WCCP Network Integration with Cisco Catalyst 6500: Best Practice Recommendations for Successful Deployments

What You Will Learn

This document is intended for network engineers deploying the Cisco Catalyst 6500 using the Web Cache Coordination Protocol (WCCP)[1] to deliver network-based services, including:

- Wide area application acceleration
- Web content caching
- Web security services

This paper includes detailed recommendations for deploying WCCP on the Cisco Catalyst 6500. These recommendations make sure of a robust and scalable deployment that takes full advantage of the hardware accelerated switching available in the Cisco Catalyst 6500.

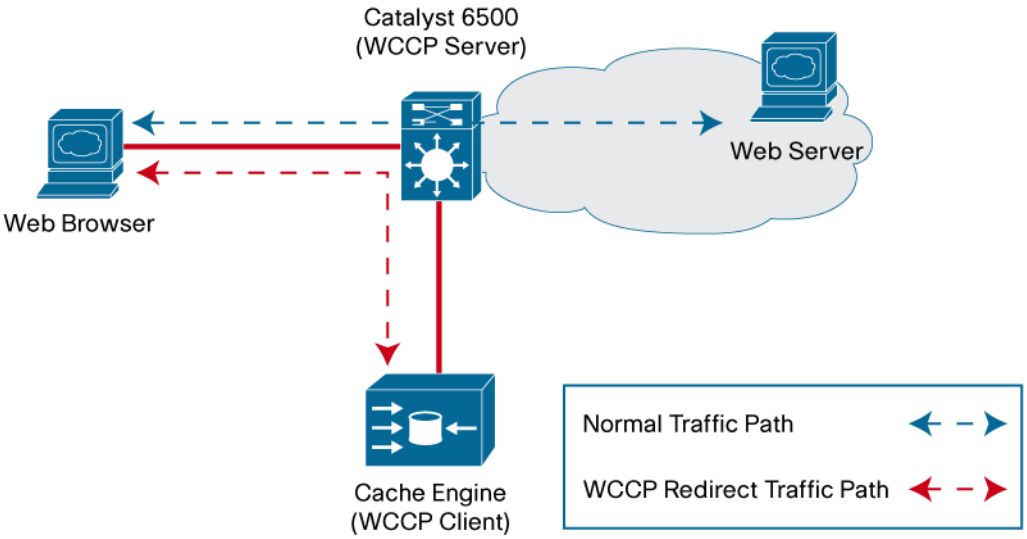
Introduction

WCCP v2[2] specifies interactions between one or more WCCP servers and one or more WCCP clients. The WCCP server role can be performed by a Cisco Catalyst 6500 or some other intelligent router device; the WCCP client could be a content caching engine or some other service delivering appliance. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic flowing through a router or group of routers. The selected traffic is redirected to a cache engine or group of caches with the aim of providing some kind of service such as optimizing network resource usage, lowering response times, improving security and so on.

Figure 1 is a high-level example of a web-cache service being performed using WCCP. The WCCP server in this case is the Cisco Catalyst 6500, where it is filtering traffic for redirection to the WCCP client, a content caching engine. The normal traffic path indicates how HTTP-based content requests would normally flow from the hosts toward the web servers. The Cisco Catalyst 6500 is redirecting the web traffic to the content caching engine, if the content caching engine is capable of servicing the request it will respond with the information and the host will never realize the difference. The result is faster response times for the host with less traffic toward the upper layer network infrastructure; in most cases this would also reduce traffic on the more expensive WAN links. In Figure 1, WCCP traffic redirection is being performed on the Cisco Catalyst 6500. Traffic destined for the web server is redirected by the Cisco Catalyst 6500 to the cache engine.

[1] WCCP is also commonly referred to as the Web Cache Control Protocol.
[2] WCCP v2 was written by Cisco employees Marty Cieslak, Dave Forster, Rob Wilson, and Gurumukh Tiwana and published as an internet draft in July 2000.

Figure 1. WCCP Traffic Redirection



From a configuration standpoint the WCCP service requires a coordinated configuration on both the routers and cache engines. The WCCP protocol is used by the server and clients to coordinate service configuration options and make the WCCP service operational. One important point of the configuration process is that the WCCP server and WCCP clients negotiate capabilities for the service. For example, traffic forwarding methods and traffic distribution methods are configured at the router and cache engine individually; the router then uses the WCCP to advertise its supported capabilities, and the cache engines use a WCCP message to acknowledge and indicate which methods they can support. Finally, not all configuration options are available on all devices. A cache engine might not support a certain traffic redirection method, for example.

WCCP on the Cisco Catalyst 6500

The Cisco Catalyst 6500 is designed for hardware-based switching and forwarding, classifying traffic based on Layer 2–4 criteria. The specialized ASICs in the Cisco Catalyst 6500 are capable of switching millions of packets per second. However, traffic that is switched via the hardware forwarding path must meet certain criteria. Traffic that cannot be classified and switched by the hardware will be forwarded using either a full software path or combination software/hardware-based forwarding path.

Some amount of software-based forwarding is inevitable and is perfectly acceptable as long as the traffic does not oversubscribe the software-based forwarding capacity. The Cisco Catalyst 6500 software-based forwarding performance varies between tens of thousands of packets per second to hundreds of thousands of packets per second depending upon the specific traffic type and contents. Control protocols such as spanning tree BPDUs, routing protocol packets, Internet Control Message Protocol packets, and other types of control traffic are examples of the traffic exceptions that are forwarded and processed in software.

When designing a WCCP service with the Cisco Catalyst 6500, it is important to use the hardware-based forwarding path whenever possible. Bear in mind that the Cisco IOS® Software running on the Cisco Catalyst 6500 supports many different options and features related to WCCP, also that the Cisco IOS Software is built to run on multiple switch and router platforms providing a common infrastructure and feature set. However, not all of the WCCP features are supported in hardware on the Cisco Catalyst 6500; therefore, it is important to manage the configuration to use the hardware accelerated forwarding. This means configuring certain specific options for the WCCP service. Table 1 provides a list of the primary recommendations that support hardware-based forwarding.

Table 1. Best Practice Configuration Options for Cisco Catalyst 6500

WCCP Configuration Option	Best Practice Recommendation
Traffic interception direction	Ingress
Redirection transport method	WCCP-GRE or Layer 2
Assignment method	Mask-based
Return traffic transport method	Generic GRE or Layer 2

The remainder of this document will discuss the hardware accelerated configuration options for WCCP in more detail.

Cisco Catalyst 6500 Hardware and Software Recommendations

The currently shipping supervisor and line-card modules are all capable of providing WCCP services. The following hardware and software are recommended with WCCP services enabled:

- WS-SUP720-3B/3BXL
- WS-SUP720-10G-3C/3CXL
- WS-SUP32-3B
- All supported Ethernet LAN/WAN modules
- Distributed forwarding cards are optional
- Cisco IOS Software Release 12.2(33)SXH4 or newer
- Cisco IOS Software Release 12.2(33)SXI or newer

WCCP Client Registration

The WCCP client registration is initiated by the WCCP client with a “here I am” (HIA) message. The WCCP client sends the HIA messages to either the configured router’s IP address or a multicast group address. The router or WCCP server replies with an “I see you” (ISU) message. HIA messages are typically sent every 10 seconds, although the WAAS sends them every 2 seconds.

The WCCP HIA and ISU messages are also used to advertise optional capabilities and acknowledge two-way communication between the WCCP server and client.

Best Practice Recommendations for Client Registration

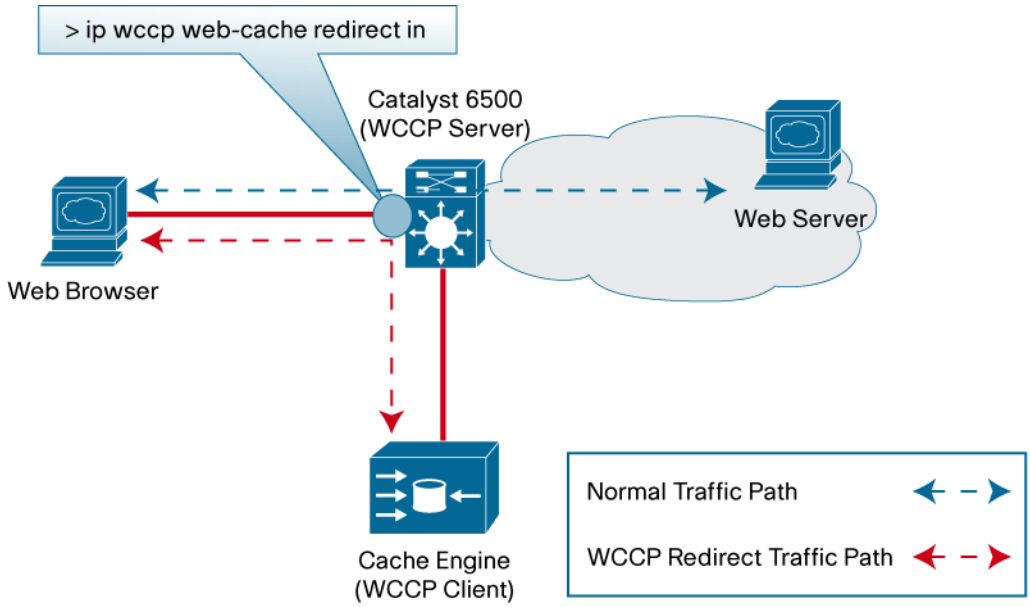
- Use WCCP version 2 only
- Register to local a VLAN IP address if the WCCP client is Layer 2 adjacent
- Register to the highest loopback address if the engine is not Layer 2 adjacent
- Do not register to a virtual address created using HSRP, GLBP, VRRP, and so on
- Limit MTU size to 1500 bytes or less on WCCP client interfaces

Intercept Method

Traffic interception direction or the “intercept method” describes the direction in which traffic will be intercepted for the WCCP service. The WCCP configuration allows for traffic to be intercepted on ingress or on egress. The service is applied from the router’s perspective as it processes the request and response between the end host and the destination server.

Figure 2 depicts WCCP ingress interception service.

Figure 2. WCCP Ingress Interception Service



- **Use ingress redirection.** The Cisco Catalyst 6500 supports hardware-based traffic redirection options only when applied to traffic as it enters the switch.
- **Do not use egress redirection.** Egress redirection is supported but not recommended. If a WCCP service is configured as an egress feature, traffic will be forwarded in software.

Assignment Method

The assignment method determines how traffic will be distributed among multiple WCCP clients in a given service group. There are two assignment methods available, hash-based and mask-based. The assignment method chosen for a given service-group is negotiated between the router and the WCCP clients.

There are two primary recommendations for the assignment method on a Cisco Catalyst 6500:

- **Use mask assignment.**

  The combination of an ingress traffic intercept method with mask-based assignment provides a full hardware-based traffic assignment method. Traffic is filtered for WCCP redirection using an Access Control List. The WCCP mask value is then applied to the redirect ACL to create entries in the Cisco Catalyst 6500 ACL TCAM[3]. The TCAM entries are used to provide hardware accelerated lookups and to derive a specific WCCP client which will service the traffic flow. In this way the forwarding path is performed completely in the Cisco Catalyst 6500 hardware resources. The actual mask itself is configured at the cache engine and is communicated to the router via WCCP. The negotiation of the assignment method is performed between the router and the clients via the WCCPv2 ISU and WCCPv2 HIA messages, respectively. The Cisco Catalyst 6500 supports both the hash-based and mask-based assignment methods and will advertise these capabilities in its ISU messages. The WCCP client must be configured for mask-based assignment and then implicitly choose the mask-based assignment method by first observing the supported method in the router's ISU message and then advertising mask-based assignment in its subsequent HIA messages. The hash-based assignment method is the default and will be chosen unless the client is configured to support the mask-based assignment method.

[3] TCAM or Ternary Content Addressable Memory is hardware-based high-speed memory store capable of performing binary bit comparisons matching a value of 1, 0 or “X” where “X” can be either a 1 or 0.

Hash-based assignment method is supported but not recommended on the Cisco Catalyst 6500. A hash-based assignment method will utilize a combination of software and hardware forwarding resources. Traffic flows will need to be forwarded via software initially while also setting up flow entries using the Cisco Catalyst 6500 Netflow resources. This approach is certainly viable for some deployments but is not the best practice solution for the Cisco Catalyst 6500.

- **Minimize the number of mask bits when using WCCP redirect ACL.**

  The Cisco Catalyst 6500 has a finite number of ACL TCAM entries (Table 2). If the TCAM resources are exceeded, the Cisco Catalyst 6500 will revert to software-based forwarding for any traffic that meets the ACL criteria. Of course software-based forwarding can lead to higher CPU utilization and as a best practice this is to be avoided. The Cisco Catalyst 6500 supervisor module provides two ACL TCAM resources: one is dedicated for security ACLs, and the other is dedicated for quality of service ACLs. The WCCP redirect ACL will consume entries from the security ACL TCAM. Each TCAM can support up to 32k entries.

Table 2. Cisco Catalyst 6500 ACL TCAM Entries

Supervisor Model	Security ACL Entries	QoS ACL Entries
Supervisor 720 -3B/XL	32K	32K
Supervisor 32-3B/XL	32K	32K
Supervisor 720-10G-3C/XL	32K	32K

The numbers of mask bits used in conjunction with the number of permit statements in the redirect ACL are directly related to the number of security ACL TCAM entries used. Using fewer mask bits will correspond to fewer ACL TCAM entries being used. (See Table 3.)

Table 3. Examples for Effective TCAM Utilization When Using WCCP Mask Assignment

Number of WCCP Clients	Example: WCCP Mask	Number of Mask Bits Used
1-2	0x1	1
3-4	0x3	2
5-8	0x7	3

Keep in mind that the security ACL TCAM resources are used across multiple features in the Cisco Catalyst 6500.

It is recommended to verify the available TCAM resources prior to deploying the WCCP service and if possible predict the amount of TCAM resources that will be consumed by the service.

The CLI command `show platform hardware capacity acl` provides a summary of the ACL TCAM utilization.

Figure 3 shows the output from a show platform hardware capacity ACL with minimal TCAM ACL utilization of 1 percent.

Figure 3. Sample Output

```
SW1#show platform hardware capacity ACL
ACL/QoS TCAM Resources
  Key: ACLent - ACL TCAM entries, ACLmsk - ACL TCAM masks, AND - ANDOR,
       QoSent - QoS TCAM entries, QOSmsk - QoS TCAM masks, OR - ORAND,
       Lbl-in - ingress label, Lbl-eg - egress label, LOUsrc - LOU source,
       LOUdst - LOU destination, ADJ - ACL adjacency

  Module ACLent ACLmsk QoSent QoSmsk Lbl-in Lbl-eg LOUsrc LOUdst  AND  OR  ADJ
  1          1%     2%     1%     1%     1%     1%     0%     0%   0%   0%   1%
  2          1%     2%     1%     1%     1%     1%     0%     0%   0%   0%   1%
SW1#
```

Use the following formula to predict the amount of TCAM resources required for a specific mask and redirect ACL combination:

The number of entries created in the TCAM will be a product of the following:

r redirection and processing by the WCCP client. The following ACL is a typical example of a redirect ACL used to permit redirection of web and file services only. Note that an ACL to include specific ports will not capture TCP fragments, so make sure that fragmentation is not commonly done.

```
ip access-list extended waas
remark WAAS WCCP Redirect List
permit tcp any any eq 80
permit tcp any any eq 8080
permit tcp any any eq 139
permit tcp any any eq 445
permit tcp any eq 80 any
permit tcp any eq 8080 any
permit tcp any eq 139 any
permit tcp any eq 445 any
deny tcp any any
```

- Redirect ACL restrictions: The following restrictions apply to the redirect-list ACL:
  - Permit statements in the redirect ACL will consume more security TCAM entries compared to deny statements, be sure the TCAM does not become oversubscribed.
  - Sup720 with PFC 3B/3C and Sup32 with PFC 3B do not have hardware controls to catch IP options. All IP options packets are punted to software by default by the common hardware forwarding logic.
  - The ACL must be an IPV4 simple or extended ACL.
  - The protocol must be IP, UDP, or TCP. In case a UDP ACE is used with TCP promiscuous service group (61, 62 – used for WAAS), this ACE will result in punting packets to RP for processing. Similarly a TCP ACE if used with UDP-based service group will result in punting traffic to RP for processing. The system will not log any error message for such combinations. Refer to defect CSCsz78401 for more details.
  - Only individual source or destination port numbers may be specified; port ranges cannot be specified.
  - The only valid matching criterion besides individual source or destination port numbers is DSCP or ToS.
  - The use of fragments, time range, options ,or any TCP flags is not permitted.
  - The show ip access-list command for the redirect ACL will not show the correct counter matches.
  - If the redirect ACL does not meet the above restrictions, the system will log the following error message: WCCP-3-BADACE: Service <service group>, invalid access-list entry (seq:<sequence>, reason:<reason>).

Note: If these restrictions are not followed, WCCP continues to redirect packets, but the redirection is carried out in software (Netflow switching) until the access list is adjusted.

Return

The return method refers to the transport method used by the WCCP clients to return traffic that has been successfully serviced back to the originally requesting host device. For the Cisco Catalyst 6500 the preferred method is the L2 return method since this method is fully supported in hardware; this of course requires a topology where the WCCP clients are L2 connected to the Cisco Catalyst 6500.

For topologies where the WCCP clients are not directly connected via L2, the alternative is to use GRE tunnels to forward the response back to the Cisco Catalyst 6500, which can then deencapsulate the packet and forward it to the original requesting host.

- Cisco Catalyst 6500 WCCP L2 return is supported from Cisco IOS Software 12.2(33) SXH.
- Cisco Catalyst 6500 WCCP GRE return is handled in software.

Egress Method

Some WCCP clients, such as a Cisco WAE, use the terminology egress method to describe traffic that has been successfully serviced by the WAE. The WCCP client may support a number of different egress transport method options including:

- **IP Forward:** Traffic is simply sent back using the original source and destination IP addresses. The Cisco Catalyst 6500 supports this method in hardware.
- **WCCP GRE:** Traffic is sent back to the WCCP server encapsulated within a WCCP and a GRE header similar to the WCCP GRE return traffic method. Again, the Cisco Catalyst 6500 supports this transport method in software only.
- **Generic GRE:** Traffic is sent back using a GRE header only. The Cisco Catalyst 6500 supports this method in hardware. The generic GRE egress method is supported only when the WCCP GRE interception method is used.

Because the Cisco Catalyst 6500 does not support WCCP GRE return in hardware, the recommended return methods are either generic GRE return or IP forwarding.

- Use IP forwarding return when there is no cross data center asymmetric routing or need to return the traffic to the same router it came from.
- Use generic GRE return when there is cross data center asymmetric routing or a need to return traffic to the same router it came from.
- For generic GRE return, implement a WCCP client static /32 route to the WCCP router ID or GRE loopback address for optimal return.
- For generic GRE return, implement a point to multipoint GRE tunnel on the Cisco Catalyst 6500 (see below details).

WCCP Client Connect

The following best practices are recommended for connecting a WCCP client to WCCP server:

- For a single WCCP server (router) to a single WCCP client configuration, use and etherchannel if it is supported by the client.
- For a pair of redundant WCCP servers with an SVI between them, connect the WCCP clients using standby NIC teaming for N+1 availability. Implement Multigroup Hot Standby Redundancy Protocol on the WAE client subnet to load balance WAE IP forwarded return traffic.
- For a pair of redundant WCCP servers with a routed link between them, connect the WCCP clients using etherchannel for N:N availability.
- For Layer 2 redirect configurations use a dedicated subnet for WCCP clients.

Service Group Use

The following best practices are recommended for service group usage:

For WAAS, use service group 61 to redirect traffic inbound from the client and use service group 62 to redirect traffic inbound from the server. Service group 61 does the load balancing on the source IP address, whereas service group 62 does the load balancing on the destination IP address. Always use service group 61 from the client and service group 62 from the server. In other words, at the remote sites, use service group 61 on the LAN side and service group 62 on the WAN side. For the data center, reverse the orientation with service group 61 on the WAN side and service group 62 on the LAN. This would mean the WCCP load balancing at both the data center and the remote sites would be based on the client IP's addresses.

WCCP Operational Best Practices

The following operational best practices are recommended while configuring/modifying the WCCP.

Router Initial Configuration

1. Create WCCP redirect ACL
2. Configure global IP WCCP # redirect-list
3. Enable WCCP service IDs with redirect-list ACL

For changes made to an existing configuration:

- Global service group configuration changes

1. Unregister all affected WCCP clients with no WCCP version 2
2. Remove interface config
3. Remove/change global config
4. Apply new global config
5. Apply new interface config
6. Re-register WCCP clients
   - Interface Configuration Changes—Leave WAE WCCP clients registered
   - Redirect-list Changes—Leave WAE WCCP clients registered

WAE Add or Replacement Procedure

1. Disable WCCP on all the WAEs. By default WCCP will wait for 180 seconds for the existing TCP sessions to close by the end hosts.
2. Disable WCCP globally using ‘no ip wccp 61/62’ on all the routers that are part of WCCP farm.
3. Remove the failed WAE from the network.
4. Add the new WAE and enabled WCCP version 2 on all WAEs in the WCCP farm.
5. After all WAEs are enabled for WCCP then enable WCCP globally for WCCP service group (61 and 62 for WAAS).

Caveats and Considerations

The following caveats and considerations apply to WCCPv2:

- For routers servicing a multicast cluster, the Time To Live (TTL) value must be set at 15 or fewer.
- Service groups can comprise up to 32 content engines and 32 routers.

- Because the CE routers (for example, WAAS and ACNS) currently do not support the use of jumbo Ethernet frames, the IP MTU size on an interface should not be increased above the Ethernet default value.

The following limitations apply to WCCP Layer 2 forwarding and return:

- Layer 2 redirection requires that the WCCP client be Layer 2 adjacent to an interface on each WCCP router. Unless multicast IP addresses are used, WCCP configuration of the content engine must reference the directly connected interface IP address of the WCCP router and not a loopback IP address or any other IP address configured on the WCCP router.

Cisco Catalyst 6500 WCCP Performance Examples

Cisco's network integration test teams have performed comparative test scenarios verifying the functionality and performance of WCCP on the Cisco Catalyst 6500 as well as other platforms. Included here are a few examples that highlight performance metrics including the lower CPU utilization when using a fully hardware accelerated configuration based on these best practice design recommendations.

The first comparison uses GRE redirection and return methods with a generic GRE egress method. This type of configuration would allow for WCCP clients to be connected across multiple L3 hops if so desired.

Figure 4 provides a high-level network diagram that shows the primary difference between the two scenarios which is the direction in which the services are applied. In configuration 1/scenario 1 both WCCP service 61 and service 62 are applied to the same interface. The WCCP 61 service is applied on ingress traffic and WCCP 62 service is applied on egress traffic. The WCCP 62 service being applied on egress will cause traffic to be software switched. Again the Cisco Catalyst 6500 can only hardware accelerate the traffic applied to the ingress direction. (See Table 5.)

Figure 4. Configuration 1/Scenario 1 Network Diagram Comparison to the Recommended Configuration

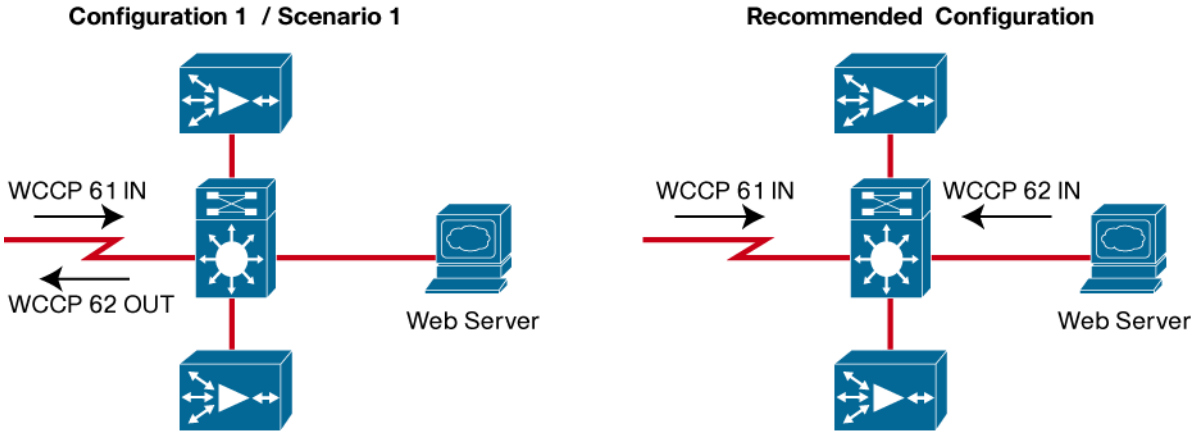


Table 4. Configuration 1/Scenario 1 Comparison

Configuration 1	Scenario 1	Recommended Configuration
Service	**61 Ingress/62 Egress**	**61 Ingress/62 Ingress**
Assignment Method	Mask	Mask
Redirection	GRE	GRE
Egress Method	Generic GRE	Generic GRE
Return Method	GRE	GRE
CPU % (5 Min. Avg.)		
415 CPS	CPU – 50%	CPU < 6%
675 CPS	CPU – 80%	CPU < 6%
745 CPS	CPU – 90%	CPU <6%

CPS= Connections Per Second

In configuration 1/scenario 2 the service directions are both applied in the ingress direction; however, the default hash-based assignment method is configured. This will force the Cisco Catalyst 6500 to implement a partial software/hardware forwarding implementation, which uses the Netflow resources. (See Figure 5 and Table 6.)

Figure 5. Configuration 1/Scenario 2 Network Diagram Comparison to Recommended Configuration

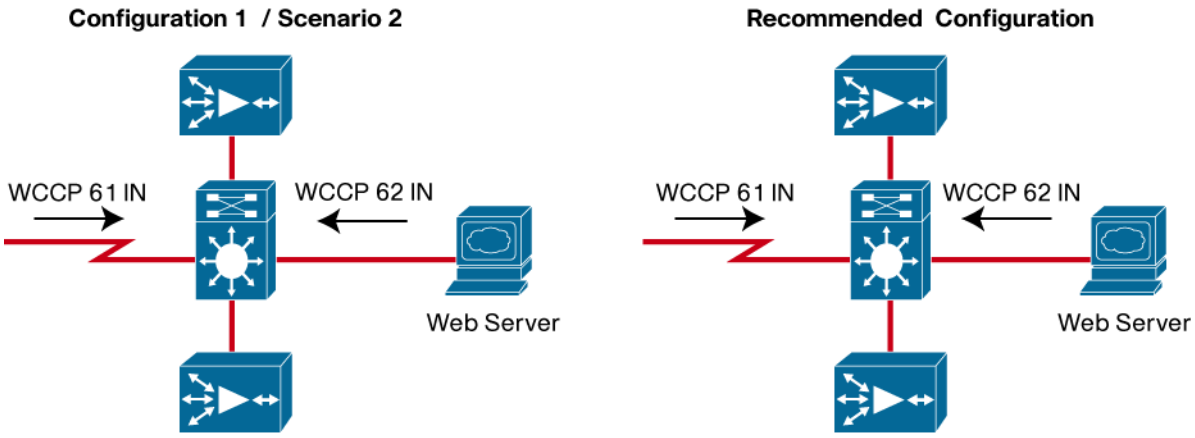


Table 5. Configuration 1/Scenario 2 Comparison

Configuration 1	Scenario 2	Recommended Configuration
Service	**61 Ingress/62 Ingress**	**61 Ingress/62 Ingress**
Assignment Method	**Hash**	**Mask**
Redirection	GRE	GRE
Egress Method	Generic GRE	Generic GRE
Return Method	GRE	GRE
CPU % (5 Min. Avg.)		
475 CPS	CPU – 50%	CPU < 6%
675 CPS	CPU – 80%	CPU < 6%
750 CPS	CPU – 90%	CPU < 6%

CPS= Connections Per Second

Configuration number 2 uses Layer 2 redirection available with the Sup720 PFC3B and PFC3C-based system as well as the SUP32 PFC3B systems. In configuration 2/scenario 1 the WCCP services are applied on the same interface in both an ingress and egress direction. Once again software forwarding will occur for the egress service; the CPU effect is reflected in Table 7 versus the recommended configuration. The Layer 2 redirection design is recommended when the WCCP clients can be connected Layer 2 adjacent to the traffic being redirected. (See Figure 6.)

Figure 6. Configuration 2/Scenario 1 Network Diagram Comparison to Recommended Configuration

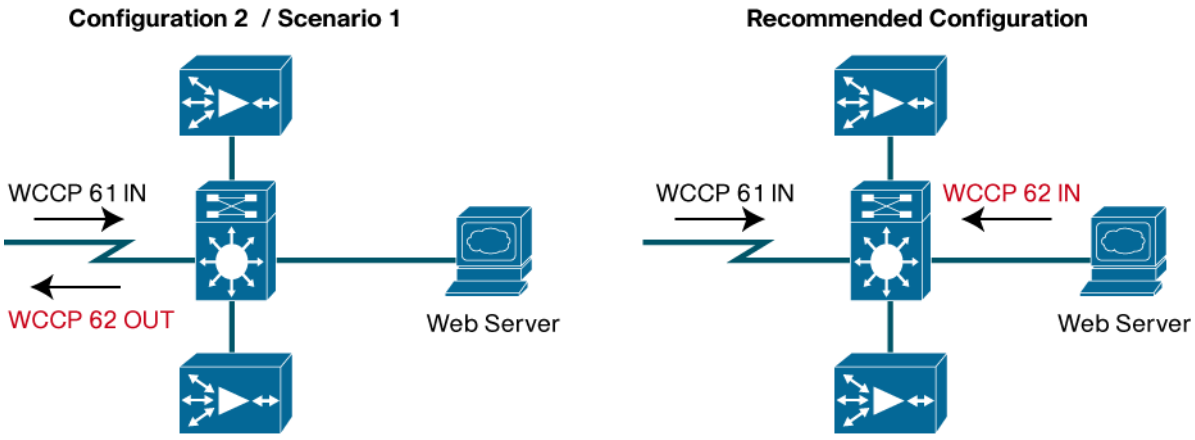


Table 6. Configuration 2/Scenario 1 Comparison

Configuration 2	Scenario 1	Recommended Configuration
Service	**61 Ingress/62 Egress**	**61 Ingress/62 Ingress**
Assignment Method	Mask	Mask
Redirection	L2	L2
Egress Method	IP Forwarding	IP Forwarding
Return Method	L2	L2
CPU % (5 Min. Avg.)		
475 CPS	CPU – 50%	CPU < 6%
675 CPS	CPU – 80%	CPU < 6%
750 CPS	CPU – 90%	CPU < 6%

Finally, in configuration 2/scenario 2 the WCCP services are both applied in the ingress direction but the default hash assignment method is used. This also uses software forwarding for the initial flow setup into the Netflow tables. Therefore the CPU is affected considerably when compared to a full hardware forwarding configuration shown in the recommended design. (See Figure 7 and Table 8.)

Figure 7. Configuration 2/Scenario 2 Network Diagram Comparison to Recommended Configuration

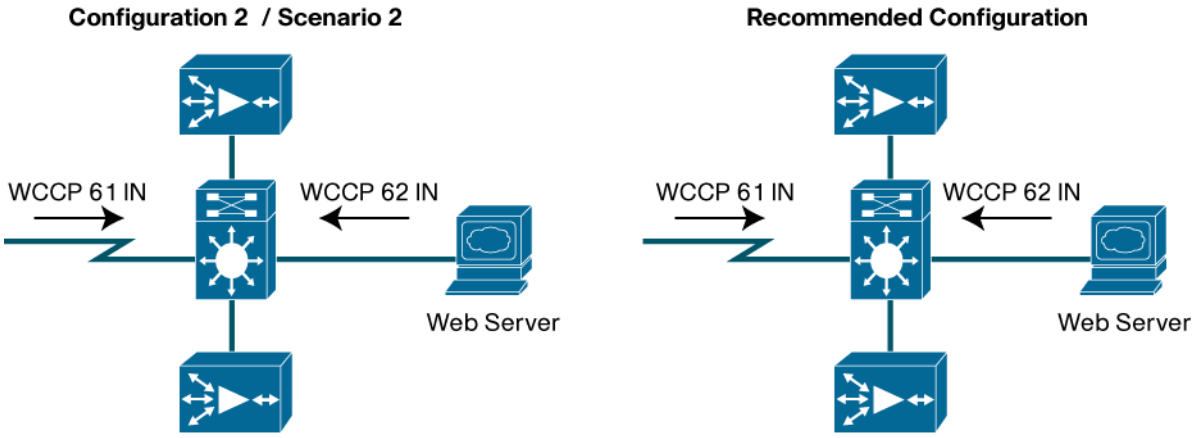


Table 7. Configuration 2/Scenario 2 Comparison

Configuration 2	Scenario 2	Recommended Configuration
Service	**61 Ingress/62 Ingress**	**61 Ingress/62 Ingress**
Assignment Method	**Hash**	**Mask**
Redirection	L2	L2
Egress Method	IP Forwarding	IP Forwarding
Return Method	L2	L2
CPU % (5 Min. Avg.)		
475 CPS	CPU – 50%	CPU < 6%
675 CPS	CPU – 80%	CPU < 6%
750 CPS	CPU – 90%	CPU < 6%

Conclusion

Deploying WCCP continues to be a valuable tool for delivering services in today's networks. Cisco IOS Software provides the most comprehensive set of WCCP features and capabilities in the industry and is designed to run on range of Cisco routing and switching platforms. The Cisco Catalyst 6500 running Cisco IOS Software provides an ideal platform to deliver WCCP services when the configuration uses hardware resources correctly.

The Cisco Catalyst 6500 supports two main recommended configurations for deploying WCCP; one configuration uses L2 traffic transport methods with full hardware-based switching, and this method should be used whenever possible. For designs where the WCCP clients are not L2 adjacent, the WCCP GRE transport methods are supported and can use fully hardware-based switching path or combination hardware and software forwarding. Following these best practice recommendations and using the hardware forwarding resources in the Cisco Catalyst 6500 will make sure of a scalable and robust WCCP service deployment.

For More Information

- **WCCP v2 Internet Draft:** http://tools.ietf.org/id/draft-wilson-wrec-wccp-v2-01.txt
- **Configuring WCCP Services:** http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf018_ps1835_TSD_Products_Configuration_Guide_Chapter.html

Appendix: Cisco Catalyst 6500 WCCP Feature Support Matrix

Feature/Supervisor	Supervisor 32 PFC3B/XL	Supervisor 720 PFC3B/XL	VS -Sup720-10GE PFC3C/XL
WCCP Service Direction			
Ingress (in)	HW	HW	HW
Egress (out)	SW	SW	SW
Feature Coexistence			
Policy-Based Routing[4]	HW	HW	HW
Network Address Translation	HW	HW	HW
Router ACL	HW	HW	HW
VLAN ACL	HW	HW	HW
QoS – MQC	HW	HW	HW
Netflow	HW	HW	HW
VRF-aware	No	No	No
Registration			
Priority	Not supported	Not supported	Not supported
Multicast address	Yes	Yes	Yes
Access Group Security	Yes	Yes	Yes
Assignment			
Hash	SW	SW	SW
Mask	HW	HW	HW
Redirect			
GRE	HW	HW	HW
L2[5]	HW	HW	HW
Redirect List			
Permit	HW	HW	HW
Deny	HW	HW	HW
L4 ACL Operator	HW	HW	HW
Object Groups	HW	HW	HW
ACL Entry Counters	HW	HW	HW
ACL logging	SW	SW	SW
Return			
GRE	SW	SW	SW
L2	HW	HW	HW

HW= Hardware Support SW=Software Support

[4] Policy-Based Routing – PBR and WCCP may be configured on the same interface and can coexist with hardware support provided the features are not applied to the same traffic. If the features do overlap then the traffic will be switched in software.
[5] L2 Traffic Redirection and Return is supported in hardware beginning with Cisco IOS Software Release 12.2(33)SXH.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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 C11-629052-00 10/10