Avaya Virtual Services Platform 4000 Configuration — QoS and ACL-Based Traffic Filtering

Release 5.1
NN46251-502
Issue 08.04
October 2016

Notice

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

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees 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 websites referenced within this site or Documentation 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 Avaya hardware and software. 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 website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the

documentation, Hosted Service, and the product 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 unless expressly authorized by Avaya. 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.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, 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, Hosted Service(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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document provides information on features in VSP Operating System Software (VOSS). VOSS runs on the following product families:

- Avaya Virtual Services Platform 4000 Series
- Avaya Virtual Services Platform 7200 Series
- Avaya Virtual Services Platform 8000 Series

This document provides conceptual information and configuration instructions to use Quality of Service (QoS) and ACL-based filters on the Avaya Virtual Services Platform 4000 Series.

For conceptual information and configuration instructions to use Quality of Service (QoS) and ACL-based filters on Avaya Virtual Services Platform 7200 Series and 8000 Series switches, see *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 7200 Series and 8000 Series*, NN47227-502.

Related resources

Documentation

See the *Documentation Roadmap for Avaya Virtual Services Platform 4000 Series*, NN46251-100 for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, access the website at http://avaya-learning.com/.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:

Videos are not available for all products.

Subscribing to e-notifications

Subscribe to e-notifications to receive an email notification when documents are added to or changed on the Avaya Support website.

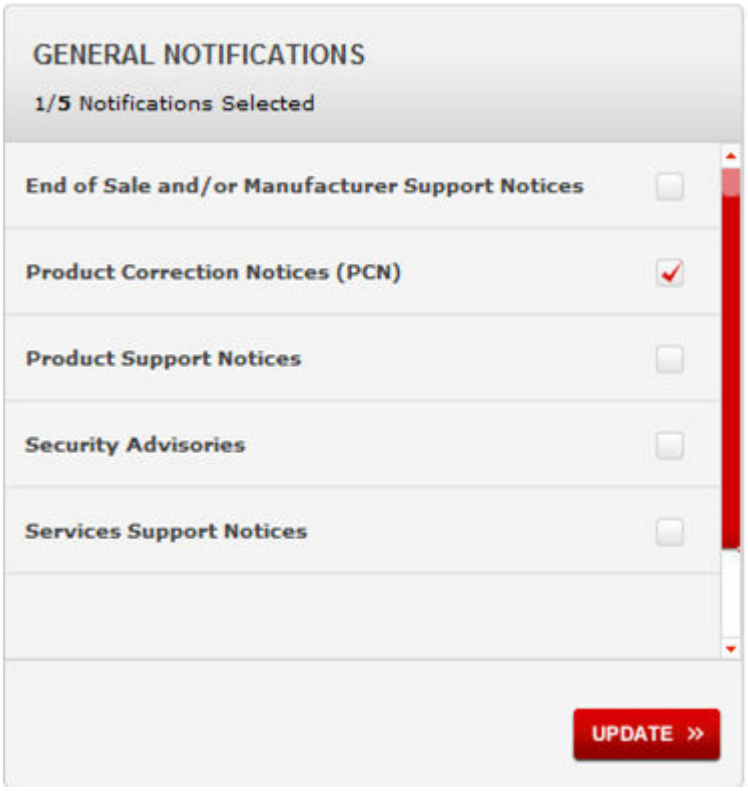
About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), which apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Virtual Services Platform 7000.

Procedure

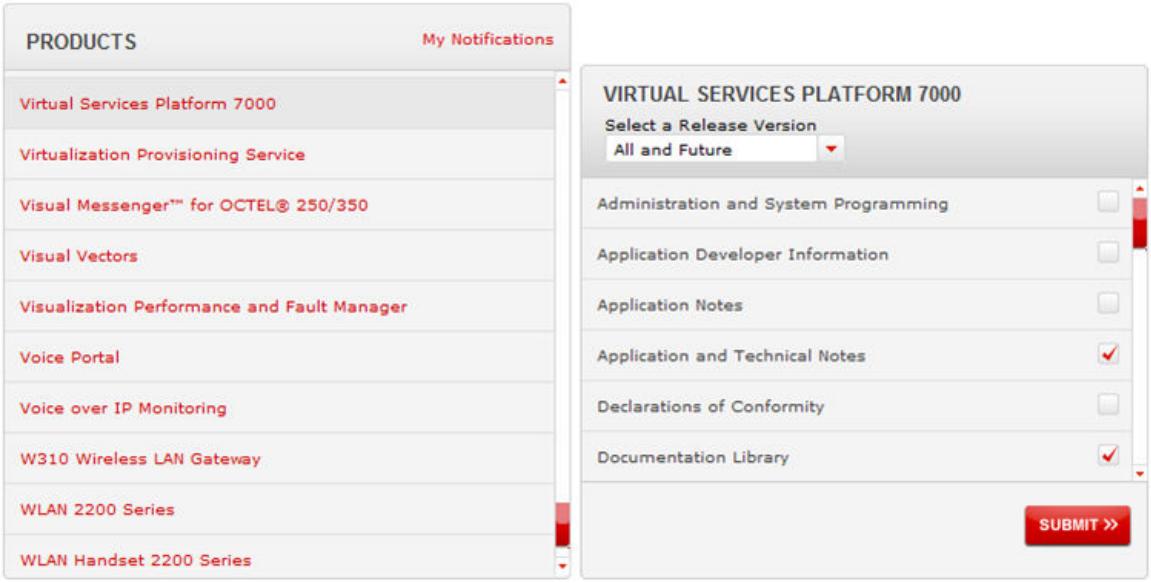
1. In an Internet browser, go to https://support.avaya.com.
2. Type your username and password, and then click **Login**.
3. Under **My Information**, select **SSO login Profile**.
4. Click **E-NOTIFICATIONS**.

5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.

8. Scroll through the list, and then select the product name.
9. Select a release version.
10. Select the check box next to the required documentation types.



11. Click **Submit**.

Support

Go to the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Searching a documentation collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx.

3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
   - Whole Words Only
   - Case-Sensitive
   - Include Bookmarks
   - Include Comments
6. Click **Search**.

   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance Ranking.

Chapter 2: New in this document

The following sections detail what is new in *Configuration - QoS and ACL-Based Traffic Filtering Avaya Virtual Services Platform 4000 Series*, NN46251-502.

Per-Queue Rate Limiting

This release enhances QoS per-queue rate limiting. Earlier releases supported egress rate limiting on the port level, and queues 6 and 7 only. With this enhancement, you can create a queue profile to modify the weight and rate limiting for an individual egress queue.

Note:

This release supports only one queue profile with a default ID of 1.

Currently the switch supports only one queue profile that is automatically created on system boot up, with an ID of 1 and name of default. You cannot delete this profile.

For more information see Queue profiles on page 30.

For configuration information using the ACLI, see Configuring an egress QoS queue profile on page 64.

For configuration using the EDM, see:

- Configuring an egress QoS queue profile on page 73
- Editing queue profile information on page 74

Chapter 3: QoS fundamentals

Use the information in this section to help you understand Quality of Service (QoS).

This section describes a range of features that you can use with the Avaya Virtual Services Platform 4000 Series to allocate network resources to critical applications. You can configure your network to prioritize specific types of traffic to ensure traffic receives the appropriate QoS level. Allocate priority to protocol and application data depending on required parameters, for example, minimum data rate or minimum time delay

Introduction to QoS

Quality of Service (QoS) is the extent to which a service delivery meets user expectations. In a QoS-aware network, a user can expect the network to meet certain performance expectations. These performance expectations are specified in terms of service availability, packet loss, packet delay, and packet delay variation.

By assigning QoS levels to traffic flows on your Local Area Network (LAN), you can ensure you allocate network resources where you need them most. To be effective, you must configure QoS functionality from end-to-end in the network: across different devices, such as routers, switches, and end stations; across platforms and media; and across link layers, such as Ethernet.

Avaya Virtual Services Platform 4000 Series supports QoS classification for both Layer 2 (802.1p bits) and Layer 3 (Differentiated Services Code Point bits) parameters. Avaya Virtual Services Platform 4000 Series provides QoS functionality that can differ for Layer 2 (bridged) and Layer 3 (routed) traffic flows. The Avaya Virtual Services Platform 4000 Series can also assign QoS levels based on multiple criteria including, but not limited to, Transport Control Protocol (TCP) or Internet Protocol (IP) ports used by an application.

To effectively use QoS functions in your network, you must

- identify traffic sources and types
- determine the required QoS parameters based on the traffic to carry
- perform traffic management (QoS) operations based on the required parameters

Avaya Virtual Services Platform 4000 Series implements QoS functionality for IP traffic through a Differentiated Services (DiffServ) network architecture. The QoS implementation on Avaya Virtual Services Platform 4000 Series supports the following options:

- port-based egress shaping
- port-based ingress policers
- port-based broadcast and multicast rate limiting

- Avaya Automatic QoS
- ingress and egress mapping between internal QoS level and Differentiated Services Code Point (DSCP) and internal QoS level and 802.1p-bits

Configuration considerations

If you modify the QoS configuration for a port that is a member of MultiLink Trunking (MLT), all ports in the MLT inherit the same configuration. If you remove the port from the MLT, it keeps the QoS configuration it inherited from the MLT.

QoS support for 10G interface in 1G mode

If you use QoS with a 10G interface as a 10G interface and re-purpose the interface as a 1G interface, you must make the necessary configuration changes to accommodate the new link speed of 1G in the QoS configuration.

Queuing

Queuing is a congestion-avoidance function that prioritizes packet delivery. Queuing ensures discriminate packet discard during network congestion, and can delay a packet in memory until the scheduled transmission.

You can use queuing to manage congestion. Congestion management involves the creation of queues, assignment of packets to the queues based on the classification of the packet, and scheduling of the packets in a queue for transmission.

The system schedules packets for transmission according to their assigned priority and the queuing mechanism configured for the interface. The scheduler determines the order of packet transmission by controlling how the system services queues with respect to each other. The switch uses 16 CPU queues (used by traffic destined to the CPU), and eight unicast and eight multicast queues for each port. The deepest queue does not go beyond 60,000 packets.

A scheduler services the eight queues for each port, using a combination of strict priority and round-robin. Queue zero through five use round robin, and queues six and seven drain completely, or up to certain rate limits.

There are eight priorities on each egress port. Class of Service (CoS) 0 to CoS 5 are Weighted Deficit Round Robin (WDRR), and the weights are 5, 20, 30, 40, 50, 50 respectively. CoS 6 and CoS 7 are strict priority queues, and the switch subjects CoS 6 and CoS 7 to traffic shaping at 50 per cent and five per cent of line rate respectively.

The current release does not support Weighted Random Early Detection (WRED).

Avaya Service Class

Avaya Service Classes define a standard architecture to provide end-to-end QoS on a broad range of Avaya Ethernet switching and voice products. They function as default QoS policies built in to the product. They incorporate the various QoS technologies to provide a complete end-to-end QoS behavioral treatment. The Avaya Virtual Services Platform 4000 Series includes a built-in QoS implementation for Avaya Service Classes.

The Avaya Virtual Services Platform 4000 Series includes eight preconfigured queues (corresponding to the eight Service Classes) on each port of an interface module.

An Avaya Service Class domain classifies traffic as either

- network control traffic (Critical/Network)
- subscriber traffic (Premium, Metal, or Standard)

Critical/Network Avaya Service Class

The switch uses the Critical/Network Avaya Service Class for traffic within a single administrative network domain. If such traffic does not get through, the network cannot function. Examples of such types of traffic are heartbeats between core network switches or routers.

Premium Avaya Service Class

The switch uses the Premium Avaya Service Class for IP telephony services, and provides the low latency and low jitter required to support such services. IP telephony services include Voice over IP (VoIP), voice signaling, Fax over IP (FoIP), and voice-band data services over IP (for example, analog modem). The switch can also use the Premium Avaya Service Class for Circuit Emulation Services over IP (CESoIP).

Metal Avaya Service Class

The Platinum, Gold, Silver, and Bronze Avaya Service Class are collectively referred to as the metal classes. The metal Avaya Service Class provide a minimum bandwidth guarantee and are for variable bit rate or bursty types of traffic. Applications that use the metal Avaya Service Class support mechanisms that dynamically adjust their transmit rate and burst size based on congestion (packet loss) detected in the network. The following list describes the individual metal classes:

- Platinum Avaya Service Class

  The switch uses the Platinum Avaya Service Class for applications that require low latency, for example, real-time services such as video conferencing and interactive gaming. Platinum Avaya Service Class traffic provides the low latency required for interhuman (interactive) communications. The Platinum Avaya Service Class provides a minimum bandwidth assurance for Assured Forwarding (AF) 41 and Class Selector (CS) 4-marked flows.

- Gold Avaya Service Class

  The switch uses the Gold Avaya Service Class for applications that require near-real-time service and are not as delay-sensitive as applications that use the Platinum service. Such applications include streaming audio and video, video on demand, and surveillance video.

The Gold Avaya Service Class assumes that traffic buffers at the source and destination and, therefore, the traffic is less sensitive to delay and jitter. By default, the Gold Avaya Service Class provides a minimum bandwidth assurance for AF31, AF32, AF33 and CS3-marked flows.

- Silver Avaya Service Class

  The switch uses the Silver Avaya Service Class for responsive (typically client- and server-based) applications. Such applications include Systems Network Architecture (SNA) terminals (for example, a PC or Automatic Teller Machine) to mainframe (host) transactions that use Data Link Switching (SNA over IP), Telnet sessions, Web-based ordering and credit card processing, financial wire transfers, and Enterprise Resource Planning applications.

  Silver Avaya Service Class applications require a fast response and have asymmetrical bandwidth needs. The client sends a short message to the server and the server responds with a much larger data flow back to the client. For example, after a user clicks a hyperlink (that sends a few dozen bytes) on a Web page, a new Web page appears (that downloads kilobytes of data). The Silver Avaya Service Class provides a minimum bandwidth assurance for AF21 and CS2-marked flows.

  The Silver Avaya Service Class favors short-lived, low-bandwidth TCP-based flows.

- Bronze Avaya Service Class

  The switch uses the Bronze Avaya Service Class for longer-lived TCP-based flows, such as file transfers, e-mail, or noncritical Operation, Administration, and Maintenance (OAM) traffic. The Bronze Avaya Service Class provides a minimum bandwidth assurance for AF11 and CS1-marked flows. Avaya recommends that you use the Bronze Avaya Service Class for noncritical OAM traffic with the CS1 DSCP marking.

Standard Avaya Service Class

The switch uses the Standard Avaya Service Class for best-effort services. Avaya does not specify delay, loss, or jitter guarantees for this Avaya Service Class.

Network congestion and QoS design

When you provide QoS in a network, one of the major elements you must consider is congestion, and the traffic management behavior during congestion. Congestion in a network is caused by many different conditions and events, including node failures, link outages, broadcast storms, and user traffic bursts.

At a high level, three main types or stages of congestion exist:

1. No congestion
2. Bursty congestion
3. Severe congestion

In a noncongested network, QoS actions ensure that delay-sensitive applications, such as real-time voice and video traffic, are sent before lower-priority traffic. The prioritization of delay-sensitive traffic is essential to minimize delay and reduce or eliminate jitter, which has a detrimental impact on these applications.

A network can experience momentary bursts of congestion for various reasons, such as network failures, rerouting, and broadcast storms. The switch has sufficient capacity to handle bursts of congestion in a seamless and transparent manner. If the burst is not sustained, the traffic management and buffering process on the switch allows all the traffic to pass without loss.

Severe congestion is defined as a condition where the network or certain elements of the network experience a prolonged period of sustained congestion. Under such congestion conditions, congestion thresholds are reached, buffers overflow, and a substantial amount of traffic is lost.

When you perform traffic engineering and link capacity analysis for a network, the standard design rule is to design the network links and trunks for a maximum average-peak utilization of no more than 80%. This value means that the network peaks to up to 100% capacity, but the average-peak utilization does not exceed 80%. The network is expected to handle momentary peaks above 100% capacity.

Internal QoS level

The internal QoS level or effective QoS level is a key element in the Virtual Services Platform 4000 QoS architecture. The internal QoS level specifies the kind of treatment a packet receives. Virtual Services Platform 4000 classifies every packet that enters and assigns it an internal QoS level.

Internal QoS levels map to the queues on a port. For example, for an access port the internal QoS level is derived from the port QoS level. For Layer 3 trusted (core) ports, the system honors incoming DSCP or type of service (TOS) bits. The system assigns the internal QoS level using the ingress DSCP to QoS level map.

Classification and mapping

Traffic classification includes functions that examine a packet to determine further actions according to defined rules. Classification involves identifying flows so that the router can modify the packet contents or Per-Hop Behavior (PHB), apply conditioning treatments to the packet, and determine how to forward the packet to the egress interface. Packet classification depends on the service type of the packet and the point in the traffic management process where the classification occurs.

The device classifies traffic as it enters the DiffServ network, and assigns appropriate PHB based on the classification. To differentiate between classes of service, the device marks the DiffServ (DS) parameter in the IP packet header, as defined in RFC2474 and RFC2475. The DSCP marking defines the forwarding treatment of the packet at each network hop. This marking (or classification) occurs at the edge of the DiffServ domain, and is based on the policy (or filter) associated with the particular microflow or aggregate flow.

You can configure the mapping of DSCP-to-forwarding behaviors and DSCP re-markings. Re-marking the DSCP resets the treatment of packets based on new network specifications or desired levels of service.

Layer 3 marking uses the DSCP parameter. Layer 2 (Ethernet) marking involves the 802.1p-bits parameter.

For Layer 2 packets, priority bits (or 802.1p bits) define the traffic priority of the Ethernet packet. You can configure an interface to map DSCP or 802.1p bits to internal QoS levels on ingress. You can configure an interface to map internal QoS levels to DSCP, or 802.1p bits at egress. 802.1p bit mapping, which assesses the 802.1p bit and derives an appropriate DSCP, provides the Ethernet VLAN QoS requirements.

Within the network, a packet PHB associated with the DSCP determines how a device forwards the packet to the next hop—if at all. Consequently, nodes can allocate buffer and bandwidth resources to each competing traffic stream. The initial DSCP value is based on network policies for the type of service required. The objective of DSCP-to-Avaya Service Class mapping is to translate the QoS characteristics defined by the packet DSCP marker to an Avaya Service Class. The DSCP-to-Avaya Service Class mapping occurs at ingress. For each received packet, the mapping function assigns an Avaya Service Class.

The Virtual Services Platform 4000 maintains four mapping tables. These tables translate the ingress 802.1p-bits or DSCP markings to an internal QoS level, and then retranslate the internal QoS level to an egress DSCP or 802.1p-bits marking as follows:

- ingress 802.1p-bits to QoS level
- ingress DSCP to QoS level
- QoS level to egress 802.1p-bits
- QoS level to egress DSCP

DiffServ

DiffServ divides traffic into various classes (behavior aggregates) to give each class differentiated treatment. DiffServ applies only to IP packets.

A DiffServ network provides either end-to-end or intradomain QoS functionality by implementing classification and mapping functions at the network boundary or access points. Within a core network, DiffServ regulates packet behavior by this classification and mapping.

DiffServ, as defined by RFC2475, provides QoS for aggregate traffic flows (as opposed to individual traffic flows, which use an Integrated Services architecture [IntServ—RFC1633]). DiffServ provides QoS by using traffic management and conditioning functions (packet classification, marking, policing, and shaping) on network edge devices, and by using PHBs on network core devices, which includes queueing. The Virtual Services Platform 4000 can perform all of these QoS functions. The following list identifies the order of DiffServ operations for a packet:

- packet classification: IEEE 802.1p and DSCP markings classify (map) the packet to its appropriate PHB and QoS level.
- re-marking: The switch can re-mark packets according to QoS actions you configure on the switch (internal QoS mappings).
- shaping: The Avaya Virtual Services Platform 4000 Series provides port-based shaping. Port-based shaping shapes all outgoing traffic to a specific rate.

Although you do not require filters for QoS operation, you can use filters to provide traffic management actions. Filter-based QoS rules and actions override other less specific QoS rules and actions.

The Avaya Virtual Services Platform 4000 Series implements a DiffServ architecture as defined in RFC2474 and RFC2475. The device uses the IEEE 802.1p and the DSCP markings found in virtual local area networks (VLAN) to classify the packet to the appropriate PHB and QoS level to provide Layer 2 and Layer 3 QoS functionality, respectively.

You can use the Avaya Virtual Services Platform 4000 Series in the network core. The devices can perform classification, marking, policing, or shaping; they perform the actions defined by the PHB of the packet. You configure ports as access (edge) or core ports. The default is core.

The following figure illustrates DiffServ network operations. The Virtual Services Platform 4000 devices are on the network edge where they perform classification, marking, policing, and shaping functions.

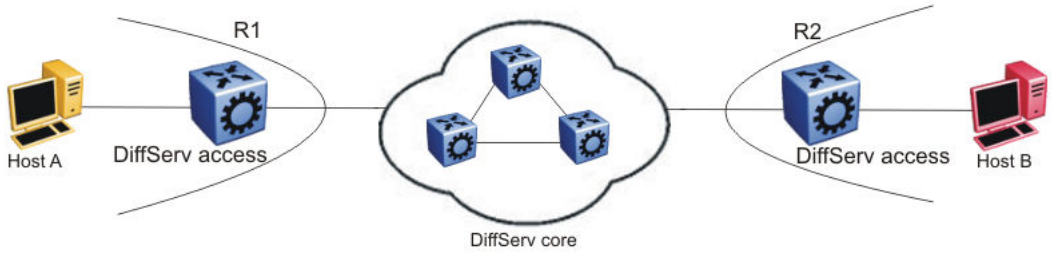


Figure 1: DiffServ network core and edge devices

If you configure a port as a core port, the system trusts packet markings. If you configure a port as an access port, the system does not trust packet markings.

Use a DiffServ access port at the edge of a DiffServ network. The access port classifies traffic according to port QoS. Outgoing packet DSCP and 802.1p values are derived from port QoS and QoS maps. The system strips Dot1Q headers at ingress, and adds them back at egress only if you configure the egress port as a tagged or trunk port.

A DiffServ core port does not change packet classification or markings; the port trusts the incoming traffic markings. A core port preserves the DSCP marking of all incoming packets, and uses these markings to assign the packet to an internal QoS level. For tagged packets, the port honors the 802.1p bits within a Dot1Q header, and uses these bits to classify ingress traffic. You can control the honoring (or not) of 802.1p bits by configuring the 802.1p override in ACLI or Enterprise Device Manager (EDM).

PHB

When traffic enters the DiffServ network, packets enter a queue according to their marking, which determines the PHB of the packets. For example, if the system marks a video stream to receive the highest priority, it enters a high-priority queue. As these packets traverse the DiffServ network, the system forwards the video stream before other packets.

RFC2598 defines standard PHB: the AF PHB group and the Expedited Forwarding (EF) PHB group. The Avaya Virtual Services Platform 4000 Series also uses the Default (DF) and CS groups. Class Selector in a DiffServ network provides backward compatibility with IP precedence.

RFC2598 describes the EF PHB group as the premium service: the best service the network can offer. Expedited Forwarding PHB is a forwarding treatment for a DiffServ microflow when the transmission rate ensures that it is the highest priority and it experiences no packet loss for in-profile traffic.

DiffServ and filters

QoS (DiffServ) and filters operate independently; you do not have to use filters to provide QoS. However, filters can override QoS operations. For more information about traffic filtering, see QoS and filters on page 25.

Ingress mappings

The system uses ingress maps to translate incoming packet QoS markings to the internal QoS level. The system uses the internal QoS level to classify packets.

Ingress mappings include

- 802.1p to (internal) QoS level
- DSCP to (internal) QoS level

The following logical table shows how the system performs ingress mappings for data packets and for control packets not destined for the Control Processor (CP).

Table 1: Data packet ingress mapping

DSCP	Layer 2 trusted	Layer 3 trusted and DiffServ enabled	IP packet	Routed packet	Ingress tagged	Internal QoS
x	No	x	No	x	x	Use port QoS
x	Yes	x	No	x	No	Use port QoS
x	Yes	x	No	x	Yes	Use ingress p-bits mapping
0x1B	x	x	Yes	x	x	4
0x23	x	x	Yes	x	x	5
0x29	x	x	Yes	x	x	5
0x2F	x	x	Yes	x	x	6
x	No	No	x	x	x	Use port QoS
x	No	Yes	Yes	x	x	Use ingress DSCP mapping
x	Yes	No	Yes	x	No	Use port QoS

Table continues…

DSCP	Layer 2 trusted	Layer 3 trusted and DiffServ enabled	IP packet	Routed packet	Ingress tagged	Internal QoS
x	Yes	No	Yes	x	Yes	Use ingress p-bits mapping
x	Yes	Yes	Yes	No	No	Use ingress DSCP mapping
x	Yes	Yes	Yes	No	Yes	Use ingress p-bits mapping
x	Yes	Yes	Yes	Yes	Yes	Use ingress DSCP mapping

Important:

On a tagged port that is Layer-2 trusted, Layer-3 trusted and DiffServ enabled, all multicast packets honor the ingress DSCP value.

The QoS level for control packets destined for the CPU is assigned internally to ensure timely packet processing and scaling numbers. You cannot configure the QoS level for these control packets. The system assigns the highest QoS-level to time-critical protocols.

The following table shows ingress IEEE 802.1p to QoS level mappings.

Table 2: Default ingress 802.1p to QoS mappings

Ingress IEEE 802.1p	PHB	QoS Level	Network Service Class (NSC)
0	CS0/DF	1	Standard
1	Custom	0	Custom
2	CS1/AF11	2	Bronze
3	CS2/AF21	3	Silver
4	CS3/AF31	4	Gold
5	CS4/AF41	5	Platinum
6	CS5/EF	6	Premium/EF
7	CS6/CS7	7	Network/Critical

The following table shows DSCP to internal QoS level mappings.

Table 3: Default ingress DSCP to QoS mapping

Ingress				Internal QoS level	PHB level
DSCP	**DSCP (binary)**	**DSCP (hexadecimal)**	**TOS**		
00	000000	00	00	1	CS0
00	000000	00	00	1	DF
01	000001	01	04	1	CS0
02	000010	02	08	1	CS0
03	000011	03	0C	1	CS0
04	000100	04	10	1	CS0
05	000101	05	14	1	CS0
06	000110	06	18	1	CS0
07	000111	07	1C	1	CS0
08	001000	08	20	2	CS1
09	001001	09	24	1	CS0
10	001010	0A	28	1	AF11
11	001011	0B	2C	1	CS0
12	001100	0C	30	2	CS1
13	001101	0D	34	1	CS0
14	001110	0E	38	2	CS1
15	001111	0F	3C	1	CS0
16	010000	10	40	3	CS2
17	010001	11	44	1	CS0
18	010010	12	48	3	AF21
19	010011	13	4C	1	CS0
20	010100	14	50	3	CS2
21	010101	15	54	1	CS0
22	010110	16	58	3	CS2
23	010111	17	5C	1	CS0
24	011000	18	60	4	CS3
25	011001	19	64	1	CS0
26	011010	1A	68	4	AF31
27	011011	1B	6C	4	CS3
28	011100	1C	70	4	CS3
29	011101	1D	74	1	CS0

Table continues…

Ingress				Internal QoS level	PHB level
DSCP	DSCP (binary)	DSCP (hexadecimal)	TOS		
30	011110	1E	78	4	CS3
31	011111	1F	7C	1	CS0
32	100000	20	80	5	CS4
33	100001	21	84	1	CS0
34	100010	22	88	5	AF41
35	100011	23	8C	5	CS4
36	100100	24	90	5	CS4
37	100101	25	94	1	CS0
38	100110	26	98	5	CS4
39	100111	27	9C	1	CS0
40	101000	28	A0	5	CS4
41	101001	29	A4	5	CS4
42	101010	2A	A8	1	CS0
43	101011	2B	AC	1	CS0
44	101100	2C	B0	1	CS0
45	101101	2D	B4	1	CS0
46	101110	2E	B8	6	EF
47	101111	2F	BC	6	CS5
48	110000	30	C0	7	CS6
49	110001	31	C4	1	CS0
50	110010	32	C8	1	CS0
51	110011	33	CC	1	CS0
52	110100	34	D0	1	CS0
53	110101	35	D4	1	CS0
54	110110	36	D8	1	CS0
55	110111	37	DC	1	CS0
56	111000	38	E0	7	CS7
57	111001	39	E4	1	CS0
58	111010	3A	E8	1	CS0
59	111011	3B	EC	1	CS0
60	111100	3C	F0	1	CS0
61	111101	3D	F4	1	CS0

Table continues…

Ingress				Internal QoS level	PHB level
DSCP	DSCP (binary)	DSCP (hexadecimal)	TOS		
62	111110	3E	F8	1	CS0
63	111111	3F	FC	1	CS0

Egress mappings

Egress mappings include:

- QoS level to IEEE 802.1p mappings
- QoS level to DSCP mappings

The following table shows egress QoS level to IEEE 802.1p mappings.

Table 4: Default egress QoS level to IEEE 802.1p mappings

QoS level	PHB	Default 1p remarking on egress	Network Service Class (NSC)
0	Custom	1	Custom
1	CS0/DF	0	Standard
2	CS1/AF11	2	Bronze
3	CS2/AF21	3	Silver
4	CS3/AF31	4	Gold
5	CS4/AF41	5	Platinum
6	CS5/EF	6	Premium/EF
7	CS6/CS7	7	Network/Critical

The following table shows QoS level to DSCP mappings.

Table 5: Default egress QoS level to DSCP mappings

Egress			
QoS level	DSCP (binary)	DSCP (hexadecimal)	DSCP
0	000000	00	0
1	000000	00	0
2	001010	0A	10
3	010010	12	18

Table continues…

Egress			
QoS level	**DSCP (binary)**	**DSCP (hexadecimal)**	**DSCP**
4	011010	1A	26
5	100010	22	34
6	101110	2E	46
7	101110	2E	46

QoS and filters

The Avaya Virtual Services Platform 4000 Series has functions you can use to provide appropriate QoS levels to traffic for each customer, application, or packet. These functions include port-based shapers, DiffServ access or core port settings, and port-based policers. The Avaya Virtual Services Platform 4000 Series also provides access control list (ACL)-based filters. You do not need to use filters to provide QoS; however, filters aid in prioritizing customer traffic. Filters also provide protection by blocking unwanted traffic.

Policers apply at ingress; shapers apply at egress. ACL-based filters apply at ingress and egress.

Policing and shaping

The Virtual Services Platform 4000 QoS implementation supports the following two features for bandwidth management and traffic control:

- ingress traffic policing—a mechanism to limit the number of packets in a stream that matches a particular classification
- egress traffic shaping—the process by which the system delays and transmits packets to produce an even and predictable flow rate

Each feature is important to deliver DiffServ within a QoS network domain.

Token buckets and policing

Tokens are a key concept in traffic control. A policer or shaper calculates the number of packets that passed, and at what data rate. Each packet corresponds to a token, and the policer or shaper transmits or passes the packet if the token is available. For more information, see Figure 2: Token flow on page 26.

The token container is like a bucket. In this view, the bucket represents both the number of tokens that a policer or shaper can use instantaneously (the depth of the bucket) and the rate at which the tokens replenish (how fast the bucket refills).

In the Virtual Services Platform 4000, each policer has two token buckets: one for the peak rate and the other for the service rate. The following figure shows the flow of tokens.

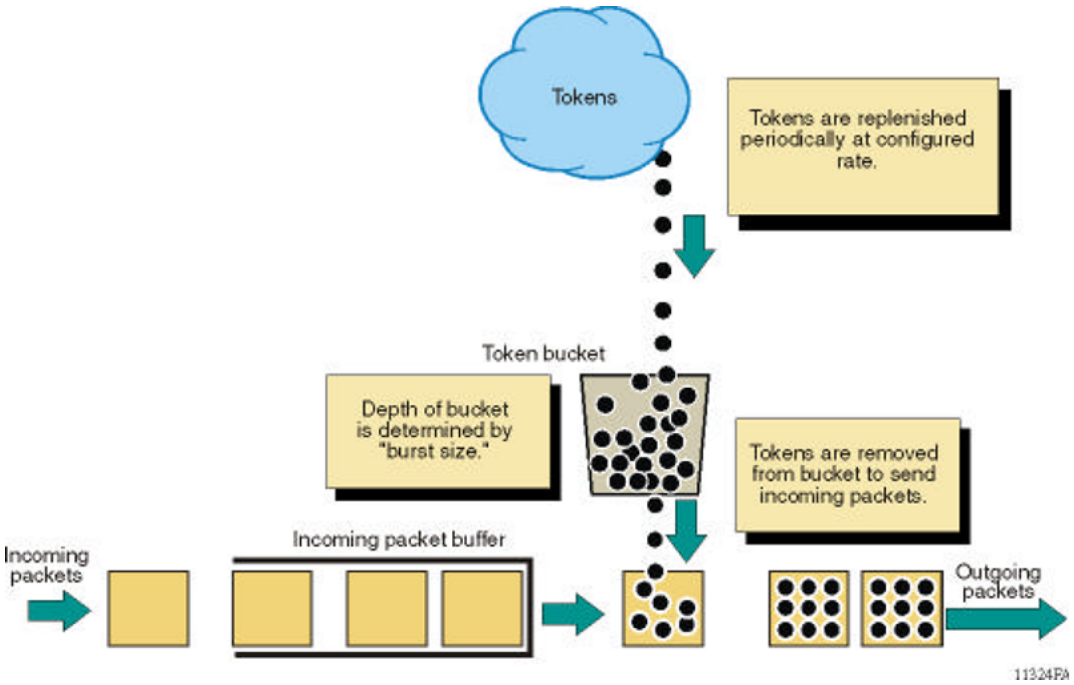


Figure 2: Token flow

Layer 2 and Layer 3 trusted and untrusted ports

You can configure interface module ports as trusted or untrusted at both Layer 2 (802.1p) or Layer 3 (DSCP) for ingress packet classification.

The Avaya Virtual Services Platform 4000 Series provides eight internal QoS levels. These eight levels, numbered zero to seven, map to the queues through

- the ingress 8021p to (internal) QoS mapping table
- the ingress DSCP to (internal) QoS mapping table

Layer 2 untrusted and Layer 3 untrusted

To configure a port as Layer 2 untrusted and Layer 3 untrusted, assign the following parameter values:

- DiffServ = true
- Layer3Trust = access
- Layer2 8021p Override = true

For more information, see Table 1: Data packet ingress mapping on page 20.

Layer 2 untrusted and Layer 3 trusted

To configure a port as Layer 2 untrusted and Layer 3 trusted, assign the following parameter values:

- DiffServ = true

- Layer3Trust = core
- Layer2 8021p Override = true

Use these configuration options to classify packet QoS through the DSCP parameter for all IP packets, whether tagged or untagged. Use this configuration when another QoS or DiffServ enabled and configured switch marks the IP packets at the edge. These already-marked packets arrive Layer 3 trusted, and the Virtual Services Platform 4000 continues with the trust (DiffServ core port operation). For tagged packets, the system does not examine the 802.1p bits. For non-IP packets, this configuration causes classification by port QoS settings.

For more information, see Table 1: Data packet ingress mapping on page 20.

Layer 2 trusted and Layer 3 trusted

To configure a port as Layer 2 trusted and Layer 3 trusted, assign the following parameter values:

- DiffServ = true
- Layer3Trust = core
- Layer2 8021p Override = false

Use these configuration options to classify packet QoS through 802.1p for all tagged packets, and through DSCP for all untagged routed IP packets.If the packet is tagged and bridged, 802.1p bits are used. If the packet is untagged or routed, DSCP is used. This action is independent of tagged (trunk) or untagged (access) port settings. An exception is an untagged port with a DiscardTaggedFrames parameter of true (nondefault); the system discards the packet rather than classifies the packet for QoS treatment.

For more information, see Table 1: Data packet ingress mapping on page 20.

Layer 2 trusted and Layer 3 untrusted

To configure a port as Layer 2 trusted and Layer 3 untrusted, assign the following parameter values:

- DiffServ = True
- Layer3Trust = Access
- Layer2 8021p Override = false

Use these configuration options to classify packet QoS through 802.1p for all tagged packets, and port QoS levels for all untagged (IP or non-IP) packets. If the packet is an IP packet, the system does not modify or examine the DSCP parameter bits.

For more information, see Table 1: Data packet ingress mapping on page 20.

DiffServ disabled

If you disable the DiffServ parameter, the system ignores the Layer 3 DSCP parameter. For more information, see Table 1: Data packet ingress mapping on page 20.

802.1p and 802.1Q recommendations

In a network, to map the 802.1p user priority bits, use 802.1Q-tagged encapsulation on customer-premises equipment (CPE). You require encapsulation because the switch does not provide classification when it operates in bridging mode.

At the egress access node, packets are examined to determine if their IEEE 802.1p or DSCP values must be re-marked before leaving the network. Upon examination, if the packet is a tagged packet, the IEEE 802.1p tag is configured based on the QoS level-to-IEEE 802.1p-bit mapping. For bridged packets, the DSCP is re-marked based on the QoS level.

Broadcast and multicast traffic bandwidth limiters

Interface modules support bandwidth limiters for ingress broadcast and multicast traffic. The system drops traffic that violates the bandwidth limit. Enable this feature and configure the rate limit on an individual port basis.

QoS and VoIP

VoIP traffic requires low latency and jitter.

If you use the Avaya Virtual Services Platform 4000 Series as a edge router, to treat VoIP traffic appropriately, configure ingress ports as core ports. In this case, the system trusts QoS markings that apply to VoIP traffic, and the system does not re-mark QoS settings. However, if this configuration is not sufficient, you can also apply filters, route policies, or re-mark traffic.

Avaya Automatic QoS

Virtual Services Platform 4000 includes Avaya Automatic QoS to specifically support Avaya converged voice deployments. Avaya Automatic QoS automatically recognizes the DSCP value Avaya voice applications can use, and associates these DSCP values with the proper queue.

Using Avaya Automatic QoS, the system recognizes Avaya application traffic and prioritizes the traffic through the system. Avaya Automatic QoS offers a simplified and resource-efficient mechanism to prioritize Avaya application traffic within the network. Avaya Automatic QoS supersedes DiffServ mode configuration.

The following table shows the traffic types, the standard DSCP value, the specific Avaya Automatic QoS DSCP values, and the queue mappings for the Avaya Automatic QoS DSCP values.

Table 6: Avaya Automatic QoS DSCP values

Traffic type	Avaya Automatic QoS DSCP value	Queue
VoIP data (Premium)	0x2F (47)	6
VoIP signaling (Platinum)	0x29 (41)	5
Video (Platinum)	0x23 (35)	5
Streaming (Gold)	0x1B (27)	4

Traffic the system identifies based on these DSCP values receives preferential queuing treatment within the system and is re-marked for preferential downstream processing.

The system associates additional filtering (ACL filters) to ensure that Auto-QOS DSCP values are honored no matter what the QOS configuration of the ingress is.

These additional filtering components target ingress traffic with the designated private Avaya DSCP values. After a match occurs, the system re-marks the traffic based on the application mode. Ingress traffic that is not marked with a recognized private Avaya DSCP value receives the same treatment as it receives without the Avaya Automatic QoS feature.

The switch activates Avaya Automatic QoS automatically; you cannot deactivate this feature but you can remap these DSCP values to use a different queue. The system displays a warning that modifying these values is not recommended.

```
Switch:1(config)#qos ingressmap ds 47 2
Avaya-on-Avaya DSCP values should not be modified.
Do you want to continue ? (y/n) ? y
```

You do not need to configure individual QoS components across a variety of platforms. Automatic QoS applies end-to-end, from the application traffic to the Avaya or third party data infrastructure, and does not affect non-Avaya application traffic.

QoS re-marking on a Transparent Port UNI

A *Transparent Port UNI* port is normally configured as a Layer 2 trusted port. The T-UNI port honors incoming customer 802.1p bits and derives an internal QoS level. The 802.1p bit marking of the Backbone VLAN (BVLAN) is derived from the internal QoS level. If the T-UNI port is set as a Layer 2 untrusted port, a best-effort queue is assigned. Customer packet headers are not modified.

The T-UNI port QoS configurations are:

- DiffServ = disable
- Layer3Trusted = access

QoS considerations when a port is associated with a T-UNI I-SID

- You cannot configure `access-diffserv` and `enable diffserv` on a T-UNI port.
- When a port is associated with a T-UNI ISID, the T-UNI QoS configuration automatically takes effect.
- When the port is removed from the T-UNI ISID, the default port QoS configuration takes effect.

QoS considerations when an MLT is associated with a T-UNI I-SID

- When an MLT, static or LACP, is added to a T-UNI ISID, the T-UNI QoS configuration take effect on all the ports of the MLT.
- When an MLT, static or LACP, is removed from a T-UNI ISID, the port default QoS configuration is configured on all the member ports of the MLT.
- If a port is added dynamically to a T-UNI MLT, static or LACP, the port inherits the QoS properties of the T-UNI MLT ports.
- If a port is dynamically removed from a T-UNI MLT, static or LACP, the port retains the QoS configuration inherited from the MLT.

Queue profiles

This section identifies optional ways to customize the egress queues and scheduling depending on your need to override the default configuration. You can also enable **egress** queue rate limiting, if desired.

Use a queue profile to apply configured egress queue parameters and modify each queue individually. You can use the queue profile to configure a minimum weight for the queue and to enable rate limiting for the queue. The queue profile applies to all ports in the switch.

Currently the switch supports only one queue profile that is automatically created on system boot up, with an ID of 1 and name of default. You cannot delete this profile.

Note:

The egress queues with rate limiting enabled must be **contiguous**. For example, you can configure queues 3–6, but you cannot configure 3 and 6.

After you make a configuration change to a queue profile, you must apply the profile before the changes take effect.

QoS examples and recommendations

The sections that follow present QoS network scenarios for bridged and routed traffic over the core network.

Bridged traffic

If you bridge traffic over the core network, you keep customer VLANs separate (similar to a Virtual Private Network). Normally, a service provider implements VLAN bridging (Layer 2) and no routing. In this case, the 802.1p-bit marking determines the QoS level assigned to each packet. If DiffServ is active on core ports, the level of service received is based on the highest of the DiffServ or 802.1p settings.

The following cases provide sample QoS design guidelines you can use to provide and maintain high service quality in a network.

If you configure a core port, you assume that, for all incoming traffic, the QoS value is properly marked. All core switch ports simply read and forward packets; they are not re-marked or reclassified. All initial QoS markings are performed at the customer device or on the edge devices.

The following figure illustrates the actions performed on three different bridged traffic flows (that is VoIP, video conference, and email) at access and core ports throughout the network.

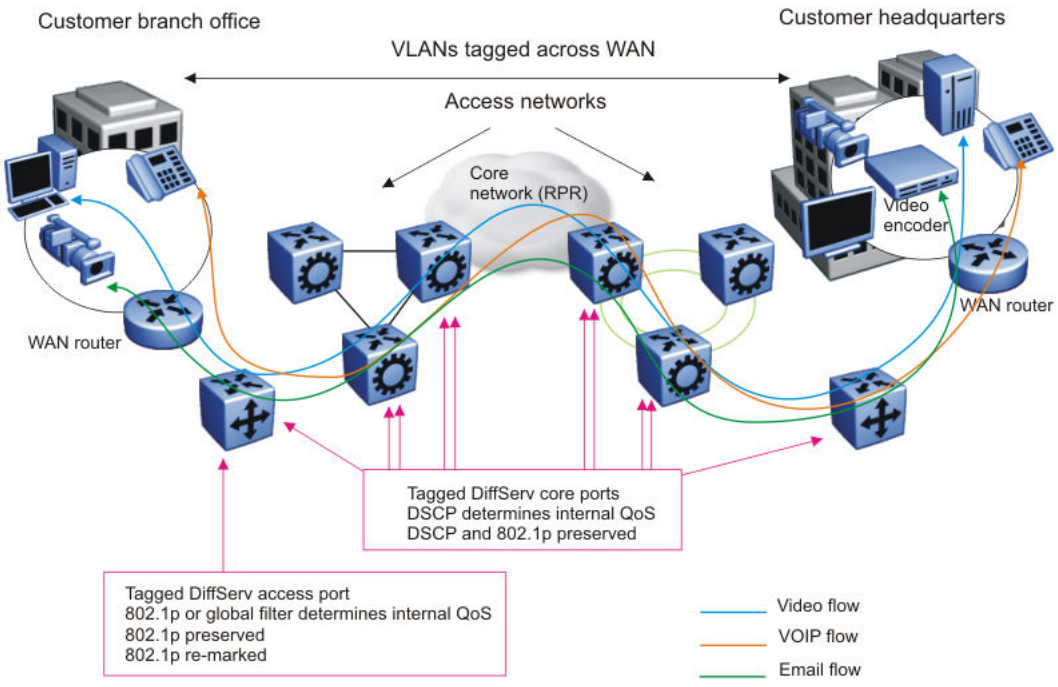


Figure 3: Trusted bridged traffic

For bridged, untrusted traffic, if you configure the port to access, mark and prioritize traffic on the access node using global filters. Reclassify the traffic to ensure it complies with the class of service specified in the SLA.

For Resilient Packet Ring (RPR) interworking, you can assume that, for all incoming traffic, the QoS configuration is properly marked by the access nodes. The core switch ports, configured as core or trunk ports, perform the RPR interworking. These ports preserve the DSCP marking and re-mark the 802.1p bit to match the 802.1p bit of the RPR. The following figure shows the actions performed on three different traffic flows (VoIP, video conference, and email) over an RPR core network.

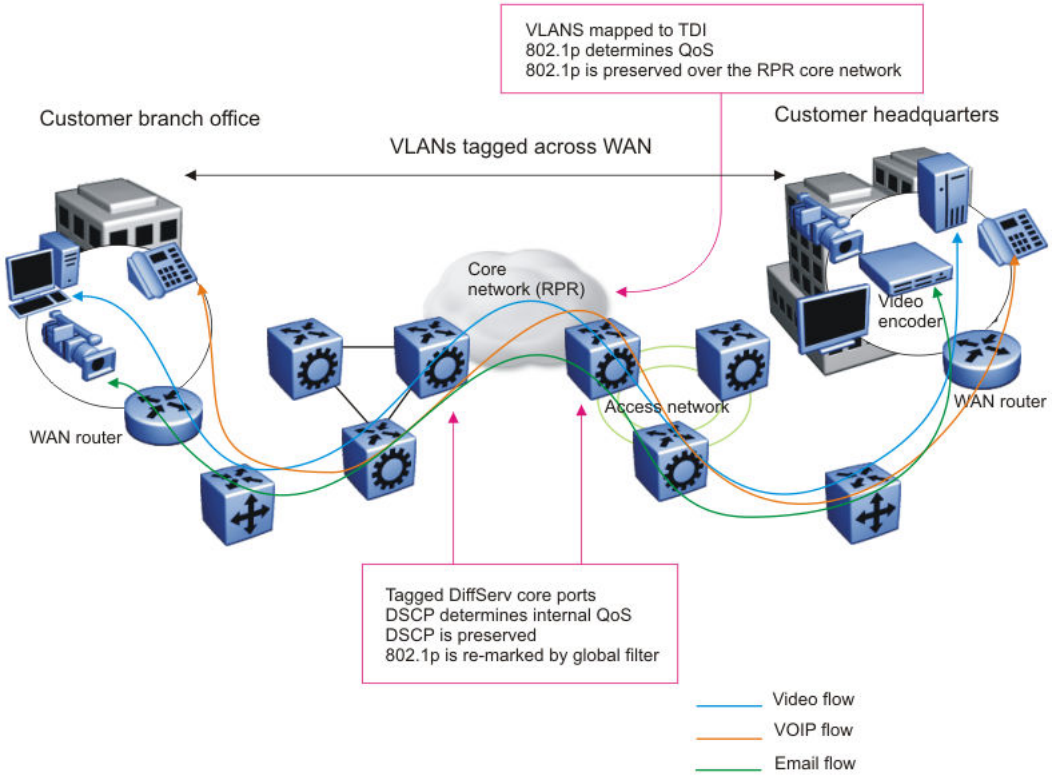


Figure 4: RPR QoS internetworking

Routed traffic

If you route traffic over the core network, VLANs are not kept separate.

If you configure the port to core, you assume that, for all incoming traffic, the QoS configuration is properly marked. All core switch ports simply read and forward packets. The switch does not re-mark or classify the packets. The customer device or the edge devices perform all initial QoS markings.

The following figure shows the actions performed on three different routed traffic flows (that is VoIP, video conference, and email) at access and core ports throughout the network.

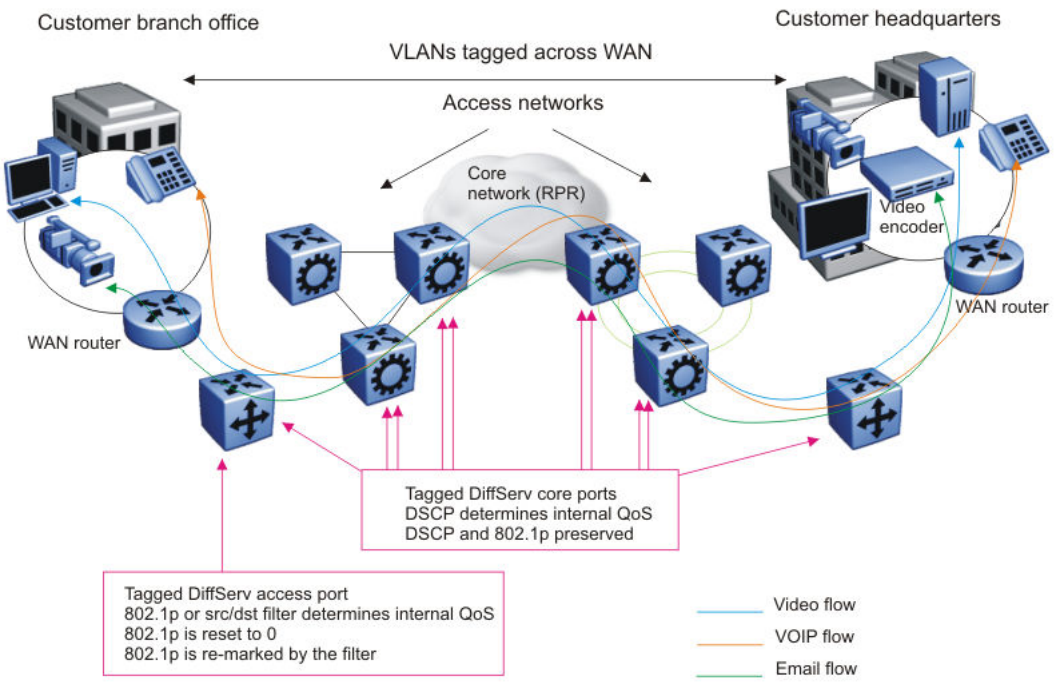


Figure 5: Trusted routed traffic

For routed, untrusted traffic, in an access node, packets that enter through a tagged or untagged access port exit through a tagged or untagged core port.

Chapter 4: Traffic filtering fundamentals

Use the information in this section to help you understand filtering. This section describes a range of features that you can use with the Avaya Virtual Services Platform 4000 Series to allocate network resources to apply filters.

In a large and busy network, traffic management is very important and can be complex. Traffic filtering can generally provide a mechanism to accurately manage and secure network flows or prioritize crucial information over other network traffic. Some of the primary uses of filtering are:

- accurately manage traffic flows
- implement security permissions on network traffic
- prioritize mission critical traffic flows
- redirecting traffic to firewalls or other devices to efficiently manage bandwidth

Overview

Traffic filtering on the Avaya Virtual Services Platform 4000 Series is based on an ACL filter implementation. Access Control List (ACL) based filters are a means to provide predictable and flexible traffic filtering. ACL Traffic filters can be configured using the Avaya Command line interface (ACLI) or the Enterprise Device Manager (EDM). ACL filters set a list of criteria for the network traffic to be matched against, performing a predefined set of actions. Access Control Lists and Action Control Entries provide traffic filtering services on the Virtual Service Platform 4000.

QoS and filters

The switch has functions that you can use to provide appropriate QoS levels to traffic for each customer, application, or packet. These functions include port-based shapers, DiffServ access or core port settings, and port-based policers. The switch also provides access control list (ACL)-based filters. You do not need to use filters to provide QoS; however, filters aid in prioritizing customer traffic. Filters also provide protection by blocking unwanted traffic.

Policers apply at ingress; shapers apply at egress. ACL-based filters apply at ingress and egress.

There are four ingress filter groups:

- Port-based Security ACEs

- Port-based QoS ACEs
- VLAN-based Security ACEs
- VLAN-based QoS ACEs

Filters help you provide QoS by permitting or dropping traffic based on the parameters you configure. You can use filters to mark packets for specific treatment.

Typically, filters act as firewalls or are used for Layer 3 redirection. In more advanced cases, traffic filters can identify Layer 3 and Layer 4 traffic streams. The filters cause the streams to be re-marked and classified to attain a specific QoS level at both Layer 2 (802.1p) and Layer 3 (DSCP).

Traffic filtering is a key QoS feature. The switch, by default, determines incoming packet 802.1p or DiffServ markings, and forwards traffic based on their assigned QoS levels. However, situations exist where the markings are incorrect, or the originating user application does not have 802.1p or DiffServ marking capabilities. Also, you can give a higher priority to select users (executive class). In these situations, use filters to prioritize specific traffic streams.

You can use filters to assign QoS levels to devices and applications. To help you decide whether to use a filter, key questions include:

1. Does the user or application have the ability to mark QoS information on data packets?
2. Is the traffic source trusted? Are the QoS levels configured appropriately for each data source?

   Users can maliciously configure QoS levels on their devices to take advantage of higher priority levels.
3. Do you want to prioritize traffic streams?

This decision-making process is outlined in the following figure.

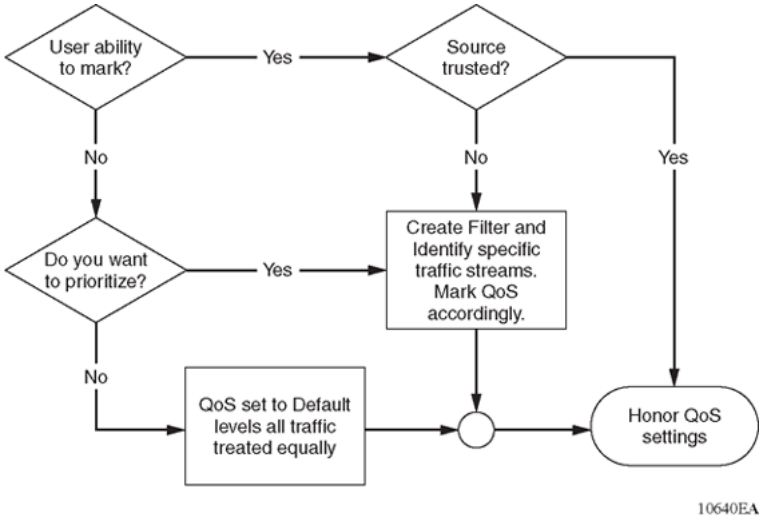


Figure 6: Filter decision-making process

Configure filters through the use of Access Control Lists (ACL) and Access Control Entries (ACE), which are implemented in hardware. An ACL can include both security and QoS type ACEs. The

platform supports 2048 ACLs and 1000 ACEs for each ACL to a maximum of 16,000 ACEs for each plaform.

Note:

The switch supports a maximum of 256 IPv6 ingress port/vlan security ACL/Filters. IPv6 ingress QoS ACL/Filters and IPv6 egress security and QoS ACL/Filters are not supported.

The following steps summarize the filter configuration process:

1. Determine your desired match fields.
2. Create an ACL.
3. Create an ACE within the ACL.
4. Configure the desired precedence, traffic type, and action.

   You determine the traffic type by creating an ingress or egress ACL.
5. Modify the parameters for the ACE.

Access control lists

Rules can be applied to incoming and outgoing traffic. An ACL can be associated with either a port interface or a VLAN interface. The total number of ACLs that can be configured on the Virtual Services Platform 4000 system is 1500.

There are three ways an ACL can be associated with interfaces:

- Ingress port (inPort)
- Ingress VLAN (inVLAN)
- Egress port (outPort)

Note:

VSP 4000 supports a maximum of 256 IPv6 ingress port/vlan security ACL/Filters. IPv6 ingress QoS ACL/Filters and IPv6 egress security and QoS ACL/Filters are not supported.

The ingress VLAN ACL associations apply to all the active port members of a VLAN. An ACL is created in the enabled state by default.

An ACL can contain multiple filter rules called Access Control Entries (ACE). ACEs provide match criteria and rules for ACL-based filters. An ACE can provide actions such as dropping a packet, monitoring a packet, or remarking QoS on a packet. Complete lists of actions are provided in the Access Control Entries section. After an ingress or egress packet meets the match criteria specified in ACEs within an ACL, the system executes the predefined action.

ACLs provide the ability to configure default and global actions. A default action is applied when no filter rule (ACE) matches on a packet flow. The global action is executed when any filter rule (ACE) matches on a packet flow. The default action mode for ACLs is permit. ACL global actions are:

- monitor-dst-mlt
- monitor-dst-ports

The following figure shows the relationships between ACEs and ACLs.

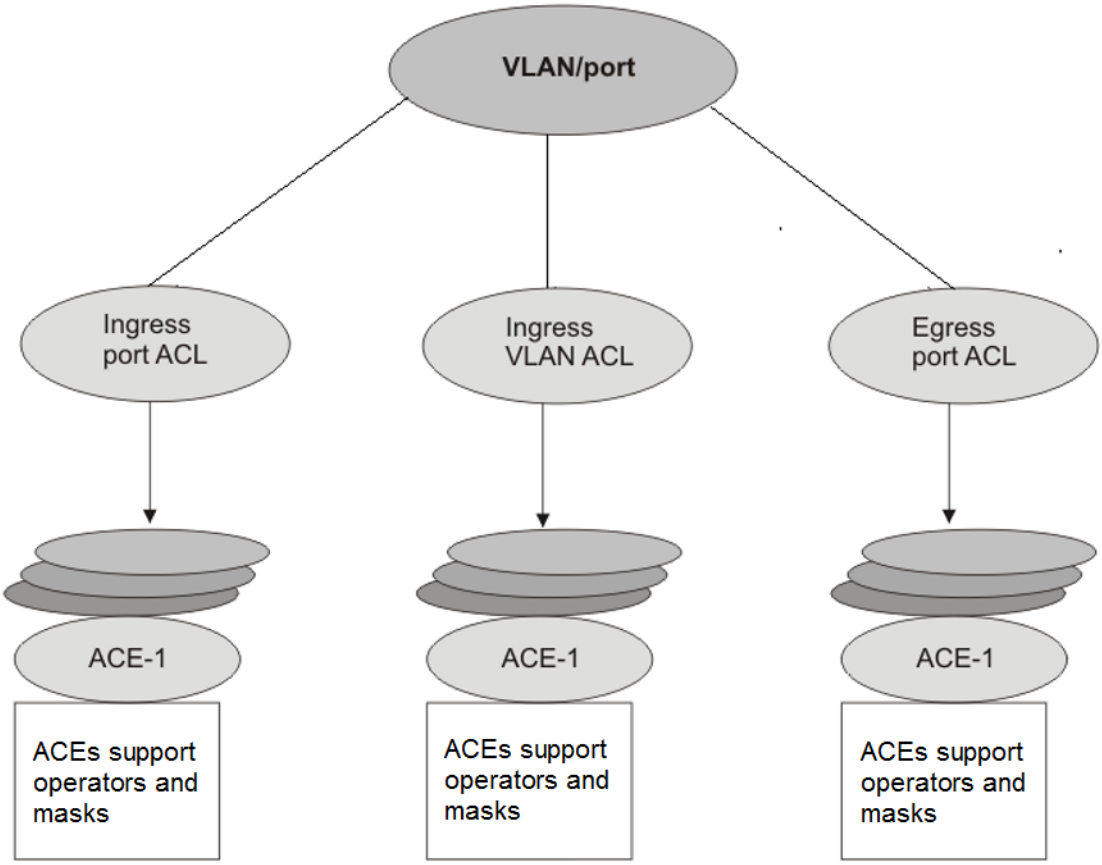


Figure 7: ACE and ACL relationships

Switched UNI ACL Filters

InPort and OutPort filters are supported on Switched UNI (S-UNI) and Fabric Attach ports.

Note:

InPort and outPort filters are supported on S-UNI and Fabric Attach ports for the traffic mapped to an I-SID which does not have platform VLAN associated. The Customer VLAN-ID (CVID) can be applied as VLAN-ID qualifier in inPort and outPort filters.

Note:

InPort, outPort, and inVLAN filters are supported on S-UNI and Fabric Attach ports for the traffic mapped to an I-SID which has platform VLAN associated. The platform VLAN should be used as VLAN-ID in inPort and inVLAN filters, and the CVID as VLAN-ID in the outPort filter.

Access control entries

The Virtual Services Platform 4000 filter rules are defined using Access Control Entries (ACE). An ACE is an ordered set of filter rules contained in an Access Control List (ACL). ACE rules are divided into 3 different components:

1. Operators
2. Attributes
3. Actions

An ACE generally operates on fields in a packet. If a packet field matches an ACE rule, the system executes the action specified. As each packet enters through an interface with an associated ACL, the system scans the ACE list configured on that ACL and matches on the packet fields. If multiple ACE rules are associated with the ACL, the lower ACE ID will have a higher precedence. The system supports a maximum 766 ACE in ingress, and 252 in egress globally for each individual ACL. If you disable an ACL, the ACL state affects the administrative state of all of the ACEs within it.

Operators

ACEs use operators to match on packet fields. The Virtual Services Platform 4000 supports the following operators:

- Equal-to

  This rule operator looks for an exact match with the field defined. If the field matches exactly with the rule, the system will return a match (hit). If the rule does not match, the search continues and at the end of the search a miss is returned.

- Mask

  ACL-based filters provide the mask operator to match on Layer 2, Layer 3, and Layer 4 packet fields. The mask operator is used to mask bits in packet fields during a search or to match on a partial value of a packet field. This section provides examples of the mask operator.

  If a mask bit is set to 1, it means it is not part of the match criteria (treated as do not care), and a mask bit of 0 means that the value represented is part of the match criteria. You can use the mask operator for the following attributes:

  - source MAC address
  - destination MAC address
  - VLAN ID
  - Dot1p
  - source IP address
  - destination IP address
  - DSCP
  - Layer 4 source port
  - Layer 4 destination port
  - TCP flags

  The ACL and ACE configuration syntax for a mask is similar to how you use the equal operator except that you must provide the mask value. As part of the configuration you can specify a

mask value (number) to represent the bits to mask in the attribute. You can define a mask in different ways depending on the attribute you need to mask. If you use a decimal number for the mask, the mask value applies to the least significant bits on that attribute. For example, a mask of 24 used with an IP address is the same as a mask of 0.255.255.255, and a mask of 24 used with a MAC address is the same as 0x000000ffffff. A mask of 16 used with an IP address is the same as a mask of 0.0.255.255, and a mask of 32 used with a MAC address is the same as 0x00000000ffff.

The following table explains the mask operator for MAC addresses.

Table 7: Mask operator for MAC address

Rule	Result
`filter acl ace ethernet 10 10 dst-mac mask 01:00:5e:00:00:01 0x000000FFFFFF`	The rule matches only on the most significant 24 bits as they are not masked, for example, 01:00:5e, and does not care about the least significant 24 bits because they are masked; the least significant 24 bits can have a value of 00:00:00 - FF:FF:FF.
`filter acl ace ethernet 10 10 dst-mac mask 0x01:00:5e:00:00:01 0xFFFFFFFF0000`	The rule matches only on the least significant 16 bits because they are not masked, for example, 00:01, and does not care about the most significant 32 bits because they are masked; the most significant 32 bits can have a value of 00:00:00:00 – FF:FF:FF:FF.
`filter acl ace ethernet 10 10 dst-mac mask 0x01:00:5e:00:00:01 0xFF00FF0000FF`	The rule matches only on the unmasked bits, for example, 0xXX:00:XX:00:00:XX. The rule matches only on the bits not masked, for example, all the zeroes and the x represents a do not care (0xXX: 00:XX:00:00:XX)

The following table explains the mask operator for IP addresses.

Table 8: Mask operator for IP address

Rule	Result
`filter acl ace ip 10 10 src-ip mask 2.10.10.12 0.255.255.255`	The rule matches only the most significant 8 bits, and does not care about the value of the remaining 24 bits as they are considered masked. For example, 10.10.12. Packets with a source IP address of 2.15.16.122 or 2.3.4.5 match on the filter rule while packets with a source IP address of 3.10.10.12 and 4.10.10.12 do not match on the filter rule.
`filter acl ace ip 10 10 src-ip mask 3.4.5.6 255.255.255.0`	The rule matches only the least significant 8 bits, for example, 6, and does not case about the most significant 24 bits, 3.4.5. Packets with a source IP address of 17.16.5.6 or 192.168.1.6 match on the filter rule while packets with a source IP address of 3.4.5.4 or 3.4.5.7 do not match on the filter rule.

The following table explains the mask operator for Layer 4 source port.

Table 9: Mask operator for Layer 4 source port

Rule	Result
`filter acl ace protocol 10 10 src-port mask 80 0xF`	The filter rule matches on Layer 4 source port 80 (1010000). The mask value 0xF (1111) masks the least significant 4 bits, which means source port 81 (1010001) through 95 (1011111) also match this filter rule. This means the range 80–95 is a match on this rule.

The following table demonstrates the resulting action based on mask configuration and example packets.

Table 10: Mask operator configuration examples

Filter configuration	Address examples that match the filter	Address examples that do not match the filter

Ethernet mask:
`filter acl 1000 type inport`
`filter acl port 1000 1/5,1/11`
`filter acl ace 1000 12`
`filter acl ace ethernet 1000 12 src-mac mask 00:00:11:11:16:00 0x00ff000000f0`
`filter acl ace action 1000 12 permit count`
`filter acl ace 1000 12 enable`
	Source MAC:
	00:01:11:11:16:10
	00:10:11:11:16:f0 00:1f:11:11:16:10 00:ff:11:11:16:f0
	00:00:11:11:16:60
	00:e6:11:11:16:e0
		Source MAC:
		00:00:11:11:16:01
		00:ff:11:11:16:f1

`filter acl ace 1000 1000`
`filter acl ace ethernet 1000 1000 dst-mac mask 00:00:00:64:16:00 0x00000060001f`
`filter acl ace action 1000 1000 deny count`
`filter acl ace 1000 1000 enable`
	Destination MAC:
	00:00:00:64:16:01
	00:00:00:04:16:01
	00:00:00:24:16:1f
	00:00:00:64:16:1f
	00:00:00:44:16:10
	00:00:00:04:16:05
		Destination MAC:
		00:00:00:24:16:20
		00:00:00:64:16:20
		00:00:00:63:16:01
		00:00:00:65:16:01

IP mask (dotted decimal notation):
`filter acl 10 type outport`
`filter acl port 10 1/13`
`filter acl ace 10 11`
`filter acl ace ethernet 10 11 ether-type eq ip`
`filter acl ace ip 10 11 src-ip mask 192.168.4.0 0.0.0.31`
`filter acl ace action 10 11 permit count`
`filter acl ace 10 11 enable`
	Source IP: 192.168.4.1
	192.168.4.10
	192.168.4.30
	192.168.4.31
		Source IP:
		192.168.3.1
		192.168.4.32

`filter acl ace 10 12`
`filter acl ace ethernet 10 12 ether-type eq ip`
`filter acl ace ip 10 12 dst-ip mask 192.168.7.0 0.0.0.3`
`filter acl ace action 10 12 deny count`
`filter acl ace 10 12 enable`
	Destination IP:
	192.168.7.1 192.168.7.3
		Destination IP:
		192.168.7.4
		192.168.7.5

Table continues…

Filter configuration	Address examples that match the filter	Address examples that do not match the filter

IP mask (decimal notation):
`filter acl 10 type outport`
`filter acl port 10 1/13`
`filter acl ace 10 11`
`filter acl ace ethernet 10 11 ether-type eq ip`
`filter acl ace ip 10 11 src-ip mask 192.168.4.0 255.255.255.31`
`filter acl ace action 10 11 permit count`
`filter acl ace 10 11 enable`
	Source IP: 192.168.4.1
	192.168.4.10
	192.168.4.30
	192.168.4.31
		Source IP:
		192.168.3.1
		192.168.4.32

`filter acl ace 10 12`
`filter acl ace ethernet 10 12 ether-type eq ip`
`filter acl ace ip 10 12 dst-ip mask 192.168.7.0 255.255.255.3`
`filter acl ace action 10 12 deny count`
`filter acl ace 10 12 enable`
	Destination IP:
	192.168.7.1
	192.168.7.3
		Destination IP:
		192.168.7.4
		192.168.7.5

Protocol mask:
`filter acl 901 type inport`
`filter acl port 901 1/2`
`filter acl ace 901 1`
`filter acl ace ip 901 1 ip-protocol-type eq tcp`
`filter acl ace protocol 901 1 src-port mask 256 0xff`
`filter acl ace action 901 1 deny count`
`filter acl ace 901 1 enable`
	TCP source port 256
	TCP source port 356
	TCP source port 511
	This mask implies packets with TCP source port 256–511 match the filter, while 0–255 and > 511 miss the filter.
		TCP source port 255
		TCP source port 512

Attributes

Attributes are fields in a packet (Layer 2, Layer 3, Layer 4) or other information related to the packet on which an ACE rule is applied like slot/port. The list of all the attributes and the operators that could be applied on them are listed below.

Table 11: Attribute list

Attribute Name	Operator
Slot/Port	Equal
Destination MAC	Equal, Mask
Source MAC	Equal, Mask
VLAN ID	Equal, Mask
.1p bits	Equal, Mask
Ether Type	Equal
ARP Opcode	Equal
Source IP	Equal, Mask
Destination IP	Equal, Mask

Table continues…

Attribute Name	Operator
Protocol Type	Equal
Type of Service	Equal, Mask
IP Fragmentation	Equal
IP Options	Equal
Layer 4 Destination Port	Equal, Mask
Layer 4 Source Port	Equal, Mask
TCP Flags	Equal, Mask
ICMP Message Type	Equal

Actions

Actions occur when the filter rule is hit or missed. The types of actions filter configuration can execute are split into two categories:

- Security actions supported by the ACE IDs in the range of 1-1000
- QoS actions supported by the ACE IDs in the range of 1001-2000

Filter rules supporting Security actions and QOS actions are stored separately. When an ACL filter is applied to a traffic flow, the Virtual Services Platform 4000 performs a parallel search on both Security and QOS ACE lists, resulting in distinct and non-conflicting actions.

Virtual Services Platform 4000 supports the following actions on both ingress and egress:

- Redirect Next Hop
- Count
- Mirror
- Remark

Note:

Egress filters (port based) do not support the action of remark-dot.1p.

Note:

Security and QoS ACE actions are only supported on Ingress ACLs. Egress ACLs do not support QoS ACEs.

The supported Virtual Services Platform 4000 actions are listed below.

Table 12: Security ACE Actions

Security ACE Actions	User supplied parameters	Comments
Mode	Permit or Deny	Applies to both ingress and egress ACLs.
Redirect Next-Hop	IP address	Re-directs the packet to the user supplied IP address. If the switch cannot resolve ARP for the user-specified next-hop, packets that match the filter are dropped. Applies to ingress ACLs only.
Count	None	Collect ACE statistics . Applies to ingress and egress ACLs.
Mirror	Port or list of ports or MLT-ID.	Applies to ingress and egress ACLs.

Table 13: QoS ACE Actions

QOS ACE Actions	User supplied parameters	Comments
Remark	• DCSP • .dot1p (ingress only) • Internal-qos	Applied to Ingress ACLs.
Count	None	Applied on Ingress/Egress ACLs.

Conflict and Precedence

The Virtual Services Platform 4000 supports both port-based and VLAN-based ACLs. As shown in Figure 7: ACE and ACL relationships on page 37, a port can be associated with both Port-based ACL and a VLAN-based ACL. Within an ACL, a rule match can generate Security actions and QOS actions. The Virtual Services Platform 4000 system goes through a set of precedence levels to resolve any conflicting actions between Port-based ACL and VLAN-based ACL lookup. The table below lists all decisions for all possible conflicts between Port and VLAN-based ACLs and Security and QoS ACE search results in each of those ACLs.

Table 14: Conflict and Precedence resolution

Port-based ACL look up		Actions performed on Port-based ACL		If VLAN-based ACL is enabled		Actions perform on VLAN-based ACL search	
Security	**QoS**	**Security Action**	**QoS Action**	**Security**	**QoS**	**Security Action**	**QoS Action**
Security ACE search is a Miss and ACL mode is Permit.	QoS ACE search is a Miss	Default security statistics collected	Default QoS statistics collected	Security ACE search is a Miss and mode is set to Permit	QoS ACE search is a Miss	Collect default Miss statistics	Collect default Miss statistics
				Security ACE search is a Miss and mode is set to Permit	QOS ACE search returns a Hit	Collect default Miss statistics	Execute configured ACE and default ACL actions
				Security ACE search is a Miss and mode is set to Deny	Search result is invalid, since security mode is set to Deny	Drop packet and collect default Miss statistics	No action is executed
				Security ACE search is a Hit and mode is set to Permit	QOS ACE search returns a Miss	Execute configured ACE and default ACL actions	Collect default Miss statistics
				Security ACE search is a Hit and mode is set to Permit	QoS ACE search is a Hit	Execute configured ACE and default ACL actions	Execute configured ACE and default ACL actions
				Security ACE search is a Hit and mode is set to Deny	QoS ACE search returns a Hit	Discard the packet and execute configured ACE and global actions	No action is executed
Security ACE is	Search result is	Discard the packet and	No action is executed	VLAN-based ACL	VLAN-based ACL	No action is executed	No action is executed

Table continues…

Port-based ACL look up		Actions performed on Port-based ACL		If VLAN-based ACL is enabled		Actions perform on VLAN-based ACL search	
Security	**QoS**	**Security Action**	**QoS Action**	**Security**	**QoS**	**Security Action**	**QoS Action**
Miss and ACL mode is Deny	invalid since security mode is set to Deny	collect default statistics		is not configured	is not configured		
Security ACE search is a Miss and ACL mode is set to Permit	QoS ACE search is a Hit	Default search statistics collected	Execute configured ACE and default ACL actions	Security ACE search is a Miss and mode is set to Permit	Port-based ACL's QoS action take precedence . QoS search result invalid.	Collect default Miss statistics	No action is executed
				Security ACE search is a Miss and mode is set to Deny	Port-based ACL's QoS action take precedence . QoS search result invalid.	Drop packet and collect default Miss statistics	No action is executed
				Security ACE search is a Hit and mode is set to Permit	Port-based ACL's QoS action take precedence . QoS search result invalid.	Execute configured ACE and default ACL actions	No action is executed
				Security ACE search is a Hit and mode is set to Deny	Port-based ACL's QoS action take precedence . QoS search result invalid.	Discard the packet and execute configured ACE and global Actions	No action is executed
Security ACE search is a Hit and	QoS ACE search is a Miss	Execute configured ACE and default ACL actions	Collect default Miss statistics	Port-based ACL's Security action take precedence	QoS ACE search returns a Miss	No action is executed	Collect default Miss statistics

Table continues…

Port-based ACL look up		Actions performed on Port-based ACL		If VLAN-based ACL is enabled		Actions perform on VLAN-based ACL search	
Security	**QoS**	**Security Action**	**QoS Action**	**Security**	**QoS**	**Security Action**	**QoS Action**
ACE mode is Permit				. Security search result invalid			
				Port-based ACL's Security action take precedence . Security search result invalid.	QoS ACE search returns a Hit	No action is executed	Execute configured ACE and default ACL actions
Security ACE search is a Hit and ACE mode is Permit	QoS ACE search is a Hit	Execute configured ACE and default ACL actions	Execute configured ACE and default ACL actions.	Port-based ACL's Security action take precedence . Security search result invalid	Port-based ACL's QoS action take precedence . QoS search result invalid.	No action is executed	No action is executed
Security ACE search is a Hit and ACE mode is Deny	Search result is invalid since Security mode is set to Deny	Discard the packet and collect default statistics	No action is executed	Port-based ACL's Security action take precedence . Security search result invalid	Port-based ACL's QoS action take precedence . QoS search result invalid.	No action is executed	No action is executed

Common ACE uses and configuration

The following table describes configurations you can use to perform common actions.

Table 15: Common ACE uses and configurations

Function	ACE configuration
Permit a specific host to access the network	• Use action permit.

Table continues…

Function	ACE configuration

	• Configure the source IP address to be the host IP address.
	`filter acl ace 1 5 name "Permit_access_to_1.2.3.4"`
	`filter acl ace action 1 5 permit`
	`filter acl ace ethernet 1 5 ether-type eq ip`
	`filter acl ace ip 1 5 src-ip eq 1.2.3.4`
	`filter acl ace 1 5 enable`

Deny a specific host from accessing the network	• Use action deny.
	• Configure the source IP address to be the host IP address.
	`filter acl ace 1 5 name "Deny_access_to_1.2.3.4"`
	`filter acl ace action 1 5 deny`
	`filter acl ace ethernet 1 5 ether-type eq ip`
	`filter acl ace ip 1 5 src-ip eq 1.2.3.4`
	`filter acl ace 1 5 enable`

Deny Telnet traffic	• Use action deny.
	• Configure the protocol as TCP and the TCP destination port to be 23.
	`filter acl ace 1 5 name "Deny_telnet"`
	`filter acl ace action 1 5 deny`
	`filter acl ace ethernet 1 5 ethertype eq ip`
	`filter acl ace ip 1 5 ip-protocol-type eq tcp`
	`filter acl ace protocol 1 5 dst-port eq 23`
	`filter acl ace 1 5 enable`

Deny FTP traffic	• Use action deny.
	• Configure the protocol as TCP and the TCP destination port to be 21.
	`filter acl ace 1 5 name "Deny_ftp"`
	`filter acl ace action 1 5 deny`
	`filter acl ace ethernet 1 5 ethertype eq ip`
	`filter acl ace ip 1 5 ip-protocoltype eq tcp`
	`filter acl ace protocol 1 5 dst-port eq 21`
	`filter acl ace 1 5 enable`

Traffic filter configuration

Traffic filtering manages traffic by defining filtering conditions and associating these conditions with specific actions. The following steps summarize the filtering configuration process:

1. Determine your desired match fields.
2. Configure an ACL and associate it with Ingress or Egress traffic flow.

3. Configure an ACE within the ACL.
4. Configure the desired precedence, attributes, and action.
5. Enable the ACE.

ACL filters behavior

The implementation of ACL filters in VSP 4000is similar to VSP 8000 and VSP 7200, but there are some differences as summarized in the following table.

	VSP 4000	VSP 8000 / VSP 7200
Hardware filter engine resources	Support for four ingress filter groups 1. port-based Security ACEs 2. port-based QoS ACEs 3. VLAN-based Security ACEs 4. VLAN-based QoS ACEs	Support for two ingress filter groups 1. port-based and VLAN-based Security ACEs 2. port-based and VLAN-based QoS ACEs
	For each ingress packet a parallel search is performed on each of the four groups.	For each ingress packet a parallel search is performed on each of two groups.
Behavior of incoming packets An incoming packet can match both port-based and VLAN-based ACL/ACE	Regardless of the type of matching ACEs (Security or QoS), the action of either the highest priority matching ACE or the default action will be performed.	Port-based ACLs have precedence over VLAN-based ACLs. If the matching ACEs are of the same type (both Security or both QoS), then the VLAN based ACL/ACE will be ignored.

Filter limitations

The switch does not support logging and pcap with filters.

The following identifies known ACL limitations with the switch:

- Only Port-based ACLs are supported on egress. VLAN-based ACLs are not supported.
- On egress (outPort) ACLs, the global-action is not supported.
- IPv6 ingress QoS ACL/Filters and IPv6 egress security and QoS ACL/Filters are not supported.
- Control packet action is not supported on IPv6 filters.
- IPv4/IPv6 VLAN based ACL filters will be applied on traffic received on all the ports if it matches VLAN ID associated with the ACL.

- Scaling numbers are reduced for IPv6 filters. For more information about scaling numbers, see *Release Notes for VSP Operating System Software*, NN47227-401

The following identifies known ACE limitations with the switch:

- When an ACE with action count is disabled, the statistics associated with the ACE are reset.
- Only security ACEs are supported on egress. Qos ACEs are not supported.
- ICMP type code qualifier is supported only on ingress filters.

  For port-based ACLs, you can configure VLAN qualifiers. Configuring Port qualifiers are not permitted.
- For VLAN-based ACLs, you can configure port qualifiers. Configuring VLAN qualifiers are not permitted.
- Mirroring actions (monitor-dst-ports, monitor-dst-mlt) are only supported on ingress filters.
- Egress Security/QoS filters are not supported for IPv6 filters.
- Ingress QoS filters are not supported for IPv6 filters.
- Source/Destination MAC addresses cannot be added as attributes for IPv6 filters ACEs.
- If more than 256 IPv6 filters are configured, number of IPv4 filters will get reduced.

Chapter 5: Basic DiffServ configuration using ACLI

Use Differentiated Services (DiffServ) to provide appropriate Quality of Service (QoS) to specific traffic types.

Note:

The default prompt for the non-PowerPlus chassis is VSP-4850GTS. The default prompt for the PowerPlus chassis is VSP-4850GTS-PWR+. The default prompt for the PowerPlus chassis with additional fiber ports is VSP-4450GSX-PWR+. For consistency, this document uses the VSP-4850GTS prompt.

Enabling DiffServ on a port

Enable DiffServ so that the system provides DiffServ-based QoS on the port. By default, DiffServ is enabled.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet {slot/port[-slot/port][,...]}
   ```

2. Enable DiffServ:

   ```
   enable-diffserv [port {slot/port[-slot/port][,...]}] [enable]
   ```

3. Disable Diffserv:

   ```
   no enable-diffserv [port {slot/port[-slot/port][,...]}] [enable]
   ```

Variable definitions

Use the data in the following table to use the `enable-diffserv` command.

Table 16: Variable definitions

Variable	Value
enable	Enables DiffServ for the specified port. The default is enabled.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (1/1) or a range of slots and ports (1/1-1/48).

Configuring Layer 3 trusted or untrusted ports

Configure a port as trusted or untrusted to determine the Layer 3 QoS actions the switch performs. A trusted (core) port honors incoming Differentiated Services Code Point (DSCP) markings. An untrusted (access) port overrides DSCP markings. The default configuration is trusted.

Before you begin

- DiffServ is enabled.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet {slot/port[-slot/port][,...]}
   ```

2. Configure the port as an access port:

   ```
   access-diffserv [port {slot/port[-slot/port][,...]}] [enable]
   ```

3. Configure the port as a core port:

   ```
   no access-diffserv [port {slot/port[-slot/port][,...]}] [enable]
   ```

Variable definitions

Use the data in the following table to use the `access-diffserv` commands.

Table 17: Variable definitions

Variable	Value
enable	If enabled, specifies an access port and overrides incoming DSCP bits. If disabled, specifies a core port that honors and services incoming DSCP bits.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (1/1) or a range of slots and ports (1/1-1/48).

Configuring Layer 2 trusted or untrusted ports

Configure a port as trusted or untrusted to determine the Layer 2 QoS actions the switch performs. A trusted port (override disabled) honors incoming 802.1p bit markings. An untrusted port (override enabled) overrides 802.1p bit markings.

Before you begin

- DiffServ is enabled.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet {slot/port[-slot/port][,...]}
   ```

2. Configure the port as Layer 2 untrusted:

   ```
   qos 802.1p-override [enable]
   ```

3. Configure the port as Layer 2 trusted:

   ```
   no qos 802.1p-override [enable]
   ```

Variable definitions

Use the data in the following table to use the `qos 802.1p-override` command.

Table 18: Variable definitions

Variable	Value
enable	If you use this variable, the port overrides incoming 802.1p bits; if you do not use this variable, the port honors and services incoming 802.1p bits. The default is disable (Layer 2 trusted).

Configuring the port QoS level

Configure the port QoS level to assign a default QoS level for all traffic if the packet does not match an access control list (ACL) that re-marks the packet. If you configure port QoS levels, Layer 2 and Layer 3 traffic from the same port use the same QoS level. The default value is 1.

About this task

For VoIP traffic, Avaya recommends that you use QoS level 6.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet {slot/port[-slot/port][,...]}
   ```

2. Configure the port QoS level:

   ```
   qos level [port {slot/port}] <0-6>
   ```

Variable definitions

Use the data in the following table to use the `qos level` command.

Table 19: Variable definitions

Variable	Value
<0-6>	Specifies the default QoS level for the port traffic. The system reserves QoS level 7 for network control traffic. The default is 1.
port {slot/port}	Specifies the slot and port

Chapter 6: Basic DiffServ configuration using EDM

Use DiffServ to implement classification and mapping functions at the network boundary or access points to regulate packet behavior. You can configure a port as a trusted (core) or an untrusted (access) port at both Layer 2 and Layer 3.

You can also perform many of the procedures in this section on the Interface tab for the selected port. The procedures in this section show only one configuration method.

Enabling DiffServ for a port

Enable DiffServ so that the switch provides DiffServ-based Quality of Service (QoS) on the port.

About this task

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **Port QoS Config**.
3. In the row for the port, double-click the cell in the **DiffServ** column.
4. Select **true**.
5. Click **Apply**.

QoS Port Config field descriptions

Use the data in the following table to use the **Port QoS Config** tab.

Name	Description
Index	Specifies an index value that uniquely identifies a port.
DiffServ	Specifies whether DiffServ is enabled (true) or disabled (false) on the port. The default is true. This variable works in conjunction with Layer3Trust. The DiffServ variable is a global parameter that affects QoS DSCP operations. If the DiffServ parameter is false (DiffServ

Table continues…

Name	Description
	disabled), the system does not use the DSCP parameter for classification or modify it. If this variable is true, it activates the Layer3Trust parameter.
Layer3Trust	Configures the Layer 3 trusted port as an access or core port. The default is core. Core configures the port to a trusted state and access configures the port to an untrusted state. The DiffServ parameter determines the operation of this variable. The operation depends on whether the port is tagged or untagged. Tagged packet operation depends on the Layer2 8021p Override variable. If DiffServ is false, Layer3Trust has no effect; no modification of the DSCP or TOS bits occurs. If DiffServ is true, the core and access configuration take affect.
Layer2Override8021p	Specifies whether Layer 2 802.1p override is enabled (true) or disabled (false) on the port. The default is false. This variable primarily affects tagged packet treatment, but can also affect the treatment of the DSCP parameter. If Layer2Override8021p is false, the port trusts the 802.1p-bits portion of a Q-tagged packet. The port trusts the 802.1p-bits marking regardless of the port setting (tagged or untagged); however, if the discard tagged packets parameter (DiscardTaggedFrames) on an untagged port is true, the system discards the packet. If Layer2Override8021p is true, the port does not trust the 802.1p bit marking. In this case, the QoS operation depends on other parameters, such as DiffServ and Layer3Trust, or the port QoS level.
QosLevel	Specifies the QoS level to use when the system processes packets carried on this port. Values range from level 0–6 (the system reserves 7 for network control traffic). The default is 1.

Configuring Layer 3 trusted or untrusted ports

Configure a port as trusted or untrusted to determine the Layer 3 QoS actions the switch performs. A trusted port honors incoming DSCP markings. An untrusted port overrides DSCP markings. The default is trusted.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **Port QoS Config**.
3. In the row for the port, double-click the cell in the **Layer3Trust** column.
4. Select **core** (trusted) or **access** (untrusted) as the port setting.
5. Click **Apply**.

Configuring Layer 2 trusted or untrusted ports

Configure a port as trusted or untrusted to determine the Layer 2 QoS actions the switch performs. A trusted port (override false) honors incoming 802.1p bit markings. An untrusted port (override true) overrides 802.1p bit markings.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **Port QoS Config**.
3. In the row for the port, double-click the cell in the**Layer2 Override 8021p** column.
4. To configure the port as a Layer 2 untrusted port, select **true**. To configure it as a Layer 2 trusted port, select **false**.

   By default, all ports are Layer 2 trusted (Layer2 Override 8021p is false).
5. Click **Apply**.

Configuring the port QoS level

Use the default port QoS level to assign a default QoS level for all traffic, if the packet does not match an access control list (ACL) to remark the packet.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **Port QoS Config**.
3. In the row for the port, double-click the cell in the **QosLevel** column.
4. Select the new level.
5. Click **Apply**.

Chapter 7: QoS configuration using ACLI

Use the procedures in this section to configure Quality of Service (QoS) on the Avaya Virtual Services Platform 4000 Series.

Note:

The default prompt for the non-PowerPlus chassis is VSP-4850GTS. The default prompt for the PowerPlus chassis is VSP-4850GTS-PWR+. The default prompt for the PowerPlus chassis with additional fiber ports is VSP-4450GSX-PWR+. For consistency, this document uses the VSP-4850GTS prompt.

Configuring broadcast and multicast bandwidth limiting

Configure broadcast and multicast bandwidth limiting to limit the amount of ingress broadcast and multicast traffic on a port. The switch drops traffic that violates the bandwidth limit.

You can configure broadcast and multicast bandwidth limiting through ACLI only; you cannot use Enterprise Device Manager (EDM).

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet {slot/port[-slot/port][,...]}
   ```

2. Configure broadcast bandwidth limiting:

   ```
   rate-limit [port {slot/port[-slot/port][,...]}] broadcast <1-65535>
   ```

3. Configure multicast bandwidth limiting:

   ```
   rate-limit [port {slot/port[-slot/port][,...]}] multicast <1-65535>
   ```

Variable definitions

Use the data in the following table to use the `rate-limit` command.

Table 20: Variable definitions

Variable	Value
<1-65535>	Specifies the bandwidth limit for broadcast and multicast traffic from 1–65535 packets per second.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (1/1) or a range of slots and ports (1/1-1/48).

Configuring the port-based shaper

Use port-based shaping to rate-limit all outgoing traffic to a specific rate.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet {slot/port[-slot/port][,...]}
   ```

2. Configure port-based shaping:

   ```
   qos if-shaper [port {slot/port}] shape-rate <64-10000000>
   ```

Variable definitions

Use the data in the following table to use the `qos if-shaper` command.

Table 21: Variable definitions

Variable	Value
port {slot/port}	Specifies the slot and port number to which to apply shaping. This variable is optional.
shape-rate *<1000-10000000>*	Configures the shaping rate from 1000–10000000 Kb/s.

Configuring a port-based policer

Use a port policer to bandwidth-limit incoming traffic. The port drops or re-marks violating traffic.

About this task

The interface policer has two configurable rates: peak rate (PIR) and service or committed rate (CIR). Traffic above PIR is marked as red. Traffic above CIR is qualified as yellow. Normally, CIR is lower than PIR. However, in ACLI you can configure these rates to equal values. Each rate has a maximum burst size associated with it, peak burst size (PBS) and committed burst size (CBS) respectively. You cannot configure the burst sizes. These values ensure maximum traffic fairness between the ports; the CBS value is lower than the PBS value. Depending on the traffic pattern, this configuration can result in a small percentage of traffic qualified as yellow or above CIR, but not red or above PIR, even if the rates are equal.

Procedure

1. Enter Interface Configuration mode:

   ```
   enable

   configure terminal

   interface GigabitEthernet {slot/port[-slot/port][,...]}
   ```

2. Configure the policing limit:

   ```
   qos if-policer [port {slot/port[-slot/port][,...]}] peak-rate
   <64-10000000> svc-rate <64-10000000>
   ```

Variable definitions

Use the data in the following table to use the `qos if-policer` command.

Table 22: Variable definitions

Variable	Value
64-10000000	Specifies the ingress rate limit in Kb/s. The range is 64–10000000.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (1/1) or a range of slots and ports (1/1-1/48).

Configuring ingress mappings

You can modify the ingress mappings to change traffic priorities. However, Avaya recommends that you use the default mappings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure 802.1p bit to QoS ingress mappings:

   `qos ingressmap 1p <0-7> <0-6>`

3. Configure DSCP to QoS ingress mappings:

   `qos ingressmap ds <0-63> <0-6>`

4. Ensure the configuration is correct:

   `show qos ingressmap [1p <0-7>] [ds <0-63>]`

Variable definitions

Use the data in the following table to use the `qos ingressmap` command.

Table 23: Variable definitions

Variable	Value
1p<*0-7*> <*0-6*>	Maps the IEEE 802.1p bit to QoS level. Each QoS level has a default IEEE 1P value: • level 0—1 • level 1—0 • level 2—2 • level 3—3 • level 4—4 • level 5—5 • level 6—6 The system reserves level 7 for Network Control. To use the default configuration, use the default option in the command: `default qos ingressmap 1p`
ds <*0-63*> <*0-6*>	Maps the DS byte to QoS level. The system reserves level 7 for Network Control. To use the default configuration, use the default option in the command: `default qos ingressmap ds`

Configuring egress mappings

You can modify the egress mappings to change traffic priorities. However, Avaya recommends that you use the default mappings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure QoS to 802.1p bit egress mappings:

   ```
   qos egressmap 1p <0-6> <0-7>
   ```

3. Configure QoS to DSCP egress mappings:

   ```
   qos egressmap ds <0-7> WORD<1-6>
   ```

4. Ensure the configuration is correct:

   ```
   show qos egressmap [1p <0-7>] [ds <0-7>]
   ```

Variable definitions

Use the data in the following table to use the `qos egressmap` command.

Table 24: Variable definitions

Variable	Value
1p<*0-6*> <*0-7*>	Maps the QoS level to IEEE 802.1p bit. Each QoS level has a default IEEE 1P value: • level 0—1 • level 1—0 • level 2—2 • level 3—3 • level 4—4 • level 5—5 • level 6—6 The system reserves level 7 for Network Control. To use the default configuration, use the default option in the command: `default qos egressmap 1p`
ds <*0-7*> *WORD<1-6>*	Maps the QoS level to DS byte. You can specify the DSCP in either hexadecimal, binary, or decimal format. To use the default configuration, use the default option in the command: `default qos egressmap ds`

Viewing port egress CoS queue statistics

View the port egress CoS queue statistics. The system displays the statistics of the forwarded packets and bytes, and the dropped packets and bytes.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. View the port egress CoS queue statistics:

   ```
   show qos cosq-stats interface <PT_PORT>
   ```

Variable definitions

Use the data in the following table to use the `show qos cosq-stats interface <PT_PORT>` command.

Table 25: Variable definitions

Variable	Value
<PT_PORT>	PT indicates the slot number; PORT indicates the port number.

The following table describes the column headings in the command output for `show qos cosq-stats interface <PT_PORT>`.

Table 26: Variable definitions

Variable	Value
Cos	Indicates the Cos queue.
Out Packets	Indicates the out packets for the Cos queue.
Out Bytes	Indicates the out bytes for the Cos queue.
Drop Packets	Indicates the drop packets for the Cos queue.
Drop Bytes	Indicates the drop bytes for the Cos queue.

Clearing port egress CoS queue statistics

Clear the port egress CoS queue statistics in the hardware.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Clear the port egress CoS queue statistics:

   ```
   clear qos cosq-stats interface <PT_PORT>
   ```

Variable definitions

Use the data in the following table to use the `clear qos cosq-stats interface <PT_PORT>` command.

Table 27: Variable definitions

Variable	Definition
<PT_PORT>	PT indicates the slot number; PORT indicates the port number.

Viewing CPU queue statistics

View the statistics of the forwarded packets and bytes, and the dropped packets and bytes for the traffic sent toward CP. The queue assignment is based on the protocol types, not on the internal CoS value. These statistics are useful for debugging purposes.

Note:

When a neighbor transitions to the STALE state, to initiate Neighbor Unreachability detection (NUD), a duplicate copy of the traffic destined to this neighbor is sent to the switch Control Processor (CP) on a low priority queue (queue 0). The original packet is forwarded to this neighbor. Once NUD is initiated, the hardware records are updated and the traffic is no longer sent to the CP. When a high rate of such traffic is sent to CP, the switch can drop some of these packets due to the in built CP rate limiting feature, which protects the CP from DOS attacks.

Use the command **`show qos cosq-stats cpu-port`** to view drop statistics on the CPU queue. This design does not result in loss of traffic.

Use the command **`ipv6 nd reachable-time <0-3600000>`** to increase the default value of 3000 milliseconds which in turn delays the scenario of data path sending STALE neighbor destined packets to the CP.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. View the CPU queue statistics:

```
show qos cosq-stats  cpu-port
```

Variable definitions

The following table describes the column headings in the command output for `show qos cosq-stats  cpu-port` .

Table 28: Variable definitions

Variable	Value
CoS	Indicates the CoS queue number.
Out Packets	Indicates the out packets for the CoS queue.
Out Bytes	Indicates the out bytes for the CoS queue.
Drop Packets	Indicates the drop packets for the CoS queue.
Drop Bytes	Indicates the drop bytes for the CoS queue.

Clearing CPU queue statistics

Clear the CPU queue statistics.

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Clear CPU queue statistics:

```
clear qos cosq-stats cpu-port
```

Configuring an egress QoS queue profile

Configure a queue profile to apply the configured egress queue parameters to queues and ports.

About this task

After you make a configuration change to a queue profile, you must apply the profile before the changes take effect.

Note:

Currently the switch supports only one queue profile that is automatically created on system boot up, with an ID of 1 and name of default. You cannot delete this profile.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the minimum weight for a specific queue:

   ```
   qos queue-profile queue <1-5> <0-7> min-weight <1-100>
   ```

3. Enable rate limiting on a weighted queue:

   ```
   qos queue-profile queue <1-5> <0-7> rate-limit-enable
   ```

4. Apply the queue profile:

   ```
   qos queue-profile <1-5> apply
   ```

5. Verify the egress queue configuration:

   ```
   show qos queue-profile [<1-5> queue <0-7>|all]
   ```

6. **(Optional)** Configure the default settings for an egress queue:

   - Configure the default minimum weight using one of the following commands:

     ```
     default qos queue-profile queue <1-5> <0-7> min-weight
     no qos queue-profile queue <1-5> <0-7> min-weight
     ```

   - Configure the default rate limiting on a weighted queue using one of the following commands:

     ```
     default qos queue-profile queue <1-5> <0-7> rate-limit-enable
     no qos queue-profile queue <1-5> <0-7> rate-limit-enable
     ```

Example

Configure the queue profile for queue 1 to use a weight of 20, and enable rate limiting.

```
Switch:1(config)#qos queue-profile queue 1 1 min-weight 20
Switch:1(config)#qos queue-profile queue 1 1 rate-limit-enable
Switch:1(config)#qos queue-profile 1 apply
```

View the queue profile configuration.

```
Switch:1#show qos queue-profile
================================================================================
                              Qos Queue Profile

================================================================================
```

```
Profile Profile
ID      Name
--------------------------------------------------------------------------------
1       default
```

```
Switch:1(config)#show qos queue-profile 1 queue 1

================================================================================
                            Qos Queue Profile Table

================================================================================

Profile Profile Queue Weight  Weight     Rate-limit Rate-limit
ID      Name    ID    Applied Configured Applied    Configured
--------------------------------------------------------------------------------
1       default 1     20      10         ENABLE     ENABLE
```

Variable definitions

Use the data in the following table to use the **`qos queue-profile queue`** command.

Variable	Value
<1–5>	Specifies the queue profile ID. **Note:** The current release supports only one queue profile with profile ID 1.
<0-7>	Specifies the egress queue to configure.
min-weight <1-100>	Configures the queue weight for weighted round robin, or the rate-limit in percentage of the link rate for queue shaping enabled on the queue. The following list identifies the default minimum weight for each queue: • Queue 0 — 5 • Queue 1 — 20 • Queue 2 — 30 • Queue 3 — 40 • Queue 4 — 50 • Queue 5 — 50 • Queue 6 — 50 • Queue 7 — 5
rate-limit-enable	Enables rate limiting on the queue. By default, rate limiting is enabled for queues 6 and 7 only; it is disabled for queues 0 through 5.

Use the data in the following table to use the **show qos queue-profile** command.

Variable	Value
<1–5>	Specifies the queue profile ID. If you do not include a queue profile ID, the command output displays all configured profiles. **Note:** The current release supports only one queue profile with a default ID of 1.
<0-7>	Specifies the egress queue. Displays configuration settings of the specified egress queue.
all	The command output displays the configuration settings of all 8 egress queues of the queue profile.

Chapter 8: QoS configuration using EDM

Configure Quality of Service (QoS) to allocate network resources where you need them most.

Configuring port-based shaping

Configure egress port-based shaping to bind the maximum rate at which traffic leaves the port.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **Interface** tab.
5. From **EgressRateLimitState**, select **enable**.
6. In the**EgressRateLimit** box, type an egress rate limit in kilobits per second (Kb/s).
7. Click **Apply**.

Configuring port-based policing

Use a port-based policer to bandwidth-limit ingress traffic. The system drops or re-marks violating traffic.

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **Interface** tab.
5. From **IngressRatePeak** , type the value for the peak rate in Kb/s.

   The peak rate must be greater than or equal to the service rate.

6. From **IngressRateSvc** , type the value for the service rate in Kb/s.
7. Click **Apply**.

Modifying ingress 802.1p to QoS mappings

Modify the ingress mappings to change traffic priorities. Avaya recommends that you use the default mappings.

About this task

Avaya recommends that you do not change the default values. If you change the values, make sure that the values are consistent on all other devices in the network. Inconsistent mapping of table values can result in unpredictable service levels.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **Mapping Tables**.
3. Click the **Ingress 8021p to QoS** tab.
4. Double-click a QosLevel field to change the value.
5. Click **Apply**.

Ingress 8021p To QoS field descriptions

Use the data in the following table to use the **Ingress 8021p to QoS** tab.

Name	Description
InIeee8021P	Specifies the value of the IEEE 802.1p bit of the incoming packet.
QosLevel	Specifies the equivalent egress QoS level (0–7).

Modifying ingress DSCP to QoS mappings

Modify the ingress Differentiated Services Code Point (DSCP) to QoS mappings to change traffic priorities. Avaya recommends that you use the default mappings. Changes to the mapping table take effect after you restart the system.

About this task

Avaya recommends that you do not change the default values. If you change the values, make sure that the values are consistent on all other devices in the network. Inconsistent mapping of table values can result in unpredictable service levels.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **Mapping Tables**.
3. Click the **Ingress Dscp To QoS** tab.
4. Double-click a QosLevel field to change the value.
5. Click **Apply**.

Ingress Dscp To QoS field descriptions

Use the data in the following table to use the **Ingress Dscp To QoS** tab.

Name	Description
InDscp	Specifies the value of the DiffServ codepoint (in decimal format) in the IP header of the incoming packet.
InDscpBinaryFormat	Specifies the value of the DiffServ codepoint (in binary format) in the IP header of the incoming packet.
QosLevel	Specifies the equivalent QoS level.

Modifying egress QoS to 802.1p mappings

Modify the egress mappings to change the mappings between the QoS levels and the IEEE 802.1p bits.

About this task

Avaya recommends that you do not change the default values. If you change the values, make sure that the values are consistent on all other devices in the network. Inconsistent mapping of table values can result in unpredictable service levels.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **Mapping Tables**.
3. Click the **Egress QoS to 8021p** tab.

4. Double-click the Outleee8021P field to change the value.
5. Click **Apply**.

Egress QoS to 8021p field descriptions

Use the data in the following table to use the **Egress QoS to 8021p** tab.

Name	Description
QosLevel	Specifies the QoS level of the outgoing packet.
Outleee8021P	Specifies the equivalent value of the IEEE 802.1p bit.

Modifying egress QoS to DSCP mappings

Modify the egress QoS to DSCP mappings to change traffic priorities. Avaya recommends that you use the default mappings.

About this task

Avaya recommends that you do not change the default values. If you change the values, make sure that the values are consistent on all other devices in the network. Inconsistent mapping of table values can result in unpredictable service levels.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **Mapping Tables**.
3. Click the **Egress QoS To Dscp** tab.
4. Double-click the OutDscp file to change the value.
5. Click **Apply**.

Egress QoS To Dscp field descriptions

Use the data in the following table to use the **Egress QoS To Dscp** tab.

Name	Description
QosLevel	Specifies the QoS level of the outgoing packet.
OutDscp	Specifies the equivalent value of the DiffServ code point (in decimal format).
OutDscpBinaryFormat	Specifies the equivalent value of the DiffServ code point (in binary format).

Viewing port egress CoS queue statistics

Use the following procedure to retrieve the port egress CoS queue statistics. The system displays the statistics of the forwarded packets and bytes, and the dropped packets and bytes.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **CoS Queue Stats**.
3. Select the **Interface** tab.

Interface field descriptions

The following table describes the fields from the CoS Queue Stats Interface tab.

Table 29: Variable definitions

Name	Description
Index	Indicates the loopback port number from 192(1/1) to 241(1/50).
Que<1–8>OutPackets	Indicates the out packets by CoS queue number 1–8.
Que<1–8>OutBytes	Indicates the out bytes by CoS queue number 1–8.
Que<1–8>DropPackets	Indicates the drop packets by CoS queue number 1–8.
Que<1–8>DropBytes	Indicates the drop bytes by CoS queue number 1–8.
ClearStat	Clears the port egress statistics.

Clearing CPU statistics for the VSP 4000 chassis

Use the following procedure to clear the CPU statistics for the VSP 4000 chassis.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **CoS Queue Stats**.
3. Select the **CPU-Stats-Clear** tab.
4. Select the **CpuStatsClear** check box.
5. Click **Apply**.

Viewing CPU queue statistics

Use the following procedure to retrieve the statistics of the forwarded packets and bytes, and the dropped packets and bytes for the traffic sent toward CP. The queue assignment is based on the protocol types, not on the internal CoS value These statistics are useful for debugging purposes.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.
2. Click **CoS Queue Stats**.
3. Select the **CPU-Port** tab.

CPU-Port field descriptions

The following table describes the fields from the CoS Queue Statistics CPU-Port tab.

Table 30: Variable definitions

Name	Description
Index	Indicates the CoS queue number from 0-15.
OutPackets	Indicates the out packets for the CPU port.
OutBytes	Indicates the out bytes for the CPU port.
DropPackets	Indicates the drop packets for the CPU port.
DropBytes	Indicates the drop bytes for the CPU port.

Configuring an egress QoS queue profile

Configure a queue profile to apply the configured egress queue parameters to queues and ports. You must apply the profile before the changes take effect.

Currently the switch supports only one queue profile that is automatically created on system boot up, with an ID of 1 and name of default. You cannot delete this profile.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **QoS**.
2. Click **Queue Profile**.
3. Click the **Queue Profile** tab.

   The default queue profile displays.
4. In the **Apply** field, double click and select **true** to apply the profile.
5. Click **Apply**.

Queue Profile field descriptions

Use the data in the following table to use the **Queue Profile** tab.

Field	Description
Id	Displays the default queue profile ID. The default ID is 1.
Name	Displays the name of the queue profile as default.
Apply	Specifies the status of the queue profile, as true or false.

Editing queue profile information

About this task

Use the following procedure to edit queues of a queue profile, to configure a queue weight or enable rate limiting on the queue.

Note:

After you make the configuration changes, you must apply the queue profile before the changes take effect.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **QoS**.
2. Click **Queue Profile**.
3. Update a queue to configure queue weight or rate limiting.
   a. Click the **Queue** tab.
   b. Edit the **AdminWeight** and **AdminRateLimitStatus** fields by double-clicking on them, and then selecting or typing the new value.
   c. Click **Apply**.
4. Apply the queue profile for the queue configuration to take effect.
   a. Click the **Queue Profile** tab.
   b. In the **Apply** field, double-click and select **true**.
   c. Click **Apply**.
5. Click the **Queue** tab again, to verify updates to the **OperWeight** and the **OperRateLimitStatus** fields, for the respective queue.

Queue field descriptions

Use the data in the following table to use the **Queue** tab.

Field	Description
PId	Displays the queue profile ID.
Id	Displays the queue ID.
AdminWeight	Specifies the administrative weight of the queue.
OperWeight	Displays the operational weight of the profile, described as a percentage.
AdminRateLimitStatus	Specifies the administrative status of the queue rate limit as true or false.
OperRateLimitStatus	Displays the operational status of the queue rate limit.

Chapter 9: Access control list configuration using ACLI

Use an access control list (ACL) to specify an ordered list of access control entries (ACE), or filter rules. The ACEs provide specific actions that you want the filter to perform.

The following task flow shows you the sequence of procedures you perform to create and configure an ACL.

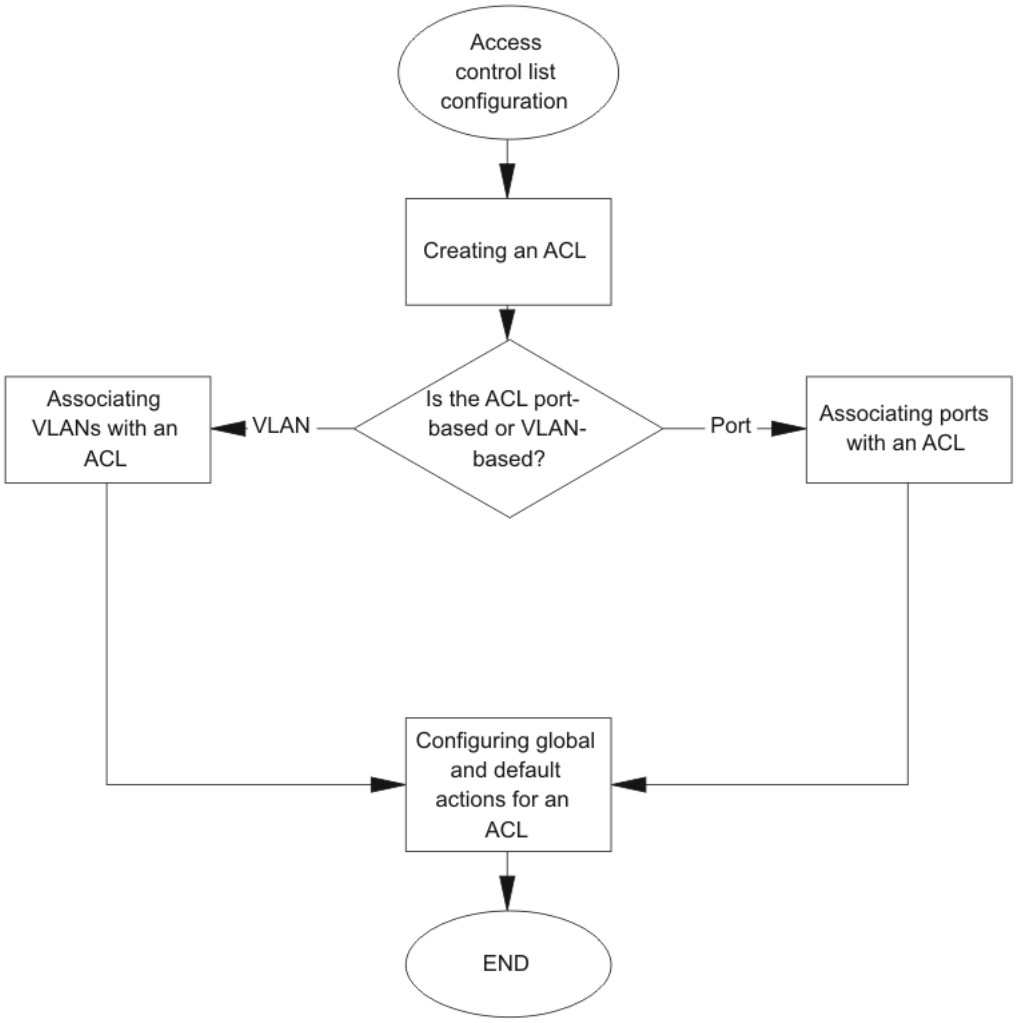


Figure 8: Access control list configuration using ACLI procedures

Note:

The default prompt for the non-PowerPlus chassis is VSP-4850GTS. The default prompt for the PowerPlus chassis is VSP-4850GTS-PWR+. The default prompt for the PowerPlus chassis with additional fiber ports is VSP-4450GSX-PWR+. For consistency, this document uses the VSP-4850GTS prompt.

Creating an ACL

Create an ACL to specify an ordered list of ACEs, or filter rules.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create an ACL:

   ```
   filter acl <1-2048> type <inVlan|inPort|outPort> [name WORD<0-32>]
   [enable]
   ```

3. Ensure the configuration is correct:

   ```
   show filter acl [<1-2048>]
   ```

Variable definitions

Use the data in the following table to use the `filter acl` command.

Table 31: Variable definitions

Variable	Value
<1-2048>	Specifies a unique identifier (1–2048) for the ACL.
enable	Enables the ACL state, and all associated ACEs. Enabled is the default state.
name *WORD<0-32>*	Specifies an optional descriptive name for the ACL.
type <inVlan|inPort|outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outPort are egress ACLs. A port-based ACL has precedence over a VLAN-based ACL.

Creating an IPv6 ACL

Create an IPv6 ACL to specify an ordered list of ACEs, or filter rules.

You must specify the packet type as IPv6 at the ACL level to enable IPv6 filtering. By default, an ACL filters non IPv6 packets.

Note:

You cannot change packet type for the ACL once you have configured it. If you want a different packet type, you must delete the ACL and re-create it using the other packet type.

Procedure

1. Enter Global Configuration mode:

```
enable

configure terminal
```

2. Create an IPv6 ACL:

```
filter acl <1-2048> type <inVlan|inPort> [name WORD<0-32>] [pktType
ipv6] [enable]
```

Note:

IPv6 ingress QoS ACL/Filters and IPv6 egress security and QoS ACL/Filters are not supported.

3. Ensure the configuration is correct:

```
show filter acl [<1-2048>]
```

Variable definitions

Use the data in the following table to use the `filter acl` command.

Table 32: Variable definitions

Variable	Value
<1-2048>	Specifies a unique identifier (1–2048) for the ACL.
enable	Enables the ACL state, and all associated ACEs. Enabled is the default state.
name *WORD<0-32>*	Specifies an optional descriptive name for the ACL.
type <inVlan|inPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs. IPv6 ingress QoS ACL/Filters and IPv6 egress security and QoS ACL/Filters are not supported. A port-based ACL has precedence over a VLAN-based ACL.
pktType <ipv6>	Specifies the IP version as IPv6. The default is nonipv6. **Note:** You cannot change packet type for the ACL once you have configured it. If you want a different packet type, you must delete the ACL and re-create it using the other packet type.

Associating VLANs with an ACL

Associate VLANs with an ACL to apply filters to VLAN traffic.

Before you begin

- The ACL exists.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Add VLAN interfaces to an ACL:

   ```
   filter acl vlan <1-2048> <2-4084>
   ```

3. Remove specified VLAN interfaces from an ACL:

   ```
   no filter acl vlan <1-2048> <2-4084>
   ```

Variable definitions

Use the data in the following table to use the `filter acl vlan` command.

Table 33: Variable definitions

Variable	Value
<1-2048>	Specifies an ACL ID from 1–2048.
<2-4084>	Specifies the VLAN IDs from 2–4084. **Note:** VLANs 4061-4084 are reserved for internal use in Release 3.0.0.0. If you attempt to configure a VLAN in this range, the following message appears: `Error: Invalid Vlan Id. Vlan 4061 to 4084 is being used internally.`

Associating ports with an ACL

Associate ports with an ACL to apply filters to port traffic.

Before you begin

- The ACL exists.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Associate port interfaces with a particular ACL:

   ```
   filter acl port <1-2048> {slot/port[-slot/port][,...]}
   ```

3. Remove port interfaces from a particular ACL:

   ```
   no filter acl port <1-2048> {slot/port[-slot/port][,...]}
   ```

Variable definitions

Use the data in the following table to use the `filter acl port` command.

Table 34: Variable definitions

Variable	Value
<1-2048>	Specifies an ACL ID from 1–2048.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (1/1) or a range of slots and ports (1/2-1/4).

Configuring global and default actions for an ACL

Configure the default action to specify packet treatment if a packet does not match any ACE.

Configure the global action to specify packet treatment if a packet does match an ACE.

Before you begin

- The ACL exists.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the global action for an ACL:

   ```
   filter acl set <1-2048> global-action [monitor-dst-ports {slot/
   port[-slot/port][,...]}] [monitor-dst-mlt <1-512>]
   ```

3. Configure an ACL to the default global action settings:

   ```
   default filter acl set <1-2048> global-action [monitor-dst-ports]
   ```

4. Configure the default action for an ACL:

   ```
   filter acl set <1-2048> default-action <permit|deny>
   ```

5. Configure an ACL to the default action settings:

```
default filter acl set <1-2048> default-action
```

Variable definitions

Use the data in the following table to use the `filter acl set` commands.

Table 35: Variable definitions

Variable	Value
<1-2048>	Specifies the ACL ID.
default-action <deny|permit>	Specifies the default action to take when none of the ACEs match. Options are <deny|permit>. The default is permit.
monitor-dst-ports {slot/port[-slot/port][,...]}	Specifies the global action to take for matching ACEs: • monitor destination ports—Configures mirroring to a destination port or ports.
monitor-dst-mlt <1–512>	Configures mirroring to a destination MLT in the range of 1 to 512.

Renaming an ACL

Perform this procedure to change the name of an existing ACL.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Rename an ACL:

   ```
   filter acl <1-2048> name WORD<0-32>
   ```

3. Reset the ACL name to the default name:

   ```
   default filter acl <1-2048> name
   ```

Variable definitions

Use the data in the following table to use the `filter acl` command.

Table 36: Variable definitions

Variable	Value
<1-2048>	Specifies a unique identifier (1–2048) for the ACL.
enable	Enables the ACL state, and all associated ACEs. Enabled is the default state.
name *WORD<0-32>*	Specifies an optional descriptive name for the ACL.
type <inVlan|inPort|outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outPort are egress ACLs. A port-based ACL has precedence over a VLAN-based ACL.

Disabling an ACL

Perform this procedure to disable an ACL and all ACEs that belong to it.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Disable an ACL:

   ```
   no filter acl <1-2048> enable
   ```

Variable definitions

Use the data in the following table to use the `filter acl` command.

Table 37: Variable definitions

Variable	Value
<1-2048>	Specifies a unique identifier (1–2048) for the ACL.
enable	Enables the ACL state, and all associated ACEs. Enabled is the default state.
name *WORD<0-32>*	Specifies an optional descriptive name for the ACL.
type <inVlan|inPort|outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outPort are egress ACLs. A port-based ACL has precedence over a VLAN-based ACL.

Resetting an ACL to default values

Reset an ACL to change the ACL name to the default name and the filter ACL mode to a default of enable.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Reset an ACL to default values:

   ```
   default filter acl <1-2048>
   ```

Variable definitions

Use the data in the following table to use the `filter acl` command.

Table 38: Variable definitions

Variable	Value
<1-2048>	Specifies a unique identifier (1–2048) for the ACL.
enable	Enables the ACL state, and all associated ACEs. Enabled is the default state.
name *WORD<0-32>*	Specifies an optional descriptive name for the ACL.
type <inVlan|inPort|outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outPort are egress ACLs. A port-based ACL has precedence over a VLAN-based ACL.

Deleting an ACL

Delete an ACL to remove an ordered list of filter rules.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Delete an ACL:

   ```
   no filter acl <1-2048>
   ```

The following message appears:

```
WARNING: All ACE entries under this ACL will be Deleted.
Do you wish to delete this ACL? (y/n)?
```

3. Enter `y`.

Variable definitions

Use the data in the following table to use the `filter acl` command.

Table 39: Variable definitions

Variable	Value
<1-2048>	Specifies a unique identifier (1–2048) for the ACL.
enable	Enables the ACL state, and all associated ACEs. Enabled is the default state.
name *WORD<0-32>*	Specifies an optional descriptive name for the ACL.
type <inVlan|inPort|outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outPort are egress ACLs. A port-based ACL has precedence over a VLAN-based ACL.

Chapter 10: Access control list configuration using EDM

Use traffic filtering to provide security by blocking unwanted traffic and prioritizing other traffic.

Configuring an access control list

Use an access control list (ACL) to specify an ordered list of access control entries (ACE), or filter rules. The ACEs provide specific actions for the filter to perform.

About this task

To modify an ACL parameter, double-click the parameter you wish to change. Change the value, and then click Apply. You cannot change a parameter that appears dimmed; in this case, delete the ACL, and then configure a new one.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Click **Insert**.
5. In the **AclId**box, type an ACL ID from 1 to 2048 or accept the default value .
6. In **Type**, specify whether the ACL is VLAN or port-based, and whether it is ingress (in) or egress (out).
7. Specify a name for the ACL in the **Name** box.
8. If the ACL is VLAN-based, click the **VlanList** ellipsis (**...**) and choose a VLAN list.
9. If the ACL is port-based, select the **PortList** by clicking the ellipsis (**...**).
10. Select the desired ports and then click **Ok**.
11. Configure the **DefaultAction**.
12. Enable or disable the **State**, as required.
13. Configure the remaining fields as appropriate.

14. Click **Insert**.
15. To delete an ACL, select the ACL, and then click **Delete**.

ACL field descriptions

Use the data in the following table to use the **ACL** tab.

Name	Description
AclId	Specifies a unique identifier for the ACL from 1–2048.
Type	Specifies whether the ACL is VLAN- or port-based. Valid options are • inVlan • inPort • outPort **Important:** The inVlan ACLs drop packets if you add a VLAN after ACE creation.
Name	Specifies a descriptive user-defined name for the ACL.
VlanList	For inVlan ACL types, specifies all VLANs to associate with the ACL.
PortList	For inPort and outPort ACL types, specifies the ports to associate with the ACL.
DefaultAction	Specifies the action taken when no ACEs in the ACL match. Valid options are deny and permit, with permit as the default. Deny means the system drops the packets; permit means the system forwards packets.
State	Enables or disables all of the ACEs in the ACL. The default value is enable.
PktType	Indicates the packet type that this ACLI is applicable to.
MirrorVlanId	Configures mirroring to a destination VLAN.
MirrorDstPortList	Configures mirroring to a destination port or ports.

Chapter 11: Access control entry configuration using ACLI

Use an access control entry (ACE) to provide an ordered list of traffic filtering rules.

Note:

The default prompt for the non-PowerPlus chassis is VSP-4850GTS. The default prompt for the PowerPlus chassis is VSP-4850GTS-PWR+. The default prompt for the PowerPlus chassis with additional fiber ports is VSP-4450GSX-PWR+. For consistency, this document uses the VSP-4850GTS prompt.

Configuring ACEs

Use an ACE to define packet attributes and the desired behavior for packets that carry the attribute or list of attributes.

Before you begin

- The ACL exists.

About this task

You can configure a maximum of 766 ACE in ingress, and 252 in egress ACEs for each access control list (ACL). The system supports a maximum of 1018 ACEs. The system reserves ACE IDs in the range of 1 to 1000 for security, and the range of 1001 to 2000 for QoS.

ACLs are by default created in enabled state while ACEs are by default created in disabled state. Use ACLI commands to enable an ACE.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Create and name an ACE:

   ```
   filter acl ace <1-2048> <1-2000> [name WORD<0-32>]
   ```

The ACE ID determines ACE precedence (that is, the lower the ID, the higher the precedence).

3. Configure the mode as deny or permit:

   ```
   filter acl ace action <1-2048> <1-2000> <deny|permit>
   ```

4. Configure ACE actions as required.
5. Ensure the configuration is correct:

   ```
   show filter acl ace [<1-2048>] [<1-2000>]
   ```

6. Ensure the filter is enabled:

   ```
   filter acl ace <1-2048> <1-2000> enable
   ```

7. Optionally, reset an ACE to default values (reset the ACE name to the default name and the administrative state to the default value of disable):

   ```
   default filter acl ace <1-2048> <1-2000>
   ```

8. Optionally, delete an ACE ID:

   ```
   no filter acl ace <1-2048> <1-2000>
   ```

Variable definitions

Use the data in the following table to use the `filter acl ace` and the `filter acl ace action` commands.

Table 40: Variable definitions

Variable	Value
<1-2048>	Specifies the ACL ID.
<1-2000>	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
<deny|permit>	Configures the action mode for security ACEs (1–1000). **Note:** For each Security ACE (1-1000), you must define one or more actions as well as the associated action mode (permit or deny). Otherwise, the security ACE cannot be enabled. There is no default configuration for Security ACEs. With QoS ACEs (1001-2000), the action mode is not configurable. QoS ACEs are always set to action mode permit.
enable	Enables an ACE within an ACL. After you enable an ACE, to make changes, first disable it.
name*WORD<0-32>*	Specifies an optional descriptive name for the ACE that uses 0–32 characters.

Configuring ACE actions

Configure ACE actions to determine the process that occurs after a packet matches an ACE.

Before you begin

- The ACE exists.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure ACE actions:

   ```
   filter acl ace action <1-2048> <1-2000> <deny|permit> [count]
   [internal-qos <0-7>] [monitor-dst-ports {slot/port[-slot/port]
   [,...]}][monitor—dst—mlt <1-512>][redirect-next-hop WORD<1-15>]
   [remark-dot1p <0-7>] [remark-dscp  <phbcs0 |phbcs1 |phbaf11|phbaf12|
   phbaf13|phbcs2|phbaf21|phbaf22|phbaf23|phbcs3|phbaf31|phbaf32|
   phbaf33|phbcs4|phbaf41|phbaf42|phbaf43|phbcs5|phbcs6|phbef|phbcs7>]
   ```

3. Ensure the configuration is correct:

   ```
   show filter acl action [<1-2048>] [<1-2000>]
   ```

Variable definitions

Use the data in the following table to use the `filter acl ace action` command.

Table 41: Variable definitions

Variable	Value
<1-2048>	Specifies the ACL ID.
<1-2000>	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
count	Enables the ability to count matching packets. Use this parameter with either a security or QoS ACE. The default is disabled.
<deny|permit>	Configures the action mode for security ACEs. **Note:** For each Security ACE (1-1000), you must define one or more actions as well as the associated action mode (permit or deny). Otherwise, the security ACE cannot be enabled. There is no default configuration for Security ACEs. With QoS ACEs

Table continues…

Variable	Value
	(1001-2000), the action mode is not configurable. QoS ACEs are always set to action mode permit.
internal-qos	This variable is a QoS action. The ACE ID must be in the range of 1001–2000. The default value is 1.
monitor-dst-ports {slot/port[-slot/port][,...]}	Configures mirroring to a destination port or ports. This action is a security action. The ACE ID must be in the range of 1–1000. {slot/port[-slot/port][,...]} identifies the slot and port in one of the following formats: a single slot and port (1/1) or a a range of slots and ports (1/2-1/4).
monitor-dst-mlt <1–512>	Configures mirroring to a destination MLT in the range of 1 to 512.
redirect-next-hop <ip_address>	Specifies the next-hop IP address for redirect mode (a.b.c.d). This action is a security action. The ACE ID must be in the range of 1–1000.
remark-dscp <phbcs0|phbcs1|phbaf11|phbaf12|phbaf13|phbcs2|phbaf21|phbaf22|phbaf23|phbcs3|phbaf31|phbaf32|phbaf33|phbcs4|phbaf41|phbaf42|phbaf43|phbcs5|phbcs6|phbef|phbcs7>	Specifies the new Per-Hop Behavior (PHB) for matching packets: phbcs0, phbcs1, phbaf11, phbaf12, phbaf13, phbcs2, phbaf21, phbaf22, phbaf23, phbcs3, phbaf31, phbaf32, phbaf33, phbcs4, phbaf41, phbaf42, phbaf43, phbcs5, phbef, phbcs6, phbcs7. This action is a QoS action. The ACE ID must be in the range of 1001–2000.
remark-dot1p <0–7>	Specifies the new 802.1 priority bit for matching packets: zero, one, two, three, four, five, six, or seven. This action is a QoS action. The ACE ID must be in the range of 1001–2000.

Configuring ARP ACEs

Use ACE Address Resolution Protocol (ARP) entries to ensure the filter looks for ARP requests or responses.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure an ACE for ARP packets:

```
filter acl ace arp <1-2048> <1-2000> operation eq <arprequest|
arpresponse>
```

3. Ensure the configuration is correct:

   ```
   show filter acl arp [<1-2048>] [<1-2000>]
   ```

4. Optionally, delete the individual attributes from the ARP portion of the ACE:

   ```
   no filter acl ace arp <1-2048> <1-2000> [operation]
   ```

5. Optionally, delete all the attributes from the ARP portion of the ACE:

   ```
   default filter acl ace arp <1-2048> <1-2000>
   ```

Variable definitions

Use the data in the following table to use the `filter acl ace arp` command.

Table 42: Variable definitions

Variable	Value
<1-2048>	Specifies the ACL ID.
<1-2000>	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
operation eq <arprequest| arpresponse>	Specifies the type of ARP operation to filter: arpRequest or arpResponse.

Configuring an Ethernet ACE

Configure an Ethernet ACE to filter on Ethernet parameters.

Before you begin

- The ACE exists.
- The ACL exists.

About this task

The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure an ACE for the destination or source MAC address attribute:

   ```
   filter acl ace ethernet <1-2048> <1-2000> <dst-mac|src-mac> eq
   WORD<1-1024>
   ```

   OR

   ```
   filter acl ace ethernet <1-2048> <1-2000> <dst-mac|src-mac> mask
   WORD<1-1024> WORD<1-1024>
   ```

3. Configure an ACE for an Ethernet type attribute:

   ```
   filter acl ace ethernet <1-2048> <1-2000> ether-type eq WORD<1-200>
   ```

4. Configure an ACE for a port attribute:

   ```
   filter acl ace ethernet <1-2048> <1-2000> port eq {slot/port}
   ```

5. Configure an ACE for a VLAN attribute:

   ```
   filter acl ace ethernet <1-2048> <1-2000> vlan-id eq <2-4084>
   ```

   OR

   ```
   filter acl ace ethernet <1-2048> <1-2000> vlan-id mask <2-4084>
   <0-0xFFF>
   ```

6. Configure an ACE for a VLAN tagged priority attribute:

   ```
   filter acl ace ethernet <1-2048> <1-2000> vlan-tag-prio eq <0-7>
   ```

   OR

   ```
   filter acl ace ethernet <1-2048> <1-2000> vlan-tag-prio mask <0-7>
   <0-0x7>
   ```

7. Ensure the configuration is correct:

   ```
   show filter acl ethernet [<1-2048>] [<1-2000>]
   ```

8. Optionally, delete the individual attributes from the Ethernet portion of the ACE:

   ```
   no filter acl ace ethernet <1-2048> <1-2000>
   ```

9. Optionally, delete all the attributes from the Ethernet portion of the ACE:

   ```
   default filter acl ace ethernet <1-2048> <1-2000>
   ```

Variable definitions

Use the data in the following table to use the `filter acl ace ethernet` command.

Table 43: Variable definitions

Variable	Value
<0-7>	Specifies the priority bits (3-bit field) from the 802.1Q/p tag.
<0–0x7>	Specifies the mask value for VLAN tagged priority attribute.

<0-0xFFF>	Specifies the mask value for a VLAN attribute.
	For example:
	`filter acl ace ethernet 10 10 vlan-id eq 10`
	`filter acl ace ethernet 10 10 vlan-id mask 1025 0xF`

<1-2000>	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
<1-2048>	Specifies the ACL ID.
<2–4084>	Specifies the VLAN or VLANs to match.
{slot/port}	Identifies the slot and port.
WORD<1–200>	Specifies an ether-type name or number: • 0x0–0xffff • ip, arp, ipx802dot3, ipx802dot2, ipxSnap, ipxEthernet2, appleTalk, decLat, decOther, sna802dot2, snaEthernet2, netBios, xns, vines, rarp, or PPPoE

WORD<1–1024>	If the operator is mask, the *WORD<1–1024>* parameter is {“”|1..48 ,| mac address mask 0x0..FFFFFFFFFFFF}}
	If the operator is eq, the *WORD<1–1024>* parameter is the destination or source MAC address: AA:BB:CC:DD:EE:FF
	For example:
	`filter acl ace ethernet 10 10 dst-mac eq 01:00:5e:00:00:01`
	`filter acl ace ethernet 10 10 dst-mac mask 01:00:5e:00:00:01 24`
	`filter acl ace ethernet 10 10 src-mac mask 01:00:5e:00:00:01 FFFFFFFF0000`

Configuring an IP ACE

Configure an IP ACE to filter on the source IP address, destination IP address, DiffServ Code Point (DSCP), protocol, IP options, and IP fragmentation parameters.

Before you begin

- The ACE exists.
- The ACL exists.

About this task

The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Configure an ACE for the DSCP attribute:

   ```
   filter acl ace ip <1-2048> <1-2000> dscp eq <phbcs0|phbcs1|phbaf11|
   phbaf12|phbaf13|phbcs2|phbaf21|phbaf22|phbaf23|phbcs3|phbaf31|
   phbaf32|phbaf33|phbcs4|phbaf41|phbaf42|phbaf43|phbcs5|phbcs6|phbef|
   phbcs7>
   ```

   OR

   ```
   filter acl ace ip <1-2048> <1-2000> dscp mask <phbcs0|phbcs1|
   phbaf11|phbaf12|phbaf13|phbcs2|phbaf21|phbaf22|phbaf23|phbcs3|
   phbaf31|phbaf32|phbaf33|phbcs4|phbaf41|phbaf42|phbaf43|phbcs5|
   phbcs6|phbef|phbcs7> WORD<0x0-0x40>
   ```

3. Configure an ACE for the destination or source IP address attribute:

   ```
   filter acl ace ip <1-2048> <1-2000> <dst-ip|src-ip> eq WORD<1-1024>
   ```

   OR

   ```
   filter acl ace ip <1-2048> <1-2000> <dst-ip|src-ip> mask WORD<1-
   1024> {<0-32>|null|<A.B.C.D>}
   ```

4. Configure an ACE for the IP fragmentation attribute:

   ```
   filter acl ace ip <1-2048> <1-2000> ip-frag-flag eq <noFragment|
   anyFragment>
   ```

5. Configure an ACE for the IP options attribute:

   ```
   filter acl ace ip <1-2048> <1-2000> ip-options any
   ```

6. Configure an ACE for the protocol type attribute:

   ```
   filter acl ace ip <1-2048> <1-2000> ip-protocol-type eq WORD<1-256>
   ```

7. Ensure the configuration is correct:

   ```
   show filter acl ip [<1-2048>] [<1-2000>]
   ```

8. Optionally, delete the individual attributes from the IP portion of the ACE:

   ```
   no filter acl ace ip <1-2048> <1-2000> [dscp] [dstIp] [ipFragFlag]
   [ipOptions] [ipProtoType] [srcIp]
   ```

9. Optionally, delete all the attributes from the IP (Layer 3) portion of the ACE:

```
default filter acl ace ip <1-2048> <1-2000>
```

Example

```
VSP-4850GTS# filter acl ace ip 1 12 dst-ip eq 121.202.2.3
```

Variable definitions

Use the data in the following table to use the `filter acl ace ip` command.

Table 44: Variable definitions

Variable	Value
<1-2000>	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
<1-2048>	Specifies the ACL ID.

{<0–32>|null|<A.B.C.D>}	Specifies the mask value for the destination or source IP address
	For example:
	`filter acl ace ip 10 10 dst-ip mask 1.1.1.1 25`
	`filter acl ace ip 10 10 dst-ip mask 1.1.1.1 255.192.128.0`
	`filter acl ace ip 10 10 src-ip mask 2.2.2.2 22`
	`filter acl ace ip 10 10 src-ip mask 3.3.3.3 255.0.0.0`

<noFragment|anyFragment>	Specifies a match option for IP fragments noFragment or anyFragment.
<phbcs0|phbcs1|phbaf11|phbaf12|phbaf13|phbcs2|phbaf21|phbaf22|phbaf23|phbcs3|phbaf31|phbaf32|phbaf33|phbcs4|phbaf41|phbaf42|phbaf43|phbcs5|phbcs6|phbef|phbcs7>	Specifies the DSCP value (0 to 256) or PHB name: • phbcs0 • phbcs1 • phbaf11 • phbaf12 • phbaf13 • phbcs2 • phbaf21 • phbaf22 • phbaf23 • phbcs3 • phbaf31 • phbaf32

Table continues…

Variable	Value
	• phbaf33 • phbcs4 • phbaf41 • phbaf42 • phbaf43 • |phbcs5 • phbcs6 • phbef • phbcs7
WORD<0x0-0x40>	Specifies the mask value, for example, `filter acl ace ip 10 10 dscp mask 129 0x40`
WORD<1-256>	Specifies one or more IP protocol types: (1–256), or tcp, udp, ipsecesp, vrrp, snmp or undefined.
WORD<1–1024>	Specifies the destination or source IP address (a.b.c.d).

Configuring an IPv6 ACE

Configure an IPv6 ACE to filter traffic based on Source IPv6 address, Destination IPv6 address, IPv6 next header and IPv6 traffic class.

Source IPv6 and destination IPv6 support equal (eq) and mask operators. Next header and traffic class attributes support the equal (eq) operator. The equal to rule operator looks for an exact match with the field defined. If the field matches exactly with the rule, the system will return a match (hit). ACL-based filters provide the mask operator to match on Layer 2, Layer 3, and Layer 4 packet fields. The mask operator is used to mask bits in packet fields during a search or to match on a partial value of a packet field.

Before you begin

- The ACL exists. The ACL exists with the IPv6 packet type. You can only configure ACE IPv6 attributes to filter on an IPv6 packet.
- The ACE exists.

About this task

The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Create and name an ACE:

   ```
   filter acl ace <1-2048> <1-2000> [name Word<1-32>]
   ```

3. Configure an ACE for the destination IPv6 address attribute:

   ```
   filter acl ace ipv6 <1-2048> <1-2000> dst-ipv6 eq WORD<0-255>
   ```

   OR

   ```
   filter acl ace ipv6 <1-2048> <1-2000> dst-ipv6 mask WORD<1-128>
   WORD<0-255>
   ```

4. Configure an ACE for the source IP address attribute:

   ```
   filter acl ace ipv6 <1-2048> <1-2000> src—ipv6 eq WORD<0-255>
   ```

   OR

   ```
   filter acl ace ipv6 src-ipv6 <1-2048> <1-2000> mask WORD<1-128>
   WORD<0-255>
   ```

5. Specify the next header of the IP header:

   ```
   filter acl ace ipv6 <1-2048> <1-2000> nxt-hdr eq {fragment|hop-by-
   hop|icmpv6|ipsecah|ipsecesp|noHdr|routing|tcp|udp|undefined}
   ```

   You must configure next header to configure the protocol attributes.

6. Specify the traffic class attribute of the IPv6 header:

   ```
   filter acl ace ipv6 <1-2048> <1-2000> traffic-class eq WORD<0-255>
   ```

7. Ensure that your configuration is correct:

   ```
   show filter acl ipv6[<1-2048>] [<1-2000>]
   ```

8. Optionally, delete the individual attributes from the IPv6 portion of the ACE:

   ```
   no filter acl ace ipv6 <1-2048> <1-2000> [dst-ipv6 ] [nxt-hdr] [src-
   ipv6] [traffic-class]
   ```

Example

```
Switch:1# filter acl ace ipv6 15 15 dst-ipv6 eq 30:0:0:0:0:0:0:ffff/64
```

Configuring a protocol ACE

Configure a protocol ACE to filter on the source port, destination port, ICMP message type, or TCP flags.

Before you begin

- The ACE exists.

- The ACL exists.

About this task

The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure an ACE for destination port attributes:

   ```
   filter acl ace protocol <1-2048> <1-2000> dst-port eq WORD<1-60>
   ```

   OR

   ```
   filter acl ace protocol <1-2048> <1-2000> dst-port mask WORD<1-60>
   WORD<1-256>
   ```

3. Configure an ACE for source port attributes:

   ```
   filter acl ace protocol <1-2048> <1-2000> src-port eq WORD<1-65535>
   ```

   OR

   ```
   filter acl ace protocol <1-2048> <1-2000> src-port mask WORD<1-
   65535> WORD<1-256>
   ```

4. Configure an ACE for ICMP message type attributes:

   ```
   filter acl ace protocol <1-2048> <1-2000> icmp-msg-type eq WORD<1-
   200>
   ```

   The icmp-msg-type command options support lists.

5. Configure an ACE for TCP flags attributes:

   ```
   filter acl ace protocol <1-2048> <1-2000> tcp-flags eq WORD<1-50>
   ```

   OR

   ```
   filter acl ace protocol <1-2048> <1-2000> tcp-flags mask {0-0x3F|
   0-0x3F}
   ```

   The tcp-flags command options support lists.

6. Ensure the configuration is correct:

   ```
   show filter acl protocol [<1-2048>] [<1-2000>]
   ```

7. Optionally, delete the individual attributes from the protocol portion of the ACE:

   ```
   no filter acl ace protocol <1-2048> <1-2000> [dstPort] [icmpMsgType]
   [srcPort] [tcp-flags]
   ```

8. Optionally, delete all the attributes from the protocol portion of the ACE:

```
default filter acl ace protocol <1-2048> <1-2000>
```

Example

Specify ICMP packets:

```
VSP-4850GTS# filter acl ace protocol 1 12 icmp-msg-type eq echo-request
```

Variable definitions

Use the data in the following table to use the `filter acl ace protocol` command.

Table 45: Variable definitions

Variable	Value
{0-0x3F}	Specifies the mask value.
<1-2000>	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
<1-2048>	Specifies the ACL ID.
WORD<1–50>	Specifies one or more TCP flags—none, fin (finish connection), syn (synchronize), rst (reset connection), push, ack (acknowledge), urg (urgent), and undefined.
WORD<1–60>	Specifies the destination port: (0–65535), or echo, ftpdata, ftpcontrol, ssh, telnet, dns, http, hdot323, bootpServer, bootpClient, tftp, rtp, rtcp, or undefined.
WORD<1–200>	Specifies the ICMP message type (0–255), or echoreply, destunreach, sourcequench, redirect, echo-request, routeradv, routerselect, time-exceeded, param-problem, timestamp-request, timestamp-reply, addressmask-request, addressmask-reply, or traceroute.
WORD<1–256>	Specifies the mask parameter, {0-0xFFFF}.
WORD<0–65535>	Specifies the source port (0–65535).

Viewing ACL and ACE configuration data

View your configuration to review the information and ensure it is correct.

Procedure

1. Enter the Privileged EXEC mode:

   ```
   enable
   ```

2. View ACL information:

   ```
   show filter acl [<1-2048>]
   ```

3. View the running configuration for an ACL and corresponding ACE:

   `show filter acl config [<1-2048>] [<1-2000>]`

Variable definitions

Use the data in the following table to use the `show filter acl` and `show filter acl config` commands.

Table 46: Variable definitions

Variable	Value
<1-2000>	Specifies an ACE ID from 1–2000. ACE IDs in the range 1–1000 are security ACEs; ACE IDs in the range 1001–2000 are QoS ACEs.
<1-2048>	Specifies an ACL ID from 1–2048.

Chapter 12: Access control entry configuration using EDM

Use an access control entry (ACE) to define a pattern (found in a packet) and the desired behavior for packets that carry the pattern.

Avaya recommends that you create access control lists (ACL) with a default action of permit, and with an ACE mode of deny. For deny or permit ACLs or ACEs, the default action and the mode must be opposite for the ACE (filter) to have meaning.

Configuring an ACE

Configure an ACE to define filter actions, for example, re-marking the Differentiated Services Code Point (DSCP), or mirroring.

Before you begin

- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the ACL to which to add an ACE.
5. Click **ACE**.
6. Click the **ACE Common** tab.
7. Click **Insert**.
8. Configure the ACE ID.
9. Name the ACE.
10. Choose the mode: **deny** (drop packets) or **permit** (forward packets).
11. Configure the ACE actions as required.
12. Click **Insert**.

13. Configure the ACE attributes as required.
14. To enable the ACE, in the **ACE Common** tab, configure **AdminState** to enable, and then click **Apply**.
15. To delete an ACE Common entry, select the entry, and then click **Delete**.

ACE Common field descriptions

Use the data in the following table to use the **ACE Common** tab.

Name	Description
AclId	Specifies the ACL ID.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Name	Specifies a descriptive user-defined name for the ACE. The system automatically assigns a name if you do not type one.
AdminState	Indicates the status of the ACE as enabled or disabled. You can modify an ACE only if you disable it.
OperState	Indicates the current operational state of the ACE.
Mode	Indicates the operating mode for this ACE. Valid options are deny and permit, with deny as the default.
RedirectNextHop	Redirects matching IP traffic to the next hop. Use this option to create a security ACE.
RemarkDscp	Specifies whether the DSCP parameter marks nonstandard traffic classes and local-use Per-Hop Behavior. The default is disable. Use this option to create a QoS ACE.
RemarkDot1Priority	Specifies whether Dot1 Priority, as described by Layer 2 standards (802.1Q and 802.1p) is enabled. The default is disable. Use this option to create a QoS ACE.

Configuring ACE actions

Configure ACE actions to determine the process that occurs after a packet matches (or does not match) an ACE. Use debug actions (flags) to use filters for troubleshooting and monitoring procedures.

Before you begin

- The ACE exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.

2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select an **AceId**.
7. Click **Action**.
8. Configure the actions as required, and then click **Apply**.

Action field descriptions

Use the data in the following table to use the **Action** tab.

Note:

The table lists the options for both Security ACEs and QoS ACEs. Dependent upon the ACE different options appear on the EDM interface.

Name	Description
AclId	Specifies the ACL ID from 1–2048
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Mode	Configures the action mode for security ACEs. The default value is deny.
RemarkDscp	Specifies the new Per-Hop Behavior (PHB) for matching packets: phbcs0, phbcs1, phbaf11, phbaf12, phbaf13, phbcs2, phbaf21, phbaf22, phbaf23, phbcs3, phbaf31, phbaf32, phbaf33, phbcs4, phbaf41, phbaf42, phbaf43, phbcs5, phbef, phbcs6, phbcs7. This action is a QoS action. The ACE ID must be in the range of 1001–2000.
RemarkDot1Priority	Specifies the new 802.1 priority bit for matching packets: zero, one, two, three, four, five, six, or seven. This action is a QoS action. The ACE ID must be in the range of 1001–2000.
InternalQoS	This variable is a QoS action. The ACE ID must be in the range of 1001–2000. The default value is 1.

Table continues…

Name	Description
RedirectNextHop	Specifies the next-hop IP address for redirect mode (a.b.c.d). This action is a security action. The ACE ID must be in the range of 1–1000.
Count	Enables the ability to count matching packets. Use this parameter with either a security or QoS ACE. The default is disabled.
DstPortList	Configures mirroring to a destination port or ports. This action is a security action. The ACE ID must be in the range of 1–1000.
DstMltId	Configures mirroring to a destination MLT. This action is a security action. The ACE ID range is 1-1000.

Configuring ACE ARP entries

Use ACE Address Resolution Protocol (ARP) entries so that the filter looks for ARP request or response packets.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select a parameter for the appropriate ACL.
5. Click **ACE**.
6. Select a parameter for the appropriate ACE.
7. Click **Arp**.
8. Click **Insert**.
9. Select ARP request or response.
10. Click **Insert**.

ARP field descriptions

Use the data in the following table to use the **ARP** tab.

Name	Description
AclId	Specifies the ACL ID from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Type	Specifies the ACE ARP operation. The only option is operation.
Oper	Specifies the operator for the ACE ARP operation. The only option is eq (equal).
Value	Specifies the ARP packet type. Valid options are arpRequest and arpResponse.

Viewing all ACE ARP entries for an ACL

View all of the ACE ARP entries associated with an ACL.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **Arp**.
6. To modify a parameter, double-click the parameter, select the option, and then click **Apply**.

ARP field descriptions

Use the data in the following table to use the **ARP** tab.

Name	Description
AclId	Specifies the ACL ID from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Type	Specifies the ACE ARP operation. The only option is operation.
Oper	Specifies the operator for the ACE ARP operation. The only option is eq (equal).
Value	Specifies the ARP packet type. Valid options are arpRequest and arpResponse.

Configuring an ACE Ethernet source address

Perform this procedure to filter on specific Ethernet source addresses.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **Eth**.
8. Click the **Source Address** tab.
9. Click **Insert**.
10. Specify the ACE Ethernet operation.
11. In the **List** dialog box, specify the Ethernet source address.
12. Click **Insert**.

Source Address field descriptions

Use the data in the following table to use the **Source Address** tab.

Table 47: Variable definitions

Variable	Value
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
List	Specifies the MAC address to match.
OperMask	Specifies the MAC Address mask value in hexadecimal format. The value for this variable is empty or 000000000000 if the **Oper** variable is eq.

Configuring an ACE LAN traffic type

Perform this procedure to filter for specific LAN traffic packets.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **Eth**.
8. Click the **Ethernet Type** tab.
9. Click **Insert**.
10. Specify the operation type.
11. In the **TypeList** box, type the Ethernet types.
12. Click **Insert**.

Ethernet Type field descriptions

Use the data in the following table to use the **Ethernet Type** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
TypeOper	The eq parameter specifies an operator for a field match condition: equal to.
TypeList	Specifies the Ethernet type. Entries include: 0 to 0xffff or ip, arp, ipx802.3, ipx802.2, ipxSnap, ipxEthernet2, appleTalk, appleTalk-ARP, sna802.2, snaEthernet2, netBios, xns, vines, rarp, PPPoE-discovery, and PPPoE-session.

Configuring an ACE Ethernet VLAN tag priority

Perform this procedure to filter for specific VLAN tag priorities.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **Eth**.
8. Click the **Vlan Tag Priority** tab.
9. Click **Insert**.
10. Specify the operation type.
11. In the **VlanTagPrio** box, select the priority bits.
12. Click **Insert**.

Configuring an ACE Ethernet destination address

Perform this procedure to filter on specific Ethernet destination addresses.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.

7. Click **Eth**.
8. Click the **Destination Address** tab.
9. Click **Insert**.
10. Specify the ACE Ethernet operation.
11. In the **List** dialog box, specify the Ethernet source address.
12. Click **Insert**.

Destination Address field descriptions

Use the data in the following table to use the **Destination Address** tab.

Table 48: Variable definitions

Variable	Value
AclId	Specifies the ACL ID.
AceId	Specifies the associated ACE index.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
List	Specifies the MAC address to match.
OperMask	Specifies the MAC address mask value in hexadecimal format if the **Oper** variable is mask. The value of this variable is empty or 000000000000 if **Oper** is eq.

VLAN Tag Priority field descriptions

Use the data in the following table to use the **Vlan Tag Priority** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
OperMask	Specifies the mask value in hexadecimal format if the **Oper** value is mask.
VlanTagPrio	Specifies the priority bits (3-bit field) from the 802.1Q/p tag: • zero • one • two

Table continues…

Name	Description
	• three • four • five • six • seven

Configuring an ACE Ethernet port

Use ACE Ethernet port entries so that the filter looks for traffic on specific ports. You can only insert an ACE Common Ethernet port for VLAN ACL types.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **Eth**.
8. Click the **Port** tab.
9. Click **Insert**.
10. Specify the operation type.
11. Click the **Port** ellipses (**...**).
12. Choose the ports.
13. Click **OK**.
14. Click **Insert**.

Port field descriptions

Use the data in the following table to use the **Port** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq parameter specifies an operator for a field match condition: equal to.
Port	Specifies the port or port list on which to perform a match.

Configuring an ACE Ethernet VLAN ID

Use ACE Ethernet VLAN ID entries so that the filter looks for traffic on specific VLANs. You can insert an ACE Ethernet VLAN ID only for ACL VLAN types.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **Eth**.
8. Click the **Vlan Id** tab.
9. Click **Insert**.
10. Specify the operation type.
11. Enter the VLAN ID or select from a list.
12. Click **Insert**.

VLAN ID field descriptions

Use the data in the following table to use the **Vlan Id** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq parameter specifies an operator for a field match condition: equal to.
VlanIdList	Specifies the VLAN ID on which to perform a match.
OperMask	Specifies the mask value for a VLAN attribute.

Viewing all ACE Ethernet entries for an ACL

View all of the ACE Ethernet entries associated with an ACL.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **Eth**.

Ethernet field descriptions

Use the data in the following table to use the **Ethernet** tab.

Name	Description
AclId	Shows the ACL ID.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
SrcAddrList	Shows the list of Ethernet source addresses to match.
SrcAddrOper	Shows the operators for the ACE Ethernet source MAC address.
SrcAddrOperMask	Shows the source MAC address mask value in hexadecimal format if the **SrcAddrOper** variable is mask. The value of this field is empty or 000000000000 if the **SrcAddrOper** field is eq.
DstAddrList	Shows the list of Ethernet destination addresses to match.
DstAddrOper	Shows the operators for the ACE Ethernet destination MAC address.

Table continues…

Name	Description
DstAddrOperMask	Shows the destination MAC address mask value in hexadecimal format if the **DstAddrOper** variable is mask. The value for this field is empty or 000000000000 if the **DstAddrOper** field is eq
EtherTypeList	Shows the EtherType value from the Ethernet header. For example, ARP uses 0x0806 and IP uses 0x0800. Platform support determines the behavior for 802.1Q/p tagged packets. The EtherType for 802.1Q tagged frames is 0x8100. The range is 0–65535 and supports lists and ranges of values. An invalid Ether-type of 65536 indicates that you do not want the parameter in the match criteria.
EtherTypeOper	Shows the Ethernet type operators.
VlanTagPrio	Shows the priority bits (3-bit field) from the 802.1Q/p tag.
VlanTagPrioOper	Shows the operators for the ACE Ethernet VLAN tag priority.
VlanTagPrioOperMask	Shows the VLAN tag priority mask value in hexadecimal format if the **VlanTagPrioOper** field is mask.
Port	Shows the port number or port list to match.
PortOper	Shows the operator for the ACE Ethernet port.
VlanId	Shows the VLAN ID to match.
VlanIdOper	Shows the operator for the ACE Ethernet VLAN ID.
VlanIdOperMask	Shows the VLAN ID mask value in hexadecimal format if the **VlanIdOper** field is mask.

Configuring an ACE IP source address

Configure ACE IP source address entries to have the filter look for specific source IP addresses.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.

7. Click **IP**.
8. Click the Source Address tab.
9. Click **Insert**.
10. Specify the operation type.
11. In the **IPAddr** box, enter the source IP address.
12. Click **Insert**.

Source Address field descriptions

Use the data in the following table to use the **Source Address** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
IPAddr	Specifies the source IP address.
OperMask	Specifies the mask value for the source IP address.

Configuring an ACE IP destination address

Configure ACE IP destination address entries to have the filter look for specific destination IP addresses.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.

7. Click **IP**.
8. Click the **Destination Address** tab.
9. Click **Insert**.
10. Specify the operation type.
11. In the **IPAddr** box, enter the destination IP address.
12. Click **Insert**.

Destination Address field descriptions

Use the data in the following table to use the **Destination Address** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
IPAddr	Specifies the destination IP address.
OperMask	Specifies the mask value for the destination IP address.

Configuring an ACE IP DSCP

Configure ACE IP DSCP entries to have the filter look for packets with specific DSCP markings.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **IP**.

8. Click the **DSCP** tab.
9. Click **Insert**.
10. Specify the operation type.
11. In the **List** box, enter the count for the DSCP values.
12. Click **Insert**.

DSCP field descriptions

Use the data in the following table to use the **DSCP** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
List	Specifies a count for the number of discrete ranges entered for the DSCP values. Entries include 0–256, disable, phbcs0, phbcs1, phbaf11, phbaf12, phbaf13, phbcs2, phbaf21, phbaf22, phbaf23, phbcs3, phbaf31, phbaf32, phbaf33, phbcs4, phbaf41, phbaf42, phbaf43, phbcs5, phbcs6, phbef, and phbcs7.
OperMask	Specifies the mask value.

Configuring ACE IP options

Configure ACE IP option entries to have the filter look for packets with an IP option specified.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.

6. Select the appropriate ACE.
7. Click **IP**.
8. Click the **Options** tab.
9. Click **Insert**.
10. Specify the logical operator.

    Any is the only choice.
11. Click **Insert**.

Configuring an ACE IP protocol

Configure ACE IP protocol entries to have the filter look for packets of specific protocols.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **IP**.
8. Click the **Protocol** tab.
9. Click **Insert**.
10. Specify the operation type.
11. In the **List** box, enter the IP protocol type.
12. Click **Insert**.

Protocol field descriptions

Use the data in the following table to use the **Protocol** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.

Table continues…

Name	Description
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq parameter specifies an operator for a field match condition: equal to.
List	Specifies the IP protocol type. Entries include 0–256, undefined, tcp, udp, ipsecesp, vrrp, and undefined.

Options field descriptions

Use the data in the following table to use the **Options** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	Specifies the logical operator for the ACE IP options. Any is the only option.

Configuring ACE IP fragmentation

Configure ACE IP fragmentation entries to have the filter look for packets with the fragmentation flag.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **IP**.
8. Click the **Fragmentation** tab.
9. Click **Insert**.

10. Specify the operator for IP fragmentation.

    Eq is the only choice.

11. Specify the fragmentation bits to match from the IP header.
12. Click **Insert**.

Fragmentation field descriptions

Use the data in the following table to use the **Fragmentation** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Fragmentation	Specifies the IP fragmentation bits to match from the IP header: • noFragment • anyFragment The default is noFragment.

Viewing all ACE IP entries for an ACL

View all of the ACE IP entries associated with an ACL.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **IP**.

IP field descriptions

Use the data in the following table to use the **IP** tab.

Name	Description
AclId	Shows the ACL IP ID.
AceId	Shows the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
SrcAddrOper	Shows the operators for the ACE IP source address.
SrcAddrIpAddr	Shows the IP source address to match from the IP header.
SrcAddrOperMaskRange	Shows the IP mask value if **SrcAddrOper** is set to mask, or the highest IP address if **SrcAddrOper** is set to range.
DstAddrOper	Shows the operators for the ACE IP destination address.
DstAddrIpAddr	Shows the IP destination address to match from the IP header.
DstAddrOperMaskRange	Shows the IP mask value if **DstAddrIpAddr** is set to mask, or the highest IP address if **DstAddrIpAddr** is set to range.
DscpList	Shows how the 6-bit DSCP parameter from the TOS byte in the IPv4 header encodes PHB information following RFC 2474.
DscpOper	Shows the operators for the ACE IP DSCP.
DscpOperMask	Shows the mask value in hexadecimal format when the mask option is selected in **DscpOper**.
ProtoList	Shows the IP protocol type from the IP header to match. The range is 0–255.
ProtoOper	Shows the operators for the ACE IP protocols.
Options	Shows the IP options to match from the IP header.
OptionsOper	Shows the logical operator. Any is the only option.
Fragmentation	Shows the IP fragmentation bits to match from the IP header.
FragOper	Shows the operator for IP fragmentation.

Configuring an ACE IPv6 source address

Configure ACE IPv6 source address entries to have the filter look for specific source IP addresses.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.

5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **IPv6**.
8. Click the **Source Address** tab.
9. Click **Insert**.
10. In the **Oper** field, select the operation type.
11. In the **List** field, enter the source IP address.
12. Click **Insert**.

Source Address field descriptions

Use the data in the following table to use the **Source Address** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
List	Specifies the source IP address.
OperMask	Specifies the mask value for the source IP address.

Configuring an ACE IPv6 destination address

Configure ACE IPv6 destination address entries to have the filter look for specific destination IP addresses.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.

5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **IPv6**.
8. Click the **Destination Address** tab.
9. Click **Insert**.
10. In the **Oper** field, select the operation type.
11. In the **List** field, enter the destination IP address.
12. Click **Insert**.

Destination Address field descriptions

Use the data in the following table to use the **Destination Address** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
List	Specifies the destination IP address.
OperMask	Specifies the mask value for the destination IP address.

Configuring an ACE IPv6 next header

Configure ACE IPv6 next header entries to have the filter look for specific next headers.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.

6. Select the appropriate ACE.
7. Click **IPv6**.
8. Click the **Next Hdr** tab.
9. Click **Insert**.
10. In the **Oper** field, select the operation type.
11. In the **NextHdr** field, enter the next header number.
12. Click **Insert**.

Next Header field descriptions

Use the data in the following table to use the **Next Hdr** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq parameter specifies an operator for an “equal to” field match condition.
NextHdr	Specifies the next header of the IPv6 header. Specifies hop-by-hop, tcp, udp, routing, fragment, ipsecESP, ipsecAH, icmpv6, noNxtHdr, or undefined.

Configuring an ACE IPv6 traffic class

Configure ACE IPv6 traffic class.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.

7. Click **IPv6**.
8. Click the **Traffic Class** tab.
9. Click **Insert**.
10. In the **Oper** field, select the operation type.
11. In the **TrafficCls** field, enter the traffic class number.
12. Click **Insert**.

Traffic Class field descriptions

Use the data in the following table to use the **Traffic Class** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq parameter specifies an operator for an “equal to” field match condition.
TrafficCls	Specifies the traffic class attribute of the IPv6 header. Traffic class identifies different classes or priorities of IPv6 packets. The range is 0–255.

Viewing all ACE IPv6 entries for an ACL

View all of the ACE IPv6 entries associated with an ACL.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **IPv6**.

8. Click the **IPv6** tab.

IPv6 field descriptions

Use the data in the following table to use the **IPv6** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
SrcAddrList	Shows the source IP address.
SrcAddrOper	Shows the operators for the ACE IP source address.
DstAddrList	Shows the destination IP address.
DstAddrOper	Shows the operators for the ACE IP destination address.
NxtHdrNxtHdr	Shows the next header of the IPv6 header.
NxtHdrOper	Shows the operators for the next header.
TrafficClsOper	Shows the operators for the traffic class.
TrafficCls	Shows the traffic class attribute of the IPv6 header.
SrcAddrMask	Shows the mask value for the source IP address.
DstAddrMask	Shows the mask value for the destination IP address.

Configuring an ACE source port

Configure ACE source port entries to have the filter look for packets with a specific source port.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **Proto**.

8. Click the **Source Port** tab.
9. Click **Insert**.
10. Specify the operator for the source port.
11. Specify the port number or port list to match.
12. Click **Insert**.

Source Port field descriptions

Use the data in the following table to use the **Source Port** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Port	Specifies the source port (1–65535).
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
OperMask	Specifies the mask parameter, {0-0xFFFF}.

Configuring an ACE destination port

Configure ACE destination port entries to have the filter look for packets with a specific destination port.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **Proto**.

8. Click the **Destination Port** tab.
9. Click **Insert**.
10. Specify the operator for the destination port.
11. Specify the port number or port list to match.
12. Click **Insert**.

Destination Port field descriptions

Use the data in the following table to use the **Destination Port** tab.

Name	Description
AclId	Specifies the ACL index, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Port	Specifies the port number. As noted at the bottom of the tab, potential entries include 0–65535, echo, ftpdata, ftpcontrol, ssh, telnet, dns, http, h.323, and undefined.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
OperMask	Specifies the mask parameter, {0-0xFFFF}.

Configuring an ACE ICMP message type

Configure ACE Internet Control Message Protocol (ICMP) message type entries to have the filter look for packets of a specific ICMP message type.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.

7. Click **Proto**.
8. Click the **Icmp Msg Type** tab.
9. Click **Insert**.
10. Specify the operator for the ICMP message type.
11. In the **List** box, specify the ICMP messages to match.
12. Click **Insert**.

Icmp Msg Type field descriptions

Use the data in the following table to use the **Icmp Msg Type** tab.

Name	Description
AclId	Specifies the ACL Id, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	Specifies the operator for the ACE protocol ICMP message type. Equal (eq) is the only option.
List	Specifies the ICMP message type (0–255), or echoreply, destunreach, sourcequench, redirect, echo-request, routeradv, routerselect, time-exceeded, param-problem, timestamp-request, timestamp-reply, addressmask-request, addressmask-reply, or traceroute.

Configuring an ACE TCP flag

Configure ACE TCP flag entries to have the filter look for packets with a specific TCP flag.

Before you begin

- The ACE exists.
- The ACL exists.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **ACE**.
6. Select the appropriate ACE.
7. Click **Proto**.

8. Click the **TCP Flags** tab.
9. Click **Insert**.
10. Specify the operator for the TCP flags entry.
11. In the **List** box, specify the TCP flags to match.
12. Click **Insert**.

TCP Flags field descriptions

Use the data in the following table to use the **TCP Flags** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
Oper	The eq and mask parameters specify an operator for a field match condition: equal to or mask. The mask operator is an implied eq on the mask bits.
List	Specifies one or more TCP flags—none, fin (finish connection), syn (synchronize), rst (reset connection), push, ack (acknowledge), urg (urgent), and undefined.
OperMask	Specifies the mask value.

Viewing all ACE protocol entries for an ACL

View all of the ACE protocol entries associated with an ACL.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **ACL** tab.
4. Select the appropriate ACL.
5. Click **Proto**.

Protocol field descriptions

Use the data in the following table to use the **Protocol** tab.

Name	Description
AclId	Specifies the ACL ID, from 1–2048.
AceId	Specifies the ACE ID. Use ACE IDs 1–1000 for security rules. Use ACE IDs 1001–2000 for QoS rules.
SrcPort	Specifies the port number or port list to match.
SrcPortOper	Specifies the operator for the ACE protocol source port.
SrcPortOperMaskRange	The value is displayed in hexadecimal format when **SrcPortOper** is set to mask. When **SrcPortOper** is set to range, this field is used as the high range value. in this case, the value is displayed in decimal format. When **SrcPortOper** is set to eq, this field is set to 0.
DstPort	Specifies port number or port list to match.
DstPortOper	Specifies the operator for the ACE protocol destination port.
DstPortOperMaskRange	The value is displayed in hexadecimal format when **DstPortOper** is set to mask. When **DstPortOper** is set to range, this field is used as the high range value. In this case, the value is displayed in decimal format. When **SrcPortOper** is set to eq, this field is set to 0.
IcmpMsgTypeList	Specifies one or a list of ICMP messages to match. The valid range is 0–255 (reserved).
IcmpMsgTypeOper	Specifies the operator for the ACE protocol ICMP message types.
TcpFlagsList	Specifies one or a list of TCP flags to match. The valid range is 0–63.
TcpFlagsOper	Specifies the operator for the ACE protocol TCP flags.
TcpFlagsOperMask	Displays the mask value in hexadecimal format when **TcpFlagsOper** is set to mask. When **TcpFlagsOper** is set to eq, this field displays 0x0.

Chapter 13: Common procedures using ACLI

The following section describes common procedures that you use while you configure and monitor the Avaya Virtual Services Platform 4000 Series Quality of Service (QoS) and filter operations.

Note:

The default prompt for the non-PowerPlus chassis is VSP-4850GTS. The default prompt for the PowerPlus chassis is VSP-4850GTS-PWR+. The default prompt for the PowerPlus chassis with additional fiber ports is VSP-4450GSX-PWR+. For consistency, this document uses the VSP-4850GTS prompt.

Saving the configuration

Save the configuration to a file to retain the configuration settings.

About this task

File Transfer Protocol (FTP) and Trivial File Transfer Protocol (TFTP) support both IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Procedure

1. Enter the Privileged EXEC mode:

   ```
   enable
   ```

2. Save the running configuration:

   ```
   save config [backup WORD<1-99>] [file WORD<1-99>] [verbose]
   ```

Example

```
VSP-4850GTS>enable
```

Save the file to the default location:

```
VSP-4850GTS#save config
```

Variable definitions

Use the data in the following table to use the `save config` command.

Table 49: Variable definitions

Variable	Value
backup *WORD<1–99>*	Saves the specified file name and identifies the file as a backup file. `WORD` uses one of the following formats: • a.b.c.d:<file> • /intflash/<file> The file name, including the directory structure, can include up to 99 characters.
file *WORD<1–99>*	Specifies the file name in one of the following formats: • a.b.c.d:<file> • /intflash/<file> The file name, including the directory structure, can include up to 99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

Restarting the platform

Restart the switch to implement configuration changes or recover from a system failure.

About this task

When you restart the system, you can specify the boot source (flash file or TFTP server) and file name. If you do not specify a device and file, the run-time ACLI uses the software and configuration files on the primary boot device defined by the `boot config choice` command.

After the switch restarts normally, it sends a cold trap within 45 seconds after a restart.

Procedure

1. Enter the Privileged EXEC mode:

   ```
   enable
   ```

2. Restart the switch:

```
boot [config WORD<1-99>] [-y]
```

Important:

If you enter the `boot` command with no arguments, you cause the switch to start using the current boot choices defined by the `boot config choice` command.

Variable definitions

Use the data in the following table to use the `boot` command.

Table 50: Variable definitions

Variable	Value
config *WORD<1–99>*	Specifies the software configuration device and file name in one of the following format: • a.b.c.d:<file> The file name, including the directory structure, can include up to 99 characters.
-y	Suppresses the confirmation message before the switch restarts. If you omit this parameter, you must confirm the action before the system restarts.

Chapter 14: Common procedures using EDM

The following section describes common procedures that you use while you configure and monitor the Avaya Virtual Services Platform 4000 Series Quality of Service (QoS) and filter operations using Enterprise Device Manager (EDM).

Saving the configuration

Save the configuration to a file to retain the configuration settings.

Procedure

1. In the Device Physical View tab, select the Device.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit**.
3. Double-click **Chassis**.
4. Click the **System** tab.
5. In ActionGroup1, select **saveRuntimeConfig** .
6. Optionally, specify a filename in **ConfigFileName**.

   If you do not specify a filename, the system saves the information to the default file.
7. Click **Apply**.

Chapter 15: Advanced filter examples

This section provides a detailed advanced filter configuration example.

ACE filters for secure networks

The following example shows filters for two Layer 2 switched hosts and two Layer 3 routed hosts for an IP Deskphone and computer VLAN network.

These filters apply after an analysis of the traffic types flowing on the network. The filters provide security by permitting legitimate traffic and denying (dropping) all other traffic. Filters redirect certain traffic to another IP address. The filters can also determine which traffic is permitted on which parts of the network.

The access control entries (ACE) named DENY ANY or DENY ANY ANY are the clean-up filters. These filters drop traffic that does not match another ACE.

The ACEs permit the following traffic (this is not an exhaustive list):

- Domain Name Service (DNS) traffic
- Internet Control Message Protocol (ICMP) traffic
- Virtual Router Redundancy Protocol (VRRP) traffic (in certain areas)
- BootStrap Protocol server and client traffic
- Dynamic Host Configuration Protocol (DHCP) traffic
- Network Basic Input/Output System (NetBIOS) traffic (in certain areas)
- Transport Control Protocol (TCP) traffic with the Established flag on
- traffic with specific IP addresses
- Microsoft Operations Manager 2005 agent (MOM 2005) traffic
- Hypertext Transfer Protocol (HTTP), HTTP proxy, and HTTP, Secure (HTTPS) traffic
- remote desktop traffic
- Internet Security Association and Key Management Protocol (ISAKMP) and Internet Key Exchange (IKE) traffic
- SQL database system traffic

Other ACEs are configured to deny (drop):

- VRRP traffic (in certain areas)

- NetBIOS traffic (UDP destination ports 137, 138)
- specific multicast traffic (UDP destination ports 61011, 64046)
- specific UDP traffic
- instant messaging traffic (UDP destination port 1900)

Layer 2 host configuration

This section shows the filters configured for the first Layer 2 switched host.

```
#
# FILTER CONFIGURATION
#

filter acl 1 type outPort name "VRRP_Drop"
filter acl port 1 1/24-1/25,1/37
filter acl ace 1 1 name "VRRP"
filter acl ace ethernet 1 1 ether-type eq ip
filter acl ace ip 1 1 ip-protocol-type eq vrrp
filter acl ace 1 1 enable
filter acl ace 1 2 name "NetbIOS_Drop"
filter acl ace ethernet 1 2 ether-type eq netBios
filter acl ace ip 1 2 ip-protocol-type eq udp
filter acl ace protocol 1 2 dst-port eq 137
filter acl ace 1 2 enable
filter acl ace 1 3 name "NetbIOS2_Drop"
filter acl ace ip 1 3 ip-protocol-type eq udp
filter acl ace protocol 1 3 dst-port eq 138
filter acl ace 1 3 enable
filter acl ace 1 4 name "WL_Multicast1_Drop"
filter acl ace ip 1 4 ip-protocol-type eq udp
filter acl ace protocol 1 4 dst-port eq 61011
filter acl ace 1 4 enable
filter acl ace 1 5 name "WL_Multicast2_Drop"
filter acl ace ip 1 5 ip-protocol-type eq udp
filter acl ace protocol 1 5 dst-port eq 64046
filter acl ace 1 5 enable
filter acl ace 1 6 name "UDP_1100_Drop"
filter acl ace ethernet 1 6 ether-type eq ip
```

```
filter acl ace ip 1 6 dst-ip eq 100.20.100.255
filter acl ace ip 1 6 ip-protocol-type eq udp
filter acl ace protocol 1 6 dst-port eq 1100
filter acl ace 1 6 enable
filter acl ace 1 7 name "UDP_67_Drop"
filter acl ace ip 1 7 ip-protocol-type eq udp
filter acl ace protocol 1 7 dst-port eq 67
filter acl ace 1 7 enable
filter acl ace 1 8 name "Messenger"
filter acl ace ip 1 8 ip-protocol-type eq udp
filter acl ace protocol 1 8 dst-port eq 1900
filter acl ace 1 8 enable
filter acl 20 type inVlan name "Symantec-Drop"
filter acl vlan 20 2
filter acl ace 20 10 name "Othello-drop"
filter acl ace ethernet 20 10 ether-type eq ip
filter acl ace ip 20 10 src-ip eq 100.20.2.47
filter acl ace ip 20 10 ip-protocol-type eq tcp
filter acl ace protocol 20 10 src-port eq 80
filter acl ace 20 10 enable
filter acl ace 20 15 name "Macbeth-drop"
filter acl ace action 20 15 deny
filter acl ace ethernet 20 15 ether-type eq ip
filter acl ace ip 20 15 src-ip eq 100.20.2.29
filter acl ace ip 20 15 ip-protocol-type eq tcp
filter acl ace protocol 20 15 src-port eq 80
filter acl 902 type inVlan name "ITD_REMOTE_in"
filter acl vlan 902 902
no filter acl 902 enable
filter acl ace 902 5 name "ITD_TO_ITD"
filter acl ace action 902 5 permit
filter acl ace ethernet 902 5 ether-type eq ip
filter acl ace ip 902 5 dst-ip eq 100.20.103.65
```

```
filter acl ace 902 5 enable
filter acl ace 902 10 name "ICMP_PERMIT"
filter acl ace action 902 10 permit
filter acl ace ethernet 902 10 ether-type eq ip
filter acl ace ip 902 10 ip-protocol-type eq icmp
filter acl ace 902 10 enable
filter acl ace 902 20 name "IGMP_PERMIT"
filter acl ace action 902 20 permit
filter acl ace ethernet 902 20 ether-type eq ip
filter acl ace ip 902 20 ip-protocol-type eq 2
filter acl ace 902 20 enable
filter acl ace 902 30 name "VRRP_PERMIT"
filter acl ace action 902 30 permit
filter acl ace ethernet 902 30 ether-type eq ip
filter acl ace ip 902 30 ip-protocol-type eq vrrp
filter acl ace 902 30 enable
filter acl ace 902 35 name "BOOTPS"
filter acl ace action 902 35 permit
filter acl ace protocol 902 35 dst-port eq 67
filter acl ace 902 35 enable
filter acl ace 902 36 name "BOOTPC"
filter acl ace action 902 36 permit
filter acl ace protocol 902 36 dst-port eq 68
filter acl ace 902 36 enable
filter acl ace 902 40 name "DNS_PERMIT"
filter acl ace action 902 40 permit
filter acl ace ethernet 902 40 ether-type eq ip
filter acl ace ip 902 40 src-ip eq 100.20.103.65
filter acl ace protocol 902 40 dst-port eq dns
filter acl ace 902 40 enable
filter acl ace 902 43 name "Netbios_Erisim"
filter acl ace action 902 43 permit
filter acl ace ethernet 902 43 ether-type eq ip
```

```
filter acl ace ip 902 43 src-ip eq 100.20.103.65
filter acl ace protocol 902 43 dst-port eq 135
filter acl ace 902 43 enable
filter acl ace 902 45 name "ESTABLISHED"
filter acl ace action 902 45 permit
filter acl ace ethernet 902 45 ether-type eq ip
filter acl ace ip 902 45 src-ip eq 100.20.103.65
filter acl ace ip 902 45 ip-protocol-type eq tcp
filter acl ace protocol 902 45 dst-port eq 1023
filter acl ace protocol 902 45 tcp-flags eq rst
filter acl ace 902 45 enable
filter acl ace 902 46 name "ESTABLISHED2"
filter acl ace action 902 46 permit
filter acl ace ethernet 902 46 ether-type eq ip
filter acl ace ip 902 46 src-ip eq 100.20.103.65
filter acl ace ip 902 46 ip-protocol-type eq tcp
filter acl ace protocol 902 46 dst-port eq 1023
filter acl ace protocol 902 46 tcp-flags eq ack
filter acl ace 902 46 enable
filter acl ace 902 50 name "DC-EXCH-DNS"
filter acl ace action 902 50 permit
filter acl ace ethernet 902 50 ether-type eq ip
filter acl ace ip 902 50 src-ip eq 100.20.103.65
filter acl ace ip 902 50 dst-ip eq 100.20.104.0
filter acl ace 902 50 enable
filter acl ace 902 55 name "DC-EXCH-DNS_OPC"
filter acl ace action 902 55 permit
filter acl ace ethernet 902 55 ether-type eq ip
filter acl ace ip 902 55 src-ip eq 100.20.103.65
filter acl ace ip 902 55 dst-ip eq 100.6.105.0
filter acl ace 902 55 enable
filter acl ace 902 60 name "Filesharing_Erisim"
filter acl ace action 902 60 permit
```

```
filter acl ace ethernet 902 60 ether-type eq ip
filter acl ace ip 902 60 src-ip eq 100.20.103.65
filter acl ace ip 902 60 dst-ip eq 100.20.103.71
filter acl ace 902 60 enable
filter acl ace 902 65 name "Filesharing_Erisim_Ek"
filter acl ace action 902 65 permit
filter acl ace ethernet 902 65 ether-type eq ip
filter acl ace ip 902 65 src-ip eq 100.20.103.65
filter acl ace ip 902 65 dst-ip eq 10.10.230.6
filter acl ace 902 65 enable
filter acl ace 902 70 name "IBPSQL_Erisim"
filter acl ace action 902 70 permit
filter acl ace ethernet 902 70 ether-type eq ip
filter acl ace ip 902 70 src-ip eq 100.20.103.65
filter acl ace ip 902 70 dst-ip eq 100.20.100.176
filter acl ace ip 902 70 ip-protocol-type eq tcp
filter acl ace protocol 902 70 dst-port eq 4450
filter acl ace 902 70 enable
filter acl ace 902 75 name "CTI_Erisim"
filter acl ace action 902 75 permit
filter acl ace ethernet 902 75 ether-type eq ip
filter acl ace ip 902 75 src-ip eq 100.20.103.65
filter acl ace ip 902 75 dst-ip eq 100.6.100.161
filter acl ace ip 902 75 ip-protocol-type eq tcp
filter acl ace protocol 902 75 dst-port eq 1433
filter acl ace 902 75 enable
filter acl ace 902 80 name "PVA_ERISIM"
filter acl ace action 902 80 permit
filter acl ace ethernet 902 80 ether-type eq ip
filter acl ace ip 902 80 src-ip eq 100.20.103.65
filter acl ace ip 902 80 dst-ip eq 100.6.100.138
filter acl ace ip 902 80 ip-protocol-type eq tcp
filter acl ace protocol 902 80 dst-port eq 1521
```

```
filter acl ace 902 80 enable
filter acl ace 902 85 name "PWC_ERISIM"
filter acl ace action 902 85 permit
filter acl ace ethernet 902 85 ether-type eq ip
filter acl ace ip 902 85 src-ip eq 100.20.103.65
filter acl ace ip 902 85 dst-ip eq 100.6.100.113
filter acl ace ip 902 85 ip-protocol-type eq tcp
filter acl ace protocol 902 85 dst-port eq 1521
filter acl ace 902 85 enable
filter acl ace 902 90 name "OASIS_ERISIM"
filter acl ace action 902 90 permit
filter acl ace ethernet 902 90 ether-type eq ip
filter acl ace ip 902 90 src-ip eq 100.20.103.65
filter acl ace ip 902 90 dst-ip eq 100.6.100.112
filter acl ace ip 902 90 ip-protocol-type eq tcp
filter acl ace protocol 902 90 dst-port eq 1521
filter acl ace 902 90 enable
filter acl ace 902 95 name "AV-YAMA_YONETIM__9968"
filter acl ace action 902 95 permit
filter acl ace ethernet 902 95 ether-type eq ip
filter acl ace ip 902 95 src-ip eq 100.20.103.65
filter acl ace ip 902 95 ip-protocol-type eq tcp
filter acl ace protocol 902 95 dst-port eq 9968
filter acl ace 902 95 enable
filter acl ace 902 100 name "AV-YAMA_YONETIM_2967"
filter acl ace action 902 100 permit
filter acl ace ethernet 902 100 ether-type eq ip
filter acl ace ip 902 100 src-ip eq 100.20.103.65
filter acl ace ip 902 100 ip-protocol-type eq tcp
filter acl ace protocol 902 100 dst-port eq 2967
filter acl ace 902 100 enable
filter acl ace 902 105 name "AV-YAMA_YONETIM_UDP_2967"
filter acl ace action 902 105 permit
```

```
filter acl ace ip 902 105 src-ip eq 100.20.103.65
filter acl ace ip 902 105 ip-protocol-type eq udp
filter acl ace protocol 902 105 dst-port eq 2967
filter acl ace 902 105 enable
filter acl ace 902 108 name "AV-YAMA_YONETIM_SOURCE_9968"
filter acl ace action 902 108 permit
filter acl ace ethernet 902 108 ether-type eq ip
filter acl ace ip 902 108 src-ip eq 100.20.103.65
filter acl ace ip 902 108 ip-protocol-type eq udp
filter acl ace protocol 902 108 src-port eq 9968
filter acl ace 902 108 enable
filter acl ace 902 110 name "ALERT_MOM_SMS_ERISIM_TCP_1270"
filter acl ace action 902 110 permit
filter acl ace ethernet 902 110 ether-type eq ip
filter acl ace ip 902 110 src-ip eq 100.20.103.65
filter acl ace ip 902 110 dst-ip eq 100.6.140.10
filter acl ace ip 902 110 ip-protocol-type eq tcp
filter acl ace protocol 902 110 dst-port eq 1270
filter acl ace 902 110 enable
filter acl ace 902 120 name "ALERT_MOM_SMS_ERISIM_UDP_1270"
filter acl ace action 902 120 permit
filter acl ace ethernet 902 120 ether-type eq ip
filter acl ace ip 902 120 src-ip eq 100.20.103.65
filter acl ace ip 902 120 dst-ip eq 100.6.140.10
filter acl ace ip 902 120 ip-protocol-type eq udp
filter acl ace protocol 902 120 dst-port eq 1270
filter acl ace 902 120 enable
filter acl ace 902 130 name "ALERT_MOM_SMS_ERISIM_HTTP"
filter acl ace action 902 130 permit
filter acl ace ethernet 902 130 ether-type eq ip
filter acl ace ip 902 130 src-ip eq 100.20.103.65
filter acl ace ip 902 130 dst-ip eq 100.6.140.13
filter acl ace ip 902 130 ip-protocol-type eq tcp
```

```
filter acl ace protocol 902 130 dst-port eq 80
filter acl ace 902 130 enable
filter acl ace 902 135 name "ALERT_MOM_SMS_ERISIM_HTTP2"
filter acl ace action 902 135 permit
filter acl ace ethernet 902 135 ether-type eq ip
filter acl ace ip 902 135 src-ip eq 100.20.103.65
filter acl ace ip 902 135 dst-ip eq 100.6.106.92
filter acl ace ip 902 135 ip-protocol-type eq tcp
filter acl ace protocol 902 135 dst-port eq 80
filter acl ace 902 135 enable
filter acl ace 902 140 name "ALERT_MOM_SMS_ERISIM_1521"
filter acl ace action 902 140 permit
filter acl ace ethernet 902 140 ether-type eq ip
filter acl ace ip 902 140 src-ip eq 100.20.103.65
filter acl ace ip 902 140 dst-ip eq 100.6.100.126
filter acl ace ip 902 140 ip-protocol-type eq tcp
filter acl ace protocol 902 140 dst-port eq 1521
filter acl ace 902 140 enable
filter acl ace 902 150 name "ALERT_MOM_SMS_ERISIM_1521x"
filter acl ace action 902 150 permit
filter acl ace ethernet 902 150 ether-type eq ip
filter acl ace ip 902 150 src-ip eq 100.20.103.65
filter acl ace ip 902 150 dst-ip eq 100.20.100.47
filter acl ace ip 902 150 ip-protocol-type eq tcp
filter acl ace protocol 902 150 dst-port eq 1521
filter acl ace 902 150 enable
filter acl ace 902 155 name "FULL_ERISIM"
filter acl ace action 902 155 permit
filter acl ace ethernet 902 155 ether-type eq ip
filter acl ace ip 902 155 dst-ip eq 100.20.100.149
filter acl ace 902 155 enable
filter acl ace 902 160 name "LOGLAMAK_ICIN"
filter acl ace action 902 160 permit redirect-next-hop 100.20.150.34
```

```
filter acl ace ethernet 902 160 ether-type eq ip
filter acl ace ip 902 160 src-ip eq 0.0.0.0
filter acl ace 902 170 name "DENY_ANY_ANY"
filter acl ace action 902 170 deny
filter acl ace ethernet 902 170 ether-type eq ip
filter acl ace ip 902 170 src-ip eq 0.0.0.0
filter acl ace ip 902 170 dst-ip eq 0.0.0.0
filter acl ace 902 170 enable
```

The following section provides details about the filter configuration for the second switched Layer 2 host.

```
#
# FILTER CONFIGURATION
#

filter acl 1 type outPort name "VRRP Drop"
filter acl port 1 add 1/24-1/25,1/37
filter acl ace 1 1 name "VRRP"
filter acl ace action 1 1 deny
filter acl ace ethernet 1 1 ether-type eq ip
filter acl ace ip 1 1 ip-protocol-type eq vrrp
filter acl ace 1 1 enable
filter acl ace 1 2 name "NetbIOS_Drop"
filter acl ace action 1 2 deny
filter acl ace ethernet 1 2 ether-type eq ip
filter acl ace ip 1 2 ip-protocol-type eq udp
filter acl ace protocol 1 2 dst-port eq 137
filter acl ace 1 2 enable
filter acl ace 1 3 name "NetbIOS2_Drop"
filter acl ace action 1 3 deny
filter acl ace ethernet 1 3 ether-type eq ip
filter acl ace ip 1 3 ip-protocol-type eq udp
filter acl ace protocol 1 3 dst-port eq 138
filter acl ace 1 3 enable
filter acl ace 1 4 name "WL_Multicast1_Drop"
```

```
filter acl ace action 1 4 deny
filter acl ace ethernet 1 4ether-type eq ip
filter acl ace ip 1 4 ip-protocol-type eq udp
filter acl ace protocol 1 4 dst-port eq 61011
filter acl ace 1 4 enable
filter acl ace 1 5 name "WL_Multicast2_Drop"
filter acl ace action 1 5 deny
filter acl ace ethernet 1 5 ether-type eq ip
filter acl ace ip 1 5 ip-protocol-type eq udp
filter acl ace protocol 1 5 dst-port eq 64046
filter acl ace 1 5 enable
filter acl 20 type inVlan name "Symantec-Drop"
filter acl vlan 20 2
filter acl ace 20 10 name "Othello-drop"
filter acl ace action 20 10 deny
filter acl ace ethernet 20 10 ether-type eq ip
filter acl ace ip 20 10 src-ip eq 100.20.2.47
filter acl ace ip 20 10 ip-protocol-type eq tcp
filter acl ace protocol 20 10 src-port eq 80
filter acl ace 20 10 enable
filter acl ace 20 15 name "Macbeth-drop"
filter acl ace 20 15 action deny
filter acl ace ethernet 20 15 ether-type eq ip
filter acl ace ip 20 15 src-ip eq 100.20.2.29
filter acl ace ip 20 15 ip-protocol-type eq tcp
filter acl ace protocol 20 15 src-port eq 80

filter acl 902 type inVlan name "ITD_REMOTE_in"
filter acl vlan 902 902
filter acl 902 disable
filter acl ace 902 5 name "ITD_TO_ITD"
filter acl ace action 902 5 permit
filter acl ace ethernet 902 5 ether-type eq ip
filter acl ace ip 902 5 dst-ip eq 100.20.103.65
```

```
filter acl ace 902 5 enable
filter acl ace 902 10 name "ICMP_PERMIT"
filter acl ace action 902 10 permit
filter acl ace ethernet 902 10 ether-type eq ip
filter acl ace ip 902 10 ip-protocol-type eq icmp
filter acl ace 902 10 enable
filter acl ace 902 20 name "IGMP_PERMIT"
filter acl ace action 902 20 permit
filter acl ace ethernet 902 20 ether-type eq ip
filter acl ace ip 902 20 ip-protocol-type eq 2
filter acl ace 902 20 enable
filter acl ace 902 30 name "VRRP_PERMIT"
filter acl ace action 902 30 permit
filter acl ace ethernet 902 30 ether-type eq ip
filter acl ace ip 902 30 ip-protocol-type eq vrrp
filter acl ace 902 30 enable
filter acl ace 902 35 name "BOOTPS"
filter acl ace action 902 35 permit
filter acl ace protocol 902 35 dst-port eq 67
filter acl ace 902 35 enable
filter acl ace 902 36 name "BOOTPC"
filter acl ace action 902 36 permit
filter acl ace protocol 902 36 dst-port eq 68
filter acl ace 902 36 enable
filter acl ace 902 40 name "DNS_PERMIT"
filter acl ace action 902 40 permit
filter acl ace ethernet 902 40 ether-type eq ip
filter acl ace ip 902 40 src-ip eq 100.20.103.65
filter acl ace protocol 902 40 dst-port eq dns
filter acl ace 902 40 enable
filter acl ace 902 43 name "Netbios_Erisim"
filter acl ace action 902 43 permit
filter acl ace ethernet 902 43 ether-type eq ip
```

```
filter acl ace ip 902 43 src-ip eq 100.20.103.65
filter acl ace protocol 902 43 dst-port eq 135
filter acl ace 902 43 enable
filter acl ace 902 45 name "ESTABLISHED ACK"
filter acl ace action 902 45 permit
filter acl ace ethernet 902 45 ether-type eq ip
filter acl ace ip 902 45 src-ip eq 100.20.103.65
filter acl ace ip 902 45 ip-protocol-type eq tcp
filter acl ace protocol 902 45 dst-port eq 1023
filter acl ace protocol 902 45 tcp-flags eq ack
filter acl ace 902 45 enable
filter acl ace 902 46 name "ESTABLISHED RST"
filter acl ace action 902 46 permit
filter acl ace ethernet 902 46 ether-type eq ip
filter acl ace protocol 902 46 tcp-flags eq rst
filter acl ace 902 46 enable
filter acl ace 902 50 name "DC-EXCH-DNS"
filter acl ace action 902 50 permit
filter acl ace ethernet 902 50 ether-type eq ip
filter acl ace ip 902 50 src-ip eq 100.20.103.65
filter acl ace ip 902 50 dst-ip eq 100.20.104.0
filter acl ace 902 50 enable
filter acl ace 902 55 name "DC-EXCH-DNS_OPC"
filter acl ace action 902 55 permit
filter acl ace ethernet 902 55 ether-type eq ip
filter acl ace ip 902 55 src-ip eq 100.20.103.65
filter acl ace ip 902 55 dst-ip eq 100.6.105.0
filter acl ace 902 55 enable
filter acl ace 902 60 name "Filesharing_Erisim"
filter acl ace action 902 60 permit
filter acl ace ethernet 902 60 ether-type eq ip
filter acl ace ip 902 60 src-ip eq 100.20.103.65
filter acl ace ip 902 60 dst-ip eq 100.20.103.71
```

```
filter acl ace 902 60 enable
filter acl ace 902 65 name "Filesharing_Erisim_Ek"
filter acl ace action 902 65 permit
filter acl ace ethernet 902 65 ether-type eq ip
filter acl ace ip 902 65 src-ip eq 100.20.103.65
filter acl ace ip 902 65 dst-ip eq 10.10.230.6
filter acl ace 902 65 enable
filter acl ace 902 70 name "IBPSQL_Erisim"
filter acl ace action 902 70 permit
filter acl ace ethernet 902 70 ether-type eq ip
filter acl ace ip 902 70 src-ip eq 100.20.103.65
filter acl ace ip 902 70 dst-ip eq 100.20.100.176
filter acl ace ip 902 70 ip-protocol-type eq tcp
filter acl ace protocol 902 70 dst-port eq 4450
filter acl ace 902 70 enable
filter acl ace 902 75 name "CTI_Erisim"
filter acl ace action 902 75 permit
filter acl ace ethernet 902 75 ether-type eq ip
filter acl ace ip 902 75 src-ip eq 100.20.103.65
filter acl ace ip 902 75 dst-ip eq 100.6.100.161
filter acl ace ip 902 75 ip-protocol-type eq tcp
filter acl ace protocol 902 75 dst-port eq 1433
filter acl ace 902 75 enable
filter acl ace 902 80 name "PVA_ERISIM"
filter acl ace action 902 80 permit
filter acl ace ethernet 902 80 ether-type eq ip
filter acl ace ip 902 80 src-ip eq 100.20.103.65
filter acl ace ip 902 80 ip eq 100.6.100.138
filter acl ace ip 902 80 ip-protocol-type eq tcp
filter acl ace protocol 902 80 dst-port eq 1521
filter acl ace 902 80 enable
filter acl ace 902 85 name "PWC_ERISIM"
filter acl ace action 902 85 permit
```

```
filter acl ace ethernet 902 85 ether-type eq ip
filter acl ace ip 902 85 src-ip eq 100.20.103.65
filter acl ace ip 902 85 dst-ip eq 100.6.100.113
filter acl ace ip 902 85 ip-protocol-type eq tcp
filter acl ace protocol 902 85 dst-port eq 1521
filter acl ace 902 85 enable
filter acl ace 902 90 name "OASIS_ERISIM"
filter acl ace action 902 90 permit
filter acl ace ethernet 902 90 ether-type eq ip
filter acl ace ip 902 90 src-ip eq 100.20.103.65
filter acl ace ip 902 90 dst-ip eq 100.6.100.112
filter acl ace ip 902 90 ip-protocol-type eq tcp
filter acl ace protocol 902 90 dst-port eq 1521
filter acl ace 902 90 enable
filter acl ace 902 95 name "AV-YAMA_YONETIM__9968"
filter acl ace action 902 95 permit
filter acl ace ethernet 902 95 ether-type eq ip
filter acl ace ip 902 95 src-ip eq 100.20.103.65
filter acl ace ip 902 95 ip-protocol-type eq tcp
filter acl ace protocol 902 95 dst-port eq 9968
filter acl ace 902 95 enable
filter acl ace 902 100 name "AV-YAMA_YONETIM_2967"
filter acl ace action 902 100 permit
filter acl ace ethernet 902 100 ether-type eq ip
filter acl ace ip 902 100 src-ip eq 100.20.103.65
filter acl ace ip 902 100 ip-protocol-type eq tcp
filter acl ace protocol 902 100 dst-port eq 2967
filter acl ace 902 100 enable
filter acl ace 902 105 name "AV-YAMA_YONETIM_UDP_2967"
filter acl ace action 902 105 permit
filter acl ace ethernet 902 105 ether-type eq ip
filter acl ace ip 902 105 src-ip eq 100.20.103.65
filter acl ace ip 902 105 ip-protocol-type eq udp
```

```
filter acl ace protocol 902 105 dst-port eq 2967
filter acl ace 902 105 enable
filter acl ace 902 108 name "AV-YAMA_YONETIM_SOURCE_9968"
filter acl ace action 902 108 permit
filter acl ace ethernet 902 108 ether-type eq ip
filter acl ace ip 902 108 src-ip eq 100.20.103.65
filter acl ace ip 902 108 ip-protocol-type eq udp
filter acl ace protocol 902 108 src-port eq 9968
filter acl ace 902 108 enable
filter acl ace 902 110 name "ALERT_MOM_SMS_ERISIM_TCP_1270"
filter acl ace action 902 110 permit
filter acl ace ethernet 902 110 ether-type eq ip
filter acl ace ip 902 110 src-ip eq 100.20.103.65
filter acl ace ip 902 110 dst-ip eq 100.6.140.10
filter acl ace ip 902 110 ip-protocol-type eq tcp
filter acl ace protocol 902 110 dst-port eq 1270
filter acl ace 902 110 enable
filter acl ace 902 120 name "ALERT_MOM_SMS_ERISIM_UDP_1270"
filter acl ace action 902 120 permit
filter acl ace ethernet 902 120 ether-type eq ip
filter acl ace ip 902 120 src-ip eq 100.20.103.65
filter acl ace ip 902 120 dst-ip eq 100.6.140.10
filter acl ace ip 902 120 ip-protocol-type eq udp
filter acl ace protocol 902 120 dst-port eq 1270
filter acl ace 902 120 enable
filter acl ace 902 130 name "ALERT_MOM_SMS_ERISIM_HTTP"
filter acl ace action 902 130 permit
filter acl ace ethernet 902 130 ether-type eq ip
filter acl ace ip 902 130 src-ip eq 100.20.103.65
filter acl ace ip 902 130 dst-ip eq 100.6.140.13
filter acl ace ip 902 130 ip-protocol-type eq tcp
filter acl ace protocol 902 130 dst-port eq 80
filter acl ace 902 130 enable
```

```
filter acl ace 902 135 name "ALERT_MOM_SMS_ERISIM_HTTP2"
filter acl ace action 902 135 permit
filter acl ace ethernet 902 135 ether-type eq ip
filter acl ace ip 902 135 src-ip eq 100.20.103.65
filter acl ace ip 902 135 dst-ip eq 100.6.106.92
filter acl ace ip 902 135 ip-protocol-type eq tcp
filter acl ace protocol 902 135 dst-port eq 80
filter acl ace 902 135 enable
filter acl ace 902 140 create name "ALERT_MOM_SMS_ERISIM_1521"
filter acl ace action 902 140 permit
filter acl ace ethernet 902 140 ether-type eq ip
filter acl ace ip 902 140 src-ip eq 100.20.103.65
filter acl ace ip 902 140 dst-ip eq 100.6.100.126
filter acl ace ip 902 140 ip-protocol-type eq tcp
filter acl ace protocol 902 140 dst-port eq 1521
filter acl ace 902 140 enable
filter acl ace 902 150 name "ALERT_MOM_SMS_ERISIM_1521x"
filter acl ace action 902 150 permit
filter acl ace ethernet 902 150 ether-type eq ip
filter acl ace ip 902 150 src-ip eq 100.20.103.65
filter acl ace ip 902 150 dst-ip eq 100.20.100.47
filter acl ace ip 902 150 ip-protocol-type eq tcp
filter acl ace protocol 902 150 dst-port eq 1521
filter acl ace 902 150 enable
filter acl ace 902 155 name "FULL_ERISIM"
filter acl ace action 902 155 permit
filter acl ace ethernet 902 155 ether-type eq ip
filter acl ace ip 901 155 dst-ip eq 100.20.100.149
filter acl ace 902 155 enable
filter acl ace 902 160 name "LOGLAMAK_ICIN"
filter acl ace action 902 160 permit redirect-next-hop 100.20.150.34
filter acl ace ethernet 902 160 ether-type eq ip
filter acl ace ip 902 160 src-ip ge 0.0.0.0
```

```
filter acl ace 902 170 name "DENY_ANY_ANY"
filter acl ace action 902 170 deny
filter acl ace ethernet 902 170 ether-type eq ip
filter acl ace ip 902 170 src-ip eq 0.0.0.0
filter acl ace ip 902 170 dst-ip eq 0.0.0.0
filter acl ace 902 170 enable
```

Layer 3 host configuration

The following section provides details about the filter configuration for the first core Layer 3 host.

```
#
# FILTER CONFIGURATION
#

filter acl 1 type outPort name "VRRP_Drop_ACL"
filter acl port 1 1/46
filter acl ace 1 1 name "Vrrp"
filter acl ace action 1 1 deny
filter acl ace ethernet 1 1 ether-type eq ip
filter acl ace ip 1 1 ip-protocol-type eq vrrp
filter acl ace 1 1 enable
filter acl 171 type inVlan name "TOPLANTI_VE_EGITIM_ACL"
filter acl vlan 171 171
filter acl 171 disable
filter acl ace 171 10 name "ICMP_PERMIT"
filter acl ace action 171 10 permit
filter acl ace ethernet 171 10 ether-type eq ip
filter acl ace ip 171 10 ip-protocol-type eq icmp
filter acl ace 171 10 enable
filter acl ace 171 20 name "IGMP_PERMIT"
filter acl ace action 171 20 permit
filter acl ace ethernet 171 20 ether-type eq ip
filter acl ace ip 171 20 ip-protocol-type eq 2
filter acl ace 171 20 enable
filter acl ace 171 30 name "VRRP_PERMIT"
filter acl ace action 171 30 permit
```

```
filter acl ace ethernet 171 30 ether-type eq ip
filter acl ace ip 171 30 ip-protocol-type eq vrrp
filter acl ace 171 30 enable
filter acl ace 171 40 name "DNS_PERMIT"
filter acl ace action 171 40 permit
filter acl ace ethernet 171 40 ether-type eq ip
filter acl ace ip 171 40 src-ip eq 100.20.171.0
filter acl ace ip 171 40 dst-ip eq 100.20.104.0
filter acl ace protocol 171 40 dst-port eq dns
filter acl ace 171 40 enable
filter acl ace 171 50 name "ESTABLISHED RST"
filter acl ace action 171 50 permit
filter acl ace ethernet 171 50 ether-type eq ip
filter acl ace ip 171 50 src-ip eq 100.6.172.0
filter acl ace ip 171 50 ip-protocol-type eq tcp
filter acl ace protocol 171 50 dst-port eq 1023
filter acl ace protocol 171 50 tcp-flags eq rst
filter acl ace 171 50 enable
filter acl ace 171 51 name "ESTABLISHED ACK"
filter acl ace action 171 51 permit
filter acl ace ethernet 171 51 ether-type eq ip
filter acl ace ip 171 51 src-ip eq 100.6.172.0
filter acl ace ip 171 51 ip-protocol-type eq tcp
filter acl ace protocol 171 51 dst-port eq 1023
filter acl ace protocol 171 51 tcp-flags eq ack
filter acl ace 171 51 enable
filter acl ace 171 60 name "DHCP_PERMIT"
filter acl ace action 171 60 permit
filter acl ace ethernet 171 60 ether-type eq ip
filter acl ace protocol 171 60 dst-port eq bootpServer
filter acl ace 171 60 enable
filter acl ace 171 80 name "DC_DNS_EXC_PERMIT"
filter acl ace action 171 80 permit
```

```
filter acl ace ethernet 171 80 ether-type eq ip
filter acl ace ip 171 80 src-ip eq 100.20.172.0
filter acl ace ip 181 70 dst-ip eq 100.20.104.0
filter acl ace 171 80 enable
filter acl ace 171 90 name "HTTP_PERMIT"
filter acl ace action 171 90 permit
filter acl ace ethernet 171 90 ether-type eq ip
filter acl ace ip 171 90 src-ip eq 100.20.172.0
filter acl ace protocol 171 90 dst-port eq 80
filter acl ace 171 90 enable
filter acl ace 171 100 name "HTTPS_PERMIT"
filter acl ace action 171 100 permit
filter acl ace ethernet 171 100 ether-type eq ip
filter acl ace ip 171 100 src-ip eq 100.20.172.0
filter acl ace protocol 171 100 dst-port eq 443
filter acl ace 171 100 enable
filter acl ace 171 110 name "PROXY_8080_PERMIT"
filter acl ace action 171 110 permit
filter acl ace ethernet 171 110 ether-type eq ip
filter acl ace ip 171 110 src-ip eq 100.20.172.0
filter acl ace ip 171 110 dst-ip eq 100.20.189.0
filter acl ace protocol 171 110 dst-port eq 8080
filter acl ace 171 110 enable
filter acl ace 171 120 name "CITRIX_Conn"
filter acl ace action 171 120 permit
filter acl ace ethernet 171 120 ether-type eq ip
filter acl ace protocol 171 120 dst-port eq 1494
filter acl ace protocol 171 120 dst-port eq 1604
filter acl ace 171 120 enable
filter acl ace 171 130 name "PWC_VPN_ERISIM"
filter acl ace action 171 130 permit
filter acl ace ethernet 171 130 ether-type eq ip
filter acl ace ip 171 130 src-ip eq 100.20.172.0
```

```
filter acl ace protocol 171 130 dst-port eq 11160
filter acl ace 171 130 enable
filter acl ace 171 150 name "Microsoft_FileSharing_PERMIT"
filter acl ace action 171 150 permit
filter acl ace protocol 171 150 dst-port eq 445
filter acl ace 171 150 enable

filter acl 172 type inVlan name "MISAFIR_ACL"
filter acl vlan 172 172
filter acl 172 disable
filter acl ace 172 5 name "Misafir_to_Misafir"
filter acl ace action 172 5 permit
filter acl ace ethernet 172 5 ether-type eq ip
filter acl ace ip 172 5 dst-ip eq 100.20.172.0
filter acl ace 172 5 enable
filter acl ace 172 10 name "ICMP_PERMIT"
filter acl ace action 172 10 permit
filter acl ace ethernet 172 10 ether-type eq ip
filter acl ace ip 172 10 ip-protocol-type eq icmp
filter acl ace 172 10 enable
filter acl ace 172 20 name "IGMP_PERMIT"
filter acl ace action 172 20 permit
filter acl ace ethernet 172 20 ether-type eq ip
filter acl ace ip 172 20 ip-protocol-type eq 2
filter acl ace 172 20 enable
filter acl ace 172 30 name "VRRP_PERMIT"
filter acl ace action 172 30 permit
filter acl ace ethernet 172 30 ether-type eq ip
filter acl ace ip 172 30 ip-protocol-type eq vrrp
filter acl ace 172 30 enable
filter acl ace 172 40 name "DNS_PERMIT"
filter acl ace action 172 40 permit
filter acl ace ethernet 172 40 ether-type eq ip
filter acl ace ip 172 40 src-ip eq 100.20.172.0
```

```
filter acl ace ip 172 40 dst-ip eq 100.20.104.0
filter acl ace protocol 172 40 dst-port eq dns
filter acl ace 172 40 enable
filter acl ace 172 50 name "ESTABLISHED RST"
filter acl ace action 172 50 permit
filter acl ace ethernet 172 50 ether-type eq ip
filter acl ace ip 172 50 src-ip eq 100.20.172.0
filter acl ace ip 172 50 ip-protocol-type eq tcp
filter acl ace protocol 172 50 dst-port eq 1023
filter acl ace protocol 172 50 tcp-flags eq rst
filter acl ace 172 50 enable
filter acl ace 172 51 name "ESTABLISHED ACK"
filter acl ace action 172 51 permit
filter acl ace ethernet 172 51 ether-type eq ip
filter acl ace ip 172 51 src-ip eq 100.20.172.0
filter acl ace ip 172 51 ip-protocol-type eq tcp
filter acl ace protocol 172 51 dst-port eq 1023
filter acl ace protocol 172 51 tcp-flags eq ack
filter acl ace 172 51 enable
filter acl ace 172 60 name "DHCP_PERMIT"
filter acl ace action 172 60 permit
filter acl ace protocol 172 60 dst-port eq bootpServer
filter acl ace 172 60 enable
filter acl ace 172 80 name "DC_DNS_EXC_PERMIT"
filter acl ace action 172 80 permit
filter acl ace ethernet 172 80 ether-type eq ip
filter acl ace ip 172 80 src-ip eq 100.20.172.0
filter acl ace ip 172 80 dst-ip eq 100.20.104.0
filter acl ace 172 80 enable
filter acl ace 172 90 name "HTTP_PERMIT"
filter acl ace action 172 90 permit
filter acl ace ethernet 172 90 ether-type eq ip
filter acl ace ip 172 90 src-ip eq 100.20.172.0
```

```
filter acl ace ip 172 90 ip-protocol-type eq tcp
filter acl ace protocol 172 90 dst-port eq 80
filter acl ace 172 90 enable
filter acl ace 172 100 name "HTTPS_PERMIT"
filter acl ace action 172 100 permit
filter acl ace ethernet 172 100 ether-type eq ip
filter acl ace ip 172 100 src-ip eq 100.20.172.0
filter acl ace ip 172 100 ip-protocol-type eq tcp
filter acl ace protocol 172 100 dst-port eq 443
filter acl ace 172 100 enable
filter acl ace 172 105 name "REMDESKTOP_PERMIT"
filter acl ace action 172 105 permit
filter acl ace ethernet 172 105 ether-type eq ip
filter acl ace ip 172 105 src-ip eq 100.20.172.0
filter acl ace ip 172 105 ip-protocol-type eq tcp
filter acl ace protocol 172 105 dst-port eq 3389
filter acl ace 172 105 enable
filter acl ace 172 106 name "NORKOM_PERMIT"
filter acl ace action 172 106 permit
filter acl ace ethernet 172 106 ether-type eq ip
filter acl ace ip 172 106 src-ip eq 100.20.172.0
filter acl ace ip 172 106 dst-ip eq 100.6.106.0
filter acl ace 172 106 enable
filter acl ace 172 107 name "SPECTRUM_PERMIT"
filter acl ace action 172 107 permit
filter acl ace ethernet 172 107 ether-type eq ip
filter acl ace ip 172 107 src-ip eq 100.20.172.0
filter acl ace ip 172 107 dst-ip eq 100.20.17.0
filter acl ace 172 107 enable
filter acl ace 172 110 name "PROXY_8080_PERMIT"
filter acl ace action 172 110 permit
filter acl ace ethernet 172 110 ether-type eq ip
filter acl ace ip 172 110 src-ip eq 100.20.172.0
```

```
filter acl ace ip 172 110 dst-ip eq 100.20.189.0
filter acl ace ip 172 110 ip-protocol-type eq tcp
filter acl ace protocol 172 110 dst-port eq 8080
filter acl ace 172 110 enable
filter acl ace 172 120 name "CITRIX_Conn-tcp"
filter acl ace action 172 120 permit
filter acl ace ethernet 172 120 ether-type eq ip
filter acl ace ip 172 120 ip-protocol-type eq tcp
filter acl ace protocol 172 120 dst-port eq 1494
filter acl ace 172 120 enable
filter acl ace 172 121 name "CITRIX_Conn-udp"
filter acl ace action 172 121 permit
filter acl ace ethernet 172 121 ether-type eq ip
filter acl ace ip 172 121 ip-protocol-type eq udp
filter acl ace protocol 172 121 dst-port eq 1604
filter acl ace 172 121 enable
filter acl ace 172 128 name "VOIP_VLAN_PERMIT"
filter acl ace action 172 128 permit
filter acl ace ethernet 172 128 ether-type eq ip
filter acl ace ip 172 128 dst-ip eq 10.201.0.0
filter acl ace 172 128 enable
filter acl ace 172 129 name "GANYMEDE-PERMIT"
filter acl ace action 172 129 permit
filter acl ace ethernet 172 130 ether-type eq ip
filter acl ace ip 172 129 src-ip eq 100.20.172.0
filter acl ace ip 172 129 dst-ip eq 100.6.100.225
filter acl ace 172 129 enable
filter acl ace 172 130 name "PWC_VPN_ERISIM"
filter acl ace action 172 130 permit
filter acl ace ethernet 172 51 ether-type eq ip
filter acl ace ip 172 130 src-ip eq 100.20.172.0
filter acl ace ip 172 130 ip-protocol-type eq tcp
filter acl ace protocol 172 130 tcp-dst-port eq 11160
```

```
filter acl ace 172 130 enable
filter acl ace 172 131 name "ISAKMP"
filter acl ace action 172 131 permit
filter acl ace ethernet 172 131 ether-type eq ip
filter acl ace ip 172 131 ip-protocol-type eq udp
filter acl ace protocol 172 131 dst-port eq 500
filter acl ace 172 131 enable
filter acl ace 172 132 name "ESP"
filter acl ace action 172 132 permit
filter acl ace ethernet 172 132 ether-type eq ip
filter acl ace ip 172 132 ip-protocol-type eq 50
filter acl ace 172 132 enable
filter acl ace 172 133 name "LOGLAMAK_ICIN"
filter acl ace action 172 133 permit redirect-next-hop 100.20.150.34
filter acl ace ip 172 133 src-ip eq 0.0.0.0
filter acl ace 172 140 name "DENY_ANY_ANY"
filter acl ace action 172 140 deny
filter acl ace ethernet 172 140 ether-type eq ip
filter acl ace ip 172 140 src-ip eq 0.0.0.0
filter acl ace ip 172 140 dst-ip eq 0.0.0.0
filter acl ace 172 140 enable
filter acl 802 type inVlan name "NICE-CLS_ACL-in"
filter acl vlan 802 802
filter acl 802 disable
filter acl ace 802 1 name "NICE_to_NICE"
filter acl ace action 802 1 permit
filter acl ace ethernet 802 1 ether-type eq ip
filter acl ace ip 802 1 dst-ip eq 100.20.174.32
filter acl ace 802 1 enable
filter acl ace 802 10 name "ICMP_PERMIT"
filter acl ace action 802 10 permit
filter acl ace ethernet 802 10 ether-type eq ip
filter acl ace ip 802 10 ip-protocol-type eq icmp
```

```
filter acl ace 802 10 enable
filter acl ace 802 20 name "IGMP_PERMIT"
filter acl ace action 802 20 permit
filter acl ace ethernet 802 20ether-type eq ip
filter acl ace ip 802 20 ip-protocol-type eq 2
filter acl ace 802 20 enable
filter acl ace 802 30 name "VRRP_PERMIT"
filter acl ace action 802 30 permit
filter acl ace ethernet 802 30 ether-type eq ip
filter acl ace ip 802 30 ip-protocol-type eq vrrp
filter acl ace 802 30 enable
filter acl ace 802 40 name "DNS_PERMIT"
filter acl ace action 802 40 permit
filter acl ace ethernet 802 40 ether-type eq ip
filter acl ace ip 802 40 src-ip eq 100.20.174.32
filter acl ace ip 802 40 dst-ip eq 100.20.104.0
filter acl ace protocol 802 40 dst-port eq dns
filter acl ace 802 40 enable
filter acl ace 802 45 name "DC-EXCH-DNS"
filter acl ace action 802 45 permit
filter acl ace ethernet 802 45 ether-type eq ip
filter acl ace ip 802 45 dst-ip eq 100.20.104.0
filter acl ace 802 45 enable
filter acl ace 802 50 name "ESTABLISHED RST"
filter acl ace action 802 50 permit
filter acl ace ethernet 802 50 ether-type eq ip
filter acl ace ip 802 50 src-ip eq 100.20.174.32
filter acl ace ip 802 50 ip-protocol-type eq tcp
filter acl ace protocol 802 50 dst-port eq 1023
filter acl ace protocol 802 50 tcp-flags eq rst
filter acl ace 802 50 enable
filter acl ace 802 51 name "ESTABLISHED ACK"
filter acl ace action 802 51 permit
```

```
filter acl ace ethernet 802 51 ether-type eq ip
filter acl ace ip 802 51 src-ip eq 100.20.174.32
filter acl ace ip 802 51 ip-protocol-type eq tcp
filter acl ace protocol 802 51 dst-port eq 1023
filter acl ace protocol 802 51 tcp-flags eq ack
filter acl ace 802 51 enable
filter acl ace 802 52 name "UDP_Permit"
filter acl ace action 802 52 permit
filter acl ace ethernet 802 52 ether-type eq ip
filter acl ace ip 802 52 ip-protocol-type eq udp
filter acl ace 802 52 enable
filter acl ace 802 60 name "NICE_Logging"
filter acl ace action 802 60 permit
filter acl ace ethernet 802 60 ether-type eq ip
filter acl ace ip 802 60 src-ip eq 100.20.174.32
filter acl ace ip 802 60 ip-protocol-type eq tcp
filter acl ace protocol 802 60 dst-port eq 2011
filter acl ace 802 60 enable
filter acl ace 802 65 name "RTS_Conn"
filter acl ace action 802 65 permit
filter acl ace ethernet 802 65 ether-type eq ip
filter acl ace ip 802 65 dst-ip eq 100.20.152.20
filter acl ace 802 65 enable
filter acl ace 802 70 name "CTI_Conn"
filter acl ace action 802 70 permit
filter acl ace ethernet 802 70 ether-type eq ip
filter acl ace ip 802 70 src-ip eq 100.20.174.32
filter acl ace ip 802 70 ip-protocol-type eq tcp
filter acl ace protocol 802 70 dst-port eq 3750
filter acl ace 802 70 enable
filter acl ace 802 90 name "LOGLAMA"
filter acl ace action 802 90 permit redirect-next-hop 100.20.150.217
filter acl ace ethernet 802 90 ether-type eq ip
```

```
filter acl ace ip 802 90 src-ip eq 0.0.0.0
filter acl ace 802 100 name "DENY_ANY"
filter acl ace action 802 100 deny
filter acl ace ip 802 100 src-ip eq 0.0.0.0
filter acl ace ip 802 100 dst-ip eq 0.0.0.0
filter acl ace 802 100 enable

filter acl 804 type inVlan name "BASIM_LIMITED-in"
filter acl vlan 804 804
filter acl ace 804 5 name "Basim_to_Basim"
filter acl ace action 804 5 permit
filter acl ace ethernet 804 5 ether-type eq ip
filter acl ace ip 804 5 dst-ip eq 100.20.174.96
filter acl ace 804 5 enable
filter acl ace 804 10 name "ICMP_PERMIT"
filter acl ace action 804 10 permit
filter acl ace ethernet 804 10 ether-type eq ip
filter acl ace ip 804 10 ip-protocol-type eq icmp
filter acl ace 804 10 enable
filter acl ace 804 20 name "IGMP_PERMIT"
filter acl ace action 804 20 permit
filter acl ace ethernet 804 20 ether-type eq ip
filter acl ace ip 804 20 ip-protocol-type eq 2
filter acl ace 804 20 enable
filter acl ace 804 30 name "VRRP_PERMIT"
filter acl ace action 804 30 permit
filter acl ace ethernet 804 30 ether-type eq ip
filter acl ace ip 804 30 ip-protocol-type eq vrrp
filter acl ace 804 30 enable
filter acl ace 804 40 name "DNS_PERMIT"
filter acl ace action 804 40 permit
filter acl ace protocol 804 40 dst-port eq dns
filter acl ace 804 40 enable
filter acl ace 804 45 name "DC-EXCH-DNS"
```

```
filter acl ace action 804 45 permit
filter acl ace ethernet 804 45 ether-type eq ip
filter acl ace ip 804 45 dst-ip eq 100.20.104.0
filter acl ace 804 45 enable
filter acl ace 804 50 name "ESTABLISHED RST"
filter acl ace action 804 50 permit
filter acl ace ethernet 804 50 ether-type eq ip
filter acl ace ip 804 50 src-ip eq 100.20.174.97
filter acl ace ip 804 50 ip-protocol-type eq tcp
filter acl ace protocol 804 50 dst-port eq 1023
filter acl ace protocol 804 50 tcp-flags eq rst
filter acl ace 804 50 enable
filter acl ace 804 51 name "ESTABLISHED ACK"
filter acl ace action 804 51 permit
filter acl ace ethernet 804 51 ether-type eq ip
filter acl ace ip 804 51 src-ip eq 100.20.174.97
filter acl ace ip 804 51 ip-protocol-type eq tcp
filter acl ace protocol 804 51 dst-port eq 1023
filter acl ace protocol 804 51 tcp-flags eq ack
filter acl ace 804 51 enable
filter acl ace 804 60 name "E-BANK_ERISIM"
filter acl ace action 804 60 permit
filter acl ace ethernet 804 60 ether-type eq ip
filter acl ace ip 804 60 dst-ip eq 100.20.115.11
filter acl ace ip 804 60 ip-protocol-type eq tcp
filter acl ace protocol 804 60 dst-port eq 80
filter acl ace 804 60 enable
filter acl ace 804 70 name "E-BANK_ERISIM_HTTPS"
filter acl ace action 804 70 permit
filter acl ace ethernet 804 70 ether-type eq ip
filter acl ace ip 802 70 dst-ip eq 100.20.115.11
filter acl ace ip 804 70 ip-protocol-type eq tcp
filter acl ace protocol 804 70 dst-port eq 443
```

```
filter acl ace 804 70 enable
filter acl ace 804 80 name "FRED_Erisim"
filter acl ace action 804 80 permit
filter acl ace ethernet 804 80 ether-type eq ip
filter acl ace ip 804 80 dst-ip eq 100.20.100.145
filter acl ace 804 80 enable
filter acl ace 804 81 name "BARNEY_Erisim"
filter acl ace action 804 81 permit
filter acl ace ethernet 804 81 ether-type eq ip
filter acl ace ip 804 81 dst-ip eq 100.20.100.151
filter acl ace 804 81 enable
filter acl ace 804 90 name "BUFFY_ERISIM"
filter acl ace action 804 90 permit
filter acl ace ethernet 804 90 ether-type eq ip
filter acl ace ip 804 90 dst-ip eq 100.20.100.77
filter acl ace ip 804 90 ip-protocol-type eq tcp
filter acl ace protocol 804 90 dst-port eq 1433
filter acl ace 804 90 enable
filter acl ace 804 100 name "ROMTest_ERISIM"
filter acl ace action 804 100 permit
filter acl ace ethernet 804 100 ether-type eq ip
filter acl ace ip 804 100 dst-ip eq 100.20.24.77
filter acl ace ip 804 100 ip-protocol-type eq tcp
filter acl ace protocol 804 100 dst-port eq 1433
filter acl ace 804 100 enable
filter acl ace 804 101 name "Mrksql-t0_ERISIM"
filter acl ace action 804 101 permit
filter acl ace ethernet 804 101 ether-type eq ip
filter acl ace ip 804 101 dst-ip eq 100.20.20.77
filter acl ace ip 804 101 ip-protocol-type eq tcp
filter acl ace protocol 804 101 dst-port eq 1433
filter acl ace 804 101 enable
filter acl ace 804 110 name "ROSETTA_ERISIM"
```

```
filter acl ace action 804 110 permit
filter acl ace ethernet 804 110 ether-type eq ip
filter acl ace ip 804 110 dst-ip eq 172.17.1.100
filter acl ace 804 110 enable
filter acl ace 804 120 name "PLAST_ERISIM"
filter acl ace action 804 120 permit
filter acl ace ethernet 804 120 ether-type eq ip
filter acl ace ip 804 120 dst-ip eq 212.57.7.20
filter acl ace 804 120 enable
filter acl ace 804 130 name "AV-Yama_YONETIM_2967"
filter acl ace action 804 130 permit
filter acl ace ethernet 804 130 ether-type eq ip
filter acl ace ip 804 130 ip-protocol-type eq tcp
filter acl ace protocol 804 130 dst-port eq 2967
filter acl ace 804 130 enable
filter acl ace 804 140 name "AV-Yama_YONETIM_9968"
filter acl ace action 804 140 permit
filter acl ace ethernet 804 140 ether-type eq ip
filter acl ace ip 804 140 ip-protocol-type eq tcp
filter acl ace protocol 804 140 dst-port eq 9968
filter acl ace 804 140 enable
filter acl ace 804 150 name "AV-Yama_YONETIM_UDP_2967"
filter acl ace action 804 150 permit
filter acl ace ethernet 804 150 ether-type eq ip
filter acl ace ip 804 150 ip-protocol-type eq udp
filter acl ace protocol 804 150 dst-port eq 2967
filter acl ace 804 150 enable
filter acl ace 804 160 name "AV-Yama_YONETIM_UDP_9968"
filter acl ace action 804 160 permit
filter acl ace ip 804 160 ip-protocol-type eq udp
filter acl ace protocol 804 160 dst-port eq 9968
filter acl ace 804 160 enable
filter acl ace 804 170 name "AV-Yama_YONETIM_UDP_Source"
```

```
filter acl ace action 804 170 permit
filter acl ace ethernet 804 170 ether-type eq ip
filter acl ace ip 804 170 ip-protocol-type eq udp
filter acl ace protocol 804 170 src-port eq 9968
filter acl ace 804 170 enable
filter acl ace 804 210 name "PROXY_ERISIM_EK"
filter acl ace action 804 210 permit
filter acl ace ethernet 804 210 ether-type eq ip
filter acl ace ip 804 210 dst-ip eq 100.20.189.0
filter acl ace ip 804 210 ip-protocol-type eq tcp
filter acl ace protocol 804 210 dst-port eq 8080
filter acl ace 804 210 enable
filter acl ace 804 220 name "LOGLAMA"
filter acl ace action 804 220 permit redirect-next-hop 100.20.150.217
filter acl ace ethernet 804 220 ether-type eq ip
filter acl ace ip 804 220 src-ip eq 0.0.0.0
filter acl ace 804 230 name "DENY_ANY"
filter acl ace action 804 230 deny
filter acl ace ip 804 230 src-ip eq 0.0.0.0
filter acl ace ip 804 230 dst-ip eq 0.0.0.0
filter acl ace 804 230 enable

filter acl 805 type inVlan name "SBS-Remote"
filter acl vlan 805 805
filter acl ace 805 5 name "SBS-to-SBS"
filter acl ace action 805 5 permit
filter acl ace ethernet 805 5 ether-type eq ip
filter acl ace ip 805 5 dst-ip eq 100.20.174.128
filter acl ace 805 5 enable
filter acl ace 805 10 name "ICMP_PERMIT"
filter acl ace action 805 10 permit
filter acl ace ethernet 805 10 ether-type eq ip
filter acl ace ip 805 10 ip-protocol-type eq icmp
filter acl ace 805 10 enable
```

```
filter acl ace 805 20 name "IGMP_PERMIT"
filter acl ace action 805 20 permit
filter acl ace ethernet 805 20 ether-type eq ip
filter acl ace ip 805 20 ip-protocol-type eq 2
filter acl ace 805 20 enable
filter acl ace 805 30 name "VRRP_PERMIT"
filter acl ace action 805 30 permit
filter acl ace ethernet 805 30 ether-type eq ip
filter acl ace ip 805 30 ip-protocol-type eq vrrp
filter acl ace 805 30 enable
filter acl ace 805 40 name "DNS_PERMIT"
filter acl ace action 805 40 permit
filter acl ace protocol 805 40 dst-port eq 53
filter acl ace 805 40 enable
filter acl ace 805 50 name "ESTABLISHED RST"
filter acl ace action 805 50 permit
filter acl ace ethernet 805 50 ether-type eq ip
filter acl ace ip 805 50 src-ip eq 100.20.174.128
filter acl ace ip 805 50 ip-protocol-type eq tcp
filter acl ace protocol 805 50 dst-port eq 1023
filter acl ace protocol 805 50 tcp-flags eq rst
filter acl ace 805 50 enable
filter acl ace 805 51 name "ESTABLISHED ACK"
filter acl ace action 805 51 permit
filter acl ace ethernet 805 51 ether-type eq ip
filter acl ace ip 805 51 src-ip eq 100.20.174.128
filter acl ace ip 805 51 ip-protocol-type eq tcp
filter acl ace protocol 805 51 dst-port eq 1023
filter acl ace protocol 805 51 tcp-flags eq ack
filter acl ace 805 51 enable
filter acl ace 805 80 name "DC_DNS_EXCH_PERMIT"
filter acl ace action 805 80 permit
filter acl ace ethernet 805 80 ether-type eq ip
```

```
filter acl ace ip 805 80 dst-ip eq 100.20.104.0
filter acl ace 805 80 enable
filter acl ace 805 90 name "HTTP_PERMIT"
filter acl ace action 805 90 permit
filter acl ace ethernet 805 90 ether-type eq ip
filter acl ace ip 805 90 ip-protocol-type eq tcp
filter acl ace protocol 805 90 dst-port eq 80
filter acl ace 805 90 enable
filter acl ace 805 100 name "HTTPS_PERMIT"
filter acl ace action 805 100 permit
filter acl ace ethernet 805 100 ether-type eq ip
filter acl ace ip 805 100 ip-protocol-type eq tcp
filter acl ace protocol 805 100 dst-port eq 443
filter acl ace 805 100 enable
filter acl ace 805 105 name "REMDESKTOP_PERMIT"
filter acl ace action 805 105 permit
filter acl ace ethernet 805 105 ether-type eq ip
filter acl ace ip 805 105 ip-protocol-type eq tcp
filter acl ace protocol 805 105 dst-port eq 3389
filter acl ace 805 105 enable
filter acl ace 805 110 name "PROXY_8080_PERMIT"
filter acl ace action 805 110 permit
filter acl ace ethernet 805 110 ether-type eq ip
filter acl ace ip 805 110 dst-ip eq 100.20.189.0
filter acl ace ip 805 110 ip-protocol-type eq tcp
filter acl ace protocol 805 110 dst-port eq 8080
filter acl ace 805 110 enable
filter acl ace 805 120 name "DAMEWARE_PERMIT"
filter acl ace action 805 120 permit
filter acl ace ethernet 805 120 ether-type eq ip
filter acl ace ip 805 120 src-ip eq 100.20.174.128
filter acl ace protocol 805 120 dst-port eq 445,6129
filter acl ace 805 120 enable
```

```
filter acl ace 805 140 name "DENY_ANY_ANY"
filter acl ace action 805 140 deny
filter acl ace ethernet 805 140 ether-type eq ip
filter acl ace ip 805 140 src-ip eq 0.0.0.0
filter acl ace ip 805 140 dst-ip eq 0.0.0.0
filter acl ace 805 140 enable

filter acl 1000 type inPort name "CS1K-RemDesk"
filter acl port 1000 1/33
filter acl ace 1000 10 name "ICMP"
filter acl ace action 1000 10 permit
filter acl ace ethernet 1000 10 ether-type eq ip
filter acl ace ip 1000 10 ip-protocol-type eq icmp
filter acl ace 1000 10 enable
filter acl ace 1000 15 name "ESTABLISHED_PERMIT RST"
filter acl ace action 1000 15 permit
filter acl ace ethernet 1000 15 ether-type eq ip
filter acl ace protocol 1000 15 dst-port eq 1023
filter acl ace protocol 1000 15 tcp-flags eq rst,ack
filter acl ace 1000 15 enable
filter acl ace 1000 16 name "ESTABLISHED_PERMIT ACK"
filter acl ace action 1000 16 permit
filter acl ace ethernet 1000 16 ether-type eq ip
filter acl ace protocol 1000 16 dst-port eq 1023
filter acl ace protocol 1000 16 tcp-flags eq ack
filter acl ace 1000 16 enable
filter acl ace 1000 20 name "LOGLAMAK_ICIN"
filter acl ace action 1000 20 permit redirect-next-hop 10.201.12.8
filter acl ace ethernet 1000 20 ether-type eq ip
filter acl ace ip 1000 20 src-ip eq 0.0.0.0
filter acl ace 1000 30 name "DENY-ANY_ANY"
filter acl ace action 1000 30 deny
filter acl ace ethernet 1000 30 ether-type eq ip
filter acl ace ip 1000 30 src-ip eq 0.0.0.0
```

```
filter acl ace 1000 30 enable

filter acl vlan 1802 802
filter acl 1802 disable
filter acl ace 1802 10 name "ICMP_PERMIT"
filter acl ace action 1802 10 permit
filter acl ace ethernet 1802 10 ether-type eq ip
filter acl ace ip 1802 10 ip-protocol-type eq icmp
filter acl ace 1802 10 enable
filter acl ace 1802 20 name "IGMP_PERMIT"
filter acl ace action 1802 20 permit
filter acl ace ethernet 1802 20 ether-type eq ip
filter acl ace ip 1802 20 ip-protocol-type eq 2
filter acl ace 1802 20 enable
filter acl ace 1802 30 name "VRRP_PERMIT"
filter acl ace action 1802 30 permit
filter acl ace ethernet 1802 30 ether-type eq ip
filter acl ace ip 1802 30 ip-protocol-type eq vrrp
filter acl ace 1802 30 enable
filter acl ace 1802 51 name "UDP_Permit"
filter acl ace action 1802 51 permit
filter acl ace ethernet 1802 51 ether-type eq ip
filter acl ace ip 1802 51 ip-protocol-type eq udp
filter acl ace 1802 51 enable
filter acl ace 1802 60 name "NICE_Logging"
filter acl ace action 1802 60 permit
filter acl ace ethernet 1802 60 ether-type eq ip
filter acl ace ip 1802 60 src-ip eq 100.20.174.32
filter acl ace protocol 1802 60 dst-port eq 2011
filter acl ace 1802 60 enable
filter acl ace 1802 65 name "RTS_Conn"
filter acl ace action 1802 65 permit
filter acl ace 1802 100 name "DENY_ANY"
filter acl ace action 1802 100 deny
```

```
filter acl ace ethernet 1802 100 ether-type eq ip
filter acl ace ip 1802 100 src-ip eq 0.0.0.0
filter acl ace ip 1802 100 dst-ip eq 0.0.0.0
filter acl ace 1802 100 enable

filter acl vlan 1804 804
filter acl ace 1804 5 name "BASIM_to_BASIM"
filter acl ace action 1804 5 permit
filter acl ace ethernet 1804 5 ether-type eq ip
filter acl ace ip 1804 5 src-ip eq 100.20.174.96
filter acl ace 1804 5 enable
filter acl ace 1804 10 name "ICMP_PERMIT"
filter acl ace action 1804 10 permit
filter acl ace ethernet 1804 10 ether-type eq ip
filter acl ace ip 1804 10 ip-protocol-type eq icmp
filter acl ace 1804 10 enable
filter acl ace 1804 20 name "IGMP_PERMIT"
filter acl ace action 1804 20 permit
filter acl ace ethernet 1804 20 ether-type eq ip
filter acl ace ip 1804 20 ip-protocol-type eq 2
filter acl ace 1804 20 enable
filter acl ace 1804 30 name "VRRP_PERMIT"
filter acl ace action 1804 30 permit
filter acl ace ethernet 1804 30 ether-type eq ip
filter acl ace ip 1804 30 ip-protocol-type eq vrrp
filter acl ace 1804 30 enable
filter acl ace 1804 40 name "DNS_PERMIT"
filter acl ace action 1804 40 permit
filter acl ace protocol 1804 40 src-port eq 53
filter acl ace 1804 40 enable
filter acl ace 1804 45 name "DC-EXCH-DNS"
filter acl ace action 1804 45 permit
filter acl ace ethernet 1804 45 ether-type eq ip
filter acl ace ip 1804 45 src-ip eq 100.20.104.0
```

```
filter acl ace 1804 45 enable
filter acl ace 1804 50 name "ESTABLISHED RST"
filter acl ace action 1804 50 permit
filter acl ace ethernet 1804 50 ether-type eq ip
filter acl ace ip 1804 50 dst-ip eq 100.20.174.97
filter acl ace ip 1804 50 ip-protocol-type eq tcp
filter acl ace protocol 1804 50 tcp-dst-port eq 1023
filter acl ace protocol 1804 50 tcp-flags eq rst
filter acl ace 1804 50 enable
filter acl ace 1804 51 name "ESTABLISHED ACK"
filter acl ace action 1804 51 permit
filter acl ace ethernet 1804 51 ether-type eq ip
filter acl ace ip 1804 51 dst-ip eq 100.20.174.97
filter acl ace ip 1804 51 ip-protocol-type eq tcp
filter acl ace protocol 1804 51 tcp-dst-port eq 1023
filter acl ace protocol 1804 51 tcp-flags eq ack
filter acl ace 1804 51 enable
filter acl ace 1804 80 name "PWC_ERISIM"
filter acl ace action 1804 80 permit
filter acl ace ethernet 1804 80 ether-type eq ip
filter acl ace ip 1804 80 src-ip eq 100.20.100.145
filter acl ace 1804 80 enable
filter acl ace 1804 110 name "ROSETTA_ERISIM"
filter acl ace action 1804 110 permit
filter acl ace ethernet 1804 110 ether-type eq ip
filter acl ace ip 1804 110 src-ip eq 172.17.1.100
filter acl ace 1804 110 enable
filter acl ace 1804 120 name "PLAST_ERISIM"
filter acl ace action 1804 120 permit
filter acl ace ethernet 1804 120 ether-type eq ip
filter acl ace ip 1804 120 src-ip eq 212.57.7.20
filter acl ace 1804 120 enable
filter acl ace 1804 130 name "AV-Yama_YONETIM_9968"
```

```
filter acl ace action 1804 130 permit
filter acl ace ethernet 1804 130 ether-type eq ip
filter acl ace ip 1804 130 ip-protocol-type eq tcp
filter acl ace protocol 1804 130 dst-port eq 9968
filter acl ace 1804 130 enable
filter acl ace 1804 140 name "AV-Yama_YONETIM_2967"
filter acl ace action 1804 140 permit
filter acl ace ethernet 1804 140 ether-type eq ip
filter acl ace ip 1804 140 ip-protocol-type eq tcp
filter acl ace protocol 1804 140 dst-port eq 2967
filter acl ace 1804 140 enable
filter acl ace 1804 150 name "AV-Yama_YONETIM_UDP_9968"
filter acl ace action 1804 150 permit
filter acl ace ethernet 1804 150 ether-type eq ip
filter acl ace ip 1840 150 ip-protocol-type eq udp
filter acl ace protocol 1804 150 dst-port eq 9968
filter acl ace 1804 150 enable
filter acl ace 1804 160 name "AV-Yama_YONETIM_UDP_2967"
filter acl ace action 1804 160 permit
filter acl ace ethernet 1804 160 ether-type eq ip
filter acl acl ip 1804 160 ip-protocol-type eq udp
filter acl ace protocol 1804 160 dst-port eq 2967
filter acl ace 1804 160 enable
filter acl ace 1804 180 name "SUNUCU_YONETIM"
filter acl ace action 1804 180 permit
filter acl ace ethernet 1804 180 ether-type eq ip
filter acl ace ip 1804 180 src-ip eq 100.20.150.80
filter acl ace ip 1804 180 ip-protocol-type eq tcp
filter acl ace protocol 1804 180 dst-port eq 3389
filter acl ace 1804 180 enable
filter acl ace 1804 200 name "OTOMIZE_DEBIT_CARD_OPS"
filter acl ace action 1804 200 permit
filter acl ace ethernet 1804 200 ether-type eq ip
```

```
filter acl ace ip 1804 200 src-ip eq 100.20.114.0
filter acl ace ip 1804 200 ip-protocol-type eq tcp
filter acl ace protocol 1804 200 dst-port eq 445
filter acl ace 1804 200 enable
filter acl ace 1804 210 name "OTOMIZE_DEBIT_CARD_OPS"
filter acl ace action 1804 210 permit
filter acl ace ethernet 1804 210 ether-type eq ip
filter acl ace ip 1804 210 src-ip eq 100.20.24.0
filter acl ace ip 1804 210 ip-protocol-type eq tcp
filter acl ace protocol 1804 210 dst-port eq 445
filter acl ace 1804 210 enable
filter acl ace 1804 220 name "LOGLAMA"
filter acl ace action 1804 220 permit
filter acl ace ethernet 1804 220 ether-type eq ip
filter acl ace ip 1804 220 src-ip eq 0.0.0.0
filter acl ace 1804 220 enable
filter acl ace 1804 230 name "DENY_ANY"
filter acl ace action 1804 230 deny
filter acl ace ethernet 1804 230 ether-type eq ip
filter acl ace ip 1804 230 src-ip eq 0.0.0.0
filter acl ace ip 1804 230 dst-ip eq 0.0.0.0
filter acl ace 1804 230 enable
```

The following section provides details about the filter configuration for the second core Layer 3 host

```
#
# FILTER CONFIGURATION
#
filter acl port 1 1/46
filter acl ace 1 1 name "Vrrp"
filter acl ace action 1 1 deny
filter acl ace ethernet 1 1 ether-type eq ip
filter acl ace ip 1 1 ip-protocol-type eq vrrp
filter acl ace 1 1 enable

filter acl 171 type inVlan name "TOPLANTI_VE_EGITIM_ACL"
```

```
filter acl vlan 171 171
filter acl 171 disable
filter acl ace 171 10 name "ICMP_PERMIT"
filter acl ace action 171 10 permit
filter acl ace ethernet 171 10 ether-type eq ip
filter acl ace ip 171 10 ip-protocol-type eq icmp
filter acl ace 171 10 enable
filter acl ace 171 20 name "IGMP_PERMIT"
filter acl ace action 171 20 permit
filter acl ace ethernet 171 20 ether-type eq ip
filter acl ace ip 171 20 ip-protocol-type eq 2
filter acl ace 171 20 enable
filter acl ace 171 30 name "VRRP_PERMIT"
filter acl ace action 171 30 permit
filter acl ace ethernet 171 30 ether-type eq ip
filter acl ace ip 171 30 ip-protocol-type eq vrrp
filter acl ace 171 30 enable
filter acl ace 171 40 name "DNS_PERMIT"
filter acl ace action 171 40 permit
filter acl ace ethernet 171 40 ether-type eq ip
filter acl ace ip 171 40 src-ip eq 100.20.171.0
filter acl ace ip 171 40 dst-ip eq 100.20.104.0
filter acl ace protocol 171 40 dst-port eq dns
filter acl ace 171 40 enable
filter acl ace 171 50 name "ESTABLISHED RST"
filter acl ace action 171 50 permit
filter acl ace ethernet 171 50 ether-type eq ip
filter acl ace ip 171 50 src-ip eq 100.6.172.0
filter acl ace ip 171 50 ip-protocol-type eq tcp
filter acl ace protocol 171 50 dst-port eq 1023
filter acl ace protocol 171 50 flags eq rst
filter acl ace 171 50 enable
filter acl ace 171 51 name "ESTABLISHED ACK"
```

```
filter acl ace action 171 51 permit
filter acl ace ethernet 171 51 ether-type eq ip
filter acl ace ip 171 51 src-ip eq 100.6.172.0
filter acl ace ip 171 51 ip-protocol-type eq tcp
filter acl ace protocol 171 51 dst-port eq 1023
filter acl ace protocol 171 51 flags eq ack
filter acl ace 171 51 enable
filter acl ace 171 60 name "DHCP_PERMIT"
filter acl ace action 171 60 permit
filter acl ace protocol 171 60 dst-port eq bootpServer
filter acl ace 171 60 enable
filter acl ace 171 80 name "DC_DNS_EXC_PERMIT"
filter acl ace action 171 80 permit
filter acl ace ethernet 171 80 ether-type eq ip
filter acl ace ip 171 80 src-ip eq 100.20.172.0
filter acl ace ip 171 80 dst-ip eq 100.20.104.0
filter acl ace 171 80 enable
filter acl ace 171 90 name "HTTP_PERMIT"
filter acl ace action 171 90 permit
filter acl ace ethernet 171 90 ether-type eq ip
filter acl ace ip 171 90 src-ip eq 100.20.172.0
filter acl ace protocol 171 90 dst-port eq 80
filter acl ace 171 90 enable
filter acl ace 171 100 name "HTTPS_PERMIT"
filter acl ace action 171 100 permit
filter acl ace ethernet 171 100 ether-type eq ip
filter acl ace ip 171 100 src-ip eq 100.20.172.0
filter acl ace protocol 171 100 dst-port eq 443
filter acl ace 171 100 enable
filter acl ace 171 110 name "PROXY_8080_PERMIT"
filter acl ace action 171 110 permit
filter acl ace ethernet 171 110 ether-type eq ip
filter acl ace ip 171 110 src-ip eq 100.20.172.0
```

```
filter acl ace ip 171 110 dst-ip eq 100.20.189.0
filter acl ace protocol 171 110 dst-port eq 8080
filter acl ace 171 110 enable
filter acl ace 171 120 name "CITRIX_Conn"
filter acl ace action 171 120 permit
filter acl ace ethernet 171 120 ether-type eq ip
filter acl ace protocol 171 120 dst-port eq 1494
filter acl ace protocol 171 120 dst-port eq 1604
filter acl ace 171 120 enable
filter acl ace 171 130 name "PWC_VPN_ERISIM"
filter acl ace action 171 130 permit
filter acl ace ethernet 171 130 ether-type eq ip
filter acl ace ip 171 130 src-ip eq 100.20.172.0
filter acl ace protocol 171 130 dst-port eq 11160
filter acl ace 171 130 enable
filter acl ace 171 140 name "Microsoft_FileSharing_PERMIT"
filter acl ace action 171 140 permit
filter acl ace protocol 171 140 dst-port eq 135-139
filter acl ace 171 140 enable
filter acl ace 171 150 create name "Microsoft_FileSharing_PERMIT"
filter acl ace action 171 150 permit
filter acl ace protocol 171 150 dst-port eq 445
filter acl ace 171 150 enable

filter acl 172 type inVlan name "MISAFIR_ACL"
filter acl vlan 172 172
filter acl 172 disable
filter acl ace 172 5 name "Misafir_to_Misafir"
filter acl ace action 172 5 permit
filter acl ace ethernet 172 5 ether-type eq ip
filter acl ace ip 172 5 dst-ip eq 100.20.172.0
filter acl ace 172 5 enable
filter acl ace 172 10 name "ICMP_PERMIT"
filter acl ace action 172 10 permit
```

```
filter acl ace ethernet 172 10 ether-type eq ip
filter acl ace ip 172 10 ip-protocol-type eq icmp
filter acl ace 172 10 enable
filter acl ace 172 20 name "IGMP_PERMIT"
filter acl ace action 172 20 permit
filter acl ace ethernet 172 20 ether-type eq ip
filter acl ace ip 172 20 ip-protocol-type eq 2
filter acl ace 172 20 enable
filter acl ace 172 30 name "VRRP_PERMIT"
filter acl ace action 172 30 permit
filter acl ace ethernet 172 30 ether-type eq ip
filter acl ace ip 172 30 ip-protocol-type eq vrrp
filter acl ace 172 30 enable
filter acl ace 172 40 name "DNS_PERMIT"
filter acl ace action 172 40 permit
filter acl ace ethernet 172 40 ether-type eq ip
filter acl ace ip 172 40 src-ip eq 100.20.172.0
filter acl ace ip 172 40 dst-ip eq 100.20.104.0
filter acl ace protocol 172 40 dst-port eq dns
filter acl ace 172 40 enable
filter acl ace 172 50 name "ESTABLISHED RST"
filter acl ace action 172 50 permit
filter acl ace ethernet 172 50 ether-type eq ip
filter acl ace ip 172 50 src-ip eq 100.20.172.0
filter acl ace ip 172 50 ip-protocol-type eq tcp
filter acl ace protocol 172 50 dst-port eq 1023
filter acl ace protocol 172 50 tcp-flags eq ack
filter acl ace 172 50 enable
filter acl ace 172 51 name "ESTABLISHED ACK"
filter acl ace action 172 51 permit
filter acl ace ethernet 172 51 ether-type eq ip
filter acl ace ip 172 51 src-ip eq 100.20.172.0
filter acl ace ip 172 51 ip-protocol-type eq tcp
```

```
filter acl ace protocol 172 51 dst-port eq 1023
filter acl ace protocol 172 51 tcp-flags eq ack
filter acl ace 172 51 enable
filter acl ace 172 60 name "DHCP_PERMIT"
filter acl ace action 172 60 permit
filter acl ace protocol 172 60 dst-port eq bootpServer
filter acl ace 172 60 enable
filter acl ace 172 80 name "DC_DNS_EXC_PERMIT"
filter acl ace action 172 80 permit
filter acl ace ethernet 172 80 ether-type eq ip
filter acl ace ip 172 80 src-ip eq 100.20.172.0
filter acl ace ip 172 80 dst-ip eq 100.20.104.0
filter acl ace 172 80 enable
filter acl ace 172 90 name "HTTP_PERMIT"
filter acl ace action 172 90 permit
filter acl ace ethernet 172 90 ether-type eq ip
filter acl ace ip 172 90 src-ip eq 100.20.172.0
filter acl ace ip 172 90 ip-protocol-type eq tcp
filter acl ace protocol 172 90 dst-port eq 80
filter acl ace 172 100 name "HTTPS_PERMIT"
filter acl ace action 172 100 permit
filter acl ace ethernet 172 100 ether-type eq ip
filter acl ace ip 172 100 src-ip eq 100.20.172.0
filter acl ace ip 172 100 ip-protocol-type eq tcp
filter acl ace protocol 172 100 dst-port eq 443
filter acl ace 172 100 enable
filter acl ace 172 105 name "REMDESKTOP_PERMIT"
filter acl ace action 172 105 permit
filter acl ace ethernet 172 105 ether-type eq ip
filter acl ace ip 172 105 src-ip eq 100.20.172.0
filter acl ace ip 172 105 ip-protocol-type eq tcp
filter acl ace protocol 172 105 dst-port eq 3389
filter acl ace 172 105 enable
```

```
filter acl ace 172 106 name "NORKOM_PERMIT"
filter acl ace action 172 106 permit
filter acl ace ethernet 172 106 ether-type eq ip
filter acl ace ip 172 106 src-ip eq 100.20.172.0
filter acl ace ip 172 106 dst-ip eq 100.6.106.0
filter acl ace 172 106 enable
filter acl ace 172 107 name "SPECTRUM_PERMIT"
filter acl ace action 172 107 permit
filter acl ace ethernet 172 107 ether-type eq ip
filter acl ace ip 172 107 src-ip eq 100.20.172.0
filter acl ace ip 172 107 dst-ip eq 100.20.17.0
filter acl ace 172 107 enable
filter acl ace 172 110 name "PROXY_8080_PERMIT"
filter acl ace action 172 110 permit
filter acl ace ethernet 172 110 ether-type eq ip
filter acl ace ip 172 110 src-ip eq 100.20.172.0
filter acl ace ip 172 110 dst-ip eq 100.20.189.0
filter acl ace ip 172 110 ip-protocol-type eq tcp
filter acl ace protocol 172 110 dst-port eq 8080
filter acl ace 172 110 enable
filter acl ace 172 120 name "CITRIX_Conn-tcp"
filter acl ace action 172 120 permit
filter acl ace ethernet 172 120 ether-type eq ip
filter acl ace ip 172 120 ip-protocol-type eq tcp
filter acl ace protocol 172 120 dst-port eq 1494
filter acl ace 172 120 enable
filter acl ace 172 121 name "CITRIX_Conn-udp"
filter acl ace action 172 121 permit
filter acl ace ethernet 172 121 ether-type eq ip
filter acl ace ip 172 121 ip-protocol-type eq udp
filter acl ace protocol 172 121 dst-port eq 1604
filter acl ace 172 121 enable
filter acl ace 172 128 name "VOIP_VLAN_PERMIT"
```

```
filter acl ace action 172 128 permit
filter acl ace ethernet 172 128 ether-type eq ip
filter acl ace ip 172 128 src-ip eq 100.20.172.0
filter acl ace ip 172 128 dst-ip eq 10.201.0.0
filter acl ace 172 128 enable
filter acl ace 172 129 name "GANYMEDE_PERMIT"
filter acl ace action 172 129 permit
filter acl ace ethernet 172 129 ether-type eq ip
filter acl ace ip 172 129 src-ip eq 100.20.172.0
filter acl ace ip 172 129 dst-ip eq 100.6.100.225
filter acl ace 172 129 enable
filter acl ace 172 130 name "PWC_VPN_ERISIM"
filter acl ace action 172 130 permit
filter acl ace ethernet 172 130 ether-type eq ip
filter acl ace ip 172 130 src-ip eq 100.20.172.0
filter acl ace ip 172 130 ip-protocol-type eq tcp
filter acl ace protocol 172 130 dst-port eq 11160
filter acl ace 172 130 enable
filter acl ace 172 131 name "ISAKMP"
filter acl ace action 172 131 permit
filter acl ace ethernet 172 131 ether-type eq ip
filter acl ace ip 172 131 ip-protocol-type eq udp
filter acl ace protocol 172 131 dst-port eq 500
filter acl ace 172 131 enable
filter acl ace 172 132 name "ESP"
filter acl ace action 172 132 permit
filter acl ace ethernet 172 132 ether-type eq ip
filter acl ace ip 172 132 ip-protocol-type eq 50
filter acl ace 172 132 enable
filter acl ace 172 133 name "LOGLAMAK_ICIN"
filter acl ace action 172 133 permit redirect-next-hop 100.20.150.34
filter acl ace ethernet 172 133 ether-type eq ip
filter acl ace ip 172 133 src-ip eq 100.20.172.72
```

```
filter acl ace 172 140 name "DENY_ANY_ANY"
filter acl ace action 172 140 deny
filter acl ace ethernet 172 140 ether-type eq ip
filter acl ace ip 172 140 src-ip eq 0.0.0.0
filter acl ace ip 172 140 dst-ip eq 0.0.0.0
filter acl ace 172 140 enable

filter acl 802 type inVlan name "NICE-CLS_ACL-in"
filter acl vlan 802 802
filter acl 802 disable
filter acl ace 802 1 name "NICE_to_NICE"
filter acl ace action 802 1 permit
filter acl ace ethernet 802 1 ether-type eq ip
filter acl ace ip 802 1 dst-ip eq 100.20.174.32
filter acl ace 802 1 enable
filter acl ace 802 10 name "ICMP_PERMIT"
filter acl ace action 802 10 permit
filter acl ace ethernet 802 10 ether-type eq ip
filter acl ace ip 802 10 ip-protocol-type eq icmp
filter acl ace 802 10 enable
filter acl ace 802 20 name "IGMP_PERMIT"
filter acl ace action 802 20 permit
filter acl ace ethernet 802 20 ether-type eq ip
filter acl ace ip 802 20 ip-protocol-type eq 2
filter acl ace 802 20 enable
filter acl ace 802 30 name "VRRP_PERMIT"
filter acl ace action 802 30 permit
filter acl ace ethernet 802 30 ether-type eq ip
filter acl ace ip 802 30 ip-protocol-type eq vrrp
filter acl ace 802 30 enable
filter acl ace 802 40 name "DNS_PERMIT"
filter acl ace action 802 40 permit
filter acl ace ethernet 802 40 ether-type eq ip
filter acl ace ip 802 40 src-ip eq 100.20.174.32
```

```
filter acl ace ip 802 40 dst-ip eq 100.20.104.0
filter acl ace protocol 802 40 dst-port eq dns
filter acl ace 802 40 enable
filter acl ace 802 45 name "DC-EXCH-DNS"
filter acl ace action 802 45 permit
filter acl ace ethernet 802 45 ether-type eq ip
filter acl ace ip 802 45 dst-ip eq 100.20.104.0
filter acl ace 802 45 enable
filter acl ace 802 50 name "ESTABLISHED RST"
filter acl ace action 802 50 permit
filter acl ace ethernet 802 50 ether-type eq ip
filter acl ace ip 802 50 src-ip eq 100.20.174.32
filter acl ace ip 802 50 ip-protocol-type eq tcp
filter acl ace protocol 802 50 dst-port eq 1023
filter acl ace protocol 802 50 tcp-flags eq rst
filter acl ace 802 50 enable
filter acl ace 802 51 name "ESTABLISHED ACK"
filter acl ace action 802 51 permit
filter acl ace ethernet 802 51 ether-type eq ip
filter acl ace ip 802 51 src-ip eq 100.20.174.32
filter acl ace ip 802 51 ip-protocol-type eq tcp
filter acl ace protocol 802 51 dst-port eq 1023
filter acl ace protocol 802 51 tcp-flags eq ack
filter acl ace 802 51 enable
filter acl ace 802 52 ame "UDP_Permit"
filter acl ace 802 52 action permit
filter acl ace ethernet 802 52 ether-type eq ip
filter acl ace ip 802 52 ip-protocol-type eq udp
filter acl ace 802 52 enable
filter acl ace 802 60 name "NICE_Logging"
filter acl ace action 802 60 permit
filter acl ace ethernet 802 60 ether-type eq ip
filter acl ace ip 802 60 src-ip eq 100.20.174.32
```

```
filter acl ace ip 802 60 ip-protocol-type eq tcp
filter acl ace protocol 802 60 dst-port eq 2011
filter acl ace 802 60 enable
filter acl ace 802 65 name "RTS_Conn"
filter acl ace action 802 65 permit
filter acl ace ethernet 802 65 ether-type eq ip
filter acl ace ip 802 65 dst-ip eq 100.20.152.20
filter acl ace 802 65 enable
filter acl ace 802 70 name "CTI_Conn"
filter acl ace action 802 70 permit
filter acl ace ethernet 802 70 ether-type eq ip
filter acl ace ip 802 70 src-ip eq 100.20.174.32
filter acl ace ip 802 70 ip-protocol-type eq tcp
filter acl ace protocol 802 70 dst-port eq 3750
filter acl ace 802 70 enable
filter acl ace 802 90 name "LOGLAMA"
filter acl ace action 802 90 permit redirect-next-hop 100.20.150.217
filter acl ace ethernet 802 90 ether-type eq ip
filter acl ace ip 802 90 src-ip eq 0.0.0.0
filter acl ace 802 100 name "DENY_ANY"
filter acl ace action 802 100 deny
filter acl ace ethernet 802 100 ether-type eq ip
filter acl ace ip 802 100 src-ip eq 0.0.0.0
filter acl ace ip 802 100 dst-ip eq 0.0.0.0
filter acl ace 802 100 enable

filter acl 804 type inVlan name "BASIM_LIMITED-in"
filter acl vlan 804 804
filter acl ace 804 5 name "Basim_to_Basim"
filter acl ace action 804 5 permit
filter acl ace ethernet 804 5 ether-type eq ip
filter acl ace ip 804 5 dst-ip eq 100.20.174.96
filter acl ace 804 5 enable
filter acl ace 804 10 name "ICMP_PERMIT"
```

```
filter acl ace action 804 10 permit
filter acl ace ethernet 804 10 ether-type eq ip
filter acl ace ip 804 10 ip-protocol-type eq icmp
filter acl ace 804 10 enable
filter acl ace 804 20 name "IGMP_PERMIT"
filter acl ace action 804 20 permit
filter acl ace ethernet 804 20 ether-type eq ip
filter acl ace ip 804 20 ip-protocol-type eq 2
filter acl ace 804 20 enable
filter acl ace 804 30 name "VRRP_PERMIT"
filter acl ace action 804 30 permit
filter acl ace ethernet 804 30 ether-type eq ip
filter acl ace ip 804 30 ip-protocol-type eq vrrp
filter acl ace 804 30 enable
filter acl ace 804 40 name "DNS_PERMIT"
filter acl ace action 804 40 permit
filter acl ace protocol 804 40 dst-port eq dns
filter acl ace 804 40 enable
filter acl ace 804 45 name "DC-EXCH-DNS"
filter acl ace action 804 45 permit
filter acl ace ethernet 804 45 ether-type eq ip
filter acl ace ip 804 45 dst-ip eq 100.20.104.0
filter acl ace 804 45 enable
filter acl ace 804 50 name "ESTABLISHED RST"
filter acl ace action 804 50 permit
filter acl ace ethernet 804 50 ether-type eq ip
filter acl ace ip 804 50 src-ip eq 100.20.174.97
filter acl ace ip 804 50 ip-protocol-type eq tcp
filter acl ace protocol 804 50 dst-port eq 1023
filter acl ace protocol 804 50 tcp-flags eq rst
filter acl ace 804 50 enable
filter acl ace 804 51 name "ESTABLISHED ACK"
filter acl ace action 804 51 permit
```

```
filter acl ace ethernet 804 51 ether-type eq ip
filter acl ace ip 804 51 src-ip eq 100.20.174.97
filter acl ace ip 804 51 ip-protocol-type eq tcp
filter acl ace protocol 804 51 dst-port eq 1023
filter acl ace protocol 804 51 tcp-flags eq ack
filter acl ace 804 51 enable
filter acl ace 804 60 name "E-BANK_ERISIM"
filter acl ace action 804 60 permit
filter acl ace ethernet 804 60 ether-type eq ip
filter acl ace ip 804 60 dst-ip eq 100.20.115.11
filter acl ace ip 804 60 ip-protocol-type eq tcp
filter acl ace protocol 804 60 tcp-dst-port eq 80
filter acl ace 804 60 enable
filter acl ace 804 70 name "E-BANK_ERISIM_HTTPS"
filter acl ace action 804 70 permit
filter acl ace ethernet 804 70 ether-type eq ip
filter acl ace ip 804 70 dst-ip eq 100.20.115.11
filter acl ace ip 804 70 ip-protocol-type eq tcp
filter acl ace protocol 804 70 dst-port eq 443
filter acl ace 804 70 enable
filter acl ace 804 80 name "FRED_Erisim"
filter acl ace action 804 80 permit
filter acl ace ethernet 804 80 ether-type eq ip
filter acl ace ip 804 80 dst-ip eq 100.20.100.145
filter acl ace 804 80 enable
filter acl ace 804 81 name "BARNEY_Erisim"
filter acl ace action 804 81 permit
filter acl ace ethernet 804 81 ether-type eq ip
filter acl ace ip 804 81 dst-ip eq 100.20.100.151
filter acl ace 804 81 enable
filter acl ace 804 90 name "BUFFY_ERISIM"
filter acl ace action 804 90 permit
filter acl ace ethernet 804 90 ether-type eq ip
```

```
filter acl ace ip 804 90 dst-ip eq 100.20.100.77
filter acl ace ip 804 90 ip-protocol-type eq tcp
filter acl ace protocol 804 90 dst-port eq 1433
filter acl ace 804 90 enable
filter acl ace create 804 100 name "ROMTest_ERISIM"
filter acl ace action 804 100 permit
filter acl ace ethernet 804 100 ether-type eq ip
filter acl ace ip 804 100 dst-ip eq 100.20.24.77
filter acl ace ip 804 100 ip-protocol-type eq tcp
filter acl ace protocol 804 100 dst-port eq 1433
filter acl ace 804 100 enable
filter acl ace 804 101 name "Mrksql-t0_ERISIM"
filter acl ace action 804 101 permit
filter acl ace ethernet 804 101 ether-type eq ip
filter acl ace ip 804 101 dst-ip eq 100.20.20.77
filter acl ace ip 804 101 ip-protocol-type eq tcp
filter acl ace protocol 804 101 dst-port eq 1433
filter acl ace 804 101 enable
filter acl ace 804 110 name "ROSETTA_ERISIM"
filter acl ace action 804 110 permit
filter acl ace ethernet 804 110 ether-type eq ip
filter acl ace ip 804 110 dst-ip eq 172.17.1.100
filter acl ace 804 110 enable
filter acl ace 804 120 name "PLAST_ERISIM"
filter acl ace action 804 120 permit
filter acl ace ethernet 804 120 ether-type eq ip
filter acl ace ip 804 120 dst-ip eq 212.57.7.20
filter acl ace 804 120 enable
filter acl ace 804 130 name "AV-Yama_YONETIM_2967"
filter acl ace action 804 130 permit
filter acl ace ethernet 804 130 ether-type eq ip
filter acl ace ip 804 130 ip-protocol-type eq tcp
filter acl ace protocol 804 130 dst-port eq 2967
```

```
filter acl ace 804 130 enable
filter acl ace 804 140 name "AV-Yama_YONETIM_9968"
filter acl ace action 804 140 permit
filter acl ace ethernet 804 140 ether-type eq ip
filter acl ace ip 804 140 ip-protocol-type eq tcp
filter acl ace protocol 804 140 dst-port eq 9968
filter acl ace 804 140 enable
filter acl ace 804 150 name "AV-Yama_YONETIM_UDP_2967"
filter acl ace action 804 150 permit
filter acl ace ethernet 804 150 ether-type eq ip
filter acl ace ip 804 150 ip-protocol-type eq udp
filter acl ace protocol 804 150 dst-port eq 2967
filter acl ace 804 150 enable
filter acl ace 804 160 name "AV-Yama_YONETIM_UDP_9968"
filter acl ace action 804 160 permit
filter acl ace ethernet 804 160 ether-type eq ip
filter acl ace ip 804 160 ip-protocol-type eq udp
filter acl ace protocol 804 160 dst-port eq 9968
filter acl ace 804 160 enable
filter acl ace 804 170 name "AV-Yama_YONETIM_UDP_Source"
filter acl ace action 804 170 permit
filter acl ace ethernet 804 170 ether-type eq ip
filter acl ace ip 804 170 ip-protocol-type eq udp
filter acl ace protocol 804 170 src-port eq 9968
filter acl ace 804 170 enable
filter acl ace 804 210 name "PROXY_ERISIM_EK"
filter acl ace action 804 210 permit
filter acl ace ethernet 804 210 ether-type eq ip
filter acl ace ip 804 210 dst-ip eq 100.20.189.0
filter acl ace ip 804 210 ip-protocol-type eq tcp
filter acl ace protocol 804 210 dst-port eq 8080
filter acl ace 804 210 enable
filter acl ace 804 220 name "LOGLAMA"
```

```
filter acl ace action 804 220 permit redirect-next-hop 100.20.150.217
filter acl ace ethernet 804 220 ether-type eq ip
filter acl ace ip 804 220 src-ip eq 0.0.0.0
filter acl ace 804 230 name "DENY_ANY"
filter acl ace action 804 230 deny
filter acl ace ethernet 804 230 ether-type eq ip
filter acl ace ip 804 230 src-ip eq 0.0.0.0
filter acl ace ip 804 230 dst-ip eq 0.0.0.0
filter acl ace 804 230 enable

filter acl 805 type inVlan name "SBS_Remote"
filter acl vlan 805 805
filter acl ace 805 5 name "SBS-to-SBS"
filter acl ace action 805 5 permit
filter acl ace ethernet 804 5 ether-type eq ip
filter acl ace ip 805 5 dst-ip eq 100.20.174.128
filter acl ace 805 5 enable
filter acl ace 805 10 name "ICMP_PERMIT"
filter acl ace action 805 10 permit
filter acl ace ethernet 805 10 ether-type eq ip
filter acl ace ip 805 10 ip-protocol-type eq icmp
filter acl ace 805 10 enable
filter acl ace 805 20 name "IGMP_PERMIT"
filter acl ace action 805 20 permit
filter acl ace ethernet 805 20 ether-type eq ip
filter acl ace ip 805 20 ip-protocol-type eq 2
filter acl ace 805 20 enable
filter acl ace 805 30 name "VRRP_PERMIT"
filter acl ace action 805 30 permit
filter acl ace ethernet 805 30 ether-type eq ip
filter acl ace ip 805 30 ip-protocol-type eq vrrp
filter acl ace 805 30 enable
filter acl ace 805 40 name "DNS_PERMIT"
filter acl ace action 805 40 permit
```

```
filter acl ace protocol 805 40 dst-port eq 53
filter acl ace 805 40 enable
filter acl ace 805 50 name "ESTABLISHED RST"
filter acl ace action 805 50 permit
filter acl ace ethernet 805 50 ether-type eq ip
filter acl ace ip 805 50 src-ip eq 100.20.174.128
filter acl ace ip 805 50 ip-protocol-type eq tcp
filter acl ace protocol 805 50 dst-port eq 1023
filter acl ace protocol 805 50 tcp-flags eq rst
filter acl ace 805 50 enable
filter acl ace 805 51 name "ESTABLISHED ACK"
filter acl ace action 805 51 permit
filter acl ace ethernet 805 51 ether-type eq ip
filter acl ace ip 805 51 src-ip eq 100.20.174.128
filter acl ace ip 805 51 ip-protocol-type eq tcp
filter acl ace protocol 805 51 dst-port eq 1023
filter acl ace protocol 805 51 tcp-flags eq ack
filter acl ace 805 51 enable
filter acl ace 805 80 name "DC_DNS_EXCH_PERMIT"
filter acl ace action 805 80 permit
filter acl ace ethernet 805 80 ether-type eq ip
filter acl ace ip 805 80 dst-ip eq 100.20.104.0
filter acl ace 805 80 enable
filter acl ace 805 90 name "HTTP_PERMIT"
filter acl ace action 805 90 permit
filter acl ace ethernet 805 90 ether-type eq ip
filter acl ace ip 805 90 ip-protocol-type eq tcp
filter acl ace protocol 805 90 dst-port eq 80
filter acl ace 805 90 enable
filter acl ace 805 100 name "HTTPS_PERMIT"
filter acl ace action 805 100 permit
filter acl ace ethernet 805 100 ether-type eq ip
filter acl ace ip 805 100 ip-protocol-type eq tcp
```

```
filter acl ace protocol 805 100 dst-port eq 443
filter acl ace 805 100 enable
filter acl ace 805 105 name "REMDESKTOP_PERMIT"
filter acl ace action 805 105 permit
filter acl ace ethernet 805 105 ether-type eq ip
filter acl ace ip 805 105 ip-protocol-type eq tcp
filter acl ace protocol 805 105 dst-port eq 3389
filter acl ace 805 105 enable
filter acl ace 805 110 name "PROXY_8080_PERMIT"
filter acl ace action 805 110 permit
filter acl ace ethernet 805 110 ether-type eq ip
filter acl ace ip 805 110 dst-ip eq 100.20.189.0
filter acl ace ip 805 110 ip-protocol-type eq tcp
filter acl ace protocol 805 110 dst-port eq 8080
filter acl ace 805 110 enable
filter acl ace 805 120 name "DAMEWARE_PERMIT"
filter acl ace action 805 120 permit
filter acl ace ethernet 805 120 ether-type eq ip
filter acl ace ip 805 120 src-ip eq 100.20.174.128
filter acl ace protocol 805 120 dst-port eq 445,6129
filter acl ace 805 120 enable
filter acl ace 805 140 name "DENY_ANY_ANY"
filter acl ace action 805 140 deny
filter acl ace ethernet 805 140 ether-type eq ip
filter acl ace ip 805 140 src-ip eq 0.0.0.0
filter acl ace ip 805 140 dst-ip eq 0.0.0.0
filter acl ace 805 140 enable

filter acl vlan 1802 802
filter acl 1802 disable
filter acl ace 1802 10 name "ICMP_PERMIT"
filter acl ace action 1802 10 permit
filter acl ace ethernet 1802 10 ether-type eq ip
filter acl ace ip 1802 10 ip-protocol-type eq icmp
```

```
filter acl ace 1802 10 enable
filter acl ace 1802 20 name "IGMP_PERMIT"
filter acl ace action 1802 20 permit
filter acl ace ethernet 1802 20 ether-type eq ip
filter acl ace ip 1802 20 ip-protocol-type eq 2
filter acl ace 1802 20 enable
filter acl ace 1802 30 name "VRRP_PERMIT"
filter acl ace action 1802 30 permit
filter acl ace ethernet 1802 30 ether-type eq ip
filter acl ace ip 1802 30 ip-protocol-type eq vrrp
filter acl ace 1802 30 enable
filter acl ace 1802 51 name "UDP_Permit"
filter acl ace action 1802 51 permit
filter acl ace ethernet 1802 51 ether-type eq ip
filter acl ace ip 1802 51 ip-protocol-type eq udp
filter acl ace 1802 51 enable
filter acl ace 1802 60 name "NICE_Logging"
filter acl ace action 1802 60 permit
filter acl ace ethernet 1802 60 ether-type eq ip
filter acl ace ip 1802 60 src-ip eq 100.20.174.32
filter acl ace protocol 1802 60 dst-port eq 2011
filter acl ace 1802 60 enable
filter acl ace 1802 100 name "DENY_ANY"
filter acl ace action 1802 100 deny
filter acl ace ip 1802 100 src-ip eq 0.0.0.0
filter acl ace ip 1802 100 dst-ip eq 0.0.0.0
filter acl ace 1802 100 enable
filter acl vlan 1804 804
filter acl ace 1804 5 name "BASIM-to-BASIM"
filter acl ace action 1804 5 permit
filter acl ace ethernet 1804 10 ether-type eq ip
filter acl ace ip 1804 5 src-ip eq 100.20.174.96
filter acl ace ip 1804 5 dst-ip eq 100.20.174.96
```

```
filter acl ace 1804 5 enable
filter acl ace 1804 10 name "ICMP_PERMIT"
filter acl ace action 1804 10 permit
filter acl ace ethernet 1804 10 ether-type eq ip
filter acl ace ip 1804 10 ip-protocol-type eq icmp
filter acl ace 1804 10 enable
filter acl ace 1804 20 create name "IGMP_PERMIT"
filter acl ace action 1804 20 permit
filter acl ace ethernet 1804 20 ether-type eq ip
filter acl ace ip 1804 20 ip-protocol-type eq 2
filter acl ace 1804 20 enable
filter acl ace 1804 30 name "VRRP_PERMIT"
filter acl ace action 1804 30 permit
filter acl ace ethernet 1804 30 ether-type eq ip
filter acl ace ip 1804 30 ip-protocol-type eq vrrp
filter acl ace 1804 30 enable
filter acl ace 1804 40 create name "DNS_PERMIT"
filter acl ace action 1804 40 permit
filter acl ace protocol 1804 40 src-port eq 53
filter acl ace 1804 40 enable
filter acl ace 1804 45 name "DC-EXCH-DNS"
filter acl ace action 1804 45 permit
filter acl ace ethernet 1804 45 ether-type eq ip
filter acl ace ip 1804 45 src-ip eq 100.20.104.0
filter acl ace 1804 45 enable
filter acl ace 1804 50 name "ESTABLISHED RST"
filter acl ace action 1804 50 permit
filter acl ace ethernet 1804 50 ether-type eq ip
filter acl ace ip 1804 50 dst-ip eq 100.20.174.97
filter acl ace ip 1804 50 ip-protocol-type eq tcp
filter acl ace protocol 1804 50 dst-port eq 1023
filter acl ace protocol 1804 50 tcp-flags eq rst
filter acl ace 1804 50 enable
```

```
filter acl ace 1804 51 name "ESTABLISHED ACK"
filter acl ace action 1804 51 permit
filter acl ace ethernet 1804 51 ether-type eq ip
filter acl ace ip 1804 51 dst-ip eq 100.20.174.97
filter acl ace ip 1804 51 ip-protocol-type eq tcp
filter acl ace protocol 1804 51 dst-port eq 1023
filter acl ace protocol 1804 51 tcp-flags eq ack
filter acl ace 1804 51 enable
filter acl ace 1804 80 name "PWC_ERISIM"
filter acl ace action 1804 80 permit
filter acl ace ethernet 1804 80 ether-type eq ip
filter acl ace ip 1804 80 src-ip eq 100.20.100.145
filter acl ace 1804 80 enable
filter acl ace 1804 110 name "ROSETTA_ERISIM"
filter acl ace action 1804 110 permit
filter acl ace ethernet 1804 110 ether-type eq ip
filter acl ace ip 1804 110 src-ip eq 172.17.1.100
filter acl ace 1804 110 enable
filter acl ace 1804 120 name "PLAST_ERISIM"
filter acl ace action 1804 120 permit
filter acl ace ethernet 1804 120 ether-type eq ip
filter acl ace ip 1804 120 src-ip eq 212.57.7.20
filter acl ace 1804 120 enable
filter acl ace 1804 130 name "AV-Yama_YONETIM_9968"
filter acl ace action 1804 130 permit
filter acl ace ethernet 1804 130 ether-type eq ip
filter acl ace ip 1804 130 ip-protocol-type eq tcp
filter acl ace protocol 1804 130 dst-port eq 9968
filter acl ace 1804 130 enable
filter acl ace 1804 140 name "AV-Yama_YONETIM_2967"
filter acl ace action 1804 140 permit
filter acl ace ethernet 1804 140 ether-type eq ip
filter acl ace ip 1804 140 ip-protocol-type eq tcp
```

```
filter acl ace protocol 1804 140 dst-port eq 2967
filter acl ace 1804 140 enable
filter acl ace 1804 150 name "AV-Yama_YONETIM_UDP_9968"
filter acl ace action 1804 150 permit
filter acl ace ethernet 1804 150 ether-type eq ip
filter acl ace ip 1804 50 ip-protocol-type eq udp
filter acl ace protocol 1804 50 dst-port eq 9968
filter acl ace 1804 40 enable
filter acl ace 1804 160 name "AV-Yama_YONETIM_UDP_2967"
filter acl ace action 1804 160 permit
filter acl ace ethernet 1804 160 ether-type eq ip
filter acl ace ip 1804 160 ip-protocol-type eq udp
filter acl ace protocol 1804 160 dst-port eq 2967
filter acl ace 1804 160 enable
filter acl ace 1804 180 create name "SUNUCU_YONETIM"
filter acl ace action 1804 180 permit
filter acl ace ethernet 1804 180 ether-type eq ip
filter acl ace ip 1804 180 src-ip eq 100.20.150.80
filter acl ace ip 1804 180 ip-protocol-type eq tcp
filter acl ace protocol 1804 180 dst-port eq 3389
filter acl ace 1804 180 enable
filter acl ace 1804 200 name "OTOMIZE_DEBIT_CARD_OPS"
filter acl ace action 1804 200 permit
filter acl ace ethernet 1804 200 ether-type eq ip
filter acl ace ip 1804 200 src-ip eq 100.20.114.0
filter acl ace ip 1804 200 ip-protocol-type eq tcp
filter acl ace protocol 1804 200 dst-port eq 445
filter acl ace 1804 200 enable
filter acl ace 1804 210 name "OTOMIZE_DEBIT_CARD_OPS"
filter acl ace action 1804 210 permit
filter acl ace ethernet 1804 210 ether-type eq ip
filter acl ace ip 1804 210 src-ip eq 100.20.24.0
filter acl ace ip 1804 210 ip-protocol-type eq tcp
```

```
filter acl ace protocol 1804 210 dst-port eq 445
filter acl ace 1804 210 enable
filter acl ace 1804 230 name "DENY_ANY"
filter acl ace action 1804 230 deny
filter acl ace ethernet 1804 230 ether-type eq ip
filter acl ace ip 1804 230 src-ip eq 0.0.0.0
filter acl ace ip 1804 230 dst-ip eq 0.0.0.0
filter acl ace 1804 230 enable
```