

# Configure Interface Settings for Edges with new Orchestrator UI

A DRAFT

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

BETA DRAFT

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

Copyright © 2023 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

# Contents

Contents .....	3
Configure Interface Settings for Edges with new Orchestrator UI .....	4
IPv4 Settings .....	7
IPv6 Settings .....	10
Wi-Fi Access Control based on MAC Address .....	13

# Configure Interface Settings for Edges with new Orchestrator UI

An Edge has different types of Interfaces. By default, the Interface configuration settings of an Edge are inherited from the associated Profile. You can modify and configure more settings for each Edge.

The Interface Settings options vary based on the Edge model.

To configure Interface settings for a specific Edge, perform the following steps:

- 1 In the Enterprise portal, click **Configure > Edges**.
- 2 The **Edges** page displays the existing Edges.
- 3 Click the link to an Edge or click the **View** link in the **Device** column of the Edge.
- 4 The configuration options for the selected Edge are displayed in the **Device** tab.
- 5 In the **Connectivity** category, expand **Interfaces**.
- 6 The different types of Interfaces available for the selected Edge are displayed. Click the link to an Interface to edit the settings. The following screen appears:

⚠ If IPv4/IPv6 DHCP Server is activated and if DNS proxy is deactivated then the DNS resolution will not work as expected and may result in DNS resolution failure.

## Interface GE5

☒ Override

## Description

Maximum 256 characters

## Interface Enabled

☒ Enabled

## Capability

Routed

## Segments

Global Segment

## Radius Authentication

☐ Enabled ⚠ Intra-VLAN traffic will not be filtered on hardware switching platforms (Edge 500, 520, 540, and 610)

## ICMP Echo Response

☒ Enabled

## Underlay Accounting ⓘ

☒ Enabled

## Enable WAN Overlay

☐ Enabled

## DNS Proxy

☐ Enabled

## VLAN

## EVDSL Modem Attached

☐ Enabled

## IPv4 Settings

☒ Enabled

## Addressing Type

Static

IP Address \* 172.16.1.2

CIDR Prefix \* 29

Gateway 172.16.1.3

## OSPF

⊗ OSPF not enabled for the selected Segment

## Multicast

⊗ Multicast is not enabled for the selected segment

## VNF Insertion

⊗ Trusted Source must be enabled to configure VNF insertion

## Advertise

☐ Enabled

## NAT Direct Traffic

☒ Enabled

## Trusted Source ⓘ

☐ Enabled

You can edit the settings for the following types of Interfaces, based on the Edge model:

- Switch Port
- Routed Interface
- WLAN Interface

You can also add Sub Interface, Secondary IP address, and Wi-Fi SSID based on the Edge model.

7 You can configure the following settings for a Routed Interface of an Edge.

Option	Description
Description	Enter a description. This field is optional.
Interface Enabled	This option is activated by default. If required, you can deactivate the Interface. When deactivated, the Interface is not available for any communication.
Capability	For a Switch Port, the option <b>Switched</b> is selected by default. You can choose to convert the port to a routed Interface by selecting the option <b>Routed</b> from the drop-down menu.
Segments	By default, the configuration settings are applicable to all the segments.
Radius Authentication	Deactivate the <b>Enable WAN Overlay</b> check box to configure <b>Radius Authentication</b> . Select the <b>Radius Authentication</b> check box and add the MAC addresses of pre-authenticated devices.
ICMP Echo Response	This check box is selected by default. This helps the Interface to respond to ICMP echo messages. You can deactivate this option for security purposes.
Underlay Accounting	<p>This check box is selected by default. If a private WAN overlay is defined on the Interface, all underlay traffic traversing the interface are counted against the measured rate of the WAN link to prevent over-subscription. Deactivate this option to avoid this behavior.</p> <p><b>Note</b> Underlay Accounting is supported for both, IPv4 and IPv6 addresses.</p>
Enable WAN Overlay	Select the check box to activate WAN overlay for the Interface.
DNS Proxy	<p>This option allows you to activate or deactivate a <b>DNS Proxy</b>, irrespective of the IPv4 or IPv6 DHCP Server setting.</p> <p><b>Note</b> This check box is available only for a Routed Interface and a Routed Sub Interface.</p>

Option	Description
VLAN	For an Access port, select an existing VLAN from the drop-down menu. For a Trunk port, you can select multiple VLANs and select an untagged VLAN.
EVDSL Modem Attached	Select this check box to activate an EVDSL Modem.
IPv4 Settings	Select the <b>Enable</b> check box and configure the IPv4 settings. For more information, see <a href="#">IPv4 Settings</a> section below.
IPv6 Settings	Select the <b>Enable</b> check box and configure the IPv6 settings. For more information, see <a href="#">IPv6 Settings</a> section below.
L2 Settings	
Autonegotiate	This option is selected by default. When selected, Auto-negotiation allows the port to communicate with the device on the other end of the link to determine the optimal duplex mode and speed for the connection.
Speed	This option is available only when <b>Autonegotiate</b> is not selected. Select the speed that the port has to communicate with other links. By default, <b>100 Mbps</b> is selected.
Duplex	This option is available only when <b>Autonegotiate</b> is not selected. Select the mode of the connection as <b>Full duplex</b> or <b>Half duplex</b> . By default, <b>Full duplex</b> is selected.
MTU	The default MTU size for frames received and sent on all routed interfaces is <b>1500</b> bytes. You can change the MTU size for an Interface.
LOS Detection	<p>This option is available only for a routed Interface of an Edge. Select the check box to activate Loss of Signal (LoS) detection by using ARP monitoring.</p> <p><b>Note</b> You can select the check box only when you have activated High Availability on the Edge.</p>

## IPv4 Settings

Select the **Enabled** check box to configure the following **IPv4 Settings**:

Option	Description
Addressing Type	<p>Select an addressing type:</p> <ul style="list-style-type: none"> <li>■ <b>DHCP</b>: Assigns an IPv4 address dynamically.</li> <li>■ <b>PPPoE</b>: You must configure the addressing details for each Edge.</li> <li>■ <b>Static</b>: You must enter the <b>IP address</b>, <b>CIDR Prefix</b>, and <b>Gateway</b> for the selected routed Interface.</li> </ul>

OSPF	<p>This option is available only when you have configured OSPF for the selected <b>Segment</b>. Select the check box and choose an OSPF from the drop-down menu. Click <b>toggle advance ospf settings</b> to configure the Interface settings for the selected OSPF.</p> <hr/> <p><b>Note</b> OSPF is not supported on Sub Interfaces, and it is not supported on non Global Segments.</p> <p>The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6.</p> <hr/> <p><b>Note</b> OSPFv3 is only available in the 5.2 release.</p>
------	--

Option	Description
Multicast	<p>This option is available only when you have configured multicast settings for the selected <b>Segment</b>. You can configure the following multicast settings for the selected Interface.</p> <ul style="list-style-type: none"> <li>■ <b>IGMP</b> - Select the check box to activate Internet Group Management Protocol (IGMP). Only IGMP v2 is supported.</li> <li>■ <b>PIM</b> - Select the check box to activate Protocol Independent Multicast. Only PIM Sparse Mode (PIM- SM) is supported.</li> </ul> <p>Click <b>toggle advanced multicast settings</b> to configure the following timers:</p> <ul style="list-style-type: none"> <li>■ <b>PIM Hello Timer</b> - The time interval at which a PIM Interface sends out <b>Hello</b> messages to discover PIM neighbors. The range is from 1 to 180 seconds and the default value is 30 seconds.</li> <li>■ <b>IGMP Host Query Interval</b> - The time interval at which the IGMP querier sends out host-query messages to discover the multicast groups with members, on the attached network. The range is from 1 to 1800 seconds and the default value is 125 seconds.</li> <li>■ <b>IGMP Max Query Response Value</b> - The maximum time that the host has to respond to an IGMP query. The range is from 10 to 250 deciseconds and the default value is 100 deciseconds.</li> </ul> <hr/> <p><b>Note</b> Currently, Multicast Listener Discovery (MLD) is deactivated. Hence, Edge does not send the multicast listener report when IPv6 address is assigned to Interface. If there is a snooping switch in the network then not sending MLD report may result in Edge not receiving multicast packets which are used in Duplicate Address Detection (DAD). This results in DAD success even with duplicate address.</p>

VNF Insertion	You must deactivate <b>WAN Overlay</b> and select the <b>Trusted Source</b> check box to activate <b>VNF Insertion</b> . When you insert the VNF into Layer 3 interfaces or sub-interfaces, the system redirects traffic from the Layer 3 interfaces or sub interfaces to the VNF.
Advertise	Select the check box to advertise the Interface to other branches in the network.
NAT Direct Traffic	Select the check box to apply NAT for IPv4 to network traffic sent from the Interface.

Option	Description
Trusted Source	Select the check box to set the Interface as a trusted source.
Reverse Path Forwarding	<p>You can choose an option for Reverse Path Forwarding (RPF) only when you have selected the <b>Trusted Source</b> check box. This option allows traffic on the interface only if return traffic can be forwarded on the same interface. This helps to prevent traffic from unknown sources like malicious traffic on an Enterprise network. If the incoming source is unknown, then the packet is dropped at ingress without creating flows. Select one of the following options from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ <b>Not Enabled</b> – Allows incoming traffic even if there is no matching route in the route table.</li> <li>■ <b>Specific</b> – This option is selected by default, even when the <b>Trusted Source</b> option is deactivated. The incoming traffic should match a specific return route on the incoming interface. If a specific match is not found, then the incoming packet is dropped. This is a commonly used mode on interfaces configured with public overlays and NAT.</li> <li>■ <b>Loose</b> – The incoming traffic should match any route (Connected/Static/Routed) in the routing table. This allows asymmetrical routing and is commonly used on interfaces that are configured without next hop.</li> </ul>

For IPv4 address, configure the **IPv4 DHCP Server** as follows:

**Note** This option appears only when you select the **Addressing Type** as **Static**.

- **Activated:** Activates DHCP with the Edge as the DHCP server. If you choose this option, configure the following details:
  - **DHCP Start:** Enter a valid IP address available within the subnet.
  - **Num. Addresses:** Enter the number of IP addresses available on a subnet in the DHCP Server.
  - **Lease Time :** Select the period of time from the drop-down menu. This is the duration the VLAN is allowed to use an IP address dynamically assigned by the DHCP Server.

- **Options:** Click **Add** to add pre-defined or custom DHCP options from the drop-down menu. The DHCP option is a network service passed to the clients from the DHCP server. Choose a custom option and enter the code, data type, and value.
- **Relay** – Allows DHCP with the DHCP Relay Agent installed at a remote location. If you choose this option, configure the following:
  - **Relay Agent IP(s):** Specify the IP address of Relay Agent. Click **Add** to add more IP addresses.
- **Deactivated** – Deactivates the DHCP server.

## IPv6 Settings

Select the **Enabled** check box to configure the following **IPv6 Settings**:

Option	Description
Addressing Type	<p>Select an addressing type:</p> <ul style="list-style-type: none"> <li>■ <b>DHCP Stateless:</b></li> <li>■ <b>DHCP Stateful:</b></li> <li>■ <b>Static:</b> You must enter the <b>IP address</b>, <b>CIDR Prefix</b>, and <b>Gateway</b> for the selected routed Interface.</li> </ul>
OSPF	<p>This option is available only when you have configured OSPF for the selected <b>Segment</b>. Select the check box and choose an OSPF from the drop-down menu. Click <b>toggle advance ospf settings</b> to configure the Interface settings for the selected OSPF.</p> <p><b>Note</b> OSPF is not supported on Sub Interfaces, and it is not supported on non Global Segments.</p> <p>The OSPFv2 configuration supports only IPv4. The OSPFv3 configuration supports only IPv6, which is only available in the 5.2 release.</p> <p><b>Note</b> OSFPv3 is only available in the 5.2 release.</p>
Advertise	Select the check box to advertise the Interface to other branches in the network.
NAT Direct Traffic	Select the check box to apply NAT for IPv6 to network traffic sent from the Interface.

Option	Description
Trusted Source	Select the check box to set the Interface as a trusted source.

Reverse Path Forwarding	<p>You can choose an option for Reverse Path Forwarding (RPF) only when you have selected the <b>Trusted Source</b> check box. This option allows traffic on the interface only if return traffic can be forwarded on the same interface. This helps to prevent traffic from unknown sources like malicious traffic on an Enterprise network. If the incoming source is unknown, then the packet is dropped at ingress without creating flows. Select one of the following options from the drop-down menu:</p> <ul style="list-style-type: none"> <li>■ <b>Not Enabled</b> – Allows incoming traffic even if there is no matching route in the route table.</li> <li>■ <b>Specific</b> – This option is selected by default, even when the <b>Trusted Source</b> option is deactivated. The incoming traffic should match a specific return route on the incoming interface. If a specific match is not found, then the incoming packet is dropped. This is a commonly used mode on interfaces configured with public overlays and NAT.</li> <li>■ <b>Loose</b> – The incoming traffic should match any route (Connected/Static/Routed) in the routing table. This allows asymmetrical routing and is commonly used on interfaces that are configured without next hop.</li> </ul>
-------------------------	---

For IPv6 address, configure the **IPv6 DHCP Server** as follows:

**Note** This option appears only when you select the **Addressing Type** as **Static**.

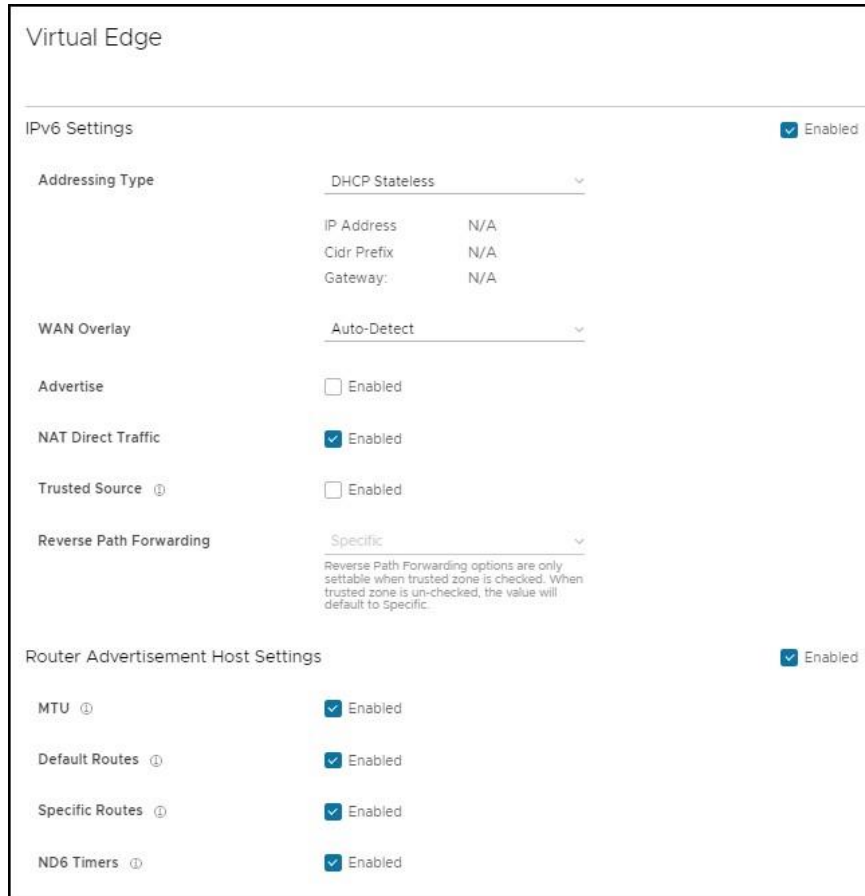
- **Activated:** Activates DHCPv6 with the Edge as the DHCPv6 server. If you choose this option, configure the following details:
  - **DHCP Start:** Enter a valid IPv6 address available within the subnet.
  - **Num. Addresses:** Enter the number of IP addresses available on a subnet in the DHCPv6 Server.
  - **Lease Time :** Select the period of time from the drop-down list. This is the duration the VLAN is allowed to use an IPv6 address dynamically assigned by the DHCPv6 Server.
  - **DHCPv6 Prefix Delegation:** Click **Add** to assign prefixes chosen from a global pool to DHCP clients. Enter the prefix pool name along with the prefix start and end details.
  - **Options** – Click **Add** to add pre-defined or custom DHCP options from the drop-down menu. The DHCP option is a network service passed to the clients from the DHCP server. Choose a custom option and enter the code, data type, and value.
- **Relay** – Allows DHCP with the DHCP Relay Agent installed at a remote location. If you choose this option, configure the following:
  - **Relay Agent IP(s):** Specify the IP address of Relay Agent. Click **Add** to add more IP addresses.

**Note**

- You must provide the Server IP address as the **Relay Agent IP** address on the customer-facing Interface.
- If this Interface belongs to a non-global segment, the Server must be reached through the same non-global segment.

- **Deactivated:** Deactivates the DHCP server.

**Router Advertisement Host Settings:** The Router Advertisement (RA) parameters are available only when you activate **IPv6 Settings**, and then choose the **Addressing Type** as **DHCP Stateless** or **DHCP Stateful**.



The screenshot shows the 'Virtual Edge' configuration page. Under 'IPv6 Settings', 'Enabled' is checked. 'Addressing Type' is set to 'DHCP Stateless', with 'IP Address', 'Cidr Prefix', and 'Gateway' all set to 'N/A'. 'WAN Overlay' is set to 'Auto-Detect'. 'Advertise' is unchecked, 'NAT Direct Traffic' is checked, and 'Trusted Source' is unchecked. 'Reverse Path Forwarding' is set to 'Specific'. Below this, 'Router Advertisement Host Settings' are shown, with 'Enabled' checked. Under these settings, 'MTU', 'Default Routes', 'Specific Routes', and 'ND6 Timers' are all checked.

The following RA parameters are selected by default. If required, you can turn them off.

Option	Description
MTU	Accepts the MTU value received through Route Advertisement. If you turn off this option, the MTU configuration of the Interface is considered.
Default Routes	Installs default routes when Route Advertisement is received on the Interface. If you turn off this option, then there are no default routes available for the Interface.

Specific Routes	Installs specific routes when Route Advertisement receives route information on the Interface. If you turn off this option, the Interface does not install the route information.
ND6 Timers	Accepts ND6 timers received through Route Advertisement. If you turn off this option, default ND6 timers are considered. The default value for NDP retransmit timer is 1 second and NDP reachable timeout is 30 seconds.

---

**Note** When RA host parameters are deactivated and activated again, then Edge waits for the next RA to be received before installing routes, MTU, and ND/NS parameters.

---

## Wi-Fi Access Control based on MAC Address

Wi-Fi Access Control can be used as an additional layer of security for wireless networks. When activated, only known and approved MAC addresses are permitted to associate with the base station.

Edge 500

WLAN1

☒ Override

Interface Enabled

☒ Enabled

VLAN

1 - Corporate

SSID

vc-wifi

☒ Broadcast

Security

WPA2/Personal

Password

.....

☐

Static MAC Allow List

☒ Enabled

+ ADD

☐ DELETE

<input type="checkbox"/>	MAC Address	Description
<input type="checkbox"/>	00:16:3e:00: ...	Enter De...
<input type="checkbox"/>	Enter MAC A...	Enter De...
		2 items

MAC filtering for AP probes

☒ Enabled

CANCEL

SAVE

- 1 In the Enterprise portal, click **Configure > Edges** and choose an existing WLAN interface to configure the following parameters.

Option	Description
Interface Enabled	Select the check box to activate the interface.
VLAN	Choose the <b>VLAN</b> ID from the drop-down menu.
SSID	Enter the <b>SSID</b> .

Option	Description
Security	Select either <b>WPA2/Enterprise</b> or <b>WPA2/Personal</b> as the Security option.
Static MAC Allow List	<p>Select the check box to permit only the listed MACs to associate with the access point.</p> <p>When <b>Static MAC Allow List</b> is configured, only the Mac addresses specified in the list are permitted to associate with the access point.</p>
Radius ACL Check	<p>Select the check box to associate the MAC address with a RADIUS server. If an access-accept is received, the MAC is allowed to associate with the access point.</p> <p><b>Note</b> RADIUS ACL checks are limited to <b>WPA2/Enterprise</b> security mode.</p>
Add	Click to enter a new MAC address.
Delete	Click to remove an existing MAC address.
MAC filtering for AP Probes	<p>Enabling MAC Filtering for AP probes prevents probes from unapproved MAC Addresses from actively discovering AP parameters. When the SSID is not broadcast, this can assist in preventing unknown stations from connecting to the network. Some devices are known to use random MAC addresses for probing regardless of AP settings and probe filtering may cause these devices to fail to discover or connect to the network even if their device MAC has been approved.</p>

**Note** Both, **MAC filtering for AP Probes** and **RADIUS ACL Check** cannot happen at the same time.