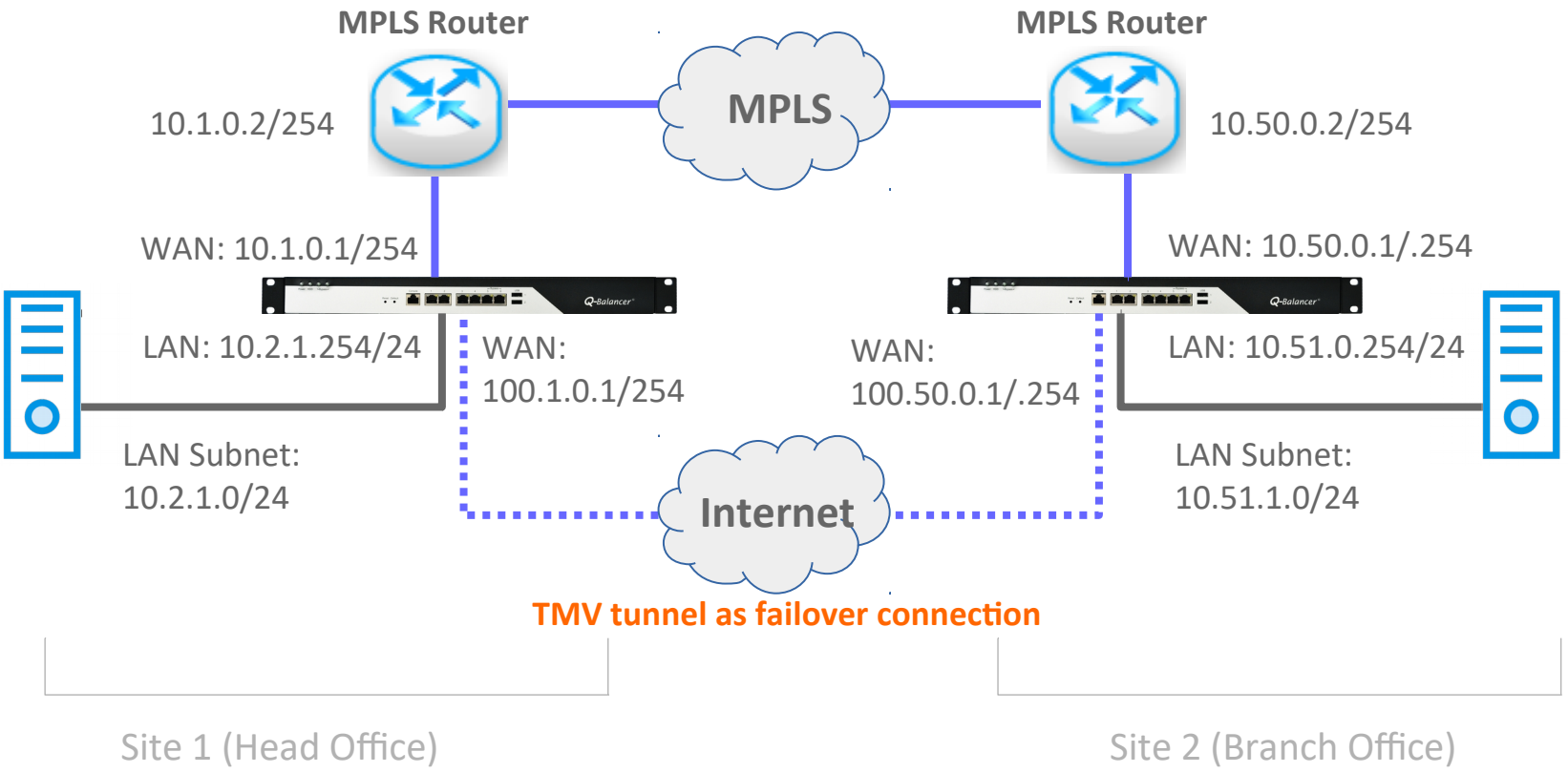
How To Guide:

Hybrid WAN Configuration

Introduction

This article outlines the configuration of hybrid WAN network, which augments the traditional private WAN network. In the following example, a company with multiple locations wants users to experience high-quality and reliable VoIP calls over a private WAN network. The diagram below shows the network topology for this example, where branch and head office sites are connected using a single dedicated private network that is a point to point connection.

Diagram Example



Requirement

In this case, the configuration is requested to:

1. Direct VoIP traffic to the correspondent destinations mainly via MPLS network.

2. Divert VoIP traffic to internet connection If network issues such as disconnection, packet loss, latency, and jitter occur on the MPLS link.

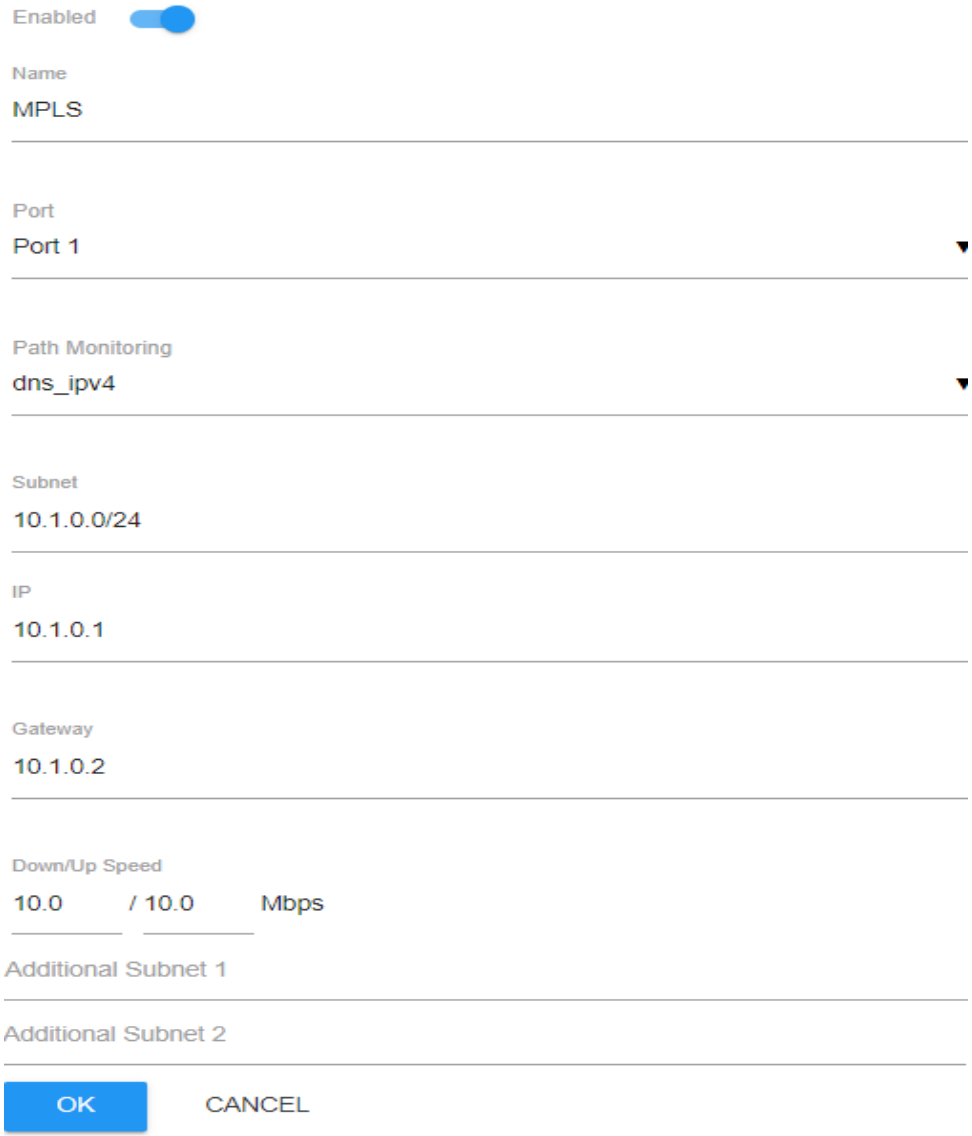
3. Failback all VoIP traffic immediately to the MPLS link as soon as the link reinstated.

Configuring Hybrid WAN on the Head Office Appliance

Follow the steps below to configure Hybrid WAN on the head office appliance with the IP details given:

1. *WAN > ADD*
2. *LAN > ADD*
3. *Tunnels > ADD*
4. *Object > DPS > ADD*
5. *Policy Routing > ADD*

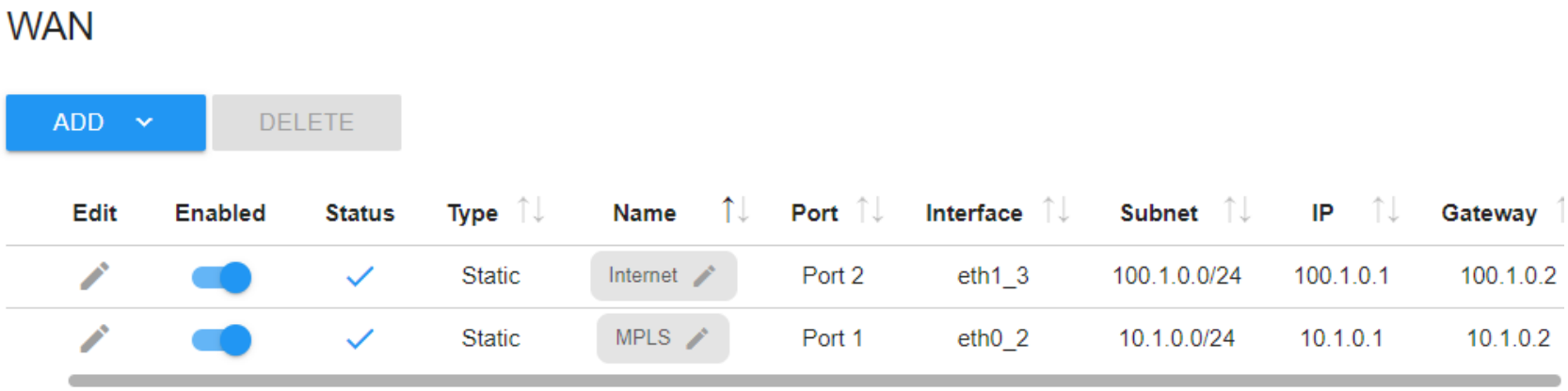
WAN > ADD > Static



WAN > ADD > Static

WAN

WAN configuration on the head office appliance is done as follows:



LAN > ADD

Enabled

Name

LAN_Head_Office

Related ISP

Auto

Port

Port 4

Subnet

10.2.1.0/24

Route

Interface Gateway

IP

10.2.1.254

DHCP

Enabled

OK CANCEL

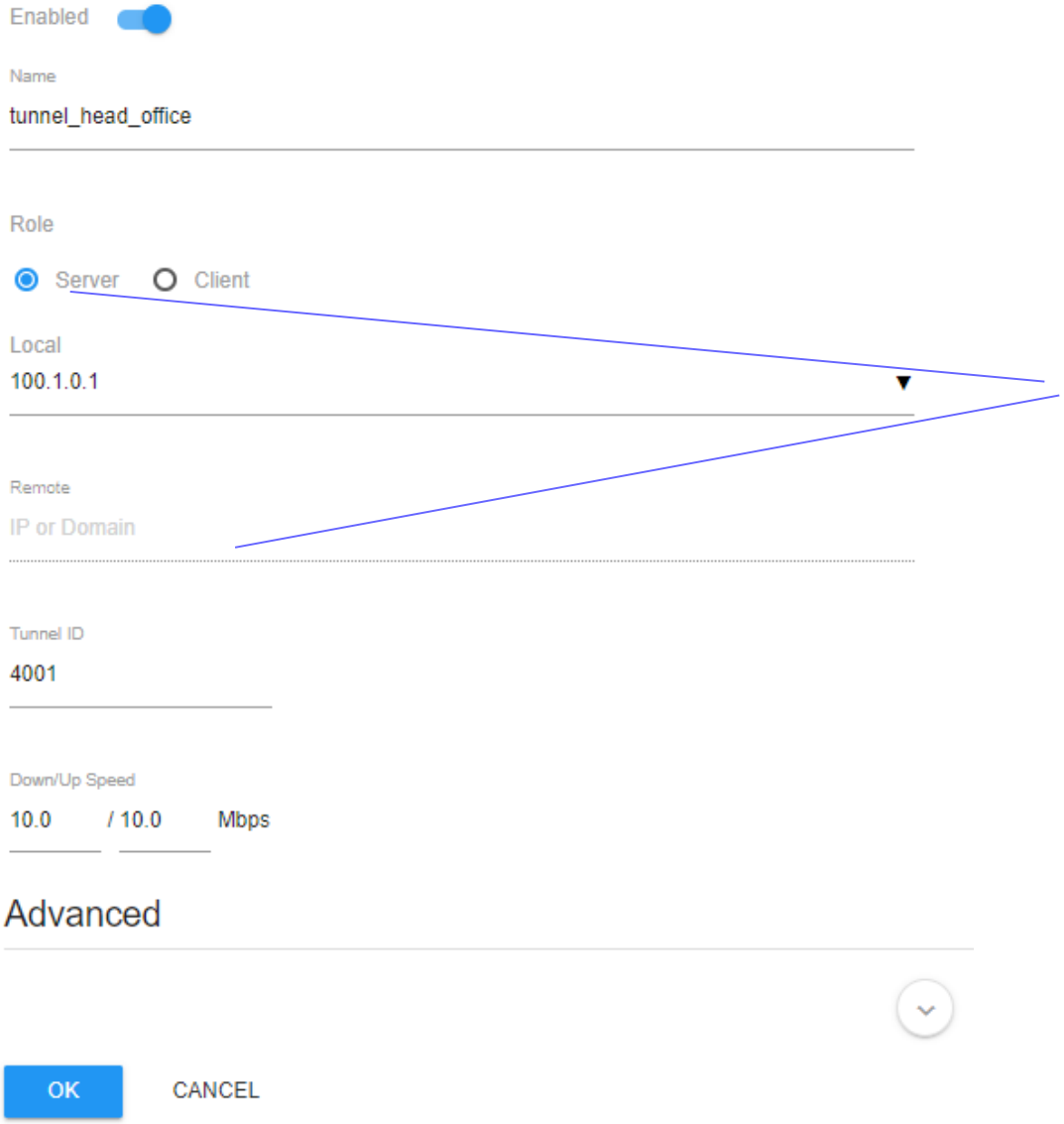
LAN

LAN configuration on the head office appliance is done as follows:

Tunnels > ADD

To set up a backup overlay connection to the MPLS link, there are two options to choose from the appliance, ***TMV*** and ***IPSec(QB2QB)***. In this case, we use ***TMV*** tunnel as a backup link to the MPLS link.

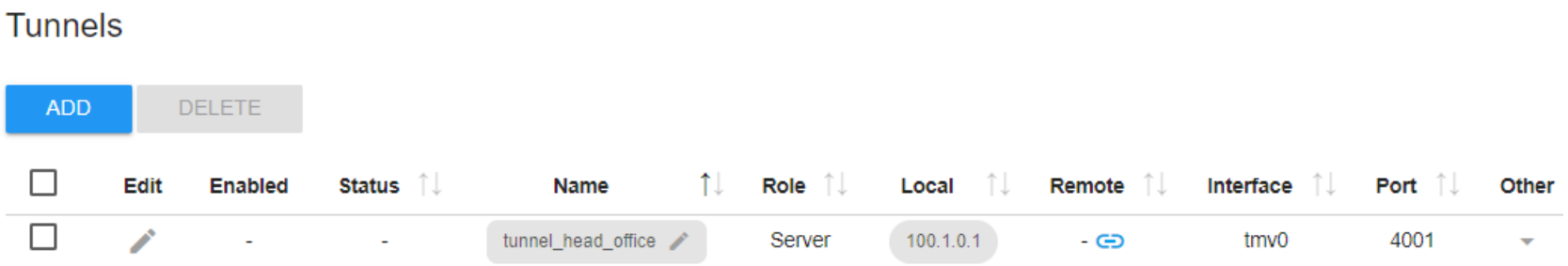
Tunnels > ADD



Skip this field when it is in server role.

Tunnels > ADD

TMV configuration on the head office appliance is done as follows:



Objects > DPS > ADD

Name

Priority_DPS

Backup Pool

None

Algorithm

Priority

Links

MPLS, tunnel_head_office

Priority

MPLS

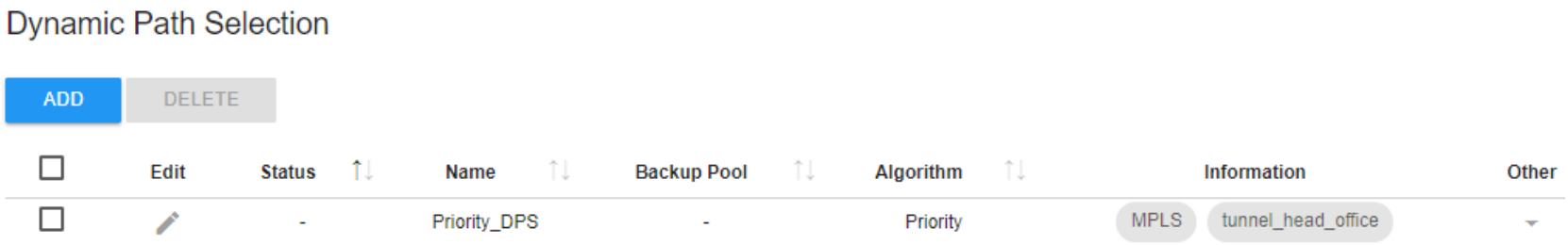
tunnel_head_office

Proxy

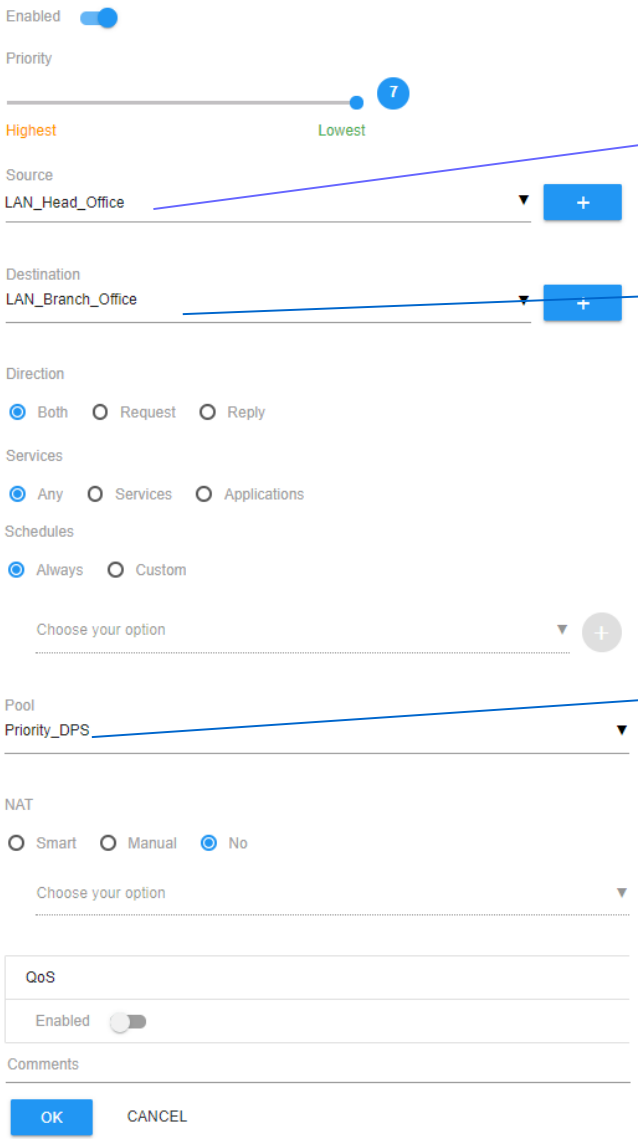
OK CANCEL

Objects > DPS

Configuration for ***DPS*** on the head office appliance is done as follows:



Policy Routing > ADD



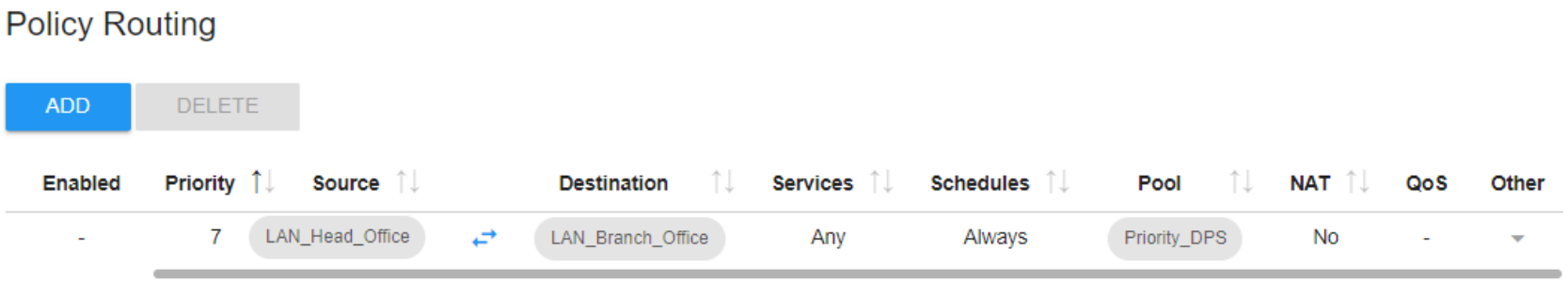
Set head office subnet here, which covers IP addresses of VoIP devices.

Set branch office subnet here, which covers IP addresses of VoIP devices.

Choose the DPS object Priority_DPS.

Policy Routing

Policy Routing for hybrid WAN configuration on the head office appliance is done as follows:

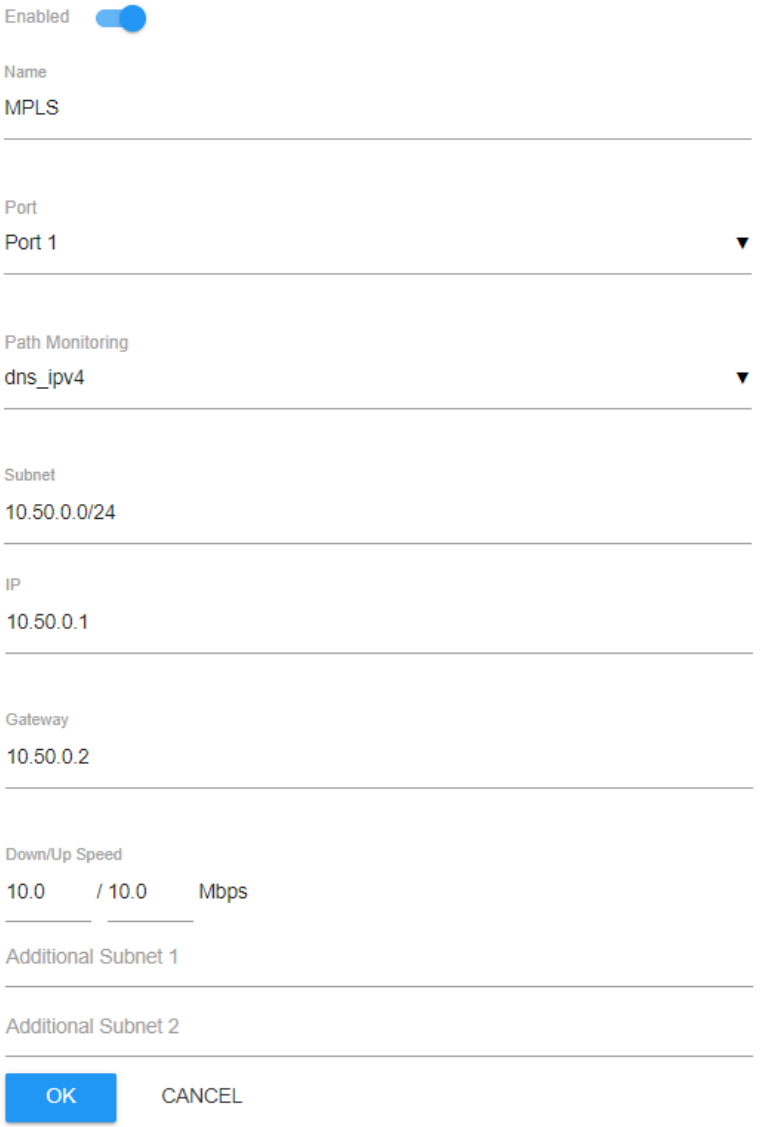


Configuring Hybrid WAN on the Branch Office Appliance

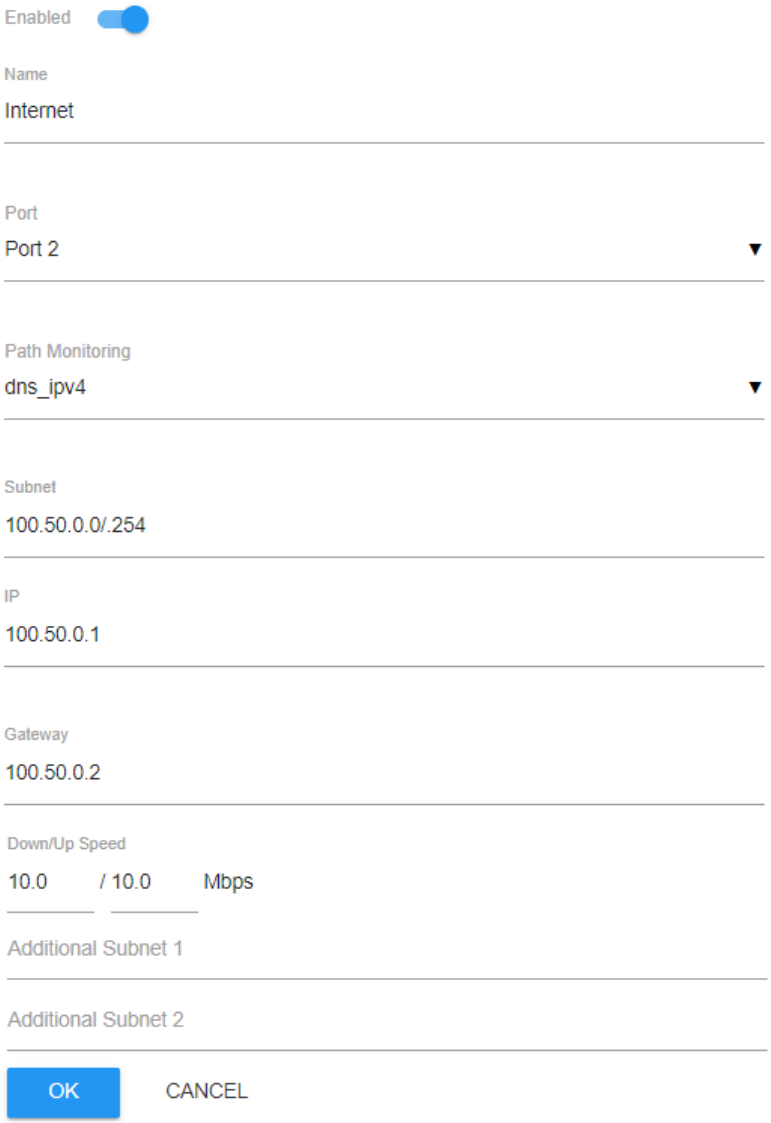
Follow the steps below to configure hybrid WAN on the branch office appliance:

1. *WAN > ADD*
2. *LAN > ADD*
3. *Tunnels > ADD*
4. *Object > DPS > ADD*
5. *Policy Routing > ADD*

WAN > ADD > Static



WAN > ADD > Static



WAN

WAN configuration on the branch appliance is done as follows:

LAN > ADD

Enabled

Name

LAN_Branch_Office

Related ISP

Auto

Port

Port 4

Subnet

10.51.0.0/24

Route

Interface Gateway

IP

10.51.0.254

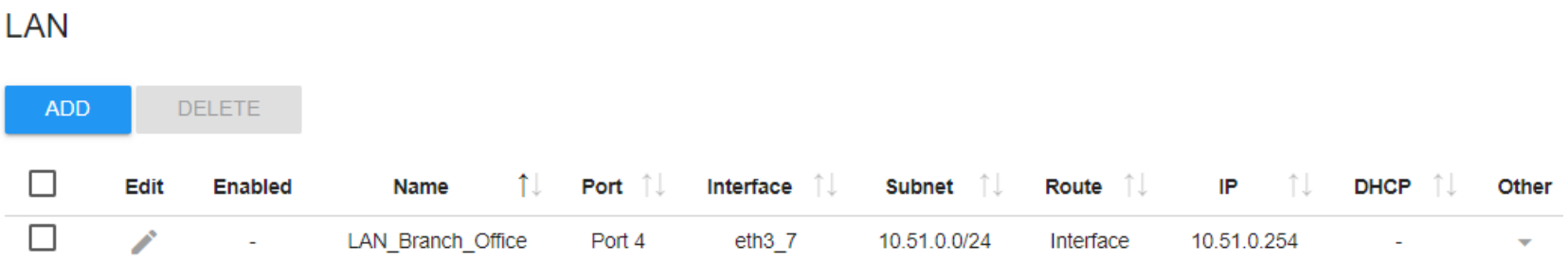
DHCP

Enabled

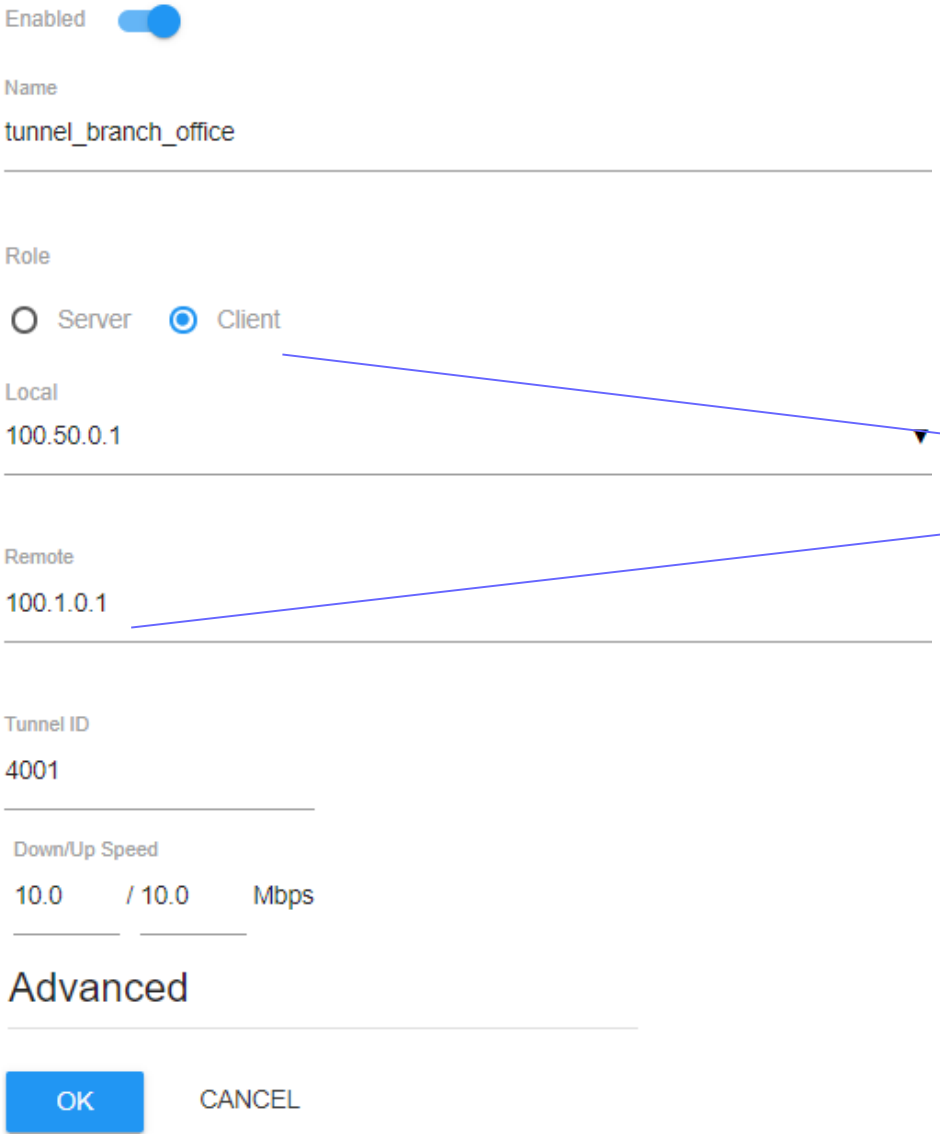
OK CANCEL

LAN

LAN configuration on the branch office appliance is done as follows:



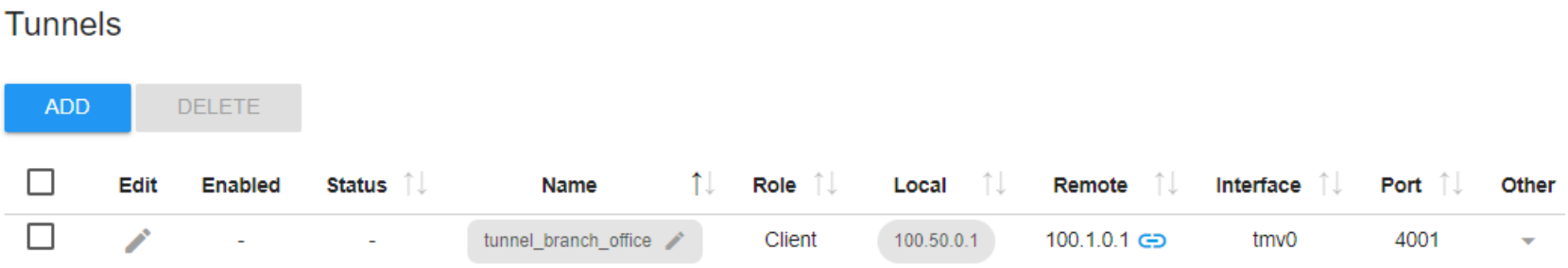
Tunnels > ADD



It is required to type in the remote IP when the tunnel is in client role.

Tunnels > ADD

TMV configuration on the branch appliance is done as follows:



Objects > DPS > ADD

Name

Priority_DPS

Backup Pool

None

Algorithm

Priority

Links

MPLS, tunnel_branch_office

Priority

MPLS

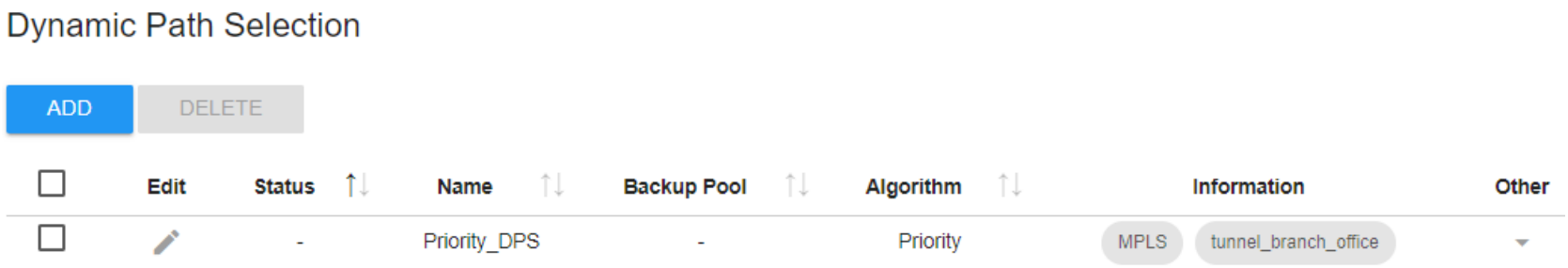
tunnel_branch_office

Proxy

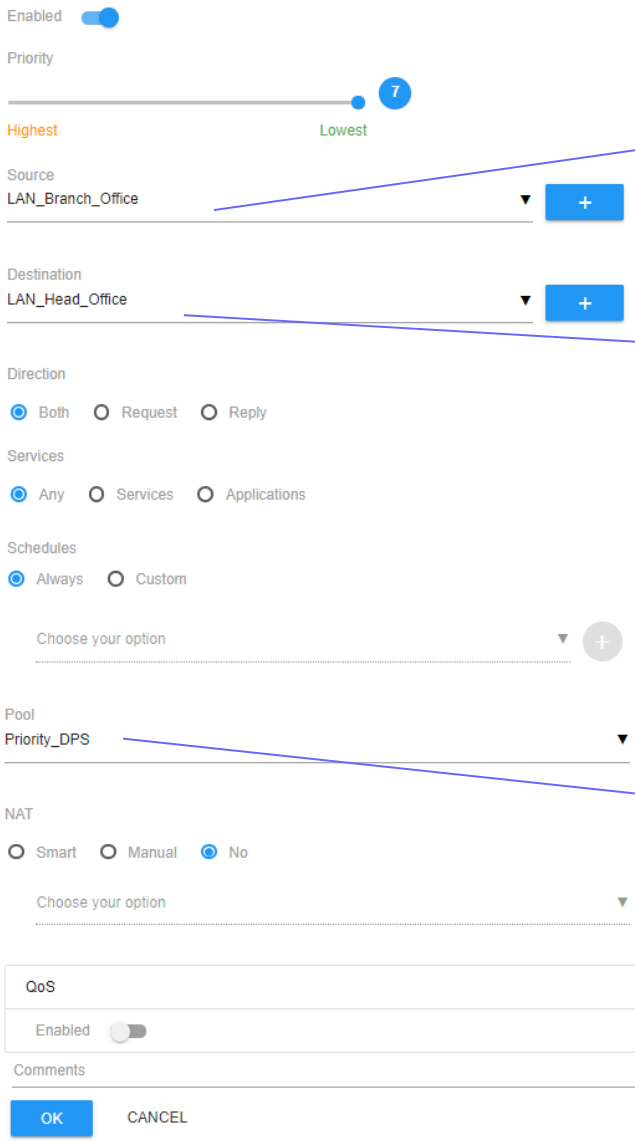
OK CANCEL

Objects > DPS

Configuration for ***DPS*** on the branch office appliance is done as follows:



Policy Routing > ADD



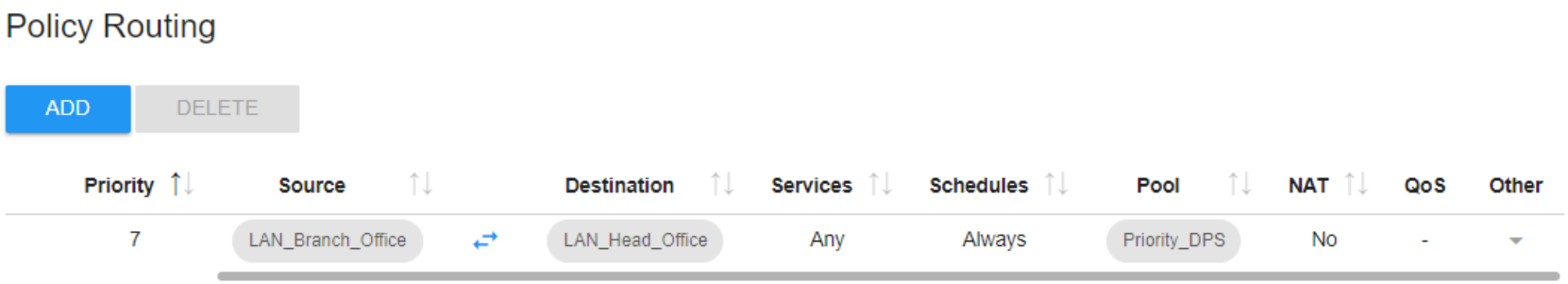
Set branch office subnet here, which covers IP addresses of VoIP devices.

Set head office subnet here, which covers IP addresses of VoIP devices.

Select the DPS object Priority_DPS.

Policy Routing

Policy Routing for hybrid WAN configuration on the branch office appliance is done as follows:



Done!

Do simple tests as follows:

1. if the devices on both ends are able to ping each other now.

2. If the devices on both ends are still able to ping each other when the MPLS link failed.