



ACI Configuration & Operation Guide

2016.07



Configuration Guide 목차 내역

슬라이드No.	내용	슬라이드No.	내용	
1) APIC Initialization			30 Link Level Policy 설정	
6 – 7 APIC Initial Setup (Setup Utility)			31 PC / VPC Policy 설정	
8 APIC Initial Setup (Verify)			32 VPC Switch Policies 설정	
9 APIC Factory Reset			33 Link Level & PC / VPC Policy 적용	
10 APIC GUI Access			34 Interface Profile 적용	
2) Fabric Discovery			35 Switch Profile 적용	
12 Fabric Membership (Register S/W)			36 FEX 연동	
13 Fabric Inventory (Topology)			5) Tenants Setting	
14 OOB MGMT 설정			38 Tenants 설정	
3) System Setting			39 VRF 설정	
16 – 18 NTP 설정			40 – 41 BD (Bridge Domain) 설정	
19 SNMP Polling 설정			42 – 43 EPG (End-Point Group) 설정	
20 Syslog 설정 (Destination Group)			44 – 49 L3OUT 설정	
21 Syslog 설정 (Source: Access)			50 Contract 설정 – Networks (Subnet)	
22 Syslog 설정 (Source: Fabric)			51 Contract 설정 – Provided / Consumed	
23 BGP RR(Route Reflector) 설정			52 Contract 설정 – Filter	
4) Access Policy Setting			53 Contract 설정 – Contracts 정의	
25 VLAN Pool 설정			54 L4 연동 시 Static MAC 설정	
26 – 27 Physical Domain 설정				
28 – 29 Attachable Access Entity Profile 설정				

Operation Guide 목차 내역

슬라이드No.	내용	슬라이드No.	내용
1) Basic Operation		4) Management	
57 – 59	1. Basic Operation > 1.1 Controller Status	106	3. Monitoring > 3.4 Atomic counters (Traffic MAP)
60 – 61	1. Basic Operation > 1.2 Spine & Leaf Status	107 – 108	3. Monitoring > 3.4 Atomic counters (Troubleshooting Policy)
62 – 65	1. Basic Operation > 1.3 Fabric Discovery	109 – 111	3. Monitoring > 3.4 Statistics
66 – 70	1. Basic Operation > 1.4 Interface 확인	112	3. Monitoring > 3.5 Fabric Capacity Dashboard
71 – 72	1. Basic Operation > 1.5 VRF 확인	113 – 114	3. Monitoring > 3.6 Contract Deny Log
73 – 74	1. Basic Operation > 1.6 BD 확인	5) Troubleshooting	
75 – 78	1. Basic Operation > 1.7 EP(End Point) 확인	116 – 123	4. Management > 4.1 Image Management
79 – 82	1. Basic Operation > 1.8 L3Out 확인	124 – 127	4. Management > 4.2 Configuration Management
83 – 84	1. Basic Operation > 1.9 NTP 설정 확인	128	4. Management > 4.3 Tech support collection
85 – 86	1. Basic Operation > 1.10 SNMP Polling 확인	2) Post Deployment Lifecycle	
87 – 88	1. Basic Operation > 1.11 DHCP Relay 확인	130	5. Troubleshooting > 5.1 iPing
89	1. Basic Operation > 1.12 SPAN (Tenant SPAN)	131	5. Troubleshooting > 5.2 iTraceroute
90	1. Basic Operation > 1.12 SPAN (Infra SPAN)	132 – 137	5. Troubleshooting > 5.3 Visibility & Troubleshooting
2) Post Deployment Lifecycle			
92	2. Post Deployment Lifecycle		
3) Monitoring			
93 - 98	3. Monitoring > 3.1 Fault		
99	3. Monitoring > 3.2 Event		
100 - 105	3. Monitoring > 3.3 Health Score		



Agenda

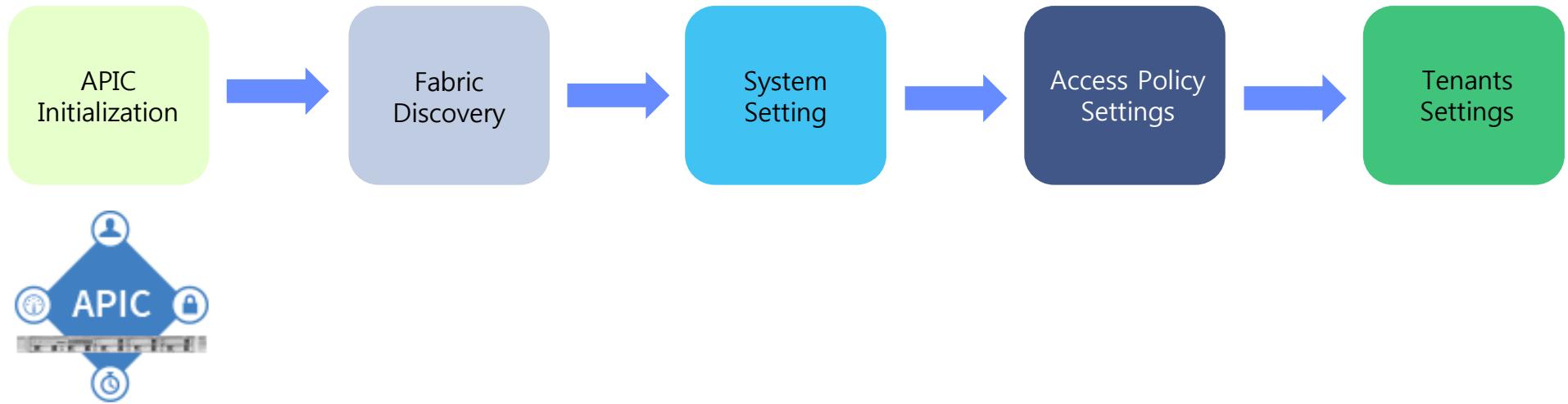
1. Configuration Guide

2. Operation Guide



1) APIC Initialization

- APIC 의 Initial Setup 및 초기화 설정 방법



APIC Initial Setup (Setup Utility)

APIC Initial Setup

Configure the APIC setup wizard with IP mgmt, subnet, gateway, subnet infra, VLAN infra, password.

Press any key to continue...

Press any key

Starting Setup Utility

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

*Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values.

Press Enter at anytime to assume the default values. Use ctrl-c at anytime to restart from the begining.

Cluster configuration ...

Enter the fabric name [ACI_Fabric1]:

From the following page
We will start the initial setup wizard

APIC Initial Setup (Setup Utility)

APIC Initial Setup

Start the initial setup wizard (Continued)

```
Cluster configuration ...
Enter the fabric name [ACI Fabric1]:
Enter the number of controllers in the fabric (1-9) [3]: 1
Enter the controller ID (1-1) [1]:
Enter the controller name [apic1]:
Enter address pool for TEP addresses [10.0.0.0/16]:
Enter the VLAN ID for infra network (1-4094) [4093]:
Enter address pool for BD multicast addresses (GIPO) [225.0.0.0/15]:

Out-of-band management configuration ...
Enter the IP address [192.168.10.1/24]:
Enter the IP address of the default gateway [None]:
Enter the interface speed/duplex mode [auto]:

admin user configuration ...
Enable strong passwords? [Y]: N
Enter the password for admin:

Reenter the password for admin:
```

Name of Fabric
Total number of controllers in Cluster (APIC 댓수)
Controller ID : 1 for Master
Infra VLAN ID
OoB Management Network
- IP address: x.x.x.x/x
- Default gateway: x.x.x.x
- Speed/duplex mode: auto
Strong passwords: N
Password: 1234qwer

APIC Initial Setup (Verify)

APIC Verify

Username : admin

Password : 1234qwer

```
apic1#  
apic1# show version  
Role      Id      Name          Version  
-----  -----  
controller 1      apic1        1.2 (3c)  
apic1# show controller detail  
ID          : 1*  
Name        : apic1  
UUID        : 1c48d5c0-15f8-11e6-aa2b-3d964ceb2e8b  
Address     : 10.0.0.1  
In-Band IPv4 Address : 0.0.0.0  
In-Band IPv6 Address : fc00::1  
OOB IPv4 Address   : 10.72.74.51  
OOB IPv6 Address   : fe80::5af3:9cff:fef7:ce10  
Serial Number    : FCH1830V00U  
Version         : 1.2 (3c)  
Commissioned     : in-service  
Registered       : available  
Valid Certificate: yes  
Validity Start   : 2014-09-05T04:28:00.000+00:00  
Validity End     : 2024-09-05T04:38:00.000+00:00  
Up Time          : 00:00:41:35.000  
Health           : fully-fit
```

ID & Name of Controller

OoO IP of Controller

State of Controller

APIC Factory Reset

APIC Factory Reset

```
apic1# bash configure end      exit      firmware show terminal trigger where  
clear debug      eraseconfig fabric reload  
apic1# eraseconfig  
Do you want to restore this APIC to factory settings? The system will be REBOOTED. (Y/n): Y  
apic1#
```

..... Rebooting

```
apic1# apic1# acidiag touch setup  
apic1# acidiag reboot  
  
Broadcast message from root@apic1  
          (unknown) at 15:49 ...  
  
The system is going down for reboot NOW!  
apic1#
```

※ Leaf Node 초기화

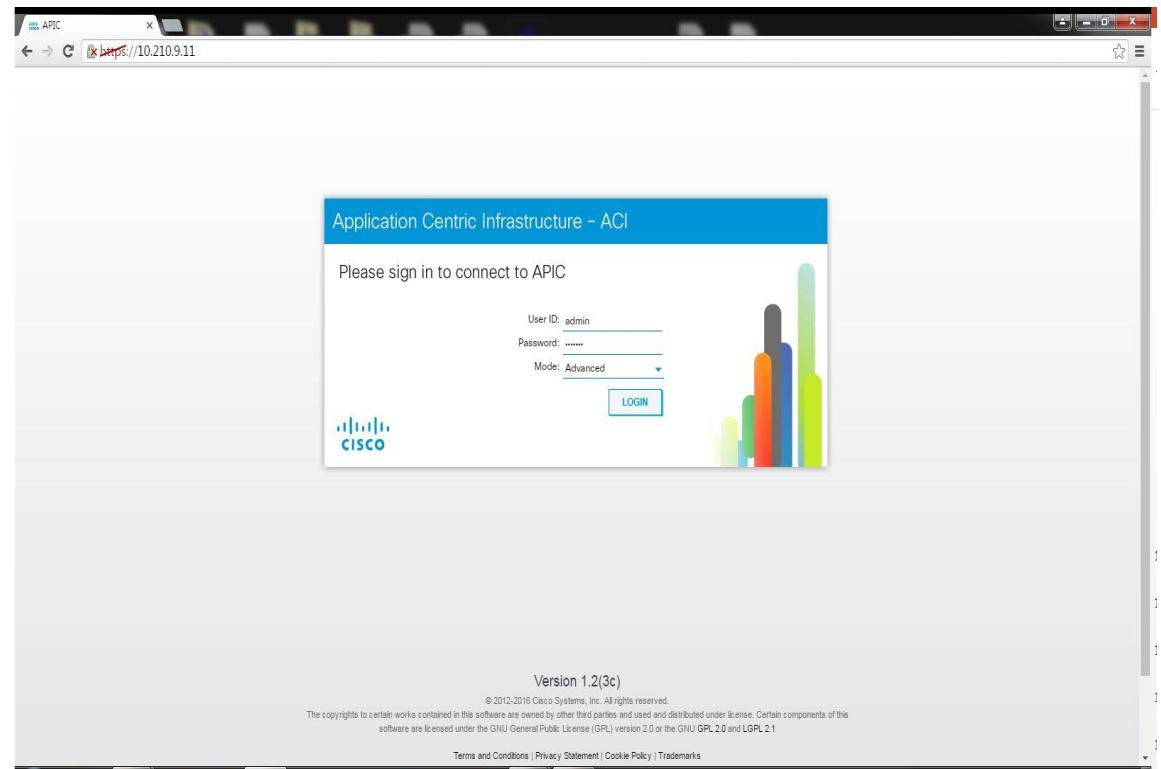
- Node# `setup-clean-config.sh`
- Node# `reload`
- This command will reload the chassis, Proceed (y/n)? [n]: y

APIC GUI Access

Please use the Chrome Browser & Firefox

<https://x.x.x.x> To Access

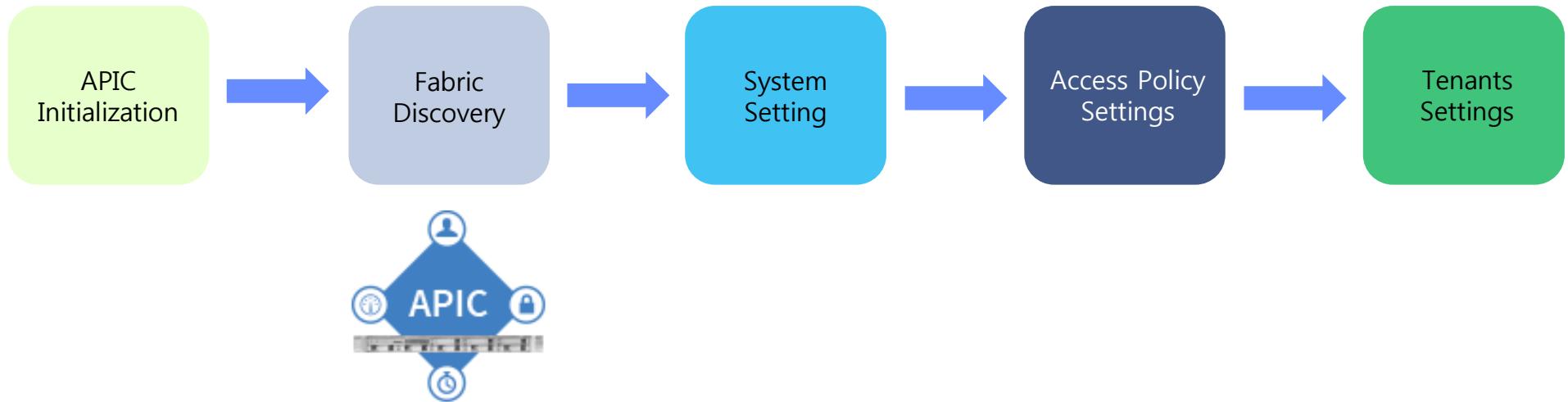
- Username : admin
- Password : 1234qwer



- Ignore the certificate error and proceed to site.

2) Fabric Discovery

- SPINE / LEAF Node Fabric 등록 및 Management 설정 방법



Fabric Membership (Register S/W)

Fabric > Inventory > Fabric Membership

The screenshot shows the Cisco Fabric Management interface. The top navigation bar includes tabs for System, Tenants, Fabric (highlighted with a red box), VM Networking, L4-L7 Services, Admin, and Operations. Below the navigation is an Advanced Mode welcome message. The left sidebar under the Inventory heading shows a tree view with nodes like Quick Start, Topology, Pod 1, and Fabric Membership (also highlighted with a red box). The main area is titled 'Fabric Membership' and displays a table of nodes. The table columns are: Serial Number, Node ID, Node Name, Rack Name, Model, Role, IP, Decommissioned, Supported Model, and SSL Certificate. The data in the table is as follows:

Serial Number	Node ID	Node Name	Rack Name	Model	Role	IP	Decommissioned	Supported Model	SSL Certificate
SAL1922G0F1	204	LEAF_204		N9K-C9372TX	leaf	10.0.88.93/32	False	True	yes
SAL1923G78T	203	LEAF_203		N9K-C9372TX	leaf	10.0.88.92/32	False	True	yes
SAL1931LA4J	101	SPINE_101		N9K-C9336PQ	spine	10.0.88.94/32	False	True	yes
SAL1934MR76	201	EXT_LEAF_201		N9K-C9372PX	leaf	10.0.88.95/32	False	True	yes

Enter Node ID, Node Name

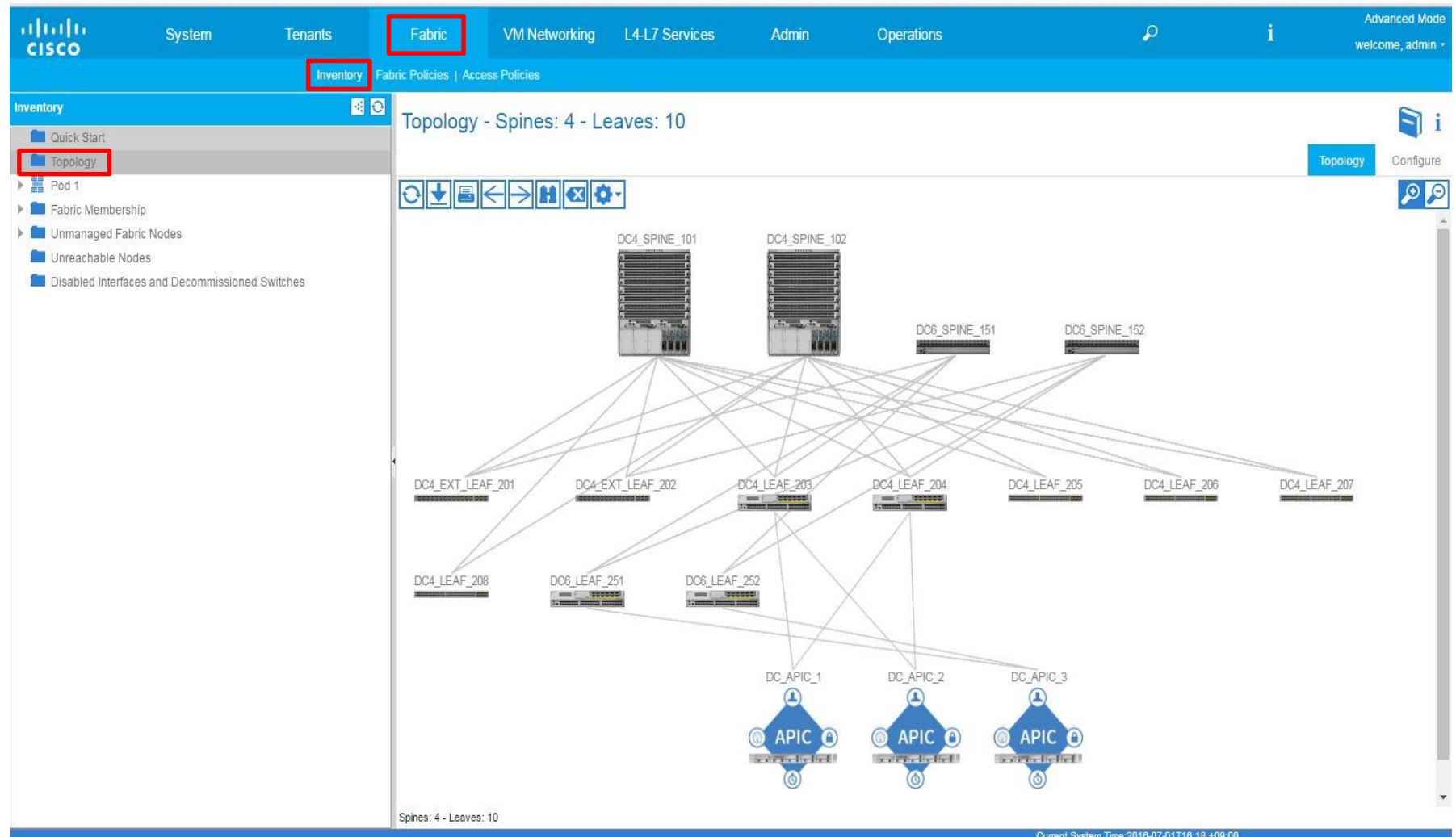
SAL1931LA4J
(사전에 Serial Number 확인 필요)
NODE ID: 101
NODE NAME: SPINE_101

This screenshot shows the 'Fabric Membership' update dialog box. It contains a table with the same columns as the main list. The 'Node Name' column for the row with Serial Number SAL1931LA4J is currently set to 'SPINE_101'. A yellow arrow points from the text entry field in the dialog to the corresponding cell in the table. At the bottom of the dialog are two buttons: 'UPDATE' (highlighted with a red box) and 'CANCEL'.

Serial Number	Node ID	Node Name	Rack Name	Model	Role	IP	Decommissioned	Supported Model	SSL Certificate
SAL1922G0F1	204	LEAF_204		N9K-C9372TX	leaf	10.0.88.93/32	False	True	yes
SAL1923G78T	203	LEAF_203		N9K-C9372TX	leaf	10.0.88.92/32	False	True	yes
SAL1931LA4J	101	SPINE_101	select	N9K-C9336PQ	spine	10.0.88.94/32	False	True	yes
SAL1934MR76	201	EXT_LEAF_201				10.0.88.95/32	False	True	yes

Fabric Inventory (Topology)

Fabric > Inventory > Topology



OOB MGMT 설정

Tenants > mgmt > Node Management Address > Static Node Management Addresses

The screenshot shows the Cisco Application Centric Infrastructure (ACI) web interface. The top navigation bar includes tabs for System, Tenants (highlighted with a red box), Fabric, VM Networking, L4-L7 Services, Admin, and Operations. A search bar and user information (welcome, admin) are also present. The main content area is titled "Static Node Management Addresses". On the left, a sidebar under "Tenant mgmt" shows various management profiles, with "Static Node Management Addresses" highlighted by a red box. A yellow callout box labeled "마우스 우 클릭 Create Static Node Management Addresses" points to the sidebar entry. Another yellow callout box labeled "각 Node에 대한 MGMT IP 설정" points to the table header. The table lists a single row for "node-251" with Out-Of-Band type, default EPG, and IP addresses 10.210.10.101/24 and 10.210.10.1. A modal window titled "Create Static Node Management Addresses" is open, prompting for a policy name (251) and node range (From 251 To 251). It includes checkboxes for "Out-Of-Band Addresses" (checked) and "In-Band Addresses". Below this, the "Out-Of-Band Addresses" section is expanded, showing settings for Out-Of-Band Management EPG (default), Out-Of-Band IPv4 Address (10.210.10.101/24), and Out-Of-Band IPv4 Gateway (10.210.10.1). The bottom right of the modal has "SUBMIT" and "CANCEL" buttons, with "SUBMIT" highlighted by a red box.

Node	Type	EPG	IPv4 Address	IPv4 Gateway	IPv6 Address	IPv6 Gateway
node-251	Out-Of-Band	default	10.210.10.101/24	10.210.10.1

Create Static Node Management Addresses

Specify policy name and a node range, and set their IPs.

Node Range: 251 - 251

Config: Out-Of-Band Addresses In-Band Addresses

Out-Of-Band Addresses

Out-Of-Band Management EPG: default

Out-Of-Band IPv4 Address: 10.210.10.101/24

Out-Of-Band IPv4 Gateway: 10.210.10.1

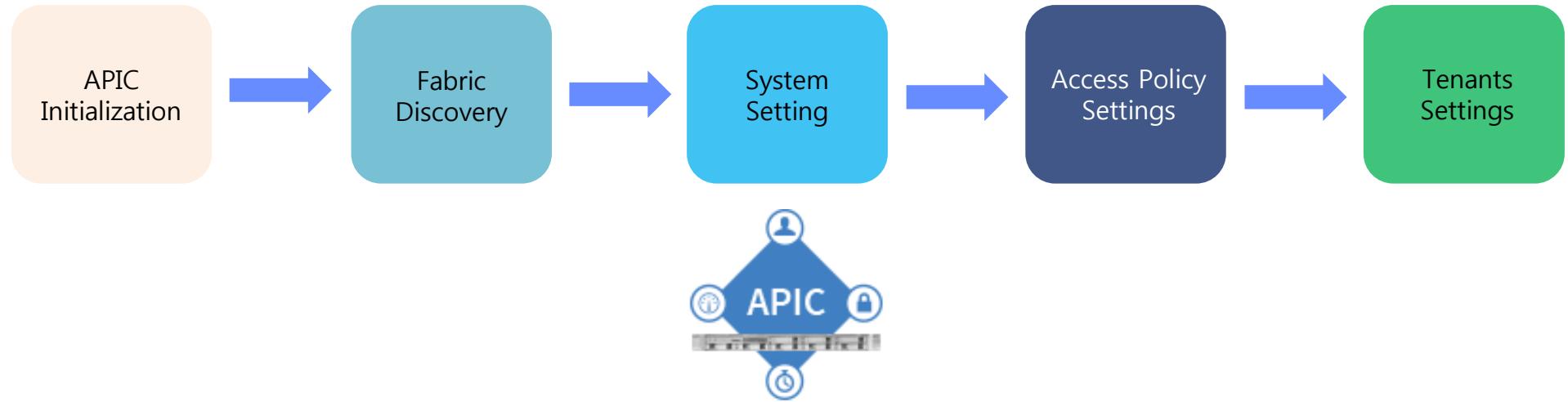
Out-Of-Band IPv6 Address:

Out-Of-Band IPv6 Gateway:

SUBMIT CANCEL

3) System Setting

- System (NTP, SNMP, SYSLOG 등) 연동을 위한 설정 방법



NTP 설정(1)

Fabric > Fabric Policy > POD Policy > Policies > Date and Time

The screenshot shows the Cisco Fabric Manager interface. The top navigation bar includes System, Tenants, Fabric (highlighted with a red box), VM Networking, L4-L7 Services, Admin, and Operations. The right side shows a welcome message for 'admin'. The main area is titled 'Policies - Date and Time'. On the left, a sidebar lists Policies (Quick Start, Switch Policies, Module Policies, Interface Policies, Pod Policies, Policies, Date and Time, SNMP, Management). A yellow callout box with the text '마우스 우 클릭 Create Date and Time Policy' points to the 'Date and Time' option. The central panel shows two entries: 'default' (Administrative State: enabled) and 'NTP_Server' (Administrative State: enabled). Below this is a 'Create Date And Time Policy' dialog box. It has a 'STEP 1 > Identity' section with fields: Name (NTP_Server), Description (optional), Administrative State (disabled/enabled), and Authentication State (disabled/enabled). A red box highlights the 'Name' field. A red arrow points from this dialog to a 'Create Providers' dialog box on the right. This second dialog is titled 'Specify the information about the NTP Server' and contains fields: Name (177.125.7.177), Description (optional), Preferred (checkbox), Minimum Polling Interval (4), Maximum Polling Interval (6), Management EPG (dropdown set to default (Out-of-Band)), and OK/CANCEL buttons. A yellow box labeled 'NTP Server IP 입력' highlights the 'Name' field, and another yellow box labeled 'MGMT NTP 설정' highlights the 'Management EPG' dropdown.

마우스 우 클릭
Create Date and Time Policy

STEP 1 > Identity

Name: NTP_Server

Description: optional

Administrative State: disabled enabled

Authentication State: disabled enabled

PREVIOUS NEXT CANCEL

Create Providers

Specify the information about the NTP Server

Name: 177.125.7.177

Description: optional

Preferred:

Minimum Polling Interval: 4

Maximum Polling Interval: 6

Management EPG: default (Out-of-Band)

OK CANCEL

NTP 설정(2)

Fabric > Fabric Policy > POD Policy > Policy Groups

The screenshot shows the Cisco Application Centric Infrastructure (ACI) policy configuration interface. The top navigation bar includes tabs for System, Tenants, Fabric (selected), VM Networking, L4-L7 Services, Admin, and Operations, along with search and filter icons. The right side shows a user session with 'Advanced Mode' and 'welcome, admin'. The main content area is titled 'Pod Policies - Policy Groups'.

Policies sidebar:

- Quick Start
- Switch Policies
- Module Policies
- Interface Policies
- Pod Policies** (selected)
- Policies
 - Date and Time
 - SNMP
- Management Access
 - ISIS Policy default
 - COOP Group Policy default
 - BGP Route Reflector default
- Policy Groups** (highlighted with a red box)
- DC_Fabric
- Global Policies
- Monitoring Policies
- Troubleshoot Policies
- Geolocation Policies
- Tags

Create Pod Policy Group dialog:

Specify the Policy Group properties:

- Name: DC_Fabric (highlighted with a red box)
- Description: optional
- Date Time Policy: NTP_Server (highlighted with a red box)
- ISIS Policy: default
- COOP Group Policy: default
- BGP Route Reflector Policy: default
- Management Access Policy: default
- SNMP Policy: default

A yellow callout box points to the 'NTP_Server' entry in the Date Time Policy dropdown, containing the text: "NTP_Server에 대해 정의 해 놓은 Policies를 적용".

At the bottom of the dialog are 'SUBMIT' and 'CANCEL' buttons, with 'SUBMIT' highlighted with a red box.

NTP 설정(3)

Fabric > Fabric Policy > POD Policy > Profiles

The screenshot shows the Cisco ACI Policy Manager interface. The top navigation bar includes tabs for System, Tenants, Fabric (selected), VM Networking, L4-L7 Services, Admin, and Operations, along with search and information icons. The right side of the header shows the user is in Advanced Mode with the welcome, admin user.

The left sidebar displays a hierarchical tree of policy categories: Policies, Pod Policies, Policies, Policy Groups, DC_Fabric, default, and Profiles. The 'default' profile under Profiles is currently selected, as indicated by a grey background.

The main content area is titled 'Pod Selector - default'. It contains a 'Properties' section with fields for Name (default), Description (optional), Type (ALL), and Fabric Policy Group (DC_Fabric). A yellow callout box highlights the 'Fabric Policy Group' dropdown, which is set to 'DC_Fabric'. The dropdown menu also lists 'default' and a 'Create Pod Policy Group' option. The entire 'Fabric Policy Group' field is highlighted with a red box.

A yellow callout box with the text 'DC_Fabric에 대해 정의 해 놓은 Policy Groups 을 적용' (Apply defined Policy Groups for DC_Fabric) points to the 'Fabric Policy Group' dropdown.

SNMP Polling 설정

Fabric > Fabric Policy > POD Policy > Policy Groups > SNMP

❖ Fabric > Fabric Policies
 > Pod Policies > SNMP ⇒ Create SNMP Policy

The screenshot shows the 'SNMP Policy - NMS_POLICY' configuration screen. Key fields highlighted in red include:

- SNMP Policy Name:** NMS_POLICY
- Associated Management EPG:** default (Out-of-Band)
- Community string:** infra

POD Policy 등록

❖ Fabric > Fabric Policies > Policy Groups

*SNMP Policy를 POD Policy Group (SNMP Policy)에 등록해야 함

SNMP Client Group 등록

The screenshot shows the 'SNMP Client Group Profile - CYGNUS' configuration screen. Key fields highlighted in red include:

- Name:** CYGNUS
- Associated Management EPG:** default (Out-of-Band)
- Address:** 10.192.29.35, 10.192.29.34, 10.192.29.33

NMS 서버 리스트

Syslog 설정 (Destination Group)

Admin > External Data Collectors > Monitoring Destinations > Syslog

❖ Syslog ⇒ Create Syslog Monitoring Destination Group

The screenshot shows the Cisco Application Centric Infrastructure (ACI) web interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking L4-L7 Services, Admin, Operations, and Advanced Mode (welcome, admin). The Admin tab is selected.

The main content area displays the 'External Data Collectors' section under 'Monitoring Destinations'. A 'SYSLOG_SVR' entry is selected. A yellow arrow points from the 'SYSLOG_SVR' entry in the left sidebar to the 'Name' field ('SYSLOG_SVR') in the 'Property' section of the right panel.

The 'Property' section contains the following fields:

- Name: SYSLOG_SVR (highlighted by a red box)
- Description: (optional)
- Transport Protocol: udp
- Port Number: 514
- Admin State: disabled

Below these fields, there are two destination sections:

- Local File Destination:** Admin State: enabled, Severity: warnings. A note next to it says "Syslog 전달 시 Local File에 저장 여부".
- Console Destination:** Admin State: enabled, Severity: alerts. A note next to it says "Syslog 전달 시 Console에 표시 여부".

A yellow arrow points from the 'Create Syslog Remote Destination' dialog box to the 'Host Name/IP' field ('10.192.14.33') in the 'Property' section.

The 'Create Syslog Remote Destination' dialog box contains the following fields:

- Host Name/IP: 10.192.14.33 (highlighted by a red box)
- Name: (highlighted by a red box)
- Admin State: disabled (highlighted by a red box)
- Severity: information (highlighted by a red box)
- Port: 514
- Forwarding Facility: local7
- Management EPG: default (Out-of-Band) (highlighted by a red box)

Annotations in red text provide additional context:

- Syslog Server IP: Points to the 'Host Name/IP' field.
- Packet Deny Log 전송을 위해서 information 선택: Points to the 'Severity' dropdown set to 'information'.
- Forwarding Facility: Points to the 'Forwarding Facility' dropdown set to 'local7'.
- OoO N/W으로 전송: Points to the 'Management EPG' dropdown set to 'default (Out-of-Band)'.

At the bottom of the dialog box are 'OK' and 'CANCEL' buttons.

Syslog 설정 (Source: Access)

Fabric > Fabric Policies > Monitoring Policies > default > Callhome/SNMP/Syslog

❖ Syslog ⇒ Create Syslog Source

The screenshot shows the Cisco Fabric Manager web interface. The top navigation bar includes links for System, Tenants, Fabric (which is selected), VM Networking L4-L7 Services, Admin, and Operations. A search bar and an information icon are also present. The main content area has tabs for Inventory, Fabric Policies, and Access Policies. On the left, a sidebar lists various policy categories under Policies, with Monitoring Policies expanded and Callhome/SNMP/Syslog selected. The main panel displays the 'Callhome/SNMP/Syslog' configuration page. It shows a table with one row for 'ACCESS_SYSLOG_SRC', which includes 'Events', 'Faults', and 'Session logs' under 'Include' and 'information' under 'Min Severity'. The 'Destination Group' is set to 'SYSLOG_SVR'. A modal window titled 'Create Syslog Source' is open, prompting for 'Name' (set to 'ACCESS_SYSLOG_SRC'), 'Min Severity' (set to 'information'), and 'Include' options (with 'Events', 'Faults', and 'Session logs' checked). A note in red text explains that these include Audit logs, Events, Faults, and Session logs. The 'Dest Group' is also set to 'SYSLOG_SVR'. Buttons for 'SUBMIT' and 'CANCEL' are at the bottom of the modal.

Syslog 설정 (Source: Fabric)

Fabric > Fabric Policies > Monitoring Polices > default > Callhome/SNMP/Syslog

❖ Syslog ⇒ Create Syslog Source

The screenshot shows the Cisco Fabric Manager interface. The top navigation bar includes System, Tenants, Fabric (selected), VM Networking L4-L7 Services, Admin, and Operations. The right side shows Advanced Mode with user welcome, admin. The left sidebar under Policies lists various policy types, with Monitoring Policies expanded and Callhome/SNMP/Syslog selected. The main content area displays the 'Callhome/SNMP/Syslog' configuration page. A table shows a single entry for 'FABRIC_SYSLOG_SRC' with 'Events', 'Faults', and 'Session logs' selected under 'Include' and 'information' as 'Min Severity'. Below this, a 'Create Syslog Source' dialog box is open, showing the same configuration: Name: FABRIC_SYSLOG_SRC, Min Severity: information, and 'Events', 'Faults', and 'Session logs' selected under 'Include'. The 'Dest Group' is set to 'SYSLOG_SVR'. Buttons for 'SUBMIT' and 'CANCEL' are at the bottom.

❖ Deny packet log를 위한 설정

Fabric > Access Policies
> Monitoring Destination
> Common Policy
> Syslog Message Policies
> Policy for system log messages

⇒ Facility Filters 중
'default'의 Severity를
information으로 변경

❖ Deny packet log 확인

Fabric > Inventory
> Pod1
⇒ History ⇒ EVENTS

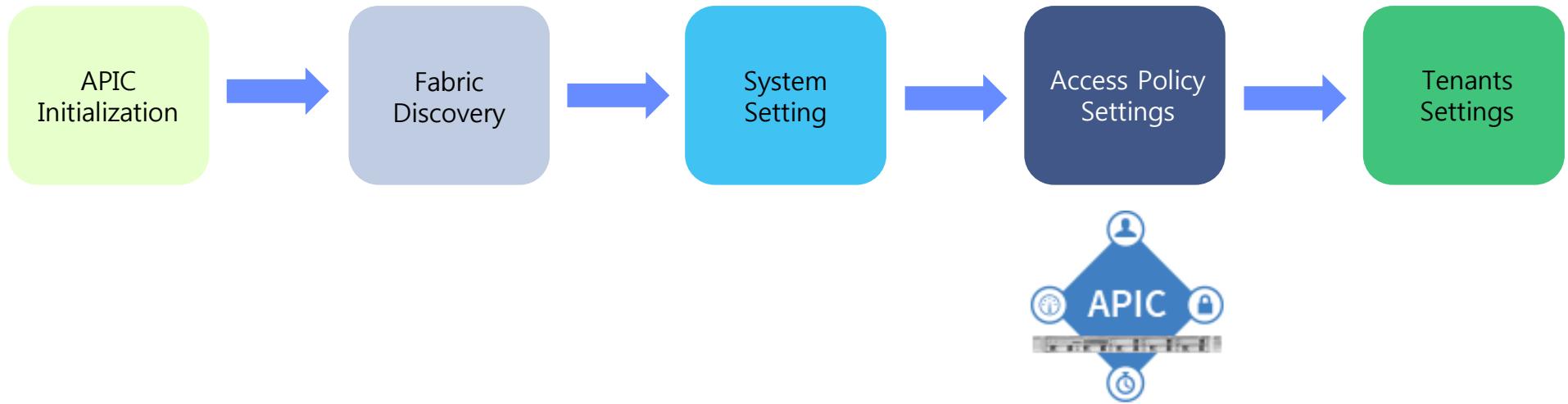
BGP RR(Route Reflector) 설정

Fabric > Fabric Policy > POD Policy > Policy Groups > BGP Route Reflector default

The screenshot shows the Cisco ACI Fabric Policy interface. The top navigation bar has tabs for System, Tenants, Fabric (highlighted with a red box), VM Networking, L4-L7 Services, Admin, and Operations. Below the navigation is a search bar and a help icon. The main area is titled "BGP Route Reflector Policy - BGP Route Reflector default". On the left, there's a sidebar with "Policies" and several policy categories. Under "Pod Policies", "Pod Policies" is expanded, and "BGP Route Reflector default" is selected (highlighted with a red box). A yellow callout bubble points to this selection with the text "각 SPINE Node 선택". A modal window titled "Create Route Reflector Node Policy Ep" is open, prompting to "Specify route reflector node EP id". It shows a dropdown menu labeled "Spine Node" with the placeholder "select an option" and a list of options: 101, 102, 151, and 152. At the bottom of the modal are "SUBMIT" and "CANCEL" buttons.

4) Access Policy Setting

- SPINE / LEAF Node 및 Interface Policy 정의 또는 Profile 설정 방법



VLAN Pool 설정

Fabric > Access Policies > VLAN

- ❖ VLAN > Create VLAN Pool
 - VLAN Database 생성

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) interface. The URL is <https://10.210.9.11/#cd|root|fvnsVlanInstPs,fvnsNamespacesandaddresses>. The navigation bar includes System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and Advanced Mode (welcome, admin). The main menu on the left has sections for Policies (Quick Start, Switch Policies, Module Policies, Interface Policies, Global Policies, Monitoring Policies, Troubleshoot Policies), Pools (VLAN, VXLAN, Multicast Address, Physical and External Domains), and a selected Pools section. Under Pools, there is a 'V11-200 (Static Allocation)' entry. The central area displays 'Pools - VLAN' with a table showing one row: Name (V11-200), Allocation Mode (Static Allocation), Encap Blocks ([11-200]), and Description (optional). Below this is a 'Create VLAN Pool' dialog box with fields for Name (V11-200), Description (optional), Allocation Mode (Dynamic Allocation, Static Allocation, selected), and Encap Blocks (VLAN Range and Allocation Mode). A red box highlights the 'Static Allocation' button. A red arrow points from this button to a 'Create Ranges' dialog box, which shows Type (VLAN), Range (11 - 200), Allocation Mode (Dynamic Allocation, Inherit allocMode from parent, Static Allocation, selected), and OK/CANCEL buttons. A red box highlights the 'Static Allocation' button in the 'Create Ranges' dialog.

※ 초기 VLAN Range 설정 후 서비스 중에도 영향 없이 VLAN 대역 추가 가능

Physical Domain 설정(1)

Fabric > Access Polices > Physical and External Domains > Physical Domains

❖ Physical Domains > Create Physical Domains

The screenshot shows the Cisco ACI Fabric interface. The top navigation bar includes tabs for System, Tenants, Fabric (highlighted with a red box), VM Networking, L4-L7 Services, Admin, and Operations. A search bar and user information (Advanced Mode, welcome, admin) are also present. Below the navigation is a breadcrumb path: Inventory > Fabric Policies > Access Policies.

The left sidebar contains a tree view under Policies, with Physical and External Domains expanded, and Physical Domains selected (highlighted with a red box). Other options include Quick Start, Switch Policies, Module Policies, Interface Policies, Global Policies, Monitoring Policies, Troubleshoot Policies, Pools, and External Bridged Domains/External Routed Domains.

The main content area displays the "Physical Domain - PD_V11-200" configuration page. The "Properties" section shows the Name as "PD_V11-200" and the Associated Attachable Entity Profile as "AEP_V11-200". The "VLAN Pools" dropdown is set to "[V11-200]-static" (highlighted with a red box). The "Security Domains" section is currently empty. At the bottom are buttons for SHOW USAGE, SUBMIT, and RESET.

Physical Domain 설정(2)

Fabric > Access Polices > Physical and External Domains > External Routed Domains

❖ External Routed Domains > Create External Routed Domains (L3)

L3 Domain Profile - Domain L3OUT_ROUTED

Name: L3OUT_ROUTED

Associated Attachable Entity Profile: AEP_L3OUT_ROUTED

VLAN Pool: select an option

Security Domains:

Create Layer 3 Domain

Name: L3OUT Domain Name 지정

Associated Attachable Entity Profile: select a value

VLAN Pool: select an option

Security Domains:

SUBMIT CANCEL

SHOW USAGE SUBMIT RESET

Attachable Access Entity Profile 설정(1)

Fabric > Access Polices > Global Policies > Attachable Access Entity Profiles

- ❖ Attachable Access Entity Profiles > Create Attachable Access Entity Profiles
 - 논리적 / 물리적인 구성 묶어주는 맵핑 역할

CISCO

System Tenants Fabric VM Networking L4-L7 Services Admin Operations Advanced Mode welcome, admin

Policies

- Quick Start
- Switch Policies
- Module Policies
- Interface Policies
- Global Policies
- Attachable Access Entity Profiles
- AEP_L3OUT_ROUTED
- AEP_V11-200
- default
- QOS Class Policies
- DHCP Relay Policies
- MCP Instance Policy default
- EP Loop Protection Policy
- Error Disabled Recovery Policy
- Port Tracking
- Monitoring Policies
- Troubleshoot Policies
- Pools
- Physical and External Domains

Create Attachable Access Entity Profile

STEP 1 > Profile

1. Profile 2. Association To Interfaces

Name: AEP_V11-200

Description: optional

Enable Infrastructure VLAN:

Domains (VMM, Physical or External) To Be Associated To Interfaces: Domain Profile

PD_V11-200 (Physical)

Encapsulation: UPDATE CANCEL

이전에 설정 하였던 Physical Domain Profile 적용

설정 완료 화면

Attachable Access Entity Profile - AEP_V11-200

Properties

Name: AEP_V11-200

Description: optional

Enable Infrastructure VLAN:

Domains (VMM, Physical or External) Associated to Interfaces:

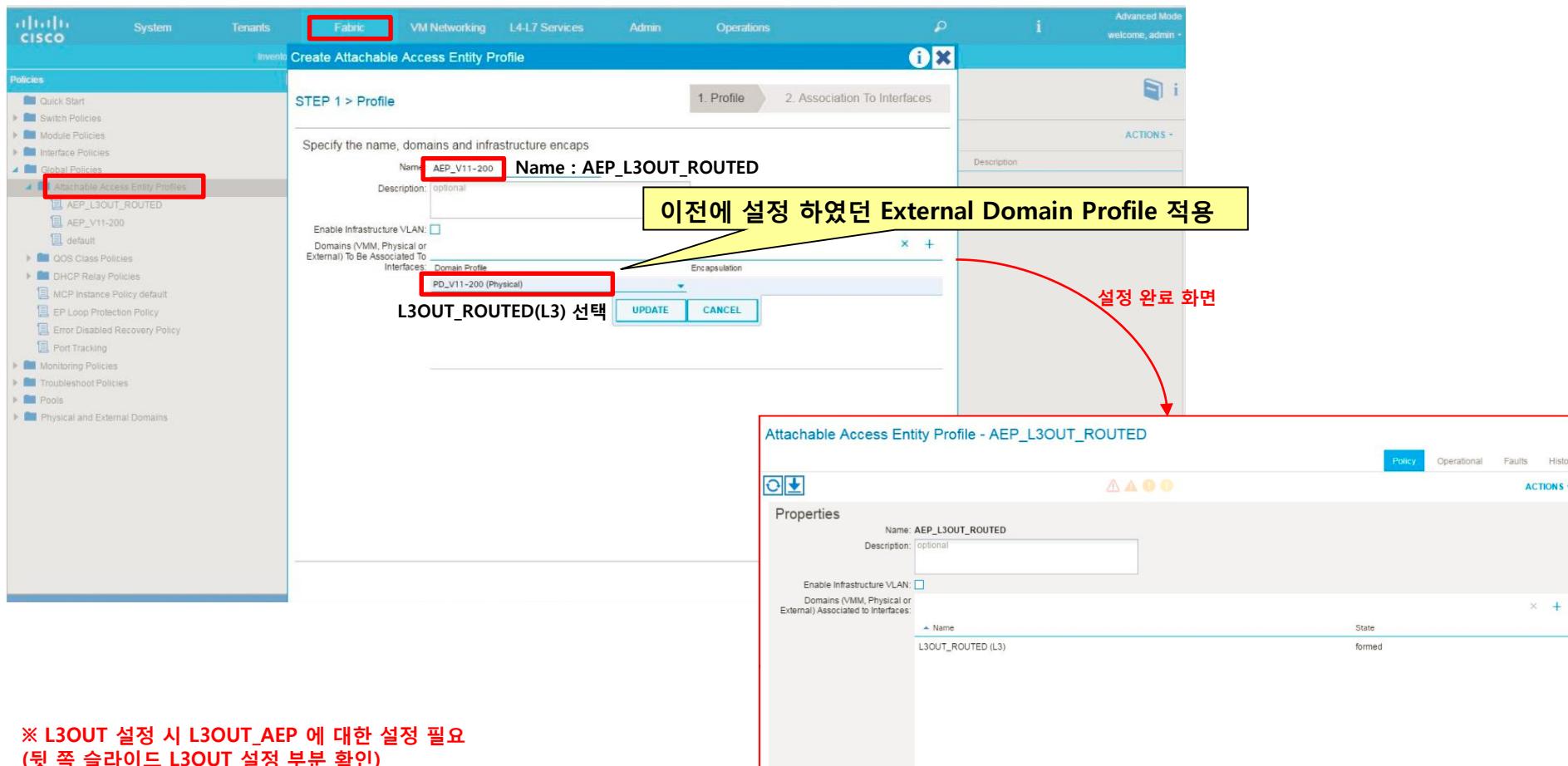
Name	State
PD_V11-200 (Physical)	formed

Policy Operational Faults History ACTIONS

Attachable Access Entity Profile 설정(2)

Fabric > Access Policies > Global Policies > Attachable Access Entity Profiles

- ❖ Attachable Access Entity Profiles > Create Attachable Access Entity Profiles
 - 논리적 / 물리적인 구성 묶어주는 맵핑 역할



※ L3OUT 설정 시 L3OUT_AEP 에 대한 설정 필요
(뒷 쪽 슬라이드 L3OUT 설정 부분 확인)

Link Level Policy 설정

Fabric > Access Policies > Interface Policies > Policies > Link Level

❖ Link Level > Create Link Level > 1G / 10G / 40G / Auto(Inherit) 설정

The screenshot shows the Cisco Application Centric Infrastructure (ACI) interface for creating Link Level Policies.

Left Panel (Navigation):

- System
- Tenants
- Fabric** (highlighted)
- VM Networking
- L4-L7 Services
- Admin
- Operations

Top Bar:

- Inventory | Fabric Policies | **Access Policies**
- Advanced Mode welcome, admin ·

Properties for 1G_AUTO:

- Name: **1G_AUTO** (highlighted)
- Description: optional
- Label:
- Auto Negotiation: **on** (radio button selected)
- Speed: **1 Gbps** (highlighted)
- Link debounce interval (msec): 100

Properties for AUTO:

- Name: **AUTO** (highlighted)
- Description: optional
- Label:
- Auto Negotiation: **on** (radio button selected)
- Speed: **inherit** (highlighted)
- Link debounce interval (msec): 100

Bottom Navigation:

- System
- Tenants
- Fabric
- VM Networking
- L4-L7 Services
- Admin
- Operations

Bottom Left Panel (Navigation):

- Quick Start
- Switch Policies
- Module Policies
- Interface Policies** (highlighted)
- Policies
- Link Level** (highlighted)
- 1G_AUTO
- 1G_NONEGO
- 10G_AUTO
- 10G_NONEGO
- 40G_AUTO
- AUTO
- default
- CDP Interface
- LLDP Interface
- Port Channel
- Port Channel Member
- Spanning Tree Interface
- Storm Control
- Data Plane Policing
- MCP Interface
- L2 Interface
- Firewall
- Policy Groups
- Profiles
- Interface Overrides
- Global Policies
- Monitoring Policies

PC / VPC Policy 설정

Fabric > Access Polices > Interface Policies > Policies > Port Channel

- ❖ Port Channel > LACP Active Mode 설정
 - Port Channel Policy 설정

The screenshot shows the Cisco ACI Policy Manager interface. The top navigation bar includes tabs for System, Tenants, Fabric (highlighted with a red box), VM Networking, L4-L7 Services, Admin, and Operations. Below the navigation is a search bar and user information (welcome, admin). The main content area has tabs for Inventory, Fabric Policies, and Access Policies (also highlighted with a red box). On the left, a sidebar lists policy categories: Policies, Quick Start, Switch Policies, Module Policies, Interface Policies, Policies (Link Level, CDP Interface, LLDP Interface, Port Channel), Port Channel Member, Spanning Tree Interface, Storm Control, Data Plane Policing, MCP Interface, L2 Interface, Firewall, Policy Groups, Profiles, Interface Overrides, Global Policies, Monitoring Policies, Troubleshoot Policies, Pools, and Physical and External Domains. Under Policies, the Port Channel category is expanded, and its sub-item 'LACP_ACTIVE' is selected (highlighted with a red box). The main panel displays the 'Port Channel Policy - LACP_ACTIVE' configuration. It shows the 'Properties' section with 'Name' set to 'LACP_ACTIVE' and 'Mode' set to 'LACP Active' (highlighted with a red box). A yellow callout box labeled 'Name 설정' points to the Name field. Another yellow callout box labeled 'LACP Mode 설정' points to the Mode field. Below these are 'Control' settings: Fast Select Hot Standby Ports (checked), Graceful Convergence (checked), Load Defer Member Ports (unchecked), and Suspend Individual Port (checked). Buttons for 'CHECK ALL' and 'UNCHECK ALL' are present. At the bottom, 'Minimum Number of Links' is set to 1 (Not Applicable for FEX PC/VPC) and 'Maximum Number of Links' is set to 16 (Not Applicable for FEX PC/VPC). At the very bottom are buttons for 'SHOW USAGE', 'SUBMIT' (highlighted with a blue box), and 'RESET'.

VPC Switch Policies 설정

Fabric > Access Polices > Switch Policies > Policies

- ❖ ① VPC Domain > Create VPC Domain
- ❖ ② Virtual Port Channel default

The screenshot shows two overlapping windows from the Cisco Fabric Manager interface.

Top Window: VPC Domain Policy - VPC_203-204

- Properties:** Name: VPC_203-204, Description: optional, Peer Dead Interval: 200.
- Bottom Window: Virtual Port Channel Security Policy - Virtual Port Channel default**
- Properties:** Description: optional, Pairing Type: explicit, Explicit VPC Protection Groups:
 - Name: VPC_203-204, Domain Policy: VPC_203-204, Switches: DC4_LEAF_203 (203), DC4_LEA..., Logical Pair ID: 1, Virtual IP: 20.0.88.64/32
 - Name: VPC_251-252, Domain Policy: VPC_251-252, Switches: DC6_LEAF_251 (203), DC6_LEA..., Logical Pair ID: 2, Virtual IP: 20.0.88.65/32

Annotations:

- Create VPC Domain > Name : VPC_203-204** ** VPC로 구성 될 해당 LEAF Node ID로 입력
- 앞서 설정한 VPC Domain Policy 적용**
- VPC ID 설정**
- VPC Domain Name 과 동일하게 설정**
- VPC로 구성 될 해당 LEAF Node 선택**

Link Level & PC / VPC Policy 적용

Fabric > Access Polices > Interface Policies > Policy Groups

❖ Policy Groups > Create Policy Groups

- 실제 물리적 인터페이스에 적용 할 Interface Group 설정 (Link Level / LACP / AEP 등)

The screenshot shows the Cisco Fabric Manager interface with the following details:

- AUTO_HOST Policy Group (Left Panel):**
 - Name: AUTO_HOST
 - Description: optional
 - Label: (empty)
 - Link Level Policy: AUTO (highlighted with a yellow box)
 - Attached Entity Profile: AEP_V11-200 (highlighted with a red box)
- VPC49_203-204 Policy Group (Right Panel):**
 - Name: VPC49_203-204
 - Description: optional
 - Link Aggregation Type: Port Channel (highlighted with a blue box)
 - Link Level Policy: 1G_AUTO (highlighted with a red box)
 - Port Channel Policy: LACP_ACTIVE (highlighted with a red box)
 - Attached Entity Profile: AEP_V11-200 (highlighted with a red box)

Annotations in Korean:

- 설정 한 Link Level Policy 적용** (Applied Link Level Policy settings) - Points to the AUTO_HOST panel.
- VPC Name 설정 시 Port Number 및 LEAF Number 까지 입력해주는 것이 향후 Interface 확인 시 좋음
ex) VPC49_203-204
- 49 : Port Number
- 203-204 : LEAF Number** - Points to the VPC49_203-204 panel.
- LACP 적용** (LACP applied) - Points to the VPC49_203-204 panel.

Interface Profile 적용

Fabric > Access Polices > Interface Policies > Profiles

- Profiles > Create Profiles > 1) LEAF_203 Node Profiles 생성
2) LEAF_203의 Interface Port Profiles 생성

The screenshot shows the Cisco ACI interface with the following details:

- Left Panel (Fabric View):** Shows a list of nodes: FEX_101, FEX_102, FEX_103, FEX_104, LEAF_203, and many LEAF_203-1-XX entries. A yellow box highlights "LEAF Node Profile 생성".
- Top Navigation:** Fabric (highlighted), VM Networking, L4-L7 Services, Admin, Operations.
- Sub-Menu:** Inventory > Fabric Policies > Access Policies.
- Current View:** Access Port Selector - LEAF_203-1-01.
- Properties Panel:** Name: LEAF_203-1-01, Description: optional, Type: range, Policy Group: 1G_HOST, Port Blocks: Interfaces 1/1.
- Create Access Port Selector Dialog:**
 - Name: LEAF203-1-01 (highlighted).
 - Description: optional.
 - Interface ID: 1/1 (highlighted).
 - Connected To Fex:
 - Interface Policy Group: select an option (highlighted).
- Buttons at the bottom:** SUBMIT and CANCEL.

Annotations in yellow boxes:

- LEAF Node Profile 생성 (Left Panel)
- Interface Port Number로 정의 (Create Access Port Selector Dialog, pointing to Name field)
- Interface Port Number 할당 (Create Access Port Selector Dialog, pointing to Interface ID field)
- Policy Group 정의 - 앞서 설정한 Policy Group 할당 (Create Access Port Selector Dialog, pointing to Interface Policy Group dropdown)

Switch Profile 적용

Fabric > Access Polices > Switch Policies > Profiles

- Profiles > Create Profiles > 1) Switch Selectors > Name : LEAF_203 > Blocks : 203
- 2) Associated Interface Selector Profiles > Name : LEAF_203

The screenshot shows the Cisco ACI WebUI interface for creating a Switch Profile named "LEAF_203". The top navigation bar includes tabs for System, Tenants, Fabric (highlighted with a red box), VM Networking, L4-L7 Services, Admin, and Operations. Below the navigation is a search bar and user information. The main content area is titled "Switch Profile - LEAF_203".
Properties: The profile is named "LEAF_203" and has an optional description.
Switch Selectors: One selector is defined with the name "LEAF_203" and block "203".
Associated Interface Selector Profiles: One profile is listed with the name "LEAF_203" and state "formed".
Associated Module Selector Profiles: No items have been found.
At the bottom are buttons for SHOW USAGE, SUBMIT, and RESET.

FEX 연동

Fabric > Access Policies > Interface Policies > Profiles

- ❖ ① Profiles > Create FEX Associate
- ❖ ② Profiles > FEX 연결 된 LEAF에 Interface 정의

The screenshot shows the Cisco Application Policy Infrastructure Controller (APIC) web interface. The top navigation bar includes tabs for System, Tenants, Fabric (highlighted with a red box), VM Networking, L4-L7 Services, Admin, and Operations. The URL in the address bar is https://10.210.9.11/#cd|uni/infra/acccportprof-LEAF_203.

The left sidebar lists various FEX profiles under the 'Fabric' category, with 'FEX_101' highlighted (red box). The main content area displays the 'Create Access Port Selector' dialog box.

① FEX Profile 생성: The 'Name' field is set to 'LEAF203-1-01'. A note below states: 'FEX 연결 된 Interface Port Name 지정' (Specify the selector identity).

② FEX 연결 된 Interface Port 정의: The 'Description' field is set to 'optional'. The 'Interface IDs' field contains '1/1'. A note below states: 'FEX 연결 된 Interface Port 지정' (Specify the selector identity).

Connected To Fex: FEX Profile: FEX_101 FEX ID: 101

A callout box points to the 'Connected To Fex' section with the text: '1. FEX Name 설정
2. FEX ID 설정 (101 ~ 164 까지 가능)'.

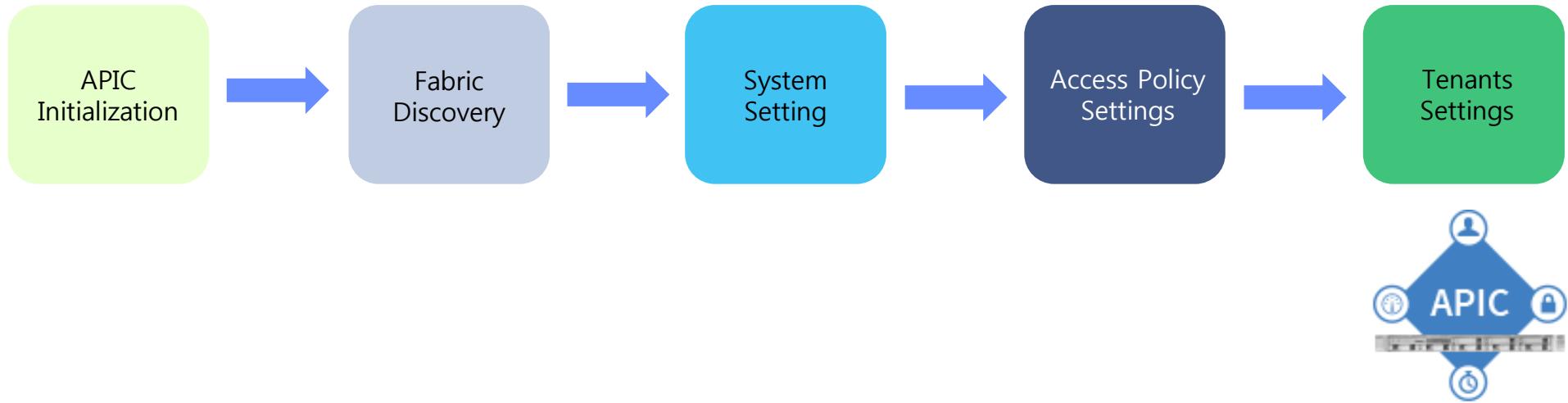
At the bottom of the dialog, a note says: '※ 현재 Single-Home 방식만 지원 됨'.

The right side of the interface shows a list of 'Policy Group' entries, all labeled '1G_HOST'.

At the bottom of the page, there are buttons for 'SHOW USAGE', 'SUBMIT', and 'RESET', along with a timestamp: 'Current System Time: 2016-06-30T16:50 +00:00'.

5) Tenants Setting

- Tenant / VRF / BD / EPG 설정 방법 (External L3 Routed 및 Contract 포함)



Tenants 설정

Tenants

❖ Tenants > ACTIONS > Create Tenant

The screenshot shows the Cisco Application Centric Infrastructure (ACI) web interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, and Operations. The Tenants tab is selected. On the left, a sidebar titled 'All Tenants' lists existing tenants: common, DC_TENANT, infra, mgmt, and SPAN_TENANT. The main content area displays a 'Create Tenant' dialog box. The 'Name' field is populated with 'DC_TENANT'. The 'Description' field is labeled 'optional'. The 'Tags' field contains 'enter tags separated by comma'. The 'Monitoring Policy' dropdown is set to 'select a value'. The 'Security Domains' section shows a table with columns 'Select', 'Name', and 'Description', which is currently empty. Below these fields are 'VRF Name' (optional) and a checked checkbox for 'Take me to this tenant when I click finish'. At the bottom of the dialog are 'SUBMIT' and 'CANCEL' buttons, with 'SUBMIT' highlighted with a red box. To the right of the dialog, there is a 'Health Score' table with five rows, each showing a green box with the value '100'. The top right corner of the screen shows 'Advanced Mode' and user information 'welcome, admin'. The bottom of the page includes navigation icons, a page number 'Page 1 Of 1', an 'Objects Per Page' dropdown set to '15', and a footer note 'Displaying Objects 1 - 5 Of 5'.

VRF 설정

Tenants > 해당 TENANT > Networking > VRFs

❖ VRFs > Create VRF

The screenshot shows the 'Create VRF' interface on a Cisco networking device. The left sidebar lists tenants and various networking profiles. The main window is titled 'Create VRF' and is currently at 'STEP 1 > VRF'. It prompts for 'Specify Tenant VRF' with fields for Name (set to 'DC_VRF1'), Description (optional), Policy Control Enforcement Preference (Enforced), Policy Control Enforcement Direction (Egress), End Point Retention Policy (select a value), Monitoring Policy (select a value), DNS Labels (empty), Route Tag Policy (select a value), and checkboxes for creating a Bridge Domain and configuring BGP, OSPF, and EIGRP policies. A yellow callout box points to the 'NEXT' button at the bottom right, with Korean text explaining that after pressing 'NEXT', a separate step will be required to create the Bridge Domain.

NEXT 이후 Bridge Domain 생성은
별도로 생성 할 것 이므로 Submit 클릭

PREVIOUS NEXT CANCEL

BD (Bridge Domain) 설정(1)

Tenants > 해당 TENANT > Networking > Bridge Domains

❖ Bridge Domains > Create Bridge Domains

- Interface VLAN 을 만드는 것과 같음 (하나의 Broadcast Domain)

The screenshot shows the 'Create Bridge Domain' wizard in the Cisco ACI interface. The left sidebar shows the tenant structure under 'Tenants'. The main window is titled 'Create Bridge Domain' and is on 'STEP 1 > Main'. It asks to 'Specify Bridge Domain for the VRF'. The configuration fields are as follows:

- Name:** WT_BD (highlighted with a red box) BD Name 정의
- Description:** optional
- VRF:** DC_TENANT/DC_VRF1 (highlighted with a red box) VRF 정의
- Forwarding:** optimize
- End Point Retention Policy:** default (highlighted with a red box) default 설정
- IGMP Snoop Policy:** IGMP_SNOOP (highlighted with a red box) Multicast 사용 시 IGMP_SNOOP 정의

The right side of the interface shows a table of existing Bridge Domains with columns: Flooding, Unicast Routing, and Description. The table shows three entries, all with 'True' in the Flooding column.

BD (Bridge Domain) 설정(2)

Tenants > 해당 TENANT > Networking > Bridge Domains

❖ Bridge Domains > Create Bridge Domains

- Interface VLAN 을 만드는 것과 같음 (하나의 Broadcast Domain)

The screenshot shows the Cisco ACI configuration interface for creating a Bridge Domain (BD). The main window displays the 'STEP 2 > L3 Configurations' screen, which includes settings for Unicast Routing, ARP Flooding, and Subnets. A red box highlights the '+ Add' button under 'Subnets'. An arrow points from this button to a 'Create Subnet' dialog box on the right, which is also highlighted with a red border. The 'Create Subnet' dialog box contains fields for Gateway IP (10.192.53.1/24), Scope (Private to VRF, Advertised Externally checked), and Description (optional). The 'OK' button is also highlighted with a red box. Another red box highlights the '+ Add' button under 'Associated L3 Outs', which points to a smaller 'Associated L3 Outs' dialog box at the bottom right. This dialog box shows an entry for 'L3 Out' with the value 'DC_TENANT/L3OUT_BB' and an 'UPDATE' button highlighted with a red box.

EPG (End-Point Group) 설정(1)

Tenants > 해당 TENANT > Application Profiles

- ❖ ① Application Profiles > Create Application Profile
- ❖ ② Application Profiles > 해당 Application Profile > Application EPGs > Create Application EPG
- ❖ ③ Application Profiles > 해당 Application Profile > Application EPGs > 해당 EPG > Domains > Add Physical Domain Association

The screenshot displays the Cisco Application Centric Infrastructure (ACI) graphical user interface across three panels, each with a circled number indicating the step:

- Panel 1 (Top Left):** Shows the "Create Application Profile" dialog. The "Name" field is set to "DC_AP". A red box highlights the "Name" field, and the text "Application Profiles Name 설정" (Application Profiles Name Setting) is overlaid. The "SUBMIT" button is highlighted with a red box.
- Panel 2 (Top Right):** Shows the "Create Application EPG" dialog, specifically "STEP 1 > Identity". The "Name" field is set to "WT_EPG". A red box highlights the "Name" field, and the text "EPG Name 설정" (EPG Name Setting) is overlaid. The "Bridge Domains" dropdown is set to "DC_TENANT/WT_BD". A red box highlights this dropdown, and the text "해당 EPG의 BD 할당" (Assignment of this EPG's BD) is overlaid. The "FINISH" button is highlighted with a red box.
- Panel 3 (Bottom):** Shows the "Domains (VMs and Bare-Metals)" list and the "Add Physical Domain Association" dialog. The "Physical Domain" dropdown is set to "PD_V11-209". A red box highlights this dropdown, and the text "Physical Domain 할당" (Physical Domain Assignment) is overlaid. The "SUBMIT" button is highlighted with a red box.

EPG (End-Point Group) 설정(2)

Tenants > 해당 TENANT > Application Profiles

- ❖ ④ Application Profiles > 해당 Application Profile > Application EPGs > 해당 EPG > Static Bindings(Paths) > Deploy Static EPG On PC, VPC, Or Interface

L3OUT 설정(1)

Tenants > 해당 TENANT > Networking > External Routed Networks

❖ External Routed Networks > Create Routed Outside

STEP 1 > Identity

1. Identity 2. External EPG Networks

Define the Routed Outside

Name: **L3OUT_BB**

Description: optional

BGP **OSPF** EIGRP

OSPF Area ID: **0**

OSPF Area Control:

- Send redistributed LSAs into NSSA area
- Originate summary LSA
- Suppress forwarding address in translated LSA

OSPF Area Type: **NSSA area** **Regular area** **Stub area**

OSPF Area Cost: 1

Route Control Enforcement: Import Export

Target DSCP: unspecified

VRF: **DC_TENANT/DC_VRF1**

External Routed Domain: **L3OUT_ROUTED** 앞서 설정한 AEP L3 OUT Domain

Route Profile for Interleaf: select a value

Route Control For Dampening:

Address Family Type	Route Dampening Policy

Nodes And Interfaces Protocol Profiles

Name	Description	DSCP	Nodes

PREVIOUS **NEXT** CANCEL

Displaying Objects 1 - 1 Of 1

Actions

Advanced Mode
welcome, admin *

일반적인 OSPF 설정

다음 슬라이드

L3OUT 설정(2)

Tenants > 해당 TENANT > Networking > External Routed Networks

❖ External Routed Networks > Create Routed Outside > Nodes And Interfaces Protocol Profiles (Create Node Profile)

The screenshot shows two overlapping windows from the Cisco ACI GUI.

Create Node Profile Window:

- Name:** L3OUT_EXT_LEAF_2p1 (highlighted with a red box)
- Description:** optional
- Target DSCP:** unspecified
- Nodes:** A table with columns: Node ID, Router ID, State, Routes, Loopback Address. An empty row is shown with a red plus sign button to its right.
- OSPF Interface Profiles:** A table with columns: Name, Description, Interfaces, OSPF Policy. An empty row is shown with a red plus sign button to its right.
- Buttons:** OK, CANCEL, PREVIOUS, NEXT, and a red-highlighted CANCEL button at the bottom left of the modal.

Select Node Window:

- Select Node and Configure Static Routes:**
- Node ID:** topology/pod-1/node-201 (highlighted with a red box)
- Router ID:** 1.1.1.1 (highlighted with a red box)
- Use Router ID as Loopback Address:**
- Loopback Addresses:** IP: 1.1.1.1
- Static Routes:** IP Address: _____, Next Hop IP: _____
- Buttons:** OK, CANCEL

Annotations in red text:

- L3OUT으로 연결 될 LEAF Name 지정
- 다음 슬라이드 +
- 해당 LEAF 선택 및 Loopback IP 지정

L3OUT 설정(3)

Tenants > 해당 TENANT > Networking > External Routed Networks

- External Routed Networks > Create Routed Outside > Nodes And Interfaces Protocol Profiles (Create Node Profile) > OSPF Interface Profile

The screenshot shows the APIC (10.210.9.11) interface. On the left, the navigation tree includes Tenant DC_TENANT, Application Profiles, Networking, Bridge Domains, VRFs, External Bridged Networks, and External Routed Networks. The 'External Routed Networks' node is selected.

The main window displays the 'Create Interface Profile' dialog. In the 'Specify the Interface Profile' section, the 'Name' field is set to 'L3OUT_LEAF_201-1-01'. A red box highlights this field with the text 'L3OUT으로 연결 될 LEAF Interface Name 지정' (Specify the Interface Name to be connected to L3OUT).

In the 'OSPF Profile' section, the 'OSPF Policy' dropdown is set to 'OSPF_P2P_COST1'. A red box highlights this field with the text '※ P2P 구성이 아닐 시 설정 안함' (Not applicable if not configured as P2P).

A red arrow points from the 'OSPF Policy' field in the main dialog to the 'OSPF Interface Policy - OSPF_P2P_COST1' configuration dialog on the right.

The 'OSPF Interface Policy - OSPF_P2P_COST1' dialog shows the 'Properties' section. The 'Name' field is 'OSPF_P2P_COST1'. The 'Network Type' dropdown is set to 'Point-to-point'. A red box highlights this field with the text 'OSPF Point-to-Point Policy 설정' (Configure OSPF Point-to-Point Policy). The 'Priority' is set to 1. The 'Cost of Interface' is 1. The 'Interface Controls' section contains several checkboxes: 'Advertise subnet', 'BFD', 'MTU ignore', and 'Passive participation'. Buttons for 'CHECK ALL' and 'UNCHECK ALL' are present. The 'Hello Interval (sec)' is 10, 'Dead Interval (sec)' is 40, and 'Retransmit Interval (sec)' is 5.

At the bottom right of the configuration dialog, there are 'SHOW USAGE', 'SUBMIT', and 'CLOSE' buttons. The 'CLOSE' button is highlighted with a red box.

L3OUT 설정(4)

Tenants > 해당 TENANT > Networking > External Routed Networks

❖ External Routed Networks > Create Routed Outside > Nodes And Interfaces Protocol Profiles (Create Node Profile) > Routed Interfaces

The screenshot shows the APIC (Application Policy Infrastructure Controller) interface. On the left, the navigation tree includes System, Tenant, Application Profiles, DC_AP, Networking, Bridge Domains, VRFs, External Bridged Networks, and External Routed Networks. The External Routed Networks node is selected.

The main window displays the "Create Interface Profile" dialog. In the "Specify the Interface Profile" section, the Name is set to "L3OUT_LEAF_201-1-01" and the Description is "optional". Under OSPF Profile, the Authentication Type is "No authentication" and the OSPF Policy is "OSPF_P2P_COST". Under BFD Interface Profile, the Authentication Type is "No authentication" and the BFD Interface Policy is "select a value".

On the right, a modal dialog titled "Select Routed Interface" is open. It shows the "Specify the Interface" section with the path "topology/pod-1/paths-201/pathep-1". The IPv4 Primary / IPv6 Preferred Address is "2.2.2.2/30". A red box highlights this address with the text "L3 구간 IP 설정" (L3 Segment IP Configuration). Below it, the MTU (bytes) is set to "1500" with a red box and the text "MTU 설정" (MTU Configuration). The "OK" button at the bottom right of the modal is also highlighted with a red box.

L3OUT 설정(5)

Tenants > 해당 TENANT > Networking > External Routed Networks

❖ 설정 완료 확인(1)

The screenshot shows the Cisco ACI Network Controller interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, and Operations. The Tenant section shows "ALL TENANTS | Add Tenant | Search enter name, descr" and a search bar. The main content area is titled "Logical Interface Profile - L3OUT_201-1-25".
The left sidebar shows the tenant structure: Tenant DC_TENANT, Application Profiles (DC_AP), Networking (Bridge Domains: FC_GPDB_BD, MASK_BD, WT_BD; VRFs, External Bridged Networks, External Routed Networks, Set Action Rule Profiles, Match Action Rule Profiles), L3OUT_BB (Logical Node Profiles: L3OUT_EXT_LEAF_201, Logical Interface Profiles: L3OUT_201-1-25, L3OUT_201-1-26), Configured Nodes (L3OUT_EXT_LEAF_202), Networks, Route Profiles, Route Profiles, Protocol Policies, L4-L7 Service Parameters, and Security Policies.
The main panel displays the "Properties" for the selected L3OUT profile:

- Name: L3OUT_201-1-25
- Description: optional
- Label:
- ND policy: select a value
- Egress Data Plane Policing Policy: select a value
- Ingress Data Plane Policing Policy: select a value

The "Routed Interfaces" table lists one entry:

Path	IP Address	MAC Address	MTU (Bytes)
Node-201/eth1/25	10.201.242.22/30	00:22:BD:F8:19:FF	1500

The "SVI" table is empty, displaying the message: "No items have been found. Select Actions to create a new item."

At the bottom right are buttons for SHOW USAGE, SUBMIT, and RESET.

L3OUT 설정(6)

Tenants > 해당 TENANT > Networking > External Routed Networks

❖ 설정 완료 확인(2)

The screenshot shows the Cisco ACI Network Controller interface. The top navigation bar includes System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and Advanced Mode (welcome, admin). The main menu on the left is under Tenant DC_TENANT, with sections like Application Profiles, Networking, VRFs, External Bridged Networks, External Routed Networks, and L3OUT_BB. The current view is OSPF - DC_TENANT:DC_VRF1. The properties section shows Name: DC_TENANT:DC_VRF1, Route ID: 10.201.1.182, Distance: 110, Max ECMP: 8, Bandwidth Reference: 40000 (Mbps), and Operational State: Up. The stats section provides detailed information about interfaces, active areas, stub areas, and ext areas. The neighbors section lists two entries: 10.201.1.1 and 10.201.1.2, both in Full state. The inter protocol route leak section shows three entries: DC_TENANT:DC_VRF1 (BGP, exp-ctx-proto-2686977, Inter protocol leak, Asn 65011), DC_TENANT:DC_VRF1 (Direct, exp-ctx-st-2686977, Inter protocol leak, Asn 1), and DC_TENANT:DC_VRF1 (EIGRP, exp-ctx-proto-2686977, Inter protocol leak, Asn 1).

Name	Redistribution Protocol	Route Map	Scope	Asn
DC_TENANT:DC_VRF1	BGP	exp-ctx-proto-2686977	Inter protocol leak	65011
DC_TENANT:DC_VRF1	Direct	exp-ctx-st-2686977	Inter protocol leak	1
DC_TENANT:DC_VRF1	EIGRP	exp-ctx-proto-2686977	Inter protocol leak	1

Contract 설정 – Networks (Subnet)

Tenants > 해당 TENANT > Networking > External Routed Networks

- ❖ ① External Routed Networks > L3OUT_BB (앞서 생성했던 Policy) > Networks > Create External Network
- ❖ ② External Routed Networks > L3OUT_BB (앞서 생성했던 Policy) > Networks > Create External Network > Subnet

The screenshot shows the Cisco ACI Network Controller interface. On the left, the navigation pane is open for Tenant DC_TENANT, showing various profiles and domains. The main area displays the 'Networks' tab under 'External Routed Networks'. Two windows are overlaid on the interface:

- Create External Network (Left Window):** A modal window titled 'Create External Network'. It has fields for 'Name' (set to 'L3OUT_INTERNET'), 'Tags' (empty), 'QoS class' (Unspecified), 'Description' (Optional), and 'Target DSCP' (unspecified). Below this is a 'Subnet' table with a single row. The 'IP Address' column contains '0.0.0.0/0'. A red circle labeled '1' highlights the 'Name' field, and a red box highlights the '0.0.0.0/0' entry in the table. Buttons at the bottom are 'SUBMIT' and 'CANCEL'.
- Create Subnet (Right Window):** A modal window titled 'Create Subnet'. It has a message: '0.0.0.0/0은 외부로 가는 모든 IP에 대한 것을 의미 ex) 10.0.0.0/8, 177.98.0.0/16 등 설정 가능'. It includes fields for 'IP Address' (0.0.0.0/0), 'Scope' (checkboxes for Export Route Control Subnet, Import Route Control Subnet, External Subnets for the External EPG, Shared Route Control Subnet, Shared Security Import Subnet), 'OSPF Route Summarization Policy' (dropdown), 'aggregate' (checkboxes for Aggregate Export, Aggregate Import, Aggregate Shared Routes), and 'Route Control Profile' (table with columns Name and Direction). Buttons at the bottom are 'OK' and 'CANCEL'.

Contract 설정 – Provided / Consumed

Tenants > 해당 TENANT > Application Profiles > DC_AP > Application EPGs > EPG

- ❖ 해당 EPG > Contracts > Add Provided Contract
- ❖ 해당 EPG > Contracts > Add Consumed Contract

The screenshot shows the Cisco ACI UI interface for managing contracts. On the left, the navigation tree shows the tenant structure: Tenant DC_TENANT > Application Profiles > DC_AP > Application EPGs > EPG WT_EPG. A red box highlights the 'Contracts' link under EPG WT_EPG. On the right, the 'Contracts' list page displays four contracts. A red box highlights the third row, 'DC_TENANT IP_ALL Contract Provided Unspecified formed'. A red arrow points from this row to the 'Add Provided Contract' button in a modal dialog. The modal dialog, titled 'Add Provided Contract', contains fields for 'Contract' (set to 'DC_TENANT/IP_ALL'), 'QoS' (set to 'Unspecified'), 'Contract Label', and 'Subject Label'. A red box highlights the 'Contract' field. A red arrow points from the 'Add Provided Contract' button in the modal to the 'Add Provided Contract' button in the main Contracts list page. Below the list, a note in red text reads 'Provided / Consumed Contract 지정' with sub-points '- Provided : 공급자 (WT_EPG 서버)' and '- Consumed : 소비자 (L3_OUT 단말)'. Another note in blue text states '※ Traffic Flow는 역방향' and '★ EPG가 2개 이상 존재 할 시 Provided / Consumed 모두 설정 해야 EPG간 양방향 통신 가능'.

Tenant Name	Contract Name	Contract Type	Provided / Consumed	QoS Class	State	Label	Subject Label
DC_TENANT	HYNIX_IP_ALL	Contract	Provided	Unspecified	formed		
DC_TENANT	HYNIX_IP_ALL	Contract	Consumed	Unspecified	formed		
DC_TENANT	IP_ALL	Contract	Provided	Unspecified	formed		
DC_TENANT	IP_ALL	Contract	Consumed	Unspecified	formed		

Contract 설정 – Filter

Tenants > 해당 TENANT > Security Policies > Filters

❖ Security Policies > Filters > Create Filters

The screenshot shows the Cisco ACI Management interface under the 'Tenants' tab for the 'Tenant DC_TENANT'. On the left navigation bar, 'Security Policies' and 'Filters' are highlighted with red boxes. In the main panel, a filter named 'IP_ALL' is being configured. The 'Properties' section shows the name 'IP_ALL' highlighted with a red box. The 'Entries' table lists two entries: 'IP_ALL' and 'IP', both highlighted with red boxes. A red box also highlights the text '모든 IP에 대하여 Permit' (Permit all IP). At the bottom right, the 'SUBMIT' button is highlighted with a red box.

Properties

Name	EtherType	ARP Flag	IP Protocol	Match Only Fragmen	Stateful	Source Port / Range	Destination Port / Range	TCP Session Rules
IP_ALL	IP		unspecified	False	False	From	To	

모든 IP에 대하여 Permit

SHOW USAGE SUBMIT RESET

Contract 설정 – Contracts 정의

Tenants > 해당 TENANT > Security Policies > Contracts

❖ Security Policies > Contracts > Create Contract

The screenshot shows the Cisco ACI UI interface for creating a new contract. The main window is titled "Create Contract" under "Specify Identity Of Contract". The "Name" field is set to "IP_ALL" and the "Scope" is "VRF". A red box highlights the "Name" field. A red arrow points from this field to the "Name" field in the "Create Contract Subject" dialog box, which is also labeled "IP_ALL". Another red box highlights the "Name" field in the "Create Contract Subject" dialog. Below the "Name" field in the "Create Contract Subject" dialog, there is a note: "Filter Name 정의" (Filter Name Definition). In the "Filter Chain" section of the "Create Contract Subject" dialog, the filter "DO_TENANT/IP_ALL" is listed, with a note: "앞서 정의한 Filter 적용" (Apply previous defined Filter). The "UPDATE" button in the "Filters" dialog is highlighted with a red box.

CISCO System Tenants Fabric VM Networking L4-L7 Services Admin Operations Advanced Model welcome, admin Tenant DC_TENANT ALL TENANT | Add Tenant | Search | comm | config | device | policy | right | SPAN_TENANT Tenant DC_TENANT Quick Start Tenant DC_TENANT Application Profiles DC_AP Application EPGs EPG FC_GPDB_EPG EPG MASK_EPG EPG WT_EPG uSeq EPGs L4-L7 Service Parameters Networking L4-L7 Service Parameters Security Policies Contracts HYNIX_IP_ALL VRF IP_ALL VRF QoS Class: Unspecified Target DSCP: unspecified Description: optional Subjects: Name Description + SUBMIT CANCEL

Create Contract Specify Identity Of Contract Name: IP_ALL Scope: VRF QoS Class: Unspecified Target DSCP: unspecified Description: optional Subjects: Name Description + SUBMIT CANCEL

Create Contract Subject Specify Identity Of Subject Name: IP_ALL Description: optional Target DSCP: unspecified Apply Both Directions: Reverse Filter Ports: 양방향 Filter 적용 Filter Chain Filters Name: DO_TENANT/IP_ALL 앞서 정의한 Filter 적용 UPDATE CANCEL

L4-L7 SERVICE GRAPH Service Graph: select an option PRIORITY QoS: OK CANCEL

L4 연동 시 Static MAC 설정

Tenants > 해당 TENANT > Application Profiles > 해당 AP > Application EPGs > 해당 EPG > Static EndPoint

❖ Static EndPoint > Create Static EndPoint

The screenshot shows the Cisco Application Centric Infrastructure (ACI) User Interface. The top navigation bar has tabs: System, Tenants (highlighted with a red box), Fabric, VM Networking, L4-L7 Services, Admin, and Operations. Below the navigation is a search bar with placeholder text 'enter name, descr' and a dropdown menu showing 'DC_TENANT'. The main content area is titled 'Static EndPoint'.

Create Static EndPoint dialog box:

- Specify the Static EndPoint** section:
 - MAC: (L4 Virtual MAC 입력)
 - Type:
 - Path Type: Port (L4 연결된 Port 지정)
 - Path: (Node ID/Card ID/Port ID Example: Node-17/eth1/6)
 - IP Address:
 - Encap: (해당 VLAN 설정)
 - Additional IP Address: (추가적인 서비스 IP 지정)
- Buttons: UPDATE, CANCEL, SUBMIT (highlighted with a red box).

Properties panel (right side):

- Properties:
 - MAC: 00:00:5E:00:01:46
 - Type: silent-host
 - Path: topology/pod-1/paths-207/pathp-[eth1/44]
 - IP Address: 10.192.70.33
 - Encap: vlan-70
e.g., vlan-1
- Additional IP Address:
 - IP: 10.192.70.36
 - IP: 10.192.70.39

Message: 설정 완료 화면 (Setup Complete Screen)

Buttons: SHOW USAGE, SUBMIT, CLOSE (highlighted with a red box).



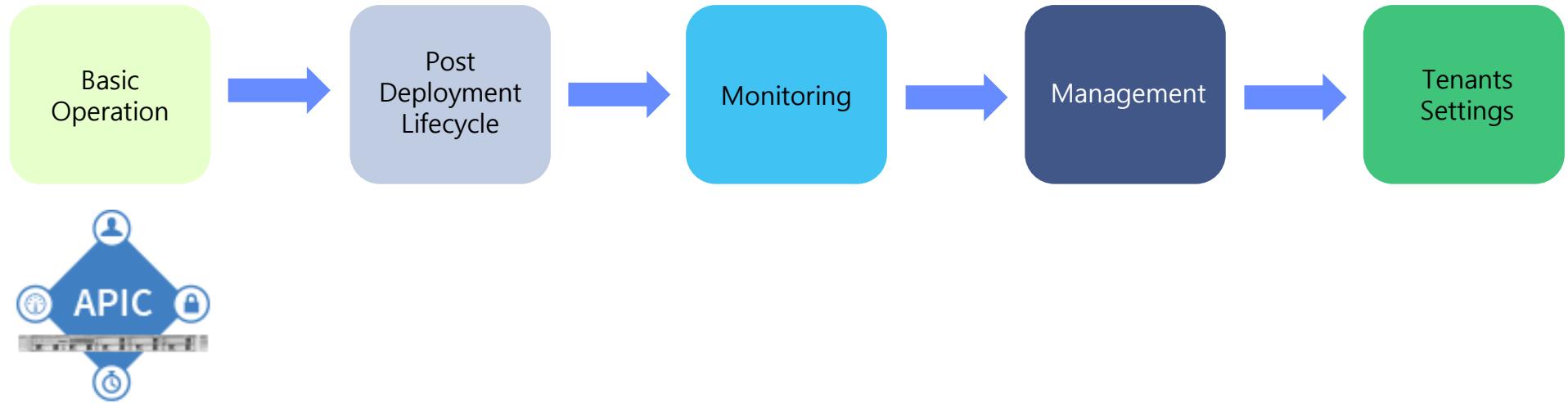
Agenda

1. Configuration Guide

2. Operation Guide



1) Basic Operation



1. Basic Operation > 1.1 Controller Status

Controller Topology

❖ System > Controllers
 > Controllers

CISCO System Tenants Fabric VM Networking L4-L7 Services Admin Operations Advanced Mode welcome, admin -

QuickStart | Dashboard | Controllers | Faults | Config Zones

Controllers

- Quick Start
- Controllers
- DC_APIC_1 (Node-1)
 - Cluster as Seen by Node
 - Interfaces
 - Storage
 - NTP Details
 - Equipment Fans
 - Power Supply Units
 - Equipment Sensors
 - Processes
- DC_APIC_2 (Node-2)
- Controller Policies

Controllers

DC4_LEAF_203

DC4_LEAF_204

DC_APIC_1

DC_APIC_2

DC_APIC_3

Cluster Health

ID	Name	IP	Admin State	Operational State	Health State
1	DC_APIC_1	20.0.0.1	In Service	Available	Fully Fit
2	DC_APIC_2	20.0.0.2	In Service	Available	Fully Fit
3	DC_APIC_3	20.0.0.3	In Service	Unavailable	Unknown

1. Basic Operation > 1.1 Controller Status (계속)

Cluster status

- ❖ System > Controllers
 - > Controllers > DC_APIC_1 (Node-1) > Cluster as Seen by Node

The screenshot shows the 'Cluster as Seen by Node' page. At the top, it displays the fabric properties: Fabric Name: DC_FABRIC, Target Size: 3, Current Size: 3, and a note about the time difference: Difference Between Local Time and Unified Cluster Time (ms): -25214221. Below this, the 'Controllers' section lists three controllers: DC_APIC_1 (IP 20.0.0.1, Admin State In Service, Operational State Available, Health State Fully Fit), DC_APIC_2 (IP 20.0.0.2, Admin State In Service, Operational State Available, Health State Fully Fit), and DC_APIC_3 (IP 20.0.0.3, Admin State In Service, Operational State Unavailable, Health State Unknown). The 'Unauthorized Controllers' section is empty. At the bottom right are 'SUBMIT' and 'RESET' buttons.

Interface Status

- ❖ System > Controllers
 - > Controllers > DC_APIC_1 (Node-1) > Interfaces

The screenshot shows the 'Interfaces' page. It lists physical interfaces: eth1-1 (IP 20.0.0.1, MTU 1500, MAC 00:C8:8B:9A:49:DE, State up), eth1-2 (IP 20.0.0.2, MTU 1500, MAC 00:C8:8B:9A:49:DE, State down), eth2-1 (IP 20.0.0.3, MTU 1500, MAC 00:C8:8B:43:36:10, State up), and eth2-2 (IP 20.0.0.4, MTU 1500, MAC 00:C8:8B:43:36:10, State up). Below this are aggregated interfaces: bond0 (IP 20.0.0.5, MTU 1500, MAC 00:C8:8B:43:36:10, Associated Physical Interfaces eth2/1, eth2/2, Active Interface eth2/1) and bond1 (IP 20.0.0.6, MTU 1500, MAC 00:C8:8B:9A:49:DE, Associated Physical Interfaces eth1/1, eth1/2, Active Interface eth1/1). At the bottom right are 'Member Port' and 'Active I/F' buttons.

1. Basic Operation > 1.1 Controller Status (계속)

Storage Status

- ❖ System > Controllers
 - > Controllers > DC_APIC_1 (Node-1)
 - > Storage

Storage

Mount Point	File System	Utilized (Percentage)	Blocks (KB)	State
/	/dev/dm-1	<div style="width: 37%;">37%</div>	41282880	OK
/boot	/dev/sda1	<div style="width: 8%;">8%</div>	2882592	OK
/data	/dev/mapper/vg_ifc0_ssddata	<div style="width: 3%;">3%</div>	108372960	OK
/data2	/dev/mapper/vg_ifc0-data2	<div style="width: 1%;">1%</div>	619273992	OK
/data/log	tmpfs	<div style="width: 22%;">22%</div>	2097152	OK
/data/shell-data	tmpfs	<div style="width: 1%;">1%</div>	1048576	OK
/dev/sda	/dev/sda	<div style="width: 0%;">0%</div>	Unspecified	OK
/dev/shm	tmpfs	<div style="width: 2%;">2%</div>	4194304	OK
/dmecores	/dev/mapper/vg_ifc0-dmecores	<div style="width: 1%;">1%</div>	51606140	OK
/efiboot	/dev/sda2	<div style="width: 7%;">7%</div>	1948944	OK
/firmware	/dev/mapper/vg_ifc0-firmware	<div style="width: 22%;">22%</div>	41284928	OK
/logs	/dev/mapper/vg_ifc0-logs	<div style="width: 3%;">3%</div>	41284928	OK
/rfs1	/dev/dm-11	<div style="width: 32%;">32%</div>	41282880	OK
/rfs2	/dev/dm-11	<div style="width: 37%;">37%</div>	41282880	OK
/scratch	/dev/mapper/vg_ifc0-scratch	<div style="width: 1%;">1%</div>	41284928	OK
/securedata	/dev/dm-12	<div style="width: 3%;">3%</div>	2062160	OK
/techsupport	/dev/mapper/vg_ifc0-techsup...	<div style="width: 1%;">1%</div>	41284928	OK
/tmp	tmpfs	<div style="width: 1%;">1%</div>	65878208	OK
/tmp/bootflash	/dev/sdc1	<div style="width: 10%;">10%</div>	59493	OK
/tmp/flashenc	/dev/mapper/123456	<div style="width: 3%;">3%</div>	3780600	OK

Process Status

- ❖ System > Controllers
 - > Controllers > DC_APIC_1 (Node-1)
 - > Processes

All Processes



1. Basic Operation > 1.2 Spine & Leaf Status

Node Status (Chassis)

❖ Fabric > Inventory

> Pod1 > DC4_SPINE_101 (Node-101)

> Chassis > Supervisor Modules / Line Module / Fabric Modules / Fan Trays / Power supply / System Controller Module

Inventory

- Quick Start
- Topology
- Pod 1
 - DC4_EXT_LEAF_201 (Node-201)
 - DC4_EXT_LEAF_202 (Node-202)
 - DC4_LEAF_203 (Node-203)
 - DC4_LEAF_204 (Node-204)
 - DC4_LEAF_205 (Node-205)
 - DC4_LEAF_206 (Node-206)
 - DC4_SPINE_101 (Node-101)**
 - Supervisor Modules**
 - Line Modules
 - Fabric Modules
 - Fan Trays
 - Power Supply Units
 - System Controller Modules
 - Interfaces
 - Protocols
 - Processes
 - Span Sessions
 - Pools
 - Rules
 - DC4_SPINE_102 (Node-102)- Fabric Membership
- Unmanaged Fabric Nodes
- Unreachable Nodes
- Disabled Interfaces and Decommissioned ...

Supervisor Status

ID	Operational State	Redundancy State	Model	Vendor	Serial
1	Online	Active	N9K-SUP-B	Cisco Systems, Inc.	SAL2007YSLV
2	Online	Standby	N9K-SUP-B	Cisco Systems, Inc.	SAL2007YSNA

Line Module Status

ID	Number Of Ports	Operational State	Redundancy State	Type	Model	Vendor	Serial
1	36	Online	Active	Line card	N9K-X9736PQ	Cisco Systems, Inc.	SAL2012MJPZ

Fabric Module Status

ID	Number Of Ports	Operational State	Redundancy State	Type	Model	Vendor	Serial
1	0	Online	Active	Fabric card	N9K-C9508-FM	Cisco Systems, Inc.	SAL2010ZZJ2
2	0	Online	Active	Fabric card	N9K-C9508-FM	Cisco Systems, Inc.	SAL2010ZZF5
3	0	Online	Active	Fabric card	N9K-C9508-FM	Cisco Systems, Inc.	SAL2010ZZAR
4	0	Online	Active	Fabric card	N9K-C9508-FM	Cisco Systems, Inc.	SAL2010ZZB3
5	0	Online	Active	Fabric card	N9K-C9508-FM	Cisco Systems, Inc.	SAL2007YSR
6	0	Online	Active	Fabric card	N9K-C9508-FM	Cisco Systems, Inc.	SAL2007YSAH

Fan Trays Status

ID	Operational State	Model	Vendor	Serial
1	OK	N9K-C9508-FAN	Cisco	FGE2001004G
2	OK	N9K-C9508-FAN	Cisco	FGE2001001D
3	OK	N9K-C9508-FAN	Cisco	FGE2001002H

Power Supply Status

Slot ID	Capacity (A)	Voltage Source	Voltage (V)	Alarm Reg	Operational State	Model	Vendor	Serial
1	250.000000	220v	12.000000	0	OK	N9K-PAC-3000W-B	Cisco Systems, Inc.	DTM194800CH
2	250.000000	220v	12.000000	0	OK	N9K-PAC-3000W-B	Cisco Systems, Inc.	DTM19480054
3	250.000000	220v	12.000000	0	OK	N9K-PAC-3000W-B	Cisco Systems, Inc.	DTM19480057
4	250.000000	220v	12.000000	0	OK	N9K-PAC-3000W-B	Cisco Systems, Inc.	DTM194800CB

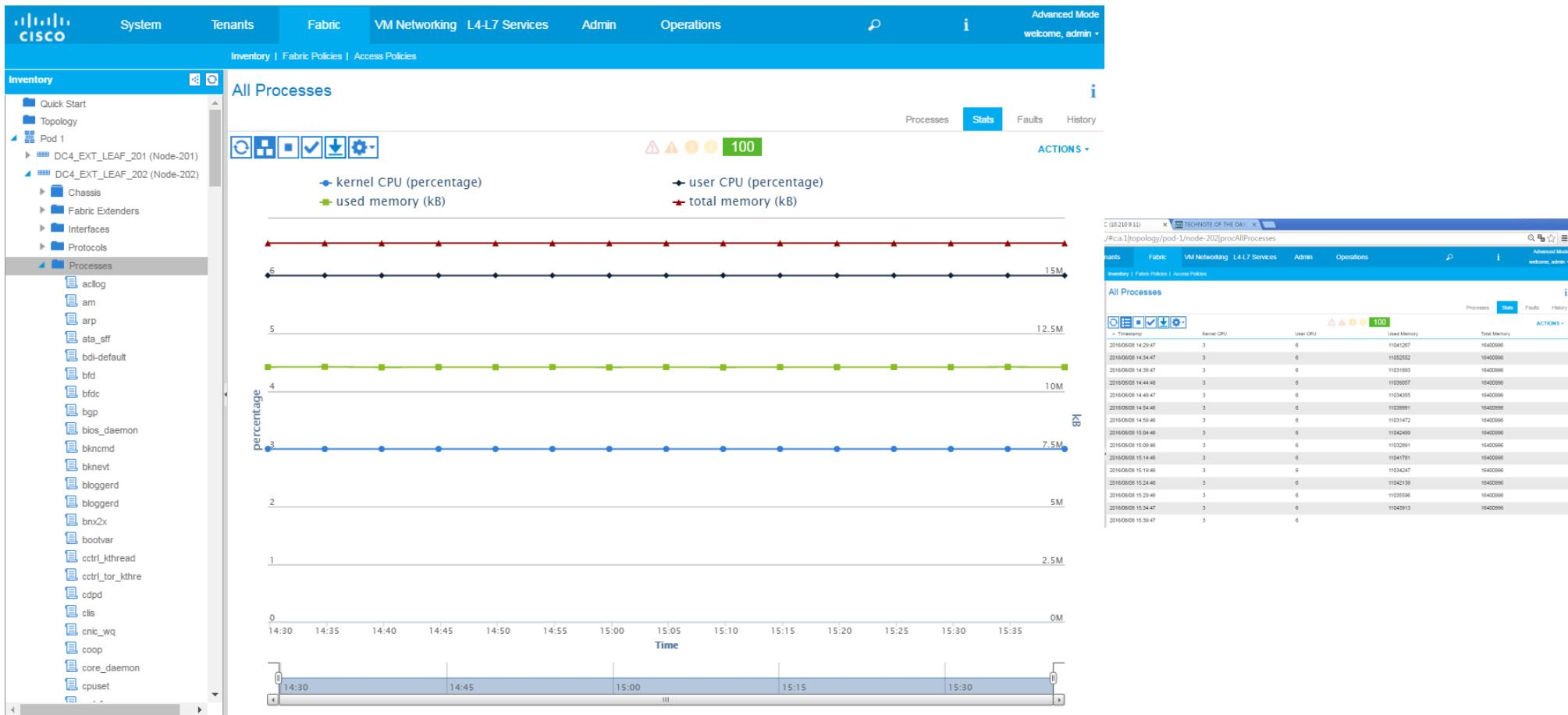
System Controller Status

ID	Number Of Ports	Operational State	Redundancy State	Model	Vendor	Revision	Serial	Type
1	0	Online	Standby	N9K-SC-A	Cisco Systems, Inc.	F0	SAL2006Y5MR	System control card
2	0	Online	Active	N9K-SC-A	Cisco Systems, Inc.	F0	SAL2006Y5LZ	System control card

1. Basic Operation > 1.2 Spine & Leaf Status (계속)

Node Status (Chassis)

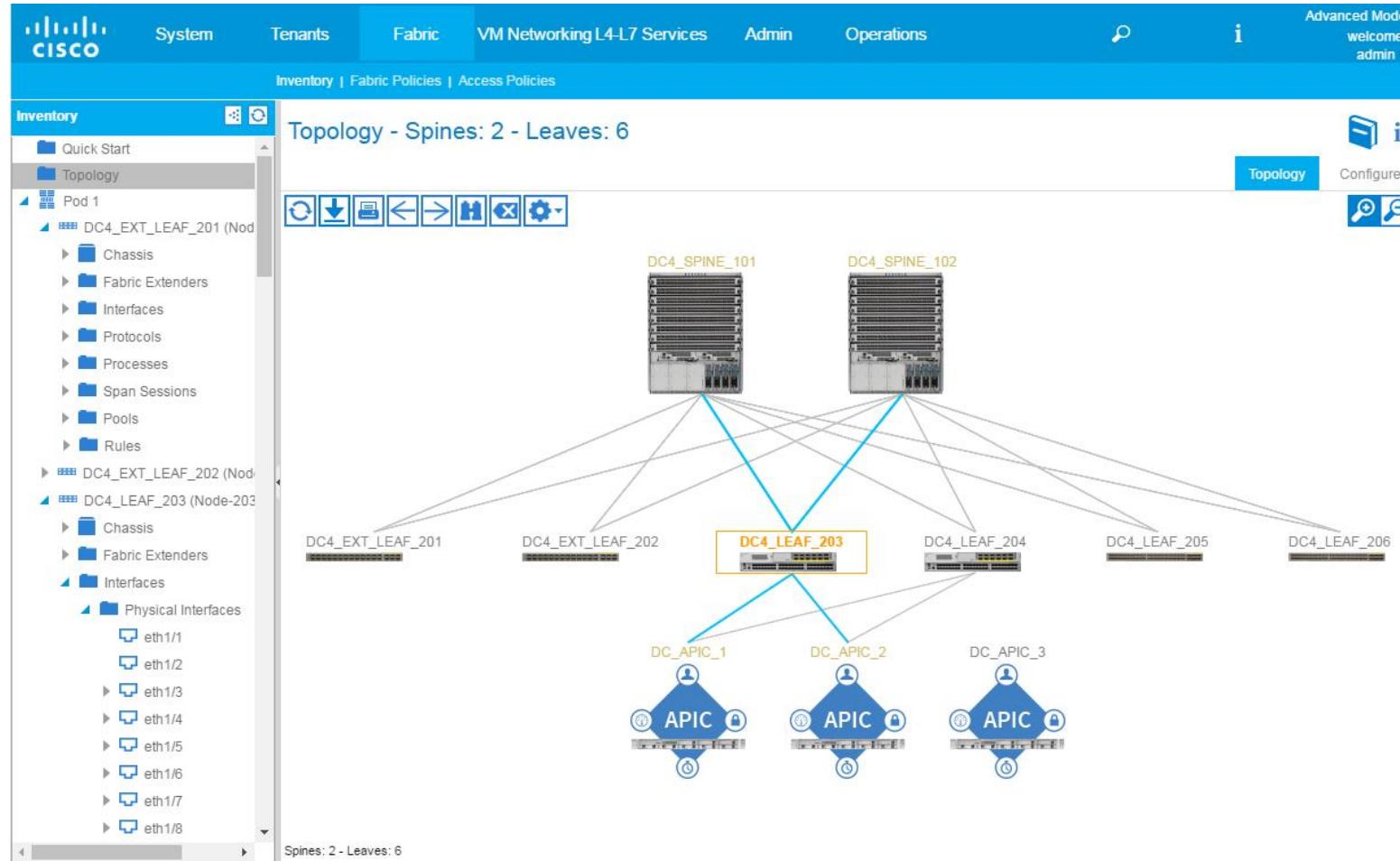
- ❖ Fabric > Inventory
 - > Pod1 > DC4_SPINE_101 (Node-101)
 - > Chassis > Process (CPU & Memory Utilization)



1. Basic Operation > 1.3 Fabric Discovery

Topology 확인

- ❖ Fabric > Inventory
> Topology



1. Basic Operation > 1.3 Fabric Discovery (계속)

Fabric Discovery

- ❖ Fabric > Inventory
> Fabric Membership

The screenshot shows the Cisco Fabric Management interface with the following details:

- Header:** Advanced Mode, welcome, admin.
- Navigation:** System, Tenants, **Fabric**, VM Networking, L4-L7 Services, Admin, Operations.
- Sub-Header:** Inventory | Fabric Policies | Access Policies.
- Left Sidebar (Inventory):**
 - Quick Start
 - Topology
 - Pod 1
 - Fabric Membership** (selected)
 - Unmanaged Fabric Nodes
 - Unreachable Nodes
 - Disabled Interfaces and Decommissioned Switches
- Main Content:** Fabric Membership table.

Serial Number	Node ID	Node Name	Rack Name	Model	Role	IP	Decommissioned	Supported Model	SSL Certificate
SAL1923G78T	201	LEAF_201		N9K-C9372...	leaf	20.0.112.92...	False	True	yes
SAL1922G0F1	202	LEAF_202		N9K-C9372...	leaf	20.0.112.91...	False	True	yes
SAL1934MR76	301	LEAF_301		N9K-C9372...	leaf	20.0.112.90...	False	True	yes
SAL1934MR1X	302	LEAF_302		N9K-C9372...	leaf	20.0.112.95...	False	True	yes
SAL1931LA4J	101	SPINE_101		N9K-C9336...	spine	20.0.112.94...	False	True	yes
SAL1925H0JH	102	SPINE_102		N9K-C9336...	spine	20.0.112.93...	False	True	yes

Annotations in Korean:

- Serial Number와 Node ID가 정상으로 할당되는지 확인
- 장비 Hostname
- 장비 모델과 Role이 정상 인식되는지 확인
- Fabric IP 대역이 정상으로 할당되는지 확인
- 모델이 정상으로 인식되고 SSL certificate인지 확인

1. Basic Operation > 1.3 Fabric Discovery (계속)

Fabric Discovery

❖ Controller CLI ⇒ show switch

ID	Address	In-Band IPv4 Address	In-Band IPv6 Address	OOB IPv4 Address	OOB IPv6 Address	Version	Flags	Serial Number	Name
101	20.0.112.93	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	n9000-11.2(3 c)	-s-v asiv	SAL1931LA4J SAL1925HOJH	SPINE_101 SPINE_102
201	20.0.112.92	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	n9000-11.2(3 c)	aliv	SAL1923G78T	LEAF_201
202	20.0.112.91	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	n9000-11.2(3 c)	aliv	SAL1922G0F1	LEAF_202
301	20.0.112.90	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	n9000-11.2(3 c)	aliv	SAL1934MR76	LEAF_301
302	20.0.112.95	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	n9000-11.2(3 c)	aliv	SAL1934MR1X	LEAF_302

Flags - a:Active | l/s:Leaf/Spine | v:Valid Certificate | i:In-Service

Flag로 장비 상태 확인

```
apic1#
```

1. Basic Operation > 1.3 Fabric Discovery (계속)

Device Discovery Fail 시 확인

1. 다른 Node와 LLDP Neighbor 확인

⇒ show lldp neighbors

```
LEAF_301# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID          Local Intf      Hold-time  Capability  Port ID
apic1            Eth1/1           120          eth2-2
SPINE_102         Eth1/50          120          BR           Eth1/31
Total entries displayed: 2
LEAF_301#
```

2. Neighbor 인식이 안될 경우 Interface와 Link 상태 확인

⇒ show Interface brief

3. Interface와 LLDP가 정상일 경우 DHCP를 통해 IP 할당여부 확인

⇒ show dhcp internal info client

```
LEAF_301# show dhcp internal info client
DHCP client configuration information:
Client intf ID : loopback0
Client intf mode : Pseudo
Client intf adminSt : Enabled
Client request address: 20.0.112.90
Client ID: SAL1934MR76
Client hostname: LEAF_301
Client vendor TLVs:
tlv type: 1 length: 1,    2 tlv type: 6 length: 1,    1
tlv type: 3 length: 2,    1  0
tlv type: 4 length: 4,    2d 1  0  0
tlv type: 7 length: 11,   4e 39 4b 2d 43 39 33 37 32 50 58
```

4. DHCP에서 IP 할당이 정상이고 정상동작 하는지 확인

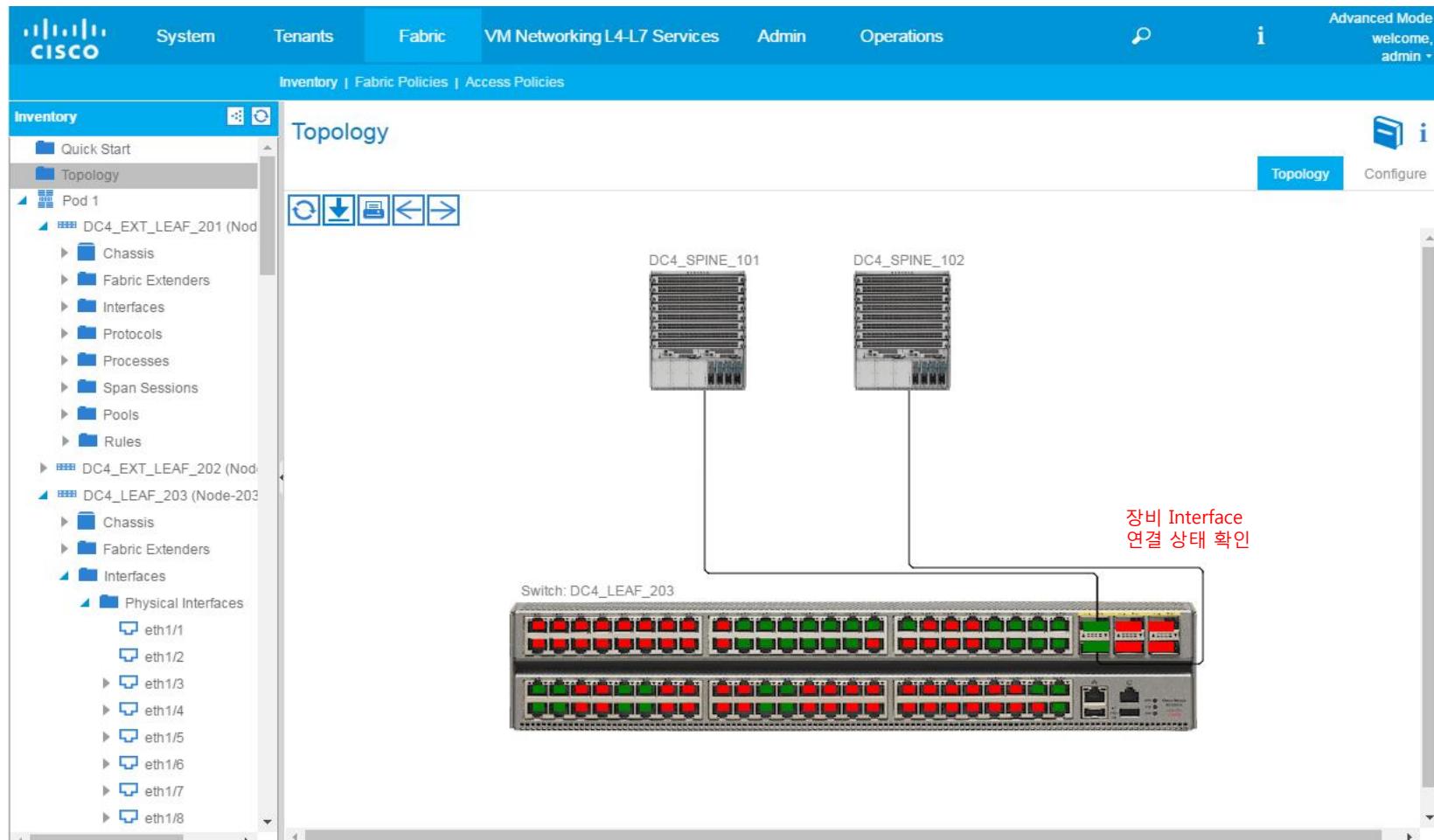
⇒ cat /mit/sys/summary

```
LEAF_301# cat /mit/sys/summary
# System
address      : 20.0.112.90
childAction   :
configIssues  :
currentTime   : 2016-06-08T10:41:30.620+00:00
dn           : sys
fabricId     : 1
fabricMAC    : 00:22:BD:F8:19:FF
id           : 301
inbMgmtAddr  : 0.0.0.0
inbMgmtAddr6 : 0.0.0.0
lcOwn        : local
modTs        : 2016-06-08T09:51:16.532+00:00
mode         : unspecified
monPolDn    : uni/fabric/monfab-default
name         : LEAF_301
oobMgmtAddr  : 0.0.0.0
oobMgmtAddr6 : 0.0.0.0
podId        : 1
rn           : sys
role         : leaf
serial       : SAL1934MR76
state        : in-service
status       :
systemUpTime : 00:00:51:20.000
```

1. Basic Operation > 1.4 Interface 확인

Topology & Link 확인

- ❖ Fabric > Inventory
 - > Topology ⇒ Node(DC4_LEAF_203) 선택



1. Basic Operation > 1.4 Interface 확인 (계속)

전체 Physical Interface 확인 (Node별)

❖ Fabric > Inventory
> Pod1 > DC4_LEAF_203 (Node 선택)

Inventory | Fabric Policies | Access Policies

Inventory

- Quick Start
- Topology
- Pod 1
 - DC4_EXT_LEAF_201 (Node-201)
 - DC4_EXT_LEAF_202 (Node-202)
 - DC4_LEAF_203 (Node-203)
 - Chassis
 - Fabric Extenders
 - Interfaces
 - Physical Interfaces
 - eth1/1
 - eth1/2
 - eth1/3
 - eth1/4
 - eth1/5
 - eth1/6
 - eth1/7
 - eth1/8
 - eth1/9
 - eth1/10
 - eth1/11
 - eth1/12
 - eth1/13
 - eth1/14
 - eth1/15
 - eth1/16
 - eth1/17
 - eth1/18
 - eth1/19
 - eth1/20
 - eth1/21
 - eth1/22
 - eth1/23
 - eth1/24
 - eth1/25
 - eth1/26
 - eth1/27
 - eth1/28
 - eth1/29
 - eth1/30

Physical Interfaces

Interface	Speed	Layer	Mode	Switching State	Usage	Oper Vlans	Configured Vlans	Bundle Index	Oper Duplex	Duplex 설정	Up상태 확인
eth1/16	inherit	switched	trunk	disabled	Discovery			unspecifi...	full	down	link-failure
eth1/17	inherit	switched	trunk	disabled	Discovery			unspecifi...	full	down	link-failure
eth1/18	inherit	switched	trunk	disabled	Discovery			unspecifi...	full	down	link-failure
eth1/19	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/20	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/21	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/22	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/23	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/24	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/25	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/26	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/27	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/28	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/29	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none
eth1/30	1 Gbps	switched	trunk	enabled	EPG	8-9	8-9	unspecifi...	full	up	none

| < | Page 2 Of 7 | > |

Objects Per Page: 15

Displaying Objects 16 - 30 Of 102

1. Basic Operation > 1.4 Interface 확인 (계속)

개별 포트 Physical Interface 확인

❖ Fabric > Inventory

- > Pod1 > DC4_LEAF_203 (Node 선택)
- > Interface > Physical Interface > eth1/19 (해당 포트 선택) > Operational

The screenshot shows the 'Layer 1 Physical Interface Configuration - 203/eth1/19' interface. On the left, a tree view of network interfaces is shown, with 'eth1/19' selected. The main panel displays the 'Properties' and 'Operational' tabs.

Properties Tab:

- Interface: eth1/19
- Description: cpbeap11 53.41
- Admin State: up
- Usage: EPG
- Bandwidth (kb): 0
- Delay (usec): 1
- Mdix: auto
- Medium: broadcast
- Mtu: 9000
- Router Mac: N/A
- Speed: 1 Gbps
- Auto Negotiation: on
- Dot1Q Ether Type: 0x8100
- Layer: switched
- Mode: trunk
- Switching State: enabled
- Destination SPAN Mode: not-a-span-dest
 - Load Interval 1: 30
 - Load Interval 2: 300
 - Load Interval 3: 0
 - Eee Lat: variable
 - Eee Lpi: aggressive
 - Eee State: not-applicable
- Indicator LED Color: Green
- Locator LED: Off
- Locator LED Color: No color
- Backplane Mac: 00:78:88:83:DE:0D
- Last Link St Change: 2016-05-17T16:24:19.706+09:00
- Oper Router Mac: 00:00:00:00:00:00
- Oper Mdix: auto

Oper Router Mac: 00:00:00:00:00:00

Oper Mdix: auto

Oper Mode: trunk

Oper Speed: 1 Gbps

Oper State: up

Oper State Reason: connected

Cfg Access Vlan: vlan-9

Cfg Native Vlan: vlan-9

Reset Counter: 72

Transceiver Present: false

Portcap Speed: 100,1000,10000,auto

Portcap Mdix: 1

Channeling State: unknown

Attached Entity Profile: AEP_V11-200

CDP Neighbor:

LLDP Neighbor:

Attached IP: <div style="max-width: 800px;">10.192.53.41</div>

Attached MAC: <div style="max-width: 800px;">78:2B:CB:78:A9:5E</div>

Oper Vlans: 8-9

Configured Vlans: 8-9

Port Channel Bundle: unspecified

Attached VM:

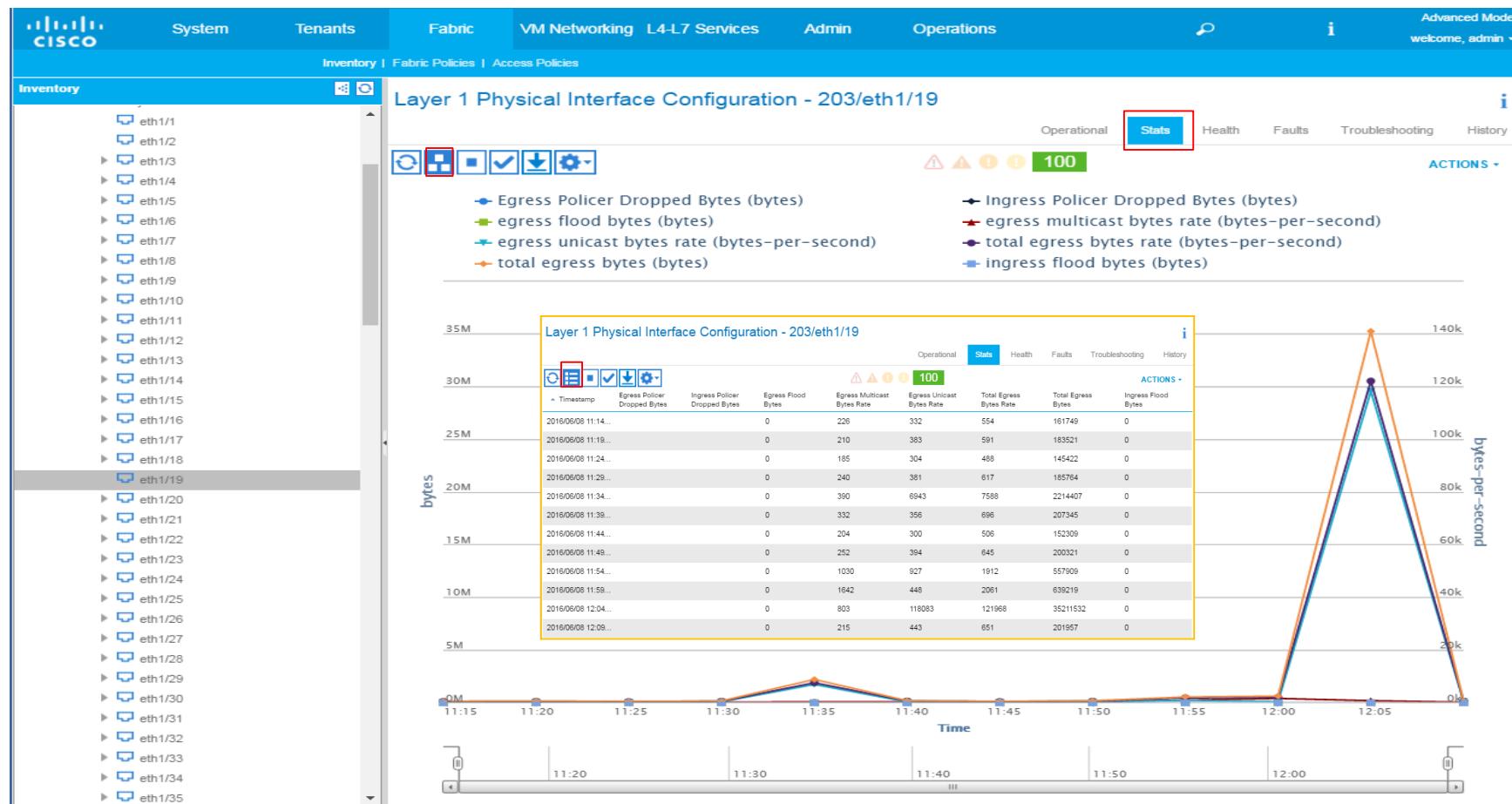
연결된 EP

1. Basic Operation > 1.4 Interface 확인 (계속)

개별 포트 Physical Interface 확인 (Statistics)

❖ Fabric > Inventory

- > Pod1 > DC4_LEAF_203 (Node 선택)
- > Interface > Physical Interface > eth1/19 (해당 포트 선택) > Operational



1. Basic Operation > 1.4 Interface 확인 (계속)

Interface 확인 (CLI)

1. Node에서 전체 Interface 상태 확인 ⇒ show Interface brief

```
DC4_LEAF_203# show interface brief
-----
Port      VRF      Status IP Address          Speed      MTU
-----  
mgmt0    --       up     10.210.9.53           1000      9000
-----  
Ethernet   VLAN   Type Mode  Status Reason          Speed      Port
Interface          Ch #
-----  
Eth1/1      9      eth  trunk  down   link-failure    1000(D)  --
Eth1/2      0      eth  trunk  down   link-failure    1000(D)  --
Eth1/3      0      eth  trunk  down   link-failure    1000(D)  --
Eth1/4      0      eth  trunk  down   link-failure    1000(D)  --
Eth1/5      0      eth  trunk  down   link-failure    1000(D)  --
Eth1/6      0      eth  trunk  down   link-failure    1000(D)  --
Eth1/7      0      eth  trunk  down   link-failure    1000(D)  --
Eth1/8      0      eth  trunk  down   link-failure    1000(D)  --
Eth1/9      0      eth  trunk  down   link-failure    10G(D)   --
Eth1/10     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/11     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/12     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/13     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/14     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/15     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/16     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/17     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/18     0      eth  trunk  down   link-failure    10G(D)   --
Eth1/19     9      eth  trunk  up    none            1000(D)  --
Eth1/20     9      eth  trunk  up    none            1000(D)  --
Eth1/21     9      eth  trunk  up    none            1000(D)  --
Eth1/22     9      eth  trunk  up    none            1000(D)  --
Eth1/23     9      eth  trunk  up    none            1000(D)  --
Eth1/24     9      eth  trunk  up    none            1000(D)  --
Eth1/25     9      eth  trunk  up    none            1000(D)  --
Eth1/26     9      eth  trunk  up    none            1000(D)  --
Eth1/27     9      eth  trunk  up    none            1000(D)  --
Eth1/28     9      eth  trunk  up    none            1000(D)  --
Eth1/29     9      eth  trunk  up    none            1000(D)  --
Eth1/30     9      eth  trunk  up    none            1000(D)  --
Eth1/31     9      eth  trunk  up    none            1000(D)  --
Eth1/32     9      eth  trunk  up    none            1000(D)  --
Eth1/33     9      eth  trunk  up    none            1000(D)  --
Eth1/34     9      eth  trunk  up    none            1000(D)  --
Eth1/35     0      eth  trunk  down  link-failure    10G(D)   --
Eth1/36     9      eth  trunk  down  link-failure    1000(D)  --
```

1. Node에서 개별 Interface 상태 확인 ⇒ show Interface ethernet 1/19

```
DC4_LEAF_203# show interface ethernet 1/19
Ethernet1/19 is up
admin state is up, Dedicated Interface
Port description is cpbeap11 53.41
Hardware: 100/1000/10000/auto Ethernet, address: 0078.8883.de0d (bia 0078.8883.d
e0d)
MTU 9000 bytes, BW 1000000 Kbit, DLY 1 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, medium is broadcast
Port mode is trunk
full-duplex, 1000 Mb/s
Beacon is turned off
Auto-Negotiation is turned on
Input flow-control is off, output flow-control is off
Auto-mdix is turned on
Switchport monitor is off
EtherType is 0x8100
EEE (efficient-ethernet) : n/a
Last link flapped 03w21d
Last clearing of "show interface" counters never
72 interface resets
30 seconds input rate 34360 bits/sec, 10 packets/sec
30 seconds output rate 175128 bits/sec, 102 packets/sec
Load-Interval #2: 5 minute (300 seconds)
    input rate 178864 bps, 34 pps; output rate 187272 bps, 113 pps
RX
24568318 unicast packets 3955997 multicast packets 4486 broadcast packets
28528801 input packets 6609404858 bytes
0 jumbo packets 0 storm suppression bytes
0 runts 0 giants 0 CRC 0 no buffer
0 input error 0 short frame 0 overrun 0 underrun 0 ignored
0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop
0 input with dribble 0 input discard
0 Rx pause
TX
23233551 unicast packets 51402616 multicast packets 625020 broadcast packets
75261187 output packets 19007949616 bytes
0 jumbo packets
0 output error 0 collision 0 deferred 0 late collision
0 lost carrier 0 no carrier 0 babble 0 output discard
0 Tx pause
```

1. Basic Operation > 1.5 VRF 확인

VRF 확인

- ❖ Tenant > DC_TENANT(User Tenant)
 > Tenant DC_TENANT > Networking > VRFs > DC_VRF1(User VRF)

The screenshot shows the Cisco Application Centric Infrastructure (ACI) User Interface. The top navigation bar includes System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and Advanced Mode (welcome, admin). The left sidebar lists various tenant configurations under Tenant DC_TENANT, with DC_VRF1 selected. The main content area displays the properties of VRF DC_VRF1. Key fields shown include:

- Name: DC_VRF1 (highlighted with a red box)
- Description: optional
- Label: 2686977
- Segment: 100
- Policy Control Enforcement Preference: Enforced (selected, highlighted with a red box)
- Policy Control Enforcement Direction: Egress, Ingress (highlighted with a red box)
- BGP Timers: select a value
- OSPF Timers: select a value
- End Point Retention Policy: select a value (Note: This policy only applies to remote L3 entries)
- Monitoring Policy: select a value

A red callout box labeled "Policy control option" points to the Policy Control Enforcement Preference and Direction settings.

1. Basic Operation > 15 VRF 확인 (계속)

VRF 확인 (CLI)

- ❖ VRF 상태 확인
⇒ `show vrf`
- ❖ VRF routing table 확인
⇒ `show ip route summary vrf DC_TENANT:DC_VRF1`

```
DC4_LEAF_203# show vrf
VRF-Name                      VRF-ID State   Reason
black-hole                      3 Up     --
DC_TENANT:DC_VRF1                4 Up     --
management                      2 Up     --
overlay-1                        5 Up     --
SPAN_TENANT:SPAN_VRF             6 Up     --

DC4_LEAF_203# show ip route summary vrf DC_TENANT:DC_VRF1
IP Route Table for VRF "DC_TENANT:DC_VRF1"
Total number of routes: 772
Total number of paths: 1540

Best paths per protocol:      Backup paths per protocol:
  static            : 1           bgp-65011       : 4
  local             : 1
  bgp-65011        : 1534

Number of routes per mask-length:
 /0 : 1           /16: 6          /18: 1          /19: 2          /22: 2
 /23: 2           /24: 362         /26: 1          /28: 9          /29: 17
 /30: 242         /32: 127

DC4 LEAF 203#
```

1. Basic Operation > 1.6 BD 확인

BD 확인(forwarding policy)

- ❖ Tenant > DC_TENANT(User Tenant)
> Tenant DC_TENANT > Networking > Bridge Domain > WT_BD(User BD)

Bridge Domain - WT_BD

Main

Properties

Name: WT_BD

Description: optional

Label:

Legacy Mode: No

VRF: DC_TENANT/DC_VRF1

Resolved VRF: DC_TENANT/DC_VRF1

L2 Unknown Unicast: Flood Hardware Proxy

L3 Unknown Multicast Flooding: Flood Optimized Flood

Multi Destination Flooding: Flood in BD Drop Flood in Encapsulation

ARP Flooding:

End Point Retention Policy: default

IGMP Snoop Policy: IGMP_SNOOP

SHOW USAGE SUBMIT RESET

1. Basic Operation > 1.6 BD 확인(계속)

BD 확인(L3 configuration)

- ❖ Tenant > DC_TENANT(User Tenant)
 > Tenant DC_TENANT > Networking > Bridge Domain > WT_BD(User BD)

The screenshot shows the Cisco ACI UI interface. The top navigation bar includes System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and Advanced Mode (welcome, admin). The main navigation on the left is under Tenant DC_TENANT, with sections for Quick Start, Tenant DC_TENANT, Application Profiles, Networking, Bridge Domains, VRFs, DC_VRF1, and various policy and security sections.

The central panel displays the "Bridge Domain - WT_BD" configuration. The "L3 Configurations" tab is selected. The "Properties" section contains the following details:

- Unicast Routing: Operational Value for Unicast Routing: true
- Custom MAC Address: 00:22:BD:F8:19:FF
- Virtual MAC Address: Not Configured
- Subnets:
 - Gateway Address: 10.192.53.1/24
 - Scope: Advertised Externally
 - Primary IP Address: False
 - Virtual IP: False
 - Subnet Control: None

Annotations in red highlight specific fields:

- Operational Value for Unicast Routing: true (labeled "routing enable")
- Advertised Externally (labeled "subnet 확인, 외부연동을 위한 Advertised Externally 확인")
- L3OUT_BB (labeled "외부 라우팅 연동을 위한 L3Out 확인")

At the bottom of the panel are buttons for SHOW USAGE, SUBMIT, and RESET.

1. Basic Operation > 1.7 EP(End Point) 확인

EPG 확인

- ❖ Tenant > DC_TENANT(User Tenant)
> Tenant DC_TENANT > Application Profiles > DC_AP(User AP) > WT_EPG(User EPG)

Endpoint	MAC	IP	Learning Source	Hosting Server	Reporting Controller Name	Interface	Multicast Address	Primary VLAN For Micro-Seg	Port Encap (Or Secondary VLAN For Micro-Seg)
EP-00:0A:F7:84:3B:C7	00:0A:F7:84:3B:C7	10.192.53.101	learned	---	---	Node-204/eth1/71 (learned)	---	---	vlan-20
EP-00:0A:F7:8A:92:43	00:0A:F7:8A:92:43	10.192.53.57	learned	---	---	Node-204/eth1/28 (learned)	---	---	vlan-20
EP-00:17:59:0E:A7:B1	00:17:59:0E:A7:B1	10.192.53.4	learned	---	---	Node-203/eth1/93 (learned)	---	---	vlan-20
EP-00:24:E8:33:C7:3F	00:24:E8:33:C7:3F	10.192.53.27	learned	---	---	Node-203/eth1/30 (learned)	---	---	vlan-20
EP-00:24:E8:6B:0D:21	00:24:E8:6B:0D:21	10.192.53.26	learned	---	---	Node-203/eth1/29 (learned)	---	---	vlan-20
EP-00:25:B3:B4:AA:AE	00:25:B3:B4:AA:AE	10.192.53.81	learned	---	---	Node-203-204/VPC52_203-204 (learned)	---	---	vlan-20
EP-00:25:B3:B4:B0:B2	00:25:B3:B4:B0:B2	10.192.53.82, 10.192.53.83	learned	---	---	Node-203-204/VPC60_203-204 (learned)	---	---	vlan-20
EP-00:25:B3:B4:C0:BE	00:25:B3:B4:C0:BE	10.192.53.87	learned	---	---	Node-203-204/VPC50_203-204 (learned)	---	---	vlan-20
EP-00:25:B3:B4:C2:03	00:25:B3:B4:C2:03	10.192.53.68	learned	---	---	Node-203-204/VPC58_203-204 (learned)	---	---	vlan-20
EP-00:25:B3:B5:07:2F	00:25:B3:B5:07:2F	10.192.53.73, 10.192.53.74, 169.254.28.59	learned	---	---	Node-203-204/VPC57_203-204 (learned)	---	---	vlan-20
EP-00:25:B3:B5:07:EE	00:25:B3:B5:07:EE	10.192.53.71, 10.192.53.72, 10.192.53.75, 169.254.169.2	learned	---	---	Node-203-204/VPC49_203-204 (learned)	---	---	vlan-20
EP-00:25:B3:B5:33:77	00:25:B3:B5:33:77	10.192.53.101, 10.192.53.102, 10.192.53.105	learned	---	---	Node-203-204/VPC51_203-204 (learned)	---	---	vlan-20
EP-00:25:B3:B5:38:0B	00:25:B3:B5:38:0B	10.192.53.103, 10.192.53.104, 169.254.110.147	learned	---	---	Node-203-204/VPC50_203-204 (learned)	---	---	vlan-20
EP-00:E0:ED:46:A7:19	00:E0:ED:46:A7:19	10.192.53.9	learned	---	---	Node-208/eth1/48 (learned)	---	---	vlan-20
EP-00:E0:ED:46:A7:1D	00:E0:ED:46:A7:1D	10.192.53.10, 10.192.53.8	learned	---	---	Node-205/eth1/48 (learned)	---	---	vlan-20

1. Basic Operation > 17 EP(End Point) 확인 (계속)

EPG Traffic (Statistics)

❖ Tenant > DC_TENANT(User Tenant)
> Tenant DC_TENANT > Application Profiles > DC_AP(User AP) > WT_EPG(User EPG) ⇒ Stats



1. Basic Operation > 17 EP(End Point) 확인 (계속)

EP 확인

- ❖ Endpoint 확인
⇒ show endpoint

```
DC4_LEAF_203# show endpoint
Legend:
O - peer-attached    H - vtep          a - locally-aged    S - static
V - vpc-attached    p - peer-aged     L - local         M - span
s - static-arp       B - bounce

+-----+-----+-----+-----+-----+
| VLAN/ | Encap | MAC Address | MAC Info/ | Interface |
| Domain| VLAN | IP Address | IP Info   |           |
+-----+-----+-----+-----+-----+
DC_TENANT:DC_VRF1          10.192.53.8      tunnel19
DC_TENANT:DC_VRF1          10.192.53.9      tunnel19
8/DC_TENANT:DC_VRF1        vxlan-16318374  00e0.ed46.a71d  tunnel19
8/DC_TENANT:DC_VRF1        vxlan-16318374  00e0.ed46.a719  tunnel19
9/DC_TENANT:DC_VRF1        vlan-20          d89d.671f.0053 O eth1/42
9/DC_TENANT:DC_VRF1        vlan-20          d89d.671c.3c48 L eth1/43
DC_TENANT:DC_VRF1          vlan-20          10.192.53.33 L eth1/43
9/DC_TENANT:DC_VRF1        vlan-20          d89d.671d.a2eb O eth1/43
9/DC_TENANT:DC_VRF1        vlan-20          c81f.66ee.7cca L eth1/31
DC_TENANT:DC_VRF1          vlan-20          10.192.53.91 L eth1/31
9/DC_TENANT:DC_VRF1        vlan-20          c81f.66ee.87b3 L eth1/33
DC_TENANT:DC_VRF1          vlan-20          10.192.53.96 L eth1/33
9/DC_TENANT:DC_VRF1        vlan-20          d4ae.52b7.fba0 O eth1/24
DC_TENANT:DC_VRF1          vlan-20          10.192.53.46 O eth1/24
9/DC_TENANT:DC_VRF1        vlan-20          d89d.671c.3c68 O eth1/46
DC_TENANT:DC_VRF1          vlan-20          10.192.53.36 O eth1/46
9/DC_TENANT:DC_VRF1        vlan-20          d89d.671d.e36f L eth1/46
9/DC_TENANT:DC_VRF1        vlan-20          d89d.671c.3740 L eth1/45
DC_TENANT:DC_VRF1          vlan-20          10.192.53.35 L eth1/45
9/DC_TENANT:DC_VRF1        vlan-20          ac16.2d87.b737 O eth1/45
9/DC_TENANT:DC_VRF1        vlan-20          d89d.671b.8568 O eth1/44
DC_TENANT:DC_VRF1          vlan-20          10.192.53.34 O eth1/44
9/DC_TENANT:DC_VRF1        vlan-20          d89d.671f.14b3 L eth1/44
9/DC_TENANT:DC_VRF1        vlan-20          0025.b3b4.aaaae LV po15
DC_TENANT:DC_VRF1          vlan-20          10.192.53.81 LV po15
9/DC_TENANT:DC_VRF1        vlan-20          c81f.66ed.4aaa L eth1/32
DC_TENANT:DC_VRF1          vlan-20          10.192.53.92 L eth1/32
9/DC_TENANT:DC_VRF1        vlan-20          c81f.66ee.75f9 L eth1/34
DC_TENANT:DC_VRF1          vlan-20          10.192.53.97 L eth1/34
9/DC_TENANT:DC_VRF1        vlan-20          0025.b3b5.07ee LV po8
DC_TENANT:DC_VRF1          vlan-20          10.192.53.71 LV po8
9/DC_TENANT:DC_VRF1        vlan-20          10.192.53.75 LV po8
DC_TENANT:DC_VRF1          vlan-20          169.254.169.229 LV po8
DC_TENANT:DC_VRF1          vlan-20          10.192.53.72 LV po8
9/DC_TENANT:DC_VRF1        vlan-20          0025.b3b5.3377 LV po14
DC_TENANT:DC_VRF1          vlan-20          10.192.53.101 LV po14
```

1. Basic Operation > 17 EP(End Point) 확인 (계속)

VLAN 확인 (BD & EPG)

❖ VLAN 확인

⇒ show vlan extended

```
DC4_LEAF_203# show vlan extended
```

VLAN Name	Status	Ports
7 infra:default	active	Eth1/95, Eth1/96
8 DC_TENANT:WT_BD	active	Eth1/1, Eth1/19, Eth1/20, Eth1/21, Eth1/22, Eth1/23, Eth1/24, Eth1/25, Eth1/26, Eth1/27, Eth1/28, Eth1/29, Eth1/30, Eth1/31, Eth1/32, Eth1/33, Eth1/34, Eth1/36, Eth1/37, Eth1/38, Eth1/41, Eth1/42, Eth1/43, Eth1/44, Eth1/45, Eth1/46, Eth1/47, Eth1/48, Eth1/49, Eth1/50, Eth1/51, Eth1/52, Eth1/53, Eth1/54, Eth1/57, Eth1/58, Eth1/59, Eth1/60, Eth1/61, Eth1/62, Eth1/65, Eth1/66, Eth1/67, Eth1/68, Eth1/69, Eth1/70, Eth1/71, Eth1/72, Eth1/90, Eth1/92, Eth1/93, Po8, Po14, Po15, Po16, Po17, Po18, Po19, Po20, Po21, Po22, Po24, Po25
9 DC_TENANT:DC_AP:WT_EPG	active	Eth1/1, Eth1/19, Eth1/20, Eth1/21, Eth1/22, Eth1/23, Eth1/24, Eth1/25, Eth1/26, Eth1/27, Eth1/28, Eth1/29, Eth1/30, Eth1/31, Eth1/32, Eth1/33, Eth1/34, Eth1/36, Eth1/37, Eth1/38, Eth1/41, Eth1/42, Eth1/43, Eth1/44, Eth1/45, Eth1/46, Eth1/47, Eth1/48, Eth1/49, Eth1/50, Eth1/51, Eth1/52, Eth1/53, Eth1/54, Eth1/57, Eth1/58, Eth1/59, Eth1/60, Eth1/61, Eth1/62, Eth1/65, Eth1/66, Eth1/67, Eth1/68, Eth1/69, Eth1/70, Eth1/71, Eth1/72, Eth1/90, Eth1/92, Eth1/93, Po8, Po14, Po15, Po16, Po17, Po18, Po19, Po20, Po21, Po22, Po24, Po25

VLAN	Type	Vlan-mode	Encap
7	enet	CE	vxlan-16777209, vlan-4093
8	enet	CE	vxlan-16318374
9	enet	CE	vlan-20

❖ VLAN 확인 (VLAN to VxLan)

⇒ show system internal epm vlan all

```
DC4_LEAF_203# show system internal epm vlan all
```

VLAN ID	Type	Access Encap (Type Value)	Fabric Encap	H/W id	BD VLAN	Endpoint Count
7	Infra BD	802.1Q	4093 16777209	1	7	1
8	Tenant BD	NONE	0 16318374	2	8	1
9	FD vlan	802.1Q	20 8201	3	8	45

1. Basic Operation > 1.8 L3Out 확인

L3Out OSPF 설정 확인

- ❖ Tenant > DC_TENANT(User Tenant)
> Tenant DC_TENANT > Networking > External Routed Network > L3OUT_BB (User L3Out)

The screenshot shows the Cisco ACI UI interface for configuring an L3Out. The left sidebar navigation tree is expanded to show the path: ALL TENANTS > Tenant DC_TENANT > Networking > External Routed Network > L3OUT_BB.

L3 Outside - L3OUT_BB Properties:

- Name:** L3OUT_BB (highlighted with a red box)
- Description:** optional
- Tags:** enter tags separated by comma
- Label:** unspecified
- Target DSCP:** unspecified
- Route Control Enforcement:** Import (checkbox checked), Export (checkbox checked)
- VRF:** DC_TENANT/DO_VRF1 (highlighted with a red box)
- Resolved VRF:** DC_TENANT/DC_VRF1 (highlighted with a red box)
- External Routed Domain:** L3OUT_ROUTED (highlighted with a red box)
- Route Profile for Interleak:** select a value
- Route Control For Dampening:** Address Family Type (dropdown menu)
- Route Dampening Policy:** No items have been found. Select Actions to create a new item.

Enable BGP/EIGRP/OSPF:

- BGP:** checkbox (unchecked)
- EIGRP:** checkbox (unchecked)
- OSPF:** checkbox (checked)

OSPF Area ID: 0

OSPF Area Control:

- Send redistributed LSAs into NSSA area
- Originate summary LSA
- Suppress forwarding address in translated LSA

OSPF Area Type: NSSA area (radio button selected), Regular area, Stub area

OSPF Area Cost: 1

Buttons at the bottom: SHOW USAGE, SUBMIT, RESET

Annotations in red:

- VRF 확인 (VRF confirmation) - points to the VRF field.
- External Routed Domain 확인 (External Routed Domain confirmation) - points to the External Routed Domain field.
- OSPF 설정 확인 - Regular area = 0 (OSPF configuration confirmation - Regular area = 0) - points to the OSPF configuration section.

1. Basic Operation > 1.8 L3Out 확인 (계속)

L3Out OSPF Adjacency 확인

❖ Tenant > DC_TENANT(User Tenant)

> Tenant DC_TENANT > Networking > External Routed Network > L3OUT_BB (User L3Out)

> Logical Interface Profile > L3OUT_EXT_LEAF_201 > Configured Nodes > Topology/pod-1/node-201 > OSPF for VRF-DC_TENANT:DC_VRF1

The screenshot shows the Cisco ACI Management interface. The left sidebar navigation tree is expanded to show the following structure under Tenant DC_TENANT:

- uSeg EPGs
- L4-L7 Service Parameters
- Networking
 - Bridge Domains
 - VRFs
 - External Bridged Networks
 - Set Action Rule Profiles
 - Match Action Rule Profiles
 - L3OUT_BB
 - Logical Node Profiles
 - L3OUT_EXT_LEAF_201
 - Logical Interface Profiles
 - L3OUT_201-1-25
 - L3OUT_201-1-26
 - Configured Nodes
 - topology/pod-1/node-201
 - BGP for VRF-DC_TENANT:DC_VRF1
 - OSPF for VRF-DC_TENANT:DC_VRF1
 - Areas
 - Interfaces
 - Routes
 - L3OUT_EXT_LEAF_202
 - Networks
 - Route Profiles
 - Route Profiles
 - Protocol Policies
 - L4-L7 Service Parameters
 - Security Policies
 - Troubleshoot Policies
 - Monitoring Policies
 - L4-L7 Services

PROPERTIES		STATS
Name: DC_TENANT:DC_VRF1	Route ID: 10.201.1.182	Interface Count: 3
Distance: 110	Activeareacnt: 1	Active Nssa Areacnt: 0
Max ECMP: 8	Active Stub Areacnt: 0	Active Ext Areacnt: 1
Bandwidth Reference: 40000 (Mbps)	Extareacnt: 1	Nssa Areacnt: 0
Operational State: Up	Stbareacnt: 0	Areacnt: 1
	Opaque Lsacnt: 0	Ext Lsacnt: 202

OSPF Protocol Info.

Neighbors

Neighbor Id	State	Peer Ip	Interface
10.201.1.1	Full	10.201.242.21	eth1/25
10.201.1.2	Full	10.201.242.25	eth1/26

OSPF Neighbors

Inter Protocol Route Leak Into OSPF

Name	Redistribution Protocol	Route Map	Scope	Asn
DC_TENANT:DC_VRF1	BGP	exp-ctx-proto-2686977	Inter protocol leak	65011
DC_TENANT:DC_VRF1	Direct	exp-ctx-st-2686977	Inter protocol leak	1
DC_TENANT:DC_VRF1	EIGRP	exp-ctx-proto-2686977	Inter protocol leak	1
DC_TENANT:DC_VRF1	Static	exp-ctx-st-2686977	Inter protocol leak	1

Current System Time: 2016-06-08T21:33 +09:00

1. Basic Operation > 1.8 L3Out 확인 (계속)

L3Out OSPF routing table 확인

❖ Tenant > DC_TENANT(User Tenant)

> Tenant DC_TENANT > Networking > External Routed Network > L3OUT_BB (User L3Out)

> Logical Interface Profile > L3OUT_EXT_LEAF_201 > Configured Nodes > Topology/pod-1/node-201 > OSPF for VRF-DC_TENANT:DC_VRF1

The screenshot shows the Cisco ACI Tenant configuration interface. The left sidebar is expanded to show the tenant structure under 'Tenant DC_TENANT'. The 'Routes' section is selected, displaying a table of routes. The table has columns for Name, Pfx, Path Type, Area, Flags, Cost, Admin Distance, and Addr. The table lists 771 routes, with the first 25 displayed. The routes include various network prefixes like 10.196.66.0/24, 10.201.91.40/30, and 10.201.1.185/32, with costs ranging from 2 to 20 and admin distances from 1 to 110. Most routes are backbone routes (ext2, intra) with flags 'in-rib,v4'.

Name	Pfx	Path Type	Area	Flags	Cost	Admin Distance	Addr
Route 10.196.66.0/24, Flags:in-rib,v4, Unicast Cost: 20	10.196.66.0/24	ext2	backbone	in-rib,v4	20	110	
Route 10.201.91.40/30, Flags:in-rib,v4, Unicast Cost: 2	10.201.91.40/30	intra	backbone	in-rib,v4	2	110	
Route 10.201.1.185/32, Flags:in-rib,v4, Unicast Cost: 3	10.201.1.185/32	intra	backbone	in-rib,v4	3	110	
Route 10.201.91.48/30, Flags:in-rib,v4, Unicast Cost: 2	10.201.91.48/30	intra	backbone	in-rib,v4	2	110	
Route 192.168.64.0/24, Flags:in-rib,v4, Unicast Cost: 14	192.168.64.0/24	inter	backbone	in-rib,v4	14	110	
Route 10.196.138.0/24, Flags:in-rib,v4, Unicast Cost: 14	10.196.138.0/24	inter	backbone	in-rib,v4	14	110	
Route 10.196.139.0/24, Flags:in-rib,v4, Unicast Cost: 14	10.196.139.0/24	inter	backbone	in-rib,v4	14	110	
Route 10.196.142.0/24, Flags:in-rib,v4, Unicast Cost: 14	10.196.142.0/24	inter	backbone	in-rib,v4	14	110	
Route 10.201.51.168/30, Flags:in-rib,v4, Unicast Cost: 14	10.201.51.168/30	intra	backbone	in-rib,v4	14	110	
Route 10.201.51.172/30, Flags:in-rib,v4, Unicast Cost: 14	10.201.51.172/30	intra	backbone	in-rib,v4	14	110	
Route 9.9.9.93/32, Flags:in-rib,v4, Unicast Cost: 15	9.9.9.93/32	inter	backbone	in-rib,v4	15	110	
Route 10.196.140.0/24, Flags:in-rib,v4, Unicast Cost: 15	10.196.140.0/24	inter	backbone	in-rib,v4	15	110	
Route 10.201.1.182/32, Flags:direct,v4, Unicast Cost: 1	10.201.1.182/32	intra	backbone	direct,v4	1	110	
Route 10.201.242.20/30, Flags:direct,v4, Unicast Cost: 1	10.201.242.20/30	intra	backbone	direct,v4	1	110	
Route 10.201.242.24/30, Flags:direct,v4, Unicast Cost: 1	10.201.242.24/30	intra	backbone	direct,v4	1	110	
Route 10.201.242.32/30, Flags:in-rib,v4, Unicast Cost: 2	10.201.242.32/30	intra	backbone	in-rib,v4	2	110	
Route 10.201.1.183/32, Flags:in-rib,v4, Unicast Cost: 3	10.201.1.183/32	intra	backbone	in-rib,v4	3	110	
Route 10.201.242.28/30, Flags:in-rib,v4, Unicast Cost: 2	10.201.242.28/30	intra	backbone	in-rib,v4	2	110	
Route 10.201.242.48/30, Flags:in-rib,v4, Unicast Cost: 2	10.201.242.48/30	inter	backbone	in-rib,v4	2	110	
Route 10.210.9.0/24, Flags:in-rib,v4, Unicast Cost: 3	10.210.9.0/24	inter	backbone	in-rib,v4	3	110	
Route 10.201.242.44/30, Flags:in-rib,v4, Unicast Cost: 2	10.201.242.44/30	inter	backbone	in-rib,v4	2	110	
Route 10.201.1.188/32, Flags:in-rib,v4, Unicast Cost: 2	10.201.1.188/32	inter	backbone	in-rib,v4	2	110	
Route 10.192.53.0/24, Flags:in-rib,v4, Unicast Cost: 20	10.192.53.0/24	ext2	backbone	in-rib,v4	20	110	
Route 10.201.1.1/32, Flags:in-rib,v4, Unicast Cost: 2	10.201.1.1/32	intra	backbone	in-rib,v4	2	110	
Route 10.201.242.16/30, Flags:in-rib,v4, Unicast Cost: 2	10.201.242.16/30	intra	backbone	in-rib,v4	2	110	

1. Basic Operation > 1.8 L3Out 확인 (계속)

L3Out EPG 및 Contract 확인

❖ Tenant > DC_TENANT(User Tenant)

- > Tenant DC_TENANT > Networking > External Routed Network > L3OUT_BB (User L3Out)
- > Networks > L3OUT (User N/W) ⇒ Policy

The screenshot shows the Cisco ACI Network Controller interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, and Operations. The Tenant section is selected, showing 'Tenant DC_TENANT'.

The main content area displays the 'External Network Instance Profile - L3OUT_HYNIX'. The 'Properties' section shows the following details:

- Name: L3OUT_HYNIX
- Tags: (empty)
- Description: (optional)
- Configured VRF name: DC_VRF1
- Resolved VRF: uniltn-DC_TENANT/ctx-DC_VRF1
- QoS Class: Unspecified
- Target DSCP: unspecified
- Configuration Status: applied
- Configuration Issues: (empty)
- Subnets:
 - IP Address: 166.125.0.0/16
 - Scope: External Subnets for the External EPG
 - IP Address: 177.0.0/8
 - Scope: External Subnets for the External EPG
 - IP Address: 192.168.0.0/16
 - Scope: External Subnets for the External EPG

The 'Route Control Profile' section shows a single entry:

Name	Direction
No items have been found. Select Actions to create a new item.	

Below the main profile view, a separate window titled 'EPG0| contract association 상태 확인' shows the 'Contracts' tab for the EPG. It lists a single contract entry:

To EPG	Type	Contract Subject	Filter	Egress 15min Cumulative Packets	Ingress 15min Cumulative Packets
DC_TENANT/DC_AP/WT_EPG	Provider	DC_TENANT/HYNIX_IP_ALL/HY...	EtherT:Protocol:srcFromPort-toPort to destFromPort-descToPort ip:/* to */	0	0

1. Basic Operation > 1.9 NTP 설정 확인

NTP Server 등록

- ❖ Fabric > Fabric Policies
> Pod Policies > Date and Time

The screenshot shows the Cisco Fabric Manager interface with the following details:

- Policies** section on the left: Quick Start, Switch Policies, Module Policies, Interface Policies, Pod Policies, Policies, Date and Time, Policy NTP_Server, Policy default, default, SNMP, Management Access, ISIS Policy default, COOP Group Policy default, BGP Route Reflector default, Policy Groups, Profiles, Global Policies, Monitoring Policies, Troubleshoot Policies, Geolocation Policies, Tags.
- Date and Time Policy - Policy NTP_Server** page:
 - Properties**: Name: NTP_Server, Description: optional, Administrative State: enabled, Authentication State: enabled.
 - NTP Servers** table:

Host Name/IP Address	Preferred	Minimum Polling Interval	Maximum Polling Interval	Management EPG
166.125.7.177	True	4	6	default (Out-of-Band)
166.125.7.178	False	4	6	default (Out-of-Band)
 - Buttons**: SHOW USAGE, SUBMIT, RESET.

POD Policy 등록

- ❖ Fabric > Fabric Policies
> Policy Groups

The screenshot shows the Cisco Fabric Manager interface with the following details:

- Policies** section on the left: Quick Start, Switch Policies, Module Policies, Interface Policies, Pod Policies, Policies, Date and Time, Policy NTP_SERVER, Policy default, default, SNMP, Management Access, ISIS Policy default, COOP Group Policy default, BGP Route Reflector default, Policy Groups, Profiles, Global Policies, Monitoring Policies, Troubleshoot Policies, Geolocation Policies, Tags.
- Pod Policy Group - WT_Fabric** page:
 - Properties**: Name: WT_Fabric, Description: optional.
 - Resolved Policies**: NTP SERVER (highlighted in red), NTP Policy (highlighted in red).
 - Resolved Policies**: Resolved Date Time Policy: NTP SERVER, Resolved ISIS Policy: default, Resolved COOP Group Policy: default, Resolved BGP Route Reflector Policy: default, Resolved Management Access Policy: default, Resolved SNMP Policy: NMS_POLICY, Resolved SNMPPolicy: NMS_POLICY.

1. Basic Operation > 1.9 NTP 설정 확인 (계속)

NTP Server 연동 확인 (GUI)

- ❖ Fabric > Fabric Policies
 - > Pod Policies > Date and Time > NTP 서버 : Operational

The screenshot shows the Cisco Fabric Manager interface. On the left, the navigation tree is expanded to show 'Fabric Policies' under 'Pod Policies'. A specific policy named 'Policy NTP_SERVER' is selected. The main pane displays a table titled 'Providers - NTP Server 166.125.7.177'. The table lists various nodes and their synchronization status relative to the remote NTP server at 166.125.7.177. The 'Sync Status' column for all listed nodes shows 'Synced to Remote NTP Server', which is highlighted with a red box.

Name	Switch	VRF	Preferred	Sync Status
166.125.7.177	Node-227	management	True	Synced to Remote NTP Server
166.125.7.177	Node-202	management	True	Synced to Remote NTP Server
166.125.7.177	Node-206	management	True	Synced to Remote NTP Server
166.125.7.177	Node-203	management	True	Synced to Remote NTP Server
166.125.7.177	Node-101	management	True	Synced to Remote NTP Server
166.125.7.177	Node-102	management	True	Synced to Remote NTP Server
166.125.7.177	Node-201	management	True	Synced to Remote NTP Server
166.125.7.177	Node-208	management	True	Synced to Remote NTP Server
166.125.7.177	Node-103	management	True	Synced to Remote NTP Server
166.125.7.177	Node-212	management	True	Synced to Remote NTP Server
166.125.7.177	Node-210	management	True	Synced to Remote NTP Server
166.125.7.177	Node-214	management	True	Synced to Remote NTP Server
166.125.7.177	Node-219	management	True	Synced to Remote NTP Server
166.125.7.177	Node-104	management	True	Synced to Remote NTP Server

NTP Server 연동 확인 (CLI)

- ❖ Leaf node
 - >show ntp peers
 - >show ntp peer-status

```
DC4_LEAF_203# show ntp peers
-----
Peer IP Address          Serv/Peer
-----
166.125.7.178           Server (configured)
166.125.7.177           Server (configured)
DC4_LEAF_203# show ntp peer-status
Total peers : 2
* - selected for sync, + - peer mode(active),
- - peer mode(passive), = - polled in client mode
      remote                local          st poll reach delay vrf
-----=166.125.7.178          0.0.0.0       3 64   377  0.002 management
*166.125.7.177          0.0.0.0       3 64   377  0.002 management
DC4_LEAF_203# show clock
13:56:32.891688 KST Mon May 30 2016
DC4_LEAF_203#
```

1. Basic Operation > 1.10 SNMP Polling 확인

NMS Server 등록

- ❖ Fabric > Fabric Policies
> Pod Policies > SNMP ⇒ Create SNMP Policy

The screenshot shows the 'SNMP Policy - NMS_POLICY' configuration screen. Key fields highlighted in red include:

- Name: NMS_POLICY
- Description: optional
- Admin State: Enabled
- Associated Management EPG: default (Out-of-Band)
- Community string: infra

SNMP Client Group 등록

The screenshot shows the 'SNMP Client Group Profile - CYGNUS' configuration screen. Key fields highlighted in red include:

- Name: CYGNUS
- Description: optional
- Associated Management EPG: default (Out-of-Band)
- Client Entries:
 - Name: 10.192.29.35
 - Name: 10.192.29.34
 - Name: 10.192.29.33

POD Policy 등록

- ❖ Fabric > Fabric Policies > Policy Groups

*SNMP Policy를 POD Policy Group (SNMP Policy)에 등록해야 함

1. Basic Operation > 1.10 SNMP Polling 확인 (계속)

SNMP Polling 동작 확인

❖ LEAF & SPINE Node SSH 접속

> show snmp summary ⇒ Infra & Client Group status

```
DC4_LEAF_203# show snmp summary

Admin State : enabled, running (pid:5282)

Local SNMP engineID: [Hex] 800000090300788883DE74
                  [Dec] 128:000:000:009:003:000:120:136:131:222:116

-----
Community          Context          Status
-----
infra                           ok

-----
User                Authentication   Privacy   Status
-----

-----
Context            VRF           Status
-----

-----
Client             VRF           Status
-----
10.192.29.35      management    ok
10.192.29.33      management    ok
10.192.29.34      management    ok

-----
Host               Port Ver  Level   SecName   VRF
-----
10.192.25.5        162   v2c   noauth   infra     management

DC4_LEAF_203#
```

❖ LEAF & SPINE Node SSH 접속

> show snmp ⇒ SNMP In/Out packet

```
DC4_LEAF_203# show snmp
sys contact:
sys location:

1127143 SNMP packets input
  0 Bad SNMP versions
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  14098331 Number of requested variables
  0 Number of altered variables
  345266 Get-request PDUs
  781169 Get-next PDUs
  0 Set-request PDUs
  0 No such name PDU
  0 Bad value PDU
  0 Read Only PDU
  0 General errors
  0 Get Responses
  708 Unknown Context name
1128201 SNMP packets output
  1766 Trap PDU
  0 Too big errors (Maximum packet size 0)
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Get Requests
  0 Get Next Requests
  0 Set Requests
  1126435 Get Responses
  0 Silent drops

Community      Group / Access      context      acl_filter
-----
infra           network-admin
```

1. Basic Operation > 1.11 DHCP Relay 확인

DHCP Relay Provider 등록

- ❖ Fabric > Access Policies
- > Global Policies > DHCP Relay Policies ⇒ Create DHCP Relay Policy

The screenshot shows the Cisco ACI UI interface. On the left, there's a navigation bar with tabs like System, Tenants, Fabric, etc. The main area is titled "Global Policies - DHCP Relay Policies". It lists a single policy named "DHCP_RELAY_POLICY" with details: "DHCP Server" is 10.211.11.11 and "Associated EPG" is L3OUT_HYNIX. A yellow arrow points from the "Associated EPG" field to the "Create DHCP Provider" dialog box below.

Create DHCP Provider

Create DHCP Relay Provider

EPG Type: Application EPG
 L3 External Network
 L2 External Network
 DN

L3 External Network: WT_TENANT
Tenant:

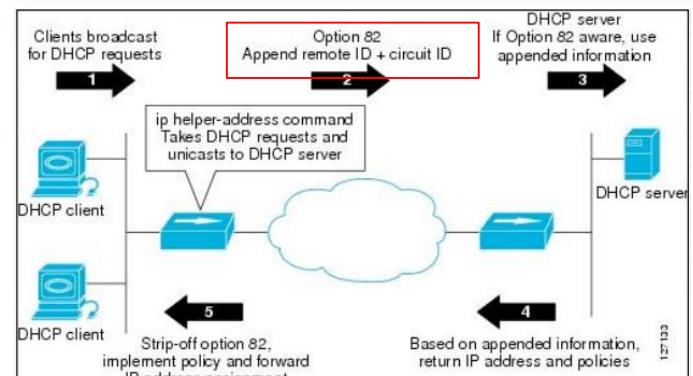
L3 Out:
L3OUT_BB
External Network: L3OUT_HYNIX

DHCP Server Address: 10.211.11.11

DHCP 서버가 연결되는 EPG 정의
(Fabric이 L3OUT을 통해 DHCP Server와 통신)

OK CANCEL

DHCP Relay 동작



1. Basic Operation > 1.11 DHCP Relay 확인 (계속)

BD에 DHCP Relay Label 할당

- ❖ Tenants > User Tenant(WT_TENANT)
 - > Networking > Bridge Domains > User_BD(PC1_BD) >DHCP Relay Labels
⇒ Create DHCP Relay Policy

The screenshot shows the Cisco ACI GUI interface. The top navigation bar includes System, Tenants, Fabric, Networking, Admin, Operations, and Advanced Mode. The Tenant dropdown is set to 'welcome, admin'. The main content area shows the 'Tenants' view for 'WT_TENANT'. On the left, a navigation tree lists various network components like Quick Start, Tenant WT_TENANT, Application Profiles, Networking, Bridge Domains (with entries for LINE_A_BD, LINE_B_BD, LINE_C_BD, LINE_D_BD, and PC1_BD), and DHCP Relay Labels (with a specific entry for 'DHCP_RELAY_POLICY'). A red box highlights this entry. A yellow arrow points from this entry to a 'Create DHCP Relay Label' dialog box on the right. This dialog box has fields for Scope (set to 'infra'), Name ('DHCP_RELAY_POLICY'), and DHCP Option Policy ('select a value'). It also features 'SUBMIT' and 'CANCEL' buttons.

1. Basic Operation > 1.12 SPAN (Tenant SPAN)

SPAN Destination (EPG)

- ❖ Fabric > Access Policies
 - > Troubleshooting Policies > SPAN > SPAN Destination Groups

The screenshot shows the 'SPAN Destination - SPAN_DEST_EPG' configuration page. The 'Properties' section includes fields for Name (SPAN_DEST_EPG) and Description (optional). The 'Destination EPG' section is highlighted with a red box and contains the following details:

- Destination EPG: uni/t-TEST_TENANT/ap-TEST_APN/epg-TEST_EPG
- SPAN Version: Version 1
- Destination IP: 192.168.30.221
- Source IP/Prefix: 192.168.30.1
- Flow ID: 1
- TTL: 64
- MTU: 1518
- DSCP: Unspecified

SPAN Source (EPG & Path)

- ❖ Fabric > Access Policies
 - > Troubleshooting Policies > SPAN > SPAN Source Groups

The screenshot shows the 'SPAN Source - SPAN_SRC' configuration page. The 'Properties' section includes fields for Name (SPAN_SRC) and Description (optional). The 'Source EPG' field is highlighted with a red box and contains the value: uni/t-TEST_TENANT/ap-TEST_APN/epg-TEST_EPG. Below it, the 'Source Paths' section lists a single path: Node-202/eth1/1.

1. Basic Operation > 1.12 SPAN (Infra SPAN)

SPAN Destination (Port)

- ❖ Fabric > Access Policies
 - > Troubleshooting Policies > SPAN > SPAN Destination Groups

The screenshot shows the 'SPAN Destination Group - SPAN_DEST1' configuration page. The 'Properties' section has 'Name: SPAN_DEST1' and 'Description: optional'. The 'Destinations' table has one row:

Name	Description	Destination EPG	Destination Path
SPAN_DEST_Port			Node-201/eth1/10

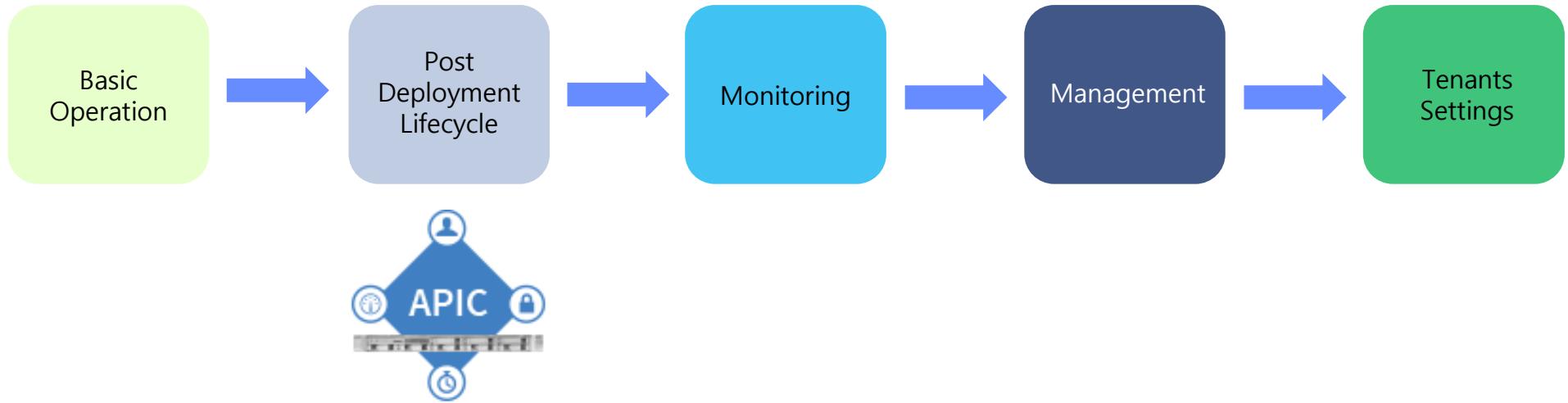
SPAN Source (Port)

- ❖ Fabric > Access Policies
 - > Troubleshooting Policies > SPAN > SPAN Source Groups

The screenshot shows the 'SPAN Source - SPAN_SRC_Port' configuration page. The 'Properties' section has 'Name: SPAN_SRC_Port' and 'Description: optional'. The 'Source Paths' table has one row:

Source Access Path
Node-201/eth1/3

2) Post Deployment Lifecycle



2. Post Deployment Lifecycle

Monitoring

- Faults
- Events
- Health Score
- Atomic Counter
- Contract deny logs
- Statistics
- Fabric Capacity
- Dashboard
- Call Home / SNMP / Syslog

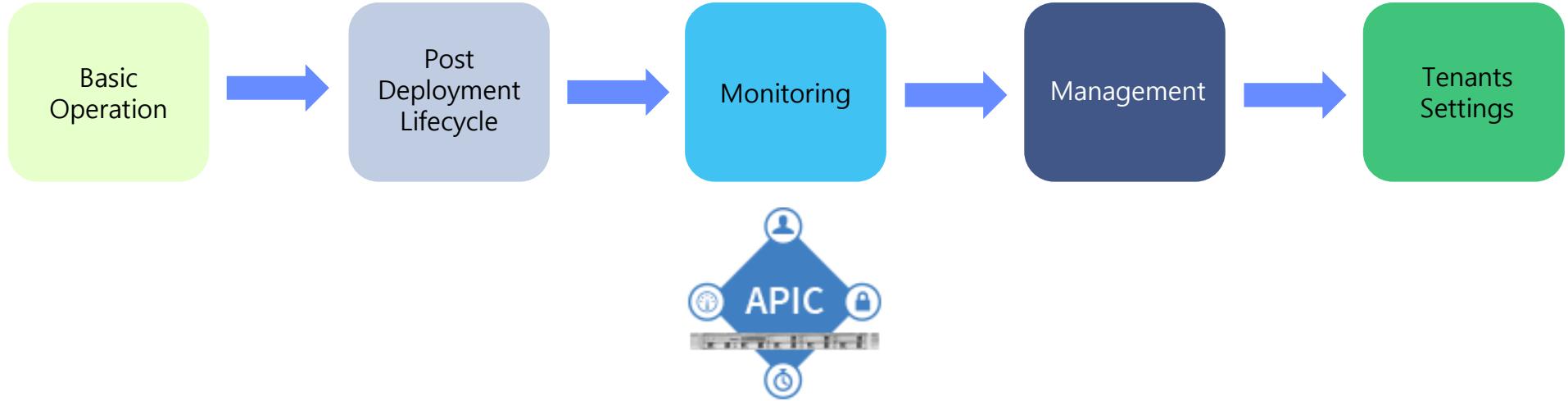
Management

- Image Management
- Config Export / Import
- Fabric Inventory

Troubleshooting

- Audit Logs
- iPing
- iTraceroute
- SPAN
- Managed Object Browser (Visore)
- Troubleshooting Wizard

3) Monitoring

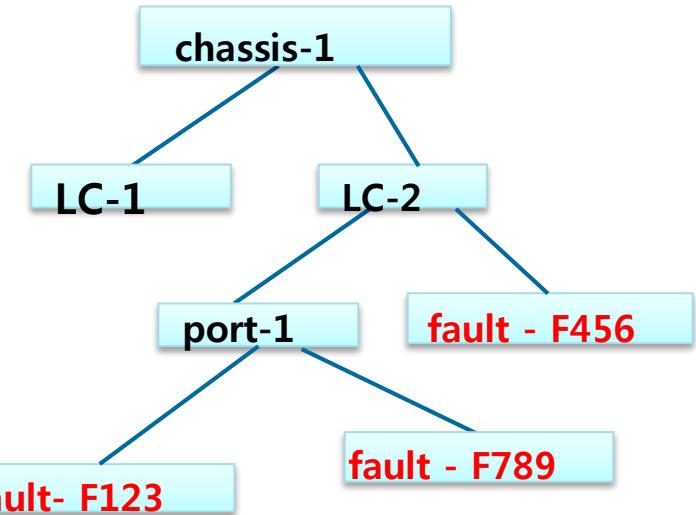


3. Monitoring > 3.1 Fault

What is Fault ?

- ❖ System 의 비정상적인 상황을 파악하도록 함
- ❖ Fault는 MIT(Management Information Tree)에서 정의된 Managed Object의 하위 MO임
- ❖ Fault Properties
 - Code
 - Severity
 - Lifecycle
 - Description
 - Timestamps

Fault Example



Condition	User Action
Operational (example: link down)	Check link, SFP, etc.
Physical resource unavailable (example: not enough fans)	Provide missing resource
HW malfunction (example: memory errors, CRC errors, component failures, spurious resets, etc.)	reset component, run diags, call Cisco TAC
Environmental (example: board temperature too high)	Clear air flow or shutdown overheated component
Inconsistent or incomplete configuration (example: ports in a port-channel have different config)	Correct the configuration
Failed policy deployment, clustering issues	Debug connectivity issues
Logical resource unavailable (example: ID, address, ...)	Provide missing resource

3. Monitoring > 3.1 Fault (계속)

Fault Lifecycle

❖ Fault Triggers

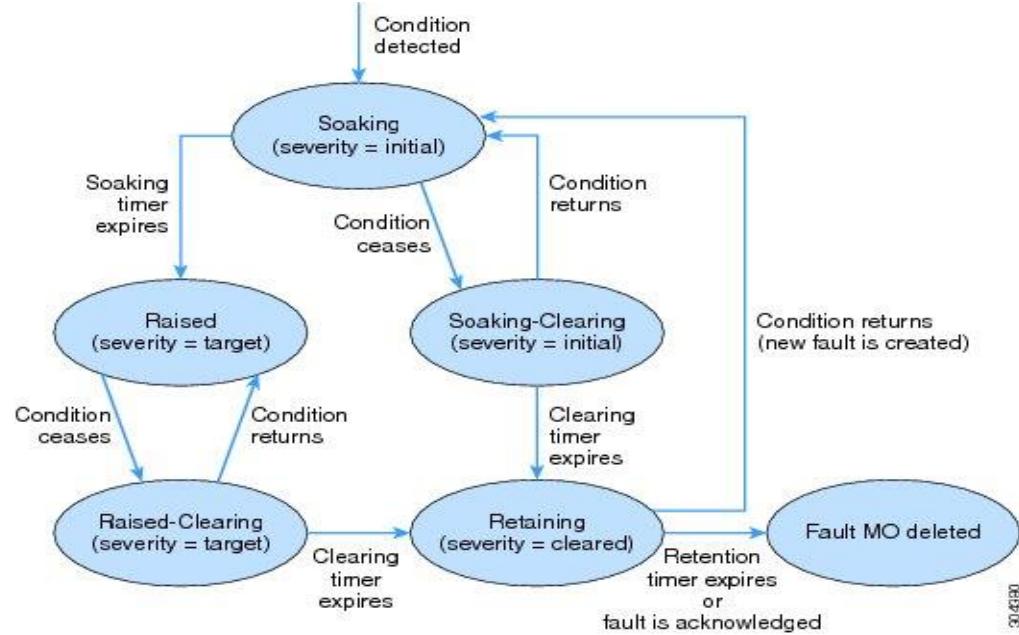
- MO에서 정의된 fault rule의 조건에 부합할 경우
- 특정 counter 가 사용자가 정의한 threshold 이상일 때
- Task 또는 FSM Failure 발생 시
- Object Resolution failure

❖ Fault Life cycle

- Soacking (fault condition 감지) \Rightarrow Soaking-Clearing
- Raised (Soaking timer expire & severity=target)
- Raised Clearing (fault condition 중지)
- Retaining (Clearing timer expire)
- Deleted (Retention timer expire / fault acknowledged)

❖ Fault 동작

- Fault는 fault 조건이 발생한 Switch 또는 Controller에서 Raised 되고 Managed 됨
- Fault는 system에 의해서 자동적으로 Raised 되고 Cleared 됨
- 사용자는 신규 Fault를 정의할 수 없음



3. Monitoring > 3.1 Fault (계속)

Fault Summary

❖ System > Faults

CISCO System Tenants Fabric VM Networking L4-L7 Services Admin Operations Faults Config Zones Advanced Mode welcome, admin *

QuickStart | Dashboard | Controllers Faults Config Zones

Faults i

↻ ⬇ ◀ ▶

Severity	Code	Count	Cause	Sample Fault Description
⚠	F1543	4	node-inactive	This fault occurs when a node is not reachable
⚠	F0532	31	interface-phys...	This fault occurs when a port is down and is in use for infra and epg
⚠	F107496	2	threshold-cros...	Threshold crossing alert for clusterinfraClusterState5min_property_uTimelast
⚠	F0321	2	unhealthy	
⚠	F1296	16	interface-vpc...	
⚠	F2194	26	policy-deploy...	
⚠	F0103	2	port-down	
⚠	F1371	44	policy-deploy...	
⚠	F0475	7	interface-tunn...	
⚠	F0467	1	configuration-...	
⚠	F1298	4	configuration-...	
⚠	F1299	10	configuration-...	
⚠	F1394	3	interface-phys...	
⚠	F1262	18	unhealthy	
⚠	F1700	1	protocol-ntp-s...	

Faults Fault Code 별 Fault list i

↻ ⬇ ✓ □ ◀ ▶ ⚙️

Severity	Acknowledged	Code	Cause	Creation Time	Last Transition	Affected Object	Lifecycle
⚠	<input checked="" type="checkbox"/>	F1543	node-inactive	2016-05-04T19:51:58.406+09:00	2016-05-04T19:54:12.223+09:00	topology/pod-1/node-152	Raised
⚠	<input checked="" type="checkbox"/>	F1543	node-inactive	2016-05-04T19:51:58.407+09:00	2016-05-04T19:54:12.218+09:00	topology/pod-1/node-151	Raised
⚠	<input checked="" type="checkbox"/>	F1543	node-inactive	2016-05-04T19:51:58.406+09:00	2016-05-04T19:54:12.220+09:00	topology/pod-1/node-251	Raised
⚠	<input checked="" type="checkbox"/>	F1543	node-inactive	2016-05-04T19:52:39.761+09:00	2016-05-04T19:55:07.920+09:00	topology/pod-1/node-252	Raised

Page 1 Of 2 | Objects Per Page: 15 | Displaying Objects 1 - 15 Of 19

nynix INSANG 인성정보

3. Monitoring > 3.1 Fault (계속)

Fault Properties

Fault Properties



Properties

Fault Code: F1543
Severity: critical
Last Transition: 2016-05-04T19:54:12.223+09:00
Lifecycle: Raised
Affected Object: topology/pod-1/node-152
Description: Node 152 is inactive and not reachable.

Explanation:
This fault occurs when a node is not reachable

Recommended Action:
If you see this fault, take the following action:

Check connectivity for the node that cannot be reached
Check if the node is powered up
If the node is decommissioned, clean reboot the node manually as a workaround
If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Details

Type: Environmental
Cause: node-inactive
Change Set: adSt (Old: on, New: off), fabricSt (Old: active, New: inactive)
Created: 2016-05-04T19:51:58.406+09:00
Code: F1543
Number of Occurrences: 1
Original Severity: critical
Previous Severity: critical
Highest Severity: critical



General

Action

Fault에 대한 help information

Cisco System Model: Fault fitFabricNodeInactive Cisco System Model: Class ifc:topoMqr#fitFabricNodeInactive - Chrome
https://10.210.9.11/doc/html/FAULT-F1543.html

Fault fitFabricNodeInactive

Rule ID:1543

Explanation:
This fault occurs when a node is not reachable

Recommended Action:
If you see this fault, take the following action:

1. Check connectivity for the node that cannot be reached
2. Check if the node is powered up
3. If the node is decommissioned, clean reboot the node manually as a workaround
4. If the above actions did not resolve the issue, create a **show tech-support** file and contact Cisco TAC.

Raised on MO: [fabric.Node](#)
Fault Name: fitFabricNodeInactive
Unqualified API Name: Inactive
Code: F1543
Applied Mo DN Format:
[topology/pod-\[id\]/node-\[id\]](#)

Type: environmental
Cause: node-inactive
Severity: critical
Weight: 100
Tags:
Message: Node [id](#) is inactive and not reachable.

Help:

Triggered By:
[fabricSt](#) equals inactive
and
[role](#) not equals controller

3. Monitoring > 3.1 Fault (계속)

Fault Lifecycle Policy

- ❖ Fabric > Fabric Policies
 - > Monitoring Policies > Common Policy > Fault Lifecycle Policy

The screenshot shows the Cisco Fabric Manager interface under the 'Fault Lifecycle Policy' section. On the left sidebar, 'Fault Lifecycle Policy' is highlighted with a red box. In the main panel, there's a 'Properties' section with fields for 'Code: any', 'Clearing Interval (s): 120', 'Retention Interval (s): 3600', and 'Soaking Interval (s): 120'. A red box highlights this section. Below it, a yellow arrow points from the 'Fault Severity Assignment Policies' section to the 'Properties' section, with the text 'Fault Code 별 severity 변경' (Change Fault Code by severity). Another yellow arrow points from the 'Fault Lifecycle Policies' section to the 'Properties' section, with the text 'Fault Code 별 Lifecycle Timer 변경' (Change Fault Code by Lifecycle Timer).

Fault Acknowledgement

- ❖ Fault Acknowledgement
 - "Acknowledged"는 단순히 확인하였다는 의미임
 - "retaining" 상태의 fault는 acknowledging 하는 순간 fault 가 delete 됨
 - 다른 상태의 fault는 acknowledging 해도 영향 없음

The screenshot shows two configuration panels. The top panel is 'Fault Severity Assignment Policies' for 'Fabric Module (eqpt.FC)'. It lists a rule: 'Code: F0416 [fitEqptCardUnknownSwld]', 'Initial Severity: warning', and 'Target Severity: critical'. Buttons for 'UPDATE' and 'CANCEL' are at the bottom. The bottom panel is 'Fault Lifecycle Policies' for the same object. It shows the same rule with clearing, retention, and soaking intervals all set to 120 seconds. Buttons for 'UPDATE' and 'CANCEL' are at the bottom.

3. Monitoring > 3.2 Event

Events in GUI

❖ Fabric > Inventory
 > Pod1 ⇒ History / Events

The screenshot shows the Cisco ACI GUI interface. The top navigation bar includes System, Tenants, Fabric, VM Networking L4-L7 Services, Admin, Operations, and Advanced Mode (welcome, admin). The Fabric menu is selected. Below the navigation is a sub-menu for Inventory, with 'Pod 1' highlighted by a red box. The main content area is titled 'POD - 1' and shows a table of events. The 'Events' tab is selected. The table columns are Severity, Affected Object, Code, Cause, Creation Time, and Description. One event row is highlighted with a red box and a yellow arrow points to its detailed view. The detailed view is titled 'Record - 8589944930' and contains properties such as ID, Description, Severity, Affected Object, Created, Code, Cause, Change Set, Action, Action Trigger, Transaction ID, and User.

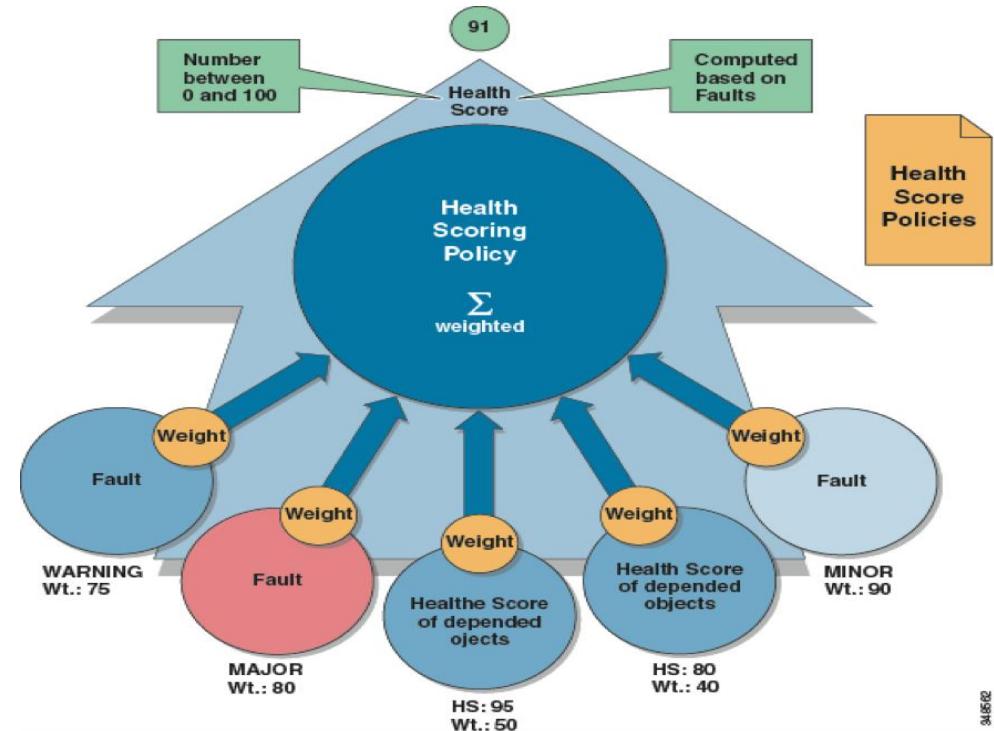
Severity	Affected Object	Code	Cause	Creation Time	Description
Info	topology/pod-1/node-203/sys/phys-[eth1/44]/phys	E4205125	port-up	2016-06-07T12:53:08.417+09:00	Port is up
Info	topology/pod-1/node-204/sys/phys-[eth1/44]/phys	E4205125	port-up	2016-06-07T12:53:08.229+09:00	Port is up
Info	topology/pod-1/node-203/sys/phys-[eth1/44]/phys	E4205126	port-down	2016-06-07T12:53:02.773+09:00	Port is down. Reason: notconnect
Info	topology/pod-1/node-204/sys/phys-[eth1/44]/phys	E4205126	port-down	2016-06-07T12:53:02.615+09:00	Port is down. Reason: notconnect
Info	topology/pod-1/node-204/sys/phys-[eth1/44]/phys	E4205125	port-up	2016-06-07T12:50:37.449+09:00	Port is up
Info	uni/tn-DC_TENANT/ap-DC_AP/epg-WT_EPG/cep-D8:9D:67:1B:85:68/ip-[10.192.53.34]	E4209236	transition	2016-06-07T12:50:36.403+09:00	IP detached. EPG: uni/tn-DC_TENANT/ap-DC_AP/epg-WT_EPG. IP: 10.192.53.34
Info	topology/pod-1/node-203/sys/phys-[eth1/44]/phys	E4205125	port-up	2016-06-07T12:50:35.134+09:00	Port is up
Info	topology/pod-1/node-204/sys/phys-[eth1/44]/phys	E4205126	port-down	2016-06-07T12:50:31.805+09:00	Port is down. Reason: notconnect
Info	topology/pod-1/node-204/sys/phys-[eth1/44]/phys	E4205125	port-up	2016-06-07T12:50:31.621+09:00	Port is up
Info	topology/pod-1/node-203/sys/phys-[eth1/44]/phys	E4205126	port-down	2016-06-07T12:50:26.302+09:00	Port is down. Reason: notconnect
Info	topology/pod-1/node-204/sys/phys-[eth1/44]/phys	E4205126	port-down	2016-06-07T12:50:26.003+09:00	Port is down. Reason: notconnect
Info	topology/pod-1/node-204/sys/phys-[eth1/45]/phys	E4205125	port-up	2016-06-07T12:13:10.202+09:00	Port is up
Info	topology/pod-1/node-203/sys/phys-[eth1/45]/phys	E4205125	port-up	2016-06-07T12:13:10.023+09:00	Port is up
Info	topology/pod-1/node-204/sys/phys-[eth1/45]/phys	E4205126	port-down	2016-06-07T12:13:04.570+09:00	Port is down. Reason: notconnect
Info	topology/pod-1/node-203/sys/phys-[eth1/45]/phys	E4205126	port-down	2016-06-07T12:13:04.424+09:00	Port is down. Reason: notconnect

- ❖ Event is ...
- Log file과 유사
(개발자가 정의한 event rule을 충족한 상황에서 발생)
 - System MO에서 event:Record class로 표시됨
 - Event가 생성되면 수정 되지 않음
 - Monitoring과 Debugging에 유용함
 - Fault와 같이 전체 Pod 또는 Switch별 확인이 가능함

3. Monitoring > 3.3 Health Score

What is Health Score

- ❖ System 과 Module의 상태를 직관적인 점수로 보여줌
- ❖ Health Score는 Fault에 의해 결정됨
 - Range: 0 ~ 100
 - Fault 의 severity에 의해서 score가 감소됨
 - Score는 관련된 MO로 전파됨
 - HealthScore Policy로 penalty value, propagation 및 Health Records를 제어할 수 있음
- ❖ Health Score Views
 - System level
Pod score+(System fault count, APIC cluster health state)
 - POD
POD(Spine & Leaf) score, POD-wide fault count
 - Tenant
Tenant(EPG) score, Performance data, tenant fault count
 - Managed Object
MO health score



3. Monitoring > 3.3 Health Score (계속)

System Health Score

❖ System > Dashboard

CISCO System Tenants Fabric VM Networking L4-L7 Services Admin Operations Advanced Mode welcome, admin -

QuickStart | Dashboard | Controllers | Faults | Config Zones

System Health

System Health Score: 56

Fault Counts By Domain

Fault Level:	!	⚠	!	!
SYSTEM WIDE	39	103	37	72
Access	31	7	3	18
External	0	0	0	6
Framework	0	78	0	0
Infra	8	18	29	48
Management	0	0	0	0
Security	0	0	0	0
Tenant	0	0	5	0

Nodes With Health ≤ 99

Name	Type	Health Score
DC4_EXT_LEAF_201	leaf	95
DC4_EXT_LEAF_202	leaf	95
DC4_LEAF_203	leaf	59
DC4_LEAF_204	leaf	62
DC4_LEAF_205	leaf	95

Node Health Score

99

Tenants With Health ≤ 99

Name	Health Score
DC_TENANT	40

Tenant Health Score

99

Fault Counts By Type

Fault Level:	!	⚠	!	!
Communication	31	23	3	2
Config	0	0	15	0
Environmental	4	0	0	0
Operational	4	80	19	70

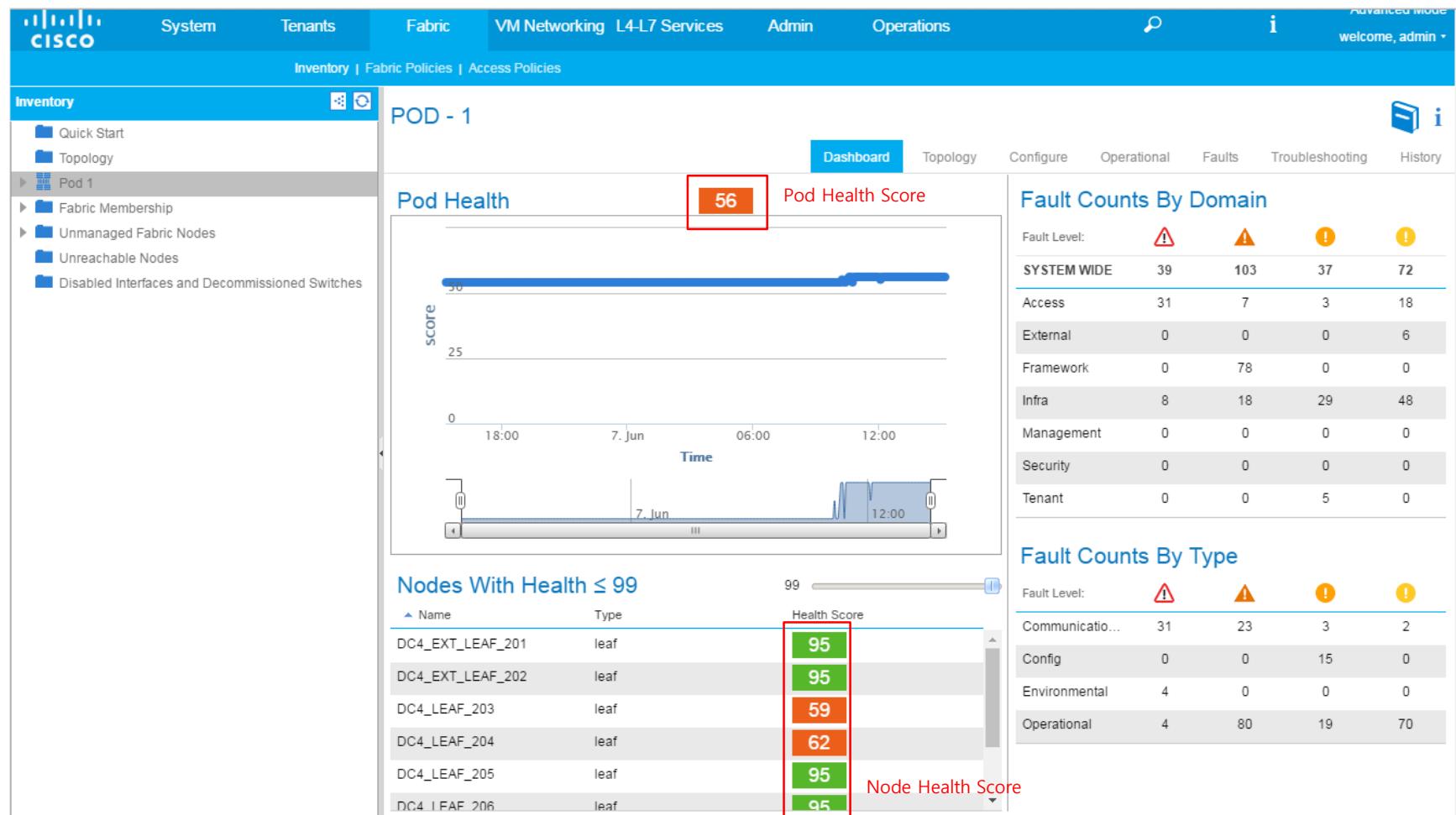
Controller Status

ID	Name	IP	Admin State	Operational State	Health State
1	DC_AP...	20.0.0.1	In Service	Available	Fully Fit
2	DC_AP...	20.0.0.2	In Service	Available	Fully Fit
3	DC_AP...	20.0.0.3	In Service	Unavailable	Unknown

3. Monitoring > 3.3 Health Score (계속)

Pod Health Score

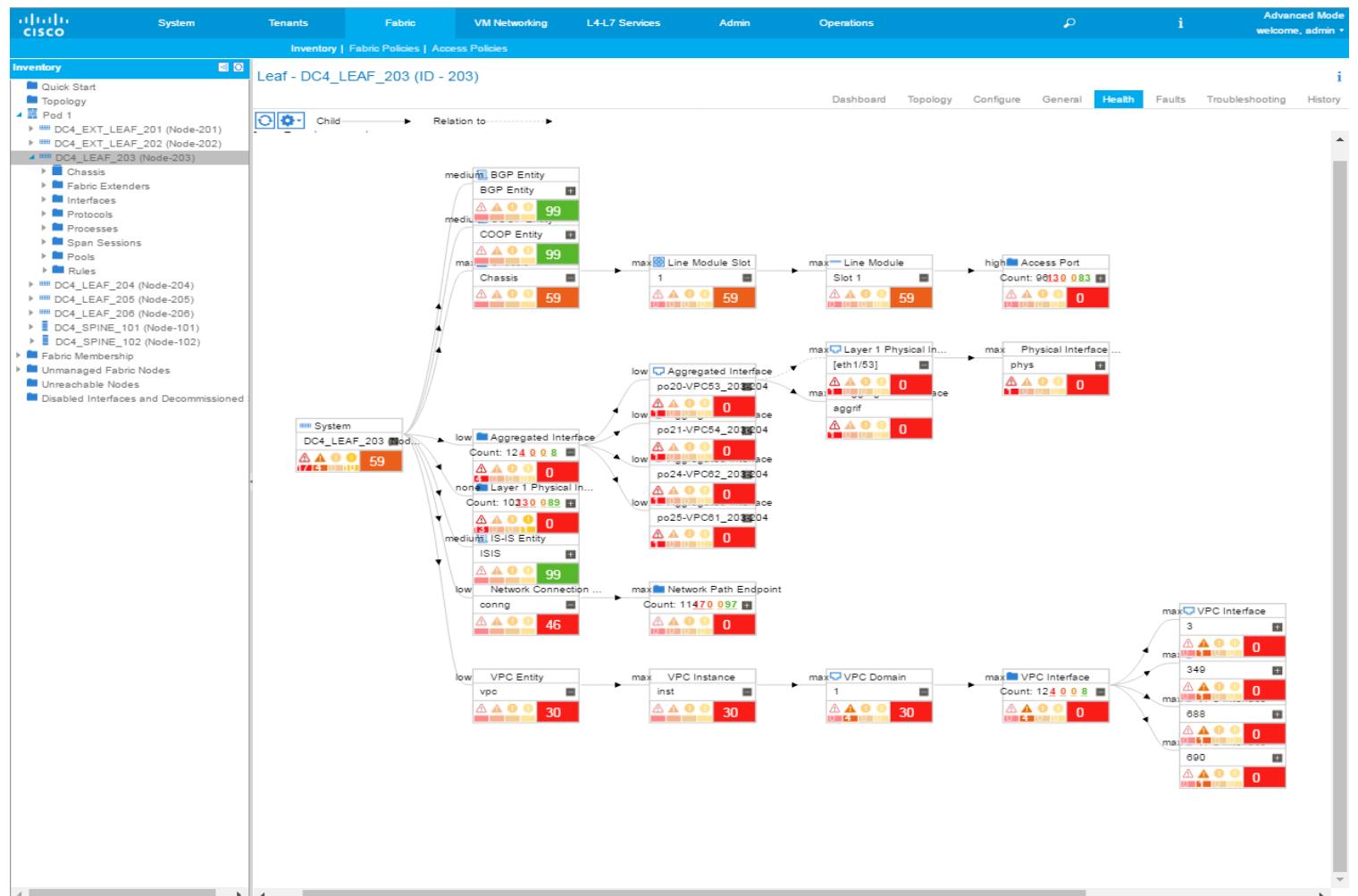
❖ Fabric > Inventory
> Pod



3. Monitoring > 3.3 Health Score (계속)

Node Health Score

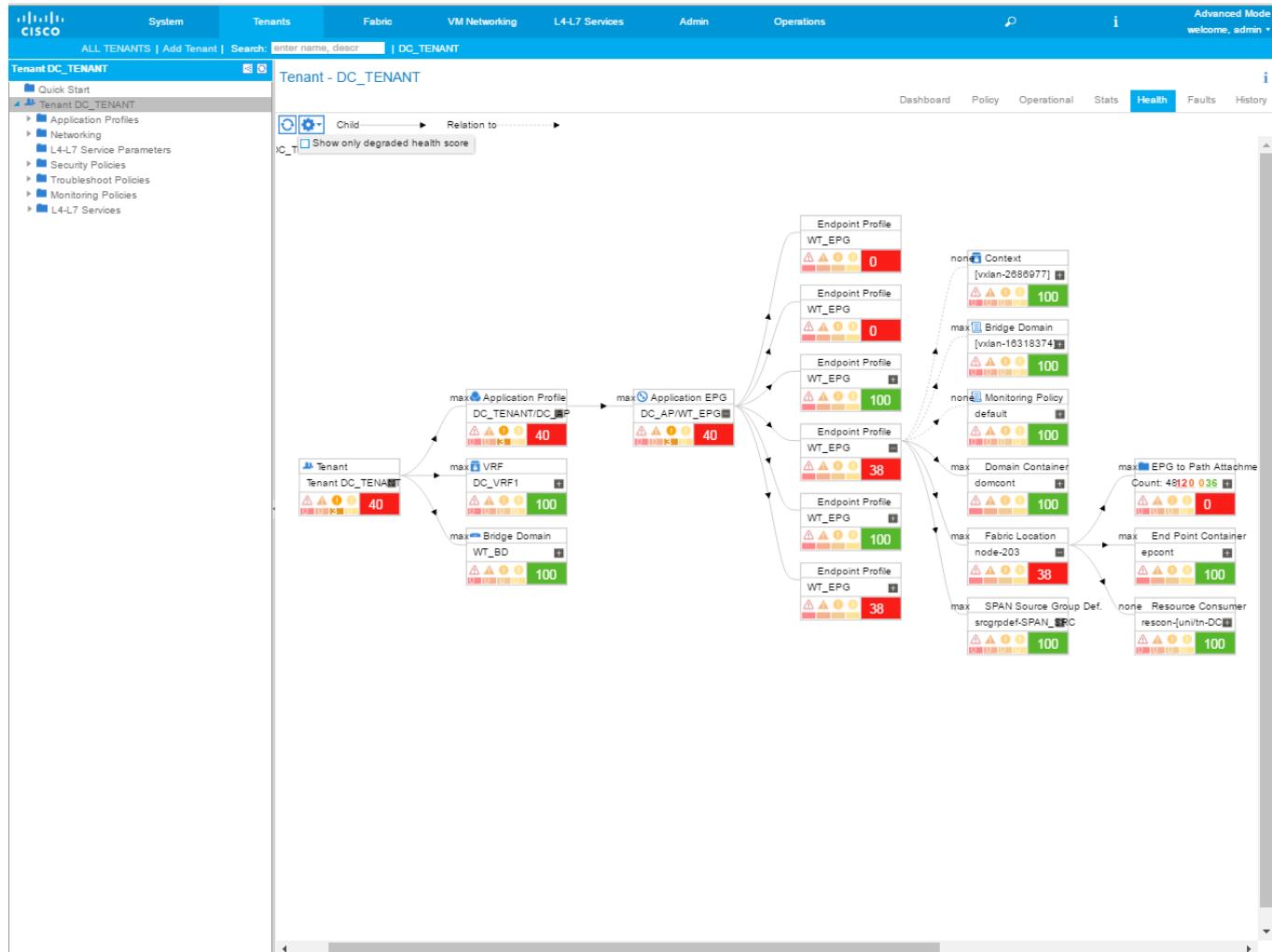
- ❖ Fabric > Inventory
 - > Pod1
 - > Node(LEAF203)
 - ⇒ Health



3. Monitoring > 3.3 Health Score (계속)

❖ Tenants
 > User_Tenant
 ⇒ Health

Tenant Health Score



3. Monitoring > 3.3 Health Score (계속)

Health Score Evaluation Policy

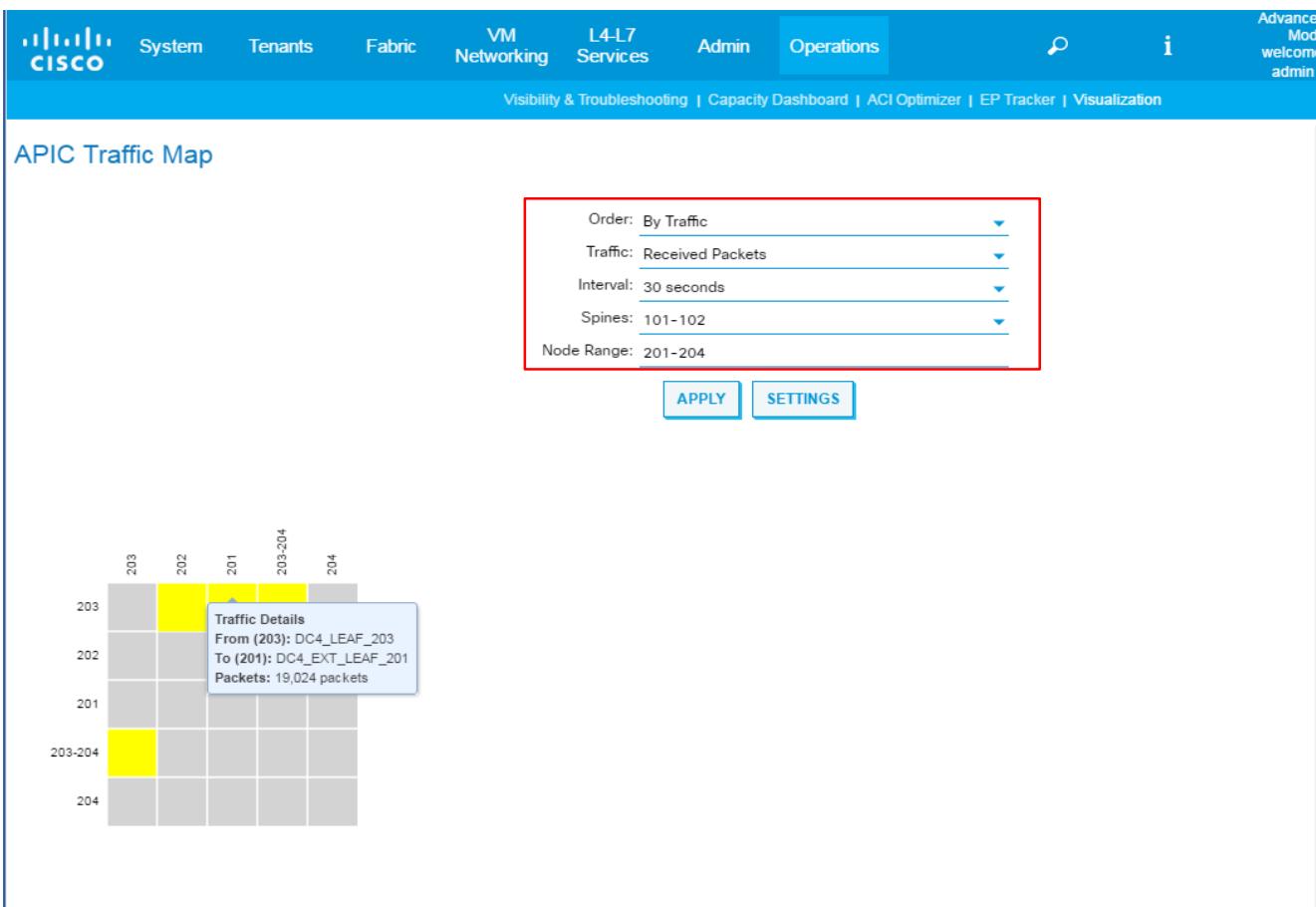
- ❖ Fabric > Fabric Policies
 - > Monitoring Policy > Common Policy
 - > Health Score Evaluation Policies > Health Score Evaluation Policy

The screenshot shows the Cisco ACI Policy Manager interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and Advanced Mode (welcome, admin). The Fabric tab is selected. Below the navigation is a breadcrumb trail: Inventory | Fabric Policies | Access Policies. On the left, a sidebar titled 'Policies' lists various policy types: Quick Start, Switch Policies, Module Policies, Interface Policies, Pod Policies, Global Policies, Monitoring Policies, Common Policy, Health Score Evaluation Policies, and a selected 'Health Score Evaluation Policy'. The main content area is titled 'Health Evaluation Policy - Health Score Evaluation Policy'. It displays a 'Properties' section with a 'Description' field containing 'Default Health Score Evaluation Policy from IFC'. Below this are four input fields for fault severity penalties: 'Penalty of fault severity critical (in %): 100', 'Penalty of fault severity major (in %): 10', 'Penalty of fault severity minor (in %): 2', and 'Penalty of fault severity warning (in %): 1'. A red box highlights the first three input fields. To the right of these fields is a note in Korean: 'Severity Level에 따른 Penalty 변경이 가능' and '개별 fault에 대해서는 Penalty 변경이 안됨'. The bottom of the properties section has an 'Ignore Acknowledged Faults' checkbox.

3. Monitoring > 3.4 Atomic counters (Traffic MAP)

Atomic counters (Traffic Map)

- ❖ Operations > Visualization
 > APIC Traffic Map



Atomic Counters

- ❖ Atomic Counter is ...
 - Fabric을 경유하는 packet에 대한 counting value 제공
 - Local switched되는 packet은 해당하지 않음
 - Hypervisor 내부에서 switched 되는 packet은 해당하지 않음

❖ APIC Traffic Map

- Leaf-To-Leaf 통신에 대한 Atomic Counter 값 제공
- Interval Cumulative (누적값)
30seconds (30초마다 refresh)
- Node Traffic이 경유하는 SPINE과 Leaf node 지정
- Traffic Map Source Leaf ~ Destination Leaf 간 packet counter 제공

3. Monitoring > 3.4 Atomic counters (Troubleshooting Policy)

Atomic Counter Policy

- ❖ Tenant > User_Tenant
 - > Troubleshooting Policies >
 - > Atomic Counter Policy > Ext to EP (트래픽 유형별 선택) > TEST4

The screenshot shows the Cisco ACI Troubleshooting Policy interface. The left sidebar navigation includes:

- System
- Tenants
- Fabric
- VM Networking
- L4-L7 Services
- Admin
- Operations

The Tenant DC_TENANT section is expanded, showing:

- Quick Start
- Tenant DC_TENANT
- Application Profiles
- Networking
- L4-L7 Service Parameters
- Security Policies
- Troubleshoot Policies
 - SPAN
 - Endpoint-to-Endpoint Traceroute Policies
 - Endpoint-to-External-IP Traceroute Policies
 - Atomic Counter Policy
 - EP to EP
 - EP to EPG
 - EP to Ext
 - TEST4_dst_ext
 - EPG to EP
 - EPG to EPG
 - EPG to IP
 - Ext to EP
 - TEST4_ext_dst
 - Any to EP
 - IP to EPG
 - EP to Any
- Monitoring Policies
- L4-L7 Services

The main panel displays the configuration for the policy "Ext-to-EP TEST4_ext_dst". The "Properties" section includes:

- Name: TEST4_ext_dst
- Source IP: 10.192.29.14 (highlighted with a red box)
- Description: optional
- Administrative State: Enabled (highlighted with a blue box)
- Destination IP: DC_TENANT/DC_AP/28:80:23:9A:DA:87/10.192.53.22 (highlighted with a red box)
- State: formed

The "Filters" section shows a table with the following columns: Name, Protocol, Source Port, Destination Port, and Description. The table currently displays the message: "No items have been found. Select Actions to create a new item."

At the bottom right of the main panel are three buttons: SHOW USAGE, SUBMIT, and RESET.

3. Monitoring > 3.4 Atomic counters (Troubleshooting Policy)

Atomic Counter Policy (Operational)

- ❖ Tenant > User_Tenant
 - > Troubleshooting Policies >
 - > Atomic Counter Policy > Ext to EP > TEST4(사용자 트래픽) ⇒ Operational

CISCO System Tenants Fabric VM Networking L4-L7 Services Admin Operations Advanced Mode welcome, admin ▾

ALL TENANTS | Add Tenant | Search: enter name, descr | common | DC_TENANT | SPAN_TENANT | infra | mgmt

Tenant DC_TENANT

- Quick Start
- Tenant DC_TENANT
 - Application Profiles
 - Networking
 - L4-L7 Service Parameters
 - Security Policies
 - Troubleshoot Policies
 - SPAN
 - Endpoint-to-Endpoint Traffic
 - Endpoint-to-External-IP Traffic
 - Atomic Counter Policy
 - EP to EP
 - EP to EPG
 - EP to Ext
 - TEST4_dst_ext
 - EPG to EP
 - EPG to EPG
 - EPG to IP
 - Ext to EP
- TEST4_ext_dst
- Any to EP
- IP to EPG
- EP to Any
- Monitoring Policies
- L4-L7 Services

Ext-to-EP TEST4_ext_dst

Ext-to-EP Counter TEST4_ext_dst Traffic

Source	Destination	Last Collection (30 Seconds)			Tot				Percentage			
		Transmit Pkt	Admitted Pkt	Dropped Pkt	Transmit Pkt	Admitted Pkt	Dropped Pkt	Excess Pkt	Drop Pkt %	Excess Pkt %	Tot Drop Pkt %	Tot Excess Pkt %
10.19...	uni/tn-...	34	34	0	1383960	1383960	0	0	0	0	0	0

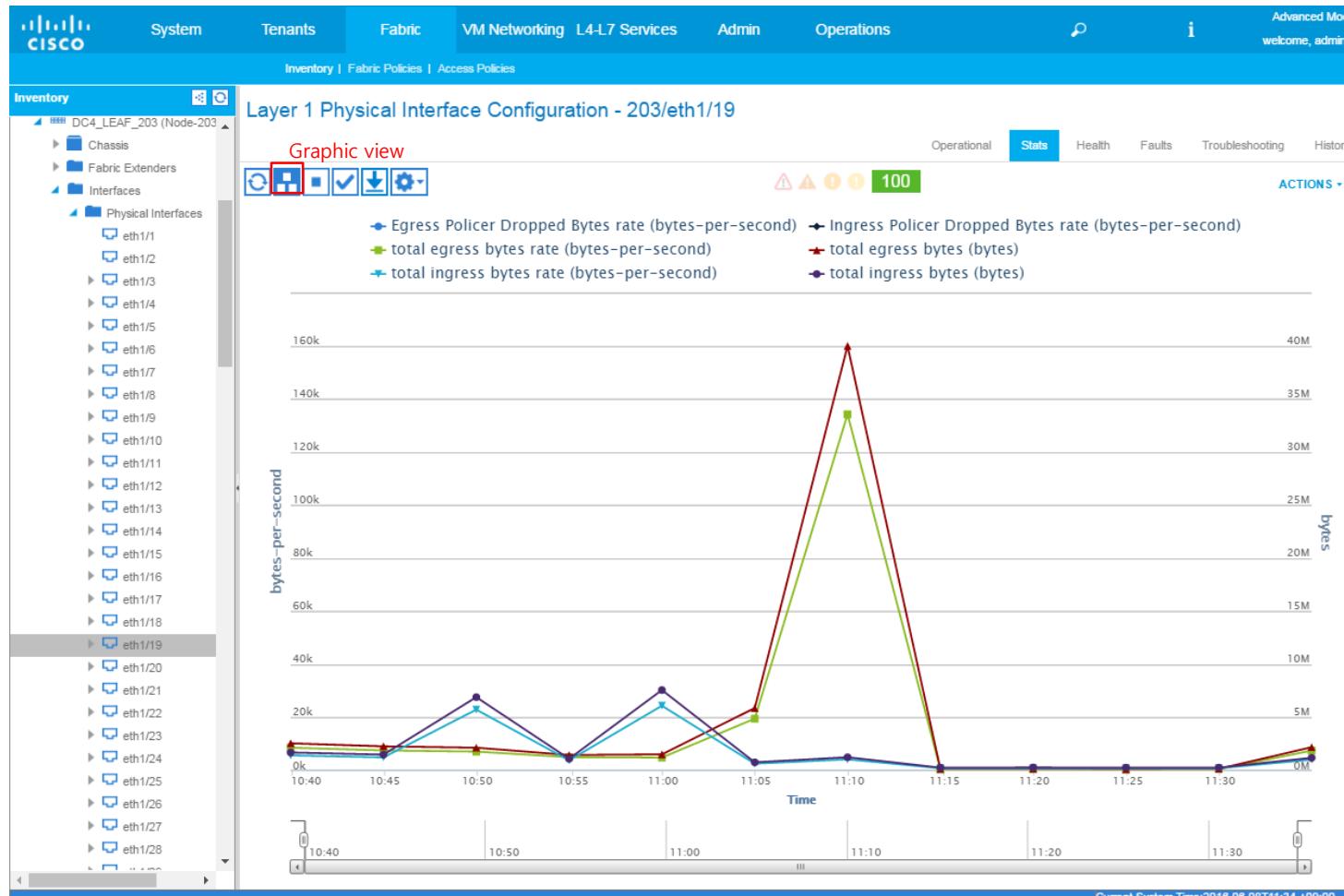
Source IP Destination IP 30초 단위 packet counter 누적 packet counter Percentage

SHOW USAGE SUBMIT RESET

3. Monitoring > 3.4 Statistics

Statistics (Chart view)

❖ Fabric > Inventory
 > Pod1 > DC4_LEAF_203(Node-203) > Interfaces > Physical Interface ⇒ Stats



- ❖ Statistics 제공 기능
- Provides historical data
 - Generic Threshold definition
 - Streamed export of statistical data in real time
 - Enables analytics and trending
 - Configurable options for retention and collection intervals

3. Monitoring > 3.4 Statistics (계속)

Statistics (Table View)

❖ Fabric > Inventory
> Pod1 > DC4_LEAF_203(Node-203) > Interfaces > Physical Interface ⇒ Stats

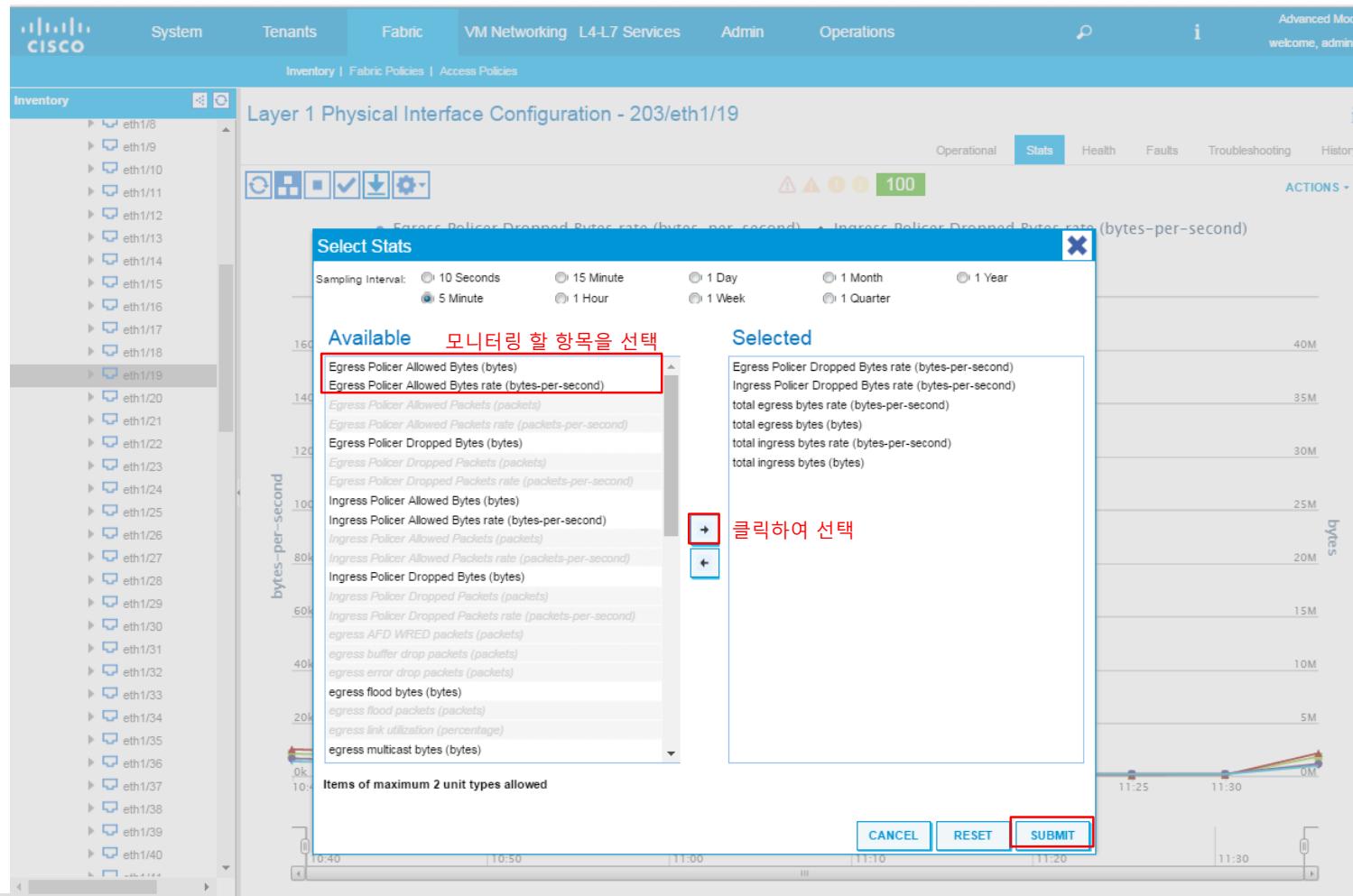
The screenshot shows the Cisco ACI Fabric Manager interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and a search bar. The Fabric tab is selected. The left sidebar shows the inventory structure under DC4_LEAF_203, including Chassis, Fabric Extenders, and various interfaces (eth1/1 through eth1/18). The main content area displays the "Layer 1 Physical Interface Configuration - 203/eth1/19". The interface has a status of "Operational" and is currently monitoring "Stats". The table below shows traffic statistics over time:

Timestamp	Egress Policer Dropped Bytes Rate	Ingress Policer Dropped Bytes Rate	Total Egress Bytes Rate	Total Egress Bytes	Total Ingress Bytes Rate	Total Ingress Bytes
2016/06/08 10:39:55			8687	2588524	5786	1724289
2016/06/08 10:44:56			7652	2303197	5054	1521238
2016/06/08 10:49:57			7228	2175051	23040	6933282
2016/06/08 10:54:46			5130	1481330	3913	1130084
2016/06/08 10:59:57			4994	1548939	24495	7597177
2016/06/08 11:04:57			19631	5906149	2660	800443
2016/06/08 11:09:55			134221	39984201	4286	1277054
2016/06/08 11:14:46			554	161749	991	289404
2016/06/08 11:19:57			591	183521	1009	313239
2016/06/08 11:24:54			488	145422	973	290044
2016/06/08 11:29:56			617	185764	977	294400
2016/06/08 11:34:47			7588	2214407	4168	1216254

3. Monitoring > 3.4 Statistics (계속)

Statistics (Select Stats)

❖ Fabric > Inventory
> Pod1 > DC4_LEAF_203(Node-203) > Interfaces > Physical Interface ⇒ Stats



3. Monitoring > 3.5 Fabric Capacity Dashboard

Capacity Dashboard

❖ Operations > Capacity Dashboard

Cisco System Tenants Fabric VM Networking L4-L7 Services Admin Operations Advanced Mode welcome, admin •

Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer | EP Tracker | Visualization

Capacity Dashboard

Endpoints 1 47 of 180000(<1%)

Bridge Domains 5 of 15000(<1%)

L3 Contexts 6 of 3000(<1%)

Endpoint Groups 3 of 15000(<1%)

L4/L7 Devices 0 of 1200(0%)

L4/L7 Graphs 0 of 600(0%)

Usage Overview

Switch	VRF	BD	EPG	Mac (learned)	IPv4 (learned)	IPv6 (learned)	Multicast	Policy CAM	VLAN
node-201	<1% 4 of 500	0% 0 of 3500	0% 0 of 3500	0% 0 of 12288	0% 0 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 45 of 32768	<1% 20 of 3500
node-202	<1% 4 of 500	0% 0 of 3500	0% 0 of 3500	0% 0 of 12288	0% 0 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 45 of 32768	<1% 20 of 3500
node-203	1% 5 of 500	<1% 2 of 3500	<1% 1 of 3500	<1% 35 of 12288	<1% 52 of 12288	0% 0 of 8192	6 of 8192 <1%	<1% 57 of 32768	<1% 21 of 3500
node-204	1% 5 of 500	<1% 2 of 3500	<1% 1 of 3500	<1% 20 of 12288	<1% 25 of 12288	0% 0 of 8192	5 of 8192 <1%	<1% 57 of 32768	<1% 21 of 3500
node-205	1% 5 of 500	<1% 1 of 3500	<1% 1 of 3500	<1% 2 of 12288	<1% 3 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 57 of 32768	<1% 19 of 3500
node-206	1% 5 of 500	<1% 1 of 3500	<1% 1 of 3500	<1% 2 of 12288	<1% 2 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 57 of 32768	<1% 19 of 3500
node-251	1% 5 of 500	<1% 2 of 3500	<1% 1 of 3500	<1% 1 of 12288	<1% 1 of 12288	0% 0 of 8192	0% 0 of 8192	<1% 57 of 32768	<1% 21 of 3500
node-252	1% 5 of 500	<1% 1 of 3500	<1% 1 of 3500	<1%	<1%	0% 0 of 8192	0% 0 of 8192	<1%	<1%

3. Monitoring > 3.7 Contract Deny Log

Contract Deny Log 확인

❖ Fabric > Inventory

> Pod1

⇒ History ⇒ EVENTS

(syslog message policy에서
default severity가 변경이
선행되어야 함)

❖ Contract Deny log

-Contract rule에 정의되지
않는 packet은 Drop되며
Log에 남음

-Pod 또는 해당 node에
event 형태로 보여짐

The screenshot shows the Cisco ACI Management interface. The top navigation bar includes links for SYSTEM, TENANTS, FABRIC, VM NETWORKING, L4-L7 SERVICES, ADMIN, and various search/filter icons. The FABRIC section is currently selected. Below the navigation is a sub-menu for INVENTORY, FABRIC POLICIES, and ACCESS POLICIES, with INVENTORY being the active tab. On the left, there's a sidebar for Inventory with options like Quick Start, Topology, Pod 1 (which is selected), Fabric Membership, Unmanaged Fabric Nodes, Unreachable Nodes, and Disabled Interfaces and Decommissioned Switches. The main content area is titled 'POD - 1' and displays a table of 'Contract Deny Log' events. The table has columns for SEVERITY (Information), AFFECTED OBJECT (topology/pod-1/node-1017/sys), CODE (E4204936), CAUSE (transition), CREATION TIME (e.g., 2015-03-03T19:24:43.077+00:00), and DESCRIPTION (e.g., %ACLOG-5-ACLOG_PKTLOG: Src IP: 126.1.2.46, Dst IP: 10.15.237.38, Src Port: 0, Dst Port: 0, Src Intf: Tunnel11 , Protocol: 61). There are 15 objects per page, and the current page is 1 of 8836. The bottom status bar indicates the current system time as 2015-03-03T19:24+00:00 and displays 15 of 132529 objects.

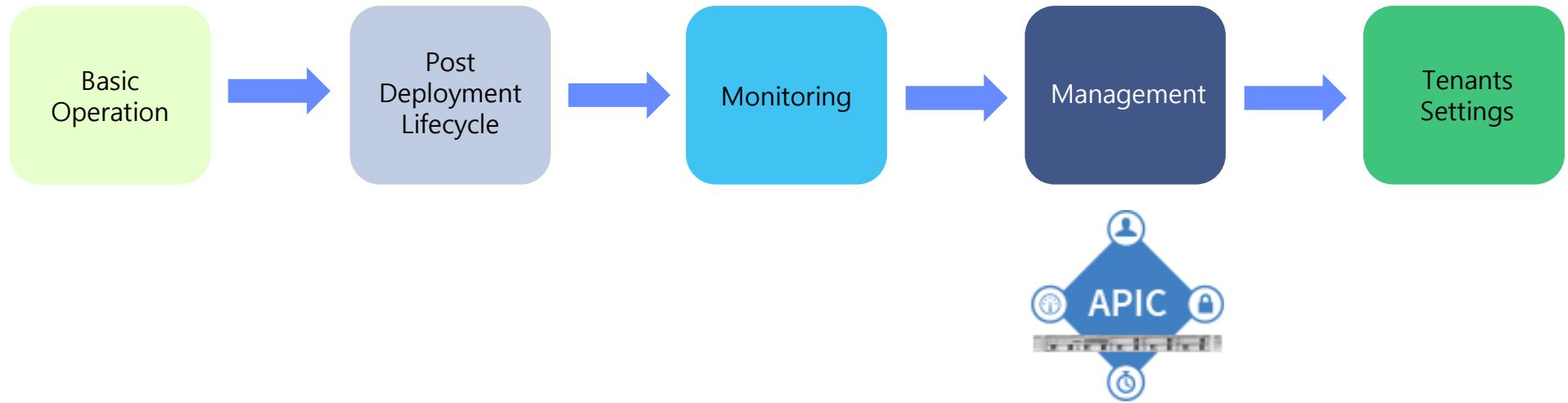
3. Monitoring > 3.7 Contract Deny Log (계속)

Packet Deny Log 확인 (Leaf Node CLI: show logging ip access-list internal packet-log deny)

```
192.168.10.25 - PuTTY
Password:
Access denied
Using keyboard-interactive authentication.
Password:
Last login: Tue May 17 22:27:43 2016 from 192.168.10.250
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lmpl-2.1.php
LEAF203# show logging ip access-list internal packet-log deny
[ Tue May 17 22:32:33 2016 186123 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 192.168.20.10, SPort: 0, DPort: 0, Src Intf: Tunnel11, Proto: 1, PktLen: 74
[ Tue May 17 22:32:28 2016 200939 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 192.168.20.10, SPort: 0, DPort: 0, Src Intf: Tunnel11, Proto: 1, PktLen: 74
[ Tue May 17 22:32:23 2016 201098 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 192.168.20.10, SPort: 0, DPort: 0, Src Intf: Tunnel11, Proto: 1, PktLen: 74
[ Tue May 17 22:32:18 2016 191613 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 192.168.20.10, SPort: 0, DPort: 0, Src Intf: Tunnel11, Proto: 1, PktLen: 74
[ Tue May 17 22:32:13 2016 189062 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 192.168.20.10, SPort: 0, DPort: 0, Src Intf: Tunnel11, Proto: 1, PktLen: 74
[ Tue May 17 22:32:08 2016 188215 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 192.168.20.10, SPort: 0, DPort: 0, Src Intf: Tunnel11, Proto: 1, PktLen: 74
192.168.10.26 - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:
Last login: Tue May 17 22:28:01 2016 from 192.168.10.250
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2016, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lmpl-2.1.php
LEAF204# show logging ip access-list internal packet-log deny
[ Tue May 17 22:33:10 2016 331619 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 177.97.6.30, SPort: 137, DPort: 137, Src Intf: Ethernet1/48, Proto: 17, PktLen: 92
[ Tue May 17 22:33:05 2016 317142 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 177.97.6.29, SPort: 137, DPort: 137, Src Intf: Ethernet1/48, Proto: 17, PktLen: 92
[ Tue May 17 22:33:00 2016 308092 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 161.69.199.22, SPort: 53153, DPort: 443, Src Intf: Ethernet1/48, Proto: 6, PktLen: 66
[ Tue May 17 22:32:08 2016 119851 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 177.97.6.30, SPort: 137, DPort: 137, Src Intf: Ethernet1/48, Proto: 17, PktLen: 10
[ Tue May 17 22:32:01 2016 418265 usecs]: CName: MAIN_TENANT:VRF1(VXLAN: 3047424), VlanType: Unknown, SMac: 0x28d244762e41, DMac:0x0022bdf819ff, SIP: 192.168.10.250, DIP: 177.97.6.30, SPort: 137, DPort: 137, Src Intf: Ethernet1/48, Proto: 17, PktLen: 92
```

SIP: 192.168.10.250 DIP:192.168.20.10 Protocol:1(ICMP) Drop 확인

4) Management



4. Management > 4.1 Image Management

현재 Image 확인(Spine & Leaf)

❖ Admin > Firmware
> Fabric Node Firmware

The screenshot shows the Cisco ACI Fabric Node Firmware management interface. The left sidebar is titled 'Firmware Management' and includes options like Quick Start, Fabric Node Firmware (selected), Firmware Groups, Maintenance Groups, Controller Firmware, Catalog Firmware, Firmware Repository, and Download Tasks. The main content area is titled 'Fabric Node Firmware' and shows the 'Firmware Default Policy' section with a dropdown for 'Default Firmware Version: any'. Below this is the 'All Nodes' table, which lists 12 nodes with their details:

Node id	Node name	Model	Current Firmware	Status	Role	Firmware Group	Maintenance Group
101	DC4_SPIN...	N9K-C9508	n9000-11.2(3c)	Upgraded successfully on 2016-05-03...	spine	DC_Fabric	DC_Fabric
102	DC4_SPIN...	N9K-C9508	n9000-11.2(3c)	Upgraded successfully on 2016-05-03...	spine	DC_Fabric	DC_Fabric
151	DC6_SPIN...	N9K-C9336PQ	n9000-11.2(3c)	Upgraded successfully on 2016-05-02...	spine	DC_Fabric	DC_Fabric
152	DC6_SPIN...	N9K-C9336PQ	n9000-11.2(3c)	Upgraded successfully on 2016-05-02...	spine	DC_Fabric	DC_Fabric
201	DC4_EXT...	N9K-C9332PQ	n9000-11.2(3c)	Upgraded successfully on 2016-05-04...	leaf	DC_Fabric	DC_Fabric
202	DC4_EXT...	N9K-C9332PQ	n9000-11.2(3c)	Upgraded successfully on 2016-05-02...	leaf	DC_Fabric	DC_Fabric
203	DC4_LEA...	N9K-C93120TX	n9000-11.2(3c)	Upgraded successfully on 2016-04-28...	leaf	DC_Fabric	DC_Fabric
204	DC4_LEA...	N9K-C93120TX	n9000-11.2(3c)	Upgraded successfully on 2016-04-28...	leaf	DC_Fabric	DC_Fabric
205	DC4_LEA...	N9K-C9372PX-E	n9000-11.2(3c)	Upgraded successfully on 2016-05-02...	leaf	DC_Fabric	DC_Fabric
206	DC4_LEA...	N9K-C9372PX-E	n9000-11.2(3c)	Upgraded successfully on 2016-05-02...	leaf	DC_Fabric	DC_Fabric
251	DC6_LEA...	N9K-C93120TX	n9000-11.2(3c)	Upgraded successfully on 2016-06-08...	leaf	DC_Fabric	DC_Fabric
252	DC6_LEA...	N9K-C93120TX	n9000-11.2(3c)	Upgraded successfully on 2016-06-08...	leaf	DC_Fabric	DC6_Fabric

A red box highlights the 'Current Firmware: n9000-11.2(3c) (12 Nodes)' header. Below the table, a red text box contains the message 'Node별 Version 확인'.

4. Management > 4.1 Image Management (계속)

현재 Image 확인 (Controller)

❖ Admin > Firmware
> Controller Firmware

The screenshot shows the Cisco ACI Controller Firmware Management interface. The left sidebar has a tree view under 'Firmware Management' with options like Quick Start, Fabric Node Firmware, Maintenance Groups, Controller Firmware (which is selected), Catalog Firmware, Firmware Repository, and Download Tasks. The main panel displays 'Controller Firmware' information: 'Ignore Compatibility Check: false' and 'Target Firmware Version: apic-1.2(3c)'. Below this is the 'Controller Maintenance Policy'. A table titled 'API Controllers' lists three nodes: DC_APIC_1, DC_APIC_2, and DC_APIC_3, all showing 100% upgrade progress.

Node id	Node name	Model	Current Firmware	Status	Upgrade Progress
1	DC_APIC_1	APIC-SERVER-L2	1.2(3c)	Upgraded successfully on 2016-05-02T15:52:19.350+09:00	100%
2	DC_APIC_2	APIC-SERVER-L2	1.2(3c)	Upgraded successfully on 2016-05-02T16:41:50.336+09:00	100%
3	DC_APIC_3	APIC-SERVER-L2	1.2(3c)	Upgraded successfully on 2016-05-02T16:56:28.286+09:00	100%

❖ Admin > Firmware
> Catalog Firmware

The screenshot shows the Cisco ACI Catalog Firmware Management interface. The left sidebar has a tree view under 'Firmware Management' with options like Quick Start, Fabric Node Firmware, Maintenance Groups, Controller Firmware, Catalog Firmware (which is selected), Firmware Repository, and Download Tasks. The main panel displays 'Catalog Firmware' information: 'Target Firmware Version: catalog-1.2(3c)' and 'Current Firmware Version: catalog-1.2(3c)'. Below this is the 'Catalog Maintenance Policy'.

4. Management > 4.1 Image Management (계속)

신규 Image Upload

- ❖ Admin > Firmware
 - > Download Task
 - ⇒ Upload Firmware To APIC

The screenshot shows the Cisco Application Centric Infrastructure (ACI) Controller interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and several monitoring and configuration links. The Admin tab is active. On the left, a sidebar under 'Firmware Management' lists options like Quick Start, Fabric Node Firmware, Controller Firmware, Catalog Firmware, Firmware Repository, and Download Tasks, with 'Download Tasks' currently selected. The main content area displays a 'Download Tasks' table with no items found. A modal dialog box titled 'Upload Firmware To APIC' is open in the foreground, prompting the user to browse for a file named 'aci-apic-dk9.1.2.3e.iso'. It includes 'SUBMIT' and 'CLOSE' buttons.

4. Management > 4.1 Image Management (계속)

Firmware repository 확인

❖ Admin > Firmware
> Firmware Repository

The screenshot shows the Cisco Management interface with the following details:

- Header:** Advanced Mode, welcome, admin.
- Top Navigation:** System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, Search icon, Help icon.
- Breadcrumbs:** AAA | Schedulers | Historical Record Policies | Firmware | External Data Collectors | Config Rollbacks | Import/Export.
- Left Sidebar (Firmware Management):** Quick Start, Fabric Node Firmware, Controller Firmware, Catalog Firmware, **Firmware Repository** (selected), Download Tasks.
- Central Content:** Firmware Repository page with a table of firmware images.
- Table Headers:** Name, Full Version, Size (Bytes), Type, Release Date, Description.
- Table Rows:**
 - version: 1.2**
 - aci-apic-dk9.1.2.3c: 1.2(3c), 156131328, Controller, 2016-04-07T16:41:14.000+09:00, This is a Released Image
 - aci-catalog-dk9.1.2.1i.bin: 1.2(1i), 25361, Catalog, 2015-12-08T16:02:39.000+09:00, This is a Released Image
 - aci-catalog-dk9.1.2.3c.bin: 1.2(3c), 30871, Catalog, 2016-04-07T14:58:30.000+09:00, This is a Released Image
 - version: 11.2**
 - aci-n9000-system.11.2.3c.bin: 11.2(3c), 805802782, Switch, 2016-04-07T15:32:29.000+09:00
- Actions:** ACTIONS ▾

4. Management > 4.1 Image Management (계속)

Controller Firmware Upgrade

❖ Admin > Firmware
 > Controller Firmware

The screenshot shows the Cisco ACI management interface. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and a search bar. The Admin tab is selected. The left sidebar under 'Firmware Management' has 'Controller Firmware' selected. The main content area displays 'Controller Firmware' information and a 'Controller Upgrade' dialog box.

Controller Upgrade Dialog Box:

- Message: "The fabric has 7 Critical Faults and 16 Major Faults. It's recommended that these faults are resolved before performing a controller upgrade."
- Checkboxes:
 - Ignore Compatibility Check:
 - Target Firmware Version:
- Buttons:
 - Apply Policy: (highlighted with a red box)
 -
 -
 -
- Text: "즉시 실행" (Execute Now) in red Korean text.

The background shows a table for 'Controller Maintenance' and a progress bar for 'Upgrade Progress' at 100%.

4. Management > 4.1 Image Management (계속)

Spine & Leaf Upgrade (Firmware Group 설정)

- ❖ Admin > Firmware
 - > Fabric Node Firmware
 - > Firmware Group
 - ⇒ Create Firmware Group

The screenshot shows the Cisco Management interface with the following details:

- Header:** System, Tenants, Fabric, VM Networking L4-L7 Services, Admin, Operations, search, help, user: welcome, admin.
- Breadcrumb:** Firmware Management > Firmware Groups
- Left Sidebar:** Quick Start, Fabric Node Firmware, Firmware Groups (selected), Maintenance Groups, Controller Firmware, Catalog Firmware, Firmware Repository, Download Tasks.
- Main Content:** Firmware Groups table showing 5 nodes:

Selected	Node id	Node name	Model	Current Firmware	Status	Role	Firmware Group	Maintenance Group
	102	SPINE_102	N9K-C9336...	n9000-11.2(3c)	Upgraded successfully on 201...	spine		
	201	LEAF_201	N9K-C9372TX	n9000-11.2(3c)	Upgraded successfully on 201...	leaf		
	202	LEAF_202	N9K-C9372TX	n9000-11.2(3c)	Upgraded successfully on 201...	leaf		
	301							
	302							
- Create Firmware Group Dialog:**
 - Enter info for the new group
 - Group Name: test
 - Ignore Compatibility Check:
 - Target Firmware Version: select an option (highlighted with a red box)
 - Group Node Ids: 101 (highlighted with a red box)
 - Buttons: SUBMIT, CANCEL

Annotations:

- Target version 선택 (Target Firmware Version)
- Target Node 선택 (Group Node Ids)

4. Management > 4.1 Image Management (계속)

Spine & Leaf Upgrade (Maintenance Group 설정)

- ❖ Admin > Firmware
 - > Fabric Node Firmware
 - > Maintenance Group
 - ⇒ Create POD Maint. Group

The screenshot shows the Cisco Management interface with the following details:

- Header:** CISCO, System, Tenants, Fabric, VM Networking L4-L7 Services, Admin, Operations, search, help, user: welcome, admin.
- Breadcrumb:** AAA | Schedulers | Historical Record Policies | Firmware | External Data Collectors | Config Rollbacks | Import/Export.
- Left Sidebar:** Firmware Management (selected), Quick Start, Fabric Node Firmware, Firmware Groups, Maintenance Groups (selected), Maint_Group, Controller Firmware, Catalog Firmware, Firmware Repository, Download Tasks.
- Middle Content:** Maintenance Groups table showing All Nodes. It lists four nodes under "Maintenance Group: (4 Nodes)" and one node under "Maintenance Group: Maint_Group (1 Nodes)".

Selected	Node id	Node name	Model	Current Firmware	Status	Role	Firmware Group	Maintenance Group
<input type="checkbox"/>	102	SPINE_102	N9K-C9336...	n9000-11.2(3c)	Upgraded successfully on 201...	spine		
<input type="checkbox"/>	201	LEAF_201	N9K-C9372TX	n9000-11.2(3c)	Upgraded successfully on 201...	leaf		
<input type="checkbox"/>	202	LEAF_202	N9K-C9372TX	n9000-11.2(3c)	Upgraded successfully on 201...	leaf		
<input type="checkbox"/>	302	LEAF_302	N9K-C9372PX	n9000-11.2(3c)	Upgraded successfully on 201...	leaf		
<input type="checkbox"/>	301	LEAF_301	N9K-C9372PX	n9000-11.2(3c)	Scheduled for upgrade with gr...	leaf		Maint_Group
- Bottom Modal:** Create POD Maintenance Group. It asks for info for the new group. Fields include:
 - Group Name: Maint_Group
 - Run Mode: Pause upon upgrade failure
 - Group Node Ids: 302 (highlighted with a red box)
 - Scheduler: select a value
- Text Overlay:** Target Node 선택 Scheduling 가능 (Target Node Selection, Scheduling is possible) and 이중화를 고려하여 Maintenance Group 설정 (Consider redundancy when setting up Maintenance Group).
- Footer:** Current System Time: 2016-08-10T13:30 +00:00.

4. Management > 4.1 Image Management (계속)

Spine & Leaf Upgrade (Maintenance Group 설정)

- ❖ Admin > Firmware
 - > Fabric Node Firmware
 - > Maintenance Group
 - ⇒ Upgrade Now

The screenshot shows the Cisco Fabric Node Firmware Maintenance Group configuration interface. The top navigation bar includes links for System, Tenants, Fabric, VM Networking L4-L7 Services, Admin, Operations, and user information (welcome, admin). The main menu on the left under 'Fabric Management' has 'Maintenance Groups' selected, showing a sub-menu with options: Quick Start, Fabric Node Firmware, Firmware Groups, Maintenance Groups, Maint_Group (selected), Controller Firmware, Catalog Firmware, Firmware Repository, Download Tasks, Edit Group Membership, Create One Time Window Trigger, Create Recurring Window Trigger, Upgrade Now (highlighted with a red box), Delete Maintenance Group, Save as ..., and Post The central panel displays the 'POD Maintenance Group - Maint_Group' configuration. It shows the 'Name' as 'Maint_Group', 'Run Mode' set to 'Do not pause on failure and do not wait on cluster health' (selected), and 'Pause upon upgrade failure'. Below this is a 'Maintenance windows' section with a note: 'No items have been found. Select Actions to create a new item.' The 'Group Nodes' table lists one node: Node id 301, Node name LEAF_301, Role leaf, Model N9K-C9372..., Current Firmware n9000-11.2(3c), Target Firmware (empty), Status Scheduled for upgrade with ..., Maintenance Group Maint_Group, and Upgrade Progress 0%. At the bottom are buttons for SHOW USAGE, SUBMIT, and RESET.

Name	Description	Max Concurrent Nodes	Max Running Time
No items have been found. Select Actions to create a new item.			

Node id	Node name	Role	Model	Current Firmware	Target Firmware	Status	Maintenance Group	Upgrade Progress
301	LEAF_301	leaf	N9K-C9372...	n9000-11.2(3c)		Scheduled for upgrade with ...	Maint_Group	0%

SHOW USAGE SUBMIT RESET

4. Management > 4.2 Configuration Management

현재 Configuration Backup

❖ Admin > Config Rollbacks

The screenshot shows the Cisco Configuration Management interface under the Admin > Config Rollbacks section. A red box highlights the 'for:' dropdown menu set to 'Fabric'. To its right, a red box highlights the 'Backup 범위(All fabric / Tenant)' button. In the center, a yellow box highlights the 'select a remote location' dropdown. A red arrow points from this dropdown to a yellow box containing the 'CREATE A SNAPSHOT NOW' button. Another red arrow points from the 'CREATE A SNAPSHOT NOW' button to the text 'Click하면 즉시 backup 됨'. A yellow box highlights the '별도 파일 Server로 Backup' text. On the right, a modal window titled 'Create Remote Location' is open, showing fields for Name (Config_Backup), Description (optional), Host Name (192.168.10.100), Protocol (ftp, scp, sftp selected), Remote Path, Remote Port (22), Username (admin), Password, Confirm Password, and Management EPG (default Out-of-Band). Buttons for SUBMIT and CANCEL are at the bottom.

Backup 범위(All fabric / Tenant)

별도 파일 Server로 Backup

Click하면 즉시 backup 됨

CREATE A SNAPSHOT NOW

Define Remote Location

Name: Config_Backup

Description: optional

Host Name (or IP Address): 192.168.10.100

Protocol: ftp scp sftp

Remote Path: |

Remote Port: 22

Username: admin

Password:

Confirm Password:

Management EPG: default (Out-of-Band)

SUBMIT CANCEL

4. Management > 4.2 Configuration Management (계속)

Rollback

❖ Admin > Config Rollbacks

The screenshot shows the Cisco Management interface with the 'Config Rollbacks' feature. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and Advanced Mode. The Admin tab is selected.

The main area displays a table of snapshots:

Snapshots	File Name	File Size (KB)
2016-05-03 16:49:28.598	ce2_defaultOneTime-2016-05-03T16-49-2...	26252
2016-05-04 15:43:19.948	ce2_defaultOneTime-2016-05-04T15-43-1...	27641
2016-05-31 11:00:34.612	ce2_defaultOneTime-2016-05-31T11-00-3...	32202
2016-06-09 17:00:30.805	ce2_DailyAutoBackup-2016-06-09T17-00-...	32582
2016-06-10 01:00:11.263	ce2_DailyAutoBackup-2016-06-10T01-00-...	32446
2016-06-10 09:00:21.377	ce2_DailyAutoBackup-2016-06-10T09-00-...	32796
2016-06-10 10:04:19.797	ce2_defaultOneTime-2016-06-10T10-04-1...	32724
2016-06-10 10:05:03.193	ce2_defaultOneTime-2016-06-10T10-05-0...	32809

A red box highlights the row for '2016-06-10 10:05:03.193' and a red arrow points to the 'ROLLBACK TO THIS CONFIGURATION' button at the bottom of the interface.

Two overlapping windows show the configuration for the selected snapshot:

- The left window shows 'Configuration for selected snapshot' for 'ce2_defaultOneTime-2016-06-10T10-05-01' (32809 KB).
- The right window shows 'Configuration for selected snapshot' for 'ce2_defaultOneTime-2016-06-10T10-05-01.tar.gz' (32809 KB).

A yellow box highlights the 'Compare with previous snapshot' dropdown menu, which lists the same snapshot entries as the main table.

Annotations in Korean:

- 원하는 config를 선택하고 Click하면 즉시 Rollback됨 (Select the desired config and click to perform an immediate rollback)
- 다른 config 버전과 차이점 비교 (Compare differences between different config versions)

4. Management > 4.2 Configuration Management (계속)

Rollback

❖ Admin > Config Rollbacks

The screenshot shows the Cisco Management interface with the 'Config Rollbacks' feature selected. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and Advanced Mode. The Admin tab is active.

The main area displays a table of snapshots:

Snapshots	File Name	File Size (KB)
2016-05-03 16:49:28.598	ce2_defaultOneTime-2016-05-03T16-49-2...	26252
2016-05-04 15:43:19.948	ce2_defaultOneTime-2016-05-04T15-43-1...	27641
2016-05-31 11:00:34.612	ce2_defaultOneTime-2016-05-31T11-00-3...	32202
2016-06-09 17:00:30.805	ce2_DailyAutoBackup-2016-06-09T17-00-...	32582
2016-06-10 01:00:11.263	ce2_DailyAutoBackup-2016-06-10T01-00-...	32446
2016-06-10 09:00:21.377	ce2_DailyAutoBackup-2016-06-10T09-00-...	32796
2016-06-10 10:04:19.797	ce2_defaultOneTime-2016-06-10T10-04-1...	32724
2016-06-10 10:05:03.193	ce2_defaultOneTime-2016-06-10T10-05-0...	32809

A red box highlights the row for '2016-06-10 10:05:03.193' and a red arrow points from this row to the 'ROLLBACK TO THIS CONFIGURATION' button at the bottom of the interface.

The interface also features a 'Compare with previous snapshot' dropdown menu, which is highlighted with a yellow box. This menu lists the same set of snapshots, with the most recent one ('ce2_defaultOneTime-2016-06-10T10-05-01.tar.gz') selected.

원하는 config를 선택하고 Click하면 즉시 Rollback됨

ROLLBACK TO THIS CONFIGURATION

다른 config 버전과 차이점 비교

4. Management > 4.2 Configuration Management (계속)

Rollback

❖ Admin > Config Rollbacks

The screenshot shows the Cisco Management interface with the 'Config Rollbacks' page selected. A red box highlights the 'Import' icon in the top right corner of the main interface area. Two configuration import dialog boxes are overlaid on the page.

Top Dialog: Import remotely stored export archive to snapshot

- File Name: ce2_defaultOneTime.tar.gz
- Import Source: select an import source
- Or create a new one:
- CANCEL SUBMIT

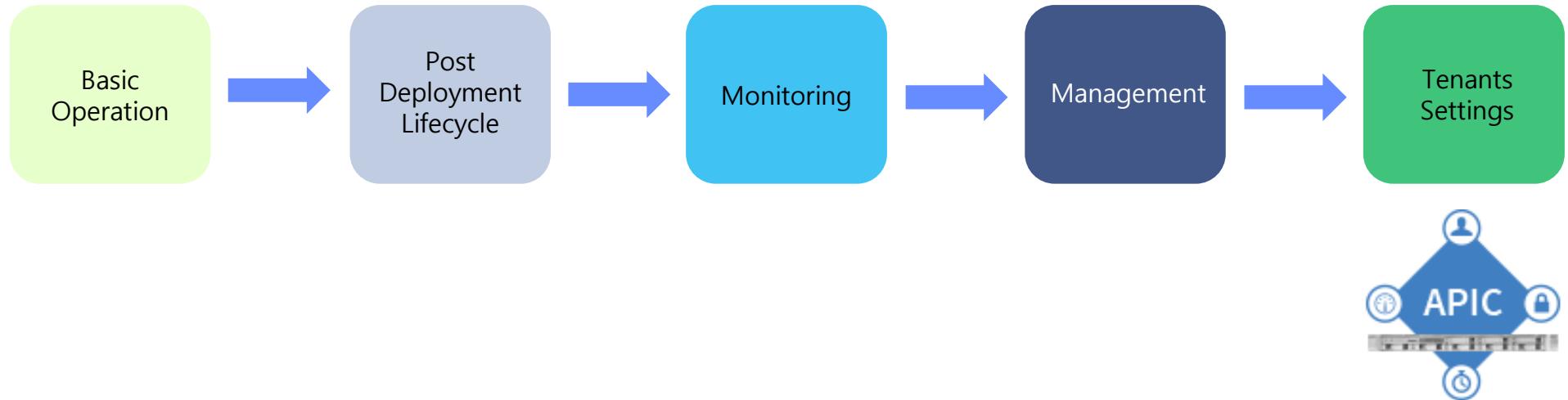
Bottom Dialog: Import remotely stored export archive to snapshot

- File Name: ce2_defaultOneTime.tar.gz
- Import Source: Or create a new one:
- Location Name: file_server
- Host Name (or IP Address): 192.168.10.100
- Protocol: ftp scp sftp
- Remote Path:
- Remote Port: 22
- Username: admin
- Password:
- Confirm Password:
- Management EPG: default (Out-of-Band)
- CANCEL SUBMIT

Red annotations in Korean:

- 파일서버로부터 config 파일 import (Import from file server)
- 파일서버 통신 방법 정의 (Define communication method for file server)

5) Troubleshooting



5. Troubleshooting > 5.1 iPing

iPing

❖ iPing : LEAF node에서 Target IP로 ping test (해당 VRF/BD의 IP가 source임)

iping [options] <target ip address>

options:

- V vrf name (tenant:context)
- c count
- i wait
- p pattern
- s packet size
- t timeout
- S source ip address or source interface

```
DC4_LEAF_203# show vrf
VRF-Name
black-hole
DC_TENANT:DC_VRF1
management
overlay-1
SPAN_TENANT:SPAN_VRF

VRF-ID State Reason
3 Up --
4 Up --
2 Up --
5 Up --
6 Up --

DC4_LEAF_203# iping 10.192.53.32 -V DC_TENANT:DC_VRF1
PING 10.192.53.32 (10.192.53.32) from 10.192.53.1: 56 data bytes
64 bytes from 10.192.53.32: icmp_seq=0 ttl=128 time=0.198 ms
64 bytes from 10.192.53.32: icmp_seq=1 ttl=128 time=0.212 ms
64 bytes from 10.192.53.32: icmp_seq=2 ttl=128 time=0.206 ms
64 bytes from 10.192.53.32: icmp_seq=3 ttl=128 time=0.25 ms
64 bytes from 10.192.53.32: icmp_seq=4 ttl=128 time=0.197 ms

--- 10.192.53.32 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.197/0.212/0.25 ms
DC4_LEAF_203#
```

5. Troubleshooting > 5.2 iTraceroute

iTraceroute

❖ 기존 Traceroute와 itraceroute 의 차이점

- Multiple path exploration을 지원함 : ACI Fabric의 multi path 환경에 적합
- High Efficient : 각 path 별로 하나의 probe packet을 전송함으로 효율적이고 소량의 packet 만 발생함
- itraceroute의 종류

Node itraceroute : 각 Leaf Node 들간 통신 경로 확인

Tenant itraceroute : EP들간의 통신 경로를 확인

```
LEAF_201#  
LEAF_201# itraceroute 20.0.112.91  
Node traceroute to 20.0.112.91, infra VRF overlay-1, from [20.0.112.92], payload 56 bytes  
Path 1  [ Complete ]  [ internal ]  
  1: TEP      20.0.112.93  intf  eth1/33  0.613 ms  
  2: TEP      20.0.112.91  intf  eth1/50  0.542 ms  
  
LEAF_201# itraceroute 10.211.11.11 vrf DC_Tenant:DC_VRF1  
Tenant traceroute to 10.211.11.11, tenant VRF DC_Tenant:DC_VRF1, source encaps vlan-53, from [1  
0.192.53.1], payload 56 bytes  
  
Path 1  [ Complete ]  [ internal ]  
  1: TEP      20.0.112.93  intf  eth1/33  0.553 ms  
  2: TEP      20.0.112.91  intf  eth1/50  0.485 ms
```

5. Troubleshooting > 5.3 Visibility & Troubleshooting

Troubleshooting (Internal EP to EP) STEP-1

❖ Operations

> Visibility & Troubleshooting

The screenshot shows the Cisco ACI Troubleshooting interface under the 'Operations' > 'Visibility & Troubleshooting' menu. The top navigation bar includes tabs for System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations, and a search bar. The 'Operations' tab is selected.

Session Configuration:

- Session Name: TEST_1
- Description: Troubleshooting 1

Source Endpoint: 10.211.11.11

Learned At	Tenant	Application	EPG	IP
Leaf202,	DC_Tenant	DC_AP	DHCP_S...	10.211.11...
Porteth1/...				

Destination Endpoint: 10.211.21.6

Learned At	Tenant	Application	EPG	IP
Leaf201,	DC_Tenant	DC_AP	WLC_EPG	10.211.21...
Porteth1/...				

Search Buttons: External IP (next to Source), SEARCH (highlighted in red), External IP (next to Destination), SEARCH (highlighted in red).

Time Window: Latest Minutes: 240, To: now, Use fixed time (unchecked).

Report Generation: GENERATE REPORT, SHOW GENERATED REPORTS, START (highlighted in red).

Annotations: A yellow arrow points from the text 'External IP 일 경우 선택' to the 'External IP' checkbox next to the Source endpoint table. The 'SEARCH' button in the Source section and the 'START' button at the bottom right are also highlighted with red boxes.

5. Troubleshooting > 5.3 Visibility & Troubleshooting (계속)

Troubleshooting (Internal EP to EP) STEP-2

Your Cluster contains less than 3 in-service Controllers. Please Backup the cluster and do not utilize the fabric in its current state for production.

CISCO System Tenants Fabric VM Networking L4-L7 Services Admin Operations Advanced Mode welcome, admin -

Visibility & Troubleshooting | Capacity Dashboard | ACI Optimizer | EP Tracker | Visualization

TEST_1

Faults

Critical Major Minor Warning

Drop/Stats Contracts Events and Audits Traceroute Atomic Counter SPAN

Time Window From latest 240 minutes To now Session Information Source 10.211.11.11 Destination 10.211.21.6 Session Type Endpoint → Endpoint

Topology 상에 장비의 Fault 표시

Spine SPINE_102 (node-102)

Leaf LEAF_202 eth1/50 (node-202) eth1/11

Source Endpoint IP: 10.211.11.11 C4:54:44:05:72:9F

Leaf LEAF_201 eth1/60 (node-201) eth1/13

Destination Endpoint IP: 10.211.21.6 MAC: 00:1E:13:50:BF:E0

Endpoint 장비의 연결 history 표시

Endpoint Information

IP: 10.211.11.11	MAC: C4:54:44:05:72:9F
Tenant: DC_Tenant	Application: DC_AP
EPG: DHCP_SVR_EPG	Encap: vlan-111

State Transitions

Date	Action	Node	Interface	Encap
2016/06/10 11:2...	detached	Node-201	eth1/11	vlan-111
2016/06/10 11:2...	attached	Node-202	eth1/11	vlan-111
2016/06/10 11:2...	attached	Node-201	eth1/11	vlan-111

5. Troubleshooting > 5.3 Visibility & Troubleshooting (계속)

Troubleshooting (Internal EP to EP) STEP-3

The screenshot shows the Cisco ACI Operations interface. The top navigation bar includes System, Tenants, Fabric, VM Networking, L4-L7 Services, Admin, Operations (selected), and Advanced Mode. The main content area displays a network topology with a Spine node (SPINE_102) connected to two Leaf nodes (LEAF_202 and LEAF_201). A Source Endpoint (IP: 10.211.11.11, MAC: C4:54:44:05:72:9F) is connected to LEAF_202, and a Destination Endpoint (IP: 10.211.21.8, MAC: 00:1E:13:50:BF:E0) is connected to LEAF_201. A red box highlights the 'Drop/Stats' link in the left sidebar. The central panel shows 'No stats available' for the Spine node, while the Leaf nodes show 'Packets dropped'. A red box highlights the 'Traffic Stats' tab in the 'Statistics - LEAF_201' table. The table lists various traffic metrics for the eth1/50 interface over a time window from 2016/06/10 12:09:48 to 2016/06/10 12:15:05.

해당 Node의 Drop과 Traffic 정보 표시
(주의: 전체 Traffic에 대한 data임)

Time	Affected Object	Stats	Value
2016/06/10 12:10:05 - 2016/06/10 12:15:05	topology/pod-1/node-201/sys	health score average value	65
2016/06/10 12:09:48 - 2016/06/10 12:14:48	topology/pod-1/node-201/sys/phys-[eth1/50]	total ingress packets rate average...	6.052603
2016/06/10 12:09:48 - 2016/06/10 12:14:48	topology/pod-1/node-201/sys/phys-[eth1/50]	total ingress packets periodic	1816
2016/06/10 12:09:48 - 2016/06/10 12:14:48	topology/pod-1/node-201/sys/phys-[eth1/50]	total ingress bytes rate average...	1971.75...
2016/06/10 12:09:48 - 2016/06/10 12:14:48	topology/pod-1/node-201/sys/phys-[eth1/50]	total ingress bytes periodic	591638
2016/06/10 12:09:48 - 2016/06/10 12:14:48	topology/pod-1/node-201/sys/phys-[eth1/50]	total egress packets rate average...	6.909428
2016/06/10 12:09:48 - 2016/06/10 12:14:48	topology/pod-1/node-201/sys/phys-[eth1/50]	total egress packets periodic	2073
2016/06/10 12:09:48 - 2016/06/10 12:14:48	topology/pod-1/node-201/sys/phys-[eth1/50]	total egress bytes rate average...	3186.89...
2016/06/10 12:09:48 - 2016/06/10 12:14:48	topology/pod-1/node-201/sys/phys-[eth1/50]	total egress bytes periodic	956091

5. Troubleshooting > 5.3 Visibility & Troubleshooting (계속)

Troubleshooting (Internal EP to EP) STEP-4

S Source Endpoint → Destination Endpoint

Filter ID: IP_ALL from DHCP_SVR_EPG to WLC_EPG							
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
(i)	ip				permit	node-201 node-202	3421 0

Filter ID: implicit BD Allow (DC_Tenant/WLC_BD)							
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
(i)					permit	node-201 node-202	0 0

Filter ID: implicit BD Allow (DC_Tenant/DHCP_BD)							
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
(i)					permit	node-201 node-202	0 626

Filter ID: implicit Context Implicit (DC_Tenant/DC_VRF1)							
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
(i)					deny,log	node-201 node-202	0 0

D Destination Endpoint → Source Endpoint

Filter ID: IP_ALL from WLC_EPG to DHCP_SVR_EPG							
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
(i)	ip				permit	node-201 node-202	3470 0

Filter ID: implicit BD Allow (DC_Tenant/WLC_BD)							
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
(i)					permit	node-201 node-202	0 0

Filter ID: implicit BD Allow (DC_Tenant/DHCP_BD)							
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
(i)					permit	node-201 node-202	220 0

Filter ID: implicit Context Implicit (DC_Tenant/DC_VRF1)							
Info	Protocol	L4 Src	L4 Dest	TCP Flags	Action	Nodes	Hits
(i)					deny,log	node-201 node-202	0 0

Source Endpoint: IP: 10.211.11.11 C:0:54:44:05:72:0F

Destination Endpoint: IP: 10.211.21.6 MAC: 00:1E:13:50:BF:E0

EPG간 Contract 상의 traffic count
(주의: 전체 Traffic에 대한 data임)

5. Troubleshooting > 5.3 Visibility & Troubleshooting (계속)

Troubleshooting (Internal EP to EP) STEP-5

The screenshot shows the Cisco ACI Operations Dashboard under the 'Operations' tab. On the left, a sidebar lists 'TEST_1' and various troubleshooting options: Faults, Drop/Stats, Contracts, Events and Audits, Traceroute, Atomic Counter, and SPAN. Below these are sections for Time Window (From: latest 240 minutes, To: now) and Session Information (Source: 10.211.11.11, Destination: 10.211.21.6, Session Type: Endpoint → Endpoint).

The main area displays a network topology with three nodes: Spine SPINE_102 (node-102, IP: 20.0.112.93), Leaf LEAF_202 (node-202, IP: 20.0.112.91), and Leaf LEAF_201 (node-201, IP: 20.0.112.92). A green line represents the traceroute path from the Source Endpoint (IP: 10.211.11.11) on Leaf_202 to the Destination Endpoint (IP: 10.211.21.6) on Leaf_201. The 'Traceroute' panel in the center shows the results: Running Time: 00:00:44, Traceroute Status: complete, Destination Port: unspecified, Protocol: icmp.

-iTTraceroute 테스트
EP간의 통신을 simulate 함 (icmp, tcp, udp)
일정시간이 경과하고 complete 후에 path가 화면에 표시
(빨간색은 문제가 있음을 표시)

5. Troubleshooting > 5.3 Visibility & Troubleshooting (계속)

Troubleshooting (Internal EP to EP) STEP-6

The screenshot shows the Cisco ACI Operations interface under the 'Operations' tab. On the left, a sidebar displays navigation links: TEST_1, Faults, Drop/Stats, Contracts, Events and Audits, Traceroute, and Atomic Counter. Below this is a 'SPAN' section with a search bar and a 'Time Window' set to 'latest 240 minutes' from 'now'. Session information shows a Source at 10.211.11.11 and a Destination at 10.211.21.6, with a Session Type of 'Endpoint → Endpoint'.

The main area displays a network diagram with three nodes: Spine SPINE_102 (node-102), Leaf LEAF_202 (node-202), and Leaf LEAF_201 (node-201). A connection line labeled 'SPAN Source' connects the Leaf LEAF_202 to the Spine SPINE_102. Another connection line labeled 'SPAN Source' connects the Leaf LEAF_201 to the Spine SPINE_102. Below the diagram, a modal window titled 'SPAN – Bidirectional ERSPAN' is open. It contains fields for 'ERSPAN Source' (unchecked) and 'ERSPAN Destination'. Under 'Destination Type', the 'Predefined Destination Group' option is selected, with a dropdown menu showing 'SPAN_DEST_1_48'. A red box highlights this 'Predefined Destination Group' field. To the right of the diagram, a note in red text reads: 'SPAN Destination(ERSPAN) (기 정의된 SPAN Destination을 사용하는 것이 편리)' (Using predefined SPAN Destination is convenient).

감사합니다.