

Blue Coat® Systems

Reference Guide

WCCP Reference Guide

For SGOS 5.3



## Contact Information

Blue Coat Systems Inc.  
420 North Mary Ave  
Sunnyvale, CA 94085-4121

<http://www.bluecoat.com/support/contact.html>

[bcs.info@bluecoat.com](mailto:bcs.info@bluecoat.com)  
<http://www.bluecoat.com>

For concerns or feedback about the documentation: [documentation@bluecoat.com](mailto:documentation@bluecoat.com)

Copyright© 1999-2008 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of Blue Coat Systems, Inc. All right, title and interest in and to the Software and documentation are and shall remain the exclusive property of Blue Coat Systems, Inc. and its licensors. ProxyAV™, CacheOS™, SGOS™, SG™, Spyware Interceptor™, Scope™, ProxyRA Connector™, ProxyRA Manager™, Remote Access™ and MACH5™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, ProxySG®, WinProxy®, AccessNow®, Osis®, Powering Internet Management®, The Ultimate Internet Sharing Solution®, Cerberian®, Permeo®, Permeo Technologies, Inc.®, and the Cerberian and Permeo logos are registered trademarks of Blue Coat Systems, Inc. All other trademarks contained in this document and in the Software are the property of their respective owners.

BLUE COAT SYSTEMS, INC. DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL BLUE COAT SYSTEMS, INC., ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF BLUE COAT SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Document Number: 231-02966

Document Revision: WCCP Reference Guide—SGOS 5.3 8/2008

# Table of Contents

---

<b>WCCP Concepts</b> .....	<b>1-1</b>
Using WCCP with the ProxySG .....	1-2
WCCP Service Groups .....	1-3
Service Group Types .....	1-4
Service Group Addressing .....	1-4
Service Group Access Control .....	1-5
What Gets Redirected? .....	1-6
How Does the Router Forward Traffic? .....	1-7
GRE Forwarding .....	1-7
L2 Forwarding .....	1-8
Which ProxySG Receives the Redirected Traffic? .....	1-9
Load Balancing Weights .....	1-9
Automatic Redistribution of Loads .....	1-9
Hash Assignment .....	1-10
Mask Assignment .....	1-10
Getting Started .....	1-11
<b>Configuring WCCP on the Router</b> .....	<b>2-1</b>
Enabling WCCP and Defining the Service Group .....	2-2
Defining the Router Address .....	2-3
Defining the Unicast Address .....	2-3
Defining a Multicast Address .....	2-4
Verifying the Home Router Address .....	2-5
Filtering Traffic for Redirection .....	2-6
Filtering Which Web Caches Can Join the Service Group .....	2-7
Securing the Service Group .....	2-7
Applying Service Group Redirection to an Interface .....	2-8
Configuring Inbound Redirection .....	2-8
Configuring Outbound Redirection .....	2-8
<b>Configuring WCCP on the ProxySG</b> .....	<b>3-1</b>
Creating the WCCP Configuration File .....	3-2
Creating the Service Group Configuration .....	3-3
Defining the Service Group and Applying it to an Interface .....	3-4
Defining the Protocol and Ports to Redirect .....	3-4
Defining the Home Router Addresses .....	3-5
Defining the Forwarding/Return Method .....	3-7
Defining the Assignment Method .....	3-7
Securing the Service Group .....	3-10
Defining Multiple Service Groups .....	3-10

Installing the WCCP Configuration on the ProxySG .....	3-11
Installing the Configuration from the Management Console Text Editor .....	3-11
Installing the Configuration from a Local File .....	3-12
Installing the Configuration from a Remote URL .....	3-12
Installing the Configuration from the CLI .....	3-13
Enabling WCCP .....	3-14
Enabling WCCP From the Management Console .....	3-14
Enabling WCCP From the CLI .....	3-14
Verifying the WCCP Configuration .....	3-15
Verifying the WCCP Configuration from the Management Console .....	3-15
Verifying the WCCP Configuration from the CLI .....	3-16
Modifying the WCCP Configuration .....	3-17
Disabling WCCP .....	3-18
Disabling WCCP From the Management Console .....	3-18
Disabling WCCP From the CLI .....	3-18
<b>WCCP Configuration Examples .....</b>	<b>4-1</b>
Basic WCCP Configuration .....	4-2
Web-Cache Configuration .....	4-3
L2 Forwarding and Return .....	4-4
Secure Service Group .....	4-5
Redirect Specific Traffic .....	4-6
Multiple Service Groups .....	4-7
Load Balancing Using Hash Assignment .....	4-9
Hotspot Detection .....	4-11
Load Balancing Using Unequal Loads .....	4-13
Load Balancing Using Mask Assignment .....	4-15
Single ProxySG Multiple Routers .....	4-17
Multicast .....	4-18
Client IP Reflection .....	4-19
<b>Monitoring and Troubleshooting WCCP .....</b>	<b>5-1</b>
Service Group States .....	5-2
Viewing ProxySG Service Group Statistics .....	5-3
Viewing Service Group Statistics from the Management Console .....	5-4
Viewing Service Group Statistics from the CLI .....	5-4
Viewing Router Statistics .....	5-5
Fixing a Home Router Mismatch .....	5-8
Tested Platform Configurations .....	5-10
<b>WCCP Command Quick Reference .....</b>	<b>A-1</b>
Router WCCP Commands .....	A-2
ProxySG WCCP Commands .....	A-5

# List of Figures

---

Figure 1-1	A Simple ProxySG WCCP Exchange.....	1-2
Figure 1-2	Multiple Service Groups .....	1-3
Figure 1-3	Service Group Access Control .....	1-5
Figure 1-4	Determining What Traffic to Redirect .....	1-6
Figure 1-5	GRE Forwarding .....	1-7
Figure 1-6	L2 Forwarding.....	1-8
Figure 1-7	Load Balancing Weights .....	1-9
Figure 1-8	Automatic Redistribution of Loads.....	1-9
Figure 1-9	Hash Assignment.....	1-10
Figure 1-10	Mask Assignment .....	1-10
Figure 4-1	Basic WCCP Configuration Example.....	4-2
Figure 4-2	Web-Cache Configuration Example.....	4-3
Figure 4-3	L2 Forwarding and Return Example.....	4-4
Figure 4-4	Secure Service Group Example.....	4-5
Figure 4-5	Redirection of Specific Protocol and Ports Example .....	4-6
Figure 4-6	Multiple Service Groups Example .....	4-7
Figure 4-7	Load Balancing Using Hash Assignment Example .....	4-9
Figure 4-8	Load Balancing Using an Alternate Hash Example .....	4-11
Figure 4-9	Load Balancing Using Unequal Weights Example.....	4-13
Figure 4-10	Service Group with Multiple Routers and a Single ProxySG Example .....	4-17
Figure 4-11	Client IP Reflection Example .....	4-19



# 1 WCCP Concepts

---

The Web Cache Communication Protocol (WCCP) is a Cisco-developed protocol that allows certain Cisco routers and switches to transparently redirect traffic to a cache engine such as a ProxySG appliance. This chapter describes the WCCP concepts that you will need to understand in order to deploy WCCP on your ProxySG appliances.

This chapter includes the following topics:

- ❑ Using WCCP with the ProxySG—on page 1-2
- ❑ WCCP Service Groups—on page 1-3
- ❑ What Gets Redirected?—on page 1-6
- ❑ How Does the Router Forward Traffic?—on page 1-7
- ❑ Which ProxySG Receives the Redirected Traffic?—on page 1-9
- ❑ Getting Started—on page 1-11



**Note** Blue Coat recommends use of WCCP version 2. WCCP is available on select Cisco routers and switches only. Additionally, not every WCCP-capable router supports the same versions and feature sets. Before you begin configuring WCCP, check the documentation that came with your router/switch to ensure that it supports WCCP version 2 and that the WCCP features you plan to use are supported on the specific platforms and IOS versions you are running.

## Using WCCP with the ProxySG

When the ProxySG appliance is not in the physical path of clients and servers, it must rely on an external device—either a Layer 4 (L4) switch or a WCCP-capable router—to redirect packets to it for transparent proxy services. This type of deployment is known as a *virtually inline* deployment. WCCP is the recommended virtually inline deployment because it provides the following advantages:

- **Scalability and Load Balancing** — Traffic can be automatically distributed to up to 32 ProxySG appliances. If one ProxySG goes down, traffic is automatically redistributed across the other ProxySG appliances in the group.
- **Security** — You can password-protect the WCCP service group so that only authorized appliances can join. Additionally, you can configure access control lists (ACLs) on the router to restrict access to specific ProxySG appliances only.
- **Failover** — In the event that there are no ProxySG appliances available for traffic redirection, the router forwards the traffic to the original destination address.
- **Flexibility** — You control exactly what traffic to redirect and how to redirect it. You can redirect all traffic entering or exiting a router interface; you can filter traffic using ACLs; or, you can define specific protocol and ports to redirect.

In transparent proxy deployments, the client does not know that it is interacting with a ProxySG rather than the origin content server (OCS). Therefore, the packet from the client is addressed to the OCS. The router inspects the traffic on WCCP-enabled interfaces—either inbound or outbound depending on the configuration—and determines whether to redirect it based on the rules that have been agreed upon by the router and the ProxySG appliance(s).

The process works as follows:

1. The client sends a packet addressed for the OCS.
2. The WCCP-enabled router redirects the packet to the ProxySG.
3. The ProxySG determines what to do with it based on the transparent proxy services that have been configured for the traffic type. If it cannot service the request locally (for example by returning a page from its local cache), it sends a request to the specified OCS on behalf of the client.
4. The OCS response is routed (or redirected depending on the configuration) back to the ProxySG.
5. The ProxySG then forwards the response back to the client.

Figure 1-1 illustrates this process:

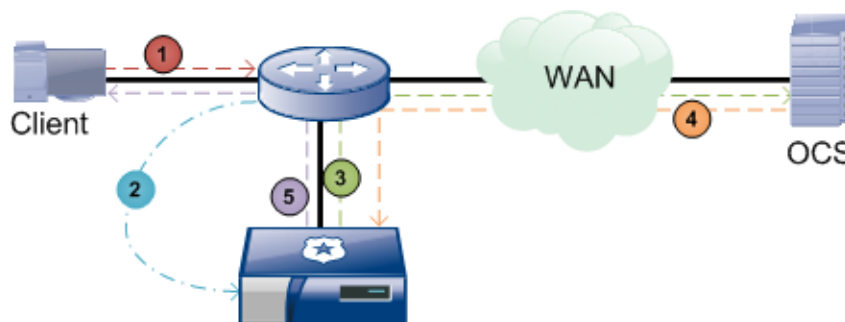


Figure 1-1 A Simple ProxySG WCCP Exchange

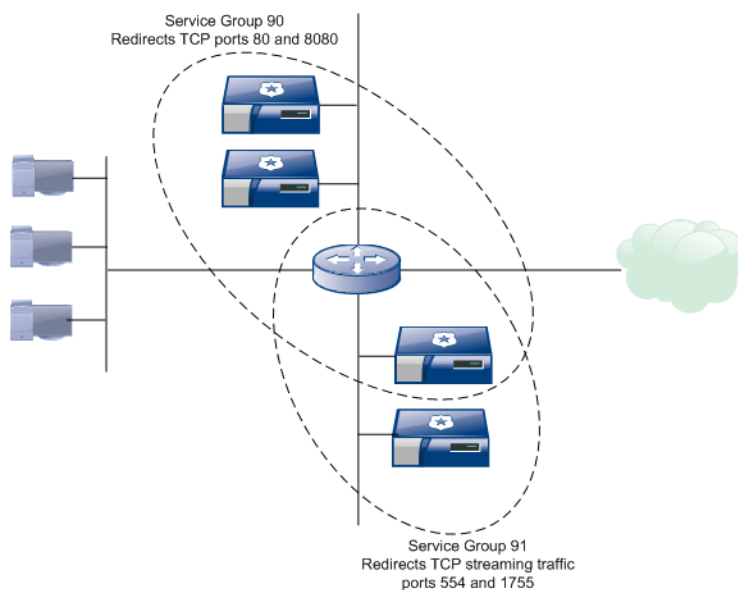


## WCCP Service Groups

A service group unites one or more routers/switches with one or more caching devices (ProxySG appliances in this case) in a transparent redirection scheme governed by a common set of rules. The service group members agree on these rules initially by announcing their specific capabilities and configurations to each other in WCCP protocol packets as follows:

1. The ProxySG appliance sends out a “Here I Am” (WCCP2\_HERE\_I\_AM) message to the routers in the group. These messages include a description of the service group that the ProxySG wants to join, including the protocol, ports to redirect, method to use to forward and return packets to each other, and load balancing instructions.
2. The routers respond with an “I See You” (WCCP2\_I\_SEE\_YOU) message that includes a Receive ID as well as a list of WCCP capabilities—such as forwarding methods or load balancing schemes—that the router supports.
3. The ProxySG appliance responds with another “Here I Am” message in which it reflects the Receive ID that was sent in the “I See You” message from the router. In addition, the ProxySG examines the capabilities advertised by the router and, if its configuration specifies a capability that has not been advertised, it will abandon its attempt to join the service group. If the capabilities it is configured to use are advertised, it will select the capabilities it wants to use and will send them back to the router in another “Here I Am” message.
4. The router inspects the capabilities that the ProxySG selected and, if the capabilities are supported, the router accepts the ProxySG as compatible and adds it to the service group. The router responds to all ProxySG appliances that it has accepted with “I See You” messages that include a listing of all ProxySG appliances in the service group (called the *router view*).
5. Each ProxySG in the group periodically sends out “Here I Am” messages to the routers in the group to maintain its service group membership. If a router doesn’t receive a “Here I Am” message from a ProxySG in the group within the designated time-out interval, it removes the ProxySG from the service group and sends out an “I See You” with an updated router view.

Note that the router and the switch can participate in multiple service groups as illustrated in Figure 1-2.



**Figure 1-2 Multiple Service Groups**

## Service Group Types

The service group configuration defines what type of traffic the routers in the group should intercept and how to handle the intercepted traffic. There are two types of service groups:

- **Well-known service groups** have a fixed set of traffic types and other characteristics that are known by the routers and the ProxySG appliances in the service group. Currently there is only one well-known service, web-cache, which redirects all TCP traffic with a destination port of 80.
- **Dynamic service groups** have characteristics that must be negotiated between the ProxySG and the routers. As soon as WCCP is enabled on the routers and the ProxySG appliances with the same service group identifier, the ProxySG appliances will begin advertising themselves and the WCCP services that have been configured for the group. If the router supports the capabilities that the ProxySG appliance advertises, the dynamic service group forms. The router maintains a list of all ProxySG appliances that are a part of the service group.

## Service Group Addressing

In order to establish and maintain a service group, the ProxySG appliances and routers must be able to communicate. The devices can communicate using unicast addresses or using a multicast group address. All devices in the group must be configured to use the same service group addressing. Each address type is described in Table 1-1.

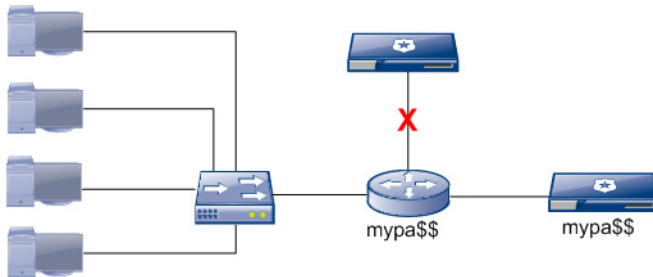
**Table 1-1 WCCP Service Group Addressing**

Service Group Addressing	Description
Unicast	With unicast addressing, each ProxySG must be configured with the IP addresses of all routers in the service group. The ProxySG will then send unicast "Here I Am" messages to each router in order to establish and maintain membership in the group. With unicast addressing, you will need to reconfigure each ProxySG whenever you add or remove a router from the group. In addition, as the number of devices in the group increases, so will the amount of WCCP traffic because each ProxySG will need to send individual messages to each router in the group rather than sending out a single, multicast message.
Multicast	With multicast addressing, the routers and ProxySG appliances in the service group communicate using a single IP address in the range of 224.0.0.0 to 239.255.255.255. To configure this, each ProxySG and each router in the group must be configured with the multicast IP address. Note that if the WCCP routers and/or ProxySG appliances are more than one hop apart, IP multicast routing must also be enabled on the intervening routers.

## Service Group Access Control

By default, when you configure a WCCP service group on one or more routers and one or more ProxySG appliances and enable WCCP on the devices, the devices will automatically begin communicating and trying to form a service group. There are two ways to restrict which Proxy SG appliances can join a service group:

- You can define an access control list (ACL) on the router that permits or denies specific ProxySG appliances and then associate the ACL with the service group. For more information, see *"Filtering Which Web Caches Can Join the Service Group"* on page 2-7.
- You can define an MD5 password on the ProxySG appliances and the routers that are authorized to join the service group so that a ProxySG appliance must authenticate before it is allowed to join the group. For instructions on how to set the password on the router, see *"Securing the Service Group"* on page 2-7. For instructions on how to set the password on the ProxySG, see *"Securing the Service Group"* on page 3-10.

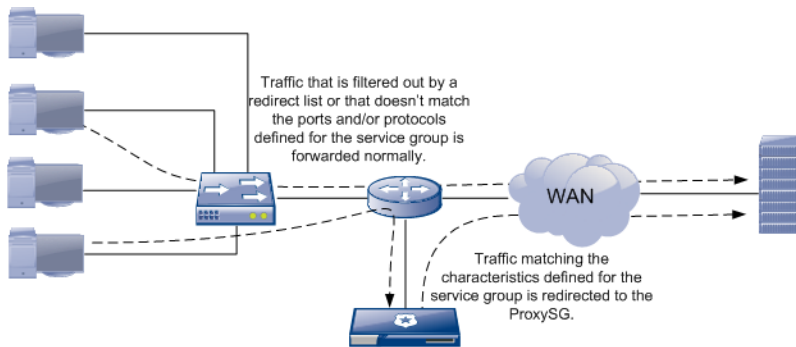


**Figure 1-3** Service Group Access Control

## What Gets Redirected?

When you configure the router and the ProxySG in a service group, you define the characteristics of the traffic that gets redirected. Without any configuration, all traffic gets redirected. However, you can use the following to configure the service group to redirect a specific set of traffic:

- **Router Redirect Lists** — On the router, you can set up access control lists (ACLs) that filter the packets to be redirected. For example, if you didn't want to redirect traffic from a specific host, you could create an ACL that denies traffic from the host and permits traffic from all other hosts and then associate the ACL with a redirect list in the router's service group configuration. For instructions, see *"Filtering Traffic for Redirection"* on page 2-6.
- **ProxySG WCCP Settings** — On the ProxySG, you can define specific port numbers and protocol to redirect. When the router receives a packet on an interface that is configured for redirection, it examines the packet header to determine whether the port numbers and protocol match those defined for the service groups that have been applied to the interface. If the traffic matches the service group characteristics, the router redirects it to the ProxySG. Otherwise, it performs a normal routing table lookup and forwards the packet to its destination. For instructions, see *"Defining the Protocol and Ports to Redirect"* on page 3-4.



**Figure 1-4** Determining What Traffic to Redirect

## How Does the Router Forward Traffic?

Because WCCP is used in transparent proxy deployments, the packets that the router intercepts use the destination address of the OCS rather than that of the ProxySG. Therefore, the router must transmit the packet to the ProxySG, yet still maintain the original characteristics of the packet so that the ProxySG will know what to do with it. When you configure the ProxySG, you specify a *forwarding method* that defines both how the router will forward packets to the ProxySG as well as how the ProxySG will return packets that it is unable to process back to the router. The ProxySG supports two forwarding methods as described in the following sections:

- GRE Forwarding—on page 1-7
- L2 Forwarding—on page 1-8



**Note** Not all routers/switches support all forwarding methods. See “*Tested Platform Configurations*” on page 5-10 for a list of the Cisco platforms that Blue Coat has tested with the ProxySG WCCP feature. Additionally, on some routers, separate methods are supported for forwarding and return. However, in this release, the ProxySG supports a single method, which is used for both packet forwarding (router to ProxySG) and return (ProxySG to router).

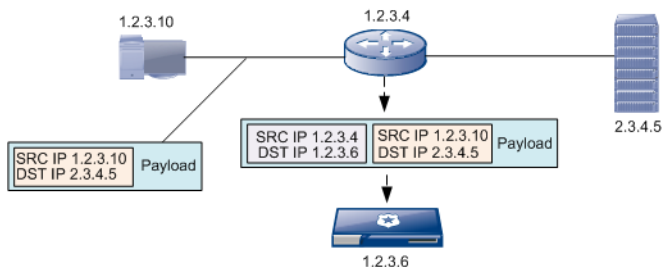
## GRE Forwarding

With Generic Routing Encapsulation (GRE) forwarding, the router encapsulates the intercepted packet in an additional IP header that shows the router address as the source IP address and the address of the ProxySG as the destination IP address. When the ProxySG receives the packet, it strips the outside header and then determines how to process the request, either forwarding the request on to the OCS or servicing it locally.



**Note** The ProxySG and the router use a reduced maximum transmission unit (MTU) for the GRE packet.

For instructions on configuring GRE forwarding, see “*Defining the Forwarding/Return Method*” on page 3-7.



**Figure 1-5** GRE Forwarding

## L2 Forwarding

With Layer 2 (L2) forwarding the router rewrites the destination MAC address of the intercepted packet to the MAC address of the ProxySG to which it is redirecting the packet. This method is faster than GRE forwarding because the forwarding is done at the hardware level and doesn't require encapsulating and decapsulating the packet at Layer 3. However, to use L2 forwarding, the ProxySG and the routers in the service group must all be on the same L2 broadcast domain (that is, there cannot be more than one hop between them). In addition, L2 forwarding is only supported on hardware-based switching platforms, such as the Catalyst series. To determine whether L2 forwarding is supported on your hardware platform, refer to your Cisco documentation. Also see *"Tested Platform Configurations"* on page 5-10 for a list of the Cisco platforms on which Blue Coat has tested L2 forwarding with the ProxySG. If you configure a forwarding method that is not supported by your WCCP-enabled routers/switches, the service group will fail to form.

For instructions on setting up L2 forwarding, see *"Defining the Forwarding/Return Method"* on page 3-7.

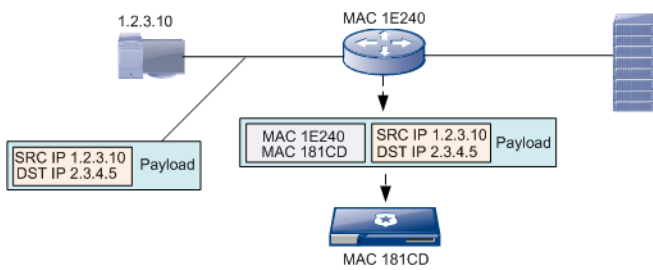


Figure 1-6 L2 Forwarding

## Which ProxySG Receives the Redirected Traffic?

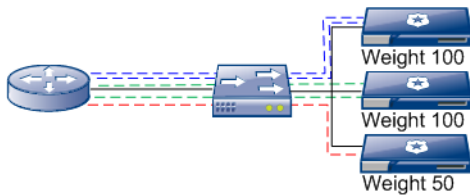
For every service group, you must configure the way the router determines the ProxySG to which to redirect a given packet. To do this you set an *assignment type* on the ProxySG. When the service group is formed, the ProxySG with the lowest IP address automatically becomes the *designated cache* (and if there is only one ProxySG in the service group, it is automatically the designated cache). The designated cache is responsible for communicating the assignment settings to the router, that is which ProxySG should be assigned a particular packet.

The ProxySG supports two assignment types as described in the following sections:

- Hash Assignment—on page 1-10
- Mask Assignment—on page 1-10

## Load Balancing Weights

Whichever assignment type you choose, each ProxySG in the service group is assigned roughly an even percentage of the load by default. However, you can override this behavior—for example if you have ProxySG appliances in the same service group that have different load capacities—by assigning a weight value to each ProxySG in the group. ProxySG appliances with higher weight values receive a higher proportion of the redirected traffic than ProxySG appliances with lower weight values. For example, suppose you have assigned the following weight values: ProxySG1=100, ProxySG2=100, and ProxySG3=50 respectively. The total weight value is 250, and so ProxySG1 and ProxySG2 will each receive 2/5 of the traffic (100/250) and ProxySG3 will receive 1/5 of the traffic (50/250).



**Figure 1-7** Load Balancing Weights

## Automatic Redistribution of Loads

If a ProxySG in the group becomes unavailable, the load will automatically be redistributed across the remaining ProxySG appliances.



**Figure 1-8** Automatic Redistribution of Loads

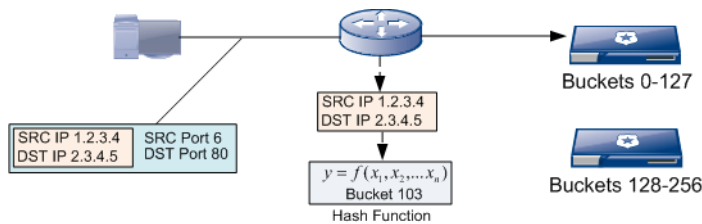
## Hash Assignment

With hash assignment—the default assignment method—the designated cache assigns each ProxySG in the service group a portion of a 256-bucket hash table and communicates the assignment to the routers in the group. When the router receives a packet for redirection, it runs the hashing algorithm against one or more of the fields in the packet header to determine the hash value. It then compares the value to the hash assignment table to see which ProxySG is assigned to the corresponding bucket and then forwards the packet to that appliance. When you configure the service group on the ProxySG appliances, you specify which field(s)—destination IP address, destination port, source IP address, and/or source port—should be used to calculate the hash value.

Because all of the packets are hashed using the same fields and algorithm, it is possible that one of the caches in the group can become overloaded. For example, if you have a large proportion of traffic that gets sent to the same server and you are using the destination IP address to run the hashing function, it is possible that the bulk of the traffic will be redirected to the same ProxySG. Therefore, you can configure an alternate field or group of fields to use to run the hashing algorithm. The router will then use this alternate hashing algorithm if the number of GRE packets or MAC addresses (depending on the forwarding method you’re using) redirected to a given ProxySG exceeds a certain number.

By default, each ProxySG in the service group is assigned roughly an even percentage of the 256-bucket hash table. However, you can override this behavior by configuring a hash-weight value to adjust the proportion of the hash table that gets assigned to the ProxySG.

For instructions on configuring hash assignment, see *“Configuring Hash Assignment”* on page 3-8.

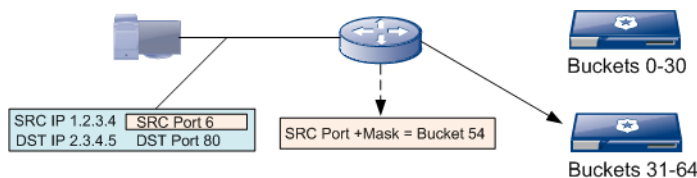


**Figure 1-9 Hash Assignment**

## Mask Assignment

With mask assignment, each router in the service group has a table of masks and values that it uses to distribute traffic across the ProxySG appliances in the service group. When the router receives a packet, it performs a bitwise AND operation between the mask value and the field of the packet header that is designated in the ProxySG mask assignment configuration. It then compares the result against its list of values for each mask; each value is assigned to a specific ProxySG in the service group.

For instructions on configuring mask assignment, see *“Configuring Mask Assignment”* on page 3-9.



**Figure 1-10 Mask Assignment**



## Getting Started

To configure WCCP on your routers and ProxySG appliances, you must complete the following steps:

1. Plan your service group:
  - ❑ Decide which routers and which ProxySG appliances will work together in the redirection scheme. Make sure that the routers that you plan to use to redirect traffic support WCCP Version 2.
  - ❑ Decide what traffic you want to redirect. Do you want to redirect all traffic, or just a specific protocol or ports? Do you want to exclude certain hosts or traffic from redirection?
  - ❑ Decide what forwarding method you plan to use. Make sure that all of the routers in the service group support the forwarding method.
  - ❑ Decide how the router will assign a specific redirected packet to a ProxySG. Make sure the router(s) in the service group support the assignment method you plan to use. If there is more than one ProxySG in the service group, decide whether you want to distribute traffic equally, or if you want to assign varying weights.
2. Configure the routers. At a minimum, you must do the following:
  - ❑ Create the service group and enable WCCP on the router. See *"Enabling WCCP and Defining the Service Group"* on page 2-2.
  - ❑ Apply the service group to the router interface where the traffic you want to redirect is entering or exiting. See *"Applying Service Group Redirection to an Interface"* on page 2-8.
  - ❑ If you're using multicast addressing, define the group address. See *"Defining a Multicast Address"* on page 2-4.
3. Configure the ProxySG appliances:
  - ❑ Create the text file that will contain the WCCP settings for the ProxySG appliance. See *"Creating the WCCP Configuration File"* on page 3-2.
  - ❑ Define the service group. When you create the service group settings on the ProxySG, you define the particulars of the redirection scheme, such as the address of the routers that will be intercepting traffic, the type of traffic to redirect, and the forwarding method that the routers and the ProxySG appliances will use to exchange packets. See *"Creating the Service Group Configuration"* on page 3-3.
  - ❑ Install the settings you defined in the WCCP text file on the ProxySG. See *"Installing the WCCP Configuration on the ProxySG"* on page 3-11.
4. Verify that the service group forms and that redirection begins. See *"Verifying the WCCP Configuration"* on page 3-15.



# 2 Configuring WCCP on the Router

---

This chapter describes how to configure WCCP on the router. It includes the following sections:

- ❑ Enabling WCCP and Defining the Service Group—on page 2-2
- ❑ Defining the Router Address—on page 2-3
- ❑ Filtering Traffic for Redirection—on page 2-6
- ❑ Filtering Which Web Caches Can Join the Service Group—on page 2-7
- ❑ Securing the Service Group—on page 2-7
- ❑ Applying Service Group Redirection to an Interface—on page 2-8

## Enabling WCCP and Defining the Service Group

Use the following procedure to enable WCCP on the router and define the service group.

<b>ROUTER CONFIGURATION—ENABLE WCCP AND DEFINE THE SERVICE GROUP</b>	
Step 1. Ensure that the router is running WCCP Version 2 (this is the default).	Router>enable Router#configure terminal Router(config)#ip wccp version 2
Step 2. Enable WCCP and specify the service group ID or keyword.	Router(config)#ip wccp 90
Step 3. Save the configuration.	Router(config)#copy running-config startup-config

## Defining the Router Address

With WCCP Version 2, routers and ProxySG appliances in a service group can either communicate directly using unicast addresses, or they can communicate to all members of the service group simultaneously using a multicast group address. Whether you use unicast or multicast addressing, you must ensure that the address you configure on the ProxySG appliances matches what is configured on the router.

On the ProxySG, you will need to configure the router address (either the unicast or multicast address) as a `home-router` in the service group. For instructions on configuring the `home-router` on the ProxySG, see *"Defining Unicast Router Addresses"* on page 3-6.

The following sections describe how to define the address on the router and how to verify what address is used as the WCCP router address.

- Defining the Unicast Address—on page 2-3
- Defining a Multicast Address—on page 2-4
- Verifying the Home Router Address—on page 2-5

## Defining the Unicast Address

In most cases, the router will already have one or more IP addresses assigned to it. You do not need to do any further configuration.

If the router does not yet have an IP address, use the following procedure to configure one on the interface(s) that will be redirecting traffic and the interface that is connected to the ProxySG.

ROUTER CONFIGURATION—DEFINE A UNICAST ADDRESS	
Step 1. Go to the router interface.	Router>enable Router#configure terminal Router(config)#interface <i>gigabitEthernet2/1</i>
Step 2. Set the IP address and subnet mask for the interface.	Router(config-if)#ip address <i>10.1.0.1</i> <i>255.255.255.0</i>
Step 3. Enable the interface.	Router(config-if)#no shutdown Router(config-if)#exit Router(config)#exit
Step 4. Save the configuration.	Router#copy running-config startup-config



**Note** For best results, attach the ProxySG to a router interface that is not used for redirection.

## Defining a Multicast Address

There are a couple of reasons why it is advantageous to use multicast in your service groups:

- It reduces the amount of WCCP protocol traffic that is running on your network.
- You can add and remove ProxySG appliances and/or routers to the service group at any time without having to reconfigure the other group members.



**Note** There are several known router issues related to the use of WCCP multicast service group addressing. If you are having trouble getting your WCCP configuration to work, consider using unicast addressing rather than multicast addressing.

Use the following procedure to define a multicast address for a service group on the router.

ROUTER CONFIGURATION—DEFINE A MULTICAST ADDRESS	
Step 1. Go to global configuration mode.	Router>enable Router#configure terminal
Step 2 Enable multicast routing. <b>Note</b> If there are any intervening routers between this router and the ProxySG appliances, you will also need to enable multicast routing on those routers.	Router(config)#ip multicast-routing
Step 3 Define the multicast address for the service group. The multicast address must be in the range 224.0.0.0 to 239.255.255.255.	Router(config)#ip wccp 90 group-address 224.1.1.103
Step 4 Go to the interface that is connected to the ProxySG.	Router(config)#interface gigabitEthernet2/1
Step 5 Enable the WCCP multicast group address on the interface.	Router(config-if)#ip wccp 90 group-listen
Step 6 (optional) On Catalyst 6500 series switches and Cisco 7600 series routers, you must also enable Protocol Independent Multicast (PIM) on the interface in order for multicast addressing to work properly on the service group. Refer to your router documentation for more information on PIM.	Router(config-if)#ip pim sparse-mode
Step 7 Save the configuration.	Router(config-if)#copy running-config startup-config

## Verifying the Home Router Address

It is always a good idea to verify that WCCP is using the IP address that you think it is using as its WCCP router identifier before you configure the `home-router` on the ProxySG appliances in the service group. Use the following procedure to verify the WCCP address that the router is using. Note that if the router has more than one IP address assigned to it, the highest IP address will be designated as the WCCP router identifier.

ROUTER CONFIGURATION—DISPLAY THE WCCP ROUTER IDENTIFIER	
Step 1 Go to privileged mode.	Router>enable
Step 2 Show the WCCP configuration for a particular service group. You must use the value of the Router Identifier as the <code>home-router</code> address when you configure the ProxySG.	<pre>Router#show ip wccp 90  Global WCCP information:   Router information:     <b>Router Identifier:</b>      <b>10.1.0.18</b>     Protocol Version:        2.0</pre>

## Filtering Traffic for Redirection

You can use an access control list (ACL) to control what traffic gets redirected using WCCP. To do this, you must define the ACL that filters the traffic and then associate the ACL with the router WCCP `redirect-list` command. For example, you might have specific hosts on your network that you do not want proxied. In this case, you could create an ACL that denies that particular host and allows all other hosts. You can then apply the ACL to the WCCP service group.



**Note** Router ACL support varies from platform to platform. Some routers do not support deny rules in ACLs; other routers do not support ACLs at all. Refer to your router/switch documentation to determine whether ACLs are supported on your specific platform.

Note that there are two types of traffic you must not filter using a redirect list. If you do, WCCP will not work:

- UDP — The router and the ProxySG communicate over UDP and blocking UDP traffic will prevent the service group from forming.
- GRE — If you block the Generic Routing Encapsulation (GRE) protocol and you are using GRE forwarding, the ProxySG will not see the redirected packets.

Use the following procedure to configure filtering of traffic to be redirected using an ACL. Note that you must define the ACL before you associate it with a WCCP redirect list.

ROUTER CONFIGURATION—FILTER TRAFFIC FOR REDIRECTION	
Step 1. Go to global configuration mode.	Router>enable Router#configure terminal
Step 2 Create the ACL to permit or deny specific traffic.  <b>Note</b> For detailed instructions on how to create an ACL, refer to your router documentation.	Router(config)#access-list 103 deny ip any host 10.1.0.43 Router(config)#access-list 103 permit ip any any
Step 3 Associate the ACL with a WCCP redirect list.	Router(config)#ip wccp 90 redirect-list 103
Step 4 Save the configuration.	Router(config)#copy running-config startup-config



## Filtering Which Web Caches Can Join the Service Group

You can use router ACLs to define which ProxySG appliances are allowed to join a particular service group. The easiest way to do this is to define a standard ACL that permits access for the specific ProxySG appliances you want to allow in the group (the implicit deny rule in the ACL will deny access to all other hosts automatically).

Use the following procedure to restrict service group access to a specific set of caches based on an ACL.

ROUTER CONFIGURATION—FILTER WEB CACHE SERVICE GROUP MEMBERSHIP	
Step 1. Go to global configuration mode.	Router>enable Router#configure terminal
Step 2. Create the ACL to permit or deny specific ProxySG appliances. <b>Note</b> For detailed instructions on how to create an ACL, refer to your router documentation.	Router(config)#access-list 3 permit 10.1.1.5 0.0.0.255
Step 3. Associate the ACL with the service group group-list.	Router(config)#ip wccp 90 group-list 3
Step 4. Save the configuration.	Router(config)#copy running-config startup-config

## Securing the Service Group

For added security, you can configure MD5 authentication between the ProxySG appliances and the routers in the group. When authentication is enabled, a ProxySG will not be allowed to join the service group unless it knows the password. To configure authentication, you must define the same password on all routers and all ProxySG appliances in the service group.

The following procedure describes how to set the password on the router. For instructions on how to set the password on the ProxySG appliances in the service group, see *"Securing the Service Group"* on page 3-10.

ROUTER CONFIGURATION—ENABLE MD5 AUTHENTICATION	
Step 1. Go to global configuration mode.	Router>enable Router#configure terminal
Step 2. Define a password (up to 8 characters) for the service group. This command must also include the encryption type, which can be 0 (indicating that password is not yet encrypted) or 7 (indicating that the password is encrypted using a Cisco-proprietary encryption algorithm).	Router(config)#ip wccp 90 password 0 \$abc123
Step 3. Save the configuration.	Router(config)#copy running-config startup-config

## Applying Service Group Redirection to an Interface

After you define a service group, you must apply the service group configuration to an interface before the router can begin intercepting traffic. The router can intercept traffic as it enters the router (inbound) or as it leaves the router (outbound). In most cases you will want to intercept the traffic as it enters the router, which speeds up the redirection process because it happens before the routing table lookup. However, the decision about where to apply the redirection really depends on your network topology and the specific capabilities of the routers/switches on which you're running WCCP.

The following sections describe how to apply service group redirection to an interface:

- "Configuring Inbound Redirection" on page 2-8
- "Configuring Outbound Redirection" on page 2-8

### Configuring Inbound Redirection

Use the following procedure to enable inbound redirection on an interface.

ROUTER CONFIGURATION—CONFIGURE INBOUND REDIRECTION	
Step 1. Go to interface configuration mode on the interface where you want to enable inbound redirection.	Router>enable Router#configure terminal Router(config)#interface <i>gigabitEthernet2/2</i>
Step 2 Enable redirection for the service group.	Router(config-if)#ip wccp 90 redirect in
Step 3 Save the configuration.	Router(config-if)#copy running-config startup-config

### Configuring Outbound Redirection

Use the following procedure to enable outbound redirection on an interface.

ROUTER CONFIGURATION—CONFIGURE OUTBOUND REDIRECTION	
Step 1. Go to interface configuration mode on the interface where you want to enable outbound redirection.	Router>enable Router#configure terminal Router(config)#interface <i>gigabitEthernet2/3</i>
Step 2 Enable redirection for the service group.	Router(config-if)#ip wccp 90 redirect out

**ROUTER CONFIGURATION—CONFIGURE OUTBOUND REDIRECTION (CONTINUED)**

Step 3 If you are using outbound redirection in a client IP reflection configuration, you must also exclude the interface where the router connects to the ProxySG from redirection. This protects ProxySG traffic from redirection.	<pre>Router(config-if)#exit Router(config)#interface <i>gigabitEthernet2/1</i> Router(config-if)#ip wccp redirect exclude in</pre>
Step 4 Save the configuration.	<pre>Router(config-if)#copy running-config startup-config</pre>



# 3 Configuring WCCP on the ProxySG

---

This chapter provides procedures for configuring WCCP on the ProxySG. To configure WCCP, you define the configuration settings in a separate text file and then install this file to the ProxySG. If you are not yet familiar with the WCCP features, see [Chapter 1, WCCP Concepts](#).

Note that you must configure the required WCCP settings on the cooperating routers before you configure the ProxySG. If you have not yet configured your WCCP routers/switches, see [Chapter 2, Configuring WCCP on the Router](#) for instructions.

This chapter includes procedures for creating the configuration settings as well as for installing the settings and enabling WCCP on the ProxySG. It includes the following topics:

- ❑ Creating the WCCP Configuration File—on page 3-2
- ❑ Creating the Service Group Configuration—on page 3-3
- ❑ Installing the WCCP Configuration on the ProxySG—on page 3-11
- ❑ Enabling WCCP—on page 3-14
- ❑ Verifying the WCCP Configuration—on page 3-15
- ❑ Modifying the WCCP Configuration—on page 3-17
- ❑ Disabling WCCP—on page 3-18


## Creating the WCCP Configuration File

In order to configure the WCCP settings on a ProxySG, you must create a WCCP configuration file, which is a text file that contains the WCCP settings specific to the ProxySG appliance. Once you’ve defined the WCCP settings in the file, you install the settings on the ProxySG.

The first step is to create the file. You can create a WCCP configuration file three ways:

- Using the text editor of your choice, create a text file on a remote machine that is accessible by the ProxySG via a URL.
- Using the text editor of your choice, create a text file locally on the system from which you run the Management Console.
- Create a text file using the text editor in the Management Console.

Use the following procedure to create a new WCCP configuration file using the text editor in the ProxySG Management Console and define the global settings, which are the WCCP settings that are not service group specific. You will add the remaining WCCP settings to the file after you create the global settings.

ProxySG CONFIGURATION—DEFINE THE GLOBAL WCCP SETTINGS	
<p>Step 1 To create the text file from within the ProxySG Management Console, log in to the web interface and then go to the <b>WCCP</b> tab in the Management Console.</p>	<p>From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b>.</p>
<p>Step 2 Open the text editor.</p> 	<p>Select <b>Text Editor</b> from the <b>Install WCCP Settings from</b> drop-down list and then click <b>Install</b>. The text editor opens. If this is a new configuration, the following comment is displayed:</p> <pre>; Empty WCCP configuration object</pre> <p>You can delete this comment.</p>
<p>Step 3 Enable WCCP. If you enable WCCP from within the configuration file, it will automatically be enabled when you install the settings. You can also enable WCCP from the ProxySG CLI or Management Console. See “Enabling WCCP” on page 3-14.</p>	<pre>wccp enable</pre>
<p>Step 4 Ensure that the ProxySG is running WCCP Version 2 (this is the default). You should not need to enter this command unless the ProxySG is currently configured to use WCCP Version 1.</p>	<pre>wccp version 2</pre>
<p>Step 5 Create the service groups.</p>	<p>See “Creating the Service Group Configuration” on page 3-3.</p>

## Creating the Service Group Configuration

The service group configuration defines what type of traffic the routers in the group should intercept and how to handle the intercepted traffic. The following sections describe how to create the service group, define its characteristics, and apply the configuration to a ProxySG interface:

- ❑ [Defining the Service Group and Applying it to an Interface—on page 3-4](#)
- ❑ [Defining the Protocol and Ports to Redirect—on page 3-4](#)
- ❑ [Defining the Home Router Addresses—on page 3-5](#)
- ❑ [Defining the Forwarding/Return Method—on page 3-7](#)
- ❑ [Defining the Assignment Method—on page 3-7](#)
- ❑ [Securing the Service Group—on page 3-10](#)
- ❑ [Defining Multiple Service Groups—on page 3-10](#)

## Defining the Service Group and Applying it to an Interface

The following procedure describes the settings that you must add to the WCCP configuration file to define a service group and apply it to a ProxySG interface.

ProxySG CONFIGURATION—DEFINE THE SERVICE GROUP AND APPLY IT TO AN INTERFACE	
<p>Step 1 Define the service group. Note that you can use the <code>web-cache</code> keyword to configure redirection on destination port 80 only, or you can specify a dynamic service group ID in the range of 0-99 inclusive.</p>	<pre>service-group 90</pre>
<p>Step 2 Apply the service group a ProxySG interface. You must apply the service group to at least one interface. As a best practice, apply the service group to the first LAN interface on the appliance, for example 0:1 on the 210 platform; 2:1 on the 510 and 810 platforms; or 3:1 on the 8100.</p>	<pre>interface 2:1</pre>
<p>Step 3 (optional) Specify the queuing priority in the range of 0 through 255 (inclusive) for the service group. If there are multiple service groups applied to the same router interface in the same direction, the priority defines the order in which the router evaluates them.</p>	<pre>priority 1</pre>

## Defining the Protocol and Ports to Redirect

The service group configuration on the ProxySG defines what protocol and ports to redirect. If you are using a well-known service group such as `web-cache`, the protocol and ports are already known to the ProxySG and the routers so you do not need to define them. However, if you are using a dynamic service group, you must define the protocol and ports as part of the service group configuration. By default, the dynamic service group redirects all ports and protocols without any additional configuration. However, if you want to redirect specific ports only, you'll need to enable port-based redirection and specify the ports (up to 8) that the service group should redirect.



**Note** You can only specify 8 ports to redirect within a single service group. If you want to redirect more than 8 ports, you must create multiple service groups.

The following procedure describes the settings you must add to the configuration file to restrict service group redirection to a specific protocol and set of ports.



<b>ProxySG CONFIGURATION—DEFINE THE PROTOCOL AND PORTS TO REDIRECT</b>	
Step 1. Define the protocol to redirect. To do this, use a standard protocol number as defined by <a href="http://www.iana.org">http://www.iana.org</a> . Typically, WCCP service groups would redirect a Web protocol such as TCP (6) or UDP (17).	<code>protocol 6</code>
Step 2 (optional) Enable port-based redirection. You only need to do this if you want to redirect a specific set of ports for the specified protocol; by default all ports are redirected.	<code>service-flags ports-defined</code>
Step 3 Specify the ports to redirect. You can redirect up to 8 ports per service group. If you are not specifying all 8 ports, you must fill the remaining port argument values with zeroes. This command is required if you enabled port-based redirection.	<code>ports 80 8080 0 0 0 0 0 0</code>
Step 4 (optional) Specify the port field on which to base redirection. By default, the service group uses the destination port to determine whether or not the packet gets redirected. However, in some cases—for example if you're redirecting inbound traffic rather than outbound traffic—you may want to redirect traffic based on the source port instead. If you want to base redirection on the destination port, you do not need to enter a command.	<code>service-flags ports-source</code>

## Defining the Home Router Addresses

To establish and maintain the service group, the ProxySG appliances and routers in the service group must be able to communicate with each other. In order to establish this communication, you must define address(es) that the ProxySG should use to contact the router(s) in the group. WCCP allows you to use unicast or multicast addresses for communication between routers and caches. The following sections provide procedures for each type of addressing:

- Defining Unicast Router Addresses—on page 3-6
- Defining a Multicast Group Address—on page 3-6

### Defining Unicast Router Addresses

If you are using unicast addresses within the service group, you must create a `home-router` setting in the ProxySG configuration for each router—up to a maximum of 32—in the service group. The `home-router` IP address that you define must be reachable from the ProxySG; as a best practice, use the IP address that is identified as the WCCP router ID on the router (see “*Verifying the Home Router Address*” on page 2-5).

Use the following procedure to define the routers in the service group.

ProxySG CONFIGURATION—DEFINE UNICAST ROUTER ADDRESSES	
<p>Step 1 On the router, verify which IP address has been designated as the WCCP router identifier, which is always the highest IP address on the router. You must use this address for the <code>home-router</code> setting on the ProxySG. Repeat this step for each WCCP router.</p>	<pre>Router&gt;enable Router#show ip wccp 90  Global WCCP information:   Router information:     <b>Router Identifier:</b>      10.1.0.18     Protocol Version:        2.0</pre>
<p>Step 2 On the ProxySG, add a <code>home-router</code> setting to the WCCP text file for each router in the service group.</p>	<pre>home-router 1.2.3.1 home-router 1.2.3.2 home-router 1.2.3.3 home-router 10.1.0.18</pre>

### Defining a Multicast Group Address

With multicast addressing, the ProxySG appliances and the routers in the service group use a single multicast address—in the range of 224.0.0.0 to 239.255.255.255—to communicate with all other group members simultaneously. In this case, you only configure a single `home-router` setting in the ProxySG configuration. You will also need to configure each router in the group to use this address as described in “*Defining a Multicast Address*” on page 2-4. Use the following procedure to define the multicast address for the service group:

ProxySG CONFIGURATION—DEFINE A MULTICAST SERVICE GROUP ADDRESS	
<p>Step 1 To use multicast addressing, create a single <code>home-router</code> entry for the service group.</p>	<pre>home-router 224.1.1.103</pre>
<p>Step 2 (optional) Define the multicast time to live (TTL) value if you want to use a value other than the default (1).</p>	<pre>multicast-ttl 3</pre>

## Defining the Forwarding/Return Method

On the ProxySG, the forwarding method specifies the method the router uses to forward packets to the ProxySG as well as the method the ProxySG uses to return packets that chooses to bypass. There is no separate return method in this version of SGOS. Because not all routers support all forwarding and return methods, you must determine what methods are supported on your specific routing/switching platform and IOS version before configuring the forwarding method.



**Note** Although SGOS versions 5.1 and 5.2 supported mixed forward and return methods, SGOS version 5.3 requires that the forward and return method be the same. There is no separate setting for configuring the return method in SGOS 5.3.

The ProxySG supports the following forwarding methods:

- Generic Routing Encapsulation (GRE) forwarding, in which the packet to be redirected is encapsulated in an additional IP header that shows the router address as the source IP address and the address of the ProxySG as the destination IP address. This is the default forwarding method and if you plan to use this method you do not need to do any further configuration. Keep in mind, however, that not all routers support GRE forwarding. Typically, GRE forwarding is supported on software-based switching platforms such as the Cisco 800, 1800, 2800, 3800, 7200, and 7500.
- Layer 2 (L2) forwarding, in which the router rewrites the destination MAC address of the packet to the MAC address of the ProxySG to which it is redirecting the packet. This method is faster than GRE forwarding, because the forwarding is done at the hardware level and doesn't require encapsulating and decapsulating the packet at Layer 3. In order to use L2 forwarding, the ProxySG and the routers in the service group must all be on the same L2 broadcast domain (that is, there cannot be more than one hop between them). Typically L2 forwarding is supported on hardware-based switching platforms such as the Cisco Catalyst 3550, 3650, 3750, 4500, 6500, and 7600.

The following procedure shows how to set the forwarding method in the WCCP configuration file.

### ProxySG CONFIGURATION—DEFINE THE FORWARDING/RETURN METHOD

If you want to use the L2 forwarding/return method rather than the default GRE forwarding/return, you must add the following command to the service group configuration.

```
forwarding-type L2
```

## Defining the Assignment Method

The assignment method instructs the router how to distribute redirected traffic. There are two supported assignment methods: hash assignment (the default) and mask assignment. Keep in mind that not all routing platforms and software versions support both assignment method; refer to your router/switch documentation to determine which assignment methods are supported on your specific platform. Also see *"Tested Platform Configurations"* on page 5-10 to see the Cisco platforms on which Blue Coat has successfully tested each assignment method. You can use different assignment methods for different service groups configured on the same ProxySG.

The following sections describe how to configure each of the assignment methods:

- Configuring Hash Assignment—on page 3-8
- Configuring Mask Assignment—on page 3-9

### Configuring Hash Assignment

With hash assignment, the router runs a value in the header of the packet it is redirecting through a hashing function. The resulting value maps to one of 256 buckets in the hash table, each of which is assigned to a ProxySG in the service group. Hash assignment can be CPU intensive, but it is the only option if you are using a software-based router.

Because the hashing function is based on a packet header field, it is possible that a disproportionate amount of traffic will be redirected to the same ProxySG. For example if the hashing function is based on destination IP address and many users are sending requests to the same destination, a disproportionate number of packets will get redirected to the same ProxySG. To prevent a given ProxySG from being inundated, you can configure an alternate hashing field for the router to use if the number of GRE packets or MAC addresses (depending on the forwarding method you’re using) redirected to a given ProxySG exceeds a certain number.

By default, each ProxySG in the service group is assigned roughly an even percentage of the 256-bucket hash table. However, you can override this behavior by configuring a hash-weight value to adjust the proportion of the hash table that gets assigned to the ProxySG.

Use the following commands to configure hash assignment in the service group:

<b>ProxySG CONFIGURATION—CONFIGURE HASH ASSIGNMENT</b>	
<p>Step 1 (optional) Enable the hash assignment method. Because this is the default assignment method, this command is not required.</p>	<pre>assignment-type hash</pre>
<p>Step 2 Specify which field(s) in the packet header to use to run the hashing function. Use a separate setting for each field. Possible values are:</p> <ul style="list-style-type: none"> <li>• source-ip-hash</li> <li>• destination-ip-hash</li> <li>• source-port</li> <li>• destination-port</li> </ul>	<pre>service-flags destination-ip-hash service-flags destination-port</pre>
<p>Step 3 (optional) Define what proportion of the hash table you want assigned to the specified interface on the ProxySG (0-255). Keep in mind that if you have assigned hash weight values to any of the ProxySG appliances in the service group, you will have to configure it on all of the others or that appliance will not receive any of the redirected traffic (because the default value is 0).</p>	<pre>primary-hash-weight 0:1 45</pre>
<p>Step 4 (optional) Define an alternate packet header field to use to run the hashing function. This setting will be used if a ProxySG in the service group gets overloaded. Possible values are:</p> <ul style="list-style-type: none"> <li>• source-ip-alternate-hash</li> <li>• destination-ip-alternate-hash</li> <li>• source-port-alternate-hash</li> <li>• destination-port-alternate-hash</li> </ul>	<pre>service-flags destination-port-alternate-hash</pre>

## Configuring Mask Assignment

With mask assignment, each router in the service group has a table of masks and values that it uses to distribute traffic across the ProxySG appliances in the service group. When the router receives a packet, it performs a bitwise AND operation between the mask value and the field of the packet header that is designated in the ProxySG mask assignment configuration. It then compares the result against its list of values for each mask; each value is assigned to a specific bucket, which corresponds to a ProxySG in the service group.

By default, each ProxySG in the service group is assigned roughly an even percentage of the mask values. However, you can override this behavior by configuring a hash-weight value to adjust the proportion of the mask values that gets assigned to the ProxySG.

The following procedure shows how to configure mask assignment in the WCCP configuration file on the ProxySG.

<b>ProxySG CONFIGURATION—CONFIGURE MASK ASSIGNMENT</b>		
Step 1	Enable the mask assignment method.	<code>assignment-type mask</code>
Step 2	(optional) Specify which field in the packet header to use to run the mask function. You only need to specify a mask-scheme if you want to use a field other than the default (destination IP) to run the mask function. Possible values are: <ul style="list-style-type: none"> <li>• <code>source-ip</code></li> <li>• <code>destination-ip</code></li> <li>• <code>source-port</code></li> <li>• <code>destination-port</code></li> </ul>	<code>mask-scheme destination-ip</code>
Step 3	(optional) Define what proportion of the mask values to assign to the specified interface on the ProxySG (0-255). If you have assigned hash weight values to any of the ProxySG appliances in the service group, you will have to configure it on all of the others or that appliance will not receive any of the redirected traffic (because the default value is 0).	<code>primary-hash-weight 0:1 45</code>

## Securing the Service Group

For added security, you can configure MD5 authentication to control access to the service group. When authentication is enabled, a ProxySG will not be allowed to join the service group unless it knows the password. To configure authentication, you must define the same password on all routers and all ProxySG appliances in the service group.

The following procedure describes how to set up a password in the WCCP configuration file on the ProxySG. For instructions on how to set up a password on the router, see *"Securing the Service Group"* on page 2-7.

ProxySG CONFIGURATION—SECURE THE SERVICE GROUP	
Define a password (up to 8 characters) for the service group.	<code>password \$abc123</code>

## Defining Multiple Service Groups

You can define up to 100 (0-99) service groups within a single ProxySG WCCP configuration file. However, you must separate each service group configuration with the `end` command. For example, the following configuration file defines service groups 90 (which redirects traffic from client to server) and 91 (which redirects traffic from server to client):

```
wccp enable
wccp version 2
service-group 90
priority 1
protocol 6
service-flags destination-ip-hash
service-flags ports-defined
ports 139 445 80 443 0 0 0 0
interface 0:0
home-router 1.1.1.1
end

service-group 91
priority 1
protocol 6
service-flags source-ip-hash
service-flags ports defined
service-flags ports-source
ports 139 445 80 443 0 0 0 0
interface 0:0
home-router 1.1.1.1
end
```

## Installing the WCCP Configuration on the ProxySG

After you define all of the service groups that you want to configure on a ProxySG in your WCCP configuration file, you must install the settings. The way you install the file depends on how and where you created it. Use one of the following procedures to install the ProxySG WCCP configuration file:

- Installing the Configuration from the Management Console Text Editor—on page 3-11
- Installing the Configuration from a Local File—on page 3-12
- Installing the Configuration from a Remote URL—on page 3-12
- Installing the Configuration from the CLI—on page 3-13

### Installing the Configuration from the Management Console Text Editor

If you entered the WCCP configuration commands directly into the Management Console text editor, you can install the file as soon as you finish creating it.

<b>ProxySG CONFIGURATION—INSTALL WCCP SETTINGS USING THE TEXT EDITOR</b>		
Step 1	Go to the <b>WCCP</b> tab in the Management Console.	From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b> .
Step 2	Open the text editor.	Select <b>Text Editor</b> from the <b>Install WCCP Settings from</b> drop-down list and then click <b>Install</b> .
Step 3	After configuring all of the service groups that this ProxySG will participate in, install the configuration file.	Click <b>Install</b> . The Management Console displays a message indicating that the configuration file was successfully installed. Click <b>OK</b> .
Step 4	Close the text editor.	Click <b>Close</b> .

## Installing the Configuration from a Local File

Use the following procedure to install a WCCP configuration text file that is located on the system from which you're accessing the web-based Management Console.

ProxySG CONFIGURATION—INSTALL WCCP SETTINGS FROM A LOCAL FILE		
Step 1	Go to the <b>WCCP</b> tab in the Management Console.	From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b> .
Step 2	Specify that you want to install the settings from a local file.	Select <b>Local File</b> from the <b>Install WCCP Settings from</b> drop-down list and then click <b>Install</b> . The <b>Open</b> dialog box displays.
Step 3	Install the file.	Browse to the WCCP text file and then click <b>Open</b> . The Management Console displays a message indicating that the configuration file was successfully installed. Click <b>OK</b> .

## Installing the Configuration from a Remote URL

Use the following procedure to install a WCCP configuration text file that is located on a remote system. Before you start this procedure, you must post the WCCP configuration file to a web server that is accessible from the machine where you are running the Management Console.

ProxySG CONFIGURATION—INSTALL WCCP SETTINGS FROM A REMOTE URL		
Step 1	Go to the <b>WCCP</b> tab in the Management Console.	From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b> .
Step 2	Specify that you want to install the settings from a remote URL.	Select <b>Remote URL</b> from the <b>Install WCCP Settings from</b> drop-down list and then click <b>Install</b> . The <b>Install WCCP Settings</b> dialog box displays.
Step 3	Specify the URL.	Enter the URL for the text file in the <b>Installation URL</b> field. For example: <b>http://10.25.36.47/files/wccp.txt</b>
Step 4	(optional) View the file to verify the WCCP settings.	Click <b>View</b> . The configuration file opens in a new browser window or tab.
Step 5	Install the file.	Click <b>Install</b> . The Management Console displays a message indicating that the configuration file was successfully downloaded and installed. Click <b>OK</b> twice.



## Installing the Configuration from the CLI

Another way to install a WCCP configuration file is from the CLI. To do this, you must post the WCCP configuration on a web server that is accessible from the ProxySG and then use the following procedure to install the file.

<b>ProxySG CONFIGURATION—INSTALL WCCP SETTINGS FROM THE CLI</b>	
Step 1 Log in to the ProxySG CLI and enter configure terminal mode.	login as: <b>admin</b> admin@10.9.59.243's password: Blue Coat SG200> <b>en</b> Enable Password: Blue Coat SG200# <b>conf t</b> Blue Coat SG200#(config)
Step 2 Specify the location of the WCCP configuration text file.	Blue Coat SG200#(config) <b>wccp path</b> <b>http://10.25.36.47/files/wccp.txt</b>
Step 3 Install the file.	Blue Coat SG200#(config) <b>load</b> <b>wccp-settings</b>

## Enabling WCCP

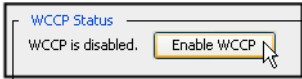
If the WCCP configuration file that you installed contained the `wccp enable` command, WCCP should already be enabled. In this case, continue to the next section, "Verifying the WCCP Configuration" on page 3-15.

If you have installed the WCCP configuration but haven't yet enabled WCCP, you can enable it now using one of the following methods:

- Enabling WCCP From the Management Console—on page 3-14
- Enabling WCCP From the CLI—on page 3-14

### Enabling WCCP From the Management Console

Use the following procedure to enable WCCP from the Management Console.

ProxySG CONFIGURATION—ENABLE WCCP FROM THE MANAGEMENT CONSOLE	
Step 1 Go to the <b>WCCP</b> tab in the Management Console.	From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b> .
Step 2 Enable WCCP. 	Click <b>Enable WCCP</b> . As soon as the service is enabled, all of the service groups that you have configured will display in the <b>WCCP Status</b> section of the screen. If you have configured and enabled WCCP on the routers in the service group, you should be able to see the service groups initialize and form. For a description of the status fields, see "Viewing ProxySG Service Group Statistics" on page 5-3.

### Enabling WCCP From the CLI

Use the following procedure to enable WCCP from the CLI.

ProxySG CONFIGURATION—ENABLE WCCP FROM THE CLI	
Step 1 Log in to the ProxySG CLI and enter configure terminal mode.	login as: <b>admin</b> admin@10.9.59.243's password: Blue Coat SG200> <b>en</b> Enable Password: Blue Coat SG200# <b>conf t</b> Blue Coat SG200#(config)
Step 2 Enable WCCP.	Blue Coat SG200#(config) <b>wccp enable</b>

## Verifying the WCCP Configuration

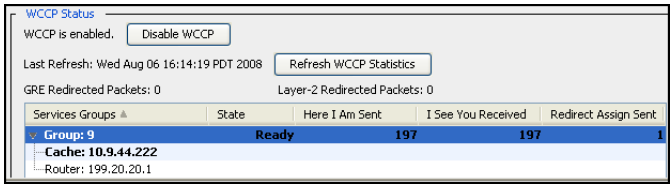
After you install the WCCP configuration, the WCCP routers and ProxySG appliances in the service groups you have defined begin negotiating the capabilities you have configured. As long as the configurations you have defined are correct and all of the routers and ProxySG appliances in the group support the capabilities that have been configured, the service group will form and the router will begin redirecting traffic to the ProxySG appliances in the service group. You can verify that the service groups you have configured on a given ProxySG are established and functioning either from the Management Console or from the CLI as described in the following sections:

- Verifying the WCCP Configuration from the Management Console—on page 3-15
- Verifying the WCCP Configuration from the CLI—on page 3-16

### Verifying the WCCP Configuration from the Management Console

Use the following procedure to verify that your WCCP service groups are working properly.

ProxySG CONFIGURATION—VIEW WCCP STATUS FROM THE MANAGEMENT CONSOLE	
Step 1 Go to the <b>WCCP</b> tab in the Management Console.	From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b> .
Step 2 Check the status of the service groups.	The status of the service groups that you have configured are displayed in the <b>WCCP Status</b> section of the screen. For a description of the status fields, see <i>"Viewing ProxySG Service Group Statistics"</i> on page 5-3.



## Verifying the WCCP Configuration from the CLI

Use the following procedure to verify that your WCCP service groups are working properly.

ProxySG CONFIGURATION—VIEW WCCP STATUS FROM THE CLI	
<p>Step 1 Log in to the ProxySG CLI and enter enabled mode.</p>	<pre>login as: <b>admin</b> admin@10.9.59.243's password: Blue Coat SG200&gt;<b>en</b> Enable Password: Blue Coat SG200#</pre>
<p>Step 2 Display the service group status.</p> <p>In this example, both service groups in which the ProxySG is configured to participate have formed successfully and the routers have started redirecting traffic.</p> <p>For a description of the status fields, see "Viewing ProxySG Service Group Statistics" on page 5-3.</p>	<pre>Blue Coat SG200#<b>show wccp status</b> ;WCCP Status ;Version 1.3 Number of GRE redirected packets: 13 Number of Layer 2 redirected packets: 10  Service group: 10   State: Ready   Number of Here_I_Am sent: 358   Number of I_See_You received: 358   Number of Redirect_Assign sent: 1   Router IP: 5.6.7.2   Cache IP: 1.2.3.1 Service group: 11   State: Ready   Number of Here_I_Am sent: 287   Number of I_See_You received: 287   Number of Redirect_Assign sent: 1   Router IP: 1.2.3.4   Cache IP: 1.2.3.1</pre>

## Modifying the WCCP Configuration

To change the WCCP configuration after you initially install it—for example if you want to add a new router to the group or add an additional service group—you can edit the settings and then reinstall the file.

Use the following procedure to modify the WCCP configuration settings:

ProxySG CONFIGURATION—MODIFY WCCP SETTINGS		
Step 1	Go to the <b>WCCP</b> tab in the Management Console.	From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b> .
Step 2	Open the existing configuration in the text editor.	Select <b>Text Editor</b> from the <b>Install WCCP Settings</b> from drop-down list and then click <b>Install</b> .
<b>Note</b>	If you originally defined your WCCP configuration in a local or remote text file, you can edit the original file and then reinstall it.	
Step 3	Edit the file. You can do any of the following:	
<b>Note</b>	<ul style="list-style-type: none"> <li>Add new or edit existing settings.</li> </ul> Some commands—such as <code>forwarding-method</code> and <code>assignment-type</code> —have default values; removing a command that has a default value automatically sets the value to the default. For example, removing the <code>assignment-type mask</code> command automatically sets the assignment type to hash.	Enter the new settings into the text editor. Make sure that if you add an additional service group that you separate the groups using the <code>end</code> command.
	<ul style="list-style-type: none"> <li>Comment a command. Commenting a command is a good way to remove it temporarily because you can easily reinstate the command by removing the comment.</li> </ul>	Enter a <code>;</code> before the command to comment it. For example, to temporarily remove a protocol statement from the service group, you could comment the command as follows:  <code>;</code> protocol 17
	<ul style="list-style-type: none"> <li>Delete a command</li> </ul>	To permanently delete a setting, delete the line from the text file.
Step 4	When you are done making your changes, reinstall the file.	Click <b>Install</b> . The Management Console displays a message indicating that the settings were successfully installed. Click <b>OK</b> .
Step 5	Close the text editor.	Click <b>Close</b> .

## Disabling WCCP

If you no longer want the ProxySG to participate in any of the service groups for which it is configured, you can disable WCCP. Disabling WCCP does not remove the WCCP configuration settings, but rather it places them out of service until you reenables WCCP. There are a couple of ways to disable WCCP as described in the following sections:

- Disabling WCCP From the Management Console—on page 3-18
- Disabling WCCP From the CLI—on page 3-18

### Disabling WCCP From the Management Console

Use the following procedure to disable WCCP from the Management Console.

ProxySG CONFIGURATION—DISABLE WCCP FROM THE MANAGEMENT CONSOLE	
Step 1 Go to the <b>WCCP</b> tab in the Management Console.	From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b> .
Step 2 Disable WCCP.	Click <b>Disable WCCP</b> . As soon as the service is disabled, all of the service groups that you previously configured will no longer be displayed in the <b>WCCP Status</b> section of the screen.

### Disabling WCCP From the CLI

Use the following procedure to disable WCCP from the CLI.

ProxySG CONFIGURATION—DISABLE WCCP FROM THE CLI	
Step 1 Log in to the ProxySG CLI and enter configure terminal mode.	login as: <b>admin</b> admin@10.9.59.243's password: Blue Coat SG200> <b>en</b> Enable Password: Blue Coat SG200# <b>conf t</b> Blue Coat SG200#(config)
Step 2 Disable WCCP.	Blue Coat SG200#(config) <b>wccp disable</b>

# 4 WCCP Configuration Examples

---

This chapter shows some common WCCP configurations, including the following:

- ❑ Basic WCCP Configuration—on page 4-2
- ❑ Web-Cache Configuration—on page 4-3
- ❑ L2 Forwarding and Return—on page 4-4
- ❑ Secure Service Group—on page 4-5
- ❑ Redirect Specific Traffic—on page 4-6
- ❑ Multiple Service Groups—on page 4-7
- ❑ Load Balancing Using Hash Assignment—on page 4-9
- ❑ Hotspot Detection—on page 4-11
- ❑ Load Balancing Using Unequal Loads—on page 4-13
- ❑ Load Balancing Using Mask Assignment—on page 4-15
- ❑ Single ProxySG Multiple Routers—on page 4-17
- ❑ Multicast—on page 4-18
- ❑ Client IP Reflection—on page 4-19

## Basic WCCP Configuration

The following example shows a simple WCCP configuration in which one router is configured to redirect all traffic to one ProxySG. Because the service group redirects all traffic by default, you do not need to define specific ports and/or protocols to redirect.

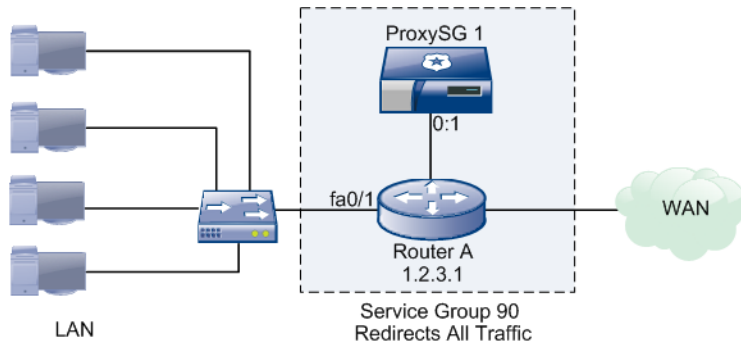


Figure 4-1 Basic WCCP Configuration Example

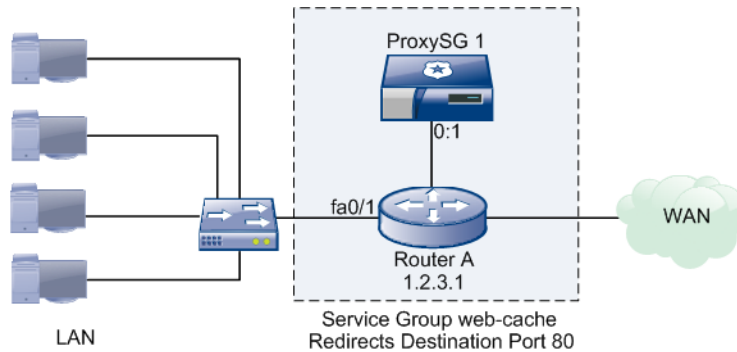
### CONFIGURATION EXAMPLE—BASIC WCCP CONFIGURATION

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp 90 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in</pre>
ProxySG 1	<pre>wccp enable wccp version 2 service-group 90 interface 0:1 protocol 6 priority 1 home-router 1.2.3.1 end</pre>



## Web-Cache Configuration

The following example shows how to configure the web-cache service on a single router and ProxySG. The web-cache service group is used to redirect HTTP traffic on destination port 80 only. Because this is a well-known service group, you do not need to configure any characteristics about it—such as port number or direction—because the router and the ProxySG already know them. Note that this configuration is supported in WCCP Version 1 and Version 2. In this example, the router and the ProxySG are both configured to use WCCP Version 1.



**Figure 4-2 Web-Cache Configuration Example**

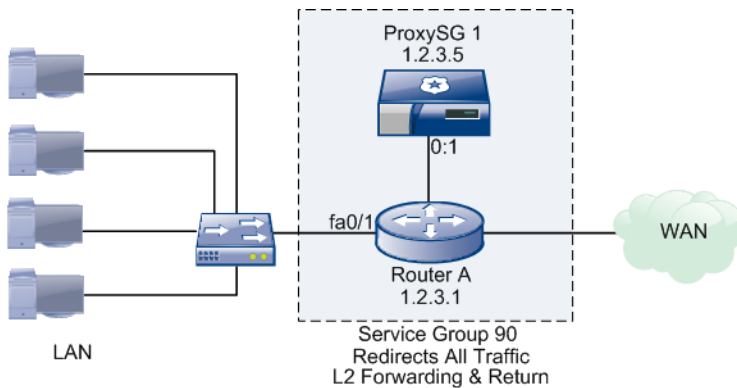
### CONFIGURATION EXAMPLE—WEB-CACHE CONFIGURATION

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp web-cache Router(config)#ip wccp version 1 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp web-cache redirect in</pre>
ProxySG 1	<pre>wccp enable wccp version 1 service-group web-cache interface 0:1 home-router 1.2.3.1 end</pre>

## L2 Forwarding and Return

By default, the router forwards packets to the ProxySG appliance using GRE forwarding and returns packets that it cannot process using GRE return. Because GRE forwarding and return is the default, no configuration is required to use these methods. If you want to use L2 forwarding/return, you will have to explicitly configure it. Keep in mind that not all routers support all forwarding and return methods.

When using L2 forwarding, the ProxySG and the router must be on the same broadcast domain (that is, they cannot be more than one router hop apart) as shown in Figure 4-3.



**Figure 4-3 L2 Forwarding and Return Example**

### CONFIGURATION EXAMPLE—L2 FORWARDING AND RETURN

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp 90 Router(config)#ip wccp version 2 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in</pre>
ProxySG 1	<pre>wccp enable wccp version 2 service-group 90 interface 0:1 protocol 6 priority 1 forwarding-type L2 home-router 1.2.3.1 end</pre>

## Secure Service Group

The following example shows how you can restrict access to a service group so that only authorized ProxySG appliances can join. This example shows two methods for restricting access:

- On the router, an ACL permits access to the ProxySG at 1.2.3.5 only; all other hosts are denied. This ACL is then associated with the group-list for the service group.
- On the router and the ProxySG, a password secures the service group. When a ProxySG attempts to join the service group, the router will only allow it to join if it can authenticate using the configured password.

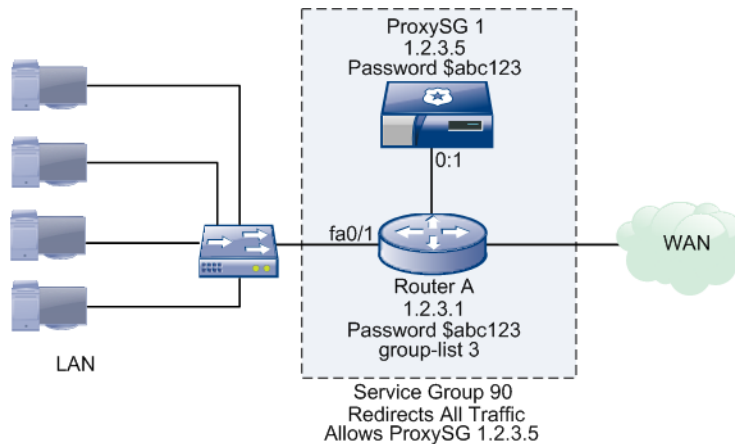


Figure 4-4 Secure Service Group Example

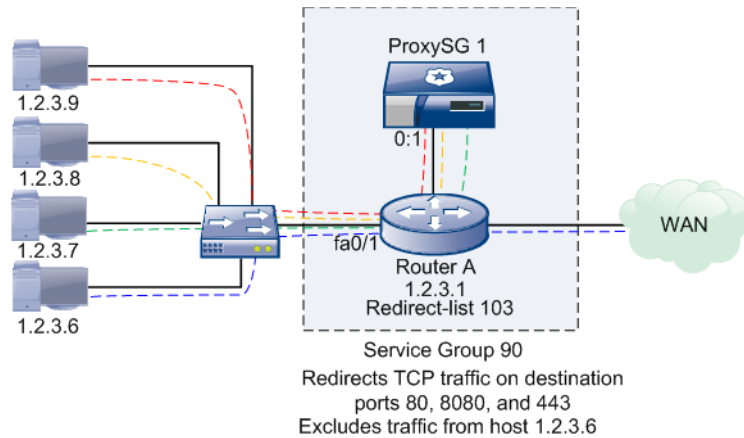
### CONFIGURATION EXAMPLE—SECURE SERVICE GROUP

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#access-list 3 permit 1.2.3.5 0.0.0.255 Router(config)#ip wccp version 2 Router(config)#ip wccp 90 group-list 3 Router(config)#ip wccp 90 password 0 \$abc123 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in</pre>
ProxySG 1	<pre>wccp enable wccp version 2 service-group 90 interface 0:1 protocol 6 priority 1 home-router 1.2.3.1 password \$abc123 end</pre>

## Redirect Specific Traffic

You can configure the router and/or the ProxySG so that only a subset of traffic is redirected. This example shows two methods for defining what traffic to redirect:

- On the router, an ACL excludes traffic from host 1.2.3.6 . This ACL is then associated with the redirect-list for the service group to let the router know not to redirect traffic that matches the ACL.
- On the ProxySG, the service group definition specifies individual ports to redirect; the router forwards traffic on all other ports normally. Note that you can only specify 8 ports to redirect within a single service group. If you want to redirect more than 8 ports, you must create multiple service groups.



**Figure 4-5 Redirection of Specific Protocol and Ports Example**

CONFIGURATION EXAMPLE—REDIRECT SPECIFIC TRAFFIC	
Router A	<pre> Router&gt;enable Router#configure terminal Router(config)#access-list 103 deny ip any host 1.2.3.6 Router(config)#access-list 103 permit ip any any Router(config)#ip wccp version 2 Router(config)#ip wccp 90 redirect-list 103 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in                     </pre>
ProxySG 1	<pre> wccp enable wccp version 2 service-group 90 interface 0:1 priority 1 home-router 1.2.3.1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 end                     </pre>

## Multiple Service Groups

In some cases you may want to create separate service groups, for example, to handle the redirection of different types of traffic. The following example shows a configuration in which a single router is configured to participate in two service groups that are handled by different ProxySG appliances.

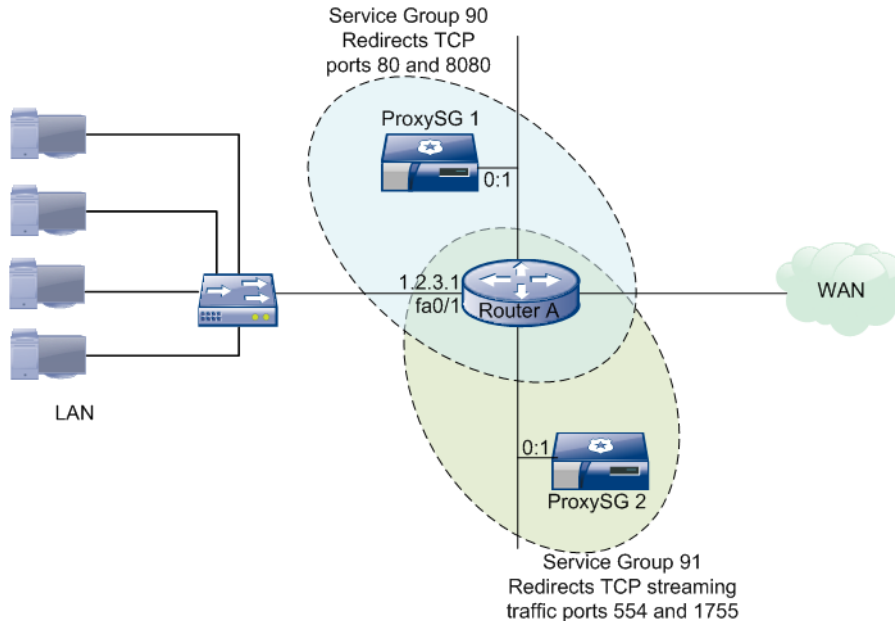


Figure 4-6 Multiple Service Groups Example

### CONFIGURATION EXAMPLE—MULTIPLE SERVICE GROUPS

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp version 2 Router(config)#ip wccp 90 Router(config)#ip wccp 91 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 91 redirect in</pre>
ProxySG 1	<pre>wccp enable wccp version 2 service-group 90 interface 0:1 protocol 6 priority 1 service-flags ports-defined ports 80 8080 0 0 0 0 0 0 home-router 1.2.3.1 end</pre>

---

**CONFIGURATION EXAMPLE—MULTIPLE SERVICE GROUPS (CONTINUED)**

---

ProxySG 2	<pre>service-group 91 service-flags ports-defined ports 554 1755 0 0 0 0 0 0 interface 0:1 protocol 6 priority 1 home-router 1.2.3.1 end</pre>
-----------	--

---

## Load Balancing Using Hash Assignment

In the following example, the two ProxySG appliances in service group 90 are configured for load balancing using hash assignment. The service group is configured so that the router uses the destination IP address and the destination port in the header of the packet it is redirecting to run the hashing algorithm. Because ProxySG 1 has the lowest IP address, it automatically becomes the designated cache and is responsible for communicating the load balancing assignment information to the router.

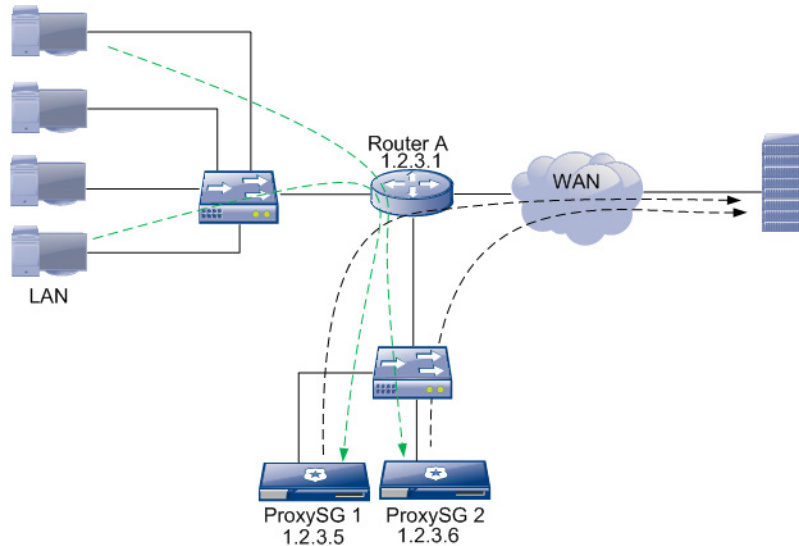


Figure 4-7 Load Balancing Using Hash Assignment Example

### CONFIGURATION EXAMPLE—LOAD BALANCING USING HASH ASSIGNMENT

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp version 2 Router(config)#ip wccp 90 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in</pre>
ProxySG 1	<pre>wccp enable wccp version 2 service-group 90 interface 2:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 home-router 1.2.3.1 assignment-type hash service-flags destination-ip-hash service-flags destination-port-hash end</pre>

**CONFIGURATION EXAMPLE—LOAD BALANCING USING HASH ASSIGNMENT (CONTINUED)**

ProxySG 2	wccp enable wccp version 2 service-group 90 interface 2:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type hash service-flags destination-ip-hash service-flags destination-port-hash end
-----------	--



## Hotspot Detection

Because the hashing function is based on a packet header field, a disproportionate amount of traffic can sometimes be redirected to the same ProxySG. For example if the hashing function is based on destination IP address and many users are sending requests to the same destination, a disproportionate number of packets will get redirected to the same ProxySG. To prevent this situation, you can configure an alternate hashing field or fields for the router to use if the number of GRE packets or MAC addresses (depending on the forwarding method you're using) redirected to a given ProxySG exceeds a certain number. Note that this is only supported when you are using hash assignment; hotspot detection is not supported with mask assignment.

In the following example, the service group is configured so that the router will perform the hash function using both the destination IP address and port. If one of the ProxySG appliances becomes overloaded, the router will perform the hash using the source IP address instead.

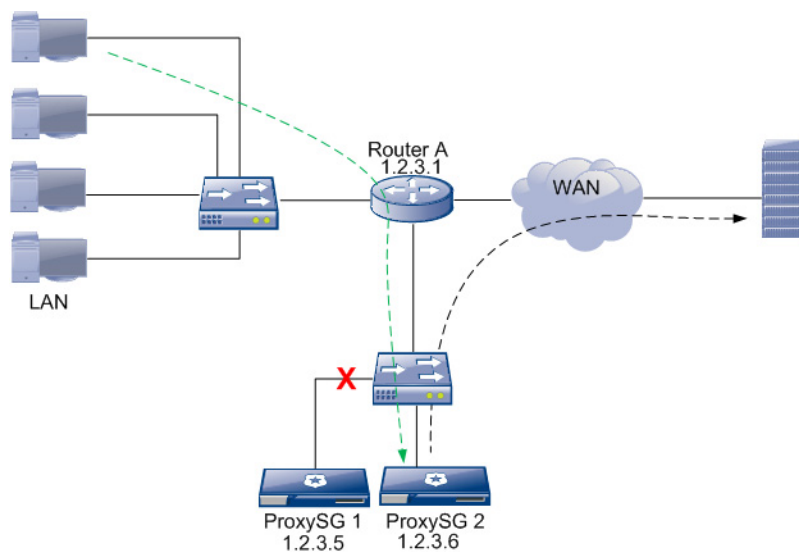


Figure 4-8 Load Balancing Using an Alternate Hash Example

### CONFIGURATION EXAMPLE—HOTSPOT DETECTION

Router A	<pre> Router&gt;enable Router#configure terminal Router(config)#ip wccp version 2 Router(config)#ip wccp 90 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in </pre>
----------	---

**CONFIGURATION EXAMPLE—HOTSPOT DETECTION (CONTINUED)**

ProxySG 1	wccp enable wccp version 2 service-group 90 interface 2:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type hash service-flags destination-ip-hash service-flags destination-port-hash service-flags source-ip-alternate-hash end
ProxySG 2	wccp enable wccp version 2 service-group 90 interface 2:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type hash service-flags destination-ip-hash service-flags destination-port-hash service-flags source-ip-alternate-hash end

## Load Balancing Using Unequal Loads

By default, each ProxySG in the service group is assigned roughly an even percentage of the 256-bucket hash table. However, you can override this behavior by configuring a hash-weight value to each ProxySG in the service group to adjust the proportion of the hash table that get assigned to it. In the following example, ProxySG 1 and ProxySG 2 have weight values of 100 and receive about twice as much redirected traffic as ProxySG 3, which has a weight value of 50.

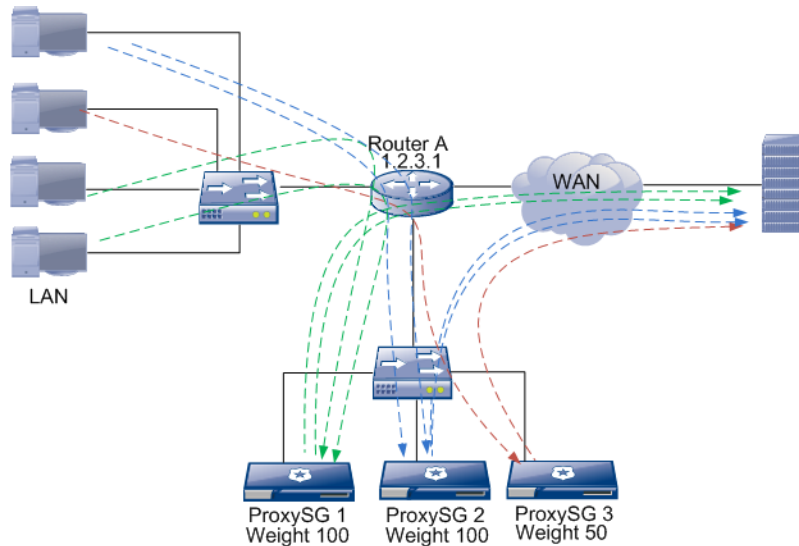


Figure 4-9 Load Balancing Using Unequal Weights Example

### CONFIGURATION EXAMPLE—LOAD BALANCING USING UNEQUAL LOADS

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp 90 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in</pre>
ProxySG 1	<pre>wccp enable service-group 90 interface 2:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type hash service-flags destination-port-hash primary-hash-weight 2:1 100 end</pre>

**CONFIGURATION EXAMPLE—LOAD BALANCING USING UNEQUAL LOADS (CONTINUED)**

ProxySG 2	wccp enable service-group 90 interface 2:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type hash service-flags destination-port-hash primary-hash-weight 2:1 100 end
ProxySG 3	wccp enable service-group 90 interface 2:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type hash service-flags destination-port-hash primary-hash-weight 2:1 50 end

## Load Balancing Using Mask Assignment

With mask assignment, each router in the service group has a table of masks and values that it uses to distribute traffic across the ProxySG appliances in the service group. When the router receives a packet, it performs a bitwise AND operation between the mask value and the field of the packet header that is designated in the ProxySG mask assignment configuration. It then compares the result against its list of values for each mask; each value is assigned to a specific ProxySG in the service group. As with hash assignment, you can also assign a weight value to each ProxySG to force unequal loads (see Figure 4-9).

### CONFIGURATION EXAMPLE—LOAD BALANCING USING MASK ASSIGNMENT

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp 90 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in</pre>
ProxySG 1	<pre>wccp enable service-group 90 interface 0:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type mask mask-scheme destination-port primary-hash-weight 0:1 100 end</pre>
ProxySG 2	<pre>wccp enable service-group 90 interface 0:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type mask mask-scheme destination-port primary-hash-weight 0:1 100 end</pre>

---

**CONFIGURATION EXAMPLE—LOAD BALANCING USING MASK ASSIGNMENT (CONTINUED)**

---

ProxySG 3	wccp enable service-group 90 interface 0:1 priority 1 protocol 6 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 assignment-type mask mask-scheme destination-port primary-hash-weight 0:1 50 end
-----------	--

---

## Single ProxySG Multiple Routers

In this example, two routers are in a service group with a single ProxySG. Therefore, the ProxySG configuration requires two `home-router` settings. Additionally, because the routers are on different subnets, GRE forwarding and return must be used.

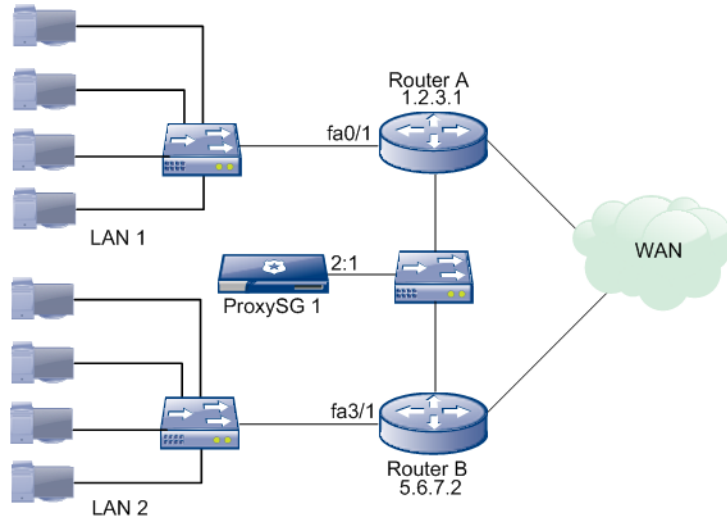


Figure 4-10 Service Group with Multiple Routers and a Single ProxySG Example

### CONFIGURATION EXAMPLE—SINGLE ProxySG MULTIPLE ROUTERS

Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp version 2 Router(config)#ip wccp 90 Router(config)#interface fastethernet 0/1 Router(config-if)#ip wccp 90 redirect in</pre>
Router B	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp version 2 Router(config)#ip wccp 90 Router(config)#interface fastethernet 3/1 Router(config-if)#ip wccp 90 redirect in</pre>
ProxySG 1	<pre>wccp enable wccp version 2 service-group 90 interface 2:1 priority 1 forwarding-method GRE home-router 1.2.3.1 home-router 5.6.7.2 end</pre>

## Multicast

With multicast addressing, the ProxySG appliances and the routers in the service group use a single multicast address—in the range of 224.0.0.0 to 239.255.255.255—to communicate with all other group members simultaneously. In the following example, the routers in service group 90 are all configured to listen on multicast address 224.1.1.103. Additionally, the ProxySG appliances in the group use the multicast address as their home-router address.

CONFIGURATION EXAMPLE—MULTICAST	
Router A	<pre>Router&gt;enable Router#configure terminal Router(config)#ip multicast Router(config)#ip wccp version 2 Router(config)#ip wccp 90 group-address 224.1.1.103 Router(config)#interface fastethernet 2/1 Router(config-if)#ip wccp 90 redirect in Router(config-if)#ip wccp 90 group-listen Router(config-if)#ip pim dense-mode</pre>
Router B	<pre>Router&gt;enable Router#configure terminal Router(config)#ip wccp version 2 Router(config)#ip wccp 90 group-address 224.1.1.103 Router(config)#interface gigabitethernet 0/0/0 Router(config-if)#ip wccp 90 redirect in Router(config-if)#ip wccp 90 group-listen Router(config-if)#ip pim dense-mode</pre>
ProxySG 1	<pre>wccp enable wccp version 2 service-group 90 interface 2:1 priority 1 forwarding-type L2 assignment-type mask home-router 224.1.1.103 end</pre>
ProxySG 2	<pre>wccp enable wccp version 2 service-group 90 interface 0:1 priority 1 forwarding-type L2 assignment-type mask home-router 224.1.1.103 end</pre>



## Client IP Reflection

If you are using WCCP in a client IP reflection configuration, you will have to redirect traffic in two directions: first as the request is sent from the client to the server and second as the server sends the response back to the client. As a best practice, you should use separate service groups for the different traffic directions: one that redirects traffic from the client based on destination port and one that redirects traffic from the server based on source port. To prevent redirection loops, you should attach the ProxySG to a third, dedicated interface as shown in Figure 4-11. Notice that although the router has multiple IP addresses, the lowest IP address is used as the home router address for both service groups.

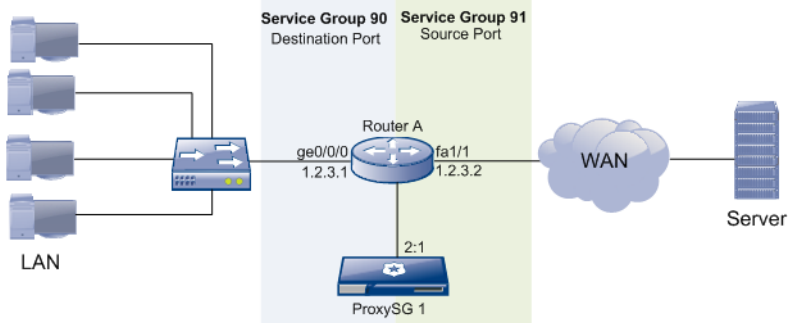


Figure 4-11 Client IP Reflection Example

### CONFIGURATION EXAMPLE—CLIENT IP REFLECTION

Router A	<pre> Router&gt;enable Router#configure terminal Router(config)#ip wccp version 2 Router(config)#ip wccp 90 Router(config)#ip wccp 91 Router(config)#interface gigabitethernet 0/0/0 Router(config-if)#ip wccp 90 redirect in Router(config)#interface fastethernet 1/1 Router(config-if)#ip wccp 91 redirect in </pre>
----------	---

---

**CONFIGURATION EXAMPLE—CLIENT IP REFLECTION (CONTINUED)**

---

ProxySG 1	wccp enable wccp version 2 service-group 90 interface 2:1 priority 1 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 home-router 1.2.3.1 end service-group 91 service-flags ports-defined ports 80 8080 443 0 0 0 0 0 service-flags ports-source interface 2:1 priority 1 home-router 1.2.3.1 end
-----------	---

---

# 5 Monitoring and Troubleshooting WCCP

---

This chapter provides information on how to verify that your WCCP configuration is working properly as well as information to help you troubleshoot problems. It includes the following topics:

- ❑ Service Group States—on page 5-2
- ❑ Viewing ProxySG Service Group Statistics—on page 5-3
- ❑ Viewing Router Statistics—on page 5-5
- ❑ Fixing a Home Router Mismatch—on page 5-8
- ❑ Tested Platform Configurations—on page 5-10

## Service Group States

The ProxySG maintains state information for its configured service groups. The state of a service group helps you monitor whether the service group was configured properly and how it is functioning. Table 5-1 lists and describes each service group state. To view the state of the service groups you have configured, see *"Viewing ProxySG Service Group Statistics"* on page 5-3.

**Table 5-1 WCCP Service Group States**

State	Description
Assignment mismatch	The router does not support the assignment type (hash or mask) that is configured for the service group.
Bad router id	The home-router specified in the service group configuration does not match the actual router ID.
Bad router view	The list of ProxySG appliances in the service group does not match.
Capability mismatch	The WCCP configuration includes capabilities that the router does not support.
Initializing	WCCP was just enabled and the ProxySG is getting ready to send out its first <code>HERE_I_AM</code> message.
Interface link is down	The ProxySG cannot send the <code>HERE_I_AM</code> message because the interface link is down.
Negotiating assignment	The ProxySG received the <code>I_SEE_YOU</code> message from the router but has not yet negotiated the service group capabilities.
Negotiating membership	The ProxySG sent the <code>HERE_I_AM</code> message and is waiting for an <code>I_SEE_YOU</code> message from the router.
Packet forwarding mismatch	The router does not support the forwarding method (GRE or L2) that is configured for the service group.
Packet return mismatch	The router does not support the return method (GRE or L2) that is configured for the service group. Note that on the ProxySG, the return method is always the same as the forwarding method.
Ready	The service group formed successfully and the ProxySG sent the <code>REDIRECT_ASSIGN</code> message to the router with the hash or mask values table.
Service group mismatch	The router and the ProxySG have a mismatch in port, protocol, priority, and/or other service flags.
Security mismatch	The service group passwords on the router and the ProxySG do not match.

## Viewing ProxySG Service Group Statistics

After you install the WCCP configuration, the WCCP routers and ProxySG appliances in the service groups you have defined begin negotiating the capabilities you have configured. As long as the configurations you have defined are correct and all of the routers and ProxySG appliances in the group support the capabilities that have been configured and have the required network connectivity, the service group will form and the router will begin redirecting traffic to the ProxySG appliances in the service group.

You can monitor statistics about the service groups you have configured on a given ProxySG from the Management Console or from the CLI as described in the following sections:

- Viewing Service Group Statistics from the Management Console—on page 5-4
- Viewing Service Group Statistics from the CLI—on page 5-4

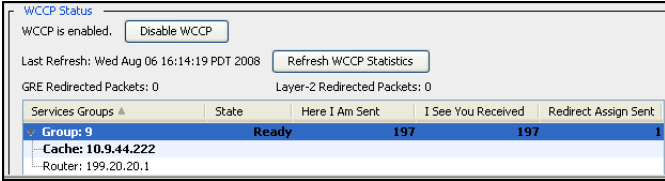
Table 5-2 lists and describes each ProxySG WCCP statistic.

**Table 5-2 ProxySG WCCP Statistics**

Statistic	Description
<b>Last Refresh</b>	The date and time the displayed statistics were last refreshed. Click <b>Refresh WCCP Statistics</b> to refresh them now.
<b>GRE Redirected Packets</b>	The number of packets that have been redirected using GRE forwarding.
<b>Layer-2 Redirected Packets</b>	The number of packets that have been redirected using L2 forwarding.
<b>Services Groups</b>	Lists the service groups that have been configured on this ProxySG. If the group has successfully formed, you can click the arrow next to the group to see a list of the caches (ProxySG appliances) and routers that have joined the group.
<b>State</b>	Shows the service group state. See Table 5-1 for a description of each state.
<b>Here I Am Sent</b>	The number of HERE_I_AM messages that this ProxySG has sent to the routers in the group.
<b>I See You Received</b>	The number of I_SEE_YOU messages that this ProxySG has received from the routers in the group.
<b>Redirect Assign Sent</b>	The number of REDIRECT_ASSIGN messages that this ProxySG has sent to the routers in the group. The REDIRECT_ASSIGN message contains the hash table or mask values table that the router will use to determine which ProxySG to redirect packets to. Only the designated cache—the cache with the lowest IP address—sends REDIRECT_ASSIGN messages.

## Viewing Service Group Statistics from the Management Console

Use the following procedure to verify that your WCCP service groups are working properly.

MONITOR WCCP—VIEW WCCP STATUS FROM THE MANAGEMENT CONSOLE	
Step 1 Go to the <b>WCCP</b> tab in the Management Console.	From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b> .
Step 2 Check the status of the service groups.	The status of the service groups that you have configured are displayed in the <b>WCCP Status</b> section of the screen. To ensure that you are viewing the most up-to-date information, click <b>Refresh WCCP Statistics</b> .
	The <b>WCCP Status</b> section indicates whether WCCP is enabled. If it is not enabled, no statistics are displayed. If it is enabled, the statistics for each service group are displayed. See Table 5-2 for a description of each statistic.

## Viewing Service Group Statistics from the CLI

Use the following procedure to verify that your WCCP service groups are working properly.

MONITOR WCCP—VIEW WCCP STATUS FROM THE CLI	
Step 1 Log in to the ProxySG CLI and enter enabled mode.	login as: <b>admin</b> admin@10.9.44.22's password: Blue Coat SG200> <b>en</b> Enable Password: Blue Coat SG200#
Step 2 Display the service group status. For a description of each field, see Table 5-2.	Blue Coat SG200# <b>show wccp status</b> ;WCCP Status ;Version 1.3 Number of GRE redirected packets: 15628 Number of Layer 2 redirected packets: 0 Service group: 9 State: Ready Number of Here_I_Am sent: 946 Number of I_See_You received: 946 Number of Redirect_Assign sent: 1 Router IP: 199.20.20.1 Cache IP: *10.9.44.22
<b>Note</b> The * next to the Cache IP indicates that ProxySG is the designated cache.	

## Viewing Router Statistics

You can also monitor the service group information from the router as follows:

MONITOR WCCP—DISPLAY ROUTER WCCP STATISTICS	
Step 1	Log in to the router CLI and enter privileged mode.
	Router>enable
Step 2	Display global WCCP statistics for all service groups that have been configured on the router.
	<pre> Router#show ip wccp Global WCCP information:   Router information:     Router Identifier:      199.20.20.1     Protocol Version:      2.0    Service Identifier: 0     Number of Service Group Clients: 0     Number of Service Group Routers: 0     Total Packets s/w Redirected: 0     Process: 0     Fast: 0     CEF: 0     Service mode: Open     Service access-list: -none-     Total Packets Dropped Closed: 0     Redirect access-list: -none-     Total Packets Denied Redirect: 0     Total Packets Unassigned: 0     Group access-list: -none-     Total Messages Denied to Group: 0     Total Authentication failures: 0     Total Bypassed Packets Received: 0   Service Identifier: 1     Number of Service Group Clients: 0     Number of Service Group Routers: 0     Total Packets s/w Redirected: 0     Process: 0     Fast: 0     CEF: 0 </pre>





**MONITOR WCCP—DISPLAY ROUTER WCCP STATISTICS**

Step 5 Display the router view. The router view contains a list of all of the caches that the router has allowed into the service group as announced in the I\_SEE\_YOU messages from the router. Use the router view to determine whether the ProxySG appliances you expect to be in a service group have joined.

**Note** WCCP Clients NOT Visible field indicates which ProxySG appliances are not visible to all other routers to which this router is connected.

```
Router#show ip wccp 9 view
WCCP Routers Informed of:
    199.20.20.1

WCCP Clients Visible:
    10.9.44.222

WCCP Clients NOT Visible:
    -none-
```

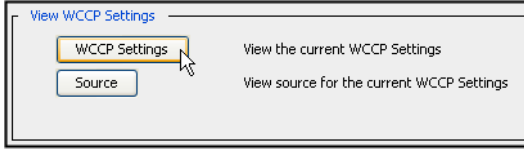


**Note** You can also use the `show ip interface` command to determine whether any WCCP redirect commands are configured on an interface.

## Fixing a Home Router Mismatch

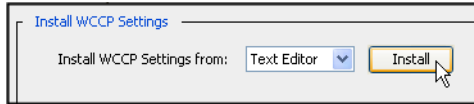
If a service group shows the state `Bad router id`, it indicates that the home router configured on the ProxySG doesn't match the actual router ID or that the configured IP address is not reachable from the ProxySG. To fix the problem, you must identify the WCCP router ID and then modify the `home-router` setting in the ProxySG configuration.

Use the following procedure to fix a home router mismatch.

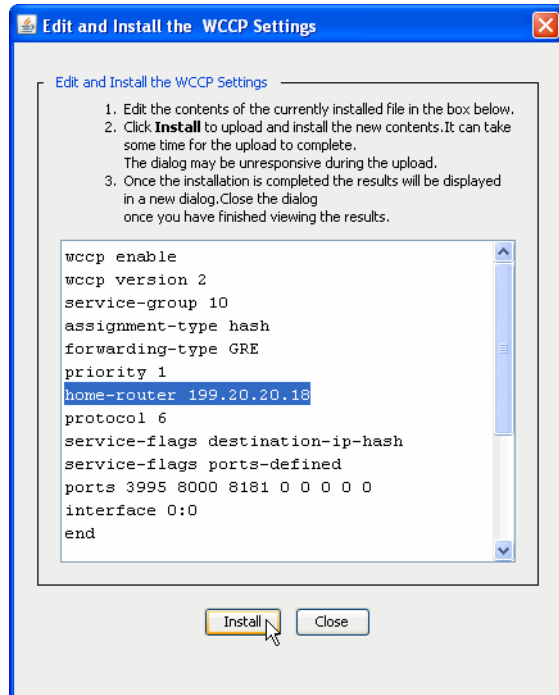
TROUBLESHOOT WCCP—FIX A HOME ROUTER MISMATCH	
<p>Step 1 On the router, display the global WCCP configuration. Make note of the Router Identifier.</p>	<pre>Router#show ip wccp Global WCCP information:   Router information:     Router Identifier:          199.20.20.18</pre>
<p>Step 2 On the ProxySG, go to the <b>WCCP</b> tab in the Management Console.</p>	<p>From within the Management Console, select <b>Configuration &gt; Network &gt; Advanced &gt; WCCP</b>.</p>
<p>Step 3 Click <b>WCCP Settings</b>.</p> 	<p>The current ProxySG WCCP configuration settings are displayed in a new browser window or tab. Notice that the <code>home-router</code> that is configured on the ProxySG does not match the Router Identifier noted on the router:</p> <pre>;WCCP Settings Version 1.3 wccp enable wccp version 2 service-group 10 forwarding-type GRE returning-type GRE assignment-type hash priority 1 protocol 6 service-flags destination-ip-hash service-flags ports-defined ports 3995 8000 8181 0 0 0 0 interface 0:0 <b>home-router 199.20.20.1</b> end</pre>

**TROUBLESHOOT WCCP—FIX A HOME ROUTER MISMATCH**

Step 4 Go back to the **WCCP** tab on the Management Console. Select **Text Editor** from the **Install WCCP Settings from** drop-down list and then click **Install**.

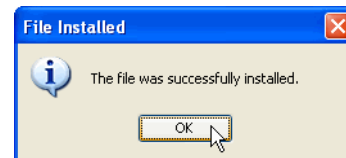


The Edit and Install WCCP Settings dialog box is displayed.



Step 5 Edit the `home-router` setting to match the Router Identifier displayed by the router and then click **Install**.

A message is displayed indicating that the file was successfully installed.



## Tested Platform Configurations

Table 5-1 summarizes the Cisco hardware and software platforms that Blue Coat has tested with the ProxySG WCCP feature. Although you can use other WCCP-capable Cisco hardware and software in your ProxySG WCCP deployment, you must check the Cisco documentation to determine the specific WCCP features that are supported on the platform.

**Table 5-1 Tested Platform Configurations**

Cisco Hardware and Software Platform	Features Tested With ProxySG			
	GRE	L2	Mask	Hash
C3845-IPBASE-M IOS Version 12.4(3g)	✓			✓
CAT6509 (s222_rp-ADVIPSERVICESK9_WAN-M) Cisco WS-C6509 (R7000) processor (revision 3.0) IOS Version 12.2(18) SXF7	✓	✓	✓	✓
C3825-ADVIPSERVICESK9-M IOS Version 12.4(11) T4	✓	✓	✓	✓
C2800NM-IPBASE-M IOS Version 12.4(3i)	✓	✓	✓	✓
C3825-IPBASE-M IOS Version 12.4(17a)	✓	✓	✓	✓
CAT6509 (s72033_rp-ADVENTERPRISEK9_WAN-M) IOS Version 12.2(18) SXF8	✓		✓	✓



**Note** Notice that the CAT6509 systems tested use an older release because the newer releases support L2 forwarding, but not L2 return. In SGOS Version 5.3, the forwarding method and return method must match. Note also that L2 forwarding/return was not tested extensively on these platforms.

# A WCCP Command Quick Reference

---

This appendix lists and describes each WCCP command on both the ProxySG and the router side. For more detailed information on how to use the router commands, see [Chapter 2, \*Configuring WCCP on the Router\*](#). For more detailed information on how to use the ProxySG WCCP commands, see [Chapter 3, \*Configuring WCCP on the ProxySG\*](#).

This appendix includes the following sections:

- ❑ Router WCCP Commands—on page A-2
- ❑ ProxySG WCCP Commands—on page A-5

## Router WCCP Commands

Table A-1 Router WCCP Command Quick Reference

Command	Description
<b>Global Commands (apply to all service groups on the router)</b>	
ip wccp version [1   2]	<p>Defines the WCCP version to use for all service groups configured on the router. Version 2 is the default and is the recommended version.</p> <p><b>Example:</b></p> <pre>Router(config)#ip wccp version 2</pre>
<b>Service Group Definition Commands</b>	
ip wccp [web-cache   <0-99>]	<p>Defines the service group and enables WCCP on the router. Use the keyword <code>web-cache</code> to create the well-known web-cache service group (redirects traffic on TCP destination port 80 only) or specify a unique service group identifier in the range of 0-99.</p> <p><b>Example:</b></p> <pre>Router(config)#ip wccp 90</pre>
ip wccp [web-cache   <0-99>] password [0   7] <password>	<p>Defines an MD5 password (up to 8 characters) to use to authenticate ProxySG appliances to the service group. The passwords you define on the router and on the ProxySG must match in order for the ProxySG to be authenticated. This command must also include the encryption type, which can be 0 (indicating that password is not yet encrypted) or 7 (indicating that the password is encrypted using a Cisco-proprietary encryption algorithm).</p> <p><b>Example:</b></p> <pre>ip wccp 90 0 mypa\$\$</pre>
<b>Multicast Addressing Commands</b>	
ip multicast-routing	<p>Enables multicast routing on the router. Note that if there are any intervening routers between the WCCP router and the ProxySG appliances, you must enable multicast routing on those routers also.</p> <p><b>Example:</b></p> <pre>Router(config)#ip multicast-routing</pre>
ip wccp [web-cache   <0-99>] group-address <address>	<p>Defines the multicast address for the service group. The multicast address must be in the range 224.0.0.0 to 239.255.255.255.</p> <p><b>Example:</b></p> <pre>Router(config)#ip wccp 90 group-address 224.1.1.103</pre>

Command	Description
ip wccp [web-cache   <0-99>] group-listen	Enables the WCCP multicast group address on an interface.  <b>Example:</b>  Router(config)#interface fastethernet1/1 Router(config-if)#ip wccp 90 group-listen
ip pim [sparse-dense-mode   sparse-mode]	Enables Protocol Independent Multicast (PIM) on an interface. This is required on certain Cisco platforms only, such as the Catalyst 6500 and Catalyst 7600. Refer to your router documentation for more information.  <b>Example:</b>  Router(config)#interface fastethernet1/1 Router(config-if)#ip pim sparse-mode

### Service Group Filtering Commands

ip wccp [web-cache   <0-99>] redirect-list <list-name>	Associates an access control list (ACL) with a WCCP service group for filtering which traffic to redirect. For information on how to create an ACL, refer to your router documentation.  <b>Example:</b>  Router(config)#access-list 103 deny ip any host 10.1.0.43 Router(config)#ip wccp 90 redirect-list 103
ip wccp [web-cache   <0-99>] group-list <list-name>	Associates an ACL with a WCCP service group for filtering which ProxySG appliances to allow into the service group. For information on how to create an ACL, refer to your router documentation.  <b>Example:</b>  Router(config)#access-list 3 permit 10.1.1.5 0.0.0.255 Router(config)#ip wccp 90 group-list 103

Command	Description
<b>Interface Redirection Commands</b>	
ip wccp [web-cache   <0-99>] redirect [in   out]	<p>Applies the service group to an interface and direction. After you apply the service group to an interface, traffic entering (redirect in) or exiting (redirect out) the interface will be evaluated for redirection. Whenever possible, you should apply WCCP service groups to inbound interfaces because it is faster and requires less processing.</p> <p><b>Example:</b></p> <pre>Router(config)#interface gigabitEthernet2/2 Router(config-if)#ip wccp 90 redirect in</pre>
ip wccp redirect exclude in	<p>Excludes inbound traffic on an interface from redirection. You should use this command on the router interface to which the ProxySG is connected to prevent redirection loops if you are using outbound redirection on the router. If you are using inbound redirection only, you do not need to use this command.</p> <p><b>Example:</b></p> <pre>Router(config)#interface gigabitEthernet2/3 Router(config-if)#ip wccp redirect exclude in</pre>



## ProxySG WCCP Commands

Table A-2 ProxySG WCCP Command Quick Reference

Command	Description
<b>Global Commands (apply to all service groups on the ProxySG)</b>	
wccp [enable   disable]	<p>Enables or disables WCCP. If you include this command in the WCCP configuration file, WCCP will automatically be enabled or disabled when you install the settings. By default WCCP is disabled. If you do not include this command in the configuration file, you can manually enable WCCP from the Management Console or the CLI.</p> <p><b>Example:</b></p> <pre>wccp enable</pre>
wccp version [1   2]	<p>Defines the WCCP version to use for all service groups configured on the ProxySG. Version 2 is the default and is the recommended version.</p> <p><b>Example:</b></p> <pre>wccp version 2</pre>
<b>Service Group Definition Commands</b>	
service-group [web-cache   <0-99>]	<p>Defines the service group. Use the keyword <code>web-cache</code> to create the well-known web-cache service group (redirects traffic on TCP destination port 80 only) or specify a unique service group identifier in the range of 0-99.</p> <p><b>Example:</b></p> <pre>service-group 90</pre>
interface <interface_number>	<p>Specifies the ProxySG interface to which to apply the service group. As a best practice, apply the service group to the first LAN interface on the appliance, for example 0:1 on the 210 platform, 2:1 on the 510 and 810 platforms, or 3:1 on the 8100.</p> <p><b>Example:</b></p> <pre>interface 2:1</pre>
priority <0-255>	<p>Specifies the queuing priority for the service group. If there are multiple service groups applied to the same router interface in the same direction, the priority defines the order in which the router evaluates them.</p> <p><b>Example:</b></p> <pre>priority 2</pre>

Command	Description
<code>password &lt;password&gt;</code>	<p>Defines the MD5 password (up to 8 characters) that is required for the ProxySG to authenticate to the service group. This field is only required if you have configured a password on the router; the passwords must match.</p> <p><b>Example:</b></p> <pre>password mypa\$\$</pre>
<code>end</code>	<p>Specifies the end of the service group. If your WCCP configuration includes multiple service group definitions, you must include the <code>end</code> command at the end of each service group configuration. If your configuration includes a single service group, include the <code>end</code> command at the end of the file.</p> <p><b>Example:</b></p> <pre>end</pre>

### Traffic Description Commands

<code>protocol &lt;protocol_number&gt;</code>	<p>Specifies which protocol to redirect. You can specify any standard protocol number as defined by IANA:</p> <p><a href="http://www.iana.org/assignments/protocol-numbers">http://www.iana.org/assignments/protocol-numbers</a></p> <p>You can include multiple <code>protocol</code> commands to redirect multiple protocols. Typically, WCCP is used to redirect TCP (6) and/or UDP (17) traffic.</p> <p><b>Example:</b></p> <pre>protocol 6</pre>
<code>service-flags ports-defined</code>	<p>Indicates that the service group will redirect traffic with specific port numbers only. By default, the service group redirects traffic on all ports. Include this command only if you want to redirect a subset of traffic based on port number.</p> <p><b>Example:</b></p> <pre>service-flags ports-defined</pre>
<code>ports [num num num num num num num num]</code>	<p>Specifies the specific ports you want to redirect. You can specify any well-known port number as defined by IANA:</p> <p><a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a></p> <p>You can specify up to eight ports per service group. Note that this command requires eight field values, so if you don't specify eight ports, you must use zeroes for any remaining field values.</p> <p><b>Example:</b></p> <pre>ports 80 8080 443 0 0 0 0 0</pre>

Command	Description
service-flags ports-source	<p>Specifies that the router should use the source port rather than the default destination port to determine whether to redirect the packet. If you want to base the service group redirection on destination port, you do not need to include this command.</p> <p><b>Example:</b></p> <pre>service-flags ports-source</pre>
<b>Router Definition Commands</b>	
home-router <address>	<p>Specifies the unicast or multicast address the ProxySG should use to communicate with the router(s) in the service group.</p> <p>If you are using unicast addressing (recommended) you must define a <code>home-router</code> entry for each router in the service group. If the router has more than one IP address configured, use the lowest IP address to avoid home router mismatch errors.</p> <p>If you are using multicast addressing, use a single address in the range of 224.0.0.0 to 239.255.255.255 for all routers in the service group. You must also enable multicast on the routers and specify the group address in the WCCP configuration.</p> <p><b>Example:</b></p> <pre>home-router 10.1.1.103</pre>
multicast-ttl <num>	<p>Specifies the multicast time to live (TTL) value. You only need to include this command if you want to use a TTL value other than 1 (the default). Cisco recommends using a value of 15 or less.</p> <p><b>Example:</b></p> <pre>multicast-ttl 3</pre>
<b>Forward and Return Method Command</b>	
forwarding-type [gre   L2]	<p>Defines the method the routers in the service group use to forward redirected packets to the ProxySG and the ProxySG appliances use to return packets that they can't process back to the router. In this release, the forwarding method and the return method are always the same. Possible values are:</p> <ul style="list-style-type: none"> <li>• <code>gre</code> — forward using Generic Routing Encapsulation (GRE). This is the default forwarding method; to use this method no configuration is required.</li> <li>• <code>L2</code> — forward using Layer 2 (L2) forwarding.</li> </ul> <p><b>Example:</b></p> <pre>forwarding-type L2</pre>

Command	Description
<b>Assignment Type Commands</b>	
assignment-type [hash   mask]	<p>In service groups that contain multiple ProxySG appliances, this command defines the method for selecting the appliance to which to redirect a given packet. Possible values are as follows:</p> <ul style="list-style-type: none"> <li>• <code>hash</code> — the router runs designated fields in the packet header through a hashing algorithm to determine the appliance to which to redirect the packet. This is the default assignment type.</li> <li>• <code>mask</code> — the router performs a bitwise AND operation between the mask value and a designated field in the packet header to determine the appliance to which to redirect the packet.</li> </ul> <p><b>Example:</b></p> <pre>assignment-type mask</pre>
service-flags [destination-ip-hash   source-ip-hash   destination-port   source-port]	<p>Specifies which field(s) in the header of the packet the router should use to run the hashing algorithm when using hash assignment. You can use multiple instances of the command to designate the use of multiple fields. If you are using hash assignment, you must specify at least one field.</p> <p><b>Example:</b></p> <pre>service-flags destination-ip-hash service-flags destination-port</pre>
service-flags [destination-port-alternate-hash   destination-ip-alternate-hash   source-port-alternate-hash   source-ip-alternate-hash]	<p>Specifies alternate packet header field(s) to use to run the hashing algorithm when using hash assignment. This setting will be used if a ProxySG in the service group gets overloaded.</p> <p><b>Example:</b></p> <pre>service-flags source-ip-alternate-hash</pre>
mask-scheme [source-ip   destination-ip   source-port   destination-port]	<p>Specifies which field(s) in the header of the packet the router should use to run the mask function when using mask assignment. By default <code>destination-ip</code> is used. You only need to specify a <code>mask-scheme</code> if you want to use a field other than the destination IP address to run the mask function.</p> <p><b>Example:</b></p> <pre>mask-scheme source-ip</pre>

Command	Description
<code>primary-hash-weight &lt;interface&gt; &lt;weight&gt;</code>	<p>Specifies the proportion of the load that should be assigned to this ProxySG in the load balancing scheme for the service group. This command can be used with either mask or hash assignment. Use this command only if you want to distribute the redirected traffic unequally among the ProxySG appliances in the service group. The weight value must be an integer in the range of 0-255. The default value is 0. Therefore, if you choose to use unequal loads, you must assign weight values to each appliance in the group in order for it to receive any of the traffic.</p> <p><b>Example:</b></p> <pre>primary-hash-weight 2:1 40</pre>

