Configuring Traffic Interception

This chapter describes the WAAS software support for intercepting all TCP traffic in an IP-based network, based on the IP and TCP header information, and redirecting them to wide area application engines (WAEs). This chapter focuses on the use of the Web Cache Communication Protocol (WCCP) and policy-based routing (PBR) for transparent redirection of traffic to WAEs.

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances and WAE Network Modules (the NME-WAE family of devices).

This chapter assumes that you have completed a basic initial installation and configuration of your WAAS network, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*. For detailed command syntax information for any of the CLI commands that are mentioned in this chapter, see the *Cisco Wide Area Application Services Command Reference*. For further information about WCCP, see the *Cisco IOS Configuration Fundamentals Configuration Guide* and the *Cisco IOS Configuration Fundamentals Command Reference*.

This chapter describes how to configure traffic interception in your WAAS network and includes the following sections:

About Request Redirection Methods

In a WAAS network, traffic between clients in the branch offices and the servers in the data center can be redirected to WAEs for optimization, redundancy elimination, and compression. Traffic is intercepted and redirected to WAEs based on policies that have been configured on the routers. The network elements that transparently redirect requests to a local WAE can be a router or a Layer 4 to Layer 7 switch (for example, the Catalyst 6500 Content Switching Module [CSM]) that uses WCCP Version 2 or PBR to transparently redirect traffic to the local WAE.

In your WAAS network, traffic can be intercepted in these modes:

- Transparent mode (WCCP or PBR)
  - For application traffic, there are no configuration changes required to the client or the client-server applications. In promiscuous WCCP mode, application traffic is transparently redirected by network elements to the local WAE.

    Note When you enable the TCP promiscuous mode service (WCCP services 61 and 62) on the routers and the Edge and Core WAEs, the CIFS caching service is also enabled on the router and the WAE.

  - For Wide Area File Services (WAFS) traffic, the Edge WAEs provide no name services. The Edge WAE does not advertise the existence of a remote CIFS file server on the local network. Instead, the CIFS client resolves the NetBIOS name of the file server to its actual IP address (on the remote network) and connects to it. The router redirects all traffic on the CIFS ports (ports 139 and 445) to the Edge WAE on the local network. The prefix to the NetBIOS name of the file server is not used; clients use the original file server name and not the prefixed one. When CIFS clients connect to the origin file server IP address, a WCCP-enabled router redirects all traffic on the CIFS ports to the Edge WAE on the local network. The prefix to the NetBIOS name of the file server is not used; clients use the original file server name and not the prefixed one. (DNS/WINS synchronization must be available at the branch office.) The only name service provided by the Edge WAE in this mode is for local print services.

    Note An Edge WAE operates in only one routing mode with all associated file servers, but can switch dynamically between the two routing modes. The routing mode is saved to persistent storage. On every Edge WAE startup, the mode is the same as the last one saved.

- Nontransparent (explicit) mode (WCCP Version 2 disabled)
  - For application traffic, the client-server applications are configured to communicate directly with WAAS as in a gateway, and no specific configuration is required to the switches or routers. The actual method of nontransparent interception depends on the client-server application and its capabilities.
  - For WAFS traffic, the CIFS clients connect to the Edge WAE explicitly after resolving NetBIOS names using WINS servers, broadcasts, and name queries (also called Name Services) in CIFS. This is the default mode.

Table 4-1 summarizes the transparent traffic interception methods that are supported in your WAAS network.

Table 4-1 Supported Methods of Transparent Traffic Interception

Method	Comment
WCCP Version 2	Used for transparent interception of application traffic and WAFS traffic. Used in branch offices and data centers to transparently redirect traffic to the local WAE. The traffic is transparently intercepted and redirected to the local WAE by a WCCP-enabled router or a Layer 3 switch. You must configure WCCP on the router and Edge WAE in the branch office and the router and Core WAE in the data center. For more information, see the following sections: • Using WCCP to Transparently Redirect TCP Traffic to WAEs, page 4-4 • Using WCCP to Transparently Redirect CIFS Client Requests, page 4-50
Microsoft DFS	Used for either transparent or nontransparent interception of WAFS traffic for CIFS clients only. See the "Using Microsoft DFS to Intercept CIFS Client Requests" section on page 4-51.
NETBIOS	Used for nontransparent interception of WAFS traffic for CIFS clients unless the WAE is publishing the origin server name, in which case NETBIOS is used for transparent interception of WAFS traffic for CIFS clients. See the "Using Explicit Naming of Shares to Explicitly Intercept CIFS Client Requests" section on page 4-50.
PBR	In branch offices, used for wide area application optimization. The branch office router is configured to use PBR to transparently intercept and redirect client-server requests to the Edge WAE that resides in the same branch office. In data centers, used for data center application optimization. The data center CSM is configured to use PBR to transparently intercept application and WAFS traffic for load-balancing purposes (load balancing these requests across the farm of servers in the data center). You must configure the Core WAE to use load balancing. See the "Using Policy-Based Routing to Transparently Redirect All TCP Traffic to WAEs" section on page 4-40.
CSS/CSM	Cisco CSS 11500 Content Services Switch and the Catalyst 6500 CSM installed in the data center for data center application optimization. Used for load-balancing purposes in the data center. Transparent traffic interception by a Layer 4 switch. Typically, you configure CSM interception on a Core WAE along with the Layer 4 switch, which are both located in the data center.

For more information, see the following sections:

- Request Redirection of All TCP Traffic, page 4-4
- Request Redirection of CIFS Client Requests, page 4-49

Request Redirection of All TCP Traffic

This section describes the methods that are supported for request redirection of TCP traffic:

Using WCCP to Transparently Redirect TCP Traffic to WAEs

The WAAS software uses the WCCP standard, Version 2 for redirection. The main features of WCCP Version 2 include support for the following:

- Up to 32 WAEs per WCCP service
- Multiple routers
- Multicasting of protocol messages between the WAE and the WCCP-enabled router
- Authentication of protocol packets
- Redirection of non-HTTP traffic
- Packet return (including GRE, allowing a WAE to reject a redirected packet and to return it to the router to be forwarded)
- Layer 2-caching (through router versus GRE) and masking (for improved load balancing)
- Multiple forwarding methods
- Packet distribution method negotiation within a service group
- Command and status interaction between the WAE and a service group

Note WCCP works only with IPv4 networks.

WAAS software supports the following WCCP services:

- TCP promiscuous mode service (services 61 and 62)
- CIFS caching service (service 89)

Both of these WCCP services require that WCCP Version 2 is running on the router and the WAE.

The TCP promiscuous mode service is a WCCP service that intercepts all TCP traffic and redirects it to the local WAE. The WCCP CIFS caching service is a dynamic service that intercepts all TCP traffic destined for ports 139 and 445 and redirects it to the corresponding redirect port (139 or 445). Load balancing distributes traffic based on the source IP address, by default. The WCCP-enabled router uses service ID 89 to access this service.

Note When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service (WCCP Version 2 service 89) on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

The WAAS software also supports service passwords, WAE failover, flow protection, and static bypass.

The Cisco 2600, Cisco 2800, Cisco 3600, Cisco 3700, Cisco 3800, and Cisco 7600 series routers are supported, and can be manually configured and enabled with WCCP Version 2 support for use with the Cisco WAEs. The Catalyst 6000 and Catalyst 6500 Series switches also support WCCP Version 2.

Note Many legacy Cisco routers, including the 2500, 2600, and 3600 routers, have far less processing power and memory than newer routing platforms such as the Integrated Services Router (ISR) models 2800 and 3800. As such, the use of WCCPv2 or PBR may cause a high level of CPU utilization on the router and cause erratic behavior. WAAS can be configured to work with these routers, but not to the same levels of performance or scalability as can be found with newer routing platforms. The Cisco ISR is the routing platform of choice for the branch office.

If you are experiencing erratic behavior, such as the WAE being ejected from the service group, enable fair-queuing, weighted fair-queuing, or rate-limiting on all physical interfaces on the router that connect to users, servers, WAEs, and the WAN. Fair-queuing cannot be configured on subinterfaces, and should be configured on both ingress and egress physical interfaces. If another form of queuing is already configured on the LAN or WAN interfaces other than fair-queuing that provides similar fairness, it should be sufficient.

Additionally, limit the amount of bandwidth that can be received on the LAN-side interface of the router, to help the router keep its interface queues less congested and provide better performance and lower CPU utilization. The bandwidth command should be used to set the maximum interface bandwidth on the router to no more than 10 times the WAN bandwidth capacity. For instance, if the WAN link is a T1, the LAN interface and WAE LAN interface bandwidth should be throttled to 10 * T1 = 10 * 1.544 Mbps, or approximately 15 Mbps.

Guidelines for Configuring WCCP

When you configure transparent redirection on a WAE using WCCP Version 2, follow these general guidelines:

- Intercept and redirect packets on the inbound interface whenever possible.
- WAEs must reside in a subnet that is separate from the traffic's destination and source. For example, an Edge WAE must be on a subnet separate from the clients, and a Core WAE must be on a subnet separate from the file and application servers. If you are deploying only the Wide Area File Services (WAFS) in your WAAS network, this requirement is the same, except that the Core WAE can be on the same subnet as the file and application servers, though this configuration is not recommended because no other WAAS optimizations can be enabled.
- Edge WAEs must not have their packets encrypted or compressed and should be part of the "inside" Network Address Translation (NAT) firewall if one is present.
- Use Layer 2 redirection as the packet forwarding method if you are using Catalyst 6500 series switches or Cisco 7600 series routers. Use Layer 3 GRE packet redirection if you are using any other Cisco series router.
- Use hardware-supported methods (CEF, dCEF) where possible. CEF is not required, but is recommended for improved performance. WCCP can use IP CEF if CEF is enabled on the router.
- Place Edge WAEs on the client side of the network to minimize client-side packets through the router.
- Use WCCP passwords to avoid denial-of-service attacks. For more information, see the "Setting a Service Group Password on a Router" section on page 4-11.

- Use WCCP redirect lists for new implementations to limit client or server populations. For more information, see the "Configuring IP Access Lists on a Router" section on page 4-9.
- The WAE must be configured to accept redirected packets from one or more WCCP-enabled routers.
- You can quickly view a list of WCCP settings and services that you can configure on a WAE, from the WAAS CLI or the WAAS Central Manager GUI (see Figure 4-4) or the WAAS CLI. From the WAAS CLI, enter the **wccp** EXEC command followed by a question mark (?). The following sample output is from a WAE with WCCP Version 2 enabled:

```
WAE(config)# wccp ?
    access-list     Configure an IP access-list for inbound WCCP encapsulated traffic
    cifs-cache      CIFS caching
    flow-redirect   Redirect moved flows
    router-list     Router List for use in WCCP services
    shutdown        Wccp Shutdown parameters
    slow-start      accept load in slow-start mode
    tcp-promiscuous  TCP promiscuous mode service
    version         WCCP Version Number
```

- To configure basic WCCP, you must enable the WCCP service on at least one router in your network and on the WAE that you want the traffic redirected to. It is not necessary to configure all of the available WCCP features or services to get your WAE up and running. For an example of how to complete a basic WCCP configuration on routers and WAEs in a branch office and data center, see the *Cisco Wide Area Application Services Quick Configuration Guide*.
- You must configure the routers and WAEs to use WCCP Version 2 instead of WCCP Version 1 because WCCP Version 1 only supports web traffic (port 80).
- After enabling WCCP on the router, you must configure the TCP promiscuous mode service (WCCP services 61 and 62) on the router and the WAE, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.
- In order for the WAE to function in TCP promiscuous mode, the WAE uses WCCP Version 2 services 61 and 62. These two WCCP services are represented by the canonical name tcp-promiscuous on the WAE.

Note When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service (WCCP Version 2 service 89) on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

- You can use CLI commands to configure basic WCCP on both the routers and the WAEs, or you can use CLI commands to configure the router for WCCP and use the WAAS Central Manager GUI to configure basic WCCP on the WAEs. In the configuration example provided in the *Cisco Wide Area Application Services Quick Configuration Guide*, the CLI is used to configure basic WCCP on the WAEs.

  We recommend that you use the WAAS CLI to complete the initial basic configuration of WCCP on your first Edge WAE and Core WAE, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.

  After you have verified that WCCP transparent redirection is working properly, you can use the WAAS Central Manager GUI to centrally modify this basic WCCP configuration or configure additional WCCP settings (for example, load balancing) for a WAE (or group of WAEs). For more information, see the "Centrally Managing WCCP Configurations for WAEs" section on page 4-12.
- After you have configured basic WCCP on the router, you can configure advanced WCCP features on the router, as described in the "Configuring Advanced WCCP Features on a WCCP-Enabled Router" section on page 4-7.

Guidelines about File Server Access Methods

Some file servers have several network interfaces and can be reached through multiple IP addresses. For these server types, you must add all the available IP addresses to the Edge WAE's WCCP accept list. This situation prevents a client from bypassing the Edge WAE by using an unregistered IP address. The WAE Device Manager GUI displays all the IP addresses in the GUI.

Some file servers have several NetBIOS names and only one IP address. For these servers, if the client connects using the IP address in the UNC path (that is, \\IP_address\share instead of \\server\share), WAAS selects the first NetBIOS name from the server list in the WAE Device Manager GUI that matches this IP address. WAAS uses that name to perform NetBIOS negotiations between the Core WAE and the file server, and to create resources in the cache. If a file server uses multiple NetBIOS names to represent virtual servers (possibly with different configurations) and has one NetBIOS name that is identified as the primary server name, put that name in the server list before the other names.

Configuring Advanced WCCP Features on a WCCP-Enabled Router

This section describes how to configure the following advanced WCCP Version 2 features on a WCCP-enabled router that is transparently redirecting requests to WAEs in your WAAS network:

- Configuring a Router to Support WCCP Service Groups, page 4-7
- Configuring IP Access Lists on a Router, page 4-9
- Setting a Service Group Password on a Router, page 4-11
- Configuring a Loopback Interface on the Router, page 4-11

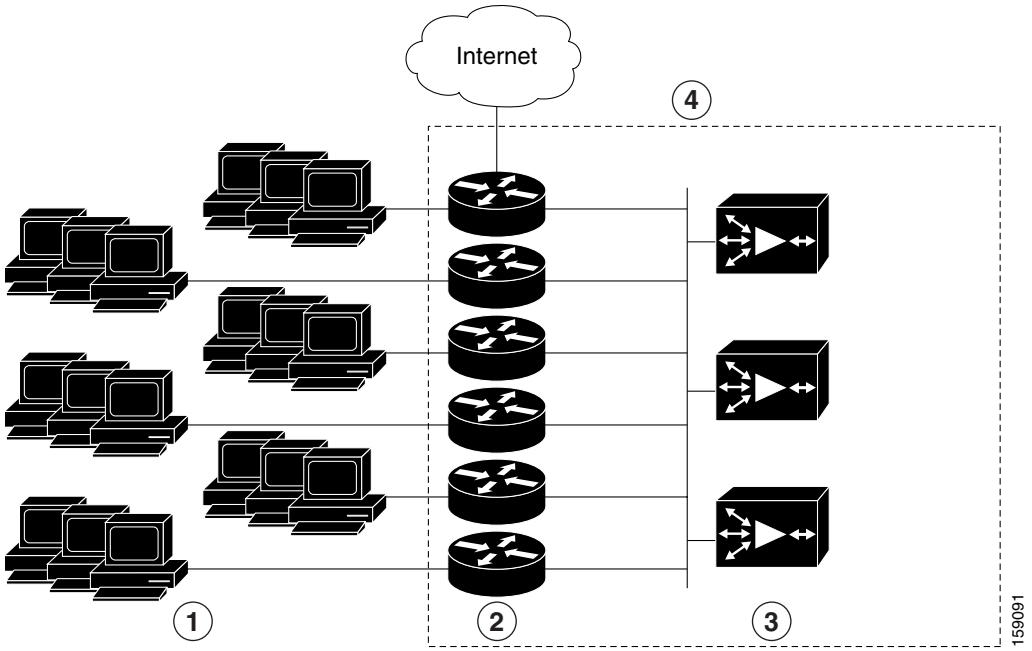
Note This section assumes that the router has already been configured for basic WCCP, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.

Configuring a Router to Support WCCP Service Groups

WCCP Version 2 enables a set of Edge WAEs in an WAE group to connect to multiple routers. The WAEs in a group and the WCCP Version 2-enabled routers connected to the WAE group that are running the same WCCP service are known as a *service group*.

Through communication with the Edge WAEs, the WCCP Version 2-enabled routers are aware of the available Edge WAEs. Routers and Edge WAEs become aware of one another and form a service group using WCCP Version 2. See Figure 4-1.

Figure 4-1 Service Groups with WCCP Version 2



1	Clients requesting file services	**3**	WAEs acting as Edge WAEs
2	Cisco routers	**4**	WAE service group

If there is a group of Edge WAEs, the one seen by all the WCCP Version 2-enabled routers and the one that has the lowest IP address becomes the lead Edge WAE.

The following procedure describes how an Edge WAE in a service group is designated as the lead:

1. Each Edge WAE is configured with a list of WCCP-enabled routers.

   Multiple WCCP-enabled routers can service a group (up to 32 routers can be specified). Any of the available routers in a service group can redirect packets to each of the Edge WAEs in the group.

2. Each Edge WAE announces its presence to each router on the router list. The routers reply with their view of Edge WAEs in the service group.

3. After the view is consistent across all of the Edge WAEs in the group, one Edge WAE is designated as the lead Edge WAE and sets the policy that the WCCP-enabled routers need to deploy in redirecting packets.

The role of this lead Edge WAE is to determine how traffic should be allocated across the Edge WAEs in the group. The assignment information is passed to the entire service group from the designated lead Edge WAE so that the WCCP-enabled routers of the group can redirect the packets properly and the Edge WAEs in the group can better manage their load.

WCCP uses service groups to define WAAS services for a WCCP Version 2-enabled router and Edge WAEs in a group. WCCP also redirects client requests to these groups in real time.

All ports receiving redirected traffic that are configured as members of the same WCCP service group share the following characteristics:

- They have the same hash or mask parameters, as configured with the WAAS Central Manager GUI (the "Modifying WCCP Service Masks for WAEs" section on page 4-28) or the WAAS CLI (the **wccp service-number mask** global configuration command).
- The WCCP Version 2 service on individual ports cannot be stopped or started individually (a WCCP Version 2 restriction).

To direct a WCCP Version 2-enabled router to enable or disable support for a WCCP service group, use the **ip wccp** global configuration command. To remove the ability of a router to control support for a WCCP service group, use the **no** form of this command.

ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*]

The following example shows how to enable the TCP promiscuous mode service (WCCP Version 2 services 61 and 62) for a group of WAEs that have a group address of 100.10.10.1:

```
Router# ip wccp 61 group-address 100.10.10.1
Router# ip wccp 62 group-address 100.10.10.1
```

Note When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service (WCCP Version 2 service 89) on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

When a new WAE is brought online, it joins the WCCP service group, and the router begins redirecting traffic to it. With a new WAE in the service group, the hash tables responsible for distributing the load are changed, and traffic that previously went to WAE1 may now go to WAE2. Flow protection must be enabled in order for WAE2 to forward packets of already connected clients to WAE1. The end result is that all requests that belong to a single session are processed by the same WAE. Should the administrator disable flow protection, adding a WAE to the service group might disconnect some of the existing clients.

When an WAE is removed from the service group, its clients are disconnected (if they reconnect, they will reach another WAE, if one is available, or the origin file server).

WAAS supports WAE failover by reconnecting clients with other Edge WAEs if an Edge WAE crashed. In the event of a crash, the Edge WAE stops issuing WCCP keepalives (constant high CPU load may also result in loss of keepalives and can also be considered a failover case). The router detects the lack of keepalives and removes the Edge WAE from the service group. The designated Edge WAE updates the WCCP configuration hash table to reflect the loss of the Edge WAE and divides its buckets among the remaining Edge WAEs. A new designated lead Edge WAE is elected if the crashed one was the lead Edge WAE. The client is disconnected, but subsequent connections are processed by another Edge WAE.

Once a TCP flow has been intercepted and received by an Edge WAE, the failure behavior is identical to that exhibited during nontransparent mode. For example, Core WAE and file server failure scenarios are not handled any differently as a result of using WCCP interception.

Configuring IP Access Lists on a Router

You can optionally configure the router to redirect traffic from your WAE based on access lists that you define on the router. These access lists are also referred to as redirect lists.

Note You can also configure static bypass lists on the WAE, as described in the "Configuring Static Bypass Lists for WAEs" section on page 4-39. We recommend that you use IP access lists on the WCCP-enabled router, rather than using the static bypass feature, because access lists are more efficient. You can also

configure IP access control lists (ACLs) on WAEs to control access to the WAE, as described in Chapter 8, "Creating and Managing IP Access Control Lists for WAAS Devices."

IP access lists that are configured on the routers have the highest priority, followed by IP ACLs that are configured on a WAE, and followed by static bypass lists on WAEs. IP ACLs that are configured on WAEs take precedence over any application definition policies that have been defined on the WAE. For more information on this topic, see the "About the Precedence of IP ACLs and Application Definition Policies on WAEs" section on page 8-3.

A WCCP Version 2-enabled router can be configured with access lists to permit or deny redirection of TCP traffic to a WAE. The following example shows that traffic conforming to the following criteria are not redirected by the router to the WAE:

- Originating from the host 10.1.1.1 destined for any other host
- Originating from any host destined for the host 10.255.1.1

```
Router(config)# ip wccp 61 redirect-list 120
Router(config)# ip wccp 62 redirect-list 120
Router(config)# access-list 120 deny ip host 10.1.1.1 any
Router(config)# access-list 120 deny ip any host 10.1.1.1
Router(config)# access-list 120 deny ip any host 10.255.1.1
Router(config)# access-list 120 deny ip host 10.255.1.1 any
Router(config)# access-list 120 permit ip any
```

Note When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service (WCCP Version 2 service 89) on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

Traffic not explicitly permitted is implicitly denied redirection. The **access-list 120 permit ip any** command explicitly permits all traffic (from any source on the way to any destination) to be redirected to the WAE. Because criteria matching occurs in the order in which the commands are entered, the global **permit** command is the last command entered.

To limit the redirection of packets to those packets matching an access list, use the **ip wccp redirect-list** global configuration command. Use this command to specify which packets should be redirected to the WAE.

When WCCP is enabled but the **ip wccp redirect-list** command is not used, all packets matching the criteria of a WCCP service are redirected to the WAE. When you specify the **ip wccp redirect-list** command, only packets that match the access list are redirected.

The **ip wccp** global configuration command and the **ip wccp redirect** interface configuration command are the only commands required to start redirecting requests to the WAE using WCCP. To instruct an interface on the WCCP-enabled router to check for appropriate outgoing packets and redirect them to a WAE, use the **ip wccp redirect** interface configuration command. If the **ip wccp** command is enabled but the **ip wccp redirect** command is disabled, the WCCP-enabled router is aware of the WAE but does not use it.

To specify the access list by name or number, use the **ip wccp group-list** global configuration command, which defines criteria for group membership. In the following example, the **access-list 1 permit 10.10.10.1** command is used to define the IP address of the WAE that is allowed to join the WCCP service group:

```
Router(config)# ip wccp 61 group-list 1
Router(config)# ip wccp 62 group-list 1
Router(config)# access-list 1 permit 10.10.10.1
```

For more information on access lists, see the Cisco IOS IP addressing and services software documentation.

Setting a Service Group Password on a Router

For security purposes, you can set a service password for your WCCP Version 2-enabled router and the WAEs that access it. Only devices configured with the correct password are allowed to participate in the WCCP service group.

From the global configuration mode of your WCCP-enabled router, enter the following commands to specify the service group password for the TCP promiscuous mode service (WCCP Version 2 services 61 and 62) on the router:

```
Router(config)# ip wccp 61 password [0-7] password
Router(config)# ip wccp 62 password [0-7] password
```

Note When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service (WCCP Version 2 service 89) on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

The required *password* argument is the string that directs the WCCP Version 2-enabled router to apply MD5 authentication to messages received from the specified service group. Messages that are not accepted by the authentication are discarded. *0-7* is the optional value that indicates the HMAC MD5 algorithm used to encrypt the password. This value is generated when an encrypted password is created for the WAE. 7 is the recommended value. The optional *password* argument is the optional password name that is combined with the HMAC MD5 value to create security for the connection between the router and the WAE.

For information about how to use the WAAS Central Manager GUI to specify the service group password on a WAE (or device group), see the "Modifying the Current Settings of a WCCP Service for WAEs" section on page 4-21.

Configuring a Loopback Interface on the Router

The IP address of the loopback interface of the router is always used to identify the router to the WAEs. If a loopback address is not present, the highest available IP address on the router is used. If an interface changes state, and no loopback address is used, another IP address is used, which could lead to reconnection problems.

The following example configures the loopback interface, exits configuration mode, and saves the running configuration to the startup configuration:

```
Router(config)# interface Loopback0
Router(config-if)# ip address 111.111.111.111 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

Centrally Managing WCCP Configurations for WAEs

For information about some key conceptions that are related to WCCP configurations on WAEs, see the following sections:

- About Load Balancing and WAEs, page 4-12
- About Packet-Forwarding Methods, page 4-14
- About WCCP Flow Redirection on WAEs, page 4-17

This section describes how to use the WAAS Central Manager GUI to centrally manage the WCCP configurations for a WAE or group of WAEs (that is, a device group):

- Viewing or Modifying the General WCCP Settings on WAEs, page 4-17
- Viewing a List of Currently Configured WCCP Services for WAEs, page 4-19
- Modifying the Current Settings of a WCCP Service for WAEs, page 4-21
- Creating a WCCP Service Mask for an Existing WCCP Service, page 4-27
- Modifying WCCP Service Masks for WAEs, page 4-28
- Creating Additional WCCP Services on WAEs, page 4-29
- Viewing a WCCP Router List Configuration for WAEs, page 4-33
- Modifying the Configuration of WCCP Router Lists for WAEs, page 4-34
- Deleting a WCCP Router List from WAEs, page 4-35
- Defining Additional WCCP Router Lists on WAEs, page 4-36
- Configuring WAEs for a Graceful Shutdown of WCCP, page 4-38
- Configuring Static Bypass Lists for WAEs, page 4-39

Note This section assumes that you have completed an initial configuration of your WAAS network, which includes the basic configuration of WCCP Version 2 and the TCP promiscuous mode service on your routers and WAEs, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.

About Load Balancing and WAEs

Multiple Edge WAEs with WCCP support can be deployed in a branch office for dynamic load balancing to enable adjustments to the loads being forwarded to the individual Edge WAEs in a service group. IP packets received by a WCCP-enabled router are examined to determine if it is a request that should be directed to an Edge WAE. Packet examination involves matching the request to a defined service criteria. These packets are passed to the processing routine on the router to determine which Edge WAE, if any, should receive the redirected packets.

Load balancing is a technique used to balance the traffic load across multiple Edge WAEs. This technique allows the set of hash address buckets assigned to an Edge WAE to be adjusted shifting the load from an overwhelmed Edge WAE to other Edge WAEs that have available capacity. Two assignment methods are used by this technique: hashing and masking.

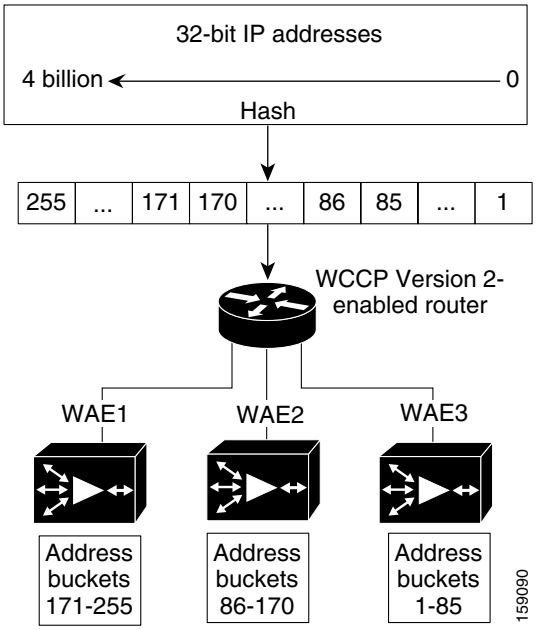
About Load-Balancing Assignment Methods

The term *assignment method* denotes the method used by WCCP to perform load distribution across Edge WAEs. The two possible load-balancing assignment methods are hashing and masking. If the mask load-balancing method is not specified, then the hash load-balancing method, which is the default method, is used.

WCCP supports redirection based on a hash function. The hash key may be based on the source or destination IP address of the packet. For WAAS, load-balancing hashing is based on a source IP address (default), a destination IP address, or both.

The hash function uses the source IP address to obtain an address bucket to which the packet is assigned. These source address buckets are then mapped to a particular Edge WAE depending on how many Edge WAEs are present and how busy they are. (See Figure 4-2.)

Figure 4-2 Load Balancing Through Hashing of IP Addresses



Note Packets that the Edge WAEs do not service are tunneled back to the same router from which they were received. When a router receives a formerly redirected packet, it knows not to redirect it again.

Destination IP address hashing guarantees that a single Edge WAE caches a given file server. This method, which allows a local coherency directive to be safely applied to the file server content (provided that no other collaboration on the content occurs), improves performance and WAN link and disk utilization. This method may distribute load unevenly, however, because of uneven activity on a file server.

Source IP address hashing has better potential for session distribution between the caches on the Edge WAEs. This method may impact performance and WAN link and disk utilization (see the previous description of factors to be aware of when load balancing is applied). Also, any change in the IP address of a client (which can happen when working in DHCP environments) may cause the client to switch to another Edge WAE, which can cause the client to experience reduced performance until the client's working set is retrieved into the new cache.

Hashing that is based on a client IP address does not guarantee any locality of the hash key. For example, clients from the same subnet (which are likely to share and collaborate on the same content) may be assigned two different hash numbers and may be redirected to different Edge WAEs, while clients from different subnets may be assigned the same hash number and may be redirected to the same Edge WAE. Hashing that is based on a client IP address does guarantee consistency. For example, a client using the same IP address is redirected to the same Edge WAE.

In the service farm, a lead Edge WAE is chosen to build the hash table that distributes the load between the available Edge WAEs. The lead Edge WAE distributes the buckets evenly. The source IP address is hashed and the resulting bucket determines the Edge WAE that will handle the packet (flow protection makes sure that it is the same Edge WAE throughout the session).

WCCP supports redirection by mask value assignments. This method relies on masking to make redirection decisions. The decisions are made using special hardware support in the WCCP-enabled router. This method can be very efficient because packets are switched by the hardware.

Note The masking method can only be used for load balancing with the Catalyst 6500 series switches and Cisco 7600 series routers.

Masking must be explicitly specified. You can specify up to four mask values based on the source or destination IP address of the packet or the source or destination port for the packet. For WAAS, the default mask value is based on the destination IP address. You can enable masks by using the default values or specifying a particular mask. The default mask values, specified in hexadecimal notation, are as follows:

- dst-ip-mask= 0x1741
- src-ip-mask= 0x0
- dst-port= 0x0
- src-port= 0x0

The mask value is specified using a maximum of seven bits. The Edge WAE creates a table of the 2^7 (or 128) combinations, assigns the Edge WAE IP addresses to them, and sends this table to the WCCP-enabled routers. The router uses this table to distribute the traffic among all the Edge WAEs that are in the service group. Each packet that matches the WCCP service parameters is compared to this table and the packets are sent to the matching Edge WAE.

About Packet-Forwarding Methods

A WCCP-enabled router redirects intercepted TCP segments to a WAE using one of the following two packet-forwarding methods:

- **Generic routing encapsulation (GRE)**—Allows packets to reach the WAE even if there are any number of routers in the path to the WAE.
- **Layer 2 redirection**—Allows packets to be switched at Layer 2 (MAC layer) and reach the WAE.

Table 4-2 describes the packet-forwarding methods.

Table 4-2 Packet-Forwarding Methods

Packet-Forwarding Method	Load-Balancing Method: Hashing	Load-Balancing Method: Masking
GRE (Layer 3)	Packet redirection is completely handled by the router software.	Packet redirection is handled by the router software. We do not recommended using mask assignment when GRE is being used as the packet-forwarding method.
Layer 2 redirection	First redirected packet is handled by the router software; all subsequent redirected packets are handled by the router hardware.	All packets are handled by the router hardware (currently supported only on the Catalyst 6500 series switches or Cisco 7600 series routers because special hardware is required).

The redirection mode is controlled by the Edge WAE. The first Edge WAE that joins the WCCP service group decides the forwarding method (GRE or Layer 2 redirection) and the assignment method (hashing or masking). The term *mask assignment* refers to WCCP Layer 2 Policy Feature Card 2 (PFC2) input redirection.

If masking is selected with WCCP output redirection, then the Edge WAE falls back to the original hardware acceleration that is used with the Multilayer Switch Feature Card (MSFC) and the Policy Feature Card (PFC).

For example, WCCP filters the packets to determine which redirected packets have been returned from the Edge WAE and which ones have not. WCCP does not redirect the ones that have been returned because the Edge WAE has determined that the packets should not be processed. WCCP Version 2 returns packets that the Edge WAE does not service to the same router from which they were transmitted.

About Returning Packets

The following are typical reasons why an Edge WAE would reject packets and initiate packet return:

- The Edge WAE is filtering out certain conditions that make processing packets unproductive, for example, when IP authentication has been turned on.
- CIFS packets are received by the Edge WAE destined to a server that is not configured to be cached by the Edge WAE.
- You have configured a static bypass list on the Edge WAE.

Note The packets are redirected to the source of the connection between the WCCP-enabled router and the Edge WAE. Depending on the Cisco IOS software version used, this source could be either the address of the outgoing interface or the router IP address. In the latter case, it is important that the Edge WAE has the IP address of the WCCP-enabled router stored in the router list. For more information on router lists, see the "Modifying the Configuration of WCCP Router Lists for WAEs" section on page 4-34.

Cisco Express Forwarding (CEF) is not required but is recommend for improved performance. WCCP can use IP CEF if CEF is enabled on the router. WCCP also allows you to configure multiple routers (router lists) to support a particular WCCP service (for example, CIFS redirection).

About Layer 3 GRE as a Packet-Forwarding Method

A WCCP-enabled router redirects intercepted requests to a WAE and can encapsulate the packets using generic routing encapsulation (GRE). This method for forwarding packets allows packets to reach the WAE even if there are routers in the path to the WAE. Packet redirection is handled entirely by the router software.

GRE is a Layer 3 technique that allows datagrams to be encapsulated into IP packets at the WCCP-enabled router and then redirected to a WAE (the transparent proxy server). At this intermediate destination, the datagrams are decapsulated and then handled by the WAAS software. If the request cannot be handled locally, the origin server may be contacted by the associated WAE to complete the request. In doing so, the trip to the origin server appears to the inner datagrams as one hop. The redirected traffic using GRE usually is referred to as GRE tunnel traffic. With GRE, all redirection is handled by the router software.

With WCCP redirection, a Cisco router does not forward the TCP SYN packet to the destination because the router has WCCP enabled on the destination port of the connection. Instead, the WCCP-enabled router encapsulates the packet using GRE tunneling and sends it to the WAE that has been configured to accept redirected packets from this WCCP-enabled router.

After receiving the redirected packet, the WAE does the following:

1. Strips the GRE layer from the packet.
2. Decides whether it should accept this redirected packet and process the request for content or deny the redirected packet as follows:
   a. If the WAE decides to accept the request, it sends a TCP SYN ACK packet to the client. In this response packet, the WAE uses the IP address of the original destination (origin server) that was specified as the source address so that the WAE can be invisible (transparent) to the client; it pretends to be the destination that the TCP SYN packet from the client was trying to reach.
   b. If the WAE decides not to accept the request, it reencapsulates the TCP SYN packet in GRE, and sends it back to the WCCP-enabled router. The router understands that the WAE is not interested in this connection and forwards the packet to its original destination (that is, the origin server).

About Layer 2 Redirection as a Packet-Forwarding Method

Layer 2 redirection is accomplished when a WCCP-enabled router or switch takes advantage of internal switching hardware that either partially or fully implements the WCCP traffic interception and redirection functions at Layer 2. This type of redirection is currently supported only with the Catalyst 6500 series switches and Cisco 7200 and 7600 series routers. With Layer 2 redirection, the first redirected traffic packet is handled by the router software. The rest of the traffic is handled by the router hardware. The Edge WAE instructs the router or switch to apply a bit mask to certain packet fields, which in turn provides a mask result or index mapped to the Edge WAE in the service group in the form of a mask index address table. The redirection process is accelerated in the switching hardware, making Layer 2 redirection more efficient than Layer 3 GRE.

Note WCCP is licensed only on the WAE and not on the redirecting router. WCCP does not interfere with normal router or switch operations.

About WCCP Flow Redirection on WAEs

Flow protection reduces the impact on existing client TCP connections when Edge WAEs are added and removed from a service group. By default, WCCP flow redirection is enabled on a WAE. Flow protection reduces the impact on existing client TCP connections when Edge WAEs are added and removed from a service group. The client impact is reduced because of flow protection in the following situations:

- **WAAS network expansion**—When Edge WAEs are added to the service group, the newly started Edge WAEs receives traffic that was previously processed by a different Edge WAE. It forwards the traffic to the relevant Edge WAE for continued processing. New connections are processed by the new Edge WAE.
- **Edge WAE replacement following a failure**—When an Edge WAE fails, another Edge WAE may receive traffic that was previously processed by either that Edge WAE or the origin file server. The receiving Edge WAE operates according to the previous two use cases.

Without flow protection, established client connections are broken through a TCP RESET in the situations listed earlier. Flow protection applies to all supported WCCP services and cannot be configured on a per-service basis.

Viewing or Modifying the General WCCP Settings on WAEs

In a WAAS network, the following set of configuration parameters for a WAE is collectively referred to as the "WCCP general settings":

- WCCP version
- Flow redirection
- Slow start
- Shutdown delay

Table 4-3 lists the default values for the WCCP general settings on a WAE.

Table 4-3 Default Values for the WCCP General Settings on a WAE

Feature	Default Value	Comment
WCCP Version 2	Disabled	WCCP Version 2 instead of WCCP Version 1 must be used because WCCP Version 1 only supports web traffic (port 80).
Flow redirection	Enabled	Keeps the TCP flow intact and avoids overwhelming the WAE when it comes up and is assigned new traffic.
Slow start	Disabled	Within a service group of WAEs, TCP connections are redirected to other WAEs as units are added or removed. A WAE can be overloaded if it is reassigned new traffic too quickly or it is introduced abruptly into a high-bandwidth connection. WCCP slow start performs the following tasks to prevent a WAE from being overwhelmed when it comes online or is reassigned new traffic: • TCP flow protection with WCCP Version 2 is enabled and a WAE is introduced into the service group • TCP flow protection when WCCP Version 2 is disabled and a WAE is leaving the service group • Load assignment to the WAE in slow increments rather than a full load at bootup
Shutdown delay	120 seconds	To prevent broken TCP connections, the WAE performs a clean shutdown of WCCP after a reload or WCCP is shut down (disabled) on the WAE.

To ensure consistency, we recommend that you change the WCCP general settings on a device group basis instead of on an individual device.

Note This section assumes that you have already completed a basic WCCP configuration for your WAAS network that includes the configuration of the TCP promiscuous mode service (WCCP Version 2 services 61 and 62), as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.

To centrally view or modify the general WCCP settings for a WAE (or a group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

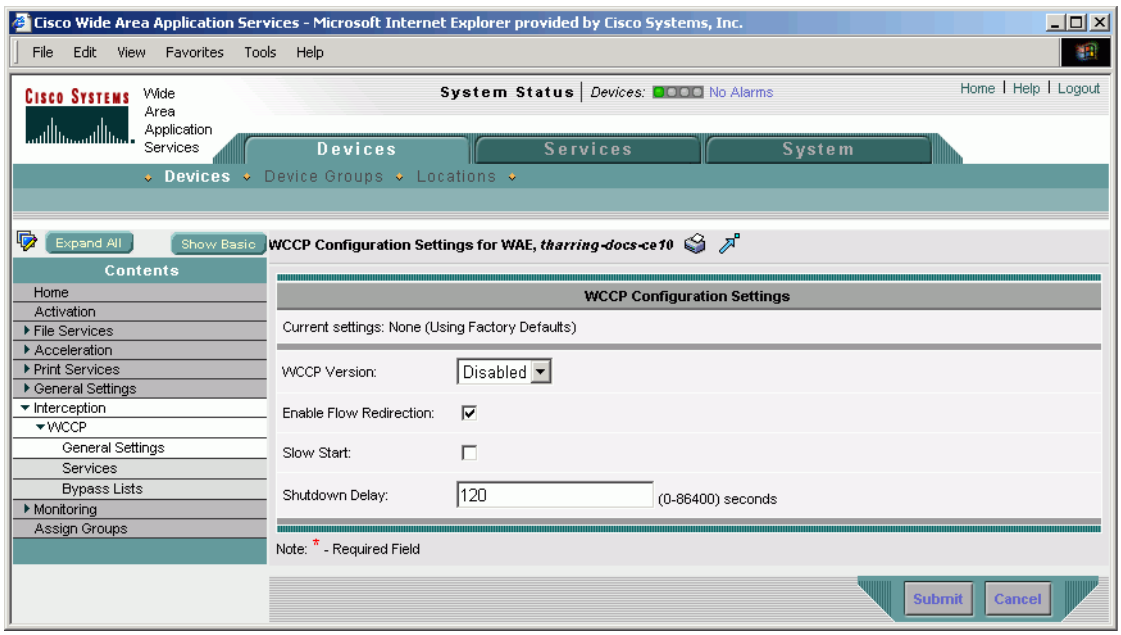
Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to change the values of the WCCP general settings.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

Step 5 In the Contents pane, choose **Interception > WCCP > General Settings**. The WCCP General Configuration Settings window appears. (See Figure 4-3.)

Figure 4-3 WCCP General Configuration Settings Window



Step 6 Check the current settings for the chosen device (or device group).

- To keep the current settings and to close the window, click **Cancel**.
- To modify the current settings, change the current setting as described in the rest of this procedure.

By default, WCCP is disabled on a WAE. However, as part of the initial configuration of WCCP in your your WAAS network, you should have enabled WCCP Version 2 on your WAEs (the Edge WAE and the Core WAE) as well as on the routers in the data center and branch office that will be transparently redirecting requests to these WAEs. For information about how to perform a basic WCCP configuration in your WAAS network, see the *Cisco Wide Area Application Services Quick Configuration Guide.*

Step 7 From the WCCP Version drop-down list, choose **2** to enable WCCP Version 2 on the chosen device (or device group), or choose **Disabled** to disable WCCP on the chosen device (or device groups).

Note You must configure the chosen device (or device group) to use WCCP Version 2 instead of WCCP Version 1 because WCCP Version 1 only supports web traffic (port 80). When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service (WCCP Version 2 service 89) on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

Be sure the routers used in the WCCP environment are running a version of the Cisco IOS software that also supports the WCCP Version 2.

Step 8 To keep the TCP flow intact, and to avoid overwhelming the device (or device groups) when they come up or are reassigned new traffic, check the **Enable Flow Redirection** check box. For more information on this feature, see the "About WCCP Flow Redirection on WAEs" section on page 4-17.

Step 9 To enable the slow start capability on the device (or device group), check the **Slow Start** check box. By default, this feature is disabled. Slow start is applicable only in the following cases:

- Initial bootup when there is no WAE present in the server farm
- When a new WAE is added to a cluster that is not handling the full load (for example, when there are some buckets that are being shed by the cluster)

In all other situations slow start is not necessary and all the WAEs can be assigned their share of traffic immediately.

Step 10 In the Shutdown Delay field, specify the maximum amount of time (in seconds) that the chosen device (or device group) waits to perform a clean shutdown of WCCP. The default is 120 seconds.

The WAE does not reboot until either all connections have been serviced or the maximum wait time (specified through this Shutdown Delay field) has elapsed for WCCP Version 2.

Step 11 Click **Submit** to save the changes.

To configure WCCP settings from the CLI, you can use the **wccp version**, **wccp flow-redirect**, **wccp slow-start**, and **wccp shutdown** global configuration commands.

For more information about a graceful shut down of WCCP Version 2 on WAEs, see the "Configuring WAEs for a Graceful Shutdown of WCCP" section on page 4-38.

Viewing a List of Currently Configured WCCP Services for WAEs

To centrally view a list of the WCCP services that are currently configured for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Devices Groups**).

The Devices window appears, listing all the device types configured in the WAAS network.

Step 2 Click the **Edit** icon next to the device (or device group) for which you want to view a list of currently configured WCCP services.

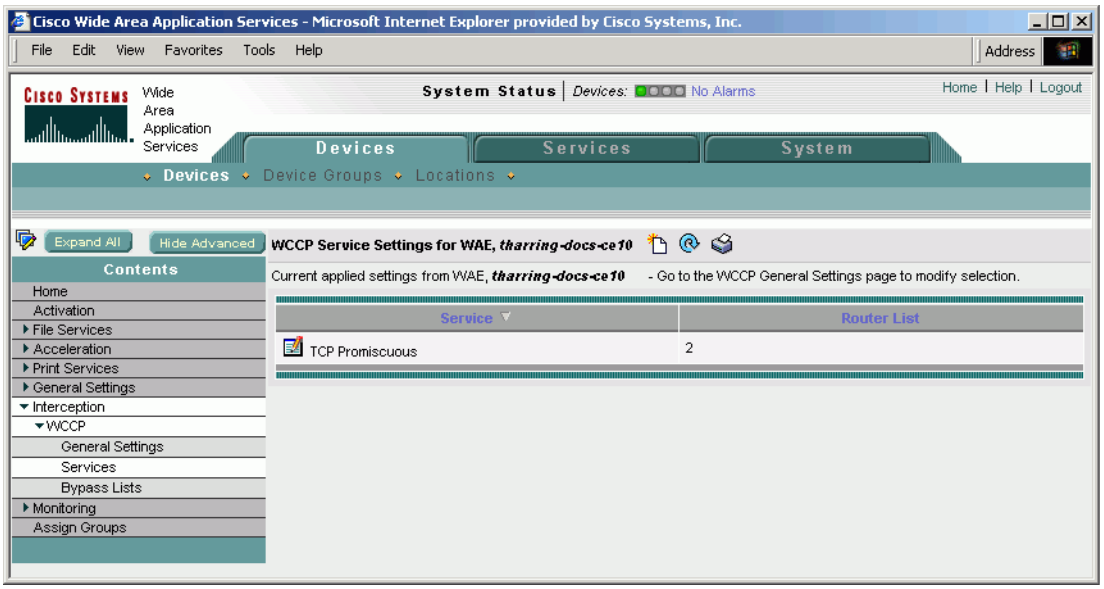
Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

Step 5 In the Contents pane, choose **Interception > WCCP > Services**.

The WCCP Service Settings for WAE window appears with a list of the currently configured WCCP services for the chosen device (or device group). (See Figure 4-4.)

Figure 4-4 Viewing a List of Currently Configured WCCP Services



In the example shown in Figure 4-4, there is currently one WCCP service, the TCP promiscuous service, configured on the chosen device and this service has been configured to use router list 2. (See Table 4-4 for a description of the types of supported WCCP services.)

Step 6 Click the **Edit WCCP Service Setting** icon next to the service that you want to modify to modify an existing WCCP service.

For more information about modifying a service, see the "Modifying the Current Settings of a WCCP Service for WAEs" section on page 4-21.

Step 7 Click the **Create New WCCP Service Setting** icon in the taskbar to create a new WCCP service for the chosen device (or device group).

For more information about creating a new WCCP service for a WAE or group of WAEs, see the "Creating Additional WCCP Services on WAEs" section on page 4-29.

To view currently configured WCCP services from the CLI, you can use the **show wccp services** EXEC command.

Modifying the Current Settings of a WCCP Service for WAEs

To centrally modify the current settings of a WCCP service for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to modify the WCCP settings or services.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

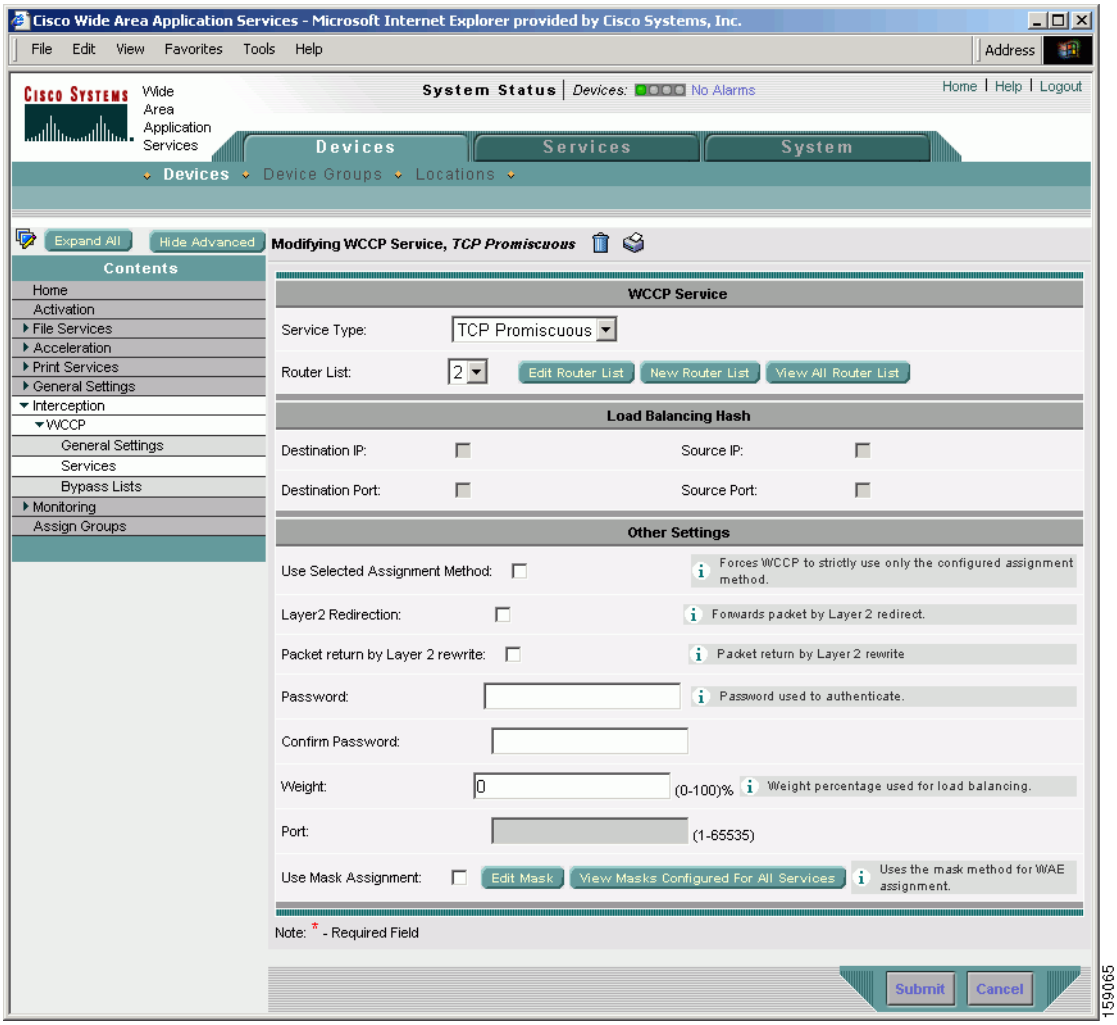
Step 5 In the Contents pane, choose **Interception > WCCP > Services**.

The WCCP Service Settings window appears with a list of the currently configured WCCP services for the chosen device (or device group).

Step 6 Click the **Edit WCCP Service Setting** icon next to the service that you want to modify.

The Modifying WCCP Service window appears. (See Figure 4-5.)

Figure 4-5 Modifying the Settings of a WCCP Service



Note All settings for a particular WCCP service can be configured only after it has been associated with a router list.

Step 7 From the Service Type drop-down list, choose the type of WCCP service that you want to modify for the chosen device (or device group). (See Table 4-4 for a description of the service types.)

Table 4-4 WCCP Service Types

Service Type	Description of Services
CIFS caching	WCCP Version 2 CIFS caching service (service 89). The WCCP CIFS caching service is a dynamic service that intercepts all TCP traffic destined for ports 139 and 445 and redirects it to the corresponding redirect port (139 or 445). Load balancing distributes traffic based on the source IP address, by default. The WCCP-enabled router uses service ID 89 to access this service.
TCP promiscuous mode	WCCP Version 2 TCP promiscuous mode service (services 61 and 62) intercepts all TCP traffic that is destined for any TCP port and transparently redirects it to the WAE. Load balancing distributes traffic based on the source IP address, by default. The WCCP-enabled router uses service IDs 61 and 62 to access this service.

Note When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service (WCCP Version 2 service 89) on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

Step 8 Associate a router list with the chosen WCCP service (for example, the TCP promiscuous mode service) by choosing the appropriate number of the WCCP router list from the Router List drop-down list.

Only configured WCCP router lists are displayed in the drop-down list. As part of the initial configuration of your WAAS network, you will have already created at least one WCCP router list for your Edge WAE and a second WCCP router list for your Core WAE, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*. For more information about WCCP router lists, see the following sections:

- Modifying the Configuration of WCCP Router Lists for WAEs, page 4-34
- Deleting a WCCP Router List from WAEs, page 4-35
- Defining Additional WCCP Router Lists on WAEs, page 4-36

Step 9 (Optional) Modify the current load-balancing settings for the chosen WCCP service, as follows:

a. To define the load-balancing hash of the destination IP address, check the **Destination IP** check box.

b. To define the load-balancing hash of the source IP address, check the **Source IP** check box.

c. To define the load-balancing hash of the destination port, check the **Destination Port** check box.

d. To define the load-balancing hash of the source port, check the **Source Port** check box.

Note For more information about load balancing, see the "About Load Balancing and WAEs" section on page 4-12.

Step 10 (Optional) Modify the other current settings for the chosen WCCP service, as follows:

a. To force WCCP to use the configured assignment method only, check the **Use Selected Assignment Method** check box. When applied, either of the two load-balancing methods, hash assignment or mask assignment, can be used.

- **Hash assignment**—For the Catalyst 6500 series switches and Cisco 7600 series routers, this load-balancing method is called WCCP Layer 2 Policy Feature Card (PFC) redirection. This method is intended to achieve forwarding performance of up to 3 Gbps using a combination of the Supervisor Engine 1A and the Multilayer Switch Feature Card 2 (MSFC2).
- **Mask assignment**—This type of load balancing is called the WCCP Layer 2 Policy Feature Card 2 (PFC2) redirection. It uses a combination of the Supervisor Engine 2 and the MSFC2.

You can specify only one load-balancing method (hashing or masking) per WCCP service in an Edge WAE group. The default hashing assignment for the CIFS caching service is based on the source IP address. For more information about load-balancing assignment methods, see the "About Load-Balancing Assignment Methods" section on page 4-13.

b. To permit the WAE (or device group) to receive transparently redirected traffic from a WCCP Version 2-enabled switch or router, if the WAE has a Layer 2 connection with the device, and the device is configured for Layer 2 redirection, check the **Layer2 Redirection** check box.

WCCP on a router or switch can take advantage of switching hardware that either partially or fully implements the traffic interception and redirection functions of WCCP in hardware at Layer 2. The WAE can then perform a Layer 2 or MAC address rewrite redirection if it is directly connected to a compatible Cisco switch. This redirection processing is accelerated in the switching hardware, which makes this method a more efficient method than Layer 3 redirection using GRE. The WAE must have a Layer 2 connection with the router or switch. Because there is no requirement for a GRE tunnel between the switch and the WAE, the switch can use a cut-through method of forwarding encapsulated packets if you check the **Layer2 Redirection** check box. For more information, see the "About Packet-Forwarding Methods" section on page 4-14.

c. To permit Layer 2 rewriting to be used for packet return, check the **Packet return by Layer 2 rewrite** check box.

d. In the Password field, specify the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service. Be sure to enable all other WAEs and routers within the cluster with the same password. Passwords must not exceed 8 characters in length. Reenter the password in the Confirm Password field.

Note For information about how to use the CLI to specify the service group password on a router, see the "Setting a Service Group Password on a Router" section on page 4-11.

e. In the Weight field, specify the weight parameter that represents a percentage of the total load redirected to the device for load-balancing purposes (for example, a WAE with a weight of 30 receives 30 percent of the total load). The weight value ranges from 0 to 100 percent. By default, weights are not assigned and the traffic load is distributed evenly between the WAEs in a service groups.

f. (Optional). You should only specify a port number in the Port field if you are filtering redirected traffic.

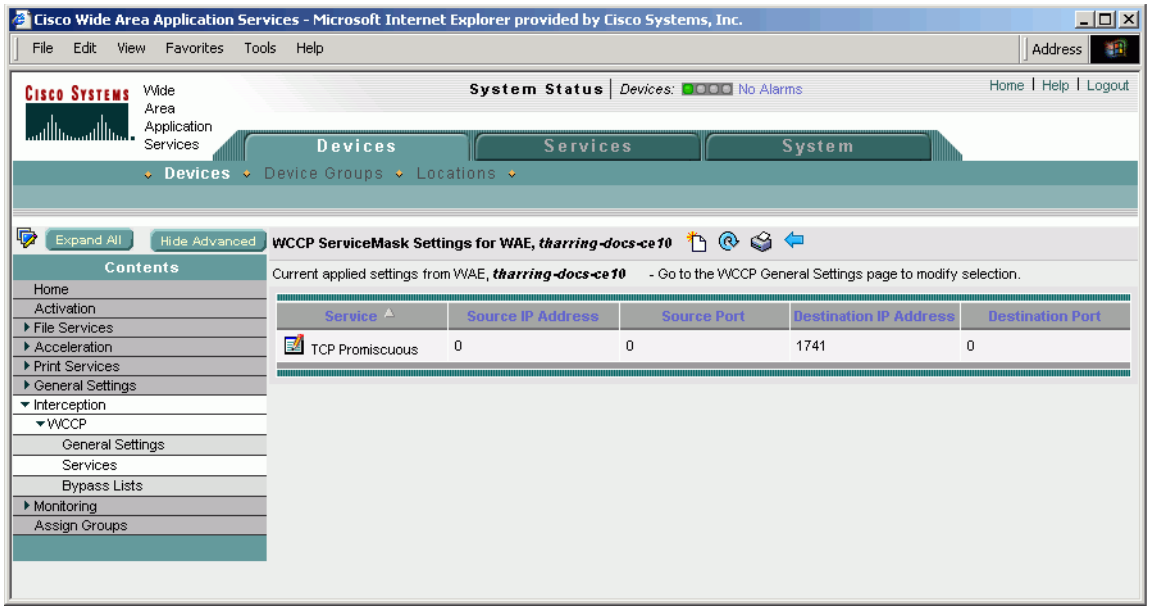
By default, the IP Protocol 6 is specified for the TCP promiscuous mode service, specifying that all TCP traffic from any TCP port will be intercepted and redirected to the WAE. Consequently, the WCCP-Version 2 enabled routers that have been configured to support the TCP promiscuous mode service for the chosen device or device group will intercept and redirect all TCP traffic destined for any TCP port to the chosen device or device group. Because the TCP promiscuous mode service is configured on the chosen device or device group, the chosen device or device groups will accept all redirected TCP traffic on any port.

g. To use the mask method for WAE assignment, check the **Use Mask Assignment** check box.

Step 11 (Optional) To modify an existing service mask for the chosen WCCP service, click the **Edit Mask** button. For more information about modifying service masks, see the "Modifying WCCP Service Masks for WAEs" section on page 4-28.

Step 12 (Optional) To view a list of all configured WCCP service masks for the chosen service, click the **View Masks Configured for All Services** button. The WCCP Service Mask Settings windows appears. (See Figure 4-6.)

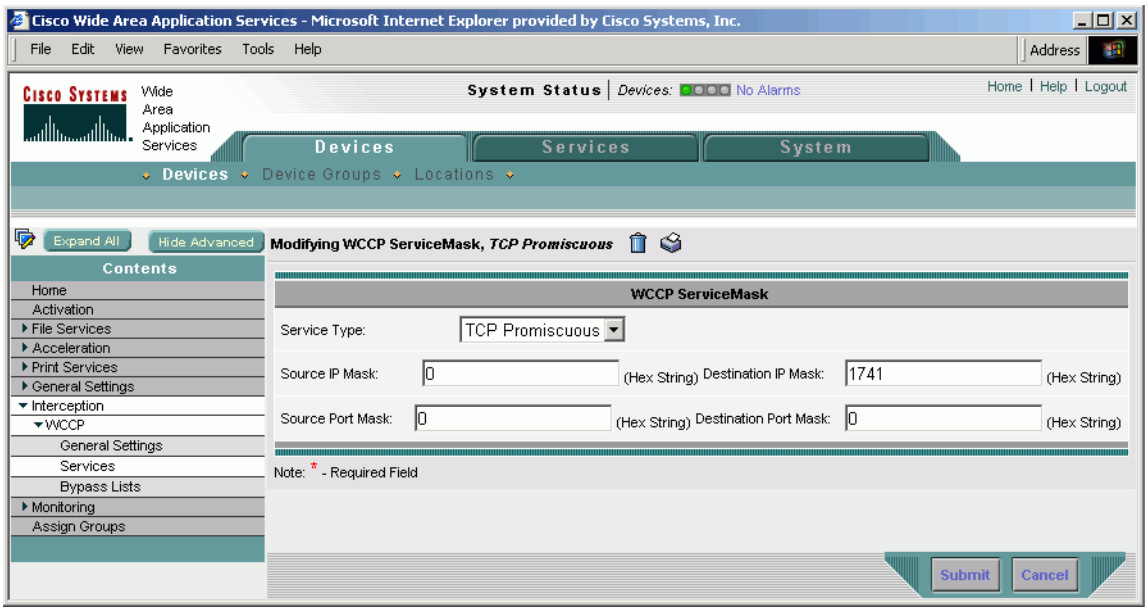
Figure 4-6 Viewing a List of WCCP Service Masks



Step 13 From the WCCP Service Mask Settings window, you can perform the following tasks:

- To edit a WCCP service mask, click the **Edit WCCP Service Mask** icon next to the service mask that you want to modify. The Modifying WCCP Service Mask window appears. (See Figure 4-7.)

Figure 4-7 Modifying a WCCP Service Mask



Change the values of the settings that you want to modify and click **Submit**, as follows:

- In the Source IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet source IP address. The range is 0x00000000–0xFE000000. The default is 0x00000000.
- In the Source Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet source port number. The port mask range is 0x00–0xFE. The default is 0x0.
- In the Destination IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet destination IP address. The range is 0x0000000–0XFE000000. The default is 0x00001741.
- In the Destination Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet destination port number. The port mask range is 0x00–0xFE. The default is 0x0.

Note You can also edit a service mask by clicking the **Edit Mask** button in the Modifying WCCP Service window. (See Figure 4-5.)

- To delete an existing WCCP service mask, click the **Edit WCCP Service Mask** icon next to the service mask that you want to delete. The Modifying WCCP Service Mask window appears. (See Figure 4-7.) Click the **Delete WCCP Service Mask** icon in the taskbar and click **Submit**.

To configure these WCCP services from the CLI, you can use the **wccp cifs-cache** and **wccp tcp-promiscuous** global configuration commands.

Creating a WCCP Service Mask for an Existing WCCP Service

To centrally create a service mask for an existing WCCP service for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Devices Group**).

Step 2 Click the **Edit** icon next to the device (or device group) for which you want to a WCCP service mask.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

Step 5 In the Contents pane, choose **Interception > WCCP > Services**.

The WCCP Service Settings for WAE window appears.

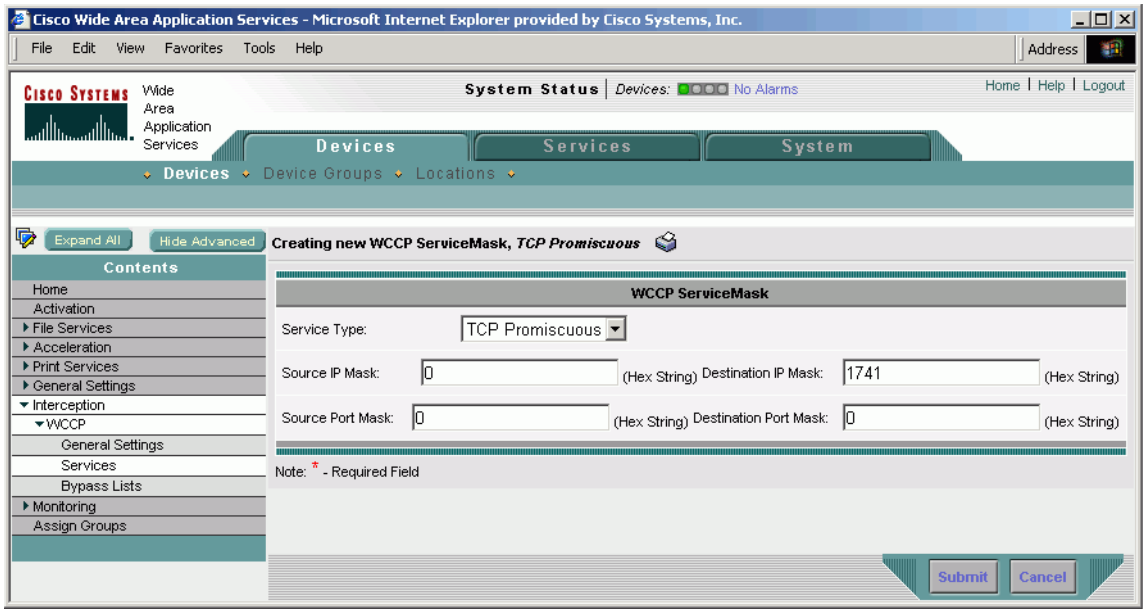
Step 6 Click the **Create New WCCP Service Setting** icon in the taskbar.

The Creating New WCCP Service window appears.

Step 7 Click the **Create New Mask** button.

The Creating New WCCP Service Mask window appears. (See Figure 4-8.)

Figure 4-8 Creating a WCCP Service Mask



You can configure up to 16 WCCP service masks. Bit masks are specified as hexadecimal numbers. All the specified bit masks together cannot have more than 7 bits set. For example, a correct way of using three masks is 0xF (4 bits), 0x1 (1 bit), and 0x3 (2 bits) for a total of 7 bits. In this situation, you cannot configure any additional mask other than 0x0, otherwise, an error message is displayed. An example of using four masks could be 0xA (2 bits), 0x7 (3 bits), 0x8 (1 bit), 0x1 (1 bit) for a total of 7 bits.

Step 8 Click **Submit** to save the settings for the WCCP service mask.

Modifying WCCP Service Masks for WAEs

To centrally modify a service mask for a WCCP service that is configured for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Devices Group**).

Step 2 Click the **Edit** icon next to the device (or device group) for which you want to modify a WCCP service mask.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

Step 5 In the Contents pane, choose **Interception > WCCP > Services**.

The WCCP Service Settings for WAE window appears.

Step 6 Click the **Create New WCCP Service Setting** icon in the taskbar.

The Creating New WCCP Service window appears.

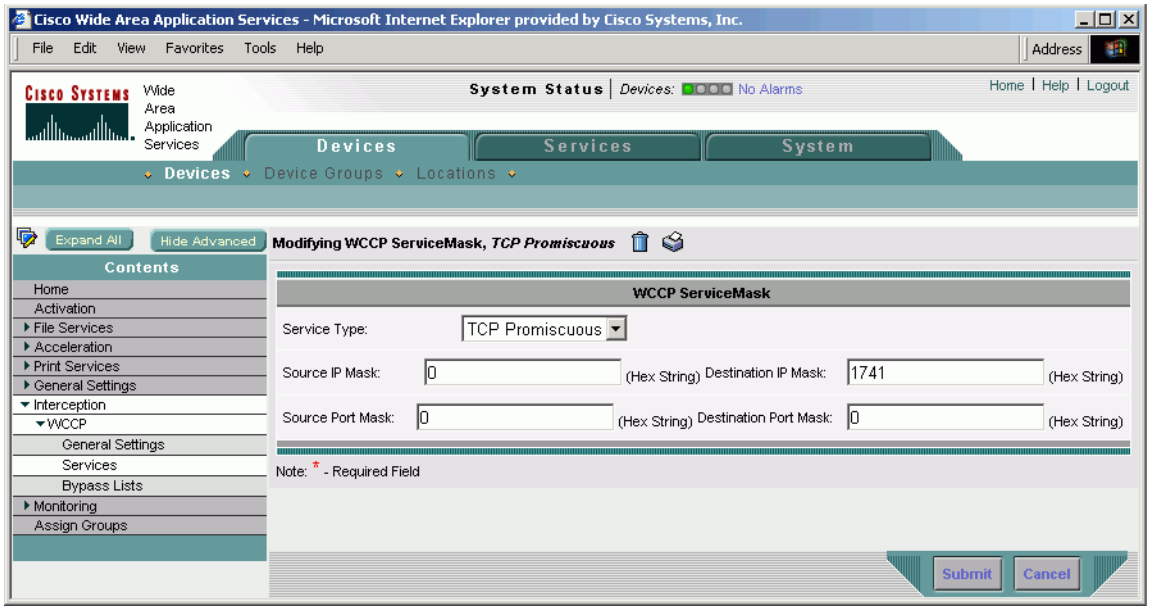
Step 7 Choose a WCCP service from the Service Type drop-down list, as follows:

- Choose **TCP Promiscuous** from the list to modify a WCCP mask for the TCP promiscuous mode service for the chosen device or device group.
- Choose **CIFS Cache** from the list to modify a WCCP mask for the CIFS caching service for the chosen device or device group.

Step 8 Click the **Edit Mask** button.

The Modifying WCCP Service Mask window appears. (See Figure 4-9.)

Figure 4-9 Modifying a WCCP Service Mask



Step 9 In the Source IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet source IP address. The range is 0x00000000–0xFE000000. The default is 0x00000000.

Step 10 In the Source Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet source port number. The port mask range is 0x00–0xFE. The default is 0x0.

Step 11 In the Destination IP Mask field, specify the IP address mask defined by a hexadecimal number (for example, 0xFE000000) used to match the packet destination IP address. The range is 0x0000000–0XFE000000. The default is 0x00001741.

Step 12 In the Destination Port Mask field, specify the port mask defined by a hexadecimal number (for example, 0xFE00) used to match the packet destination port number. The port mask range is 0x00–0xFE. The default is 0x0.

Step 13 Click **Submit** to save the new settings for the WCCP service mask.

Creating Additional WCCP Services on WAEs

To centrally create additional WCCP services for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to create an additional WCCP service.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

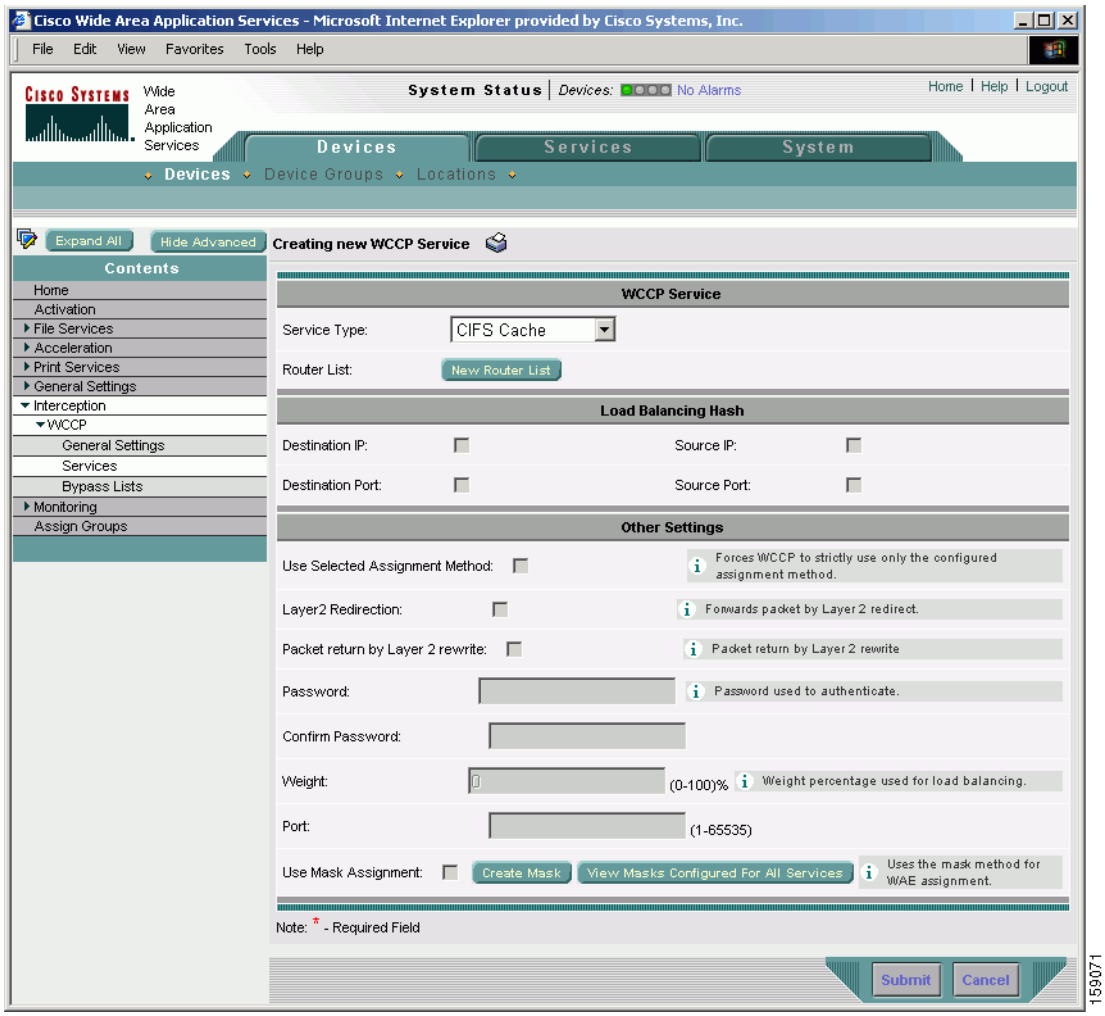
Step 5 In the Contents pane, choose **Interception > WCCP > Services**.

The WCCP Service Settings window appears with a list of the currently configured WCCP services for the chosen device (or device group).

Step 6 Click the **Create New WCCP Service Setting** icon next to the service that you want to modify.

The Creating a New WCCP Service window appears. (See Figure 4-10.)

Figure 4-10 Configuring the Settings for an Additional WCCP Service



Note You can configure the TCP promiscuous mode service (WCCP services 61 and 62) or the CIFS caching service (WCCP service 89) on a WAE (or a group of WAEs). When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

All settings for a particular WCCP service can be configured only after it has been associated with a router list.

Step 7 From the Service Type drop-down list, choose the type of WCCP service that you want to create for the chosen device (or device group). See Table 4-4 for a description of the service types.

Step 8 Associate a router list with the chosen new WCCP service (for example, the CIFS caching service) by choosing the appropriate number from the Router List drop-down list. For example, choose **3** to choose router list 3.

Only configured router lists are displayed in the drop-down list. Router lists can be configured, modified, and viewed by following the links in the Creating New WCCP Service window. WCCP Version 2 allows multiple routers to access a WAE service group. Multiple router access is useful for configurations that contain multiple routers either for redundancy or because they are aggregating a number of interfaces and either the load or the number of interfaces is too large for a single router. Sharing a WAE service group reduces the caching of redundant information that would occur with multiple service groups that are each accessed by a separate router.

As part of the initial configuration of your WAAS network, as described in the *Cisco Wide Area Application Services Quick Configuration Guide,* you will have already created at least one router list for your Edge WAE and a second router list for your Core WAE. For more information about WCCP router lists, see the following sections:

- Modifying the Configuration of WCCP Router Lists for WAEs, page 4-34
- Deleting a WCCP Router List from WAEs, page 4-35
- Defining Additional WCCP Router Lists on WAEs, page 4-36

Step 9 (Optional) Specify the load balancing settings for the chosen new WCCP service, as follows:

a. To define the load-balancing hash of the destination IP address, check the **Destination IP** check box.

b. To define the load-balancing hash of the source IP address, check the **Source IP** check box.

c. To define the load-balancing hash of the destination port, check the **Destination Port** check box.

d. To define the load-balancing hash of the source port, check the **Source Port** check box.

Note For more information on load balancing, see the "About Load Balancing and WAEs" section on page 4-12.

Step 10 (Optional) Specify the other settings for the chosen new WCCP service, as follows:

a. To force WCCP to use the configured assignment method only, check the **Use Selected Assignment Method** check box. When applied, either of the two load-balancing methods, hash assignment or mask assignment, can be used.

- **Hash assignment**—For the Catalyst 6500 series switches and Cisco 7600 series routers, this load-balancing method is called WCCP Layer 2 Policy Feature Card (PFC) redirection. This method is intended to achieve forwarding performance of up to 3 Gbps using a combination of the Supervisor Engine 1A and the Multilayer Switch Feature Card 2 (MSFC2).
- **Mask assignment**—This type of load-balancing is called the WCCP Layer 2 Policy Feature Card 2 (PFC2) redirection. It uses a combination of the Supervisor Engine 2 and the MSFC2.

You can specify only one load-balancing method (hashing or masking) per WCCP service in an Edge WAE group. The default hashing assignment for the CIFS caching service is based on the source IP address. For more information about load-balancing assignment methods, see the "About Load-Balancing Assignment Methods" section on page 4-13.

b. To permit the WAE (or device group) to receive transparently redirected traffic from a WCCP Version 2-enabled switch or router, if the WAE has a Layer 2 connection with the device, and the device is configured for Layer 2 redirection, check the **Layer2 Redirection** check box.

WCCP on a router or switch can take advantage of switching hardware that either partially or fully implements the traffic interception and redirection functions of WCCP in hardware at Layer 2. The WAE can then perform a Layer 2 or MAC address rewrite redirection if it is directly connected to a compatible Cisco switch. This redirection processing is accelerated in the switching hardware, which makes this method a more efficient method than Layer 3 redirection using GRE. The WAE must have a Layer 2 connection with the router or switch. Because there is no requirement for a GRE

tunnel between the switch and the WAE, the switch can use a cut-through method of forwarding encapsulated packets if you check the **Layer2 Redirection** check box. For more information, see the "About Packet-Forwarding Methods" section on page 4-14.

c. In the Password field, specify the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service. Be sure to enable all other WAEs and routers within the cluster with the same password. Passwords must not exceed 8 characters in length. Reenter the password in the Confirm Password field.

Note For information about how to use the CLI to specify the service group password on a router, see the "Setting a Service Group Password on a Router" section on page 4-11.

d. In the Weight field, specify the weight parameter that represents a percentage of the total load redirected to the device for load-balancing purposes (for example, a WAE with a weight of 30 receives 30 percent of the total load). The weight value ranges from 0 to 100 percent. By default, weights are not assigned and the traffic load is distributed evenly between the WAEs in a service groups.

e. By default, the IP Protocol 6 is specified in the WCCP service group, which means any TCP port. Consequently, you should only specify a port number in the Port field if filtering redirected traffic.

f. To use the mask method for WAE assignment, check the **Use Mask Assignment** check box.

Step 11 (Optional) To create a service mask for this new WCCP service, click the **New Mask** button.

For more information about modifying service masks, see the "Creating a WCCP Service Mask for an Existing WCCP Service" section on page 4-27.

Step 12 Click **Submit.**

Remember that after you have created an additional WCCP service for the chosen WAE (or group of WAEs), make sure that the routers that are included on the WCCP router list that has been associated with this WCCP service have also been configured to support this WCCP Version 2 service. You must use the CLI to enable WCCP Version 2 and to configure a WCCP service on a router. For an example, of how to use the CLI to enable WCCP Version 2 on a router and configure the TCP promiscuous mode service (WCCP services 61 and 62) on a router, see the *Cisco Wide Area Application Services Quick Configuration Guide*.

Viewing a WCCP Router List Configuration for WAEs

To centrally view the list of currently defined WCCP router list for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to display a WCCP router list.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

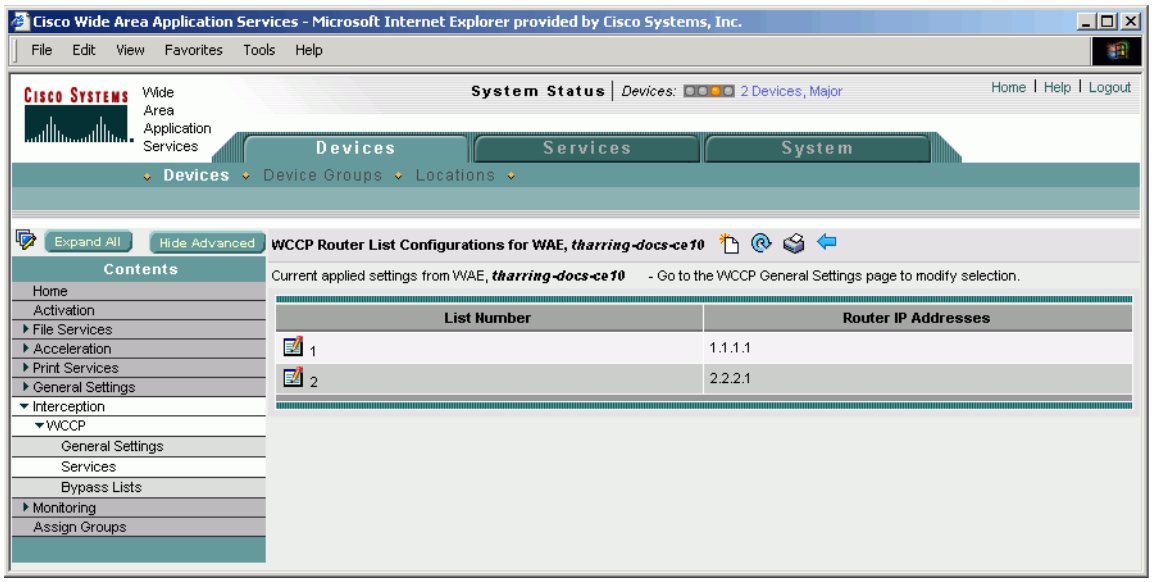
Step 5 In the Contents pane, choose **Interception > WCCP > Services**. The WCCP Service Settings window appears.

Step 6 Click the **Edit** icon next to any of the listed WCCP services. The Modifying WCCP Service window appears.

Step 7 Click the **View All Router List** button.

The WCCP Router List Configurations window for the chosen device (or device group) appears. (See Figure 4-11.)

Figure 4-11 Viewing WCCP Router List Configurations



As Figure 4-11 shows, the configuration for the WCCP router lists (the number of the router list and IP addresses of each router that is included in each router list) is displayed.

Note To modify the configuration of a specific WCCP router list, click the **Edit** icon next to the router list and use the displayed Modifying Router List to modify the chosen router list. For more information about modifying router lists, see the "Modifying the Configuration of WCCP Router Lists for WAEs" section on page 4-34. For information about how to delete a WCCP router list from a WAE (or group of WAEs), see the "Deleting a WCCP Router List from WAEs" section on page 4-35.

To view a router list from the CLI, you can use the **show wccp routers** EXEC command.

Modifying the Configuration of WCCP Router Lists for WAEs

To centrally modify the configuration of a WCCP router list (for example, add or delete a router from a router list) for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to modify the router list configuration.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

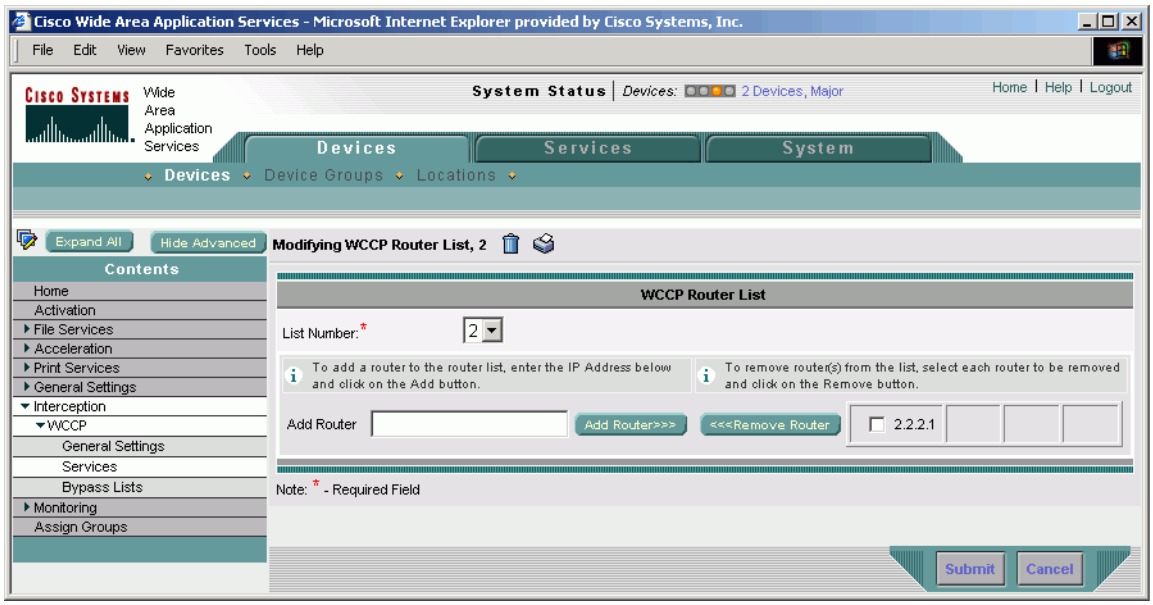
Step 5 In the Contents pane, choose **Interception > WCCP > Services**.

The WCCP Service Settings window appears.

Step 6 Click the **Edit** icon next to a WCCP service that is currently configured to use the router list that you want to modify. The Modifying WCCP Service window appears.

Step 7 Click the **Edit Router List** button. The Modifying WCCP Router List window appears. (See Figure 4-12.)

Figure 4-12 Modifying a WCCP Router List



Step 8 To add a router to the chosen router list, enter the router's IP address in the Add Router field, and click the **Add Router** button.

Step 9 To remove a router from the chosen router list, check the check box next to the IP address of the router that you want to remove and click the **Remove Router** button.

Step 10 Click **Submit** to save the settings.

Deleting a WCCP Router List from WAEs

When you delete a router list, the WCCP Version 2 services that have been configured to use this router list are also deleted. Make sure that the WCCP service is associated with a different router list, if required, before deleting the previously configured router list.

To centrally delete a WCCP router list (for example, add or delete an IP address from a router list) for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to delete a WCCP router list.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

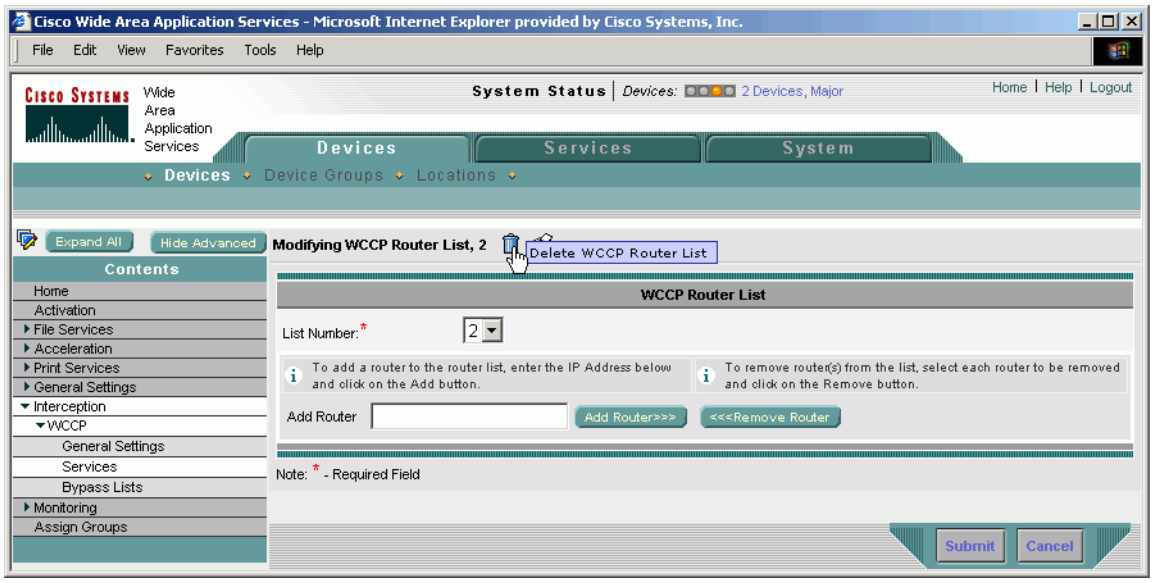
Step 5 In the Contents pane, choose **Interception > WCCP > Services**. The WCCP Service Settings window appears.

Step 6 Click the **Edit Router List** button. The Modifying WCCP Router List window appears.

Step 7 Remove all of the listed routers from the chosen router list by checking the check the check box next to the IP address of the router that you want to remove and clicking the **Remove Router** button.

Step 8 After you have removed all the routers from the chosen router list (for example, router list 2), click the **Delete Router List** icon in the taskbar. (See Figure 4-13.)

Figure 4-13 Deleting a WCCP Router List



The system displays a dialog box asking you to confirm that you want to permanently delete the router list configuration. To confirm your decision, click **OK**. The selected router list and the associated WCCP services are deleted from the chosen device (or device group).

Defining Additional WCCP Router Lists on WAEs

As part of configuring a WCCP service on a WAE, you must create a list of WCCP Version 2-enabled routers that support a specific WCCP service (for example, the TCP promiscuous service or the CIFS caching service) for the WAE. You can define a WCCP router list through the WAAS CLI (the **wccp router-list** global configuration command) or the WAAS Central Manager GUI.

Typically, WAAS administrators will use the WAAS CLI to define their initial set of WCCP router lists, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*. After you have used the WAAS CLI to complete the initial configuration of your WCCP router lists, we recommend that you use the WAAS Central Manager GUI to centrally manage and modify your WCCP router list configurations for your WAEs.

Note This section assumes that you have already completed a basic WCCP configuration for your WAAS network that includes the configuration of the TCP promiscuous mode service (WCCP Version 2 services 61 and 62), as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.

To centrally define additional WCCP router list for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to create a WCCP router list.

Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

Step 5 In the Contents pane, choose **Interception > WCCP > Services**.

The WCCP Service Settings window appears.

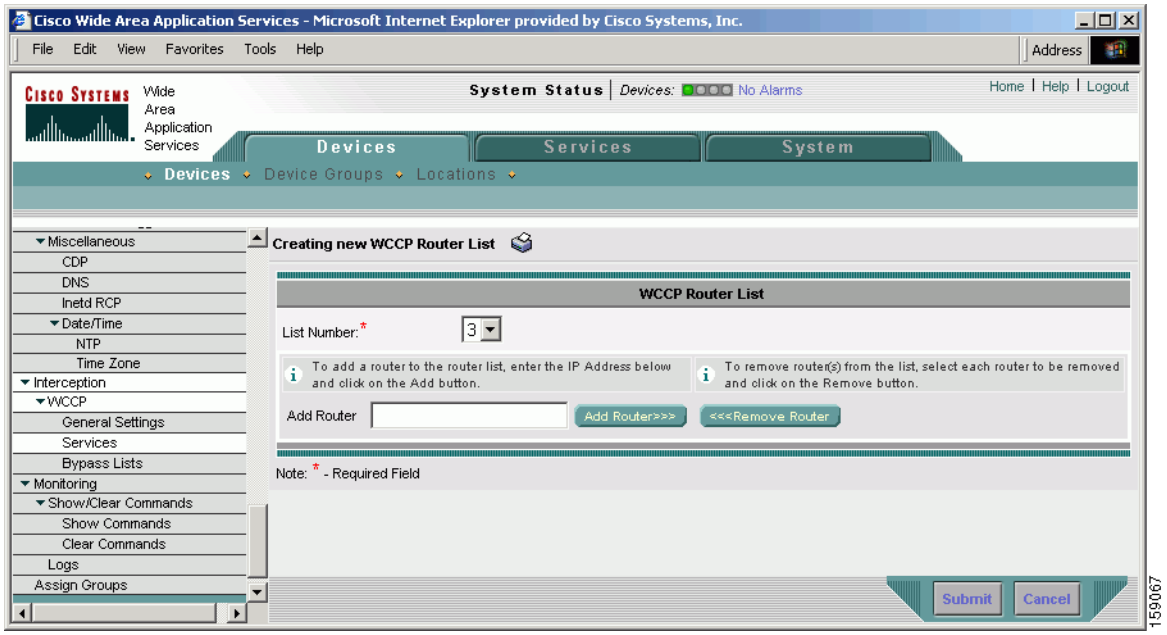
Step 6 Click the **Create New WCCP Service Settings** icon to create a new router list for a WCCP Version 2 service.

The Creating New WCCP Service window appears.

Step 7 Click the **New Router List** button.

The Creating New WCCP Router List window appears. (See Figure 4-14.)

Figure 4-14 Creating a New WCCP Router List



In the example shown in Figure 4-14, **3** is preselected in the List Number drop-down list because there are already two WCCP router lists defined for the chosen device (or device group). Router list 1 has already been defined for the WCCP router in the data center that will be transparently redirecting traffic to the Core WAE, and router list 2 was defined for the WCCP router in the branch office that will be transparently redirecting traffic to the Edge WAE that resides in the same branch office.

Step 8 In the Add Router field, specify the IP address of the router to be added to router list 3.

You must enter at least one IP address. All IP addresses added must be unique within the router list. Otherwise, an error message is displayed on submit.

Step 9 Click **Add** to add an IP address to router list 3.

This list represents the IP address of every WCCP router that is to transparently redirect traffic to the chosen WAE (or group of WAEs) for a particular WCCP service (the TCP promiscuous mode service or the CIFS caching service). If different routers will be used for different WCCP services, you must create more than one router list.

The window refreshes and the addresses are listed in numerical order. The order might not match the order in which IP addresses were entered.

Step 10 Click **Submit** to save the router list or to save any edits you have made to the router IP addresses.

To define a router list from the CLI, you can use the **wccp router-list** global configuration command.

Remember that after you have created a WCCP router list on a WAE or group of WAEs, you must associate the router list with the specific WCCP service (the TCP promiscuous mode service or the CIS-caching service) on the WAE or group of WAEs. For more information on this step, see Step 8 in the "Creating Additional WCCP Services on WAEs" section on page 4-29. Also, make sure that WCCP Version 2 and the specific WCCP service is enabled and configured on the WCCP routers that are included in this new router list, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.

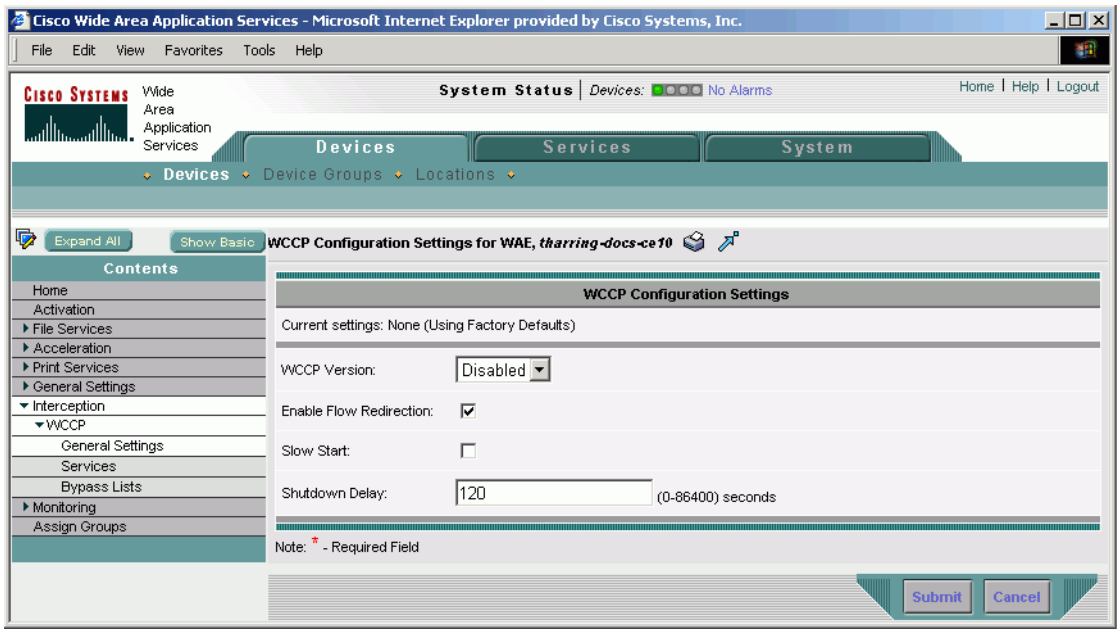
Configuring WAEs for a Graceful Shutdown of WCCP

To prevent broken TCP connections, the WAE performs a clean shutdown of WCCP after you disable WCCP Version 2 on a WAE or reload the WAE.

The WAAS Central Manager GUI lets you centrally disable WCCP Version 2 on a WAE. You can also perform this task locally through the CLI (by entering the **no wccp version** CLI command on the WAE).

To centrally disable WCCP for a chosen device or device group, choose **Disabled** from the **WCCP Version** drop-down list in the WAAS Central Manager's WCCP Configuration Settings window. (See Figure 4-15.)

Figure 4-15 WCCP Configuration Settings Window



The WAE does not reboot until one of the following occurs:

- All the connections have been serviced.
- The maximum wait time (specified through the Shutdown Delay field in the WCCP Configuration Settings window or with the **wccp shutdown max-wait** command [by default, 120 seconds]) has elapsed for WCCP Version 2.

During a clean shutdown of WCCP, the WAE continues to service the flows that it is handling, but it starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the group by having its buckets reassigned to other WAEs by the lead WAE. TCP connections can still be broken if the WAE crashes or is rebooted without WCCP being cleanly shut down.

You cannot shut down an individual WCCP service on a particular port on an WAE (for example, you cannot shut down the CIFS caching service on port 139); you must shut down WCCP on the WAE. After WCCP is shut down on the WAE, the WAE preserves its WCCP configuration settings.

Configuring Static Bypass Lists for WAEs

Using a static bypass allows traffic flows between a configurable set of clients and file servers to bypass handling by the WAE. By configuring static bypass entries on the Edge WAE, you can control traffic interception without modifying the router configuration. IP access lists may be configured separately on the router to bypass traffic without first redirecting it to the Edge WAE. Typically, the WCCP accept list defines the group of file servers that are cached (and the file servers that are not). Static bypass can be used occasionally when you want to prevent WAAS from caching a connection from a specific client to a specific file server (or from a specific client to all file servers).

Note We recommend that you use IP access lists on the WCCP-enabled router, rather than using the static bypass feature, because access lists are more efficient. For information about how to configure bypass lists on a router, see the "Configuring IP Access Lists on a Router" section on page 4-9.

To centrally configure a static bypass list for a WAE (or group of WAEs), follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Device** (or **Device > Device Groups**).

Step 2 Click the **Edit** icon next to the name of the device (or device group) for which you want to create a static bypass list.

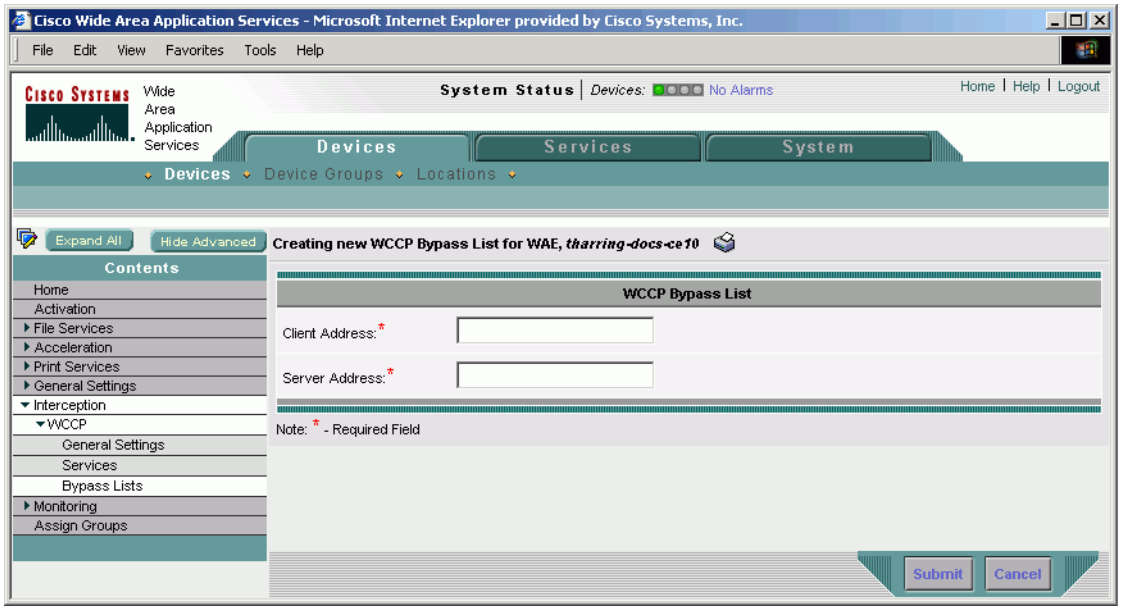
Step 3 Click **Expand All** above the Contents pane.

Step 4 Click **Show Advanced** to display all menu items in the Contents pane.

Step 5 From the Contents pane, choose **Interception > WCCP > Bypass Lists**.

Step 6 In the taskbar, click the **Create New WCCP Bypass List** icon. The Creating new WCCP Bypass List window appears. (See Figure 4-16.)

Figure 4-16 WCCP Bypass List Window



Step 7 Enter the IP address for the client in the Client Address field.

Step 8 Enter the IP address for the server in the Server Address field.

Step 9 Check **Submit** to save the settings.

To configure a static bypass list from the CLI, you can use the **bypass static** global configuration command.

Using Policy-Based Routing to Transparently Redirect All TCP Traffic to WAEs

In today's high performance internetworks, organizations need the freedom to implement packet forwarding and routing according to their own defined policies in a way that goes beyond traditional routing protocol concerns. Where administrative issues require that traffic be routed through specific

paths, policy-based routing (PBR), introduced in the Cisco IOS Software Release 11.0, can provide the solution. By using PBR, you can implement policies that selectively cause packets to take different paths.

PBR also provides a method to mark packets so that certain kinds of traffic receive differentiated, preferential service when used in combination with queuing techniques enabled through the Cisco IOS software. These queuing techniques provide an extremely powerful, simple, and flexible tool to network managers who implement routing policies in their networks.

PBR enables the router to put packets through a route map before routing them. When configuring PBR, you must create a route map that specifies the match criteria and the resulting action if all of the match clauses are met. You must enable PBR for that route map on a particular interface. All packets arriving on the specified interface matching the match clauses will be subject to PBR.

One interface can have only one route map tag; but you can have several route map entries, each with its own sequence number. Entries are evaluated in order of their sequence numbers until the first match occurs. If no match occurs, packets are routed as usual.

```
Router(config-if)# ip policy route--tag
```

The route map determines which packets are routed next.

You can enable PRB to establish a route that goes through WAAS for some or all packets. WAAS proxy applications receive PBR-redirected traffic in the same manner as WCCP redirected traffic, as follows:

1. In the branch office, define traffic of interest on the branch office router (Edge-Router1) as follows:
   a. Specify which traffic is of interest to the LAN interface (ingress interface) on Edge-Router1.

      Use extended IP access lists to define traffic of interest (traffic from all or filtered local source addresses to any or filtered destination address).
   b. Specify which traffic is of interest to the WAN interface (egress interface) on Edge-Router1.

      Use extended IP access lists to define traffic of interest (traffic from all or filtered local source addresses from any or filtered remote addresses).
2. In the data center, specify which traffic is of interest to the data center router (Core-Router1) as follows:
   a. Specify which traffic is of interest to the LAN interface (ingress interface) on Core-Router1.

      Use extended IP access lists to define traffic of interest (traffic from all or filtered local source addresses to any or filtered destination address).
   b. Specify which traffic is of interest to the WAN interface (egress interface) on Core-Router1.

      Use extended IP access lists to define traffic of interest (traffic from all or filtered local source addresses from any or filtered remote addresses).
3. In the branch office, create route maps on Edge-Router1, as follows:
   a. Create a PBR route map on the LAN interface of Edge-Router1.
   b. Create a PBR route map on the WAN interface of Edge-Router1.
4. In the data center, create route maps on Core-Router1, as follows:
   a. Create a PRB route map on the LAN interface of Core-Router1.
   b. Create a PBR route map on the WAN interface of Core-Router1.
5. In the branch office, apply the PBR route maps to Edge-Router1.
6. In the data center, apply the PBR route maps to Core-Router1.

7. Determine which PBR method to use to verify PBR next-hop availability of a WAE. For more information, see the "Methods of Verifying PBR Next-Hop Availability" section on page 4-46.

Note For a complete description of the PBR commands that are referenced in this section, see the *Cisco Quality of Service Solutions Command Reference*.

As Figure 4-17 shows, the WAEs (Edge-WAE1 and Core-WAE1) must reside in an out-of-band network that is separate from the traffic's destination and source. For example, Edge-WAE1 is on a subnet separate from the clients (the traffic source), and Core-WAE is on a subnet separate from the file servers and application servers (the traffic destination). Additionally, the WAE must be connected to the router that is redirecting traffic to it through a tertiary interface (a separate physical interface) or subinterface to avoid a routing loop.

Figure 4-17 Example of Using PBR or WCCP Version 2 for Transparent Redirection of All TCP Traffic to WAEs

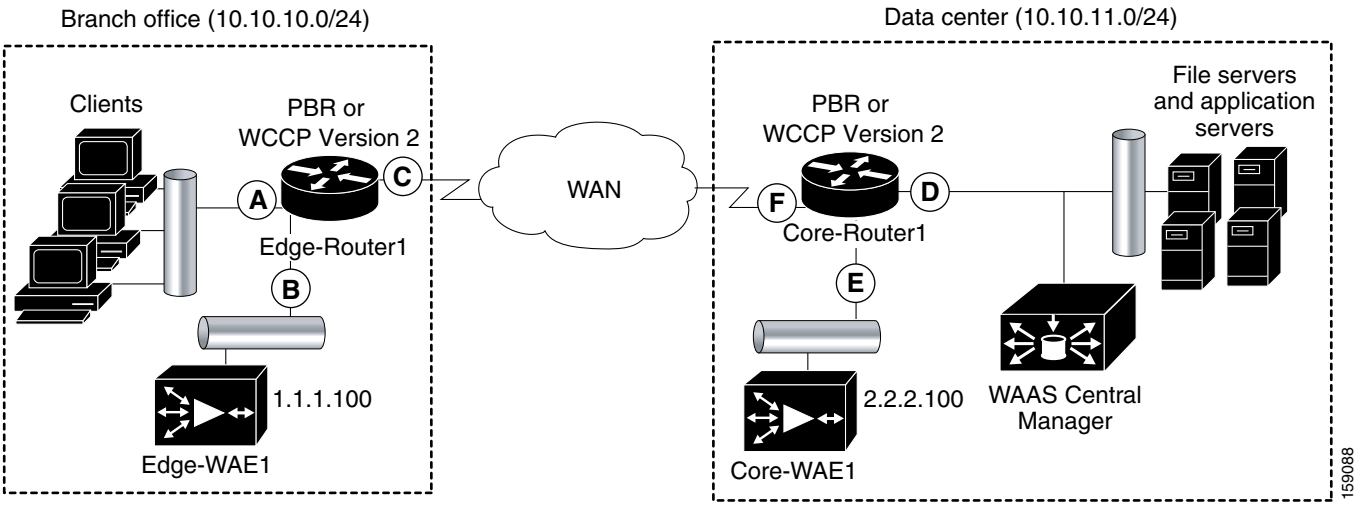


Table 4-5 provides a summary of the router interfaces that you must configure to use PBR or WCCP Version 2 to transparently redirect traffic to a WAE.

Table 4-5 Router Interfaces for WCCP or PBR Traffic Redirection to WAEs

Router interface	Comment
Edge-Router1	
A	Edge LAN interface (ingress interface) that performs redirection on outbound traffic.
B	Tertiary interface (separate physical interface) or a subinterface off of the LAN port on Edge-Router1. Used to attach Edge-WAE1 to Edge-Router1 in the branch office.
C	Edge WAN interface (egress interface) on Edge-Router1 that performs redirection on inbound traffic.
Core-Router1	
D	Core LAN interface (ingress interface) that performs redirection on outbound traffic.
E	Tertiary interface or subinterface off of the LAN port on Core-Router1. Used to attach Core-WAE1 to Core-Router1 in the data center.
F	Core WAN interface (egress interface) on Core-Router1 that performs redirection on inbound traffic.

Note In Figure 4-17, redundancy (for example, redundant routers, switches, WAEs, WAAS Central Managers, and routers) is not depicted.

The following example shows how to configure PBR as the traffic redirection method in a WAAS network that has one Edge WAE in a branch office and one Core WAE in the data center (as shown in Figure 4-17).

Note The commands that are used to configure PBR on a router, can vary based on the Cisco IOS Release installed on the router. For information about the commands that are used to configure PBR for the Cisco IOS Release that you are running on your routers, see the appropriate Cisco IOS configuration guide.

To configure PBR to transparently redirect TCP traffic to WAEs, follow these steps:

Step 1 In the branch office, use extended IP access lists to specify which traffic is of interest to the LAN interface (ingress interface-A) on Edge-Router, as follows:

a. On Edge-Router1, define an extended IP access list within the range of 100 to 199. For example, create access list 100 on Edge-Router1:

```
Edge-Router1(config)# ip access-list extended 100
```

b. On Edge-Router1, specify which traffic is of interest to this particular interface:

- For example, mark any IP/TCP traffic from any local source addresses (traffic for any branch office clients) on any TCP port to any destination as interesting:

```
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any
```

- Alternatively, you can selectively mark interesting traffic by defining the source IP subnet, destination IP address, and TCP port numbers. For example, mark IP/TCP traffic from any local source address on TCP ports 135 and 80 to any destination as interesting:

```
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any eq 135
Edge-Router1(config-ext-nac1)# permit tcp 10.10.10.0 0.0.0.255 any eq 80
```

Step 2 In the branch office, use extended IP access lists to specify which traffic is of interest to the WAN interface (egress interface-C) on Edge-Router1, as follows:

a. On Edge-Router1, define an extended IP access list within the range of 100 to 199. For example, create access list 101 on Edge-Router1:

```
Edge-Router1(config)# ip access-list extended 101
```

b. On Edge-Router1, specify which traffic is of interest to its WAN interface:

- For example, mark any IP/TCP traffic to a local device as interesting:

```
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255
```

- Alternatively, you can selectively mark interesting traffic by defining the source IP subnet, destination IP address, and TCP port numbers. For example, mark IP/TCP traffic to any local source addresses on TCP ports 135 and 80 to any destination as interesting:

```
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255 eq 135
Edge-Router1(config-ext-nac1)# permit tcp any 10.10.10.0 0.0.0.255 eq 80
```

Step 3 In the data center, use extended IP access lists to specify which traffic is of interest to the LAN interface (ingress interface-D) on Core-Router1, as follows:

a. On Core-Router1, define an extended IP access list within the range of 100 to 199. For example, create access list 102 on Core-Router1:

```
Core-Router1(config)# ip access-list extended 102
```

b. On Core-Router1, specify which traffic is of interest to its LAN interface:

- For example, mark any IP/TCP traffic sourced from any local device (for example, traffic sourced from any file server or application server in the data center) on any TCP port to any destination as interesting:

```
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any
```

- Alternatively, you can selectively mark traffic as interesting by defining the source IP subnet, destination IP address, and TCP port numbers. For example, selectively mark IP/TCP traffic sourced from any local device on TCP ports 135 and 80 to any destination as interesting:

```
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any eq 135
Core-Router1(config-ext-nac1)# permit tcp 10.10.11.0 0.0.0.255 any eq 80
```

Step 4 In the data center, use extended IP access lists to mark traffic of interest for the WAN interface (egress interface-F) on Core-Router1, as follows:

a. On Core-Router1, define an extended access list within the range of 100 to 199. For example, create access list 103 on Core-Router1:

```
Core-Router1(config)# ip access-list extended 103
```

b. On Core-Router1, mark interesting traffic for the WAN interface:

- For example, mark any IP/TCP traffic destined to any local device (for example, traffic destined to any file server or application server in the data center) as interesting:

```
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255
```

- Alternatively, you can selectively mark traffic as interesting by defining the source IP subnet, destination IP address, and TCP port numbers. For example, mark IP/TCP traffic on ports 135 and 80 to any local source addresses as interesting:

```
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255 eq 135
Core-Router1(config-ext-nac1)# permit tcp any 10.10.11.0 0.0.0.255 eq 80
```

Step 5 In the branch office, define PBR route maps on Edge-Router1, as follows:

a. Define a route map for the LAN interface (ingress interface). In the following example, the WAAS-EDGE-LAN route map is created:

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

b. Define a route map for the WAN interface (egress interface).

In the following example, the WAAS-EDGE-WAN route map is created:

```
Edge-Router1(config)# route-map WAAS-EDGE-WAN permit
```

c. Specify the match criteria.

Use the **match** command to specify the extended IP access list that Edge-Router1 should use to determine which traffic is of interest to its WAN interface. If you do not specify a **match** command, the route map applies to all packets. In the following example, Edge-Router1 is configured to use the access list 101 as the criteria for determining which traffic is of interest to its WAN interface:

```
Edge-Router1(config-route-map)# match ip address 101
```

Note The **ip address** command option matches the source or destination IP address that is permitted by one or more standard or extended access lists.

d. Specify how the matched traffic should be handled.

In the following example, Edge-Router1 is configured to send the packets that match the specified criteria to the next hop, which is Edge-WAE1 that has an IP address of 1.1.1.100:

```
Edge-Router1(config-route-map)# set ip next-hop 1.1.1.100
```

Note If you have more than one Edge WAE, you can specify the IP address of a second Edge WAE for failover purposes (for example, enter the **set ip next-hop 1.1.1.101** command on Edge-Router1) to specify a next-hop address of 1.1.1.101 (the IP address of Edge-WAE2) for failover purposes. The **next-hop** command is used for failover purposes and not for load-balancing purposes.

Step 6 In the data center, create route maps on Core-Router1, as follows:

a. Define a route map on the LAN interface (ingress interface).

In the following example, the WAAS-CORE-LAN route map is created:

```
Core-Router1(config)# route-map WAAS-CORE-LAN permit
```

b. Define a route map on the WAN interface (egress interface).

In the following example, the WAAS-CORE-WAN route map is created:

```
Core-Router1(config)# route-map WAAS-CORE-WAN permit
```

c. Specify the match criteria.

Use the **match** command to specify the extended IP access list that Core-Router 1 should use to determine which traffic is of interest to its WAN interface. If you do not enter a **match** command, the route map applies to all packets. In the following example, Core-Router1 is configured to use the access list 103 as the criteria for determining which traffic is of interest to its WAN interface:

```
Core-Router1(config-route-map)# match ip address 103
```

d. Specify how the matched traffic is to be handled.

In the following example, Core-Router1 is configured to send packets that match the specified criteria to the next hop, which is Core-WAE1 that has an IP address of 2.2.2.100:

```
Core-Router1(config-route-map)# set ip next-hop 2.2.2.100
```

Note If you have more than one Core WAE, you can specify the IP address of a second Core WAE for failover purposes (for example, enter the **set ip next-hop 2.2.2.101** command on Core-Router1) to specify a next-hop address of 2.2.2.101 (the IP address of Core-WAE2) for failover purposes. The **next-hop** command is used for failover purposes and not for load-balancing purposes.

Step 7 In the branch office, apply the route maps to the LAN interface (ingress interface) and the WAN interface (egress interface) on Edge-Router1, as follows:

a. On Edge-Router1, enter interface configuration mode.

```
Edge-Router1(config)# interface FastEthernet0/0.10
```

b. Specify that the LAN router interface should use the WAAS-EDGE-LAN route map for PBR.

```
Edge-Router1(config-if)# ip policy route-map WAAS-EDGE-LAN
```

c. Enter interface configuration mode.

```
Edge-Router1(config-if)# interface Serial0
```

d. Specify that the WAN router interface should use the WAAS-EDGE-WAN route map for PBR.

```
Edge-Router1(config-if)# ip policy route-map WAAS-EDGE-WAN
```

Step 8 In the data center, apply the route maps to the LAN interface (ingress interface) and the WAN interface (egress interface) on Core-Router1, as follows:

a. On Core-Router1, enter interface configuration mode.

```
Core-Router1(config)# interface FastEthernet0/0.10
```

b. Specify that for PBR, the LAN router interface should use the WAAS-CORE-LAN route map.

```
Core-Router1(config-if)# ip policy route-map WAAS-CORE-LAN
```

c. Enter interface configuration mode.

```
Core-Router1(config-if)# interface Serial0
```

d. Specify that for PBR, the WAN router interface should use the WAAS-CORE-WAN route map.

```
Core-Router1(config-if)# ip policy route-map WAAS-CORE-WAN
```

Methods of Verifying PBR Next-Hop Availability

When using PBR to transparently redirect traffic to WAEs, we recommend that you use one of the following methods to verify the PBR next-hop availability of a WAE. The method that you choose is based on the version of the Cisco IOS software that is running on the routers and the placement of your WAEs. However, method 2 is the preferred method whenever possible:

- **Method 1**—If the device sees the WAEs as a CDP neighbor (directly connected), it can use CDP and ICMP to verify that the WAE is operational. For more information, see the "Method 1: Using CDP to Verify Operability of WAEs" section on page 4-47.

- **Method 2 (Recommended method)**—If the device is running the Cisco IOS software Release 12.4 or later and the device does not see the WAE as a CDP neighbor, IP service level agreements (SLAs) can be used to verify that the WAE is operational using ICMP echoes. For more information, see the "Method 2: Using IP SLAs to Verify WAE Operability Using ICMP Echo Verification (Recommended Method)" section on page 4-48.
- **Method 3**—If the device is running the Cisco IOS software Release 12.4 or later and does not see the WAE as a CDP neighbor, IP SLAs can be used to verify that the WAE is operational using TCP connection attempts. For more information, see the "Method 3: Using IP SLAs to Verify WAE Operability Using TCP Connection Attempts" section on page 4-48.

Note In this section, the term device is used to refer to the router or switch that has been configured to use PBR to transparently redirect traffic to a WAE.

To verify whether the WAE is CDP visible to a device that has been configured to use PBR, enter the **show cdp neighbors** command on the device. If the WAE is CDP visible to the device, the WAE will be listed in the output of the **show cdp neighbors** command.

Method 1: Using CDP to Verify Operability of WAEs

If the device that is configured to use PBR views the WAEs as a CDP neighbor (the WAE is directly connected to the device), you can configure use CDP and ICMP to verify the availability of a WAE as a PBR next hop.

The following example shows how to use this method to verify PBR next-hop availability of a WAE. You must complete the following configuration process for each of the LAN and WAN route maps that are configured when CDP should be used.

To use CDP to verify operability of WAEs, follow these steps:

Step 1 On the router where PBR is configured (for example, on the branch office router named Edge-Router1), enter configuration mode and enable CDP on the router.

```
Edge-Router1(config)# cdp run
```

Step 2 Enable route-map configuration mode for the route map, WAAS-EGDE-LAN, which has already been created on the router.

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

Step 3 Configure the router to use CDP to verify the availability of the configured next-hop addresses.

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability
```

Step 4 Enable CDP on the WAE (for example, on the branch office WAE named Edge-WAE1) that you want the router to redirect traffic to using PBR.

```
Edge-WAE1(config)# cdp enable
```

If you are configuring PBR and have multiple WAEs and are using Method 1 to verify the PBR next-hop availability of a WAE, no additional configuration is necessary after you have completed the preceding process.

Method 2: Using IP SLAs to Verify WAE Operability Using ICMP Echo Verification (Recommended Method)

To use IP SLAs and ICMP (the recommended method) to verify PBR next-hop availability of a WAE, follow these steps:

Step 1 On the branch office router named Edge-Router1, enter the route-map configuration mode for the route map named WAAS-EDGE-LAN, which has been previously configured on this router.

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

Step 2 Configure the route map to use IP SLA tracking instance number 1 to verify the availability of the next-hop WAE (for example, the Edge WAE named Edge-WAE1 that has an IP address of 1.1.1.100).

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability 1.1.1.100 track 1
```

Note Enter the **set ip next-hop verify-availability** command for each route-map that has been configured on this branch office edge router and on the data center's core router that has also been configured to use PBR to redirect traffic to WAEs.

Step 3 Configure the IP SLA tracking instance 1.

```
Edge-Router1(config-route-map)# exit
Edge-Router1(config)# ip sla 1
Edge-Router1(config-ip-sla)#
```

Step 4 Configure the router to echo Edge-WAE1 using the specified source interface by using the **source interface** command.

```
Edge-Router1(config-ip-sla)# icmp-echo 1.1.1.100 source-interface FastEthernet 0/0.20
```

Step 5 Configure the router to perform the echo every 20 seconds.

```
Edge-Router1(config-ip-sla)# frequency 20
Edge-Router1(config-ip-sla)# exit
```

Step 6 Schedule the IP SLA tracking instance 1 to start immediately and to run continuously.

```
Edge-Router1(config)# ip sla schedule 1 life forever start-time now
```

Step 7 Configure the IP SLA tracking instance 1 to track the device, which is defined in the IP SLA tracking instance 1, by using the **track** command.

```
Edge-Router1(config)# track 1 rtr 1
```

If you are configuring PBR and have multiple WAEs, and you are using Method 2 to verify PBR next-hop availability of a WAE, you must configure a separate IP SLA per WAE and then run the **track** command per IP SLA.

Method 3: Using IP SLAs to Verify WAE Operability Using TCP Connection Attempts

If the device that is configured for PBR is running the Cisco IOS software Release 12.4 or later and does not see the WAE as a CDP neighbor, IP SLAs can be used to verify that the WAE is alive using TCP connection attempts. IP SLAs can be used to monitor a WAE's availability as the PBR next hop using TCP connection attempts at a fixed interval of 60 seconds.

To verify PBR next-hop availability of a WAE, follow these steps:

Step 1 On the branch office router named Edge-Router1, enter route-map configuration mode for the route map named WAAS-EDGE-LAN, which has been previously configured on this router.

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

Step 2 Configure the route map to use IP SLA tracking instance number 1 to verify the availability of next-hop WAE (the Edge WAE that has an IP address of 1.1.1.100).

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability 1.1.1.100 track 1
```

Note Enter the **set ip next-hop verify-availability** command for each route map that is configured on this branch office edge router and on the data center's core router that has also been configured to use PBR to transparently redirect traffic to WAEs.

Step 3 Configure the IP SLA tracking instance 1.

```
Edge-Router1(config-route-map)# exit
Edge-Router1(config)# ip sla 1
```

Step 4 Configure the router to use the specified source and destination ports to use TCP connection attempts at a fixed interval of 60 seconds to monitor the WAE availability by using the **tcp-connect** command.

```
Edge-Router1(config-ip-sla)# tcp-connect 1.1.1.100 80 source-port 51883 control disable
Edge-Router1(config-ip-sla)# exit
```

Step 5 Schedule the IP SLA tracking instance 1 to start immediately and to run forever.

```
Edge-Router1(config)# ip sla schedule 1 life forever start-time now
```

Step 6 Configure the IP SLA tracking instance 1 to track the device, which is defined in the IP SLA tracking instance 1, by using the **track** command.

```
Edge-Router1(config)# track 1 rtr 1
```

If you are configuring PBR and have multiple WAEs, and you are using Method 3 to verify PBR next-hop availability of a WAE, you must configure a separate IP SLA per WAE and then run the **track** command per IP SLA.

Request Redirection of CIFS Client Requests

In an IP-based branch office network, clients use the Common Internet File System (CIFS) protocol to request file and print services from networked servers.

The WAAS software supports three methods to redirect CIFS requests from clients to a WAE acting as an Edge WAE. An overview of each method is provided in the following sections:

- Using WCCP to Transparently Redirect CIFS Client Requests, page 4-50
- Using Explicit Naming of Shares to Explicitly Intercept CIFS Client Requests, page 4-50
- Using Microsoft DFS to Intercept CIFS Client Requests, page 4-51

Using WCCP to Transparently Redirect CIFS Client Requests

In an IP-based branch office network, clients use the CIFS protocol to request file and print services from networked servers. WAAS supports the use of WCCP Version 2 for the transparent interception of CIFS requests. This transparent interception of CIFS requests is based on the IP and TCP header information, and redirects them to WAEs that are acting as Edge WAEs.

The WAAS software supports the WCCP Version 2 service named the CIFS caching service (service 89). The CIFS caching service requires that WCCP Version 2 is running on the router and the Edge WAE. The WCCP CIFS caching service is a dynamic service. It intercepts all TCP traffic destined for ports 139 and 445 and redirects it to the corresponding redirect port (139 or 445). Load balancing distributes traffic based on the source IP address, by default. The WCCP-enabled router uses service ID 89 to access this service.

Note The WAAS software supports the TCP promiscuous mode service (WCCP Version 2 services 61 and 62). The TCP promiscuous mode service allows you to use WCCP Version 2 to transparently intercept and redirect all TCP traffic to an Edge WAE.

When you enable the TCP promiscuous mode service on a WAE and a router, you do not need to enable the CIFS caching service on the router or WAE. When the TCP promiscuous mode service is used, the CIFS caching service is not required.

Because this interception and redirection process is completely invisible or transparent to the client who is requesting the content, no desktop changes are required. The Edge WAE operation is transparent to the network; the WCCP-enabled router operates entirely in its normal role for nonredirected traffic.

When an Edge WAE operates in transparent mode, it does not publish the server name. CIFS clients use the branch office IT infrastructure to resolve a CIFS server name to an IP address (DNS, WINS). When a client connects to the file server, the router intercepts the TCP packets and redirects them to the WAE. The WAE extracts the original target server IP address and handles the request.

Client connections to CIFS servers that are not cached by the Edge WAE are supported. You can configure an accept or reject target IP list on the WCCP-enabled router. In this configuration, the router does not redirect packets to the Edge WAE but immediately forwards the packets to their destination.

If an WAE receives TCP packets destined to target servers that are not cached, it uses the WCCP packet return method to return the packets to the router for handling.

Note We recommend that accept or reject target IP lists be configured on routers in the branch offices where considerable CIFS traffic for noncached servers (either local servers residing on a different subnet or remote servers) is expected to be routed through the router. If you configure accept or reject target IP lists on routers in the central office, performance can be compromised when the WCCP packet return method is used because of excessive processing both at the router and in the cache.

Using Explicit Naming of Shares to Explicitly Intercept CIFS Client Requests

The distributed file system (DFS) from Microsoft provides an infrastructure to connect multiple file servers into one name space. Specifically, a file server can act as a DFS root, and other file servers can register as subdirectories in that root directory. For example, the main file server \\main-fs can have a root directory \\main-fs\engineering. Under that directory, a particular engineering group's file server \\eng1\ can be linked as \\main-fs\engineering\eng1.

If a client attempts to access a file in a subdirectory of \\main-fs\engineering\eng1 when request interception is being handled by Microsoft DFS, the following occurs:

1. The main file server (the DFS root server) sends a response to the client saying "this directory is not hosted here."
2. The client then sends a "Referrer-Request" message to the main file server asking "from where can I find this directory."
3. The main file server replies with \\eng1\.
4. The client connects to \\eng1\ and asks for the specified file.

The WAAS software supports the DFS infrastructure feature that allows multiple servers to be registered as the servers (also called replicas) for a directory, enabling load balancing and failover among the replica servers. When a client sends a "Referrer-Request" message for a directory that has multiple servers, the DFS root server gives the client a list of servers. The client typically chooses the first server on the list to contact. However, if the first server is not reachable, the client tries the second server and so on. By creating a number of lists where the first server on each list is a different replica server, and then providing those lists to clients, the DFS root server can load balance the replica servers.

The contents of the file servers in the network data center that need to be cached at branch offices are registered as subdirectories in a DFS root server. All branch office WAEs are configured as replica servers for those subdirectories at the DFS root server. When a client attempts access to a file in a subdirectory, the DFS root server (using the Active-Directory configuration) directs the client to the WAE at the same branch as the client. This redirection method is transparent to the client.

Using Microsoft DFS to Intercept CIFS Client Requests

Microsoft DFS can be used to intercept CIFS client requests in either Wide Area File Services (WAFS) transparent or non-transparent scenarios. The WAE can use name publishing or can rely on WCCP Version 2 to receive CIFS client requests.

When you use explicit naming of shares on your WAE, it is not transparent to the client. The client is explicitly told to access the branch WAE to access a file. Specifically, clients at branch A are told to mount a share from \\default-prefix-identifying-exported-file-server\file-server-name to access the file data. The WAAS software allows an administrator to define any name (not only a prefix) to represent the original file server. For example, users accessed their local file server, LFS1, before the file servers were grouped into the data center. After centralization, users can continue to use LFS1 even though the data has migrated to the central file server.

The branch office WAE uses both DNS and WINS and NetBIOS protocols to resolve \\WAE-at-the-branch to the IP address of the WAE. The resolution order depends on the client type. Windows 2000 and XP clients try first to resolve the address using DNS, then WINS, and then broadcast. Windows 98 resolves the address in the opposite order. To resolve the address using DNS, the WAE must be registered as \\WAE-at-the-branch in the DNS server at the enterprise. WAAS software supports only static DNS. To resolve the address using WINS and NetBIOS, during bootup the WAE registers itself as \\WAE-at-the-branch with the WINS server (which is preconfigured at the WAE). If the WINS server is absent and DNS is not available or the WAE is not registered in the DNS, the WAE answers the broadcast queries from the client. The broadcast method only works when the WAE is connected with an additional interface to the CIFS client subnet, or if non-transparent mode is used. A WAE failure requires clients to change their configuration to continue accessing the file data. Use the startup script for reconfiguration.