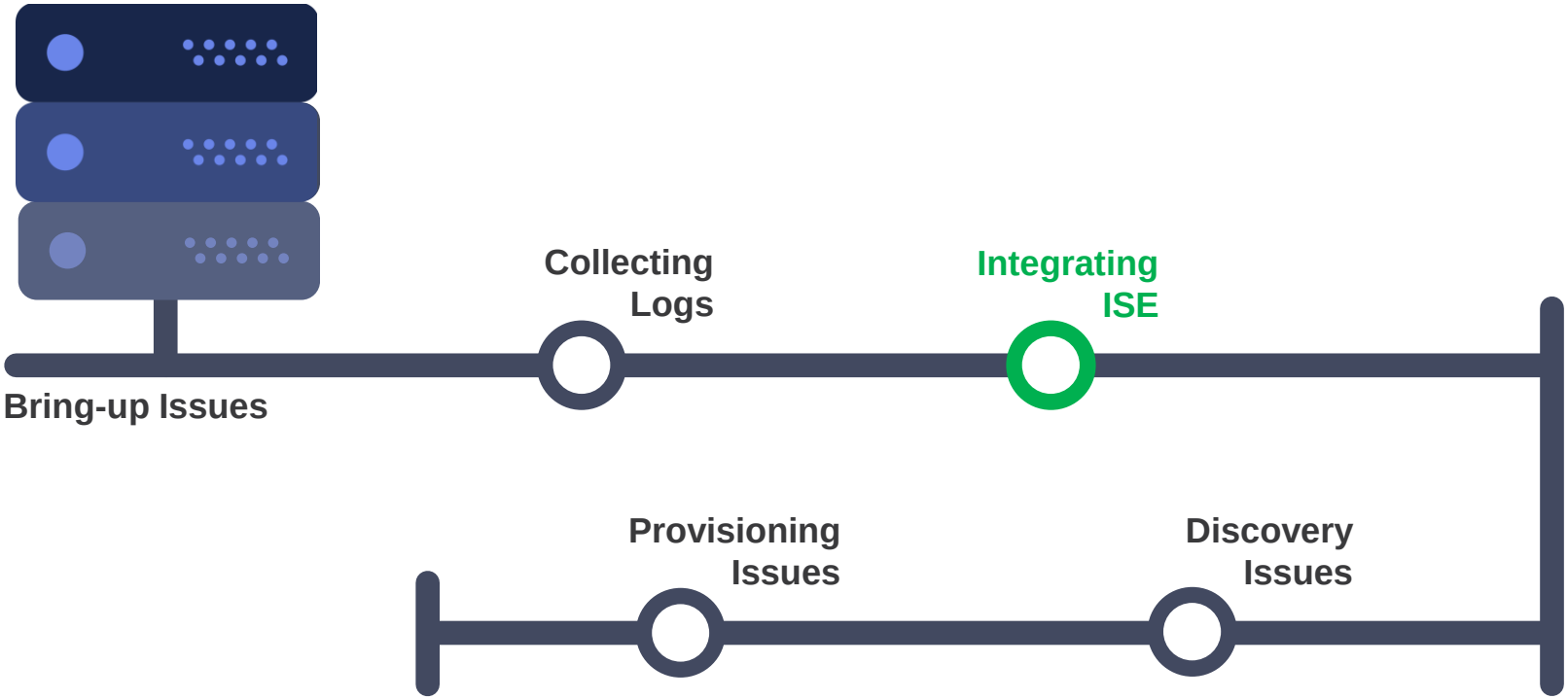
```
ssh –p 2222 maglev@<dnacenter_ip_address>
```

  - rca
  - Generated file can be copied using scp/sftp from external server

```
scp –P 2222
maglev@<dnacenter_ip_address>:<rca_filename>
```

- Error Screenshot from UI
- API Debug log using browser debugging mode

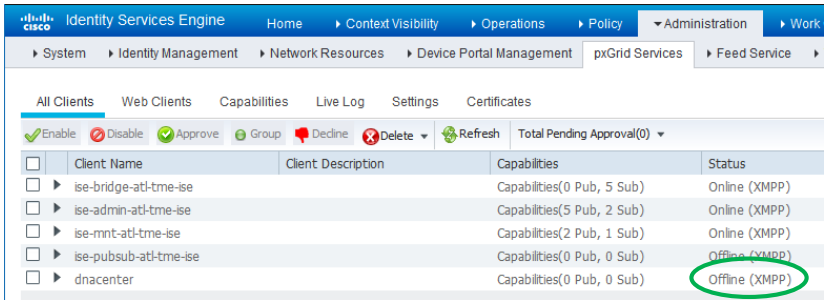
```
[Sun Feb 11 14:26:00 UTC] maglev@10.90.14.247 (maglev-master-1)
$ rca

================================================================
Verifying ssh/sudo access
================================================================
[sudo] password for maglev: <passwd>
Done
mkdir: created directory '/data/rca'
changed ownership of '/data/rca' from root:root to maglev:maglev

================================================================
Verifying administration access
================================================================
[administration] password for 'admin': <passwd>
User 'admin' logged into 'kong-frontend.maglev-
system.svc.cluster.local' successfully

================================================================
RCA package created on Sun Feb 18 14:26:14 UTC 2018
================================================================

2018-02-18 14:26:14 | INFO | Generating log for 'date'...
tar: Removing leading `/' from member names
/etc/cron.d/
/etc/cron.d/.placeholder
/etc/cron.d/clean-elasticsearch-indexes
/etc/cron.d/clean-journal-files
```



Troubleshooting - ISE - DNA Center Integration

- Check basic IP connectivity between ISE and DNA Center server
- If any server multi-homed then check for proper connectivity/reachability
  Note: Integration MUST use int 0 on both DNA Center and ISE
- Check pxGrid service is running on ISE
  - Go to Administration → pxGrid Services
  - At the bottom it should display Green bar with Connected status

- Check FQDN configuration on DNA Center and ISE
- Check DNA Center subscriber status in ISE pxGrid
  - Offline, Pending approval, Online



Troubleshooting - ISE - DNA Center Integration

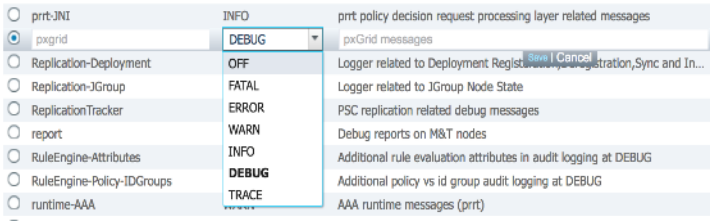
Checking pxGrid service status

- Login to ISE server using SSH
- Run “show application status ise” to check for the services running.

```
dna-ise-1/admin# show application status ise | incl pxGrid
pxGrid Infrastructure Service          running          23605
pxGrid Publisher Subscriber Service    running          23902
pxGrid Connection Manager              running          23834
pxGrid Controller                      running          24074
dna-ise-1/admin#
```

Increasing log level to debug

- Go to Administration → Logging → Debug Log Configuration
- Select the ISE server and Edit
- Find pxGrid, ERS, Infrastructure Service from the list. Click Log Level button and select Debug Level



Troubleshooting - ISE - DNA Center Integration

On DNA Center check

- network-design-service
- identity-manager-pxGrid-service
- dna-common-service

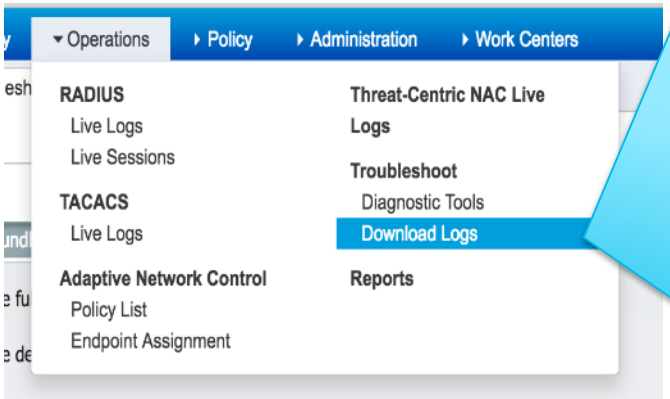
- On ISE check logs
  - ERS
  - pxGrid
  - Infrastructure Service logs

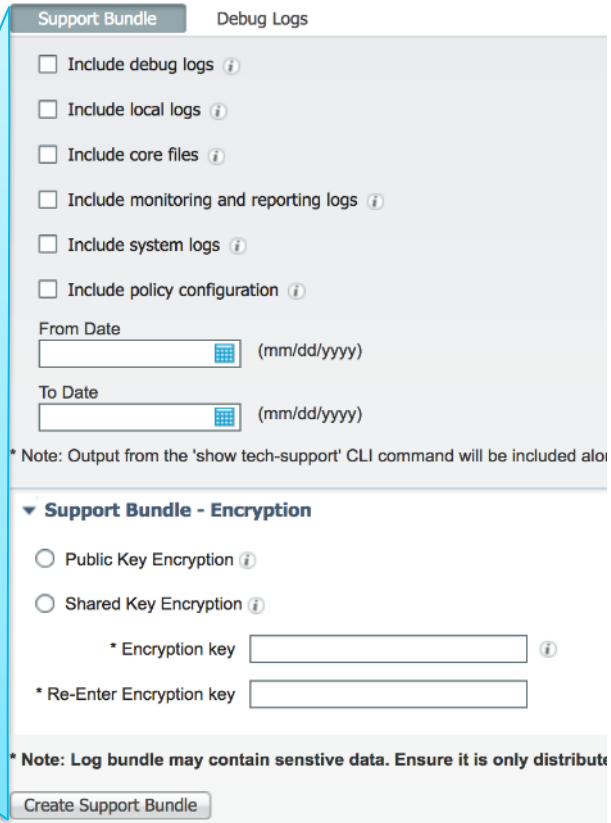
Example Error:

```
2017-08-01 05:24:36,794 |  ERROR | pool-1-thread-1    | identity-manager-pxGrid-service |
c.c.e.i.u.pxGridConfigurationUtils | An error occurred while retrieving pxGrid endpoint certificate.
Request: PUT https://bldg24-ise-1.cisco.com:9060/ers/config/endpointcert/certRequest HTTP/1.1, Response:
HttpResponseProxy{HTTP/1.1 500 Internal Server Error [Cache-Control: no-cache, no-store, must-revalidate,
Expires: Thu, 01 Jan 1970 00:00:00 GMT, Set-Cookie: JSESSIONIDSSO=9698CC02E88780EC4415A6DE80C37355;
Path=/; Secure; HttpOnly, Set-Cookie: APPSESSIONID=03A609099AD604812984C6DF27CF7A19; Path=/ers; Secure;
HttpOnly, Pragma: no-cache, Date: Tue, 01 Aug 2017 05:24:36 GMT, Content-Type:
application/json;charset=utf-8, Content-Length: 421, Connection: close, Server:  ]
ResponseEntityProxy{[Content-Type: application/json;charset=utf-8,Content-Length: 421,Chunked: false]}} |
```

Troubleshooting - ISE - DNA Center Integration

- To Capture ISE Log bundle:
  - Go to Operation → Download Logs
  - Select ISE server
  - Select any additional log to be captured
  - Provide Encryption Key and create bundle
  - Download bundle

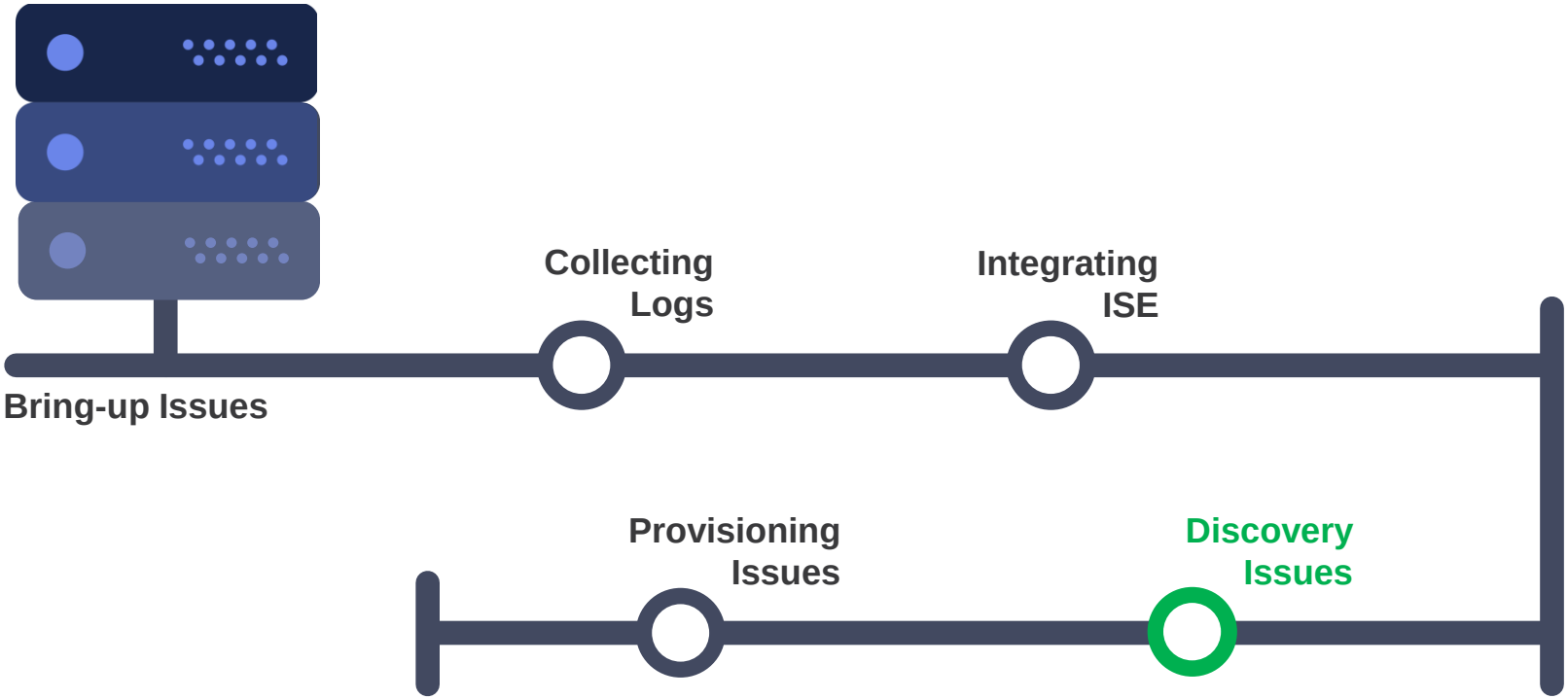




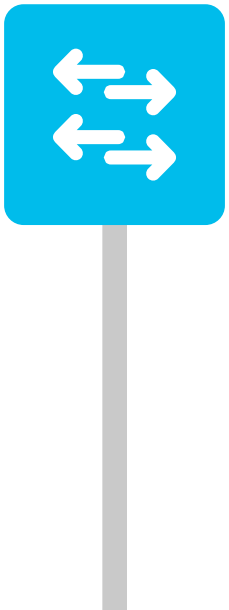
ISE - DNA Center Integration - Verification Example

- Create sample Policy from DNA Center - DNA Center will display Deployed
- Use Advance option to verify policy pushed to the ISE server
- On DNA Center Identity-service-manager log can be checked to confirm SGT ID assigned from ISE
- Sample Message:

```
2017-08-02 19:55:48,320 |   INFO | e Threaded Executor 0 (1) | identity-manager-pxGrid-service |
c.c.e.i.ScalableGroupNotificationHandler | Received Scalable Group notification from ISE with id: 38f812c2-
54db-43fb-9bad-f85e747a5c2a |

2017-08-02 19:55:48,321 |   INFO | e Threaded Executor 0 (1) | identity-manager-pxGrid-service |
c.c.e.i.ScalableGroupNotificationHandler | ciscoIseId: 38f812c2-54db-43fb-9bad-f85e747a5c2a, Security Group:
com.cisco.pxGrid.model.ise.metadata.SecurityGroup@72ed5a69[  id=93ad6890-8c01-11e6-996c-
525400b48521  name=Employees  description=Employee Security Group  tag=4 ], ChangeType: MODIFY |
```



Device Discovery



New Discovery

* Discovery Name: Discovery Name

IP RANGES

Type: CDP | Range

* IP Address: 0.0.0.0

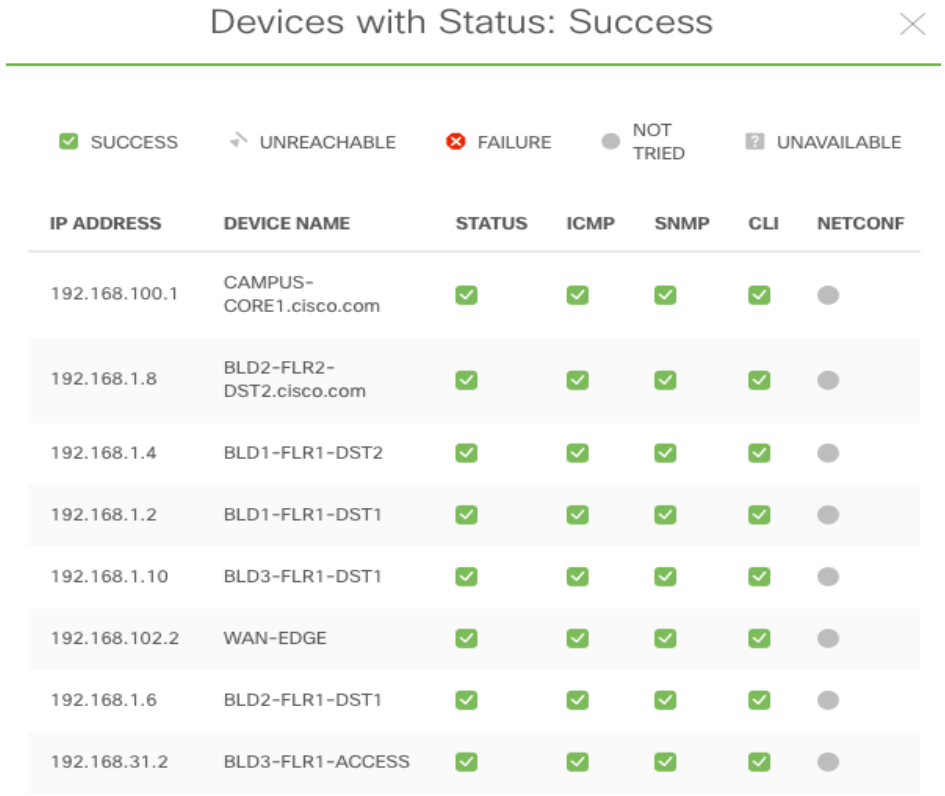
Subnet Filters: 0.0.0.0 +

CDP Level: 16

Preferred Management IP: None

Step 6

Verify all devices are green after Discovery



IP ADDRESS	DEVICE NAME	STATUS	ICMP	SNMP	CLI	NETCONF
192.168.100.1	CAMPUS-CORE1.cisco.com	✓	✓	✓	✓	●
192.168.1.8	BLD2-FLR2-DST2.cisco.com	✓	✓	✓	✓	●
192.168.1.4	BLD1-FLR1-DST2	✓	✓	✓	✓	●
192.168.1.2	BLD1-FLR1-DST1	✓	✓	✓	✓	●
192.168.1.10	BLD3-FLR1-DST1	✓	✓	✓	✓	●
192.168.102.2	WAN-EDGE	✓	✓	✓	✓	●
192.168.1.6	BLD2-FLR1-DST1	✓	✓	✓	✓	●
192.168.31.2	BLD3-FLR1-ACCESS	✓	✓	✓	✓	●

Step 7

Check if all devices in Managed state

Filter | + Add Device | Import Device(s) | Export All

Device Name	IP Address	Reachability Status	Up Time	Last Updated Time	Poller Time	Last Inventory Collection Status
BLD1-FLR1-ACCESS.cisco.com	192.168.11.2	Reachable	27 days, 21:54:52.76	13 minutes ago	00:25:00	Managed
BLD1-FLR1-DST1	192.168.1.2	Reachable	27 days, 22:33:56.49	12 minutes ago	00:25:00	Managed
BLD1-FLR1-DST2	192.168.1.4	Reachable	27 days, 22:30:31.13	12 minutes ago	00:25:00	Managed
BLD1-FLR2-ACCESS.cisco.com	192.168.12.2	Reachable	27 days, 21:48:50.50	13 minutes ago	00:25:00	Managed
BLD2-FLR1-ACCESS.cisco.com	192.168.22.4	Reachable	27 days, 21:42:28.84	13 minutes ago	00:25:00	Managed
BLD2-FLR1-DST1	192.168.1.6	Reachable	27 days, 22:24:54.40	13 minutes ago	00:25:00	Managed
BLD2-FLR2-ACCESS	192.168.21.4	Reachable	13 days, 23:20:49.66	13 minutes ago	00:25:00	Managed
BLD2-FLR2-DST2.cisco.com	192.168.1.8	Reachable	14 days, 4:23:19.14	13 minutes ago	00:25:00	Managed
BLD3-FLR1-ACCESS	192.168.31.2	Reachable	23 days, 21:14:34.31	12 minutes ago	00:25:00	Managed
BLD3-FLR1-DST1	192.168.1.10	Reachable	29 days, 0:52:32.32	13 minutes ago	00:25:00	Managed

New Configuration after Discovery

```
FE250#show archive config differences flash:underlay system:running-config
!Contextual Config Diffs:
+device-tracking tracking
+device-tracking policy IPDT_MAX_10
 +limit address-count 10
 +no protocol udp
 +tracking enable

+crypto pki trustpoint TP-self-signed-1978819505
 +enrollment selfsigned
 +subject-name cn=IOS-Self-Signed-Certificate-1978819505
 +revocation-check none
 +rsakeypair TP-self-signed-1978819505

+crypto pki trustpoint 128.107.88.241
 +enrollment mode ra
 +enrollment terminal
 +usage ssl-client
```

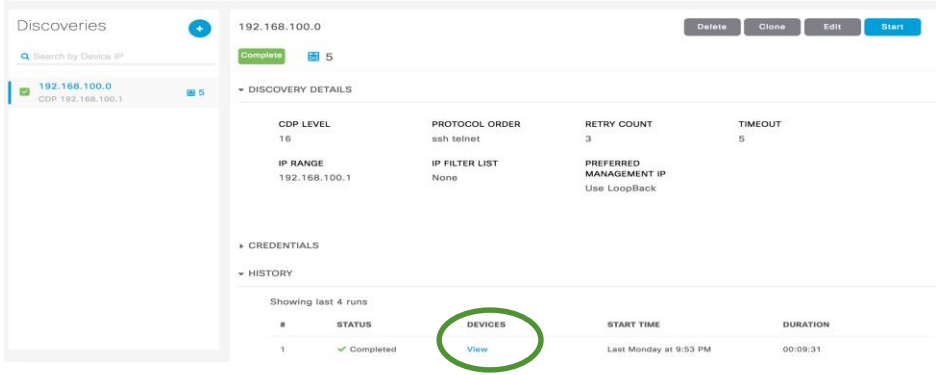
New RSA Keys are created

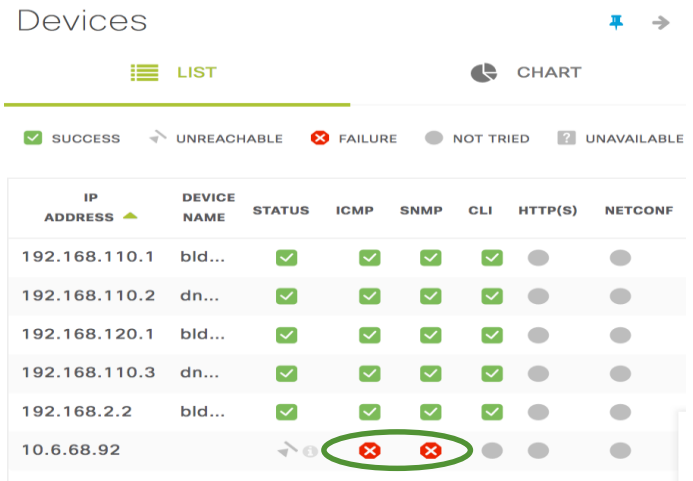
Secure connection to DNA Center using the interface 1 IP address as the certificate name

+ See Notes for Complete Configurations

Troubleshooting – Discovery/Inventory

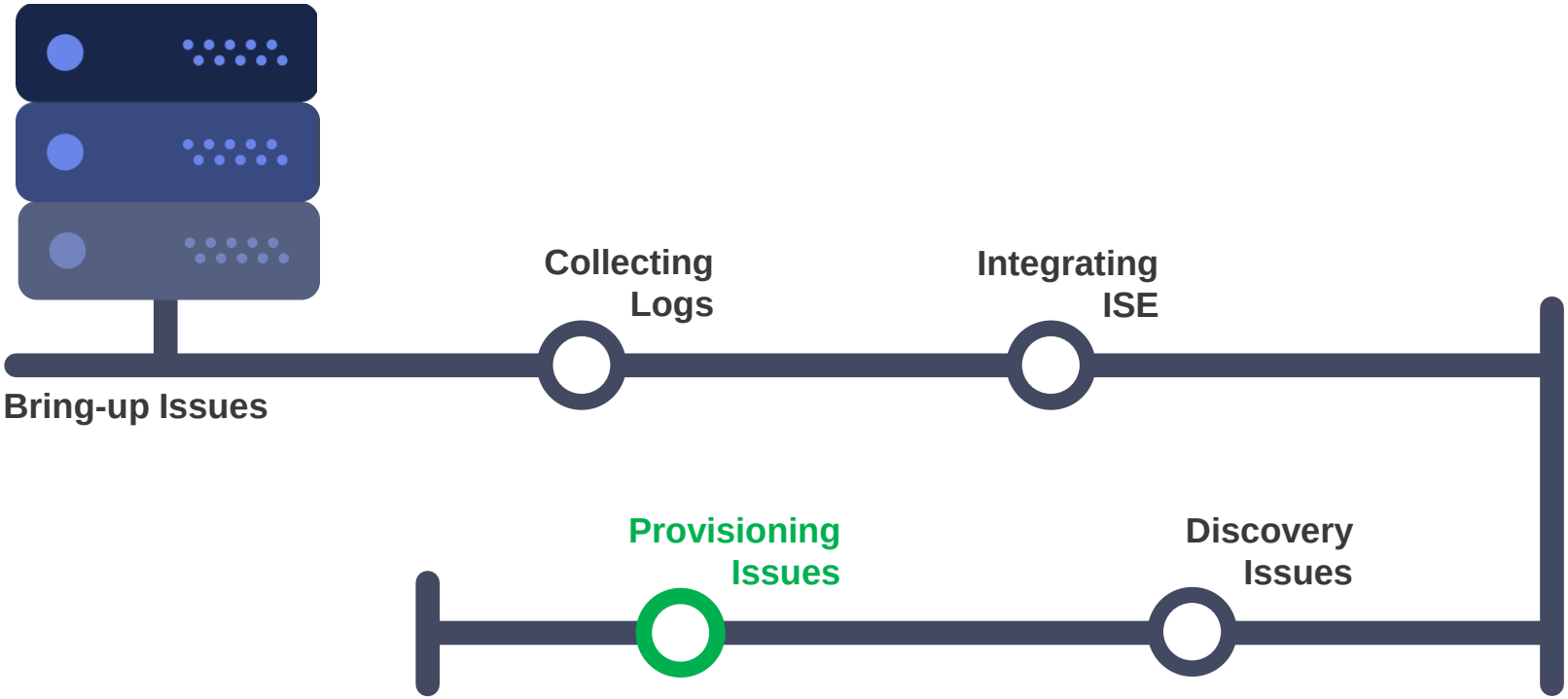
- Check for IP address reachability from DNAC to the device
- Check username/password configuration in Settings
- Check whether telnet/ssh option is properly selected
  - Check using manual telnet/ssh to the device from DNAC or any other client
- Check SNMP community configuration matches on switch and DNA-C
- Discovery View will provide additional information.



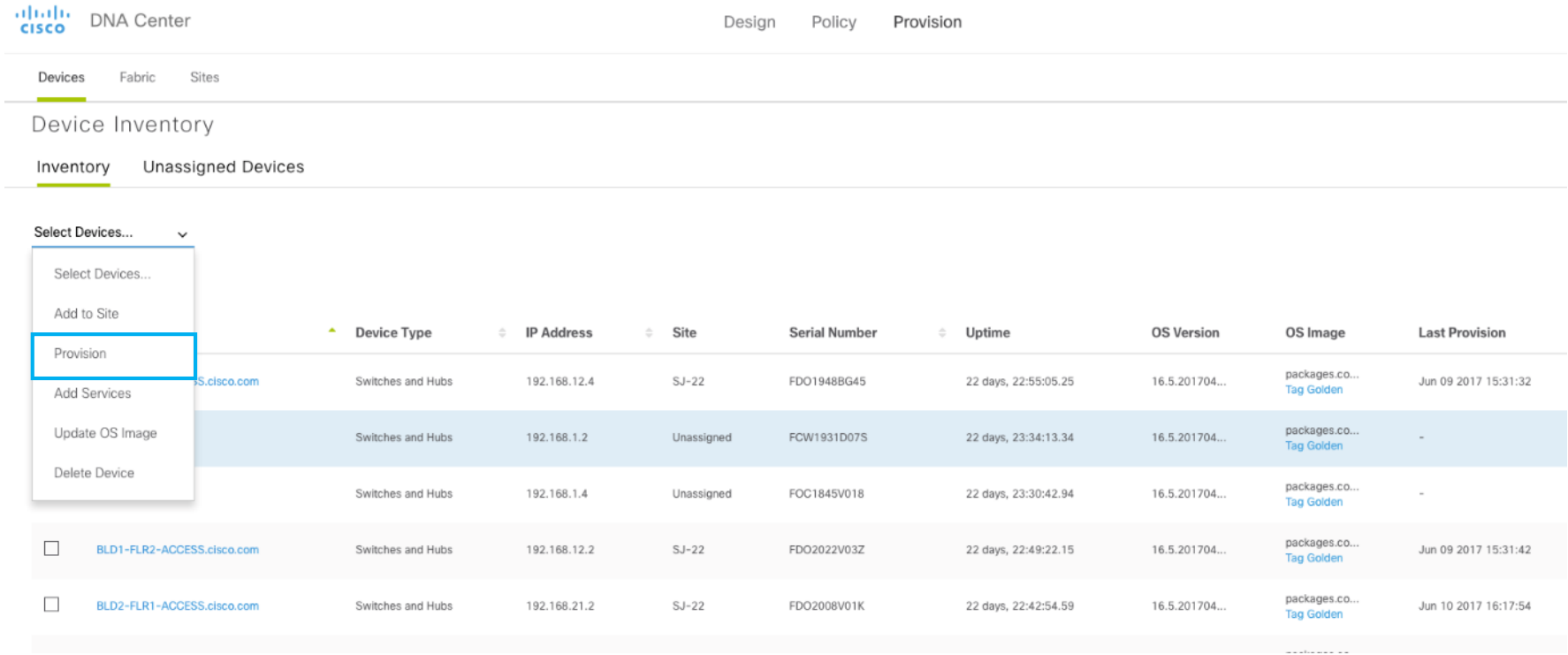


Services Involved on DNA:

apic-em-**inv**entory-manager-service



Time to Provision Devices



Pre-deployment Summary

BLD2-FLR2-DST2

System Details	Device Name:	**BLD2-FLR2-DST2**
	Platform Id:	**WS-C3650-12X48UR-E**
	Device IP:	**192.168.1.8**
	Device Location:	**SJ-22**
Network Settings	NTP Server:	
	AAA Primary Server:	**172.25.0.170**
	DNS Domain Name:	**cisco.com**
	DNS Primary Server:	**172.25.14.105**

Verifying Config Push

- While DNA Center is evolving to use NETCONF and YANG APIs, at this time it pushes most configuration by SSH.
- Exact configuration commands can be seen via show history all

```
FE2050#show history all
CMD: 'enable' 13:29:55 UTC Tue Jan 16 2018
CMD: 'terminal length 0' 13:29:55 UTC Tue Jan 16 2018
CMD: 'terminal width 0' 13:29:55 UTC Tue Jan 16 2018
CMD: 'show running-config' 13:29:55 UTC Tue Jan 16 2018
CMD: 'config t' 13:29:56 UTC Tue Jan 16 2018
CMD: 'no ip domain-lookup' 13:29:56 UTC Tue Jan 16 2018
CMD: 'no ip access-list extended DNA Center_ACL_WEBAUTH_REDIRECT' 13:29:57 UTC Tue Jan 16 2018
*Jan 16 13:29:57.023: %DMI-5-SYNC_NEEDED: Switch 1 R0/0: syncfd:  Configuration change requiring
running configuration sync detected - 'no ip access-list extended DNA
Center_ACL_WEBAUTH_REDIRECT'. The running configuration will be synchronized  to the NETCONF
running data store.
CMD: 'ip tacacs source-interface Loopback0' 13:29:57 UTC Tue Jan 16 2018
CMD: 'ip radius source-interface Loopback0' 13:29:57 UTC Tue Jan 16 2018
CMD: 'cts role-based enforcement vlan-list 1022' 13:29:57 UTC Tue Jan 16 2018
```

Crypto, DNS, aaa and Other Service

Deploy

```
no crypto pki trustpoint 172.25.14.103
crypto key zeroize rsa *

ip domain name cisco.com
ip name-server 172.25.14.105
no ip domain-lookup

crypto pki trustpoint 172.25.14.103
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl
crypto pki authenticate 172.25.14.103
```

```
ip http client source-interface GigabitEthernet1/0/1

aaa group server radius dnac-radius-group
 server name dnac-radius_172.25.0.170
 ip radius source-interface Loopback0
aaa authentication dot1x default group dnac-radius-group
aaa authorization network default group dnac-radius-group
aaa authorization network dnac-cts-list group dnac-radius-group
aaa accounting dot1x default start-stop group dnac-radius-group

radius-server dead-criteria time 2 tries 1
radius server dnac-radius_172.25.0.170
 address ipv4 172.25.0.170 auth-port 1812 acct-port 1813
 pac key cisco123

cts authorization list dnac-cts-list
cts role-based enforcement
```

AAA Configuration

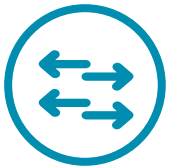
```
FE2050#show running-config | sec aaa
aaa new-model
aaa group server radius dnac-group
 server name dnac-radius_172.26.204.121
 ip radius source-interface Loopback0
aaa authentication login default group dnac-group local
aaa authentication enable default enable
aaa authentication dot1x default group dnac-group
aaa authorization exec default group dnac-group local
aaa authorization network default group dnac-group
aaa authorization network dnac-cts-list group dnacs-group
aaa accounting dot1x default start-stop group dnac-group

aaa server radius dynamic-author
 client 172.26.204.121 server-key cisco123
```

AAA server (ISE) is now used to authenticate device logins

```
FE2050#show aaa servers
RADIUS: id 1, priority 1, host 172.26.204.121, auth-port 1812, acct-port 1813
     State: current UP, duration 546s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UNKNOWN, duration 546s, previous duration 0s
     SMD Platform Dead: total time 0s, count 0
```

AAA server up and running from IOSd

Global Cisco TrustSec (CTS) Configurations



TrustSec authorization should use cts-list AAA servers

```
cts authorization list cts-list
```

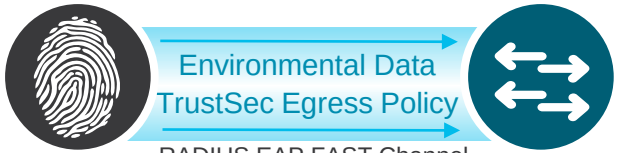
For SGT policy enforcement, if switch has to access control

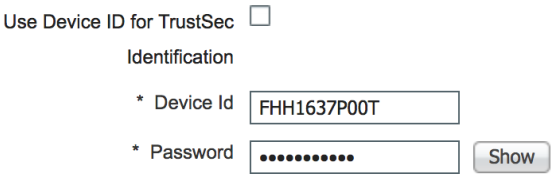
```
cts role-based enforcement
cts role-based enforcement vlan-list <VLANs>
```

Global AAA Configuration for all IOS Switches

```
aaa new-model
!
aaa authentication dot1x default group ise-group
aaa authorization network default group ise-group
aaa authorization network cts-list group ise-group
aaa accounting dot1x default start-stop group ise-group
!
aaa server radius dynamic-author
 client <Switch_IP> server-key cisco
!
radius server ise
 address ipv4 <ISE_IP> auth-port 1812 acct-port 1813
 pac key <PAC_Password>
!
aaa group server radius ise-group
 server name ise
!
```

ISE and ‘Network Device’ Transact Securely Using PAC keys





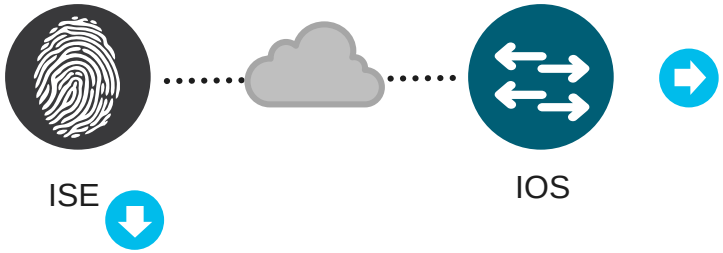
Switch *authenticates with Cisco ISE for Secure EAP FAST Channel*

```
Switch# cts credential id <device_id> password <cts_password>
```

RADIUS PAC* *keys pushed by ISE. Switch uses this to talk to ISE securely*

```
bldg24-edge-3650-1#show cts pacs
AID: 5079AA777CC3205E5D951003981CBF95
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 5079AA777CC3205E5D951003981CBF95
  I-ID: FDO1947Q1F1
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 15:30:58 PST Mon May 28 2018
PAC-Opaque:
000200B800010211000400105079AA777CC3205E5D951003981CBF950006009C0003
0100C25BAEC6DC8B90034431914E48C335DC000000135A95A90900093A8087E1E4
7B8EA12456005D6E38C41F69C19F86B884B370177982EB65469F1E5F6B2B6D96B7
1C99DA19B240FE080757F8F8BBD543AE830A5959EA4A999C310CE1FEC427213AA
552406796C8DDDA695DBCF08FB3473249DCC025598D27CD280E4D01E7877F14C6
F211CC3BAB5E3B836A6B42A9C5EE4E0E6F997549D10561
Refresh timer is set for 11w3d
```

Environmental Data



Security Groups
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

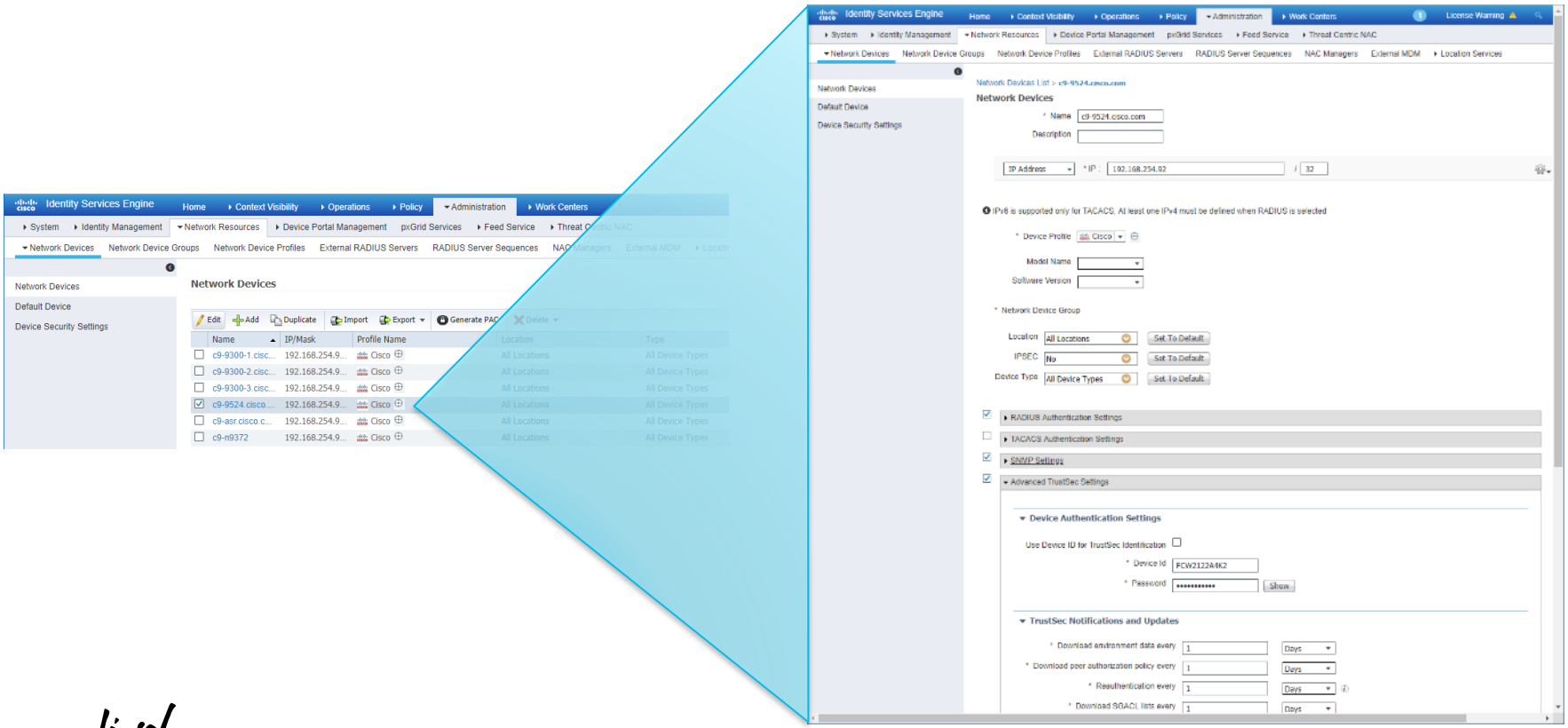
Edit | Add | Import | Export | Delete | Push

Icon	Name	SGT (Dec / Hex)
	Unknown	0/0000
	Employee_FullAccess	10/000A
	PCI_Devices	100/0064
	Web_Servers	110/006E
	Mail_Servers	120/0078
	TrustSec_Infra_SGT	2/0002
	Employee_BYOD	20/0014
	Unregist_Dev_SGT	255/00FF
	Contractors	30/001E

```
Switch# show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-00:TrustSec_Infra_SGT
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.1.1.222, port 1812, A-ID 3E465B9E3F4E012E6AD3159B403B5004
          Status = DEAD
          auto-test = TRUE, keywrap-e
= 20 secs
Multicast Group SGT Table:
Security Group Name Table:
    0-00:Unknown
    2-00:TrustSec_Infra_SGT
    10-00:Employee_FullAccess
    20-00:Employee_BYOD
    30-00:Contractors
    100-00:PCI_Devices
    110-00:Web_Servers
    120-00:Mail_Servers
    255-00:Unregist_Dev_SGT
Environment Data Lifetime = 86400 secs
Last update time = 21:57:24 UTC Thu Feb 4 2016
Env-data expires in   0:23:58:00 (dd:hr:mm:sec)
Env-data refreshes in 0:23:58:00 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

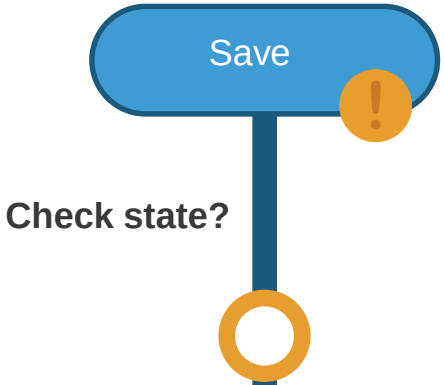
```
Security Group Name Table:
    0-00:Unknown
    2-00:TrustSec_Infra_SGT
    10-00:Employee_FullAccess
    20-00:Employee_BYOD
    30-00:Contractors
    100-00:PCI_Devices
    110-00:Web_Servers
    120-00:Mail_Servers
    255-00:Unregist_Dev_SGT
```

If CTS is not Configured, Verify the Device is a NAD



Configuration Issues

Configuration not pushed to the network device



Device Inventory

☐	BLD1-FLR1-ACCESS	192.168.12.4	Reachable	13 days, 22:29:45.45	20 minutes ago	00:25:00	Managed

Device should be Reachable aged

Debug Inventory Issue

Before You Add to Fabric

Configure Loopback 0

```
interface Loopback0
 ip address <>
 ip router isis
```

If you are using **Automated Underlay** skip this setup

This is only required for **Manual Underlay** configuration

Different Types of Error

Validation Check

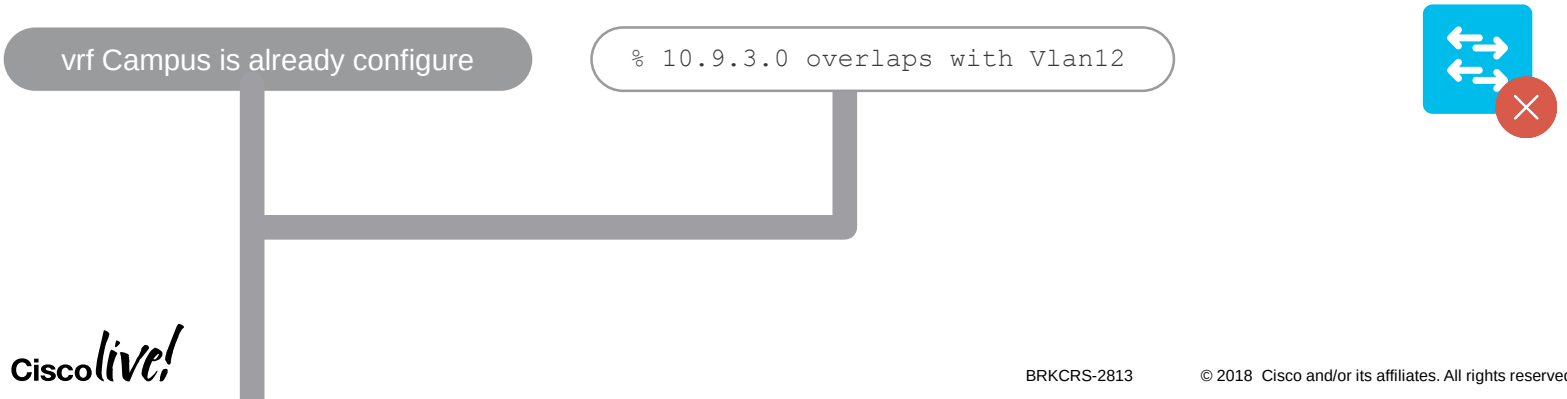
When stale config is present on the device and DNAC config validation throws an error.

Configuration Error

CLI errors out on the device

Internal Error

No config change is pushed to the device.



Fix the configuration on the device

```
(config)#no vrf definition Campus
```

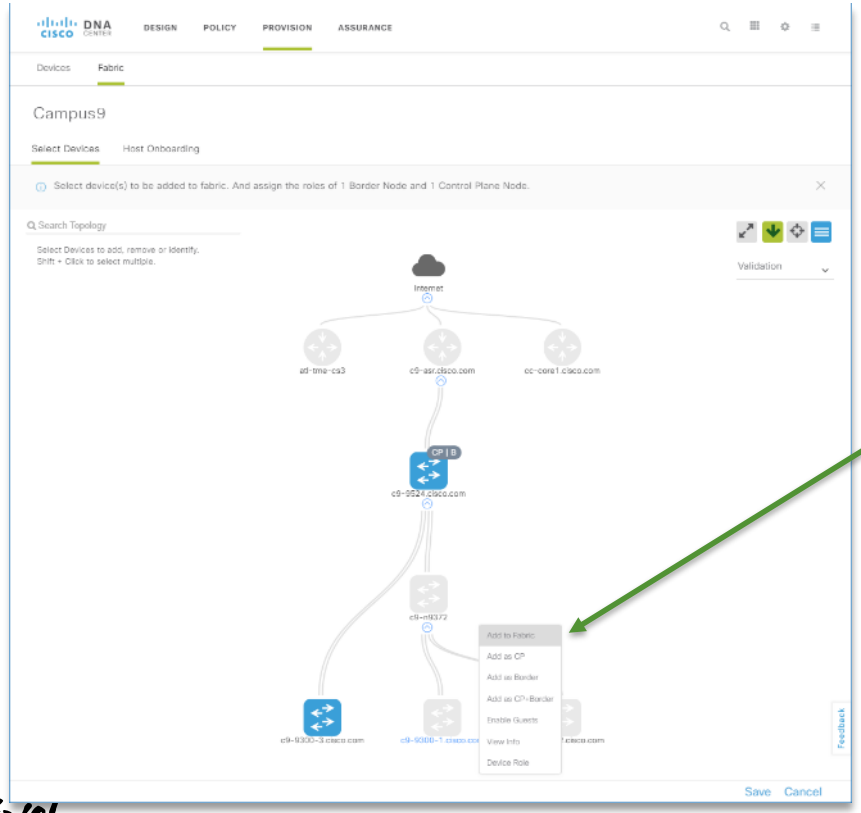
Navigate to Device inventory

Device Inventory

Select the device and click “Resync”

SD-Access Fabric Provisioning

Fabric Edge Configuration



- LISP configuration
- VRF/VLAN configuration
- SVI configuration
- Interface configuration

VLAN and VRF Configuration

```
FE2050#show run  | beg vrf
vrf definition BruEsc
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
vrf definition DEFAULT_VN
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
```

One VRF per VN

```
FE2050#show run  | sec vlan
ip dhcp snooping vlan 1021-1024
vlan 1021
 name 192_168_1_0-BruEsc
vlan 1022
 name 192_168_100_0-BruEsc
vlan 1023
 name 192_168_200_0-DEFAULT_VN
cts role-based enforcement vlan-list 1021-1023
```

One VLAN per IP Address Pool
DHCP Snooping and CTS are enabled

Control Plan Configuration

```
FE2050#show run | sec lisp
router lisp
 locator-table default
 locator-set rloc_6b293939-e713-460d-96e9-228cae628bd
  IPv4-interface Loopback0 priority 10 weight 10
  exit-locator-set
 !
 locator default-set rloc_6b293939-e713-460d-96e9-
228cae628bdf
 service ipv4
  encapsulation vxlan
  map-cache-limit 25000
  database-mapping limit dynamic 5000
  itr map-resolver 192.168.254.92
  etr map-server 192.168.254.92 key uci
  etr map-server 192.168.254.92 proxy-reply
  etr
  sgt
  no map-cache away-eids send-map-request
  proxy-itr 192.168.254.96
  exit-service-ipv4
 !
 service ethernet
  map-cache-limit 25000
  database-mapping limit dynamic 5000
  itr map-resolver 192.168.254.92
  itr
  etr map-server 192.168.254.92 key uci
  etr map-server 192.168.254.92 proxy-reply
  etr
  exit-service-Ethernet
 !
```

```
instance-id 4097
  remote-rloc-probe on-route-change
  service ipv4
   eid-table default
   map-cache 0.0.0.0/0 map-request
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 4099
  remote-rloc-probe on-route-change
  service ipv4
   eid-table vrf DEFAULT_VN
   map-cache 0.0.0.0/0 map-request
   exit-service-ipv4
  !
  exit-instance-id
 !
 instance-id 4099
  remote-rloc-probe on-route-change
  dynamic-eid 172_16_109_0-Campus9
   database-mapping 172.16.109.0/24 loca
e713-460d-96e9-228cae628bdf
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf Campus9
   map-cache 0.0.0.0/0 map-request
   exit-service-ipv4
  !
  exit-instance-id
```

```
instance-id 8188
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1021
   database-mapping mac locator-set rloc_6b293939-
e713-460d-96e9-228cae628bdf
   exit-service-ethernet
  !
  exit-instance-id
 !
 instance-id 8189
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 1022
   database-mapping mac locator-set rloc_6b293939-
e713-460d-96e9-228cae628bdf
   exit-service-ethernet
  !
  exit-instance-id
 !
 map-server nmr non-site-ttl 1440
 ipv4 locator reachability exclude-default
 exit-router-lisp
snmp-server enable traps lisp
```

Anycast Gateway Configuration

```
FE2050#show run int vlan 1021
Building configuration...

Current configuration : 319 bytes
!
interface Vlan1021
 description Configured from apic-em
 mac-address 0000.0c9f.f45c
 vrf forwarding BruEsc
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 10.254.255.58
 no ip redirects
 ip local-proxy-arp
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 192_168_1_0-BruEsc
end
```

No Layer 2 Extension

```
FE2050#show run int vlan 1023
Building configuration...

Current configuration : 313 bytes
!
interface Vlan1023
 description Configured from apic-em
 mac-address 0000.0c9f.f45e
 vrf forwarding DEFAULT_VN
 ip address 192.168.200.254 255.255.255.0
 ip helper-address 10.254.255.58
 no ip redirects
 ip route-cache same-interface
 no lisp mobility liveness test
 lisp mobility 192_168_200_0-DEFAULT_VN
end
```

Layer 2 Extension (wireless)

Host Interface Configurations

```
FE2051#show run int gi 1/0/1
Building configuration...

Current configuration : 258 bytes
!
interface GigabitEthernet1/0/1
 switchport access vlan 1021
 switchport mode access
 switchport voice vlan 1022
 device-tracking attach-policy IPDT_10
 load-interval 30
 cts manual
  policy static sgt 4
  no propagate sgt
 spanning-tree portfast
end
```

No Authentication with voice/data and static SGT

```
FE2051#show run int gi 1/0/1
Building configuration...
interface GigabitEthernet1/0/1
 switchport access vlan 1021
 switchport mode access
 switchport voice vlan 1022
 device-tracking attach-policy IPDT_MAX_10
 load-interval 30
 authentication control-direction in
 authentication host-mode multi-auth
 authentication open
 authentication order mab
 authentication priority mab
 authentication port-control auto
 mab
 spanning-tree portfast
end
```

Easy Connect (MAB)

Host Interface Configurations (cont'd)

```
FE2051#show run int gi 1/0/1
interface GigabitEthernet1/0/1
 switchport access vlan 1021
 switchport mode access
 switchport voice vlan 1022
 device-tracking attach-policy IPDT_MAX_10
 load-interval 30
 authentication control-direction in
 authentication event server dead action authorize vlan 3999
 authentication event server dead action authorize voice
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 authentication timer inactivity server dynamic
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
 spanning-tree portfast
end
```

Closed Authentication runs Dot1x and MAB

Open authentication adds "authentication open"

Troubleshooting – Device / Fabric Provision Issues

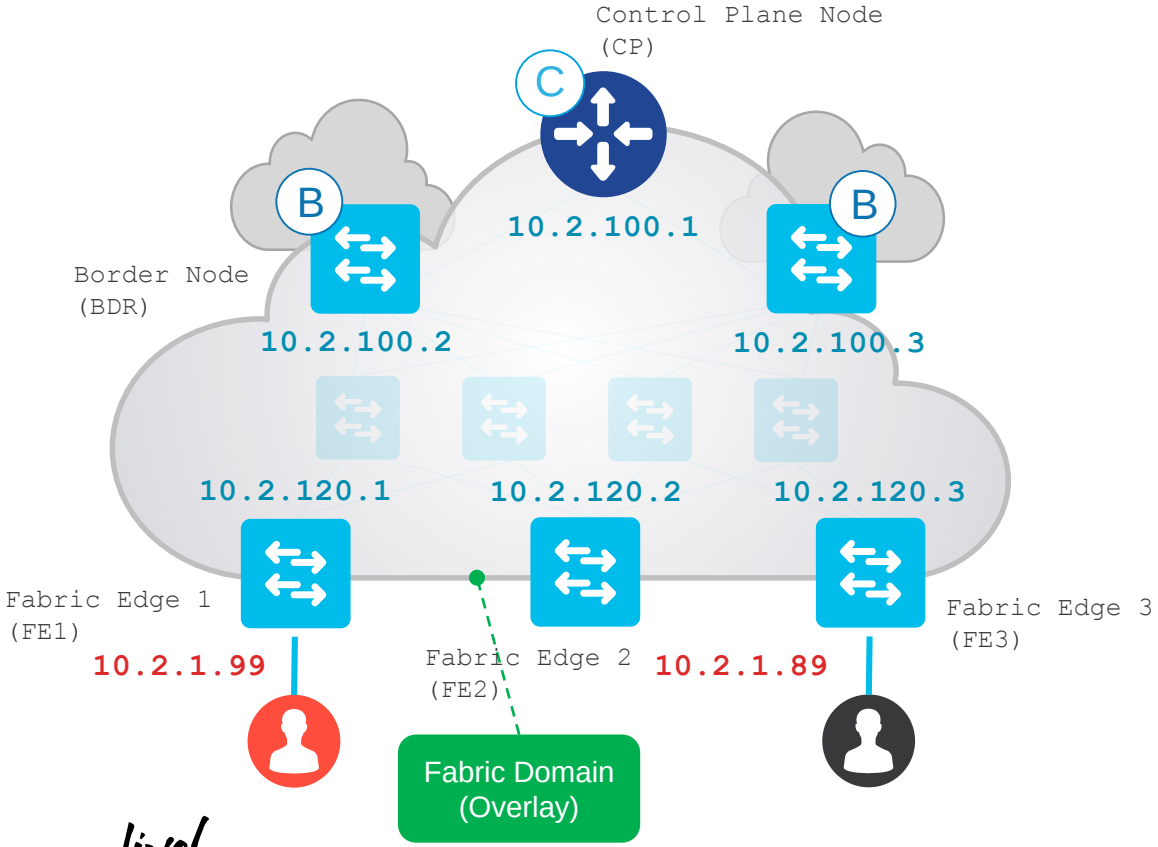
Services involved:

- orchestration-engine-service
- spf-service-manager-service
- spf-device-manager-service
- apic-em-network-programmer-service

```
2017-07-27 20:02:17,812 |   WARN | ew-4                          |  | c.c.a.o.t.task.WorkflowTaskContext | Value not found for the key spf.cfs.qualifier from the
task c48cb15b-d6fe-40c3-a1df-5d1ebfbb23b6 |
2017-07-27 20:02:17,812 |   INFO | ew-4                          |  | c.c.a.c.s.t.SPFTaskExecutionAdapter | SPF Perf Monitoring: Time taken to execute step spf.cf
sValidatorTaskAdapter with type ConnectivityDomain and qualifier null is 0 secs |
2017-07-27 20:02:17,812 |   INFO | ew-4                          |  | c.c.a.o.t.e.AbstractMessageExecutor | Notifying the Task Result com.cisco.apicem.orchestrati
on.taskengine.task.WorkflowTaskResult@6578187f for the Workflow Task Id c48cb15b-d6fe-40c3-a1df-5d1ebfbb23b6  |
2017-07-27 20:02:17,812 |   INFO | ew-4                          |  | c.c.a.o.t.s.AbstractTaskStatusNotification | Sending the response to orchestration engine: E
xecutorResponseMessage:{ workflowId: 315619b4-a9d2-4044-850a-f9ab9258d3af, executionContextId: 8229b3f2-51e7-4ee4-9695-a2aba6553d1f, taskId: c48cb15b-d6fe-40c
3-a1df-5d1ebfbb23b6, targetId: Default; shardId: 0; executorType: spf.cfsValidatorTaskAdapter; executorAction: 315619b4-a9d2-4044-850a-f9ab9258d3af, taskStatu
s: FAILED; statusMessage: ConnectivityDomain validateCFS - Device with id 0936d908-9d7b-4590-8b26-b5287defa9bf is not present in the inventory}, shardId: 0 |
2017-07-27 20:02:17,813 |   INFO | SimpleAsyncTaskExecutor-2 |  | c.c.a.c.spf.util.SpfMessageFactory | message ServiceCompletionMessage {context null, replyTo
Chain=null, version=0, payload=ServiceCompletionDTO [taskId=4d7fb849-c687-4bcb-a388-71948f863571, success=false, failureReason=Execution failed for task [Vali
date-Cfs-Task:c48cb15b-d6fe-40c3-a1df-5d1ebfbb23b6]  with error message => ConnectivityDomain validateCFS - Device with id 0936d908-9d7b-4590-8b26-b5287defa9b
f is not present in the inventory, errorCode=InternalError, snapshotVersion=-1, snapshotNamespace=4aa9bafd-36b4-44a4-8263-88432cf679f2, type=ConnectivityDomai
n, qualifier=null, spfAdapterTaskInfo=null, isRetriable=false, corelationData=null, associatedSprNamespaceVersionPairs=null]} |
2017-07-27 20:02:17,813 |   INFO | SimpleAsyncTaskExecutor-2 |  | c.c.a.c.s.h.ServiceCompletionMessageHandler | notifying serviceCompletionMessage. |
2017-07-27 20:02:18,339 |   INFO | qtp586084331-932          |  | c.c.g.r.c.i.RandomServiceInstanceCache | Waiting for instance of serviceType=cas-service, ve
rsion=latest, timeout=10000, subscriber=GrapevineCasServiceEndpointManager |
```

SD-Access Fabric Troubleshooting

Typical SD-Access Environment



- **Underlay Network**
- **Routing ID (RLOC)** – IP address of the LISP router facing ISP
- **Overlay Network**
- **Endpoint Identifier(EID)** - IP address of a host
- **VRF** - Campus
- **Instance Id** - 4099
- **Dynamic EID** – 10_2_1_0-Campus
- **VLAN** – 1021

Here Is How You Begin

- Host Registration
- Host Resolution
- External Connectivity
- DHCP Packet Flow
- East West Traffic
- Host Mobility

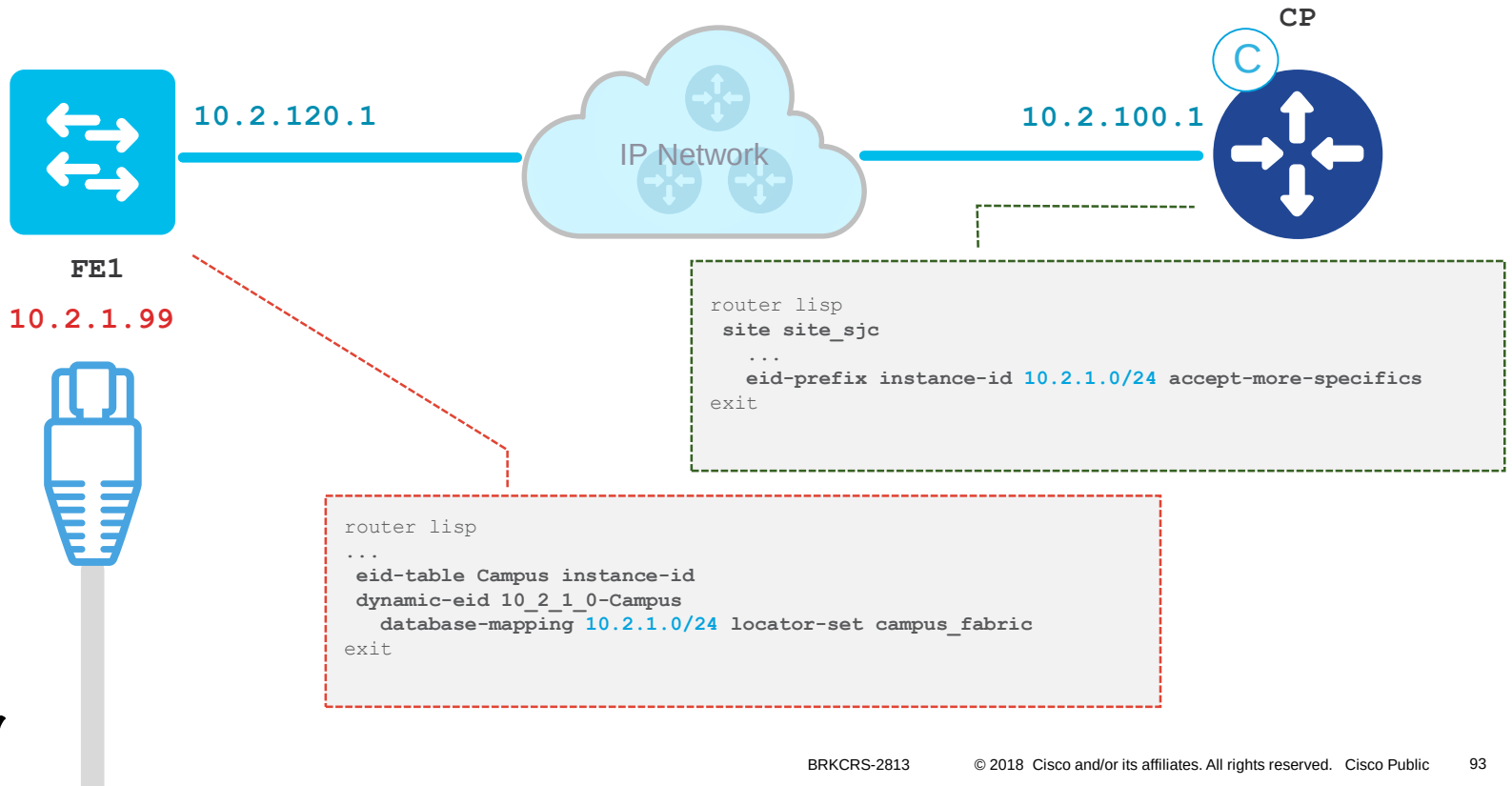
Different hosts

Wired Client

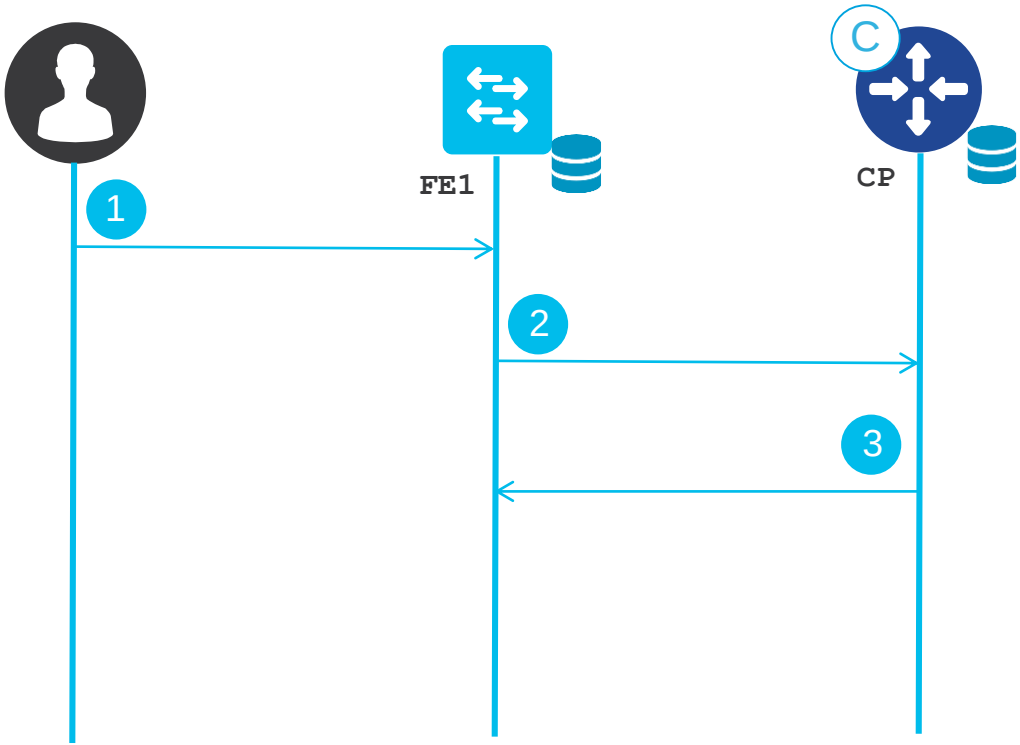
Access Point

Wireless Client

Case 1: Host Registration – Wired Client



Registration Message flow

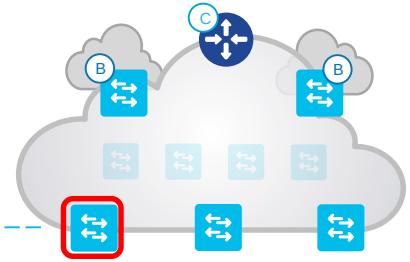


1. Client send ARP, DHCP or DATA pkt
2. FE saves the host info in local database. Send the registration message to CP (Map–server)
3. CP receives the registration message saves the host tracking database and send the reply

MAC Address ?

1

```
FE1#show mac address
1021   0013.a91f.b2b0 DYNAMIC Te1/0/23
```



If you don't see the MAC address entry, then it's a SILENT HOST.

ARP Entry ?

2

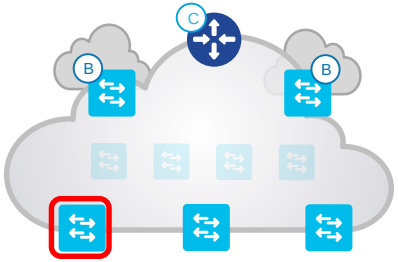
```
FE1#show arp vrf Campus
Protocol  Address      Age (min)  Hardware Addr   Type   Interface
Internet  10.2.1.99           0   0013.a91f.b2b0  ARPA   Vlan1021
```

IP Device Tracking ?

3

```
FE1#show device-tracking database
    Network Layer Address   Link Layer Address Interface  vlan
ARP 10.2.1.99               0013.a91f.b2b0     Te1/0/23   1021
```

Fabric Edge can learn the IP address from ARP, DHCP or DATA pack. If device tracking entry is missing then check if client got an IP



LISP local database ?

Fabric Edge

4

```
FE1#show ip lisp instance-id 4099 database
LISP ETR IPv4 Mapping Database for EID-table vrf Campus (IID 4099)
LSBs: 0x1 Entries total 3, no-route 0, inactive 0

10.2.1.99/32, dynamic-eid 10_2_1_0-Campus, locator-set rloc_021
  Locator      Pri/Wgt  Source     State
  10.2.120.1    10/10   cfg-intf   site-self, reachable
```

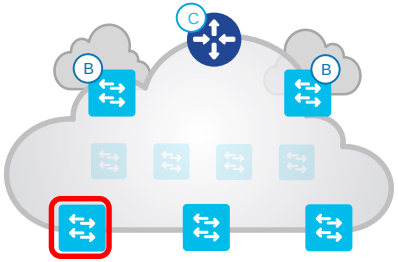
Enable debug if the database entry is missing

EID

FE1 RLOC

Instance ID

If No Local Database Entry ?



debug lisp control-plane local-eid-database

*Jan 17 01:47:15.101: LISP-0: Local EID IID **4099** prefix **10.2.1.99**/32, Setting state to active (state: inactive, rlocs: 0/0, sources: NONE).

debug lisp control-plane dynamic-eid

*Jan 17 01:47:15.102: LISP-0: Local dynEID **10_2_1_0-Campus** IID **4099** prefix **10.2.1.99**/32 RLOC **10.2.120.1** pri/wei=10/10, **Created** (IPv4 intf RLOC **Loopback0**) (state: active, rlocs: 1/1, sources: dynamic).

debug lisp forwarding data-signal-discover-dyn-eid

*Jan 17 01:47:15.102: LISP-0: DynEID IID **4099** **10.2.1.99** [10_2_1_0-Campus:Vlan1021] **Created**.

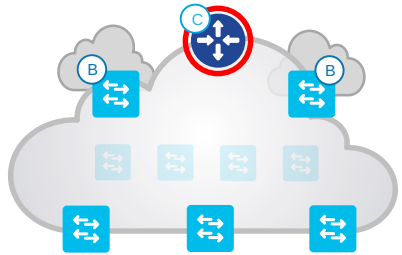
FE1 RLOC

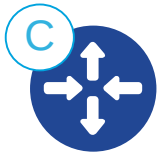
Instance ID

Dynamic EID

EID

LISP Control Plane Entry ?





5

```
CP#show lisp site instance-id 4099
Site Name      Last       Up     Who Last      Inst     EID Prefix
               Register          Registered      ID
site_sjc       never      no     --            4099     10.2.1.0/24
                 3d23h      yes#   10.2.120.1    4099     10.2.1.99/32
```

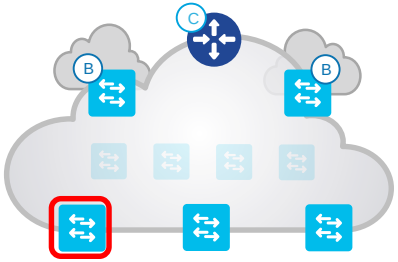
Enable debug on FE and Control Plane if the database entry is missing

FE1 RLOC

Instance ID

EID

Check if FE has sent the registration message ?

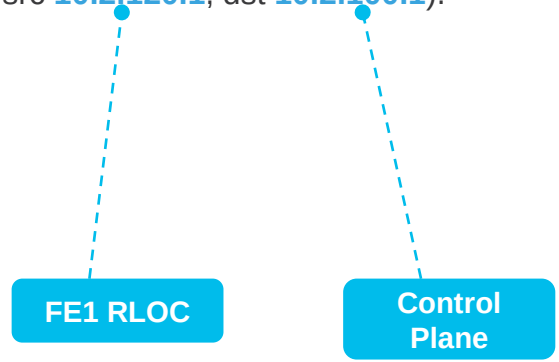


debug lisp control map-request

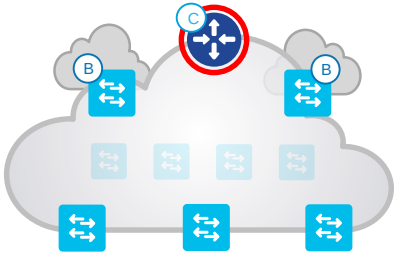
*Jan 17 01:56:01.045: LISP: Send map request for EID prefix IID **4099 10.2.1.99**/32

debug lisp forwarding data-signal-map-request

*Jan 17 01:56:02.204: LISP-0: EID-AF IPv4, **Sending map-request** from 10.2.1.99 to 10.2.1.99 for EID **10.2.1.99**/32, ITR-RLOCs 1, nonce 0x0B5B0D11-0x5110DF55 (encap src **10.2.120.1**, dst **10.2.100.1**).



Verification for registration message

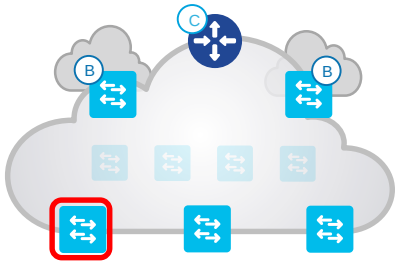


debug lisp control-plane map-server-registration

*Jan 17 01:57:27.716: LISP-0: MS EID IID **4099** prefix **10.2.1.99**/32 site site_sjc, **Forwarding map request** to ETR RLOC **10.2.120.1**

FE1 RLOC

debug lisp forwarding eligibility-process-switching

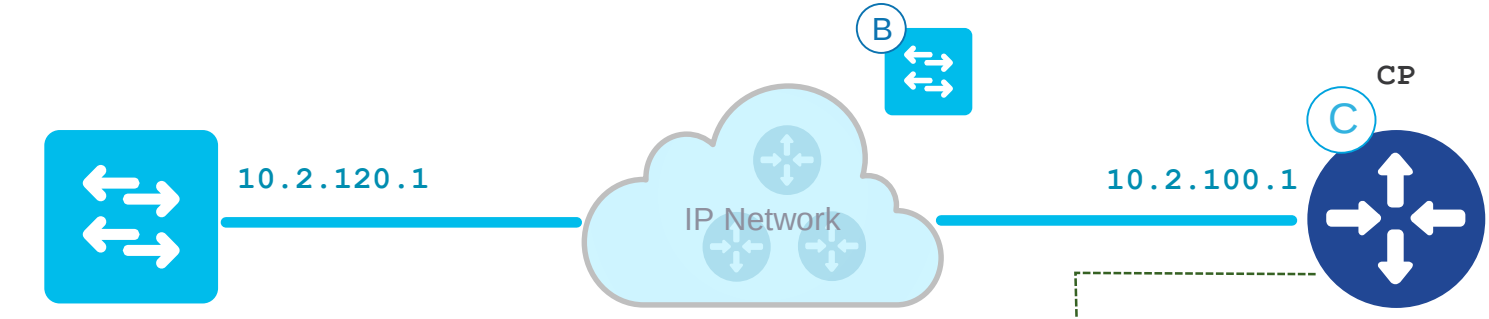


*Jan 17 01:56:02.209: LISP: Processing **received Map-Reply**(2) message on TenGigabitEthernet1/0/1 from **10.2.100.1**:4342 to **10.2.120.1**:4342

Control Plane

FE1 RLOC

Case 1b: Host Registration – Access Point

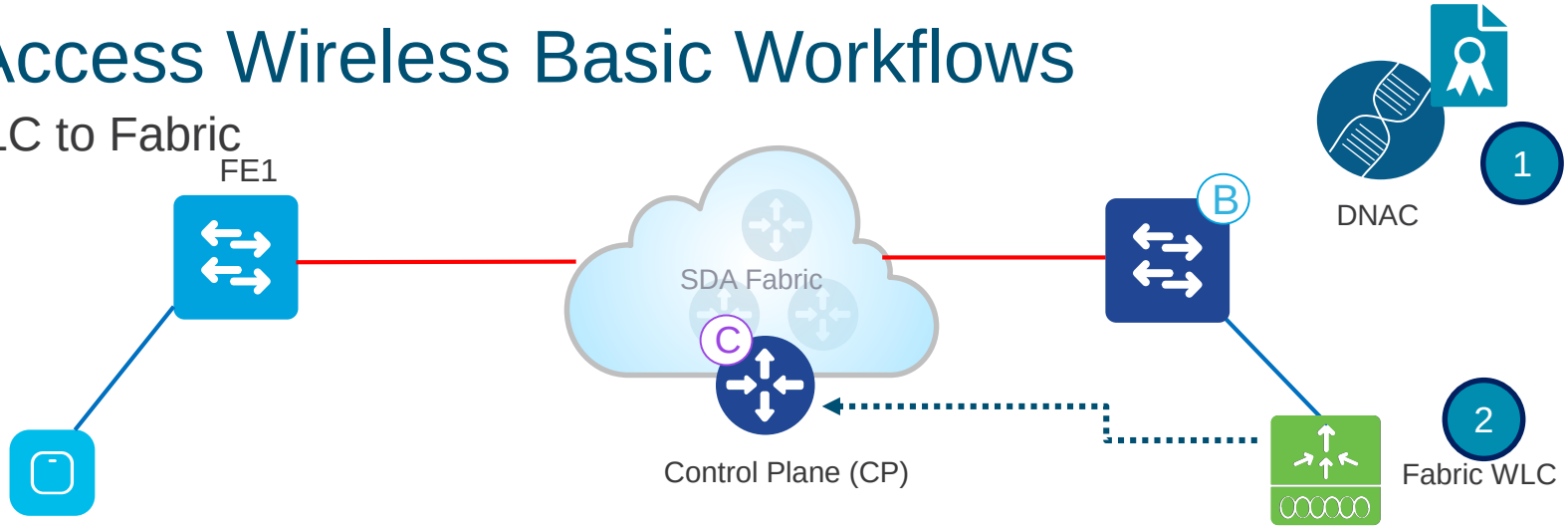



```
router lisp
 site site_sjc
   ...
   eid-prefix instance-id      10.2.1.0/24 accept-more-specifics
exit
```

```
router lisp
...
 eid-table Campus instance-id
 dynamic-eid 10_2_1_0-Campus
   database-mapping 10.2.1.0/24 locator-set campus_fabric
exit
```

SD-Access Wireless Basic Workflows

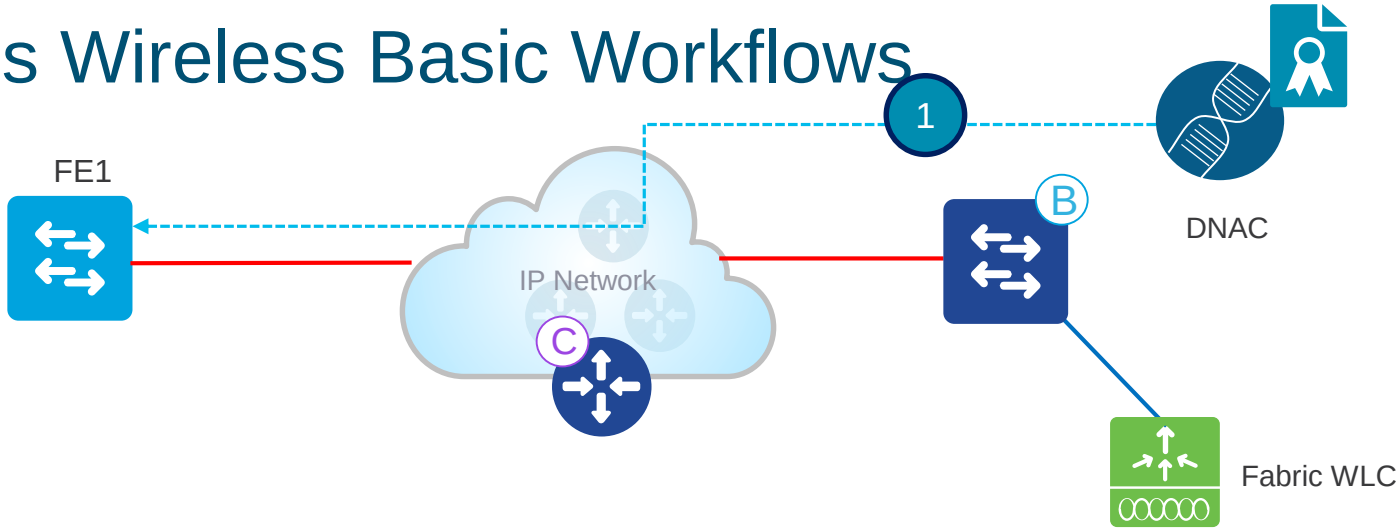
Add WLC to Fabric



1. In DNAC, first provision and then add WLC to Fabric Domain
2. Fabric configuration is pushed to WLC. WLC becomes Fabric aware. Most importantly WLC is configured with credentials to established a secure connection to CP
3. WLC is ready to participate in SD-Access Wireless

SD-Access Wireless Basic Workflows

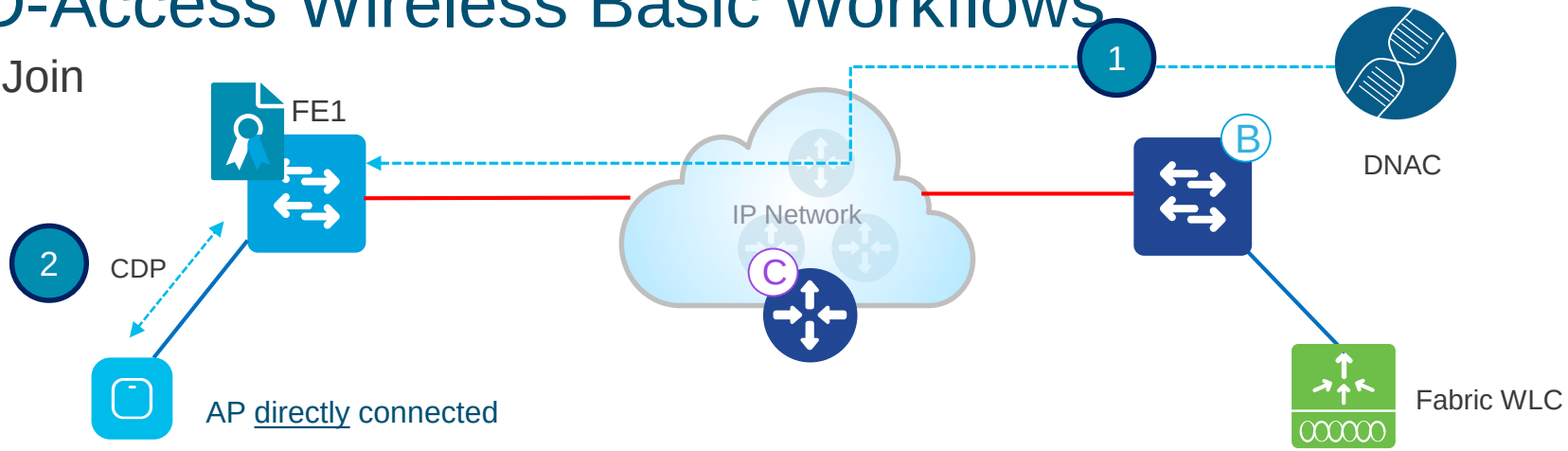
AP Join



1. Admin configures AP pool in DNAC in INFRA_VN. DNAC pre-provision a configuration macro on all the FEs

SD-Access Wireless Basic Workflows

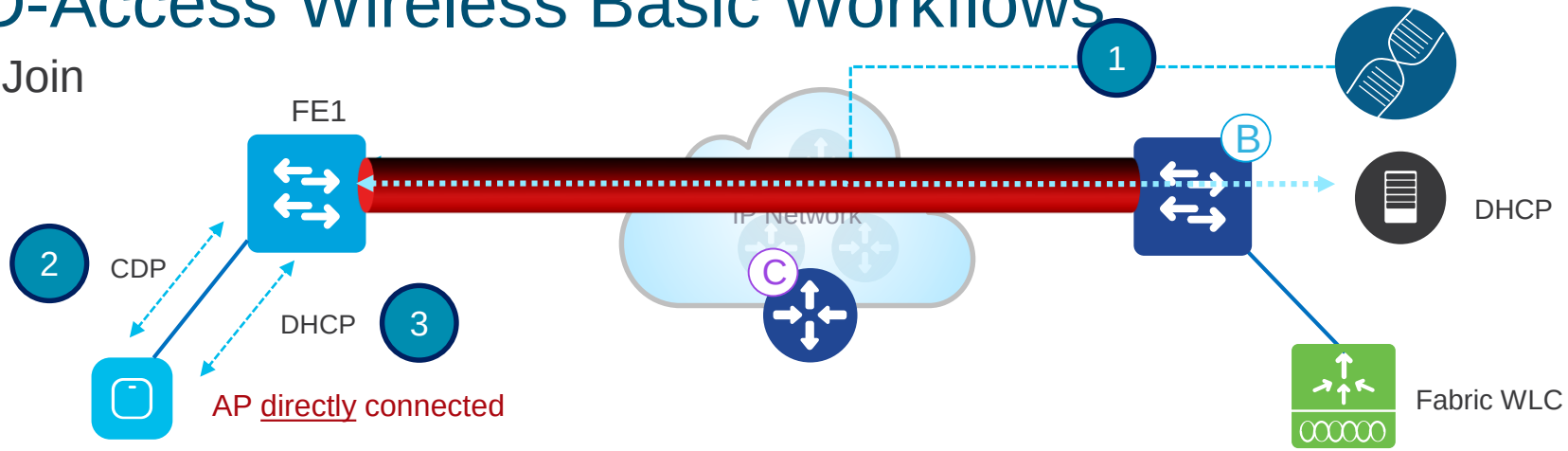
AP Join



1. Admin configures AP pool in DNAC in INFRA_VN. DNAC pre-provision a configuration macro on all the FEs
2. AP is plugged in and powers up. FE discovers it's an AP via CDP and applies the macro to assign the switch port the the right VLAN

SD-Access Wireless Basic Workflows

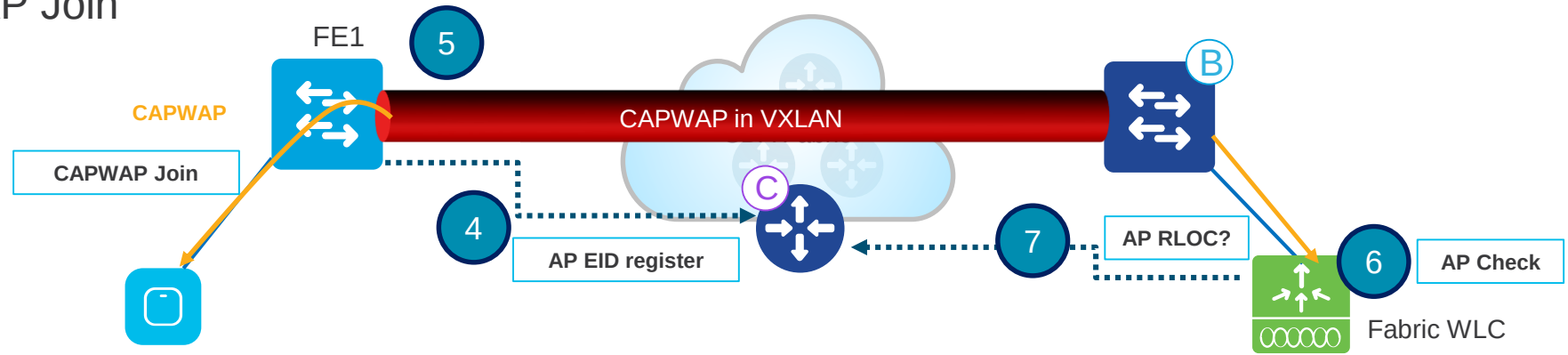
AP Join



1. Admin configures AP pool in DNAC inn INFRA_VN. DNAC pre-provision a configuration macro on all the FEs
2. AP is plugged in and powers up. FE discovers it's an AP via CDP and applies the macro to assign the switch port the the right VLAN
3. AP gets an IP address via DHCP in the overlay. Next, FE registers the AP as a "special" wired host into the Fabric

SD-Access Wireless Basic Workflows

AP Join



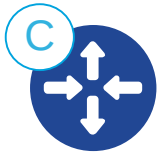
4 Fabric Edge registers AP's IP address (EID) and updates the Control Plane (CP)

5 AP learns and joins WLC using traditional methods. Fabric AP joins as a Local mode AP

6 WLC checks if it is fabric-capable (Wave 2 or Wave 1 APs)

7 If AP is supported for Fabric, WLC queries the CP to know if AP is connected to Fabric

LISP Control Plane Entry ?



1

```
CP#show lisp site instance-id 4099
Site Name        Last       Up      Who Last      Inst     EID Prefix
                 Register            Registered      ID
site_sjc         never      no      --            4099     10.2.1.0/24
                    3d23h      yes#   10.2.120.1    4099     10.2.1.7/32
```

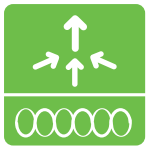
FE1 RLOC

Instance ID

EID

Is AP discovered?

2

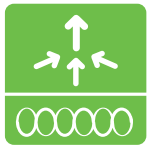


WLC

```
(Cisco Controller) >show ap summary

Number of APs.................................... 1

AP Name                 Slots  AP Model             Ethernet MAC       IP Address
----------------------  -----  -------------------  -----------------  ---------------
AP00A6.CA36.08D         2      AIR-AP3802P-T-K9     00:a6:ca:36:08:d8  10.2.1.7
```

Is AP fabric enabled?

3



WLC

```
(Cisco Controller) >show fabric summary

Fabric Support..................................... enabled

Enterprise Control Plane MS config
-----------------------------------

Primary Active MAP Server
IP Address..................................... 10.2.100.1

VNID Mappings configured: 1

Name                              L2-Vnid     L3-Vnid     IP Address/Subnet
--------------------------------  ----------  ----------  --------------------------------
ap_10_0_0_0                       41          4099            10.2.1.0 / 255.255.255.0
```

```
(Cisco Controller) >show ap config fabric AP00A6.CA36.08D8

Fabric Configuration Information For AP: AP00A6.CA36.08D8
Fabric status -   Enabled
Fabric L3vnid -   4099
Fabric L2vnid -   41
Fabric rlocIp -   10.2.120.1
```

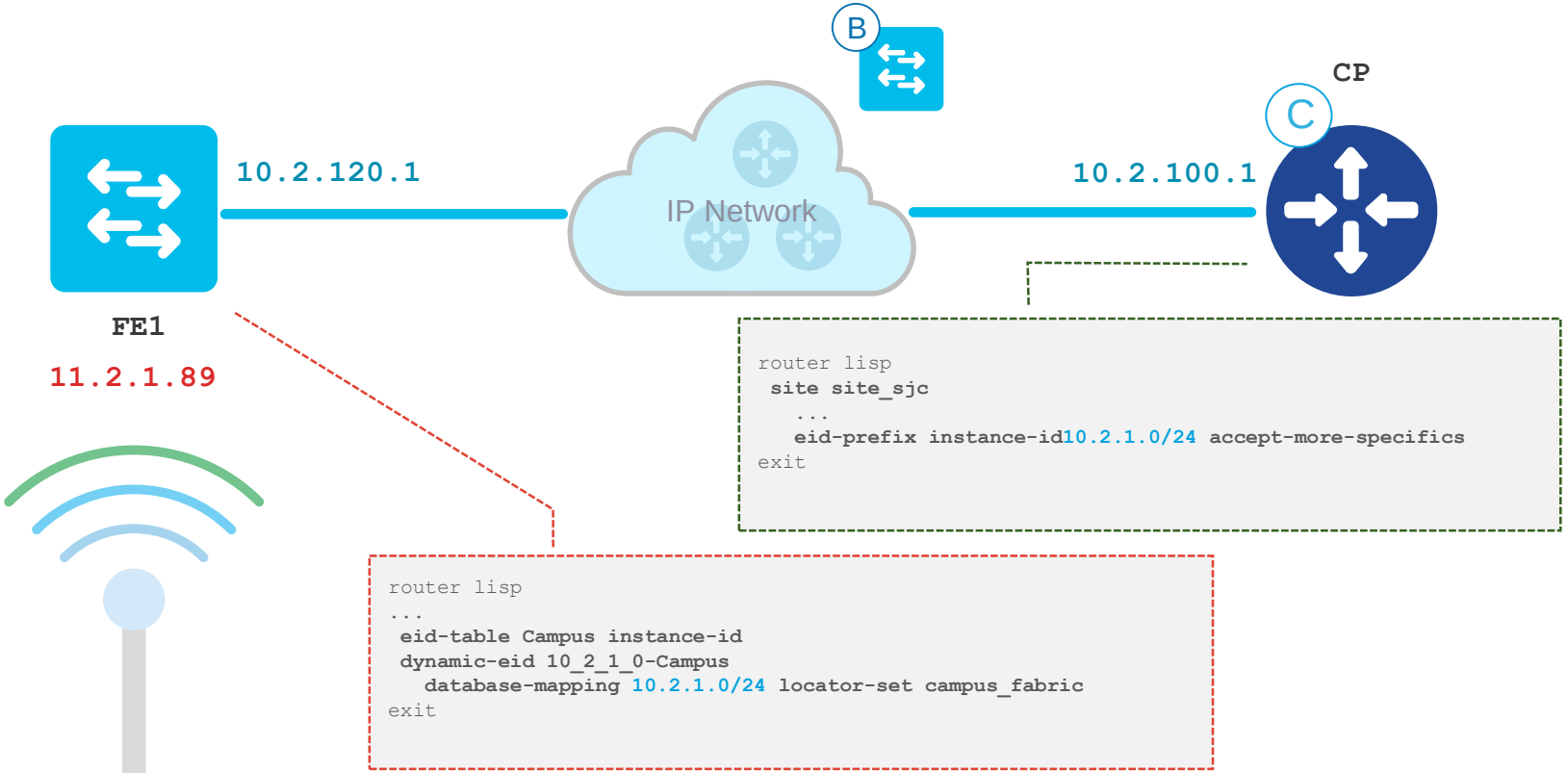
Is VXLAN tunnel UP?

4

Fabric Edge

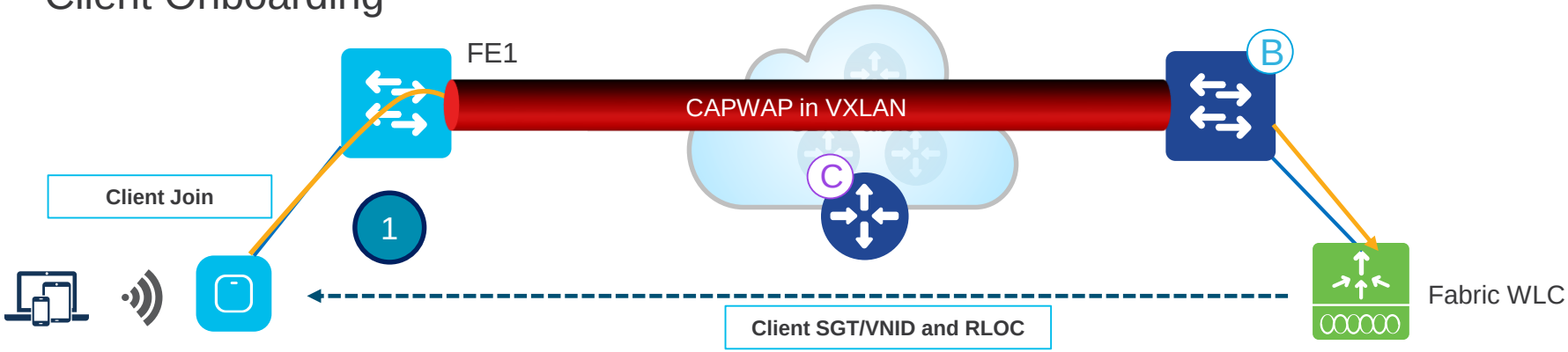
```
FE1#show lisp instance-id 41 ethernet database wlc
WLC clients/access-points information for router lisp 0 IID 41

Hardware Address    Type    Sources    Tunnel Update

----------------   ------   -------    -------------
 00d7.8fed.dba0      AP        1        Signalled

FE1#show access-tunnel summary
Access Tunnels General Statistics:
  Number of AccessTunnel Data Tunnels       = 1


Name    SrcIP            SrcPort DestIP           DstPort VrfId
------ --------------- ------- --------------- ------- ----
Ac0     10.2.120.1        N/A     10.2.1.7         4789    2

Name           IfId                 Uptime
------ ------------------ --------------------
Ac0    0x0000000000000057 4 days, 07:28:25
```

Case 1c: Host Registration – Wireless Client



SD-Access Wireless Basic Workflows

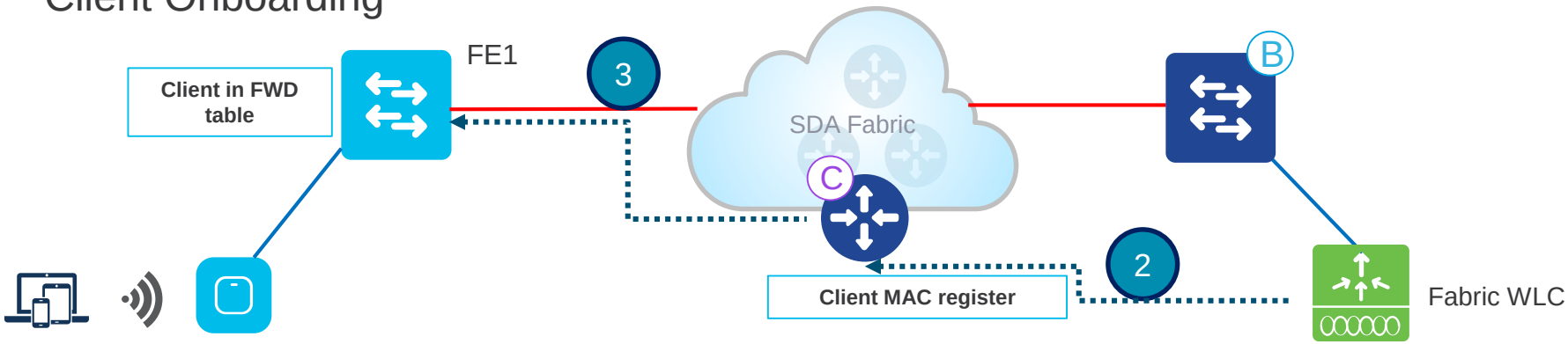
Client Onboarding



1. Client authenticates to a Fabric enabled WLAN. WLC gets SGT from ISE, updates AP with client L2VNID and SGT. WLC knows RLOC of AP from internal DB

SD-Access Wireless Basic Workflows

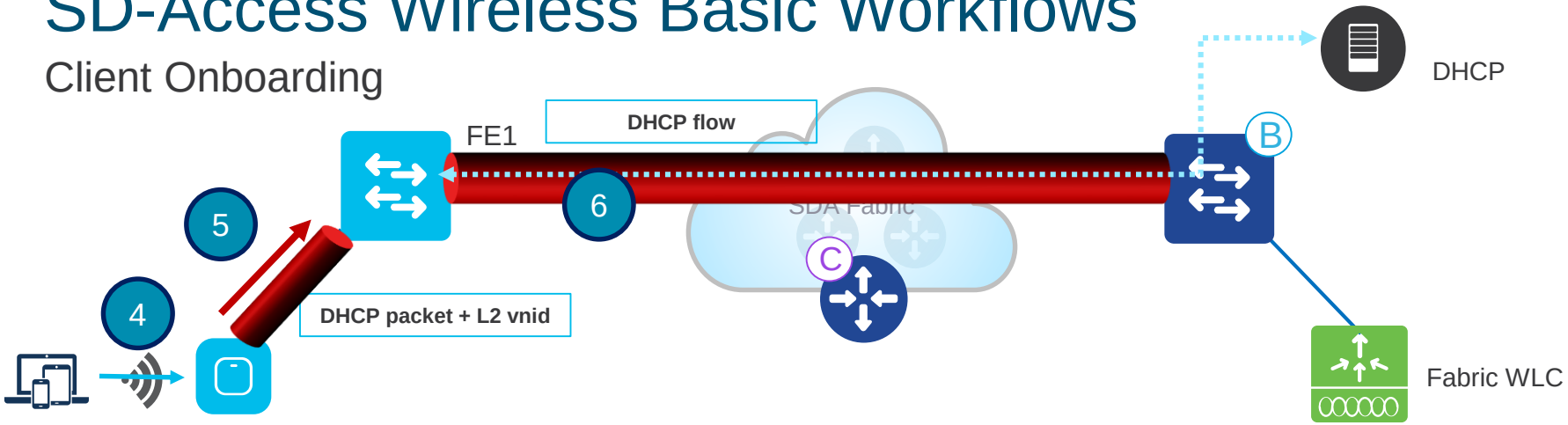
Client Onboarding



1. Client authenticates to a Fabric enabled WLAN. WLC gets SGT from ISE, updates AP with client L2VNID and SGT. WLC knows RLOC of AP from internal DB
2. WLC proxy registers Client L2 info in CP; this is LISP modified message to pass additional info, like the client SGT
3. FE gets notified by CP and adds client MAC in L2 forwarding table and go and fetch the policy from ISE based on the client SGT

SD-Access Wireless Basic Workflows

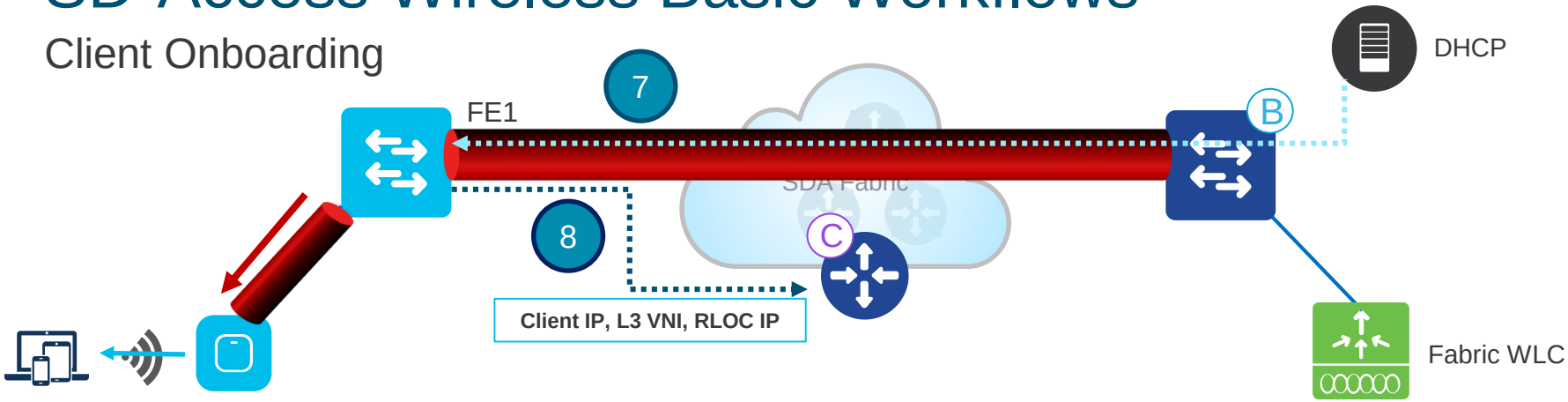
Client Onboarding



4. Client initiates DHCP Request
5. AP encapsulates it in VXLAN with L2 VNI info
6. Fabric Edge maps L2 VNID to VLAN interface and forwards DHCP in the overlay (same as for a wired Fabric client)

SD-Access Wireless Basic Workflows

Client Onboarding



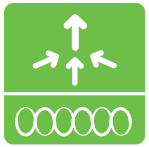
7 Client receives an IP address from DHCP

8 DHCP snooping (and/or ARP for static) triggers the client EID registration by the Fabric Edge to the CP

This completes Client onboarding process

Is WLAN fabric enabled ?

1

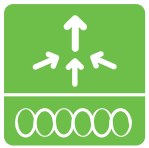


WLC

```
(Cisco Controller) >show fabric summary
VNID Mappings configured: 1

Name                              L2-Vnid     L3-Vnid     IP Address/Subnet
--------------------------------  ----------  ----------  --------------------------------
ap_10_0_0_0                       41          4099        10.2.1.0 / 255.255.255.0


Fabric Enabled Wlan summary
WLAN ID  WLAN Profile Name / SSID                Vnid        Tag       Peer ip
-------  ------------------------------------  ----------  -------  -----------
2        fabric_wlan51 / fabric_wlan51           41          0        0.0.0.0
```

Is client Associated?

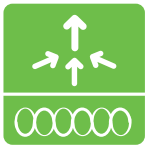
2



WLC

```
(Cisco Controller) >show client summary


Number of Clients.................................. 1
Number of PMIPV6 Clients........................... 0
Number of EoGRE Clients............................ 0

MAC Address       AP Name          Slot Status        WLAN  Auth Protocol         Port Wired Tunnel  Role
----------------- ---------------- ---- ------------- ----- ---- ---------------- ---- ----- ------- --------

b8:27:eb:ac:4c:d8 AP00A6.CA36.08D8  0   Associated      2    Yes   802.11n(2.4 GHz)
1    No    No      Local
```

Is WLAN fabric enabled ?

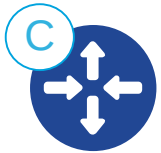


WLC

3

```
(Cisco Controller) >show client detail b8:27:eb:ac:4c:d8
Client MAC Address.............................. b8:27:eb:91:0b:80
Client Username ................................ N/A
. . .
Client State.................................... Associated
Client User Group.............................
Client NAC OOB State............................ Access
Wireless LAN Id................................. 2
. . .
Authentication Algorithm........................ Open System
802.1P Priority Tag............................. disabled
Security Group Tag.............................. 1000
. . .
Fabric Configuration
--------------------
Fabric Status: ................................. Enabled
Vnid: .......................................... 41
```

Is client registered?



4

```
CP#show lisp instance-id 41 ethernet server
LISP Site Registration Information

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_sjc       never     no     --                   41       any-mac
               00:11:34  yes#   10.2.120.1           41       18F6.43E1.3FFB /48
```

Is client entry on access-tunnel ?

5

Fabric Edge

```
FE1#show mac address-table vlan 1021
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 1021   18F6.43E1.3FFB    DYNAMIC     Ac0
```

Is AP to FE VXLAN tunnel up ?

6

AP

```
AP00A6.CA36.08D8#show ip tunnel fabric
Fabric GWs Information:
Tunnel-Id     GW-IP           GW-MAC  Adj-Status Encap-Type Packet-In Bytes-In
        1 10.2.120.1 00:42:5A:91:89:46    Forward     VXLAN       930   100370
```

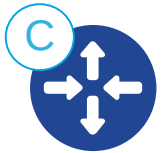
Is client entry on access-tunnel ?

7

AP

```
AP00A6.CA36.08D8#show controllers dot11Radio 0 client 18:F6:43:E1:3F:FB
                mac radio vap aid state encr Maxrate is_wgb_wired      wgb_mac_addr
18:F6:43:E1:3F:FB     0    1   2    FWD OPEN     M7         false 00:00:00:00:00:00

fabric client details:
           client IP_ACL SGT VNID     GW_IP
18:F6:43:E1:3F:FB          0   41 10.2.120.1
```

LISP Control Plane Entry ?



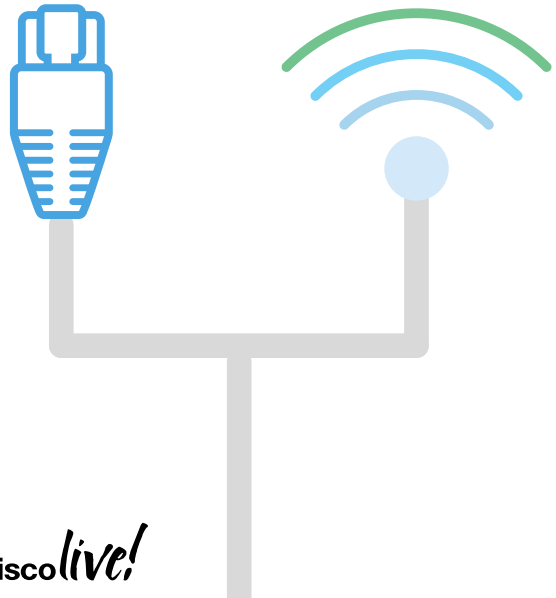
8

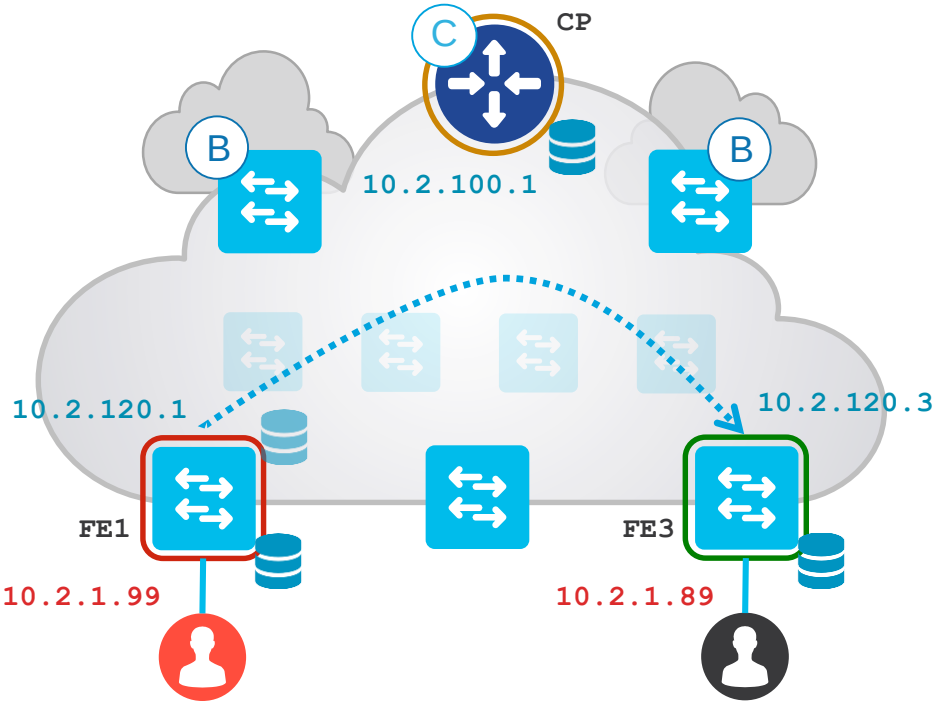
```
CP#show lisp site instance-id 4099
Site Name      Last       Up     Who Last      Inst     EID Prefix
               Register          Registered     ID
site_sjc       never      no     --             4099     10.2.1.0/24
                   3d23h      yes#   10.2.120.1     4099     10.2.1.89/32
```

Wired and Wireless Host Resolution

Wired Clients

Wireless Clients





Map Cache Entry ?

1

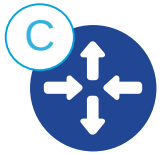
Fabric Edge

```
FE1#show ip lisp map-cache instance-id 4099
LISP IPv4 Mapping Cache for EID-table vrf Campus (IID 4099), 5 entries

10.2.1.89/32, uptime: 00:05:16, expires: 23:57:59, via map-reply, complete
  Locator      Uptime    State      Pri/Wgt
  10.2.120.3   00:04:23  up          10/10
```

If you don't see the MAC address entry, then it's a SILENT HOST.

Control Plane Entry ?

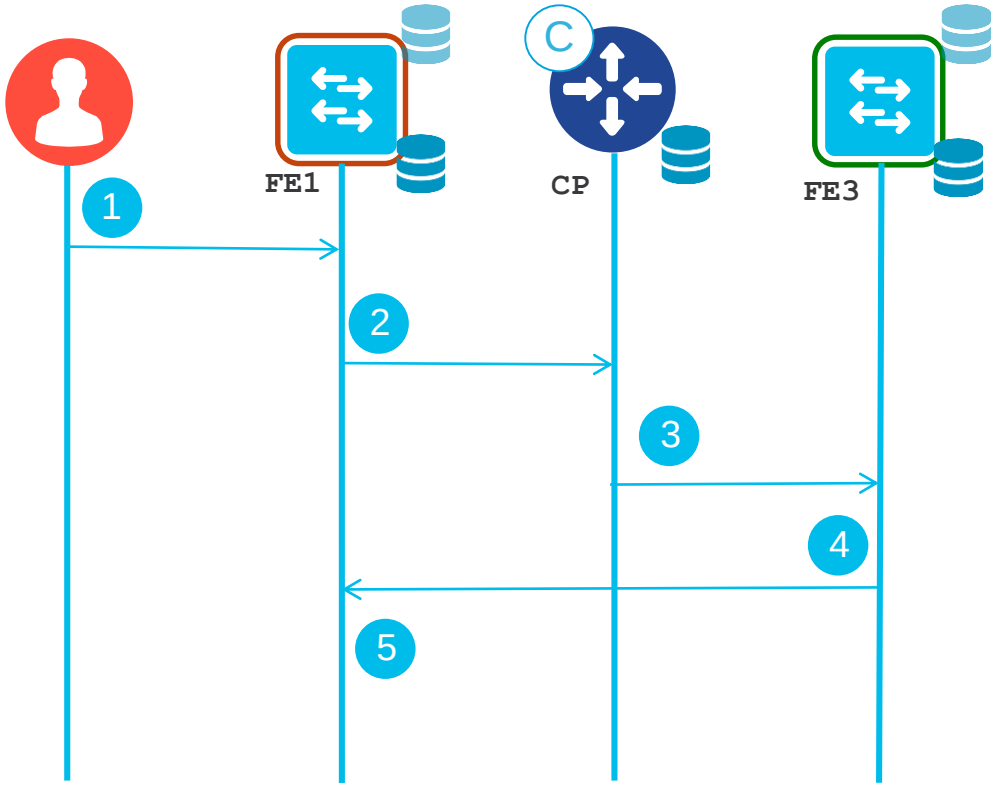
2




```
CP#show lisp site instance-id 4099
Site Name      Last       Up     Who Last              Inst     EID Prefix
               Register          Registered            ID
site_sjc       never      no     --                    4099     10.2.1.0/24
               3d23h      yes#   10.2.120.1            4099     10.2.1.99/32
               3d23h      yes#   10.2.120.3            4099     10.2.1.89/32
```

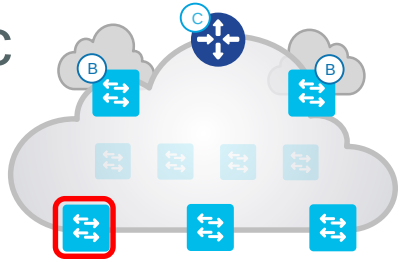
If you don't see the MAC address entry, then it's a SILENT HOST.

Host Resultion
Message flow



1. A client wants to establish communication to a Host2
2. No local map-cache entry Host2 on FE1. Map-Request is sent to the CP(Map-Resolver)
3. CP(Map Server) forwards the original Map-Request to the FE3(ETR) that last registered the EID subnet
4. FE3(ETR) sends to the FE1(ITR) a Map-Reply containing the requested mapping information
5. FE1(ITR) installs the mapping information in its local map-cache

Verify map-request messages sent to the fabric control-plane ?



debug lisp control map-request

*Jan 18 16:12:57.741: LISP: Send map request for EID prefix IID **4099 10.2.1.89**/32

debug lisp forwarding data-signal-map-request

*Jan 18 16:12:57.610: LISPdata-signal: sending signal for **10.2.1.99** ->**10.2.1.89** on in IPv4:**Campus**

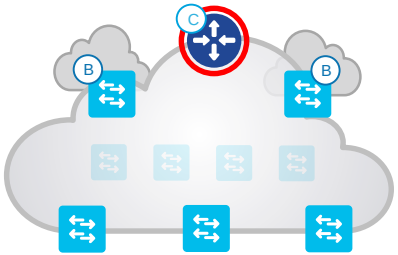
Host1 EID

debug lisp forwarding eligibility-process-switching

*Jan 18 16:12:57.741: LISP-0: EID-AF IPv4, **Sending map-request** from 10.2.1.89 to 10.2.1.89 for EID **10.2.1.89** /32, ITR-RLOCs 1, nonce 0x0579975B-0x0823B8E4 (encap src **10.2.120.1**, dst **10.2.100.1**).

Host2 EID

Verification on Control Plane ?




```
CP#show lisp site instance-id 4099
Site Name      Last       Up     Who Last              Inst     EID Prefix
               Register          Registered            ID
site_sjc       never      no     --                    4099     10.2.1.0/24
               3d23h      yes#   10.2.120.1            4099     10.2.1.99/32
               3d23h      yes#   10.2.120.3            4099     10.2.1.89/32
```

debug lisp control map-server-map-request

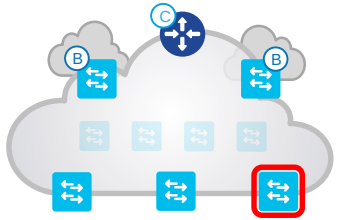
*Jan 18 16:15:27.529: LISP: **Received map request** for IID **4099** **10.2.1.89**/32, source_eid IID **4099** **10.2.1.99**, ITR-RLOCs: **10.2.120.1**, records 1, nonce 0x0579975B-0x0823B8E4

*Jan 18 16:15:27.529: LISP-0: MS EID IID **4099** prefix **10.2.1.89**/32 site site_sjc, **Forwarding map request** to ETR RLOC **10.2.120.3**.

FE1 RLOC

FE3 RLOC

Verify map-request forwarded to the fabric edge?



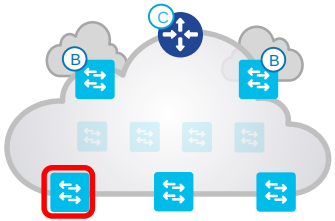
debug lisp control map-request

Jan 18 16:12:58.531: LISP: **Received map request** for IID **4099 10.2.1.89**/32, source_eid IID **4099 10.2.1.99**, ITR-RLOCs: **10.2.120.1**, records 1, nonce 0x0579975B-0x0823B8E4

Jan 18 16:12:58.531: LISP-0: **Sending map-reply** from **10.2.120.3** to **10.2.120.1**.

FE3 RLOC **FE1 RLOC**

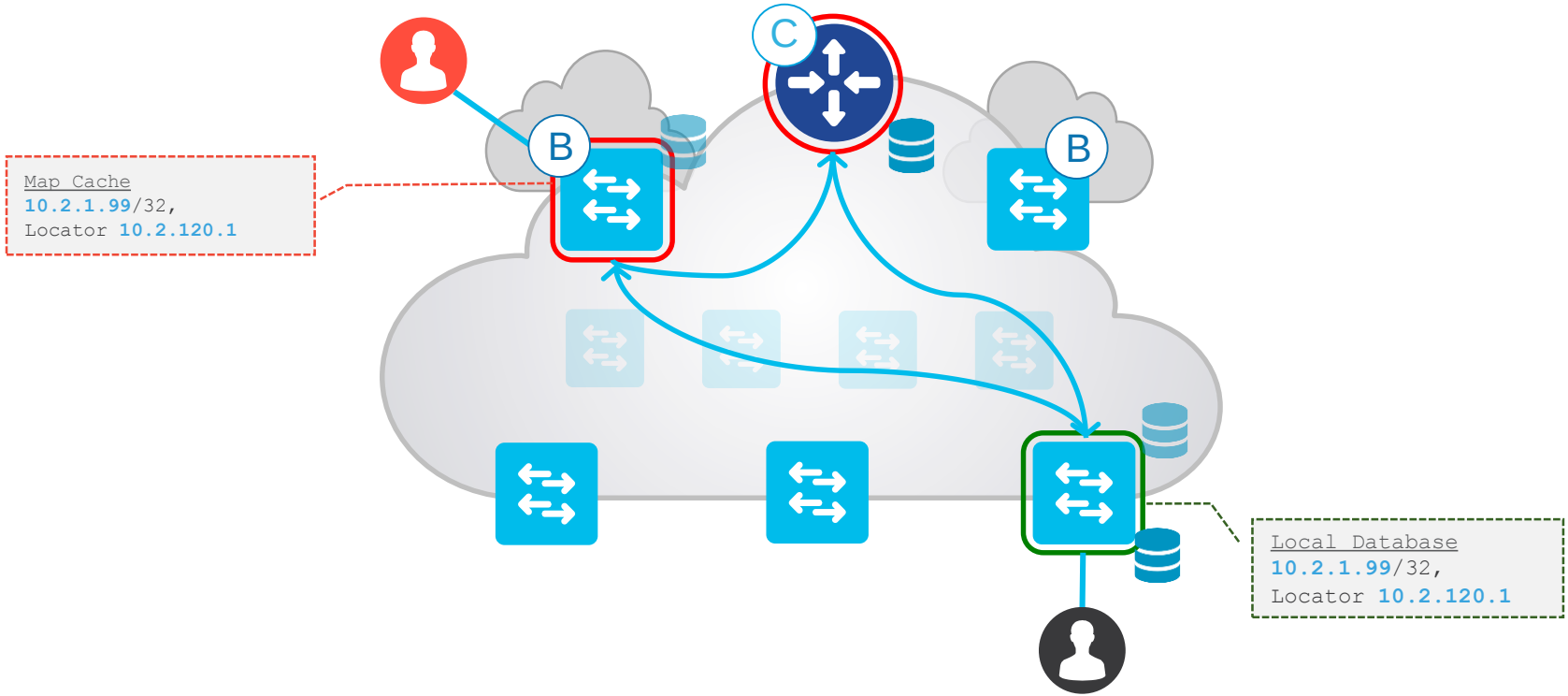
Verify map-reply recevied from FE 3?



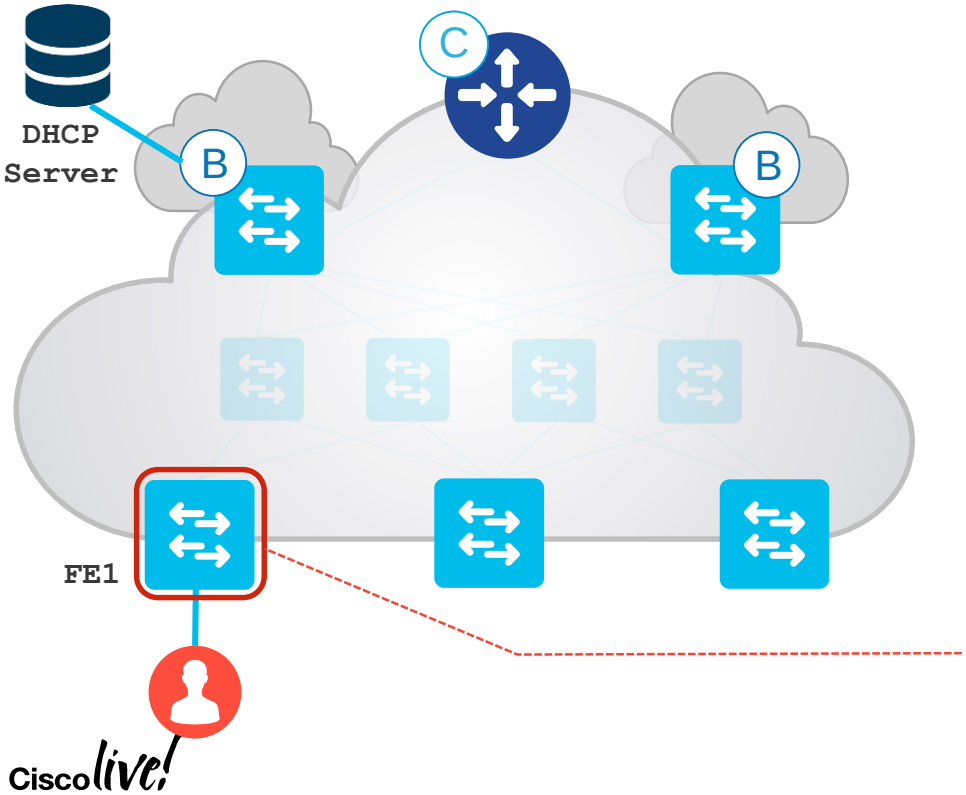
debug lisp control map-request

*Jan 18 16:12:57.748: LISP: **Processing Map-Reply** mapping record for IID **4099 10.2.1.89**/32, ttl 1440, action none, authoritative, 1 locator **10.2.120.3** pri/wei=10/10 LpR

It is the Same Sequence if Border is Requesting

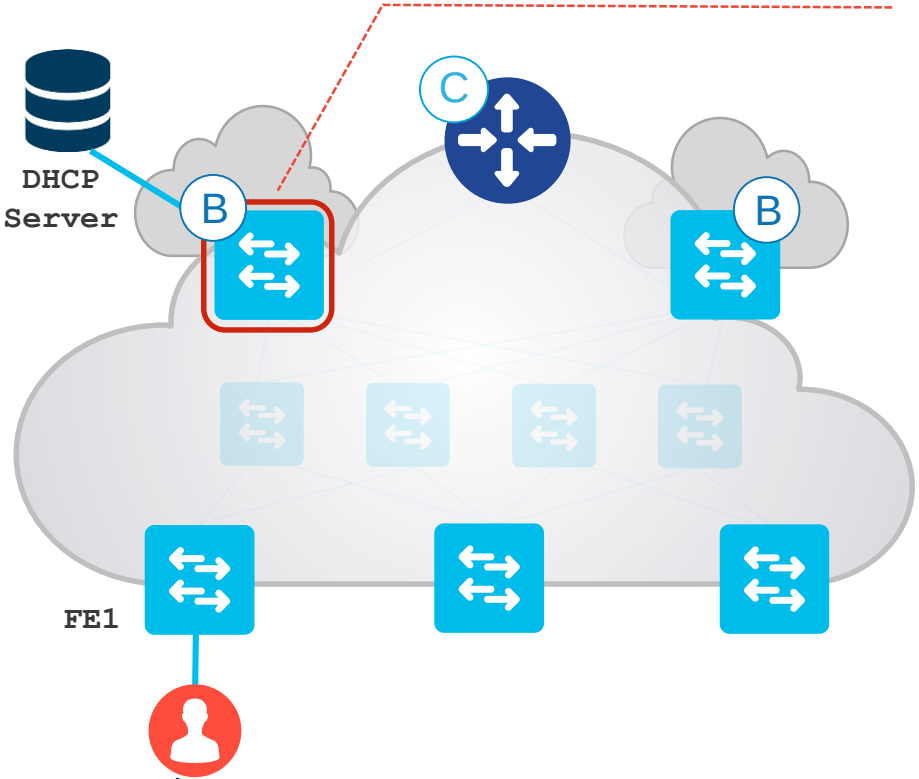


Case: 3 – DHCP Packet Flow



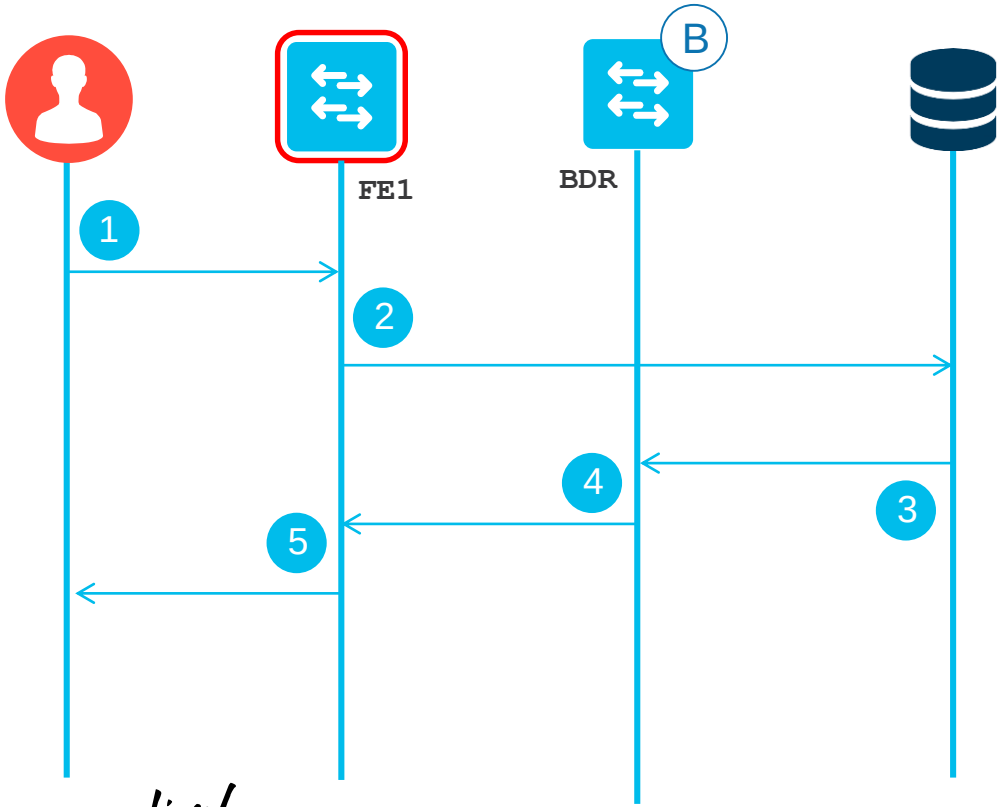

```
ip dhcp relay information option
ip dhcp snooping vlan 1021
ip dhcp snooping
interface vlan 1021
 ip vrf forwarding Campus
 ip address 10.2.1.254 255.255.255.0
 ip helper-address 60.1.1.2
 lisp mobility dhcp_1


router lisp
 instance-id 4099
  remote-rloc-probe on-route-change
  dynamic-eid 10_2_1_0-Campus
   database-mapping 172.16.109.0/24 locator-
set rloc_37ca8231-67a8-4b04-9a36-44bd5d2c0906
   exit-dynamic-eid
  !
  service ipv4
   eid-table vrf Campus9
   map-cache 0.0.0.0/0 map-request
   exit-service-ipv4
  !
  exit-instance-id!
exit-router-lisp
```

Case: 3 – DHCP Packet Flow




```
interface Loopback1021
vrf forwarding Campus
ip address 10.2.1.254 255.255.255.255


router lisp
 instance-id 4099
  service ipv4
   eid-table vrf VN1
   route-export site-registrations
   distance site-registrations 240
   map-cache site-registration
   exit-service-ipv4
  !
  exit-instance-id
!
exit-router-lisp
router bgp 100
 address-family ipv4 vrf Campus
  network 10.2.1.254 mask 255.255.255.255
  aggregate-address 10.2.1.0 255.255.255.0 summary-only
   exit-address-family
```

DHCP Packet Flow in Campus Fabric



1. The DHCP client generates a DHCP request and broadcasts it on the network
2. FE adds remote ID in option 82.
   The packet is sent with src IP of the SVI.
3. DHCP Server replies with offer.
4. Border uses the remote ID in option 82 to forward the packet.
5. FE installs the DHCP binding and forwards the reply to client

DHCP Binding on FE

```
FE#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:13:a9:1f:b2:b0    10.1.2.99       691197      dhcp-snooping  1021  TenGigabitEthernet1/0/23
```

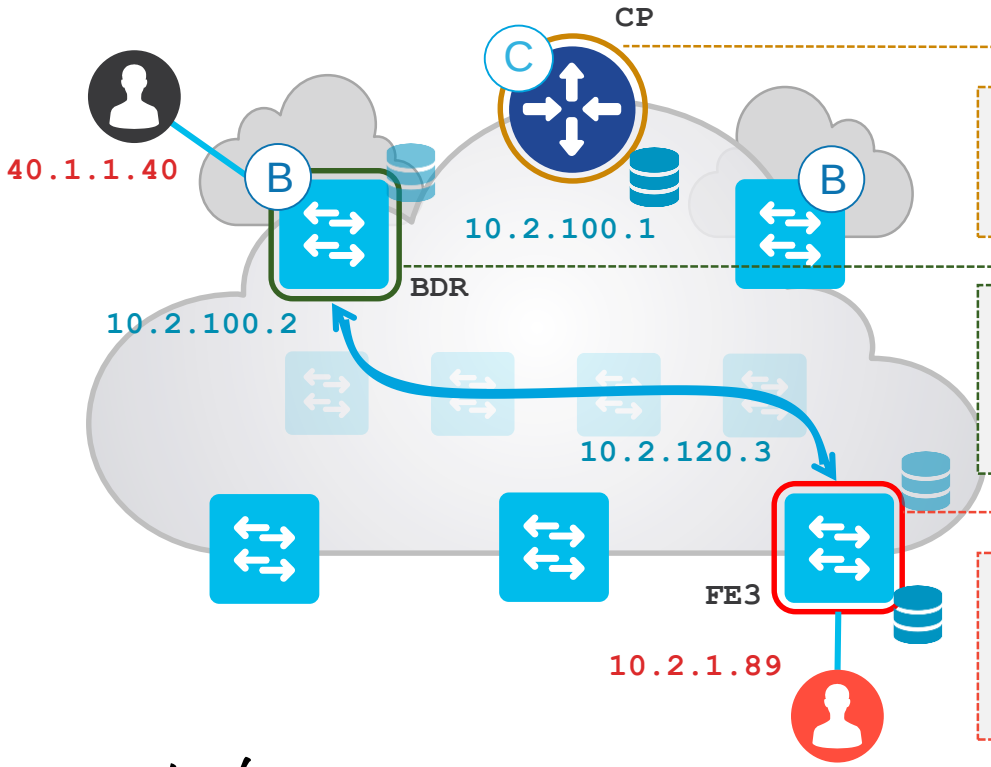
```
FE#debug ip dhcp snooping ?
  H.H.H       DHCP packet MAC address
  agent       DHCP Snooping agent
  event       DHCP Snooping event
  packet      DHCP Snooping packet
  redundancy  DHCP Snooping redundancy
```

Debug ip dhcp snooping
- Enables showing detail with regards to DHCP snooping and the insertion of option 82 remote circuit

Debug ip dhcp server packet
- Enables debug with regards to the relay function , insertion giaddress and relay functionality to the Server

Debug dhcp detail
- Adds additional detail with regards to LISP in DHCP debugs

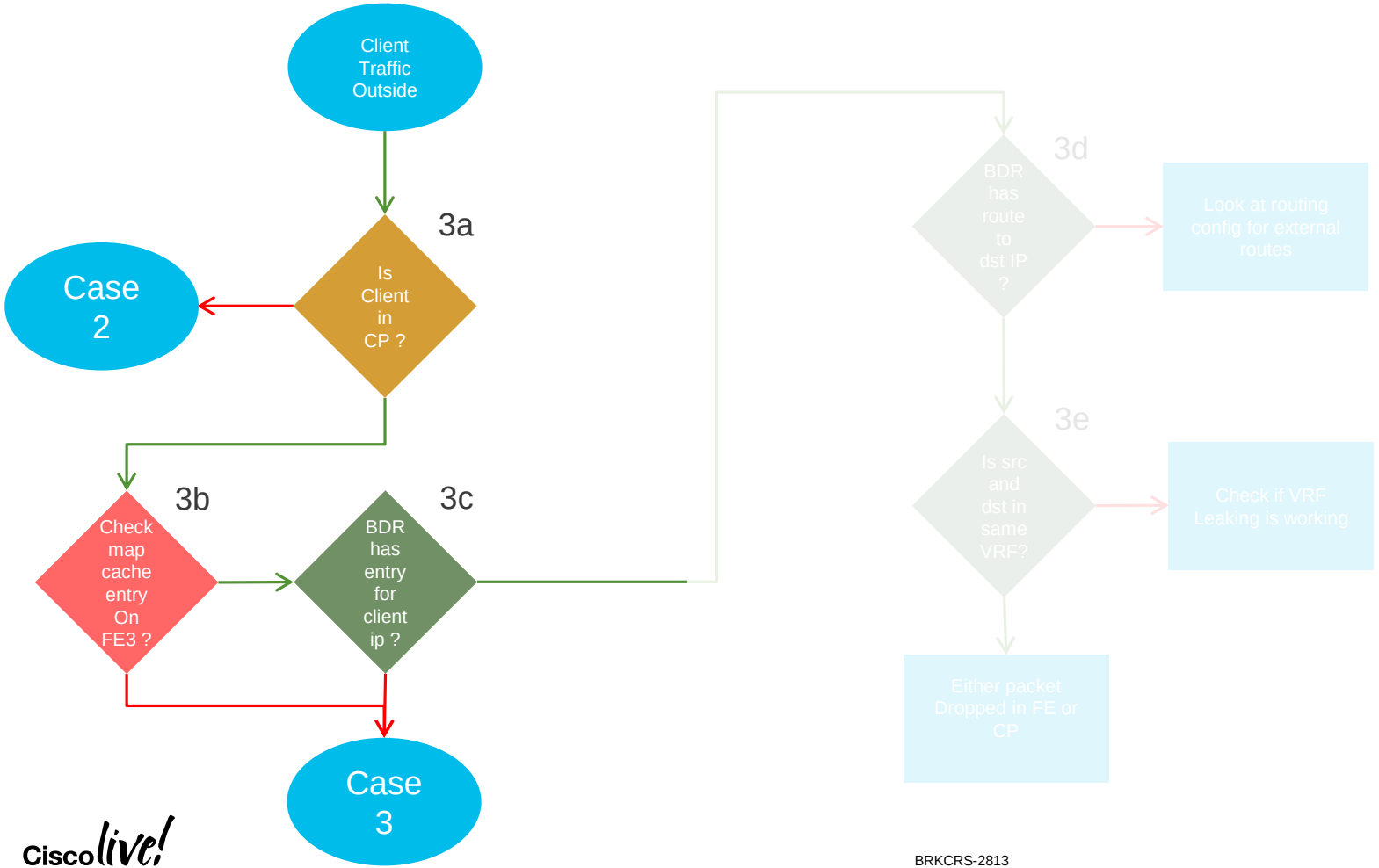
Case: 4 - External Connectivity



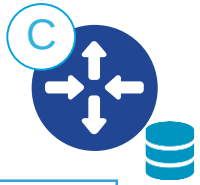

```
router lisp
 site site_sjc
   ...
   eid-prefix instance-id 4099 10.2.1.0/24 accept-more-specifics
exit
```

```
router lisp
 encapsulation vxlan
!
 eid-table Campus instance-id 4099
   map-cache 10.2.1.0/24 map-request exit
```

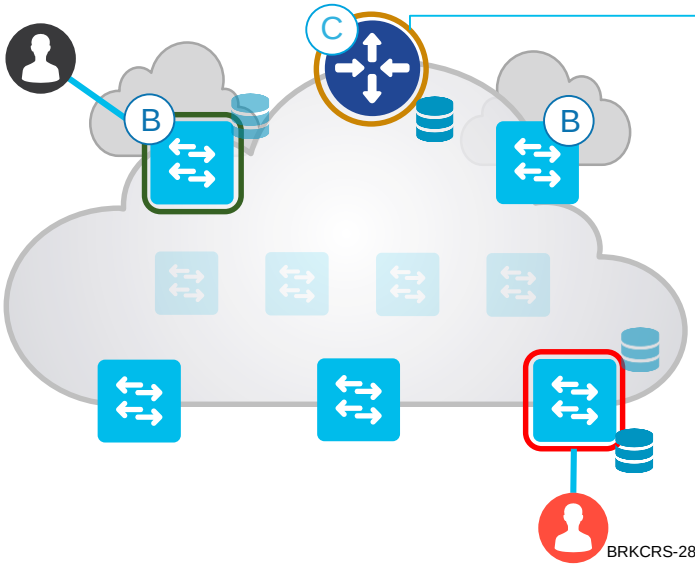
```
router lisp
...
 eid-table Campus instance-id 4099
 dynamic-eid 10_2_1_0-Campus
   database-mapping 10.2.1.0/24 locator-set campus_fabric
exit
```


Client Traffic Outside
3a
Is Client in CP ?
Case 2
3b
Check map cache entry On FE3 ?
3c
BDR has entry for client ip ?
Case 3
3d
BDR has route to dst IP ?
Look at routing config for external routes
3e
Is src and dst in same VRF?
Check if VRF Leaking is working
Either packet Dropped in FE or CP

Verification on Control Plane

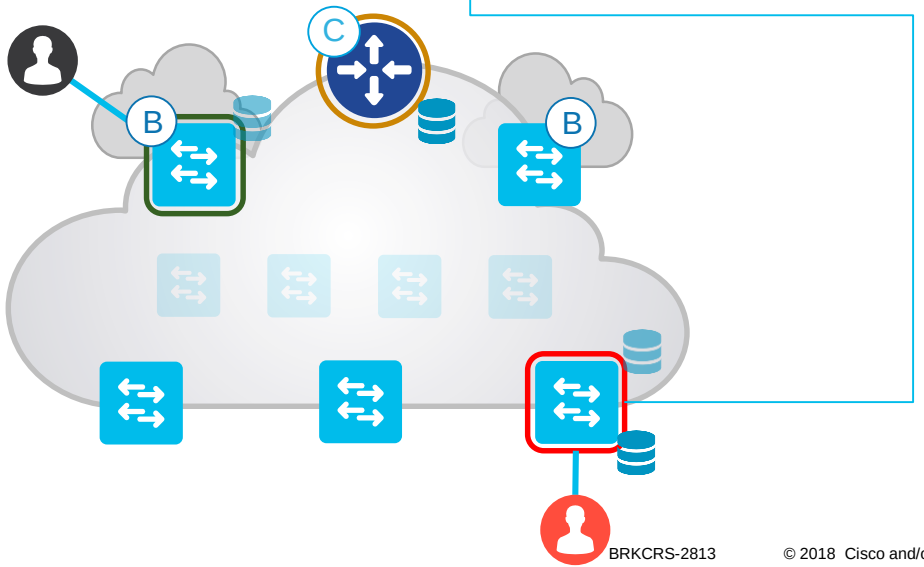


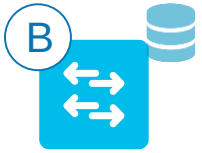

```
CP#show lisp site instance-id 4099
Site Name       Last        Up      Who Last                Inst      EID Prefix
                Register            Registered              ID
site_sjc        never       no      --                      4099      10.2.1.0/24
                3d23h       yes#    10.2.120.3              4099      10.2.1.89/32
```



Verification at the FE

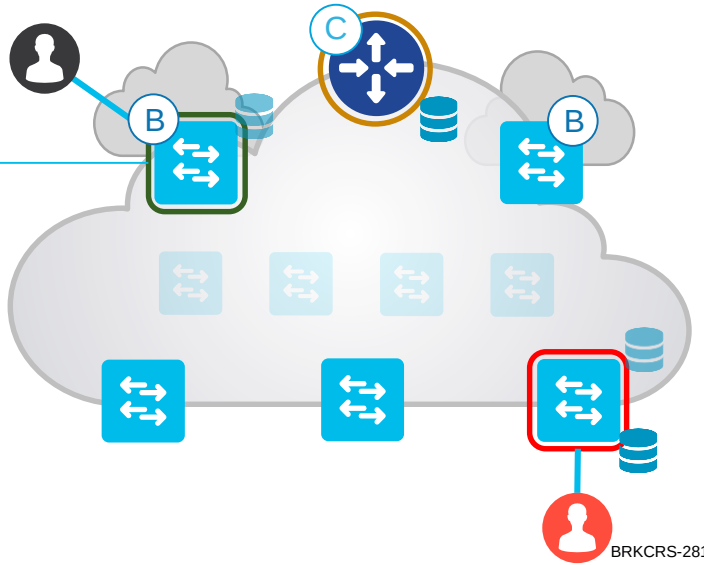
```
FE3#show ip lisp map-cache instance-id 4099
LISP IPv4 Mapping Cache for EID-table vrf Campus (IID 4099), 5 entries

32.0.0.0/4, uptime: 00:01:30, expires: 00:00:21, via map-reply, forward-native
  Encapsulating to proxy ETR
```

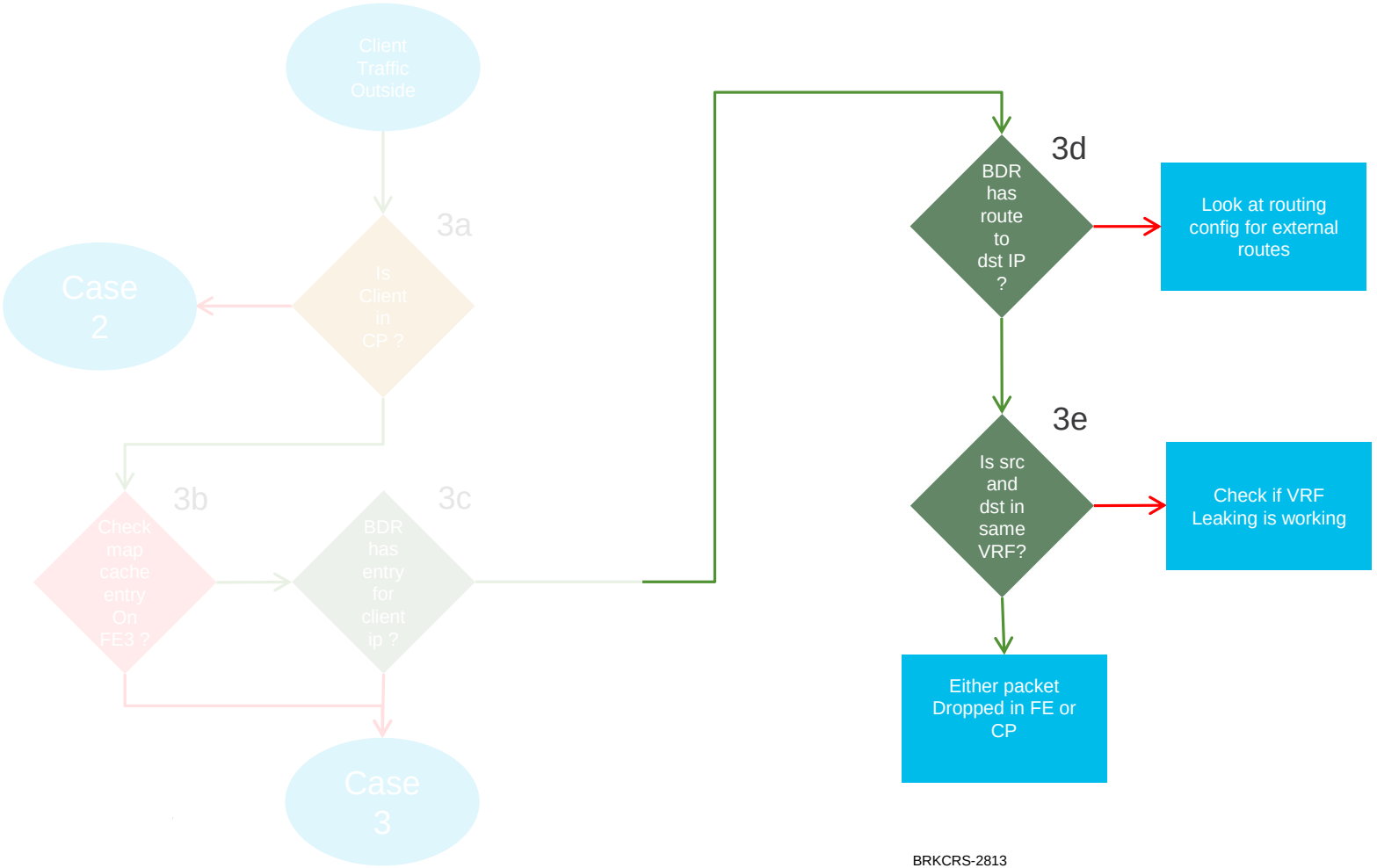




Verification at the Border

```
BDR#show ip lisp map-cache instance-id 4099
LISP IPv4 Mapping Cache for EID-table vrf Campus (IID 4099), 5 entries

10.2.1.89/32, uptime: 00:05:16, expires: 23:57:59, via map-reply, complete
  Locator      Uptime    State      Pri/Wgt
  10.2.120.3   00:04:23  up           10/10
```



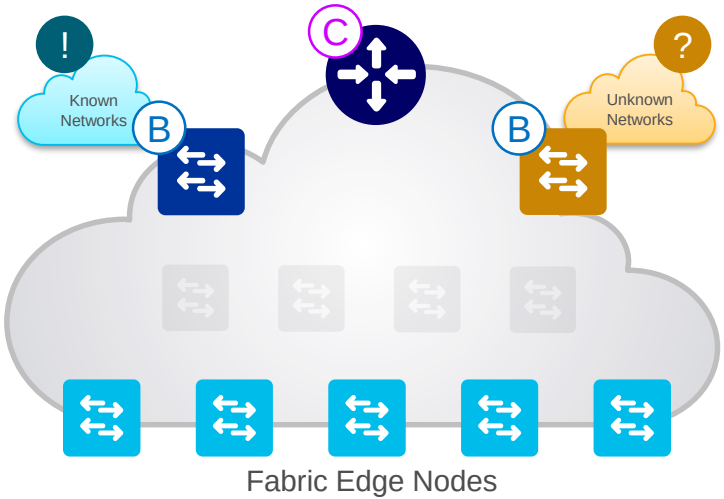

Client Traffic Outside
3a
Is Client in CP ?
Case 2
3b
Check map cache entry On FE3 ?
3c
BDR has entry for client ip ?
Case 3
3d
BDR has route to dst IP ?
Look at routing config for external routes
3e
Is src and dst in same VRF?
Check if VRF Leaking is working
Either packet Dropped in FE or CP

SD-Access Borders

Border Node is an entry & exit point for all data traffic coming in or going out of the Fabric

There are 2 Types of Border Nodes:

- **Fabric Border (Internal)**
  - Used for “Known” Routes in your company
- **Default Border (External)**
  - Used for “Unknown” Routes outside your company

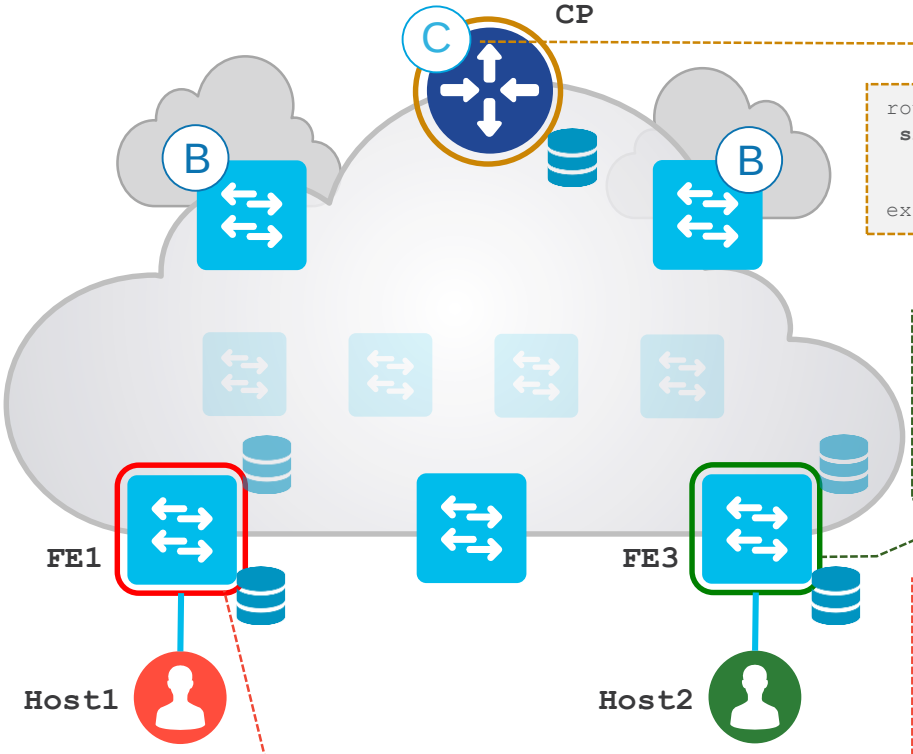


In case of Internal Border

Verify the routes that are being imported

```
Internal-BDR#show ip lisp route-import map-cache instance 10
LISP IPv4 imported routes for EID-table vrf PACAF (IID 10)
Config: 1, Entries: 7 (limit 1000)
Prefix                    Uptime    Source               RLOC-set   Cache/DB   State
10.1.18.0/24              21:59:17  bgp 65002                       installed
10.1.100.1/32             21:59:17  bgp 65002                       installed
100.1.1.0/24              21:59:17  bgp 65002                       installed
101.1.1.0/24              21:59:17  bgp 65002                       installed
192.168.111.0/24          21:59:17  bgp 65002                       installed
192.168.206.0/24          21:59:17  bgp 65002                       installed
```

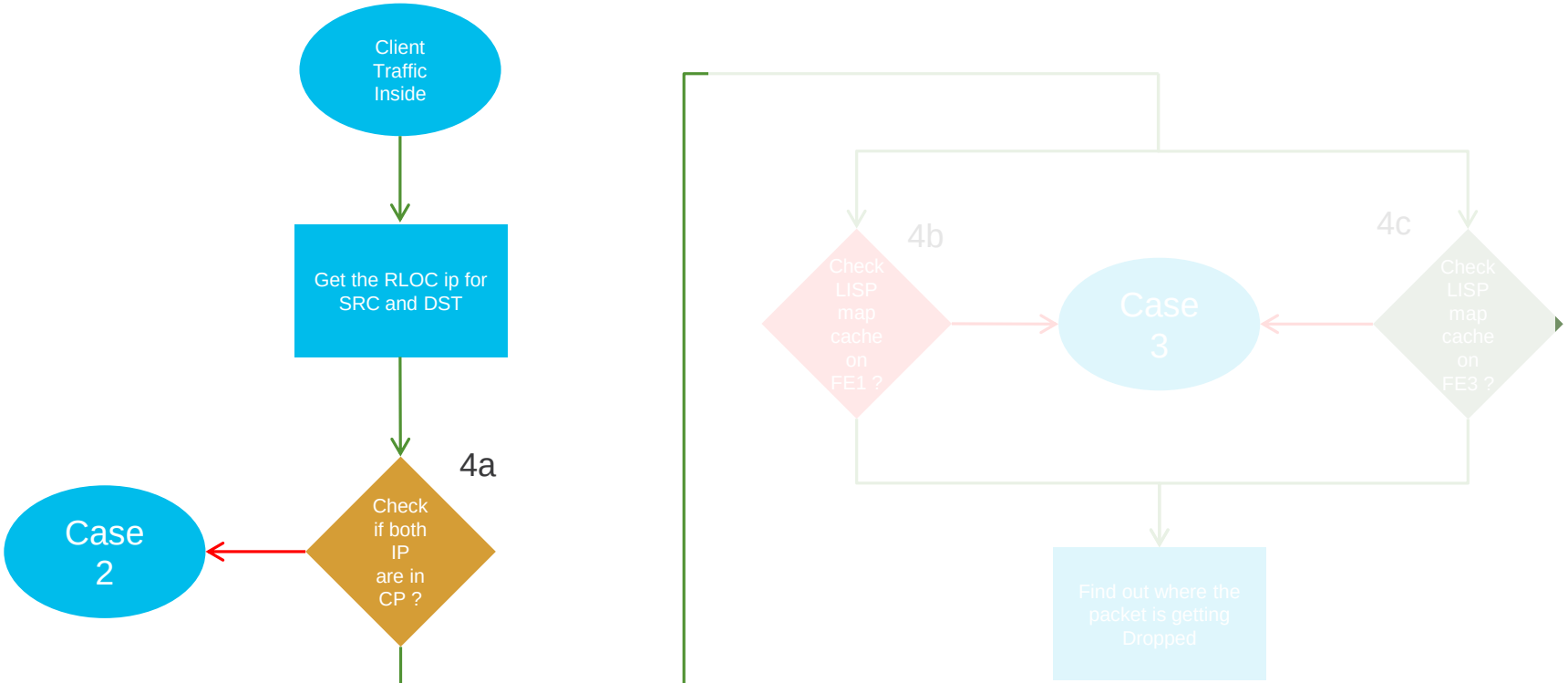
Case: 5 - East West Traffic



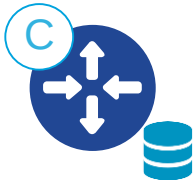

```
router lisp
 site site_sjc
   ...
   eid-prefix instance-id 4099 10.2.1.0/24 accept-more-specifics
exit
```

```
router lisp
...
 eid-table Campus instance-id 4099
 dynamic-eid 10_2_1_0-Campus
   database-mapping 10.2.1.0/24 locator-set campus_fabric
exit
```

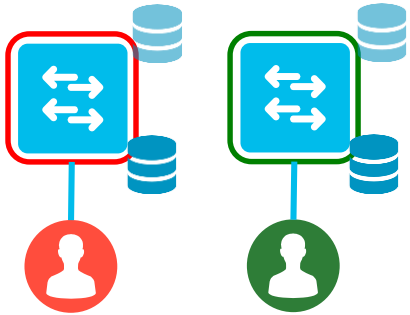
```
router lisp
...
 eid-table Campus instance-id 4099
 dynamic-eid 10_2_1_0-Campus
   database-mapping 10.2.1.0/24 locator-set campus_fabric
exit
```


Client Traffic Inside
Get the RLOC ip for SRC and DST
4a
Check if both IP are in CP ?
Case 2
4b
Check LISP map cache on FE1 ?
Case 3
4c
Check LISP map cache on FE3 ?
Find out where the packet is getting Dropped

Verification on Control Plane ?

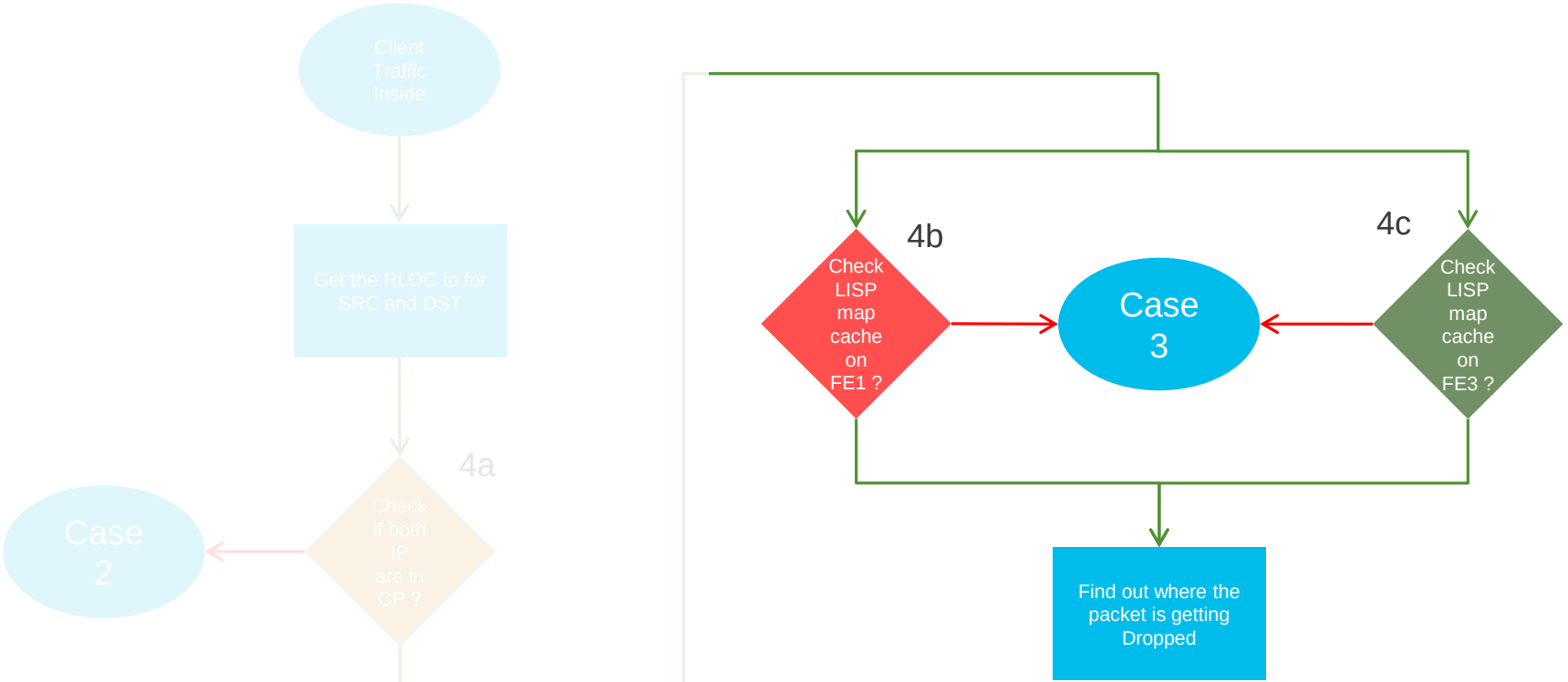



```
CP#show lisp site instance-id 4099
Site Name      Last       Up     Who Last                Inst     EID Prefix
               Register          Registered              ID
site_sjc       never      no     --                      4099     10.2.1.0/24
               2d05h      yes#   10.2.120.1              4099     10.2.1.99/32
               2d02h      yes#   10.2.120.2              4099     10.2.1.89/32
               4d02h      yes#   10.2.120.2              4099     10.2.1.88/32
```

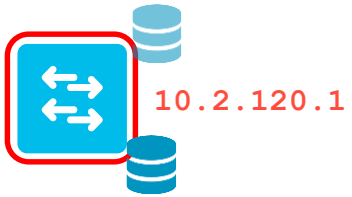


If any of Host IP are missing.

Run Host Registration flow (Case 2).


Client Traffic Inside
Get the RLOC ip for SRC and DST
4a
Check if both IP are in CP ?
Case 2
4b
Check LISP map cache on FE1 ?
Case 3
4c
Check LISP map cache on FE3 ?
Find out where the packet is getting Dropped

Verification at the FEs



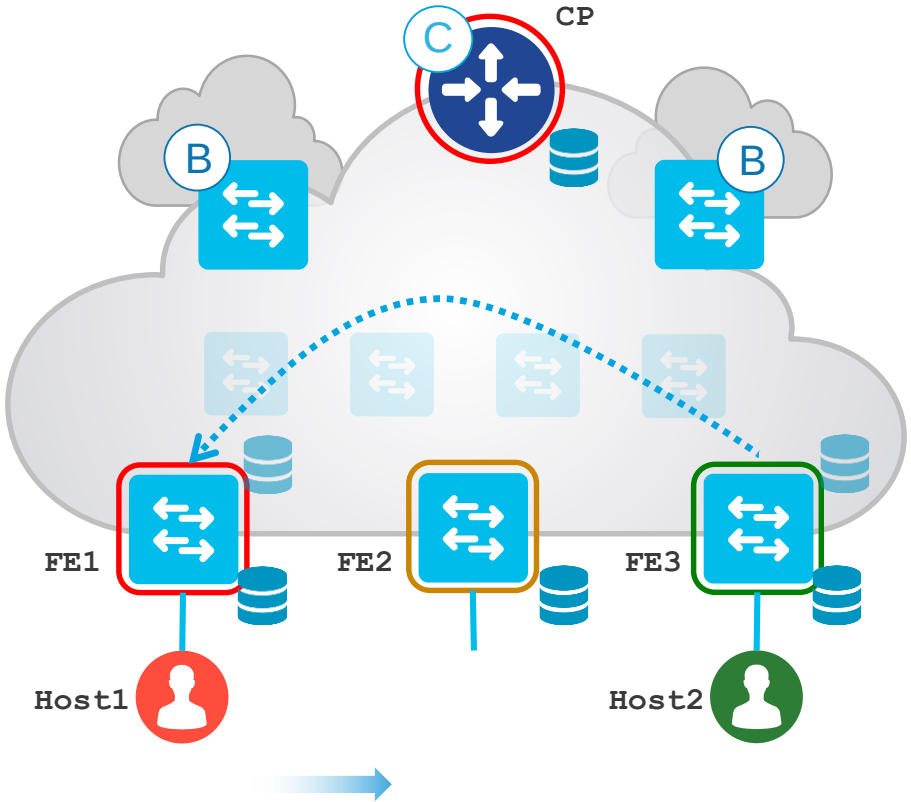
4b

```
FE1#show ip lisp instance-id 4099 database
10.2.1.99/32, locator-set rloc_021a8c01-5c45-4529-addd-b0d626971a5f
  Locator     Pri/Wgt  Source     State
  10.2.120.1   10/10   cfg-intf   site-self, reachable

FE1#show ip lisp map-cache instance-id 4099
10.2.1.89/32, uptime: 00:00:06, expires: 23:59:53, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt
 10.2.120.3 00:00:06  up          10/10
```

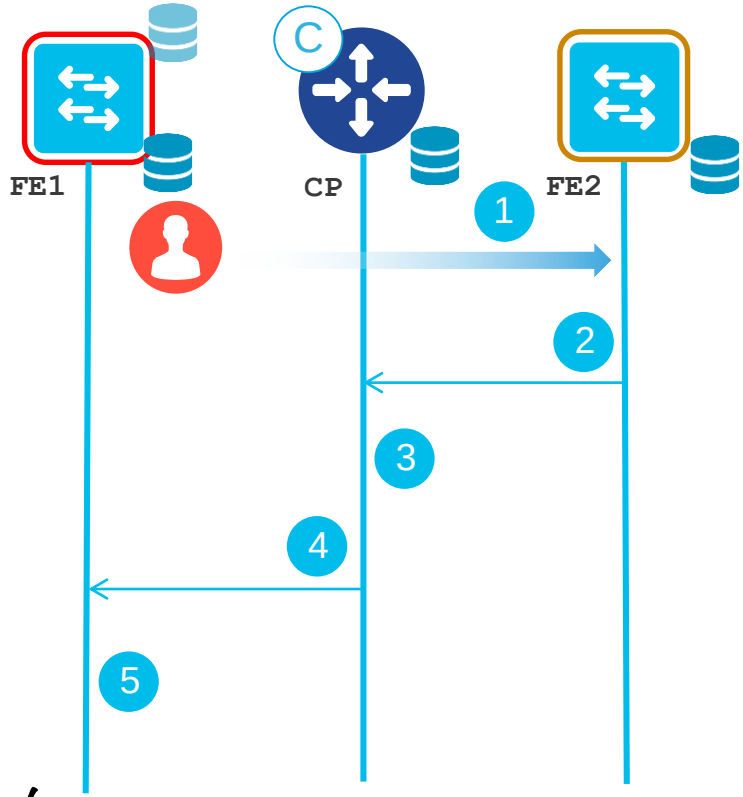
4c

```
FE3#show ip lisp instance-id 4099 database
10.2.1.89/32, locator-set rloc_021a8c01-5c45-4529-addd-b0d626971a5f
  Locator     Pri/Wgt  Source     State
  10.2.120.3   10/10   cfg-intf   site-self, reachable

FE3#show ip lisp map-cache instance-id 4099
10.2.1.99/32, uptime: 00:00:06, expires: 23:59:53, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt
 10.2.120.1 00:00:06  up          10/10
```

Case: 6 - Host Mobility



Map Request Message flow



1. Host1 moves from FE1 to FE2
2. FE2 saves the host info in local database. Send the registration message to control plane
3. The Map-Server adds to the database the entry for the specific EID, associated to the RLOCs
4. The Map-Server sends a Map-Notify message to the last FE1 that registered the 10.2.1.99/32 prefix
5. FE1 receives the Map-Notify message from the CP and adds route associated to the 10.2.1.99 EID to away table

Verification at the FEs

```
FE1#show ip lisp away instance-id 4099
LISP Away Table for router lisp 0 (Campus) IID 4099
Entries: 1
Prefix                                    Producer
10.2.1.99/32                              local EID
```

Host EID

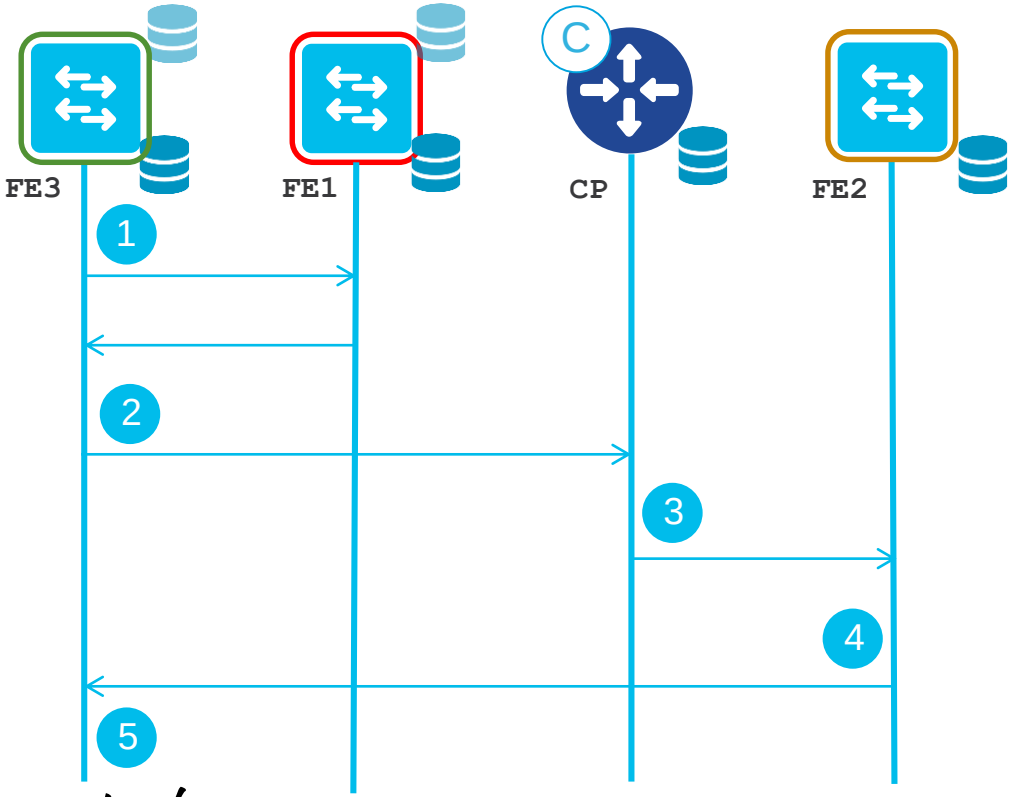
```
FE2#show ip lisp instance-id 4099 database
10.2.1.99/32, locator-set rloc_021a8c01-5c45-4529-addd-b0d626971a5f
  Locator      Pri/Wgt  Source     State
  10.2.120.2    10/10   cfg-intf   site-self, reachable
```

FE2

```
FE3#show ip lisp map-cache instance-id 4099
10.2.1.99/32, uptime: 00:00:06, expires: 23:59:53, via map-reply, complete
  Locator      Uptime    State      Pri/Wgt
 10.2.120.1 00:00:06  up          10/10
```

FE1

Map Request Message flow



1. The LISP process on FE1 receiving the first data packet creates a control plane message SMR and sends it to the remote $FE3_{(ITR)}$ that generated the packet
2. Send a new Map-Request for the desired destination (10.17.1.99) to the Map-Server
3. Map-Request is forwarded by the Map-Server to the FE2 that registered last the /32 EID address
4. FE2 replies with updated mapping information to the remote FE3
5. FE3 updates the information in its map-cache, adding the specific /32 EID address associated to the xTRs deployed in the East site (10.2.120.1 and 10.2.120.2)

Q & A

Complete Your Online Session Evaluation

- Give us your feedback and receive a **Cisco Live 2018 Cap** by completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Mobile App.

Don’t forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Global.

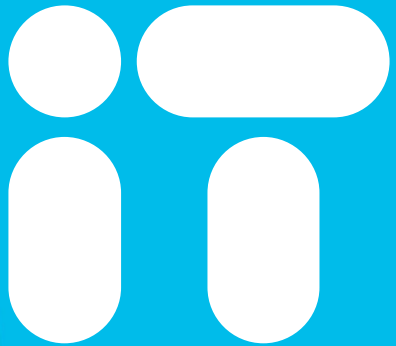
Ciscolive!

Continue Your Education

- Demos on the Cisco stand
- Walk-in Self-Paced Labs
- Meet the Expert 1:1 meetings
- Related sessions

Thank you

You're



Cisco live!

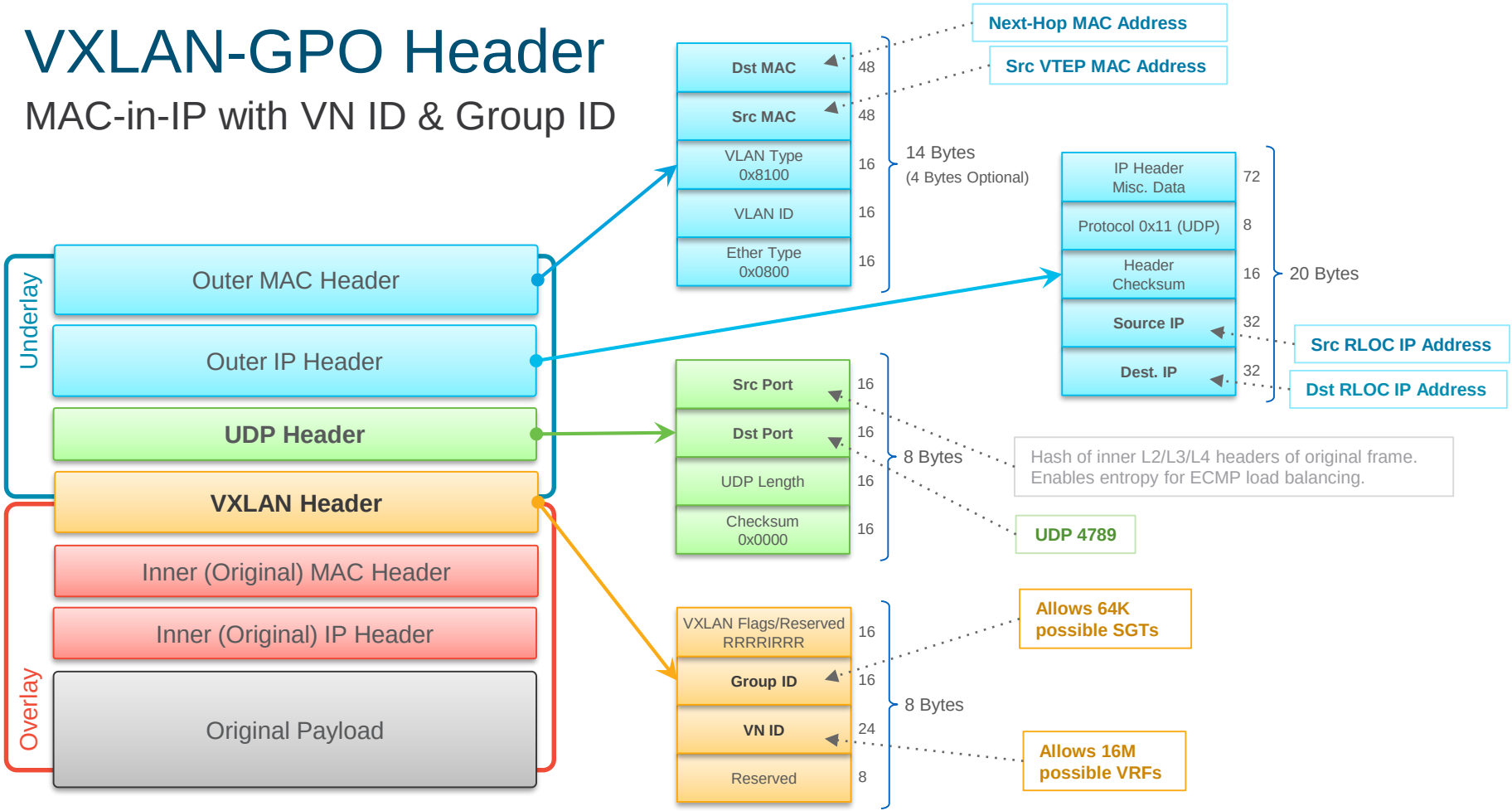
Locator/ID Separation Protocol (LISP) Internet Groper – "lig"

```
FE1#lig 18.18.18.18 instance-id 4099
Mapping information for EID 18.18.18.18 from 172.16.1.2 with RTT 7 msecs
18.18.18.18/32, uptime: 00:00:00, expires: 23:59:59, via map-reply, complete
  Locator     Uptime    State      Pri/Wgt
  10.2.120.4  00:00:00  up          10/10

FE1#lig self instance-id 4099
Mapping information for EID 10.2.1.40 from 10.2.120.2 with RTT 5 msecs
10.2.1.40/32, uptime: 00:00:00, expires: 23:59:59, via map-reply, self, complete
  Locator     Uptime    State      Pri/Wgt
  10.2.120.2  00:00:00  up, self    10/10

FE1#lig 17.17.17.17 instance-id 4099
Mapping information for EID 17.17.17.17 from 10.2.201.2 with RTT 2 msecs
16.0.0.0/4, uptime: 00:00:00, expires: 00:14:59, via map-reply, forward-native
  Encapsulating to proxy ETR
```

SD-Access Data Plane Troubleshooting

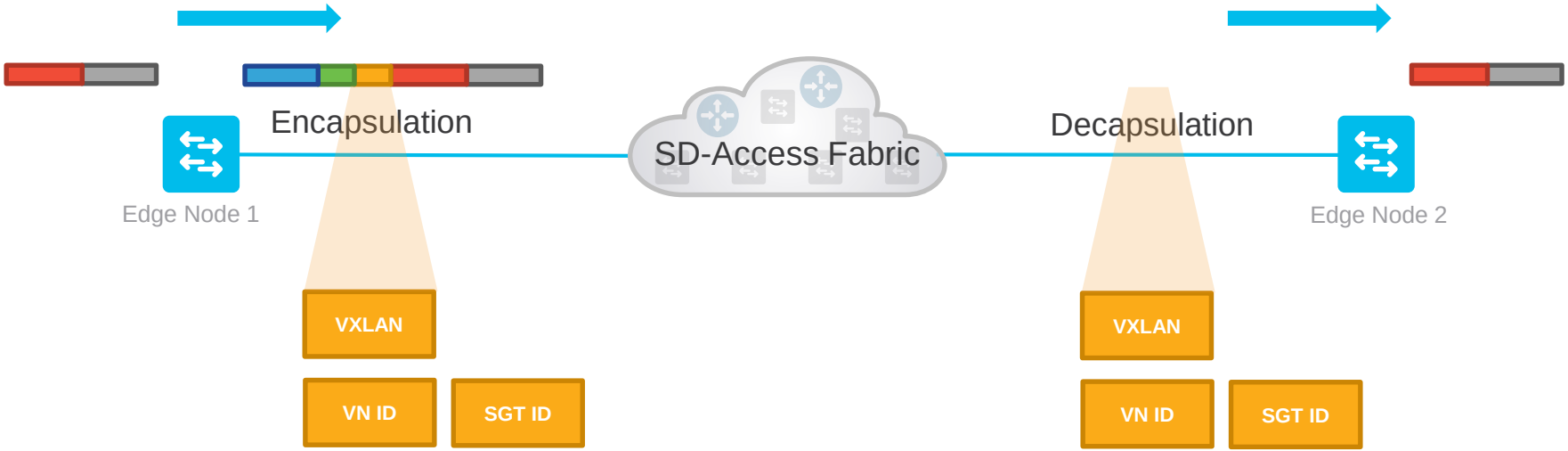
VXLAN-GPO Header

MAC-in-IP with VN ID & Group ID



Packet Flow in Fabric

VXLAN Encapsulation



Classification
Static or Dynamic VN and SGT assignments

Propagation
Carry VN and Group context across the network

Enforcement
Group Based Policies ACLs, Firewall Rules

What to Look for in Packet Capture?

Frame 1: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits)
Ethernet II, Src: CiscoInc_c5:db:47 (88:90:8d:c5:db:47), Dst: CiscoInc_5b:58:fb (0c:f5:a4:5b:58:fb)
Internet Protocol Version 4, Src: 10.2.120.1, Dst: 10.2.120.3
User Datagram Protocol, Src Port: 65354 (65354), **Dst Port: 4789 (4789)**
Source Port: 65354
Destination Port: 4789
Length: 158
Checksum: 0x0000 (none)
[Stream index: 0]

OUTER HEADER

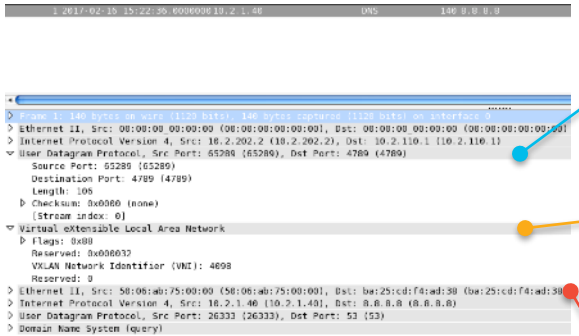
Virtual eXtensible Local Area Network
Flags: 0x0800, VXLAN Network ID (VNI)
Group Policy ID: 50
VXLAN Network Identifier (VNI): **4099**
Reserved: 0

OVERLAY HEADER

Ethernet II, Src: CiscoInc_c5:00:00 (88:90:8d:c5:00:00), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
Destination: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
Source: CiscoInc_c5:00:00 (88:90:8d:c5:00:00)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.2.1.89, Dst: 10.2.1.99
Internet Control Message Protocol

INNER HEADER

What to Look for in Packet Capture?



Frame 1: 192 bytes on wire (1536 bits), 192 bytes captured (1536 bits)
Ethernet II, Src: CiscoInc_c5:db:47 (88:90:8d:c5:db:47), Dst: CiscoInc_5b:58:fb (0c:f5:a4:5b:58:fb)
Internet Protocol Version 4, Src: 10.2.120.1, Dst: 10.2.120.3
User Datagram Protocol, Src Port: 65354 (65354), **Dst Port: 4789 (4789)**
Source Port: 65354
Destination Port: 4789
Length: 158
Checksum: 0x0000 (none)
[Stream index: 0]

OUTER HEADER

Virtual eXtensible Local Area Network
Flags: 0x0800, VXLAN Network ID (VNI)
Group Policy ID: 50
VXLAN Network Identifier (VNI): **4099**
Reserved: 0

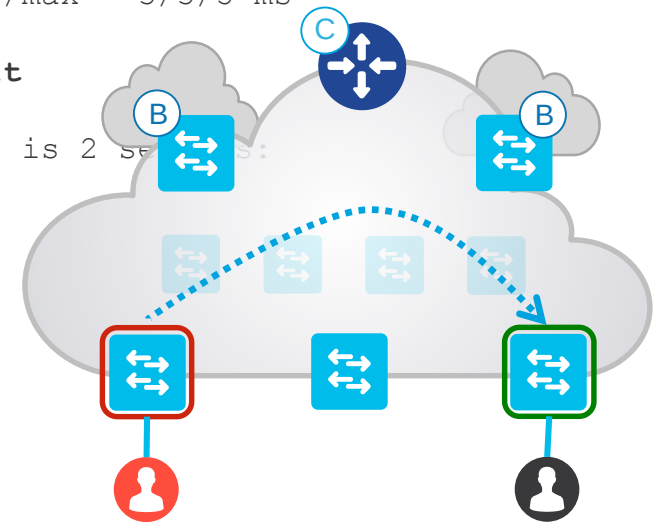
OVERLAY HEADER

Ethernet II, Src: CiscoInc_c5:00:00 (88:90:8d:c5:00:00), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
Destination: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
Source: CiscoInc_c5:00:00 (88:90:8d:c5:00:00)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.2.1.89, Dst: 10.2.1.99
Internet Control Message Protocol

INNER HEADER

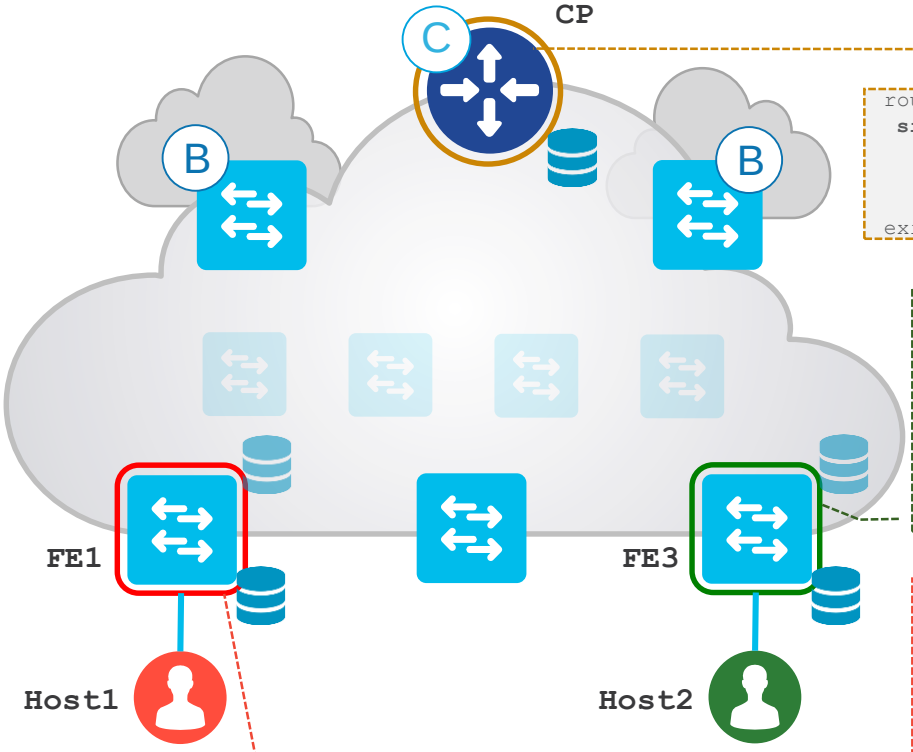
Underlay MTU

```
FE1#ping 10.2.120.3 source 10.2.120.1 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.120.3, timeout is 2 seconds:
Packet sent with a source address of 10.2.120.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/5 ms
FE1#
FE1#ping 10.2.120.3 source 10.2.120.1 size 1501 df-bit
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.120.3, timeout is 2 seconds:
Packet sent with a source address of 10.2.120.1
.....
Success rate is 0 percent (0/5)
FE1#
```



Configure jumbo MTU on the devices participating in underlay connectivity

Overlay EID Loopback




```
router lisp
 site site_sjc
   ...
   eid-prefix instance-id 4099 20.20.20.20/32
   eid-prefix instance-id 4099 21.21.21.21/32
exit
```

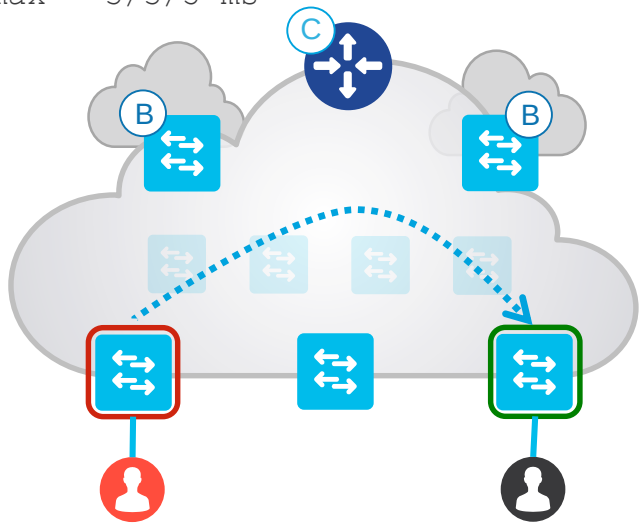
```
router lisp
...
 eid-table Campus instance-id 4099
 database-mapping 20.20.20.20/32 locator-set campus_fabric

interface Loopback20
 ip vrf forwarding Campus
 ip address 20.20.20.20 255.255.255.255
```

```
router lisp
...
 eid-table Campus instance-id 4099
 database-mapping 21.21.21.21/32 locator-set campus_fabric

interface Loopback21
 ip vrf forwarding Campus
 ip address 21.21.21.21 255.255.255.255
```

Fabric Edge Loopback Ping Test

```
FE1#ping vrf Campus 20.20.20.20 source 21.21.21.21 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.20.20.20, timeout is 2 seconds:
Packet sent with a source address of 21.21.21.21
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 3/3/5 ms
FE1#
```

Initial packets get dropped until Host Resolution is complete



Embedded Packet Capture

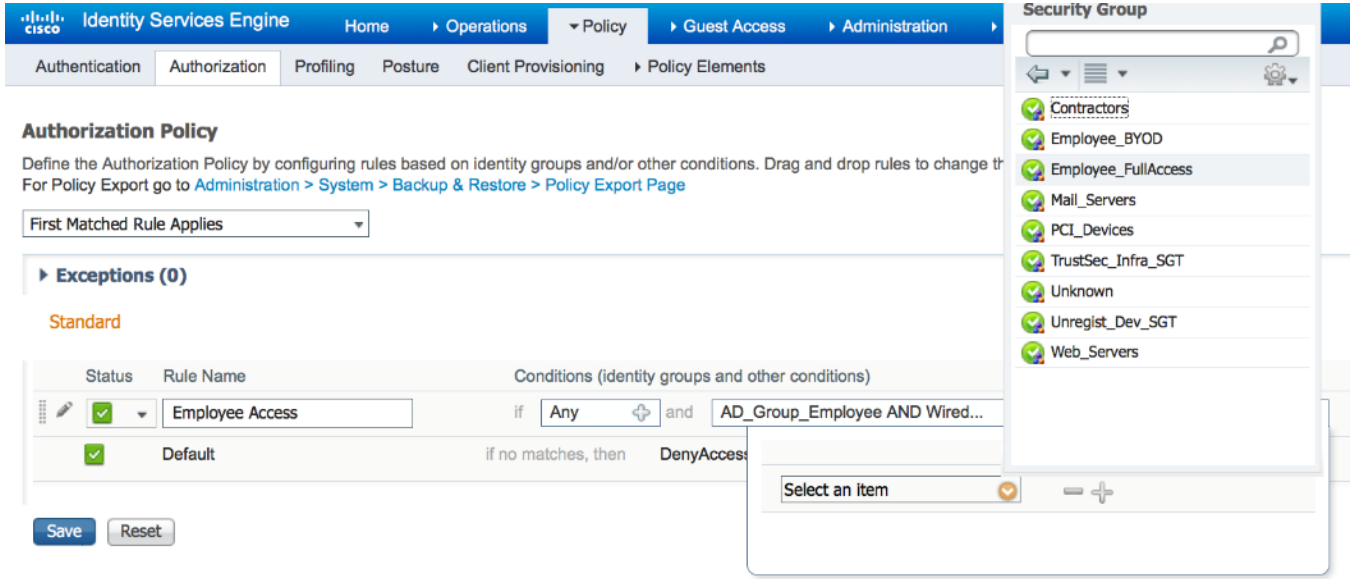
```
FE#monitor capture lispcap interface te 1/0/1 both match any
limit file location flash:lispcap
```

```
FE#show monitor capture file flash:lispcap
Starting the packet display ........ Press Ctrl + Shift + 6 to exit

  1 0.000000000   172.16.1.2 -> 10.2.110.2   UDP 124 Source port: 65357  Destination port: vxlan
  2 0.001160000   10.2.203.2 -> 10.2.120.4   UDP 124 Source port: 65351  Destination port: vxlan
  3 0.114937000   172.16.1.1 -> 224.0.0.10   EIGRP 74 Hello
  4 1.013745000   172.16.1.2 -> 10.2.110.2   UDP 124 Source port: 65357  Destination port: vxlan
  5 1.017345000   10.2.203.2 -> 10.2.120.4   UDP 124 Source port: 65351  Destination port: vxlan
  6 2.012271000   172.16.1.2 -> 10.2.110.2   UDP 124 Source port: 65357  Destination port: vxlan
  7 2.014704000   10.2.203.2 -> 10.2.120.4   UDP 124 Source port: 65351  Destination port: vxlan
  8 2.199264000   172.16.1.2 -> 10.2.110.1   UDP 116 Source port: 65474  Destination port: vxlan
  9 2.202622000   10.2.200.2 -> 172.16.1.2   ICMP 70 Destination unreachable (Port unreachable)
```

SD-Access Policy Plane Troubleshooting

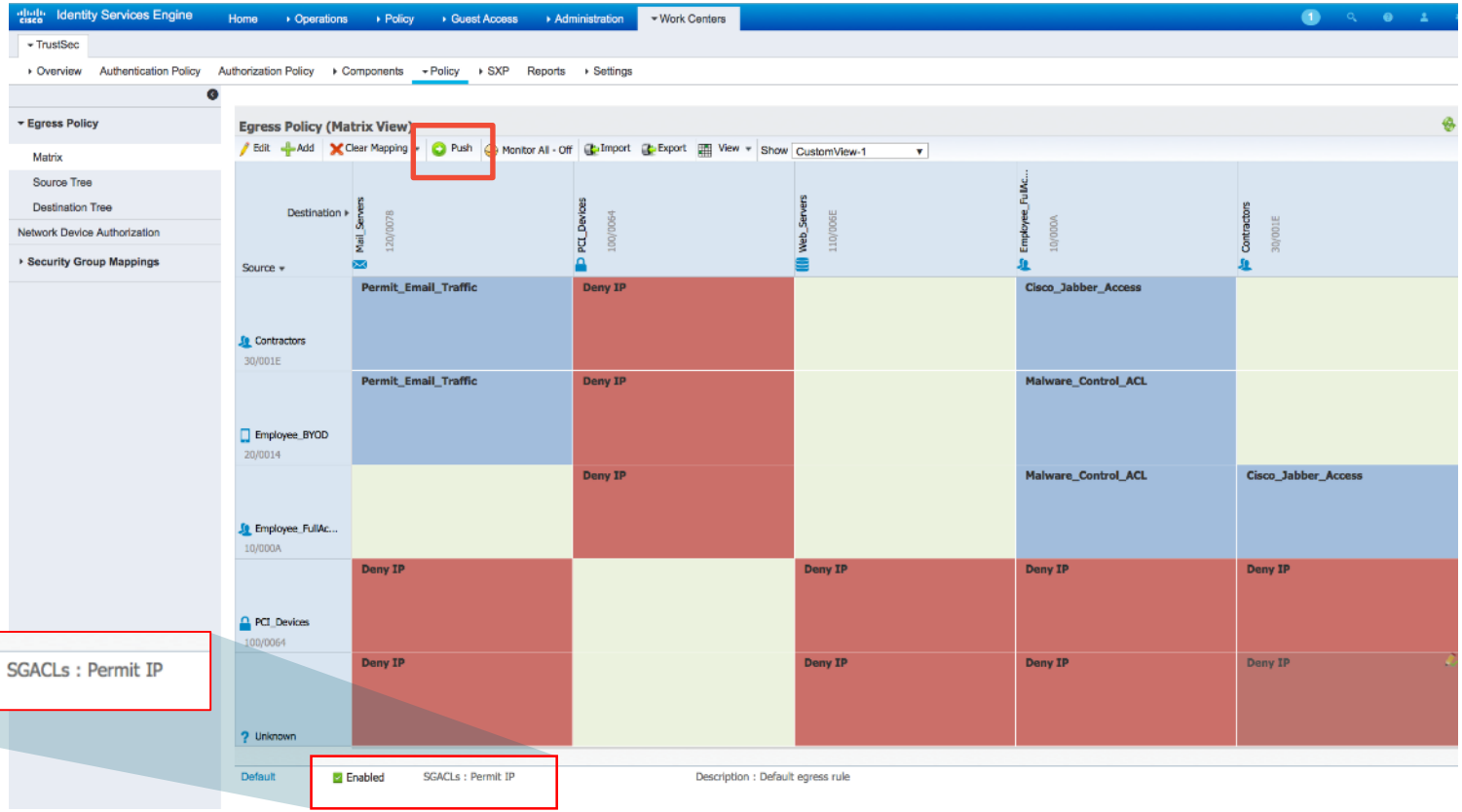
Check Authorisation Policies for Users and Devices

802.1X / MAB / Web Authentication policy to assign SGTs to the Users and Devices

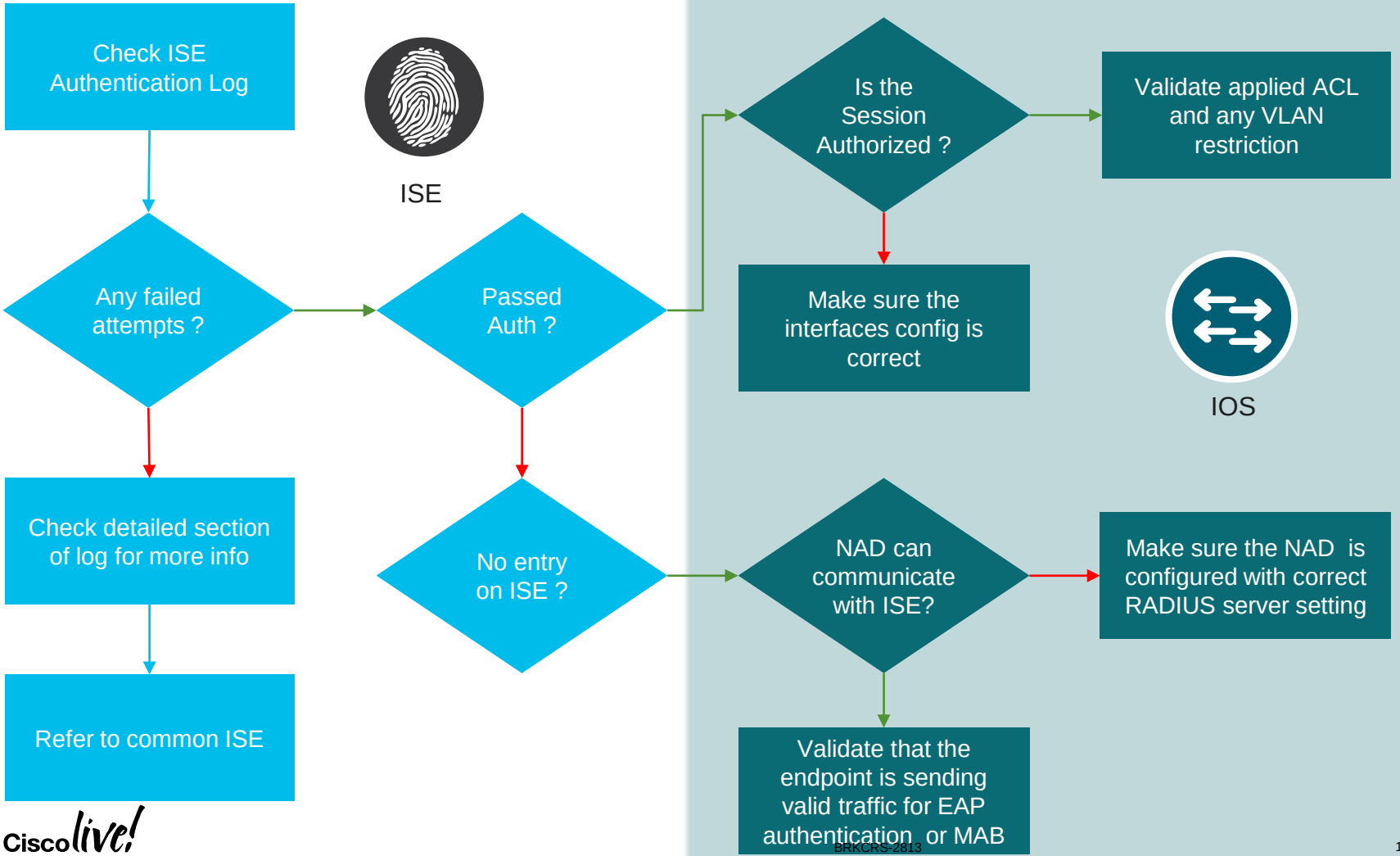


Policy Matrix

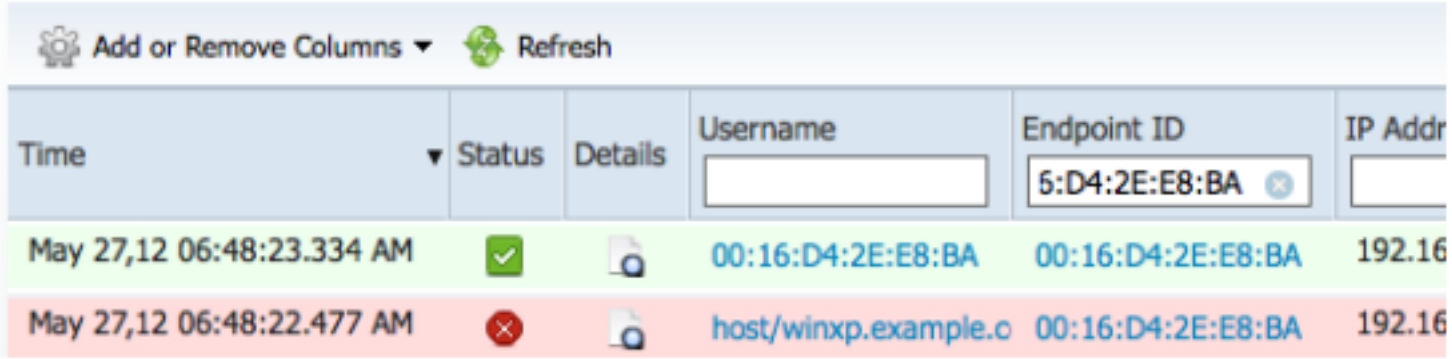
Egress
Policy Matrix



Default Rule, Can be Permit or Deny


Check ISE Authentication Log
ISE
Any failed attempts ?
Passed Auth ?
Is the Session Authorized ?
Validate applied ACL and any VLAN restriction
Make sure the interfaces config is correct
IOS
Check detailed section of log for more info
No entry on ISE ?
NAD can communicate with ISE?
Make sure the NAD is configured with correct RADIUS server setting
Refer to common ISE
Validate that the endpoint is sending valid traffic for EAP authentication or MAB

Authentication Log



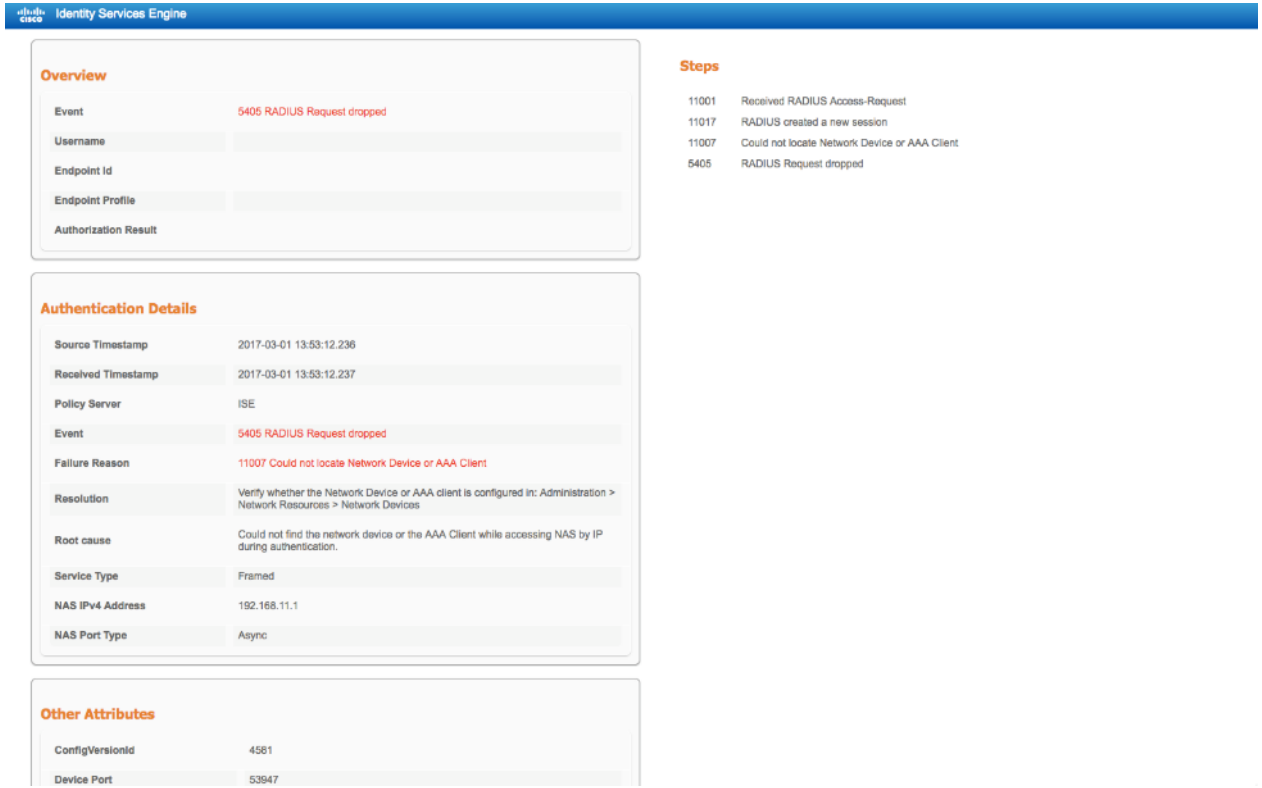
Successful events will have

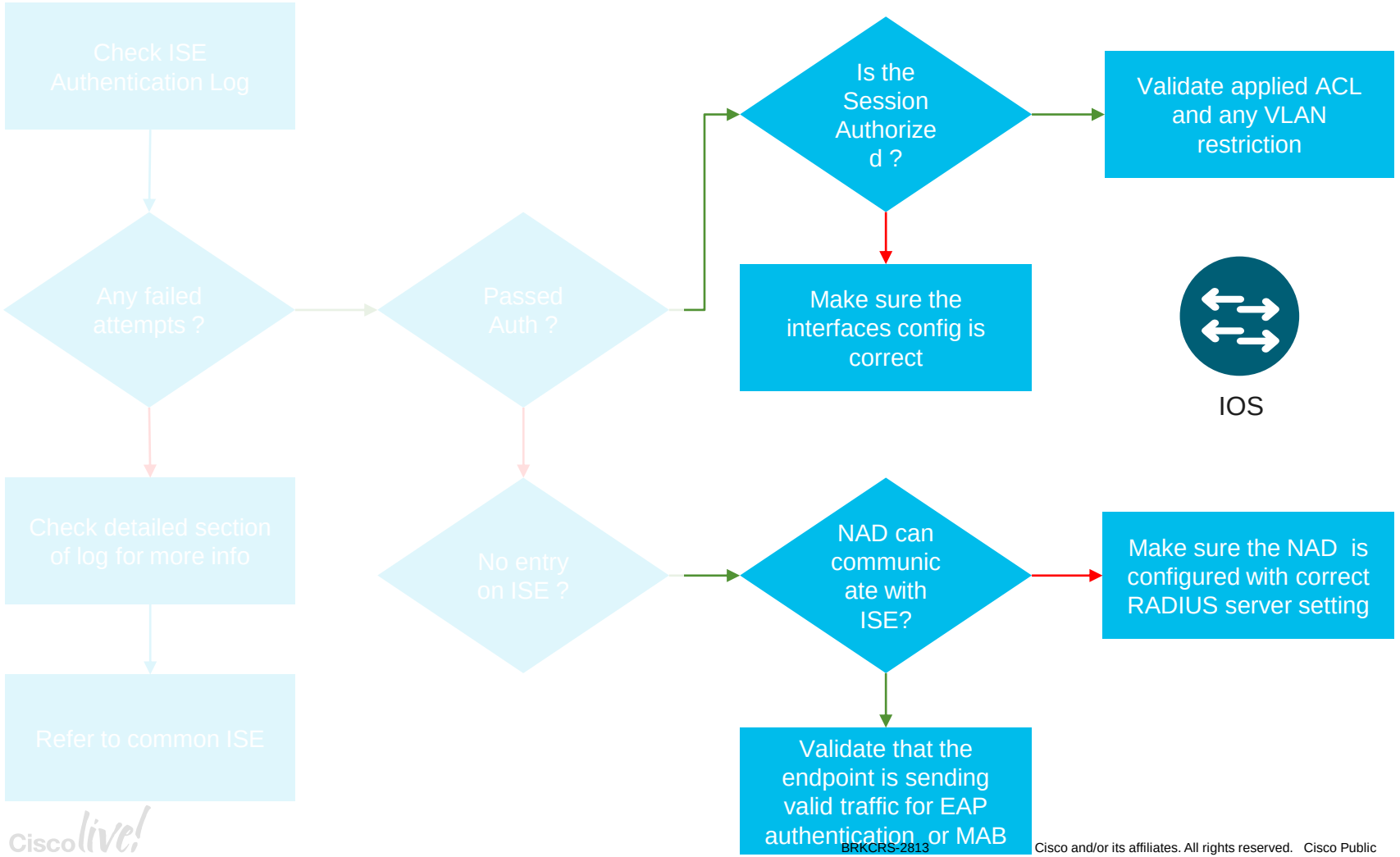
Failed event will have

Click on

Details button for more information.

Detail Report

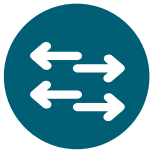




Verify Config on the Switch

Switch Global Config

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default group radius
radius-server host 10.100.10.150 auth-port 1812 acct-port 1813
key cisco
```

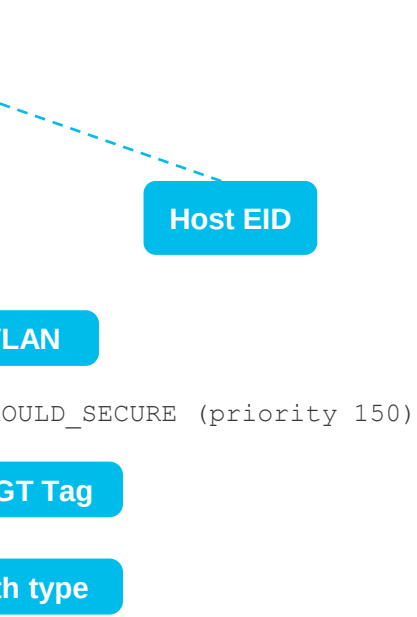


Switch Interface Config

```
interface GigabitEthernet1/4
         switchport mode access
         switchport voice vlan 4000
         authentication control-direction in
         authentication event server dead action authorize vlan
3999
         authentication host-mode multi-auth
         authentication order dot1x mab
         authentication priority dot1x mab
         mab
         dot1x pae authenticator
         authentication violation restrict
```

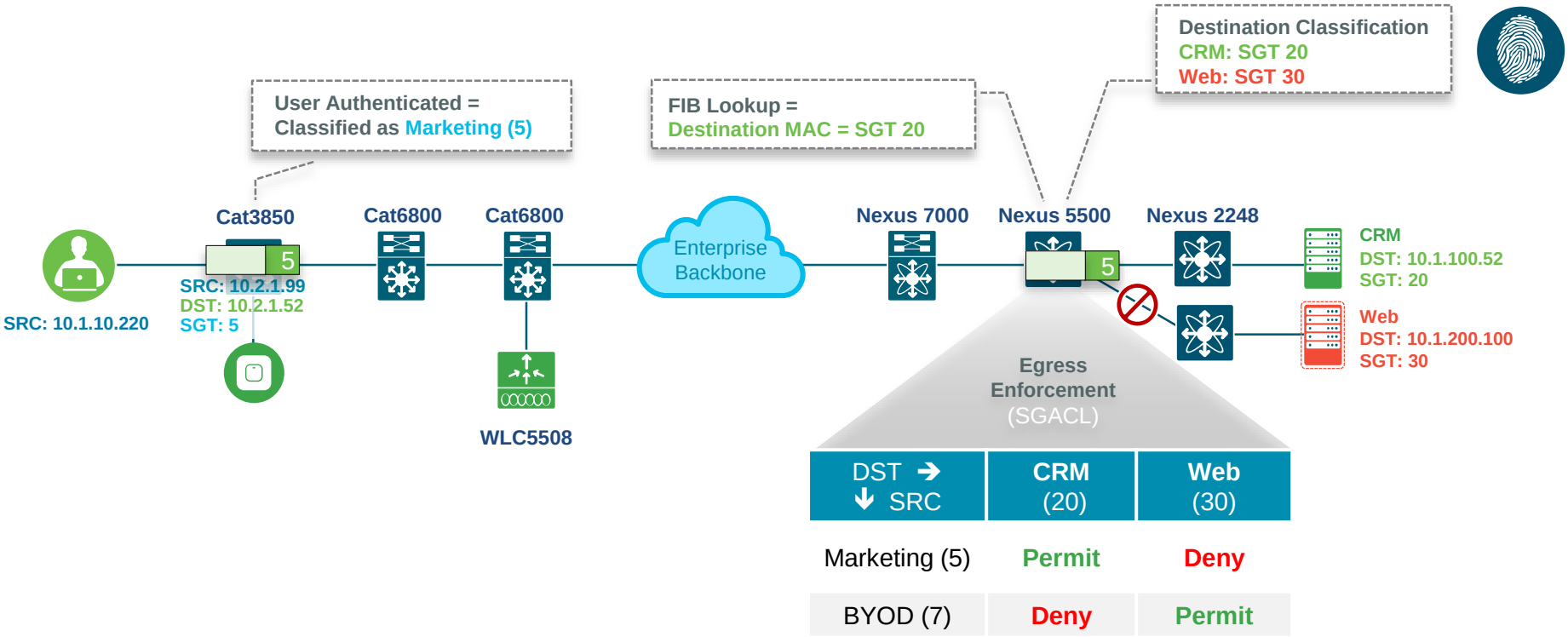
Verification on FEs

```
FE1#show authentication sessions mac 0050.5694.d054 details
            Interface:  GigabitEthernet1/0/2
               IIF-ID:  0x100CBC000000088
          MAC Address:  0050.5694.d054
         IPv6 Address:  Unknown
         IPv4 Address:  10.2.1.99
            User-Name:  joe
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
       Session Uptime:  28127s
    Common Session ID:  0A04010300000FB00003640C
      Acct Session ID:  0x00000FA5
               Handle:  0x98000003
       Current Policy:  POLICY_Gi1/0/2
Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Server Policies:
            Vlan Group: Vlan: 1021
            SGT Value:  5
Method status list:
       Method           State
       dot1x            Authc Success
```

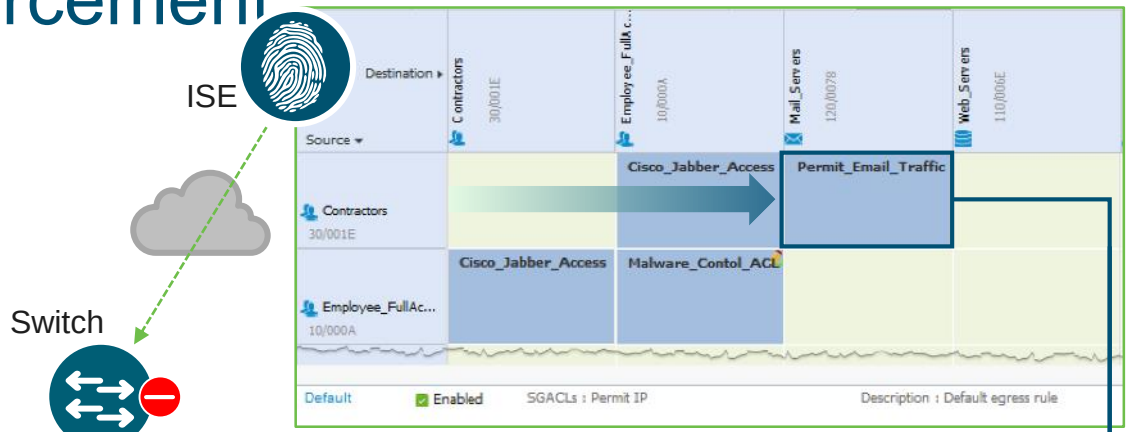


Cisco Trust Security

Ingress Classification with Egress Enforcement



‘cts role-based enforcement’




```
Switch#show cts rbacl Permit_Email_Traffic
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
  name    = Permit_Email_Traffic-40
  IP protocol version = IPV4
  refcnt = 1
  flag    = 0x40000000
  stale   = FALSE
  RBACL ACEs:
    permit tcp dst eq 110
    permit tcp dst eq 143
    permit tcp dst eq 25
    permit tcp dst eq 465
    permit tcp dst eq 585
    permit tcp dst eq 993
    permit tcp dst eq 995
    deny all log
```

IOS switch as enforcer

```
Switch#show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
...
IPv4 Role-based permissions from group 10:Employee_FullAccess to group
10:Employee_FullAccess:
        Malware_Contol_ACL-10
IPv4 Role-based permissions from group 10:Employee_FullAccess to group 30:Contractors:
        Cisco_Jabber_Access-10
IPv4 Role-based permissions from group 30:Contractors to group 10:Employee_FullAccess:
        Cisco_Jabber_Access-10
IPv4 Role-based permissions from group 30:Contractors to group 120:Mail_Servers:
        Permit_Email_Traffic
...
```

Verifying Host Traffic Monitor Capture

Embedded Wireshark can help determine traffic
what traff is ingressing on an interface

```
FE2050#monitor capture test interface gigabitEthernet 1/0/10 both match any limit duration 60


FE2050#monitor capture test start display
Starting the packet display ........ Press Ctrl + Shift + 6 to exit
  1   8.469826      0.0.0.0 -> 255.255.255.255 DHCP 618 DHCP Discover - Transaction ID 0x1688
  2   8.483191      0.0.0.0 -> 255.255.255.255 DHCP 618 DHCP Request  - Transaction ID 0x1688
  3   8.705606 CiscoInc_35:53:43 -> Broadcast    ARP 60 Gratuitous ARP for 192.168.1.10 (Reply)
```

Control Plane Exchange

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.12	192.168.0.12	LISP	170	Encapsulated Map-Request for [4097] 192.168.0.12/32
2	0.001039	10.254.1.2	10.254.255.50	LISP	94	Map-Reply for [4097] 192.168.0.12/32
3	0.137652	10.255.1.22	10.254.255.52	LISP	82	Map-Request (RLOC-probe) for [4097] 192.168.0.12/32
4	0.139044	10.255.1.14	10.254.255.50	LISP	94	Map-Reply (RLOC-probe reply) for [4097] 192.168.0.12/32
5	0.863252	192.168.0.1	192.168.0.12	ICMP	148	Echo (ping) request id=0x0b50, seq=1/256, ttl=63 (reply in 9)
6	0.870066	192.168.0.1	192.168.0.12	ICMP	148	Echo (ping) request id=0x0b50, seq=2/512, ttl=63 (reply in 10)
7	1.139082	10.255.1.14	10.254.255.50	LISP	82	Map-Request (RLOC-probe) for [4097] 192.168.0.1/32
8	1.140831	10.255.1.22	10.254.255.52	LISP	94	Map-Reply (RLOC-probe reply) for [4097] 192.168.0.1/32
9	1.864089	192.168.0.12	192.168.0.1	ICMP	148	Echo (ping) reply id=0x0b50, seq=1/256, ttl=63 (request in 5)
10	1.864135	192.168.0.12	192.168.0.1	ICMP	148	Echo (ping) reply id=0x0b50, seq=2/512, ttl=63 (request in 6)

1 Ingress Edge Node -> Control Node, where is 192.168.0.12 (Egress Edge Node)

2 Control Node -> Ingress Edge Node, sending info for Egress node

3 Ingress Edge Node -> Egress Edge node , map request for RLOC info

4 Egress Edge Node -> Ingress Edge node, gives RLOC info

5/6 Encapsulated Data packets

7/8 Exchange for return packets

Packet Capture

```
    5 0.863252    192.168.0.1     192.168.0.12    ICMP    148 Echo (ping) request  id=0x0b50, seq=1/256, ttl=63 (reply in 9)
    6 0.870066    192.168.0.1     192.168.0.12    ICMP    148 Echo (ping) request  id=0x0b50, seq=2/512, ttl=63 (reply in 10)
    7 1.139082    10.255.1.14     10.254.255.50   LISP     82 Map-Request (RLOC-probe) for [4097] 192.168.0.1/32
    8 1.140831    10.255.1.22     10.254.255.52   LISP     94 Map-Reply (RLOC-probe reply) for [4097] 192.168.0.1/32
    9 1.864089    192.168.0.12    192.168.0.1     ICMP    148 Echo (ping) reply    id=0x0b50, seq=1/256, ttl=63 (request in 5)
   10 1.864135    192.168.0.12    192.168.0.1     ICMP    148 Echo (ping) reply    id=0x0b50, seq=2/512, ttl=63 (request in 6)
   11 1.869295    192.168.0.1     192.168.0.12    ICMP    148 Echo (ping) request  id=0x0b50, seq=3/768, ttl=63 (reply in 12)
   12 1.869346    192.168.0.12    192.168.0.1     ICMP    148 Echo (ping) reply    id=0x0b50, seq=3/768, ttl=63 (request in 11)
   13 2.868296    192.168.0.1     192.168.0.12    ICMP    148 Echo (ping) request  id=0x0b50, seq=4/1024, ttl=63 (reply in 14)
   14 2.868352    192.168.0.12    192.168.0.1     ICMP    148 Echo (ping) reply    id=0x0b50, seq=4/1024, ttl=63 (request in 13)
```

```
> Frame 5: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits) on interface 0
> Ethernet II, Src: Cisco_9f:1d:40 (00:00:0c:9f:1d:40), Dst: Cisco_e9:4c:7f (fc:99:47:e9:4c:7f)
> Internet Protocol Version 4, Src: 10.255.1.22, Dst: 10.254.255.52
> User Datagram Protocol, Src Port: 65359, Dst Port: 4789
v Virtual eXtensible Local Area Network
  > Flags: 0x8800, GBP Extension, VXLAN Network ID (VNI)
    Group Policy ID: 13
    VXLAN Network Identifier (VNI): 4097
    Reserved: 0
> Ethernet II, Src: Cisco_9f:00:00 (00:00:0c:9f:00:00), Dst: ba:25:cd:f4:ad:38 (ba:25:cd:f4:ad:38)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.12
> Internet Control Message Protocol
```

New Header

VXLAN Header

Payload

Remote Destinations

Control Node View

```
ControlNode#show lisp site instance-id 4099
LISP Site Registration Information
* = Some locators are down or unreachable
# = Some registrations are sourced by reliable transport

Site Name      Last      Up     Who Last             Inst     EID Prefix
               Register         Registered           ID
site_uci       never     no     --                   4099     0.0.0.0/0
               01:49:32  yes#   10.254.255.3         4099     10.254.255.58/32
               never     no     --                   4099     192.168.1.0/24
               01:49:32  yes#   10.254.255.50        4099     192.168.1.10/32
               00:02:31  yes#   10.254.255.51        4099     192.168.1.11/32
               never     no     --                   4099     192.168.100.0/24
```

DHCP server IP imported by border

Control node shows registered hosts and subnets

Lisp Control Plane Statistics

```
ControlNode#show ip lisp statistics
LISP EID Statistics for all EID instances - last cleared:
Control Packets:
  Map-Requests in/out:                        8349/0
    Encapsulated Map-Requests in/out:         8349/0
    RLOC-probe Map-Requests in/out:           0/0
    SMR-based Map-Requests in/out:            0/0
    Map-Requests expired on-queue/no-reply    0/0
    Map-Resolver Map-Requests forwarded:      60
    Map-Server Map-Requests forwarded:        0
  Map-Reply records in/out:                   0/8349
    Authoritative records in/out:             0/8294
    Non-authoritative records in/out:         0/55
    Negative records in/out:                  0/8294
    RLOC-probe records in/out:                0/0
```

```
FE2051#show ip lisp statistics
LISP EID Statistics for all EID instances
Control Packets:
  Map-Requests in/out:                        1/84
    Encapsulated Map-Requests in/out:         0/83
    RLOC-probe Map-Requests in/out:           1/1
    SMR-based Map-Requests in/out:            0/0
    Map-Requests expired on-queue/no-reply    0/0
    Map-Resolver Map-Requests forwarded:      0
    Map-Server Map-Requests forwarded:        0
  Map-Reply records in/out:                   84/1
    Authoritative records in/out:             83/1
    Non-authoritative records in/out:         1/0
    Negative records in/out:                  82/0
    RLOC-probe records in/out:                 1/1
    Map-Server Proxy-Reply records out:        0
```

Lisp statistics output shows many error counters with related to the control plan.

Forwarding to Remote Locations not in Cache

```
FE2050#show ip lisp eid-table vrf BruEsc forwarding eid remote
Prefix                Fwd action  Locator status bits   encap_iid
0.0.0.0/0             signal      0x00000000           N/A
  packets/bytes       2/608
10.254.255.58/32      encap       0x00000001           N/A
  packets/bytes     827/277311
192.168.1.0/24        signal      0x00000000
  packets/bytes       0/0
192.168.100.0/24      signal      0x00000000
  packets/bytes       0/0

FE2050#show ip cef vrf BruEsc exact-route 192.168.1.9 192.168.1.11
192.168.1.9 -> 192.168.1.11 =>glean for LISP0.4099

FE2050#show ip lisp eid-table vrf BruEsc map-cache 192.168.1.0/24
LISP IPv4 Mapping Cache for EID-table vrf BruEsc (IID 4099), 4 entries

192.168.1.0/24, uptime: 1d00h, expires: never, via dynamic-EID, send-map-request
  Sources: dynamic-EID
  State: send-map-request, last modified: 1d00h, map-source: local
…
  Negative cache entry, action: send-map-request
```

The total EID space showing as “signal”. Traffic will trigged a map request

Forwarding to Remote Destination in Cache

```
FE2050#show ip lisp eid-table vrf BruEsc map-cache 192.168.1.11/32
LISP IPv4 Mapping Cache for EID-table vrf BruEsc (IID 4099), 5 entries

192.168.1.11/32, uptime: 00:00:18, expires: 23:59:41, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 00:00:18, map-source: 10.199.1.65
  Active, Packets out: 0(0 bytes)
  Encapsulating dynamic-EID traffic
  Locator        Uptime    State      Pri/Wgt     Encap-IID
  10.254.255.51  00:00:18  up          10/10        -
    Last up-down state change:         00:00:18, state change count: 1
    Last route reachability change:    00:00:18, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            00:00:18 (rtt 4ms)


FE2050#show ip cef vrf BruEsc exact-route 192.168.1.9 192.168.1.11
192.168.1.9 -> 192.168.1.11 =>IP adj out of GigabitEthernet1/0/14, addr 10.199.1.65
```

Forwarding to Remote Destination in Cache

```
FE2050#show ip lisp eid-table vrf BruEsc map-cache
LISP IPv4 Mapping Cache for EID-table vrf BruEsc (IID 4099), 5 entries
0.0.0.0/0, uptime: 1d00h, expires: never, via static-send-map-request
  Negative cache entry, action: send-map-request
192.168.1.0/24, uptime: 1d00h, expires: never, via dynamic-EID, send-map-request
  Negative cache entry, action: send-map-request
192.168.1.11/32, uptime: 00:29:58, expires: 23:30:01, via map-reply, complete
  Locator        Uptime    State      Pri/Wgt     Encap-IID
  10.254.255.51  00:29:58  up          10/10        -

FE2050#show ip cef vrf BruEsc 192.168.1.11/32  detail
192.168.1.11/32, epoch 1, flags [subtree context, check lisp eligibility]
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
  LISP remote EID: 0 packets 0 bytes fwd action encap, cfg as EID space, dynamic EID need encap
  SC inherited: LISP cfg dyn-EID - LISP configured dynamic-EID
  LISP EID attributes: localEID No, c-dynEID Yes, d-dynEID No
  LISP source path list
    nexthop 10.254.255.51 LISP0.4099
  2 IPL sources [no flags]
  nexthop 10.254.255.51 LISP0.4099
```

Border Node - BGP

```
Border#sh ip bgp vpnv4 al summary
BGP router identifier 10.254.255.3, local AS number 65001
BGP table version is 11, main routing table version 11
7 network entries using 1792 bytes of memory
8 path entries using 1088 bytes of memory
7/5 BGP path/bestpath attribute entries using 2072 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
1 BGP community entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 5048 total bytes of memory
BGP activity 16/8 prefixes, 19/10 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.254.255.2    4        65001      10       5       11    0    0 00:01:43        4
172.16.200.2    4        65002       6       4       11    0    0 00:01:47        1
```

iBGP session to CP
eBGP session to Fusion

Control Node - iBGP

```
ControlNode#show ip bgp vpnv4 all summary
BGP router identifier 10.254.255.2, local AS number 65001
BGP table version is 90, main routing table version 90
9 network entries using 2304 bytes of memory
13 path entries using 1768 bytes of memory
8/5 BGP path/bestpath attribute entries using 2368 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6512 total bytes of memory
BGP activity 21/11 prefixes, 50/36 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.254.255.3    4        65001      11      14       90    0    0 00:04:47        4
```

Control Plane has iBGP session(s) to Border node.

iBGP Internal Routes

```
Border#sh ip bgp vpnv4 all 192.168.1.0/24
BGP routing table entry for 1:4099:192.168.1.0/24, version 10
Paths: (1 available, best #1, table BruEsc)
  Advertised to update-groups:
     3
  Refresh Epoch 1
  Local, (aggregated by 65001 10.254.255.2)
    10.254.255.2 (metric 20) (via default) from 10.254.255.2 (10.254.255.2)
      Origin IGP, metric 0, localpref 100, valid, internal, atomic-aggregate, best
      Community: 655370
      Extended Community: RT:1:4099
```

```
ControlNode#show route-map
route-map tag, permit, sequence 10
  Match clauses:
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
    community 655370
```

Control Plane node inserts the EID space into iBGP with community set


cisco
You're
Cisco live!