Deploying Cisco Wide Area Application Services in MPLS VPN and VRF Lite Environments

What You Will Learn

Customers increasingly want to deploy Cisco® Wide Area Application Services (WAAS) in Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environments to optimize application performance and enable infrastructure consolidation. This document describes the options available for deploying Cisco WAAS in MPLS VPN environments and provides a sample configuration to support Web Cache Communication Protocol (WCCP) on VRF interfaces in an MPLS environment.

VRF Overview

VRF is an extension of IP routing that allows multiple routing instances to coexist in the same router. This feature provides a separate IP routing and forwarding table for each VPN. A VRF instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. Each of these items is discrete and fully contained within the VRF instance and not shared with other VRF instances.

Interception Mechanisms

Cisco WAAS offers four interception and redirection methods that can be used to redirect TCP connections to adjacent Cisco Wide Area Application Engine (WAE) devices to achieve optimization benefits:

- Inline
- WCCP
- Policy-Based Routing (PBR)
- Load balancers such as Cisco Application Control Engine (ACE)

In general, Cisco WAAS recommends using inline deployment in branch locations and WCCP in the data center; however, this is not a hard and fast rule. If, for example, your customer has deployed Cisco Integrated Services Routers with Cisco WAAS NME-WAE network modules for branch locations, then inline deployment is not possible, and WCCP redirection may be needed to redirect TCP traffic. The eventual design must be tailored to the customer's needs and requirements as dictated by the network design and device models used.

Note: The inline and WCCP methods are the most widely deployed interception mechanisms for Cisco WAAS.

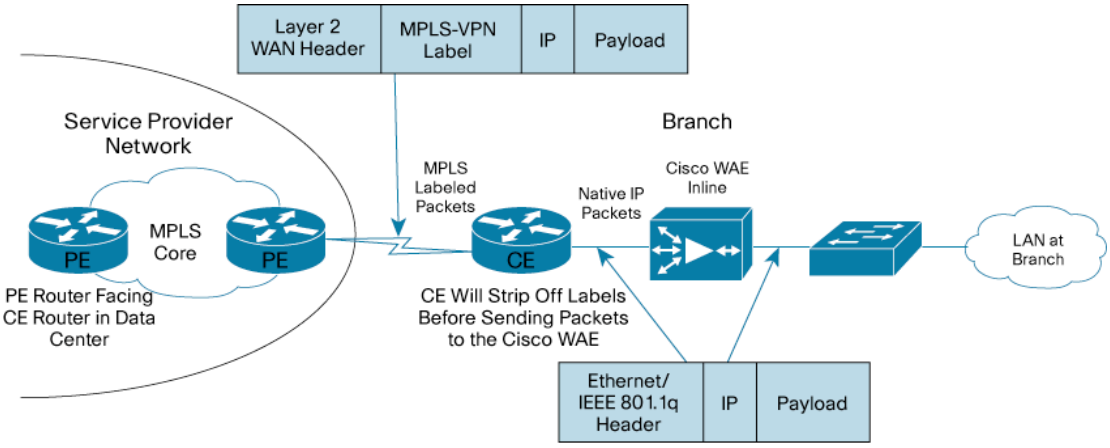
Solution Options

Customers and managed service providers (MSPs) require a solution that provides off-path deployment with near-linear scalability and performance improvements as devices are added to the network. Similarly, customers and MSPs require network path affinity: that the solution preserves the path originally chosen by the host system or network elements.

Inline Deployment

Use inline deployment with a Cisco WAE inline module or the built-in inline capability of the Cisco Wide Area Virtualization Engine (WAVE) appliances at branch locations, but have the customer-edge (CE) router strip off the labels before sending packets to the LAN side where the Cisco WAE with the inline module is plugged in as shown in Figure 1.

Figure 1. Inline Development



WCCP Deployment

WCCP enables off-path deployment of Cisco WAE devices, including Cisco WAAS NME-WAE network modules for the branch office, as well as near-linear scale, performance, and capacity increases as devices are added to the network. WCCP provides compatibility to integrate into environments in which MPLS VRF is deployed as described here.

Option 1: Service Provider Label Stripping

If any WCCP device is used at a branch location, including Cisco WAAS NME-WAE network modules and Cisco WAE and WAVE appliances, then the service provider can be directed to strip off the labels at the provider-edge (PE) router. With the labels stripped, packets arriving at the branch router (customer-edge router) will be native IP packets, allowing WCCP to redirect packets from the router to the Cisco WAAS device for optimization.

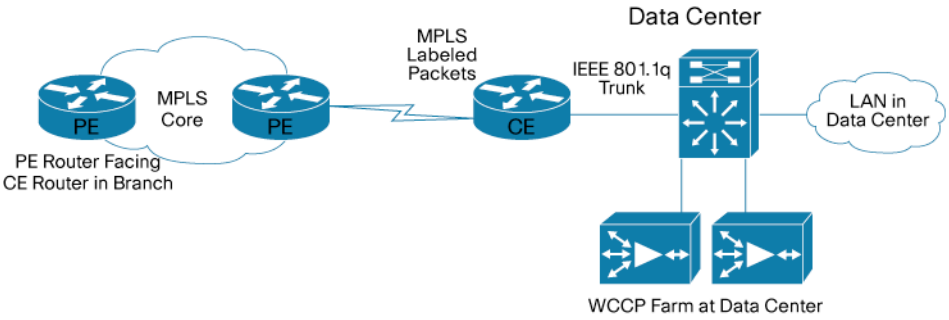
Option 2: Route Leaking at Branch Location

If a Cisco WAAS NME-WAE network module or Cisco WAE appliance is used at a branch location and the service provider cannot strip off the labels, WCCP can be used with a route-leaking option as long as there are no overlapping IP addresses. Note that, as per routing requirements, this option will be available only if there are no overlapping IP addresses. For examples of how to implement route leaking, see the sample configuration provided under Option 4.

Option 3: Data Center Label Stripping

In the data center, deploy the Cisco WAAS WAEs farther from the WAN edge router in the LAN, as shown in Figure 2. In this scenario, the customer-edge router in the data center will strip off the labels. Each VRF instance must be mapped to a VLAN and be trunked to a Cisco Catalyst® 6500 Series Switch, from which WCCP will redirect the packets and TCP flow to a Cisco WAE.

Figure 2. Data Center Deployment



Option 4: Data Center Route Leaking

In the data center, WCCP can be deployed using the route-leaking workaround as long as there are no overlapping IP addresses. This limitation is required because the network layer may potentially be unable to discern the correct VRF instance into which the packets should be reinserted. See the sample configuration that follows for an example of route leaking. You can find more information about route leaking at http://www.cisco.com/en/US/tech/tk436/tk832/technologies_configuration_example09186a0080231a3e.shtml and http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a00801445fb.shtml.

Attention: When considering route leaking, make sure there are no overlapping IP addresses.

Here is the sample configuration for route leaking:

```
POD7-DC-RTR#sh run
Building configuration...

Current configuration : 2391 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname POD7-DC-RTR
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip wccp 61
ip wccp 62
!
ip cef
!
ip vrf 1
 rd 1:1
!
interface Loopback0
```

```
 ip address 100.0.92.1 255.255.255.255
!
interface GigabitEthernet0/0
 description WAN interface
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.1001
 description WAN interface
 encapsulation dot1Q 1001
 ip vrf forwarding 1
ip wccp 61 redirect in
 ip address 2.8.71.1 255.255.255.0
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/1.3001
 description DC LAN interface
 encapsulation dot1Q 3001
 ip address 2.8.1.7 255.255.255.0
!
interface GigabitEthernet0/1.4011
 encapsulation dot1Q 4011
 ip vrf forwarding 1
 ip wccp 62 redirect in
 ip address 2.8.45.1 255.255.255.0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 no auto-summary
!
 address-family ipv4 vrf 1
  neighbor 2.8.45.11 remote-as 4001
  neighbor 2.8.45.11 activate
  neighbor 2.8.71.2 remote-as 65001
  neighbor 2.8.71.2 activate
  neighbor 2.8.71.3 remote-as 65001
  neighbor 2.8.71.3 activate
  no synchronization
  network 2.8.40.0 mask 255.255.255.0
  network 2.8.45.0 mask 255.255.255.0
  network 2.8.71.0 mask 255.255.255.0
```

Enables VRF for this interface

Enables VRF for this interface

```
 exit-address-family
!
ip default-gateway 2.8.1.254
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 2.8.1.254
ip route 2.8.71.0 255.255.255.0 GigabitEthernet0/0.1001
ip route vrf 1 10.0.2.0 255.255.255.0 2.8.1.1 global

POD7-DC-RTR#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 2.8.1.254 to network 0.0.0.0

     2.0.0.0/24 is subnetted, 2 subnets
C       2.8.1.0 is directly connected, GigabitEthernet0/1.3001
S       2.8.71.0 is directly connected, GigabitEthernet0/0.1001
     100.0.0.0/32 is subnetted, 1 subnets
C       100.0.92.1 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 2.8.1.254
POD7-DC-RTR#
POD7-DC-RTR#sh ip route vrf 1

Routing Table: 1
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 5 subnets
B       2.8.4.0 [20/0] via 2.8.45.11, 3w4d
C       2.8.45.0 is directly connected, GigabitEthernet0/1.4011
B       2.8.74.0 [20/0] via 2.8.71.3, 5w5d
B       2.8.75.0 [20/0] via 2.8.71.3, 5w5d
C       2.8.71.0 is directly connected, GigabitEthernet0/0.1001
     10.0.0.0/24 is subnetted, 1 subnets
S       10.0.2.0 [1/0] via 2.8.1.1
POD7-DC-RTR#
```

VRF Interface is leaked into the global routing table

VRF 1 is informed of 10.0.2.0 through global routing table

With the static route defined, the VRF routes can be injected into the global routing table. The loopback address, which is used as the router ID for WCCP, is then announced to the VRF instance at the location where the Cisco WAE is connected. The Cisco WAE can then establish a WCCP session with the router, and the address of the Cisco WAE is announced to the global routing table.

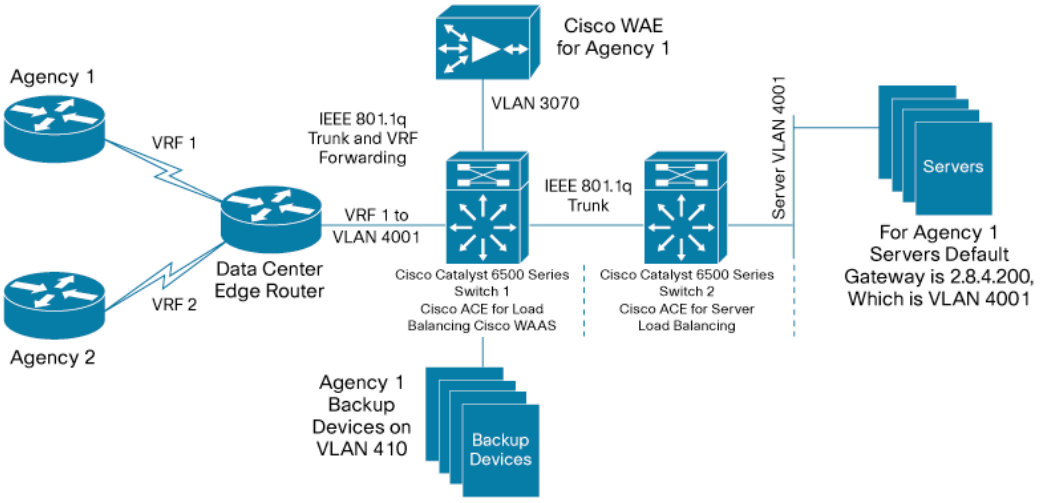
Cisco ACE Deployment

Deploying Cisco WAAS in a multiple-VRF (VRF Lite) network using Cisco ACE in the data center requires dedicated VLANs for servers and backup devices, which are mapped to a VRF instance (Figure 3). These VRF instances can have overlapping IP addresses.

The solution requirements are:

- There should not be any communication between VRF instances
- When a backup job starts for a particular VRF instance, the traffic between servers and backup devices should not go through the Cisco ACE module

Figure 3. Multiple-VRF Technology



Traffic Flow for Agency 1: Client to Server

1. Client traffic comes on VRF 1, which is then encapsulated into VLAN 4011 at the data center edge router.
2. Cisco Catalyst 6500 Series Switch 1 receives the packet on interface VLAN 4011. As soon as the packet is received on interface VLAN 4011, PBR routes the packet to context 1 on the Cisco ACE module. The Cisco ACE is dedicated for Agency 1 traffic by matching the source and destination IP as defined on the route map clsid-ag1.
3. The Cisco ACE on Cisco Catalyst 6500 Series Switch 1 load balances the traffic to the Cisco WAE dedicated for Agency 1.
4. Since the Cisco WAE's default gateway is pointing back to the Cisco ACE, it will send the packet back to context 1 on the Cisco ACE.
5. For context 1 on the Cisco ACE, the default gateway is 2.8.46.1, which is owned by interface VLAN 4010 on the Cisco Catalyst 6000 Multilayer Switch Feature Card (MSFC).
6. Upon receiving the traffic on interface VLAN 4010, the Cisco Catalyst 6000 MSFC will peek at the VRF 1 routing table to reach the destination IP address, which can be either the server's IP address or the virtual IP address on the second Cisco ACE.
7. The destination server receives the traffic.

Traffic Flow for Agency 1: Server to Client

1. The virtual IP address (on the Cisco ACE) or the server's default gateway is pointing to interface VLAN 4001 on the Cisco Catalyst MSFC, so traffic will be received by interface VLAN 4001.
2. As soon as traffic is received on interface VLAN 4001, the PBR routes the packet to context 1 on the Cisco ACE module. The Cisco ACE is dedicated for Agency 1 traffic by matching the source and destination IP as defined on route map srvsid-ag1.
3. The Cisco ACE on Cisco Catalyst 6500 Series Switch 1 load balances the traffic to the Cisco WAE that is dedicated for Agency 1.
4. Since the Cisco WAEs default gateway is pointing back to the Cisco ACE, it will send the packet back to context 1 on the Cisco ACE.
5. For context 1 on the Cisco ACE, the default gateway is 2.8.46.1 which is owned by interface VLAN 4010 on the Cisco Catalyst 6000 MSFC.
6. Upon receiving the traffic on interface VLAN 4010, the Cisco Catalyst 6000 MSFC will peek at the VRF 1 routing table to reach the destination IP address that is the client IP address.
7. The client receives the traffic.

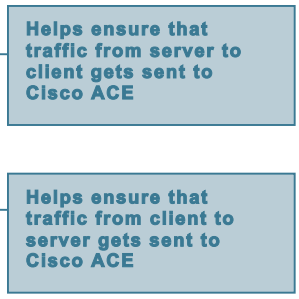
Here is the sample configuration for Cisco Catalyst 6500 Series Switch 1:

```
ip vrf 1
 rd 1:1
!
svclc multiple-vlan-interfaces
svclc module 2 vlan-group 1
svclc vlan-group 1  3070,4010
!
interface Vlan4011
 description Client-side-vlan for Agency1
 ip vrf forwarding 1
 ip address 2.8.45.11 255.255.255.0
 ip policy route-map clsid-ag1
!
interface Vlan4001
 description Server-side-vlan for Agency1
 ip vrf forwarding 1
 ip address 2.8.4.200 255.255.255.0
 ip policy route-map srvsid-ag1
!
interface Vlan410
 description Backup-Server-vlan for Agency1
 ip vrf forwarding 1
 ip address 2.8.44.1 255.255.255.0
!
interface Vlan4010
 description ACE Vlan for all Agencies
 ip vrf forwarding 1
 ip address 2.8.46.1 255.255.255.0
```

VLAN 3070 dedicated for Agency 1 Cisco WAE

Server's default gateway is pointing to this IP address

```
!
access-list 101 permit ip host 2.8.75.70 2.8.4.0 0.0.0.255
access-list 102 permit ip host 2.8.4.30 host 2.8.75.70
!
route-map srvsid-ag1 permit 10
 description Server Side route-map for Agency1
 match ip address 102
 set ip vrf 1 next-hop 2.8.46.254
!
route-map clsid-ag1 permit 10
 description Client Side route-map for Agency1
 match ip address 101
 set ip vrf 1 next-hop 2.8.46.254
!
router bgp 4001
 no synchronization
 bgp log-neighbor-changes
 no auto-summary
 !
 address-family ipv4 vrf 1
 neighbor 2.8.45.1 remote-as 1
 neighbor 2.8.45.1 activate
 no synchronization
 network 2.8.4.0 mask 255.255.255.0
 network 2.8.45.0 mask 255.255.255.0
 exit-address-family
!
end
```



Here are various **show** commands from Cisco Catalyst 6500 Series Switch 1:

```
6500-1# show module
Mod Ports Card Type                                  Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1     5  Supervisor Engine 720 10GE (Active)    VS-S720-10G        SAL1229XMVQ
  2     1  Application Control Engine Module      ACE20-MOD-K9       SAD122900J3
  3    48  CEF720 48 port 10/100/1000mb Ethernet  WS-X6748-GE-TX     SAL1229XKAZ

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  0019.e8bb.46e4 to 0019.e8bb.46eb   2.0    8.5(2)       12.2(33.0.5) Ok
  2  001d.70d1.69d0 to 001d.70d1.69d7   2.4    8.7(0.22)ACE A2(1.2)      Ok
  3  0021.d8be.2080 to 0021.d8be.20af   3.0    12.2(18r)S1  12.2(33.0.5) Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  1  Policy Feature Card 3       VS-F6K-PFC3CXL     SAL1232ZKTZ  1.0    Ok
```

```
  1  MSFC3 Daughterboard         VS-F6K-MSFC3       SAD122404A3  1.0    Ok
  3  Centralized Forwarding Card WS-F6700-CFC       SAL1229XK0P  4.1    Ok

Mod  Online Diag Status
---- -------------------
  1  Pass
  2  Pass
  3  Pass
6500-1#
6500-1#sh ver
Cisco IOS Software, s72033_rp Software (s72033_rp-IPSERVICES_WAN-VM), Version
12.2(33.0.5)SXI ENGINEERING WEEKLY BUILD, synced to sierra
SIERRA_T_SYNC_POINT_V122_33_SXI_THROTTLE
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Thu 26-Feb-09 13:56 by integ

ROM: System Bootstrap, Version 12.2(17r)SX5, RELEASE SOFTWARE (fc1)

 6500-1 uptime is 1 day, 2 hours, 52 minutes
Uptime for this control processor is 1 day, 2 hours, 51 minutes
Time since 6500-1 switched to active is 1 day, 2 hours, 51 minutes
System returned to ROM by reload at 17:13:32 UTC Thu Mar 5 2009 (SP by reload)
System image file is "sup-bootdisk:s72033-ipservices_wan-vz.122-33.0.5.SXI"
Last reload reason: Unknown reason



cisco WS-C6503-E (R7000) processor (revision 1.3) with 1040384K/8192K bytes of m
emory.
Processor board ID FOX1228G33D
SR71000 CPU at 600Mhz, Implementation 1284, Rev 1.2, 512KB L2 Cache
Last reset from s/w reset
6 Virtual Ethernet interfaces
51 Gigabit Ethernet interfaces
3 Ten Gigabit Ethernet interfaces
1917K bytes of non-volatile configuration memory.

65536K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2102

6500-1#
6500-1#show ip vrf 1
  Name                             Default RD          Interfaces
  1                                1:1                 Vl410
                                                       Vl14001
                                                       Vl14011
                                                       Vl14010
6500-1#
6500-1#
```

```
6500-1#show ip route vrf 1

Routing Table: 1
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     2.0.0.0/24 is subnetted, 7 subnets
C       2.8.4.0 is directly connected, Vlan4001
B       2.8.74.0 [20/0] via 2.8.45.1, 1d01h
C       2.8.46.0 is directly connected, Vlan4010
C       2.8.44.0 is directly connected, Vlan410
B       2.8.71.0 [20/0] via 2.8.45.1, 1d01h
B       2.8.75.0 [20/0] via 2.8.45.1, 1d01h
C       2.8.45.0 is directly connected, Vlan4011
6500-1#
```

VRF instance 1 routing table

```
6500-1# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 2.8.1.254 to network 0.0.0.0

     2.0.0.0/24 is subnetted, 2 subnets
C       2.2.2.0 is directly connected, Vif1
C       2.8.1.0 is directly connected, Vlan3001
S*   0.0.0.0/0 [1/0] via 2.8.1.254
```

Global routing table

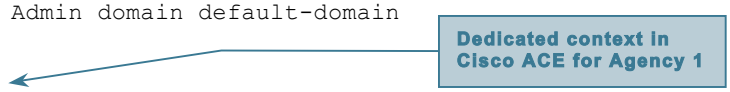
For backbone and management access

Here's the ACE Module configuration and associate show commands:

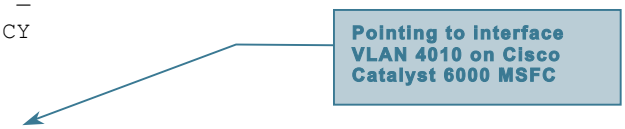
```
switch/Admin# show run

boot system image:c6ace-t1k9-mz.A2_1_2.bin

context agency1
  allocate-interface vlan 3070
```

For Cisco WAE that is dedicated for Agency 1

```
  allocate-interface vlan 4010

username admin password 5 $1$LkCMSAm7$WEkyLI2NQC05gV6sRSxMX.  role Admin domain
default-domain
username www password 5 *  role Admin domain default-domain

switch/Admin# changeto agency1
switch/agency1#

switch/agency1# sh run
Generating configuration....

access-list EVERYONE line 10 extended permit ip any any

rserver host WAAS-CORE1
  ip address 2.8.70.10
  inservice

serverfarm host WAAS
  transparent
  rserver WAAS-CORE1
    inservice

class-map match-all L4_ANY_TCP
  2 match virtual-address 0.0.0.0 0.0.0.0 tcp any
class-map type management match-any REMOTE-ACCESS
  2 match protocol telnet any
  3 match protocol ssh any
  4 match protocol icmp any

policy-map type management first-match MGMT_POLICY
  class REMOTE-ACCESS
    permit

policy-map type loadbalance first-match WAAS_POLICY
  class class-default
    serverfarm WAAS

policy-map multi-match L4_LB_WAAS_POLICY
  class L4_ANY_TCP
    loadbalance vip inservice
    loadbalance policy WAAS_POLICY

interface vlan 3070
  description WAAS WAE Server farm
  ip address 2.8.70.1 255.255.255.0
  no normalization
```



```
  mac-sticky enable
  no icmp-guard
  access-group input EVERYONE
  no shutdown
interface vlan 4010
  description ACE Vlan
  ip address 2.8.46.254 255.255.255.0
  no normalization
  no icmp-guard
  access-group input EVERYONE
  service-policy input L4_LB_WAAS_POLICY
  service-policy input MGMT_POLICY
  no shutdown

ip route 0.0.0.0 0.0.0.0 2.8.46.1

switch/agency1# sh arp

Context agency1
================================================================
IP ADDRESS      MAC-ADDRESS        Interface  Type      Encap  NextArp(s) Status
================================================================
2.8.70.1        00.1d.70.d1.69.d1  vlan3070   INTERFACE LOCAL     _          up
2.8.70.10       00.14.5e.95.29.a3  vlan3070   RSERVER   6       88 sec     up
2.8.46.1        00.1f.ca.b3.bb.40  vlan4010   GATEWAY   7       65 sec     up
2.8.46.254      00.1d.70.d1.69.d1  vlan4010   INTERFACE LOCAL     _          up
================================================================
Total arp entries 4
```



For More Information

To find out more about Cisco WAAS, visit http://www.cisco.com/go/waas or contact your Cisco account manager.

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 C11-560131-00 09/09