Ethernet Routing Switch
4500, 5500, 5600
Engineering

# Private VLAN Edge Technical Configuration Guide

Avaya Data Solutions
Document Date: July 2010
Document Number: NN48500-592
Document Version: 1.1

**Notices**
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

**Documentation disclaimer**
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

**Link disclaimer**
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

**Warranty**
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

**Licenses**
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

**Copyright**
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Third Party Components**
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

**Trademarks**
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

**Downloading documents**
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support.

**Contact Avaya Support**
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support.

# Abstract

This Technical Configuration Guide illustrates the configurations necessary for the Private VLAN Edge functionality on the Ethernet Routing Switches. The use of the Secure Router is also included for a specific scenario.

# Table of Contents

# Document Updates

July 2010

# Conventions

This section describes the text, image, and command conventions used in this document.

### Symbols:

Tip – Highlights a configuration or technical tip.

Note – Highlights important information to the reader.

Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

### Text:

**Bold** text indicates emphasis.

***Italic*** text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

ERS5520-48T# ***show running-config***

Output examples from Avaya devices are displayed in a Lucinda Console font:

ERS5520-48T# ***show running-config***

```
! Embedded ASCII Configuration Generator Script
! Model = Ethernet Routing Switch 5520-24T-PWR
! Software version = v5.0.0.011
enable
configure terminal
```

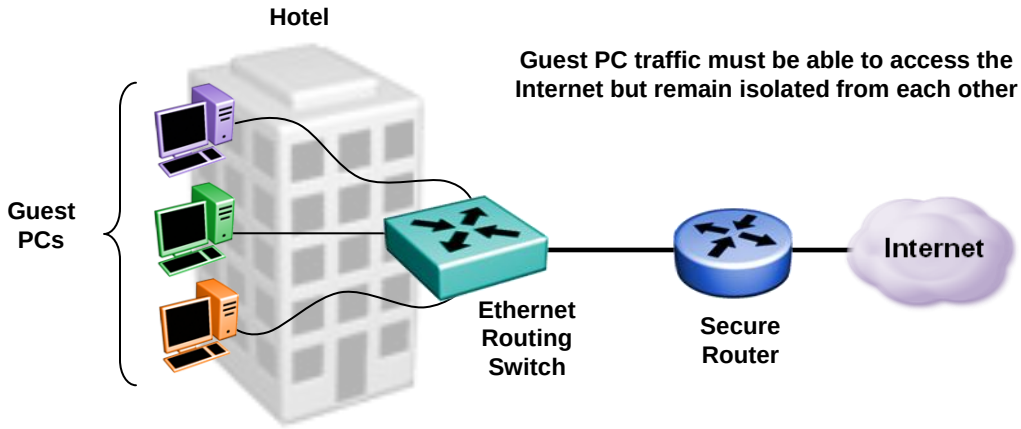
# 1. Private VLAN Edge

One of the challenges that face many enterprise customers is the ability to ensure traffic separation at the edge of the network. That is, the multiple end-users should not be able to communicate with one another without having to pass through a firewall. On the Ethernet edge switch this is especially a concern given that different end users may be connected to different ports on the same switch. Thus, the Ethernet edge switch must be configured such that the various hosts are isolated from one another.

One way to do this is to configure the Ethernet edge switch such that the group of ports for a given set of users are in a unique VLAN. This method provides the desired security and isolation; however, as the total number of users increases so do the total number of VLANs. This may place higher demands on the scalability requirements of the downstream Ethernet aggregation switch.

A simple and elegant solution is to use Private VLANs which provide end user and server separation in a Layer 2 (L2) broadcast domain by forcing all unicast and broadcast traffic to be forwarded only to a specific egress port. In a L2 domain, private VLANs prevent end users or servers from communicating with each other, while at the same time, allowing traffic to be forwarded via a specific egress port.

A common requirement for Private VLANs exist in hotel applications where guest room traffic must be separated from each other and forwarded only via the switch uplink port for internet access.




The private VLAN edge is a feature available on the Ethernet Routing Switch 5000 and Ethernet Routing Switch 4500 series of switches and can be enabled by configuring a policy.

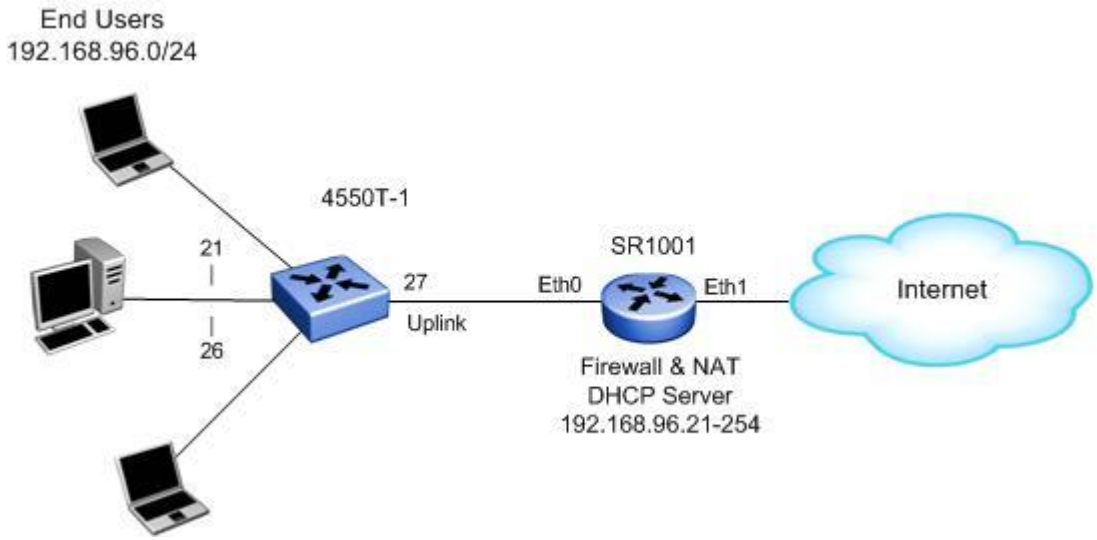
Please note the policy that is used for Private VLAN Edge can only force all traffic to one egress port. Thus, the policy cannot be applied to either a Multilink Trunking (MLT) or LACP group with two or more port members. However, on a 5000 series SMLT Switch Cluster, it could be applied on a Single Link Trunk (SLT) port member.

# 2. Configuration Example

## 2.1 Private VLAN Example for Internet Access using an Avaya Ethernet Routing Switch 4500 Series

The following configuration example details the configuration of an Ethernet Routing Switch 4550T-PWR (4550T-1) for Private VLAN Edge in a L2 broadcast domain. After proper configuration, all end-user traffic, both unicast and non-unicast, from ports 21 through 26 will be forwarded only to port 27 where the Secure Router is connected. The Secure Router will provide DHCP, firewall, and NAT/PAT services.

Note that any ERS 4500 or 5000 series Ethernet Routing Switch can be used in this scenario.




For this example:

- Configure 4550T-1 as follows:
  - Add data VLAN 1000 with port members 21 to 27
  - Add a policy with an Interface action extension to force all traffic from ports 21 to 26 to uplink port 27
  - All ports are untagged
- Configure Secure Router 1001 as follows:
  - Add a DHCP scope (192.168.96.21-254) for the end users
  - Enable PAT between Eth0 and Eth1 using the internal firewall

In this example, the Secure Router is configured with Firewall to perform NAT/PAT functionality. The Secure Router in this case will not forward traffic between the end users. If you are using a router without firewall capability, it is suggested to add a filter on the router to drop traffic on the local end user subnet to prevent the users from communicating with each other via the router. For example, if using the local subnet as illustrated in the drawing above, create a filter on the router to drop traffic with a destination address of 192.168.96.0/24 applied to interface Eth0.

### 2.1.1 Configuration – 4550T-1

#### 2.1.1.1 Go to configuration mode

**4550T-1 Step 1 - Enter configuration mode**

```
4550T-PWR> enable
4550T-PWR# cmd cli
4550T-PWR# configure terminal
4550T-PWR(config)# banner disable
4550T-PWR(config)# snmp-server name 4550-1
```

#### 2.1.1.2 Create the VLAN

**4550T-1 Step 1 – Change the VLAN configuration control mode from default setting of strict to automatic; this will automatically add the PVID to the VLAN port member**

```
4550T-1(config)# vlan configcontrol automatic
```

**4550T-1 Step 2 – Add VLAN 1000**

```
4550T-1(config)# vlan create 1000 name vlan1000_pri_v type port
```

**4550T-1 Step 3 – Add port members**

```
4550T-1(config)# vlan members add 1000 21-27
```

Add a policy to forward all traffic to port 27

**4550T-1 Step 1 – Create a new interface group with a class of unrestricted and add only the access port members**

```
4550T-1(config)# qos if-group name pri_vlan class unrestricted
4550T-1(config)# qos if-assign port 21-26 name pri_vlan
```

**4550T-1 Step 2 – Configure a new action extension and action with the uplink port member (port 27 as used in our example) which in turn will be used when we configure the QoS policy. Please note that you must start with action number 10 or higher as the first 9 actions are already used. The various actions be viewed by entering the *show qos action* CLI command**

```
4550T-1(config)# qos if-action-extension 1 name fwd_port_27 egress-ucast 27 egress-non-ucast 27
4550T-1(config)# qos action 10 name fwd_27 drop-action disable action-ext 1
```

| **4550T-1 Step 3 – Configure a Layer-2 classifier and classifier element to select all ingress traffic** |
|---|
| 4550T-1(config)# ***qos l2-element 1*** |
| 4550T-1(config)# ***qos classifier 1 set-id 1 name all_traffic element-type l2 element-id 1*** |
| **4550T-1 Step 4 – Add a policy and apply the QoS action to the interface group configured above for all the access port members** |
| 4550T-1(config)# ***qos policy 1 name fwd_port_27 if-group pri_vlan clfr-type classifier clfr-id 1 in-profile-action 10 precedence 6*** |

Please note the ERS4500 series support up to 7 policy precedence levels. By default, you can only select a precedence level as high as 6 unless DHCP Relay is globally disabled. Hence, if you will never use DHCP Relay, you can disable DHCP Relay globally using the CLI command *no ip dhcp-relay* which in turn will allow you to use precedence level 7.

Use the CLI command *show qos diag* to view the total filter resources used and available.

Configuration - Secure Router

```
interface  ethernet 0
    ip  address 192.168.96.1 255.255.255.0
    mtu 1500
    qos
      exit qos
    crypto trusted
    exit ethernet
interface  ethernet 1
    ip  address 47.133.58.50 255.255.255.0
    mtu 1500
    qos
      exit qos
    crypto untrusted
    exit ethernet
telnet_server
system  display-boot-config no
reverse_telnet
  set_baud_rate 56000
  exit reverse_telnet
ip
  pname_server 47.129.29.80
  name_server 47.129.30.110
  load_balance per_flow
  route 0.0.0.0 0.0.0.0 47.133.58.1 1
  dhcps
    pool hotel.net
      dnsserver 47.129.29.80
      exit pool
    pool pvlan
      domain hotel.net
      dnsserver 47.129.29.80
      dnsserver 47.129.30.110
      network 192.168.96.0 255.255.255.0
      default_router 192.168.96.1
      exclude-range 192.168.96.2 192.168.96.20
      commit
      exit pool
```

```
    interface ethernet0
    enable
    exit dhcps
  exit ip
crypto
  exit crypto
firewall global
  no reset-invalid-acks
  algs
    dns
      exit dns
    exit algs
  max-connection-limit self 2048
  exit firewall
firewall internet
  interface ethernet1
  exit firewall
firewall corp
  interface ethernet0
  policy 1020 out permit nat-ip ethernet1
    exit policy
  policy 1024 out permit
    exit policy
  exit firewall
snmp-server
  chassis-id sr1001
  trap-version 1
  exit snmp-server
```

### 2.1.2 Verify Operations

#### 2.1.2.1 Verify policy configuration

**Step 1** – Verify Action Extension:

```
4550T-1# show qos if-action-extension
```

**Result:**

```
        Id: 1
        Name: fwd_port_27
        Egress Ucast Ifc: 27
        Egress NUcast Ifc: 27
        Session Id: 0
        Storage Type: NonVolatile
```

**Step 2** – Verify Action:

```
4550T-1# show qos action
```

**Result:**

```
        Id: 1
        Name: Drop_Traffic
        Drop: Yes
        Update DSCP: Ignore
        802.1p Priority: Ignore
        Set Drop Precedence: High Drop
        Extension:
        Session Id: 0
        Storage Type: ReadOnly

        Id: 2
        Name: Standard_Service
        Drop: No
        Update DSCP: 0x0
        802.1p Priority: Priority 0
        Set Drop Precedence: High Drop
        Extension:
        Session Id: 0
        Storage Type: ReadOnly
        |
        |
```

```
        Id: 10
        Name: fwd_27
        Drop: No
        Update DSCP: Ignore
        802.1p Priority: Ignore
        Set Drop Precedence: Low Drop
        Extension: fwd_port_27
        Session Id: 0
        Storage Type: NonVolatile
```

**Step 1** – Verify QoS Policy:

```
4550T-1# show qos policy
```

**Result:**

```
        Id: 1
        Policy Name: fwd_port_27
        State: Enabled
        Classifier Type: Classifier
        Classifier Name: all_traffic
        Classifier Id: 1
        Role Combination: pri_vlan
        Meter:
        Meter Id:
        In-Profile Action: fwd_27
        In-Profile Action Id: 10
        Non-Match Action:
        Non-Match Action Id:
        Track Statistics: No
        Precedence: 10
        Version: Version 1
        Session Id: 0
        Storage Type: NonVolatile
```

Verify the following information:

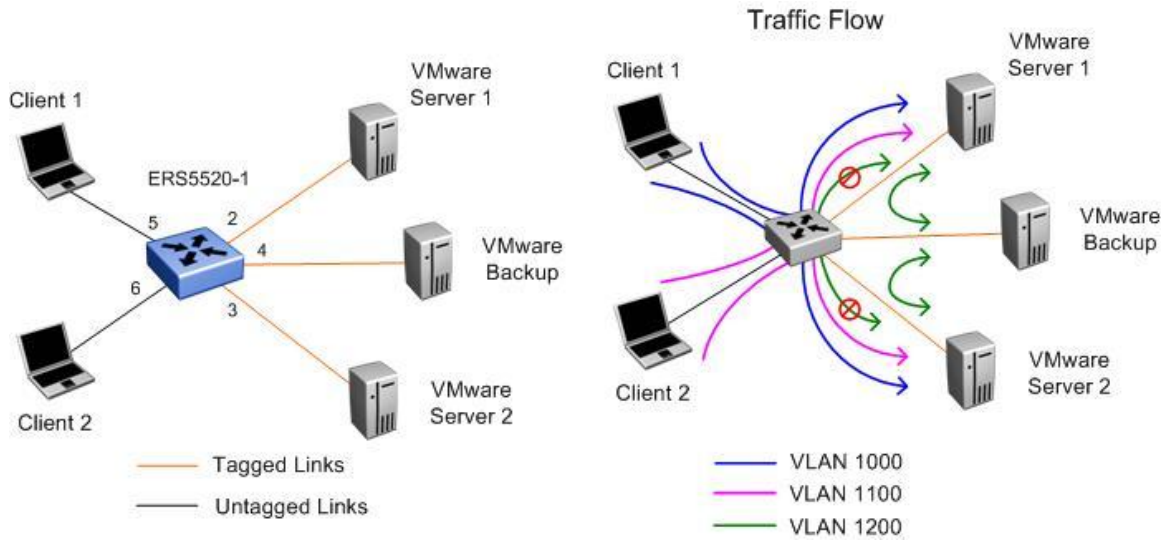
| Option | Verify |
|---|---|
| if-action-extension 1:<br>Name<br>Egress Ucast Ifc<br>Egress NUcast Ifc | Displays the egress port used by the action extension, ID = ***1*** using a name of ***fwd_port_27***, where Egress Icast Ifc and Egress NUcast Ifc should both display ***27***. Port 27, as used by for this example, is used as the unicast and non-unicast forwarding port. |

| | |
|---|---|
| QoS Action ID 10:<br>Name<br>Extension | By default, actions 1 to 9 are pre-assigned QoS actions which can be assigned to a policy. In our example, we selected action ID ***10*** although any ID from 10-55000 could have been used. The information shown via the *show qos action* command for our example should display if-action-extension name of ***fwd_port_27*** via Extension. Via Name, as used in this example, ***fwd_27*** is used which will be used by the policy |
| Policy ID 1:<br>Classifier Name<br>Role Combination<br>In-Profile Action | In our example, as no previous policies have been defined, our policy will show up with ID = ***1***. Here we selected the L2 classifier name of ***all_traffic*** and assigned to ports 21 to 27 via the role combination we created above named ***pri_vlan***. The In-Profile-Action should display the QoS Action name ***fwd_27***. |

## 2.2 Private VLAN Example using VLAN Tagging for Server Backup an Avaya Ethernet Routing Switch 5520-24T-PWR

The following configuration example details the configuration of an Ethernet Routing Switch 5520-24T-PWR (ERS5520-1) for Private VLAN in a L2 broadcast domain with VLAN tagging. This configuration example will show how to force all ingress traffic from a VLAN out to a specific egress port. As illustrated in the diagram below, all backup traffic from VMware Server 1 and VMware Server 2 will be forwarded only to the VMware backup server.

Note that any ERS 4500 or 5000 series Ethernet Routing Switch can be used in this scenario.




For this example:

- Configure ERS5520-1 as follows:
  - Add data VLAN 1000 with port members 2, 3, and 5 for Client 1's traffic to both VMware Server 1 and VMware Server 2

- Add data VLAN 1100 with port members 2, 3, and 6 for Client 2's traffic to both VMware Server 1 and VMware Server 2
- Add data VLAN 1200 with port members 2, 3, and 4 to allow traffic between the VMware backup server and VMware Server 1 and VMware Server 2
- Add a policy with an Interface action extension to force all traffic from VLAN 1200 from ports 2 and 3 to be forwarded to port 4
- Ports 5 and 6 are untagged while ports 2, 3, and 4 are tagged

### 2.2.1 Configuration – ERS5520-1

#### 2.2.1.1 Go to configuration mode.

**ERS5520-1 Step 1 - Enter configuration mode**

```
5520-24T-PWR> enable
5520-24T-PWR# cmd cli
5520-24T-PWR# configure terminal
5520-24T-PWR(config)# banner disable
5520-24T-PWR(config)# snmp-server name ERS5520-1
```

#### 2.2.1.2 Create VLAN

**ERS5520-1 Step 1 – Change the VLAN configuration control mode from default setting of strict to automatic; this will automatically add the PVID to the VLAN port member**

```
ERS5520-1(config)# vlan configcontrol automatic
```

**ERS5520-1 Step 2 – Create VLANs 1000, 1100, and 1200**

```
ERS5520-1(config)# vlan create 1000 name Client1 type port
ERS5520-1(config)# vlan create 1100 name Client2 type port
ERS5520-1(config)# vlan create 1200 name Backup type port
```

**ERS5520-1 Step 3 – Enable VLAN tagging on ports 2, 3, and 4**

```
ERS5520-1(config)# vlan ports 2-4 tagging tagall
```

**ERS5520-1 Step 4 – Add port members**

```
ERS5520-1(config)# vlan members add 1000 2-3,5
ERS5520-1(config)# vlan members add 1100 2-3,6
ERS5520-1(config)# vlan members add 1200 2-4
```

**ERS5520-1 Step 5 – Remove port members from default VLAN**

```
ERS5520-1(config)# vlan members remove 1 2-6
```

#### 2.2.1.3 Add Policy to forward all VMware backup traffic to port 4

**ERS5520-1 Step 1 – Create a new interface group with a class of unrestricted and add only the VMware Server ports**

```
ERS5520-1(config)# qos if-group name VMware-Servers class unrestricted
ERS5520-1(config)# qos if-assign port 2-3 name VMware-Servers
```

**ERS5520-1 Step 2 – Configure a new action extension and action with the uplink port member (port 4 as used in our example) which in turn will be used when we configure the policy. Please note that you must start with action number 10 or higher as the first 9 actions are already used. The various actions be viewed by entering the *show qos action* CLI command**

```
ERS5520-1(config)# qos if-action-extension 1 name fwd_port_4 egress-ucast 4  egress-non-ucast 4
ERS5520-1(config)# qos action 10 name fwd_4 drop-action disable action-ext 1
```

**ERS5520-1 Step 3 – Configure a Layer-2 classifier and classifier element to select VLAN 1200, the VLAN used for VMware backup**

```
ERS5520-1(config)# qos l2-element 1 vlan-min 1200 vlan-max 1200 vlan-tag tagged
ERS5520-1(config)# qos classifier 1 set-id 1 name Vlan1200 element-type l2 element-id 1
```

**ERS5520-1 Step 4 – Add a policy and apply the QoS action to the interface group configured above**

```
ERS5520-1(config)# qos policy 1 name fwd_port_4 if-group VMware-Servers clfr-type classifier clfr-id 1 in-profile-action 10 precedence 10
```

Please note the ERS5000 series supports up to 11 policy precedence levels. If you will never use DHCP Relay, you can disable DHCP Relay globally using the CLI command *no ip dhcp-relay* which in turn will allow you to use precedence level 15.

Use the CLI command *show qos diag* to view the total filter resources used and available.

# 3. Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

## 3.1 Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

## 3.2 Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

## 3.3 Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

## 3.4 Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.