Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 9000

Release 4.0
NN46250-502
Issue 06.01
December 2014

© 2014 Avaya Inc.

All Rights Reserved.

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: http://support.avaya.com 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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.

License 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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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.

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: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://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, 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 7
Purpose 7
Related resources 7
Documentation 7
Training 7
Viewing Avaya Mentor videos 7
Support 8
Searching a documentation collection 8
Chapter 2: New in this release 10
Features 10
Other changes 10
Chapter 3: QoS fundamentals 11
Introduction to QoS 11
Configuration considerations 12
Queuing 12
Avaya Service Class 13
Internal QoS level 14
Classification and mapping 15
DiffServ 15
Ingress mappings 17
Egress mappings 21
QoS and filters 22
Policing and shaping 22
Layer 2 and Layer 3 trusted and untrusted ports 28
Broadcast and multicast traffic bandwidth limiters 29
CPU protection 29
QoS and VoIP 30
Traffic management profiles 31
SLA Mon™ 32
Chapter 4: Basic DiffServ configuration using ACLI 33
Enabling DiffServ on a port 33
Configuring Layer 3 trusted or untrusted ports 34
Configuring Layer 2 trusted or untrusted ports 35
Configuring the port QoS level 36
Chapter 5: Basic DiffServ configuration using EDM 38
Enabling DiffServ for a port 38
Configuring Layer 3 trusted or untrusted ports 39
Configuring Layer 2 trusted or untrusted ports 40
Configuring the port QoS level 40

Chapter 6: QoS configuration using ACLI 41
Configuring a QoS profile 41
Configuring broadcast and multicast bandwidth limiting 42
Configuring the port-based shaper 43
Configuring a port-based policer 44
Configuring a policy-based policer 45
Configuring ingress mappings 47
Configuring egress mappings 49
Saving the configuration 51
Restarting the platform 53
Chapter 7: QoS configuration using EDM 54
Configuring a QoS profile 54
Configuring port-based shaping 57
Configuring port-based policing 57
Configuring a policy-based policer 57
Modifying ingress 802.1p to QoS mappings 58
Modifying ingress DSCP to QoS mappings 59
Modifying egress QoS to 802.1p mappings 60
Modifying egress QoS to DSCP mappings 60
Saving the configuration 61
Chapter 8: Traffic filtering fundamentals 62
Overview 62
Access control lists 62
Access control entries 64
Actions 68
Conflict and Precedence 70
Common ACE uses and configuration 73
Traffic filter configuration 74
ACL and ACE configuration guidelines 74
Filter limitations 74
Chapter 9: Access control list configuration using ACLI 76
Creating an ACL 77
Associating VLANs with an ACL 79
Associating ports with an ACL 79
Configuring global and default actions for an ACL 80
Renaming an ACL 82
Disabling an ACL 83
Resetting an ACL to default values 83
Deleting an ACL 84
Chapter 10: Access control list configuration using EDM 86
Configuring an access control list 86
Chapter 11: Access control entry configuration using ACLI 88

Configuring ACEs ... 88
Configuring ACE actions ... 91
Configuring ARP ACEs ... 94
Configuring an Ethernet ACE ... 96
Configuring an IP ACE ... 99
Configuring a protocol ACE ... 102
Viewing ACL and ACE configuration data ... 105
Viewing filtered packets ... 106
Chapter 12: Access control entry configuration using EDM ... 109
Configuring an ACE ... 109
Configuring ACE actions ... 111
Configuring ACE ARP entries ... 113
Viewing all ACE ARP entries for an ACL ... 114
Configuring an ACE Ethernet source address ... 115
Configuring an ACE Ethernet destination address ... 116
Configuring an ACE LAN traffic type ... 117
Configuring an ACE Ethernet VLAN tag priority ... 118
Configuring an ACE Ethernet port ... 119
Configuring an ACE Ethernet VLAN ID ... 120
Viewing all ACE Ethernet entries for an ACL ... 121
Configuring an ACE IP source address ... 123
Configuring an ACE IP destination address ... 124
Configuring an ACE IP DSCP ... 125
Configuring an ACE IP protocol ... 126
Configuring ACE IP options ... 127
Configuring ACE IP fragmentation ... 127
Viewing all ACE IP entries for an ACL ... 129
Configuring an ACE source port ... 130
Configuring an ACE TCP flag ... 133
Viewing all ACE protocol entries for an ACL ... 134
Configuring the packet log ... 135
Chapter 13: Advanced filter examples ... 136
ACE filters for secure networks ... 136
Glossary ... 198

Chapter 1: Introduction

Purpose

This document provides conceptual information and configuration instructions to use Quality of Service (QoS) and ACL-based filters on the Avaya Virtual Services Platform 9000.

Related resources

Documentation

See *Documentation Reference for Avaya Virtual Services Platform 9000,* NN46250-100 for a list of the documentation for this product.

Training

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

Course code	Course title
4D00010E	Knowledge Access: ACIS - Avaya ERS 8000 and VSP 9000 Implementation
5D00040E	Knowledge Access: ACSS - Avaya VSP 9000 Support

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.

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 release

The following sections detail what is new in *Configuring QoS and ACL-Based Traffic Filtering on Avaya Virtual Services Platform 9000,* NN46250-502, for Release 4.0.

Features

This section describes features introduced in Release 4.0.

Update to qos if-shaper command

Release 4.0 updates the **`qos if-shaper`** command with the variable *{slot/port[-slot/port][,...]}*, which allows you to configure more than one port at a time. For more information, see: Configuring the port-based shaper on page 43.

Update to qos if-policer command

Release 4.0 updates the **`qos if-policer`** command parameters peak-rate and svc-rate to <*64–40000000*>. For more information, see Configuring a port-based policer on page 44.

9012QQ-2 Input/Output module

Release 4.0.1 introduces a second generation 9012QQ-2 Input/Output (I/O) module. The 9012QQ-2 module is a 12-port 40 gigabit per second (Gbps) module that supports the 40GBASE-R QSFP+ transceivers. You can use second generation I/O modules in first generation mode or second generation mode. For more information, see Traffic management profiles on page 31.

For more information on the 9012QQ-2 I/O module, see *Installing Modules in Avaya Virtual Services Platform 9000,* NN46250-301.

Other changes

See the following sections for other changes to the document.

Document title

Release 4.0 updates the document title to *Configuring QoS and ACL-Based Filtering on Avaya Virtual Services Platform 9000*, NN46250–502, from *Avaya Virtual Services Platform 9000 Configuration – QoS and ACL-Based Traffic Filtering*, NN46250–502.

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 9000 to allocate network resources for 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 9000 supports QoS classification for both Layer 2 (802.1p bits) and Layer 3 (Differentiated Services Code Point bits) parameters. Avaya Virtual Services Platform 9000 provides QoS functionality that can differ for Layer 2 (bridged) and Layer 3 (routed) traffic flows. The Avaya Virtual Services Platform 9000 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 9000 implements QoS functionality for IP traffic through a Differentiated Services (DiffServ) network architecture. The QoS implementation on Avaya Virtual Services Platform 9000 supports the following options:

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

- filter-based policing
- 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. The only exception to this situation is the high qos cp-limit values; after you remove the port from the MLT, the port uses the previously configured value.

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. Virtual Services Platform 9000 scheduler determines the order of packet transmission by controlling how the system services queues with respect to each other.

Weighted Random Early Detection (WRED) is supported on the fabric queues to provide congestion avoidance capabilities.

The basic operating philosophy of WRED is that it detects the onset of congestion and starts dropping packets in a random fashion before queue overflow leads to tail drops. Random drops not only improve throughput of adaptive applications using TCP but are also more suitable than tail drops for voice and streaming audio or video, as they result in less perceptible degradation.

WRED is enabled for all queues except the highest priority expedited forwarding queue (EF). Expedited Forwarding Per Hop Bevhaviour (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.

With WRED, early discard starts when the queue reaches 75 percent of its maximum allowed length. If the queue reaches 100 percent of its maximum allowed length packets destined to it are tail dropped. WRED parameters are independent of the fabric profile and are not user configurable in the 3.1 release.

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 9000 includes a built-in QoS implementation for Avaya Service Classes.

The Avaya Virtual Services Platform 9000 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. This Avaya Service Class also includes network control traffic packets for Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and other protocols.

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. During periods of network congestion, DiffServ nodes use drop precedence to control variable bit rates that exceed the minimum assured bandwidth.

- 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. During periods of network congestion, DiffServ nodes use drop precedence to control variable bit rates and burst sizes that exceed the minimum assured bandwidth.

- 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. During network congestion, DiffServ nodes use drop precedence to control variable bit rates and burst sizes that exceed the minimum assured bandwidth.

- 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. During network congestion, DiffServ nodes use drop precedence to control variable bit rates and burst sizes that exceed the minimum assured bandwidth. 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.

Internal QoS level

The internal QoS level or effective QoS level is a key element in the Virtual Services Platform 9000 QoS architecture. The internal QoS level specifies the kind of treatment a packet receives. Virtual Services Platform 9000 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 9000 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 and dropping traffic. The Virtual Services Platform 9000 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.
- flow-based and port-based policing: The switch rate-limits and colors packets; the switch drops or re-marks excessive traffic.
- 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 9000 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 9000 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 9000 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 9000 devices are on the network edge where they perform classification, marking, policing, and shaping functions.

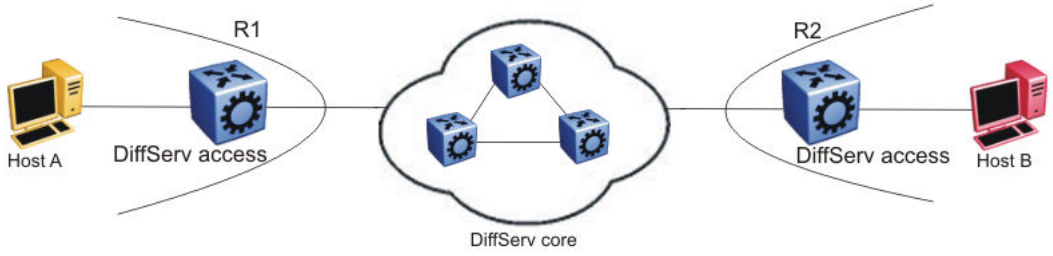


Figure 1: DiffServ network core and edge devices

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.

RFC2597 and RFC2598 define two standard PHB: the AF PHB group and the Expedited Forwarding (EF) PHB group. The Avaya Virtual Services Platform 9000 also uses the Default (DF) and CS groups. Class Selector in a DiffServ network provides backward compatibility with IP precedence.

RFC2597 describes the AF PHB group, which divides delivery of IP packets into four independent classes. The AF PHB group offers different levels of forwarding resources in each DiffServ node. Within each AF PHB group, the system marks IP packets with one of three possible drop precedence values. During network congestion, the drop precedence of a packet determines its relative importance within the AF PHB group.

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 22.

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	No	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
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

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	Custom	1	Custom
1	CS0/DF	0	Standard

Ingress IEEE 802.1p	PHB	QoS Level	Network Service Class (NSC)
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	Premium/EF

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 (hexadecimal)		
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	2	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

Ingress				Internal QoS level	PHB level
DSCP	**DSCP (binary)**	**DSCP (hexadecimal)**	**TOS (hexadecimal)**		
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
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	6	CS5
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

Ingress				Internal QoS level	PHB level
DSCP	**DSCP (binary)**	**DSCP (hexadecimal)**	**TOS (hexadecimal)**		
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
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	Premium/EF

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
4	011010	1A	26
5	100010	22	34
6	101110	2E	46
7	101110	2E	46

QoS and filters

The Avaya Virtual Services Platform 9000 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, policy-based policers, and port-based policers. The Avaya Virtual Services Platform 9000 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 9000 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. The following figure shows basic policing and shaping behavior.

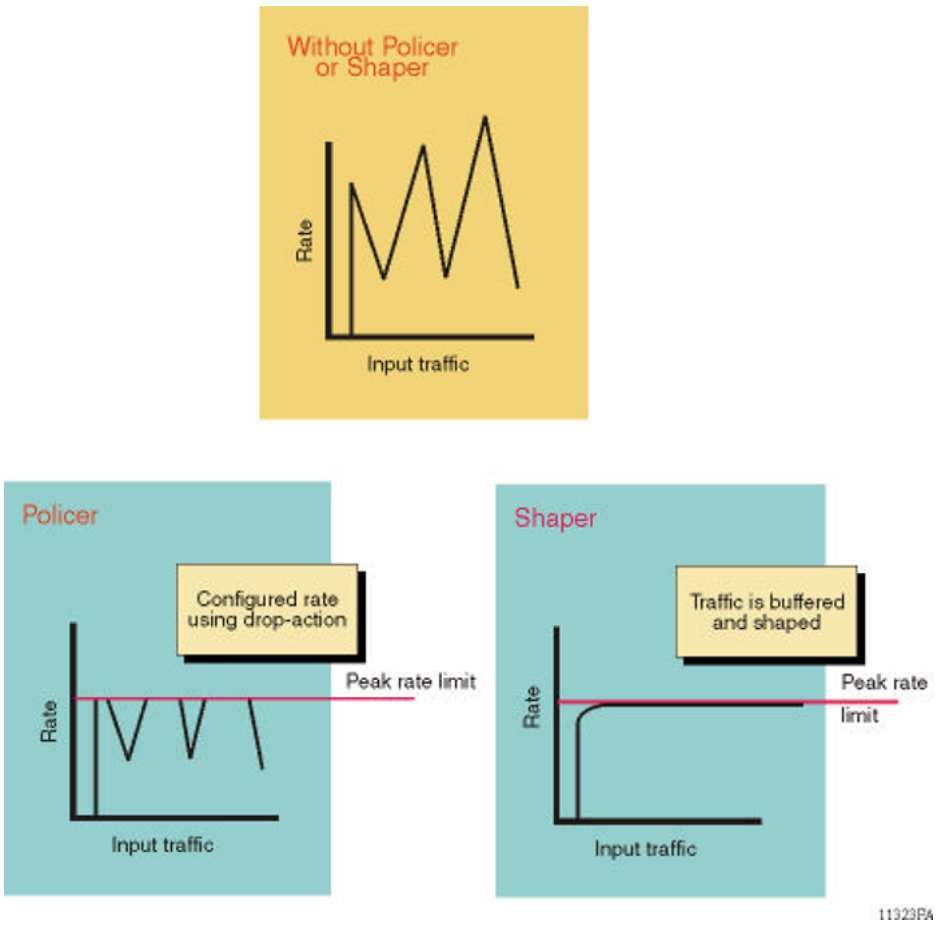


Figure 2: Basic policer and shaper behavior

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 3: Token flow on page 24.

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 9000, 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.

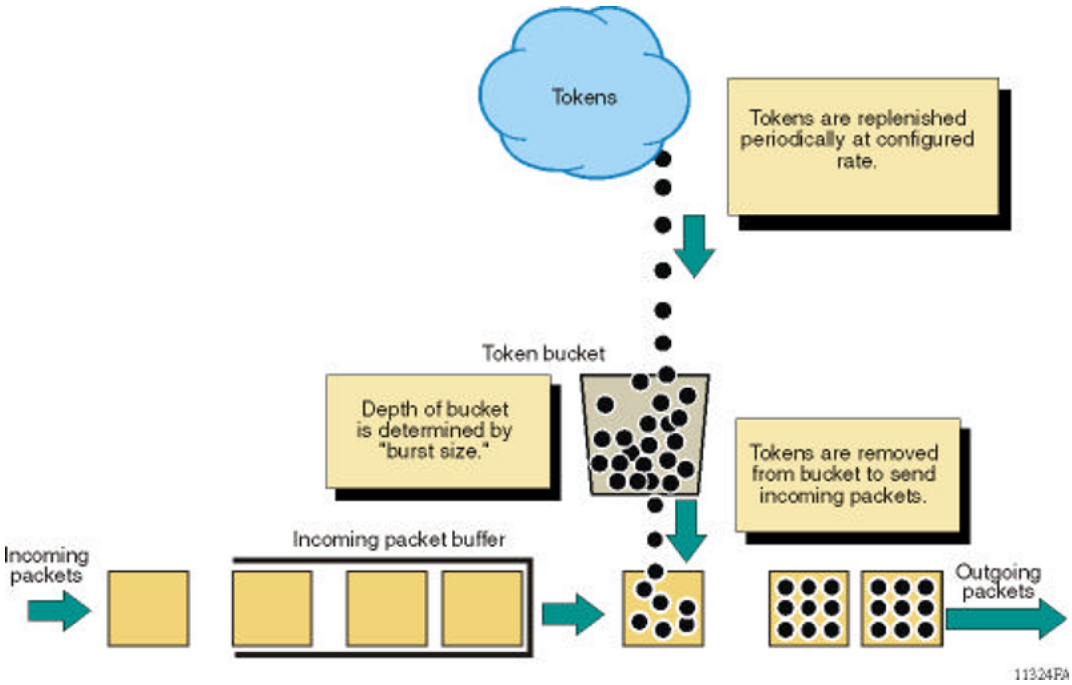


Figure 3: Token flow

Policy-based policer versus shaper

Policy-based traffic policers and traffic shapers identify traffic using a policy (a contract). Traffic that conforms to this policy (a service contract) is guaranteed transmission, and nonconforming traffic is considered in violation.

Policy-based policers and shapers differ in how they treat violations:

- Traffic shapers buffer and delay traffic that violates the contract. If no tokens are available in the token bucket, the shapers delay packets until a token is available. Queueing buffers excessive packets and shapes the flow when the source data rate is higher than expected. The Virtual Services Platform 9000 supports traffic shaping at the port level for outgoing (egress) traffic.
- Traffic policers drop packets when traffic is excessive, or re-mark the DSCP or 802.1p markings using filter actions. Policing occurs at ingress.

With the Virtual Services Platform 9000, you can define multiple actions in case of traffic violation.

Policy-based traffic policing

The Virtual Services Platform 9000 supports up to 16 000 policers.

The system supports the following options:

- service rate limiting
- peak information rate limiting
- three internal colors to which to re-mark packets
  - red (discard right away)
  - yellow (discard during network congestion)

- green (forward)

The system supports ingress policing on port ACLs or VLAN ACLs. Port ACLs apply to individual port-based policers. VLAN ACLs apply to global policers.

Policy-based policing in the Virtual Services Platform 9000 offers three primary functions:

- rate limiting based on peak and service rates
- dropping packets in excess of the peak rate
- packet coloring as green, yellow, and red

The switch forwards packets classified as EF, colors them green, and does not drop a packet. The switch colors packets classified as AF as green, yellow, or red. The switch drops red packets immediately and drops yellow packets during congestion.

Two Rate Three Color Marking

Virtual Services Platform 900 traffic policing supports RFC2698 (Two Rate Three Color Marker—trTCM). The traffic policer meters a packet stream and marks packets either green, yellow, or red. The policer marks a packet red if it exceeds the peak rate. The policer marks a packet yellow if it exceeds the service rate, and green if it falls below that rate.

The policer assigns drop probabilities to packets in the red, yellow, and green zones. The switch is more likely to drop yellow packets during congestion than green packets.

Three color marking is useful for ingress policing of a service in which you must enforce a peak rate separately from a committed (service) rate.

Traffic policies

Policing ensures flow conformance with the rate metrics of a configured policy. The policer drops the packets above the peak rate and recolors the packets above the service rate. When you configure traffic policies, you must define the peak and service rates.

A policy is a template that defines policing characteristics. You can reference a policy by ID or by name. You can apply a policy to an individual port or an entire VLAN using an ACL.

Policies and access control entries

You must bind a policy with a filter through an access control entry (ACE). The filter classifies the packet from the input stream and applies the appropriate traffic policy based on the flow classification criteria configured in the filter. An ACE policer overrides a port-based policer. The following figure shows the building blocks for traffic policing.

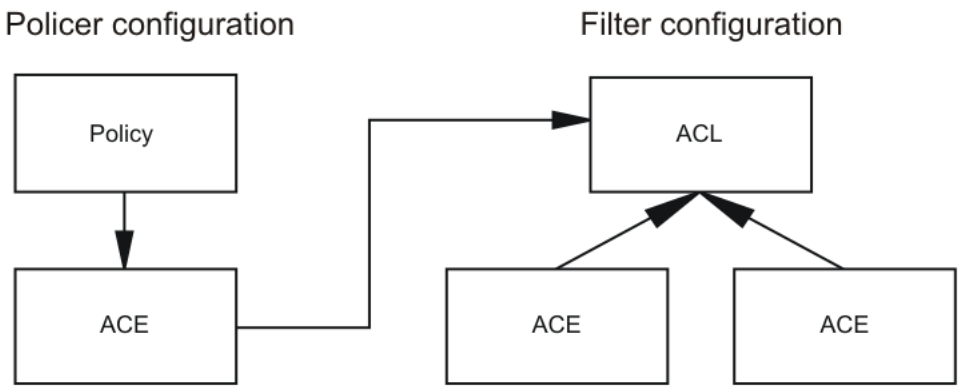


Figure 4: QoS traffic policing configuration building blocks

Policy-based policing actions

The following figure depicts policing actions. Packet coloring and drop actions depend on the peak and service rates. The system drops packets transmitted above the configured peak rate and recolors packets transmitted above the committed service rate.

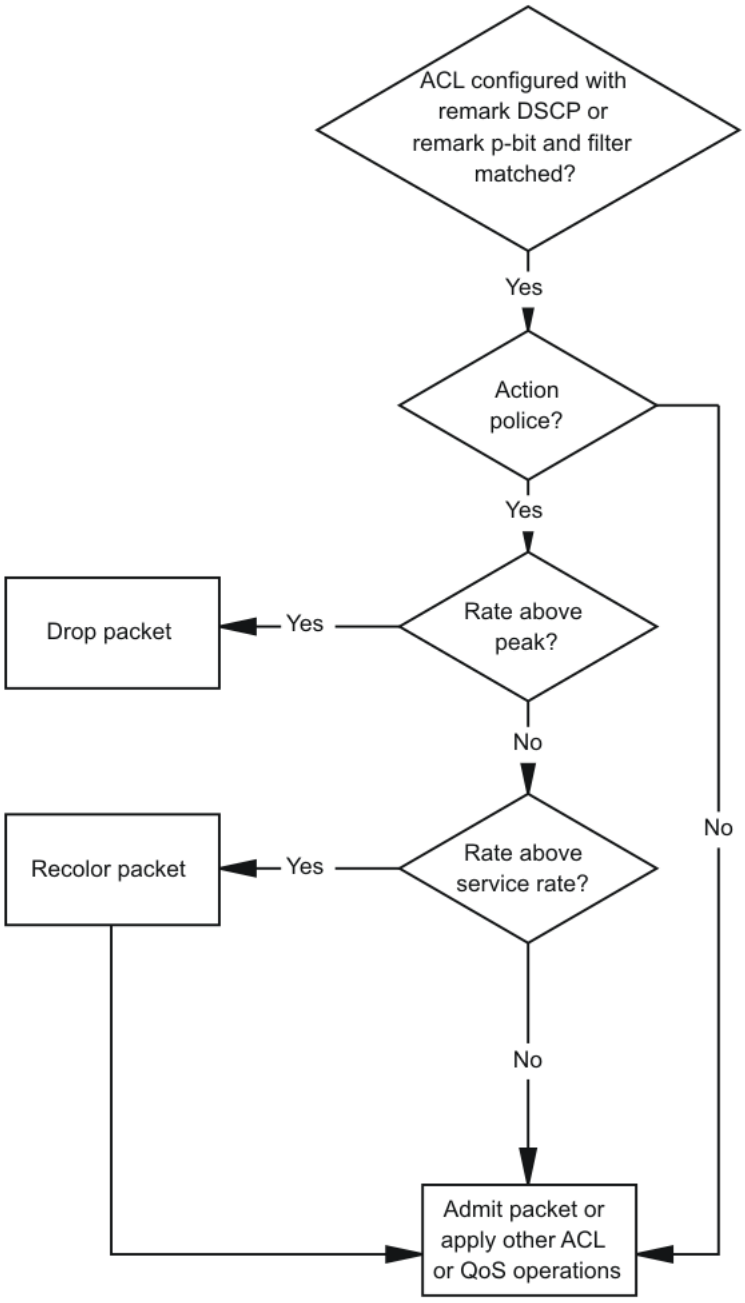


Figure 5: Policing actions

Port-based shaping

The port-based shaper rate limits the output traffic to the configured value for each port. By default, port-based shaping is disabled. The Virtual Services Platform 9000 supports a minimum shaper rate of 10 Mb/s and a maximum of 10 Gb/s 40 Gb/s. The system drops offending traffic.

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 9000 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 18.

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 9000 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 18.

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 18.

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 18.

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 18.

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.

CPU protection

Avaya Virtual Services Platform 9000 protects the CPU from Denial-of-Service (DOS) attacks through the following methods:

- CPU meters

  CPU meters are another mechanism to protect the CPU on the Control Processor (CP) module from becoming overloaded. The hardware counts every packet destined to each CPU over a specific time period. If the packet count exceeds the packet limit, the system drops the packets. Avaya limits the number of packets to each CPU on the CP module. You cannot configure CPU meters.

  CPU meters also provide packet priority scheduling. CPU meters use eight FIFO queues in FPGA. You cannot configure which packet types go into which queue. Each queue has a meter with packet limits. A scheduler services the eight queues, using a combination of strict priority and round-robin. Queues six and seven drain completely. Queues one through five use round-robin and queue zero uses best effort.

- port and MLT meters

  Use port and MLT meters to configure the limit on the number of control and data exception packets that can enter on each port or MLT interface. You can configure port and MLT meters

to shutdown the port or all ports in the MLT. If the number of packets exceeds the configured limit, the system generates a message in the log file. If enabled, the system shuts down the port or all ports in the MLT and raises an alarm. You can disable the port to clear the alarm. The default value is 8000 packets per second with no shutdown.

- protocol meters

  Protocol meters configure the limit on the number of control packets of specific packet types that can reach the CPU on the CP module. The system classifies every packet and assigns it an internal packet type. Protocol meters use the internal packet type to limit the number of each type of packet. You cannot configure protocol meters.

For more information about how to protect the CPU from DOS attacks, see *Administering Avaya Virtual Services Platform 9000,* NN46250-600.

QoS and VoIP

VoIP traffic requires low latency and jitter.

If you use the Avaya Virtual Services Platform 9000 as a core 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 9000 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 with all supported interface classes: untrusted (access), trusted (core), and unrestricted.

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.

Avaya Virtual Services Platform 9000 activates Avaya Automatic QoS automatically; you cannot deactivate this feature. 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.

Traffic management profiles

The Avaya Virtual Services Platform 9000 provides different paths through the switch fabric for unicast and multicast traffic. You can configure the system to give preference to one type of traffic over the other in times of over-subscription.

In these situations of high traffic flow, the Virtual Services Platform 9000 needs to drop traffic. You can control what traffic is dropped and what traffic is switched or routed by the system by using the fabric-profile boot configuration flag.

Use the boot configuration flag fabric-profile to configure preferences. You can select one of the following three profiles:

- balanced

  In the balanced profile, if the egress port is over-subscribed and the unicast traffic is greater than 80% of line rate, the system limits multicast traffic to 20%.

- unicast optimized

  In the unicast optimized profile, if the egress port is over-subscribed and the unicast traffic is greater than 90% of line rate, the system limits multicast traffic to 10%.

- multicast optimized

  In the multicast optimized profile, if the egress port is over subscribed and the unicast traffic is greater than 70% of line rate, the system limits multicast traffic to 30%.

Note:

9012QQ-2 traffic profiles depend on particular traffic flows, distribution, and may deviate from the exact numbers due to the hashing architecture.

After you make this configuration change, you need to restart the system. After the restart, the correct fabric-profile configuration is applied.

Oversubscription Behavior

There are eight unicast queues per egress port. There are one EF queue and seven Weighted RED queues. The EF traffic limits at 10% of line rate. The other queues have a minimum guaranteed

bandwidth as shown in the table below. Multicast traffic uses the remaining bandwidth. If there is no multicast traffic, the unicast traffic is distributed across the other WRED queues.

Avaya Class Naming	PHB	DSC	802.1P	Queue Type	Description	Minimum Balanced Bandwidth	Minimum Unicast Bandwidth	Minimum Multicast Bandwidth
Network/ Critical	CS7, CS6	48, 56	7	Strict Priority	Network Control - Strict Queue, 10% shaped	10.00%	10.00%	10.00%
Premium	EF, CS5	46, 40	6	WRED	Real Time Voice - Weighted	25.00%	27.00%	20.00%
Platinum	AF4x , CS4	32,34 , 36,38	5	WRED	Real Time Video - Weighted	15.00%	20.00%	15.00%
Gold	AF3x , CS3	24,26 , 28,30	4	WRED	Non-Real Time Streaming - Weighted	12.00%	12.00%	10.00%
Silver	AF2x , CS2	16,18 , 20,22	3	WRED	Non-Real Time - Weighted	8.00%	9.00%	7.00%
Bronze	AF1x , CS1	8,10, 12,14	2	WRED	Non-Real Time - Weighted	6.00%	7.00%	5.00%
Standard(Default)	DF, CSO	0-4	0	WRED	Best Effort - Weighted	4.00%	5.00%	3.00%
Custom	n/a	n/a	1	WRED	Scavenger	0.00%	0.00%	0.00%

SLA Mon™

SLA Mon™ helps network administrators ensure that the network maintains a high level of data and voice communication quality by measuring network performance, monitoring IP services, and assisting with network troubleshooting.

For more information about SLA Mon™, see *Monitoring Performance on Avaya Virtual Services Platform 9000,* NN46250-701.

Chapter 4: Basic DiffServ configuration using ACLI

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

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 GigabitEthernet 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]
   ```

Example

Enable DiffServ on a particular port. If you only want to enable DiffServ on one port you do not need to use the port parameter.

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface gigabitethernet 4/22
VSP-9012:1(config-if)#enable-diffserv
```

Enable DiffServ on multiple ports at once:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface gigabitethernet 4/10,4/11,4/12
VSP-9012:1(config-if)#enable-diffserv port 4/10,4/11,4/12 enable
```

Variable definitions

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

Table 7: 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 (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

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 GigabitEthernet 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]
   ```

Example

Configure ports 4/10 to 4/12 as access ports:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface gigabitethernet 4/10,4/11,4/12
VSP-9012:1(config-if)#access-diffserv port 4/10,4/11,4/12 enable
```

Variable definitions

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

Table 8: 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 (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

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 GigabitEthernet 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]
   ```

Example

Configure port 4/10 as Layer 2 untrusted:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface gigabitethernet 4/10
VSP-9012:1(config-if)#qos 802.1p-override enable
```

Variable definitions

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

Table 9: 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 GigabitEthernet 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>
   ```

Example

Configure the port 4/10 QoS level to 6:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface gigabitethernet 4/10
VSP-9012:1(config-if)#qos level port 4/10 6
```

Variable definitions

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

Table 10: 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 5: 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 States field descriptions

Use the data in the following table to use the **QoS Port States** 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 disabled), the system does not use the DSCP parameter for

Name	Description
	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 6: QoS configuration using ACLI

Use the procedures in this section to configure Quality of Service (QoS) on the Avaya Virtual Services Platform 9000.

Configuring a QoS profile

Configure a QoS profile to configure preferences between unicast and multicast traffic during times of over subscription.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the QoS profile:

   ```
   boot config flags fabric-profile <1-3>
   ```

   Note:

   Changes made during this procedure only take effect after the chassis has been rebooted.

Example

Configure the QoS profile to unicast optimized and reboot the chassis:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#boot config flags fabric-profile 2
VSP-9012:1(config)#save config
VSP-9012:1(config)#reset -y
```

Variable definitions

Use the data in the following table to use the **`boot config flags fabric-profile`** command.

Table 11: Variable definitions

Variable	Value
1–3	Configures the system to give preference to one type of traffic over the other in times of over subscription. The values are • 1: balanced • 2: unicast optimized • 3: multicast optimized The default profile is 1, balanced.

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 GigabitEthernet 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>
   ```

Example

Configure the broadcast bandwidth limiting to 5000 for port 4/10:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface gigabitethernet 4/10
VSP-9012:1(config-if)#rate-limit port 4/10 broadcast 5000
```

Variable definitions

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

Table 12: 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 (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

Configuring the port-based shaper

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

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

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

2. Configure port-based shaping:

   ```
   qos if-shaper [port {slot/port[-slot/port][,...]}] [shape-rate <10000-40000000>]
   ```

   Note:

   An error message displays if the value of more than 10Gbs is specified for an interface that is not on a 40Gbs card.

3. **(Optional)** Remove port-based shaping ports:

   ```
   no qos if-shaper [port {slot/port[-slot/port][,...]}]
   ```

4. **(Optional)** Configure port-based shaping to the default:

   ```
   default qos if-shaper [{slot/port[-slot/port][,...]}]
   ```

Example

- Configure port-based shaping rate to 10000 for port 4/10:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface gigabitethernet 4/10
VSP-9012:1(config-if)#qos if-shaper port 4/10 shape-rate 10000
```

- Configure port-based shaping rate to 20000000 for port 7/1:

```
VSP-9012:1(config-if)#qos if-shaper shape-rate 20000000
Error: port 7/1, Shape rate cannot exceed 10000000 kbps for this interface
```

Variable definitions

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

Table 13: Variable definitions

Variable	Value
port *{slot/port[-slot/port][,...]}*	Specifies the slot and port number, or a list of slot and port numbers, to which to apply shaping. This variable is optional.
shape-rate <*10000-10000000*>	Configures the shaping rate from 10000–10000000 Kb/s.
shape-rate <*10000-40000000*>	Configures the shaping rate from 10000–40000000 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 GigabitEthernet 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
   <64-40000000> svc-rate <64-40000000>
   ```

Example

Configure the policing limit to a peak-rate of 10000 and the service rate limit to 5000 for port 4/10:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#interface gigabitethernet 4/10
VSP-9012:1(config-if)#qos if-policer port 4/10 peak-rate 10000 svc-rate 5000
```

Variable definitions

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

Table 14: Variable definitions

Variable	Value
peak-rate<*64-40000000*>	Specifies the peak rate limit in Kbps.
port {slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
svc-rate<*64-40000000*>	Specifies the service rate limit in Kbps.

Configuring a policy-based policer

Use a QoS policy to configure peak and service policing rates. If all policy based policers have unique peak/svc rate combinations, then only 1020 policers is supported.

Note:

You can configure more than 1020 policers if some of the policers have the same peak/svc rate.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure a policer (traffic policy):

   ```
   qos policy <1-16000> peak-rate <64-5000000> svc-rate <64-5000000>
   [name WORD<1-32>]
   ```

3. Ensure that your configuration is correct:

   ```
   show qos policy-config [<1-16000>]
   ```

Example

Configure a traffic policy peak-rate of 1000 and a service rate of 688, with a Policer ID of 3 and the name 3:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#qos policy 3 peak-rate 1000 svc-rate 688 name 3
VSP-9012:1(config)#show qos policy-config

================================================================================
                              QOS Policer Table
```

```
 ================================================================================
PolicerID  Name          peak-rate    svc-rate
1          1             376          64
2          2             688          376
3          3             1000         688
4          4             1312         1000
5          5             1624         1312
6          6             1936         1624
7          7             2248         1936
8          8             2560         2248
9          9             2872         2560
10         10            3184         2872
11         11            3496         3184
12         12            3808         3496
13         13            4120         3808
14         14            4432         4120
15         15            4744         4432
16         16            5056         4744
17         17            5368         5056

17 out of 35 Total Num of Policers displayed
```

Variable definitions

Use the data in the following table to use the **qos policy** and **show qos policy-config** commands.

Table 15: Variable definitions

Variable	Value
<1-16000>	Specifies the policer ID number.
peak-rate *<64-5000000>*	Configures the policer peak rate in Kb/s.
srv-rate *<64-5000000>*	Configures the policer service rate in Kb/s.
name *WORD<1-32>*	Names the policer template.

Job aid

The following table describes the headings in the show command output.

Table 16: show qos policy-config output

Field	Description
PolicerID	Specifies the policer ID number.
Name	Specifies the name of the policer.
peak-rate	Specifies a policer peak rate in Kb/s.
svc-rate	Specifies a local policer service rate in Kb/s.

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> <0-7>
   ```

3. Configure DSCP to QoS ingress mappings:

   ```
   qos ingressmap ds <0-63> <0-7>
   ```

4. Ensure the configuration is correct:

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

Example

Note:

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

Configure the ingress mapping for port 4/10 to QoS Level 6 and an IEEE 802.1p bit of 6 and the DiffServ Code Point as Index 60 and QoS Level 6:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#qos ingressmap 1p 6 6
Do you want to continue with this QOS Level modification? (y/n) ? y
VSP-9012:1(config)#qos ingressmap ds 60 6
VSP-9012:1(config)#show qos ingressmap
              1p
                  ieee1p : 0
                   level : 1
              1p
                  ieee1p : 1
                   level : 0
              1p
                  ieee1p : 2
                   level : 2
              1p
                  ieee1p : 3
                   level : 3
              1p
                  ieee1p : 4
                   level : 4
              1p
                  ieee1p : 5
                   level : 5
              1p
                  ieee1p : 6
                   level : 6
```

```
                1p
                    ieee1p : 7

                   level : 6
               ds
                      DSCP : 0
                 DSCP-bin : 000000
                    level : 1
                ds
                      DSCP : 1
                 DSCP-bin : 000001
                    level : 1
                ds
                      DSCP : 2
                 DSCP-bin : 000010
                    level : 1
                ds
                      DSCP : 3
                 DSCP-bin : 000011
                    level : 1
                ds
                      DSCP : 4
                 DSCP-bin : 000100
                    level : 1
                ds
                      DSCP : 5
                 DSCP-bin : 000101

                         level : 1
                ds
                      DSCP : 6
                 DSCP-bin : 000110
                    level : 1
                ds
                      DSCP : 7
                 DSCP-bin : 000111
                    level : 1
                ds
                      DSCP : 8
                 DSCP-bin : 001000
                    level : 2
                ds
                      DSCP : 9
                 DSCP-bin : 001001
                    level : 1
                ds
                      DSCP : 10
                 DSCP-bin : 001010
                    level : 2
                ds
                      DSCP : 11

--More-- (q = quit)
```

Variable definitions

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

Table 17: Variable definitions

Variable	Value
1p<*0-7*> <*0-7*>	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 • level 7—7 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*> <*0-7*>	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 <0-7> <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>]
```

Example

Note:

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

Configure the egress mapping for port 4/10 to an IEEE 802.1p bit of 3 to a QoS level of 3 and a DiffServ Code Point of 3 and a DS byte of 3 to a Diff-Serv code point of 101110:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#qos egressmap 1p 3 3
VSP-9012:1(config)#qos egressmap ds 3 101110
VSP-9012:1(config)#show qos egressmap 1p 3

================================================================================
                    Qos Egress QOS-Level to IEEE Priority Map
================================================================================
QOSLEVEL        IEEE1P
--------------------------------------------------------------------------------

3               3
```

Variable definitions

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

Table 18: Variable definitions

Variable	Value
1p *<0-7>* *<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 • level 7—7 The system reserves level 7 for Network Control. To use the default configuration, use the default option in the command: `default qos egressmap 1p`

Variable	Value
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`

Saving the configuration

After you change the configuration, you must save the changes to both the master and the standby CP modules. Save the configuration to a file to retain the configuration settings.

Before you begin

- To save a file to the standby CP module, you must enable the Trivial File Transfer Protocol (TFTP) on the standby CP module.

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 Privileged EXEC mode:

   ```
   enable
   ```

2. Save the running configuration:

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

Example

Save the file to the default location:

```
VSP-9012:1>enable
VSP-9012:1#save config
```

Variable definitions

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

Table 19: Variable definitions

Variable	Value
backup *WORD<1–99>*	Saves the specified file name and identifies the file as a backup file.

Variable	Value
	WORD uses one of the following formats: • a.b.c.d:<file> • /intflash/<file> • /extflash/<file> • /mnt/intflash/<file> to use the internal flash of the backup CP module • /mnt/extflash/<file> to use the external flash of the backup CP module • /usb/<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> • /extflash/<file> • /mnt/intflash/<file> to use the internal flash of the backup CP module • /mnt/extflash/<file> to use the external flash of the backup CP module • /usb/<file> The file name, including the directory structure, can include up to 99 characters.
standby *WORD<1–99>*	Saves the specified file name to the standby CPU in the following format: • /intflash/<file> • /extflash/<file> • /usb/ <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. You cannot use this variable if you enable HA mode.

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 (internal flash, external flash, USB, 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. If a single strand fiber (SSF) switchover occurs, the switch sends a warm-start management trap within 45 seconds of a restart.

Procedure

1. Enter 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.

3.

Example

Restart the switch:

```
VSP-9012:1>enable
VSP-9012:1>#boot
Are you sure you want to re-boot the switch (y/n) ? y
```

Chapter 7: QoS configuration using EDM

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

Configuring a QoS profile

Configure a QoS profile to configure preferences between unicast and multicast traffic during times of over subscription.

Procedure

1. In the Navigation tree, expand the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **System Flags** tab.
4. In **ProfileType**, select a QoS profile.
5. Click **Apply**.

System Flags field descriptions

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

Name	Description
EnableAccessPolicy	Activates access policies. The default is disabled.
MrouteStreamLimit	Activates or disables Mroute Stream Limit. The default is disabled.
ForceTrapSender	Configures circuitless IP as a trap originator. The default is disabled.
ForceIpHdrSender	If you enable Force IP Header Sender, the system matches the IP header source address with SNMP header sender networks. The default is disabled.
AuthSuccessTrapEnable	Enables the system to send the authentication success trap, rcnAuthenticationSuccess. The default is disabled.

Name	Description
	Note: You must also enable SNMP authentication traps. For more information on configuration of SNMP authentication traps, see *Troubleshooting Avaya Virtual Services Platform 9000,* NN46250-700.
ForceTopologyIpFlagEnable	Activates or disables the flag that configures the CLIP ID as the topology IP. Values are true or false. The default is disabled.
CircuitlessIpId	Uses the CLIP ID as the topology IP. Enter a value from 1–256.
ProfileType	Configures the system to give preference to one type of traffic over the other in times of over subscription. The values are: • balanced • unicastOptimized • multicastOptimized The default is balanced.
Lossless8021p	Specifies the lossless-802.1p value. The range is 0 to 6. The default is 3. **Note:** The internal QoS level that corresponds to the lossless 802.1p value must be 3. Avaya recommends that you do not use filters to remark the internal QoS level. When you enable lossless-PFC on a port, the port cannot become lossless-PFC if the lossless-802.1p value maps to an internal QoS level other than 3, or if the internal QoS level 3 maps to another 802.1p value. In a Lossless-PFC (802.1Qbb) domain, the lossless behavior is guaranteed as long as the Lossless 802.1p, ingress 1p to QoS map and the egress QoS to 1p map are consistent. When you change the Lossless 802.1p and ingress 1p to QoS map, you must configure the egress QoS to 1p map correctly. For more information about Lossless Ethernet, see *Network Design Reference for Avaya Virtual Services Platform 9000,* NN46250-200, and *Administering Avaya Virtual Services Platform 9000,* NN46250-600.
HaCpu	Activates or disables the CPU High Availability feature.

Name	Description
	If you enable or disable High Availability mode, the secondary CPU resets automatically to load settings from the saved configuration file. The default is enable.
HaCpuState	Indicates the CPU High Availability state. • initialization—Indicates the CPU is in this state. • oneWayActive—Specifies modules that need to synchronize register with the framework (either locally or a message received from a remote CPU). • twoWayActive—Specifies modules that need to synchronize register with the framework (either locally or a message received from a remote CPU). • synchronized—Specifies table-based synchronization is complete on the current CPU. • remoteIncompatible—Specifies CPU framework version is incompatible with the remote CPU. • error—Specifies if an invalid event is generated in a specific state the CPU enters Error state. • disabled—Specifies High Availability is not activated. • peerNotConnected—Specifies no established peer connection. • peerConnected—Specifies peer connection is established. • lostPeerConnection—Specifies a lost connection to peer or standby CPU. • notSynchronized—Specifies table-based synchronization is not complete.
HaEvent	Indicates the High Availability event status. • restart—Causes the state machine to restart. • systemRegistrationDone—Causes the CPU to transfer to One Way or Two Way Active state. • tableSynchronizationDone—Causes the CPU to transfer to synchronized state. • versionIncompatible—Causes the CPU to go to remote incompatible state • noEvent—Means no event occurred to date.
StandbyCpu	Indicates the state of the standby CPU.

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 Kbps.

   The peak rate must be greater than or equal to the service rate.
6. From **IngressRateSvc** , type the value for the service rate in Kbps.
7. Click **Apply**.

Configuring a policy-based policer

Use a QoS policy to configure peak and service policing rates. Use an access control entry (ACE) to apply the policy to traffic.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **QOS**.

2. Click **Policy**.
3. Click **Insert**.
4. Configure the name and ID as required.
5. Configure the peak and service rates.

   The peak rate must be greater than or equal to the service rate.
6. Click **Insert**.
7. Configure a filter to use the policy by using the Police parameter as you configure an ACE.

Policy field descriptions

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

Name	Description
PolicyId	Identifies a global policer (GP) ID value that corresponds to the local policer. Valid values range from 1–16000.
PeakRate	Identifies a local policer peak rate in Kb/s equal to the corresponding GP ID.
SvcRate	Identifies a local policer service rate in Kb/s equal to the corresponding GP ID.
Name	Specifies an administratively assigned name for this global policer.

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).

Saving the configuration

After you change the configuration, you must save the changes to both the master and the standby CP modules. You can save configuration changes or changes to the boot parameters. Save the configuration to a file to retain the configuration settings.

Procedure

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

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

Chapter 8: 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 9000 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 9000 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 9000.

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 9000 system is 2048.

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

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

The associations of the ingress and egress VLAN ACLs 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
- monitor-dst-vlan

The following figure shows the relationships between ACEs and ACLs.

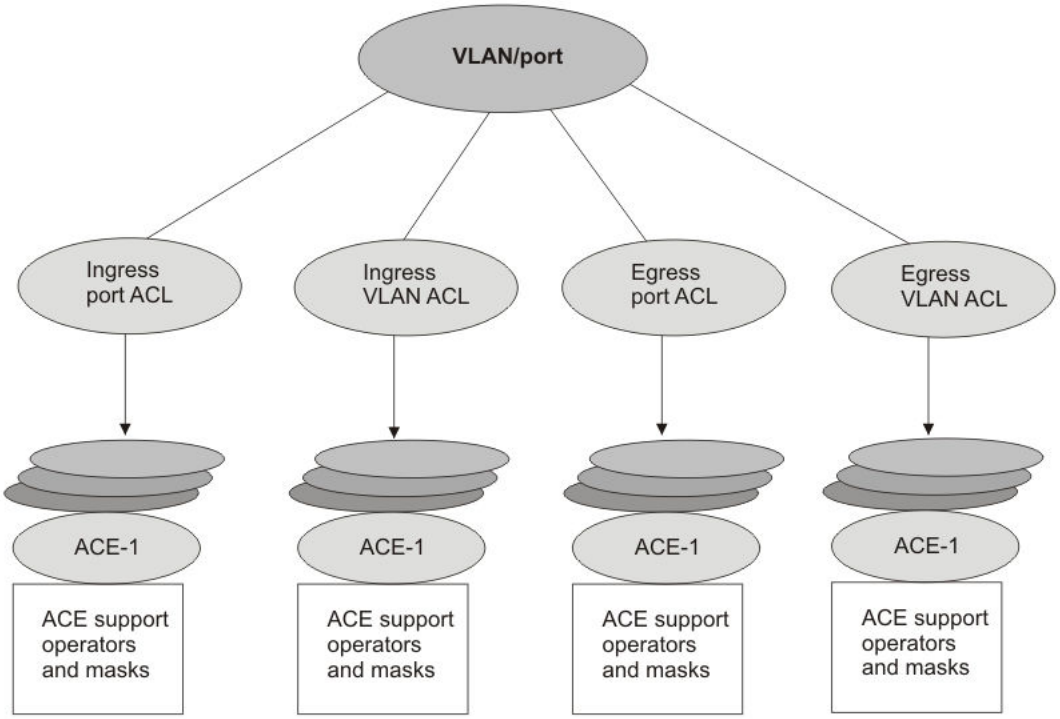


Figure 6: ACE and ACL relationships

Access control entries

The Virtual Services Platform 9000 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 of 16,000 ACEs globally and a maximum of 1000 ACEs 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 9000 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 0x0000ffffffff.

The following table explains the mask operator for MAC addresses.

Table 20: Mask operator for MAC address

Rule	Result

`filter acl ace ethernet 10 10 dst-mac mask 0x01:00:5e:00:00:01 24`
which is the same as
`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 21: Mask operator for IP address

Rule	Result

`filter acl ace ip 10 10 src-ip mask 2.10.10.12 24`
which is the same as
`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, for example, 2, and does not care about the value of the remaining 24 bits because they are 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.
	The mask appears as 0.255.255.255 in the command output for **`show filter acl config`**.

`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

Rule	Result
	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. If you use the mask value in decimal format <0–31> with an IP address, do not interpreted the mask as or associated with the subnet-mask in IP configuration. This mask value represents the least significant bits to treat as "do not care" and are ignored when matching filter attributes.

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

Table 22: 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 23: 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 6/5,9/11`
`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 log 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 5/13`
	Source IP: 192.168.4.1
	192.168.4.10
		Source IP:
		192.168.3.1
		192.168.4.32

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

`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`
	192.168.4.30
	192.168.4.31	

`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

IP mask (decimal notation):
`filter acl 10 type outport`
`filter acl port 10 5/13`
`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 5`
`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 2`
`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 6/2`
`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`
This mask implies packets with TCP source port 256–511 match the filter, while 0–255 and > 511 miss the filter.
	TCP source port 256
	TCP source port 356
	TCP source port 511
		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 24: Attribute list

Attribute Name	Operator
Slot/Port	Equal

Attribute Name	Operator
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
Protocol Type	Equal
Type of Service	Equal, Mask
IP Fragmentation	Equal
IP Options	Equal
TCP option	Equal
Layer 4 Destination Port	Equal, Mask
Layer 4 Source Port	Equal, Mask
TCP Flags	Equal
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 9000 performs a parallel search on both Security and QOS ACE lists, resulting in distinct and non-conflicting actions. The supported Virtual Services Platform 9000 actions are listed below.

Table 25: Security ACE Actions

Security ACE Actions	User supplied parameters	Comments
Mode	Permit or Deny	Applies to both ingress and egress ACLs.
PCAP	None	Packet Capture: A copy of the packet is sent to the secondary CPU. Applies to both ingress and egress ACL .

Security ACE Actions	User supplied parameters	Comments
Log	None	Packet header is logged and it can be seen using an ACLI command along with time stamp and actions taken. Applies to both ingress and egress ACLs.
• Redirect Next-Hop • Unreachable	IP address, Mode	Re-directs the packet to the user supplied IP address if the user supplied IP address is unreachable, the user may specify a mode action. If mode is Deny, the packet is dropped; else the packet forwarded as normal. Applies to ingress ACLs only.
MLT index	Index value	The user supplied index overrides the computed hash ID based on fields within the packet. Applies to ingress ACLs.
Count	None	Collect ACE statistics. Applies to ingress and egress ACLs.
Mirror	Port or list of ports, VLAN-ID, MLT-ID, or IP address	Applies to ingress and egress ACLs.

Table 26: QoS ACE Actions

QOS ACE Actions	User supplied parameters	Comments
Remark	• DCSP • .1P • Internal-qos	Applied to Ingress ACLs.
Police	Profile ID	Policer profile ID refers to a user defined profile. Applied on Ingress ACLs.
Count	None	Applied on Ingress/Egress ACLs.
Log	None	Packet header is logged and it can be seen using an ACLI command along with time stamp and actions taken. Applied to both Ingress/ Egress ACLs
IPFIX	None	Configures IPFIX metering. Applies to ingress ACLs. **Note:** Virtual Services Platform 9000 does not support IPFIX on Intermediate-System-to-

QOS ACE Actions	User supplied parameters	Comments
		Intermediate-System (IS-IS) interfaces.

Conflict and Precedence

The Virtual Services Platform 9000 supports both port-based and VLAN-based ACLs. As shown in Figure 6: ACE and ACL relationships on page 63, 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 9000 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 27: 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 ACE 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

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 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 Miss and ACL 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	VLAN-based ACL is not configured	VLAN-based ACL is not configured	No action is executed	No action is executed
Security ACE search is a Miss and ACE 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	Execute configured ACE and default ACL actions	No action is executed

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**
					result invalid.		
				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 ACE is mode is Permit	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 . Security search result invalid	QoS ACE search returns a Miss	No action is executed	Collect default Miss statistics
				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 is 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 is 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	VLAN-based ACL is not configured	VLAN-based ACL is not configured	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 28: Common ACE uses and configurations

Function	ACE configuration

Permit a specific host to access the network	• Use action permit.
	• 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 ip 1 5 src-ip eq 1.2.3.4`
	`filter acl ace 1 5 enable filter acl ace ethernet 1 5 ether-type eq ip`

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 ip 1 5 src-ip eq 1.2.3.4`
	`filter acl ace 1 5 enable filter acl ace ethernet 1 5 ether-type eq ip`

Permit a specific range of hosts to access the network	• Use action permit.
	• Configure the source IP address to be the range of host IP addresses.
	`filter acl ace 1 5 name "Permit_access_to_1.2.3.4-5.6.7.8" filter acl ace action 1 5 permit`
	`filter acl ace ip 1 5 src-ip eq 1.2.3.4-5.6.7.8 filter acl ace 1 5 enable filter acl ace ethernet 1 5 ether-type eq ip`

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 ip 1 5 ip-protocol-type eq tcp filter acl ace protocol`
	`1 5 dst-port eq 23 filter acl ace 1 5 enable filter acl ace ethernet`
	`1 5 ether-type eq ip`

Deny FTP traffic	• Use action deny.

Function	ACE configuration

	• 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 ip 1 5 ip-protocol-type eq tcp filter acl ace protocol 1 5 dst-port eq 21 filter acl ace 1 5 enable filter acl ace ethernet 1 5 ether-type eq ip`

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 and ACE configuration guidelines

Virtual Services Platform 9000 supports the maximum number of ACLs and ACEs listed in the following table.

Table 29: ACE and ACL scaling

Parameter	Maximum number
ACLs for each switch	2048
ACEs for each switch	16 000
ACEs for each ACL	1000 (all QoS, all security, or QoS and security combined)

Filter limitations

The following list identifies known filter limitations with Virtual Services Platform 9000:

- The system does not perform the ACE action to remark DSCP for bridged packets when action IP option is enabled.

- When an ACE with action count is disabled, the statistics associated with the ACE are reset.
- ACL filters cannot be applied to packets generated by the VSP 9000 such as BPDUs and OSPF Hellos.
- Only 1000 packets can be collected per line card using ACE Logging Action.
- Virtual Services Platform 9000 does not support IPFIX on Intermediate-System-to-Intermediate-System (IS-IS) interfaces.
- For port based filter if there are any ports on ROF card, then ignore the byte counts of filter ACL and ACE statistics.
- For VLAN based filter if any VLAN members are on ROF card, then ignore the byte counts of filter ACL and ACE statistics.

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.

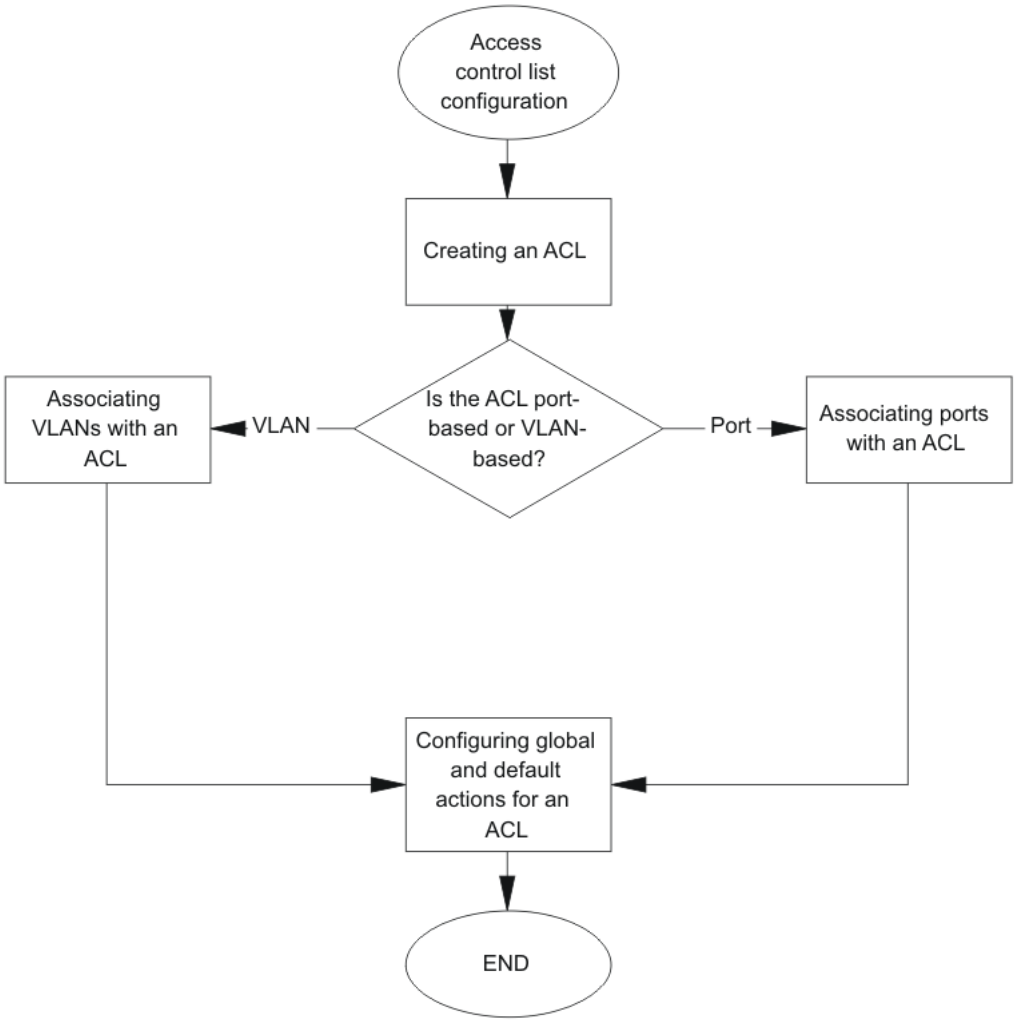


Figure 7: Access control list configuration using ACLI procedures

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|outVlan|inPort|outPort> [name
WORD<0-32>] [enable]
```

3. Ensure the configuration is correct:

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

Example

Create an ACL with the ID 1, with an ingress VLAN, with the name test:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#filter acl 1 type inVlan name test
VSP-9012:1(config)#show filter acl 3

================================================================================
                                Vlan ACL Table
================================================================================
Acl  Type    AclName             PktType State    # of Default CtrPkt Vlan
Id                                                ACEs Action  Rule   Id
--------------------------------------------------------------------------------
3    Ingress ACL-3               nonipv6 enabled  1    permit permit  5

================================================================================
                          Vlan ACL Global-Action Table
================================================================================
Acl  Type    Ipfix       Monitor     Monitor     Monitor
Id                       Dst-Mlt     Dst-Vlan    Dst-Port
--------------------------------------------------------------------------------
3    Ingress Disable     0           0

Displayed 1 of 1 Entries
```

Variable definitions

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

Table 30: 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|outVlan|inPort|outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outVlan and outPort are egress ACLs. A port-based ACL has precedence over a VLAN-based ACL.

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> <1-4084>
   ```

3. Remove specified VLAN interfaces from an ACL:

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

Example

Add VLAN 1 to ACL 1:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#filter acl vlan 1 1
```

Variable definitions

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

Table 31: Variable definitions

Variable	Value
<1-2048>	Specifies an ACL ID from 1–2048.
<1-4084>	Specifies the VLAN IDs from 1–4084. The system reserves VLAN IDs 4085–4096 for internal use.

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][,...]}
   ```

Example

Associate port 4/10 with ACL 2:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#filter acl port 2 4/10
```

Variable definitions

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

Table 32: 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 (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

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 [ipfix-enable|monitor-dst-mlt <1-512>|monitor-dst-ports {slot/port[-slot/port][,...]}|monitor-dst-vlan <1-4084>]
   ```

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

   ```
   default filter acl set <1-2048> global-action [ipfix-enable|monitor-dst-mlt|monitor-dst-ports|monitor-dst-vlan]
   ```

4. Configure the default action for an ACL:

   ```
   filter acl set <1-2048> default-action <permit|deny> [control-packet-action <permit|deny>]
   ```

5. Configure an ACL to the default action settings:

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

Example

Configure ACL 1 to mirror to destination VLAN 2 and specify the default action to deny when none of the ACEs match:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#filter acl set 1 global-action monitor-dst-vlan 2
VSP-9012:1(config)#filter acl set 1 default-action deny
```

Variable definitions

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

Table 33: Variable definitions

Variable	Value
<1-2048>	Specifies the ACL ID.
control-packet-action <permit|deny>	Protects control traffic when the port is in drop mode. The default is permit. You can only configure this variable if the default action is deny.
default-action <deny|permit>	Specifies the default action to take when none of the ACEs match. Options are <deny|permit>. The default is permit.
global-action ipfix-enable|monitor-dst-mlt *<1–512>*|monitor-dst-ports {slot/port[-slot/port][,...]}|monitor-dst-vlan *<1–4084>*	Specifies the global action to take for matching ACEs: • ipfix-enable—Configures IPFIX metering using filters to use IPFIX on selected flows. The default is disable. • monitor destination MLT—Configures mirroring to a destination MLT group.

Variable	Value
	• monitor destination ports—Configures mirroring to a destination port or ports. • monitor destination VLAN—Configures mirroring to a destination VLAN.

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
   ```

Example

Change the name of ACL 1 to test3:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#filter acl 1 name test3
```

Variable definitions

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

Table 34: 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|outVlan|inPort|outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outVlan 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
   ```

Example

Disable ACL 1:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#no filter acl 1 enable
```

Variable definitions

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

Table 35: 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|outVlan|inPort|outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outVlan 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>
```

Example

Reset ACL 2 to the default values:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#default filter acl 2
```

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|outVlan|inPort| outPort>	Specifies the ACL type. The values inVlan and inPort are ingress ACLs, and outVlan 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`.

Example

Delete ACL 1:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#no filter acl 1
WARNING: All ACE entries under this ACL will be Deleted.
Do you wish to delete this ACL? (y/n)? y
```

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 • outVlan • inPort • outPort **Important:** The inVlan and outVlan ACLs drop packets if you add a VLAN after ACE creation.
Name	Specifies a descriptive user-defined name for the ACL.
VlanList	For inVlan and outVlan 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. Deny means the system drops the packets; permit means the system forwards packets. The default is permit.
ControlPktAction	Specifies the action for control packets, if you configure DefaultAction to deny. If DefaultAction is permit, this value is ignored.
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. The default is IPv4.
IpfixState	Enables or disables the Internet Protocol Flow Information eXport (IPFIX) option on the ACL. Use IPFIX to monitor IP flows. The default is disabled.
MirrorVlanId	Configures mirroring to a destination VLAN.
MirrorMltId	Configures mirroring to a destination MLT group.
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.

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 1000 ACEs for each access control list (ACL). The system supports a maximum of 16 000 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 for filtering:

   ```
   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>
   ```

Example

Create a security ACE with ACL ID 1 and ACE ID 1 with the action mode permit:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#filter acl ace 1 1
VSP-9012:1(config)#filter acl ace action 1 1 permit
VSP-9012:1(config)#show filter acl ace 1 1

================================================================================
                          Ace Action Table (Part I)
================================================================================
Acl  Ace  AceName                 Admin   Oper    Mode   Mlt Remark  Remark
Id   Id                           State   State           Id DSCP    Dot1p
--------------------------------------------------------------------------------
1    1    ACE-1                   Disable Down    permit 0   disable disable

================================================================================
                          Ace Action Table (Part II)
================================================================================
Acl  Ace  Redirect                                Unreach Police  Internal
Id   Id   Next-Hop                                -able           Qos
--------------------------------------------------------------------------------
1    1    0.0.0.0                                 deny    0       0

================================================================================
                         Ace Action Table (Part III)
================================================================================
Acl  Ace  Ipfix   Count   Log     CopyTo  Monitor  Monitor   Monitor
Id   Id                          Pcap    Dst-Mlt  Dst-Vlan  Dst-Port
--------------------------------------------------------------------------------

1    1    disable disable disable disable 0        0

================================================================================
                          Ace Action Table (Part IV)
================================================================================
Acl  Ace  Monitor           Dscp     Ttl
Id   Id   Dst-Ip
--------------------------------------------------------------------------------
1    1    0.0.0.0           ----     ----


Displayed 1 of 1 Entries


================================================================================
                                ACE Arp Table
```

```
================================================================================
AclId  AceId  Operation
--------------------------------------------------------------------------------
1      1

Displayed 1 of 1 entries



================================================================================
                          ACE Ethernet Table (Part I)
================================================================================
Acl  Ace  Operator/             Operator/             Operator/
Id   Id   SourceMac             DestMac               PortList
--------------------------------------------------------------------------------
1    1

================================================================================
                          ACE Ethernet Table (Part II)
================================================================================
Acl  Ace  Operator/             Operator/             Operator/
Id   Id   EtherType             VlanId                VlanTagPrio
--------------------------------------------------------------------------------
1    1

Displayed 1 of 1 entries


================================================================================
                            ACE Ip Table (Part I)
================================================================================

Acl  Ace  Operator/          SourceIp        Operator/          DestIp
Id   Id   SourceIp           mask            DestIp             mask
--------------------------------------------------------------------------------
1    1

================================================================================
                            ACE Ip Table (Part II)
================================================================================
Acl  Ace  Ip     Operator/           Operator/           Operator/
Id   Id   Option IpFragFlag          IpProtoType         Dscp
--------------------------------------------------------------------------------
1    1

Displayed 1 of 1 entries


--More-- (q = quit)
```

Variable definitions

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

Table 37: Variable definitions

Variable	Value
<1-2048>	Specifies the ACL ID.

Variable	Value
<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.
- To use a policer, a policy must exist.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure ACE actions:

   ```
   filter acl ace action <1-2048> <1-2000> <deny|permit> [copy-to-pcap]
   [count] [internal-qos <0-7>] [ipfix-enable] [log] [mlt-index <1-16>]
   [monitor-dst-ip {A.B.C.D} [dscp <0-63>] [ttl <2-255>]] [monitor-dst-
   mlt <1-512>] [monitor-dst-ports {slot/port[-slot/port][,...]}]
   [monitor-dst-vlan <1-4084>] [police <1-16000>] [redirect-next-
   hop WORD<1-15>] [remark-dot1p <zero|one|two|three|four|five|six|
   seven>] [remark-dscp <phbcs0|phbcs1|phbaf11|phbaf12|phbaf13|phbcs2|
   phbaf21|phbaf22|phbaf23|phbcs3|phbaf31|phbaf32|phbaf33|phbcs4|
   phbaf41|phbaf42|phbaf43|phbcs5|phbcs6|phbef|phbcs7>]
   [unreachable <deny|permit>]
   ```

3. Ensure the configuration is correct:

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

Example

Configure a security ACE with ACL ID 1 and ACE ID 1 to permit Layer 3 mirroring to destination VLAN 100:

```
VSP-9012:1(config)#enable
VSP-9012:1(config)#configure terminal
VSP-9012:1(config)#filter acl ace action 1 1 permit monitor-dst-vlan 100
VSP-9012:1(config)#show filter acl ace 1 1

================================================================================
                          Ace Action Table (Part I)
================================================================================
Acl  Ace  AceName                 Admin   Oper    Mode   Mlt Remark  Remark
Id   Id                           State   State           Id DSCP    Dot1p
--------------------------------------------------------------------------------
1    1    ACE-1                   Disable Down    permit 0   disable disable

================================================================================
                          Ace Action Table (Part II)
================================================================================
Acl  Ace  Redirect                                Unreach Police  Internal
Id   Id   Next-Hop                                -able           Qos
--------------------------------------------------------------------------------
1    1    0.0.0.0                                 deny    0       0

================================================================================
                         Ace Action Table (Part III)
================================================================================
Acl  Ace  Ipfix   Count   Log     CopyTo  Monitor  Monitor   Monitor
Id   Id                          Pcap    Dst-Mlt  Dst-Vlan  Dst-Port
--------------------------------------------------------------------------------

--More-- (q = quit)
```

Variable definitions

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

Table 38: 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.
copy-to-pcap	This variable is a security action that sends a copy of the packet to the secondary CP module. The ACE ID must be in the range of 1–1000. The default is disabled.
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.

Variable	Value
	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.
internal-qos	This variable is a QoS action. The ACE ID must be in the range of 1001–2000. The default value is 1.
ipfix-enable	Configures IPFIX metering using filters to use IPFIX on selected flows. An ACL can have multiple ACEs and each ACE can have an action of ipfix-enable. The default value is disable. If multiple ACEs have actions of ipfix-enable, the system performs metering only once for a packet. A packet matches multiple ACEs because you configure the ACEs to match overlapping flows. IPFIX metering further categorizes this packet into a flow record based on the unique ipfix-handle. The packet matches n ACEs that correspond to n different ACE flows, but it is still a single IPFIX flow.
log	This action logs to the master CP module. Use this parameter with either a security or QoS ACE. The default is disabled.
mlt-index <*1-16*>	If you use this action, the ACE overrides the mlt-index chosen by the MLT algorithm for packets sent on MLT ports. The MLT index ranges from 1–16. If three ports exist in an MLT (for example, A, B, and C) and you specify an index of 6, the Virtual Services Platform 9000 applies the MOD function and chooses port C. If port C becomes nonoperational, the filtered packets exit the platform from port B. Multicast traffic does not support the MLT index. This variable is a security action. The ACE ID must be in the range of 1–1000.
monitor-dst-ip {A.B.C.D} [dscp<*0–63*>] [ttl <*2–255*>]	Configures Layer 3 mirroring. The destination must be an IP address {A.B.C.D}. The default DSCP is 256 (disabled) and the default TTL is 64. For Layer 3 mirroring, the last hop in the path from the mirrored port to the remote mirroring destination should be on a VLAN by itself. Avaya recommends that you configure the remote mirrored port in its own VLAN at the last hop to prevent flooding. The hops between the mirror source port and the last hop can be on the same VLAN or on different VLANs and the hops between the mirror source port and the last hop can connect through bridging or routing.
monitor-dst-mlt <*1–512*>	Configures mirroring to a destination MLT group. This action is a security action. The ACE ID must be in the range of 1–1000.

Variable	Value
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 (3/1), a range of slots and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).
monitor-dst-vlan <*1–4084*>	Configures mirroring to a destination VLAN. This action is a security action. The ACE ID must be in the range of 1–1000.
police <*1-16000*>	Polices the packet according to the specified policy ID (1–16000). A policy must exist. This action is a QoS action. The ACE ID must be in the range of 1001–2000.
redirect-next-hop WORD<1–45>	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 <zero|one|two|three|four|five|six|seven>	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.
unreachable <deny|permit>	Denies or permits packet dropping when the next-hop for the packet is unreachable. The default value is deny. This action is a security action. The ACE ID must be in the range of 1–1000.

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.
- You must configure the ACE ethertype.

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>
   ```

Example

Configure a security ACE with ACL ID 200 and ACE ID 200, and configure the ACE ethertype to eq ARP. Then, configure ACE 200 for ARP packets:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#filter acl ace ethernet 200 200 ether-type eq arp
VSP-9012:1(config)#filter acl ace arp 200 200 operation eq arprequest
VSP-9012:1(config)#show filter acl arp 200 200

================================================================================
                                ACE Arp Table
================================================================================
AclId  AceId  Operation
--------------------------------------------------------------------------------
200    200    eq arprequest

Displayed 1 of 1 entries
```

Variable definitions

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

Table 39: 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 <1-4084>
   ```

   OR

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

Example

Configure a QoS ACE 2000 for the destination MAC address of 00:00:00:00:00:12.

Configure security a security ACE 200 for ether-type eq ARP.

Configure a QoS ACE 10 for a port attribute on port 5/17.

```
VSP-9012:1(config)#filter acl ace ethernet 1 2000 dst-mac eq 00:00:00:00:00:12
VSP-9012:1(config)#filter acl ace ethernet 200 200 ether-type eq arp
VSP-9012:1(config)#filter acl ace ethernet 2 10 port eq 5/17

VSP-9012:1(config)#show filter acl ethernet

================================================================================
                          ACE Ethernet Table (Part I)
================================================================================
Acl  Ace  Operator/             Operator/             Operator/
Id   Id   SourceMac             DestMac               PortList
--------------------------------------------------------------------------------
1    2000                       eq 00:00:00:00:00:12
2    10                                               eq 5/17
200  200

================================================================================
                          ACE Ethernet Table (Part II)
================================================================================
Acl  Ace  Operator/             Operator/             Operator/
Id   Id   EtherType             VlanId                VlanTagPrio
--------------------------------------------------------------------------------
1    2000
2    10
200  200  eq arp

Displayed 3 of 3 entries

VSP-9012:1(config)#show filter acl ethernet 1 2000

================================================================================
                          ACE Ethernet Table (Part I)
================================================================================
Acl  Ace  Operator/             Operator/             Operator/
Id   Id   SourceMac             DestMac               PortList
--------------------------------------------------------------------------------
1    2000                       eq 00:00:00:00:00:12

================================================================================
                          ACE Ethernet Table (Part II)
================================================================================
Acl  Ace  Operator/             Operator/             Operator/
Id   Id   EtherType             VlanId                VlanTagPrio
--------------------------------------------------------------------------------
1    2000

Displayed 1 of 1 entries
```

Variable definitions

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

Table 40: 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.
<1–4084>	Specifies the VLAN or VLANs to match
{slot/port}	Identifies the slot and port
WORD<1–200>	Specifies an Ethertype 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 0x01:00:5e:00:00:01`
	`filter acl ace ethernet 10 10 dst-mac mask 0x01:00:5e:00:00:01 24`
	`filter acl ace ethernet 10 10 src-mac mask 0x01:00:5e:00:00:01 0xFFFFFFFF0000`

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

Configure ACE 201 to ether-type IP. Configure ACE 201 to the PHB name phbcs0.

Configure ACE 11 to ether-type IP. Configure the destination IP address attribute to 192.0.2.2.

Configure ACE 7 to ether-type IP. Configure ACE 7 for IP fragmentation to match anyFragment.

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#filter acl ace ethernet 5 201 ether-type eq ip
VSP-9012:1(config)#filter acl ace ip 5 201 dscp eq phbcs0
VSP-9012:1(config)#filter acl ace ethernet 6 11 ether-type eq ip
VSP-9012:1(config)#filter acl ace ip 6 11 dst-ip eq 192.0.2.2
VSP-9012:1(config)#filter acl ace ethernet 7 7 ether-type eq ip
VSP-9012:1(config)#filter acl ace ip 7 7 ip-frag-flag eq anyFragment
VSP-9012:1(config)#show filter acl ip

================================================================================
                            ACE Ip Table (Part I)
================================================================================
Acl  Ace  Operator/          SourceIp        Operator/          DestIp
Id   Id   SourceIp           mask            DestIp             mask
--------------------------------------------------------------------------------
1    2000
2    10
3    2
4    1
5    201
6    11                                      eq 192.0.2.2
7    7
8    22
200  200

================================================================================
                            ACE Ip Table (Part II)
================================================================================
Acl  Ace  Ip     Operator/           Operator/           Operator/
Id   Id   Option IpFragFlag          IpProtoType         Dscp
--------------------------------------------------------------------------------

1    2000
2    10
3    2
4    1                               eq tcp
5    201                                                 eq phbcs0
6    11
7    7          eq anyFragment
8    22   any
200  200
```

```
Displayed 9 of 9 entries

VSP-9012:1(config)#show filter acl ip 8 22

================================================================================
                            ACE Ip Table (Part I)
================================================================================
Acl  Ace  Operator/          SourceIp        Operator/          DestIp
Id   Id   SourceIp           mask            DestIp             mask
--------------------------------------------------------------------------------
8    22

================================================================================
                            ACE Ip Table (Part II)
================================================================================
Acl  Ace  Ip     Operator/            Operator/            Operator/
Id   Id   Option IpFragFlag           IpProtoType          Dscp
--------------------------------------------------------------------------------
8    22   any

Displayed 1 of 1 entries
```

Variable definitions

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

Table 41: 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

Variable	Value
	• phbaf13 • phbcs2 • phbaf21 • phbaf22 • phbaf23 • phbcs3 • phbaf31 • phbaf32 • 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 icmp, tcp, udp, ipsecesp, ipsecah, ospf, vrrp, snmp or undefined.
WORD<1–1024>	Specifies the destination or source IP address (a.b.c.d).

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

Create security ACE 400 with ethertype IP. Configure the IP protocol type for ICMP messages. Configure the security ACE 400 for ICMP message type attributes.

```
VSP-9012:>enable
VSP-9012:#configure terminal
VSP-9012:(config)#filter acl ace ethernet 9 400 ether-type eq ip
VSP-9012:1(config)#filter acl ace ip 9 400 ip-protocol-type eq icmp
VSP-9012:1(config)#filter acl ace protocol 9 400 icmp-msg-type eq 1

VSP-9012:1(config)#show filter acl protocol 9 400
================================================================================
                          ACE Protocol Table (Part I)
================================================================================
Acl  Ace  Operator/             Operator/
Id   Id   SrcPort               DstPort
--------------------------------------------------------------------------------
9    400

================================================================================
                          ACE Protocol Table (Part II)
================================================================================
Acl  Ace  Operator/             Operator/
Id   Id   TcpFlags              IcmpMsgType
--------------------------------------------------------------------------------
9    400                        eq 1

Displayed 1 of 1 entries
VSP-9012:1(config)#show filter acl protocol

================================================================================
                          ACE Protocol Table (Part I)
================================================================================
Acl  Ace  Operator/             Operator/
Id   Id   SrcPort               DstPort
--------------------------------------------------------------------------------
1    2000
2    10
3    2
4    1
5    201
6    11
7    7
8    22
9    400
10   501
11   500
12   700
200  200

================================================================================
                          ACE Protocol Table (Part II)

================================================================================
Acl  Ace  Operator/             Operator/
Id   Id   TcpFlags              IcmpMsgType
--------------------------------------------------------------------------------
1    2000
2    10
3    2
4    1
5    201
6    11
7    7
```

```
8     22
9     400                          eq 1
10    501
11    500
12    700   eq none
200   200

Displayed 13 of 13 entries
```

Variable definitions

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

Table 42: 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, bgp, hdot323, bootpServer, bootpClient, tftp, rip, 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 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>]
   ```

Example

Display the running configuration for ACL 30:

```
VSP-9012:1>enable
VSP-9012:1#configure terminal
VSP-9012:1(config)#show filter acl config 30

================================================================================
                          Filter ACL-ACE Configuration
================================================================================
--------------------------------------------------------------------------------

filter acl 30 type inVlan name "PBR"
filter acl set 30 default-action deny
filter acl vlan 30 151,1200
filter acl ace 30 50 name "ACE-50"
filter acl ace action 30 50 permit redirect-next-hop 172.31.254.51 count
filter acl ace ethernet 30 50 ether-type eq ip
filter acl ace 30 50 enable
```

Variable definitions

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

Table 43: 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.

Viewing filtered packets

You can log and display filtered packets for ingress and egress based ACLs to log packet headers and the relevant ACL and ACE actions. Configure logging as an ACE action on either security- or QoS-based ACEs.

Before you begin

- The ACE exists with an action of log.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Show the packet header and relevant filter information for logged packets:

   ```
   show filter acl log {slot/port[-slot/port][,...]} [<1-2048>] [<1-2000>]
   ```

3. Clear the filter log buffer on all slots:

   ```
   clear filter acl log
   ```

4. In the Global Configuration mode, allow the log buffer to wrap:

   ```
   filter acl log buffer-wrap
   ```

   This option is disabled by default, which means that logging stops after packets fill the log buffer

Example

Display the packet header and relevant filter information for logged packets on port 5/37:

```
VSP-9012:1(config)#show filter acl log 5/37
 ================================================================================
                                  Filter Log
 ================================================================================
Port = 5/37
------------
Index    : 1                            Time     : Fri Jul 09 20:05:10 2010 UTC
AclId    : 901                          AclName  : ACL-901
###Security Actions:
AceId    : 1                              AceName  : ACE-1
Mode     : permit    Count    : enable    Pcap     : disable
Unreach  : enable    Mirror   : disable   Mlt-Id   : 0

SrcMac : 00:00:00:00:00:01       DstMac : 00:00:00:00:00:02
Ether-Type: 0x8100   VlanId : 33     Dot1P : 4              IsTagged : Yes
  PktType : IPv4   DiffServ : 0x0    SrcIP : 4.4.4.4           DstIP: 1.1.1.1
Protocol : 114

###Packet Dump :
45 00 00 2a 00 00 00 00 40 72 70 59 04 04 04 04 01 01 01 01
00 01 e2 40 00 03 94 47 50 10 10 00 27 4f 5c 01 00 00 00 00
```

Variable definitions

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

Table 44: Variable definitions

Variable	Value
1–2000	Specifies an ACE ID.
1–2048	Specifies an ACL ID.
{slot/port[-slot/port][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (3/1), a range of slots

Variable	Value
	and ports (3/2-3/4), or a series of slots and ports (3/2,5/3,6/2).

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.
MltIndex	Specifies whether to override the MLT-index picked by the MLT algorithm when the system sends a packet from MLT ports. Valid values range from 0–16, with 0 as the default. Multicast traffic does not support the MLT index. Use this option to create a security ACE.
RedirectNextHop	Redirects matching IP traffic to the next hop. Use this option to create a security ACE.
RedirectUnreach	Configures the desired behavior for redirected traffic when the specified next hop is not reachable. The default value is deny. 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.
Police	Specifies the policer. Valid values range from 0–16000, with 0 (zero) as the default. When you do not want to use policing, configure the value to 0. Use this option to create a QoS ACE. The ACL must apply at ingress.

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.
MltIndex	If you use this action, the ACE overrides the mlt-index chosen by the MLT algorithm for packets sent on MLT ports. The MLT index ranges from 0–16. If three ports exist in an MLT (for example, A, B, and C) and you specify an index of 6, the Virtual Services Platform 9000 applies the MOD function and chooses port C. If port

Name	Description
	C becomes nonoperational, the filtered packets exit the platform from port B. Multicast traffic does not support the MLT index.This variable is a security action. The ACE ID must be in the rangeof 1–1000.
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.
Police	Polices the packet according to the specified policy ID (0–16000). A policy must exist. 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.
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. The default is 0.0.0.0.
RedirectUnreach	Denies or permits packet dropping when the next-hop for the packet is unreachable. The default value is deny. This action is a security action. The ACE ID must be in the range of 1–1000.
IpfixState	Configures IPFIX metering using filters to use IPFIX on selected flows. An ACL can have multiple ACEs and each ACE can have an action enable. The default is disable.
Count	Enables the ability to count matching packets. Use this parameter with either a security or QoS ACE. The default is disabled.
Log	This action logs to the master CP module. Use this parameter with either a security or QoS ACE. The default is disabled.

Name	Description
CopytoPcap	This variable is a security action that sends a copy of the packet to the secondary CP module. The ACE ID must be in the range of 1–1000. 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.
DstVlanId	Configures mirroring to a destination VLAN. This action is a security action. The ACE ID must be in the range of 1–1000.
DstMltdId	Configures mirroring to a destination MLT group. This action is a security action. The ACE ID must be in the range of 1–1000.
DstIp	Configures Layer 3 mirroring. The destination must be an IP address {A.B.C.D}. For Layer 3 mirroring, the last hop in the path from the mirrored port to the remote mirroring destination should be on a VLAN by itself. Avaya recommends that you configure the remote mirrored port in its own VLAN at the last hop to prevent flooding. The hops between the mirror source port and the last hop can be on the same VLAN or on different VLANs and the hops between the mirror source port and the last hop can connect through bridging or routing.
DstIpDscp	Optionally, if you configure a destination IP address for mirroring, you can also configure the DSCP value. The **DstIpDscp** range is <0–63>. The default is 256 (disabled).
DstIpTtl	Optionally, if you configure a destination IP address for mirroring, you can also configure the time-to-live value. The **DstIpTtl** range is <2–255>. The default is 64.

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 45: 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 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 46: 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.

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**.

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 • 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.
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 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.
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, icmp, tcp, udp, ipsecesp, ipsecah, ospf, vrrp, and undefined.

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**.

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 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, bgp, 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.

Configuring the packet log

Configure the packet log to clear the log or to allow the buffer to wrap.

Before you begin

- The ACE exists with an action of log.

About this task

You can log and display filtered packets for ingress and egress based ACLs to log packet headers and the relevant ACL and ACE actions. Configure logging as an ACE action on either security- or QoS-based ACEs.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **Advanced Filters (ACE/ACLs)**.
3. Click the **Log** tab.
4. Optionally, click **ClearLog** to erase the current log entries.
5. Select **BufferWrap** to permit the buffer to wrap.
6. Click **Apply**.

Log field descriptions

Use the information in the following table to use the **Log** tab.

Name	Description
BufferWrap	Permits the buffer to wrap and logging to continue. This option is disabled by default, which means that logging stops after packets fill the log buffer.

Chapter 13: 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
- Internet Group Management Protocol (IGMP) 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 4/24-4/25,8/37
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 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 action 1 3 deny
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 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 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 action 1 6 deny
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 action 1 7 deny
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 action 1 8 deny
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 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 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 4/24-4/25,8/37
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 4/46
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 4/33
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 1802 type outVlan name "NICE-CLS_ACL-out"
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 1804 type outVlan name "BASIM_LIMITED-out"
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 4/46
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 1802 type outVlan name "NICE-CLS_ACL-out"
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 1804 type outVlan name "BASIM_LIMITED-out"
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
```

Glossary

access control entry (ACE)	One of the filter rules that comprise an access control list (ACL). An ACE statement defines pattern match criteria for a packet and the desired behavior for packets that carry the pattern. When the packets match an ACE rule, the specified action executes.
access control list (ACL)	An ordered list of filter rules referred to as access control entries. The ACEs provide specific actions, such as dropping packets within a specified IP range, or a specific Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port or port range. When an ingress or egress packet meets the match criteria specified in one or more ACEs within an ACL, the corresponding action executes.
Avaya command line interface (ACLI)	A textual user interface. When you use ACLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.
Circuitless IP (CLIP)	A CLIP is often called a loopback and is a virtual interface that does not map to any physical interface.
class of service (CoS)	A method used to manage traffic congestion based on the CoS level assigned to the packet.
constant bit rate (CBR)	A data service that conveys bits regularly in time and at a constant rate, between source (transmitter) and sink (receiver), for example, follows a timing source or clock.
Control Processor (CP) module	The Control Processor module runs all high level protocols (BGP, OSPF) and distributes the results (routing updates) to the rest of the system. The CP manages and configures the IO and Switch Fabric modules, and maintains and monitors the health of the chassis.
Differentiated Services Code Point (DSCP)	The first six bits of the DS field. The DSCP uses packet marking to guarantee a fixed percentage of total bandwidth to each of several applications (guarantees quality of service).
DiffServ (DS) boundary or access point	The edge of a DS domain in which classifiers and traffic conditioners are deployed.

Enterprise Device Manager (EDM)	A Web-based embedded management system to support single-element management. EDM provides complete configuration management functionality for the supported devices and is supplied to the customer as embedded software in the device.
expedited forwarding per hop behavior (PHB)	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.
I/O module	An I/O module is a module that provides network connectivity for various media (sometimes called Layer 0) and protocol types. I/O modules are also called Ethernet modules.
Institute of Electrical and Electronics Engineers (IEEE)	An international professional society that issues standards and is a member of the American National Standards Institute, the International Standards Institute, and the International Standards Organization.
Internet Control Message Protocol (ICMP)	A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.
Internet Group Management Protocol (IGMP)	IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.
Internet Protocol Flow Information eXport (IPFIX)	An IETF standard that improves the Netflow V9 protocol. IPFIX monitors IP flows.
jitter	The delay variance between received packets. Packets may not arrive at the destination address in consecutive order, or on a timely basis, and the signal can vary from its original reference timing. This distortion damages multimedia traffic.
latency	The time between when a node sends a message and receipt of the message by another node; also referred to as propagation delay.
Layer 2	Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.
Layer 3	Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).
Layer 4	The Transport Layer of the OSI model. An example of a Layer 4 protocol is Transmission Control Protocol (TCP).
marking	A process that uses defined rules to assign the Differentiated Services Code Point (DSCP) in a packet.

mask	A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.
maximum burst size (MBS)	One of a set of traffic characterization values that defines traffic characteristics through the traffic descriptor types. Maximum Burst Size defines the length in cells of a traffic burst relative to the peak cell rate (PCR).
media	A substance that transmits data between ports; usually fiber optic cables or category 5 unshielded twisted pair (UTP) copper wires.
Media Access Control (MAC)	Arbitrates access to and from a shared medium.
microflow	A single instance of an application-to-application packet flow identified by source address, destination address, protocol ID, and source port.
MultiLink Trunking (MLT)	A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.
Network Basic Input/ Output System (NetBIOS)	An application programming interface (API) that augments the DOS BIOS by adding special functions for Local Area Networks (LAN).
next hop	The next hop to which a packet can be sent to advance the packet to the destination.
operation, administration, and maintenance (OA&M)	All the tasks necessary for providing, maintaining, or modifying switching system services.
Packet Capture Tool (PCAP)	A data packet capture tool that captures ingress and egress (on Ethernet modules only) packets on selected ports. You can analyze captured packets for troubleshooting purposes.
packet loss	Expressed as a percentage of packets dropped over a specified interval. Keep packet loss to a minimum to deliver effective IP telephony and IP video services.
per-hop behavior (PHB)	A traffic class forwarding treatment based on criteria defined in the DiffServ field.
policing	Ensures that a traffic stream follows the domain service-provisioning policy or service-level agreement (SLA).
port	A physical interface that transmits and receives data.

port mirroring	A feature that sends received or transmitted traffic to a second destination.
quality of service (QoS)	QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.
remarking	Changes the Differentiated Services Code Point (DSCP) of a packet, in accordance with a service level agreement (SLA).
Reverse Address Resolution Protocol (RARP)	A protocol that maintains a database of mappings between physical hardware addresses and IP addresses.
Routing Information Protocol (RIP)	A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. You often use RIP as a very simple interior gateway protocol (IGP) within small networks.
Secure Shell (SSH)	SSH uses encryption to provide security for remote logons and data transfer over the Internet.
Simple Network Management Protocol (SNMP)	SNMP administratively monitors network performance through agents and management stations.
traffic profile	The temporal properties of a traffic stream, such as rate.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.
trunk	A logical group of ports that behaves like a single large port.
trunk port	A port that connects to the service provider network such as the MPLS environment.
type of service (TOS)	A field in the IPv4 header that determines the Class of Service prior to the standardization of Differentiated Services.
User Datagram Protocol (UDP)	In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.
variable bit rate	The capability of the encoding algorithm to dynamically switch between 32 and 24 kbytes/s.
virtual router	An abstract object managed by the Virtual Router Redundancy Protocol (VRRP) that acts as a default router for hosts on a shared LAN.

virtual router forwarding (VRF)	Provides traffic isolation between customers operating over the same node. Each virtual router emulates the behavior of a dedicated hardware router by providing separate routing functionality, and the network treats each VRF as a separate physical router.
Virtual Router Redundancy Protocol (VRRP)	A protocol used in static routing configurations, typically at the edge of the network. This protocol operates on multiple routers on an IP subnet and elects a primary gateway router. When the primary router fails, a backup router is quickly available to take its place.
Voice over IP (VOIP)	The technology that delivers voice information in digital form in discrete packets using the Internet Protocol (IP) rather than the traditional circuit-committed protocols of the public switched telephone network (PSTN).
Weighted Random Early Detection (WRED)	A mechanism that provides congestion avoidance capabilities. The basic operating philosophy of WRED is that it detects the onset of congestion and starts dropping packets in random fashion before queue overflow leads to tail drops.
weighted round robin (WRR)	A mechanism that uses the packet transmission opportunity (PTO) of a queue to determine which queue to process first.