



Sangfor NSF V8.0.85 Professional

High Availability





1 Basic Elements of High Availability

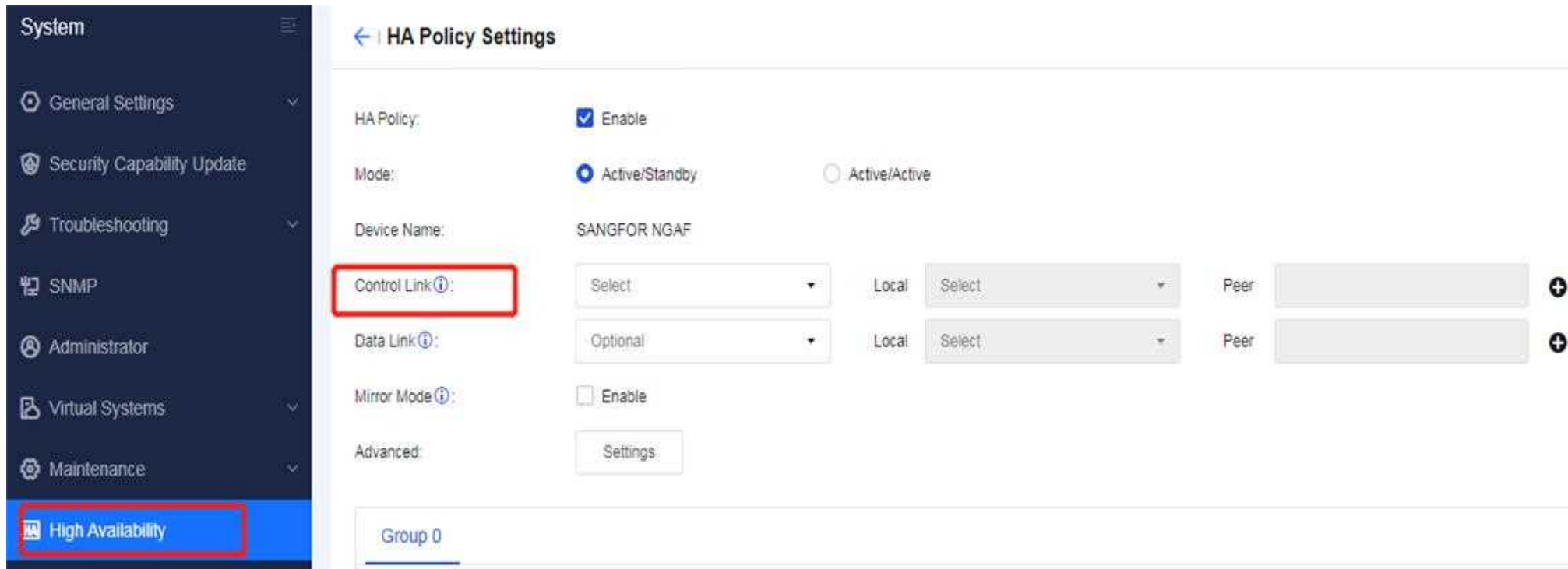
2 Types of High Availability

3 Case Study of High Availability

PART 1

Basic Elements of High Availability

The control link is in charge for synchronizing heartbeat packets, which include configuration and status information. Both remote and local sides have to appoint the same interface for control link interface. Control link is a mandatory setting which cannot be ignored.



System

- General Settings
- Security Capability Update
- Troubleshooting
- SNMP
- Administrator
- Virtual Systems
- Maintenance
- High Availability**

HA Policy Settings

HA Policy: ☒ Enable

Mode: ☒ Active/Standby ☐ Active/Active

Device Name: SANGFOR NGAF

Control Link ⓘ: Select Local Select Peer +

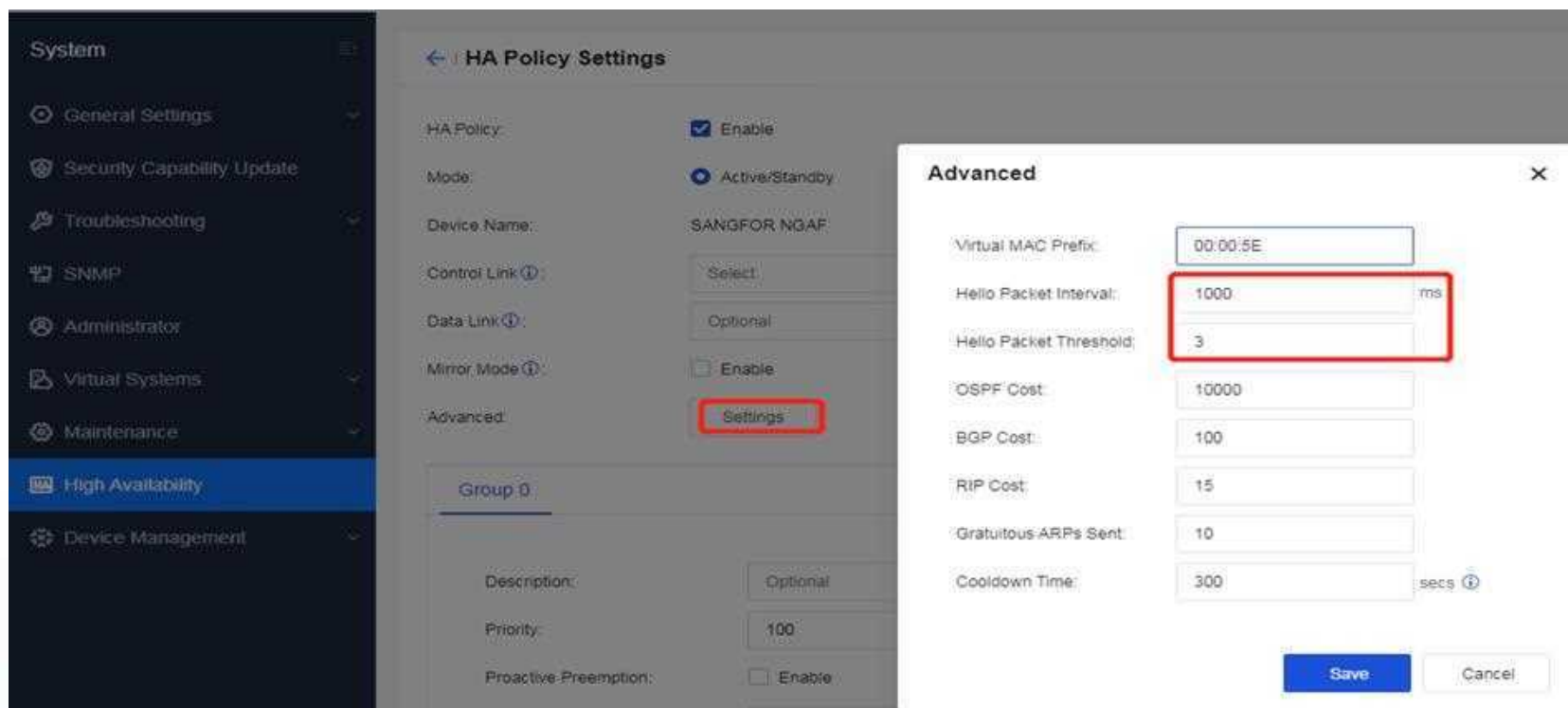
Data Link ⓘ: Optional Local Select Peer +

Mirror Mode ⓘ: ☐ Enable

Advanced: Settings

Group 0

By default, a hello message is sent every 1000 ms. If more than 3 consecutive hello messages are not received by the other side, it is considered that the remote NSF has encountered a failure. Users can modify default settings in the advanced settings page.



Data link is in charge for synchronizing sessions, which is an optional setting. If you don't configure data link, control link will take over for synchronizing sessions. If data link is configured, it will represent control link for synchronizing heart-beats packets, only as control link fails.

[←](#) | HA Policy Settings

HA Policy:

☒ Enable

Mode:

☒ Active/Standby ☐ Active/Active

Device Name:

SANGFOR Network Secure

Control Link ⓘ:

Select ▼

Local

Select ▼

Peer

+

Data Link ⓘ:

eth1 ▼

Local

192.168.1.2 ▼

Peer

+

ⓘ The data sync interfaces of the active and standby devices must be consistent. Otherwise, synchronization error may occur.

×

Mirror Mode ⓘ:

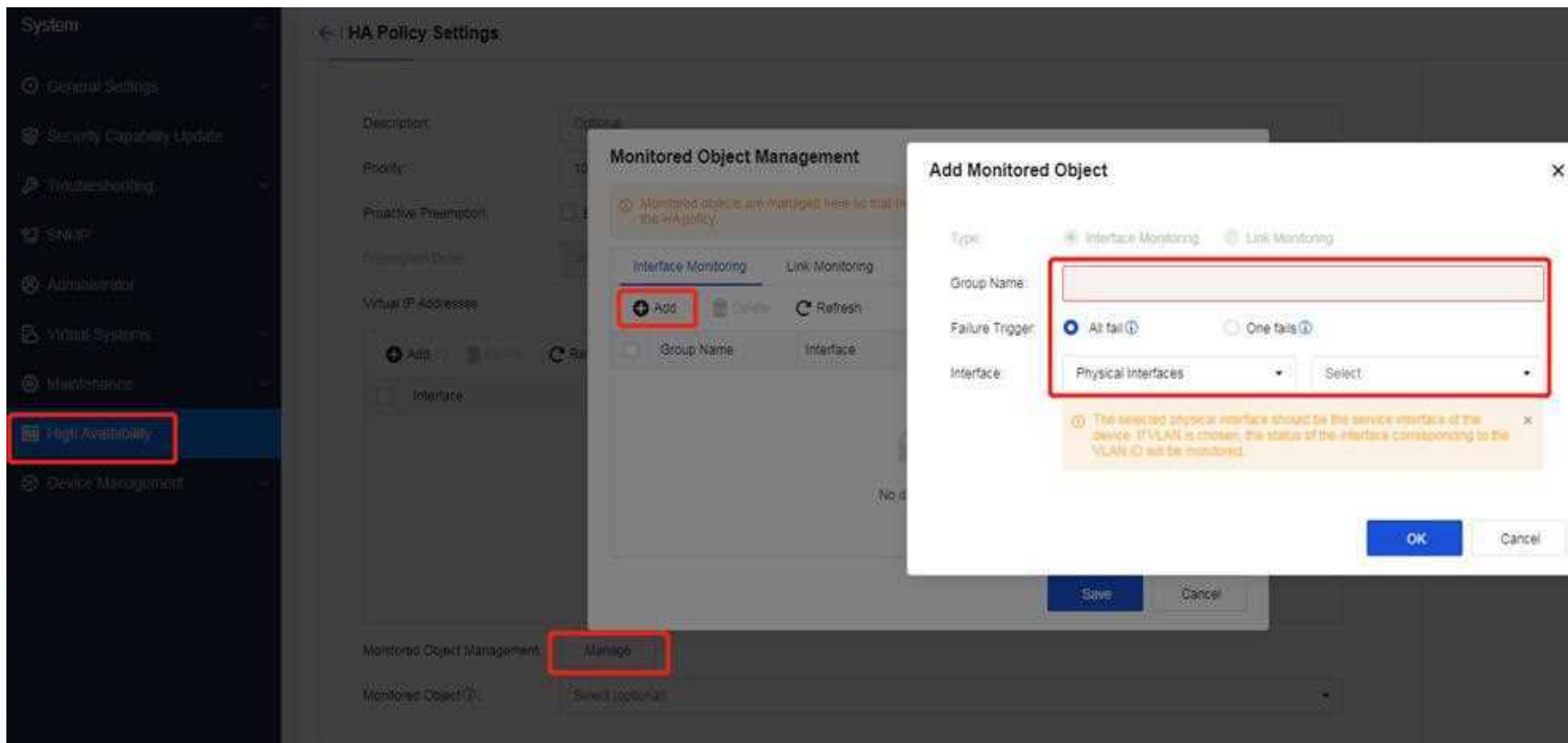
☐ Enable

Advanced:

Settings

Interface Monitoring

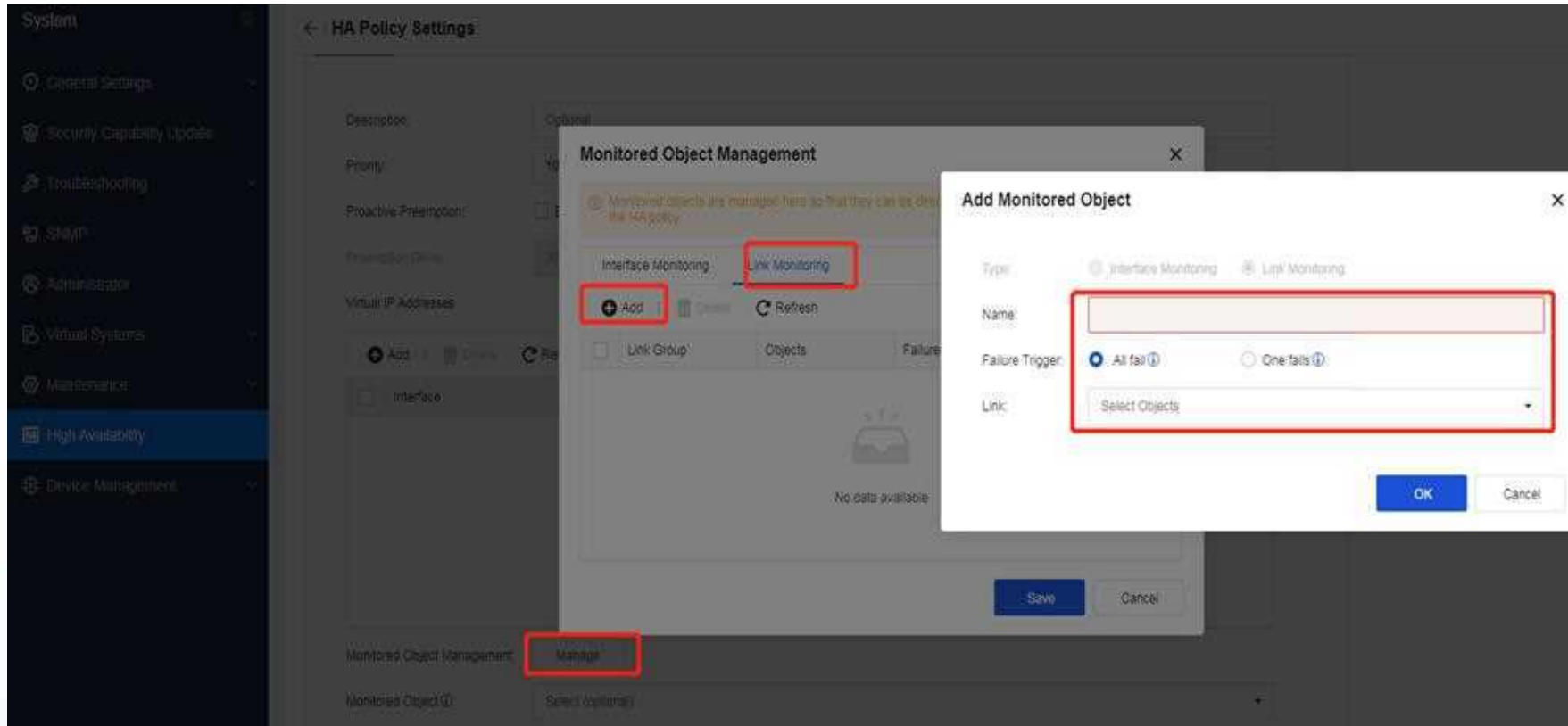
Interface monitoring is used to monitor the status of interfaces. An interface is considered to be in a "failure" state when it is either unplugged or in disabled status. The interface monitoring object can monitor multiple interfaces. If the trigger type is set to "All fail", the interface monitoring object become a "failure" status only when all the interfaces fail. If the trigger type is set to "One fails", the interface monitoring object become a "failure" status as long as one of the interfaces fails..



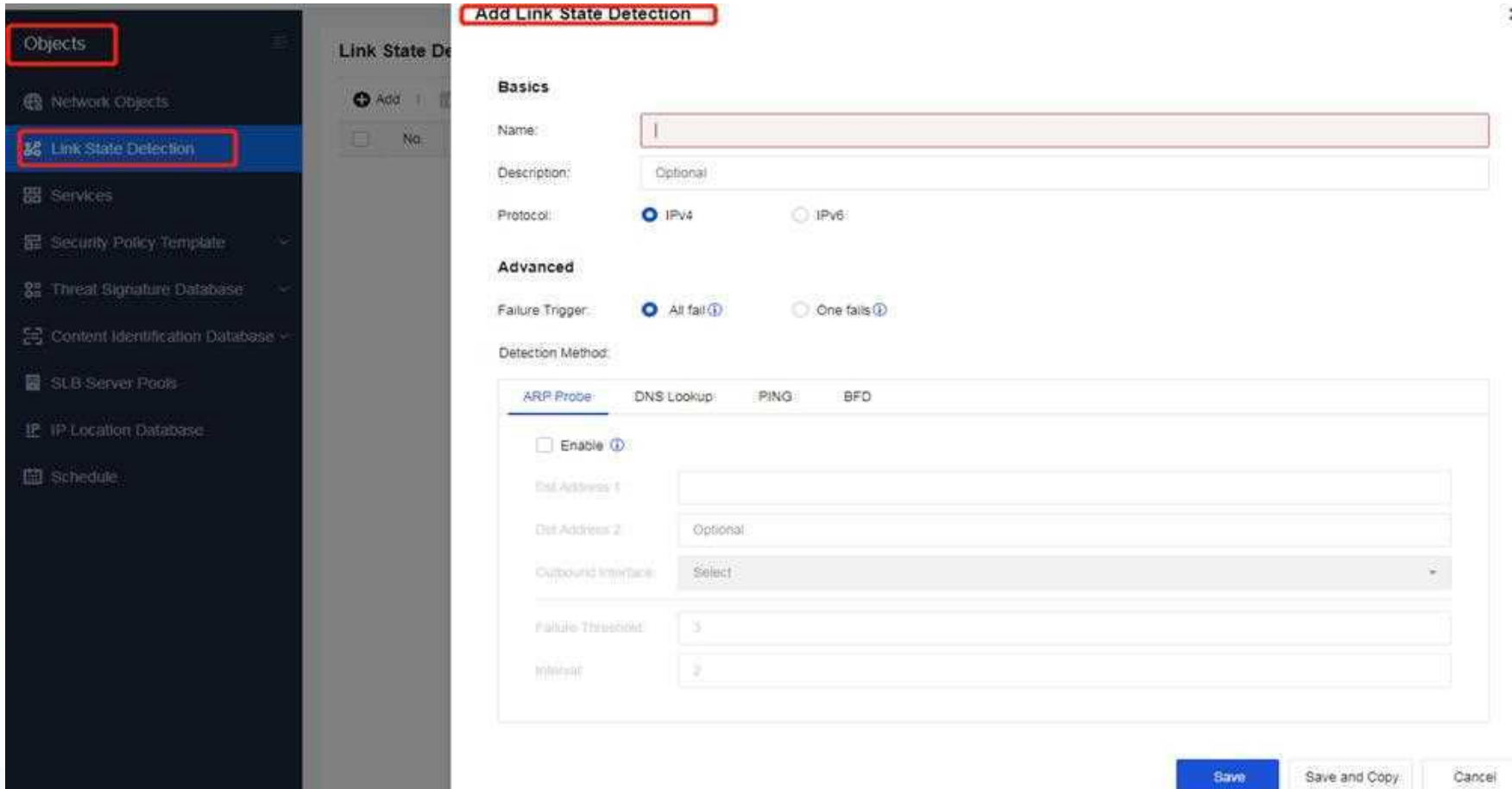
Link Monitoring



The link monitoring object is used for monitoring uplink and downlink devices. If uplink or downlink device suffer failure, the link monitoring object will become "failure" state. The link monitoring group can monitor multiple link monitoring objects. If the trigger type is set to "All fail", link monitoring object enters a "failure" status only when all the link monitoring objects fail. If the trigger type is set to "One fails", the link monitoring enters a "failure" status as long as one of the link monitoring objects fails.



When you want to monitor link objects in high availability settings, it is necessary to configure link state detection in advance. The path is **Objects > Link State Detection**. In this page you can select expected types of detection, such as ARP Probe, DNS Lookup, Ping and BFD.

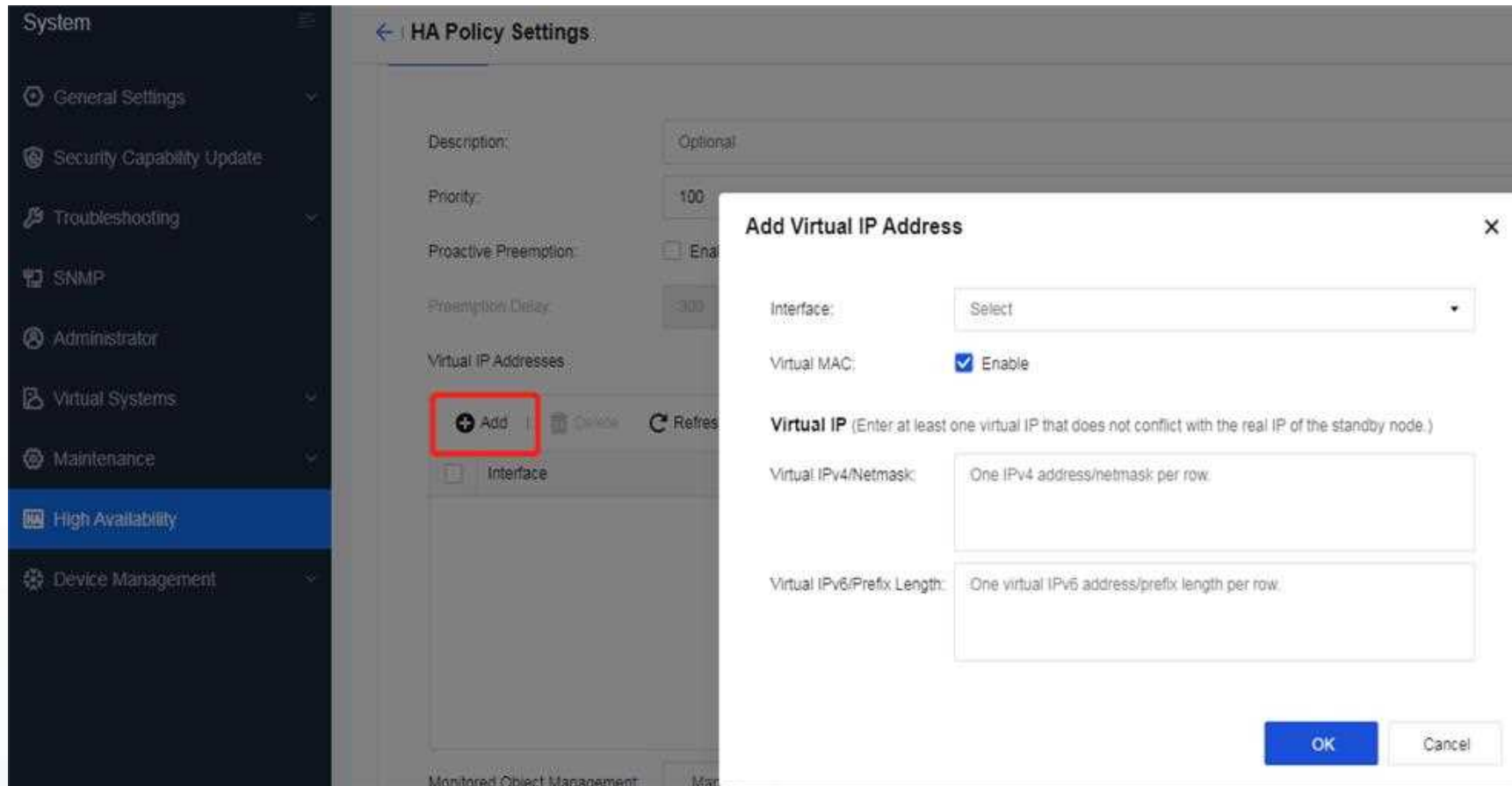


The screenshot displays the Sangfor firewall configuration interface. On the left sidebar, the 'Objects' menu is highlighted, and 'Link State Detection' is selected. The main area shows the 'Add Link State Detection' dialog box with the following fields:

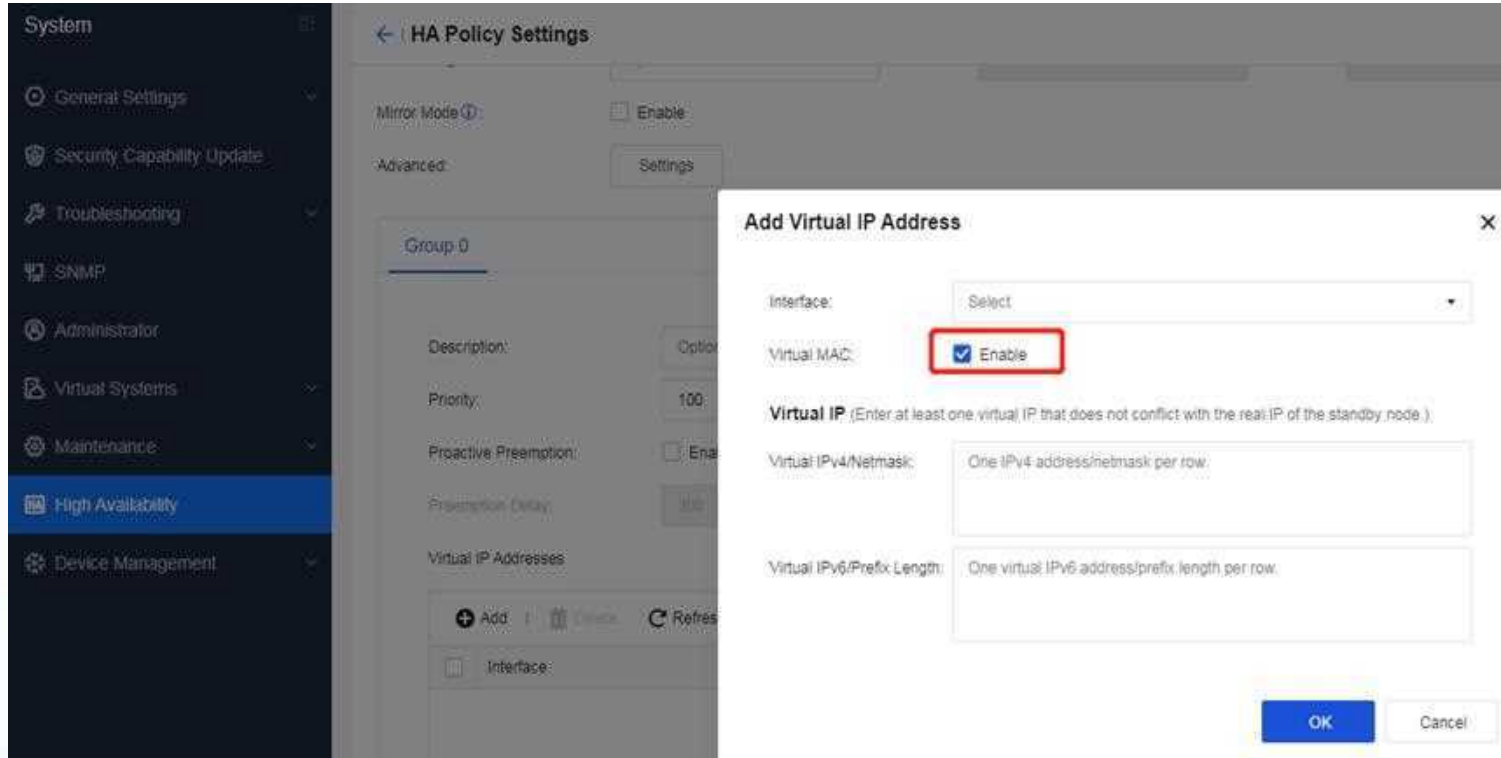
- Basics**
 - Name: [Empty text box]
 - Description: Optional [Text box]
 - Protocol: ☒ IPv4 ☐ IPv6
- Advanced**
 - Failure Trigger: ☒ All fail ☐ One fails
 - Detection Method: ARP Probe (selected), DNS Lookup, PING, BFD
- Configuration**
 - ☐ Enable
 - Dest Address 1: [Text box]
 - Dest Address 2: Optional [Text box]
 - Outbound Interface: Select [Dropdown menu]
 - Failure Threshold: 3 [Text box]
 - Interval: 2 [Text box]

At the bottom right, there are buttons for 'Save', 'Save and Copy', and 'Cancel'.

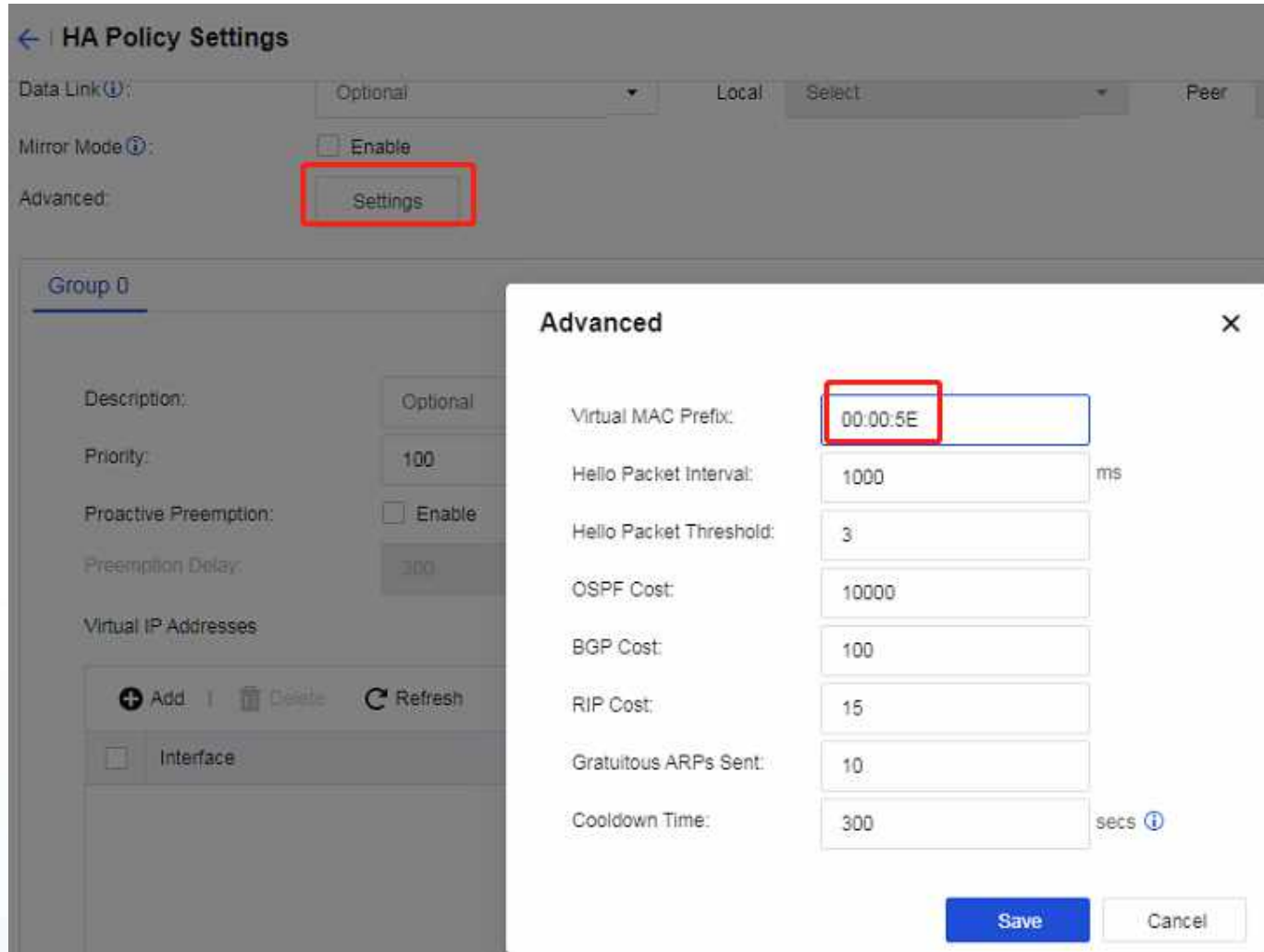
If an IP needs to be synchronized between active and standby NSF and forward business traffic, it is called the virtual IP. Compared to a real IP, the virtual IP is synchronized from active to standby NSF and only issued by the active NSF, rather than the standby NSF. When switchover occurs between active and standby NSF, the latest active NSF will issue the virtual IP.



When active and standby NSF perform a switchover, the latest active NSF sends gratuitous ARP packets to uplink and downlink devices to notify them of the MAC address. Since NIC MAC address (called real MAC address) in active and standby NSF is different. Either real MAC address or virtual MAC forwards traffic. When uplink and downlink devices receive gratuitous ARP, their MAC address table will refresh. Virtual MAC is born with virtual IP, while both in active and standby NSF, virtual MAC is same. To some extent virtual MAC address will be more efficient than real MAC address during switchover since to uplink and downlink devices the MAC address table will not be changed.



Virtual MAC can be generated automatically, while users are able to check or modify default prefix of virtual MAC.



The screenshot displays the 'HA Policy Settings' interface. In the 'Advanced' section, the 'Settings' button is highlighted with a red box. An 'Advanced' dialog box is open, showing various configuration options. The 'Virtual MAC Prefix' field is highlighted with a red box and contains the value '00:00:5E'. Other fields include 'Hello Packet Interval' (1000 ms), 'Hello Packet Threshold' (3), 'OSPF Cost' (10000), 'BGP Cost' (100), 'RIP Cost' (15), 'Gratuitous ARPs Sent' (10), and 'Cooldown Time' (300 secs). The dialog has 'Save' and 'Cancel' buttons at the bottom.

Field	Value	Unit
Virtual MAC Prefix	00:00:5E	
Hello Packet Interval	1000	ms
Hello Packet Threshold	3	
OSPF Cost	10000	
BGP Cost	100	
RIP Cost	15	
Gratuitous ARPs Sent	10	
Cooldown Time	300	secs

Group 0 and Group 1



Either group 0 or 1 represents a set of high availability. In active/standby mode, only group 0 can be seen since there is only one set of high availability. Only in active/active as well as layer-3 mode, there are two sets of high availability, requiring two NSF respectively act as active node and standby node in two groups to forward business traffic. Therefore, only the active/active as well as layer-3 mode has group 0 and group 1 .

HA Policy Settings

HA Policy: ☒ Enable

Mode: ☒ Active/Standby ☐ Active/Active

Device Name: HQ-NGAF

Control Link: Select Local Select Peer +

Data Link: Optional Local Select Peer +

Layer 2 Mode: ☐ Enable

HA Traffic: ☐ Enable

Advanced: Settings

Group 0

Description: Optional

Priority: 100

Proactive Preemption: ☐ Enable

Preemption Delay: 300 secs

Virtual IP Addresses

Interface	Virtual IP/Netmask	Virtual MAC	Operation

HA Policy Settings

HA Policy: ☒ Enable

Mode: ☐ Active/Standby ☒ Active/Active

Device Name: HQ-NGAF

Control Link: Select Local Select Peer +

Data Link: Optional Local Select Peer +

Layer 2 Mode: ☐ Enable

HA Traffic: ☐ Enable

Advanced: Settings

Group 0 **Group 1**

Description: Optional

Priority: 100

Proactive Preemption: ☐ Enable

Preemption Delay: 300 secs

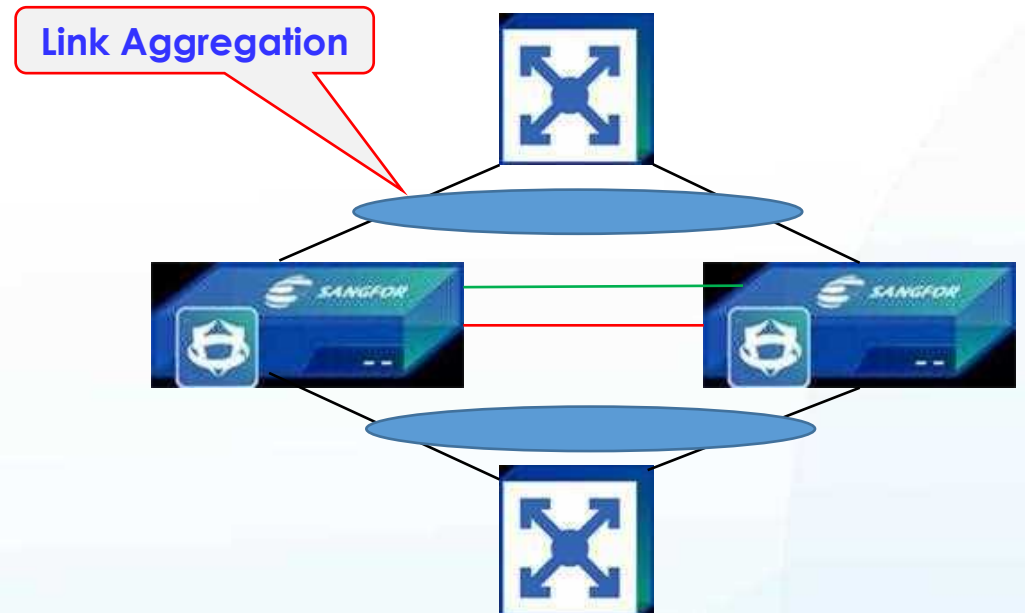
Virtual IP Addresses

Interface	Virtual IP/Netmask	Virtual MAC	Operation

- Link aggregation is mainly used in the active/active as well as layer-2 mode scenario, where link aggregation is performed on the uplink and downlink devices and traffic exists inconsistent path. After enabling this feature, each NSF will automatically generate identifier (either 0 or 1) in backend. This identifier is not visible on the web page.
- All traffic passing through the interfaces of the internal and external network areas in the NSF link aggregation configuration will be processed by an algorithm based on the source or destination IP addresses. The algorithm determines whether the computed value is 0 or 1, and forwards the corresponding data packet to specific NSF by corresponding identifier (e.g., if the computed value is 0, the data will be forwarded to the NSF with the identifier 0).

← | HA Policy Settings

HA Policy:	<input checked="" type="checkbox"/> Enable
Mode:	<input type="radio"/> Active/Standby <input checked="" type="radio"/> Active/Active
Device Name:	HQ-NGAF
Control Link ⓘ:	eth5 Local 172.16.99.5
Data Link ⓘ:	Optional Local Select
Layer 2 Mode ⓘ:	<input checked="" type="checkbox"/> Enable
HA Traffic:	<input type="checkbox"/> Enable ⓘ
Link Aggregation ⓘ:	Settings



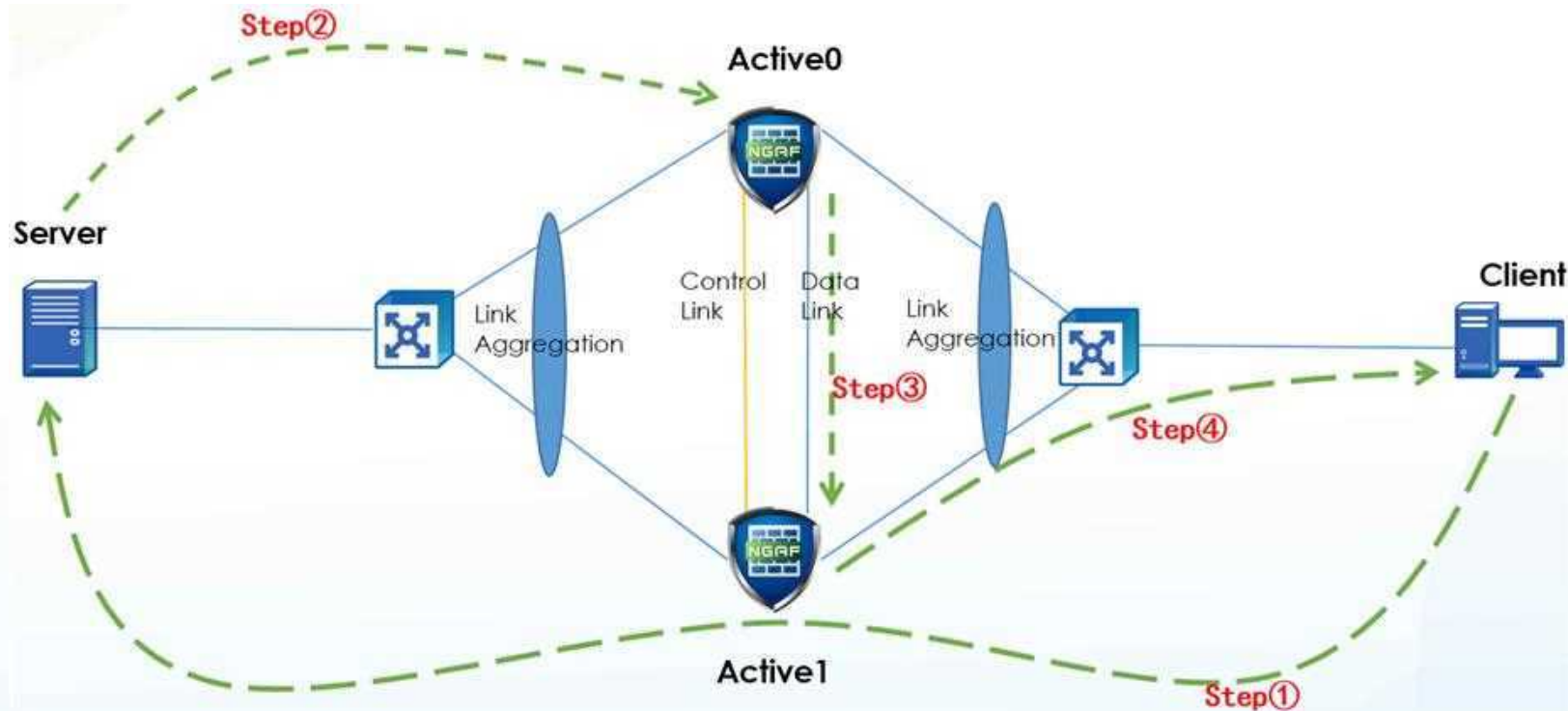
The work flow is as below:

Step① : Client traffic accessing the server passes through Active1 device. Active1 performs detection by hash algorithm. Once the detection is completed, the data packet is forwarded from Active1 to the server.

Step② : The server returns the data packet, which arrives at Active0 by link aggregation.

Step③ : Active 0 calculates the hash algorithm to determine it needs to be further checked by Active1. Same destination address yields the same calculation result as before, the data packet is forwarded to Active1 via the data link.

Step④ : Active 1 returns the data packet to the Client.



HA traffic function is only used for asymmetric traffic occasion, if not, there is no need to turn it on since this function will consume extra performance. HA traffic function is only applicable to below 2 deployment scenarios.

- **Scenario 1:** Active/Active with Virtual Wire Mode as well as enabling link aggregation function(if link aggregation function is not enabled, HA traffic will not take effect);
- **Scenario 2:** Active/Active with Layer-3 Mode;

HA Traffic



- The function is used for scenarios in which the uplink and downlink devices act as layer-3 devices, besides there exists inconsistent traffic when NSF are deployed active/active with layer-3 or active/active with virtual wire mode. “HA Traffic” feature needs to be enabled.
- After enabling this feature, some traffic is sent to the uplink device and some is sent to the downlink device, which prevents inconsistent traffic and ineffective session.
- Once the peer NS is configured on the uplink device's layer-3 interface, and the HA Traffic feature is enabled on the uplink device, it helps prevent network connectivity issues.

System

- General Settings
- Security Capability Update
- Troubleshooting
- SNMP
- Administrator
- Virtual Systems
- Maintenance
- High Availability**
- Device Management

HA Policy Settings

HA Policy: ☒ Enable

Mode: ☐ Active/Standby ☒ Active/Active

Device Name: HQ-NGAF

Control Link: Local: Peer:

Data Link: Local: Peer:

Layer 2 Mode: ☐ Enable

HA Traffic: ☒ Enable

Advanced:

Group 0 Group 1

Description:

Priority:

Proactive Preemption: ☐ Enable

Preemption Delay: secs

Virtual IP Addresses:

Interface	Virtual IP/Netmask	Virtual MAC	Operation

h algorithm
res that all
rk connectivity

data link
downlink and
device. This

The specific workflow when enabling both link aggregation and HA traffic features in active/active with virtual wire mode is as follows:

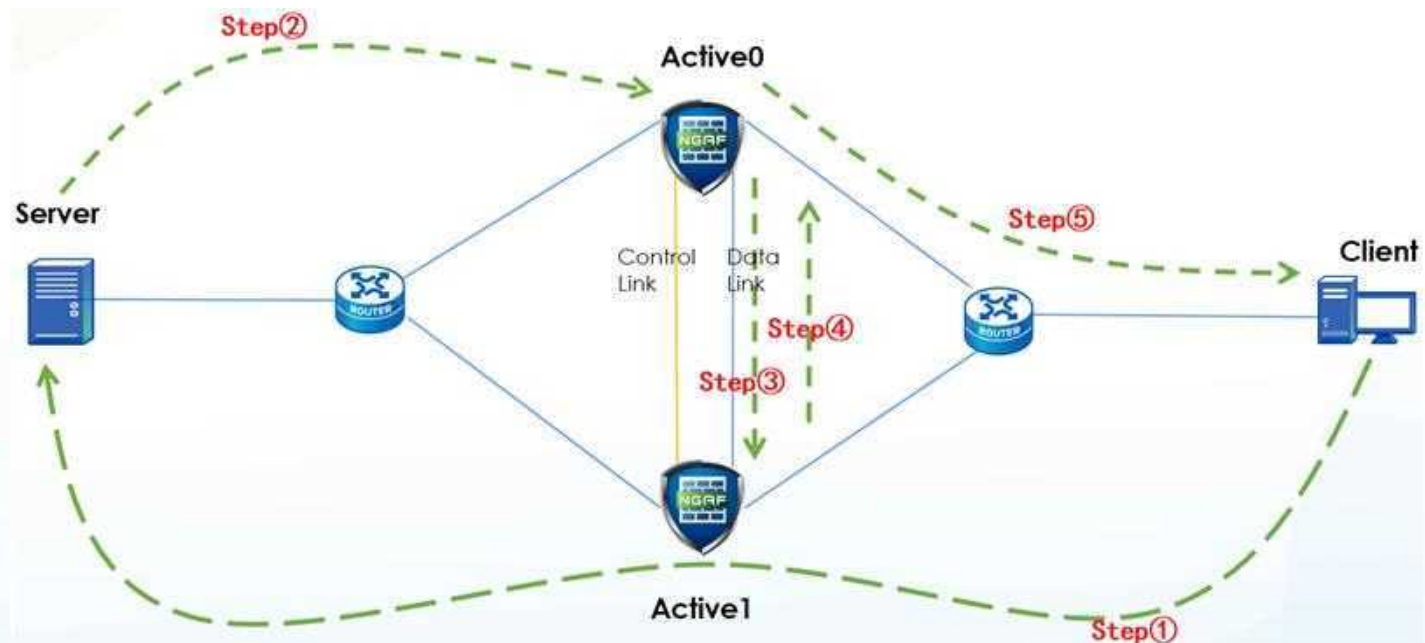
Step① : Client traffic accessing the server goes through Active 1. Active 1 performs detection by hash algorithm on the traffic, and upon completion of the detection, forwards it to the server.

Step② : The server returns the traffic, which reaches Active 0.

Step③ : Active 0 applies the hash algorithm to determine that Active 1 should perform the detection (calculating the same result for the same address). It forwards the packets to Active 1 through the data link.

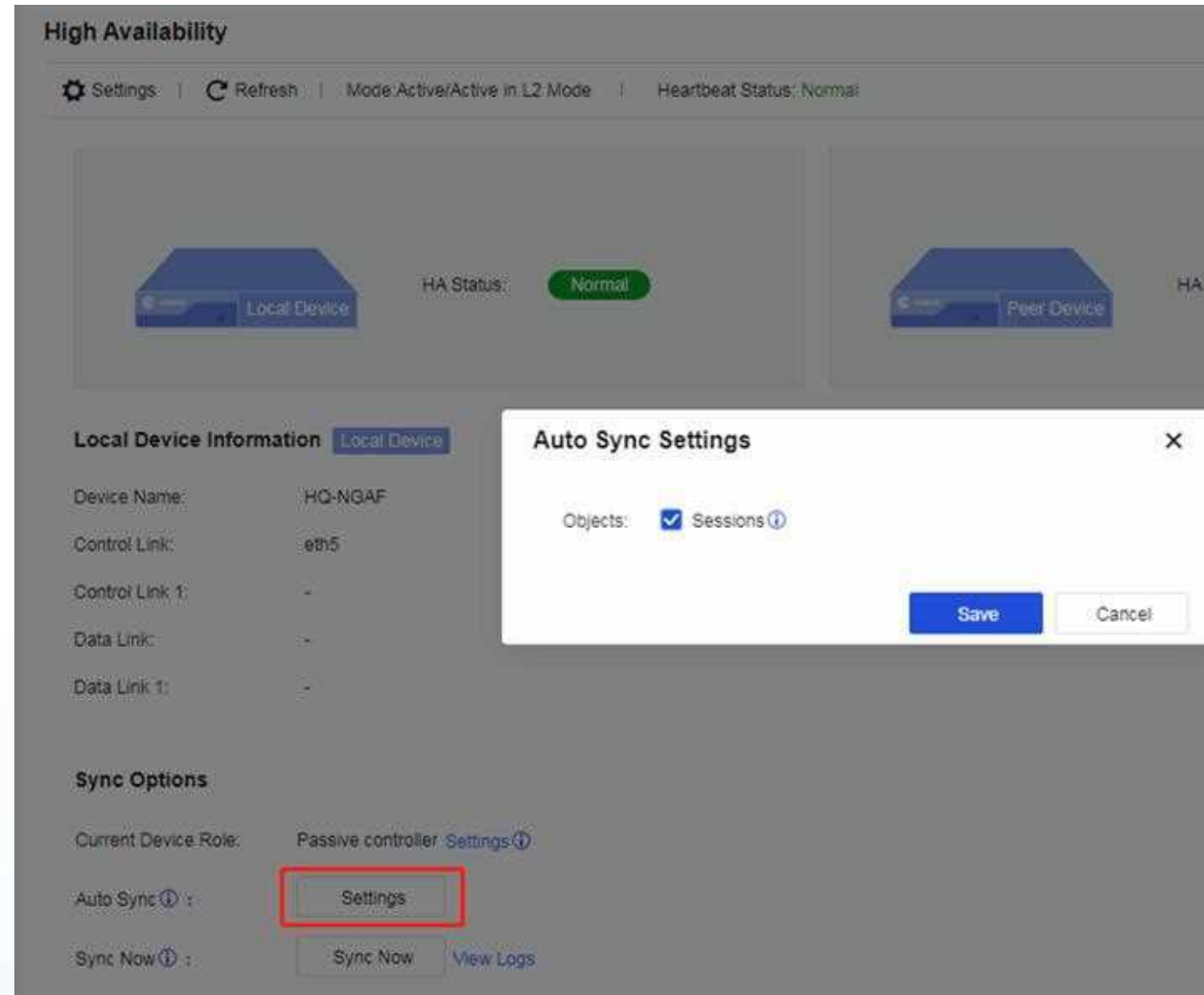
Step④ : After receiving the packets, Active 1 completes the detection and forwards them back to Active 0 through the data link.

Step⑤ : Active 0 returns the packets to the client..



Synchronization Objects

You are able to edit synchronization objects in the setting of “Auto Sync”, and currently there is only sessions which can be selected.



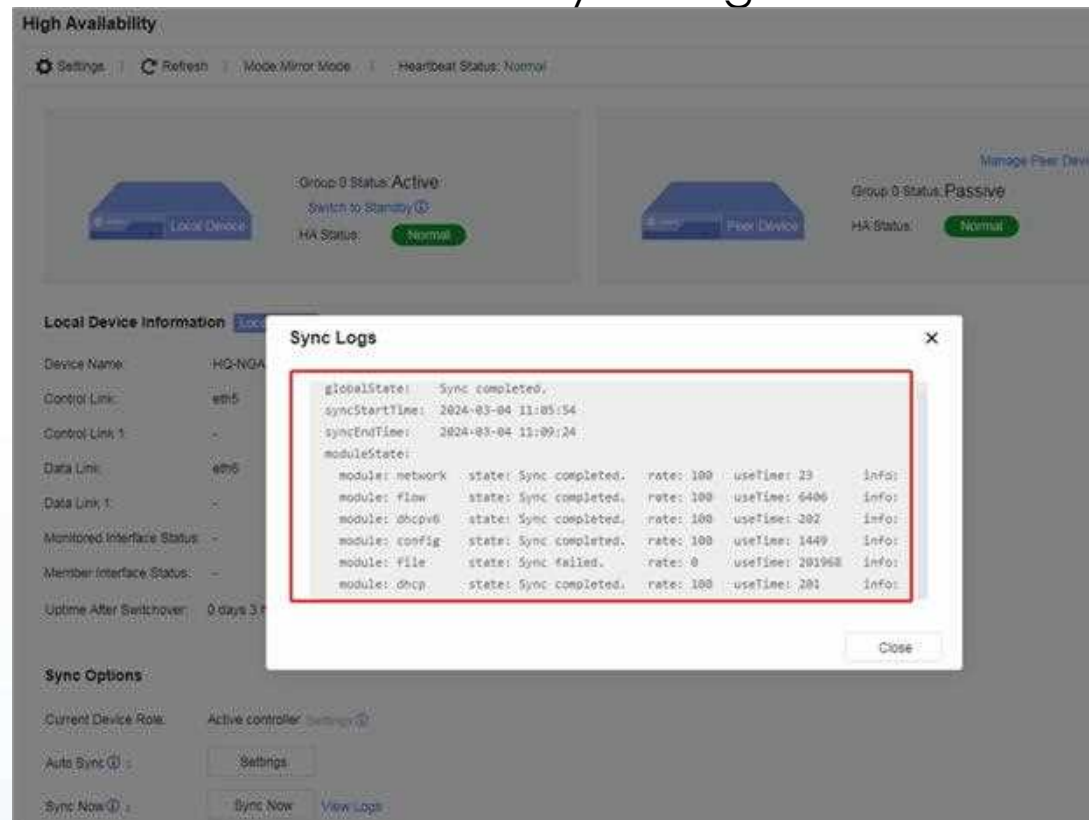
Sessions are synchronized by data link interface in usual, and if there is no data link, which can be synchronized by control link interface. There are several types of synchronization methods, they are respectively as below.

Types of Synchronization	Description
Real-time synchronization	This mainly contains sessions and is triggered as session establishment, deletion, modification and adding.
Manual synchronization	You are able to trigger it manually in web panel.
Scheduled synchronization	In backend, there exists scheduled synchronization from one NSf to another.
Full synchronization	This always happened when suffered switchover.

Note:

- As for parent-child link in the process of session synchronization, such as control channel and data channel in FTP application, parent link will be synchronized firstly and then child link.
- There are some exception which are not synchronized, such as local host sessions, sessions of ICMP, and deleted sessions when interfaces turned down.

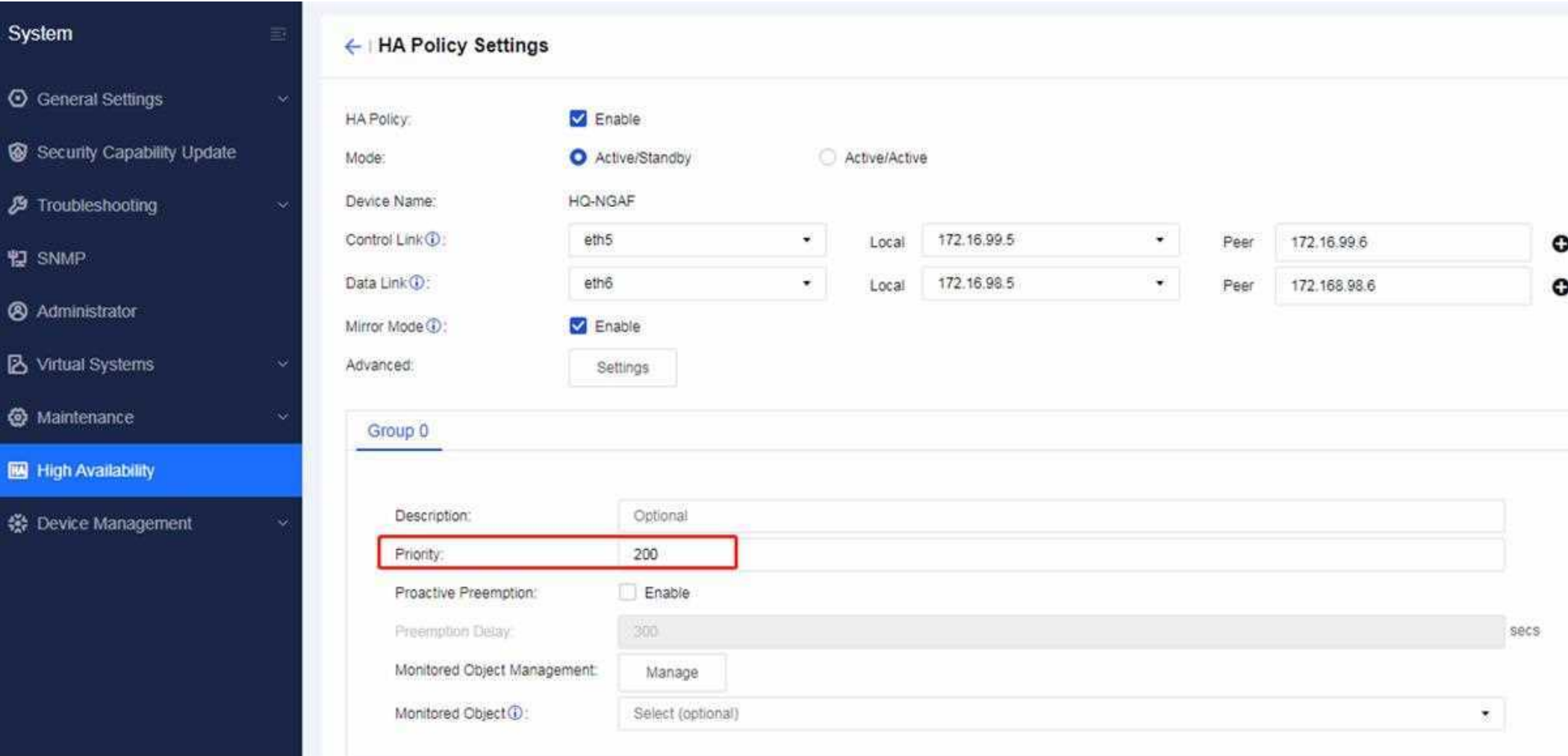
- After both NSF have been configured control link and data link interfaces, “Hello” packet determine which one is active and which one is standby.
- After negotiation process finishes, active NSF will synchronize configuration information, such as business configuration, interfaces configuration etc. to standby NSF.
- If new configuration is executed in active NSF, it will automatically synchronize to standby one, however there is no chance to delivery configuration in reverse process.



High availability switchover depends on a serial of elements, such as proactive preemption, device failure value, monitoring objects failure value, configuration priority, and real-time priority. Details of switchover delay can be referred as below.

Cause of Switchover	Switchover Delay
Modify NSF priority in proactive preemption mode	1 heartbeat cycle
Break down of monitoring interfaces	no delay
Link monitoring detection failure	no delay
NSF power off or whole NSF break down	3 heartbeats cycle

Configuration Priority: Configure in web panel



The screenshot displays the Sangfor web panel interface. On the left is a dark blue sidebar with a menu containing: System, General Settings, Security Capability Update, Troubleshooting, SNMP, Administrator, Virtual Systems, Maintenance, High Availability (highlighted in blue), and Device Management. The main content area is titled 'HA Policy Settings' and includes the following configuration options:

- HA Policy:** ☒ Enable
- Mode:** ☒ Active/Standby ☐ Active/Active
- Device Name:** HQ-NGAF
- Control Link:** eth5 (dropdown), Local: 172.16.99.5 (dropdown), Peer: 172.16.99.6 (text input)
- Data Link:** eth6 (dropdown), Local: 172.16.98.5 (dropdown), Peer: 172.168.98.6 (text input)
- Mirror Mode:** ☒ Enable
- Advanced:** Settings (button)

Below these settings is a section for **Group 0** with the following configuration:

- Description:** Optional (text input)
- Priority:** 200 (text input, highlighted with a red border)
- Proactive Preemption:** ☐ Enable
- Preemption Delay:** 300 (text input), secs (unit label)
- Monitored Object Management:** Manage (button)
- Monitored Object:** Select (optional) (dropdown menu)

■ Device failure value and monitoring objects failure value

By default the failure value of interface monitoring and link monitoring are 255 and device failure value is 0. Either interface monitoring or link monitoring happened to failure, device failure value will increase from default 0 to 255.

■ Real-time Priority

Real-time priority = configuration priority - device failure value

Note: The minimal value of real-time priority is “0”, and never be a negative number. For example if configuration priority is 100, and currently device failure value is 255, real-time priority value then is “0”

■ Proactive Preemption

Group 0

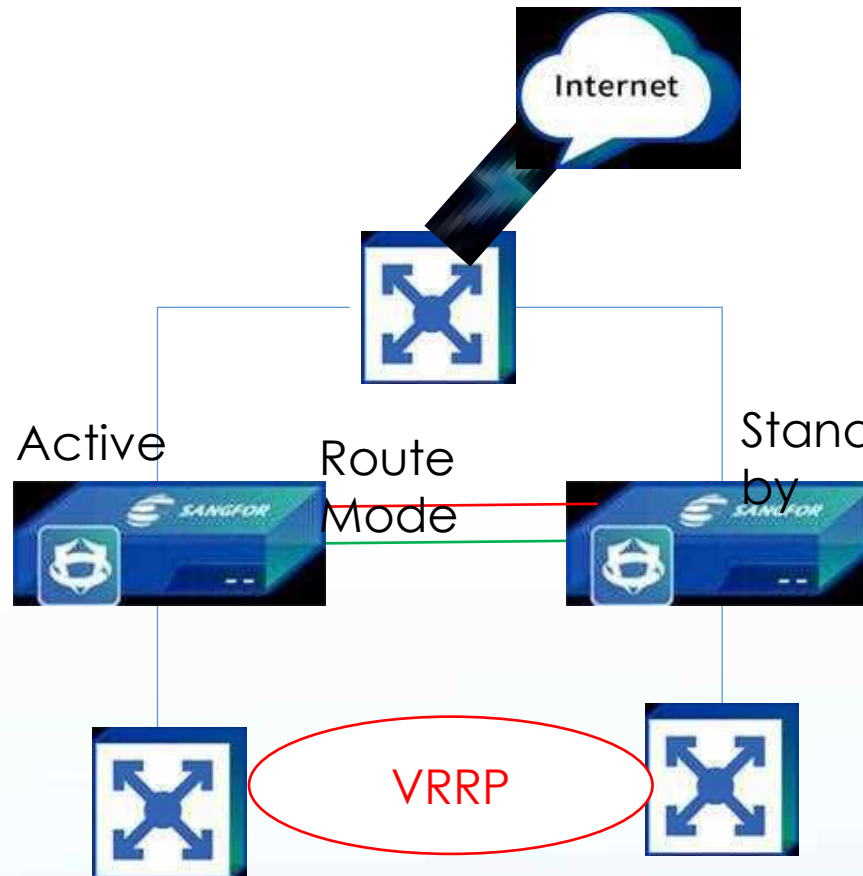
Description:	Optional
Priority:	200
Proactive Preemption:	<input checked="" type="checkbox"/> Enable
Preemption Delay:	300 secs
Monitored Object Management:	Manage
Monitored Object ⓘ:	Select (optional) ▼

PART 2

Types of High Availability

Active/Standby Mode

Only active NSF forwards traffic, standby NSF doesn't in Active/Standby mode. Only active NSF will issue virtual IP to uplink and downlink devices. When active NSF suffers failure, there will trigger switchover, and then virtual IP will be issued by latest active NSF. The configuration cannot be edited once NSF is elected as standby role.



Active/Standby with Mirror Mode



The real IP forwards traffic replacing virtual IP, when compared with Active/Standby mode. Except from OOBM interface, control link interface and data link interface, the rest interfaces information will be synchronized from active NSF to standby NSF, including MAC addresses.

Physical Interfaces

Subinterfaces

VLAN Interface

✓ Enable

✗ Disable

Refresh

Interface Name	Interface Status	WAN Attribute	Type
eth0 OOBM		No	La
eth1		Yes	La
eth2		No	La
eth3		No	La
eth4		No	La
eth5		No	La
eth6		No	La

HA Policy Settings

HA Policy:

☒ Enable

Mode:

☒ Active/Standby

☐ Active/Active

Device Name:

HQ-NGAF

Control Link

eth5

Local

172.16.99.5

Peer

172.16.99.6

Data Link

eth6

Local

172.16.98.5

Peer

172.168.98.6

Mirror Mode

☒ Enable

Advanced

Settings

Group 0

Description:

Optional

Priority:

200

Proactive Preemption:

☐ Enable

Preemption Delay:

300

secs

Monitored Object Management:

Manage

Monitored Object

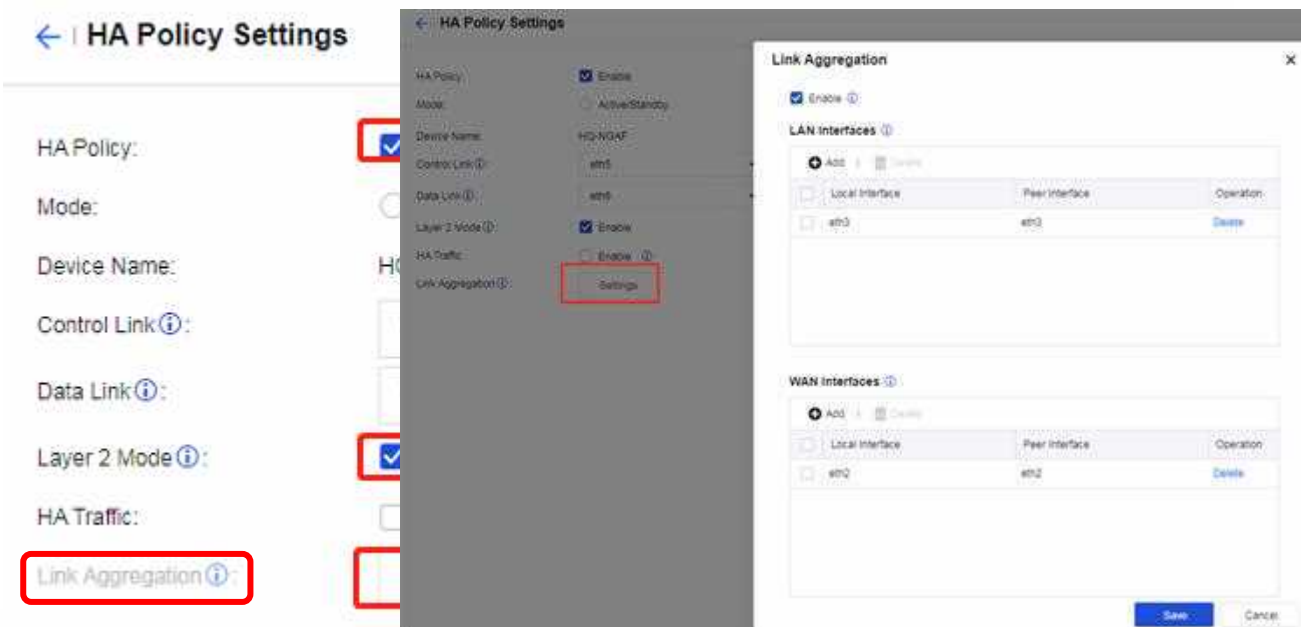
Select (optional)

non

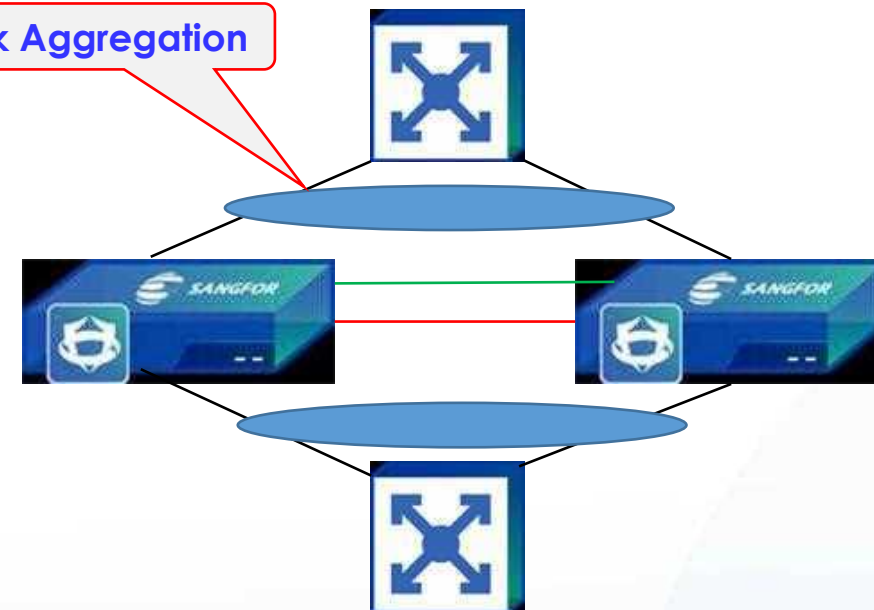
nor

Active/Active with Virtual Wire Mode

There is no group 0 nor group 1 in Active/Active with layer-2 mode. If there exists inconsistent traffic, you are required to turn on “**Link Aggregation**” function to guarantee normal forwarding.



Link Aggregation

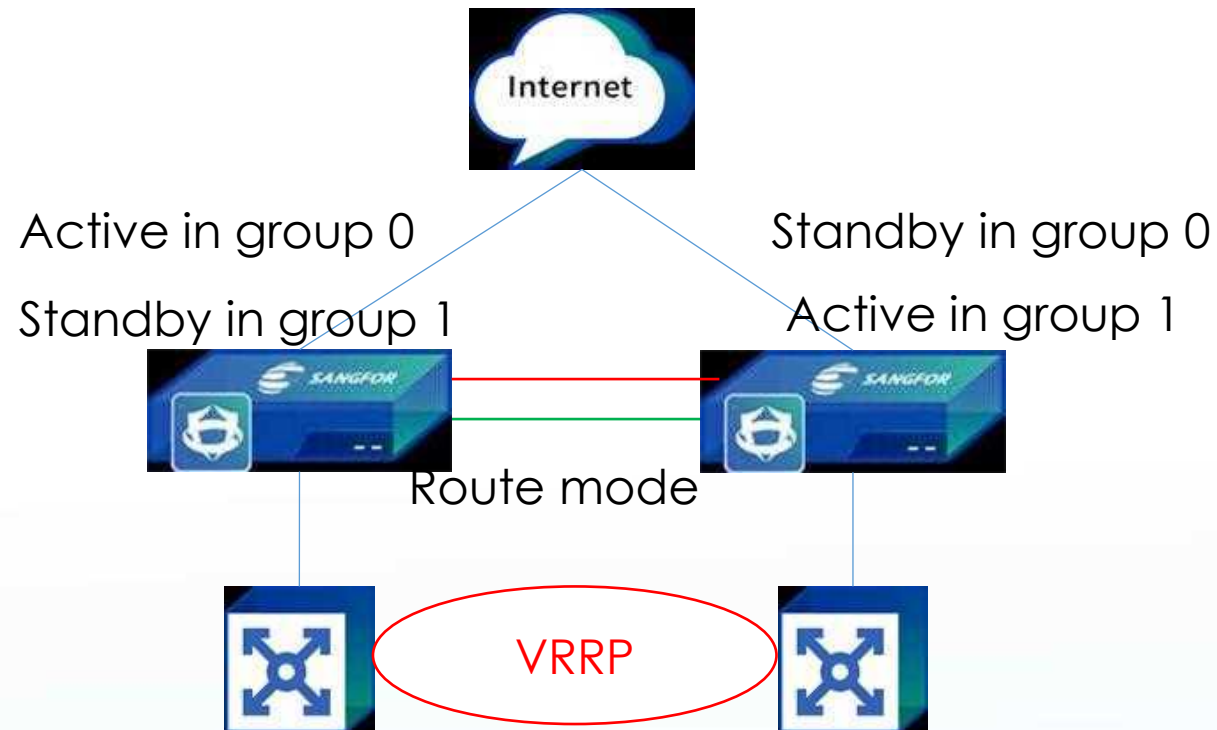


Requirements:

1. HA policy is enabled.
2. The HA mode is active/active and Layer 2 mode is enabled.
3. Data sync interface is configured.
4. At least 2 available Layer-2 interfaces are required.

Active/Active with Layer-3 Mode

Active/Active with layer-3 mode is mainly used for scenario that one NSF undertakes too much due to large size of traffic, requiring another NSF to load balance. In this mode, both NSF forward traffic as well as behave the relation between active and backup in different group.

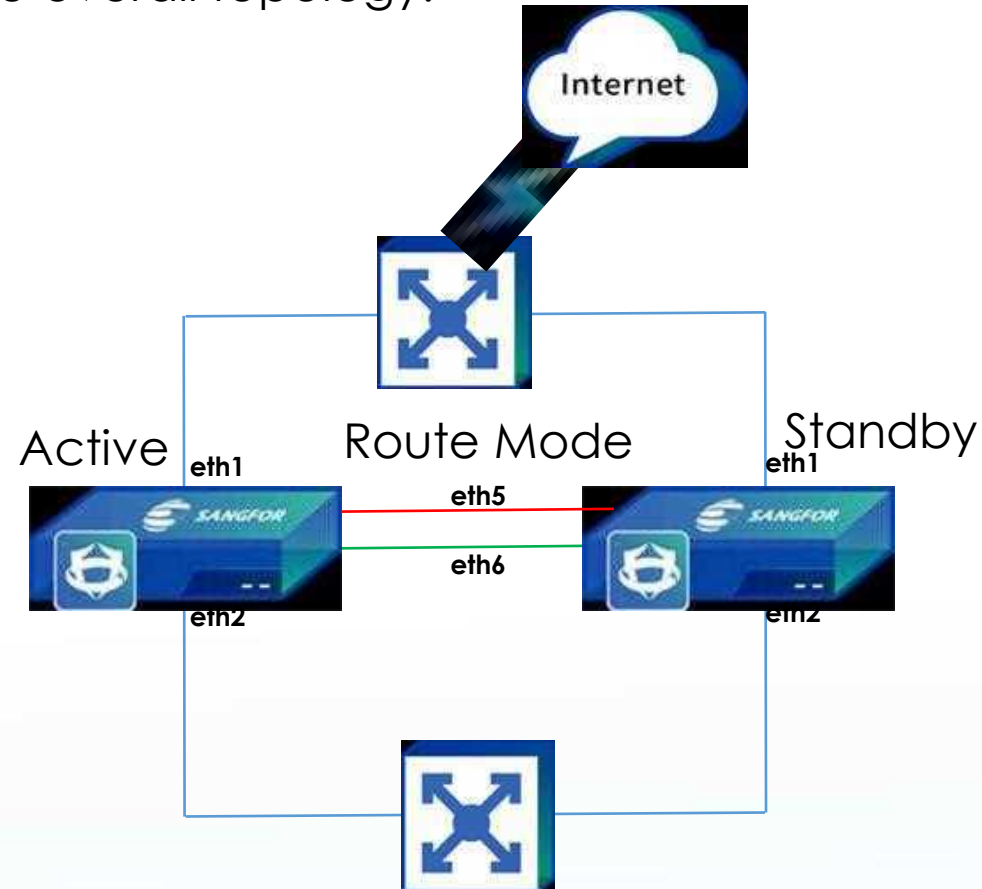


PART 3

Case Study of High Availability

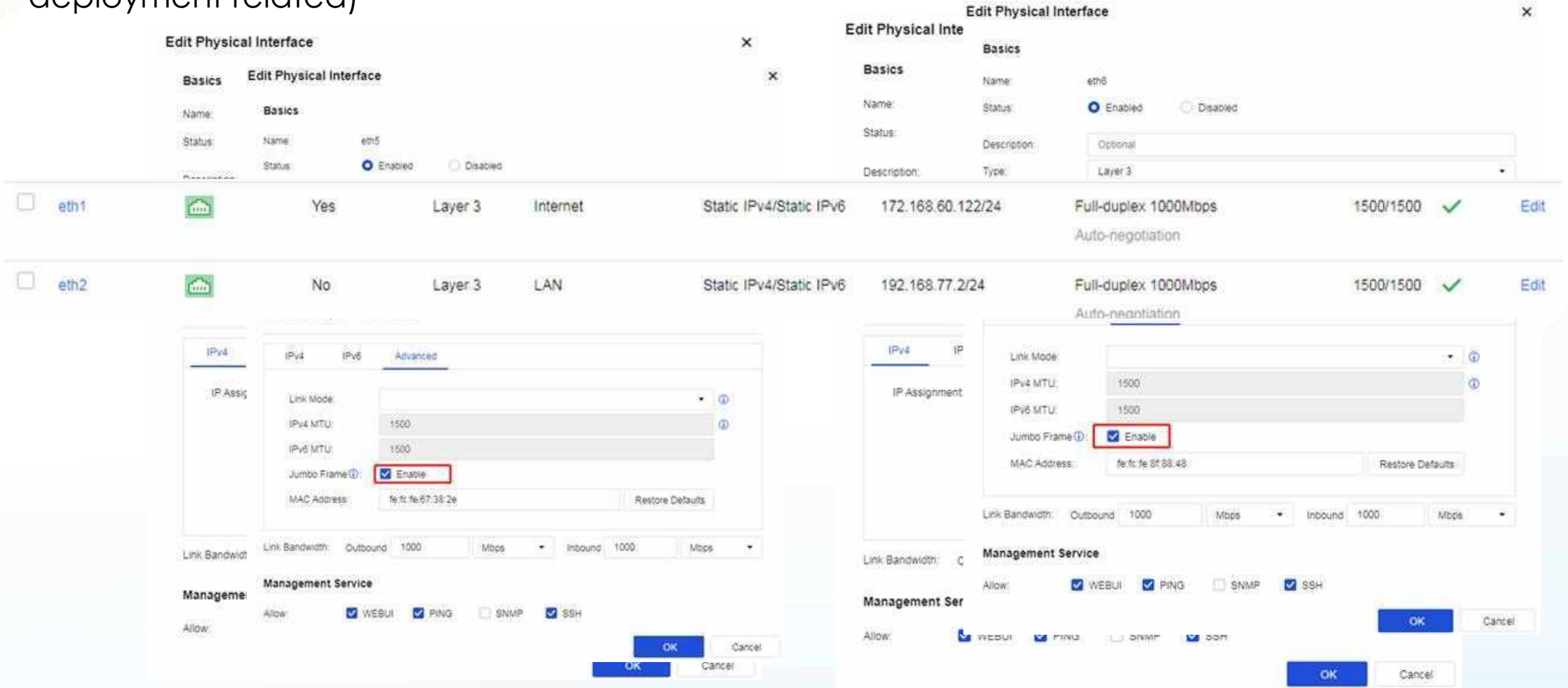
Case 1: Active/Standby with Mirror Mode

A customer now purchase 2 NSF to deploy current network and require NSF provide high availability. Below is the overall topology.



Case 1: Active/Standby with Mirror Mode

In expected active NSF, configure network and interfaces(ignore security policy and deployment related)



The screenshot displays the Sangfor firewall configuration interface, specifically the 'Edit Physical Interface' dialog box. The interface is divided into two main sections: 'Basics' and 'Advanced'.

Basics Section:

- Name:** eth5
- Status:** Enabled (radio button selected)
- Description:** Optional
- Type:** Layer 3

Advanced Section:

- Link Mode:** Auto-negotiation
- IPv4 MTU:** 1500
- IPv6 MTU:** 1500
- Jumbo Frame:** Enabled (checkbox checked)
- MAC Address:** fe:ff:fe:67:38:2e
- Link Bandwidth:** Outbound 1000 Mbps, Inbound 1000 Mbps

Management Service Section:

- Allow:** WEBUI, PING, SNMP, SSH (all checked)

Interface Table:

Interface	Status	Type	Mode	IP Address	Speed	MTU	Link Mode
eth1	Yes	Layer 3	Internet	Static IPv4/Static IPv6 172.168.60.122/24	Full-duplex 1000Mbps	1500/1500	✓
eth2	No	Layer 3	LAN	Static IPv4/Static IPv6 192.168.77.2/24	Full-duplex 1000Mbps	1500/1500	✓

The 'Jumbo Frame' checkbox is highlighted with a red box in the 'Advanced' section of the 'Edit Physical Interface' dialog box.

Case 1: Active/Standby with Mirror Mode

In expected standby NSF, configure network and interfaces.

Edit Physical Interface

Basics

Name:eth5

Status:☒ Enabled ☐ Disabled

Description:Optional

Type:Layer 3

Zone:Control-Link

Basic Attributes:☐ WAN attribute

Reverse Routing ⓘ:☐ Enabled

IPv4IPv6Advanced

IP Assignment:☒ Static ☐ DHCP ☐ PPPoE

Static IP:172.16.99.6/24 ⓘ

Default Gateway:

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow:☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

OKCancel

Edit Physical Interface

Basics

Name:eth6

Status:☒ Enabled ☐ Disabled

Description:Optional

Type:Layer 3

Zone:Data-Link

Basic Attributes:☐ WAN attribute

Reverse Routing ⓘ:☐ Enabled

IPv4IPv6Advanced

IP Assignment:☒ Static ☐ DHCP ☐ PPPoE

Static IP:172.16.98.6/24 ⓘ

Default Gateway:

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow:☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

OKCancel

Case 1: Active/Standby with Mirror Mode

In expected active NSF, configure setting of high availability.

← HA Policy Settings

HA Policy: ☒ Enable

Mode: ☒ Active/Standby ☐ Active

Device Name: HQ-NGAF

Control Link ①: eth5

Data Link ①: eth5

Mirror Mode ①: ☒ Enable

Advanced: Settings

Group 0

Description: Optional

Priority: 200

Proactive Preemption: ☐ Enable

Preemption Delay: 300

Monitored Object Management: Manage

Monitored Object ①: Select (optional)

Monitored Object Management

Monitored objects are managed here so that they can be directly referenced when the user configure the HA policy.

Interface Monitoring Link Monitoring

+ Add | Delete Refresh

<input type="checkbox"/>	Group Name	Interface	Failure Trigger	Operation	...
<input type="checkbox"/>	business interface	eth1,eth2	One fails	Edit Delete	

Save Cancel

Case 1: Active/Standby with Mirror Mode

In expected standby NSF, configure setting of high availability.

← HA Policy Settings

HA Policy:

☒ Enable

Mode:

☒ Active/Standby

☐ Active/Active

Device Name:

NSF

Control Link ①:

eth5

Local

172.16.99.6

Peer

172.16.99.5

Data Link ①:

eth6

Local

172.16.98.6

Peer

172.16.98.5

Mirror Mode ①:

☒ Enable

Advanced:

Settings

Group 0

Description:

Optional

Priority:

100

Proactive Preemption:

☐ Enable

Preemption Delay:

300

secs

Monitored Object Management:

Manage

Monitored Object ①:

Select (optional)

Case 1: Active/Standby with Mirror Mode

After high availability is established successfully, it will display below status.

High Availability

Settings Refresh Mode: Mirror Mode Heartbeat Status: Normal

This node is in secondary sync role and configurations cannot be changed via it.



Local Device Information Local Device

Device Name: HQ-NGAF
Control Link: eth5
Control Link 1: -
Data Link: eth6
Data Link 1: -
Monitored Interface Status: -
Member Interface Status: -
Uptime After Switchover: 0 days 6 hrs 21 mins [View Switchover Information](#)

Active NSF

High Availability

Settings Refresh Mode: Mirror Mode Heartbeat Status: Normal



Local Device Information Local Device

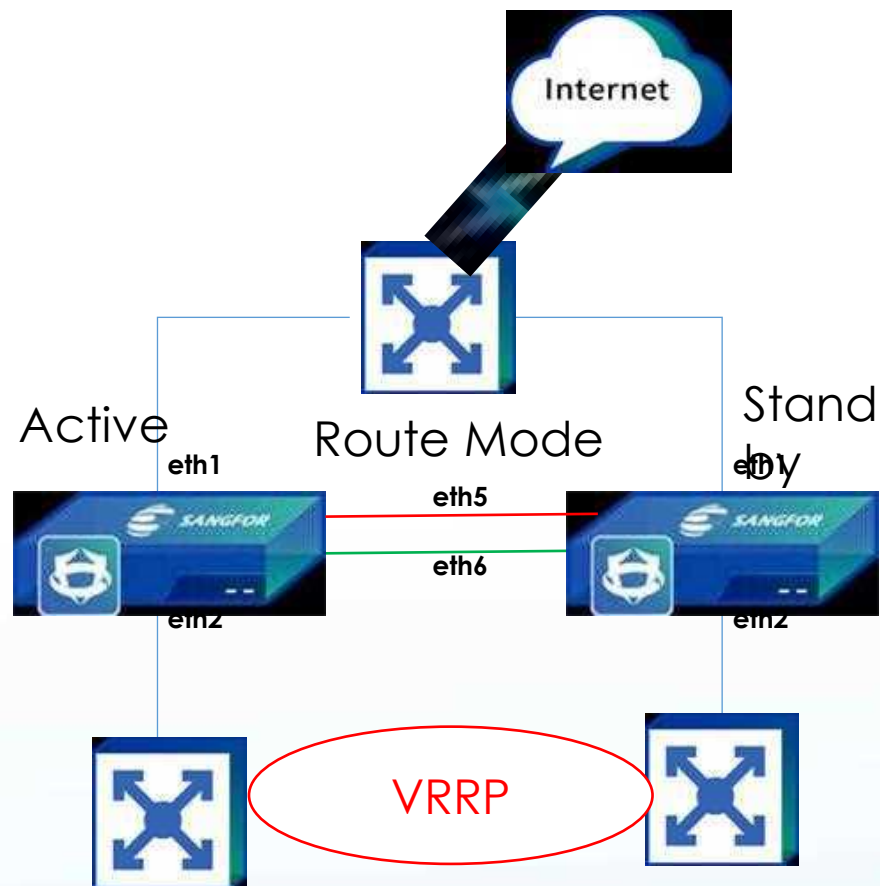
Device Name: NSF
Control Link: eth5
Control Link 1: -
Data Link: eth6
Data Link 1: -
Monitored Interface Status: -
Member Interface Status: -
Uptime After Switchover: 0 days 6 hrs 10 mins [View Switchover Information](#)

Standby NSF



Case 2: Active/Standby Mode

A customer's internal network is based on VRRP protocol, now customer purchased 2 NSF to deploy current network and require NSF provide high availability. Below is the overall topology.



Case 2: Active/Standby Mode



In expected active NSF, configure network and interfaces(ignore security policy and deployment related)

Edit | Edit Physical Interface

Ba Basics

Name: eth5
Status: ☒ Enabled ☐ Disabled
Description: Optional

Interface	Icon	Enabled	Type	Mode	IP Address	Speed	MTU	Status	Action
eth1		Yes	Layer 3	Internet	Static IPv4/Static IPv6	172.168.60.122/24	Full-duplex 1000Mbps	1500/1500	✓ Edit
eth2		No	Layer 3	LAN	Static IPv4/Static IPv6	192.168.77.2/24	Full-duplex 1000Mbps	1500/1500	✓ Edit

eth1 Advanced

Link Mode:
IPv4 MTU: 1500
IPv6 MTU: 1500
Jumbo Frame ☒ Enable
MAC Address: fe:fc:fe:67:38:2e

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Ma Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

eth2 Advanced

Link Mode:
IPv4 MTU: 1500
IPv6 MTU: 1500
Jumbo Frame ☒ Enable
MAC Address: fe:fc:fe:2f:68:48

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Ma Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

Case 2: Active/Standby Mode

In expected standby NSF, configure network and interfaces.

Edit Physical Interface

Basics


Name:eth5

Status:☒ Enabled ☐ Disabled

Description:Optional

Type:Layer 3

eth1



Yes

Layer 3

Internet

Static IPv4/Static IPv6


172.168.60.123/24

Full-duplex 1000Mbps

1500/1500

✓

☐ eth2



No

Layer 3

LAN

Static IPv4/Static IPv6

192.168.77.3/24

Full-duplex 1000Mbps

1500/1500

✓

Static IP:172.16.99.6/24

Default Gateway:

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

OK Cancel

Edit Physical Interface

Basics


Name:eth6

Status:☒ Enabled ☐ Disabled

Description:Optional

Type:Layer 3

eth6



Yes

Layer 3

Internet

Static IPv4/Static IPv6


172.168.60.123/24

Full-duplex 1000Mbps

1500/1500

✓

☐ eth7



No

Layer 3

LAN

Static IPv4/Static IPv6

192.168.77.3/24

Full-duplex 1000Mbps

1500/1500

✓

Static IP:172.16.98.6/24

Default Gateway:

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service

Allow: ☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

OK Cancel

Case 2: Active/Standby Mode

In expected active NSF, configure setting of high availability.

← HA Policy Settings

HA Policy:

☒ Enable

Mode:

Device Name:

Control Link ⓘ:

Data Link ⓘ:

Mirror Mode ⓘ:

Advanced:

Group 0

Description:

Priority:

Proactive Preem

Preemption Del

Virtual IP Addre

☒ Add

☐ Interface

☐ eth1

☐ eth2

Virtual IP Addresses

+ Add

Delete

Refresh

☐ Interface

☐ eth1

☐ eth2

Virtual

172.16

192.16

Monitored Object Management:

Manage:

Monitored Object ⓘ:

business interface

Save

Cancel

Monitored Object Management

×

Monitored objects are managed here so that they can be directly referenced when the user configure the HA policy.

Interface Monitoring

Link Monitoring

+ Add

Delete

Refresh

<input type="checkbox"/>	Group Name	Interface	Failure Trigger	Operation	...
<input type="checkbox"/>	business interface	eth1,eth2	One fails	Edit Delete	

Save

Cancel

Case 2: Active/Standby Mode

In expected standby NSF, configure setting of high availability.

← HA Policy Settings

HA Policy:

Mode:

Device Name:

Control Link:

Data Link:

Mirror Mode:

Advanced:

Group 0

Description:

Priority:

Proactive Preemption:

Preemption Delay:

Virtual IP Addresses

+ Add | Delete

☐ Interface

☐ eth1

☐ eth2

Preemption Delay:

300

Virtual IP Addresses

+ Add | Delete | Refresh

☐ Interface

Virtual

☐ eth1

172.1

☐ eth2

192.1

Monitored Object Management:

Manage

Monitored Object:

business interface

Save

Cancel

Monitored Object Management

X

Monitored objects are managed here so that they can be directly referenced when the user configure the HA policy.

Interface Monitoring

Link Monitoring

+ Add | Delete | Refresh

<input type="checkbox"/>	Group Name	Interface	Failure Trigger	Operation	...
<input type="checkbox"/>	business interface	eth1,eth2	One fails	Edit Delete	

Save

Cancel

Case 2: Active/Standby Mode

The successful high availability status is shown as below.

High Availability

Settings | Refresh | Mode: Active/Standby | Heartbeat Status: Normal

This node is in secondary sync role and configurations cannot be changed via it.

Group 0 Status: **Active**
Switch to Standby ⓘ
HA Status: **Normal**

Local Device

Peer Device

Group 0

HA Status

Local Device Information

Local Device

Device Name: HQ-NGAF
Control Link: eth5
Control Link 1: -
Data Link: eth6
Data Link 1: -
Monitored Interface Status: Normal
Member Interface Status: -
Uptime After Switchover: 0 days 0 hrs 5 mins [View Switchover Information](#)

Sync Options

Current Device Role: Active controller [Settings ⓘ](#)

Auto Sync ⓘ: [Settings](#)

Sync Now ⓘ: [Sync Now](#) [View Logs](#)

Active NSF

High Availability

Settings | Refresh | Mode: Active/Standby | Heartbeat Status: Normal

Group 0 Status: **Passive**
HA Status: **Normal**

Local Device

Peer Device

Group 0

HA Status

Manage Peer Device

Local Device Information

Local Device

Device Name: NSF
Control Link: eth5
Control Link 1: -
Data Link: eth6
Data Link 1: -
Monitored Interface Status: Normal
Member Interface Status: -
Uptime After Switchover: 0 days 0 hrs 6 mins [View Switchover Information](#)

Sync Options

Current Device Role: Passive controller [Settings ⓘ](#)

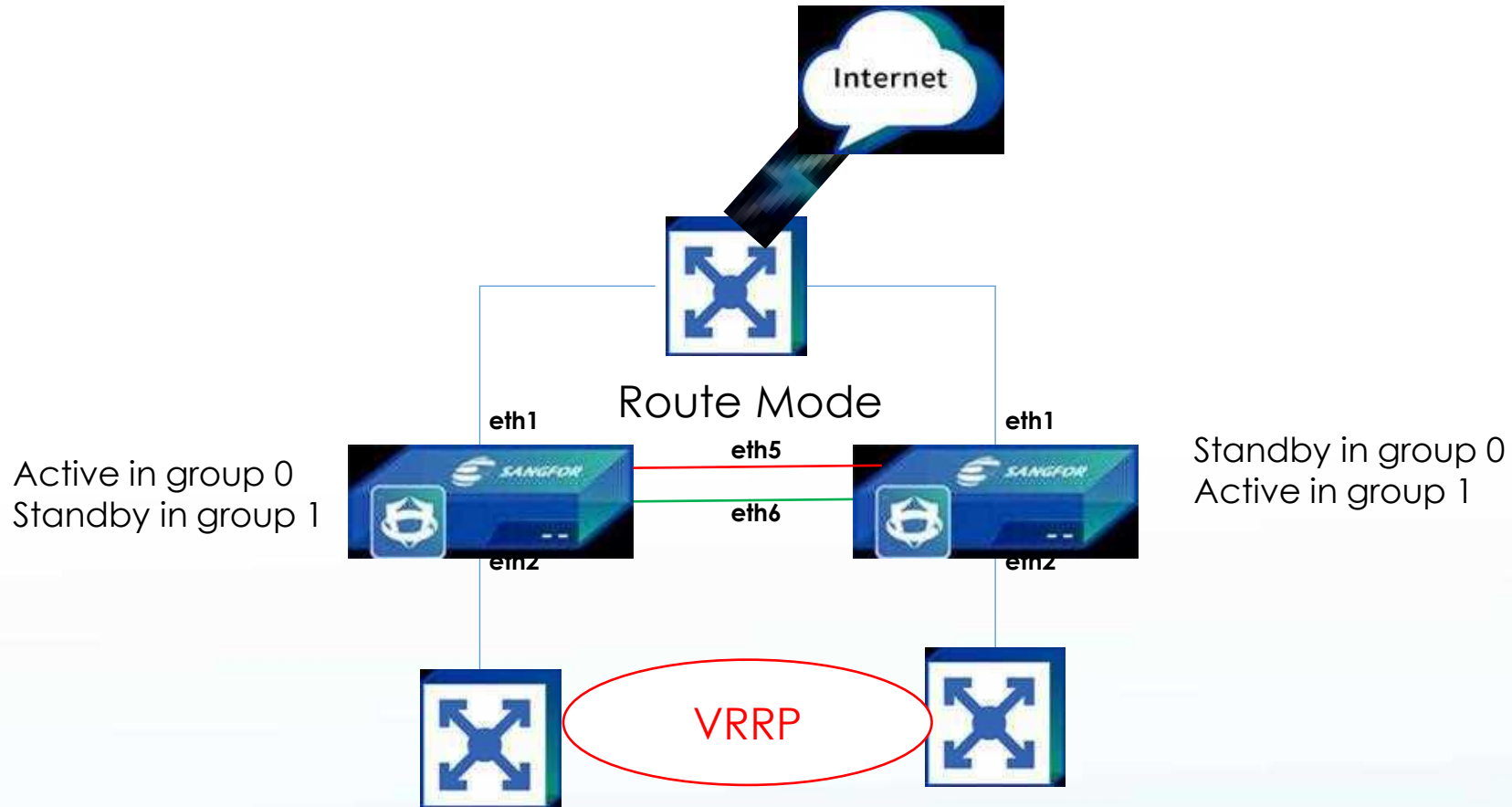
Auto Sync ⓘ: [Settings](#)

Sync Now ⓘ: [Sync Now](#) [View Logs](#)

Standby NSF

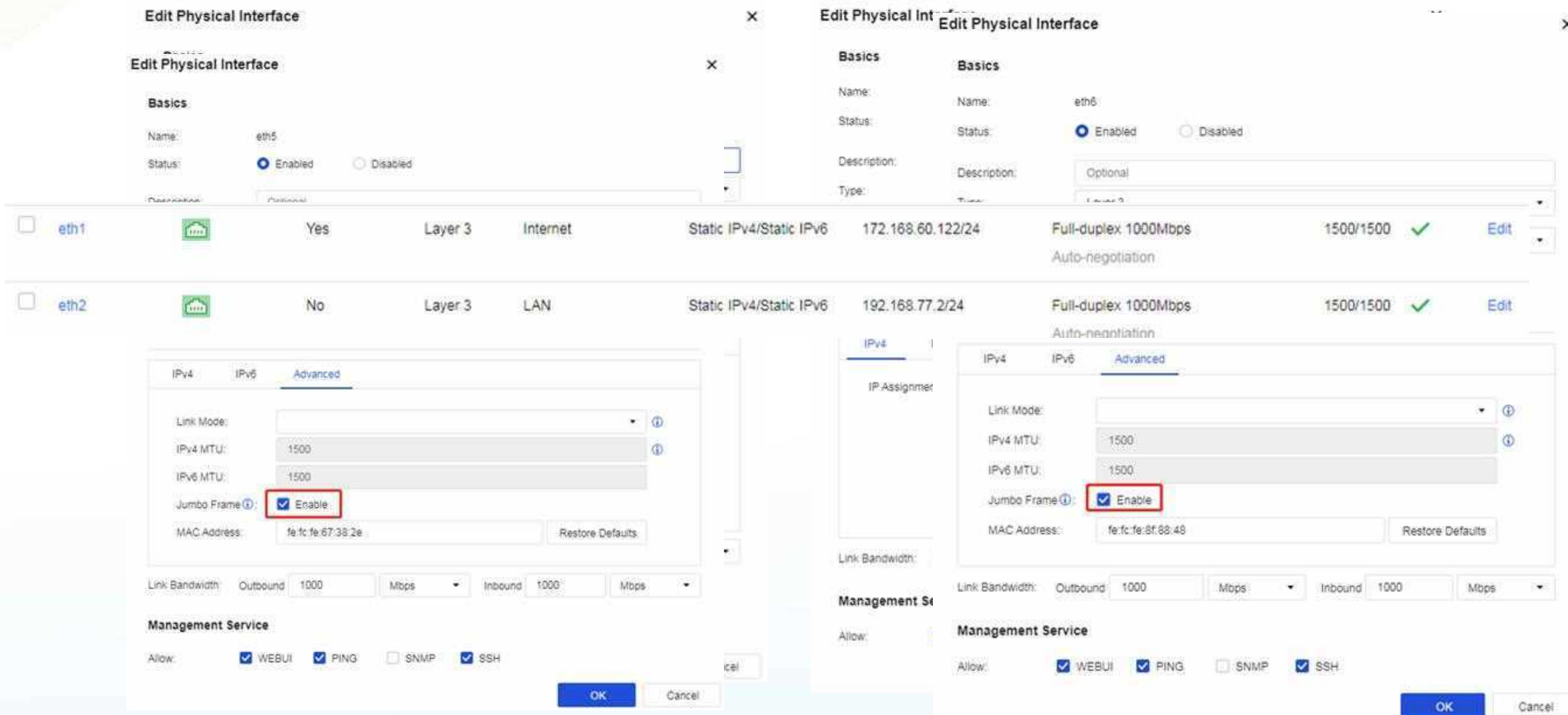
Case 3: Active/Active with Layer-3 Mode

A customer purchase 2 NSF to be deployed in egress of enterprise network and they require to achieve active/active mode for traffic load balance, besides downlink core switches is based on VRRP protocol.



Case 3: Active/Active with Layer-3 Mode

The first NSF business and high availability interfaces are configured as below.



The screenshot displays the Sangfor firewall configuration interface. At the top, there are multiple overlapping windows titled "Edit Physical Interface". Below these, a table lists the configured interfaces:

Interface	Icon	NSF	Mode	Interface Type	IP Address	Speed	MTU	Status	Action
eth1		Yes	Layer 3	Internet	Static IPv4/Static IPv6 172.168.60.122/24	Full-duplex 1000Mbps	1500/1500	✓	Edit
eth2		No	Layer 3	LAN	Static IPv4/Static IPv6 192.168.77.2/24	Full-duplex 1000Mbps	1500/1500	✓	Edit

Below the table, detailed configuration windows for eth1 and eth2 are shown. The "Advanced" tab for eth2 is highlighted, showing the following settings:

- Link Mode:
- IPv4 MTU: 1500
- IPv6 MTU: 1500
- Jumbo Frame: ☒ Enable
- MAC Address: fe:fc:fe:67:33:2e
- Link Bandwidth: Outbound 1000 Mbps, Inbound 1000 Mbps
- Management Service: Allow WEBUI, PING, SNMP, SSH

The "OK" button is visible at the bottom of the configuration window.

Case 3: Active/Active with Layer-3 Mode

It is necessary to configure link state propagation.

Physical Interfaces

Subinterfaces

VLAN Interfaces

Aggregate Interfaces

Local Loopback Interfaces

GRE Tunnels

Link State Propagation

☒ Enable link state propagation

+ Add

🗑 Delete

🔄 Refresh

<input type="checkbox"/>	Physical Interfaces	⬆	Operation	⬆
<input type="checkbox"/>	eth1, eth2		Edit	Delete

Case 3: Active/Active with Layer-3 Mode

In first NSF, configure setting of high availability.

← HA Policy Settings

HA Policy: **Group 0** **Group 1**

Mode:

Device Name: Description: Optional

Control Link ⓘ Priority: 200

Data Link ⓘ Proactive Preemption: ☒ Enable

Layer 2 Mode Preemption Delay: 3

HA Traffic: Virtual IP Addresses

Advanced: + Add | Delete Refresh

Interface	Virtual IP/Netmask
<input checked="" type="checkbox"/> eth1	172.168.60.121/24
<input checked="" type="checkbox"/> eth2	192.168.77.1/24

Monitored Object Management: Manage

Monitored Object ⓘ: business interface

Device Name: Description: Optional

Priority: 100

Proactive Preemption: ☒ Enable

Preemption Delay: 3

Virtual IP Addresses

+ Add | Delete Refresh Search

Interface	Virtual IP/Netmask	Virtual MAC	Operation	...
<input checked="" type="checkbox"/> eth1	172.168.60.124/24	00-00-5e-90-00-01	Edit Delete	
<input checked="" type="checkbox"/> eth2	192.168.77.4/24	00-00-5e-90-00-02	Edit Delete	

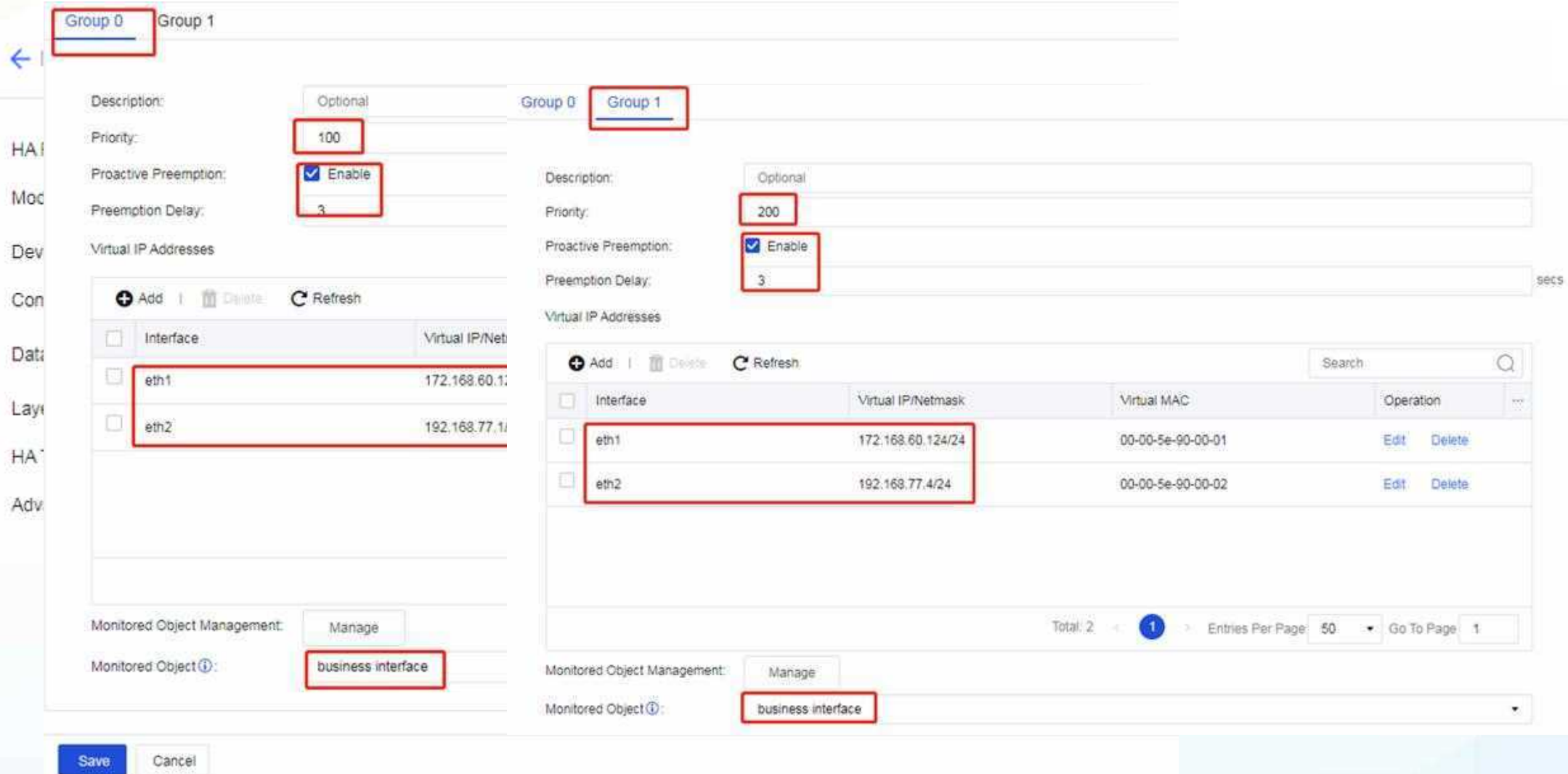
Total: 2 < 1 > Entries Per Page 50 Go To Page 1

Monitored Object Management: Manage

Monitored Object ⓘ: business interface

Case 3: Active/Active with Layer-3 Mode

The second NSF business and high availability interfaces are configured as below.



The screenshot displays the configuration interface for two groups, Group 0 and Group 1, in a Layer-3 mode. The interface is divided into two main panels, one for each group.

Group 0 Configuration:

- Description:** Optional
- Priority:** 100
- Proactive Preemption:** ☒ Enable
- Preemption Delay:** 3
- Virtual IP Addresses:**
 - Interface: eth1, Virtual IP/Netmask: 172.168.60.1/24
 - Interface: eth2, Virtual IP/Netmask: 192.168.77.1/24
- Monitored Object Management:** Manage
- Monitored Object:** business interface

Group 1 Configuration:

- Description:** Optional
- Priority:** 200
- Proactive Preemption:** ☒ Enable
- Preemption Delay:** 3
- Virtual IP Addresses:**
 - Interface: eth1, Virtual IP/Netmask: 172.168.60.124/24, Virtual MAC: 00-00-5e-90-00-01
 - Interface: eth2, Virtual IP/Netmask: 192.168.77.4/24, Virtual MAC: 00-00-5e-90-00-02
- Monitored Object Management:** Manage
- Monitored Object:** business interface

At the bottom of the interface, there are "Save" and "Cancel" buttons.

Case 3: Active/Active with Layer-3 Mode

The successful high availability status is shown as below.

High Availability

Settings | Refresh | Mode: Active/Active | Heartbeat Status: Normal



Group 0 Status: Active
Switch to Standby ⓘ
Group 1 Status: Passive
HA Status: Normal

Local Device Information Local Device

Device Name: HQ-NGAF
Control Link: eth5
Control Link 1: -
Data Link: eth6
Data Link 1: -
Monitored Interface Status: Normal
Member Interface Status: -
Uptime After Switchover: 0 days 0 hrs 7 mins [View Switchover Information](#)

Sync Options

Current Device Role: Active controller [Settings ⓘ](#)
Auto Sync ⓘ : [Settings](#)
Sync Now ⓘ : [Sync Now](#) [View Logs](#)

First NSF

High Availability

Settings | Refresh | Mode: Active/Active | Heartbeat Status: Normal



Group 0 Status: Passive
Group 1 Status: Active
Switch to Standby ⓘ
HA Status: Normal

Manage Peer Device

Group 0 Status: Active
Group 1 Status: Passive
HA Status: Normal

Local Device Information Local Device

Device Name: NSF
Control Link: eth5
Control Link 1: -
Data Link: eth6
Data Link 1: -
Monitored Interface Status: Normal
Member Interface Status: -
Uptime After Switchover: 0 days 0 hrs 8 mins [View Switchover Information](#)

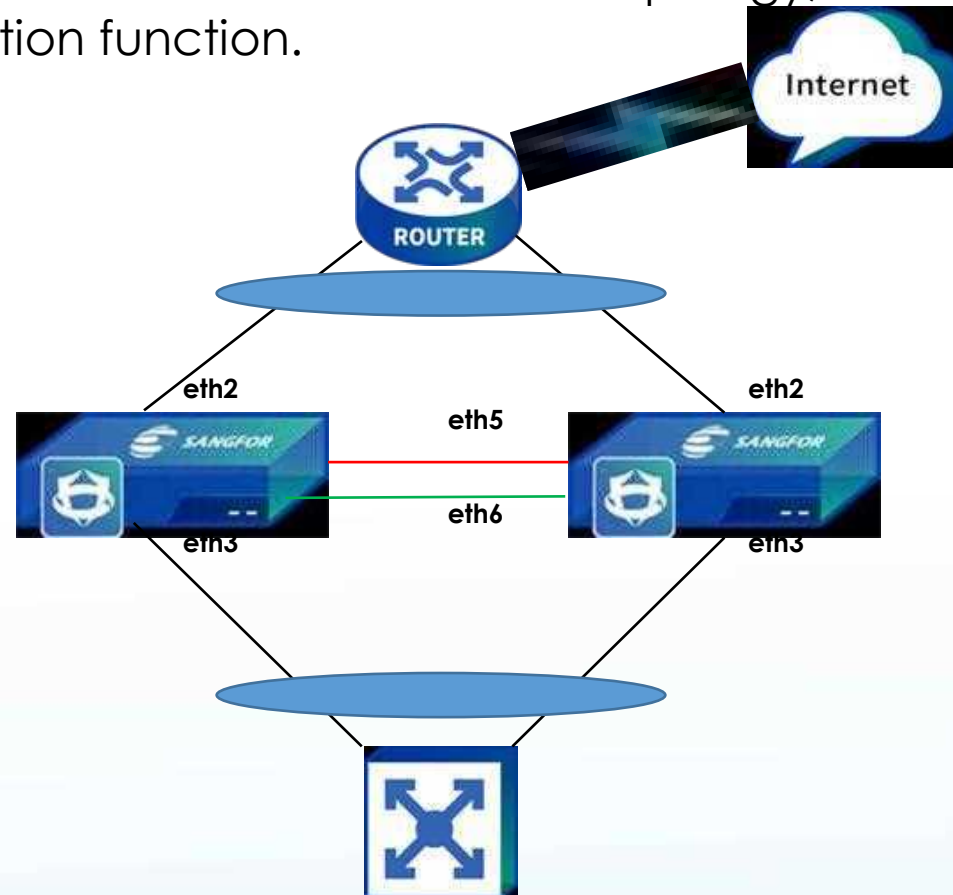
Sync Options

Current Device Role: Passive controller [Settings ⓘ](#)
Auto Sync ⓘ : [Settings](#)
Sync Now ⓘ : [Sync Now](#) [View Logs](#)

Second NSF

Case 4: Active/Active with Virtual Wire Mode

A customer's internal is connected by link aggregation from core switch to router. Now they purchase 2 NSF to be deployed in virtual wire mode between router and switch. Besides, 2 NSF need to work as active/active high availability mode. Given that there probably exists inconsistent business traffic in this topology, for 2 NSF it is necessary to configure link aggregation function.



Case 4: Active/Active with Virtual Wire Mode



In expected active controller NSF, business and high availability interfaces are configured as below.

Edit Physical Interface

Basics

Name: eth5

Status: ☒ Enabled

Description:

Edit Physical In

Basics

Name:

Status:

Description:

Edit Physical In

Basics

Name:

Status:

Description:

Edit Physical Interface

Basics

Name: eth6

Status: ☒ Enabled ☐ Disabled

Description: Optional

Type:	<input type="checkbox"/> eth2		Yes	Virtual wire	Virtual_untrust_A	-	-	Full-duplex 1000Mbps	1500/1500	✓	Edit
Zone:								Auto-negotiation			
Basic At	<input type="checkbox"/> eth3		No	Virtual wire	Virtual_untrust_A	-	-	Full-duplex 1000Mbps	1500/1500	✓	Edit
Reverse								Auto-negotiation			

IPv4

IPv6

Advanced

IP Assignment: ☒ Static

Static IP:

Default Gateway:

Link Bandwidth: Outbound 1000

Management Service: Allow: ☒ WEBUI ☒ PII

IPv4

Link Mode:

IPv4 MTU:

IPv6 MTU:

Jumbo Frame: ☒ Enable

MAC Address: fe:fc:fe:8f:88:48

Restore Defaults

Link Bandwidth: Outbound 1000 Mbps Inbound 1000 Mbps

Management Service: Allow: ☒ WEBUI ☒ PING ☐ SNMP ☒ SSH

OK

Cancel

Case 4: Active/Active with Virtual Wire Mode



In expected passive controller NSF, business and high availability interfaces are configured as below.

The image displays four screenshots of the 'Edit Physical Interface' configuration window, showing the configuration for interfaces eth5 and eth6. The configuration is divided into two main sections: Basics and Advanced.

Basics Section:

- Name:** eth5 (for the first two screenshots) and eth6 (for the last two).
- Status:** Enabled (radio button selected).
- Description:** Optional.
- Type:** Layer 3.
- Zone:** Control-Link (for eth5) and Data-Link (for eth6).
- Basic Attributes:** WAN attribute (checkbox unchecked).
- Reverse Routing:** Enabled (checkbox unchecked).

Advanced Section:

- IP Assignment:** Static (radio button selected).
- Static IP:** 172.16.98 (for eth6).
- Link Mode:** (dropdown menu).
- IPv4 MTU:** 1500.
- IPv6 MTU:** 1500.
- Jumbo Frame:** Enabled (checkbox checked, highlighted with a red box).
- MAC Address:** fe:fc:fe:7b:73:8c (for eth5) and fe:fc:fe:b5:be:48 (for eth6).
- Default Gateway:** (text field).

Management Service Section:

- Allow:** WEBUI (checkbox checked), PING (checkbox checked), and SSH (checkbox checked).

Link Bandwidth Section:

- Outbound:** 1000 Mbps.
- Inbound:** 1000 Mbps.

Buttons: OK and Cancel.

Case 4: Active/Active with Virtual Wire Mode



In expected active controller NSF, business and high availability interfaces are configured as below.

← | HA Policy Settings

HA Policy:

☒ Enable

Mode:

☐ Active/Standby

Device Name:

HQ-NGAF

Control Link ⓘ:

eth5

Data Link ⓘ:

eth6

Layer 2 Mode ⓘ:

☒ Enable

HA Traffic:

☐ Enable ⓘ

Link Aggregation ⓘ:

Settings

Link Aggregation

☒ Enable ⓘ

LAN Interfaces ⓘ

+ Add | Delete

<input type="checkbox"/> Local Interface	Peer Interface	Operation
<input type="checkbox"/> eth3	eth3	Delete

WAN Interfaces ⓘ

+ Add | Delete

<input type="checkbox"/> Local Interface	Peer Interface	Operation
<input type="checkbox"/> eth2	eth2	Delete

Save

Cancel

172.16.99.6

+

172.168.98.6

+

Case 4: Active/Active with Virtual Wire Mode



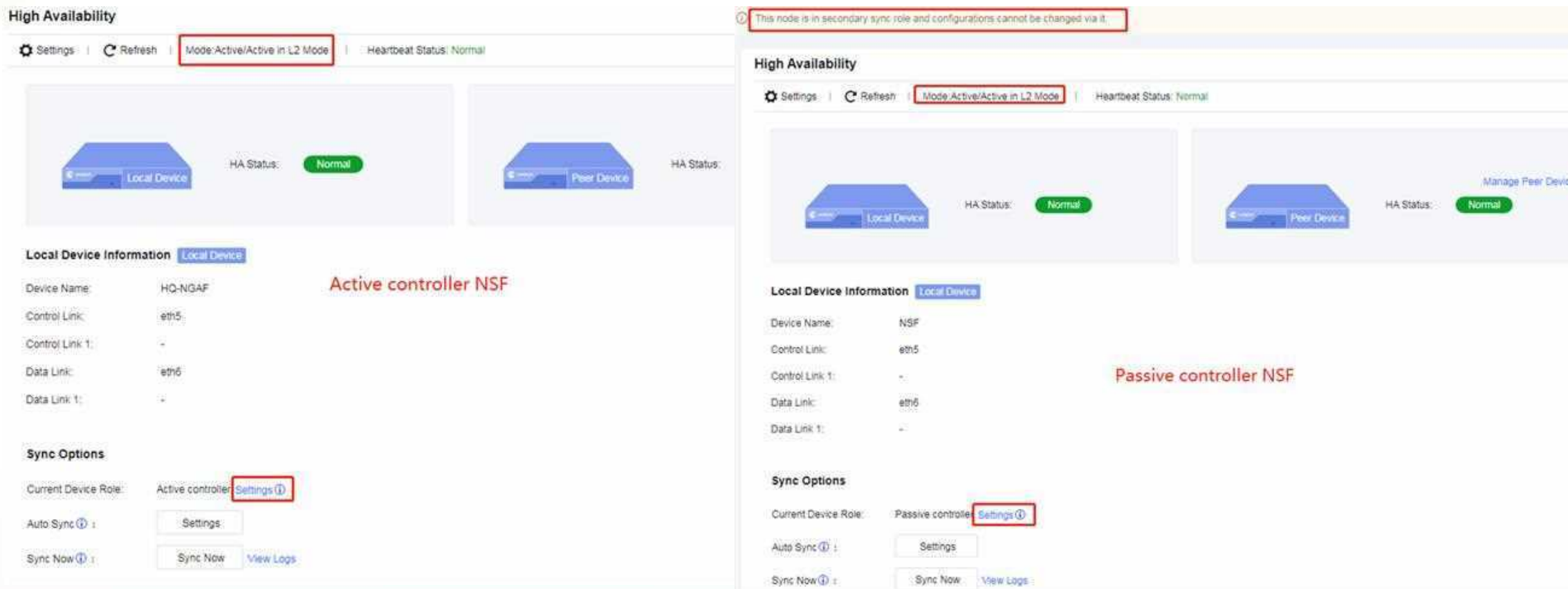
In expected passive controller NSF, business and high availability interfaces are configured as below.

← HA Policy Settings

HA Policy:	<input checked="" type="checkbox"/> Enable
Mode:	<input type="radio"/> Active/Standby <input checked="" type="radio"/> Active/Active
Device Name:	NSF
Control Link ⓘ:	<div>eth5 ▼</div> <div>Local 172.16.99.6 ▼ Peer 172.16.99.5 +</div>
Data Link ⓘ:	<div>eth6 ▼</div> <div>Local 172.16.98.6 ▼ Peer 172.16.98.5 +</div>
Layer 2 Mode ⓘ:	<input checked="" type="checkbox"/> Enable
HA Traffic:	<input type="checkbox"/> Enable ⓘ
Link Aggregation ⓘ:	<div>Settings</div>

Case 4: Active/Active with Virtual Wire Mode

The successful high availability status is shown as below.



The image displays two screenshots of the Sangfor NSP interface, illustrating the High Availability (HA) status for two devices in an Active/Active configuration with Virtual Wire Mode.

Left Screenshot (HQ-NGAF):

- High Availability:** Mode: Active/Active in L2 Mode, Heartbeat Status: Normal.
- Local Device Information:** Device Name: HQ-NGAF, Control Link: eth5, Data Link: eth6. **Active controller NSF**
- Sync Options:** Current Device Role: Active controller, Auto Sync: Settings, Sync Now: Sync Now, View Logs.

Right Screenshot (NSF):

- High Availability:** Mode: Active/Active in L2 Mode, Heartbeat Status: Normal. A warning message at the top states: "This node is in secondary sync role and configurations cannot be changed via it."
- Local Device Information:** Device Name: NSF, Control Link: eth5, Data Link: eth6. **Passive controller NSF**
- Sync Options:** Current Device Role: Passive controller, Auto Sync: Settings, Sync Now: Sync Now, View Logs.

Note:

In active/active with virtual wire mode, you are able to manually shift device role by clicking above "Setting".

- For inconsistent traffic scenario as well as active/active high availability mode, if interfaces of uplink and downlink devices NSF connected are route interfaces, it is necessary to turn on “HA traffic” feature, while in active/active with virtual wire mode, it is necessary to turn on “Link Aggregation” feature.
- You are suggested to enable “Jumbo Frame” feature for data link as well as control link interface for improving data forwarding efficiency.
- If uplink and downlink devices utilizes LACP mode link aggregation, the forwarding algorithm should be based on “source/destination IP”, otherwise there exists a chance that whole traffic may be inconsistent type.

THANK YOU

Technical Support Service

Email: tech.support@sangfor.com

Community: community.sangfor.com