

GLBP on Catalyst 6500 Switches Configuration Example

Document ID: 81565

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

GLBP Concepts

- GLBP Overview
- Virtual Gateway
- Virtual Forwarder
- Limitation
- Sup 2 and Sup 720 – GLBP Comparison
- Design Consideration

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- %GLBP-4-DUPADDR: Duplicate address

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document provides a sample configuration for Gateway Load Balancing Protocol (GLBP) on the Cisco 6500 Catalyst Switches. This document shows the GLBP configuration on the small campus network.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Configuring GLBP
- Cisco GLBP Load Balancing Options

Components Used

The information in this document is based on the Catalyst 6500 with Supervisor 720.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This command was introduced in 12.2(14)S and was integrated into Cisco IOS® Software Release 12.2(15)T. This configuration can also be used with these hardware versions:

- Cisco Catalyst 6500 Series Supervisor Engine 720
- Cisco Catalyst 6500 Series Supervisor Engine 2

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

GLBP Concepts

GLBP Overview

In order to enhance on the capabilities of Hot Standby Router Protocol (HSRP), Cisco developed GLBP. GLBP provides automatic, first-hop gateway load balancing, which allows for more efficient resource usage and reduced administrative costs. It is an extension of HSRP and specifies a protocol that dynamically assigns responsibility for a virtual IP address and distributes multiple virtual MAC addresses to members of a GLBP group.

In campus networks, Layer 3 VLAN interfaces act as the gateway for the hosts. These Layer 3 VLAN interfaces from different switches are load balanced using GLBP. Layer 3 interfaces from multiple switches form one GLBP group. Each group contains one unique virtual IP address.

Supervisor 720 can have a maximum of 1024 GLBP groups (group numbers 0 to 1023). Supervisor 2 supports only one GLBP group. A GLBP group can have a maximum of 4 members. It means that GLBP can load balance up to 4 gateways.

GLBP members have two roles:

- Virtual Gateway Assigns virtual MAC addresses to the members.
- Virtual Forwarder Forwards data for the traffic destined to the virtual MAC address.

Virtual Gateway

A member in a group can be in either of these states: active, standby, or listen. Members of a GLBP group elect one gateway to be the Active Virtual Gateway (AVG) for that group. It also elects one member as Standby Virtual Gateway (SVG). If there are more than two members, then the members that remain are in the listen state.

If an AVG fails, the SVG assumes responsibility for the virtual IP address. A new SVG is then elected from the gateways in the listen state. If the failed AVG or the new member with higher priority number comes online, it does not preempt by default. You can configure the switches so that it can preempt.

The function of the AVG is that it assigns a virtual MAC address to each member of the GLBP group. Remember that in HSRP there is only one virtual MAC address for the virtual IP address. However, in GLBP each member is assigned one virtual MAC address. AVG takes care of the virtual MAC address assignment.

Note: Because GLBP supports a maximum of 4 members for a group, AVG can assign only a maximum of 4 MAC addresses.

Virtual Forwarder

AVG assigns virtual MAC addresses to each member in sequence. The member is called Primary Virtual Forwarder (PVF) or Active Virtual Forwarder (AVF) if the MAC address is assigned directly by the AVG. The same member is Secondary Virtual Forwarder (SVF) for the MAC addresses assigned to other members. PVF is in active state and SVF is in listen state.

In short, for a GLBP group of 4 members, each member is PVF for one MAC address and SVF for three other MAC addresses.

If PVF for a virtual MAC address fails, any of the SVF assumes responsibility for that virtual MAC address. At this time, that member is PVF for 2 virtual MAC address (one assigned by AVG and the other one takes over for the failed member). The Virtual Forwarder preemptive scheme is enabled by default. Remember that the preemptive scheme for the Virtual Gateway is not enabled by default, but the preemptive scheme for the Virtual Forwarder is enabled by default.

In order to remove an AVF gracefully, use the **redirect timers** command on the other AVFs so that when the current AVF is removed, the secondary AVF will take over without causing any packet loss on the link.

By default, GLBP uses built-in timers to detect the presence of an AVF based on which keeps providing the virtual MAC aligned to the AVF. When the AVF goes down, the GLBP process waits for a specific amount of time after which it declares the AVF no longer available. It then starts to propagate the same virtual MAC which binds it to other available AVFs. The default for this timer is 300 seconds. This can be reduced to take better advantage of the situation and make a quick changeover.

In order to configure the time between hello packets sent by the GLBP gateway and the time that the virtual gateway and virtual forwarder information is considered valid, use the **glbp group timers [msec] hellotime [msec] holdtime** command in interface configuration mode.

Limitation

Cisco Non-Stop Forwarding (NSF) with Stateful Switch Over (SSO) has a restriction with GLBP. SSO is not GLBP-aware, which means the GLBP state information is not maintained between the active and standby supervisor engine during normal operation. GLBP and SSO can co-exist, but both features work independently. Traffic that relies on GLBP can switch to the GLBP standby in the event of a supervisor switchover.

Sup 2 and Sup 720 – GLBP Comparison

Supervisor 2 has few restrictions in the GLBP implementation. This summarizes the few differences in GLBP support between the Supervisor 2 and Supervisor 720.

- Supervisor 2 supports only plain text authentication.

Supervisor 720 supports both plain text and md5 authentication.

- Supervisor 2 supports only one GLBP group. The group number can be anything in between 0 – 1023.

```
Sup2(config)#interface vlan 11
Sup2(config-if)#glbp 11 ip 172.18.11.1
More than 1 GLBP groups not supported on this platform.
```

Supervisor 720 supports more than one group (0 – 1023).

- HSRP and GLBP cannot co-exist in Supervisor 2. This means that if you configure GLBP in one VLAN, you cannot configure HSRP on any VLANs in the switch.

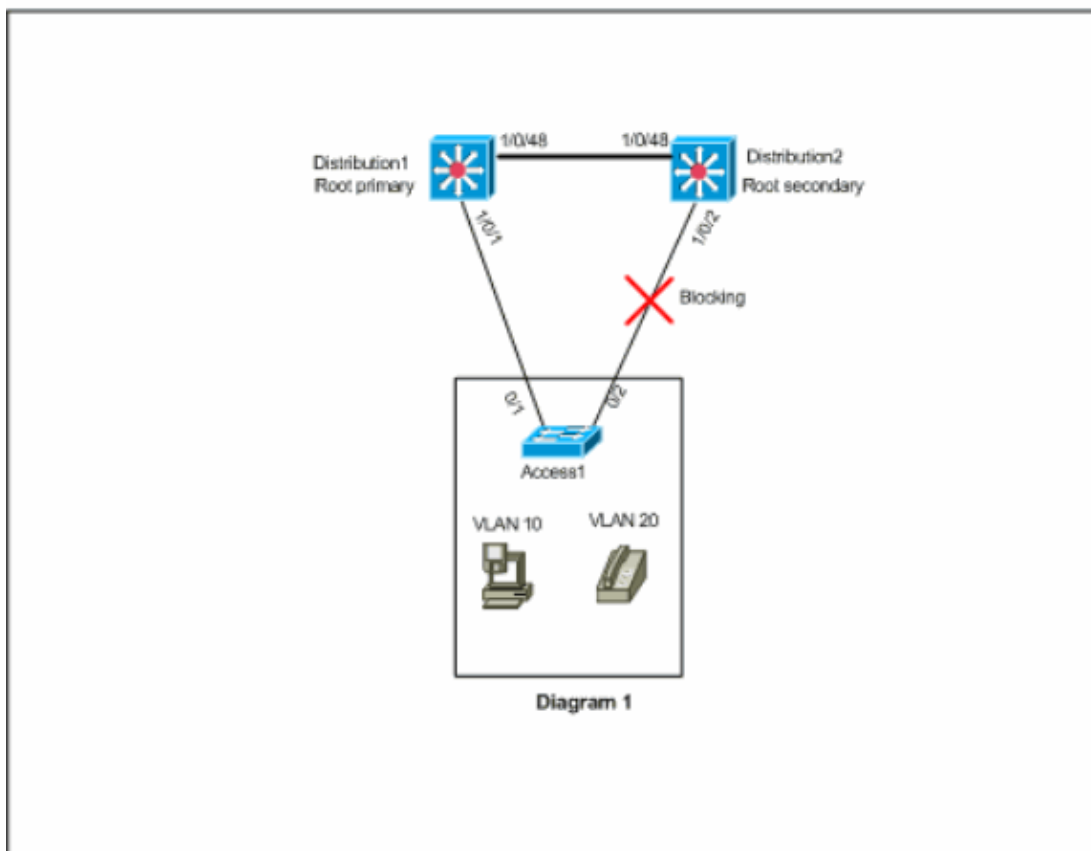
```
Sup2(config)#int vlan 31
Sup2(config-if)#standby 31 priority 120
multiple ip virtual protocols not supported in this platform.
```

HSRP and GLBP can co-exist in Supervisor 720. This means that you can configure a few VLANs with GLBP and a few other VLANs with HSRP.

Design Consideration

GLBP implementation on Catalyst switches depends on the network design. You need to consider the spanning-tree topology to use GLBP on your network. You can use this diagram as an example:

Diagram 1



In this diagram, there are two VLANs, 10 and 20, on all the three switches. In this network, Distribution1 is the root bridge for all the VLANs and the result is the port 1/0/2 in Distribution2 will be in blocking state. In this scenario, GLBP is not suitable to implement. Because you have only one path from Access1 to the distribution switch, you cannot achieve true load balancing with GLBP. However, in this scenario, you can use Spanning-Tree Protocol (STP) instead of GLBP to load balance and you can use HSRP for redundancy. You must consider your STP topology in order to decide whether to use GLBP or not. In such configurations where spanning-tree is required, the solution is to use an improved STP, such as Rapid-PVST. In order to enable Rapid-PVST, use the **spanning-tree mode rapid-pvst** command on the switches.

This is the STP that is recommended to use with GLBP. Rapid-PVST provides a fast convergence time, which allows links to reach the spanning-tree forwarding state before the default GLBP hold timer times out.

If an STP is used on a link to a GLBP router, the GLBP hold time must be greater than the time it takes for the STP to reach the forwarding state. Default parameter settings achieve this with Rapid-PVST, whereas a hold time of more than 30 seconds is required if STP is used with its default settings.

Configure

In this section, you are presented with the information to configure the features described in this document.

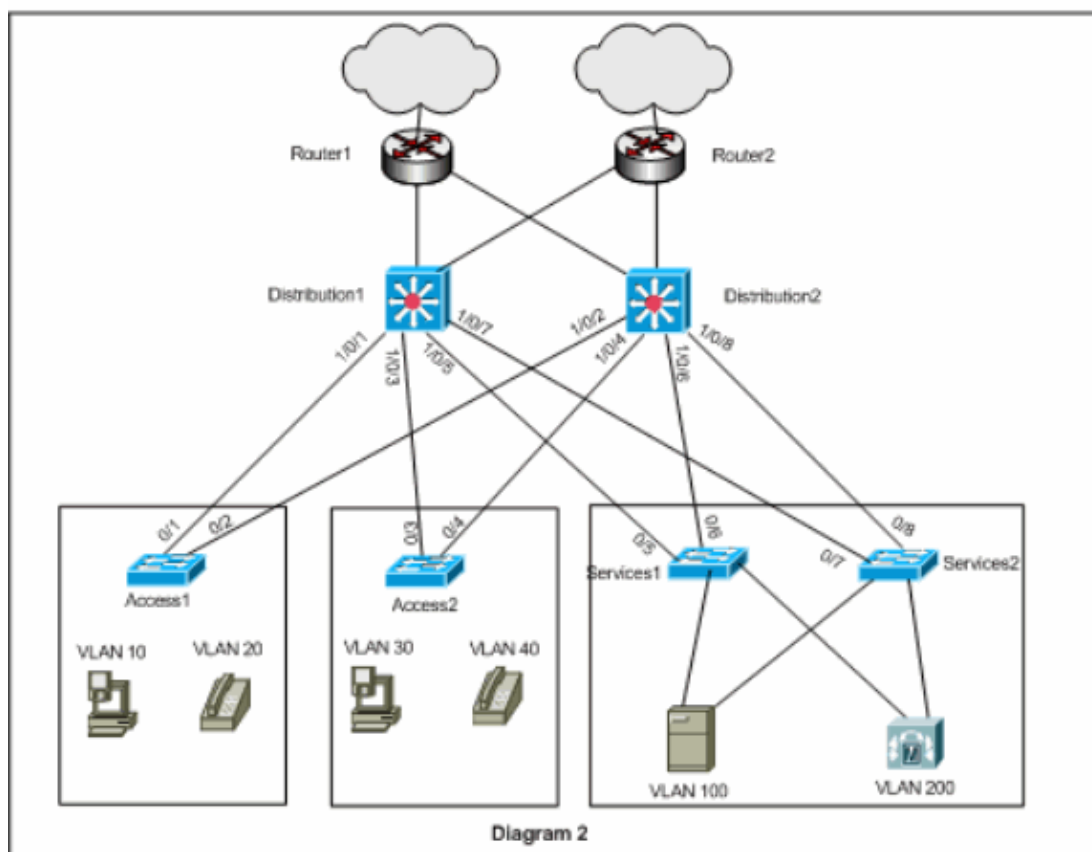
Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

The diagram shown here is an example for a small campus network. Distribution1 and Distribution 2 contain the Layer 3 VLAN interfaces and act as the gateway for the hosts in the access layer.

Diagram 2



Configurations

This document uses these configurations:

- Distribution1
- Distribution2

There are few points you need to consider before the GLBP configuration:

- When you configure the interfaces with GLBP, do not configure **glbp <group> ip <ip_address>** first. Configure the GLBP optional commands first, then configure the **glbp <group> ip <ip_address>** command.
- GLBP supports four types of load balancing. The default method is round-robin. Refer to Cisco GLBP Load Balancing Options for more information on the different load balancing options.

```
Distribution1
Distribution1(config)#interface vlan 10
Distribution1(config-if)#ip address 172.18.10.2 255.255.255.0
Distribution1(config-if)#glbp 10 priority 110
Distribution1(config-if)#glbp 10 preempt
Distribution1(config-if)#glbp 10 authentication md5 key-string s!a863
Distribution1(config-if)#glbp 10 ip 172.18.10.1
Distribution1(config-if)#exit

Distribution1(config)#interface vlan 20
Distribution1(config-if)#ip address 172.18.20.2 255.255.255.0
Distribution1(config-if)#glbp 20 priority 110
Distribution1(config-if)#glbp 20 preempt
Distribution1(config-if)#glbp 20 authentication md5 key-string s!a863
Distribution1(config-if)#glbp 20 ip 172.18.20.1
Distribution1(config-if)#exit

Distribution1(config)#interface vlan 30
Distribution1(config-if)#ip address 172.18.30.2 255.255.255.0
Distribution1(config-if)#glbp 30 priority 110
Distribution1(config-if)#glbp 30 preempt
Distribution1(config-if)#glbp 30 authentication md5 key-string s!a863
Distribution1(config-if)#glbp 30 ip 172.18.30.1
Distribution1(config-if)#exit

Distribution1(config)#interface vlan 40
Distribution1(config-if)#ip address 172.18.40.2 255.255.255.0
Distribution1(config-if)#glbp 40 priority 110
Distribution1(config-if)#glbp 40 preempt
Distribution1(config-if)#glbp 40 authentication md5 key-string s!a863
Distribution1(config-if)#glbp 40 ip 172.18.40.1
Distribution1(config-if)#exit

Distribution1(config)#interface vlan 100
Distribution1(config-if)#ip address 172.18.100.2 255.255.255.0
Distribution1(config-if)#glbp 100 priority 110
Distribution1(config-if)#glbp 100 preempt
Distribution1(config-if)#glbp 100 authentication md5 key-string s!a863
Distribution1(config-if)#glbp 100 ip 172.18.100.1
Distribution1(config-if)#exit

Distribution1(config)#interface vlan 200
Distribution1(config-if)#ip address 172.18.200.2 255.255.255.0
Distribution1(config-if)#glbp 200 priority 110
Distribution1(config-if)#glbp 200 preempt
Distribution1(config-if)#glbp 200 authentication md5 key-string s!a863
Distribution1(config-if)#glbp 200 ip 172.18.200.1
Distribution1(config-if)#exit
```

```
Distribution2
Distribution2(config)#interface vlan 10
Distribution2(config-if)#ip address 172.18.10.3 255.255.255.0
Distribution2(config-if)#glbp 10 authentication md5 key-string s!a863
Distribution2(config-if)#glbp 10 ip 172.18.10.1
```

```

Distribution2(config-if)#exit

Distribution2(config)#interface vlan 20
Distribution2(config-if)#ip address 172.18.20.3 255.255.255.0
Distribution2(config-if)#glbp 20 authentication md5 key-string s!a863
Distribution2(config-if)#glbp 20 ip 172.18.20.1
Distribution2(config-if)#exit

Distribution2(config)#interface vlan 30
Distribution2(config-if)#ip address 172.18.30.3 255.255.255.0
Distribution2(config-if)#glbp 30 authentication md5 key-string s!a863
Distribution2(config-if)#glbp 30 ip 172.18.30.1
Distribution2(config-if)#exit

Distribution2(config)#interface vlan 40
Distribution2(config-if)#ip address 172.18.40.3 255.255.255.0
Distribution2(config-if)#glbp 40 authentication md5 key-string s!a863
Distribution2(config-if)#glbp 40 ip 172.18.40.1
Distribution2(config-if)#exit

Distribution2(config)#interface vlan 100
Distribution2(config-if)#ip address 172.18.100.3 255.255.255.0
Distribution2(config-if)#glbp 100 authentication md5 key-string s!a863
Distribution2(config-if)#glbp 100 ip 172.18.100.1
Distribution2(config-if)#exit

Distribution2(config)#interface vlan 200
Distribution2(config-if)#ip address 172.18.200.3 255.255.255.0
Distribution2(config-if)#glbp 200 authentication md5 key-string s!a863
Distribution2(config-if)#glbp 200 ip 172.18.200.1
Distribution2(config-if)#exit

```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

From the configuration example, you can see that the Layer 3 VLAN interfaces in Distribution1 are set with higher GLBP priority 110 (default priority is 100). Therefore, Distribution1 becomes AVG for all the GLBP groups (10, 20, 30, 40, 100 and 200).

```

Distribution1#show glbp
VLAN10 - Group 10
  State is Active

  !--- AVG for the group 10.

  2 state changes, last state change 06:21:46
  Virtual IP address is 172.18.10.1
  Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.420 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption enabled, min delay 0 sec
  Active is local
  Standby is 172.18.10.3, priority 100 (expires in 9.824 sec)
  Priority 110 (configured)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    000f.3493.9f61 (172.18.10.3)

```

0012.80eb.9a00 (172.18.10.2) local
There are 2 forwarders (1 active)

Forwarder 1
State is Active

!--- Primary Virtual Forwarder for the virtual MAC 0007.b400.0102.

1 state change, last state change 1d01h
MAC address is **0007.b400.0102** (default)
Owner ID is 0012.80eb.9a00
Redirection enabled
Preemption enabled, min delay 30 sec
Active is local, weighting 100

Forwarder 2
State is Listen

!--- Secondary Virtual Forwarder for the virtual MAC 0007.b400.0103.

MAC address is 0007.b400.0103 (learnt)
Owner ID is 000f.3493.9f61
Redirection enabled, 598.762 sec remaining (maximum 600 sec)
Time to live: 14398.762 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 172.18.10.3 (primary), weighting 100 (expires in 8.762 sec)

!--- Output suppressed.

Distribution2#**show glbp**
VLAN10 - Group 10
State is Standby

!--- Standby Virtual Gateway for the group 10.

1 state change, last state change 02:01:19
Virtual IP address is 172.18.10.1
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.984 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption disabled
Active is 172.18.10.2, priority 110 (expires in 9.780 sec)
Standby is local
Priority 100 (default)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
There are 2 forwarders (1 active)

Forwarder 1
State is Listen

!--- Secondary Virtual Forwarder for the virtual MAC 0007.b400.0102.

MAC address is **0007.b400.0102** (learnt)
Owner ID is 0012.80eb.9a00
Time to live: 14397.280 sec (maximum 14400 sec)
Preemption enabled, min delay 30 sec
Active is 172.18.10.2 (primary), weighting 100 (expires in 7.276 sec)

Forwarder 2
State is Active

!--- Primary Virtual Forwarder for the virtual MAC 0007.b400.0103.

1 state change, last state change 02:02:57
MAC address is **0007.b400.0103** (default)
Owner ID is 000f.3493.9f61
Preemption enabled, min delay 30 sec

Active is local, weighting 100

!--- Output suppressed.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

%GLBP-4-DUPADDR: Duplicate address

The error message indicates a possible layer2 loop and STP configuration issues.

In order to resolve this issue, issue the **show interface** command to verify the MAC address of the interface. If the MAC address of the interface is the same as the one reported in the error message, then it indicates that this router is receiving its own hello packets sent. Verify the spanning-tree topology and check if there is any layer2 loop. If the interface MAC address is different from the one reported in the error message, then some other device with a MAC address reports this error message.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for LAN
Network Infrastructure: LAN Routing and Switching
Network Infrastructure: Getting Started with LANs

Related Information

- [Configuring GLBP](#)
- [Cisco GLBP Load Balancing Options](#)
- [LAN Product Support](#)
- [LAN Switching Technology Support](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 31, 2007

Document ID: 81565
