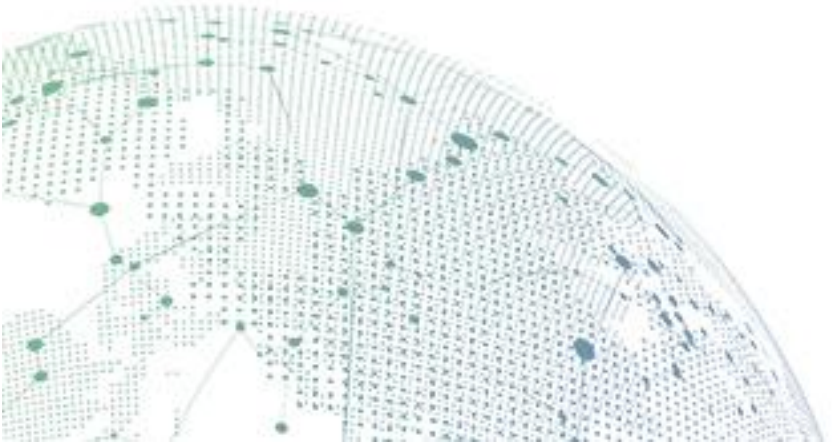
SANGFOR

IAM

Multi Bridge Mode Deployment Guide

Version 12.0.13



Change Log

Date	Change Description

CONTENT

Chapter 1 Functionality Summary

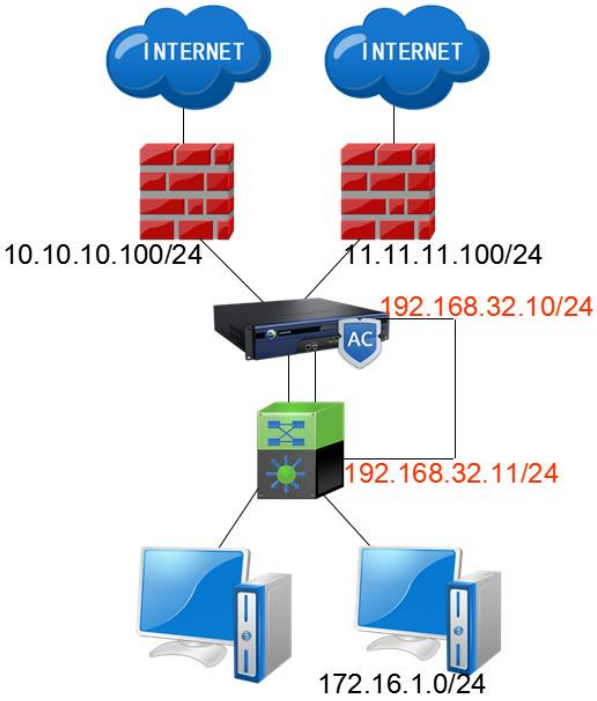
1. The device needs to be serve as a network cable with filtering function. It is generally enabled when it is not convenient to change the original network topology.
2. Connect the device between the original gateway and the intranet users. If the original gateway and the intranet users do not need to make any configuration changes, they can use the device by doing some configuration.
3. The existence of the device is not known for the original gateway and intranet users which is transparent to the original gateway and intranet users. The main feature of the bridge mode is that the bridge mode is completely transparent to the user.

Chapter 2 Application Scenario

When the device is deployed in multi-bridge mode, there is basically no change to the customer's original network. When the IAM is deployed in the bridge mode, the IAM is a transparent device for the customer. If IAM device is causing netowrk down, hardware bypass function can be enabled to resume network communication.

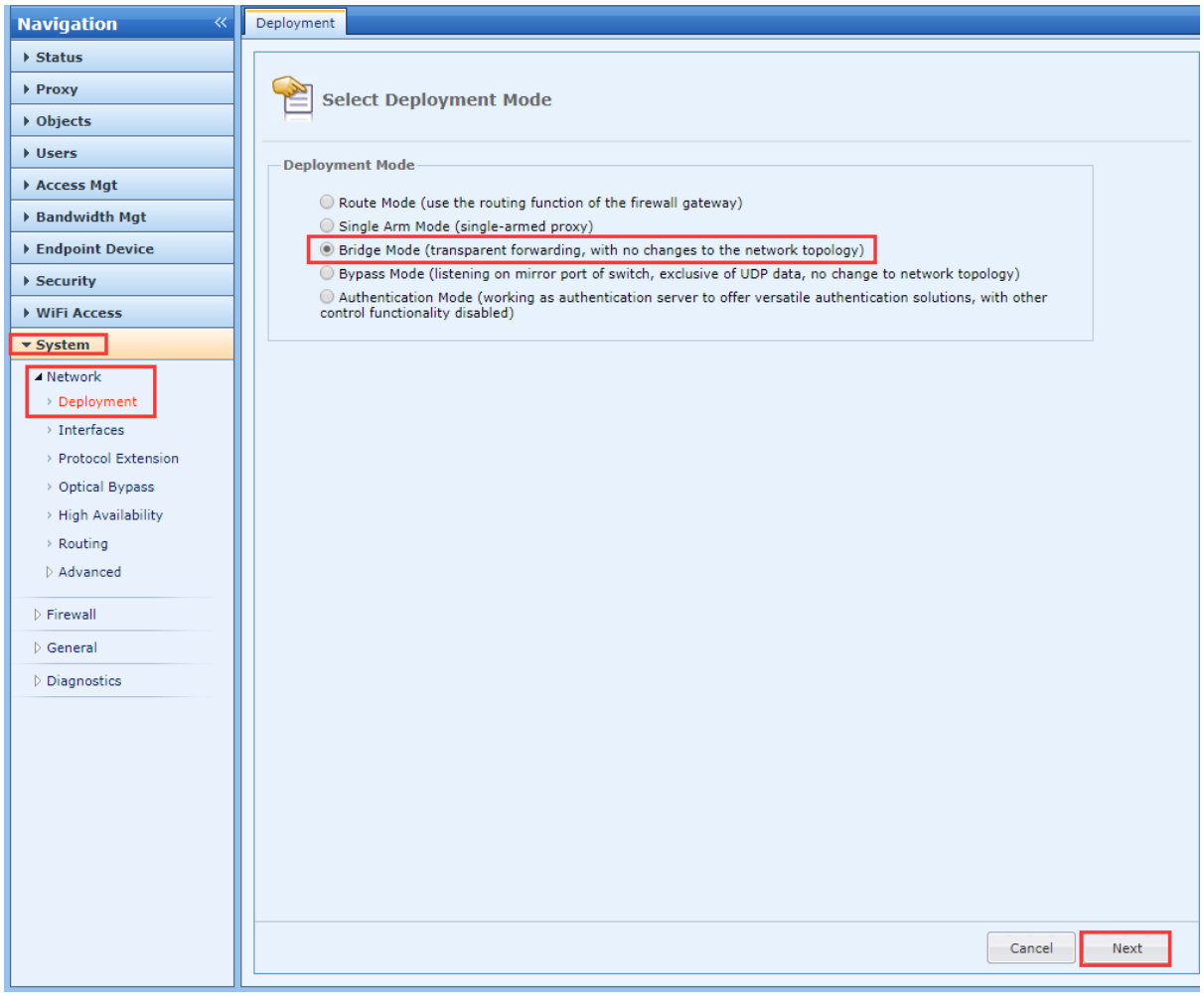
Chapter 3 Configuration

3.1 Scenario 1 : Recommend to use DMZ port to manage device



The configuration on the IAM can be divided into the configuration for deployment mode and static routes. The details are as follows:

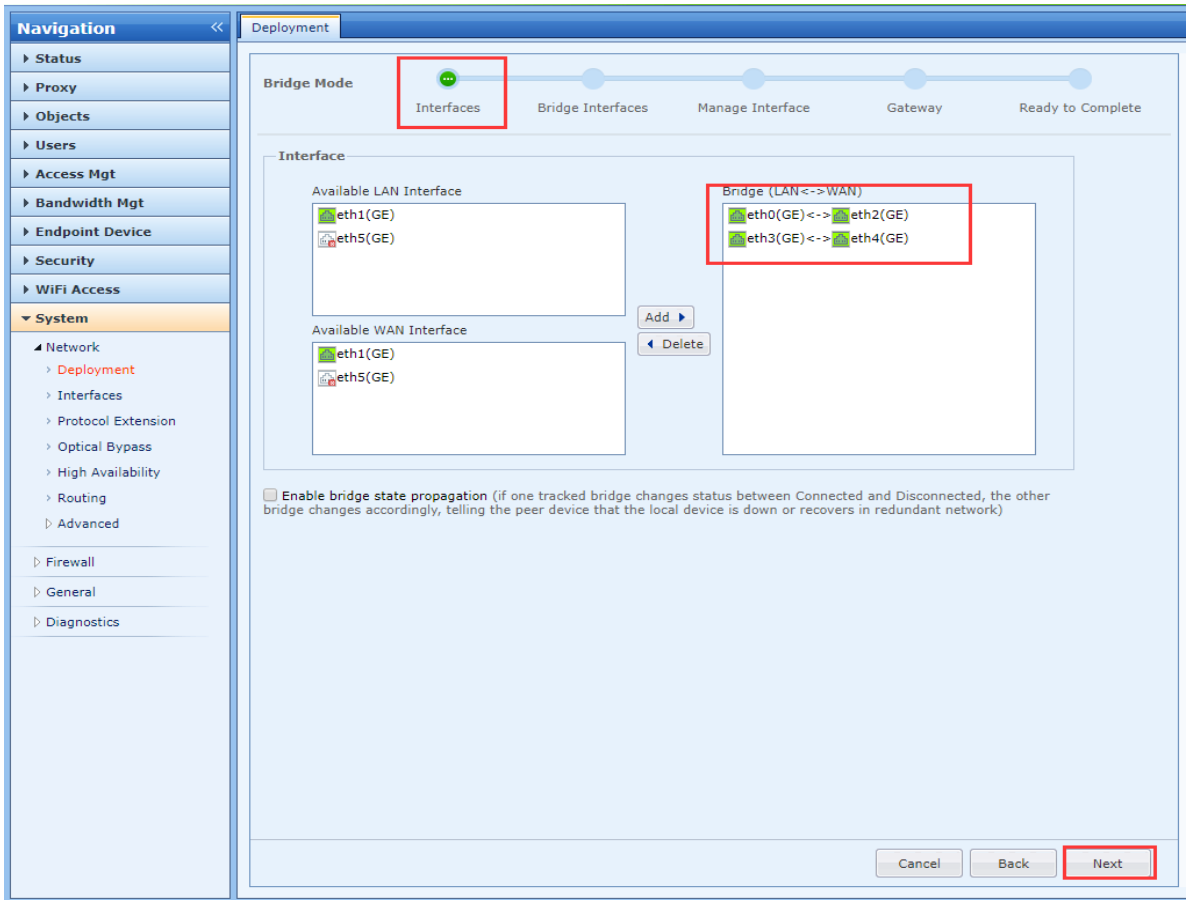
1. In **Deployment**, start the configuration by selecting Bridge Mode as shown below.



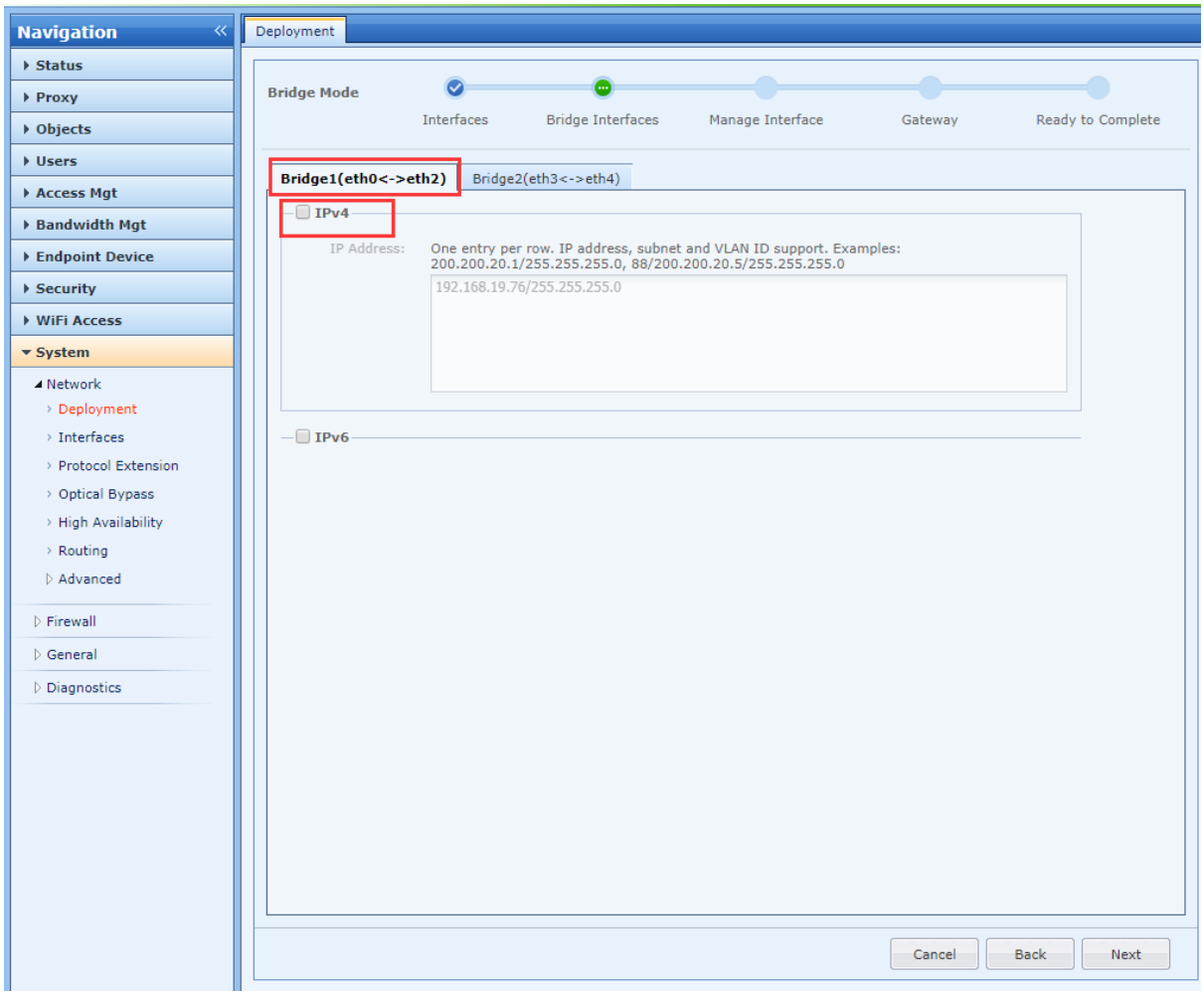
In **Interfaces**, select Bridge (LAN←→WAN), bridge state propagation is enable by default.

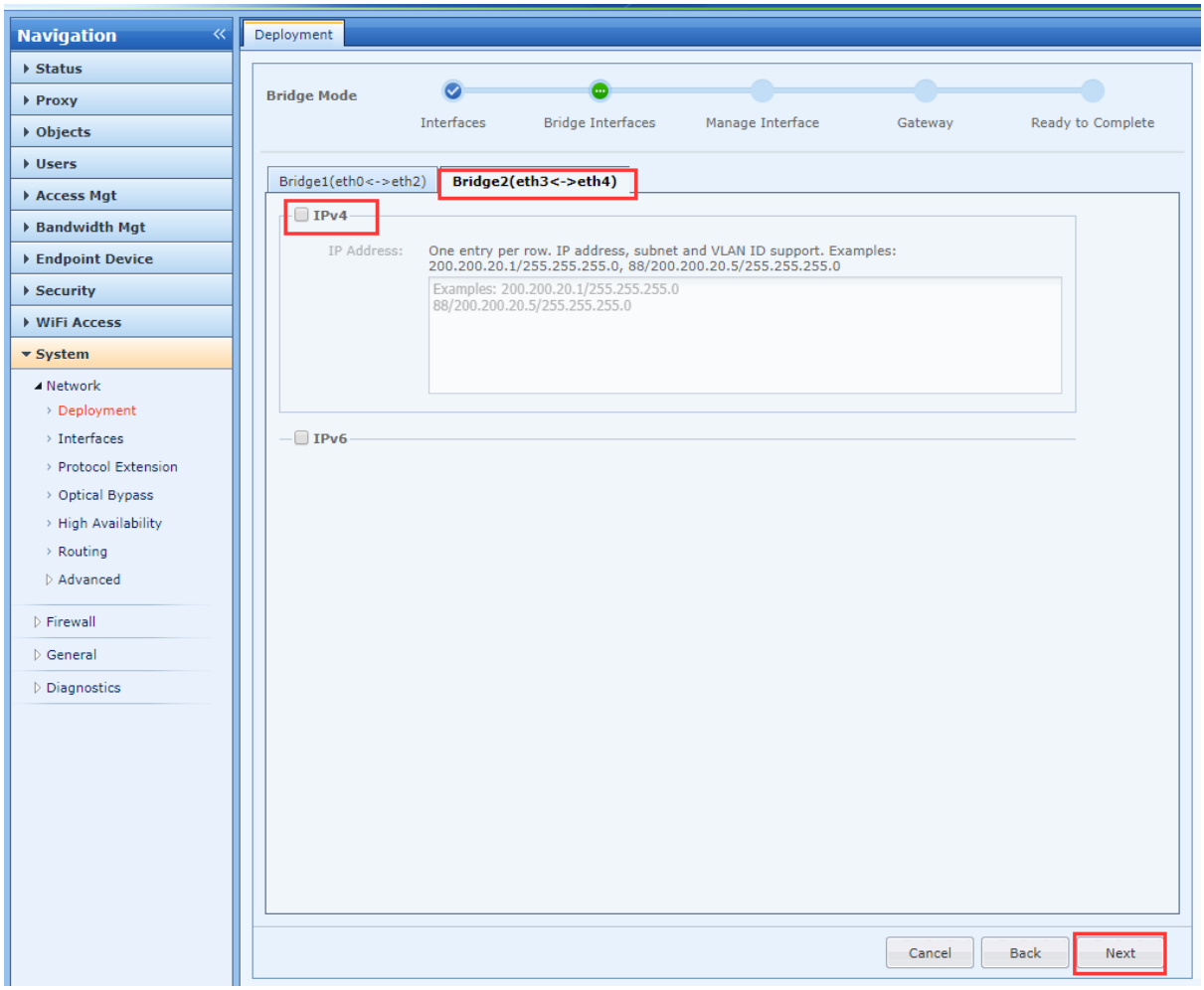
[Note]

- "Enable bridge state propagation" function is enable by default, the selected Bridge (LAN←→WAN) whether support state propagation will show in Interfaces Tracking.
- You can select one pair of interfaces for a bridge or multiple pair of interfaces for multi-bridge based on customer's network environment.

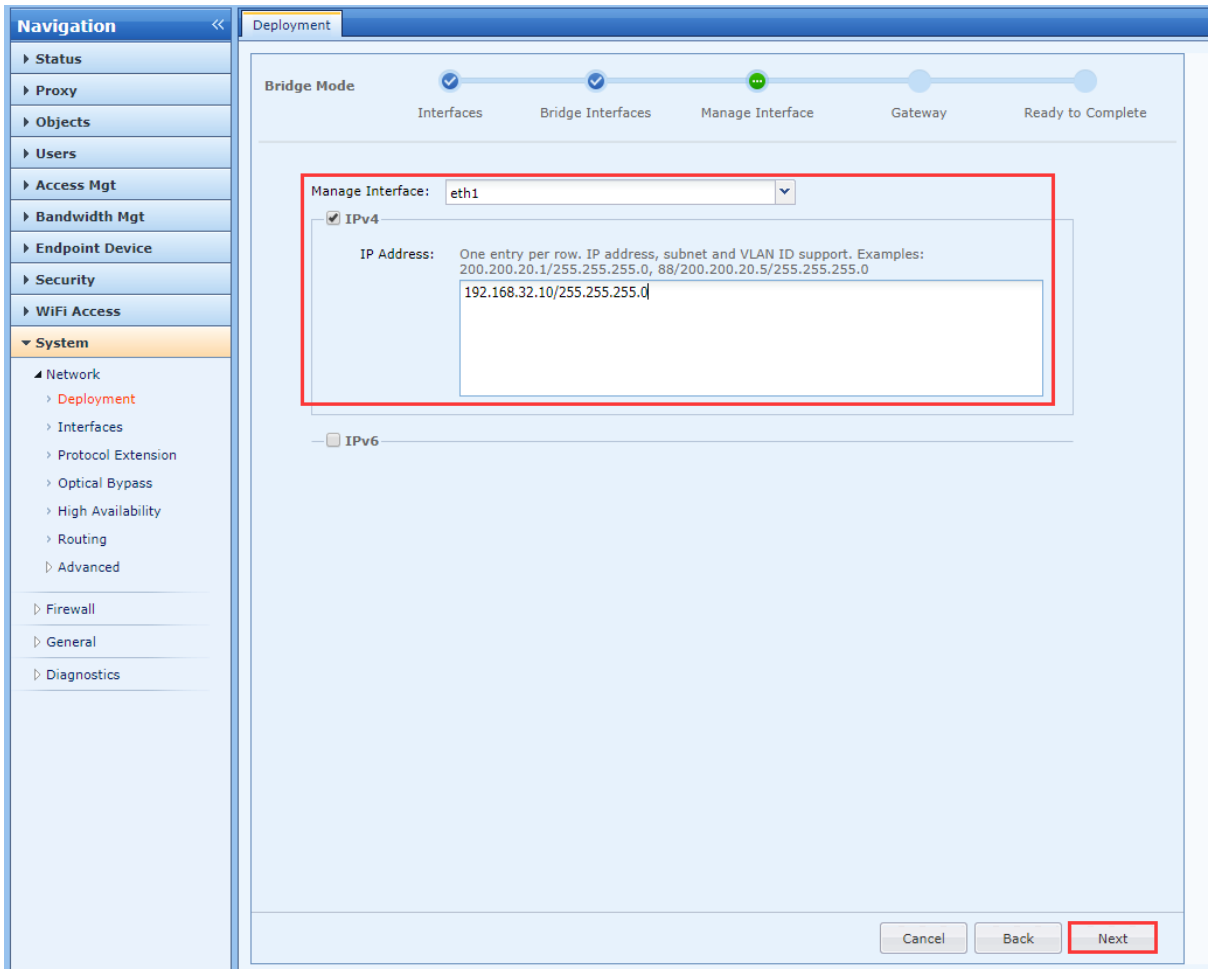


b. In **Bridge Interfaces**, do not need to configure bridge IP.

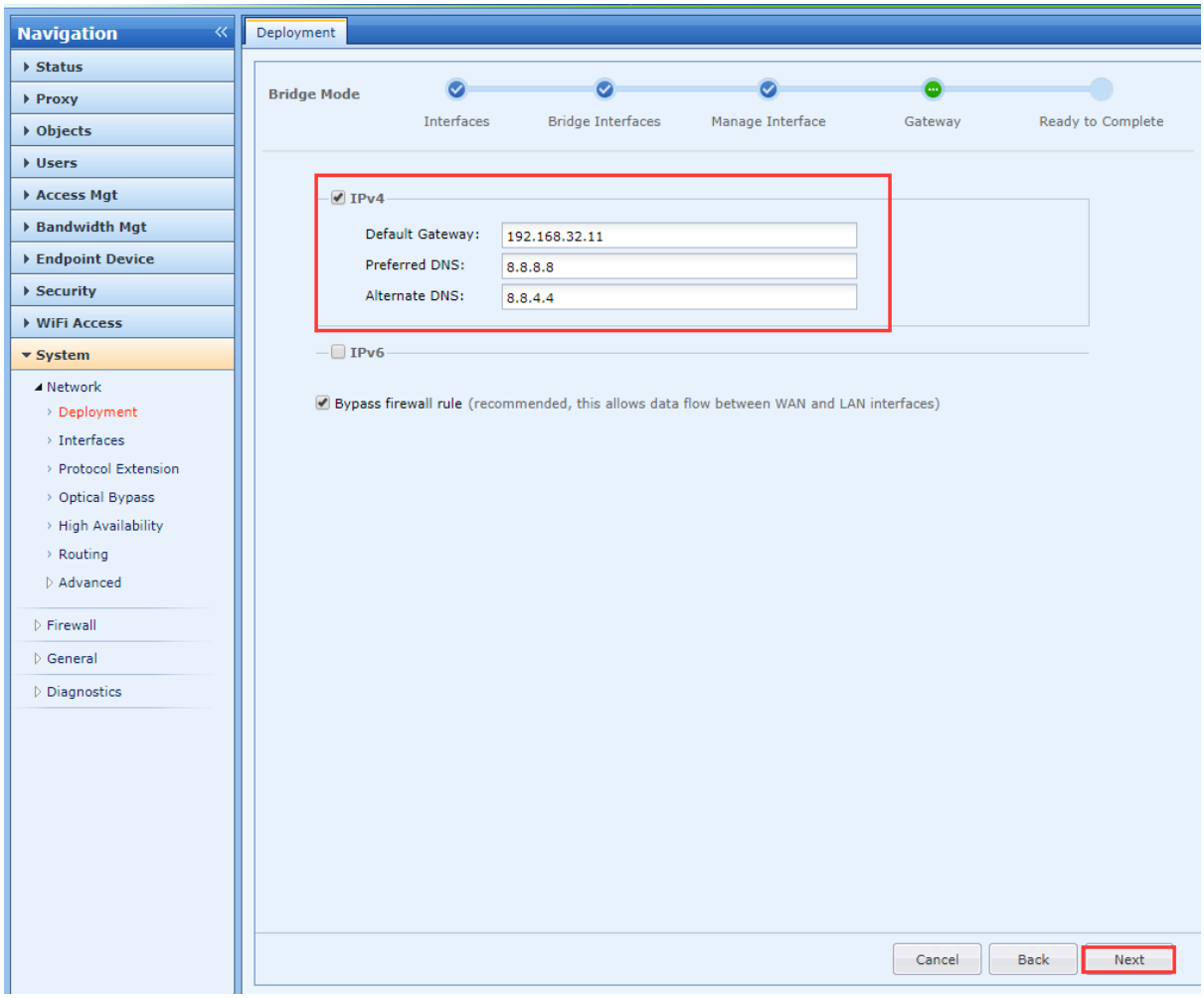

Navigation
Status
Proxy
Objects
Users
Access Mgt
Bandwidth Mgt
Endpoint Device
Security
WiFi Access
System
Network
Deployment
Interfaces
Protocol Extension
Optical Bypass
High Availability
Routing
Advanced
Firewall
General
Diagnostics
Deployment
Bridge Mode
Interfaces
Bridge Interfaces
Manage Interface
Gateway
Ready to Complete
Bridge1(eth0<->eth2)
Bridge2(eth3<->eth4)
IPv4
IP Address:
One entry per row. IP address, subnet and VLAN ID support. Examples:
200.200.20.1/255.255.255.0, 88/200.200.20.5/255.255.255.0
192.168.19.76/255.255.255.0
IPv6
Cancel
Back
Next


Navigation
Status
Proxy
Objects
Users
Access Mgt
Bandwidth Mgt
Endpoint Device
Security
WiFi Access
System
Network
Deployment
Interfaces
Protocol Extension
Optical Bypass
High Availability
Routing
Advanced
Firewall
General
Diagnostics
Deployment
Bridge Mode
Interfaces
Bridge Interfaces
Manage Interface
Gateway
Ready to Complete
Bridge1(eth0<->eth2)
Bridge2(eth3<->eth4)
IPv4
IP Address:
One entry per row. IP address, subnet and VLAN ID support. Examples:
200.200.20.1/255.255.255.0, 88/200.200.20.5/255.255.255.0
Examples: 200.200.20.1/255.255.255.0
88/200.200.20.5/255.255.255.0
IPv6
Cancel
Back
Next

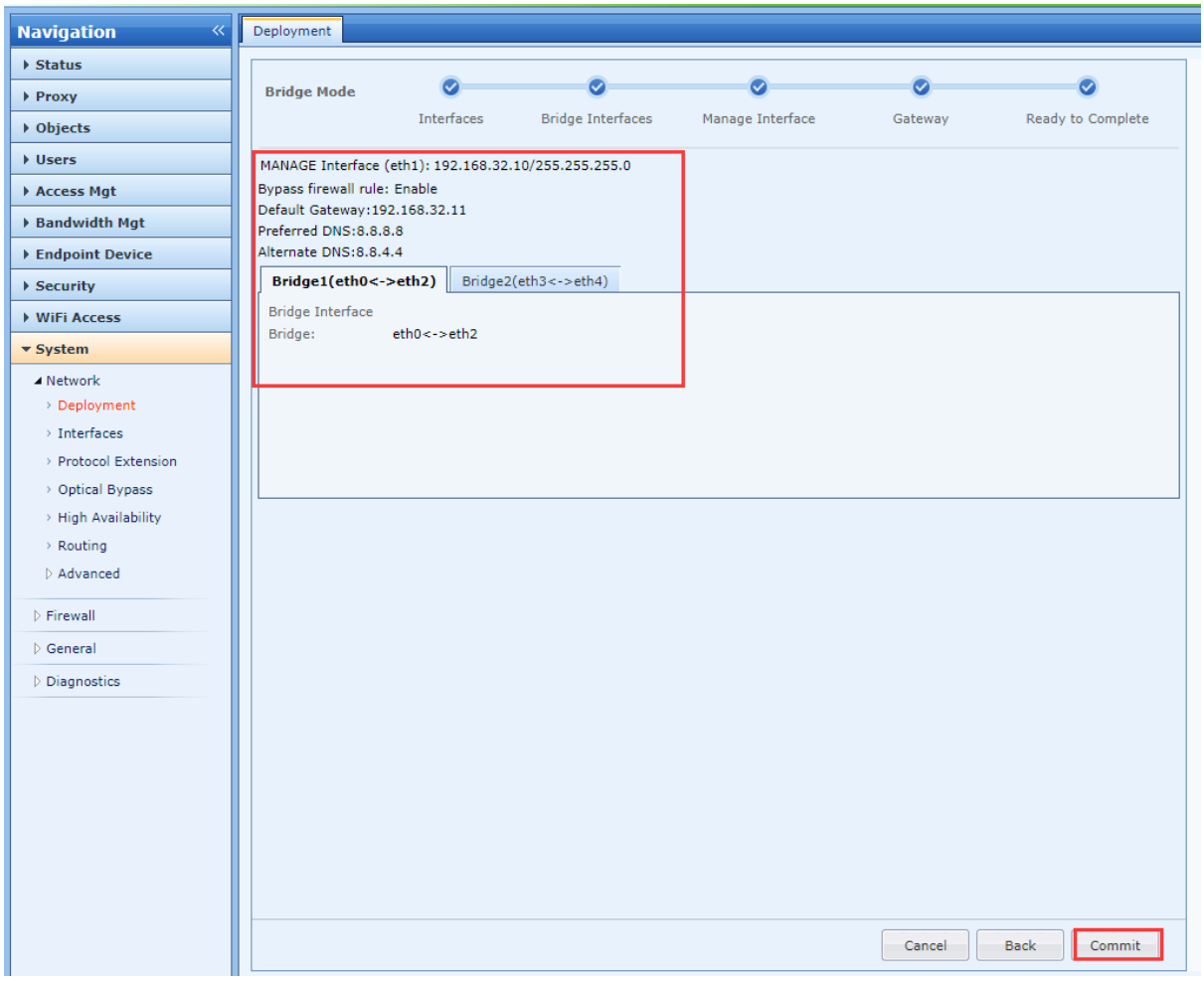
b. In **Manage Interface**, configure manage interface IP.

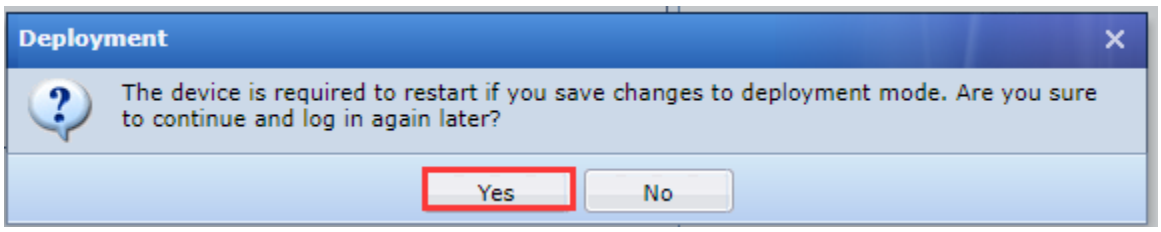


c. In **Gateway**, configure gateway IP address. Gateway point to device address that IAM manage interface connected.



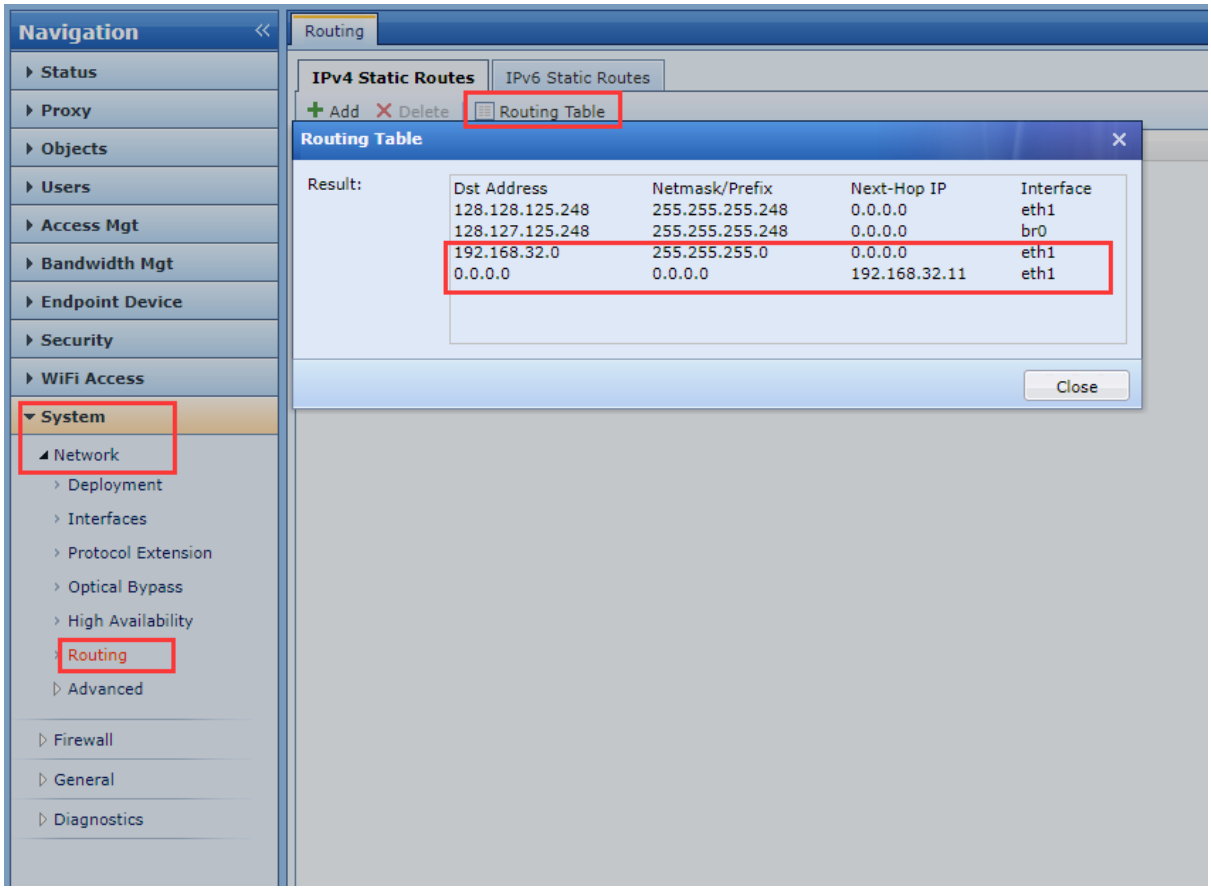
d. When click “Commit” in **Ready to Complete**, it will remind the device require to restart. When the device restart successfully after select “Yes”, the manage interface able to manage the device.





2. Add new static route

The default gateway already configure in deployment mode will automatically generate default route.

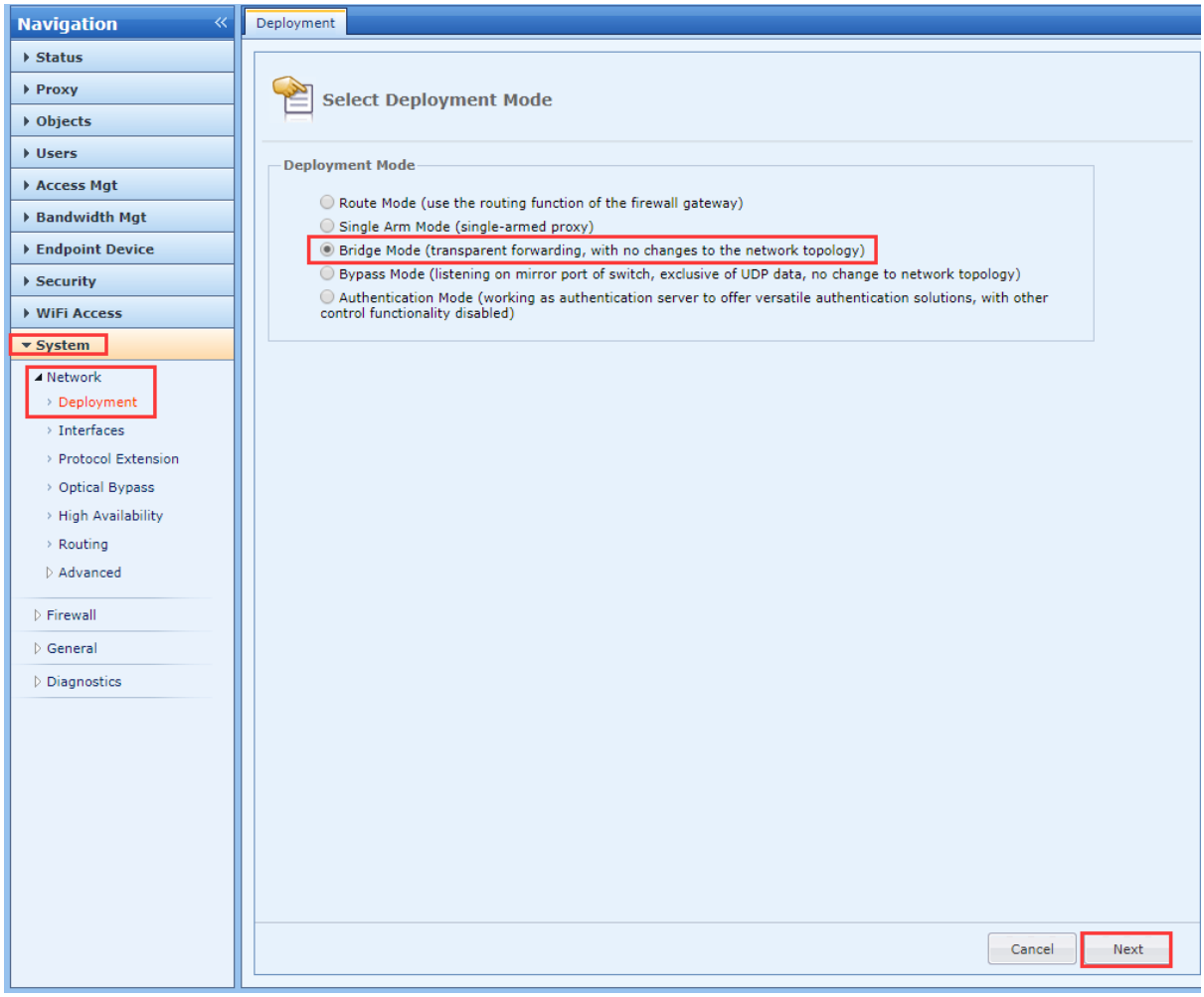


3. Add new authentication policy.

Based on the customer requirement to configure relevant authentication policy and the device is ready to be used in the network.

3.2 Scenario 2: The device does not have idle interface and require to use bridge IP to manage devices.

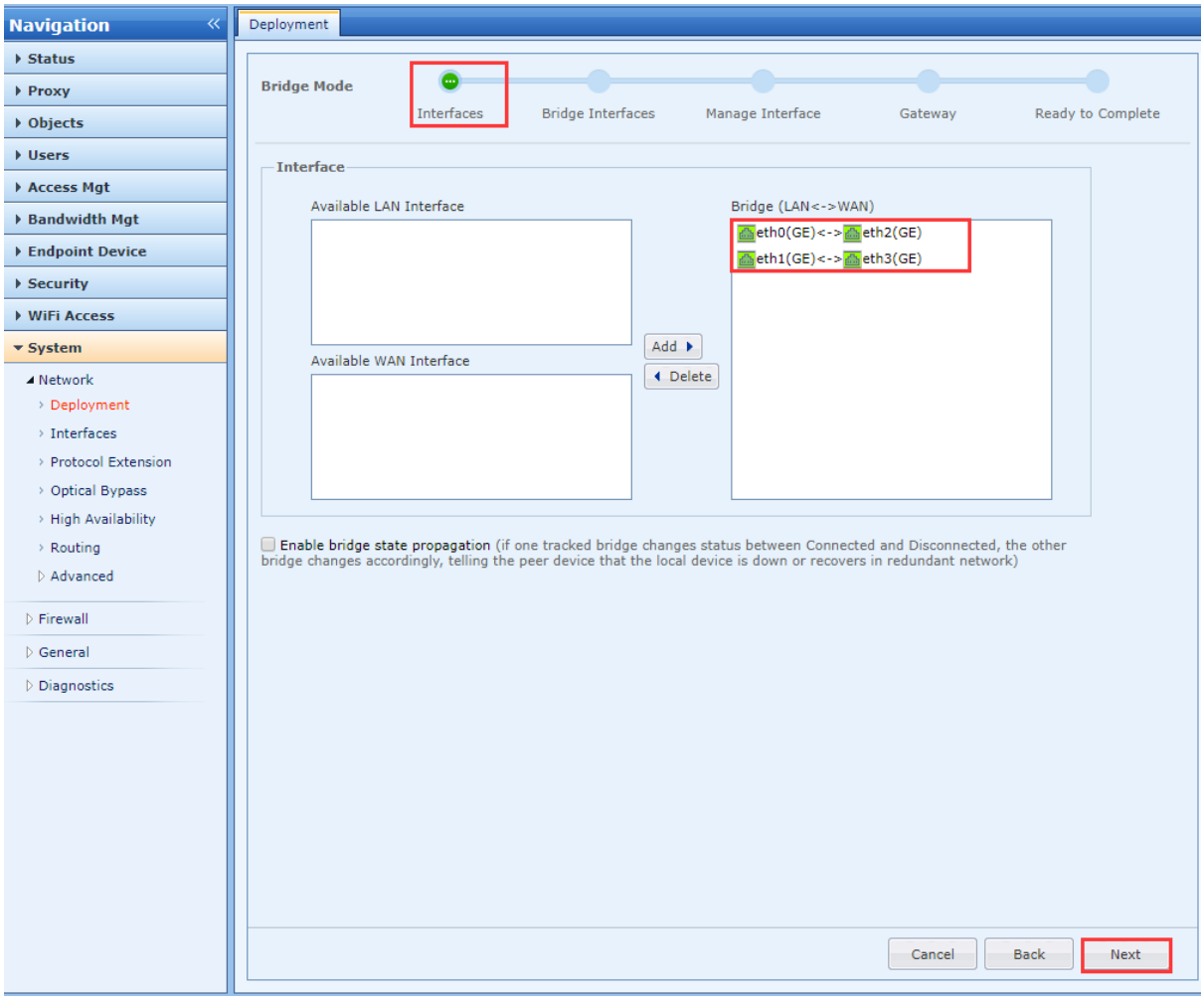
1. In **Deployment** , start the configuration by selecting Bridge Mode as shown below.



a. In **Interfaces**, select Bridge (LAN←→WAN), bridge state propagation is enable by default.

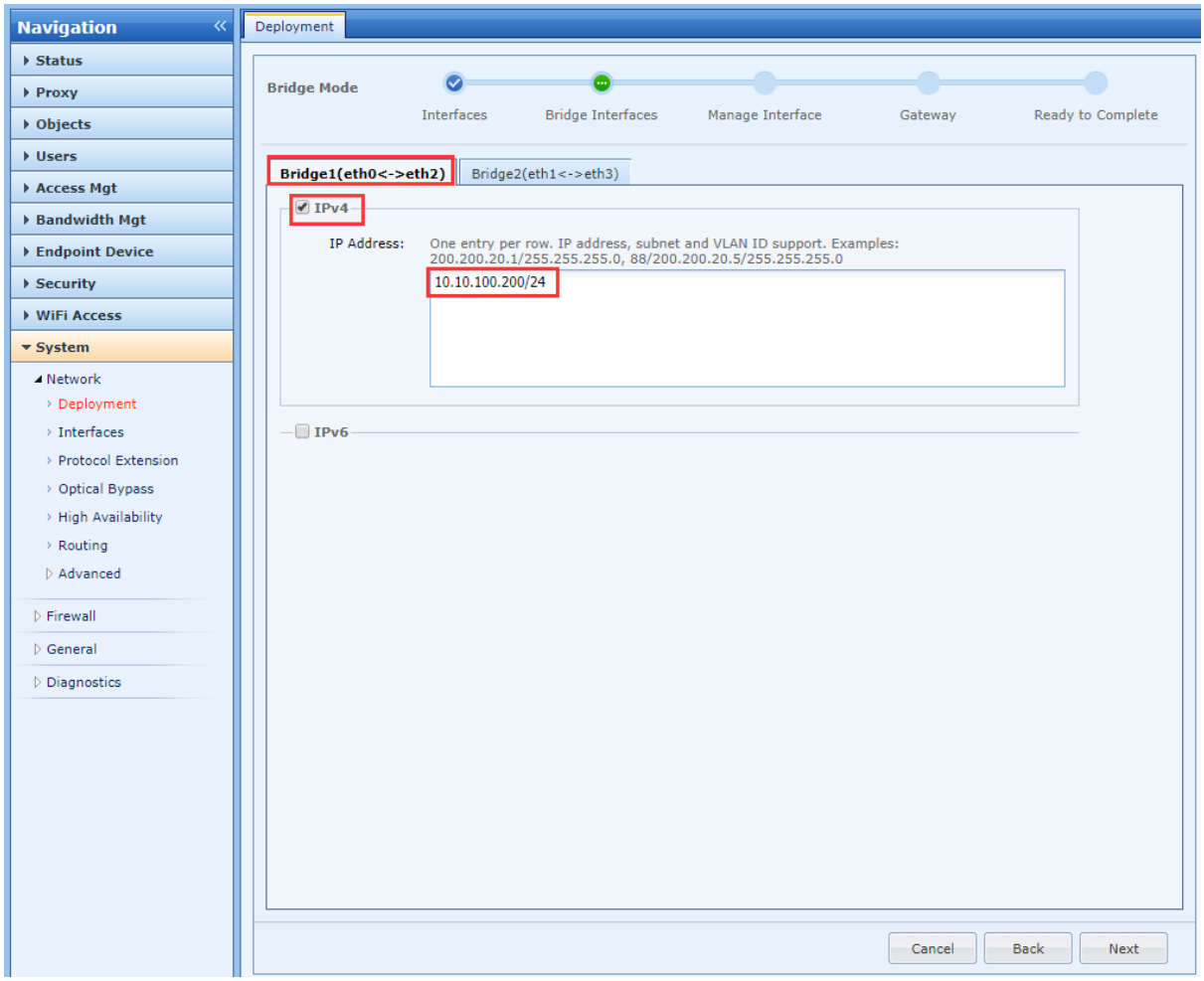
[Note]

- "Enable bridge state propagation" function is enable by default, the selected Bridge (LAN←→WAN) whether support state propagation will show in Interfaces Tracking.
- You can select one pair of interfaces for a bridge or multiple pair of interfaces for multi-bridge based on customer's network environment.

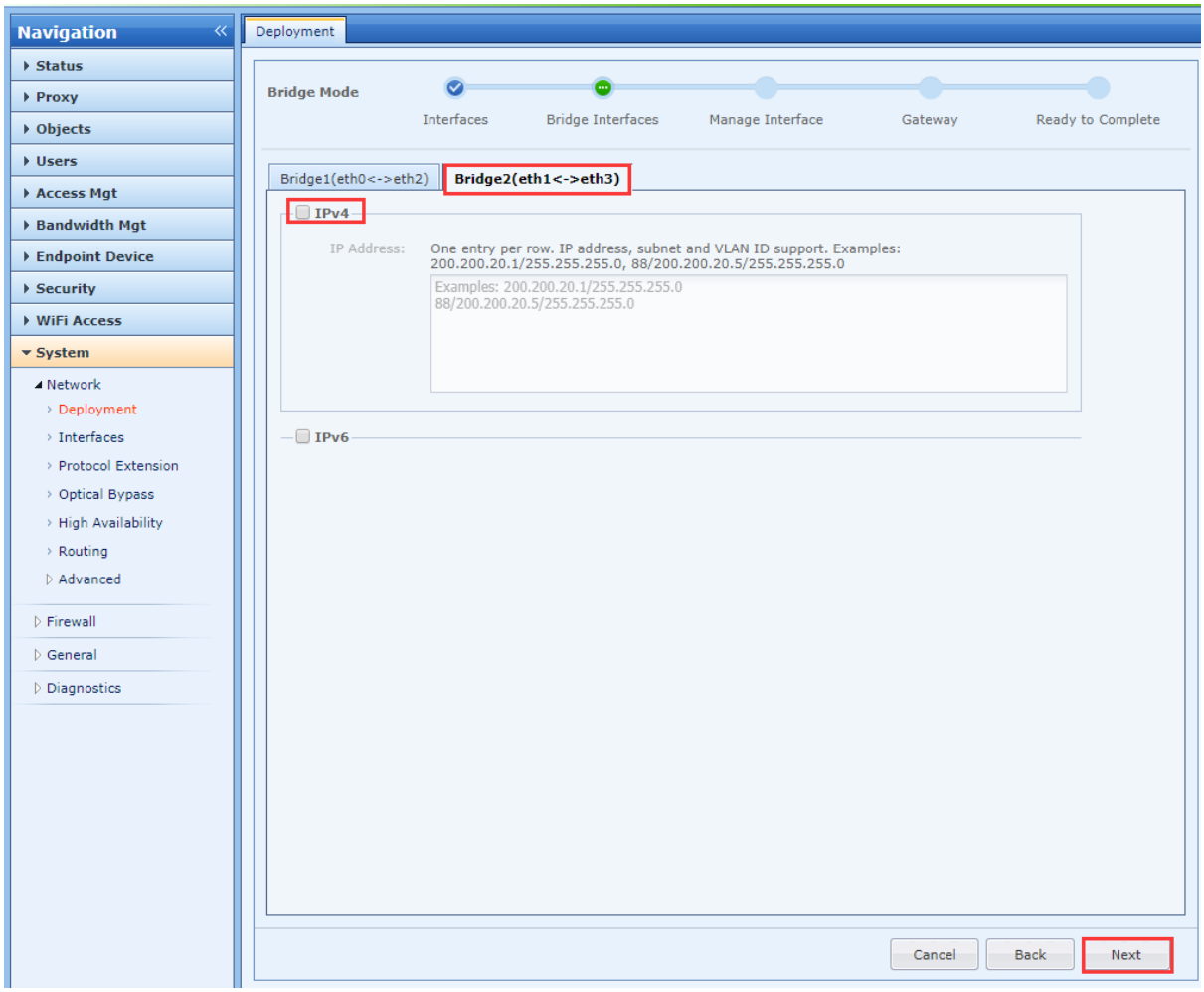

Navigation
Status
Proxy
Objects
Users
Access Mgt
Bandwidth Mgt
Endpoint Device
Security
WiFi Access
System
Network
Deployment
Interfaces
Protocol Extension
Optical Bypass
High Availability
Routing
Advanced
Firewall
General
Diagnostics
Deployment
Bridge Mode
Interfaces
Bridge Interfaces
Manage Interface
Gateway
Ready to Complete
Interface
Available LAN Interface
Available WAN Interface
Add
Delete
Bridge (LAN<->WAN)
eth0(GE)<->eth2(GE)
eth1(GE)<->eth3(GE)
Enable bridge state propagation (if one tracked bridge changes status between Connected and Disconnected, the other bridge changes accordingly, telling the peer device that the local device is down or recovers in redundant network)
Cancel
Back
Next

b. In **Bridge Interfaces**, configure a usable bridge IP for the bridge to manage the device. Bridge IP configuration support both IPV4 and IPV6, select based on the network environment.

1. Configure IP for Bridge 1.



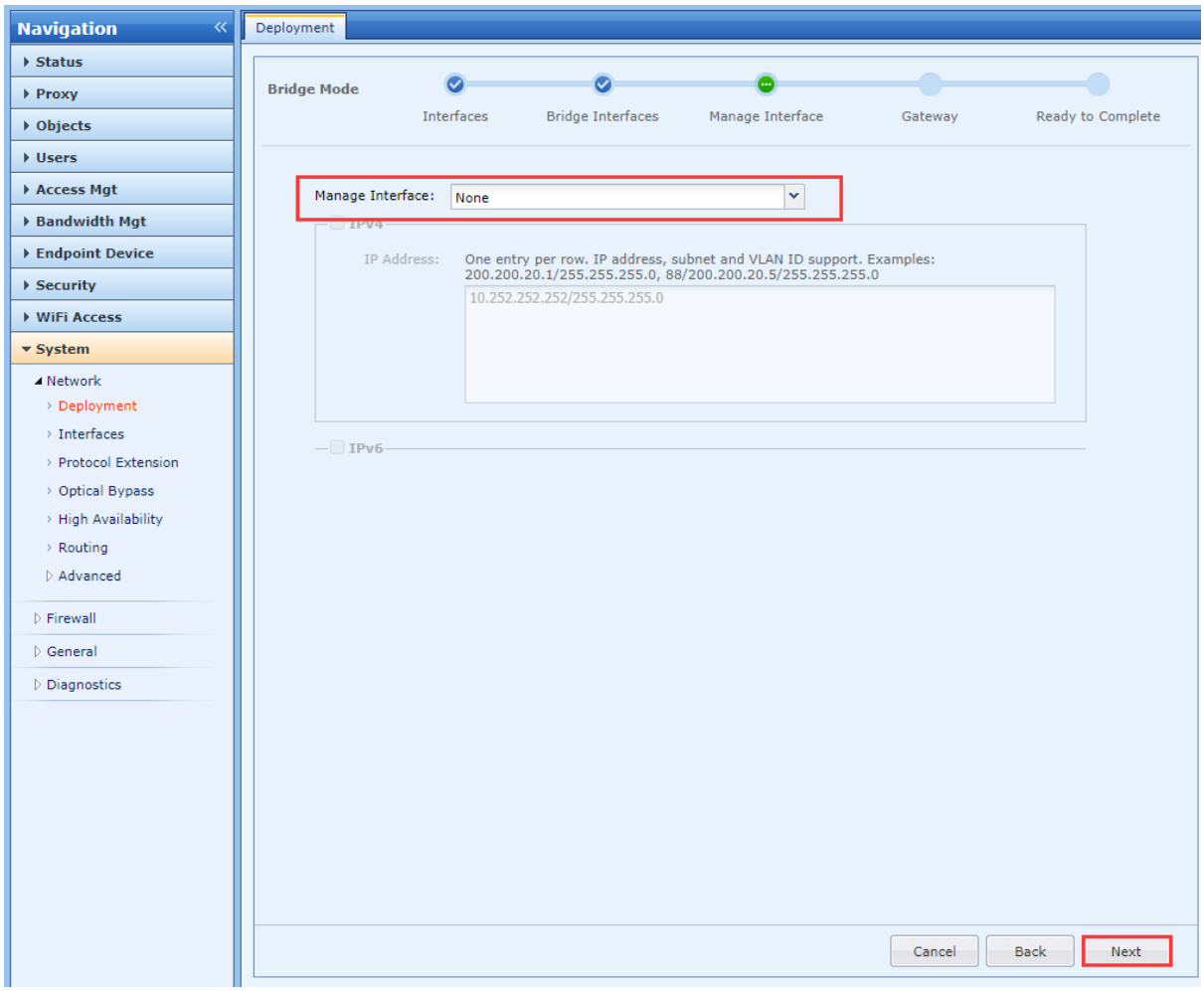
1. No configuration for another Bridge.



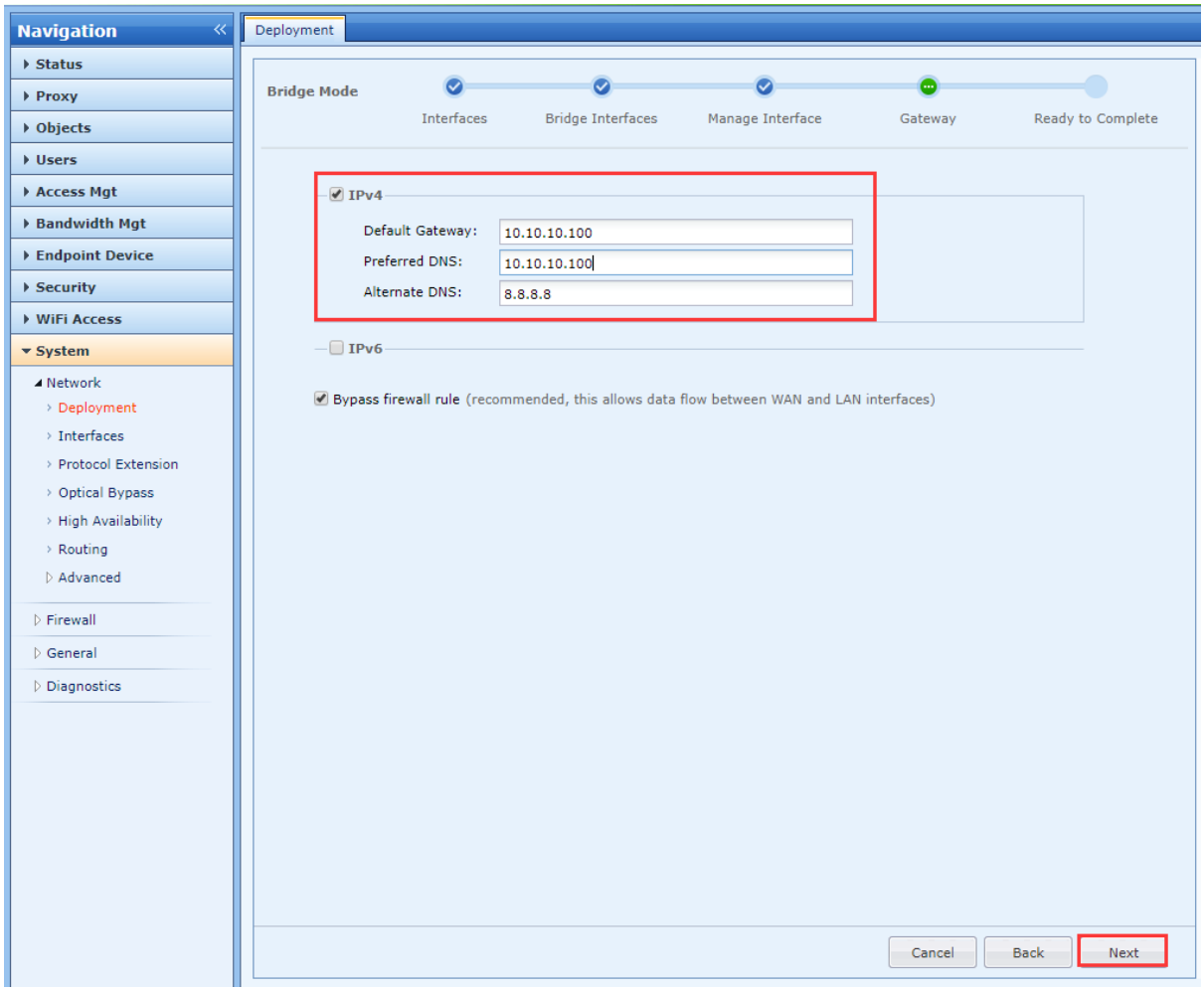
[Note]

No matter how many sets of bridges are configured, select one set of bridges to configure the bridge IP to manage the devices. Other bridges do not need to configure the bridge IP.

c. In **Manage Interface**, select None for the interface.



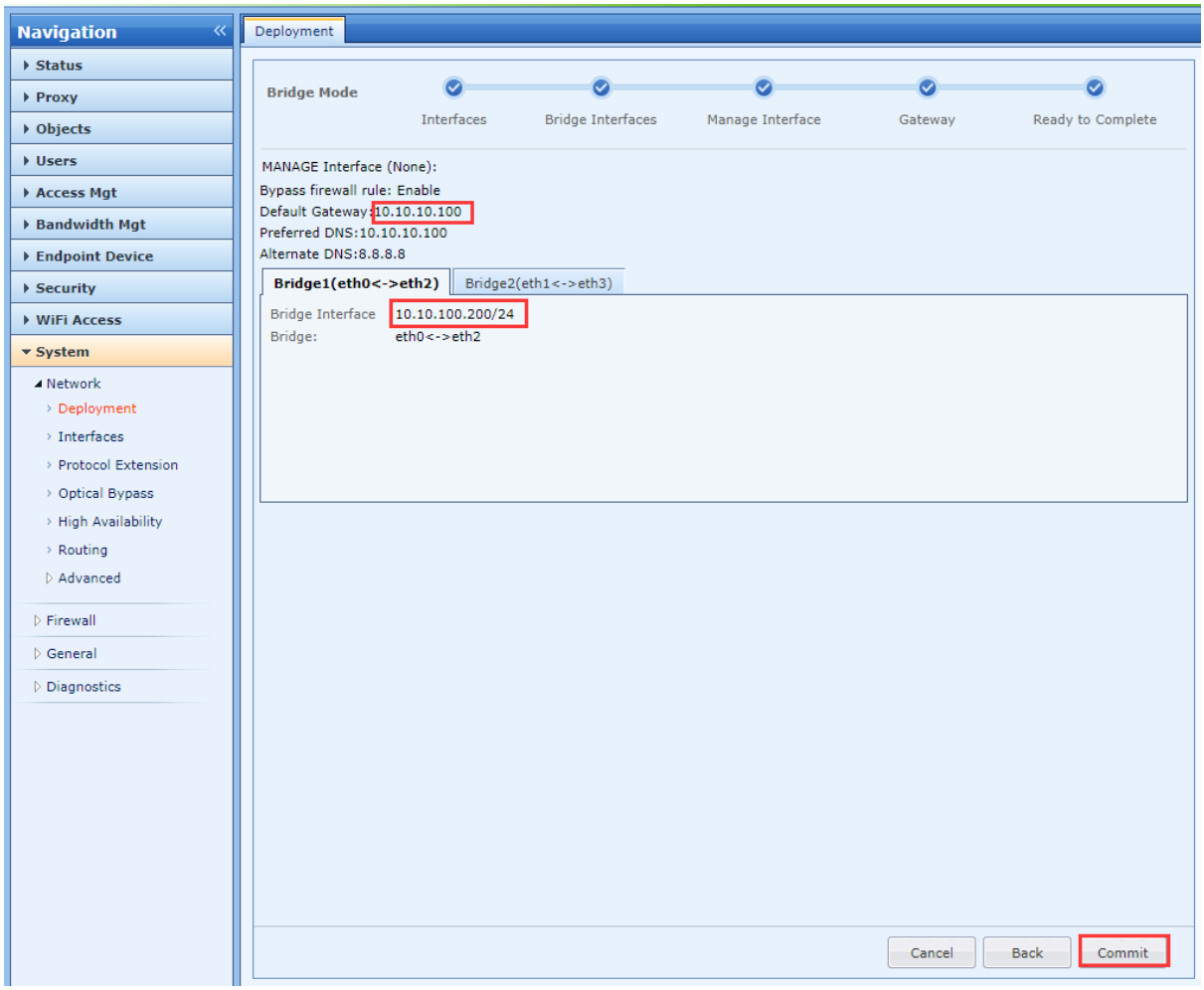
d. In **Gateway**, configure gateway IP address. Gateway point to device address that IAM WAN interface connected.

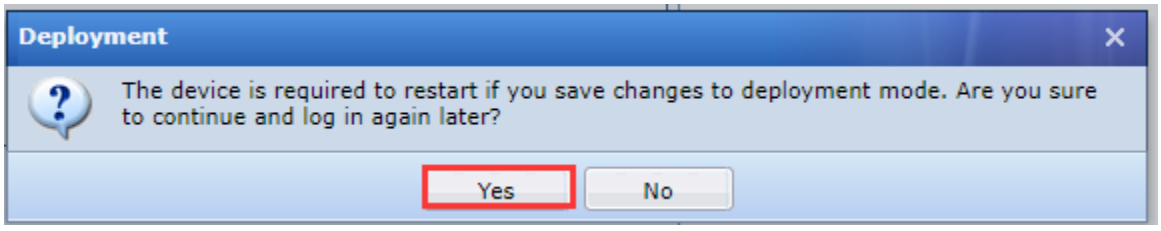


[Note]

In a multi-bridge environment, you only need to configure one gateway address which can access the Internet.

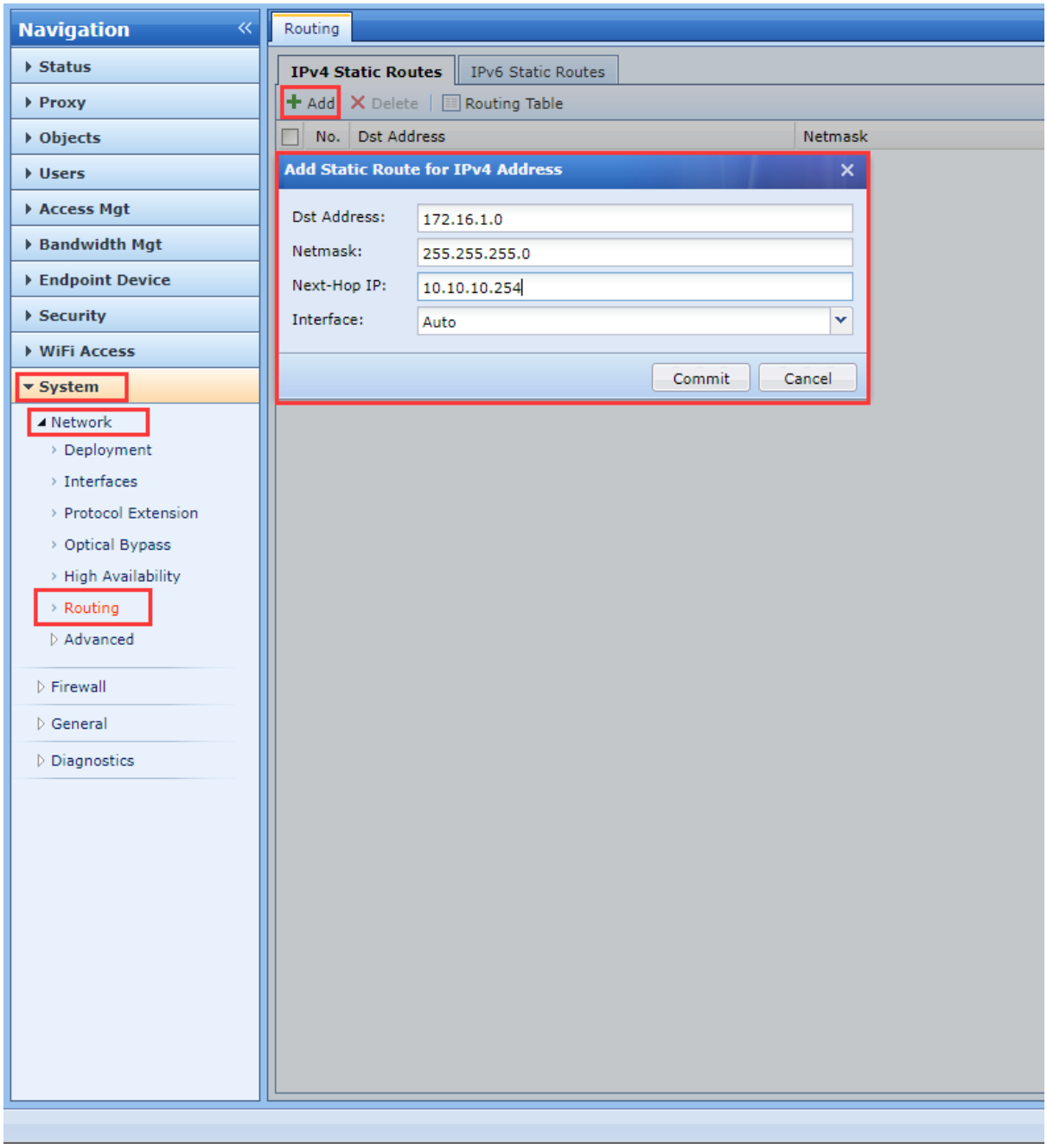
e. When click “Commit” in **Ready to Complete**, it will remind the device require to restart. When the device restart successfully after select “Yes”, the bridge interface able to manage the device.





2. Add new statis route.

If the internal network and the IAM are in a layer three environment, static route need to be configure for the internal network. Otherwise, the device cannot be redirected which cause some pages unable to be redirect such as authentication page.



3. Add new authentication policy.

Based on the customer requirement to configure relevant authentication policy and the device is ready to be deploy in the network.

Chapter 4 Precautions

4.1 Multi-bridge has no special protocol redirection function. By default, the device virtual address is used for redirection. No configuration is required here, keep the default.

4.2 The Layer 3 switch connected to the IAM management port enables the trunk to manage the device through the management port. The management port also needs to enable VLAN.