

# **L4-L7 Services Configuration**

Cisco Nexus Dashboard Fabric Controller introduces the ability to insert Layer 4-Layer 7 (L4-L7) service devices in a data center fabric, and also enables selectively redirecting traffic to these L4-L7 service devices. You can add a L4-L7 service node, create route peering between the L4-L7 service node and the L4-L7 service leaf switch, and then selectively redirect traffic to these L4-L7 service nodes.

• L4-L7 Services, on page 1

# L4-L7 Services

#### UI Path: LAN > Services

Alternatively, you can navigate from LAN > Fabrics > Fabric Overview > Services

Cisco provides ability to insert L4-L7 service devices in a data center fabric, and also enables selectively redirecting traffic to these service devices. You can add a service node, create route peering between the service node and the service switch, and then selectively redirect traffic to these service nodes.

You can also watch a video Service Redirection that demonstrates how to orchestrate a L4-L7 service appliance with a VXLAN Fabric in a data center managed by Cisco Nexus Dashboard Fabric Controller. This demo covers provisioning, defining of service policies, and monitoring of redirected flows.

#### **Service Nodes**

You have to create an External Connectivity Network and specify that a service node resides in that External Connectivity Network during service node creation. Nexus Dashboard Fabric Controller does not auto-detect or discover any service node. You also have to specify the service node name, type, and form factor. The name of the service node has to be unique within a fabric. The service node is attached to a leaf, border leaf, border spine, border super spine, or a border gateway. Nexus Dashboard Fabric Controller does not define a new switch role for a service switch.

Remove the fabric from fabric Monitor Mode to display the icon to delete the service node. This delete icon will be shown only to users with admin role access.

Nexus Dashboard Fabric Controller manages the switches that are attached to a service node. Nexus Dashboard Fabric Controller also manages the interfaces of these attached switches. Ensure that the interfaces to which the service node is attached to are in trunk mode and do not belong to any interface group. The L4-L7 service will not change its mode. In case the attached switches are forming a vPC pair, the name of the attached switch is a combination of both switches.

Double-click on required service name to view the below tabs of the service node details window:

- Overview, on page 4
- Route Peering, on page 16
- Service Policy, on page 19

#### VXLAN EVPN Multi-Site Support

This feature supports VXLAN EVPN Multi-Site. You can choose the VXLAN EVPN Multi-Site member fabric as attached fabric during service node creation, create a service node (for example, firewall, or load balancer), attach the service node to the switch in the selected VXLAN EVPN Multi-Site member fabric, define the route peering and service policies, and deploy relevant configurations on the selected VXLAN EVPN Multi-Site member fabric. For more information on the procedure to configure service, refer Configuring L4-L7 Services, on page 5.

#### **RBAC Support**

The L4-L7 service supports Role-Based Access Control (RBAC) along with fabric access mode.

The admin, stager, and operator, are pre-defined roles in Nexus Dashboard Fabric Controller. The table given below lists the various operations that each role can perform.

Service Operation	Service Node	Route Peering	Service Policy
Create/Update/Delete/Import	admin	admin, stager	admin, stager
List/Export	admin, stager, operator	admin, stager, operator	admin, stager, operator
Attach/Detach	NA	admin, stager	admin, stager
Deploy	NA	admin (blocked if fabric is in fabric monitor or read-only mode)	admin (blocked if fabric is in fabric monitor or read-only mode)
Preview/Deployment History	NA	admin, stager, operator	admin, stager, operator

#### **PBR Support on WAN Interfaces of Border Switches**

You can specify an arbitrary network, that has not been defined in the top-down configuration, as a source or destination network in the service policy. This helps in streamlining policy enforcement for north-south traffic. The Nexus Dashboard Fabric Controller UI lists out routed Layer-3 interfaces of all border switches, standalone or vPC, that have a VRF association. You can then choose the required interface that has to be associated with the defined policy. The border switches include border leaf, border spine, border super spine and border gateway. There can be multiple interface associations. For example, multiple L3 interfaces, subinterfaces, and port-channels, can be selected for one border switch. You can also select multiple border switches for interface association. For information, see NX-OS Unicast Routing Configuration Guide.

Depending on the policy direction, the border switch and interface association for 'any' or arbitrary network may not be needed. For example, for a forwarding policy, the border switch and interface input or route-map association is not needed for 'any' or arbitrary destination network. For a reversed policy, the border switch and interface or route-map association is not needed for 'any' or arbitrary destination network.

When the policy with 'any' or arbitrary network is attached, the policy related CLIs are generated and associated with the selected L3 routed interfaces of the border switches. The deployment of that policy pushes the CLIs

to the selected border switches. The deployment history will include the corresponding entries and can be quickly accessed using VRF filtering. The service policy stats diagram includes the PBR stats of route maps that are associated with the selected L3 routed interfaces of the border switches.

#### **Static Route**

The L4-L7 service pushes static routes on all VTEPs, including service leaf switches, where the VRF being referenced in the static route is attached. This expedites service node failover with static routes.

## **Guidelines and Limitations for L4-L7 Services**

- L4-L7 Service in Nexus Dashboard Fabric Controller does not manage or provision service nodes, such as firewall, load balancer, and Virtual Network Function.
- The L4-L7 Service feature is supported only on the VXLAN BGP EVPN fabrics with the Data Center VXLAN EVPN template.
- The service policies defined in this feature leverage Policy-Based Routing (PBR). Refer Nexus 9000 Series NX-OS Unicast Routing Configuration Guide for PBR related configuration, constraints, and so on.
- This feature supports Cisco Nexus 9300-EX and 9300-FX platform switches as leaf, border leaf, border spine, border super spine, and border gateway switches.
- Configurations involving intra-tenant and inter-tenant firewall for L3 networks, and one-arm Virtual Network Function and one-arm and two-arm deployed load balancer are supported.
- The existing Nexus Dashboard Fabric Controller topology view is also leveraged to display redirected flows associated with the switches that the service node is attached to, and to locate specific redirected flows.
- L4-L7 Service REST APIs are accessible via Nexus Dashboard Fabric Controller packaged REST API documentation. For more information, refer Cisco Nexus Dashboard Fabric Controller REST API Reference Guide.
- L4-L7 Services generate Kafka notifications for real-time interaction.
- Load sharing is not supported.
- From Cisco Nexus Dashboard Fabric Controller Release 12.1.1e, one-arm firewall deployment is added with eBGP peering and static peering options.
- From Cisco Nexus Dashboard Fabric Controller Release 12.1.1e, IPv6 is supported for L4-L7 Services. Refer to Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide for PBR on VXLAN with IPv6 in the Underlay constraints.
- This feature creates, updates, and deletes the service network, as required. Service Networks cannot be created or deleted from the LAN > Fabrics > Networks window.

## **Types of Service Devices**

The L4-L7 Service in Cisco Nexus Dashboard Fabric Controller supports any vendors service node attachments. Typical service node types that are deployed in a data center are Firewalls, Load Balancers, and other Layer-4 to Layer-7 products.

Examples of supported Firewall vendors are Cisco Systems, Palo Alto Networks, Fortinet, Check Point Software Technologies, and others.

Examples of supported Load Balancer vendors are F5 Networks, Citrix Systems, A10 Networks, and others.

Note that these example lists are meant to serve as examples and not intended to be **exhaustive** lists. The L4-L7 service attachment is generic and applies to any vendors service node.

### **Overview**

On Overview tab you can view Summary, Route Peering, Service Policy topology of selected service node.

Click **Refresh** icon to view the latest details.

## **Configuring Fabric Settings for L4-L7 Service**

Certain fabric settings have to be configured to enable L4-L7 Service functionality. To configure these settings, choose LAN > Fabrics and then click Actions > Create Fabric.

The **Create Fabric** window is displayed. Provide a Fabric Name and Pick a Template. Click **Advanced**. Select the **Enable Policy-Based Routing** (**PBR**) checkbox to enable routing of packets based on the specified policy.

Fabric Name				
fab2				
Pick Template				
Easy_Fabric >				
General Parameters Replication VPC	Protocols Advanced Resources	Manageability Bootstrap	Configuration Backup	Flow Monitor
Enable CDP for Bootstrapped Switch	Enable CDP on managemen	nt interface		
Enable VXLAN OAM				
	Enable the Next Generation the fabric to aid in trouble-s	I (NG) OAM feature for all switches in shooting VXLAN EVPN fabrics		
Enable Tenant DHCP				
Enable NX-API	Enable NX-API on port 443			
Enable NX-API on HTTP port	Enable NX-API on port 80			
Enable Policy-Based Routing (PBR)				

Click **Resources**. Specify a VLAN range in the **Service Network VLAN Range** field. This is a per switch overlay service network VLAN range. The minimum allowed value is 2 and the maximum allowed value is 4094. Also, specify a value for the **Route Map Sequence Number Range** field. The minimum allowed value is 1 and the maximum allowed value is 65534. Click **Save** to save the updated configuration.

bric Name	
ab2	
ck Template	
sy_Fabric >	
General Parameters Replication VPC Protocols	Advanced Resources Manageability Bootstrap Configuration Backup Flow Monitor
VRF Lite Subnet IP Range*	
22.33.0.0/16	Address range to assign P2P Interfabric Connections
VRF Lite Subnet Mask*	
30	(Mirc8, Max 31)
Service Network VLAN Range*	
3000-3199	Per Switch Overlay Service Network VLAN Range (Min:2, Max:4094)
Route Map Sequence Number Range*	
1-65534	(Min: 1, Max: 65534)

## **Configuring L4-L7 Services**

To launch the L4-L7 Services, or the Elastic Service, on the Cisco Nexus Dashboard Fabric Controller Web UI, choose LAN > Services.

You can also navigate to Services tab by one of the following below mentioned paths:

```
LAN > Fabrics > Fabric Overview > Services
```

### LAN > Switches > Switches Overview > Services

Services	
Service Nodes Audit History Sample Setup	
In a VXLAN fabric, you can define Service Node Onboard a service device such as a <i>firewall or load balancer</i> . Specify service node name, type, and interface attachment details	Leaf E
Route Peering Specify deployment type, network parameters, peering protocol, and service IP	Lose Batreer Freedal
Service Policy Specify traffic redirection rules to/from the service node	

The services configuration procedure consists of the following steps:

### **Adding Service Node**

You can navigate to Service Node tab by one of the following below mentioned paths:

LAN > Services

0	Service Node Import	×
	You need to select excel file (usually from a previous export) to import service nodes and upload it for your application.	
	(i) Import feature saves all route peering and service policies as detached. You need to attach these manually after the import is complete.	
	Accepted files: .csv, xlsx	
	Drag & Drop your files or <u>Browse</u>	
	Close Impo	ort

To create service node, click Actions > Add > Service Nodes. The Create New Service Node window is displayed.

The Create New Service Node window has three guided steps: Create New Service Node, Create Route Peering, and Create Service Policy.

The **Create New Service Node** window has two sections - **Create Service Node** and **Switch Attachment**, followed by a **Link Template** drop-down list. You can select service\_link\_trunk, service link port channel trunk and service link vpc from this drop-down list based on the specified attached

switch interface type.

The fields in the **Create New Service Node** window are as given below. It is mandatory to fill the fields marked with an asterisk.

#### **Create New Service Node**

Service Node Name: Enter a name for the service node. The name can have alphanumeric, underscore, or dash characters.

Service Node Type: Select Firewall, Load Balancer, or Virtual Networking Function.

Form Factor: Select Physical or Virtual.

External Fabric: Specify the external fabric.

Service Node Interface: Specify the service node interface.

Attached Fabric: Select a fabric from the list.

Attached Switch: Select a switch or a switch pair from the list.

Attached Switch Interface: Select the interface from the list. In case the vPC pair is selected from the Attached Leaf Switch list, the vPC channel will be shown in the Attached Switch Interface list. Otherwise, the port-channel and interfaces with trunk mode are shown in the Attached Leaf Switch Interface list.

**Link Template**: Select the service\_link\_trunk, service\_link\_port\_channel\_trunk, or the service\_link\_vpc template. For more information on template fields, refer Templates, on page 13.

A form is displayed depending on the template used. Update all the required fields in the form and click **Save**.

### **Creating Route Peering**

You can navigate to **Route Peering** tab by one of the following below mentioned paths:

LAN > Services

The fields that appear in the **Create Route Peering** window depend on the type of L4-L7 service node chosen in the **Create New Service Node** window. Depending on the type chosen (Firewall or Load Balancer or VNF), the types of deployments are Intra-Tenant Firewall, Inter-Tenant Firewall, One-Arm load balancer and Two-Arm load balancer, and One-Arm VNF.



**Note** Deletion of service network is not allowed on the **Networks** tab of detail screen from path **LAN** > **Fabrics**, click **Launch** icon **Network** window.

Peering			
	Create Service Node	2 3 Create Route Peering Create Service Policy	
Detach Attach. Peering Name* Deployment* Deployment* Deployment* Defering Option* EBGP Dynamic Peering X V Inside Network		Outside Network	
VVF* MyVRF_51000 X V Index fype* Index hotwork X V Service Notwork* out Isde lare treaset X V		VIE* MyVRE_51000 X V Network: Type* Outside Network: X V Service Network* out updidid: litter teams	
VLAN ID* 3001 Propose Network ID* 30010 Service Network Template*		VLAN ID* 3002 Network ID* 30011 Service Network Template*	
Service_Network_Universal × General Parameters Advanced		Service_Network_Universal × General Parameters Advanced	
IPv4 Gateway/NetMask* 192.168.32.1/24 IPv6 Gateway/Prefix	example 192.0.2.1/24. (pv6 or (pv6 gateway) is monitating.	IPv4 Gateway/NetMask* 32.32.32.1/24 IPv6 Gateway/Prefix	example 1920.0.1/24. (pvé of byó getweny in municatory.
VLAN Name Interface Description fw.inside:SITE_B/ASA2.Giga1/1:peeringInterTena	If + 32 chars enable system vian long- name.	VLAN Name Interface Description fivouside:STE_B/ASA2.Giga1/1:peeringinterTenant	W > 32 chars enable system vian long - neme
Peering Template* service_ebgp_route ×		Peering Template* service_ebgp_route ×	
General Parameters Advanced		General Parameters Advanced	
Neighbor IPv4 address or subnet*	Neighbor IDv6 address or address with netmask, et 12.3.4 or 12.3.174. Neighbor IDv6 address is mandatory.	Neighbor IPv4 address or subnet* 32.32.32.254	Neighbor Pv4 address or address with netrosis, et 1.2.3 or 1.2.3.104. Neighbor Pv4 or Pv4 address is mandatry.
Loopback IP* 60.1.1.60	IP address of the loopback. Loopback IPv6 or IPv6 address is mandatory.	Loopback IP* 61.1.1.60	IP address of the loopback. Loopback IPv8 or IPv8 address is mandatory.
VPC Peer's Loopback IP		vPC Peer's Loopback IP	

#### **Inside Network**

VRF: Specify the VRF.

Network Type: Select Inside Network.

Service Network: Specify the name of the service network.

**VLAN ID**: Specify the VLAN ID. Valid IDs range from 2 to 3967. Click Propose to retrieve a value from the pre-defined L4-L7 service network VLAN range pool.

Service Network Template: Select the Service\_Network\_Universal template from the drop-down list. For more information on the template fields, refer Templates, on page 13.

#### **Outside Network**

VRF: Specify the VRF.

Network Type: Select Outside Network.

Service Network: Specify the name of the L4-L7 service network.

**VLAN ID**: Specify the VLAN ID. Valid IDs range from 2 to 3967. Click Propose to retrieve a value from the pre-defined L4-L7 service network VLAN range pool.

Service Network Template: Select the Service\_Network\_Universal template from the drop-down list. For more information on the template fields, refer Templates, on page 13.

#### **Next Hop Section**

**Next Hop IP Address**: Specify the next-hop IP address. This is the IP/VIP of the service node used for traffic redirection.

**Next Hop IP Address for Reverse Traffic**: Specify the next-hop IP address for reverse traffic. This is the IP/VIP of the service node used for traffic redirection.

#### **Example: Inter-Tenant Firewall Deployment**

Peering Option - Static Peering, Inside Network Peering Template - service\_static\_route, Outside Network Peering Template - service\_static\_route

Image: Control Image: Control   Image: Control Image	Peering			
Description   personant   personant <t< th=""><th></th><th>Create Service Node</th><th>2 3 Create Route Peering Create Service Patcy</th><th></th></t<>		Create Service Node	2 3 Create Route Peering Create Service Patcy	
Provide Name   Substrate   Sub-Shared Freed   Sub-Shared	Detach 🔵 Attach			
purgrages haves   building of the series of	Peering Name*			
Disconcert   Biologic Option   Biologic Option <td>peeringInterTenant</td> <td></td> <td></td> <td></td>	peeringInterTenant			
Decomposition   Menting Outpoor				
Intervalue   Bords Promes Reveng   Word    Word <td>Deployment*</td> <td></td> <td></td> <td></td>	Deployment*			
Intersection   Stable Nuture   Vit   Moders National   Vite   Moders National   Vite   Moders National   National National   Moders National   National National   Moders National   National National   Nati				
INDER VENCY   MARK   MAR	Peering Option*			
Note:   Virt   Wirts	EBGP Dynamic Peering X V			
VP VP   Moders: Type* Moders: Type*   Index Know: Xv   Service Know: Xv   Moders: Type* Moders: Type*   Moders: Ty	Inside Network		Outside Network	
MVPE_5100 XV   Network Stype* XV   India Markason XV   Network Stype* Network Stype*   India Markason XV   Network Markason XV<	VRF*		VRF*	
Network Type*   Notice: Type* <td>MyVRF_51000 X V</td> <td></td> <td>MyVRF_51000 <math>\times</math> <math>\vee</math></td> <td></td>	MyVRF_51000 X V		MyVRF_51000 $\times$ $\vee$	
Index iteracit Image: Series Methods:   Index iteracit I	Network Type*		Network Type*	
Befores Resords   red_baside_latter_beand   VLAI D*   301   Strice Resords   VLAI D*   301   Decode   Strice Resords   Bebook Resords   Bebook Resords   Bebook Resords   Strice Resords   Decode Resords   Addressed   Prid Cateway/Restrict   Restrict Description   Restrict Description   Restrict Parameter   Prid Cateway/Restrict   Restrict Parameter   Prid Cateway/Restrict   Prid Cateway/Restrict   Prid Cateway/Restrict   Restrict Parameter	Inside Network X V		Outside Network X V	
Jandel Randoux Bindel Randoux   Ind Lindia (gring humbit K   VLAN D* 303   3031 Procose   3031 Bindia (gring humbit)   Bindia (gring humbit) Frocose   Storice Halanci Transition Bindia (gring humbit)   Bindia (gring humbit) Frocose   Storice Halanci Transition Bindia (gring humbit)   Bindia (gring humbit) Bindia (gring hu				
V.A. IC P'   301   Betronk D'   3010   Service Nations: Translater   Prid Gateway/Perfx   Prid Gateway/Perfx   Service Nations: Translater   National Service Nations: Translater   National Service Nations: Translater   Prid Gateway/Perfx   Service Nations: Translater   National Service Nations: Translater   National Service Nations: Translater   National Description   National Description   National Service Nations: Advanced   National Description   National Description   National Description   National Description   National Prime National Service National N	net_inside_inter_tenant X V		net_outside_inter_tenant X V	
VLAN D* 301 100 100 100 100 100 100 100				
add     add       Network ID*     add       addition     interface       Bencing Framewarks     Advanced       Prof Galeway/Prefix     except 2011 db.114       VLAN None     *1.2 does not interpret to a store of the cost	VLAN ID*		VLAN ID*	
Network D*     Network D*       3001     3001       3001     3001       Service Network Template     Service Network Template       Service Network Demonstration     Service Network Template       Service Network Demonstration     Service Network Template       Service Network Demonstration     Service Network Demonstration       Image: Service Network Demonstration     Service Network Demonstrat	3001		3002	
3010     3001       Service Network, Turppids*     Service, Network, Turppids*       Service, Network, Turppids*     Service, Network, Turppids*       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv4 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv1 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv1 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv1 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv1 Gateway/Parks     same 100.016 (bit or bit genes i monitory)       Prv1 Gateway/Parks     Same 100.016 (bit or	Network ID*		Network ID*	
Bencie Hannot, Turpular*     Savide Hannot, Turpular*       Bencie Hannot, Turpular     Savide Hannot, Turpular*       Bencie Hannot, Turpular*     Savide Hannot, Turpular*       Bencie Hannot, Turpular*     Savide Hannot, Turpular*       Bencie Hannot, Turpular*     Savide Hannot, Turpular*       VLN Name     # 2 dava subtaytem interpreter       Mathematic Basington     # 2 dava subtaytem interpreter       Mathematic Basing and the subtay sub	30010		30011	
Bernice, Network_Universal X         Bernice, Network_Universal X           General Frameters         Advanced           Pv4 Gateway/NetMask*         sample 102.0104 (bit or pol general metal 10	Service Network Template*		Service Network Template*	
Deneral Parameters     Advanced       PVd. Gateway/NetMaak*     exempt 1202.102, bod in fed general parameters     Advanced       PVd. Gateway/NetMaak*     exempt 1202.102, bod in fed general parameters     23.23.23.17.4     exempt 1202.102, bod in fed general parameters       PVd. Gateway/NetMaak*     exempt 2010.08.104     VLM Name       VLM Name     #-32.04 se unbits years in the long- wee     #-22.04 se unbits years in the long- wee       Netrices Description     #-22.04 se unbits years in the long- wee     #-22.04 se unbits years in the long- wee       Netrices Description     #-22.04 se unbits years in the long- wee     #-22.04 se unbits years in the long- wee       Netrices Description     #-20.04 se unbits years in the services, etbogs_provide ×       Secretal Parameters     Advanced       Netrices Description     #-20.04 setup in the long- wee       Netrices Description     #-20.04 setup in the long- wee       Netrices Description     #-20.00 setup in the long- wee       Netrices Interview Advanced     Method Setup in adview in method week in setup in method week in method week in method week in meth	Service_Network_Universal ×		Service_Network_Universal ×	
Piv4 Gateway/NetMaak*       exerpt 125.21/2 (but in pid serves in modary)         Piv4 Gateway/NetMaak*       exerpt 231.22 (but in pid serves in modary)         Piv5 Gateway/NetMaak*       serves in modary         Piv5 Gateway/NetMaak*       serves in modary         Neightor Piv4 address or suborst*       Neightor Piv4 address or suborst*         Neightor Piv4 address or suborst*       Neightor Piv4 address or suborst*         Neightor Piv4 address or suborst*       Neightor Piv4 address or suborst*         Neightor Piv4 address or suborst*       Neightor Piv4 address or suborst*         Neightor Piv4 address or suborst*       Servers of address or suborst*         Neightor Piv4 address or suborst*       <	General Parameters Advanced		General Parameters Advanced	
Instruments       events       Instruments       events       Instruments         Instruments       events       23.23.23.17/24       events       events       events       events       Instruments       events       event	Bud Gateura/BlotMack*		IBud Gataway/Nattiankt	
Prod Gateway/Predix     parama / memory       Prod Gateway/Predix     parama / memory       Prod Gateway/Predix     surges 2011.06.104       VLAN Name     #-32 class subtrageten die larget       March Dasce Straget     March Dasce Strageten       March Dasce Strageten     March Dasce Strageten       March Da	192.168.32.1/24	example 192.0.2.1/24. lpv4 or lpv6	32.32.32.1/24	example 192.0.2.1/24. Ipv6 or Ipv6
In Southersprints       earlys 2011db1184       earlys 2011db1164         VLAN Name       # - 32 char make system via large- more       # - 32 char make system via large- more       # - 32 char make system via large- more         Itsterface Description       for under STE_BASAS Gap 1/1 peering/ner/Tenant       # - 22 char make system via large- more         Peering Template*       sectors       Peering Template*         service, abge_model       Peering Template*         Peering Template*       Sectors Gap Context         Neighbor IP-4 address or submet*       Neighbor IP-4 address or submet*         192.168.32.254       Mayne IP-1.23.17.12	IBuf Catoury/Brofix	gateway is manoatory.	IBull Contourou/Brothy	gateway is manoasory.
VLAN Name     # - 32 chrs makingsmin der kog- mer       VLAN Name     # - 32 chrs makingsmin der kog- mer       Netricke Discription     frei disse STE_B ASA2 Gigs 1/1 peeringister Fleant       Peering Tamplate* sterkice, abge_route x     Peering Tamplate* serkice, abge_route x       General Parameters     Advanced       Neighbor IPv4 address or submet*     Neighbor IPv4 address or submet*       12:163 32:254     Neighbor IPv4 address or submet*       Loopback IP*     # address or submet*       00:11:30     # address or submet*       00:11:30     # address or submet*       01:11:00     # address or submet*       01:11:00     # address or submet*       01:11:01     Bages of tapers / bages	a to saturay) road	example 2001:db8::1/64		example 2001:db8::1/64
Aver time       # - 32 dee addregater de loge         Interface Description       # - 23 dee addregater de loge         Interface Description       # - 23 dee addregater de loge         Interface Description       # - 23 dee addregater de loge         Interface Description       # - 23 dee addregater de loge         Interface Description       # - 23 dee addregater de loge         Previousies STE_B.ASAZ Gigs 1/1 peeringinter flenant       #	VII AN Name		VII AM Norme	
Interface Description         Interface Description           Interface Description         Interface Description <tr< td=""><td></td><td>if &gt; 32 chars enable:system vian long- name</td><td></td><td>If &gt; 32 chars enable:system vian long-</td></tr<>		if > 32 chars enable:system vian long- name		If > 32 chars enable:system vian long-
Invision STE_RASA2 Gigs1/1 peering/inter/femant         Invocation STE_RASA2 Gigs1/1 peering/inter/femant           Peering Template* service_appg_room x         Service_appg_room x           General Farmeters         Advanced           Neighbor PV4 address or submet* 192108 32:254         Neighbor IPV4 address or submet* 192108 32:254         Neighbor IPV4 address or submet* 192108 32:252           Loopback IP* 0.11.00         Padment of the instance Pol or PV4 address in mediancy Neighbor IPV4 address or submet* 192108 32:252 254         Neighbor IPV4 address or submet* 192108 32:252 254           Loopback IP* 0.11.00         Padment of the instance Pol or PV4 address in mediancy Neighbor IPV4 address in mediancy Neighbor IPV4 address or submet*         Padment of the instance Pol or PV4 address in mediancy Neighbor IPV4 address in mediancy Neigh	Interface Description		Interface Description	
Description         Preventing Template*           Service_stepp_rolite*         Service_stepp_rolite*           Service_stepp_rolite*         Service_stepp_rolite*           Service_stepp_rolite*         Service_stepp_rolite*           Mighter PV4 address or submet*         Neighter PV4 address or submet*           192:108.32:254         Insplace PV4 address or submet*           103:13.00         Put end of address or submet*           00.13.00         Put end address or relevance           VPC Peer's Loopback IP*         Put end address or relevance           VPC Peer's Loopback IP         VPC Peer's Loopback IP           VPC Peer's Loopback IP         Externation Peer Submet IP	fw:inside:SITE_B:ASA2:Giga1/1:peeringInterTenant		fw:outside:SITE_B:ASA2:Giga1/1:peeringInterTenant	
Description         Period Tamplate*           Service, dtop, ontot ×         Service, dtop, ontot ×           Cancel Farmeters         Advanced           Neighbor IP-4 address or submet*         Neighbor IP-4 address or submet*           192:108.32:554         Mergin Dr 4 address or submet*           06.11.30         Index of the language           06.11.30         Index of the language           VPC Peer's Loopback IP*         VPC Peer's Loopback IP           06.11.10         Reservice Toopback IP           06.11.10         Reservice Toopback IP				
General Farmeters         Advanced           Neighbor IP-V4 address or submet*           192.108.32.254         memory.et 12.3102.         Neighbor IP-V4 address or submet*         Neighbor IP-V4 address or submet*           192.108.32.252.254         memory.et 12.3102.         Neighbor IP-V4 address or submet*         Neighbor IP-V4 address or submet*           Loopback IP*         Patient of P4 isotents is mediative         Neighbor IP-V4 address or submet*         Neighbor IP-V4 address or submet*           Loopback IP*         Patient of P4 isotents is mediative         Patient of P4 isotents is mediative           vPC Peer's Loopback IP         Patient of P4 address is mediative         VPC Peer's Loopback IP           00.11.10         Patient of	Peering Template* service_ebgp_route ×		Peering Template* service_ebgp_route ×	
Neighbor (Pv4 address or subnet*         Neighbor (Pv4 address or subnet*           192.169.32.254         Megter (Pv4 address or subnet*         32.32.32.254           Impland (Pv1 Pv4 address or subnet*)         Neighbor (Pv4 address or subnet*)           Loppback (P*         Pv4 address or subnet*           VPC Per's Loppback (P*         Pv4 address or houses in moders, Pv4 or Pv4 address in moders,           VPC Per's Loppback (P*         VPC Per's Loppback (P           VP1 11.10         P address free sorts houses (P	General Parameters Advanced		General Parameters Advanced	
P22 168.32.254         Hugher IP database underse with sequence (12.23.12.23	Neighbor IPv4 address or subnet*		Neighbor IPv4 address or subnet*	
Importer Multi-Prior         Magnetic	192.168.32.254	Neighbor IPv4 address or address with netmask, ex 1.2.3.4 or 1.2.3.1/24.	32.32.32.254	Neighbor IPv4 address or address with retmask, ex 1.2.3.4 or 1.2.3.1/24.
Loppback IP*         Publics		Neighbor IPv4 or IPv6 address is		Neighbor IPv4 or IPv6 address is
B0.1.1.50         P address of the loopback. Loopback         P address of the loopback. Loopback         P address of the loopback. Loopback         P address of the loopback. Loopback.           VPC Peer's Loopback. IP         VPC Peer's Loopback. IP         VPC Peer's Loopback. IP           M0.1.1.61         P address of the open's Loopback.         P address of the open's Loopback.	Loopback IP*		Loopback IP*	
VPC Peer's Loopback (P)         VPC Peer's Loopback (P)           A1 1 A1         P address of the service loopback (P)	60.1.1.60	IP address of the loopback. Loopback	61.1.1.60	IP address of the loopback. Loopback
60.11.61 Padress of the peer's localized	vPC Peer's Loopback IP		VPC Peer's Loopback IP	
	20.1.1.21	IP address of the peer's loopback	61.1.1.61	IP address of the peer's loopback

The fields in the **Create Route Peering** window for an Inter-Tenant Firewall deployment are as given below. It is mandatory to fill the fields marked with an asterisk.

**Peering Name**: Specify a name for the peering. The name can have alphanumeric, underscore, or dash characters.

Deployment: Select Inter-Tenant Firewall.

Peering Option: Select Static Peering or eBGP Dynamic Peering.

### **Inside Network**

VRF: Select a VRF from the drop-down list..

Network Type: Select Inside Network.

Service Network: Provide a L4-L7 service network name.

**VLAN ID**: Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined L4-L7 service network VLAN range pool.

Network ID: Specify the Network ID. Valid IDs range from to .

Service Network Template: Select the Service\_Network\_Universal template from the drop-down list. For more information on the template fields, refer Templates, on page 13.

**Peering Template** - Select service\_static\_route or service\_ebgp\_route from the drop-down list. For more information on the template fields, refer Templates, on page 13.

#### **Outside Network**

VRF: Select a VRF from the drop-down list..

Network Type: Select Outside Network.

Service Network: Provide a L4-L7 service network name.

**VLAN ID**: Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the predefined L4-L7 service network VLAN range pool.

Service Network Template: Select the Service\_Network\_Universal template from the drop-down list. For more information on the template fields, refer Templates, on page 13.

**Peering Template**: Select service\_static\_route or service\_ebgp\_route from the drop-down list. For more information on the template fields, refer Templates, on page 13.

#### Example: One-Arm Mode Load Balancer

The fields in the **Create Route Peering** window for a One-Arm Firewall deployment are as given below. It is mandatory to fill the fields marked with an asterisk.

**Peering Name**: Specify a name for the peering. The name can have alphanumeric, underscore, or dash characters.

Deployment: Select One-Arm F.

Peering Option: Select Static Peering or eBGP Dynamic Peering.

#### **Inside Network**

**VRF**: Select a VRF from the drop-down list..

Network Type: Select First Mode.

Service Network: Provide a L4-L7 service network name.

**VLAN ID**: Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined L4-L7 service network VLAN range pool.

Service Network Template: Select the Service\_Network\_Universal template from the drop-down list. For more information on the template fields, refer Templates, on page 13.

**Peering Template**: Select service\_static\_route or service\_ebgp\_route from the drop-down list. For more information on the template fields, refer Templates, on page 13.

Next Hop IP Address for Reverse Traffic: Specify the next-hop IP address for reverse traffic.

#### **Example: Two-Arm Mode Load Balancer**

The fields in the Create Route Peering window for a Two-Arm Mode load balancer deployment are as given below. It is mandatory to fill the fields marked with an asterisk.

**Peering Name**: Specify a name for the peering. The name can have alphanumeric, underscore, or dash characters.

Deployment: Select Two-Arm Mode.

Peering Option: Select Static Peering or eBGP Dynamic Peering.

#### First Arm

VRF: Select a VRF from the drop-down list..

Network Type: Select First Arm.

Service Network: Provide a L4-L7 service network name.

**VLAN ID**: Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined L4-L7 service network VLAN range pool.

Service Network Template: Select the Service\_Network\_Universal template from the drop-down list. For more information on the template fields, refer Templates, on page 13.

**Peering Template**: Select service\_static\_route or service\_ebgp\_route from the drop-down list. For more information on the template fields, refer Templates, on page 13.

#### Second Arm

VRF: Select a VRF from the drop-down list..

Network Type: Select Second Arm.

Service Network: Provide a L4-L7 service network name.

**VLAN ID**: Specify the VLAN ID. Valid IDs range from 2 to 3967. Click **Propose** to retrieve a value from the pre-defined L4-L7 service network VLAN range pool.

Service Network Template: Select the Service\_Network\_Universal template from the drop-down list. For more information on the template fields, refer Templates, on page 13.

#### **Next Hop Section**

Next Hop IP Address for Reverse Traffic: Specify the next-hop IP address for reverse traffic.

Now, click Save. The Create Policy window is displayed.

#### **Example: One-Arm Virtual Network Function**

The fields in the Create Route Peering window for a One-Arm Mode Virtual Network Function deployment are as given below. It is mandatory to fill the fields marked with an asterisk.

**Peering Name**: Specify a name for the peering. The name can have alphanumeric, underscore, or dash characters.

Deployment: Select One-Arm Mode.

Peering Option: Select Static Peering or eBGP Dynamic Peering.

Save

#### **One Arm**

**VRF**: Select a VRF from the drop-down list.

Network Type: Select One Arm.

Service Network: Provide a L4-L7 service network name.

**VLAN ID**: Specify the VLAN ID. Valid IDs range from 2 to 3967. Click Propose to retrieve a value from the predefined L4-L7 service network VLAN range pool.

Service Network Template: Select the Service\_Network\_Universal template from the drop-down list. For more information on the template fields, refer Templates.

IPv4 Gateway/Netmask: Specify the IPv4 gateway and netmask.

**Peering Template**: Select service\_static\_route or service\_ebgp\_route from the drop-down list. For more information on the template fields, refer Templates.

Next Hop IP Address for Reverse Traffic: Specify the next-hop IP address for reverse traffic.

Now, click Save. The Create Policy window is displayed.

### **Creating Service Policy**

You can navigate to Service Policy tab by one of the following below mentioned paths:

LAN > Services

The Create Service Policy window is displayed as given below.

Create Service Policy			? ×
	Create Service Node	Create Route Pearing Create Service Policy	
Deta	ach Attach		
Serv	vice Policy Name*		
pol	Nicy1		
Peer	ring Name*		
per	ering1	××	
Sour	ree VRE Name*		
My	vVRF_51000		
Dest	tination VRF Name*		
My	yVRF_51000	Xv	
Sour	rce Network*		
VL	AN_10: 10.1.10.1/24	XV	
Dest	tination Network*		
VL	AN_11: 10.1.11.1/24	XV	
Nevt	t kinn IP åririnss*		
20	0.200.200	XY	
	Reverse Next Hop IP Address: 201.201.201.201		
Link	Template*		
servi	ice_pbr ×		
G	ieneral Parameters Advanced		
Pr	ratocal*		
	io 🗸	The protocol, example top.	
	••• •••		
Se	ource Port*	Source port number, example any or 443. Value is ignored for 'ip'	
	any	and 'iomp' protocol	
Di	estination Port*	Periodic and service council as an AS Male is based for	
	any	log and licing' protocol	

The fields in the **Create Service Policy** window are as given below. It is mandatory to fill the fields marked with an asterisk.

Service Policy Name: Specify a name for the policy.

Peering Name: Select the name of the route peering from the drop-down list.

Source VRF Name: Select a source VRF from the drop-down list.

**Destination VRF Name**: Select a destination VRF from the drop-down list.

Source Network: Select an IP address from the drop-down list.

**Destination Network**: Select a network from the drop-down list, or type in an arbitrary network with subnet info. The same is for destination network.

Next Hop IP Address: The next-hop IP address is displayed.

**Reverse Next Hop IP Address** - The reverse next-hop IP address is displayed. By default, the check box will be chosen.

**Link Template** : Select a template from the drop-down list. For more information on the template fields, refer Templates, on page 13.

#### **General Parameters**

**Protocol**: Select a protocol from the drop-down list. The options are icmp, ip, tcp, and udp.

Source Port: Specify a source port number. In case the ip protocol is selected, this value is ignored.

**Destination Port**: Specify a destination port number. In case the ip protocol is selected, this value is ignored.

The **Advanced** tab allow you to customize the matched traffic redirection. For example, you can specify matched traffic to be redirected using PBR, or for matched traffic to bypass a firewall and use routing table rules instead, or you can specify that any matched traffic has to be dropped. You can choose to override the route map match sequence number for prioritization. You can also customize the ACL name, however ensure that the ACL name that you specify is unique and the same name is not used for another ACL. If you do not specify the route map match sequence number or ACL name, the sequence number will be auto-populated from the designated resource pool and the ACL name will be auto-generated based on 5-tuples. For more information on the fields in the **Advanced** tab, refer Templates, on page 13.

Click Save. The service policy is created.



**Note** Deletion of any service network in Top-Down provisioning that is used by Services is not allowed. Deletion of any regular network that is used in a service policy is also not allowed.

## **Templates**

Service Node Link Templates

service\_link\_trunk

**General Parameters tab** 

MTU: Specifies the MTU for the interface. By default, this is set to jumbo.

**SPEED**: Specifies the speed of the interface. By default, this is set to Auto. You can change it to different supported speeds as required.

Trunk Allowed Vlans: Specify 'none',' all', or VLAN ranges. By default, none is specified.

**Enable BPDU Guard**: Specify an option from the drop-down list. The available options are true, false, or no. By default, no is specified.

**Enable Port Type Fast**: Check this option to enable spanning tree edge port behavior. By default, this is enabled.

Enable Interface: Clear the check box to disable the interface. By default, the interface is enabled.

Advanced tab

Source Interface Description: Enter a description for the source interface.

**Destination Interface Description**: Enter a description for the destination interface.

Source Interface Freeform Config: Enter any addition CLI for the source interface.

Destination Interface Freeform Config: Enter any addition CLI for the destination interface.

#### service\_link\_port\_channel\_trunk

Port Channel Mode: Select a port channel mode from the drop-down list. By default, active is specified.

**Enable BPDU Guard**: Specify an option from the drop-down list. The available options are true, false, or no.

**MTU**: Specifies the MTU for the interface. By default, this is set to jumbo.

Trunk Allowed Vlans: Specify 'none',' all', or VLAN ranges. By default, none is specified.

Port Channel Description: Enter a description for the port channel.

Freeform Config: Specify the required freeform configuration CLIs.

**Enable Port Type Fast**: Check this option to enable spanning tree edge port behavior. By default, this is enabled.

Enable Port Channel: Check this option to enable the port channel. By default, this is enabled.

#### service\_link\_vpc

This template has no specifiable parameters.

#### **Route Peering Service Network Template**

#### Service\_Network\_Universal

#### **General Parameters tab**

IPv4 Gateway/Netmask: Specify the gateway IP address and mask of the service network.

IPv6 Gateway/Prefix: Specify the gateway IPv6 address and prefix of the service network.

Vlan Name: Specify a name for the VLAN.

**Interface Description**: Enter a description for the interface

Advanced tab

Routing Tag: Specify a routing tag. Valid values range from 0 to 4294967295.

#### **Route Peering Templates**

#### service\_static\_route

Enter the static routes in the Static Routes field. You can enter one static route per line.

#### service\_ebgp\_route

#### **General Parameters tab**

Neighbor IPv4: Specify the IPv4 address of the neighbor.

Loopback IP: Specify the IP address of the loopback.

#### Advanced tab

Neighbor IPv6: Specify the IPv6 address of the neighbor.

Loopback IPv6: Specify the IPv6 address of the loopback.

**Route-Map TAG**: Specify route-map tag that is associated with the interface ID.

Interface Description: Enter a description for the interface.

Local ASN: Specify a local ASN to override the system ASN.

Advertise Host Routes: Select this option to enable advertisement of /32 and /128 routes to edge routers.

Enable Interface: Clear this option to disable the interface. By default, the interface is enabled.

#### Service Policy Template

#### service\_pbr

#### **General Parameters tab**

Protocol: Select a protocol from the drop-down list. The options are icmp, ip, tcp, and udp.

**Source port**: Specify a source port number. In case the ip protocol is selected, this value is ignored.

**Destination port**: Specify a destination port number. In case the ip protocol is selected, this value is ignored.

#### Advanced tab

**Route Map Action**: Select an action from the drop-down list. The options are permit or deny. If you select **permit**, the matched traffic is redirected based on the next-hop option and the defined policy. If you select **deny**, the traffic is routed based on the routing table rules.

**Next Hop Option**: Specify an option for the next-hop. The options are **none**, **drop-on-fail**, and **drop**. If you select **none**, the matched traffic is redirected based on the defined PBR rules. If you select **drop-on-fail**, the matched traffic is dropped if the specified next hop is not reachable. If you select **drop**, the matched traffic is dropped.

ACL Name: Specify a name for the generated access control list (ACL). If not specified, this is auto-generated.

**ACL Name for reversed traffic**: Specify a name for the ACL that is generated for reversed traffic. If not specified, this is auto-generated.

**Route map match number**: Specify a route map match number. A valid value ranges from 1 to 65535. If not specified, a route map match sequence number will be retrieved from the predefined resource pool. This number is associated with the name of the ACL.

**Route map match number for reversed traffic**: Specify a route map match number for reversed traffic. A valid value ranges from 1 to 65535. If not specified, a route map match sequence number will be retrieved from the predefined resource pool. This number is associated with the name of the ACL that has been generated for reversed traffic.

You can also customize the templates based on specific requirements.

## **Route Peering**

UI Path: LAN > Services, double-click on required service name to view detailed window. Navigate to Route Peering tab.

Alternatively, you can choose LAN > Fabrics, click on Fabric detail view and on the Services to view Route Peering tab.

Route peering creates service networks. Nexus Dashboard Fabric Controller supports both static route and eBGP-based dynamic route peering options. After you specify the service network and select the peering policy for the tenant, Nexus Dashboard Fabric Controller automatically creates the service network under the specified tenant. Note that the terms, tenant and VRF, will be used interchangeably in this guide.

You cannot delete the service network. Deletion of service networks is handled automatically during the service route peering deletion process. There can be multiple route peerings defined per tenant/VRF.

To create Route Peering, refer to Creating Route Peering, on page 7.

The following table describes the fields that appear on Route Peering window.

Field	Description
Service Network One	
Peering Name	Specifies the peering name of service
	Doube-click on <b>Peering Name</b> , detailed window appears. For more information refer to Route Peering Details, on page 18.
Deployment	Specifies the type of deployment. The deployment can be one of the following:
	• Intra-tenant Firewall
	• Inter-tenant Firewall
	One-arm Load Balancer
	• One-arm Firewall
Peering Option	Specifies the selected peering option
Status	Specifies the status of service
Attachment Status	Specifies the status of service, whether it is attached or detached

Field	Description
VRF	Specifies the name of VRF attached with the service node
Network Name	Specifies the name of network associated with service node
Gateway IP	Specifies the gateway IP address of the service node
Service Network Two	
VRF	Specifies the name of VRF attached with the service
Network Name	Specifies the name of network associated with service node
Gateway IP	Specifies the gateway IP address
Next Hop IP	Specifies the hop IP address associated with the service node
Reverse Next Hop IP	Specifies the reverse next hop IP address associated with the service node
Next Hop IPv6	Specifies the next hop IPv6 address associated with the service node
Reverse Next Hop IPv6	Specifies the reverse next hop IPv6 address associated with the service node
Last Updated	Specifies the last modification time and date for the service node

The following table describes the action items, in the **Actions** drop-down list, that appears in the **Route Peering** window.

Action Item	Description
Add	Choose Add. The Create Route Peering window appears.
	Specify the required parameters and click Save.
Edit	Choose required peering and click Edit. The Edit Route Peering window appears.
	Use the toggle to attach or detach the route peering. When the service policy is attached or enabled, the corresponding policies are applied to the VRF (tenant), source, and destination networks.
	Specify the required parameters and click Save.
Attach	To attach a specific route peering to a switch, choose the required peering and click <b>Attach</b> .
	<b>Note</b> Bulk attachment, detachment, preview and deployment of route peering are supported and they are limited up to 10 route-peerings only.
Detach	To detach a specific route peering from a switch, choose the required peering and click <b>Detach</b> .

Action Item	Description
Preview	To display the preview, choose the required peering and click <b>Preview</b> .
	A Preview Route Peering window is displayed.
	Select a specific switch, network, or VRF from the respective drop-down lists to display the route peerings for specific switches, networks, and VRFs. Click <b>Close</b> to close the window.
Deploy	To deploy a route peering, choose required peering, click <b>Deploy</b> .
	A pop-up window appears for confirmation to deploy. Click <b>Deploy</b> .
Import	To import route peering information as an Excel file, click <b>Import</b> . The <b>Route</b> <b>Peering Import</b> window appears.
	Click <b>Browse</b> , choose appropriate file, and then click <b>Import</b> to import information about the route peerings.
Export	To export route peering information as an Excel file, click <b>Export</b> . The <b>Route</b> <b>Peering Export</b> window appears.
	Click <b>Export</b> to export information about the selected route peering.
Delete	To delete the route peering, choose appropriate route peering, and click <b>Delete</b> .

### **Route Peering Details**

To view peering details window, navigate to **Services**, double-click on required service **Name**, Peering details window appears. You can view below tabs on the window:

- Overview
- · Status Details
- Route Peering
- Service Policy

#### **Overview**

The **Overivew** tab displays **Route Peering Summary** with Inside and Outside Network details, **Service Policies**, and **Service Node** as cards.

#### **Status Details**

This tab provides a peak into the deployed configuration. Hover over the **i** icon next to the **Status Details** field in each row to display more information.

### **Service Policy**

Refer to Service Policy, on page 19.

#### **Viewing Deployment History**

This tab displays deployment history of the switches and networks that are involved in the route peering. This tab displays information such as the name of the network, VRF, and switch, status, status message, status details, and time of execution.

## **Service Policy**

You can define service policies with any or arbitrary network and associate it with L3 routed interface on border switches. For more information, see PBR Support on WAN Interfaces of Border Switches. The L4-L7 service does not create any VRF or network other than the service networks that are defined during route peering. When you define the service policy between the created networks, the source and destination network can be a subnet, an individual IP address or the networks that are defined in the **Services** tab of fabric detail screen. Choose **LAN >Fabric**, click on Fabric detail view to view services tab. For intra-tenant firewall, one-arm and two-arm load balancer, the L4-L7 service in Nexus Dashboard Fabric Controller uses Policy-Based Routing (PBR) for service insertion. The inter-tenant firewall does not have a service policy. You only need to create a service node and route peering for inter-tenant firewall.

As the source and destination network can be attached or deployed independent of service policy deployment, the tenant/VRF-related service policy configuration is only attached or pushed to the switch that is attached to the service node, and the source and destination network is updated with the service policy-related configuration. You can preview and confirm the generated configuration. By default, the service policy is defined but is not enabled or attached. You have to enable or attach the service policy to activate it.

The service configuration that is related to the source and destination network will be auto-processed when the source and destination networks are to be attached, or auto-updated in case the networks are already attached or deployed. By default, Nexus Dashboard Fabric Controller will collect statistics every 5 minutes and store it in the database for aggregation and analysis. By default, the statistics are stored for a maximum of 7 days.

The service insertion is effective only on the flows to be created. There is no impact on any existing flows. Deletion of a network is not allowed in case an enabled service policy is associated with that network.

The L4-L7 service integration is built on top of the easy fabric policy enforcement. Choose LAN > Fabrics, to create a VXLAN EVPN fabric and then import Cisco Nexus 9000 Series switches into the fabric with predefined fabric policies.

To create service policy, refer to Creating Service Policy, on page 12.

Field	Description
Policy Name	Specifies the policy name of service
	Doube-click on <b>Policy Name</b> , detailed window appears. For more information refer to Service Policy section.
Route Peering	Specifies the route peering name
Status	Specifies the status of service
Attachment Status	Specifies the status of service, whether it is attached or detached
Source VRF	Specifies the name of VRF attached with the service node

The following table describes the fields that appear on Route Peering window.

Field	Description
Source Network	Specifies the name of source network
Destination VRF	Specifies the name of destination VRF attached with the service node
Destination Network	Specifies the name of destination network
Next Hop IP	Specifies the hop IP address associated with the service node
Reverse Next Hop IP	Specifies the reverse next hop IP address associated with the service node
Next Hop IPv6	Specifies the next hop IPv6 address associated with the service node
Reverse Next Hop IPv6	Specifies the reverse next hop IPv6 address associated with the service node
Reverse Enabled	Specifes if reverse next-hop is enabled or not.
Route Map Action	The options are permit or deny. If you select <b>permit</b> , the matched traffic is redirected based on the next-hop option and the defined policy. If you select <b>deny</b> , the traffic is routed based on the routing table rules.
Next Hop Option	Specify an option for the next-hop. The options are <b>none</b> , <b>drop-on-fail</b> , and <b>drop</b> . If you select <b>none</b> , the matched traffic is redirected based on the defined PBR rules. If you select <b>drop-on-fail</b> , the matched traffic is dropped if the specified next hop is not reachable. If you select <b>drop</b> , the matched traffic is dropped.
Last Updated	Displays the time at which the service policy was last updated.

The following table describes the action items, in the **Actions** drop-down list, that appears in the **Route Peering** window.

Action Item	Description
Add	Choose Add. The Create Service Policy window appears.
	Specify the required parameters and click <b>Save</b> .
Edit	Choose required service policy and click <b>Edit</b> . The <b>Edit Service Policy</b> window appears.
	Use the toggle to attach or detach the service policy. When the service policy is attached or enabled, the corresponding policies are applied to the VRF (tenant), source, and destination networks.
	Specify the required parameters and click Save.
Attach	To attach a specific service policy to a switch, choose the required policy and click <b>Attach</b> .
	<b>Note</b> Bulk attachment, detachment, preview and deployment of route peering are supported and they are limited up to 10 service policy only.

Action Item	Description
Detach	To detach a specific service policy from a switch, choose the required service policy and click <b>Detach</b> .
Preview	To display the preview, choose the required peering and click <b>Preview</b> .
	A Preview Service Policy window is displayed.
	Select a specific switch, network, or VRF from the respective drop-down lists to display the service policy for specific switches, networks, and VRFs. Click <b>Close</b> to close the window.
Deploy	To deploy a service policy, choose required service policy, click <b>Deploy</b> .
	A pop-up window appears for confirmation to deploy. Click <b>Deploy</b> .
Import	To import service policy information as an Excel file, click <b>Import</b> . The <b>Service Policy Import</b> window appears.
	Click <b>Browse</b> , choose appropriate file, and then click <b>Import</b> to import information about the service policy.
Export	To export route service policy information as an Excel file, click <b>Export</b> . The <b>Service Policy Export</b> window appears.
	Click <b>Export</b> to export information about the selected service policy.
Delete	To delete the service policy, choose appropriate service policy, and click <b>Delete</b> .

### **Service Policy Details**

To view service policy window, navigate to **Services**, double-click on required service **Name**, service policy details window appears. You can view below tabs on the window:

- Overview
- Status Details
- Route Peering
- Service Policy

### **Overview**

The **Overivew** tab displays **Policy Summary**, **Service Node**, and **Route Peering** with Inside and Outside Network as cards.

### **Status Details**

This tab displays **Resource Type**, **Fabric Name**, **Resource Name** details associated with the selected service policy

#### **Statistics**

This tab displays statistical information about the configured service policies. Select a time range for which the statistics should be displayed from the **Time Range** drop-down box. You can select the date from the calendar displayed on the window and the time by clicking **select time** at the bottom right corner of the window. You can also display statistics from the last 15 minutes, 1 hour, 6 hours, 1 day, 1 week, and 1 month. Select the required time range and click **Apply**. Select a switch for which the statistics should be displayed from the statistics are then displayed for the selected switch in the specified time range.

Click **Clear Stats** to reset the statistics for a specific policy on all involved switches. If multiple policies are sharing the same route map, then the statistics of other policies are also impacted.

#### **Viewing Deployment History**

This tab displays deployment history of the switches and networks that are involved in the service policy. This tab displays information such as the name of the network, VRF, switch name, status, status message, status details, and time of execution.

## **Refreshing a Service Node**

To refresh the list of service node that is displayed in the Service Nodes window, click the Refresh icon .

## **Viewing Audit History**

To view audit history of the switches and networks that are involved in the selected service policy or route peering, click the **Audit History** tab in the **Services** window.

Audit Logs table in the Audit History window displays information about all the actions that have been performed:

Field	Description
User Name	Specifies the user name of service node.
User Role	Specifies the user role name by whom latest action performed.
Action Taken	Specifies the latest action performed
Entity	Specifies the name of service node.
Details	Sepcifies the details of the service node
Status	Sepcifies the status of the service node
Time	Sepcifies the action time on that node
More Info	Click <b>More Info</b> to view detailed information of selected service node.

Creation of service nodes, route peering, and service policies

· Deletion of service nodes, route peering, and service policies

- · Update of service nodes, route peering, and service policies
- · Attachment and detachment of route peering, and service policies
- · Deployment of route peering and service policies

Audit logs are generated when the below actions are performed, these audit log is saved with the name of the user who has performed the action, the role of the user, the action taken, the entity on which the action was performed, details about the action, the status, and the time at which the action was performed.

To delete older audit reports, click Action > Purge Audit History, specify the maximum retained dates and confirm deletion. Note that only users with the admin role can delete audit log entries.

## **Importing Service Nodes**

To import service nodes from an Excel file, click **Actions > Import** on the **Service Nodes** window. The **Servie Node Import** window appears.

Click **Browser** or drag and drop your file, and click **Import** button on the **Service Node Import** window to import information about the service nodes.

Service Node Import	×
You need to select excel file (usually from a previous export) to import service nodes and upload it for your application.	
(i) Import feature saves all route peering and service policies as detached. You need to attach these manually after the import complete.	ort is
Accepted files: .csv, xlsx	
Drag & Drop your files or <u>Browse</u>	
Close	Import

You can also restore the service node level data by clicking **Actions > Import** to import data about the service nodes from an excel file.

## **Exporting Service Nodes**

You can back up data at the Service node level by clicking **Actions** > **Export** option to export data about the service nodes to an excel file. Data regarding all the service nodes, the respective route peerings, and service policy, is exported.

You can also export data for a specific Service node by selecting the node and clicking **Actions > Export**. A confirmation window appears, click **Export**.

## **Editing a Service Node**

To edit a service node from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

### Procedure

Step 1	Choose a service node from the table and click <b>Actions &gt; Edit</b> .
Step 2	The Edit Service Node window is displayed.
	Make the required changes and click Save.

## **Deleting a Service Node**

To delete a service node from the Cisco Nexus Dashboard Fabric Controller Web UI, perform the following steps:

Procedure

Select a service node from the table and click **Actions > Delete**.

#### Note

Ensure that the service node that has to be deleted has no route peering or service policies associated with it. In case there are service policies or route peering associated with the service node, the deletion is blocked with a warning indicating that any route peering or service policies associated with the service node have to be removed before deleting the service node.