Release Notes - Release 3.1
Avaya Virtual Services Platform 4000

Release 3.1
NN46251-401
Issue 03.15
February 2014

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. “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 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 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, 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 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.

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.

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.

Contents

Chapter 1: Introduction

Purpose

This document describes important information about this 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 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.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, 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.

Note:

Videos are not available for all products.

Subscribing to e-notifications

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

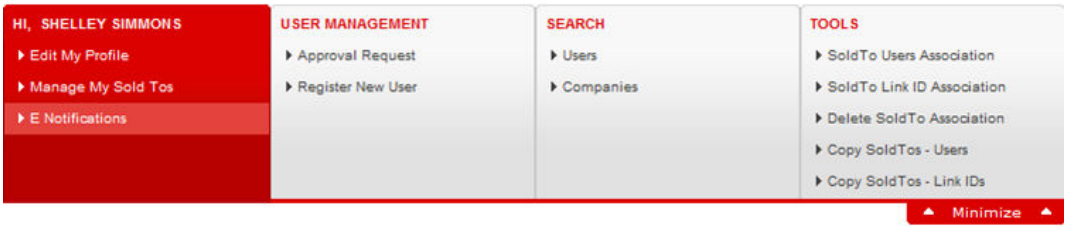
About this task

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.

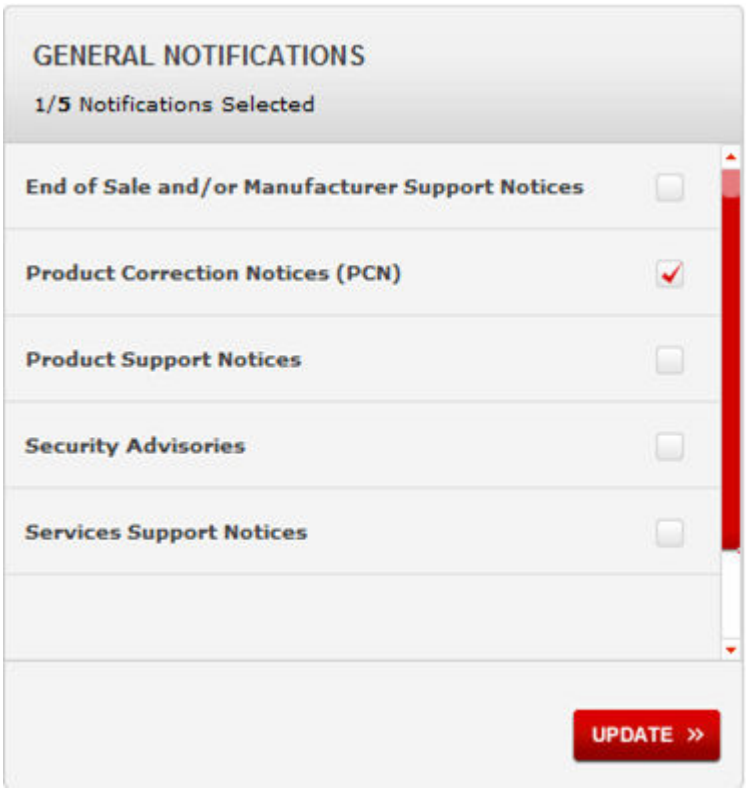
Procedure

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**.

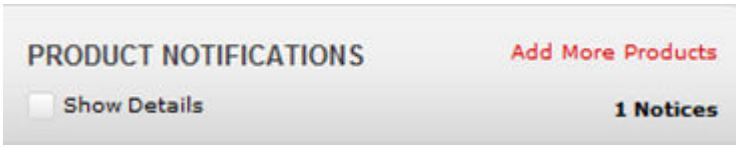
4. On the site toolbar, click your name, and then select **E Notifications**.



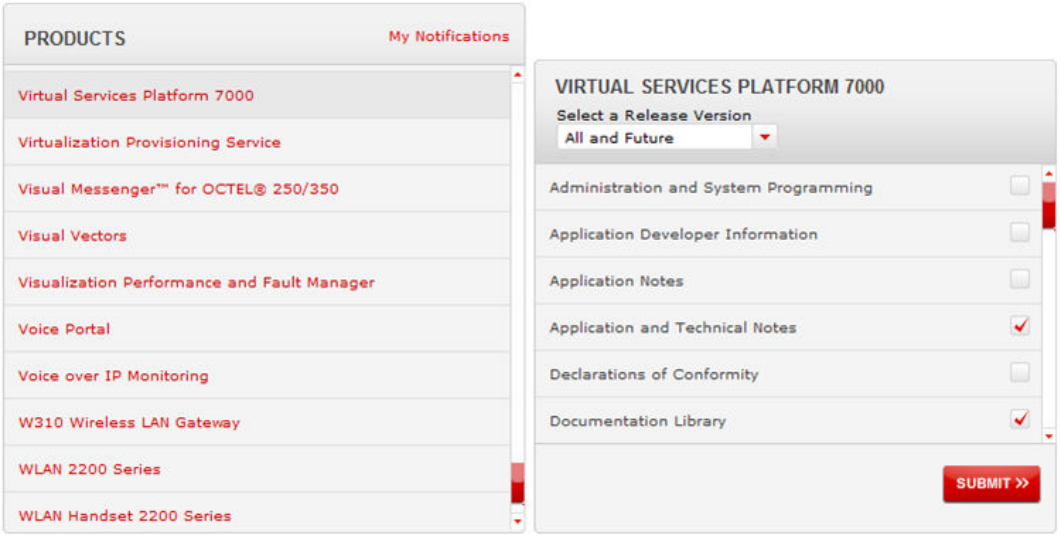
5. In the GENERAL NOTIFICATIONS area, select the required documentation types, and then click **UPDATE**.



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

The following sections detail what is new in the *Avaya Virtual Services Platform 4000 Release Notes*, NN46251–401 for release 3.1.

Features

The following table provides a listing of features that were introduced in the Virtual Services Platform (VSP) 4000 in releases 3.1, 3.0.1 and 3.0.

Click the link to view a short description of the feature. For more information on the features and their configuration, see the documents listed in the respective sections.

This document does not contain any feature updates.

Features	New in release		
	3.1	3.0.1	3.0
IP Multicast over SBPM on page 13	√		
Autogenerated CFM MEP and MIP levels on page 13	√		
BGP services on page 14	√		
OSPF and RIP on page 14	√		
Transparent UNI on page 14	√		
Private VLAN on page 15		√	
ETree configuration on page 15		√	
Inter-VSN Routing on page 14			√
9k Jumbo packet support on page 15			√
IEEE 802.1p/q Virtual LAN on page 15			√
Port and Protocol-based VLANs on page 16			√
IEEE 802.1d Mac Bridges Spanning Tree on page 16			√
IEEE 802.1w RSTP on page 16			√
IEEE 802.1s MSTP on page 17			√
MLT (Multilink trunking) on page 17			√

Features	New in release		
	3.1	3.0.1	3.0
IEEE 802.1ax (802.3ad) Link Aggregation Control Protocol (LACP) on page 17			√
Virtual LACP (VLACP) End-to-End connectivity check on page 17			√
Simple Loop Prevention Protocol (SLPP) on page 18			√
Diffserv framework on page 18			√
Ingress port policers on page 18			√
Egress port shapers on page 18			√
IP Brouter port on page 18			√
ARP and RARP on page 19			√
FTP Server on page 19			√
TFTP Client and Server on page 19			√
HTTP and HTTPS EDM management on page 19			√
Simple Network Management Protocol (SNMP) on page 19			√
Secure Shell and Secure Copy Server on page 20			√
Equal Cost MultiPath (ECMP) on page 20			√
Virtual Router Redundancy Protocol (VRRP) on page 20			√
DHCP Relay agent on page 20			√
IP Static routes on page 21			√
Virtual Routing Forwarding (VRF) Lite (24 instances) on page 21			√
Flight Recorder for system health monitoring on page 21			√
Avaya CLI (ACLI) on page 21			√
Port Mirroring ingress and egress on page 22			√
RADIUS on page 22			√
VRRP BackupMaster on page 22			√
VRRP BackupMaster on page 22			√
Line Rate Ingress and Egress Port and VLAN ACLs for L2 to L4 on page 22			√
Key Health Indicator (KHI) on page 23			√
SLPP Re-Arm on page 23			√
DHCP Relay Option 82 on page 23			√
Microsoft NLB ARP multicast-MAC-flooding support on page 23			√

Features	New in release		
	3.1	3.0.1	3.0
Secure Shell (SSH) client support on page 23			√
IEEE 802.1aq Shortest Path Bridging MACinMAC (SPBM) on page 23			√
IEEE 802.1ag Connectivity Fault Management (CFM) on page 24			√

New features in Release 3.1

IP Multicast over SBPM

The Virtual Services Platform 4000 supports IP multicast over Shortest Path Bridging MAC (SPBM). IP multicast over SPBM greatly simplifies multicast deployment, with no need for any multicast routing protocols such as PIM.

With IP multicast over SPBM, Avaya leads the industry with a new approach to transport IP multicast. SPBM uses Intermediate-System-to-Intermediate-System (IS-IS) as the control plane and relies on a Shortest Path Tree (SPT) on every switch to transport data across the Virtual Services Fabric. The Backbone Edge Bridge (BEB) can forward a multicast stream anywhere in an SPBM network where IS-IS advertises the stream to the rest of the fabric.

For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000*, NN46251–510.

Autogenerated CFM MEP and MIP levels

Release 3.1 simplifies Connectivity Fault Management (CFM) configuration with autogenerated CFM. With the simplified autogenerated CFM, you use the commands cfm spbm enable and cfm cmac enable and the device creates a default MD, MA, MEPs and MIPs.

You do not have to configure explicit MEPs and MIPs and associate multiple VLANs with MEPs and MIPs. Now you can use autogenerated CFM commands that create a MEP and MIP at a specified level for every SPBM Backbone VLAN (B-VLAN) or C-VLAN.

In Release 3.1, CFM also extends the debugging of Layer 2 networks to Customer VLANs (C15 VLANs).

- For SPBM B-VLANs, you can use either autogenerated or explicitly configured CFM MEPs.
- For C-VLANs, you can only use autogenerated CFM MEPs.

Important:

Previous explicit CFM configurations of MDs, MAs, and MEPs on SPBM B-VLANs continue to function in this release. However, if you want to enable the new autogenerated commands

you must first remove the existing MEP and MIP on the SPBM B-VLANs. VSP 4000 only supports one type of MEP or MIP for each SPBM B-VLAN.

If you choose to explicitly configure CFM, you must configure an MD, MA, and MEP ID. You do not have to configure an MD, MA, MIPs and MEPs if you configured autogenerated CFM, which enables the device to create a default MD, MA, MEPs, and MIPs for you.

For more information, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000*, NN46251–510.

Inter-VSN Routing

Inter-VSN routing allows routing between IP networks on VLANs with different I-SIDs. The Layer 2 VLANs must be in the same VRF. You cannot route traffic between two different VRFs with Inter-VSN routing.

Transparent UNI feature troubleshooting

Release 3.1, Virtual Services Platform 4000 supports the Transparent UNI feature.

Transparent UNI (T-UNI) assigns a port or MLT to an I-SID. This feature configures a transparent port where all traffic is MAC switched on an internal virtual port (I-SID). Multiple ports on the same unit and on other Backbone Edge Bridges (BEBs) are switched on a common I-SID. A port or MLT you assign to an I-SID as a Transparent UNI is referred to as a T-UNI port.

The T-UNI ports are fully transparent since tagged and untagged traffic is switched within the assigned I-SID, as well as any control protocol. T-UNI ports are not members of any VLAN, or any STG. T-UNI ports are always in a forwarding state.

CMAC learning is against the I-SID and the port or MLT instead of the C-VLAN. When a packet ingresses on a port or MLT that is associated with a T-UNI I-SID, the MAC lookup is based on I-SID.

BGP services

Support for the configuration of Border Gateway Protocol (BGP) services on the Avaya Virtual Platform (VSP) 4000 is introduced.

The following operations are supported by BGP:

- IPv4
- 4 byte AS
- Peer groups
- Redistribution

For more information, see *Avaya Virtual Services Platform 4000 Configuration — BGP*, NN46251–507.

OSPF and RIP

Support for the configuration of the Open Shortest Path First (OSPF) and the Routing Information Protocol (RIP) on the Avaya VSP 4000 is introduced.

OSPF is an Interior Gateway Protocol (IGP) that distributes routing information between routers that belong to a single autonomous system (AS). Intended for use in large networks,

OSPF is a link-state protocol that supports IP subnets, Type of Service (TOS)-based routing, and tagging of externally-derived routing information.

In routed environments, routers communicate with one another to track available routes. Routers can dynamically learn about available routes using the RIP. The Avaya VSP 4000 software implements standard RIP to exchange IP route information with other routers.

For more information, see *Avaya Virtual Services Platform 4000 Configuration — OSPF and RIP*, NN46251–506.

New features in Release 3.0.1

Private VLAN

Private VLANs provide isolation between ports within a Layer 2 service.

For more information about private VLANs, see *Avaya Virtual Services Platform 4000 Configuration — VLANs and Spanning Tree*, NN46251-500.

ETree configuration

Private VLANs consist of a primary and secondary VLAN. Etree allows the private VLANs to traverse a SPBM network by associating a private VLAN with an I-SID.

For more information about E-Tree configuration, see *Configuring Avaya VENA Fabric Connect on Avaya Virtual Services Platform 4000*, NN46251-510.

New features in Release 3.0

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 MLT 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.

For more information about SLPP, see *Avaya Virtual Services Platform 4000 Network Design Reference*, NN46251–200.

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 and 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 the 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 and 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)

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 and Secure Copy 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 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 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 and 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 4000 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 4000 Configuration – Shortest Path Bridging MAC (SPBM)*, NN46251–510.

Other Changes

See the following section for information about changes that are not feature-related.

Software upgrade

This document has been updated with software upgrade information for release 3.1. See Upgrading the software on page 39.

Software scaling capabilities

This document has been updated with software scaling capabilities information for release 3.1.
See Software scaling capabilities on page 28.

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

Software scaling capabilities

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

Table 2: Software scaling capabilities

	Maximum number supported
Layer 2	
IEEE/Port-based VLANs	4060
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

	Maximum number supported
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
OSPF areas (per system)	64
OSPF routes per VRF	16,000 **Note:** The maximum routes supported per VRF is 16000. The 16000 routes can be distributed across the 24 VRFs (+ GRT) in any manner. If all 24 VRFs are operational, 640 routes per VRF are supported.
OSPF routes	16,000
OSPF VRF support	24
e-BGP peers	12
e-BGP routes	16,000
Address Resolution Protocol (ARP) for each port, VRF, or VLAN (IPv4)	6,000 entries total
Circuitless IP interfaces	64
Maximum B-MACs	1000
ECMP routes	1000
ECMP groups	512 groups with a maximum of 4 ECMP paths per group **Note:** The maximum number of ECMP routes per VSP 4000 system is 1000. So, for example, if 500 ECMP groups are configured, the maximum number of ECMP paths per group is 2 and if 250 ECMP groups are configured, the

	Maximum number supported
	maximum number of ECMP paths per group is 4.
ECMP paths per route	4
FIB IPv4 routes	16,000
RIB IPv4 routes	16,000
IPv4 interfaces	256
Maximum VRFs	24
IPv4 CLIP interfaces	64
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 (IPv4)	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
Unique redirect next hop values for ACE Actions (IPv4)	Ingress: 1,536, Egress: 256
SPBM	
C-VLANs per VSP 4000 node	1000
Maximum number of nodes per region	1000

	Maximum number supported
MAC entries	16,000 (combination of ARP entries and Layer 2 MACs)
Backbone MAC	1,000
IP routes in the Global Router	16,000
Maximum IS-IS IP routes	16,000
IS-IS interfaces	24
IS-IS adjacencies per VSP 4000 node	24
Layer 2 VSN ISIDs per VSP 4000 node	1,000
Layer 3 VSN ISIDs per VSP 4000 node	24
IP Multicast over SPB	
Maximum unique IGMP group records per node	1000
Maximum unique Multicast Streams (S,G,V) sourced per node	1000
Maximum number of Multicast ISIDs (VSP 4000 acting as a BEB and/or BCB)	32,000
Maximum number of Layer 2 VSNs with Multicast enabled	1000
Maximum number of Layer 3 VSNs with Multicast enabled	24
Maximum number of IP interfaces with Multicast enabled	256
Number of remote senders that can be received on each VSP 4000 node, for the Universal Plug and Play Group (239.255.255.250)	3500
Maximum unique multicast streams sourced per VSP 4000 node	1000
T-UNI	
T-UNI ISIDs per VSP 4000 node	48
Maximum MAC limit on a T-Uni I-SID **Note:** This is also the device limit.	32,000

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 3: Software files

Module or file type	Description	File name	File size (bytes)
Standard Runtime Software Image	Standard image for Avaya Virtual Services Platform 4000 Series.	VSP4K.3.1.0.0.tgz	75,324,821
Encryption Module	Encryption module for Avaya Virtual Services Platform 4000 Series.	VSP4K.3.1.0.0_modules.tgz	37,799

Table 4: Enterprise Device Manager Help files

Module or file type	Description	File name	File size (bytes)
Enterprise Device Manager Help Files	Enterprise Device Manager Help files for Avaya Virtual Services Platform 4000 Series.	VSP4000v310_HELP_EDM_gzip.zip	2,070,690

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 5: Open Source software files

File name	Description	Size
VSP4K.3.1.0.0_oss-notice.html	Master copyright file. This file is located in the Licenses directory.	414231
VSP4K.3.1.0.0_OpenSource.zip	Open source base software for Virtual Services Platform 4000 Release 3.1.	95773148

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/3.1.0.0.GA/release/oss-notice.txt`.

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 26

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.

Shutting down VSP 4000

Use the following procedure to shut down VSP 4000.

Procedure

1. Enter the User EXEC configuration mode.
2. Shut down VSP 4000:
   ```
   sys shutdown [-y]
   ```

Example

```
VSP-4850GTS:1#sys shutdown

Are you sure you want shutdown the system? Y/N (y/n) ? y

CP1 [02/02/70 00:51:53.312] 0x00010813 00000000 GlobalRouter HW INFO
System shutdown initiated from CLI

CP1 [02/02/70 00:51:55.000] LifeCycle: INFO: Stopping all processes

CP1 [02/02/70 00:51:56.000] LifeCycle: INFO: All processes have
stopped

CP1 [02/02/70 00:51:56.000] LifeCycle: INFO: Stopping OS services and
powering down

INIT: Sending processes the TERM signal

Stopping OpenBSD Secure Shell server: sshdstopped /usr/sbin/sshd (pid
1981)

.

Stopping vsp...

Deconfiguring network interfaces... done.

Stopping syslogd/klogd: stopped syslogd (pid 1986)

stopped klogd (pid 1988)

done

Sending all processes the TERM signal...

Sending all processes the KILL signal...

hwclock: can't open '/dev/misc/rtc': No such file or directory

Unmounting remote filesystems...

Stopping portmap daemon: portmap.

Deactivating swap...

Unmounting local filesystems...

[2767637.035059] Power down.

[2767637.066389] System Halted, OK to turn off power
```

Chapter 4: Software Upgrade

Image upgrade fundamentals

This section details what you must know to upgrade the Virtual Services Platform 4000.

Upgrades

Install new software upgrades to add functionality to the Virtual Services Platform 4000. Major and minor upgrades are released depending on how many features the upgrade adds or modifies.

Upgrade time requirements

Image upgrades take less than 30 minutes to complete. The Virtual Services Platform 4000 continues to operate during the image download process. A service interruption occurs during the installation and subsequent reset of the device. The system returns to an operational state after a successful installation of the new software and device reset.

Before you upgrade the software image

Before you upgrade the Virtual Services Platform 4000, ensure that you read the entire upgrading procedure.

You must keep a copy of the previous configuration file (*config.cfg*), in case you need to return to the previous version. The upgrade process automatically converts, but does not save, the existing configuration file to a format that is compatible with the new software release. The new configuration file may not be backward compatible.

Related topics:

Image naming conventions on page 37
Interfaces on page 38
File storage options on page 38

Image naming conventions

VSP 4000 software use a standardized dot notation format. This standardized format is as follows:

Software images

Software images use the following format:

Product Name.Major Release.Minor Release.Maintenance Release.Maintenance Release Update.tgz

For example, the image file name **VSP4K.3.0.1.0.tgz** denotes a software image for the VSP 4K product with a major release version of 3, a minor release version of 0, a maintenance release version of 1and a maintenance release update version of 0. TGZ is the file extension.

The image file name **VSP4K.3.1.0.0.tgz** denotes a software image for the VSP 4K product with a major release version of 3, a minor release version of 1, a maintenance release version of 0 and a maintenance release update version of 0. TGZ is the file extension.

Interfaces

You can apply patches and upgrades, and add encryption modules to the Virtual Services Platform 4000 using the Avaya Command Line Interface (ACLI).

For more information about ACLI, see *Avaya Virtual Services Platform 4000 User Interface Fundamentals* (NN46251–103).

File storage options

This section details what you must know about the internal boot and system flash memory, Universal Serial Bus (USB) mass-storage device, and external flash, which you can use to store the files that start and operate the Virtual Services Platform 4000.

The Virtual Services Platform 4000 file system uses long file names.

Internal flash

The Virtual Services Platform 4000 has two internal flash memory devices: the boot flash memory and the system flash memory. The system flash memory size is 2 gigabytes (GB).

Boot flash memory is split into two banks that each contain a different copy of the boot image files. Only the Image Management feature can make changes to the boot flash.

The system flash memory stores configuration files, runtime images, the system log, and other files. You can access files on the internal flash through the /intflash/ folder.

File Transfer Protocol

You can use File Transfer Protocol (FTP) to load the software directly to the Virtual Services Platform 4000, or to download the software to the internal flash memory, external flash, or USB device.

The Virtual Services Platform 4000 can act as an FTP server. If you enable the FTP daemon (ftpd), you can use a standards-based FTP client to connect to the Control Processor (CP)

module by using the ACLI log on parameters. Copy the files from the client to either the internal flash memory or external flash.

Upgrading the software

Upgrade the Avaya Virtual Services Platform 4000 to add functionality.

The following are the supported software upgrade paths.

Upgrade path	Support
Upgrade 3.0 to 3.1	Supported
Upgrade 3.0.1 to 3.1	Supported

The image files required for the upgrade are:

- `VSP4K.3.1.0.0.tgz`
- `VSP4K.3.1.0.0_modules.tgz`
- `VSP4000v310_HELP_EDM_gzip.zip`

Before you begin

- Back up the configuration files.
- Ensure that you have not configured VLAN 4060. If you have, you must port all configuration on this VLAN to another VLAN, before you begin the upgrade.

Caution:

Starting from release 3.1, VLAN 4060 is not supported, and all configuration on this VLAN from previous releases will be lost after the upgrade.

Note:

Software upgrade configurations are case sensitive.

About this task

Perform the following procedure to upgrade 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.

It also contains steps to optionally FTP software image files from a server to the VSP 4000 system, before you begin the upgrade.

Note:

There is a limit of six software releases that can be stored on the VSP 4000 system. If you have six releases already stored on the VSP 4000 system, you will be prompted to remove

one release before you can proceed with adding and activating a new software release. For information about removing a software release, see Deleting a software release on page 46.

Procedure

1. Enter the Global Configuration mode:

   ```
   enable
   #configure terminal
   ```

2. On the VSP 4000 system, configure an in-band VLAN and a management IP interface for the VLAN.

   You can create VLANs in the range `1` to `4059`. In the following example, you create VLAN `20` and assign a management IP address of `10.9.8.1`.

   a. Create a VLAN:

      In this example, `0` is the instance Id. The range is `0` to `63`.

      ```
      (config)#vlan create 20 name Avaya type port-mstprstp 0
      ```

   b. Add VLAN members:

      ```
      (config)#vlan members add 20 1/1
      ```

      The usable port range is `1/1` to `1/50`.

   c. Configure a management IP interface for the VLAN (for example, `10.9.8.1`)

      ```
      (config)#interface vlan 20
      (config)#ip address 10.9.8.1 255.255.255.0
      ```

   d. Verify that the VSP 4000 system is reachable on this interface using the *Ping* utility.

3. (Optional) Perform the following steps to FTP software image files from a server on the network, to the VSP 4000 system. This step is not necessary if the image files are already on the VSP 4000 system.

   a. Configure a network interface between the VSP 4000 system and the server. Verify connectivity using the `show` command.

      In the following example, you establish connectivity on port `1/1` of the VSP 4000 system. The usable port range is `1/1` to `1/50`.

      ```
      (config)#interface gigabitEthernet 1/1
      (config-if)#no shut
      (config-if)#show interfaces gigabitEthernet
      (config-if)#exit
      ```

   b. (Optional) If the server is in a network that is different from that of the VSP 4000 system, configure an IP route.

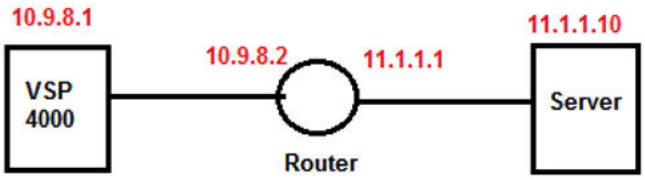


Figure 1: Example IP addresses for IP route configuration

```
(config)#ip route 11.1.1.0 255.255.255.0 10.9.8.2 weight
10
(config)#enable
```

c. Enable FTP on the VSP 4000 system.

```
(config)#boot config flag ftpd
(config)#enable
```

d. Enter Privileged EXEC configuration mode by exiting the Global Configuration mode.

```
(config)#exit
```

e. Verify network connectivity between the VSP 4000 and the server using the *Ping* utility.

f. FTP the software image files to the VSP 4000 system. Perform the following steps from the server.

`#ftp 10.9.8.1` (Log in using credentials `rwa/rwa`)

Navigate to the location of the files on the server, for example, `/intflash`.

```
ftp>cd /intflash
```

Set the FTP mode to Binary.

```
ftp>binary
```

Begin FTP

```
ftp>mput VSP*
```

Note:

The `mput VSP*` command allows you to select and FTP the image files one at a time.

When prompted, select `y` to the following image files:

- `VSP4K.3.1.0.0.tgz`
- `VSP4K.3.1.0.0_modules.tgz`
- `VSP4000v310_HELP_EDM_gzip.zip`

4. On the VSP 4000, extract the release distribution files to the `/intflash/release/` directory.

```
software add WORD<1-99>
```

Example: `#software add VSP4K.3.1.0.0.tgz`

5. (Optional) To install encryption modules on the system, extract the module files to the `/intflash/release` directory:

   `Software add-module [software version] [modules file name]`

   Example: `#software add-module 3.1.0.0.GA VSP4K.3.1.0.0_modules.tgz`

6. Install the image:

   `software activate WORD<1-99>`

   Example: `#software activate 3.1.0.0.GA`

7. Restart the Virtual Services Platform 4000 system:

   `#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.

8. After you restart the system, enter Privileged EXEC configuration mode:

   `#rwa`

   `#enable`

9. Confirm that the software is upgraded:

   `#show software`

10. Commit the software:

    `#software commit`

Example

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

VSP-4850GTS-PWR+:1#configure terminal

VSP-4850GTS-PWR+:1(config)#vlan create 20 name Avaya type port-
mstprstp 0

VSP-4850GTS-PWR+:1(config)#vlan members add 20 1/1

VSP-4850GTS-PWR+:1(config)#interface vlan 20

VSP-4850GTS-PWR+:1(config)#ip address 10.9.8.1 255.255.255.0

VSP-4850GTS-PWR+:1(config)#interface gigabitEthernet 1/1
```

```
VSP-4850GTS-PWR+:1(config-if)#no shut

VSP-4850GTS-PWR+:1(config-if)#show interfaces gigabitEthernet

VSP-4850GTS-PWR+:1(config-if)#exit
```

(Optional)
```
VSP-4850GTS-PWR+:1(config)#ip route 11.1.1.0 255.255.255.0
10.9.8.2 weight 10

VSP-4850GTS-PWR+:1(config)#enable

VSP-4850GTS-PWR+:1(config)#boot config flag ftpd

VSP-4850GTS-PWR+:1(config)#exit

VSP-4850GTS-PWR+:1#software add VSP4K.3.1.0.0.tgz

VSP-4850GTS-PWR+:1#software add-module 3.1.0.0.GA
VSP4K.3.1.0.0_modules.tgz

VSP-4850GTS-PWR+:1#software activate 3.1.0.0.GA

VSP-4850GTS-PWR+:1#reset
```

```
VSP-4850GTS-PWR+:1#show software
================================================================================
                    software releases in /intflash/release/
================================================================================
VSP4K.3.1.0.0int064 (Backup Release)
3.1.0.0.GA (Primary Release)

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

```
enable

VSP-4850GTS-PWR+:1#show software

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

Verifying the upgrade

Verify your upgrade to ensure proper Avaya Virtual Services Platform 4000 operation.

Procedure

1. Check for alarms or unexpected errors:
   ```
   show logging file tail
   ```
2. Verify all modules and slots are online:

```
show sys-info
```

Committing an upgrade

Perform the following procedure to commit an upgrade.

About this task

The commit function for software upgrades allows maximum time set by the commit timer (the default is 10 minutes) to ensure that the upgrade is successful. If you enable the auto-commit option, the system automatically commits to the new software version after the commit timer expires. If you disable the auto-commit option, you must issue the software commit command before the commit timer expires to commit the new software version, otherwise the system restarts automatically to the previous (committed) version.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. **(Optional)** Extend the time to commit the software:
   software reset-commit-time [<1–60>]
3. Commit the upgrade:
   ```
   software commit
   ```

Downgrading the software

Perform this procedure to downgrade the Avaya Virtual Services Platform 4000 from the current trusted version to a previous release.

Before you begin

Ensure that you have a previous version installed.

Procedure

1. Enter Privileged EXEC mode:
   ```
   enable
   ```
2. Activate a prior version of the software:
   ```
   software activate WORD<1-99>
   ```

3. 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 software change 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 expires. This feature ensures you can regain control of the system if an upgrade fails.

4. Commit the software change:
   `software commit`

   Important:

   If you do not enable the auto-commit functionality, you must commit the software change before the commit timer expires. This is an optional step otherwise.

5. Verify the downgrade:
   - Check for alarms or unexpected errors using the `show logging file tail` command.
   - Verify all modules and slots are online using the `show sys-info` command.

6. (Optional) Remove unused software:
   `software remove WORD<1-99>`

Related topics:

Variable definitions on page 45

Variable definitions

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

Variable	Value
activate WORD<1-99>	Specifies the name of the software release image.
add WORD<1-99>	Specifies the path and version of the compressed software release archive file.
remove WORD<1-99>	Specifies the path and version of the compressed software release archive file.

Deleting a software release

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

Note:

There is a limit of six software releases that can be stored on the VSP 4000 system. If you have six releases already stored on the VSP 4000 system, you will be prompted to remove one release before you can proceed with adding and activating a new software release. For information about removing a software release, see Deleting a software release on page 46.

For information about adding and activating a software release, see Upgrading the software on page 39.

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.3.1.0.0
```

Chapter 5: 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 6: Supported IEEE standards

IEEE standard	Description
802.1aq	Shortest Path Bridging (SPB)
802.1D	MAC bridges (Spanning Tree)
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

IEEE standard	Description
802.3i	10BaseT
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 7: 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

Request for comment	Description
RFC1340	Assigned Numbers
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 8: Supported request for comments

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

Request for comment	Description
RFC2598	An Expedited Forwarding PHB

Network management

Table 9: 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

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

MIBs

Table 10: 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

Request for comment	Description
RFC2578	Structure of Management Information v2 (SMIv2)
RFC2674	Bridges with Traffic MIB
RFC2787	Definitions of Managed Objects for the Virtual Router Redundancy Protocol
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 11: 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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB6—Simple Network Management Protocol (SNMP)	RFC1157	rfc1157.mib
STDMIB7—MIB for network management of Transfer Control Protocol/Internet Protocol (TCP/IP) based Internet MIB2	RFC1213	rfc1213.mib
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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
STDMIB26e—View-based Access Control Model (VACM) for the SNMP	RFC2575	rfc2575.mib
STDMIB26f —Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
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

Standard MIB name	Institute of Electrical and Electronics Engineers/ Request for Comments (IEEE/RFC)	File name
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 12: 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 6: 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 13: Known issues

Issue number	Description	Workaround
wi01142915	When you execute the `default SLPP` command without parameters, the command does not automatically set all SLPP parameters to default.	Always execute the `default SLPP` command with appropriate parameters. For example, to set the SLPP parameter `tx-interval` to default, execute the command `default slpp tx-interval`.
wi01138070	The 802.1 priority bits in the BVLAN tag are not copied to the I-Tag when traffic egresses out of the NNI port.	None
wi01144867	On the port that is removed from a T-UNI LACP MLT, non T-UNI configuration is blocked as a result of T-UNI consistency checks.	When a port is removed from a T-UNI LACP MLT, the LACP key of the port must be set to `default`.
wi01143509	Redundant RIP configuration is saved for BVLANs when configuration is saved in	None

Issue number	Description	Workaround
	verbose mode. Sourcing this configuration displays the error `RIP circuit for ifindex does not exist.`	
wi01142727	For traffic coming from an SPBM cloud and egressing VSP 4000 towards a UNI port, all client frames have the 802.1 priority bits set to zero, if ingress BEB is a VSP 9000 system.	None
wi01141429	The error message `GlobalRouter POE ERROR poeMgrPoeDefaultConfig: POE Driver error (bcm_poe_set_logical_port_map()` can be ignored if seen once or twice during boot up.	If the error message persists, verify that the POE driver on the hardware is up and running.
wi01141161	Traffic is not forwarded on a T-UNI LACP MLT, if the LACP MLT is *not* associated with a VLAN before adding to a T-UNI ISID.	Ensure that the LACP MLT is associated with a VLAN before adding to a T-UNI ISID. The associated VLAN can also be the default VLAN.
wi01134624	With an 8 port NNI MLT, a VSP 4000 system acting as BEB can support up to 600 multicast streams.	None
wi01127897	If the member ports of the MLT have MSTP disabled and one of the members is removed from the MLT, then all the ports in the original MLT configuration go into an MSTP-enabled state and MSTP re-converges.	Disable MSTP on all the member ports of the MLT after a port is removed from MLT.
wi01126761	Traffic convergence can take 3 to 6 seconds on NNI failover on a BEB with a large number (greater than 600) of L2 VSNs.	None

Issue number	Description	Workaround
wi01111785	Internal QoS remapping with filters is not working for certain UDP destination ports. This is due to the control packets in the VSP 4000 system that are assigned with a higher priority egress queue. The action to assign the incoming control packet with an egress queue is in conflict with the action of the egress queue derived from the internal QoS remapping with ACL filter. Hence, the internal QoS remapping with ACL filter does not work for those control packets.	The control packets received from the ingress port include the following: • Always assign queue-6: DHCP, BPDU, LLDP, SLPP, CFM, ARP, IST-ARP1, IST-SLM, BARP, EAP, PIM-MC, PIM-UC, RIPv2, RIPv1, OSPF-MC, OSPF-UC, IGMP, BGP, TELNET, SSH, RSH, RLOGIN, TFTP, FTP, RADIUS, NTP, ICMP, HTTP, HTTPS, IPV6-ND. • Always assign queue-7: ISIS control, LACP, VLACP, VRRP, SNMP, IST
wi01114420	When a route is redistributed into ISIS, you may see the following warning message: `SW WARNING ISIS local rmap head is null, using global.` This message provides additional information for the development team and does not indicate any operational errors; it can be safely ignored.	None.
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. If incoming client packets are tagged, the VSP 4000 system always derives the internal priority queue from the 802.1p tag.	None.
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.	None.

Issue number	Description	Workaround
	If incoming client packets are untagged, the internal priority queue of the VSP 4000 is always the best-effort queue.	
wi01135628	Qos filter acl to remark dot1p for tagged unicast, unknown unicast, and multicast traffic fails on an l2 trusted T-UNI port.	For any packet coming on a T-UNI port, you can use internal-qos to set the qos level instead of remark-dot1p.
wi01136168	The `metric` field in the `redistribute` command is not supported for inter-VRF redistributed routes. This impacts only inter-VRF metric settings. It does not impact inter-VRF route filtering.	
wi01136379	A node configured with all supported features, booted with base license loses all T-UNI configuration.	Loading a node with a base license fails to load configurations related to the IP VRF, ISIS SPBM IPVPN CONFIGURATION. This occurs when you exit a configuration mode after exiting multiple times in the configuration syntax.
wi01137696	A port/vlan based filter created for CFM, OSPF, RIP, PIM, or VRRP control protocols with a Deny/Permit action (ACE or Global-ctrl-pkt action), based on ethertype/ip/other qualifiers will bypass the filter rules. A port based filter created on T-UNI port or MLT for LACP, VLACP control protocols with a Deny/Permit action (ACE or Global-ctrl-pkt action), based on ethertype/ip/other qualifiers will bypass the filter rules.	None
wi01137736	On a base VSP 4000 system with revision 10 hardware	None

Issue number	Description	Workaround
	and POE support, PAUSE frames are not supported.	
wi01138595	The OUTLOSS PACKETS counter value increments when packets are dropped as a result of Source Port squelching on T-UNI ports.	None
wi01140395	Pinging a remote IP address over VRF does not work unless the source IP address is specified.	None. This behavior is as designed.

EDM related issues

Table 14: Known issues

Issue number	Description	Workaround
wi01096275	The EDM tab **IS-IS** > **Stats** > **IS-IS** > **Interface Counters and Tab** > **Stats** > **Interface Control Packet** shows 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.
wi01132300	In EDM, the output of the T-UNI ISID FDB entries when filtered on a port that is part of an MLT, is not consistent with the ACLI output.	In EDM, enter the corresponding MLT ID instead of the port.

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 15: Limitations and expected behaviors

Issue number	Description
wi01145099	IP multicast packets with TTL=1 are not switched across the SPB cloud over an L2 VSN. They are dropped by the ingress BEB. To prevent IP multicast packets from being dropped, configure multicast senders to send traffic with TTL >1.
wi01138851	Configuring and Retrieving licenses using the EDM is not supported.
wi01112491	IS-IS enabled ports cannot be added to an MLT. The current release does not support this configuration.
wi01142142	When a multicast sender moves from one port to another within the same BEB, with the old port operationally up, the source port information in the output of the `show ip igmp sender` command is not updated with new sender port information. You can perform one of the following workarounds: • On an IGMP snoop enabled interface, you can flush IGMP sender records. **Caution:** Flushing sender records can cause a transient traffic loss. • On an IGMP enabled L3 interface, you can toggle the IGMP state. **Caution:** Expect traffic loss until IGMP records are built after toggling the IGMP state.
wi01143223	Hosts connected to a VSP 4000 system acting as a VRRP backup-master, cannot ping the VRRP virtual IP, if the VRRP session is established over an L2–VSN between the VRRP master and backup-master for that VLAN. However, traffic from the hosts is routed by the VRRP backup-master, and the ARP for the VRRP virtual IP is resolved.
wi01141638	When a VLAN with 1000 multicast senders is deleted, the console or telnet session hangs and SNMP requests time out for up to 2 minutes.
wi01137195	A static multicast group cannot be configured on an L2 VLAN before enabling IGMP snooping on it. After IGMP snooping is enabled on the L2 VLAN for the first time, static multicast group configuration is allowed, even when IGMP snooping is disabled later on that L2 VLAN.
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 .

Issue number	Description
	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 .

Chapter 7: Resolved issues

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

Table 16: Resolved issues

WI reference	Description
Device related issues	
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.
wi01094114	The CLI `copy` command may in some cases not return an error if the remote FTP or TFTP server cannot accept the file due to a full disk. The file may be created with a file size of zero.
wi01096785	The ARP aging timer is broken.
wi01098428	On an Etree setup, after isis is reset, the mac entries are not learned.
wi01078025	On import, 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.
wi01091986	On one occasion a core dump has been detected following the `reset` command as the system was shutting down; the reboot sequence completed successfully and the switch came back online.
wi01093170	The show clock does not display the updated time-zone value.
wi01093913	The one shot `snmpset` command does not work for the creation and isid set for an Etree Private VLAN.
wi01094391	Configuration of BVLAN with vlan id 1, under router isis should not be allowed.
wi01094393	Unable to provide the burst-count value with the `loopback` command when the `interframe-interval` option is used.
wi01094840	The following message appears when the switch is booting: `WARNING: Check dummy: modes fastethernet_interface_configurationspanning-tree`.
wi01095494	QoS Code clean up and functionality on a 10G port when in 1G mode should have the same functions that the 1G ports use.
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

WI reference	Description
	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
wi01096838	Disable L3VSN Mac learning.
wi01098490	The license logging event ID 0x000000658 is shared with/by the internal error code log.
wi01098746	Port the fix that resolved the nnclinnclip segmentation fault.
wi01099822	If you assign a Vlan name that is longer than the display field for the commands `show vlan basic`, and `show vlan advance`, then the alignment of `show vlan advance` is improper in the output.
wi01100726	Cannot disable `ip routing` on a VRF
wi01101004	Support for `control-packet-action` of the ACL default action in ACLI is required.
wi01103000	The debug config file should not be overwritten.
wi01103789	The L3 VSN router is not learnt when there are 256 IP interfaces; and is not learnt dynamically if you delete 2 IP addresses. The workaround is to disable and then enable the router isis.
wi01104529	Customer ARP and ICMP request packets with VLAN priority 0 received on a UNI interface are being transmitted out the NNI interface with BVLAN priority equal to 6.
wi01105101	`GlobalRouter ISIS ERROR plsbScProcessBmac:getPortFromMgid Failed:Dest: 00bb.0000.6500.00 VlanId:4001 mgid 229 port 1/38.`
wi01105277	The system displays the wrong error when you change `encap dot1q` for `lacp mlt`.
wi01106504	Remove command `slot shutdown` because there is no Out-Of-Band Mgmt port.
wi01108234	The system displays the following error after boot: `0x0031c605 00000000 GlobalRouter POE ERROR poeMgrPoeDefaultConfig: POE Driver error (bcm_poe_set_logical_port_map() error: -4).`
wi01108248	Requires port fix for SPB crash.
wi01108477	The `flight-recorder archive` command logs SW Error Process died messages.
wi01108927	SNMP MIB walk stack dumps switch.
wi01108939	SNMP failure on isis `TimeStamp definition`.
wi01110177	EDM: changing the `encap dot1q` for an `lacp` interface fails with unknown error.

WI reference	Description
wi01110188	The `copy clilog` command executes with errors referring to the VSP 9000 platform.
wi01110194	Enabling edge port on an MLT interface fails with the error `operation not allowed`, and with the console and log message `GlobalRouter HW INFO Admin Edge Port status changes will take effect only after the port is bounced`.
wi01110914	The command `sysDescr` does not return the correct format which causes COM to not identify the device.
wi01111182	The brouter port vlan should not be allowed to be configured as the ACL inVlan.
wi01111396	Mirrored traffic seen on an private MLT port, from a filter created to permit , count, and mirror all pvlan traffic to a destination mlt, is never removed even after the filter is deleted.
wi01111398	Mirroring a port to a destination MLT fails. If the port to which the mirrored traffic is hashed, then the port is shut down.
wi01112536	The switch crashes when you delete ISIS SPBM configuration through COM 3.0.2 from EDM 3.0.1.
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.
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.
wi01097860	Auxiliary 2 Monitoring should not be implemented for SFP/SFP+ in the `show pluggables` command.
wi01098477	**EDM ISIS** > **ISIS** > **Adjacency & EDM ISIS** > **ISIS** > **Protocol Summary** is not lining up with ACLI.
wi01103444	The default ISIS system ID in `config` does not load after boot.
wi01112181	The rc.0 file can cause continuous crash and reboot if the command in rc.0 is not a VSP 4000 known command.
wi01094633	The command `clear mlt` must be removed from CLI.
EDM related issues	
wi01096060	EDM fails the port stat refresh when table items are selected and the bar graph is selected with cumulative results.
wi01096082	EDM fails stat refresh when 15 or more ports are selected.

WI reference	Description
wi01096089	EDM fails stat refresh for cumulative results when you clear the results.
wi01098835	In EDM, the VRF ip route table interface information is not displayed for route entry.
wi01101458	The range for Vlan aging time must be changed from 0...1000000 to 0.
wi01103729	When you have private vlans, and then create a new mlt and refresh EDM to view the updated vlan list, EDM experiences an endless loop and eventually times out.
wi01105461	There is inconsistent behavior when you create a vlan of type protocol ipv6 using ACLI and EDM.
wi01107796	If you launch EDM through COM, the ARP table for the VRF window does not populate with any entries.
wi01109986	If you launch EDM through COM, the Vlan FDB aging time does not allow you to configure on VRF, and does not display timer information.
wi01110515	If you open a 6th EDM session, the system closes an existing EDM session before opening a new session.
wi01110811	In EDM, the ip route VRF table displays the wrong interface id.
wi01113271	If you launch EDM through COM, the ip route VRF table displays the wrong interface id.
wi01103336	In EDM, the cp-limit tab must be removed from MLT because cp-limit support has been removed in VSP 4000.