SANGFOR

NGAF

High Availability Deployed in Route Mode Guide

Version 8.0.6

Table of Contents

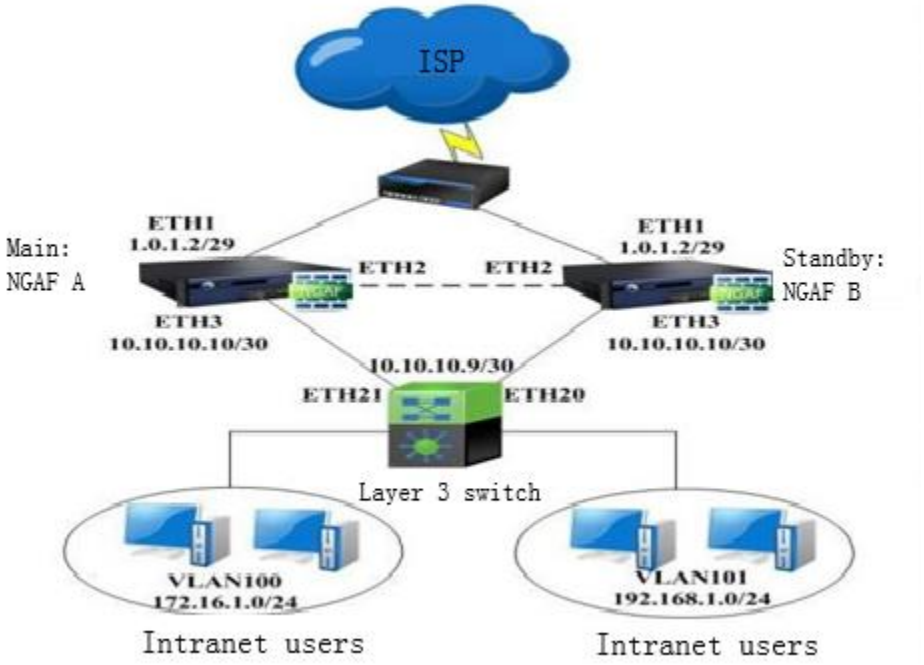
1 Functions introductions

The Internet is becoming more and more widely used in daily life, means that the stability and security of the network are becoming more and more important. Failure of a gateway device in the network may cause unpredictable losses. In order to prevent this type of failure, the high availability of the equipment is particularly important. Active – active mode is a way to achieve high availability. Two models and versions of the same NGAF can be used in parallel, connected by a heartbeat interface and keep the information and status synchronized. When a NGAF is down or the link connected to the NGAF is abnormal, it is able to assume all of its functions in a timely manner by another firewall, thus effectively ensuring customer network availability.

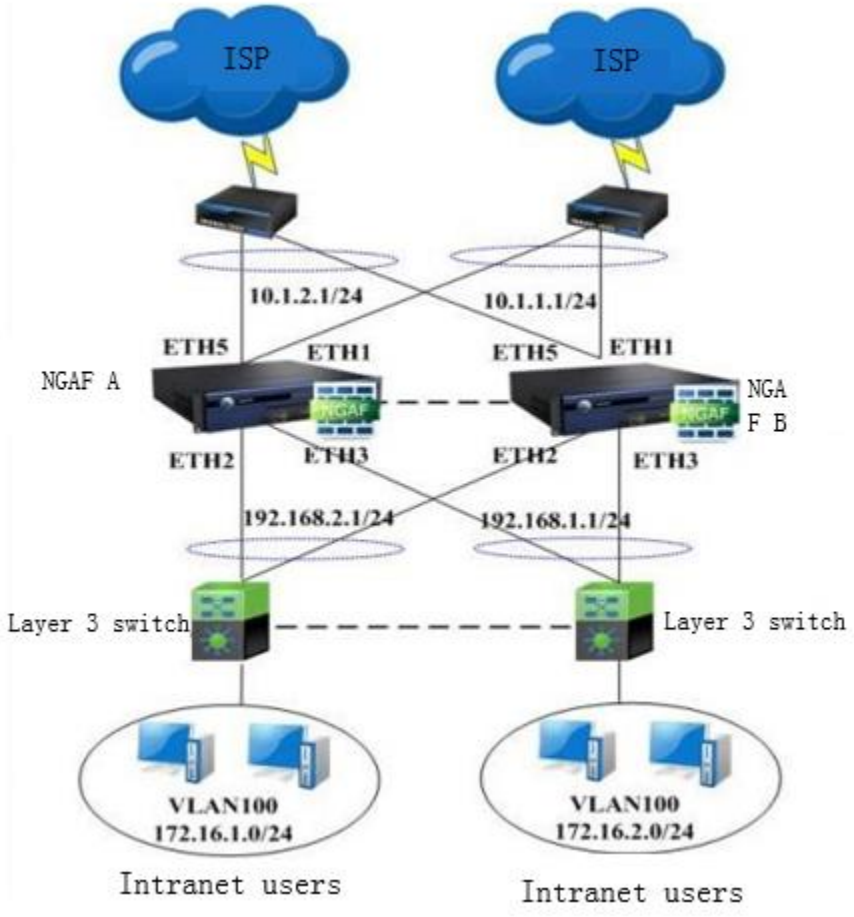
2 Application scenarios

High availability is mainly used in scenarios where the NGAF works in parallel or two devices work in parallel.

Scenario 1: Two devices, one active and one standby. As shown below:



Scenario 2: Two devices work at the same time. As shown below:



3 Description of necessary conditions

Two NGAF devices and meet the following requirements:

1. The MD5 value of the appversion file is the same.
2. The number of network ports on the device is the same (no requirement for the hardware platform).
3. Advanced Functionality license must valid.

4 Configuration ideas

1. Configure the network configuration of the active NGAF.
2. Configure the high availability of the active NGAF.
3. Configure the communication port of the standby NGAF.
4. Configure the high availability of the standby NGAF.

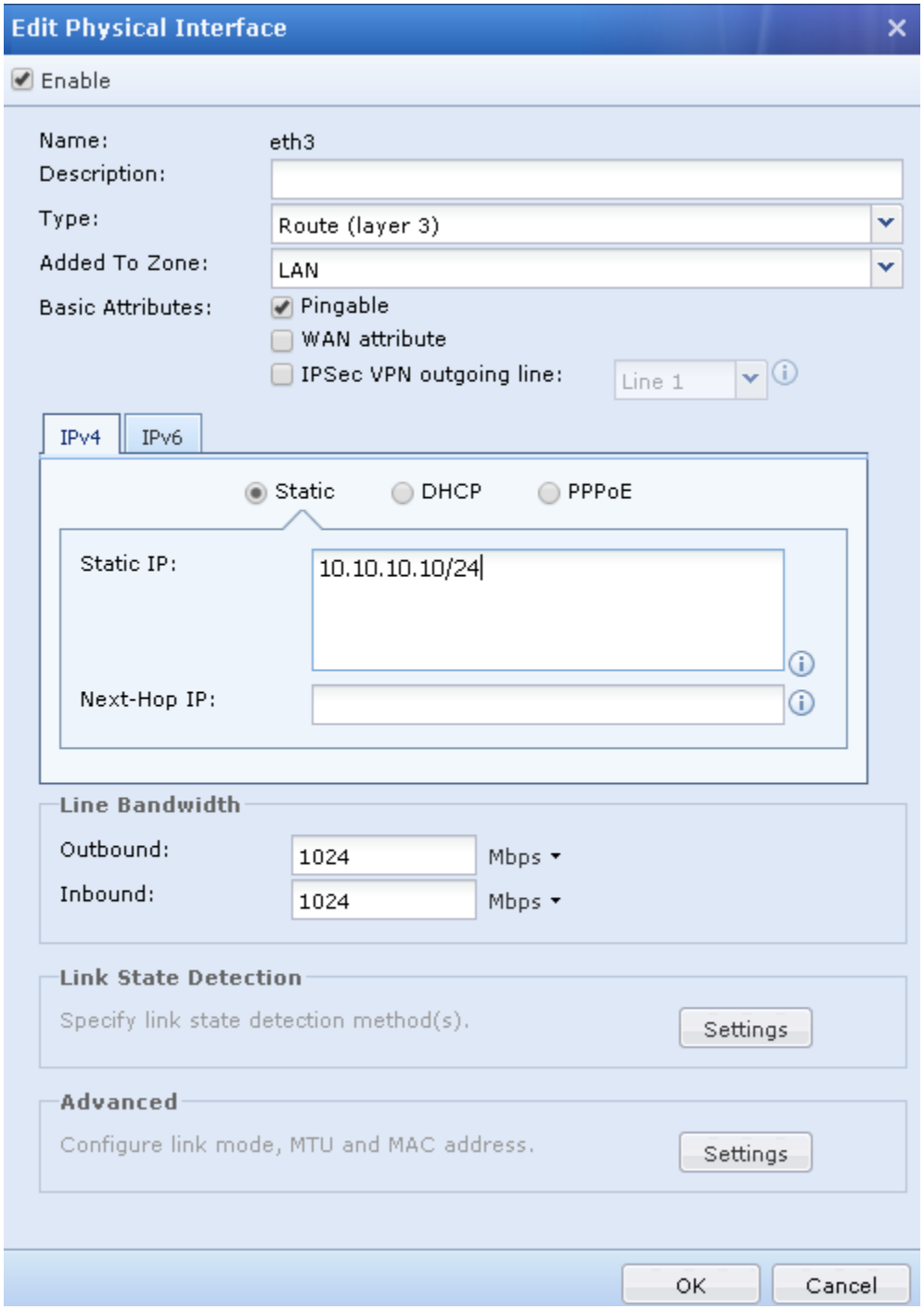
5 Configuration and screenshot

5.1 Scenario 1: Two devices, one active and one standby.

1. Configure NGAF A. Go to **Network** > **Interfaces** > **Physical interface,** configure IP address and other information.

   Eth1, port defined as WAN network area as figure below:

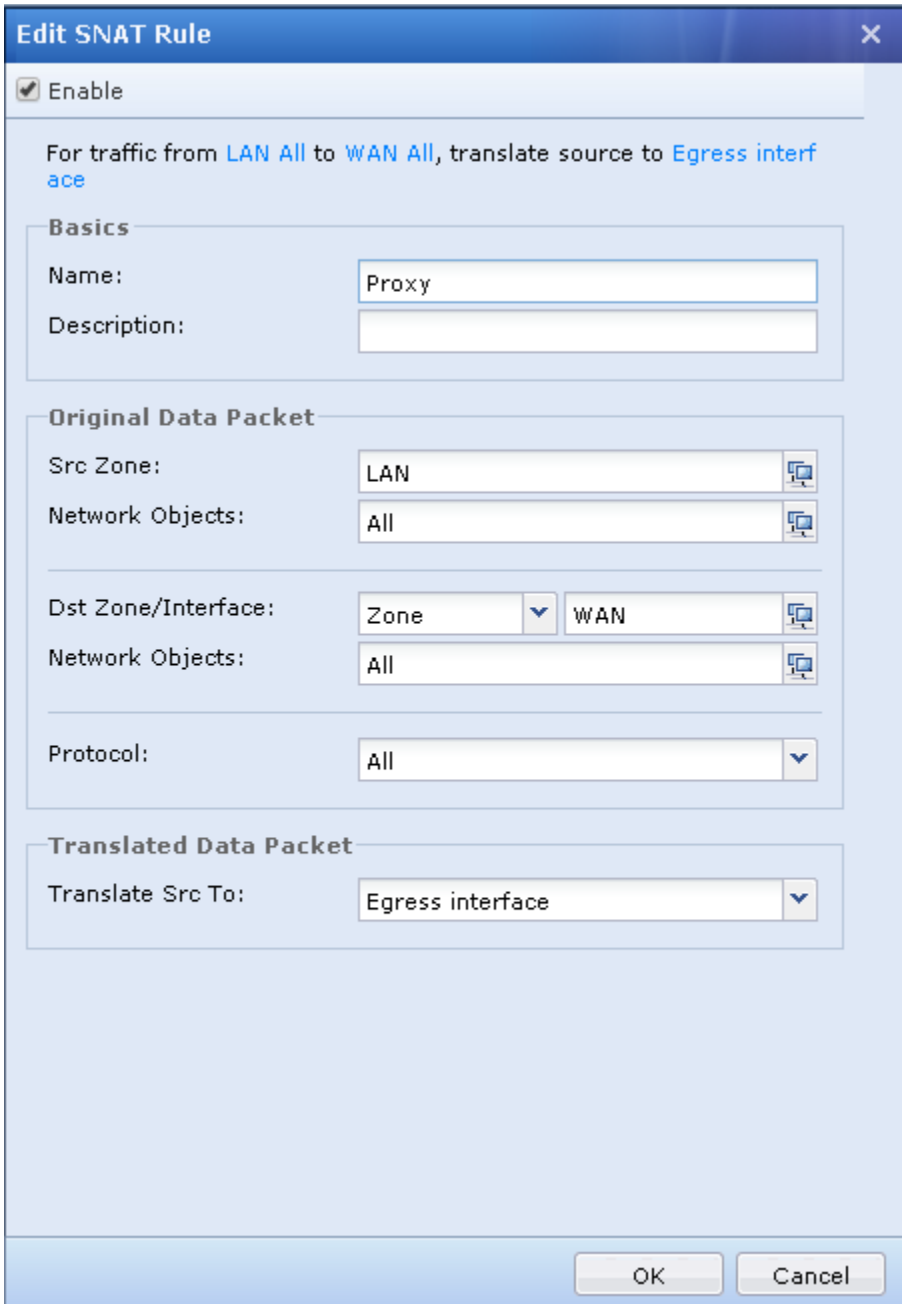
Eth3, port defined as LAN network area as figure below:



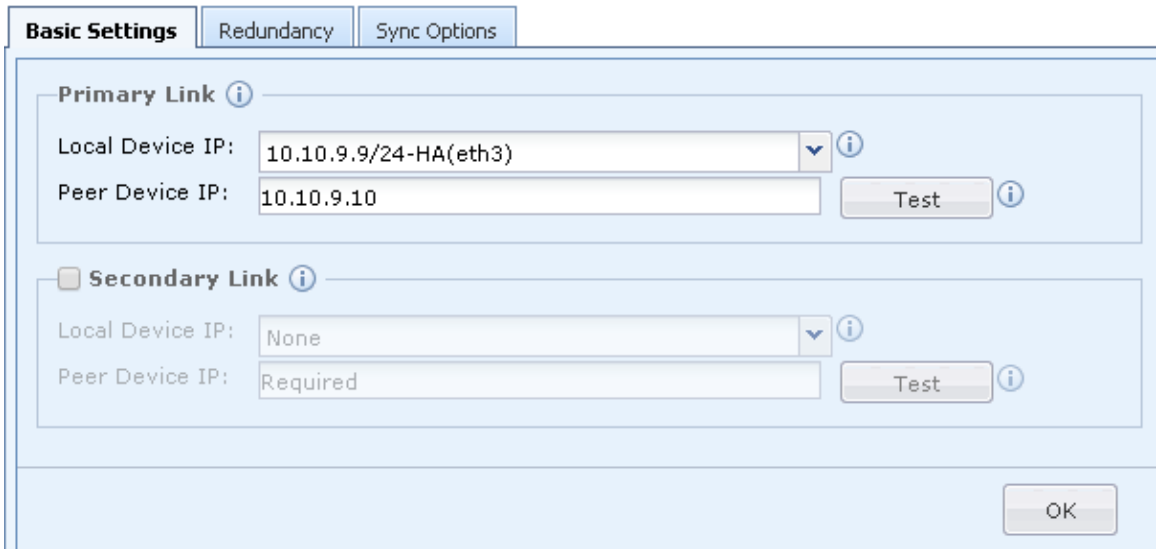
Eth2, port defined as HA port as figure below:


Edit Physical Interface
Enable
Name:
eth2
Description:
Type:
Route (layer 3)
Added To Zone:
Select zone
Basic Attributes:
Pingable
WAN attribute
IPSec VPN outgoing line:
Line 1
IPv4
IPv6
Static
DHCP
PPPoE
Static IP:
10.10.9.9/29-HA
Next-Hop IP:
Line Bandwidth
Outbound:
1024
Mbps
Inbound:
1024
Mbps
Link State Detection
Specify link state detection method(s).
Settings
Advanced
Configure link mode, MTU and MAC address.
Settings
OK
Cancel

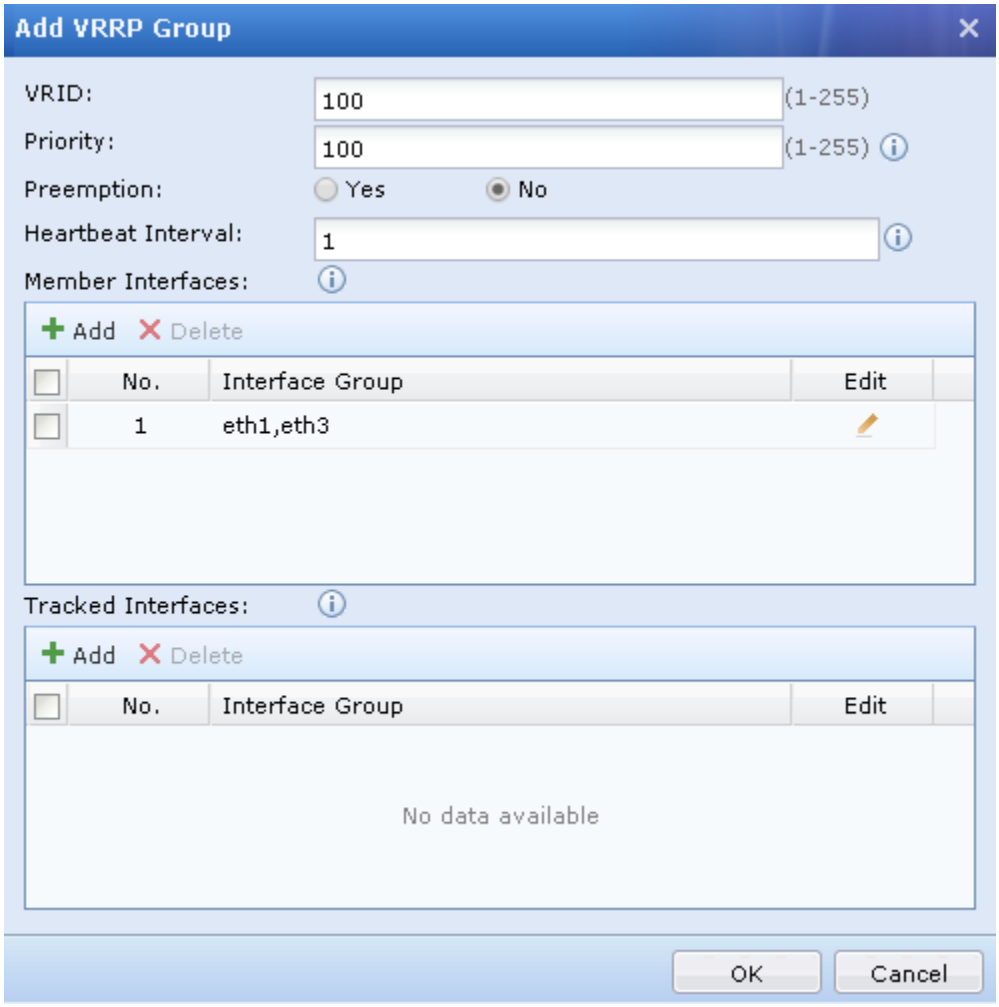
2. NGAF A: Go to **Policies** > **NAT** > **Add**, configure SNAT as figure below:



3. NGAF A. Go to **System** > **High Availability** > **Basic Settings,** select local eth2 as communication port. Fill in the peer address 10.10.9.10 as figure below:

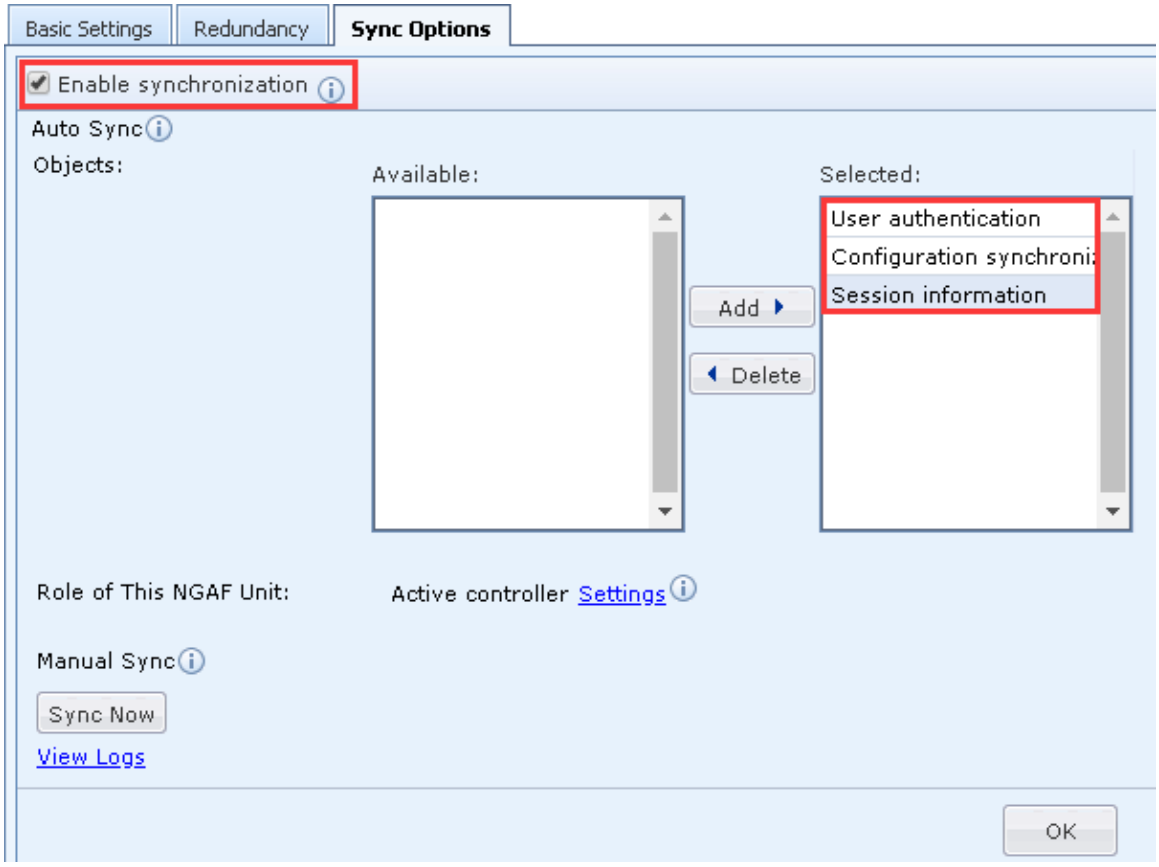


4. NGAF A. Go to **System** > **High Availability** > **Redundancy** > **Add,** configure the VRID as 100 and priority as 100 and click **No** on preemption. Member interface as eth1 and eth3 as figure below:



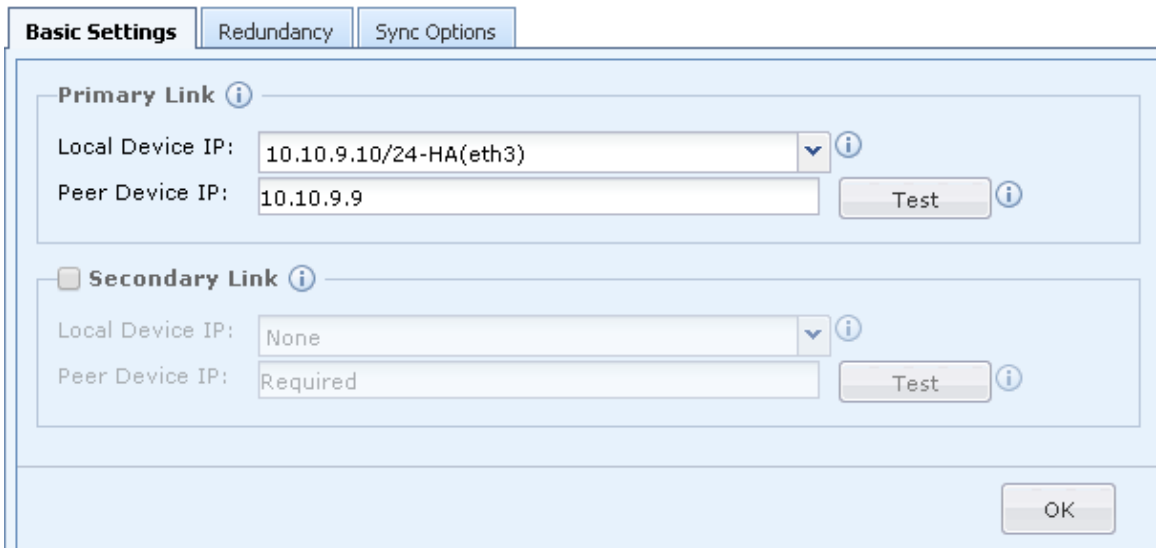
Note: In route mode, if link state detection is set, the active/standby switchover conditions are three: do not receive heartbeat packet, physical interface in DOWN status, link state detection detected link failure. The active/standby switchover is performed when any of the above condition is met.

5. NGAF A. Go to **System** > **High Availability** > **Sync Options**, enable synchronization and choose 3 object as figure below:

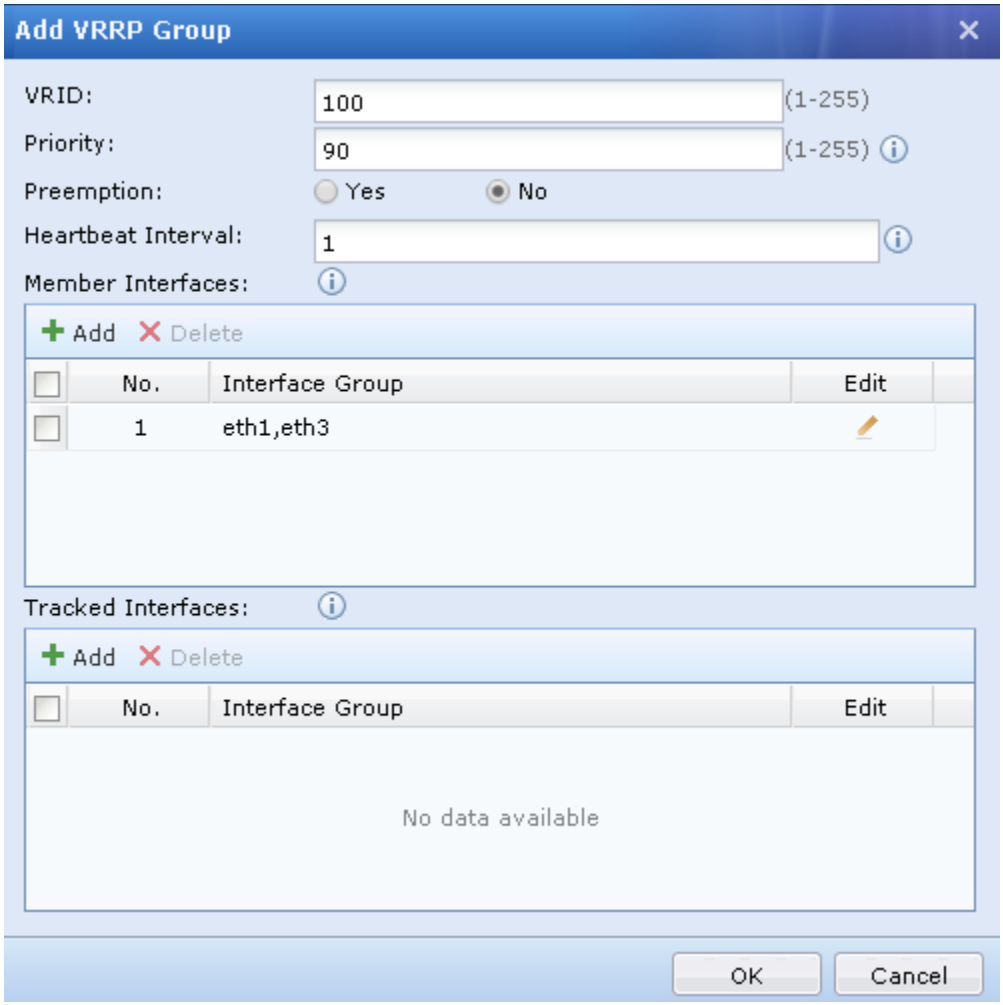


6. Configure NGAF B. Go to **Network** > **Interfaces** > **Physical interface**, configure eth2 interface IP and other information as figure below:

7. NGAF B. Go to **System** > **High Availability** > **Basic Settings**, configure local device IP of eth2 and peer device IP which is 10.10.9.9 as figure below:

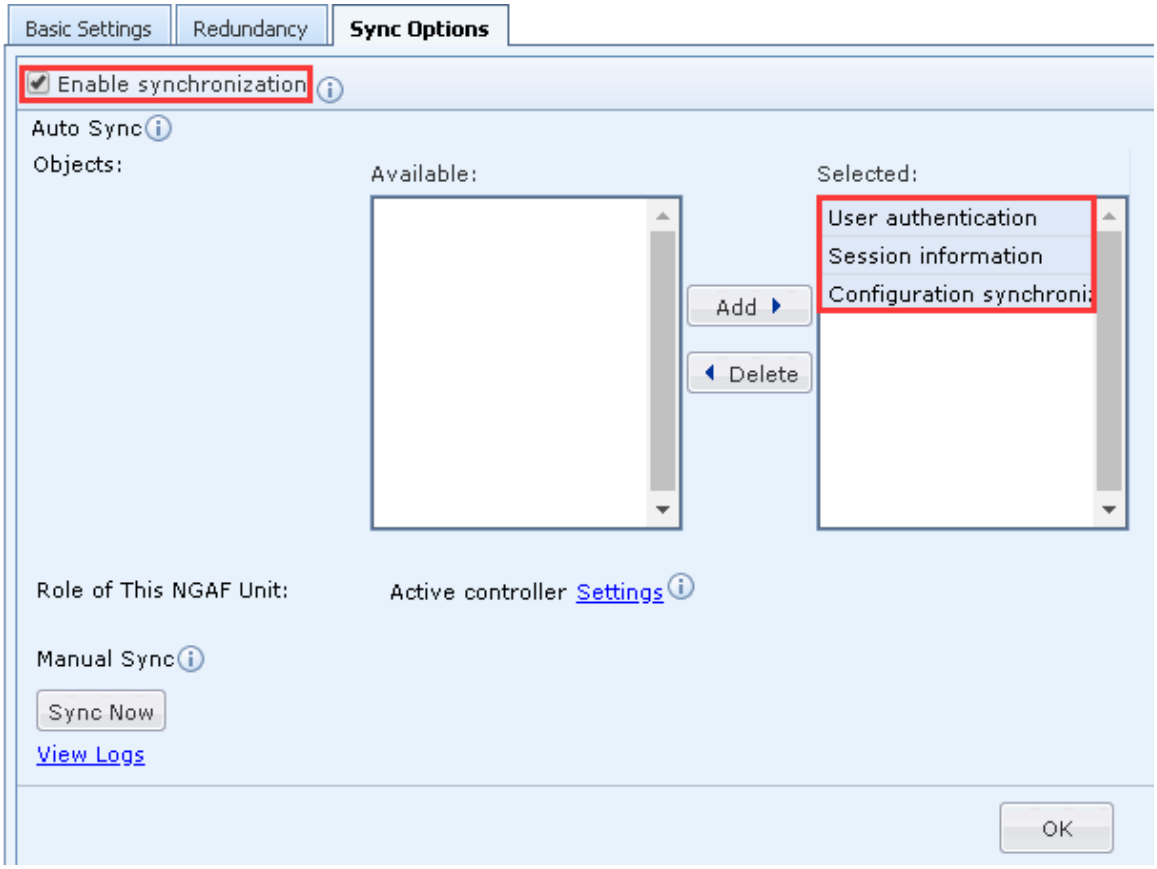


8. NGAF B. Go to **System** > **High Availability** > **Redundancy,** configure the VRID to 100 which same with peer device, then priority set to 90. Click **NO** on preemption and member interface same with peer device as figure below:



Note: In route mode, if link state detection is set, the active/standby switchover conditions are three: do not receive heartbeat packet, physical interface in DOWN status, link state detection detected link failure. The active/standby switchover is performed when any of the above condition is met.

9. NGAF B. Go to **System** > **High Availability** > **Sync Options,** enable the synchronization and select 3 objects as figure below:

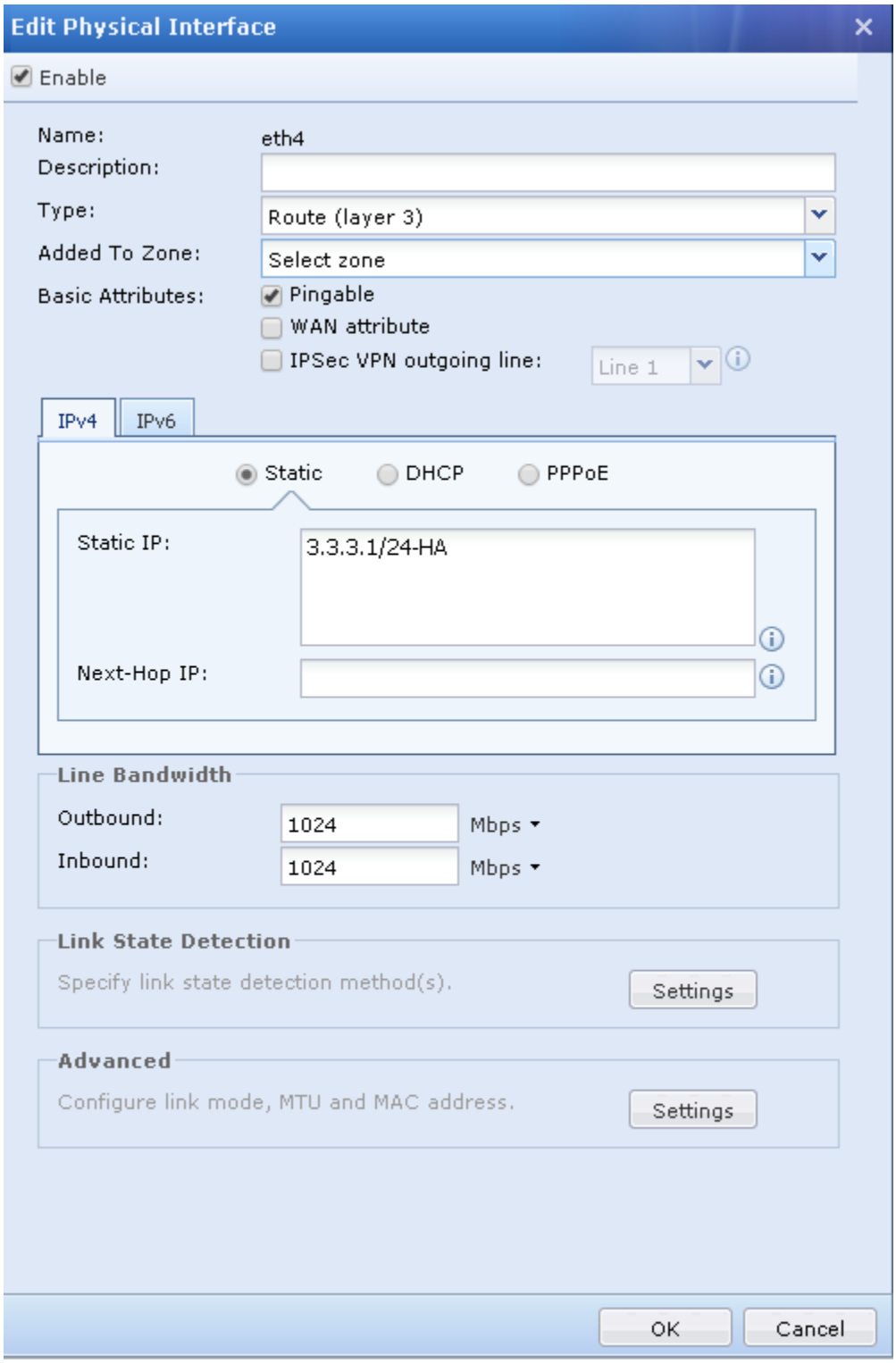


10. Power off NGAF A and NGAF B after configuration has been done, then connect all the cables. Power on the NGAF A first, after NGAF already power on then only power on NGAF B. Once NGAF B is power on, NGAF A will synchronize configuration to NGAF B.

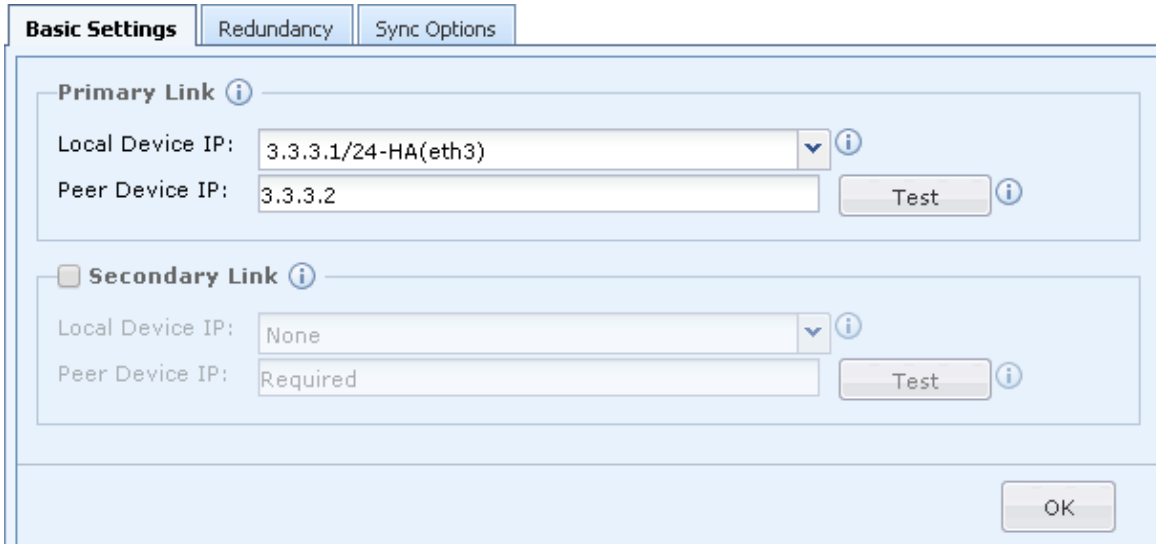
Note: The boot sequence cannot be reversed.

5.2 Scenario 2: Two devices work at the same time.

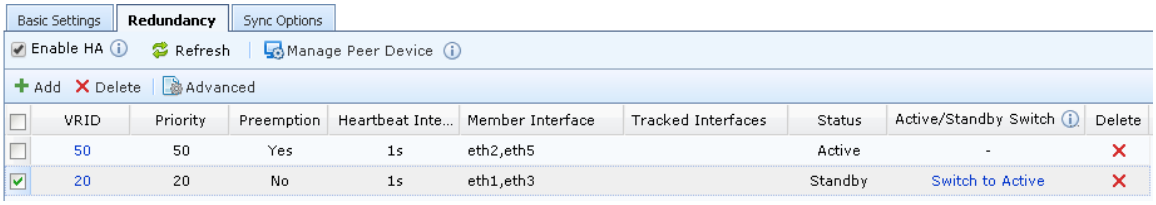
1. NGAF A. First configure interface IP and other information, SNAT, packet return routing and policy-based route. Mainly here is eth3.



2. NGAF A. Go to **System** > **High Availability** > **Basic Settings,** configure local eth4 as local device IP and fill in the peer device IP correctly. This setting is mainly for two NGAF to synchronize configuration and negotiate VRRP usage, configure as figure below:

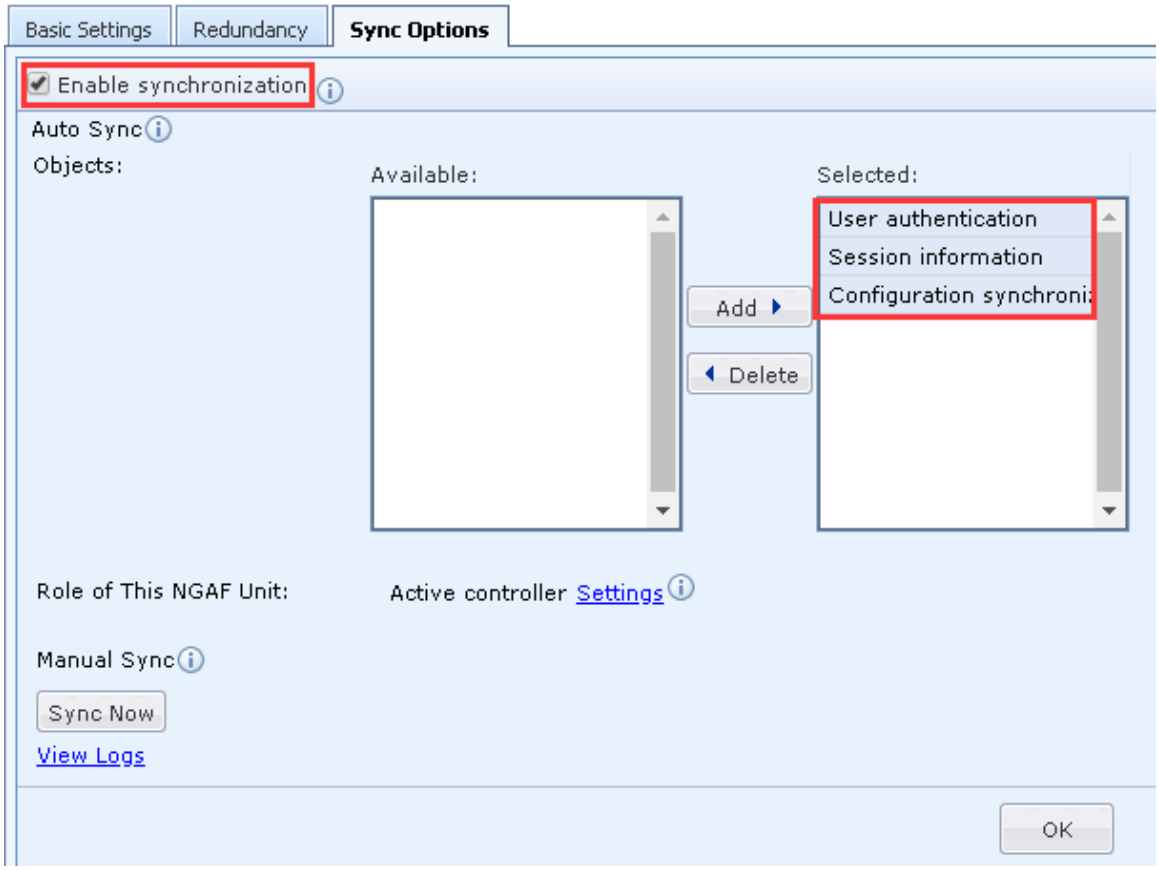


3. NGAF A. Go to **System** > **High Availability** > **Redundancy,** configure eth2 and eth 5 as member interface, VRID set to 50 and priority set to 50 and click Yes on preemption. Configure another redundancy, choose eth 1 and eth3 for member interface, VRID and priority set to 20 and click No on preemption as figure below:

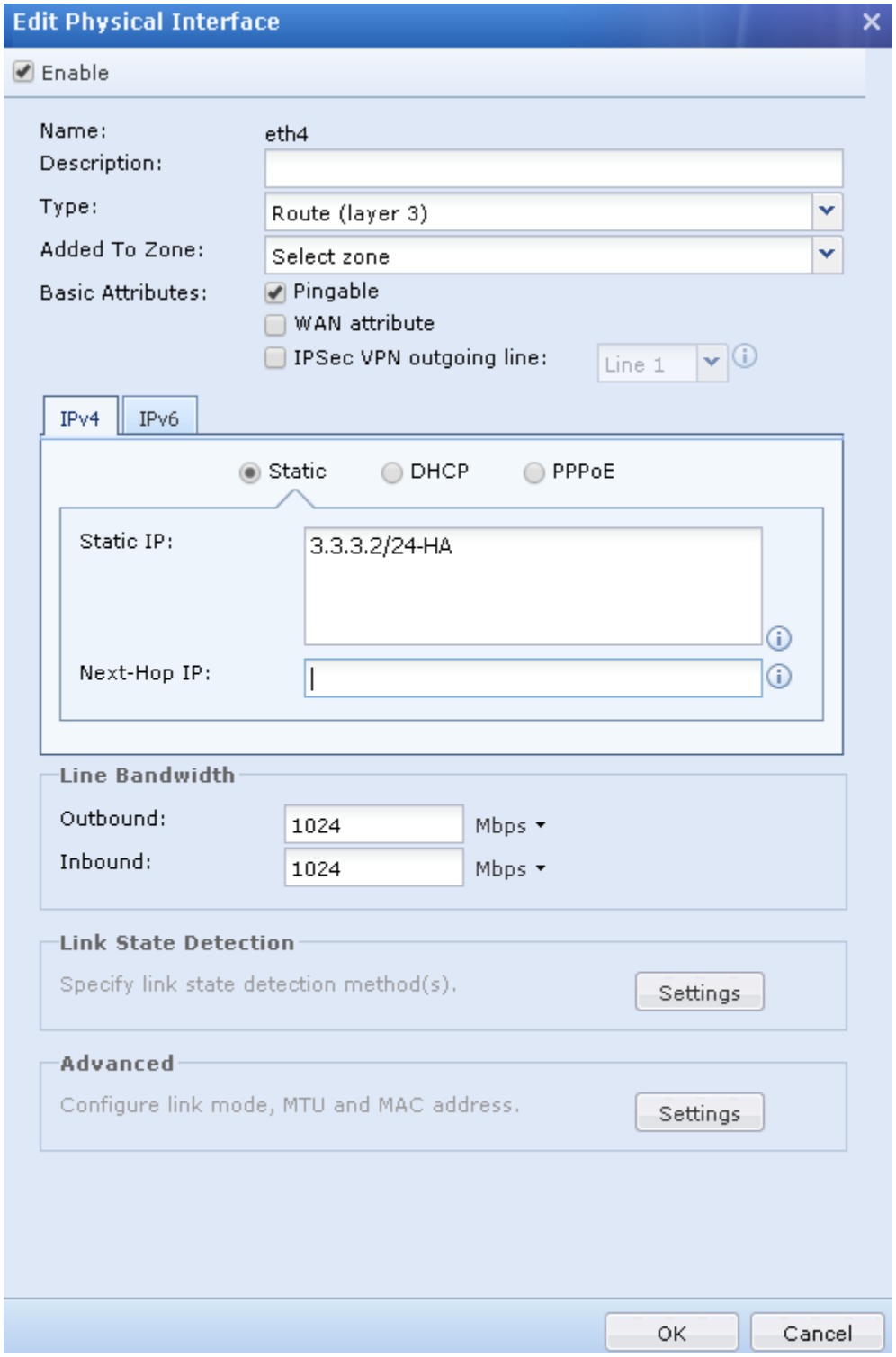


Note: In route mode, if link state detection is set, the active/standby switchover conditions are three: do not receive heartbeat packet, physical interface in DOWN status, link state detection detected link failure. The active/standby switchover is performed when any of the above condition is met.

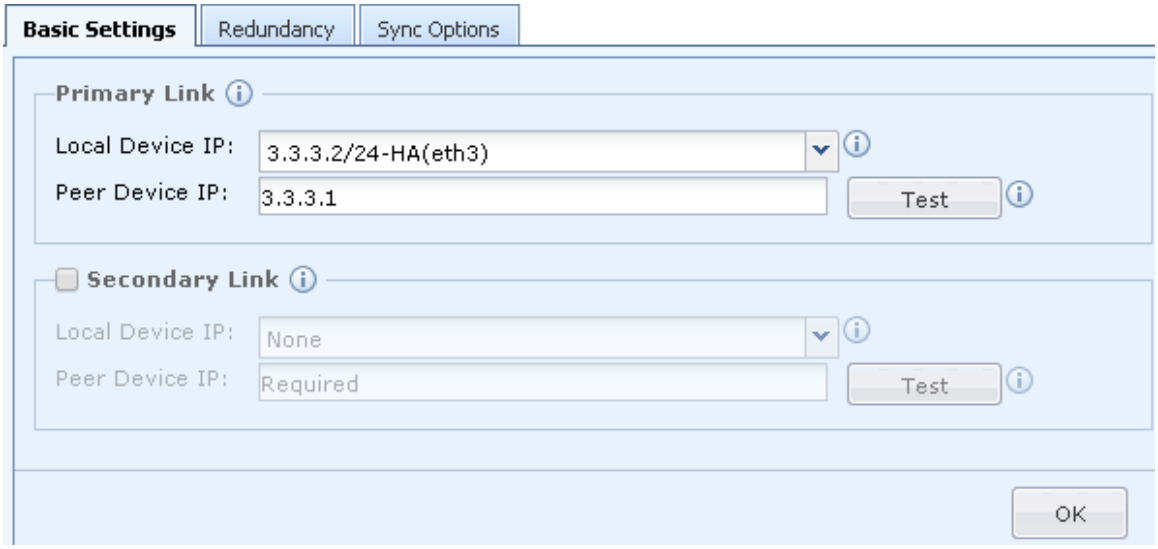
4. NGAF A. Go to **System** > **High Availability** > **Sync Options**, enable synchronization and select 3 objects as figure below:



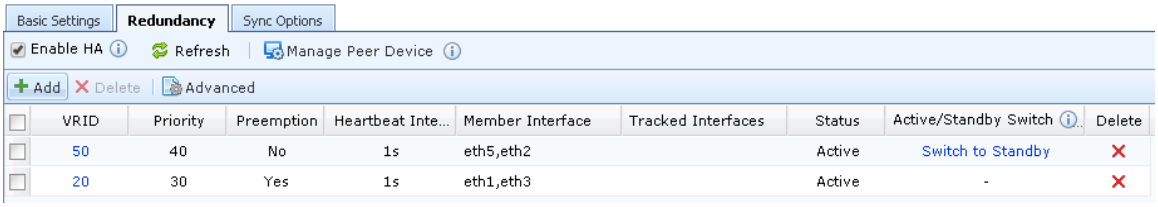
5. NGAF B. Go to **Network** > **Interfaces** > **Physical Interface,** configure IP and other information for eth4 as figure below:



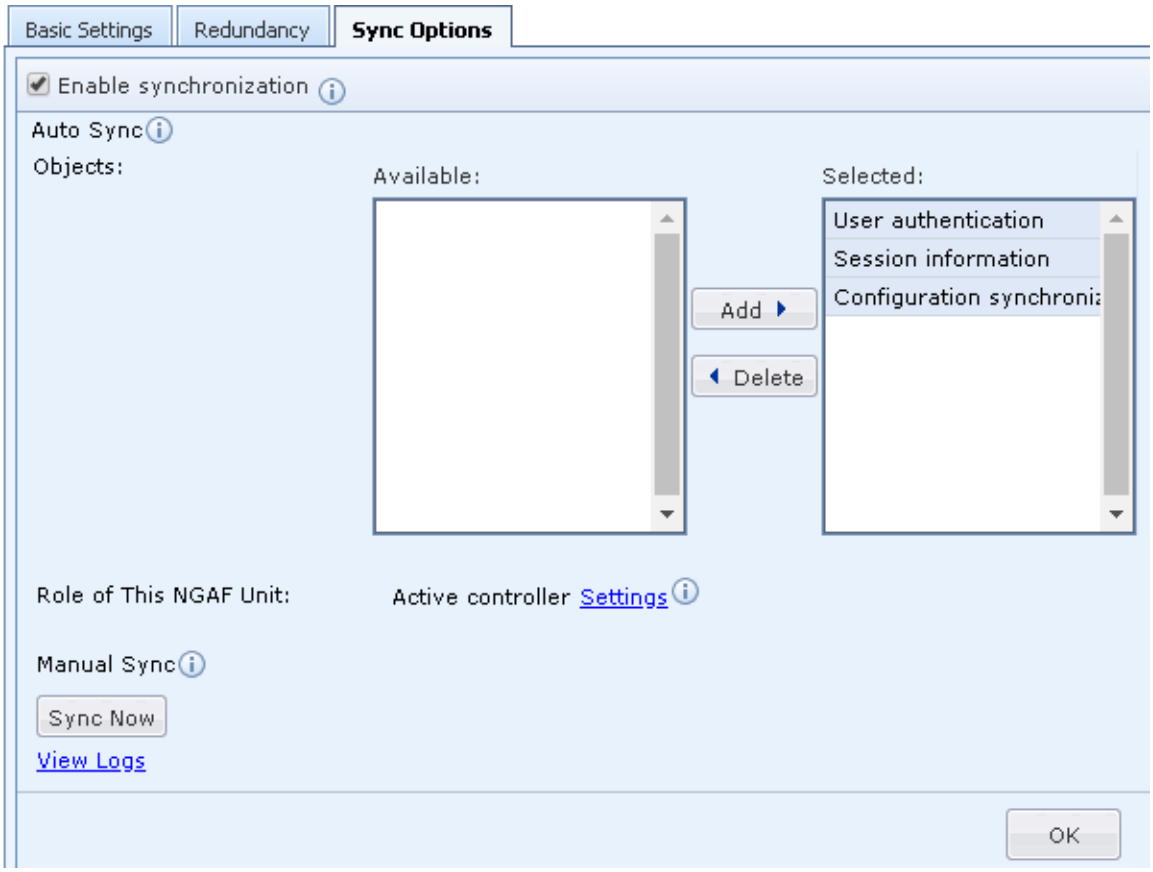
6. NGAF B. Go to **System > High Availability > Basic Settings,** configure eth4 as local device IP and fill the peer device IP correctly. This setting is mainly for two NGAF to synchronize configuration and negotiate VRRP usage, configure as figure below:



7. NGAF B. Go to **System > High Availability > Redundancy,** select eth5 and eth2 as member interface, VRID set to 50 and priority set to40 and click No on preemption. Select eth1 and eth3 as member interface, VRID set to 20 and priority set to 30 and click Yes on preemption as figure below:



8. NGAF B. Go to **System > High Availability > Sync Options** enable synchronization and select 3 objects as figure below:



9. Power off NGAF A and NGAF B, then connect all cables. Power on NGAF first, after the NGAF A is power on then only power on NGAF B. Once NGAF B is power on, NGAF A will synchronize configuration to NGAF B.

Note: The boot sequence cannot be reversed.

6 Precautions

1. Active device's member interface must be configure to be consistent, HA interface recommended to configure as consistent. Support dual-machine switching.
2. If the VRID and priority level is the same, even we enable preemption but it also will not preempt.
3. If the signature database license of device A has not expired, the signature database license of the device B rule base expires. After device A upgrades the rule base, the synchronization of the rule base of device A to the peer end fails, but does not affect the synchronization of other configurations.
4. The configuration synchronization will not synchronize the IP address information with the HA interface and the [High Availability] configuration.
5. In order to prevent the configuration of the standby device from being synchronized to the active device, the configuration of the active device is lost. It is recommended that only make configuration changes on the active device, at the same time device A is enabled the user authentication, session information and configuration synchronization are synchronized. Device B only enabled user authentication and session information.
6. Configuration synchronization support the configuration in the IPv6 network environment; session information synchronization does not support the synchronization of IPv6 sessions. After the active/standby switchover, the IPv6 service needs to be reconnected.
7. The core switch used the SVI uplink interface to do VRRP and use the track ping detection as a switching condition.
8. Preemption and link state detection cannot be enabled at the same time.
9. Do not use the bypass interface to do dual-machine in order to avoid broadcast storm.
10. There are two types of configuration synchronization: batch synchronization and incremental synchronization. After the device is power on, a configuration synchronization request is sent to the peer. It is request to synchronize the configuration of the peer device to the local device, and batch synchronization will be performed at this time. After the batch synchronization is complete, the device will check the configuration in every 10 seconds to check whether have any configuration changed. If the change is made, the configuration modified by the local device is synchronized to the peer device, and incremental synchronization is performed at this time.

SANGFOR