Cisco Wide Area Application Services (WAAS) Egress Methods

Simplifying Web Cache Communication Protocol Version 2 (WCCPv2) Deployment and Helping Ensure Network Path Affinity

Web Cache Communication Protocol Version 2 (WCCPv2) gives IT organizations a mechanism to transparently intercept and redirect network traffic to a nearby network device, such as a Cisco® Wide Area Application Engine (WAE) Appliances running Cisco Wide Area Application Services (WAAS) Software, for purposes of application acceleration and WAN optimization. By using WCCPv2 with Cisco WAAS and the Cisco WAE hardware platform, IT organizations can transparently optimize network flows for end users accessing files, applications, and other content over the WAN. The Cisco WAAS egress methods feature helps streamline and simplify WCCPv2 deployments, allowing Cisco WAEs to reside on the same subnet as users or servers and in the same address space. This feature also helps ensure that the original network path is preserved in the presence of WCCPv2 interception for Cisco WAAS. This document summarizes the egress methods available for Cisco WAAS deployment when using WCCPv2.

Overview

Cisco WAAS can be deployed using WCCPV2 as the traffic redirection method. WCCPv2 enables transparent off-path deployment of Cisco WAEs, providing high availability and load balancing. WCCPv2 is a protocol that allows devices such as the Cisco WAE to join service groups with network devices (such as routers or switches) for the purpose of injecting itself into the flow of application traffic to optimize or otherwise manipulate flows. When configured properly, the WCCPv2 process on the network device examines traffic to identify flows related to applications that match the criteria defined in the configured service groups. When this traffic is identified, the network device redirects the traffic to one of the registered service group devices, such as a Cisco WAE, using either a generic route encapsulation (GRE) tunnel or through frame header rewriting, called Layer 2 (L2) redirection. After the Cisco WAE has received packets, it can apply a function to the flow, such as local response handling, message suppression, compression, or other optimization. After the Cisco WAE applies these functions, it handles the optimized flow according to the configured egress method, which can be either IP forwarding, which causes the Cisco WAE to send the optimized packets to the configured default gateway, or negotiated return, which causes the Cisco WAE to return the optimized packets to the redirecting WCCPv2 device.

This document details the Cisco WAAS egress methods for WCCP interception modes and the configuration steps necessary to enable and configure WCCPv2 egress methods for intercepted traffic.

Cisco WAAS Support for Egress Method Configuration for WCCP Deployment

WCCPv2.0 provides means for negotiation of a redirect method and a return method. It allows a Cisco WAE to negotiate the egress methods of return traffic. This traffic can be either traffic that the Cisco WAE declines to service because of load or redirected packets that the Cisco WAE has processed. The method by which packets are returned to a router is negotiable.

In early Cisco WAAS releases, Cisco WAAS used IP forwarding as the only egress method, so that return traffic was sent to the configured default gateway. Although this is an efficient means of handling optimized traffic, it restricted Cisco WAAS deployments, requiring additional subnets in each location, and in some cases subverted the original routing path. This egress method (IP forwarding) remains a configurable option within Cisco WAAS.

Cisco WAAS Software Release 4.0.13 introduces flexibility when using WCCPv2 as the redirection method. It allows configuration of egress method that increases Cisco WAAS deployment alternatives in cases using WCCP iterception. From Cisco WAAS 4.0.13 onward, the WCCP negotiated return is also supported as the egress method. This method allows the Cisco WAE to be deployed on the same subnet as users or servers and provides better support for preservation of the routing path chosen by the network, because the optimized traffic is returned to the redirecting router. The negotiated return egress method also helps ensure compatibility with asymmetric routing, equal-cost multipath (ECMP) load-balancing, and Hot Standby Router Protocol (HSRP) environments. The return traffic egress method is negotiated based on the WCCPv2 configuration on the router and the egress method configuration on the Cisco WAE.

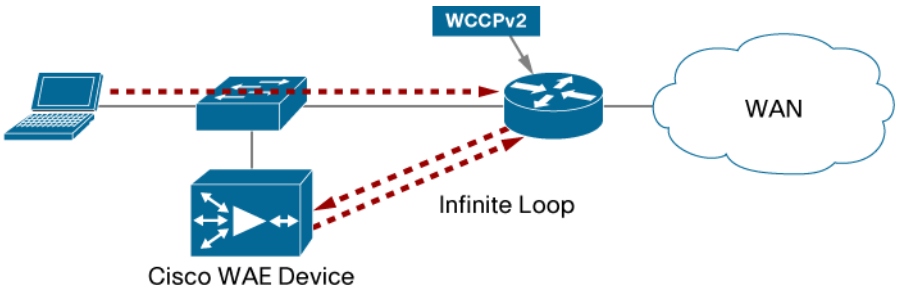
Cisco WAAS 4.0.13 allows configuration of the egress method for WCCP interception mode. WCCP interception mode supports two egress methods: IP forwarding and negotiated return. The negotiated return option currently supports WCCP GRE as the only WCCP egress method. If WCCP negotiates Layer 2 return, then the Cisco WAE defaults to IP forwarding as the egress method. Note that no notification will be received if the negotiated egress method defaults to IP forwarding; however, a syslog message will be generated if such a case occurs.

IP Forwarding Egress Method and Supported Cisco WAE Deployment Scenarios

When the IP forwarding egress method is used, the return traffic packets are forwarded to the Cisco WAE default gateway. IP forwarding is the default egress method Cisco WAE uses to return redirected traffic, and it is part of the Cisco WAE default configuration. With the IP forwarding egress method, the Cisco WAE must be deployed on a separate subnet from users and servers, which can be accomplished using subinterfaces or tertiary interfaces (Figure 1). The command-line interface (CLI) command to configure IP forwarding as the egress method is shown here:

```
WAE(config)# egress-method ip-forwarding intercept-method wccp
```

Figure 1. Limitation of IP Forwarding: Cisco WAE Must Reside on a Separate Subnet to Prevent Infinite Forwarding Loop



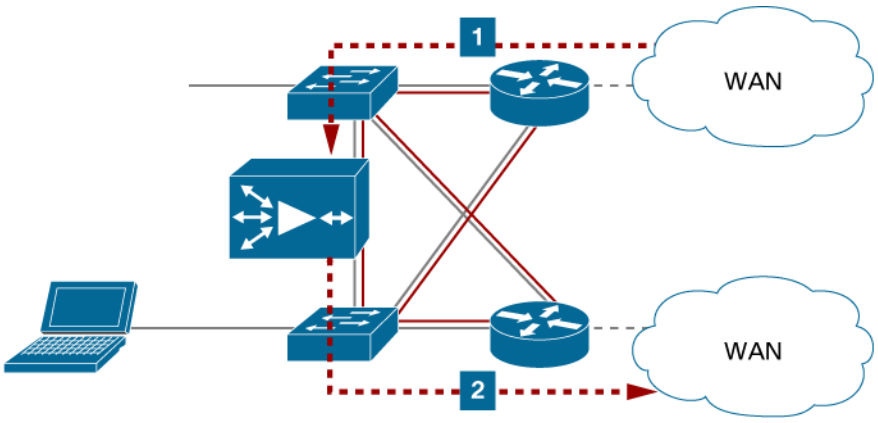
When using the GRE egress method, the return traffic packets are returned back to the intercepting router using the GRE tunnel that is created as a result of WCCP negotiation. With the GRE return egress method, the Cisco WAE can be deployed on the same subnet as users or servers, and subinterfaces or tertiary interfaces are not required (Figure 2). The CLI command to configure GRE return as the egress method is shown here:

```
WAE(config)# egress-method negotiated-return intercept-method wccp
```

When using GRE encapsulation for WCCP redirection, the router uses the router ID IP address as its source IP address. The router ID IP address is the highest loopback address on the router, or if the loopback interface is not configured, the router ID IP address is the highest address of the physical interfaces. The router ID IP address is used as the source address for packets redirected from the router to the Cisco WAE, and as a result it is also used as the destination address for traffic from the Cisco WAE to the router, Therefore, you must be sure that a route exists from the Cisco WAE to the router. This is done by configuring a static route on the Cisco WAE to the router ID IP address. The router ID can be identified with the command **show wccp routers** on the Cisco WAE. If the WCCP server group contains multiple routers, a static route should be added to each of these router's router ID. The command to configure such static routes is:

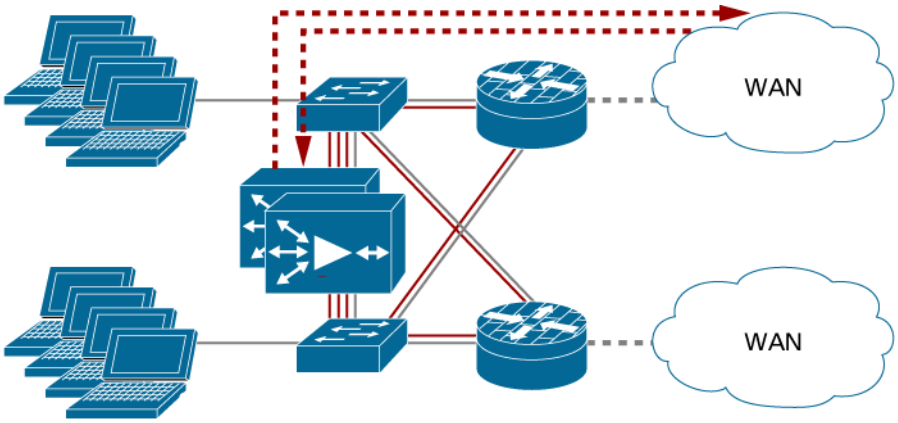
```
WAE(config)# ip route <Router ID> <netmask> <gateway's ip>
```

Figure 2. Limitation of IP Forwarding: Traffic Is Redirected to the Cisco WAE in the GRE Tunnel (1), but Traffic Leaves the Cisco WAE Destined for Its Default Gateway (2)



When router load balancing is used in the network, Cisco WAAS makes a best effort to maintain the original router selection. When the Cisco WAE applies data redundancy elimination (DRE) and compression to a TCP flow, the number of packets may be reduced. A single packet carrying optimized data may represent original data received in multiple packets redirected from different routers. That optimized data packet will egress from the Cisco WAE to the router that had last redirected a packet to the Cisco WAE for that flow direction. Likewise, the Cisco WAE can receive optimized data over multiple packets from different routers. The Cisco WAE will expand the optimized data into original data that will go out as several packets. Those original data-carrying packets will egress from the Cisco WAE to the router that last redirected a packet to the Cisco WAE for that flow direction. Pass-through flows will always follow the original router selection (Figure 3).

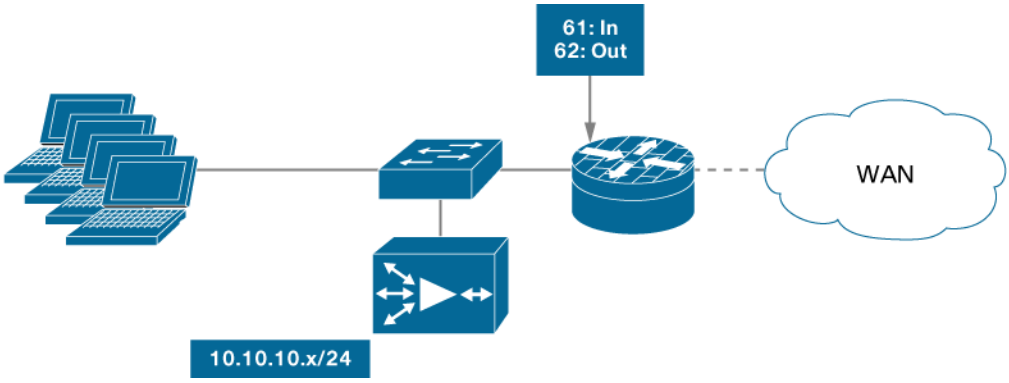
Figure 3. GRE Return Egress Method Supports Asymmetric Routing Deployments



Configuration Example

Figure 4 provides a visual representation of the configuration example that follows. The Cisco WAE resides on the same subnet as the clients.

Figure 4. Configuration Example for Cisco WAAS Deployment with the GRE Egress Method



The configuration commands for this example are shown here. Remember that Cisco WAAS requires that interception be configured on both ends of the network. This example shows interception in only one location. For more detailed information about how WCCPv2 works and about verification tasks when working with Cisco WAAS and the Cisco WAE, please refer to the document “Using WCCPv2 for Interception and Redirection with Cisco Wide Area Application Services 4.0.”

Router Configuration

!	
version 12.4	
!	
hostname Router	Enable the TCP promiscuous service groups (61 and 62) using these commands.
!	
!	
ip wccp 61	IP Cisco Address Forwarding (CEF) is recommended to improve performance and minimize router resource utilization.
ip wccp 62	
!	
ip cef	This interface is attached to the client and Cisco WAE LAN. Interface speed and duplex are defined.
!	
ip domain name yourdomain.com	Redirect all TCP traffic received on this interface to a Cisco WAE device that is registered in service groups 61 and 62.
!	
!	
interface FastEthernet0/0	
description “To Local Area Network”	
ip address 10.10.10.1 255.255.255.0	This interface is connected to the WAN.
ip wccp 61 redirect in	
ip wccp 62 redirect out	
bandwidth 100	
full-duplex	
!	
!	
!	
interface Serial0	
description “To Wide Area Network”	
ip address 172.16.223.12 255.255.255.0	
!	
end	

Cisco WAE Configuration

! WAAS version 4.0.13 ! device mode application-accelerator ! hostname WAE ! clock timezone PST -8 0 ip domain-name peap.local ! primary-interface GigabitEthernet 1/0 ! !	
interface GigabitEthernet 1/0 ip address 10.10.10.250 255.255.255.0 no autosense bandwidth 100 full-duplex exit interface GigabitEthernet 2/0 shutdown exit	This interface is connected to the LAN and is adjacent to the clients. The Cisco WAE is on the same VLAN and subnet as the users.
! ip default-gateway 10.10.10.1	The Cisco WAE uses the router IP address as its default gateway.
! ! ip route 192.168.10.1 255.255.255.255 10.1.1.1 ip route 192.168.10.11 255.255.255.255 10.1.2.1	The static routes to the router ID of the intercepting routers is configured here. The router ID is used as the destination address for egress traffic using the WCCP GRE return method.
! !ip name-server 10.10.10.100 ! wccp router-list 1 10.10.1.1 wccp tcp-promiscuous router-list-num 1 wccp version 2	The WCCPv2 router list is configured here, including the adjacent router. The Cisco WAE is instructed to join service groups 61 and 62 (TCP-promiscuous) with each router in the router list. Note that WCCP Version 2 is specified.
! egress-method negotiated-return intercept-method wccp	Set negotiated-return as the egress method. With this specification, the Cisco WAE will use GRE to return redirected traffic to the intercepting router. Note: In this case, WCCP negotiated WCCP GRE as the return method.
! central-manager address 10.10.10.10 cms enable ! policy-engine application	

Determine Router ID of Intercepting Routers

To determine the router Id IP address of the intercepting routers that should be used for the static routes configuration on a particular Cisco WAE, use the show wccp routers Exec command.

View show wccp routers on Cisco WAE

WAE#sh wccp routers Router Information for Service: TCP Promiscuous 61 Routers Configured and Seeing this File Engine(1) Router Id Sent To Recv ID 192.168.10.1 10.1.1.1 0009B9A6 192.168.10.11 10.1.2.1 0009B942 Routers not Seeing this File Engine -NONE- Routers Notified of but not Configured -NONE- Multicast Addresses Configured -NONE- Router Information for Service: TCP Promiscuous 62 Routers Configured and Seeing this File Engine(1) Router Id Sent To Recv ID 192.168.10.1 10.1.1.1 0009B9A6 192.168.10.11 10.1.2.1 0009B942 Routers not Seeing this File Engine -NONE- Routers Notified of but not Configured -NONE- Multicast Addresses Configured -NONE-	The “sh wccp routers” command will display routers seen and not seen by this WAE. For WCCP intercept method service groups 61 and 62, egress method configured is negotiated return. The actual method used is WCCP GRE.

View Configured and Actual Egress Methods for a Particular Cisco WAE

To view the egress method that is configured and that is being used on a particular Cisco WAE, use the show egress methods EXEC command.

View Egress Method on Cisco WAE

methods Intercept method : WCCP TCP Promiscuous 61 : WCCP negotiated return method : WCCP GRE Egress Method Egress Method Destination Configured Used ---------- ---------- ---------- any WCCP Negotiated Return WCCP GRE TCP Promiscuous 62 : WCCP negotiated return method : WCCP GRE Egress Method Egress Method Destination Configured Used ---------- ---------- ---------- any WCCP Negotiated Return WCCP GRE Intercept method : Generic L2 Egress Method Egress Method Destination Configured Used ---------- ---------- ---------- any not configurable IP Forwarding	The "sh egress-methods" command will display a summary of egress methods per intercept method, as well as the actual method used. For WCCP intercept method service groups 61 and 62, the egress method configured is negotiated return. The actual method used is WCCP GRE.

Summary

WCCPv2 is a powerful network interception and redirection protocol that enables IT organizations to deploy Cisco WAAS. Cisco WAAS 4.0.13 enables the use of different egress methods for WCCP interception to provide additional deployment flexibility and better support for network path affinity. As of this release, the WCCP interception can be deployed in conjunction with two egress methods, IP forwarding and negotiated return, therefore enabling additional deployment flexibility and support for asymmetric routing deployments. IT organizations can deploy Cisco WAAS to centralize costly remote-office infrastructure, minimize bandwidth consumption, and improve user productivity in a transparent manner while providing high availability, scalability, and load balancing.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-433922-01 12/07

