Release Notes - Release 3.0.0.0
Avaya Virtual Services Platform 4000

Release 3.0.0.0
NN46251-401
Issue 01.02
November 2013

© 2013 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 generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by 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 its hardware and Software (“Product(s)”). 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. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; 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. “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.

Licence types

Designated System(s) License (DS). End User may install and use each copy 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, 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”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation 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 that 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”). 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 Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. 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. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 7
- Purpose 7
- Related resources 7
- Support 10

Chapter 2: New in this release 11
- Features 11

Chapter 3: Important notices 21
- Hardware compatibility 21
- Software scaling capabilities 24
- File names for this release 26
- Upgrading the software 27
- Deleting a software release 28
- Important information and restrictions 29
  - Interoperability notes for VSP 4000 connecting to an ERS 8800 29
  - Supported browsers 29
  - User configurable SSL certificates 30
  - Feature licensing 30
  - Combination ports 30
  - SFP and SFP+ ports 31

Chapter 4: Supported standards, RFCs, and MIBs 33
- Supported IEEE standards 33
- Supported RFCs 34
- Quality of service 35
- Network management 36
- MIBs 37
- Standard MIBs 38
- Proprietary MIBs 41

Chapter 5: Known issues and limitations 43
- Known issues 43
  - Device related issues 43
  - EDM related issues 45
- Limitations 46

Chapter 6: Resolved issues 47

Chapter 1: Introduction

Purpose

This document describes important information about this first release of the Virtual Services Platform 4000 (VSP 4000). These Release Notes include supported hardware and software, scaling capabilities, and a list of known issues (including workarounds where appropriate). This document also describes known limitations and expected behaviors that may first appear to be issues.

Related resources

Related topics:

Documentation on page 7
Training on page 7
Avaya Mentor videos on page 8

Documentation

See the *Avaya Virtual Services Platform 4000 Documentation Roadmap*, NN46251–100 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 Web site at http://avaya-learning.com/.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://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 site.

Subscribing to e-notifications

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

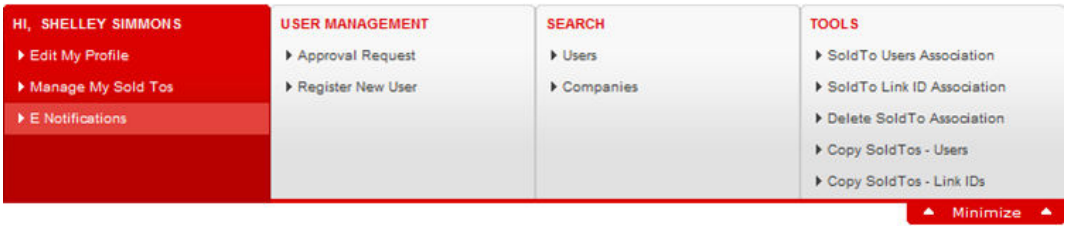
About this task

You can subscribe to different types of general notifications, for example, Product Correction Notices (PCN), that apply to any product or a specific product. You can also subscribe to specific types of documentation for a specific product, for example, Application & Technical Notes for Ethernet Routing Switch 8800.

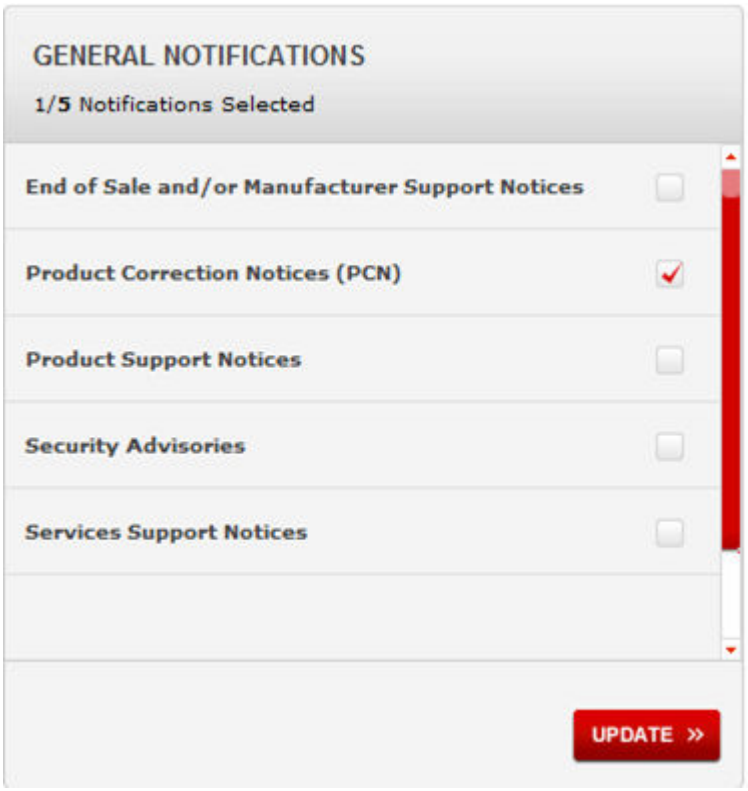
Procedure

1. In an Internet browser, go to https://support.avaya.com
2. Type your username and password, and then click **LOG IN**.
3. Click **MY PROFILE**.

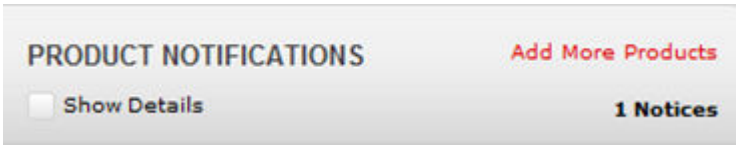
4. On the site toolbar, click your name, and then select **E Notifications**.



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

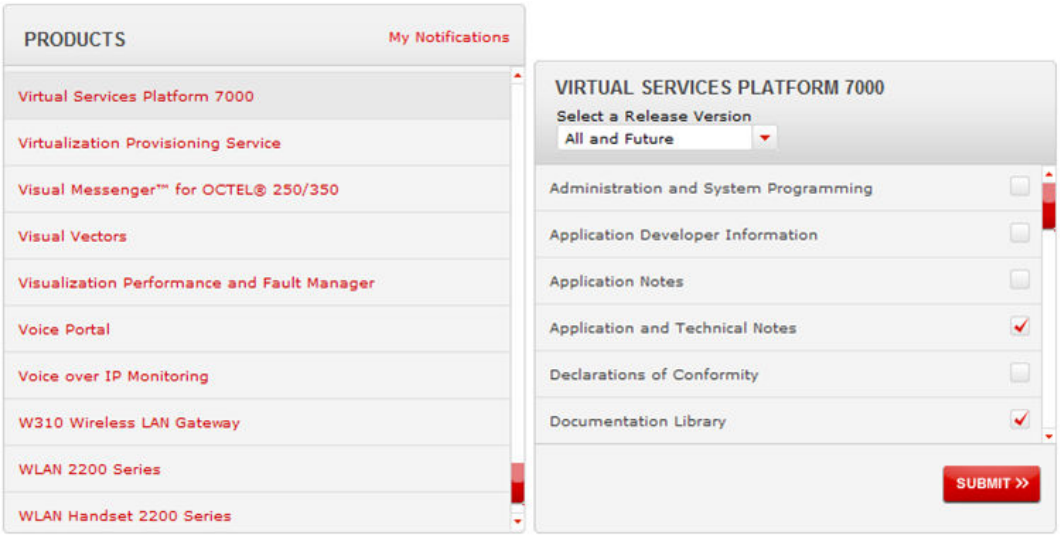


6. Click **OK**.
7. In the PRODUCT NOTIFICATIONS area, click **Add More Products**.



8. Scroll through the list, and then select the product name.
9. Select a release version.

10. Select the check box next to the required documentation types.



11. Click **Submit**.

Support

Visit 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.

Chapter 2: New in this release

Avaya Virtual Services Platform 4000 Release Notes, NN46251–401 is a new document for release 3.0.0.0 so all the features are new in this release.

Features

See the following sections for information about VSP 4000 features for release 3.0.0.0.

9k Jumbo packet support

Avaya VSP 4000 supports jumbo packets.

Jumbo packets and large packets are useful in server and storage over Ethernet applications. If the payload to header relation increases in a packet, the bandwidth can be used more efficiently. For this reason, increasing Ethernet frame size is a logical option. To transmit large amounts of data efficiently and minimize the task load on a server CPU, Avaya Virtual Services Platform 4000 supports Ethernet frames as large as 9600 bytes, compared to the standard 1518 bytes. For more information, see *Avaya Virtual Services Platform 4000 – Administration* (NN46251–600).

IEEE 802.1p/q Virtual LAN

Avaya Virtual Services Platform 4000 supports IEEE 802.1p/q based Virtual LAN.

A Virtual LAN (VLAN) is a switched network that is logically segmented by functions, project teams, or applications without regard to the physical location of users. By using a VLAN, you can divide the Local Area Network into smaller groups without interfering with the physical network.

The practical applications of VLAN include the following:

- create VLANs, or workgroups, for common interest groups
- create VLANs, or workgroups, for specific types of network traffic
- add, move, or delete members from these workgroups without making physical changes to the network

By dividing the network into separate VLANs, you can create separate broadcast domains. This arrangement conserves bandwidth, especially in networks supporting broadcast and multicast applications that flood the network with traffic. A VLAN workgroup can include members from a number of dispersed physical segments on the network, improving traffic flow between them. For more information, see *Avaya Virtual Services Platform 4000 Configuration – VLANs and Spanning Tree* (NN46251–500).

Port and Protocol-based VLANs

Avaya VSP 4000 supports port-based and protocol-based VLANs.

A port-based VLAN is a VLAN in which you explicitly configure the ports to be in the VLAN. When you create a port-based VLAN on a device, you assign a VLAN identification number (VLAN ID) and specify the ports that belong to the VLAN. These port members are always active port members. The VLAN ID is used to coordinate VLANs across multiple switches. Any type of frame can be classified to a port-based VLAN.

Protocol-based VLANs are an effective way to segment your network into broadcast domains according to the network protocols in use. A port member of a port-based VLAN can belong to multiple protocol-based VLANs. Port tagging is not required for a port to be a member of multiple protocol-based VLANs. The Virtual Services Platform 4000 supports IPv6 protocol-based VLAN only.

For more information, see *Avaya Virtual Services Platform 4000 Configuration – VLANs and Spanning Tree* (NN46251–500).

IEEE 802.1d Mac Bridges Spanning Tree

Avaya Virtual Services Platform 4000 supports IEEE 802.1d Mac Bridges based spanning trees.

Spanning Tree protocols detect and eliminate logical loops in a bridged or switched network. If multiple paths exist, the spanning tree algorithm configures the network so that a bridge or device uses the root bridge path based on hop counts. Although link speed is taken into account, the path is based on the root bridge rather than on an optimized path. If that path fails, the protocol automatically reconfigures the network and makes another path active, thereby sustaining network operations. Virtual Services Platform 4000 supports RSTP and MSTP but can downgrade a port automatically if it receives an STP Bridge Protocol Data Unit (BPDU) from a switch that runs STP. For more information, see *Avaya Virtual Services Platform 4000 Configuration – VLANs and Spanning Tree* (NN46251–500).

IEEE 802.1w RSTP

Avaya Virtual Services Platform 4000 supports IEEE 802.1w based Rapid Spanning Tree Protocol (RSTP).

The Rapid Spanning Tree Protocol (RSTP or IEEE 802.1w) reduces the recovery time after a network breakdown. It also maintains backward compatibility with IEEE 802.1d (the spanning tree implementation prior to RSTP). In certain configurations, the recovery time of RSTP can be reduced to less than 1 second. RSTP also reduces the amount of flooding in the network by enhancing the way Topology Change Notification (TCN) packets are generated. For more information, see *Avaya Virtual Services Platform 4000 Configuration – VLANs and Spanning Tree* (NN46251–500).

IEEE 802.1s MSTP

Avaya Virtual Services Platform 4000 supports IEEE 802.1s based Multiple Spanning Tree Protocol (MSTP).

With Multiple Spanning Tree Protocol (MSTP or IEEE 802.1s), you can configure multiple instances or Spanning Tree groups on the same device. Each instance or Spanning Tree group can include one or more VLANs. For more information, see *Avaya Virtual Services Platform 4000 Configuration – VLANs and Spanning Tree* (NN46251–500).

MLT (Multilink trunking)

Avaya Virtual Services Platform 4000 supports MultiLink Trunking (MLT).

MultiLink Trunking (MLT) is a point-to-point connection that aggregates multiple ports to logically act like a single port with aggregated bandwidth. Grouping multiple ports into a logical link provides a higher aggregate on a switch-to-switch or switch-to-server application. For more information, see *Avaya Virtual Services Platform 4000 Configuration – Link Aggregation and MLT* (NN46251-503).

IEEE 802.1ax (802.3ad) Link Aggregation Control Protocol (LACP)

Avaya Virtual Services Platform 4000 supports IEEE 802.1ax (802.3ad) based Link Aggregation Control Protocol.

IEEE 802.3ad based link aggregation, through the Link Aggregation Control Protocol (LACP), dynamically aggregates links as they become available to a trunk group. Link Aggregation Control Protocol dynamically detects whether links can be aggregated into a link aggregation group (LAG) and does so after links become available. Link Aggregation Control Protocol also provides link integrity checking at Layer 2 for all links within the LAG. For more information, see *Avaya Virtual Services Platform 4000 Configuration – Link Aggregation and MLT* (NN46251-503).

Virtual LACP (VLACP) End-to-End connectivity check

Avaya Virtual Services Platform 4000 supports Virtual LACP (VLACP) End-to-End connectivity check.

Use Virtual Link Aggregation Control Protocol (VLACP) as an extension to LACP for end-to-end failure detection. VLACP is not a link aggregation protocol, it is a mechanism to periodically check the end-to-end health of a point-to-point connection. VLACP uses the Hello mechanism of LACP to periodically send Hello packets to ensure end-to-end communication. When Hello packets are not received, VLACP transitions to a failure state, which indicates a service provider failure and that the port is disabled.

The VLACP only works for port-to-port communications where there is a guarantee for a logical port-to-port match through the service provider. VLACP does not work for port-to-multiport communications where there is no guarantee for a point-to-point match through the service provider. You can configure VLACP on a port. For more information, see *Avaya Virtual Services Platform 4000 Configuration – Link Aggregation and MLT* (NN46251-503).

Simple Loop Prevention Protocol (SLPP)

Avaya Virtual Services Platform 4000 supports Simple Loop Prevention Protocol (SLPP).

Use Simple Loop Prevention Protocol (SLPP) to protect against network loops. SLPP uses a small hello packet to detect network loops. The SLPP protocol checks packets from the originating switch and the peer switch in a SMLT configuration. Sending hello packets on a per VLAN basis allows SLPP to detect VLAN based network loops for un-tagged as well as tagged IEEE 802.1q VLAN link configurations. Once a loop is detected, the port is shutdown. For more information, see *Avaya Virtual Services Platform 4000 – Command Line Reference Guide* (NN46251–104).

Diffserv framework

Avaya Virtual Services Platform 4000 supports Diffserv framework.

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 per hop behaviours (PHBs) on network core devices, which includes queueing and dropping traffic. For more information, see *Avaya Virtual Services Platform 4000 Configuration – QoS and ACL-Based Traffic Filtering* (NN46251–502).

Ingress port policers

Avaya Virtual Services Platform 4000 QoS implementation uses ingress port policers to limit the number of packets in a stream that matches a particular classification. For more information, see *Avaya Virtual Services Platform 4000 Configuration – QoS and ACL-Based Traffic Filtering* (NN46251–502).

Egress port shapers

Avaya Virtual Services Platform 4000 QoS implementation uses egress port shapers to delay and transmit packets to produce an even and predictable flow rate. For more information, see *Avaya Virtual Services Platform 4000 Configuration – QoS and ACL-Based Traffic Filtering* (NN46251–502).

IP Brouter port

Avaya Virtual Services Platform 4000 supports IP Brouter port.

A brouter port is a one-port VLAN with an IP interface. The difference between a brouter port and a standard IP protocol-based VLAN configured to perform routing is that the routing interface of the brouter port is not subject to the spanning tree state of the port. A brouter port can be in the blocking state for nonroutable traffic and still route IP traffic. Because a brouter port is a single-port VLAN, it uses one VLAN ID. Each brouter port decreases the number of available VLANs by one. For more information, see *Avaya Virtual Services Platform 4000 Configuration – VLANs and Spanning Tree* (NN46251–500).

ARP and RARP

Avaya Virtual Services Platform 4000 supports ARP and RARP.

Network stations using the IP protocol need both a physical address and an IP address to transmit a packet. In situations where the station knows only the network host IP address, the network station uses Address Resolution Protocol (ARP) to determine the physical address for a network host by binding a 32-bit IP address to a 48-bit MAC address. A network station can use ARP across a single network only, and the network hardware must support physical broadcasts.

In situations where the station knows only the physical address, the network station uses Reverse Address Resolution Protocol (RARP) to determine the network host IP address for a network host.

For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

FTP Server

Avaya Virtual Services Platform 4000 supports File Transfer Protocol (FTP).

File Transfer Protocol (FTP) is used to transfer files between devices over a network. The FTP server processes file transfer requests from FTP clients and allows other authorized clients to access these files. The FTP server authenticates the client by prompting for a username and password before the client can transfer files. For more information, see *Avaya Virtual Services Platform 4000 – Administration* (NN46251–600).

TFTP Client & Server

Avaya Virtual Services Platform 4000 supports Trivial File Transfer Protocol (TFTP).

Trivial File Transfer Protocol (TFTP) is a simplified file transfer protocol used to transfer files of small size between devices over a network. TFTP connects two network devices using the client-server model but does not authenticate teh clients to connect to the server. The TFTP client sends file transfer requests to the TFTP server that allows other clients to access these files. TFTP uses UDP for transporting data. For more information, see *Avaya Virtual Services Platform 4000 – Administration* (NN46251–600).

HTTP & HTTPS EDM management

Avaya Virtual Services Platform 4000 supports management of the switch through HTTP and HTTPs using the Enterprise Device Manager (EDM). For more information, see *Avaya Virtual Services Platform 4000 – User Interface Fundamentals* (NN46251–103).

Simple Network Management Protocol SNMP v1, v2, v3

Avaya VSP 4000 supports Simple Network Management Protocol (SNMP) — SNMPv1, SNMPv2, and SNMPv3. This protocol is traditionally used to monitor Unix systems, Windows systems, printers, modem racks, switches, routers, power supplies, Web servers, and databases. Any device that runs software that can retrieve SNMP information can be monitored.

You can also use SNMP to change the state of SNMP-devices. For example, you can use SNMP to shut down an interface on your device. For more information, see *Avaya Virtual Services Platform 4000 – Security* (NN46251–601).

Secure Shell (SSHv1 & SSHv2) and Secure Copy (SCP) Server

Avaya VSP 4000 supports Secure Shell (SSHv1 and SSHv2) and Secure Copy (SCP) servers.

Secure Shell (SSH) is a client and server protocol that specifies the way to conduct secure communications over a network. Secure Copy (SCP) is a secure file transfer protocol. SCP is off by default, but you turn it on when you enable SSH using the config bootconfig flags command. The traffic these utilities generate is not encrypted when using other methods of remote access such as Telnet or FTP. Anyone that can see the network traffic can see all data, including passwords and user names. Secure Shell can replace Telnet and other remote login utilities. Secure Copy can replace FTP with an encrypted alternative. For more information, see *Avaya Virtual Services Platform 4000 – Administration* (NN46251–600).

Telnet client and server

Avaya VSP 4000 supports telnet client and server model.

Telnet is used to remotely access a device from another device as if it were locally connected. The Telnet client is the user interface that processes user commands entered from the user device and displays the output from the remote machine. The Telnet server runs on a remote computer and allows users to set up remote sessions. For more information, see *Avaya Virtual Services Platform 4000 – Administration* (NN46251–600).

Equal Cost MultiPath (ECMP)

With Equal Cost Multipath (ECMP), Avaya VSP 4000 can determine up to four equal-cost paths to the same destination prefix. You can use multiple paths for load sharing of traffic. These multiple paths allow faster convergence to other active paths in case of network failure. By maximizing load sharing among equal-cost paths, you can use your links between routers more efficiently when sending IP traffic. Equal Cost Multipath is formed using routes from the same source or protocol.

The ECMP feature supports and complements the following protocols and route types:

- Static route
- Default route

For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

Virtual Router Redundancy Protocol (VRRP)

Avaya VSP 4000 supports Virtual Router Redundancy Protocol (VRRP).

The Virtual Router Redundancy Protocol (VRRP) (RFC 2338) eliminates the single point of failure that can occur when the single static default gateway router for an end station is lost. For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

DHCP Relay agent

Avaya VSP 4000 supports the DHCP Relay agent.

The DHCP Relay Agent feature enables routers to relay DHCP broadcast messages to and from DHCP servers and clients located in different subnets within a large network. For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

IP Static routes

Avaya VSP 4000 supports IP static routes. A static route is a route to a destination IP address that you manually create.

The Layer 3 redundancy feature supports the creation of static routes to enhance network stability. Use the local next hop option to configure a static route with or without local next hop. For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

Virtual Routing Forwarding (VRF) Lite (24 instances)

Avaya VSP 4000 supports Virtual Routing Forwarding (VRF) Lite.

Use VRF Lite to offer networking capabilities and traffic isolation to customers that operate over the same node (router). Each virtual router emulates the behavior of a dedicated hardware router; the network treats each virtual router as a separate physical router. In effect, you can perform the functions of many routers using a single platform that runs VRF Lite. With multicast virtualization, the Virtual Services Platform 4000 also functions as multiple virtual multicast routers. The result is a substantial reduction in the cost associated with providing routing and traffic isolation for multiple clients. For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

Flight Recorder for system health monitoring

Avaya VSP 4000 supports the Flight Recorder for system health monitoring feature.

The Flight Recorder is a high level term for the framework in place on Virtual Services Platform 4000 to store both history and current state information for various kernel, system, and application data with minimal overhead to execution. This data can later be accessed on-demand when debugging systems issues to give engineers the best possible troubleshooting information. Functionally, the Flight Recorder consists of two elements; Persistent Memory and Always-on Trace. For more information, see *Avaya Virtual Services Platform 4000 – Troubleshooting* (NN46251-700).

Enterprise Device Manager (EDM)

Enterprise Device Manager (EDM) is a Web-based graphical user interface (GUI) you can use to configure a single Virtual Services Platform 4000. EDM runs from Virtual Services Platform 4000 and you can access it from a Web browser. You do not need to install additional client software, and you can access it with all operating systems. Virtual Services Platform 4000 3.0.0.0 is supported by COM 3.0.2. Install Configuration and Orchestration Manager (COM) on a remote server to configure multiple devices through one interface. For more information on COM documentation, see http://support.avaya.com.

Avaya CLI (ACLI)

Avaya Command Line Interface (ACLI) is an industry standard command line interface that you can use for single-device management across Avaya products. Virtual Services Platform 4000 3.0.0.0 is supported by COM 3.0.2. Install Configuration and Orchestration Manager (COM) on a remote server to configure multiple devices through one interface. For more information on COM documentation, see http://support.avaya.com.

Port Mirroring ingress and egress

The port-mirroring feature is used to analyze traffic flowing on a port. VSP 4000 supports both ingress and egress port mirroring. Any packet ingressing or egressing a specified port is forwarded normally and a copy of the packet is sent out to the mirroring or destination port to be observed using a network analyzer. For more information, see *Avaya Virtual Services Platform 4000 – Troubleshooting* (NN46251-700).

RADIUS

Remote Access Dial-In User Services (RADIUS) is a distributed client/server system that assists in securing networks against unauthorized access, allowing a number of communication servers and clients to authenticate users identity through a central database. The database within the RADIUS server stores information about clients, users, passwords, and access privileges including the use of shared secret.

RADIUS is a fully open and standard protocol, defined by two Requests for Comments (RFC) (Authentication: RFC2865, Accounting: RFC2866). With Virtual Services Platform 4000, you use RADIUS authentication to get secure access to the system (console/Telnet/SSH/EDM), and RADIUS accounting to track the management sessions (ACLI only). For more information, see *Avaya Virtual Services Platform 4000 – Security* (NN46251–601).

VRRP BackupMaster

Avaya VSP 4000 supports the VRRP BackupMaster feature.

The VRRP BackupMaster acts as an IP router for packets destined for the logical VRRP IP address. All traffic is directly routed to the destined subnetwork and not through Layer 2 switches to the VRRP master. This avoids potential limitation in the available interswitch trunk bandwidth.

The BackupMaster feature provides an additional benefit. VRRP normally sends a hello packet every second. When three hello packets are not received, all switches automatically revert to master mode. This results in a 3- second outage. For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

Line Rate Ingress and Egress Port & VLAN ACLs for L2 to L4

Avaya VSP 4000 supports Port and VLAN based Access Control Lists (ACLs) for line rate ingress and egress of Layer 2, Layer 3, and Layer 4 packets.

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

There are three ways an ACL can be associated:

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

For more information, see *Avaya Virtual Services Platform 4000 Configuration – QoS and ACL-Based Traffic Filtering* (NN46251–502).

IEEE 802.1X EAPoL

Avaya VSP 4000 supports IEEE 802.1x based Extensible Authentication Protocol over LAN (EAPoL).

EAPoL is a port-based network access control protocol. EAPoL provides security by preventing users from accessing network resources before they are authenticated. The EAPoL authentication feature prevents users from accessing a network to assume a valid identity and access confidential material or launch denial-of-service attacks. For more information, see *Avaya Virtual Services Platform 4000 – Security* (NN46251–601).

Key Health Indicator (KHI)

The Key Health Indicator (KHI) feature of Avaya Virtual Services Platform 4000 provides a subset of health information that allows for quick assessment of the overall operational state of the device. For more information, see *Avaya Virtual Services Platform 4000 – Fault Management* (NN46251–702).

SLPP Re-Arm

Avaya VSP 4000 supports SLPP Re-Arm by resetting the SLPP port receive counter.

When a per-port SLPP PDU receive counter reaches a pre-defined limit, it shuts down links wrongly after months of running. This issue is addressed by resetting the counter if the switch does not receive the expected number of SLPP packets on the port in a certain period of time. The timer to reset the counter is set to six hours.

DHCP Relay Option 82

Avaya VSP 4000 supports DHCP Relay Option 82 feature.

The DHCP option 82 is the DHCP Relay Agent Information option. The DHCP relay agent inserts option 82 when it forwards the client-originated DHCP packets to a DHCP server. The Relay Agent Information option is organized as a single DHCP option that contains one or more sub-options that convey information known by the relay agent. The DHCP server echoes the option back to the relay agent in server-to-client replies, and the relay agent removes the option before forwarding the reply to the client. For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

Microsoft NLB ARP multicast-MAC-flooding support

Avaya VSP 4000 supports multicast MAC flooding feature for Network Load Balancer (NLB). Use the ARP MAC-flooding option to support multiple NLB clusters in the same VLAN. For more information, see *Avaya Virtual Services Platform 4000 Configuration – IP Routing* (NN46251-505).

Secure Shell (SSH) client support

You can use the Secure Shell (SSH) protocol for both inbound and outbound access with the Virtual Services Platform 4000. For more information, see *Avaya Virtual Services Platform 4000 – Administration* (NN46251–600).

IEEE 802.1aq Shortest Path Bridging MACinMAC (SPBM)

Avaya VSP 4000 supports the IEEE 802.1aq standard of Shortest Path Bridging MACinMAC (SPBM). SPBM makes network virtualization much easier to deploy within the enterprise environment, reducing the complexity of the network while at the same time providing greater scalability.

SPBM eliminates the need for multiple overlay protocols in the core of the network by reducing the core control plane to a single protocol that can provide virtualization services for both Layer 2 and Layer 3, on a common Ethernet infrastructure using a pure Ethernet technology base.

SPBM separates the Ethernet network into edge and core domains with complete isolation between their MAC addresses. This technology provides all the features and benefits required by carrier-grade, enterprise, and service provider deployments without the complexity of alternative technologies, for example, Multiprotocol Label Switching (MPLS). SPBM integrates into a single control plane all the functions that MPLS requires multiple layers and protocols to support.

SPBM provides any-to-any connectivity in a network in an optimized, loop-free manner. SPBM employs shortest-path trees to each destination, without the long convergence delays experienced with Spanning Tree Protocol (STP). To do this, SPBM uses Intermediate System to-Intermediate System (IS-IS) link state routing protocol to learn and distribute network information. IS-IS dynamically learns the topology of a network and uses its inherent

knowledge to construct shortest path unicast and multicast trees from every node to every other node in the network. Also, unlike STP, IS-IS does not block ports to provide a loop free topology, so bandwidth is not wasted.

Note:

You must purchase and install the Premier License to use SPBM.

For more information about SPBM, see *Avaya Virtual Services Platform 9000 Configuration – Shortest Path Bridging MAC (SPBM)* (NN46251–510).

IEEE 802.1ag Connectivity Fault Management (CFM)

Avaya VSP 4000 supports the IEEE 802.1ag based Connectivity Fault Management (CFM) feature.

Use Connectivity Fault Management (CFM) to debug connectivity issues and isolate faults in a Shortest Path Bridging MAC (SPBM) network. CFM operates at Layer 2 and provides an equivalent of the ping and traceroute commands. To support troubleshooting of the SPBM cloud, this release supports a subset of CFM functionality. CFM is based on the IEEE 802.1ag standard.

For more information about CFM, see *Avaya Virtual Services Platform 9000 Configuration – Shortest Path Bridging MAC (SPBM)* (NN46251–510).

Chapter 3: Important notices

This section describes the supported hardware and software scaling capabilities of the Avaya Virtual Services Platform 4000 and provides important information for this release.

Hardware compatibility

The following tables describe the Avaya Virtual Services Platform 4000 hardware.

Table 1: Hardware

VSP 4000 model	Description	Part number
VSP 4850GTS	• 48 10/100/1000 BaseTX RJ-45 ports • two SFP ports • two SFP+ ports • Base Software License • one field replaceable 300W PSU	EC4800A78-E6
	• Same content as EC4800A78-E6 with a EU power cord.	EC4800B78-E6
	• Same content as EC4800A78-E6 with a UK power cord.	EC4800C78-E6
	• Same content as EC4800A78-E6 with a JP power cord.	EC4800D78-E6
	• Same content as EC4800A78-E6 with a NA power cord.	EC4800E78-E6
	• Same content as EC4800A78-E6 with a EU power cord.	EC4800F78-E6
VSP 4850GTS-PWR+	• 48 10/100/1000 802.3at PoE+ • two SFP ports • two SFP+ ports	EC4800A88-E6

VSP 4000 model	Description	Part number
	• Base Software License • one field replaceable 1000W PSU	
	• Same content as EC4800A88-E6 with a EU power cord.	EC4800B88-E6
	• Same content as EC4800A88-E6 with a UK power cord.	EC4800C88-E6
	• Same content as EC4800A88-E6 with a JP power cord.	EC4800D88-E6
	• Same content as EC4800A88-E6 with a NA power cord.	EC4800E88-E6
	• Same content a EC4800A88-E6 with a AU power cord.	EC4800F88-E6
VSP 4850GTS DC	• 48 10/100/1000 Base TX RJ-45 ports • two shared SFP ports • two 10GE SFP+ ports • one field replaceable 300W DC PSU	EC4800078-E6
Redundant power supplies		
300W AC redundant power supply	For use in the ERS 4626GTS, 4850GTS, VSP 4850GTS and WL8180, WL8180-16L wireless controllers. [EUED RoHS 5/6 compliant].	AL1905?08-E5*
Stackable 1000W AC POE + power supply.	For use in 4X00 PWR+,	AL1905?21-E6*
Redundant 300W DC power supply.	For use in the VSP 4850GTS-DC, ERS5698TFD, 5650TD, and 5632FD. (EUED RoHS 5/6 compliant). DC connector included	AL1905005-E5
*__Note__: The seventh character (?) of the switch order number must be replaced with the proper letter to indicate desired product nationalization. See the following for details: “A”: No power cord included. “B”: Includes European “Schuko” power cord common in Austria, Belgium, Finland, France, Germany, The Netherlands, Norway, and Sweden. “C”: Includes power cord commonly used in the United Kingdom and Ireland. “D”: Includes power cord commonly used in Japan. “E”: Includes North American power cord. “F”: Includes Australian power cord.		

Table 2: Compatible SFPs and SFP+s

For more information about SFP and SFP+, see *Avaya Virtual Services Platform 4000 Installation — SFP and SPF+ transceivers* (NN46251–301).

Hardware	Description	Part number
10GBASE-LR/LW SFP+	1310 nm SMF with a range up to 10 km	AA1403011-E6
10GBASE-ER/EW SFP+	1550 nm SMF with a range up to 40 km	AA1403013-E6
10GBASE-SR/SW SFP+	850nm with a range up to 300 m	AA1403015-E6
10GBASE-LRM SFP+	220 m, 1260 to 1355 nm; 1310 nm nominal MMF	AA1403017-E6
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 10m.	AA1403018-E6
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 3m.	AA1403019-E6
10GBase-CX	4-pair twinaxial copper cable that plugs into the SFP+ socket and connects two 10 Gb ports. The maximum range is 5m.	AA1403020-E6
1000BASE-T (RJ-45) SFP	Gigabit Ethernet, RJ-45 connector	AA1419043-E6
1000BASE-SX (LC) DDI	850 nm, Gigabit Ethernet, duplex LC connector	AA1419048-E6
1000BASE-LX (LC) DDI	1310 nm, Gigabit Ethernet, duplex LC connector	AA1419049-E6
1000BASE-XD DDI	1310 nm, Gigabit Ethernet, duplex LC connector	AA1419050-E6
	1550 nm, Gigabit Ethernet, duplex LC connector	AA1419051-E6
1000BASE-ZX DDI	1550 nm, Gigabit Ethernet, duplex LC connector	AA1419052-E6
1000BASE-ZX CWDM (LC)	1470 nm to 1610 nm, up to 70 km	AA1419061-E6 to AA1419068-E6
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC, up to 10 km	AA1419069-E6
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC, up to 10 km	AA1419070-E6
1000BASE-EX DDI SFP	1550 nm, up to 120 km	AA1419071-E6

Hardware	Description	Part number
1000BASE-BX bidirectional SFP	1310 nm, single fiber LC, up to 40 km	AA1419076–E6
1000BASE-BX bidirectional SFP	1490 nm, single fiber LC, up to 40 km	AA1419077–E6
100BASE-FX SFP	1310 nm, LC connector	AA1419074-E6

Important:

Avaya recommends the use of Avaya branded SFP and SFP+ transceivers as they have been through extensive qualification and testing. Avaya will not be responsible for issues related to non-Avaya branded SFP and SFP+ transceivers.

Software scaling capabilities

This section lists software scaling capabilities of Avaya Virtual Services Platform 4000.

Table 3: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4000 for demo/1000 practical
LACP	24 aggregators
LACP ports per aggregator	8 active and 8 standby
MACs in forwarding database (FDB)	32,000
Multi-Link Trunking (MLT)	24 groups
Multiple Spanning Tree Protocol (MSTP)	12 instances
Protocol-based VLANs	1
Rapid Spanning Tree Protocol (RSTP)	1 instance
SLPP	128 VLANs
VLACP Interfaces	50
Layer 3	
RIP interfaces	24
RIP routes	500
OSPF interfaces	48 (24 of these can be passive)
OSPF adjacencies	24

	Maximum number supported
OSPF areas (per instance/per system)	64
OSFP routes per VRF	100 (2400 local OSPF routes in 24 VRFs)
OSPF routes	16,000
OSPF VRF support	4
e-BGP peers	12
e-BGP routes	16,000
Address Resolution Protocol (ARP) for each port, VRF, or VLAN	6,000 entries total
Circuitless IP interfaces	64
ECMP routes	1024
ECMP paths per route	8
FIB IPv4 routes	16,000
IPv4 interfaces	256
IP routing policies	500 for each VRF 5,000 for each system
IPv4 FTP sessions	4
IPv4 Rlogin sessions	8
IPv4 SSH sessions	8
IPv4 Telnet sessions	8
IPv4 VRF instances	24
Static ARP entries	200 for each VRF 1,000 for each system
Static routes (IPv4)	1,000 per VRF/per system
UDP/DHCP forwarding entries	128 for each system
VRRP interfaces (IPv4)	64
VRRP interfaces fast timers (200 ms)	24
Diagnostics	
Mirrored ports	49
Remote Mirroring Termination (RMT) ports	4
Filters and QoS	
Port shapers (IPv4)	50
ACEs per ACL (a combination of Security and QoS ACEs)	1,000

	Maximum number supported
Unique redirect next hop values for ACE Actions (IPv4)	Ingress: 1,536, Egress: 256
SPBM	
MAC entries	16,000 (combination of ARP entries and Layer 2 MACs)
Backbone MAC	1,000
IP routes in the Global Router	25,000
IS-IS IP routes	16,000
IS-IS adjacencies	24
Layer 2 VSNs	1,000
Layer 3 VSNs	24

File names for this release

This section describes the Avaya Virtual Services Platform 4000 software files.

Software files

The following table provides the details of the Virtual Services Platform 4000 software files. File sizes are approximate.

Table 4: Software Build 64 components

Module or File Type	Description	File Name	File Size (bytes)
Standard Runtime Software Image	Standard image for the Avaya Ethernet Routing Switch 4000 Series	VSP4K.3.0.0.0.tgz	75,234,072
Enterprise Device Manager Help Files	Help files required for Avaya Ethernet Routing Switch 4000	VSP4000v300_HELP_EDM_gzip.zip	2,097,393

Table 5: Software files

File name	Description	Size (bytes)
VSP4K.3.0.0.0_modules.tgz	Encryption modules	37,795

Comments? infodev@avaya.com

Open Source software files

The following table gives the details of the Open Source software files distributed with the Virtual Services Platform 4000 software.

Table 6: Open Source software files

File name	Description	Size
VSP4K.3.0.0.0_oss-notice.html	Master copyright file. This file is located in the Licenses directory.	412 KB
VSP4K.3.0.0.0_OpenSource.zip		96 MB

You can download Avaya Virtual Services Platform 4000 software and files, including MIB files, from the Avaya Support Portal at www.avaya.com/support. Click **Downloads**.

The Open Source license text for the VSP 4000 is included on the VSP 4000 product and is accessible via the Command Line Interface by typing the following: `more release/3.0.0.0.GA/release/oss-notice.txt`.

Upgrading the software

Perform this procedure to upgrade the software on the Avaya Virtual Services Platform 4000. This procedure shows how to upgrade the software using the internal flash memory as the file storage location.

Before you begin

- Back up the configuration files.
- Ftp the VSP 4000 upgrade file to the Virtual Services Platform 4000.
- You must log on to at least the Privileged EXEC mode in ACLI.

Note:

Software upgrade configurations are case sensitive.

Procedure

1. Extract the release distribution files to the /intflash/release/ directory:
   `software add WORD<1-99>`
2. Extract the module files to the /intflash/release directory:
   `Software add-module [software version] [modules file name]`
3. Install the image:
   `software activate WORD<1-99>`
4. Restart the Virtual Services Platform 4000:

```
reset
```

Important:

After you restart the system, you have the amount of time configured for the commit timer to verify the upgrade and commit the software to gold. If you do not commit the software to gold and auto-commit is not enabled, the system restarts with the last known working version after the commit timer has expired. This feature ensures you can regain control of the system if an upgrade fails.

5. Confirm the software is upgraded:

   ```
   show software
   ```

6. Commit the software:

   ```
   software commit
   ```

Example

```
VSP-4850GTS-PWR+:1#software add VSP4K.3.0.0.0.tgz

VSP-4850GTS-PWR+:1# software add-modules 3.0.0.0.GA
VSP4K.3.0.0.0_modules.tgz

VSP-4850GTS-PWR+:1#software activate 3.0.0.0.GA

VSP-4850GTS-PWR+:1#reset

VSP-4850GTS-PWR+:1#show software
================================================================================
                    software releases in /intflash/release/
================================================================================
VSP4K.3.0.0.0int064 (Backup Release)
3.0.0.0.GA (Primary Release)

--------------------------------------------------------------------------------
Auto Commit     : enabled
Commit Timeout  : 10 minutes

VSP-4850GTS-PWR+:1#software commit
```

Deleting a software release

Perform this procedure to remove a software release from the Avaya Virtual Services Platform 4000.

Note:

For information about adding and activating a software release, see Upgrading the software on page 27.

Comments? infodev@avaya.com

Procedure

1. Enter Privileged EXEC configuration mode:
   ```
   enable
   ```
2. Remove software:
   ```
   software remove WORD<1-99>
   ```

Example

```
VSP-4850GTS-PWR+:1>enable

VSP-4850GTS-PWR+:1#software remove VSP4K.3.0.1.0.tgz
```

Important information and restrictions

This section contains important information and restrictions you must consider before you use the Avaya Virtual Services Platform 4000.

Interoperability notes for VSP 4000 connecting to an ERS 8800

- For customers running version 7.1.x: The minimum software release is 7.1.3.1, however the recommended ERS 8800 software release is 7.1.5.4 or later. On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 the minimum software version is 7.1.5.4. The “spbm version” on the ERS 8800 must be set to “802.1aq”.
- For customers running version 7.2.x: The minimum software release is 7.2.0.2, however the recommended ERS 8800 software release is 7.2.1.1 or later. On switches using 8612 XLRS or 8812XL modules for the links connecting to the VSP 4000 the minimum software version is 7.2.1.1.
- Diffserv is enabled in the VSP 4000 port settings, and is disabled in the ERS 8800 port settings, by default.

Supported browsers

Virtual Services Platform 4000 supports the following browsers to access the Enterprise Device Manager (EDM):

- Microsoft Internet Explorer 8.0
- Mozilla Firefox 7.x

User configurable SSL certificates

Virtual Services Platform 4000 does not generate SSL certificates with user-configurable parameters. You can, however, use your own certificate.

You can generate a certificate off the VSP 4000 system, and upload the key and certificate files to the `/intflash/ssh` directory. Rename the uploaded files to host.cert and host.key, and then reboot the system. The system loads the user-generated certificates during startup. If the system cannot find host.cert and host.key during startup, it generates a default certificate.

For more information about SSH and SSL certificates, see *Avaya Virtual Services Platform 4000 Administration*, NN46251–600.

Feature licensing

After you start a new system, the 60–day Premium Trial license countdown begins. You will see notification messages as the countdown approaches the end of the trial period. After 60 days, the Premium Trial license expires. You will see messages on the console and in the alarms database that the license has expired. The next time you restart the system after the license expiration, the system no longer supports Advanced or Premier services.

If you use a Base license, you do not need to install a license file. If you purchase an Advanced or Premier license, you must obtain and install a license file. For more information about how to generate and install a license file, see *Avaya Virtual Services Platform 4000 Administration*, NN46251–600.

Important:

The license filename stored on a device must meet the following requirements:

- Maximum of 63 alphanumeric characters
- Lowercase only
- No spaces or special characters allowed
- Underscore (_) is allowed
- The file extension ".dat" is required

Combination ports

When the VSP 4000 is reset, the peer connections for all ports, including combination ports 47 and 48, will transition down. During the reset, the fiber ports remain down, but only the copper ports 47 and 48 come up periodically throughout the reset. The copper ports 47 and

48 come up approximately 15 seconds into the reset, remain up for approximately 60 seconds, and then transition down until the boot sequence is complete and all ports come back up.

The following is an example of the status of the combination ports during reset.

```
CP1 [03/18/70 09:55:35.890] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW
INFO Link Down(1/47)
CP1 [03/18/70 09:55:35.903] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW
INFO Link Down(1/48)

CP1 [03/18/70 09:55:49.994] 0x0000c5ec 00300001.239 DYNAMIC CLEAR GlobalRouter HW
INFO Link Up(1/48)
CP1 [03/18/70 09:55:50.322] 0x0000c5ec 00300001.238 DYNAMIC CLEAR GlobalRouter HW
INFO Link Up(1/47)

CP1 [03/18/70 09:56:43.131] 0x0000c5e7 00300001.238 DYNAMIC SET GlobalRouter HW
INFO Link Down(1/47)
CP1 [03/18/70 09:56:43.248] 0x0000c5e7 00300001.239 DYNAMIC SET GlobalRouter HW
INFO Link Down(1/48)
```

Cabled connections for both copper and fiber ports

The following limitations apply when the combination ports have cabled connections for both the copper and fiber ports.

- Do not use the fiber port and do not insert an SFP into the optical module slot in the following situations:
  - a copper speed setting of either 10M or 100M is required
  - a copper duplex setting of half-duplex is required

Note:

These limitations are applicable only when auto-negotiation is disabled. To avoid this limitation, use auto-negotiation to determine the speed to 10/100/1000 and to determine the duplex.

- The 100M-FX SFP requires auto-negotiation to be disabled. Therefore, auto-negotiation will also be disabled for the copper port. Configure peer switch to disable auto-negotiation.

SFP and SFP+ ports

- SFP and SFP+ ports support 1000Base-T SFP (RJ-45) for 1000Mbps. Triple-speed mode is not supported.
- SFP+ port does not support slow speed SFPs. Supports 10G and 1G.

Chapter 4: Supported standards, RFCs, and MIBs

This chapter details the standards, request for comments (RFC), and Management Information Bases (MIB) that Avaya Virtual Services Platform 4000 supports.

Supported IEEE standards

The following table details the IEEE standards that Avaya Virtual Services Platform 4000 supports.

Table 7: Supported IEEE standards

IEEE standard	Description
802.1aq	Shortest Path Bridging (SPB)
802.1AX	Link Aggregation Control Protocol (LACP)
802.1p	VLAN prioritization
802.1Q	Virtual Local Area Network (VLAN) tagging
802.1s	Multiple Spanning Tree Protocol
802.1t	802.1D maintenance
802.1w-2001	Rapid Spanning Tree protocol (RSTP)
802.1X	Extended Authentication Protocol (EAP), and EAP over LAN (EAPoL)
802.1X-2004	Port Based Network Access Control
802.3 CSMA/CD Ethernet ISO/IEC 8802	International Organization for Standardization (ISO) /International Eletrotechnical Commission (IEC) 8802-3
802.3ab	Gigabit Ethernet 1000BaseT 4 pair Category 5 (Cat5) Unshieled Twisted Pair (UTP)
802.3ae	10 Gigabit Ethernet
802.3af and 802.3at	PoE – Power Over Ethernet
802.3i	10BaseT

IEEE standard	Description
802.3u	100BaseT
802.3x	flow control
802.3z	Gigabit Ethernet

Supported RFCs

The following table and sections list the RFCs that Avaya Virtual Services Platform 4000 supports.

Table 8: Supported request for comments

Request for comment	Description
RFC768	UDP Protocol
RFC783	Trivial File Transfer Protocol (TFTP)
RFC791	Internet Protocol (IP)
RFC792	Internet Control Message Protocol (ICMP)
RFC793	Transmission Control Protocol (TCP)
RFC826	Address Resolution Protocol (ARP)
RFC854	Telnet protocol
RFC894	A standard for the Transmission of IP Datagrams over Ethernet Networks
RFC896	Congestion control in IP/TCP internetworks
RFC906	Bootstrap loading using TFTP
RFC950	Internet Standard Subnetting Procedure
RFC951	BootP
RFC959, RFC1350, and RFC2428	FTP and TFTP client and server
RFC1027	Using ARP to implement transparent subnet gateways/Nortel Subnet based VLAN
RFC1122	Requirements for Internet Hosts
RFC1256	ICMP Router Discovery
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis
RFC1340	Assigned Numbers

Comments? infodev@avaya.com

Request for comment	Description
RFC1519	Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy
RFC1541	Dynamic Host Configuration Protocol1
RFC1542	Clarifications and Extensions for the Bootstrap Protocol
RFC1591	DNS Client
RFC1812	Router requirements
RFC1866	HyperText Markup Language version 2 (HTMLv2) protocol
RFC2068	Hypertext Transfer Protocol
RFC2131	Dynamic Host Control Protocol (DHCP)
RFC2138	RADIUS Authentication
RFC2139	RADIUS Accounting
RFC2338	VRRP: Virtual Redundancy Router Protocol
RFC2616	Hypertext Transfer Protocol 1.1
RFC2819	RMON
RFC2992	Analysis of an Equal-Cost Multi-Path Algorithm
RFC3046	DHCP Option 82
RFC3621	PoE – Power Over Ethernet
RFC4250–RFC4256	SSH server and client support
RFC6329	IS-IS Extensions supporting Shortest Path Bridging

Quality of service

Table 9: Supported request for comments

Request for comment	Description
RFC2474 and RFC2475	DiffServ Support
RFC2597	Assured Forwarding PHB Group
RFC2598	An Expedited Forwarding PHB

Network management

Table 10: Supported request for comments

Request for comment	Description
RFC1155	SMI
RFC1157	SNMP
RFC1215	Convention for defining traps for use with the SNMP
RFC1271	Remote Network Monitoring Management Information Base
RFC1305	Network Time Protocol v3 Specification, Implementation and Analysis3
RFC1350	The TFTP Protocol (Revision 2)
RFC1354	IP Forwarding Table MIB
RFC1757	Remote Network Monitoring Management Information Base
RFC1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1908	Coexistence between v1 & v2 of the Internet-standard Network Management Framework
RFC1930	Guidelines for creation, selection, and registration of an Autonomous System (AS)
RFC2541	Secure Shell Protocol Architecture
RFC2571	An Architecture for Describing SNMP Management Frameworks
RFC2572	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC2573	SNMP Applications
RFC2574	User-based Security Model (USM) for v3 of the Simple Network Management Protocol (SNMPv3)
RFC2575	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)

Comments? infodev@avaya.com

Request for comment	Description
RFC2576	Coexistence between v1, v2, & v3 of the Internet standard Network Management Framework
RFC2819	Remote Network Monitoring Management Information Base

MIBs

Table 11: Supported request for comments

Request for comment	Description
RFC1156	MIB for network management of TCP/IP
RFC1212	Concise MIB definitions
RFC1213	TCP/IP Management Information Base
RFC1354	IP Forwarding Table MIB
RFC1389	RIPv2 MIB Extensions
RFC1398	Ethernet MIB
RFC1442	Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)
RFC1450	Management Information Base for v2 of the Simple Network Management Protocol (SNMPv2)
RFC1573	Interface MIB
RFC1650	Definitions of Managed Objects for the Ethernet-like Interface Types
RFC1657	BGP-4 MIB using SMIv2
RFC1850	OSPF MIB
RFC2096	IP Forwarding Table MIB
RFC2578	Structure of Management Information v2 (SMIv2)
RFC2674	Bridges with Traffic MIB
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol

Request for comment	Description
RFC2863	Interface Group MIB
RFC2925	Remote Ping, Traceroute & Lookup Operations MIB
RFC3416	v2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC4113	Management Information Base for the User Datagram Protocol (UDP)

Standard MIBs

The following table details the standard MIBs that Avaya Virtual Services Platform 4000 supports.

Table 12: Supported MIBs

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB2— Link Aggregation Control Protocol (LACP) (802.3ad)	802.3ad	ieee802-lag.mib
STDMIB3—Exensible Authentication Protocol Over Local Area Networks (EAPoL) (802.1x)	802.1x	ieee8021x.mib
STDMIB4—Internet Assigned Numbers Authority (IANA) Interface Type	—	iana_if_type.mib
STDMIB5—Structure of Management Information (SMI)	RFC1155	rfc1155.mib
STDMIB6—Simple Network Management Protocol (SNMP)	RFC1157	rfc1157.mib
STDMIB7—MIB for network management of Transfer Control Protocol/Internet	RFC1213	rfc1213.mib

Comments? infodev@avaya.com

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
Protocol (TCP/IP) based Internet MIB2		
STDMIB8—A convention for defining traps for use with SNMP	RFC1215	rfc1215.mib
STDMIB10—Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib
STDMIB11—Evolution of the Interface Groups for MIB2	RFC2863	rfc2863.mib
STDMIB12—Definitions of Managed Objects for the Ethernet-like Interface Types	RFC1643	rfc1643.mib
STDMIB15—Remote Network Monitoring (RMON)	RFC2819	rfc2819.mib
STDMIB17—Management Information Base of the Simple Network Management Protocol version 2 (SNMPv2)	RFC1907	rfc1907.mib
STDMIB21—Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
STDMIB26a—An Architecture for Describing SNMP Management Frameworks	RFC2571	rfc2571.mib
STDMIB26b—Message Processing and Dispatching for the SNMP	RFC2572	rfc2572.mib
STDMIB26c—SNMP Applications	RFC2573	rfc2573.mib
STDMIB26d—User-based Security Model (USM) for version 3 of the SNMP	RFC2574	rfc2574.mib
STDMIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib
STDMIB26f —Coexistence between Version 1, Version	RFC2576	rfc2576.mib

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
2, and Version 3 of the Internet-standard Network Management Framework		
STDMIB29—Definitions of Managed Objects for the Virtual Router Redundancy Protocol	RFC2787	rfc2787.mib
STDMIB31—Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
STDMIB32—The Interface Group MIB	RFC2863	rfc2863.mib
STDMIB33—Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations	RFC2925	rfc2925.mib
STDMIB38—SNMPv3 These Request For Comments (RFC) make some previously named RFCs obsolete	RFC3411, RFC3412, RFC3413, RFC3414, RFC3415	rfc2571.mib, rfc2572.mib, rfc2573.mib, rfc2574.mib, rfc2575.mib
STDMIB39—Entity Sensor Management Information Base	RFC3433	
STDMIB40—The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model	RFC3826	rfc3826.mib
STDMIB41—Management Information Base for the Transmission Control protocol (TCP)	RFC4022	rfc4022.mib
STDMIB43—Management Information Base for the User Datagram Protocol (UDP)	RFC4113	rfc4113.mib
STDMIB44—Entity MIB	RFC4133	rfc4133.mib
STDMIB45 – Definitions of Managed Power Over Ethernet	RFC3621	rfc3621.mib

Proprietary MIBs

The following table details the proprietary MIBs that Avaya Virtual Services Platform 4000 supports.

Table 13: Proprietary MIBs

Proprietary MIB name	File name
PROMIB1 – Rapid City MIB	rapid_city.mib
PROMIB 2 – SynOptics Root MIB	synro.mib
PROMIB3 – Other SynOptics definitions	s5114roo.mib
PROMIB4 – Other SynOptics definitions	s5tcs112.mib
PROMIB5 – Other SynOptics definitions	s5emt103.mib
PROMIB6 – Avaya RSTP/MSTP proprietary MIBs	nnrst000.mib, nnmst000.mib
PROMIB11 – Avaya MIB definitions	wf_com.mib
PROMIB12 – Other SynOptic definition for Combo Ports	s5ifx.mib
PROMIB31 – Other SynOptic definition for PoE	bayStackPethExt.mib

Chapter 5: Known issues and limitations

This section details the known issues and limitations of the Avaya Virtual Services Platform 4000. Where appropriate, use the workarounds provided.

Known issues

The following sections identify the known issues in this release of the Avaya Virtual Services Platform 4000.

Device related issues

Table 14: Known issues

Issue number	Description	Workaround
wi01078025	Filter ACL default action as deny with control-packet-action as permit is not working. When filter ACL default action is configured as deny and control-packet-action is permit, control packets are dropped by the filter default action.	None. The command of control-packet-action has been removed from the command of default-action of the ACL.
wi01086954	When isis is enabled on a port which is member of vlan 1, the port is not removed from vlan 1 automatically. Since isis adds the nni ports to BVLAN automatically when the isis is enabled, the ports are not removed from vlan 1. If the nni port is member of vlan 1, it could possibly trigger mac flush in the cvlans when the nni port state changes.	Remove the nni ports from vlan 1 manually after enabling the isis on that port.

Issue number	Description	Workaround
wi01091986	On one occasion a core dump has been detected following the "reset" command as system was shutting down; the reboot sequence completed successfully and the switch came back online	None required
wi01092747	An abort from a FTP client session may not be processed right away, but may be delayed for up to 60 seconds. During this time the FTP session may show as active.	Allow up to 60 seconds for an FTP session to clear up when it is interrupted.
wi01094114	The CLI “copy” command may in some cases not return an error if the remote FTP or TFTP server can’t accept the file due to a full disk. The file may be created with a file size of zero.	Make sure there is enough disk space to store the file on the remote server. Additionally check the file size after the transfer is complete to make sure the file was transferred successfully and completely.
wi01095069	When IP ECMP is enabled on the i-sid enabled VRF, L3 VSN traffic which hashes out on secondary BVID will be dropped. The root cause is because IP ECMP enabled is not supported on the I-SID VRF on this release. There is no consistency check in place to not allow the ECMP to be enabled while the VRF is configured the L3 VSP service.	When a VRF is configured as L3 VSN VRF, please do not enable the IP ECMP on this VRF. Or, if this VRF has been configured as IPECMP enabled, Please do not configure the L3 VSN service on this VRF.
wi01096198	When a MAC-in-MAC packet is encapsulated at the SPB edge, the packet priority is carried into the pbits in the BTAG and the pbits in the ITAG, and both priority values should be consistent. However, sometimes the priority in the ITAG is not marked correctly, so that the ITAG may carry the priority	

Comments? infodev@avaya.com

Issue number	Description	Workaround
	value different from that in the BTAG. Currently only the BTAG priority is used in the L2VSN/L3VSN core forwarding and at the edge de-capsulation, and this includes the VSP 9000, ERS8800 and VSP 4000 systems. So this issue has no functionality impact so far, and the fix will be implemented in the patch and future releases.	

EDM related issues

Table 15: Known issues

Issue number	Description	Workaround
wi01096275	The EDM tab **IS-IS** > **Stats** > **IS-IS** > **Interface Counters and Tab** > **Stats** > **Interface Control Packet** show the circuit index for each entry instead of the interface index. From this tab, you cannot tell what interface the ISIS circuit is using.	The circuit index and interface mapping is shown in EDM tab **IS-IS** > **IS-IS** > **Interface**. Go to this tab to find the interface for the circuit index.
wi01112398	If we launch EDM through COM, CFM-l2 ping does not work, and displays a timeout error. EDM plug-in may not display the **Result** field of the tab of **Edit** > **Diagnostics** > **L2Ping/L2Traceroute** > **L2Ping** properly if the field contains a special character such as "new line" or "tab". This field is a read-only field.	Use on-box EDM or CLI to run the CFM-l2 ping and traceroute testing.

Limitations

This section lists known limitations and expected behaviors that may first appear to be issues. The following table provides a description of the limitation or behavior and the work around, if one exists.

Table 16: Limitations and expected behaviors

Issue number	Description
wi01068569	The system displays a warning message that routes will not inject until the apply command is issued after the enable command. The warning applies only after you enable redistribution, and not after you disable redistribution. For example, `4k2:1(config)#isis apply redistribute direct vrf 2`.
wi01122478	Stale snmp-server community entries for different VRFs appear after reboot with no VRFs . On an node with any valid config file saved with more than the default vrf0 , snmp_community entries for that VRF are created and maintained in a separate txt file, snmp_comm.txt, on every boot. The node reads this file and updates the snmp communities available on the node. As a result for a boot with config having no VRFs, you may still see snmp_community entries for VRFs other than the globalRouter vrf0 .
wi01134468	On a T-Uni port, with L2 Untrusted configuration, the internal QoS of the traffic flow is derived from the .1p bits of the ingress tagged traffic.
wi01134509	On a T-Uni port, with incoming untagged traffic, the internal QoS level of the traffic flow is set to 0, irrespective of the L2 Trust configuration on the port.
wi01136327	On a T-Uni port, the .1p bit of the CVLAN in the egress packet is changed when the .1p bits of the ingress tagged traffic is 0 or 1.

Comments? infodev@avaya.com

Chapter 6: Resolved issues

This section details all the issues that were resolved in this release.

Table 17: VSP 4000 R3.0 beta build 64 resolved issues

WI reference	Description
Management and general administration	
wi01073142	Counter is not increasing when TDP packets are received on an interface. This effects both the ingress broadcast and ingress multicast packet counters displayed by `show interfaces gigabitEthernet statistics` for ports 1/49 and 1/50. Egress counters for these ports will increment however.
wi01080007	`clear filter acl statistics default <ACL ID> /clear filter acl statistics all` does not clear ACLdefault statistics.
wi01088505	There are issues with the `ip vrrp` default command. The system displays error messages in a few scenarios and configurable critical ip addresses. Case 1: When you execute `default ip vrrp <vrrpid>`, the command outputs the following error message: “Error: VRRP fast advertisement disabled, use advertisement interval." The command is working as expected and sets all the default values, but displays the preceding error which may be confusing. The problem exists when called from ACLI only when the fast-advertisement is not enabled. To make sure no error messages are shown, the system checks to ensure whether fast-advertisement is enabled and then processed further. This issue applies to both vlan and port interfaces. Case 2: The command `default ip vrrp address 161` Backup-address option is redundant and accepts any value given. Case 3: The system displays the wrong error when you use the command `default ip vrrp 1 critical-ip-addr`. Case 4: The system displays the wrong error when you enable the critical ip address using the command `Ip vrrp critical-ip enable`. Case 3 and case 4 display a generic error message which may be confusing. These issues are resolved by displaying proper error messages. The impact is minor. The error messages may be confusing when you execute the `ip vrrp` default commands.
wi01088791	After Applying `show log transferFile <ID>` DUT is getting struck
wi01089181	You can configure the `ip vrrp critical-ip` address which is not a local interface. You can configure the critical ip address to be any irrelevant ip address that does not have to be present on the local node. Because the interface does

WI reference	Description
	not exist, the ip vrrp interface state changes to backup as soon as it is configured. Critical ip is an ip address on the local router. The command`critical-ip-addr <A.B.C.D>` configures the critical IP address for VRRP. The variable, `<A.B.C.D>` is the IP address on the local router, which is configured so that a change in its state causes a role device in the virtual router; for example, from master to backup in case the interface goes down. For more information, see *IP Routing Configuration* (NN46250-505). The current design is the same across all platforms, ERS, VSP 9000 and VSP 4000.
Alarm, logging, and error reporting	
wi01070650	Under loop condition, after SLPP detects the loopback and shuts down the port, this error message shows up on the console:`vlanProcess4KBulkDeletedMac:5403 rarDeleteMacAddress NOT FOUND for mac xx:xx:xx:xx:xx:xx vlanId xxx.`
Chassis operations	
wi01077911	sys shutdown command not shutting link down on all ports. Only fiber ports 1/47-1/50 shutdown, copper ports 1/1-1/46 do not. This could potentially cause connected devices at the far end of the link to think the link is still up, send packets to it, etc.
EDM	
wi01070861	Stale user EDM connections are left in the box after the https connection window is closed in the browser.
wi01073465	SNMP Notify Entries configured through EDM are getting lost after system reboot. In CLI, there are ACLI commands for this table creation because the notification entry is no longer required to be created separately for the Trap configuration,. EDM allows users to create/delete this entry. Once created in EDM, the device will not have the corresponding command to save the configuration.
wi01078084	With ports 1/47-1/48 , issues seen with display and access on VSP 4580 GTS and VSP 4580 GTS PWR+.
wi01080869	VRF ID does not show in VRF Context View Tab.
wi01080871	Detailed DDI info on the pluggables (SFPs) display the wrong wavelength.
wi01087193	ip->policy->RoutePolicyrclpRoutePolicySetRoutePreference is not supported (Needs to be removed).
wi01088592	You can right-click on GBIC ports without first selecting the ports. However, the UI does not select the port, and when you select enable or disable, the UC emits an error. The impact is on the VSP 4000 physical view only.

WI reference	Description
wi01088874	In a VRF context view, some values do not appear in the interface column of the VRF IP route table, but appear correctly in ACLI. The impact is on the VSP 4000 IP route table in a VRF context view.
wi01088994	EDM is not correctly reflecting SFP ports 47 thorough 50.