Deploying and Troubleshooting Web Cache Control Protocol Version 2 on Cisco ASR 1000 Series Aggregation Services Routers

Executive Summary

Cisco® ASR 1000 Series Aggregation Services Routers are next-generation, modular, services-integrated routing platforms designed with the flexibility to support a wide range of 4- to 16-millions of packets per second (mpps) packet forwarding, 5- to 20-Gbps system bandwidths, performance, and scaling.

One of the many features that are supported on the Cisco ASR 1000 Series is Web Cache Control Protocol (WCCP) Version 2. By way of this feature, the Cisco ASR 1000 Series enables a lot of new high-speed and transparent linkages to the existing advanced technologies such as WAN optimization and email security.

This document provides details of the extent of WCCPv2 protocol features that are available in Cisco IOS® Software XE Release 2.2. It will also cover the integration of the above-mentioned technologies and how they work on the Cisco ASR 1000 Series.

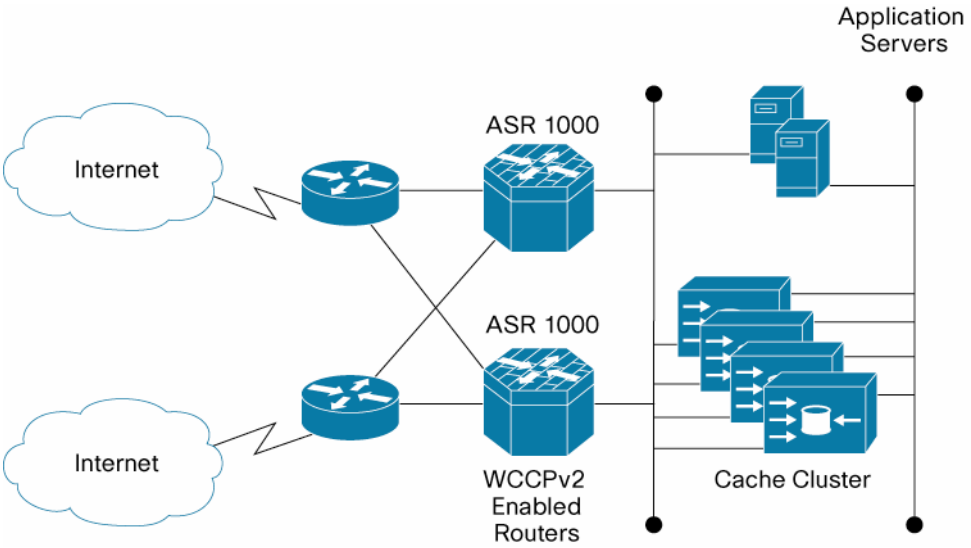
Let's first briefly review how WCCPv2 works in Cisco IOS Software.

WCCP: Technology Overview

WCCP was initially designed as a component of Cisco IOS Software whose purpose was to intercept HTTP traffic traversing a router and redirect that traffic to a local cache with the aim of reducing access times to websites and conserving wide area link upstream bandwidth.

With the introduction of WCCPv2, the scope of the protocol widened to include traffic types other than HTTP, allowing the protocol to be used as a more general interception mechanism. In WCCPv2 clients specify the nature of the traffic to be intercepted and forwarded to external devices, which are then in a position to provide services, based upon the traffic type, such as WAN optimization and application acceleration. (See Figure 1.)

Figure 1. WCCPv2 Redirection using Cisco ASR1000 Series Routers



WCCP Version 2

With WCCP Version 2, you can use Cisco cache engines or third-party cache engines to handle web traffic, reducing transmission costs and download time. This traffic includes user requests to view pages and graphics on World Wide Web servers, whether internal or external to your network, and the replies to those requests.

WCCP transparently redirects a variety of traffic types, specified by protocol (TCP or User Datagram Protocol [UDP]) and port. End users do not know that the page came from the cache engine rather than from the originally requested web server.

Routers and WCCP clients interact to form service groups (all routers/WCCP clients in a cluster running the same service)

- Up to 32 routers per service group
- Up to 32 WCCP clients per service group
- Each service group established and maintained independently
- Number of service groups implementation dependent

Cisco ASR 1000 WCCPv2 Solution Benefits

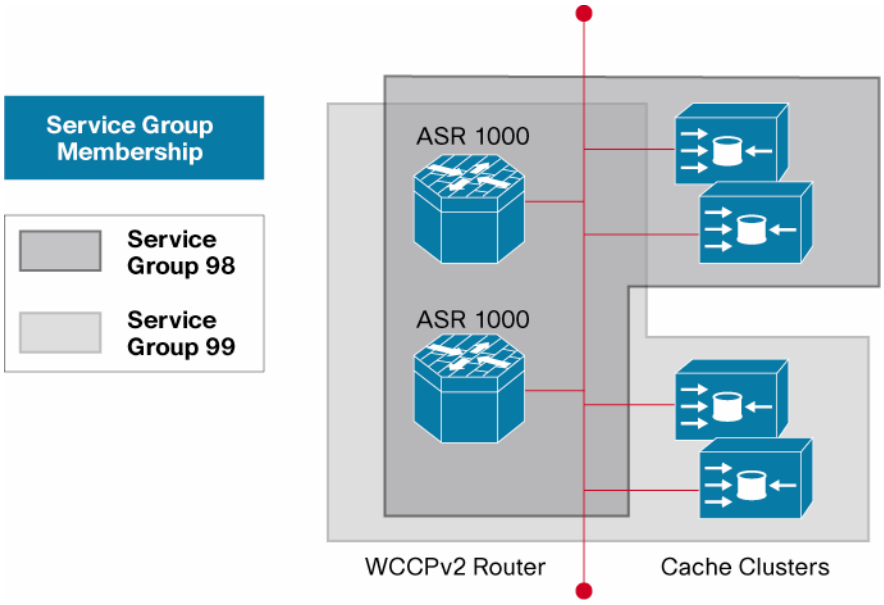
Table 1 shows the major benefits of using WCCPv2 in Cisco ASR 1000 Series Routers.

Table 1. Benefits of WCCPv2 with Cisco ASR 1000 Series Routers

Cisco ASR 1000 Platform Benefits	WCCPv2 Protocol Benefits
Multigigabit and multimillion packets per second throughput and forwarding	Fault tolerance of the service cluster
Support for both generic routing encapsulation (GRE) and Layer 2 redirect and return for tremendous deployment flexibility	Multiple router support in one service group
GRE return handled in the data plane (embedded services processor [ESP]), no punts to system route processor, hence performance boost	MD5 authentication between router and service cluster
Interoperability with Cisco IOS Firewall for Cisco Wide Area Application Services (WAAS) (by way of firewall fixup)	Multiple service groups
WCCPv2 supported in all Cisco IOS Software types starting from IP Base	Fault prevention: packet return feature (overload and bypass)
No Cisco IOS Software XE feature license required	Load distribution

Cisco ASR 1000 WCCPv2 Solution Architecture

Figure 2. WCCPv2 Service Groups Memberships



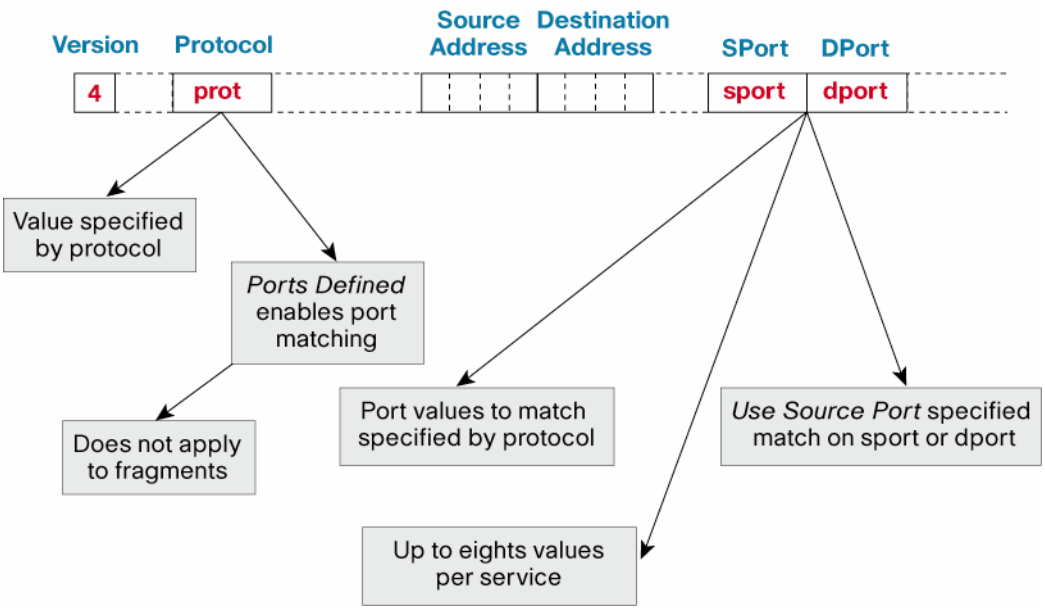
There are two parts to service definition, namely:

- Traffic profile
- Service capabilities

Traffic profile is learned from WCCP clients and a characteristic defined by external device. Capabilities are negotiated with WCCP clients. They must be the same for all members of a service group.

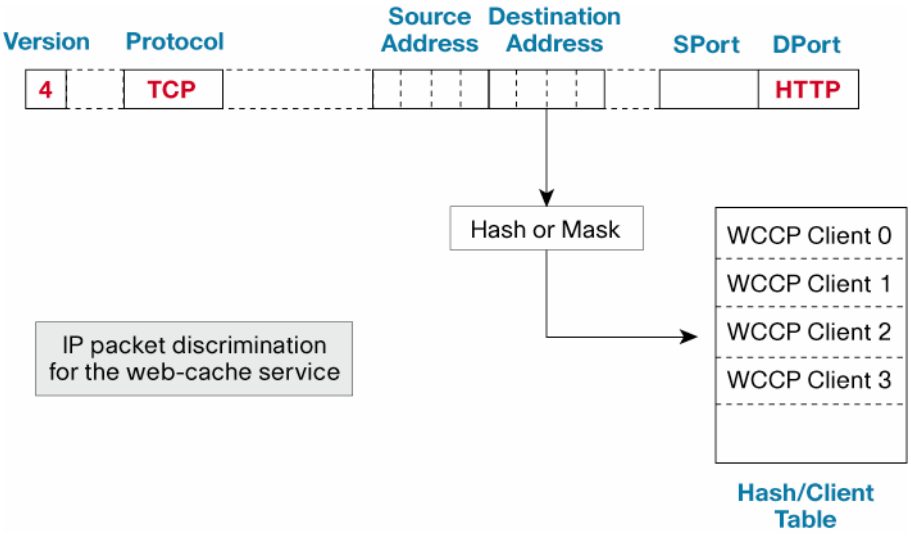
Service Definition: Traffic Profile

Figure 3. IPv4 Packet Header and Relationship with WCCPv2



Service Definition: Traffic Profile Web Cache

Figure 4. IPv4 Packet Header and Relationship with Load Distribution Mechanism



Assignment method determines how traffic is load balanced across multiple WCCP clients; appropriate load balancing depends on the deployment scenario:

- Multiservice edge
- Data center

WCCPv2 allows negotiation of either hash or mask assignment per service group; hash table and mask/value sets are supplied by the WCCP client (such as WAAS/WSA) to the router.

Note: The Cisco ASR 1000 Series supports only mask-based assignment in Cisco IOS Software XE Release 2.2; hash mode support will come in later releases.

Service Definition: Capabilities: Forwarding Method

Forwarding method determines how redirected traffic is encapsulated. WCCPv2 allows negotiation of either GRE or Layer 2 forwarding. GRE encapsulation allows the router and WCCP client to be separated by multiple hops, whereas Layer 2 requires service group members be in the same subnet. Layer 2 provides opportunities to implement high-volume/low-latency throughput.

Note: The Cisco ASR 1000 Series supports both Layer 2 MAC rewrite-based redirection/return method, and GRE redirect/return in Cisco IOS Software XE Release 2.2.

Caveats Around Redirect and Return

- WCCP client returns traffic to be forwarded normally (aka bypass traffic).
- Return method determines encapsulation.
- Protocol allows the negotiation of either GRE or Layer 2 return.
- Forwarding method does not have to match return method.

WCCPv2 and Policy-Based Routing Interaction

Currently the traffic of all software-based platforms (for example, Cisco 7200 Series Routers, Cisco 7301 Router, and integrated services routers) matching WCCP coopts the policy-based routing (PBR) path decision, and traffic is redirected to the WCCP client. Traffic not matching WCCP will follow the PBR policy. The Cisco ASR 1000 WCCP implementation preserves this Cisco IOS Software behavior.

Network-Based Application Recognition, Network Address Translation, Firewall, and WCCP Interaction

- Many network-based application recognition (NBAR) classifiers will not function if WAAS functions are applied first. Workaround is to classify on the inbound interface.
- Firewall has two issues: (a) WAAS discovery failure caused by resetting the TCP options bits; (b) WAAS modifies the TCP sequence numbers, which cause firewalls to drop the session since they track it. Workaround is to use Cisco IOS Firewall fixup for WAAS awareness (also supported in Cisco IOS Software XE Release 2.2).

For general reference, the usual Cisco IOS Software order of operation on software-based platforms is noted below:

Inside to outside:

1. decryption
2. input ACL
3. inspect
4. routing
5. **WCCP**
6. **Network Address Translation (NAT) inside to outside**
7. crypto (check map and mark for encryption)
8. output ACL
9. inspect

Outside to inside:

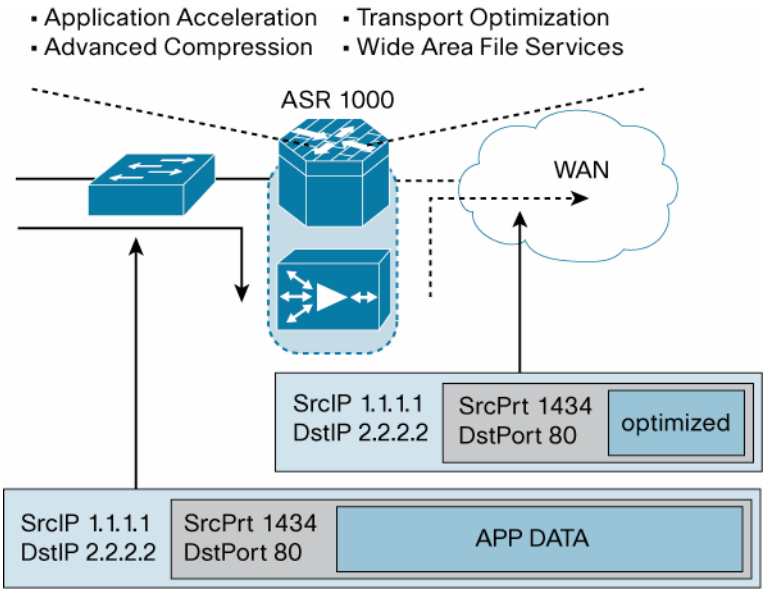
1. decryption
2. input ACL
3. inspect
4. **NAT outside to inside**
5. **WCCP**
6. routing
7. crypto (check map and mark for encryption)
8. output ACL
9. inspect

Cisco ASR 1000 and WAAS Integration Architecture

Cisco WAAS is a new technology that provides application acceleration and WAN optimization capabilities to enable organizations with multiple branch offices the ability to centralize their storage, server, and data protection infrastructure while providing LAN-like performance for remote users who access information over the WAN.

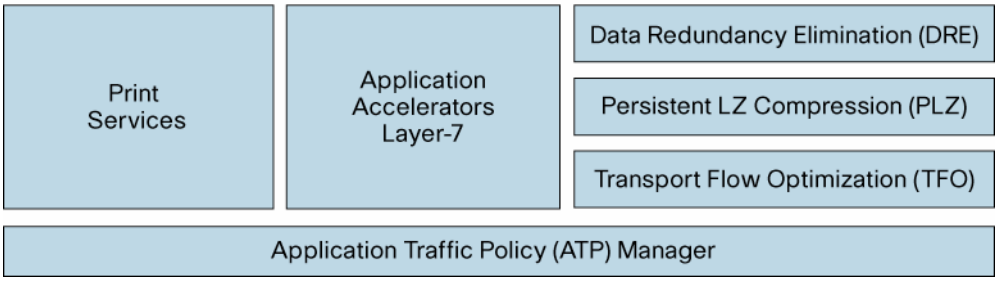
Cisco WAAS provides generic optimizations for TCP-based applications, compression, and data suppression capabilities that result in more efficient bandwidth usage and faster response times for client applications. (See Figure 5.)

Figure 5. Cisco ASR1000 integration with WAAS Solution for WAN Optimization



The Cisco ASR 1000 Series can transparently integrate with WAAS appliances using WCCPv2. Transparency helps ensure compliance with critical network features to provide the industry's only holistic and secure optimization, visibility, and control solution. (See Figure 6.)

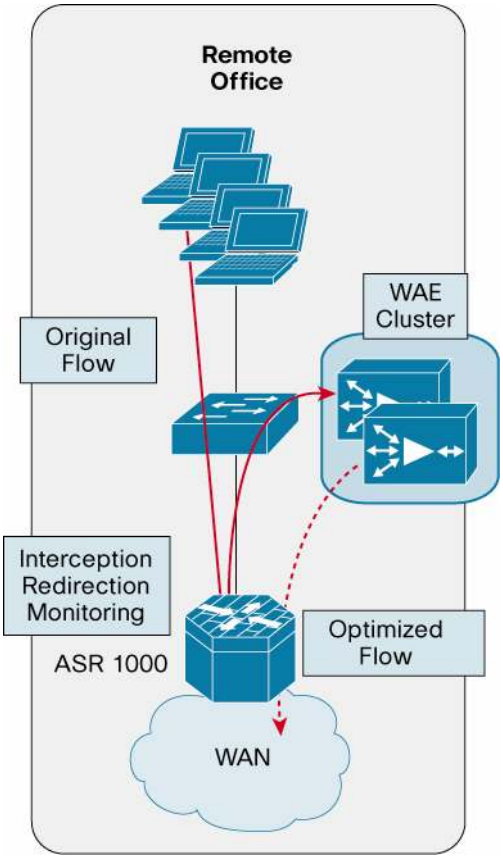
Figure 6. Architectural Pieces That Make Up Cisco WAAS Solution



The Cisco ASR 1000 Series provides two ways to intercept packets to WAAS appliances (Figure 7):

- WCCPv2 (preferred method)
- PBR

Figure 7. IPv4 Packet Paths as WCCPv2 Redirection and Return Take Place



WCCPv2 provides active-active clustering and supports up to 32 WAEsand 32 routers with automatic load-balancing, load redistribution, failover, and failthrough operation, whereas PBR allows active-passive clustering provides high availability and failover using IP SLAs as a tracking mechanism.

As of the 4.0.13 code release of the WAAS product, the ability to return traffic using GRE WCCP is possible. Previous code returned traffic (except for exceptional cases) to the router as regular IP traffic, without any kind of GRE header. This new capability allows for the deployment of new flexible topologies using the WAAS because the WAE no longer needs to sit on a dedicated Layer 3 interface off the redirecting router. In fact, now it can sit multiple hops away from the redirecting routers.

Configuration of WCCP-GRE Return

No additional configuration is required on the router. In fact, GRE WCCP is negotiated between the router and the WAAS device, and if the router is capable of supporting GRE WCCP it can be used. See Figure 8 for the WAAS configuration. Note that the additional configuration of ‘egress-method negotiated-return intercept-method wccp’ enables the use of GRE WCCP return to the router.

Figure 8. WCCP Configuration on WAAS Device

```
LX-WAE-7#sh run | in wccp
wccp router-list 1 10.17.71.1
wccp tcp-promiscuous router-list-num 1 mask-assign assign-method-strict
wccp version 2
egress-method negotiated-return intercept-method wccp
```

As mentioned before, no additional router configuration is required to support GRE WCCP. Figure 9 shows the configuration of a Cisco IOS Software router for WCCP. As service 61 and 62 are filters for TCP traffic, any TCP traffic entering on FastEthernet 1/0 or FastEthernet 1/1 will get redirected to the WAE.

Figure 9. WCCP Configuration on Cisco ASR 1000 Router

```
ip wccp 61
ip wccp 62
!
interface FastEthernet1/0
 ! ### interface facing client ###
 ip address 10.17.102.1 255.255.255.0
 ip wccp 61 redirect in
 ip flow ingress
interface FastEthernet1/1
 ! ### interface facing WAN ###
 ip address 10.17.107.1 255.255.255.0
 ip wccp 62 redirect in
 ip flow ingress
!
```

In terms of verification, the ‘show egress-methods’ command will detail the method used in specific situations. For example, Figure 10 shows that for traffic that is redirected to the WAE using service 61 or 62 the return method for that traffic is GRE WCCP. The WAE can determine the service using the Service ID field (Figure 10) in the traffic sent from the router to WAE.

Figure 10. Show Command Output on WAE of ‘show egress-methods’

```
LX-WAE-7#show egress-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
```

Cisco ASR 1000 WCCPv2 Feature Support Matrix

Cisco ASR 1000 Cisco IOS Software XE Release 2.2	WCCPv2 Features

	• WAAS/Cisco IOS Firewall interoperability
	• WCCP applied as an input feature
	• Forwarding and return method: **GRE and Layer 2**
	• Assignment method: mask mode only
	• Service Group Authentication Password
	• Statistics collection:
	  ◦ Total packets redirected
	  ◦ Total packets dropped
	  ◦ Total packets denied redirect
	  ◦ Total packets unassigned
	  ◦ Total bypassed packets received

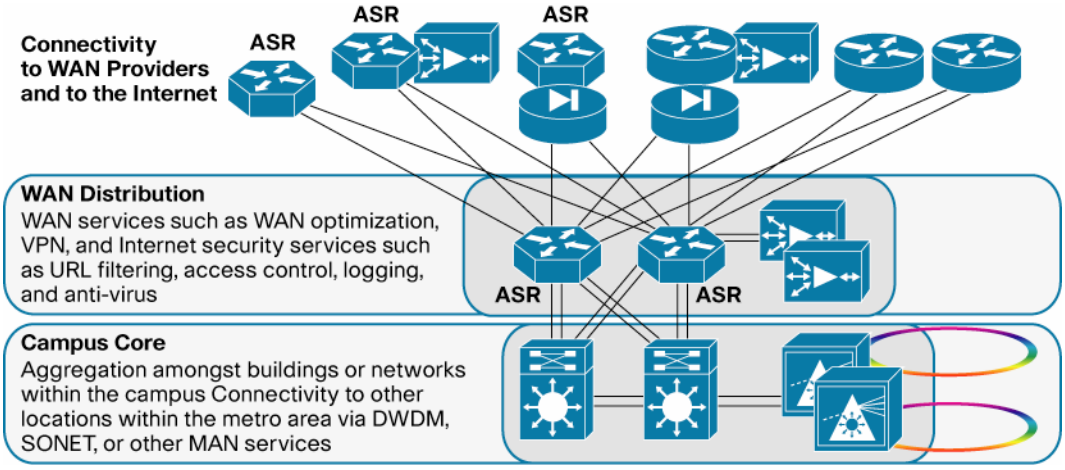
Note: Route processor-to-route processor stateful switchover (RP SSO) is not available for WCCPv2.

Cisco ASR 1000 WCCPv2/WAAS Deployment Scenarios

The Cisco ASR 1000 can be deployed both at the data center WAN headend, WAN distribution, and large access layer scenarios in the branches. Below, we'll capture the different variation of those deployments.

Let's start with the end-to-end topology that captures the various positioning of the Cisco ASR 1000 along with the Cisco WAAS solution (Figure 11).

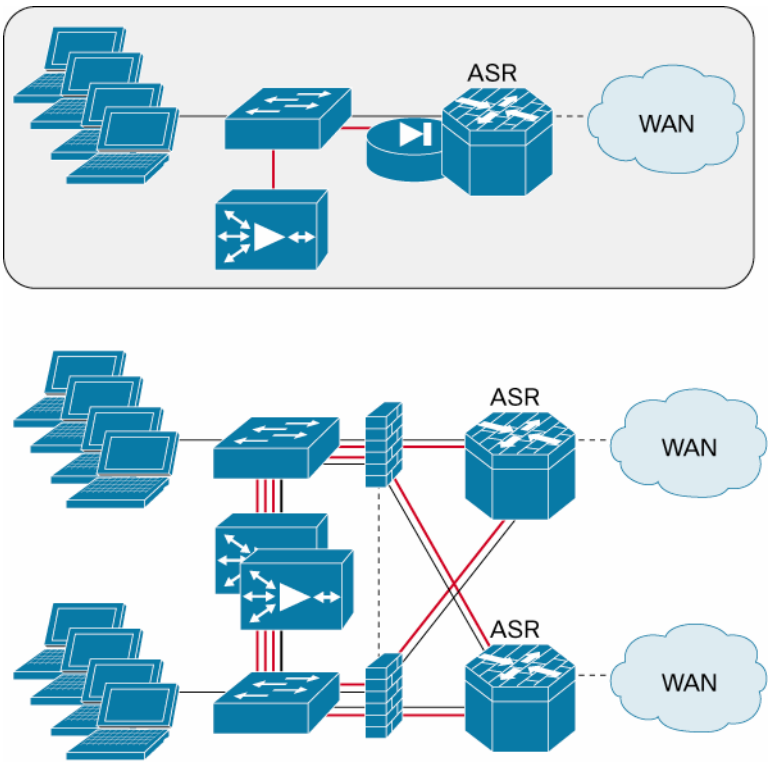
Figure 11. Cisco ASR1000 Integration with WAAS Solution



In almost all scenario, the Cisco ASR 1000 can be deployed using WCCPv2 and Cisco IOS Firewall fix-up (where applicable) alongside WAAS. WCCPv2 performance is a function of the ESP being used in the system, not the chassis itself like all other data-plane bounded features.

On the branch side, there can be two variations as to the actual deployment. Figure 12 shows the single and dual branch office router scenarios. For voice traffic, we can use redirect list to make sure that it does not get redirected to WAAS. As a best practice recommendation, Layer 2 redirect/return is to be used where performance is prime, contrast to that GRE redirect/return is used where deployment flexibility and interoperability with other features are needed.

Figure 12. Single and Dual Branch Office Router Scenarios



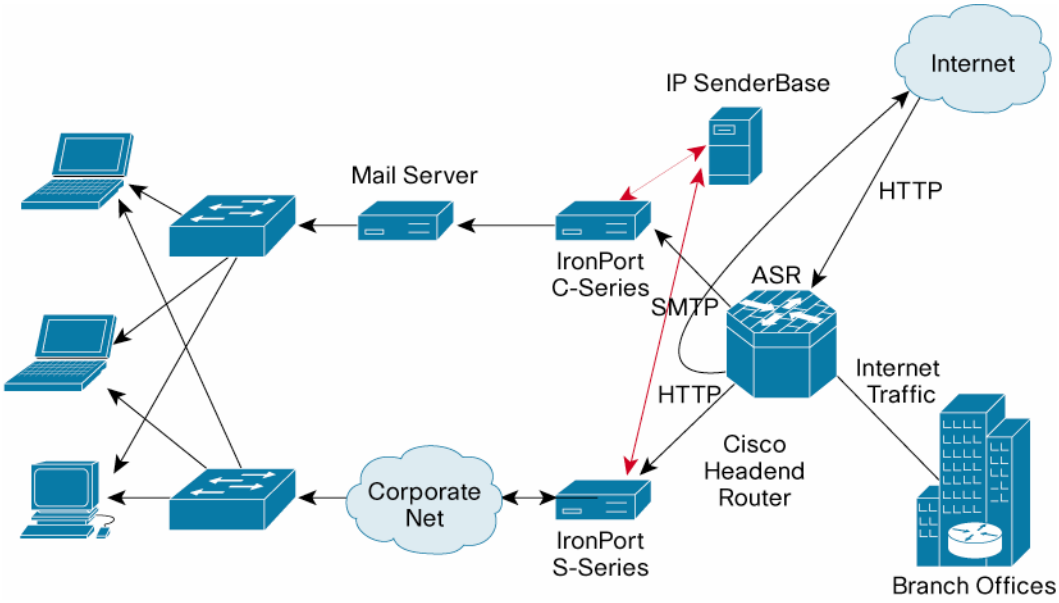
Cisco ASR 1000 WCCPv2/WSA Deployment Scenario

The Cisco ASR 1000 can integrate with WSA or IronPort appliances using WCCPv2. WSA appliances provide web and email security. More specifically, they can provide antispam, AV, and content security. This applies to both S and C series appliances.

The Cisco ASR 1000 can be used both in headquarters and in the branches alongside these appliances.

Figure 13 is the diagram that outlines a Cisco ASR 1000/WSA deployment at the headend.

Figure 13. Cisco ASR 1000/WAS Headend Deployment



Troubleshooting WCCPv2 on Cisco ASR 1000

The Cisco ASR 1000, from a user experience perspective, is another platform running Cisco IOS Software. This does not change for WCCPv2 implementation. Hence, most of the Cisco IOS Software show and debug CLIs can be used to troubleshoot and look at different WCCPv2-related statistics on the router. We will not discuss the show CLIs on the cache engine.

Show/Debug CLIs Related to Cisco IOS Software

Table 2. Cisco IOS Generic CLIs

Cisco IOS Software CLI	Description
show ip wccp <service number>	On the Cisco ASR 1000 platform all show counter stats outputs will be generated by the “show platform” CLI, hence this CLI displayed as 0 on the Cisco IOS Software as shown below.
Show ip wccp	On the Cisco ASR 1000 platform, all show counter outputs will be generated by the QFP.
clear platform software wccp counters	Clears the WCCPv2 stats.
debug ip wccp packets	Provides runtime packet statistics (only control plane packets).
debug ip wccp events	Provides runtime WCCPv2 event statistics.

```
ASR1000#sh ip wccp 61
Global WCCP information:
    Router information:
        Router Identifier:                  172.1.1.1
        Protocol Version:                   2.0
    Service Identifier: 61
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       0
          Process:                          0
          CEF:                              0
        Redirect access-list:               -none-
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
        Group access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
ASR1000#sh ip wccp 62
Global WCCP information:
    Router information:
        Router Identifier:                  171.1.1.1
        Protocol Version:                   2.0


    Service Identifier: 62
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       0
          Process:                          0
          CEF:                              0
        Redirect access-list:               -none-
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
        Group access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total Bypassed Packets Received:    0
```

Note: All the WCCPv2 related counter statistics are showing up as zero. To be able to see the actual statistics, one has to look into “show platform” CLIs.

ASR1000#**sh ip wccp interfaces detail**

WCCP interface configuration details:

POS0/1/0

Output services: 0

Input services: 1

Static: None

Dynamic: 062

Mcast services: 0

Exclude In: FALSE

GigabitEthernet0/3/0

Output services: 0

Input services: 1

Static: None

Dynamic: 061

Mcast services: 0

Exclude In: FALSE

GigabitEthernet0/3/2

Output services: 0

Input services: 1

Static: None

Dynamic: 062

Mcast services: 0

Exclude In: FALSE

Serial0/0/0

Output services: 0

Input services: 1

Static: None

Dynamic: 062

Mcast services: 0

```
    Exclude In:      FALSE
  Serial0/2/0:0
    Output services: 0
    Input services:  1
    Static:          None
    Dynamic:         062
    Mcast services:  0
    Exclude In:      FALSE

ASR1000#sh ip wccp web-cache detail
   WCCP Client information:
    WCCP Client ID:          60.1.1.2
    Protocol Version:        2.0
    State:                   Usable
    Redirection:             L2
    Packet Return:           L2
    Packets Redirected:      0
    Connect Time:            00:20:34
    Assignment:              MASK

    Mask  SrcAddr    DstAddr    SrcPort DstPort
    ----  -------    -------    ------- -------
    0000: 0x00000000 0x00001741 0x0000  0x0000

    Value SrcAddr    DstAddr    SrcPort DstPort CE-IP
    ----- -------    -------    ------- ------- -----
    0000: 0x00000000 0x00000000 0x0000  0x0000  0x3C010102 (60.1.1.2)
    0001: 0x00000000 0x00000001 0x0000  0x0000  0x3C010102 (60.1.1.2)
    0002: 0x00000000 0x00000040 0x0000  0x0000  0x3C010102 (60.1.1.2)
    0003: 0x00000000 0x00000041 0x0000  0x0000  0x3C010102 (60.1.1.2)
    0004: 0x00000000 0x00000100 0x0000  0x0000  0x3C010102 (60.1.1.2)
    0005: 0x00000000 0x00000101 0x0000  0x0000  0x3C010102 (60.1.1.2)
```

0006: 0x00000000 0x00000140 0x0000 0x0000 0x3C010102 (60.1.1.2)

0007: 0x00000000 0x00000141 0x0000 0x0000 0x3C010102 (60.1.1.2)

0008: 0x00000000 0x00000200 0x0000 0x0000 0x3C010102 (60.1.1.2)

0009: 0x00000000 0x00000201 0x0000 0x0000 0x3C010102 (60.1.1.2)

0010: 0x00000000 0x00000240 0x0000 0x0000 0x3C010102 (60.1.1.2)

0011: 0x00000000 0x00000241 0x0000 0x0000 0x3C010102 (60.1.1.2)

0012: 0x00000000 0x00000300 0x0000 0x0000 0x3C010102 (60.1.1.2)

0013: 0x00000000 0x00000301 0x0000 0x0000 0x3C010102 (60.1.1.2)

ASR1000#**show platform software wccp 61 counters**

Service Group (1, 61) counters

Unassigned count = 0

Dropped due to closed service count = 0

Bypass count = 0

Bypass failed count = 0

Denied count = 0

Redirect count = 313635910244

CE = 70.1.1.2, obj_id = 58, Redirect Packets = 42768533218

CE = 81.1.1.2, obj_id = 165, Redirect Packets = 45619768766

CE = 60.1.1.2, obj_id = 56, Redirect Packets = 45619768768

CE = 61.1.1.2, obj_id = 55, Redirect Packets = 42768533220

CE = 91.1.1.2, obj_id = 54, Redirect Packets = 34214826568

CE = 80.1.1.2, obj_id = 53, Redirect Packets = 34214826568

CE = 71.1.1.2, obj_id = 52, Redirect Packets = 34214826568

CE = 90.1.1.2, obj_id = 51, Redirect Packets = 34214826568

Cisco ASR 1000 Platform-Specific Show/Debug CLIs

Table 3 shows the CLIs that can be used to look at counter statistics and various lower level data-plane statistics.

Table 3. CLIs for Counter and Lower Level Data-Plane Statistics

Platform CLI	Description
show platform software WCCP fp active	Shows the forwarding processor, Forwarding Manager related information
show platform software wccp rp active	Shows the route processor related information
show platform software wccp interface counters	Shows the total number of redirected packets by interfaces
sh platform software wccp web-cache counters	Shows the service group related information and drop statistics
show platform so interface F0 brief	Shows the low level (data plane) QFP information

Platform CLI	Description
show platform software wccp f0 interface	Shows the low level (data plane) information
debug platform software wccp configuration	Shows low level (data plane), configuration details

ASR1000#**sh platform software wccp rp active**

Dynamic service 61

Priority: 34, Number of clients: 1

Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE

L4 proto: 6, Use Source Port: No, Is closed: No

Dynamic service 62

Priority: 34, Number of clients: 1

Assign Method: Mask, Fwd Method: GRE, Ret Method: GRE

L4 proto: 6, Use Source Port: No, Is closed: No

ASR1000#**sh platform software wccp fp active ?**

<0-255> service ID

cache-info Show cache-engine info

interface Show interface info

statistics Show messaging statistics

web-cache Web-cache type

| Output modifiers

<cr>

ASR1000#**sh platform software wccp interface counters**

Interface GigabitEthernet0/1/2

Input Redirect Packets = 391

Output Redirect Packets = 0

Interface GigabitEthernet0/1/3

Input Redirect Packets = 1800

Output Redirect Packets = 0

```
ASR1000#sh platform software wccp web-cache counters
 Service Group (0, 0) counters
      unassigned_count = 0
      dropped_closed_count = 0
      bypass_count = 0
      bypass_failed_count = 0
      denied_count = 0
      redirect_count = 0

ASR1000#sh platform so wccp web merge
Service Group (0, 0) ASR merged acl (from NULL):
   redirect acl size: 0/0, merged acl size 64/64

   1 permit tcp any  0.0.0.0 255.255.232.190 eq www
      00000000/FFFFFFFF 00000000/FFFFE8BE 0000/FFFF 0050/0000
      IP adj out of FastEthernet1/0/4, addr 60.1.1.2, mac 0014.5e85.6fe9
   2 permit tcp any  0.0.0.1 255.255.232.190 eq www
      00000000/FFFFFFFF 00000001/FFFFE8BE 0000/FFFF 0050/0000
      IP adj out of FastEthernet1/0/4, addr 60.1.1.2, mac 0014.5e85.6fe9
   3 permit tcp any  0.0.0.64 255.255.232.190 eq www
      00000000/FFFFFFFF 00000040/FFFFE8BE 0000/FFFF 0050/0000
      IP adj out of FastEthernet1/0/4, addr 60.1.1.2, mac 0014.5e85.6fe9
   4 permit tcp any  0.0.0.65 255.255.232.190 eq www
      00000000/FFFFFFFF 00000041/FFFFE8BE 0000/FFFF 0050/0000
      IP adj out of FastEthernet1/0/4, addr 60.1.1.2, mac 0014.5e85.6fe9
   5 permit tcp any  0.0.1.0 255.255.232.190 eq www
      00000000/FFFFFFFF 00000100/FFFFE8BE 0000/FFFF 0050/0000
      IP adj out of FastEthernet1/0/4, addr 60.1.1.2, mac 0014.5e85.6fe9
   6 permit tcp any  0.0.1.1 255.255.232.190 eq www
      00000000/FFFFFFFF 00000101/FFFFE8BE 0000/FFFF 0050/0000
      IP adj out of FastEthernet1/0/4, addr 60.1.1.2, mac 0014.5e85.6fe9
   7 permit tcp any  0.0.1.64 255.255.232.190 eq www
```

00000000/FFFFFFFF 00000140/FFFFE8BE 0000/FFFF 0050/0000

IP adj out of FastEthernet1/0/4, addr 60.1.1.2, mac 0014.5e85.6fe9

8 permit tcp any 0.0.1.65 255.255.232.190 eq www

00000000/FFFFFFFF 00000141/FFFFE8BE 0000/FFFF 0050/0000

IP adj out of FastEthernet1/0/4, addr 60.1.1.2, mac 0014.5e85.6fe9

9 permit tcp any 0.0.2.0 255.255.232.190 eq www

00000000/FFFFFFFF 00000200/FFFFE8BE 0000/FFFF 0050/0000

ASR1000#**show platform software wccp r0 web-cache access-list**

ASR1000#**show platform so interface F0 brief**

Forwarding Manager Interfaces Information

Name	ID	CPP ID
FastEthernet1/0/0	6	7
FastEthernet1/0/1	7	8
FastEthernet1/0/2	8	9
FastEthernet1/0/3	9	10
FastEthernet1/0/4	10	11
FastEthernet1/0/5	11	12
FastEthernet1/0/6	12	13
FastEthernet1/0/7	13	14
Null0	1	6

Router#**sh platform software wccp f0 interface**

if_handle: 8, direction: In

Standard web-cache service

if_handle: 9, direction: In

Standard web-cache service

Traffic into gi0/1/2 is set to forward packets (via redirect aCL config)

while traffic in gi0/1/3 is set to redirect packets

ASR1000#deb platform software wccp configuration

WCCP configuration event debugging is on

Router#

*May 16 11:51:03.793: %WCCP-5-SERVICEFOUND: Service web-cache acquired on WCCP Client 6.1.1.1

*May 16 11:51:12.182: FMANRP-WCCP: update ce adjacency: CE = 7.1.1.1, fwd_method = L2 adj_handle = 0x38A5C150, join = TRUE

*May 16 11:51:12.182: FMANRP-WCCP: wc list changed, Service Group (0, 0)

acl = 101, active = 1, num_wcs = 2, protocol = 6

ass_method Mask, fwd_method L2, ret_method L2

use_source_port = 0x0

wc[0] = 6.1.1.1

wc[1] = 7.1.1.1

ports[0] = 80

ports[1] = 0

ports[2] = 0

ports[3] = 0

ports[4] = 0

ports[5] = 0

ports[6] = 0

ports[7] = 0

*May 16 11:51:12.182: FMANRP-WCCP: Service Group (0, 0) generate NULL merged acl from IOS

*May 16 11:51:12.182: FMANRP-WCCP: Service Group (0, 0) cache_info is NULL from IOS

*May 16 11:51:12.183: %WCCP-5-SERVICEFOUND: Service web-cache acquired on WCCP Client 7.1.1.1

*May 16 11:51:13.793: FMANRP-WCCP: update ce adjacency: CE = 6.1.1.1, fwd_method = L2 adj_handle = 0x32895650, join = TRUE

*May 16 11:51:22.193: FMANRP-WCCP: update ce adjacency: CE = 7.1.1.1,

fwd_method = L2 adj_handle = 0x38A5C150, join = TRUE

*May 16 11:51:23.813: FMANRP-WCCP: update ce adjacency: CE = 6.1.1.1,

fwd_method = L2 adj_handle = 0x32895650, join = TRUE

*May 16 11:51:28.813: FMANRP-WCCP: update mask data, Service Group (0, 0)

acl = 101, active = 1, num_wcs = 2, protocol = 6

ass_method Mask, fwd_method L2, ret_method L2

use_source_port = 0x0

wc[0] = 6.1.1.1

wc[1] = 7.1.1.1

ports[0] = 80

ports[1] = 0

ports[2] = 0

ports[3] = 0

ports[4] = 0

ports[5] = 0

ports[6] = 0

ports[7] = 0

*May 16 11:51:28.813: FMANRP-WCCP: Service Group (0, 0) generate merged acl

from IOS

*May 16 11:51:28.813: FMANRP-WCCP: wccp merged_acl(acl=101), p=128 t=129 ASR

wccp merged_acl, num_port=1 result_len=129

*May 16 11:51:30.746: FMANRP-WCCP: (0, 0) add CE stats for obj_id 36

*May 16 11:51:30.746: FMANRP-WCCP: (0, 0) add CE stats for obj_id 55

*May 16 11:51:32.204: FMANRP-WCCP: update ce adjacency: CE = 7.1.1.1,

fwd_method = L2 adj_handle = 0x38A5C150, join = TRUE

*May 16 11:51:33.833: FMANRP-WCCP: update ce adjacency: CE = 6.1.1.1,

fwd_method = L2 adj_handle = 0x32895650, join = TRUE

Conclusion

The Cisco ASR 1000 brings tremendous value to existing WCCPv2 Cisco IOS Software implementations by combining both Layer 2 and GRE redirect/return in one platform and taking it to entirely game changing, multigigabit and multi-mpps performance levels and scale.

Due to the Cisco QFP chipset, even GRE returned packets are handled at the data plane, hence causing no loading on the system route processor CPU, making flexibility and enhanced interoperability inherent in GRE return scenarios very deployable in the production networks at those high speeds.

Related Documents and Further Reading

Configuring Web Cache Services Using WCCPv2:
http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf018.html

Cisco WCCPv2 Transparent Redirection:
http://www.cisco.com/en/US/products/hw/contnetw/ps546/products_configuration_example09186a00801abf77.shtml

Cisco WAAS Quick Configuration Guide:
http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v411/quick/guide/waasqcg.html

Cisco IronPort website:
http://www.cisco.com/web/products/ironport/index.html

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 C11-502351-01 08/11