Value-Added Services (VAS) Traffic Forwarding

Revised: February 07, 2014, OL-30621-02

Introduction

This chapter provides an overview of VAS traffic forwarding, explaining what is it and how it works. It also explains the various procedures for configuring and monitoring the VAS traffic forwarding.

Information About VAS Traffic Forwarding

The VAS feature uses the Cisco SCE platform to access an external "expert system" for classification and control of services not supported by SCA BB. Using the VAS feature, you can forward selected flows to an external, third-party system for per-subscriber processing in addition to the existing services and functions of the SCA BB solution. For example, this feature can be used to forward selected subscriber traffic to third-party servers for intrusion detection or content-filtering.

The VAS feature enables you to divert a specified part of the traffic stream to an individual VAS server or a cluster of servers. The diversion of the traffic stream is based on the subscriber package, flow type, and the availability of the VAS servers. The feature provides load balancing for even distribution of the load on the various VAS servers.

The VAS feature supports multiple VAS service types using different VAS server groups. Several servers of the same type can be deployed in a group to increase the processing capacity and provide redundancy for each VAS service type.

The Cisco SCE platform performs subscriber load sharing between the active servers of the same server group. It is able to identify the active servers among the defined servers through a dedicated health check mechanism.

VAS Service Goals

The VAS traffic forwarding functionality enables the Service Control solution to meet several important service goals:

- Service providers can provide a range of value-added services to their subscribers, thus increasing customer satisfaction.
- The Cisco SCE platform can forward part of the traffic to third-party devices that can provide additional, complementary services.

  The Cisco SCE platform, due to its strong classification capabilities, forwards only the part of the traffic that should get the additional service based on:

  - Subscriber awareness
  - Policy that was configured
- The Service Control solution can include value-added servers that cannot be deployed inline for various reasons (for example, they cannot support throughput or are not carrier grade for inline insertion).
- Easy interoperability and flexibility for setting different services.

  Because the VAS feature emulates a regular IP network for the third-party devices, no special support is required on the part of the third-party entity.

How VAS Traffic Forwarding Works

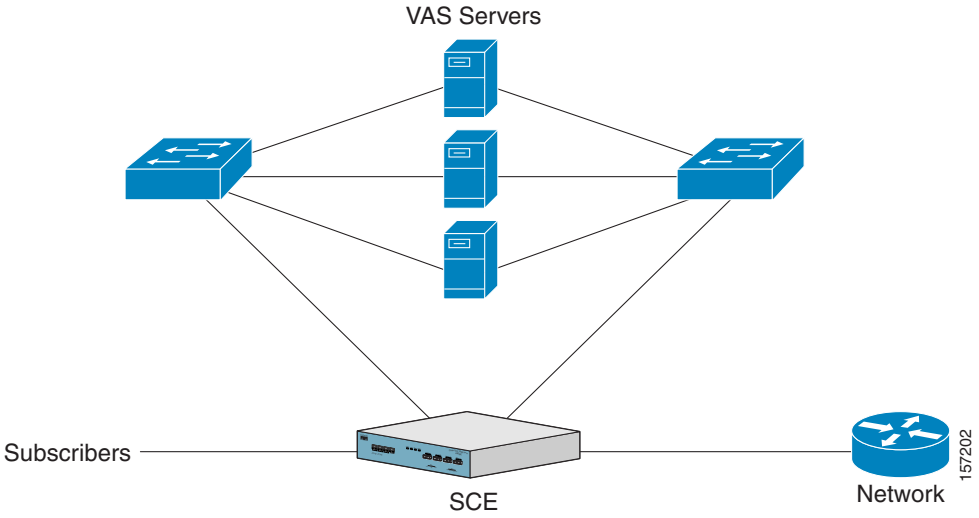
Subscribers are provisioned to the VAS services as part of the normal provisioning process of new subscribers to SCA BB.

When VAS traffic forwarding is enabled (Figure 14-1), in addition to all its basic functions, the SCA BB application classifies each flow as either a VAS flow or as a standard flow (non-VAS flow).

Flows that are classified to a VAS service get the usual SCA BB service in addition to being forwarded to the VAS servers for additional service. Traffic is processed first by the SCA BB application and then forwarded to the VAS servers.

Traffic is routed to the VAS servers using VLAN tags to identify the traffic flows.

Figure 14-1 Typical VAS Traffic Forwarding Installation



VAS traffic forwarding guidelines:

- A single Cisco SCE 8000 platform can support up to 64 VAS servers.
- A maximum of 64 Cisco SCE 8000 platforms can be connected.
- A maximum of eight VAS server groups is supported.
- The same VAS server may be used by more than one Cisco SCE platform.

Note In VAS mode, the Cisco SCE performance envelope might be up to 50 percent lower than in the normal operation mode. The exact performance envelope is specific to the traffic mix in the customer network and should be sized in advance.

The following sections provide a more detailed description of how VAS traffic forwarding works.

Requirements for VAS Servers

Because the VAS devices are installed behind the Cisco SCE platform, they should follow the network behavior of the Cisco SCE platform. Therefore, VAS devices must meet the following two requirements:

- VAS devices must be equipped with separate interfaces for the subscriber side and separate interfaces for the network side.
- Traffic towards the subscribers should be sent from the subscriber interface and from the network interface for the internet.
- VAS devices must be transparent in Layer 2. The VAS servers must act like Layer 2 switches, in that, they are not allowed to change traffic headers or to generate new traffic..

Layer 2 Transparency

To handle non-management traffic of VAS services, follow these guidelines:

- The VAS services should work in promiscuous-mode in Layer 2 and accept packets with any destination MAC address.
- When forwarding traffic back to the network after processing, the VAS devices must preserve the original Layer 2 headers containing the MAC addresses and the VLAN tag. The VAS devices must not change the MAC addresses (destination or source) or the VLAN tags. The following restrictions apply to the injected traffic:
  - The VAS device is not permitted to initiate new flows.
  - New traffic can be injected only in the context of an existing flow.
  - When injecting traffic, the Layer 2 information (MAC addresses, VLAN tags, and the TCP/IP parameters) must be taken from the flow into which the traffic is being injected.
- A VAS device must not generate its own network transactions or relay such transactions. Network transactions such as ARP requests or pings are not permitted.

VAS Management Traffic

VAS devices that are managed inband (through the traffic interface) must meet the following requirements:

- Management traffic should either be carried over a dedicated VLAN or without any VLAN header.
- The switches that are connected to the VAS devices should be directly connected to the POP router.
- The switches that are connected to the VAS devices should be configured so that management traffic is sent directly to the router and not through the Cisco SCE platform.

VAS Traffic Forwarding and SCA BB

When VAS traffic forwarding is enabled, in addition to all its basic functions, the SCA BB application classifies each flow as either a VAS flow or as a standard flow (non-VAS flow). This classification is made on the first packet of the flow (for example, TCP SYN packet). The classification must be performed on the very first packet because the classification is used to select the routing of the packet to a VAS server or to the subscriber or network.

The VAS traffic forwarding rules table is configured using the SCA BB console. These rules map certain traffic to the VAS server groups. When a flow is classified as a VAS flow, the VAS server group for this flow is selected. If the group includes more than one VAS server, traffic is forwarded so that the subscriber load is shared between the servers on the same group.

The mapping of traffic portions per package to VAS server groups is also done using the SCA BB console.

VLAN Tags for VAS Traffic Forwarding

The traffic is routed between the Cisco SCE platform and the VAS servers by VLANs. There is a unique VLAN tag for each Cisco SCE platform and VAS server combination.

Before the traffic is forwarded to the VAS servers, the Cisco SCE platform adds the VLAN tags to the original traffic. When the traffic returns to the Cisco SCE platform, the Cisco SCE platform removes the VLAN tag it previously added, and then forwards the traffic on its original link.

The VLAN tag for each VAS server is user-configured. To preserve consistency of the traffic flow, the VAS feature requires a unique VLAN tag be configured for each Cisco SCE platform and VAS server combination.

The VLAN tag has 12 bits, divided as follows:

- The lower six bits identify the VAS server.
- The higher six bits identify the Cisco SCE platform.

For example, 0x171 = 1011 10001 = SCE 11, VAS 17

Observe the following for the six bits that identify the Cisco SCE platform:

- These six bits must be the same for all VAS servers attached to a specific Cisco SCE platform.
- These six bits must be different for VAS servers attached to different Cisco SCE platforms.

The Cisco SCE platform enforces that the user-configured VLAN tags retain this format, that is, the lower bits match the VAS server number for which the VLAN tag is configured and the higher bits match the higher bits previously configured for other VAS servers on this Cisco SCE platform. However, the Cisco SCE platform cannot determine the configuration of other Cisco SCE platforms, and therefore, it is important that the configured Cisco SCE ID (higher bits) be unique for each Cisco SCE platform.

The use of VLAN tags is an integral part of the VAS feature, and therefore, requires that the VAS device be able to work in 802.1q trunk while preserving the VLAN information.

Service Flow

The Cisco SCE platform classifies a flow to a VAS server group based on the subscriber package and the TCP/UDP ports of the flow. It then selects one server within this group to handle the flow.

The Cisco SCE platform performs load sharing between multiple VAS servers belonging to the same server group; the balance is based on the subscriber load. In other words, the Cisco SCE platform ensures that the subscribers are evenly distributed between the VAS servers in the same group.The mapping of subscriber to a VAS server (per group) is maintained even when servers are added or removed from the group either due to configuration changes or changes in the operational status of the servers in the group. The mapping changes only if the same server changes its status.

The following sections explain in more detail when and how the mapping is changed:

- Non-VAS Data Flow, page 14-7
- VAS Data Flow, page 14-7

Data Flow

In a deployment using VAS traffic forwarding, there are two types of data flows:

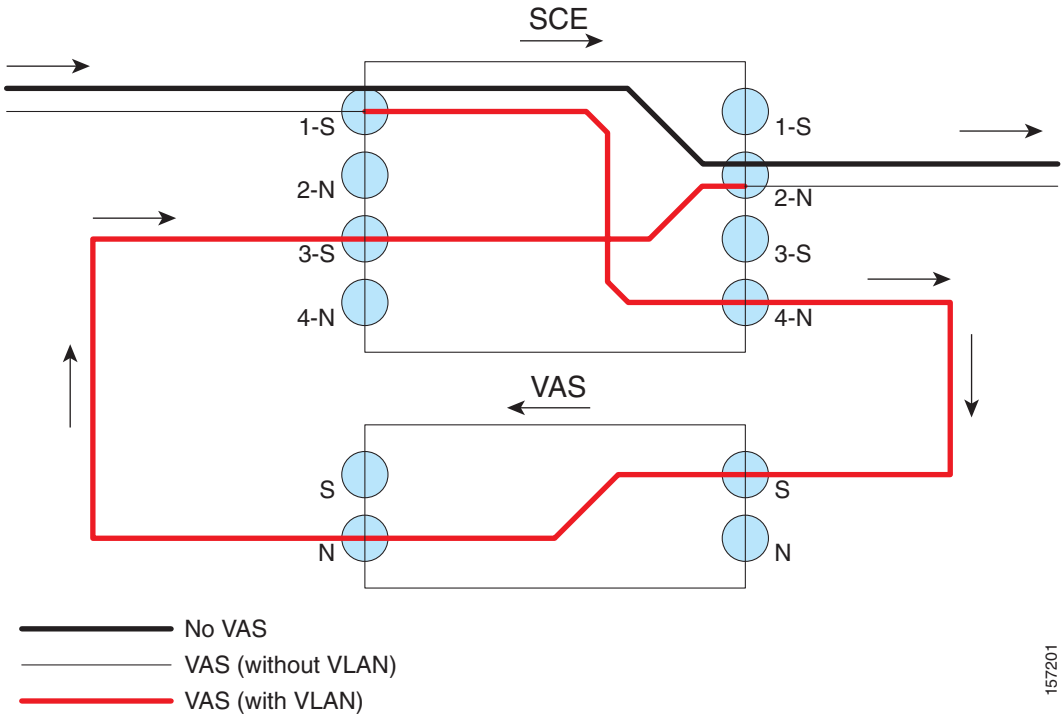
- Non-VAS flow
- VAS flow

Figure 14-2 depicts the two types of data flows running through a single Cisco SCE platform and a single VAS server.

- Ports are illustrated as two unidirectional half ports, RX (on the left side) and TX (on the right side):
  - The Cisco SCE platform has four ports.
  - The VAS server has two ports.
- For the sake of illustration, the Cisco SCE platform traffic flow direction is from left to right while the VAS traffic flow is from right to left. The arrow below the name of the element indicates the traffic flow direction.
- The Ethernet switches are omitted.
- Each line represents a flow:
  - Thick line is a non-VAS flow.
  - Thin line is a VAS flow.
  - Black line indicates part of a flow that does not have VLAN tag
  - Red line indicates part of a flow that has a VLAN tag

Figure 14-2 illustrates the data flow from the subscriber to the network. Data flow from the network to the subscriber works in the same way, but is received on the network port (N) and transmitted on the subscriber port (S).

Figure 14-2 Data Flow in a VAS System



Non-VAS Data Flow

The data flow steps for a non-VAS flow are:

1. A subscriber packet is received at the Cisco SCE platform Port 1 (S).
2. The Cisco SCE platform classifies the flow as non-VAS flow.
3. The packet is sent to the network on Port 2 (N).

VAS Data Flow

A VAS data flow is slightly more complex than the basic data flow. It is received and transmitted in the same manner as the basic non-VAS Cisco SCE platform flow, but before it is transmitted to its original destination, it flows through the VAS server.

The data flow steps for a VAS flow are:

1. A subscriber packet is received at the Cisco SCE platform Port 1 (S).
2. The Cisco SCE platform classifies the flow as a VAS flow.
3. The Cisco SCE platform adds a VLAN tag to the packet.
4. The VLAN tag is used by the Ethernet switch to route the packet to the proper VAS server.

   The packet now has a VLAN tag, which is indicated by the red line.

5. The packet is sent to the VAS subscriber port from Cisco SCE platform Port 4 (N).
6. The VAS server processes the packets and either drops the packet or sends it back to the Cisco SCE platform from the VAS network port to the Cisco SCE platform subscribers Port 3 (S).

   The VAS server passes the VLAN tag transparently. This is important to enable the Ethernet switch (not shown) to route the packet back to the proper Cisco SCE platform.
7. The Cisco SCE platform receives the packet on Port 3 (S), drops the VLAN tag, and passes the packet towards the network through Port 2 (N).

Note To use VAS, at least four interfaces should be active on the Cisco SCE device.

Load Balancing

VAS servers can be grouped logically according to their service type. Consider, for example, a system that requires both FTP caching and virus filtering. A single VAS server for each service might not have enough capacity. For example, assume that the system requires five VAS servers, three to provide FTP caching, and two to provide virus filtering. Defining two VAS server groups, for example, FTP caching and virus filtering, permits load sharing across the servers for each server group.

The subscriber package determines the VAS server group to which the flow should be attached. The selection of a specific VAS server from the VAS servers within the group is based on the current load on each VAS server. The system tries to create an equal subscriber load for all the VAS servers belonging to the same group.

In some cases, a single VAS server may be used by more than one Cisco SCE platform. Remember that the Cisco SCE platform performs load balancing only on the traffic that it sends to the VAS server; it receives no information regarding the load the VAS server may be bearing from a different Cisco SCE platform. It is vital to properly allocate available VAS servers to the Cisco SCE platforms to ensure a balanced load on each VAS server.

Load Balancing and Subscribers

The system balances the usage of the VAS servers within a VAS server group, trying to create an equal subscriber load for all the VAS servers in one VAS server group. The load balancing is subscriber based, that is, the subscribers are evenly distributed between the servers.

VAS load sharing is subscriber based rather than bandwidth based to ensure that all the traffic of the subscriber gets to the same server so that the server can make subscriber-based decisions.

The Cisco SCE platform uses the same VAS server for all the traffic of a subscriber (per server group) even if there is a change in the number of active servers in the group. Traffic from a subscriber is assigned to a new server only if the current server becomes inactive. This applies only on new flows. Flows that were already mapped to a server before it became active remain attached to it.

The mapping of subscriber to VAS servers is not saved across subscriber logouts or Cisco SCE platform reload.

Load Balancing and Subscriber Mode

Load balancing is subscriber based, therefore this feature does not work properly in subscriberless mode, because the entire traffic load would be carried by only one VAS server per group.

Tip Use anonymous mode rather than subscriberless mode with VAS traffic forwarding.

In pull mode, the first flow of the subscriber behaves as configured in the anonymous template. If no anonymous template is configured, such first flows are processed as defined by the default template. Therefore, the default template should provide a proper package, so these flows get VAS service.

VAS Redundancy

The VAS servers should be configured with high availability so that the failure of a single VAS server will not degrade total system performance and availability. This requirement must be considered when determining the number of VAS servers necessary for each VAS service.

There are two mechanisms that guarantee the performance and availability of the VAS services:

- Load sharing—The Cisco SCE platform distributes the subscribers between all the active VAS servers within a server group.
- Monitoring—The Cisco SCE platform monitors connectivity with the VAS servers and handles server failure according to the applied configuration.

In addition to failure of an individual VAS server, a complete VAS server group is considered to be failed if a defined minimum number of servers are not active.

The following sections provide more information regarding the possible points of failure in a VAS traffic forwarding deployment.

- VAS Server Failure, page 14-10
- VAS Server Group Failure, page 14-10
- Ethernet Switch Failure, page 14-11
- Disabling a VAS Server, page 14-11

VAS Server Failure

The system monitors the health of a VAS server by periodically checking the connectivity between the Cisco SCE platform and the VAS server. When the Cisco SCE platform fails to establish or maintain a connection to the server within a configurable window of time, the server is considered to be in **Down** state.

When the server is in **Down** state:

- New logged-in subscribers are distributed between the other active servers in the group.
- Subscribers that are mapped to this server are mapped to a new server if they initiate a new flow.
- The server group may move to a **Failure** state if the failure caused the number of active servers in the group to go below the minimum number configured.

If the connectivity to the server resumes, the state of the server is changed to **Up.** The server returns to the list of active servers and continues to serve subscribers that were mapped to it before the failure and have not yet been mapped to a new server during the failure time, as well as new subscribers.

VAS Server Group Failure

For each VAS server group, you can configure:

- The minimum number of active servers necessary.
- The action to take in case the actual number of active servers goes below the configured minimum.

If the minimum number of active servers equals the total number of configured servers, it means there is no redundancy and failure of one server causes the failure of the whole server group.

When the Cisco SCE platform detects that the number of active servers within a group is below the configured minimum, it changes the state of the group to **Failure**. The configured action-on-failure is then applied to all new flows mapped for that VAS server group (existing flows are not affected.)

There are two possible actions when the VAS server group has failed:

- **Block**—All new flows assigned to the failed VAS server group are blocked by the Cisco SCE platform.
- **Pass**—All new flows assigned to the failed VAS server group are considered as regular non-VAS flows, and are processed without VAS service (that is, they receive SCA BB service but not VAS service).

When the number of active servers is above the minimum and the state of the group is changed to Active again, the configured action-on-failure is no longer applied to the new flows. However, to maintain the coherency of the network, flows that were blocked or passed are not affected by the change in the state of the server group.

Ethernet Switch Failure

The Ethernet switches are a single point of failure in a VAS topology. A complete failure of an Ethernet switch causes all the VAS services to be declared as failed and the configured action (on-failure) is taken for all new VAS flows.

Disabling a VAS Server

A VAS server can be disabled for maintenance via the CLI.

No errors are reported on a disabled VAS server. However, if disabling the server reduces the number of active servers to below the minimum number configured for the group, it brings down the VAS server group because a disabled VAS server is equal to a VAS server in **Down** state.

Health check is not performed on disabled VAS servers.

VAS Status and VAS Health Check

To manage the VAS redundancy, the Cisco SCE platform needs to know the state of each VAS server. The Cisco SCE platform performs periodic health checks for all the configured VAS servers. These checks are the basis for VAS redundancy control; they enable the Cisco SCE platform to identify and react to VAS server failure, and to check the connectivity between the Cisco SCE platform and the VAS server before enabling the server to handle traffic.

The health check is performed over the VAS link, that is, the link that connects the Cisco SCE platform with the VAS servers. It validates the traffic flow between the Cisco SCE platform and the VAS server in both directions through special health check packets generated by the Cisco SCE platform.

The health check mechanism does not require special interaction with the VAS device. This is because the VAS server does not have to answer health check packets; it only passes them as they are, back to the Cisco SCE platform. As long as the packets are received by the Cisco SCE platform, the VAS server is considered to be alive. Failing to receive the packets back from the VAS server within a predefined time window is considered by the Cisco SCE platform as a failure of the VAS server and the server status is changed to **Down**.

Health check packets are:

- Carried over UDP flows.
- Contain source and destination IP addresses that can be user-configured.

  IP addresses should be:

  - Unique to the Cisco SCE platform.
  - Addresses that are not used by the network traffic (such as private IPs).

The Cisco SCE platform uses default UDP ports beginning with 63140 and 63141 for VAS Server 0, unless you configure different ports for the health check.

The Cisco SCE platform adds its own Layer 7 data on top of the UDP transport layer. This data is used by the Cisco SCE platform to validate the correctness of the packet upon retrieval.

The health check is performed under the following conditions:

- VAS mode is enabled.
- VAS server is enabled.
- Health check for the VAS server is enabled.
- Server has a VLAN tag.
- Pseudo IPs are configured for the traffic interfaces.

If the check is enabled, but any one of the conditions is not met, the server state will be **Down** (the same as if the server did not pass the health check).

Check the connectivity between the Cisco SCE platform and the VAS server before you assign the server to a server group.

The health check procedure does not require a special interface with the VAS server; the health check traffic goes through the same network channels as any other VAS traffic. However, there are two assumptions the VAS servers should fulfill:

- The VAS server should not drop traffic unless it is specifically configured to do so. Therefore, if the connectivity between the VAS server and the Cisco SCE platform is operative, the health check packets should reach the Cisco SCE platform safely.

  Alternatively, it should be possible to configure the VAS server to pass traffic on specific ports (the health check ports).

- In case of a failure, the VAS server should drop and not bypass, the traffic (cut the link), so that the Cisco SCE platform is able to identify the failure.

VAS Server States

When determining whether a VAS server is active, the system considers the following two parameters:

- User-configured Admin mode—Enabled or disabled
- VAS server state as reported by the health check

VAS Traffic Forwarding Topologies

The following sections describe the following VAS traffic forwarding topologies:

- Single Cisco SCE Platform, Multiple VAS Servers, page 14-14
- Multiple Cisco SCE Platforms, Multiple VAS Servers, page 14-15

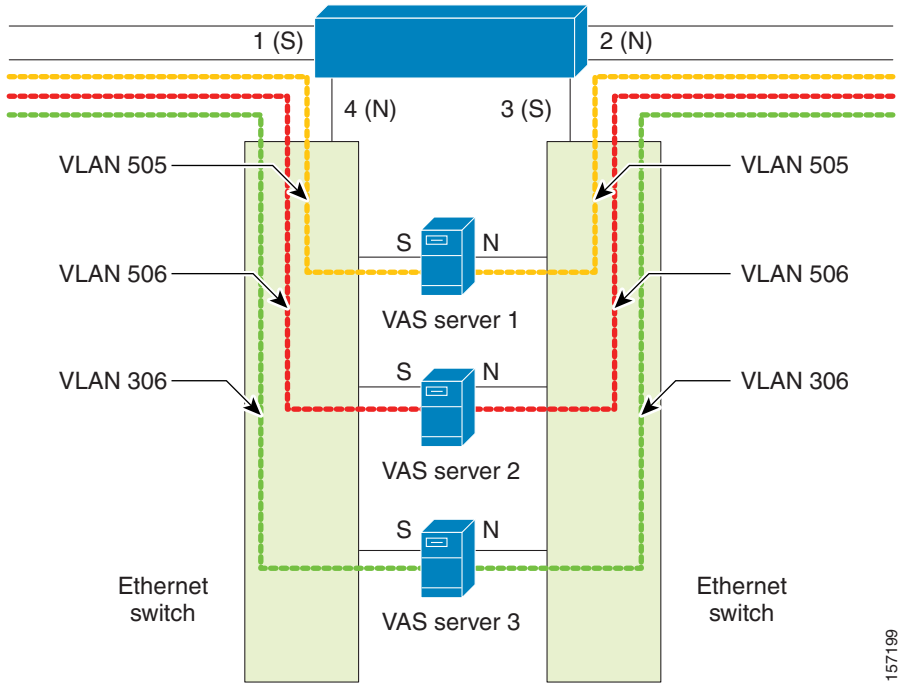
Note A topology in which a VAS server is directly connected to the Cisco SCE platform is not supported. If you want a topology of a single Cisco SCE platform connected to a single VAS server, use a switch between the Cisco SCE platform and the VAS server.

Single Cisco SCE Platform, Multiple VAS Servers

In this topology, a single Cisco SCE platform forwards VAS traffic to one or more VAS servers through two Ethernet switches (Figure 14-3).

The two Ethernet switches are necessary to avoid a situation in which a single MAC address has two ports or a single VLAN tag has two destinations. Each Ethernet switch should be configured to trunk mode with MAC learning disabled.

Figure 14-3 Single Cisco SCE Platform, Multiple VAS Servers



Data Flow

In a data flow:

1. A subscriber packet is received at Port #1 (Subscriber).
2. The Cisco SCE platform opens a flow and classifies the flow as either a non-VAS (blue) flow or as a VAS flow (red).
3. If the flow is non-VAS (blue), the Cisco SCE platform passes the packet to the network. The VAS server is not involved in this case.
4. If the flow is a VAS flow (red), the Cisco SCE platform selects the VAS server to which the packet should be sent, adds the server VLAN tag to the packet, and transmits the packet on Port #4 (Network).
5. The packet is routed by the Ethernet switch to the VAS server according to its VLAN tag (the port towards the VAS server should be the only port with this VLAN tag allowed).
6. The VAS server processes the packet and either drops or forwards it without changing the VLAN tag.
7. The packet is forwarded by the Ethernet switch to the Cisco SCE platform according to its VLAN tag (the port towards the Cisco SCE platform should be the only port with this VLAN tag allowed).
8. The Cisco SCE platform receives the packet on port #3 (Subscriber), strips the VLAN tag, and forwards the packet to the network via Port #2 (Network).

Multiple Cisco SCE Platforms, Multiple VAS Servers

n this topology, multiple Cisco SCE platforms are connected to multiple VAS servers. At least one VAS server receives traffic from more than one Cisco SCE platform; if the VAS servers are each in an exclusive relationship to a particular Cisco SCE platform, it would simply be several single Cisco SCE platform to multiple VAS server topologies grouped together.

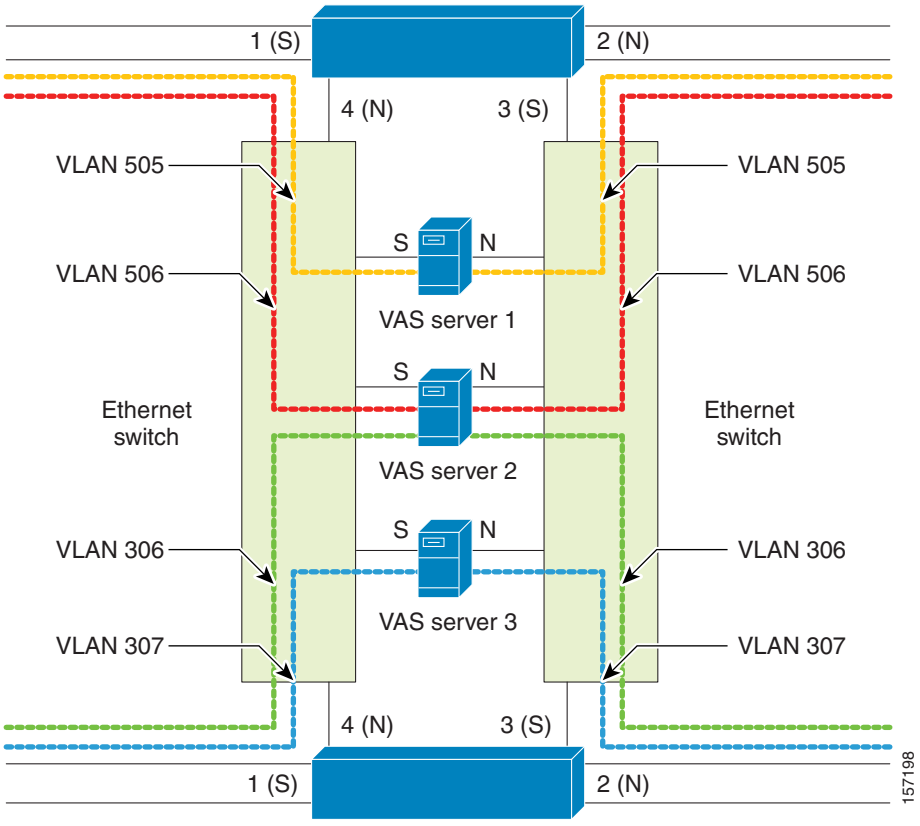
In Figure 14-4, the top Cisco SCE platform forwards traffic to VAS Server 1 and Server 2, while the bottom Cisco SCE platform forwards to VAS Server 2 and Server 3. A unique VLAN tag must designate each Cisco SCE-platform-to-VAS-server path. This topology is illustrated with two Cisco SCE platforms, but a maximum of 512 Cisco SCE platforms is supported (limited by the VLAN tag size).

The two Ethernet switches route the traffic to the VAS servers. The routing is VLAN based. The Ethernet switch should be configured to trunk mode with learning disabled.

The data flow is the same as that for the single Cisco SCE platform to multiple VAS servers topology (see "Data Flow" section on page 14-15).

Note The multiple Cisco SCE platforms to multiple VAS servers topology does not support Cisco SCE platform redundancy on the cascade ports.

Figure 14-4 Multiple Cisco SCE Platforms, Multiple VAS Servers



SNMP Support for VAS

The following items in the "PCUBE-SE-MIB" proprietary MIB support VAS traffic forwarding:

- Cisco SCE-MIB object—vasTrafficForwardingGrp Cisco SCE-MIB
- Object type—vasServersTable provides information on each VAS server operational status.
- SNMP Trap—vasServerOperationalStatusChangeTrap signifies that the agent entity has detected a change in the operational status of a VAS server.

Interactions Between VAS Traffic Forwarding and Other Cisco SCE Platform Features

Incompatible Cisco SCE Platform Features

There are certain Cisco SCE platform features that are incompatible with VAS traffic forwarding. Before enabling VAS traffic forwarding, it is the responsibility of the user to make sure that no incompatible features or modes are configured.

There are certain Cisco SCE platform features that are incompatible with VAS traffic forwarding. Before you enable VAS traffic forwarding, you must ensure that no incompatible features or modes are configured.

The features and modes listed below cannot coexist with VAS mode:

- Line-card connection modes—receive-only, receive-only-cascade, inline-cascade
- Link mode other than forwarding
- All link encapsulation protocols, including VLAN, MPLS, and L2TP
- Traffic mirroring (see "Intelligent Traffic Mirroring" section on page 14-36)

Note If VAS forwarding is enabled, Cisco SCE devices do not forward VLAN-tagged subscriber traffic received from subscriber side and network side traffic ports to the VAS interface for processing.

VAS Traffic Forwarding and DDoS Processing

VAS traffic forwarding has minor effects on the distributed denial of service (DDoS) mechanisms.

Specific IP DDoS Attack Detection

The specific IP DDoS mechanism uses software counters. The second pass VAS packets do not reach the Service Control Operating System (SCOS), so they are not counted twice.

Network-side packets are handled by the attack-detector in the first pass, when they open a flow, so they are also not counted twice.

Specific IP Attack Filter

The behavior depends on the action configured.

- Report only—VAS is not affected.

- Block—Flow is blocked, no VAS service is provided.
- Bypass—Traffic is bypassed and NO SCA BB or VAS services are provided.

VAS Traffic Forwarding and Bandwidth Management

The complexity of the VAS traffic forwarding results in the modification of some Cisco SCE platform bandwidth management capabilities:

- VAS flows are not subject to global bandwidth control.
- The number of global controllers available to regular flows is decreased from 64 to 48.

Global Controllers and VAS Flows

When VAS traffic forwarding is enabled, the global controllers function slightly differently.

- Only 48 global controllers are available.
- Global controllers 49 to 63 are used to count VAS traffic.
- Reserved global controllers cannot be configured.
- VAS flows do not get the global controller from the traffic controller to which they belong. Rather, the global controller is set according to VAS rules.

Configuring VAS Traffic Forwarding

There are three broad aspects to VAS traffic forwarding configuration in the Cisco SCE platform:

- Configuring global VAS traffic forwarding options, such as enabling or disabling VAS traffic forwarding, or specifying the VAS traffic link.
- Configuring a VAS server, such as enabling or disabling a specific VAS server, or enabling or disabling the VAS health check for a specified VAS server.
- Configuring a VAS server group, such as adding or removing a specific VAS server, configuring the minimum number of active servers per group, or configuring VAS server group failure behavior.

Note Additional VAS traffic forwarding configuration and monitoring options are available from the SCA BB Console. See "Managing VAS Settings" section in the *Cisco Service Control Application for Broadband User Guide*.

Following is a high-level description of the steps in configuring VAS traffic forwarding.

1. Configure the Cisco SCE platform— define the servers and the server groups, configure pseudo IP for the traffic interfaces used for VAS traffic, and enable VAS mode.
2. Verify the state of the individual VAS servers as well as that of the VAS server groups to make sure all are **Up** (see "Monitoring VAS Traffic Forwarding" section on page 14-32).
3. Configure which traffic goes to which server group using the SCA BB console (see "Configuring VAS Traffic Forwarding from the SCA BB Console" section on page 14-21).

This section contains the following information on configuring VAS traffic forwarding:

Configuring VAS Traffic Forwarding from the SCA BB Console

Configuration of the VAS Traffic Forwarding solution is distributed between the SCA BB console and the Cisco SCE platform CLI:

- The Cisco SCE platform CLI configuration:
  - Physical VAS server parameters—VLAN tag, Admin status and health check parameters
  - VAS server groups parameters—the VAS servers that belong to the group and the action to take if the group enters a failure state
- SCA BB console configuration—the traffic forwarding rules, meaning which portion of the subscriber traffic should be forwarded to the VAS servers.

  This configuration is defined per package so different subscribers can receive different VAS service, based on the package they bought.

Global Options

There are two global VAS traffic forwarding options:

- Enable or disable VAS traffic forwarding
- Configure the link number on which to transmit VAS traffic (necessary only if the VAS servers are connected on Link 0, rather than Link 1, which is the default VAS traffic link))

Enabling VAS Traffic Forwarding

By default, VAS traffic forwarding is disabled. If VAS traffic forwarding is required, you must enable it both from your Cisco SCE device and the SCABB console.

For instructions on how to disable VAS traffic forwarding, see "Disabling VAS Traffic Forwarding" section on page 14-22.

There are certain other Cisco SCE platform features that are incompatible with VAS traffic forwarding. Before enabling VAS traffic forwarding, make sure that no incompatible features or modes are configured.

The features and modes listed below cannot coexist with VAS mode:

- Line-card connection modes—receive-only, receive-only-cascade, inline-cascade
- Link mode other than forwarding
- All link encapsulation protocols, including VLAN, MPLS, L2TP
- Enhanced open flow mode

Options

The following options are available:

- **Enable/disable—**Enable or disable VAS traffic forwarding
  - Default—Disable

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding	Enables VAS traffic forwarding.

Disabling VAS Traffic Forwarding

Disabling the VAS Traffic Forwarding feature in runtime must be done with special care. There are two points to consider:

- You cannot disable VAS mode in the Cisco SCE platform while the applied SCA BB policy instructs the Cisco SCE platform to forward traffic to the VAS servers.

  Therefore, you must dismiss all VAS Traffic forwarding rules in the applied SCA BB policy before disabling the VAS traffic forwarding in the Cisco SCE platform.

- After the SCA BB has been reconfigured, there may still be some open flows that have already been forwarded to the VAS servers. If the VAS feature is stopped while there are still such flows open, their packets coming back from the VAS servers may be routed to their original destination with the VLAN tag of the VAS server on it.

  Therefore, it is also highly recommended to shutdown the line card before you disable the VAS traffic forwarding in the Cisco SCE platform to avoid inconsistency with flows that were already forwarded to the VAS servers.

Step 1 From the SCA BB console, remove all the VAS table associations to packages and apply the changed policy.

Step 2 From the SCE(config if)# prompt, type **shutdown** and press **Enter**.

Shuts down the line card.

Step 3 From the SCE(config if)# prompt, type **no VAS-traffic-forwarding** and press **Enter**.

Disables VAS traffic forwarding.

Step 4 From the SCE(config if)# prompt, type **no shutdown** and press **Enter**.

Re-enables the line card.

Configuring the VAS Traffic Link

By default, the VAS traffic is transmitted on Link 1. If the VAS servers are connected on Link 0, you must configure the VAS traffic link to Link 0.

Note The VAS traffic link should be in Forwarding mode.

Options

The following option is available:

- **VAS traffic-link {link-0|link-1}—**The link number on which to transmit VAS traffic
  - Default—Link 1

How to Select the Link for VAS Traffic

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding traffic-link {link-0|link-1}	Selects the link for VAS traffic.

How to Revert to the Default Link for VAS Traffic

From the SCE(config if)# prompt, type:

Command	Purpose
no VAS-traffic-forwarding traffic-link	Reverts the default link for VAS traffic.

Configuring a VAS Server

You must define the VAS servers. Each VAS server has the following parameters:

- Admin-mode—Enabled or disabled.
- Health check mode—Enabled or disabled
- Health check ports
- VLAN tag

Use the commands in this section to perform these operations for individual VAS servers:

- Enable a specified VAS server
- Disable a specified VAS server
- Define the VLAN tag for a specified VAS server
- Enable or disable the health check for a VAS server
- Define the source and destination ports to use for the health check.
- Delete all properties for a specified VAS server. The server returns to the default state, which is enabled. However, it is not operational since it does not have VLAN.

Note A VAS server is not operational until the VLAN tag is defined, even if the server itself is enabled.

Options

The following option is available:

- **number**—The number of the VAS server.

How to Enable a VAS Server

Note The server is not operational until a VLAN tag has also been defined

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding VAS server-id *number* **enable**	Enables VAS server.

How to Disable a VAS Server

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding VAS server-id *number* **disable**	Disables VAS server.

How to Restore all VAS Server Properties to Default

From the SCE(config if)# prompt, type:

Command	Purpose
no VAS-traffic-forwarding VAS server-id *number*	Restores all VAS server properties to default.

Assigning a VLAN ID to a VAS Server

This section contains the following topics:

Options

The following options are available:

- **number**—The number of the VAS server.
- **vlan-id**—The VLAN tag to use for the specified VAS server

  The VLAN tag can be redefined as necessary.
  - Default—No VLAN.

Note the following important points:

- The VAS server is not operational until the VLAN tag is defined.
- Disabling the server does not remove the VLAN tag number configured to the server.
- The **no** form of the command (same as the **default** form of the command), removes the previously configured VLAN tag (no VLAN is the default configuration).

How to Configure the VLAN Tag Number for a Specified VAS Server

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding VAS server-id *number* **VLAN** *vlan-id*	Configures the VLAN tag number for a specified VAS server.

How to Remove the VLAN Tag Number from a Specified VAS Server

From the SCE(config if)# prompt, type:

Commands	Purpose
no VAS-traffic-forwarding VAS server-id *number* **VLAN**	Removes the VLAN tag number from a specified VAS server.
default VAS-traffic-forwarding VAS server-id *number* **VLAN**	You can also use the default form of the command to remove the VLAN tag configuration.

Configuring the Health Check

This section explains how to to enable and disable the Health Check, and how to define the ports it should use.

By default, the VAS server health check is enabled, however you may disable it.

The health check will be activated only if all the following conditions are true. If the health check is enabled, the server state will be **Down** if one or more conditions are not met:

- VAS traffic forwarding mode is enabled.
- Pseudo IPs are configured for the Cisco SCE platform traffic ports on the VAS traffic link.
- VAS server is enabled.
- Server has a VLAN tag.
- Health check for the server is enabled.

If the health check of the server is disabled, its operational status depends on the following (requirements for **Up** state are in parentheses):

- admin status (enable)
- VLAN tag configuration (VLAN tag defined)
- group mapping (assigned to group)

This section contains the following topics:

- How to Enable VAS Server Health Check, page 14-26
- How to Disable VAS Server Health Check, page 14-27
- How to Define the UDP Ports to be Used for Health Check, page 14-27
- How to Remove the UDP Ports Configuration, page 14-27
- Configuring Pseudo IP Addresses for the Health Check Packets, page 14-27

Options

The following options are available:

- **number—**The ID number of the VAS server for which to enable or disable the health check
- **Enable/disable—**Enable or disable VAS server health check
  - Default—Enable
- **UDP ports—**Specify the UDP ports to be used for the health check:
  - **source portnumber—**Health check source port number
  - **destination portnumber—**Health check destination port number
  - Default—<63140,63141>used for server #0 through <63154,63155>used for server #7.

How to Enable VAS Server Health Check

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding VAS server-id *number* **health-check**	Enables VAS server health check.

How to Disable VAS Server Health Check

From the SCE(config if)# prompt, type:

Command	Purpose
no VAS-traffic-forwarding VAS server-id *number* **health-check**	Disables the VAS server health check.

How to Define the UDP Ports to be Used for Health Check

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding VAS server-id *number* **health-check UDP ports source** *portnumber* **destination** *portnumber*	Defines the UDP ports to be used for health check.

How to Remove the UDP Ports Configuration

From the SCE(config if)# prompt, type:

Commands	Purpose
no VAS-traffic-forwarding VAS server-id *number* **health-check UDP ports**	Removes UDP ports configuration.
VAS-traffic-forwarding VAS server-id *number* **health-check UDP ports**	You can also use the default form of the command to remove the UDP port configuration.

Configuring Pseudo IP Addresses for the Health Check Packets

You should configure source and destination pseudo IP address for the health check packets. The **pseudo-ip** command allows you to specify a unique IP address to be used by the health check packets.

The pseudo IP address is configured on the interfaces that connect the Cisco SCE platform with the VAS servers.

The Cisco SCE platform uses the pseudo IP as follows:

- Pseudo IP configured for the subscriber side interface:
  - Source IP address for health check packets going in the Upstream direction
  - Destination IP address for health check packets going in the Downstream direction
- Pseudo IP configured for the network side interface:
  - Source IP address for health check packets going in the Downstream direction
  - Destination IP address for health check packets going in the Upstream direction

Note This command is a ROOT level command in the Gigabit Interface Configuration mode.

Options

The following options are available:

- **ip-address**—IP address to be used (any IP address as long as it is not possible to be found in the network traffic, such as a private IP)
  - Default—no IP address
- **mask** (optional)—Defines the range of IP addresses that can be used by the Cisco SCE platform. Note that the Cisco SCE platform is not required to reside in this subnet.
  - Default—255.255.255.255 (The subnet mask can be set to 255.255.255.255, as the health check mechanism requires only one IP address per interface.)

How to Define the Pseudo IP Address

Use this command to define the pseudo IP address to be used for the health check.

From the SCE(config if)#>prompt, type:

Command	Purpose
pseudo-ip *ip-address [mask]*	Defines the pseudo IP address.

How to Delete the Pseudo IP Address

From the SCE(config if)#>prompt, type:

Command	Purpose
no pseudo-ip *ip-address [mask]*	Deletes the pseudo IP address.

Configuring a VAS Server Group

You may define up to eight VAS server groups. Each VAS server group has the following parameters:

- Server Group ID
- A list of VAS servers attached to this group.
- Failure detection—minimum number of active servers required for this group so it will be considered to be Active. If the number of active servers goes below this minimum, the group will be in Failure state.
- Failure action—action performed on all new data flows that should be mapped to this Server Group while it is in Failure state.

  Options:
  - block
  - pass

You can perform these operations for a VAS server group:

- Add a VAS server to or remove a VAS server from a specified group.
- Configure the minimum number of active servers for a specified group.
- Configure failure behavior for a specified group.

Adding and Removing Servers

Options

The following options are available:

- **group-number—**The ID number of the VAS server group
- **id-number—**The ID number of the VAS server

How to Add a VAS Server to a Specified VAS Server Group

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding VAS server-group *group-number* **server-id** *id-number*	Adds a VAS server to a specified VAS server group.

How to Remove a VAS Server from a Specified VAS Server Group

From the SCE(config if)# prompt, type:

Command	Purpose
no VAS-traffic-forwarding VAS server-group *group-number* **server-id** *id-number*	Removes a VAS server from a specified VAS server group.

How to Remove all VAS Servers from a Specified VAS Server Group

Use this command to remove all VAS servers from a specified VAS server group and set all group parameters to the default value.

From the SCE(config if)# prompt, type:

Command	Purpose
no VAS-traffic-forwarding VAS server-group *group-number*	Removes all VAS servers from a specified VAS server group.

Configuring VAS Server Group Failure Parameters

You can configure these failure parameters for a specified VAS server group:

- Minimum number of active servers—If the number of active servers in the server group goes below this number, the group will be in Failure state
- Failure action—The action to be applied to all new flows mapped to this server group while it is Failure state:
  - Block—all new flows assigned to the failed VAS server group will be blocked by the Cisco SCE platform.
  - Pass—all new flows assigned to the failed VAS server group will be considered as regular non-VAS flows, and will be processed without VAS service.

Options

The following options are available:

- **group-number**—The ID number of the VAS server group
- minimum-active-servers **min-number**—The minimum number of active servers required for the specified server group
  - Default—1
- **failure action**—Which of the following actions will be applied to all new flows for the specified server group:
  - **block**
  - **pass** (default)

How to Configure the Minimum Number of Active Servers for a Specified VAS Server Group

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding VAS server-group *group-number* **failure minimum-active-servers** *min-number*	Configures the minimum number of active servers for a specified VAS server group.

How to Reset the Minimum Number of Active Servers for a Specified VAS Server Group to the Default

From the SCE(config if)# prompt, type:

Command	Purpose
default VAS-traffic-forwarding VAS server-group *group-number* **failure minimum-active-servers** *min-number*	Resets the minimum number of active servers for a specified VAS server group to the default.

How to Configure the Failure Action for a Specified VAS Server Group

From the SCE(config if)# prompt, type:

Command	Purpose
VAS-traffic-forwarding VAS server-group *group-number* **failure action {block | pass}**	Configures the failure action for a specified VAS server group.

How to Configure the Failure Action for a Specified VAS Server Group to the Default

From the SCE(config if)# prompt, type:

Command	Purpose
default VAS-traffic-forwarding VAS server-group *group-number* **failure action**	Configures the failure action for a specified VAS server group to the default.

VAS Configuration Example

	Command	Purpose
Step 1	enable 15	Access root level to configure the pseudo IP address
Step 2	**configure** **interface range TenGigabitEthernet 3/0-1/0**	Enter Ten Gigabit Ethernet Interface configuration mode for the relevant range of 10GBE interfaces.
Step 3	**pseudo-ip** *1.1.1.1 255.255.255.252*	Configure the pseudo IP address for the health check.
Step 4	exit **interface linecard 0**	Enter Interface Linecard configuration mode
Step 5	**shutdown**	You must shutdown the linecard when configuring VAS servers and groups.
Step 6	**VAS-traffic-forwarding**	Set the Cisco SCE platform to forward VAS traffic (enable VAS traffic forwarding).
Step 7	**VAS-traffic-forwarding traffic-link** *link-0*	Set the VAS traffic forwarding link to Link 0.
Step 8	**VAS-traffic-forwarding VAS server-id** *0* **VLAN** *600* **VAS-traffic-forwarding VAS server-id** *1* **VLAN** *601* **VAS-traffic-forwarding VAS server-id** *2* **VLAN** *602*	Assign VAS servers 0-2 to VLAN 600- 602 respectively.
Step 9	**VAS-traffic-forwarding VAS server-group** *0* **server-id** *0* **VAS-traffic-forwarding VAS server-group** *0* **server-id** *1* **VAS-traffic-forwarding VAS server-group** *0* **server-id** *2*	Map VAS servers to server group 0, allowing server redundancy within the group.
Step 10	**VAS-traffic-forwarding VAS server-id** *0* **health-check UDP ports source** *63154* **destination** *63155* **VAS-traffic-forwarding VAS server-id** *1* **health-check UDP ports source** *63156* **destination** *63157* **VAS-traffic-forwarding VAS server-id** *2* **health-check UDP ports source** *63158* **destination** *63159*	Define UDP ports for health check on VAS servers.
Step 11	**VAS-traffic-forwarding VAS server-group** *0* **failure minimum-active-servers** *2*	Configure the minimum number of servers required (2).
Step 12	**VAS-traffic-forwarding VAS server-group** *0* **failure action block**	Configure the failure action to ‘block’.
Step 13	**no shutdown**	Restart the linecard.

Monitoring VAS Traffic Forwarding

Use the commands in this section to display the following information for VAS configuration and operational status summary.

- Global VAS status summary—VAS mode, the traffic link used
- VAS Server Groups information summary—operational status, number of configured servers, number of current active servers.

This information may be displayed for a specific server group or all server groups

- VAS servers information summary—operational status, Health Check operational status, number of subscribers attached to this server.

This information may be displayed for a specific server or all servers

- VAS health check counters

The following sample outputs are included.

- How to Display Global VAS Status and Configuration, page 14-32
- How to Display Operational and Configuration Information for a Specific VAS Server Group, page 14-33
- How to Display Operational and Configuration Information for All VAS Server Groups, page 14-33
- How to Display Operational and Configuration Information for a Specific VAS Server, page 14-33
- How to Display Operational and Configuration Information for All VAS Servers, page 14-34
- How to Display the VAS Servers Used by a Specified Subscriber, page 14-34
- How to Display Health Check Counters for All VAS Servers, page 14-35
- How to Clear the Health Check Counters for a Specified VAS Server, page 14-35
- How to Clear the Health Check Counters for All VAS Servers, page 14-35

How to Display Global VAS Status and Configuration

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 VAS-traffic-forwarding	Displays the global VAS status and configuration.

Example

```
SCE>show interface linecard 0 VAS-traffic-forwarding
VAS traffic forwarding is enabled
VAS traffic link configured: Link-1  actual: Link-1
```

How to Display Operational and Configuration Information for a Specific VAS Server Group

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 VAS-traffic-forwarding VAS server-group *id-number*	Displays operational and configuration information for a specific VAS server group.

Example

```
SCE>show interface linecard 0 VAS-traffic-forwarding VAS server-group 0
VAS server group 0:
State: Failure  configured servers: 0   active servers: 0
minimum active servers required for Active state: 1   failure action: Pass
```

How to Display Operational and Configuration Information for All VAS Server Groups

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 VAS-traffic-forwarding VAS server-group all	Displays operational and configuration information for all VAS server groups.

How to Display Operational and Configuration Information for a Specific VAS Server

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 VAS-traffic-forwarding VAS server-id *id-number*	Displays operational and configuration information for a specific VAS server.

Example

```
SCE>show interface linecard 0 VAS-traffic-forwarding VAS server-id 0
VAS server 0:
Configured mode: enable   actual mode: enable   VLAN:  520  server group:    3
State: UP
Health Check configured mode: enable  status: running
Health Check source port: 63140  destination port: 63141
Number of subscribers:       0
```

How to Display Operational and Configuration Information for All VAS Servers

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 VAS-traffic-forwarding VAS server-id all	Displays operational and configuration information for all VAS servers.

How to Display the VAS Servers Used by a Specified Subscriber

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 subscriber name *subscriber-name* **VAS-servers**	Displays the VAS servers used by a specified subscriber.

How to Display Health Check Counters for a Specified VAS Server

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 VAS-traffic-forwarding VAS server-id *id-number* **counters health-check**	Displays health check counters for a specified VAS server.

Example

```
SCE>show interface linecard 0 VAS-traffic-forwarding VAS server-id 0
Health Checks statistics for VAS server '0'    Upstream      Downstream
-------------------------------------------------------------------------
Flow Index '0'
-----------------
Total packets sent                          :       31028  :       31027 :
Total packets received                      :       31028  :       31027 :
Good packets received                       :       31028  :       31027 :
Error packets received                      :           0  :           0 :
Not handled packets                         :           0  :           0 :
Average roundtrip (in millisecond)          :           0  :           0 :
Error packets details                       :              :             :
--------------------                        :              :             :
Reordered packets                           :           0  :           0 :
Bad Length packets                          :           0  :           0 :
IP Checksum error packets                   :           0  :           0 :
L4 Checksum error packets                   :           0  :           0 :
L7 Checksum error packets                   :           0  :           0 :
Bad VLAN tag packets                        :           0  :           0 :
Bad Device ID packets                       :           0  :           0 :
Bad Server ID packets                       :           0  :           0 :
```

How to Display Health Check Counters for All VAS Servers

From the SCE> prompt, type:

Command	Purpose
show interface linecard 0 VAS-traffic-forwarding VAS server-id all counters health-check	Displays health check counters for all VAS servers.

How to Clear the Health Check Counters for a Specified VAS Server

From the SCE> prompt, type:

Command	Purpose
clear interface linecard 0 VAS-traffic-forwarding VAS server-id *id-number* **counters health-check**	Clears the health check counters for a specified VAS server.

How to Clear the Health Check Counters for All VAS Servers

From the SCE> prompt, type:

Command	Purpose
clear interface linecard 0 VAS-traffic-forwarding VAS server-id all counters health-check	Clears health check counters for all VAS servers.

Intelligent Traffic Mirroring

Traffic mirroring is a Cisco SCE platform capability that complements the range of services provided by the SCA BB solution. It copies a specified portion of the traffic streams and sends this copy to third-party servers who do offline analysis.

The criteria for traffic mirroring is based on Layer 7 attributes and subscriber awareness. This fine granularity, along with load sharing capability for servers providing the same service, substantially reduces the number of solution components.

The traffic that is copied is also processed by the SCA BB application and forwarded without interruption to its original destination. The copy of the traffic is presumed not to return to the Cisco SCE platform after being processed by the third party servers.

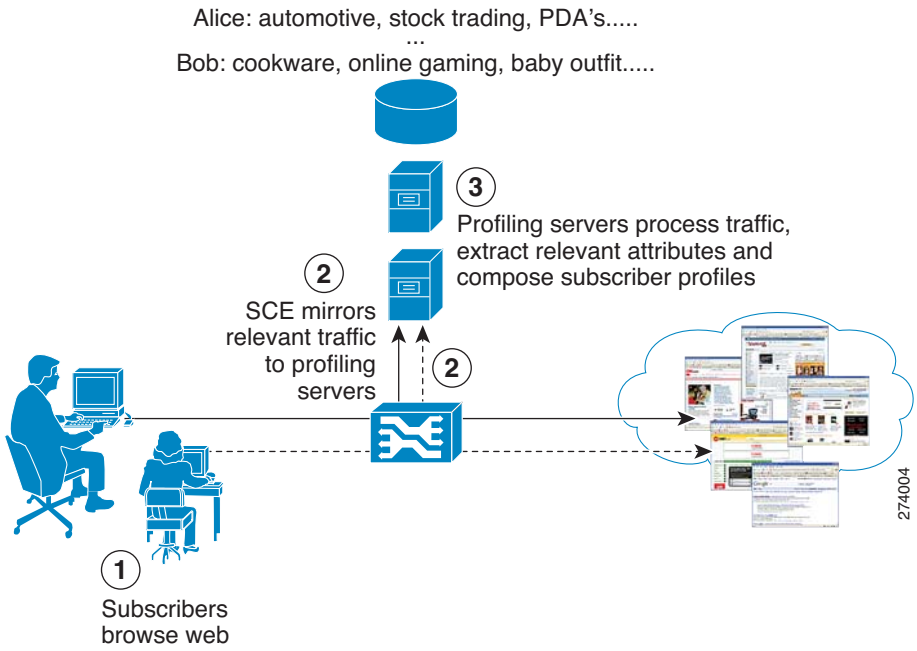
Using Traffic Mirroring for Behavioral Targeting

Today Internet advertising is being executed by content providers (or publishers) in collaboration with ad networks, which actually handle the syndication of ads from advertisers to web sites. The Cisco Service Control behavioral targeting solution provides the means for service providers to participate in the business of the online advertising. This solution allows the SPs to leverage their information about the subscribers and enables highly targeted advertising.

Based on Deep Packet Inspection (DPI) and subscriber integration, the Cisco SCE 8000 platform filters out only what is relevant for the subscriber profiling. This greatly conserves the resources of the advertising servers, by eliminating the irrelevant web traffic before it even reaches them. This filtered traffic is processed as usual by the SCA BB application along with the rest of the traffic, but in addition a copy of it is passed to an external device which can do offline analysis on the subscriber behavior. The data can then be used for the targeted advertising.

Behavioral Targeting is accomplished using several Cisco SCE platform capabilities. This section describes the intelligent traffic mirroring capability, which is one of the features that enable the solution.

Figure 14-5 High Level Overview of an Mirroring-based Behavioral Targeting Solution



For more information regarding targeted advertising, see the following documents:

- *Cisco Service Control Online Advertising Solution Guide: Behavioral Profile Creation Using RDRs*
- *Cisco Service Control Online Advertising Solution Guide: Behavioral Profile Creation Using Traffic Mirroring*

How Traffic Mirroring Works

Traffic mirroring uses the same capabilities as VAS traffic forwarding, but the traffic does not return to the Cisco SCE platform.

The following sections explain how traffic mirroring works:

Traffic Mirroring and SCA BB

When traffic mirroring is configured for a certain type of traffic, in addition to all its basic functions, the SCA BB application decides whether each flow is to be mirrored or not, based on L7 classification.

Traffic mirroring rules are configured through the SCA BB console. These rules map the traffic to be mirrored and analyzed to the VAS server groups. When a flow is marked for traffic mirroring, the VAS server group for this flow is selected. If the group includes more than one VAS server, traffic will be forwarded in such a way that the subscriber load is shared between the servers on the same group.

The mapping of traffic portions to VAS server groups is done through the standard SCA BB GUI, this definition is given per package.

Mirroring Termination

Mirroring of a flow can continue until the flow is terminated, or be limited to a certain volume passed over the flow. This enables a huge data reduction on the server side, as well as performance saving in the Cisco SCE platform.

An RST packet is sent to the server when the mirroring is stopped due to a stop condition. This is done in order to signal the server that the mirroring has stopped.

The RST packet is sent in the direction of intiator to initatee with the additional VLAN tag.

Mirroring Exceptions

Since the decision to mirror is based on service classification, which can be done on the first payload or after first few packets, the entire TCP handshake is not mirrored.

To save in performance on both sides, zero payload packets are also not mirrored. (note that this type of packets have no real value for offline analysis).

If the VLAN traffic is mirrored, Cisco SCE devices replace the VLAN information from the incoming traffic with the VAS-configured VLAN information before mirroring the traffic on the VAS port.

Mirroring the TCP-Segmented HTTP GET Packets

From Cisco SCE Release 3.7.5, traffic mirroring can be enabled for all the TCP-segmented HTTP GET packets if the HTTP port is 80, 8080, or 8081 even if the number of segmented packets are more than two.

By default, mirroring of all the segmented packets is disabled.

Configuring Cisco SCE to Mirror the TCP-Segmented HTTP GET packets

You can configure Cisco SCE to mirror the TCP-segmented HTTP GET packets using the GT_SEG_GET_MIRROR tunable.

To configure Cisco SCE to mirror the TCP segmented HTTP GET packets, from the SCE(config if)# prompt, enter:

Command	Purpose
tunable GT_SEG_GET_MIRROR value true	Enables the mirroring of all the TCP-segmented HTTP GET packets.
tunable GT_SEG_GET_MIRROR value false	Disables the mirroring of all the TCP-segmented HTTP GET packets.

Cisco SCE Connectivity

Traffic mirroring is implemented by sending the mirrored packets over a designated VLAN through a predefined link of the Cisco SCE platform. The link that has been defined for traffic mirroring can be either used exclusively for this purpose, or it can be one of the traffic ports, in which case the Tx capacity of the link will be shared between the original egress traffic and the mirrored traffic.

The direction of the flow is preserved when mirrored, so traffic that is received on the subscriber interface on either link is sent over a VLAN on the network interface over this predefined link. And traffic that is received on the network interface on either link is sent over a VLAN on the subscriber interface over this predefined link. The mirrored traffic does not return to the Cisco SCE platform.

Note Enabling traffic mirroring is expected to impact the Cisco SCE performance due to the excessive processing associated with it; the actual figure depending on the amount of the mirrored traffic. It is recommended that you monitor Cisco SCE platform performance when enabling this capability.

Figure 14-6 shows a Cisco SCE platform using a dedicated link for mirroring (Link 1).

Figure 14-6 Traffic Mirroring on a Dedicated Link

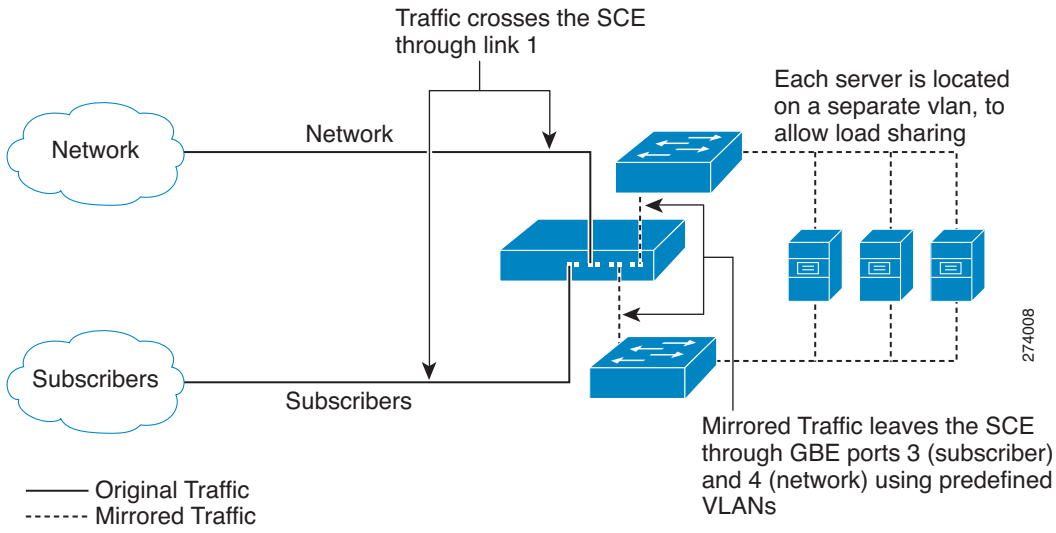
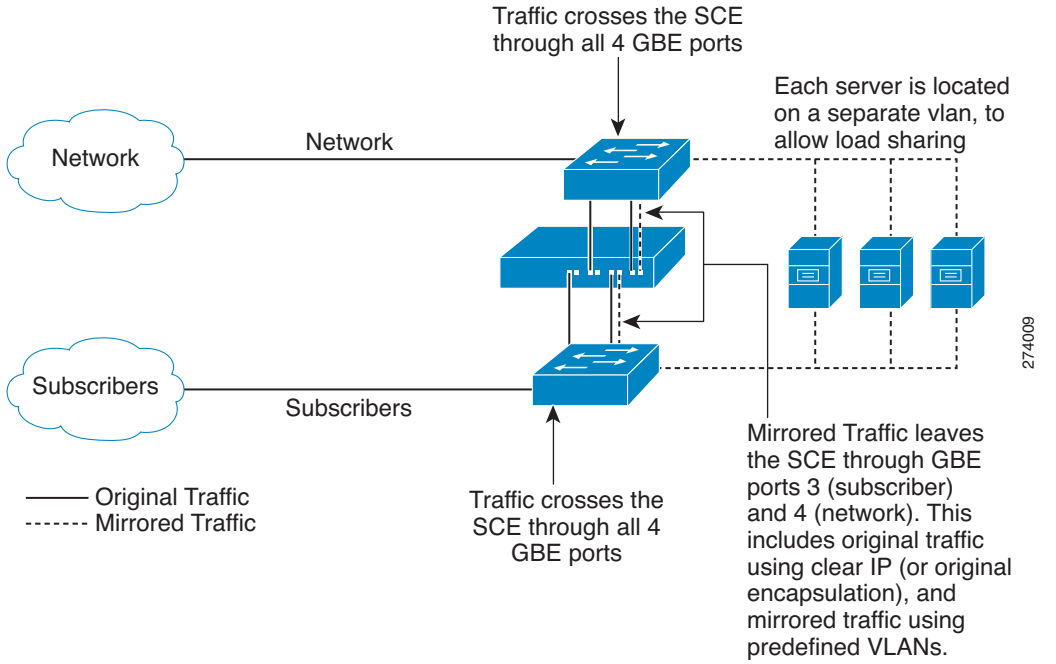


Figure 14-7 shows a Cisco SCE platform using traffic ports for mirroring.

Figure 14-7 Traffic Mirroring over Traffic Ports



Traffic Mirroring and Bandwidth Management

In general, the bandwidth management rules to be applied to flows designated for mirroring are not affected by the mirroring decision. However note the following points:

- Bandwidth enforcement applies on the two copies of the flow as if there was only one copy; that is, if the flow should be limited to 50K, then its original copy which is sent to the original destination is limited to 50K, and the copy that is sent to the VAS server is also limited to 50K. This has no effect on the total volume that should be mirrored.
- The mirrored volume is not counted and accounted in the BWM system, and therefore in cases where the mirrored traffic is congesting the link, the system will not be aware of the link congestion and will not know to shrink the BWC.

Configuring Traffic Mirroring

Following is a high-level description of the steps in configuring traffic mirroring.

1. Configure the Cisco SCE platform— define the servers and the server groups
2. Configure which traffic goes to which server group using the SCA BB console.

Note Additional traffic mirroring configuration and monitoring options are available from the SCA BB Console. See the *Cisco Service Control Application for Broadband User Guide*.

Note Traffic mirroring is not compatible with regular VAS traffic forwarding.

Traffic mirroring configuration is distributed between the SCA BB console and the Cisco SCE platform CLI:

- The Cisco SCE platform CLI configuration:

  There are three broad aspects to traffic mirroring configuration in the Cisco SCE platform:

  - Configuring the VAS traffic link.
  - Configuring the VLAN tag per VAS server.
  - Associating servers with server groups.

  The health check is not relevant to traffic mirroring, so there is no need to configure anything related to the VAS health check.

- SCA BB console configuration—Configure the traffic mirroring rules, specifying which portion of the subscriber traffic should be mirrored to the VAS servers.

  This configuration is defined per package so different subscribers can receive different mirroring service, based on the package they bought.

Monitoring Traffic Mirroring

Use the same commands to monitor traffic mirroring as for regular VAS functionality. (See "Monitoring VAS Traffic Forwarding" section on page 14-32)

Traffic Mirroring Sample Configuration

Following is a sample illustrating the steps in configuring the Cisco SCE 8000 platform for traffic mirroring.

	Command	Purpose
Step 1	**configure** **interface LineCard 0**	Enters LineCard Interface configuration mode
Step 2	**VAS-traffic-forwarding VAS server-id** *0* **VLAN** *640* **VAS-traffic-forwarding VAS server-id** *1* **VLAN** *641* **VAS-traffic-forwarding VAS server-id** *2* **VLAN** *642* **VAS-traffic-forwarding VAS server-id** *3* **VLAN** *643*	Assign VAS servers 0-3 to VLAN 640-643 respectively.
Step 3	**VAS-traffic-forwarding VAS server-group** *0* **server-id** *0* **VAS-traffic-forwarding VAS server-group** *0* **server-id** *1* **VAS-traffic-forwarding VAS server-group** *1* **server-id** *2* **VAS-traffic-forwarding VAS server-group** *1* ***server-id*** 3	Map VAS servers 0-1 and 2-3 to server groups 0 and 1 respectively, allowing server redundancy within each group.