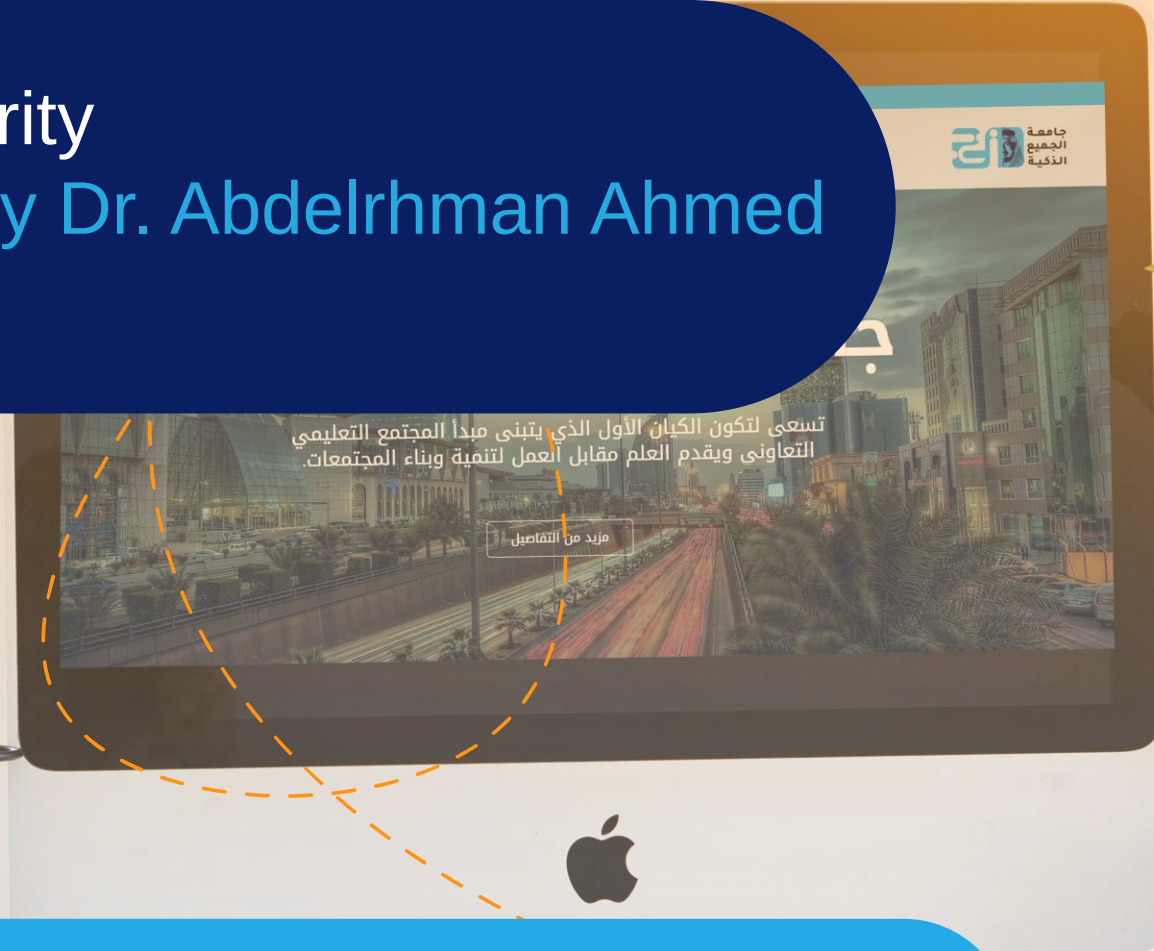


HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 7



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

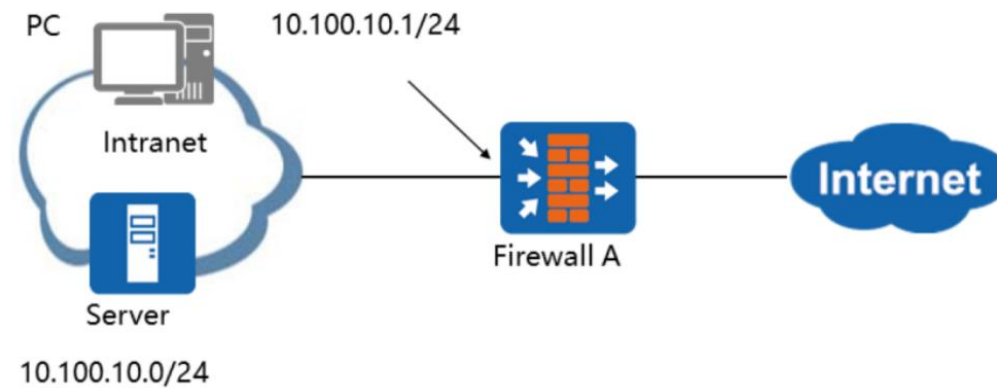
Dual-System Hot Standby

- **With the rapid development of services such as mobile office, online shopping, instant messaging, Internet finance, and Internet education, networks carry increasing services and therefore become more important. How to ensure uninterrupted network transmission is an issue that needs to be solved urgently during network development.**
- **Dual-system hot standby improves reliability. Two firewalls can be deployed at the egress of a network to ensure the communication between the intranet and Internet.**

Objectives

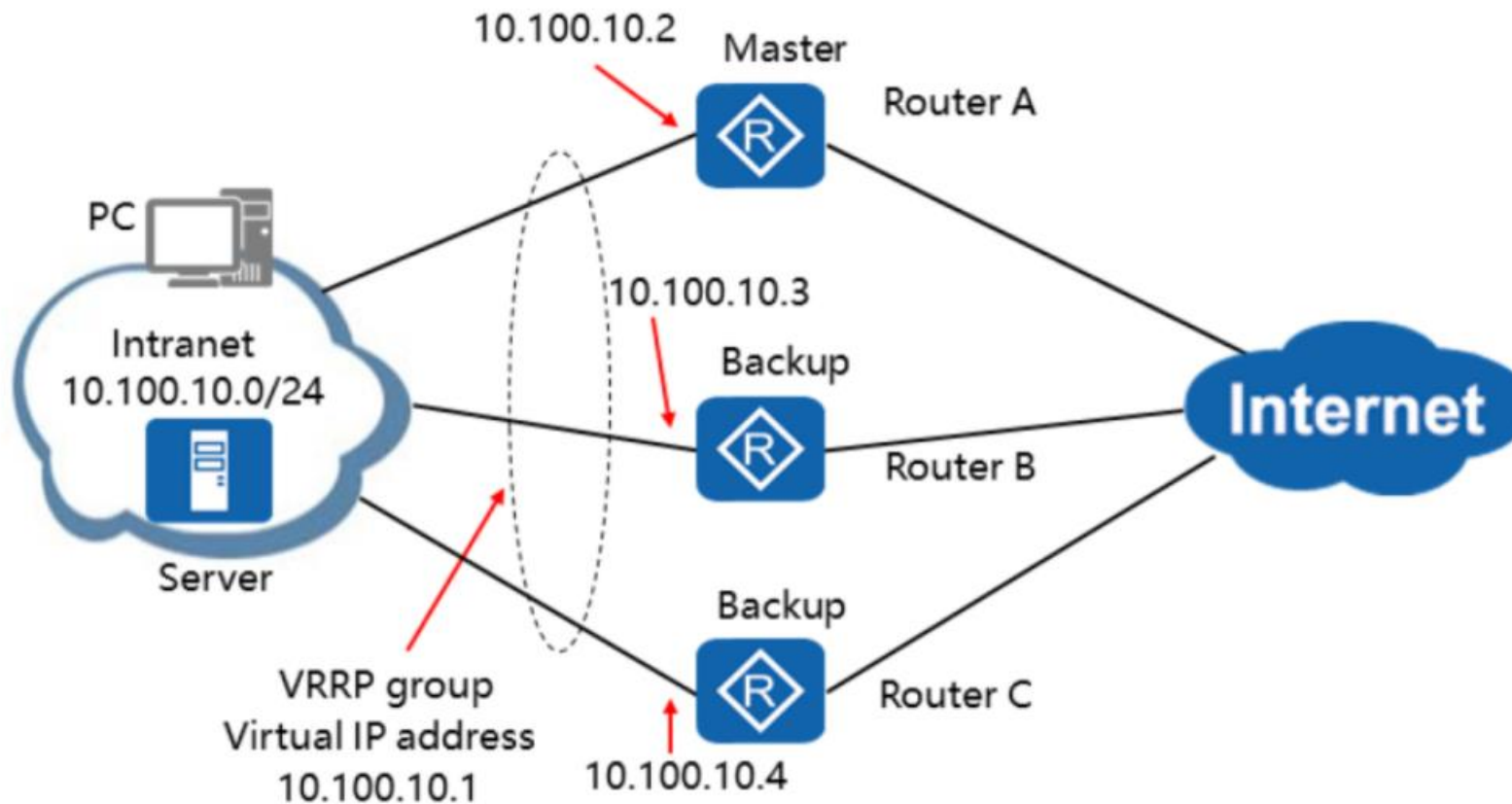
- On completion of this course, you will be able to:
 - ❑ Master the technical principles of dual-system hot standby.
 - ❑ Master the basic configuration of dual-system hot standby.

- The following figure shows a traditional networking mode: packets exchanged between intranet and Internet users are transmitted through Firewall A. If Firewall A is faulty, intranet hosts that use Firewall A as the default gateway cannot communicate with the Internet, affecting communication reliability.



- As a security device, a USG is usually located at a service connection point, between a to-be-protected network and the unprotected network. If only one USG is deployed at a service connection point, network services may be interrupted due to a single point of failure no matter how reliable the USG is. To prevent network service interruptions due to a single point of failure, we can deploy two firewalls to form a dual-system hot standby.

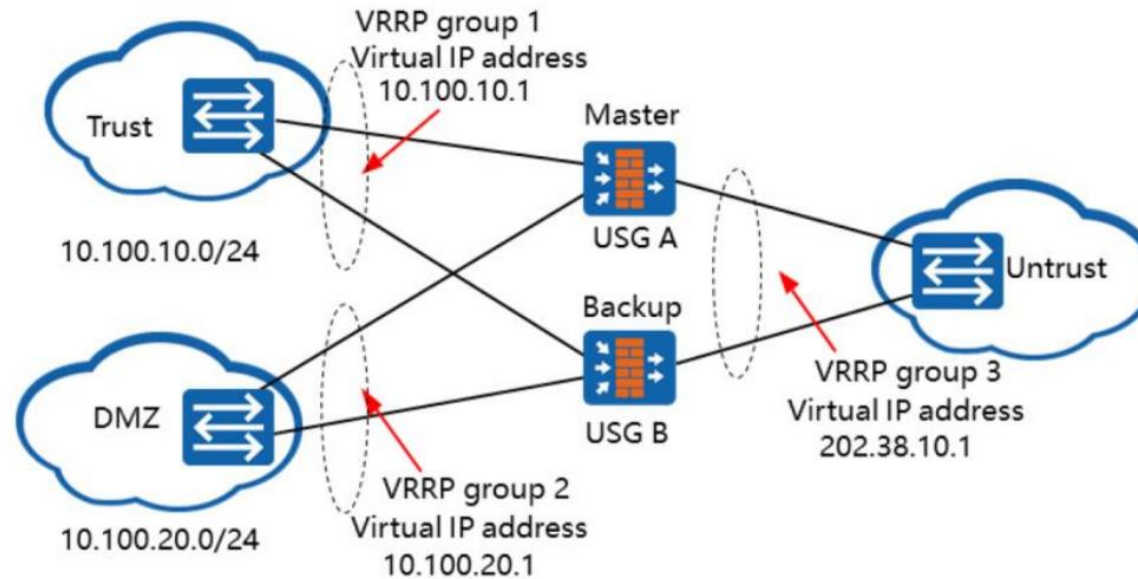
- In router networking, Virtual Router Redundancy Protocol (VRRP) is used for router redundancy.



- A common solution to a single point of failure in standard router networking is to set up a protection mechanism based on the failover between links running a dynamic routing protocol. However, this protection mechanism has limitations. If the dynamic routing protocol is unavailable, services may be interrupted due to a link fault. To address this problem, another protection mechanism, Virtual Router Redundancy Protocol (VRRP), is introduced. VRRP is a basic fault-tolerant protocol. It brings a shorter failover duration compared with the broadcast packets that depend on dynamic routing protocols, and provides link protection even if no dynamic routing protocol is available.
 - VRRP group: A group of routers in the same broadcast domain form a virtual router. All the routers in the group provide a virtual IP address as the gateway address for the intranet.
 - Master router: Among the routers in the same VRRP group, only one router is active, the master router. Only the master router can forward packets with the virtual IP address as the next hop.
 - Backup router: Except for the master router, all other routers in a VRRP group are on standby.
- The master router periodically sends a Hello packet to the backup routers in multicast mode, and the backup routers determine the status of the master router based on the Hello packet. Because VRRP Hello packets are multicast packets, the routers in the VRRP group must be interconnected through Layer 2 devices. When VRRP is enabled, the upstream and downstream devices must have the Layer 2 switching function. Otherwise, the backup routers cannot receive the Hello packets sent by the master router. If the networking requirement is not met, we should not use VRRP.

Application of VRRP in Multi-zone Firewall Networking

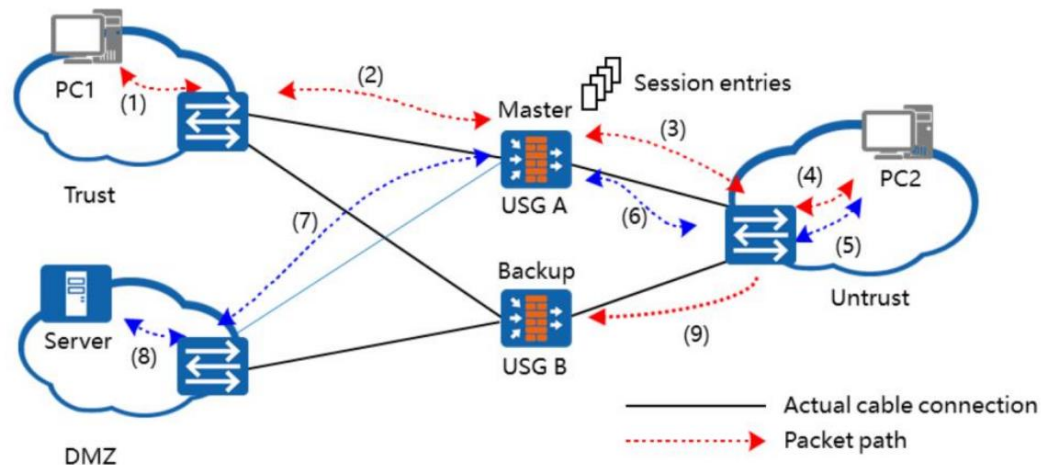
- To provide dual-system hot standby for multiple zones on firewalls, you must configure multiple VRRP groups.



- If multiple zones on firewalls require the hot standby function, you must configure multiple VRRP groups on each firewall.
- As USG firewalls are stateful firewalls, they require the forward and reverse packets to pass through the same firewall. To meet this requirement, the status of all VRRP groups on a firewall must be the same. That is, all VRRP groups on the master firewall must be in the master state, so that all packets can pass through the firewall, and the other firewall functions as the backup firewall.

Defect of VRRP in Firewall Applications

- In traditional VRRP mode, the status of the master firewall cannot be consistent with that of the backup firewall.

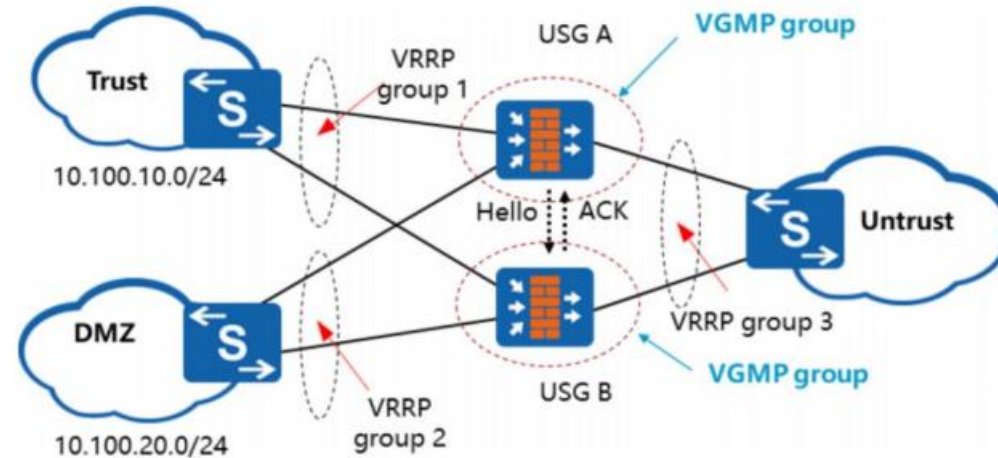


- As shown in the figure, assume that the VRRP status of USG A is the same as that of USG B. Therefore, all interfaces of USG A are in the master state, and all interfaces of USG B are in the backup state.

- PC1 in the Trust zone accesses PC2 in the Untrust zone. The packet forwarding path is (1)-(2)-(3)-(4). USG A forwards the access packet and dynamically generates a session entry. When the reverse packet from PC2 reaches USG A through (4)-(3), it matches the session entry and therefore reaches PC1 through (2)-(1). Similarly, PC2 and the server in DMZ can communicate with each other.
- Assume that the VRRP status of USG A is different from that of USG B. For example, if the interface connecting USG B to the Trust zone is in the backup state but the interface in the Untrust zone is in the master state, PC1 sends a packet to PC2 through USG A, and USG A dynamically generates a session entry. The reverse packet from PC2 returns through the path of (4)-(9). However, USG B does not have any session entry for this data flow. If there is no packet filtering rule on USG B to allow the packet to pass, USG B will discard the packet. As a result, the session is interrupted.

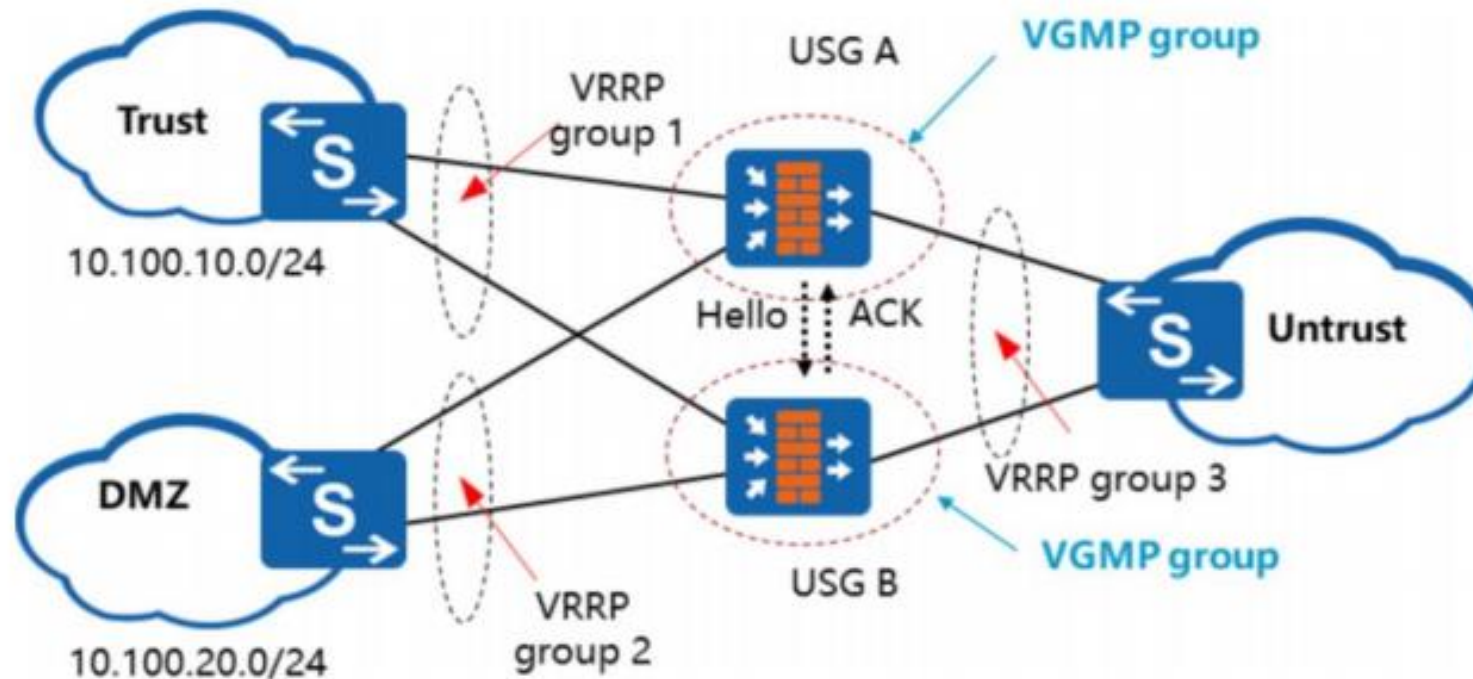
- **Cause of the problem: The packet forwarding mechanisms are different:**
 - ❑ **Router:** Each packet is forwarded based on the routing table. After a link switchover subsequent packets can still be forwarded.
 - ❑ **Stateful firewall:** If the first packet is allowed through, the firewall creates a quintuple session connection accordingly. Subsequent packets (including reverse packets) matching this session entry can pass through the firewall. If a link switchover occurs, subsequent packets cannot match the session entry, resulting in service interruption.
- **Note that if NAT is configured on a router, similar problems occur because a new entry is created after NAT.**

- To ensure the switchover consistency of all VRRP groups, the VRRP Group Management Protocol (VGMP) is developed based on VRRP.



- The requirements for the application of VRRP on firewalls are as follows:
 - ☐ VRRP status consistency
 - ☐ Session table status backup
- Multiple VRRP groups on a firewall can be added to a VGMP group, which manages the VRRP groups in a unified manner. VGMP controls the status switchover of VRRP groups in a unified manner, ensuring the consistent status of the VRRP groups.

- If the VGMP group on a firewall is in the active state, all VRRP groups in the VGMP group are in the active state. The same applies with standby.
- The firewall in the VGMP Active state regularly tests the peers' running status, including the priority and VRRP member status, by sending Hello packets.



- You can specify the VGMP group status to determine the active or standby firewall.
- If the VGMP group on a firewall is in the active state, all VRRP groups in the VGMP group are in the active state. This firewall is the active firewall, and all packets pass through this firewall. In this case, the VGMP group on the other firewall is in the standby state, and the firewall is the standby firewall.
- Each firewall has an initial VGMP group priority. If an interface or a board of the firewall is faulty, the VGMP group priority of the firewall decreases.
- The initial VGMP group priority of the USG6000 and NGFW Module is 45000. The initial VGMP group priority of the USG9500 depends on the number of cards on the line processing unit (LPU) and the number of CPUs on the service processing unit (SPU).
- Similar to VRRP, the VGMP active firewall regularly sends Hello packets to the VGMP standby firewall to inform the latter of its running status, including the priority and the status of member VRRP groups. The member status is dynamically adjusted, so that the two firewalls can perform active/standby switchovers.
- Different from VRRP, after the VGMP standby firewall receives a Hello packet, it replies with an ACK message, carrying its own priority and status of member VRRP groups.
- By default, VGMP Hello packets are sent every second. If the standby firewall does not receive any Hello packets from the active firewall after three Hello packet periods, the standby firewall regards that the peer fails, and then switches to the active state.

- Status consistency management

- Whenever the status of a VRRP group changes, the VGMP group must be notified of the change. The VGMP group determines whether to allow the master/backup switchover of the VRRP group. If the status switchover is necessary, the VGMP group instructs all its VRRP groups to perform the switchover. Therefore, after a VRRP group is added to a VGMP group, its status cannot be switched separately from the group.

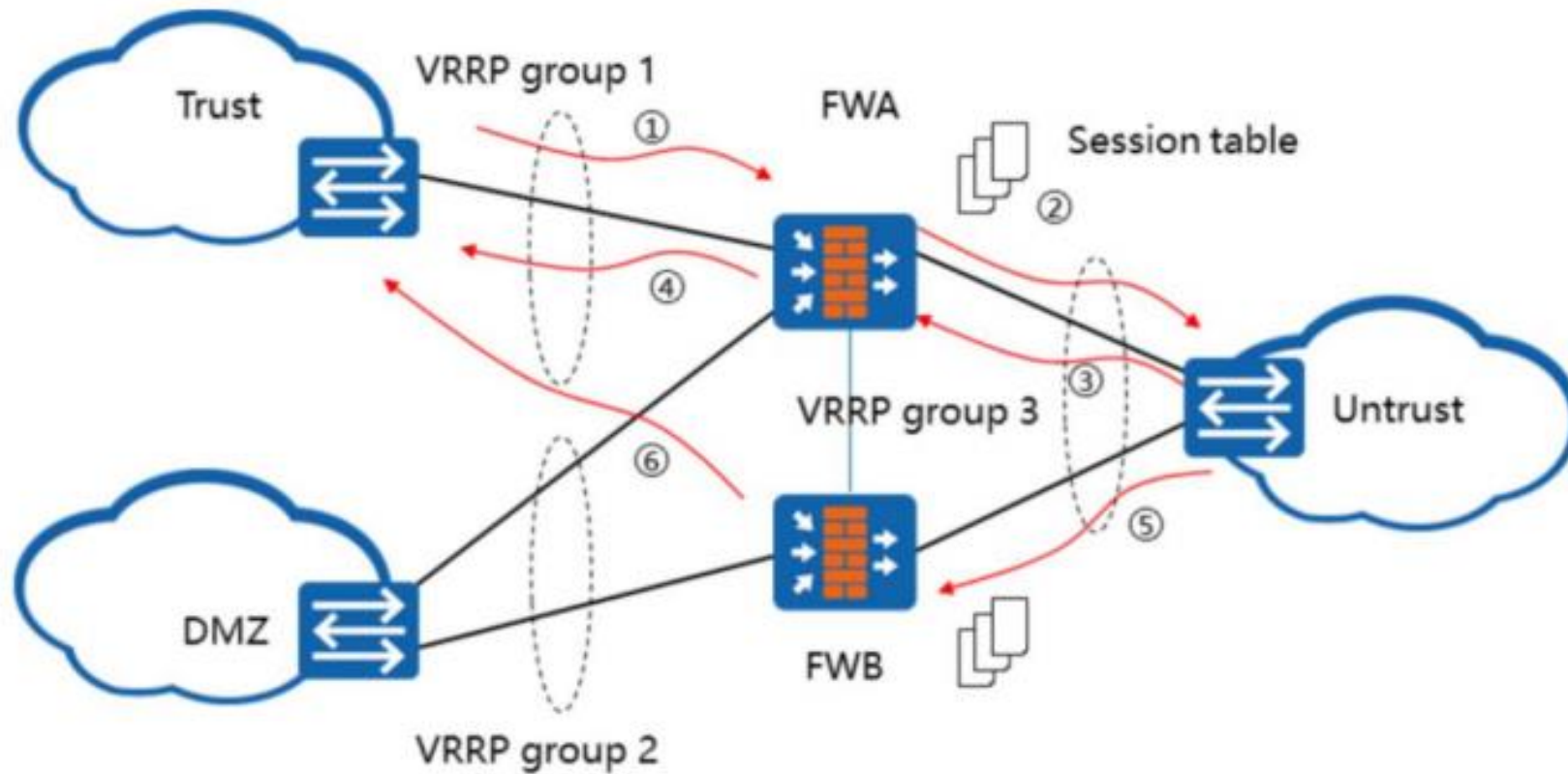
- Preemption management

- VRRP groups are capable of preemption. If the faulty master firewall recovers, so does the priority of the firewall. Therefore, the firewall can become the master firewall again through preemption.

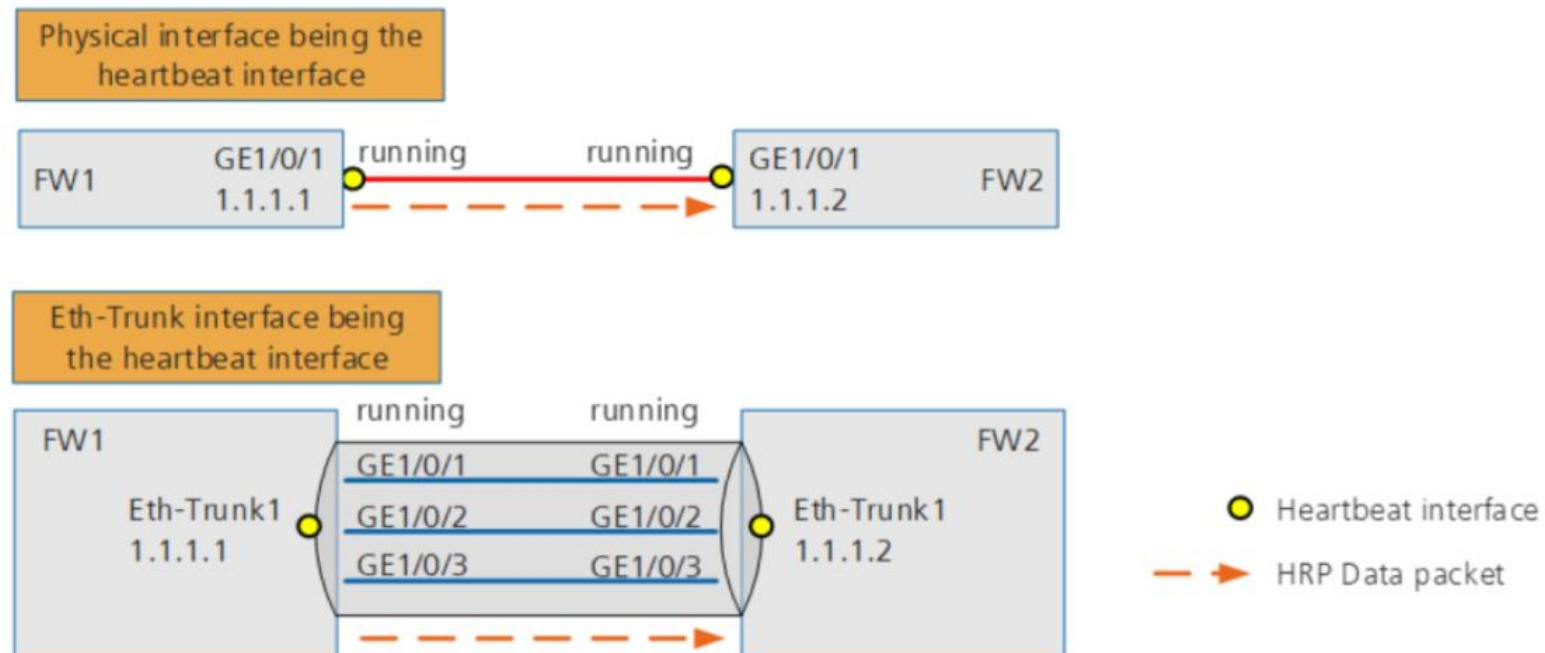
- After a VRRP group is added to a VGMP group, the preemption function of the VRRP group becomes invalid. The VGMP group determines whether to preempt.

- The preemption function of VGMP groups is similar to that of VRRP groups. If the faulty VRRP group in a VGMP group recovers, the priority of the VGMP group restores to the original value. In this case, the VGMP group determines whether to preempt to be the active firewall.

- The Huawei Redundancy Protocol (HRP) backs up dynamic status data and key configuration commands between firewalls.



- The two firewalls exchange backup data through the heartbeat interfaces over the heartbeat link.
- A heartbeat interface must be an independent interface with an IP address. It can be a physical interface (such as a GE interface) or a logical Eth-Trunk interface.
- Usually, backup data accounts for 20% to 30% of service traffic. You can determine the number of member Eth-Trunk interfaces based on the amount of backup data.



- HRP heartbeat interfaces have five states:

- Invalid
- Down
- Peerdown
- Ready
- Running



● Interface

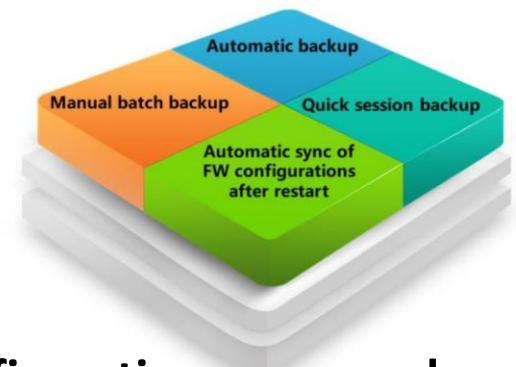
— Heartbeat link

--- HRP heartbeat link
detection packets

--- HRP data packets

- **Invalid:** The physical status is Up, and protocol status is Down. The local heartbeat interface is incorrectly configured. For example, the heartbeat interface is a Layer 2 interface, or no IP address is configured for the heartbeat interface.
- **Down:** The physical and protocol statuses of the local heartbeat interface are both Down.
- **Peer-down:** The physical and protocol statuses are both Up. The local heartbeat interface cannot receive heartbeat link detection reply packets from the peer heartbeat interface. In this case, the firewall sets the status of the local heartbeat interface to peer-down. Even so, the local heartbeat interface continues sending heartbeat link detection packets and expects to resume the heartbeat link when the peer heartbeat interface is brought Up.
- **Ready:** The physical and protocol statuses are both Up. The local heartbeat interface receives heartbeat link detection reply packets from the peer heartbeat interface. In this case, the firewall sets the status of the local heartbeat interface to ready, indicating that it is ready to send and receive heartbeat packets. In addition, it continues sending heartbeat link detection packets to keep the heartbeat link status.

- **Running:** When multiple local heartbeat interfaces are in the ready state, the firewall sets the status of the first configured one to running. If only one interface is in the ready state, the firewall sets its status to running. The running interface is used to send HRP heartbeat packets, HRP data packets, HRP link detection packets, VGMP packets, and consistency check packets.
- Other local heartbeat interfaces in the ready state serve as backups and take up services in sequence (based on the order of configuration) when the running heartbeat interface or the heartbeat link fails.
- To conclude, heartbeat link detection packets are used to detect whether the peer heartbeat interface can receive packets and determine whether the heartbeat link is available. The local heartbeat interface sends heartbeat link detection packets as long as its physical and protocol statuses are both Up.
- As described in previous sections, HRP heartbeat packets are used to detect whether the peer device (peer VGMP group) is working properly. These packets can be sent only by the running heartbeat interface in the VGMP group on the active device.



- **Automatic backup**

- ❑ By default, automatic backup is enabled on the firewall to automatically back up configuration commands in real time and status information regularly. This backup method applies to various hot standby networks.
- ❑ After automatic backup is enabled, every time you execute a command that can be backed up on a firewall, the command is immediately backed up to the other firewall.
- ❑ After automatic backup is enabled, the active device periodically backs up status information that can be backed up to the standby device. Therefore, the status information of the active device is not immediately backed up after its creation. Instead, the information is backed up to the standby device around 10 seconds after its creation.

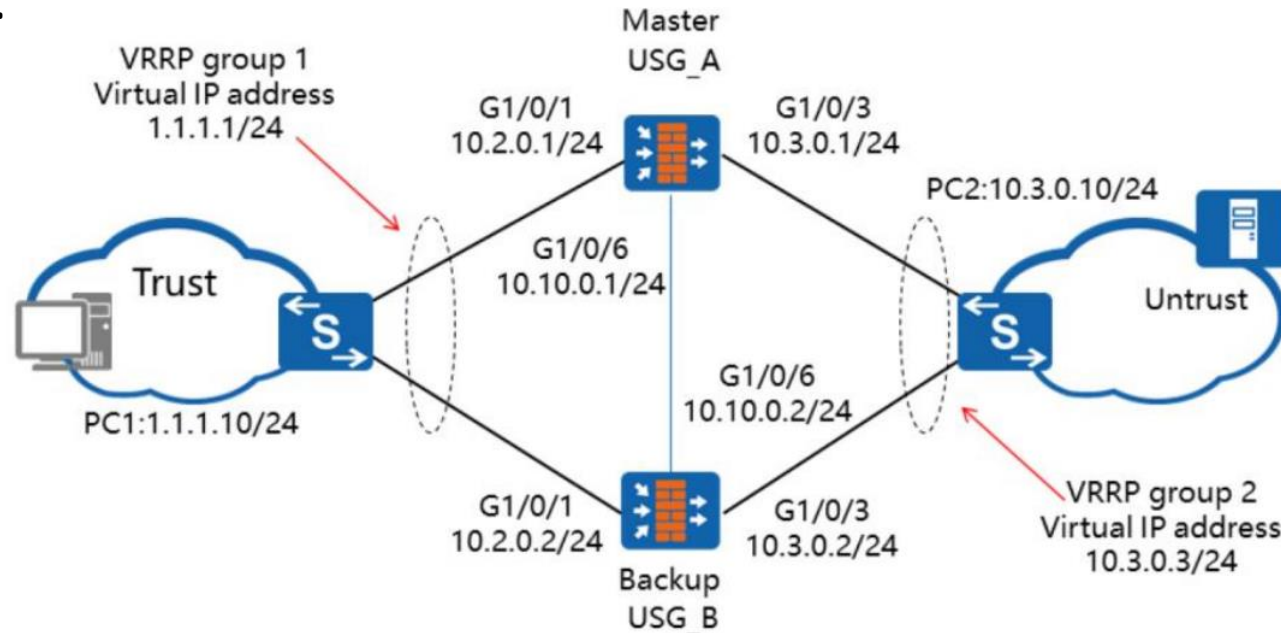
- **The following types of sessions cannot be backed up in automatic backup:**

- ❑ Sessions created by traffic destined for the firewall, for example, sessions created for administrator logins to the firewall
- ❑ TCP half-open connection sessions (these can be backed up in quick session backup)
- ❑ Sessions created by UDP first packets but not matching subsequent packets (these can be backed up in quick session backup)

- **Manual batch backup**
 - **Manual batch backup needs to be triggered by the configuration of the manual batch backup command. This backup starts immediately and applies to scenarios where manual backup is required when the configurations of two devices are asynchronous.**
 - **After the manual batch backup command is executed, the designated active device immediately synchronizes its configuration commands to the designated standby device.**
 - **After the manual batch backup command is executed, the designated active device immediately synchronizes its status information to the designated standby device with no need to wait for an automatic backup period.**
- **Quick session backup**
 - **Quick session backup applies when the forward and reverse paths are inconsistent on load balancing networks. Inconsistent forward and reverse paths may occur on load balancing networks because both devices are active and able to forward packets. If status information is not synchronized in a timely manner, reverse packets may be discarded if they do not match any sessions, causing service interruption. Therefore, quick session backup is required by the firewalls to back up status information in real time.**

- ❑ For timely synchronization, this function synchronizes status information but not configuration. The synchronization of configuration commands can be undertaken by using automatic backup.
- ❑ After quick session backup is enabled, the active firewall can synchronize all status information, including those not supported by automatic session backup, to the standby firewall. Therefore, sessions can be synchronized to the standby firewall immediately when they are set up on the active firewall.
- Automatic synchronization of active/standby firewall configurations after restart
- ❑ In the hot standby networking, if one firewall is restarted, the other firewall processes all services during the restart. In this period, the firewall that processes the services may have configurations added, deleted, or modified. To ensure that the active and standby firewalls have the same configurations, after the firewall is restarted, configurations are automatically synchronized from the firewall that processes services.
- ❑ Only configurations that can be backed up can be synchronized, such as security policies and NAT policies. Configurations that cannot be backed up, such as OSPF and BGP, remain unchanged.
- ❑ Configuration synchronization can take up to one hour, subject to the amount of configuration. During the synchronization, you are not allowed to execute configuration commands that can be backed up between firewalls.

- When upstream and downstream service interfaces on firewalls work at Layer 3 and connect to Layer 2 devices, configure VRRP groups on the service interfaces, so that the VGMP group can monitor the Layer 3 service interfaces through the VRRP groups.



- In dual-system hot standby networking, the firewalls usually work in routing mode, and the downstream switches separately connect to the firewalls through two links. In normal cases, USG A functions as the active firewall. If the uplink or downlink of USG A goes Down, USG B automatically becomes the active firewall, and switch traffic is transmitted through USG B.

- Configure VRRP in the interface view:

```
vrrp vrid virtual-router-ID virtual-ip virtual-address [ ip-  
mask | ip-mask-length ] { active | standby }
```

- After the active or standby parameter is specified, the VRRP group is added to the active or standby VGMP group.
- Up to 255 VRRP groups can be configured on each common physical interface (Gigabit Ethernet interface).
- By default, the master VRRP group sends VRRP packets every second. You can adjust the interval for sending VRRP packets in the interface view. Run the following command to change the interval for sending VRRP packets:
 - ❑ `vrrp vrid virtual-router-ID timer advertise adver-interval`
- VRRP can work with IP-link. If the uplink is disconnected, a master/backup VRRP switchover is triggered. Run the following command to configure an IP-link in the interface view:
 - ❑ `vrrp vrid virtual-router-id ip-link link-id`
- The preemption function of VGMP groups is enabled by default, and the default preemption delay is 60 seconds. Run the following command to set a preemption delay for a VGMP group:
 - ❑ `hrp preempt [ delay interval ]`

- Specify a heartbeat interface.

```
hrp interface interface-type interface-number [ remote { ip-  
address | ipv6-address } ]
```

- Enable HRP.

```
hrp enable
```

- Enable the function of configuring the standby device.

```
hrp standby config enable
```

- Enable the function of automatically backing up commands and status information.

```
hrp auto-sync [ config | connection-status]
```

- Enable quick session backup.

```
hrp mirror session enable
```

- Configuration of VRRP group 1 on USG_A:

```
[USG_A]interface GigabitEthernet 1/0/1
[USG_A-GigabitEthernet 1/0/1 ]ip address 10.2.0.1 24
[USG_A-GigabitEthernet 1/0/1 ]vrrp vrid 1 virtual-ip 1.1.1.1
255.255.255.0 active
```

- Configuration of VRRP group 1 on USG_B:

```
[USG_B]interface GigabitEthernet 1/0/1
[USG_B-GigabitEthernet1/0/1 ]ip address 10.2.0.2 24
[USG_B-GigabitEthernet 1/0/1 ]vrrp vrid 1 virtual-ip 1.1.1.1
255.255.255.0 standby
```

- HRP configuration on USG_A:

```
[USG_A]hrp enable  
[USG_A]hrp mirror session enable  
[USG_A]hrp interface GigabitEthernet 1/0/6
```

- HRP configuration on USG_B:

- ☐ [USGB]hrp enable
- ☐ [USG B]hrp mirror session enable
- ☐ [USG B]hrp interface GigabitEthernet 1/0/6

- **hrp enable//Enable HRP.**
- **hrp mirror session enable //Enable quick session backup.**
- **hrp interface GigabitEthernet 1/0/6 //Configure this interface as the heartbeat interface.**

- View the status of an interface in a VRRP group:

```
HRP_A<USG_A>display vrrp interface G1/0/3
GigabitEthernet1/0/3 | Virtual Router 2
  VRRP Group : Active
  state : Active
  Virtual IP : 10.3.0.3
  Virtual MAC : 0000-5e00-0102
  Primary IP : 10.3.0.1
  PriorityRun : 120
  PriorityConfig:100
  MasterPriority : 120
  Preempt : YES    Delay Time : 0
  Advertisement Timer : 1
  Auth Type : NONE
  Check TTL : YES
```

- View the status of the active firewall:

```
HRP_A<USG_A>dis hrp state
The firewall's config state is: ACTIVE

Current state of virtual routers configured as active:
      GigabitEthernet1/0/1      vrid    1 : active
      GigabitEthernet1/0/3      vrid    2 : active
```

- View the status of the standby firewall:

- ☐ HRP_S[USG_B] display hrp state
- ☐ The firewall's config state is: Standby

- Current state of virtual routers configured as standby:

- ☐ GigabitEthernet1/0/1 vrid 1 : standby
- ☐ GigabitEthernet1/0/3 vrid 2 : standby

- Choose System > High Availability > Dual-System Hot Standby and click Edit to configure dual-system hot standby.

Dual-System Hot Standby

 Edit

Monitored Item	Current Status	Details
Current running mode	Load Balancing	
Current Working Role	active (the stable running time: 0 days, 0 hours, 0 mins)	Details
Current HeartBeat Interface	None	
Proactive Preemption	Enabled	
Configuration Consistency	Initialization(check time:0/0/0 00:00:00)	Details Check
Virtual IP		
Interface VLAN 		
IP-Link		

- Click Edit to enter the Dual-System Hot Standby configuration page. You can set basic HRP parameters and track the interfaces, VLANs, IP-links, and BFD.
- Click Details to view the HRP switchover history.
- Click Check to check the consistency of configurations on the active and standby firewalls.

- On the Dual-System Hot Standby page, click Edit to configure the active firewall USG A. In the Configure Virtual IP Address area, click Add to create a VRRP group.

Configure Dual-System Hot Standby

Dual-System Hot Standby ☒ Enable

Operating Mode ☒ Active/Standby Backup ☐ Load Balancing

State ☒ Active ☐ Standby

Heartbeat Interface [\[Edit\]](#) IP Address Peer IP Address

Proactive Preemption ☒ Enable

Hello Packet Interval <500-60000>Milliseconds

Configure Virtual IP Address

You need to configure a virtual IP address if the service interface works at Layer 3 and is connected to a switch.

[Add](#) [Delete](#) [Refresh](#)

VRID	Interface	Interface IP Address/Mask	Virtual IP Address/Mask
☐ 2	GE1/0/3	10.2.0.1/24	10.2.0.2/24
☐ 1	GE1/0/1	10.2.0.1/24	1.1.1.1/24

Page 1 of 1 Records per page 50 Displaying 1 - 2 of 2

OK Cancel

- Configure the internal web and FTP servers.

```
[USG] nat server wwwserver protocol tcp global 202.169.10.1 80 inside  
192.168.20.2 8080  
[USG] nat server ftpserver protocol tcp global 202.169.10.1 ftp inside  
192.168.20.3 ftp
```

- Configure interzone packet filtering rules.

```
[USG] security-policy  
[USG -policy-security] rule name p1  
[USG -policy-security-rule-p1] source-zone untrust  
[USG -policy-security-rule-p1] destination-zone dmz  
[USG -policy-security-rule-p1] destination-address 192.168.20.2 32  
[USG -policy-security-rule-p1] service http  
[USG -policy-security-rule-p1] action permit  
[USG -policy-security] rule name p2  
[USG -policy-security-rule-p2] source-zone untrust  
[USG -policy-security-rule-p2] destination-zone dmz  
[USG -policy-security-rule-p2] destination-address 192.168.20.3 32  
[USG -policy-security-rule-p2] service ftp  
[USG -policy-security-rule-p2] action permit
```

- When both NAT and internal servers are configured on the USG, the internal servers have a higher priority and take effect first.
- If multiple internal servers use the same public address, you can run the nat server command multiple times to configure them, and distinguish them using protocols.

- On the Dual-System Hot Standby page, click Edit to configure the standby firewall USGB. In the Configure Virtual IP Address area, click Add to create a VRRP group.

Configure Dual-System Hot Standby

Dual-System Hot Standby ☒ Enable

Operating Mode: ☒ Active/Standby Backup ☐ Load Balancing

State: ☐ Active ☒ Standby

Heartbeat Interface: GE1/0/6 IP Address: 10.10.0.2 Peer IP Address: 10.10.0.1

Proactive Preemption: ☒ Enable

Hello Packet Interval: 1000 <500-60000>Milliseconds

Configure Virtual IP Address

You need to configure a virtual IP address if the service interface works at Layer 3 and is connected to a switch.

[Add](#) [Delete](#) [Refresh](#)

VRID	Interface	Interface IP Address/Mask	Virtual IP Address/Mask
☐ 2	GE1/0/3	10.3.0.2/24	10.3.0.3/24
☐ 1	GE1/0/1	10.2.0.2/24	1.1.1.1/24

Page 1 of 1 Records per page: 50 Displaying 1 - 2 of 2

OK Cancel

- On the Dual-System Hot Standby page, click Details to view active/standby switchover information about dual-system hot standby.

Dual-System Hot Standby

 Edit

Monitored Item	Current Status	Details
Current running mode	Active/Standby Backup	
Current Working Role	standby (the stable running time: 0 days, 0 hours, 0 mins)	Details
Current HeartBeat Interface		
Proactive Preemption		
Configuration Consistency		
Virtual IP		
10.3.0.3 (GE1/0/3)		
1.1.1.1 (GE1/0/1)		
Interface VLAN		
IP-Link		
BFD		

Active/Standby Switchover ? x

State: Standby

Time elapsed after the last switchover:
0 days 0 hours 0 minutes

History Switchover Table

Num	Time	Description	Reason
0	2018-9-5 10:2:47	Init switchover to Standby	HRP is enabled.
1	2018-9-5 10:3:5	Standby switchover to Ac...	Heartbeat packet timeout.

- On the Dual-System Hot Standby page, view the running mode, role, and VRRP group status.

Dual-System Hot Standby

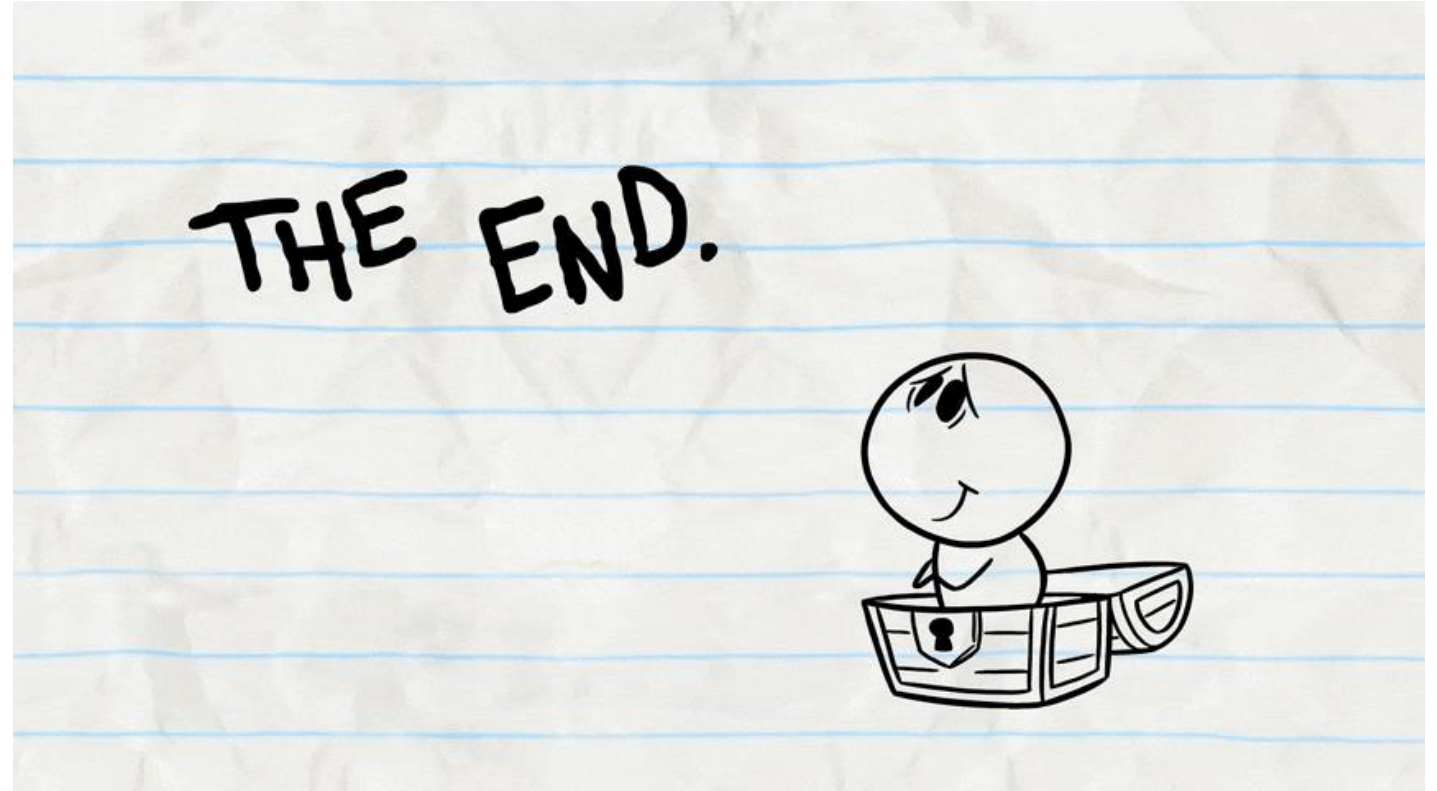
Edit

Monitored Item	Current Status	Details
Current running mode	Active/Standby Backup	
Current Working Role	active (the stable running time: 0 days, 0 hours, 0 mins)	Details
Current HeartBeat Interface	GE1/0/6(Backup channel usage:0.00%)	
Proactive Preemption	Enabled	
Configuration Consistency	Initialization(check time:0/0/0 00:00:00)	Details Check
Virtual IP		
10.3.0.3(GE1/0/3)		master
1.1.1.1(GE1/0/1)		master
Interface VLAN		
IP-Link		
BFD		

The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY