

Grandstream Networks, Inc.

---

**GCC6000 Series**

VRRP User Guide



# Introduction to VRRP

The **Virtual Router Redundancy Protocol (VRRP)** is a powerful tool for ensuring network reliability and minimizing downtime. Typically deployed on egress gateway devices within a Local Area Network (LAN), VRRP creates a seamless failover mechanism by grouping multiple gateway devices into a virtual router. This virtual router serves as the default gateway for devices in the LAN, enabling uninterrupted connectivity even if one gateway device fails.

VRRP is particularly well-suited for small networks or scenarios with limited budgets, providing a cost-effective and simple solution for network redundancy.

## Key Features of VRRP:

- **Flexible Configuration Options:** Configure VRRP protocol message parameters to suit your network's needs.
- **Load Balancing:** Distribute traffic across multiple routers for improved performance and resource utilization.
- **Interface Support:** Configure VRRP on both **WAN** and **VLAN** interfaces to ensure comprehensive redundancy.
- **Synchronization Groups:** Switch the roles of a group (e.g., VLAN ↔ WAN) as a single unit for consistent failover.
- **VPN Compatibility:** WAN port VRRP supports synchronous switching of VPN services, ensuring secure and reliable connections.
- **Multi-Vendor Support:** Group VRRP-enabled devices from different manufacturers for enhanced flexibility.
- **Comprehensive Logs:** View detailed VRRP log information to monitor and troubleshoot your setup.
- **Protocol Support:** Compatible with both **VRRPv2** and **VRRPv3** protocols. (**Note:** IPv6 is not supported).

# Configuring a VRRP Group

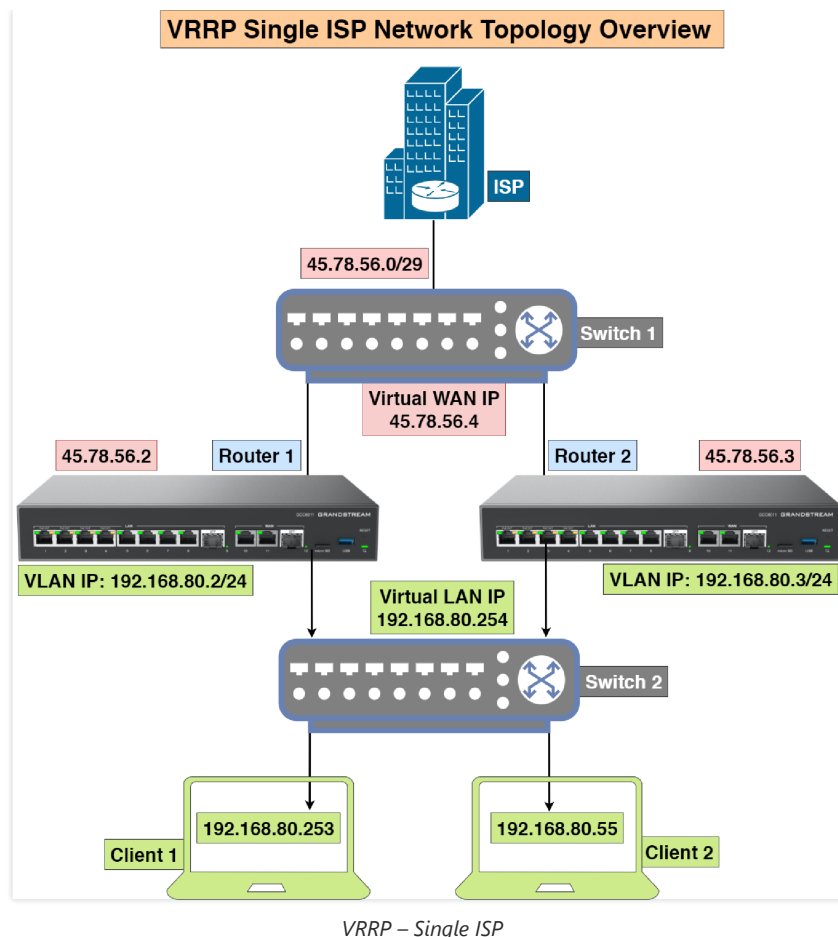
## Network Topology Overview

These two network topologies illustrate two VRRP implementation scenarios: one involving a single ISP and the other utilizing dual ISPs.

### VRRP with a Single ISP:

In a **single ISP** environment, deploying two routers configured with VRRP enhances network reliability and ensures continuous service. The **primary Router 1**, acting as the master VRRP router, handles all network traffic during normal operations. The **secondary Router 2** remains on standby, ready to assume control automatically in the event of a hardware failure, scheduled maintenance, or unexpected outages.

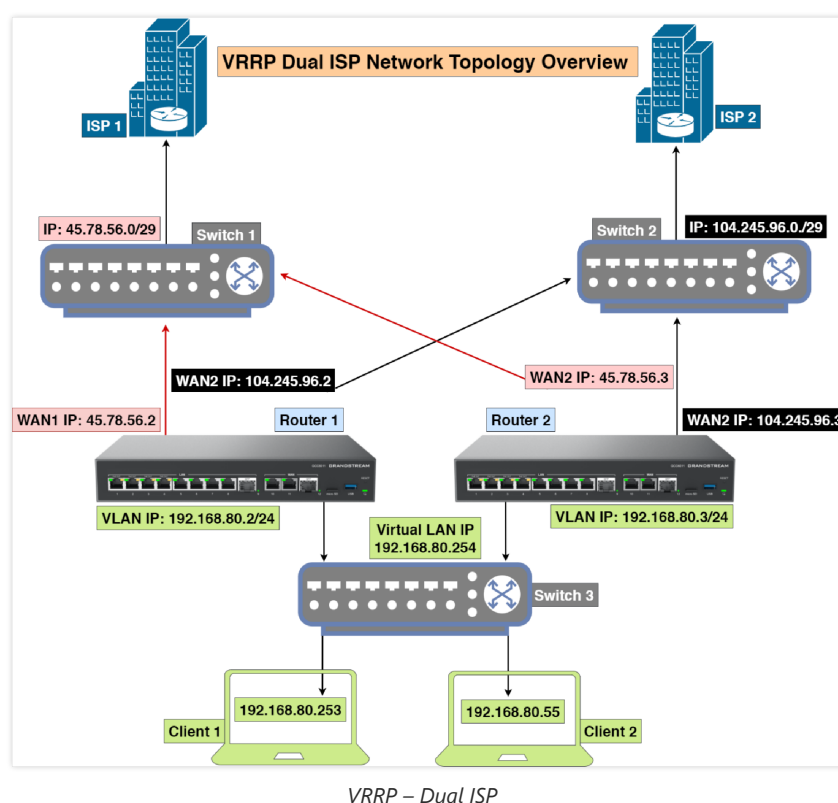
This setup significantly boosts network availability by reducing potential downtime. Seamless role switching between the master and backup devices ensures uninterrupted connectivity, maintaining critical services without manual intervention. Additionally, this redundancy improves fault tolerance and adds a layer of resilience to the overall network infrastructure.



#### VRRP with dual ISP:

In a **dual ISP** setup, two routers configured with VRRP not only provide redundancy at the device level but also enhance network resilience by leveraging **multiple ISP connections**. Each router connects to a **separate ISP**, ensuring that even if one ISP experiences an outage, the network can seamlessly failover to the secondary connection.

Unlike the single ISP configuration, this setup improves both availability and performance by enabling load balancing across ISPs. The master VRRP router manages traffic distribution, while the backup router remains in standby, ready to take over in case of device failure or network disruptions. This dual-path redundancy minimizes downtime, increases fault tolerance, and ensures high availability, offering uninterrupted connectivity even during ISP-level issues.

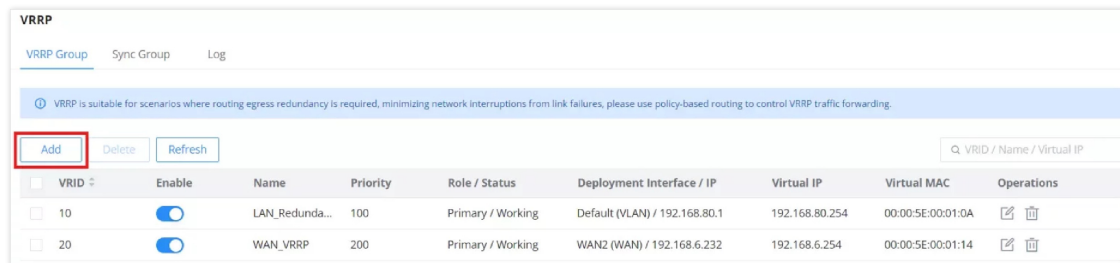






## VRRP group

To properly configure and activate a VRRP group, follow these steps:

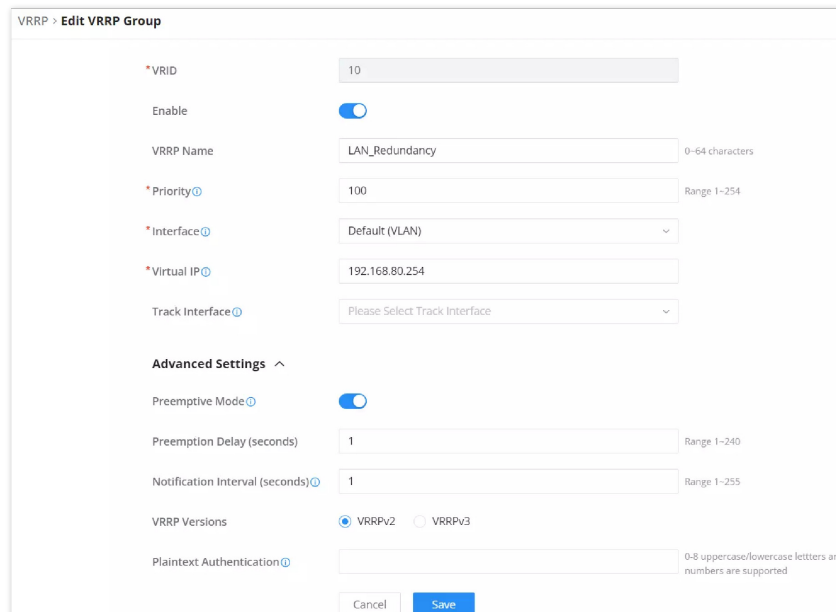
1. Navigate to **GCC WebUI** → **VRRP page** then **create the VRRP group**.
2. Configure the following key settings:
  - **VRID**: Set the unique Virtual Router ID for the group.
  - **Priority**: Assign the priority level to determine the primary device.
  - **Deployment Interface**: Select the interface where VRRP will operate.
  - **Virtual IP Address**: Specify the shared floating IP for the group.
3. **Enable the VRRP group** to ensure it functions as intended.

Please refer to the figures and table below for more details:



VRID	Enable	Name	Priority	Role / Status	Deployment Interface / IP	Virtual IP	Virtual MAC	Operations
10	<input checked="" type="checkbox"/>	LAN_Redunda...	100	Primary / Working	Default (VLAN) / 192.168.80.1	192.168.80.254	00:00:5E:00:01:0A	 
20	<input checked="" type="checkbox"/>	WAN_VRRP	200	Primary / Working	WAN2 (WAN) / 192.168.6.232	192.168.6.254	00:00:5E:00:01:14	 

VRRP Group page



**VRRP > Edit VRRP Group**

\*VRID: 10

Enable: ☒

VRRP Name: LAN\_Redundancy (0-64 characters)

\*Priority: 100 (Range 1-254)

\*Interface: Default (VLAN)

\*Virtual IP: 192.168.80.254

Track Interface: Please Select Track Interface

**Advanced Settings**

Preemptive Mode: ☒

Preemption Delay (seconds): 1 (Range 1-240)

Notification Interval (seconds): 1 (Range 1-255)

VRRP Versions: ☒ VRRPv2 ☐ VRRPv3

Plaintext Authentication: (0-8 uppercase/lowercase letters and numbers are supported)

Cancel Save

Add/Edit VRRP Group

Field	Description
VRID	Specifies the Virtual Router ID for the VRRP group. Each VRRP group must have a unique VRID, and devices within the same group must use the same VRID. A single device cannot have duplicate VRIDs.
Enable	Enables or disables the VRRP group. Toggle this option to activate VRRP for the specified configuration.
VRRP Name	Assigns a descriptive name to the VRRP group. If left blank, the system uses a default format: VRRP+VRID (e.g., VRRP10).
Priority	Determines the router's priority within the VRRP group. The router with the highest priority becomes the primary device. In case of a tie, the router with the larger interface IP address takes precedence.

<b>Interface</b>	Selects the network interface where VRRP will operate. Options include Default (VLAN) for LAN redundancy and WAN for egress redundancy. Each interface can only belong to one VRRP group.
<b>Virtual IP</b>	The Virtual IP (VIP) must be in the same subnet as the deployment interface but cannot match the interface's assigned IP. For VLAN interfaces, the VIP should be the default gateway for devices in the VLAN, ensuring seamless failover.
<b>Track Interface</b>	Monitors the status of uplink interfaces (e.g., WAN). If all tracked interfaces are down, the router relinquishes its primary role.
<b>Advanced Settings</b>	
<b>Preemption Mode</b>	Allows a backup router with a higher priority to preempt the current primary router.
<b>Preemption Delay (seconds)</b>	Specifies the time (default: 1 second) to wait before initiating preemption. This minimizes disruptions caused by transient network issues.
<b>Notification Interval (seconds)</b>	Sets the frequency at which the primary router sends VRRP advertisements. All routers in the VRRP group must use the same interval to ensure proper synchronization.
<b>VRRP Versions</b>	Configures the VRRP version: VRRPv2 supports IPv4 networks, while VRRPv3 supports both IPv4 and IPv6. Note: IPv6 is currently not supported.
<b>Plaintext Authentication</b>	Enables authentication to secure VRRP communication and prevent unauthorized devices from joining the group. Both primary and backup devices must use the same authentication string. Only supported in VRRPv2.

#### Add/Edit VRRP Group

**GCC 1: Primary:** create two VRRP Groups, one for LAN and another one for WAN with high priority.

VRRP									
<a href="#">VRRP Group</a> <a href="#">Sync Group</a> <a href="#">Log</a>									
<i> ⓘ VRRP is suitable for scenarios where routing egress redundancy is required, minimizing network interruptions from link failures, please use policy-based routing to control VRRP traffic forwarding.</i>									
<div> <a href="#">Add</a>   <a href="#">Delete</a>   <a href="#">Refresh</a> </div> <div>Q. VRID / Name / Virtual IP</div>									
<input type="checkbox"/> VRID ⚙	Enable	Name	Priority	Role / Status	Deployment Interface / IP	Virtual IP	Virtual MAC	Operations	
<input type="checkbox"/> 10	<input checked="" type="checkbox"/>	LAN_Redunda...	100	Primary / Working	Default (VLAN) / 192.168.80.1	192.168.80.254	00:00:5E:00:01:0A	<a href="#">✎</a>	<a href="#">🗑</a>
<input type="checkbox"/> 20	<input checked="" type="checkbox"/>	WAN_VRRP	200	Primary / Working	WAN2 (WAN) / 192.168.6.232	192.168.6.254	00:00:5E:00:01:14	<a href="#">✎</a>	<a href="#">🗑</a>

#### GCC 1 – Primary

**GCC 2: Secondary:** create two VRRP Groups, one for LAN and another one for WAN with lower priority.

VRRP									
<a href="#">VRRP Group</a> <a href="#">Sync Group</a> <a href="#">Log</a>									
<i> ⓘ VRRP is suitable for scenarios where routing egress redundancy is required, minimizing network interruptions from link failures, please use policy-based routing to control VRRP traffic forwarding.</i>									
<div> <a href="#">Add</a>   <a href="#">Delete</a>   <a href="#">Refresh</a> </div> <div>Q. VRID / Name / Virtual IP</div>									
<input type="checkbox"/> VRID ⚙	Enable	Name	Priority	Role / Status	Deployment Interface / IP	Virtual IP	Virtual MAC	Operations	
<input type="checkbox"/> 10	<input checked="" type="checkbox"/>	LAN_Redunda...	80	Secondary / Working	Default (VLAN) / 192.168.80.1	192.168.80.254	00:00:5E:00:01:0A	<a href="#">✎</a>	<a href="#">🗑</a>
<input type="checkbox"/> 20	<input checked="" type="checkbox"/>	WAN_VRRP	80	Secondary / Working	WAN2 (WAN) / 192.168.6.26	192.168.6.254	00:00:5E:00:01:14	<a href="#">✎</a>	<a href="#">🗑</a>

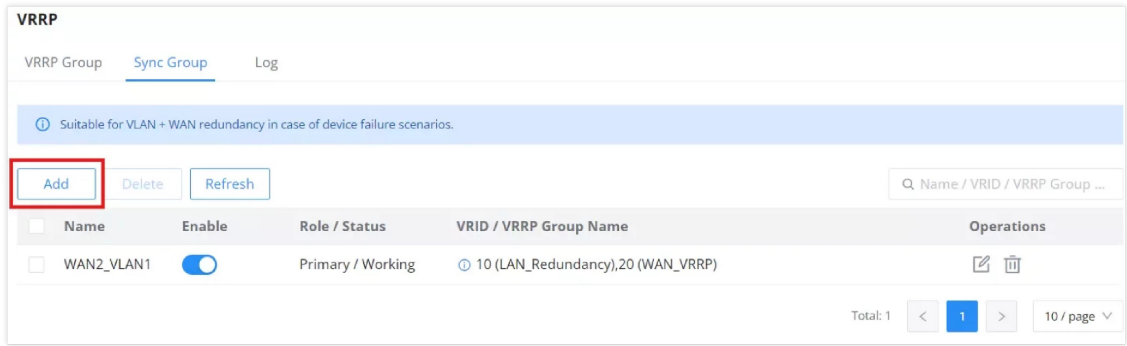
#### GCC 2 – Secondary

## VRRP Synchronization Group

A VRRP synchronization group ensures that all VRRP instances within the group maintain synchronized states. If one instance changes its role, the other instances in the group automatically transition to the same role.

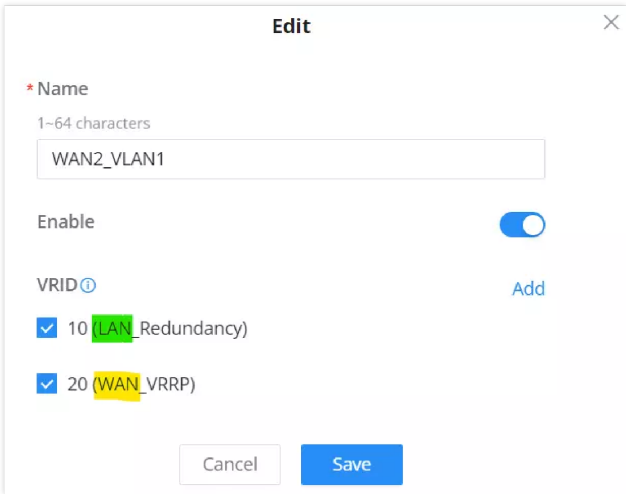
When VLAN and WAN interfaces are part of a synchronization group, policy routing must be implemented in conjunction to ensure proper functionality.

To add Sync Group, Navigate to **VRRP** → **Sync Group** then click on the **"Add"** button as shown below:



VRRP – Sync Group

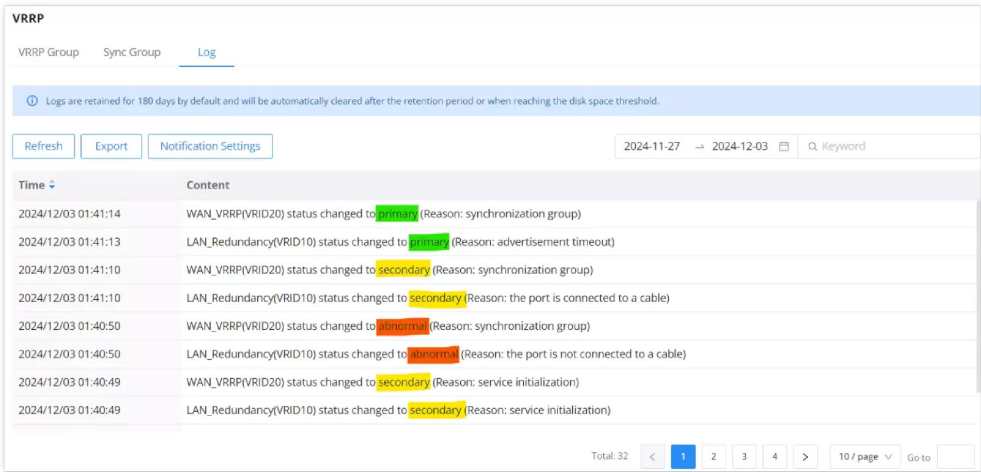
Select the VRRP Groups (WAN/LAN) combination.



VRRP – Add Sync Group

VRRP Logs

VRRP logs capture events and status changes during the operation of VRRP instances. They provide critical insights for monitoring instance behavior, diagnosing issues, and troubleshooting effectively.



VRRP – Log

Examples Using Two GCC Devices

Below are scenarios demonstrating the effective use of two Grandstream GCC devices, showcasing their combined capabilities and benefits.

**Note:**

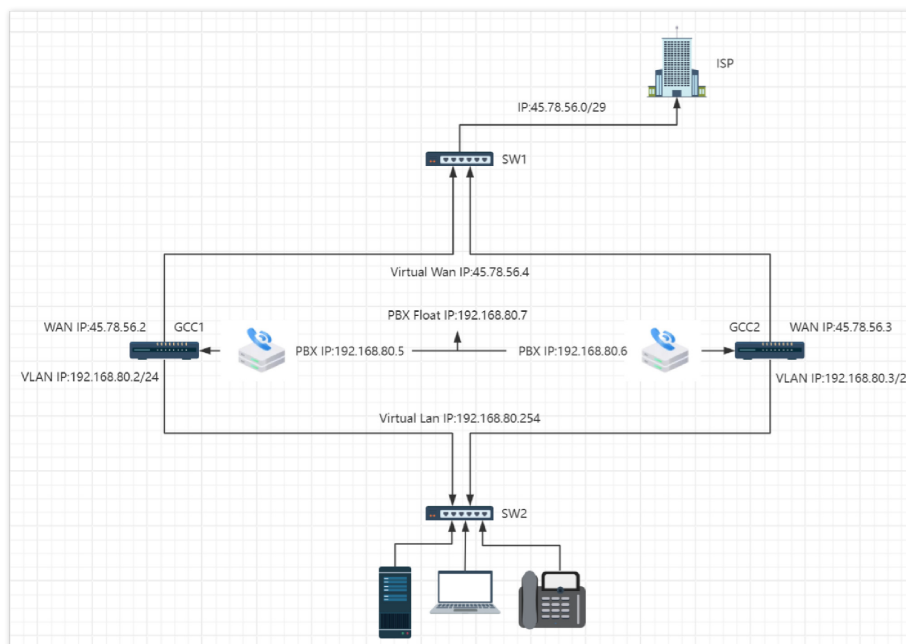
While this guide focuses on configuring VRRP with Grandstream GCC6000 series devices, it is important to note that VRRP is a standardized protocol defined by RFC 5798. As such, it is designed to work across devices from different manufacturers that also support VRRP. To ensure compatibility, make sure that key configuration parameters such as VRID, Virtual IP, Preemption Mode, and authentication settings are consistent across all devices, regardless of the manufacturer.

## Single ISP Usage Scenario

In a single ISP environment, two GCC devices can be deployed using VRRP to ensure network reliability. One device functions as the master VRRP router, managing traffic under normal conditions, while the second serves as a backup, ready to take over in case of failure or maintenance.

This configuration provides high availability and minimizes downtime, ensuring uninterrupted connectivity through seamless role-switching between the devices.

## Network Topology (Single ISP)



VRRP – Single ISP – Two GCC devices

In the topology shown, GCC1 is initially configured as the Primary router, while GCC2 serves as the Secondary. The ISP has allocated a public network segment of 45.78.56.0/29. After enabling VRRP on the WAN interface, intranet services can be accessed via the virtual IP address 45.78.56.4. On the internal LAN, the gateway IP is configured as 192.168.80.254.

### Initial State

GCC1, as the Primary node, handles both intranet access and internet connectivity. If GCC1 experiences a failure (such as a system freeze, power outage, or LAN port disconnection), GCC2 automatically assumes the Primary role. This ensures continued access to both the intranet and the Internet without interruption.

### Virtual IP Address Management

- **Intranet Gateway:** The gateway IP (192.168.80.254) is only active on the Primary router. This IP is exclusive to either GCC1 or GCC2, depending on the active Primary role.
- **External Network Access:** Similarly, the virtual WAN IP (45.78.56.4) is assigned only to the active Primary router.

### Failover Process

When GCC1 fails, VRRP seamlessly transfers the virtual WAN IP and virtual VLAN gateway IP to GCC2. A gratuitous ARP is broadcast to refresh the ARP table on the connected switch, enabling the switch to forward traffic to GCC2. This transition from Secondary to Primary is virtually transparent, ensuring clients and the ISP experience no service disruptions due to unchanged IP addresses.

### Notes:

- **WAN VRRP Considerations:** If the ISP provides fewer than three IP addresses, enabling VRRP on the WAN interface is not recommended.
- **Switch Configuration:**
  - Both routers' WAN interfaces must be connected to the same switch, and their VLAN interfaces should also be connected to the same switch for proper communication. Please refer to the [topology above](#).
  - If the switch has Spanning Tree Protocol (STP) enabled to prevent loops, the ports may not immediately enter the forwarding state. This delay can influence the VRRP role election process, potentially affecting failover performance.

## GCC1 Configuration (Single ISP)

### 1. Add WAN VRRP Group

To configure WAN VRRP, create a VRRP group and select WAN1 as the deployment interface. Ensure the following parameters match the settings on the WAN\_VRRP interface of the GCC2 router: VRID, Virtual IP, Preemption Mode, VRRP Version, and plaintext authentication. Set the WAN\_VRRP priority for GCC1 to 100 and for GCC2 to 80. With this configuration, GCC1 will assume the Primary role for WAN\_VRRP.

To begin the configuration, navigate to **Networking** → **VRRP** → **Add VRRP Group**.

The screenshot shows the 'VRRP > Add VRRP Group' configuration window. The fields are as follows:

Field	Value	Range/Constraint
*VRID	1	Range 1-255
Enable	<input checked="" type="checkbox"/>	
VRRP Name	VRRP 1	0-64 characters
*Priority	100	Range 1-254
*Interface	WAN1 (WAN)	
*Virtual IP	45.78.56.4	
Track Interface	Please Select Track Interface	

At the bottom, there is an 'Advanced Settings' dropdown, a 'Cancel' button, and a 'Save' button.

Add WAN VRRP Group

### 2. Add VLAN VRRP Group

To configure VLAN VRRP, create a VRRP group and select any VLAN as the deployment interface. Ensure that the following parameters match the VLAN\_VRRP configuration on the GCC2 router: VRID, Virtual IP, Preemption Mode, VRRP Version, and plaintext authentication. Set the VLAN\_VRRP priority of GCC1 to 100 and GCC2 to 80, making GCC1 the Primary for VLAN VRRP.

Additionally, configure the **Track Interface** to WAN1 to enable automatic role switching between Primary and Secondary in the event of a failure on the uplink interface of the Primary device, preventing service disruption.

To begin the configuration, navigate to **Networking** → **VRRP** → **VRRP Group**.



*Add LAN VRRP Group*

### 3. Configuring a VRRP Synchronization Group

To ensure seamless failover, the WAN and LAN interfaces should be synchronized. Add both the WAN and VLAN interfaces on the router to the same synchronization group. When one interface switches roles, the other will automatically follow, ensuring consistent performance.

To configure the synchronization group, navigate to **Networking** → **VRRP** → **Sync Group**.

*Configuring a VRRP Synchronization Group*

#### Note:

Set the VLAN port according to the actual network configuration. If the port associated with the VLAN has no cable connected, the VLAN link is considered abnormal. As a result, the VLAN VRRP state will switch to "abnormal," triggering the WAN role in the synchronization group to also switch to "abnormal." For example, when the NET1, NET3-NET4, and NET6-NET7 ports on the GCC device have no network cable connected, the VLAN80 VRRP state will be marked as abnormal.

To configure VLAN port settings, navigate to **Networking** → **Network Settings** → **LAN**.

LAN		
VLAN	PBX Trunk VLAN	<u>VLAN Port Settings</u>
Static IP Binding		
Local DNS Records		
Bonjour Gateway		
Port	PVID	Allowed VLANs
NET1 (GE)	80	1,10,80
NET2 (GE)	10	10
NET3 (GE)	1	1,10,80
NET4 (GE)	1	1,10,80
SFP6 (SFP)	1	1,10,80
SFP7 (SFP)	1	1,10,80

GCC – VLAN Port Settings

#### 4. Modify VLAN gateway address

If the DHCP service is enabled for the corresponding VLAN, users can change the gateway address to a virtual IP address, such as 192.168.80.254.

For clients with static IP configurations, users can manually set the gateway to the specified virtual IP address.

To configure the VLAN gateway, navigate to **Networking → Network Settings → LAN**.

VRRP – Modify the gateway

#### 5. Configuring Policy Routing

The load balancing policy pool is a configuration used to implement load balancing and failover across multiple WAN ports, which will be referenced in policy routing. Users can select the appropriate policy mode based on their requirements: **Load Balancing** or **Backup Mode**.

- **Load Balancing:** Traffic is distributed across interfaces in proportion to the set load balancing weights. Ensure weights are allocated based on actual bandwidth to optimize performance.
- **Backup Mode:** In this mode, when the preferred interface fails, traffic will automatically switch to the backup interface. Both interfaces can share traffic based on the load balancing weights to ensure uninterrupted network connectivity.

In this configuration, **Backup Mode** is selected. By default, VLAN traffic will route through the **WAN1 VRRP interface**. If the **WAN1 VRRP interface** fails, traffic will be directed to the **WAN1 interface**.

To view or configure policy routes, navigate to **Networking → Routing → Policy Routes**.

Policy Routes > **Edit Load Balance Rule**

\*Name: Default

Mode: ☐ Load Balance ☒ Backup

Balancing Strategy: Connection-Based

\*Preferred Interface: Interface: WAN1 (WAN VRRP) Weight: 1

\*Alternate Interface: Interface: WAN1 (WAN) Weight: 1

Buttons: Cancel, Save

Add Load Balance Rule

Policy Routes > **Add Policy Route**

\*Name: VLAN80 → WAN1\_VRRP

Enable: ☒

IP Family: ☒ Any ☐ IPv4

Protocol Type: All

Source Group: Default (VLAN)

Source IP Address:

Destination IP Address:

Load Balance: WAN1\_VRRP

Schedule: None

Buttons: Cancel, Save

Add Policy Route

## 6. Configure VPN

After setting up WAN VRRP, users can select the WAN VRRP interface for VPN configuration.

For example, when configuring an OpenVPN® server, select the interface as WAN1 (WAN VRRP). In this case, the WAN1 VRRP interface on the GCC1 device will be active, and the OpenVPN® server service will be supported by the GCC1 device.

To configure the OpenVPN® server, navigate to **Networking → VPN → OpenVPN®**:

OpenVPN® > **Add OpenVPN® Server**

\*Name: Open\_Server\_VRRP\_GCC1

Enable: ☒

Protocol: ☒ UDP ☐ TCP

Interface: WAN1 (WAN VRRP)

Destination: All

\*Local Port: 1194

Server Mode: SSL

Encryption Algorithm: AES-256-CBC

Digest Algorithm: SHA256

OpenVPN® Server – VRRP Interface

OpenVPN®

OpenVPN® Clients OpenVPN® Servers

Buttons: Add, Delete

<input type="checkbox"/>	Name	Enable	Interface	Server Address	Uptime	Operations
<input type="checkbox"/>	open_server_vrrp_gcc1	<input checked="" type="checkbox"/>	WAN1 (WAN VRRP)	192.168.3.6	4s	

**Note:**

If the VPN is configured with a VRRP interface, the VPN will take effect only when the VRRP is active (Primary).

## 7. Configure port forwarding

External network users can access internal web services via the virtual IP 45.78.56.4 on the GCC device.

Configure the port forwarding function on both GCC1 and GCC2. External users will be able to access the web page of the PC (192.168.80.213) in VLAN 80 by using the URL: <http://45.78.56.4:10000>.

To configure port forwarding, navigate to **Networking → External Access → Port Forwarding**:

Port Forwarding > Add Port Forwarding

\*Name: Apache\_test (1-64 characters)

Enable: ☒

Protocol Type: ☒ TCP/UDP ☐ TCP ☐ UDP

Interface: WAN1 (WAN VRRP)

Source IP Address:

\*Source Port: 10000 (The valid range is 1-65535. You can enter a single port or a port range.)

Destination Group: Default LAN

\*Destination IP Address: 192.168.80.213

\*Destination Port: 80 (The valid range is 1-65535. You can enter a single port or a port range.)

Cancel Save

VRRP interface with Port Forwarding

## 8. Configuring Firewall Rules

Users can configure firewall rules for the WAN\_VRRP interface based on specific requirements.

For example, when configuring forwarding rules, both GCC1 and GCC2 devices should define forwarding rules where the **Source Group** is set to the WAN VRRP interface, the **Destination Group** is set to the VLAN where the PC is located, and the **Destination IP Address** is the accessible IP (e.g., 192.168.80.213). This configuration allows external users to access the web page hosted on the PC in the internal subnet.

To configure forwarding rules, navigate to **Firewall → Firewall Policy → Traffic Rules**.

Traffic Rules > Add Forwarding Rule

\*Name: WAN VRRP->VLAN80 (1-64 characters)

Enable: ☒

IP Family: ☒ Any ☐ IPv4 ☐ IPv6

Protocol Type: All

\*Source Group: WAN1 (WAN VRRP)

Source MAC Address:

Source IP Address: 45.78.56.4 (Enter the IP address/mask length, such as "192.168.122.0/24")

\*Destination Group: Default LAN (VLAN) x

Destination IP Address: 192.168.80.213 (Enter the IP address/mask length, such as "192.168.122.0/24")

Action: ☒ Accept ☐ Deny ☐ Drop

Cancel Save

VRRP Interface with Firewall

**Note:**

Users can add a route to the ISP in advance with the destination address 192.168.80.213 and the next hop being the GCC virtual IP address 45.78.56.4.

## GCC2 Configuration (Single ISP)

## 1. Add WAN VRRP Group

Set the WAN\_VRRP priority of GCC1 to 100 and the **WAN\_VRRP priority of GCC2 to 80**. GCC2 WAN\_VRRP will become **Secondary**.

To configure WAN VRRP, please navigate to **Networking → VRRP → VRRP Group**:

The screenshot shows the 'VRRP > Edit VRRP Group' configuration page. The settings are as follows:

- \*VRID: 1
- Enable: ☒
- VRRP Name: WAN (0-64 characters)
- \*Priority: 80 (Range: 1-254)
- \*Interface: WAN (WAN) (dropdown)
- \*Virtual IP: 45.78.56.4
- Track Interface: Please Select Track Interface (dropdown)
- Advanced Settings** (expanded):
  - Preemptive Mode: ☐
  - Notification Interval (seconds): 1 (Range: 1-255)
  - VRRP Versions: ☒ VRRPv2 ☐ VRRPv3
  - Plaintext Authentication: (empty field, 0-8 uppercase/lowercase letters and numbers are supported)

Buttons: Cancel, Save

GCC2 Configuration – VRRP WAN

## 2. Add VLAN VRRP Group

Set the VLAN\_VRRP priority of GCC1 to 100 and **the VLAN\_VRRP priority of GCC2 to 80**. GCC2 VLAN\_VRRP will become **Secondary**.

To configure VLAN VRRP, please navigate to **Networking → VRRP → VRRP Group**:

The screenshot shows the 'VRRP > Edit VRRP Group' configuration page. The settings are as follows:

- \*VRID: 80
- Enable: ☒
- VRRP Name: VLAN80 (0-64 characters)
- \*Priority: 80 (Range: 1-254)
- \*Interface: Default LAN (VLAN) (dropdown, highlighted with a red box)
- \*Virtual IP: 192.168.80.254
- Track Interface: WAN (WAN) x (dropdown)
- Advanced Settings** (expanded):
  - Preemptive Mode: ☐
  - Notification Interval (seconds): 1 (Range: 1-255)
  - VRRP Versions: ☒ VRRPv2 ☐ VRRPv3
  - Plaintext Authentication: (empty field, 0-8 uppercase/lowercase letters and numbers are supported)

Buttons: Cancel, Save

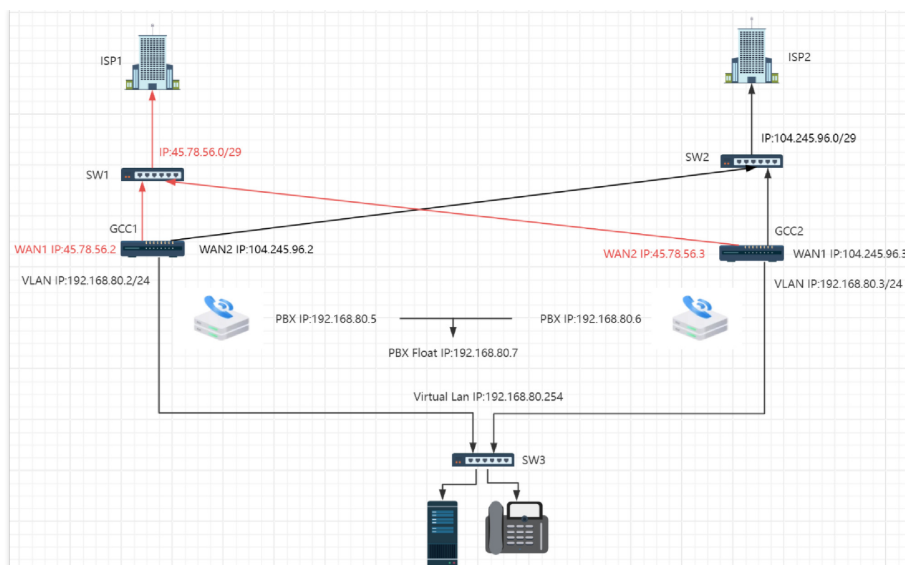
GCC 2 – VRRP VLAN Group

The rest of the steps are similar to the [GCC 1 configuration](#).

## Dual ISP usage scenario

### Network Topology (Dual ISP)

In this topology, we have now two ISPs with different IP segments as shown below:



Dual ISP & Two GCC devices

GCC1 is initially configured as the Primary router, and GCC2 is the Secondary. Two ISPs provide separate network segments: **45.78.56.0/29** and **104.245.96.0/29**, both of which can independently access the Internet. The internal LAN uses **192.168.80.254** as the gateway IP.

### Failover and Role Switching

- **Initial State:** GCC1, as the Primary, handles all network services.
- **ISP Failover:** If one of GCC1's ISP services fails, the WAN port failover feature automatically switches to the other WAN port for continued Internet access.
- **Device Failover:** If both ISP connections on GCC1 fail, or if GCC1 encounters hardware issues (e.g., freeze, power outage, or LAN port failure), VRRP triggers a role switch, promoting GCC2 to the Primary role to continue providing network services.

### Notes:

1. **WAN VRRP Considerations:** When using dual WAN, it is recommended to rely on the WAN failover feature for network switching rather than enabling the WAN VRRP feature.
2. **Independent ISP Access:** Both ISP-provided IP ranges can access the Internet independently.
3. **Switch Configuration:**
  - VLANs of both routers must connect to the same switch.
  - WAN ports on both routers should be configured to match the settings required by each ISP, including VPN, policy routing, and port forwarding.
4. **STP Impact:** If the switch uses the Spanning Tree Protocol (STP) to prevent loops, its ports may take time to enter the forwarding state, potentially delaying VRRP role elections.

### GCC1 Configuration (Dual ISP)

#### 1. Add VLAN VRRP Group

- Add a VRRP group and select a VLAN as the deployment interface.
- Ensure that the following settings match those configured on the VLAN\_VRRP interface of GCC2:
  - **VRID**
  - **Virtual IP**
  - **Preemption Mode**
  - **VRRP Version**
  - **Plaintext Authentication**
- Set the VLAN\_VRRP priority for GCC1 to **100** (Primary) and for GCC2 to **80** (Secondary).

- Configure the Track Interface to monitor **WAN1** and **WAN2** to ensure seamless role switching. If both uplink interfaces on the Primary fail, the VLAN VRRP role will switch to the Secondary, avoiding any service disruption.

To configure VLAN VRRP, navigate to **Networking → VRRP → VRRP Group**:

**VRRP Edit VRRP Group**

\*VRID: 80

Enable: ☒

VRRP Name: VLAN80 (0-64 characters)

\*Priority: 100 (Range: 1-254)

\*Interface: Default LAN (VLAN)

\*Virtual IP: 192.168.80.254

Track Interface: WAN1 (WAN) x WAN2 (WAN) x

**Advanced Settings**

Preemptive Mode: ☐

Notification Interval (seconds): 1 (Range: 1-255)

VRRP Versions: ☒ VRRPv2 ☐ VRRPv3

Plaintext Authentication: (0-8 uppercase/lowercase letters and numbers are supported)

Cancel Save

Dual ISP – Two GCC devices – VRRP VLAN Group

2. **Modify VLAN gateway address:** Please refer to the steps mentioned above.

### 3. Configuring Policy Routing

In this scenario, select **Backup Mode**. Default VLAN traffic will initially pass through the **WAN1 interface**. If the WAN1 interface becomes unavailable, the traffic will automatically switch to the **WAN2 interface**, maintaining uninterrupted connectivity.

To configure policy routes, navigate to **Networking → Routing → Policy Routes**.

**Policy Routes Add Load Balance Rule**

\* Name: WAN1\_WAN2 (1-64 characters)

Mode: ☐ Load Balance ☒ Backup

Balancing Strategy: Connection-Based

\*Preferred Interface: Interface: WAN1 (WAN) Weight: 1

\*Alternate Interface: Interface: WAN2 (WAN) Weight: 1

Cancel Save

VRRP Dual ISP GCC – Add Load Balance Rule – Part 1

**Policy Routes Edit Policy Route**

\* Name: VLAN80\_Policy Routes (1-64 characters)

Enable: ☒

IP Family: ☒ Any ☐ IPv4

Protocol Type: All

Source Group: Default (VLAN)

Source IP Address: (Enter the IP address/mask length, such as "192.168.122.0/24")

Destination IP Address: (Enter the IP address/mask length, such as "192.168.122.0/24")

\* Load Balance: WAN1\_WAN2

Schedule: None

Cancel Save

VRRP Dual ISP GCC – Add Load Balance Rule – Part 2

## GCC2 Configuration (Dual ISP)

### 1. Add VLAN VRRP Group

The VLAN\_VRRP priority is configured with GCC1 set to **100 (Primary)** and GCC2 set to **80 (Secondary)**. This setup ensures that **GCC2 operates as the Secondary**. Additionally, the Track Interface can be configured to monitor **WAN1** and **WAN2**. This allows for seamless role switching of the VLAN VRRP in the event of a complete failure of the uplink interfaces on the Primary device, effectively preventing service interruptions.

To configure VLAN VRRP, go to **Networking → VRRP → VRRP Group**:

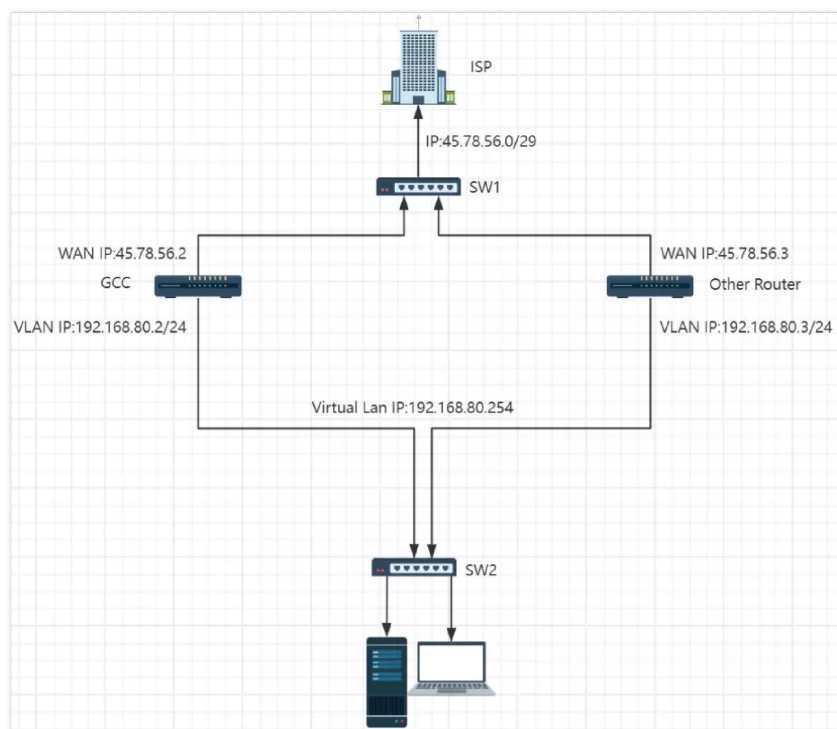
*GCC2 Configuration (Dual ISP & Two GCC devices)*

2. **Modify VLAN gateway address:** Please refer to the steps mentioned above.
3. **Configuring Policy Routing:** same steps as GCC1.

## Examples with Different Vendors

### Single ISP Scenario

#### Network Topology – Different Vendor (Single ISP)





As shown in the topology above, GCC is initially configured as the Primary router, and the Other Router as the Secondary. The ISP allocates the network segment 45.78.56.0/29, with IPs 45.78.56.2 and 45.78.56.3 assigned to the WAN ports of each router, respectively. The internal LAN gateway IP is set to 192.168.80.254.

In the event of a failure on GCC, such as a device freeze, power outage, or LAN port unavailability, the Other Router will automatically take over as the Primary and continue to provide network services.

#### Notes:

- It is recommended to enable VRRP only on the LAN side and not on the WAN port.
- In the actual deployment, both routers' WAN ports are assigned public IPs by the ISP, allowing independent Internet access.
- The VLANs of both routers must be connected to the same switch (SW2).
- If STP (Spanning Tree Protocol) is enabled on the switch to prevent network loops, it may delay the VRRP role election until the switch port reaches the forwarding state.

## GCC Configuration – Single ISP

### 1. Add VLAN VRRP Group

Any VLAN interface can be used as the deployment interface. Ensure that the **VRID**, **Virtual IP**, **Preemption Mode**, **VRRP Version**, and **Plaintext Authentication** settings match those of the other routers. The device with the higher priority will automatically assume the primary role. Additionally, users can configure the **Track Interface** to WAN1 to enable automatic switching of the VLAN VRRP primary-slave role if the primary device's uplink interface fails, preventing service disruption.

To configure VLAN VRRP, navigate to **Networking** → **VRRP** → **VRRP Group**.

The screenshot shows the 'VRRP > Edit VRRP Group' configuration window. The 'Interface' field is set to 'Default LAN (VLAN)', the 'Virtual IP' is '192.168.80.254', and the 'Track Interface' is 'WAN1 (WAN)'. The 'Advanced Settings' section includes 'Preemptive Mode' (unchecked), 'Notification Interval (seconds)' (1), 'VRRP Versions' (VRRPv2 selected), and 'Plaintext Authentication' (empty). The 'Save' button is highlighted in blue.

Add VLAN VRRP Group

### 2. Modify VLAN Gateway Address

If the DHCP service is enabled for the corresponding VLAN, users can change the gateway address to a virtual IP address, such as **192.168.80.254**.

For clients with static IP configurations, users can manually set the gateway to the specified virtual IP address.

To configure the VLAN gateway, navigate to **Networking** → **Network Settings** → **LAN**.

LAN > Edit VLAN

\*VLAN ID: 1

Name: Default LAN (0-64 characters)

Destination: All

VLAN Port IPv4 Address: ☐

\*IPv4 Address: 192.168.80.2

\*Subnet Mask: 255.255.255.0

DHCP Service: ☒

\*Gateway Address: 192.168.80.254 (Allow same as IPv4 address)

\*IPv4 Address Allocation Range: 192.168.80.4 - 192.168.80.253

\*Release Time(m): 120 (Default: 120, range 60-2880)

DHCP Option: Option: , Type: ASCII, Service: , Content: (Add)

Preferred DNS Server:

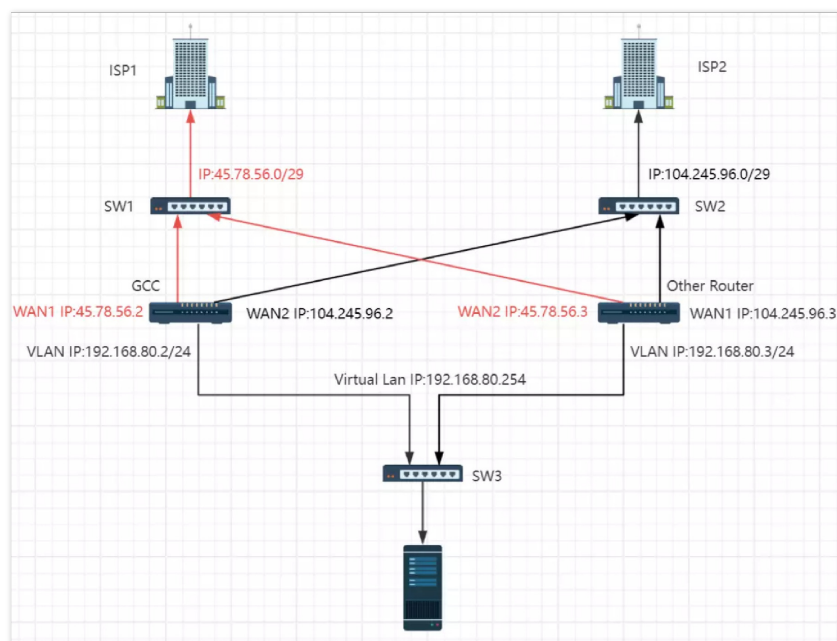
Alternative DNS Server:

Cancel Save

Modify VLAN Gateway Address

## Dual ISP Scenario

### Network Topology – Different Vendor (Dual ISP)



VRRP Dual ISP with different vendor

As shown in the topology above, GCC is initially set as the Primary router, while the Other Router serves as the Secondary. Two ISPs are assigned separate network segments: 45.78.56.0/29 and 104.245.96.0/29, with each segment having independent Internet access. The gateway IP for the internal LAN is 192.168.80.254.

Initially, GCC handles network services as the Primary router. If one of GCC's ISP services fails, the WAN port failover feature will activate, switching to the backup WAN port to maintain Internet access. If both ISP services of GCC fail, a role switch occurs, making the Other Router the Primary, ensuring continued network services. Similarly, if GCC experiences a device freeze, power outage, or LAN port failure, the Other Router will automatically assume the Primary role and continue providing services.

#### Notes:

- When using dual WAN, it's recommended to enable the dual WAN failover feature instead of the WAN VRRP feature for automatic network switching.
- The IPs from both ISPs are capable of independent Internet access.
- Both routers' VLANs should be connected to the same switch.

- WAN ports on both routers must be configured to support the respective ISP settings (including VPN, policy routing, port forwarding, etc.).
- If STP (Spanning Tree Protocol) is enabled on the switch to prevent network loops, the VRRP role election might be delayed until the switch port reaches the forwarding state.

## GCC Configuration – Dual ISP

### 1. Add VLAN VRRP Group

To configure VLAN VRRP, select any VLAN as the deployment interface and ensure the **VRID**, **Virtual IP**, **Preemption Mode**, **VRRP Version**, and **Plaintext Authentication** settings match those of the other routers. The device with the highest priority will assume the primary role. Additionally, set the **Track Interface** to WAN1 and WAN2 to ensure that the VLAN VRRP primary and secondary roles switch if the uplink interface of the primary device fails completely, preventing service interruptions.

To configure VLAN VRRP, please navigate to **Networking → VRRP → VRRP Group**:

The screenshot shows the 'VRRP > Edit VRRP Group' configuration page. The following settings are visible:

- \*VRID**: 80
- Enable**: ☒
- VRRP Name**: VLAN80 (0-64 characters)
- \*Priority**: 100 (Range 1-254)
- \*Interface**: Default LAN (VLAN)
- \*Virtual IP**: 192.168.80.254
- Track Interface**: WAN1 (WAN), WAN2 (WAN)
- Advanced Settings** (expanded):
  - Preemptive Mode**: ☐
  - Notification Interval (seconds)**: 1 (Range 1-255)
  - VRRP Versions**: ☒ VRRPv2, ☐ VRRPv3
  - Plaintext Authentication**: (empty, 0-8 uppercase/lowercase letters and numbers are supported)
- Buttons**: Cancel, Save

Add VLAN VRRP Group

### 2. Modify VLAN Gateway Address

If the DHCP service is enabled for the corresponding VLAN, users can change the gateway address to a virtual IP address, such as **192.168.80.254**.

For clients with static IP configurations, users can manually set the gateway to the specified virtual IP address.

To configure the VLAN gateway, navigate to **Networking → Network Settings → LAN**.

LAN > Edit VLAN

\*VLAN ID: 1

Name: Default (0-64 characters)

Destination: All (X)

VLAN Port IPv4 Address: ☐

\*IPv4 Address: 192.168.80.2

\*Subnet Mask: 255.255.255.0

DHCP Service: ☒

\*Gateway Address: 192.168.80.254 (allow same as IPv4 address)

\*IPv4 Address Allocation Range: 192.168.80.4 - 192.168.80.253

\*Release Time(m): 120 (Default 120, range 60-3880)

DHCP Option:

Option	Type	Service	Content
66	ASCII		https://192.168.80.55:8089
141	ASCII		192.168.80.55:6060

Preferred DNS Server:

Cancel Save

Modify VLAN Gateway Address

### 3. Configure Policy Routing

In this scenario, select **Backup Mode**. Default VLAN traffic will initially pass through the **WAN1 interface**. If the WAN1 interface becomes unavailable, the traffic will automatically switch to the **WAN2 interface**, maintaining uninterrupted connectivity.

To configure policy routes, navigate to **Networking → Routing → Policy Routes**.

Policy Routes > Add Load Balance Rule

\*Name: WAN1\_WAN2 (1~64 characters)

Mode: ☐ Load Balance ☒ Backup

Balancing Strategy: Connection-Based

\*Preferred Interface: Interface WAN1 (WAN) Weight: 1

\*Alternate Interface: Interface WAN2 (WAN) Weight: 1

Cancel Save

Configure Policy Routing – Backup

Then, apply the created Load Balance rule to the Source Group, in our case, it's the Default VLAN.

Policy Routes > Edit Policy Route

\*Name: VLAN80\_Policy Routes (1~64 characters)

Enable: ☒

IP Family: ☒ Any ☐ IPv4

Protocol Type: All

Source Group: Default (VLAN)

Source IP Address:  (Enter the IP address/mask length, such as "192.168.122.0/24")

Destination IP Address:  (Enter the IP address/mask length, such as "192.168.122.0/24")

\*Load Balance: WAN1\_WAN2

Schedule: None

Cancel Save

Configure Policy Routing – Apply to the default VLAN

