Avaya Virtual Services Platform 7000 Series Configuration Layer 2

10.0
NN47202-502, 01.03
August 2011

© 2011 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Copyright

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

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: New in this release

Configuring Layer 2 (NN47202-502) is a new document for Release 10.0 of the Avaya Virtual Services Platform 7000 Series.

Comments? infodev@avaya.com

Chapter 2: Virtual Local Area Network fundamentals

The Avaya Virtual Services Platform (VSP) 7000 Series supports up to 256 Virtual Local Area Networks (VLANs).

Important:

In Avaya Virtual Services Platform 7000, the target scaling number is up to 4,096 concurrent VLAN IDs with the scaling capacity limited to 1,024 simultaneous VLANs. It supports up to a maximum of 1,024 VLANs.

Ports are grouped into broadcast domains by assigning them to the same VLAN. Frames received in one VLAN can only be forwarded within that VLAN, and multicast frames and unknown unicast frames are flooded only to ports in the same VLAN.

Setting up virtual LANs (VLAN) is a way to segment networks to increase network capacity and performance without changing the physical network topology. With network segmentation, each switch port connects to a segment that is a single broadcast domain. When you configure a switch port to be a member of a VLAN, you add it to a group of ports (workgroup) that belong to one broadcast domain.

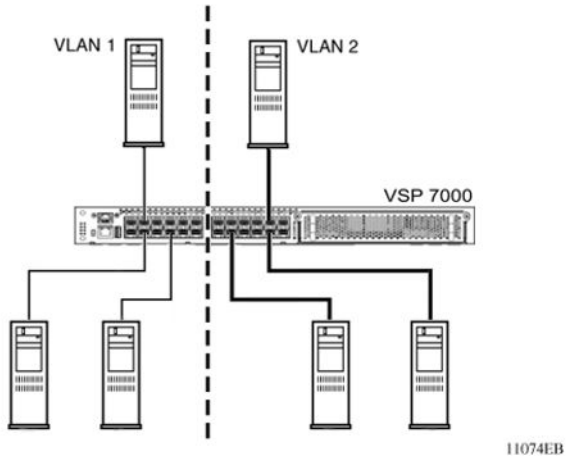

Figure 1: Port-based VLAN

With the Avaya VSP 7000 Series, you can assign ports to VLANs using the Command Line Interface. You can assign different ports (and their devices) to different broadcast domains. This feature provides network flexibility because you can assign VLANs to accommodate network moves, additions, and changes, eliminating the need to change physical cabling.

IEEE 802.1Q Tagging

The Avaya Virtual Services Platform (VSP) 7000 Series operate in accordance with the IEEE 802.1Q tagging rules. Important terms used with the 32-bit 802.1Q tagging feature are:

VLAN identifier (VID) -- the 12-bit portion of the VLAN tag in the frame header that identifies an explicit VLAN. When you enable other types of VLANs, this default value can be overridden by the values enabled in the management interfaces.

The default configuration settings for the Avaya VSP 7000 Series have all ports set as untagged members of VLAN 1 with all ports configured as PVID = 1. Every VLAN is assigned a unique VLAN identifier (VID) that distinguishes it from all other VLANs. In the default configuration example shown in the following figure, all incoming packets are assigned to VLAN 1 by the default port VLAN identifier (PVID =1). Untagged packets enter and leave the switch unchanged.

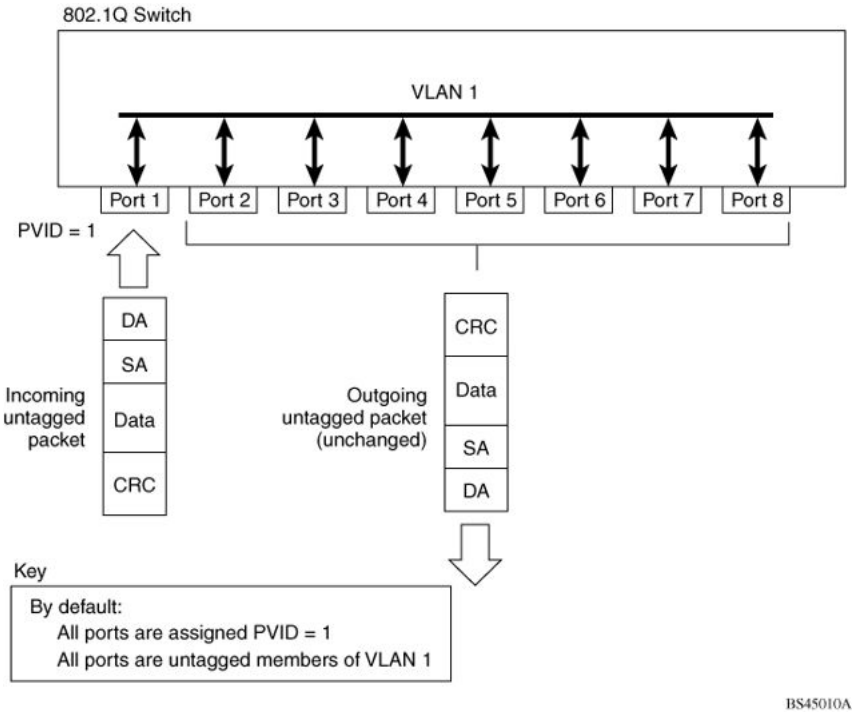

Figure 2: Default VLAN Settings

You can configure switch ports to transmit frames tagged on some VLANs, and untagged on other VLANs.

When VLANs are configured, you can configure the egress tagging of each switch port as *Untag All*, *Untag PVID Only*, *Tag All* or *Tag PVID Only*.

Comments? infodev@avaya.com

In the following figure, untagged incoming packets are assigned directly to VLAN 2 (PVID = 2). Port 5 is configured as a *tagged* member of VLAN 2, and port 7 is configured as an *untagged* member of VLAN 2.

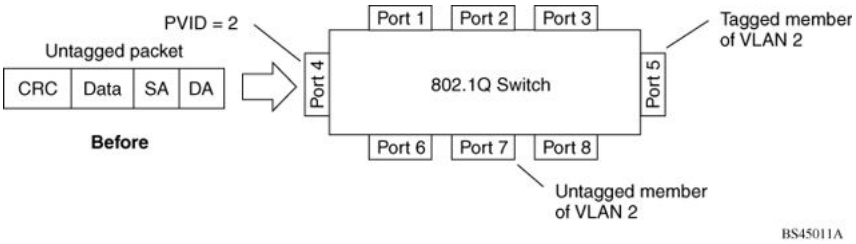

Figure 3: Port-based VLAN assignment

As shown in the following figure, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

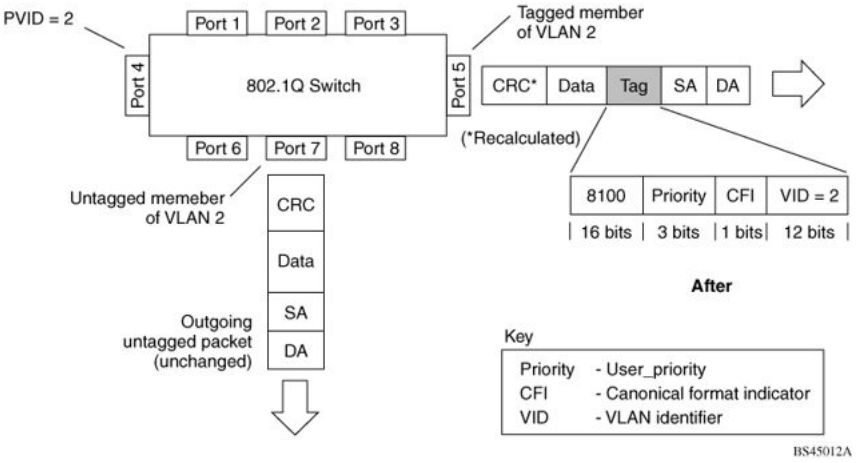

Figure 4: 802.1Q tagging (after port-based VLAN assignment)

Tagged incoming packets are assigned directly to VLAN 2 because of the tag assignment in the packet. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

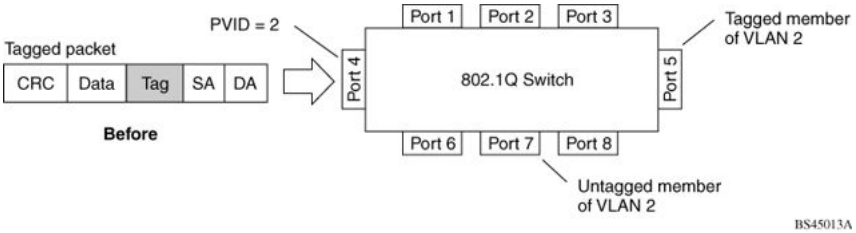

Figure 5: 802.1Q tag assignment

As shown in the next figure, the tagged packet remains unchanged as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. However, the tagged

packet is stripped (untagged) as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

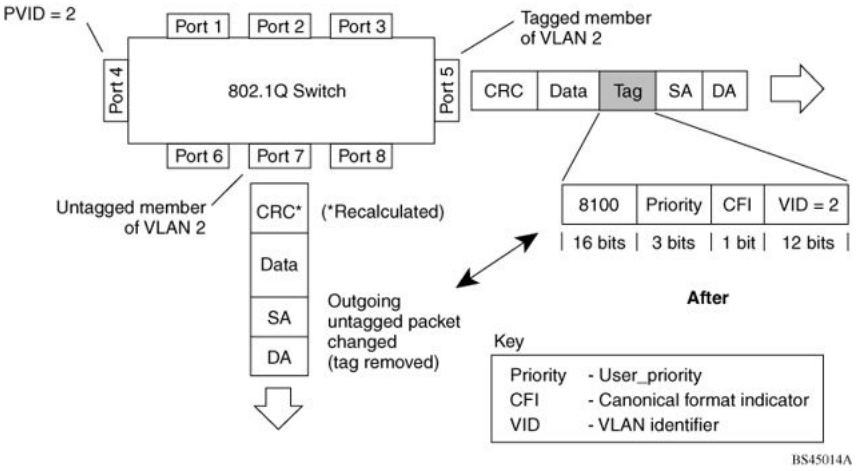

Figure 6: 802.1Q tagging (after 32–bit 802.1Q tag assignment)

As shown in the following figure, untagged incoming packets are assigned directly to VLAN 2. Port 5 is configured as a tagged member of VLAN 2, and port 7 is configured as an untagged member of VLAN 2.

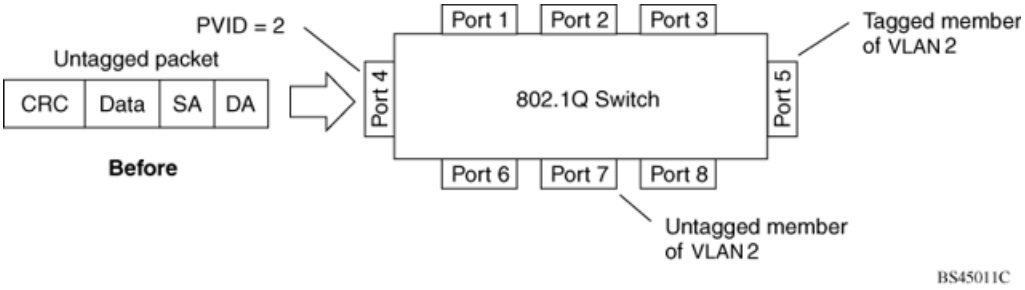

Figure 7: 802.1Q tag assignment

As shown in the next figure, the untagged packet is marked (tagged) as it leaves the switch through port 5, which is configured as a tagged member of VLAN 2. The untagged packet remains unchanged as it leaves the switch through port 7, which is configured as an untagged member of VLAN 2.

Comments? infodev@avaya.com

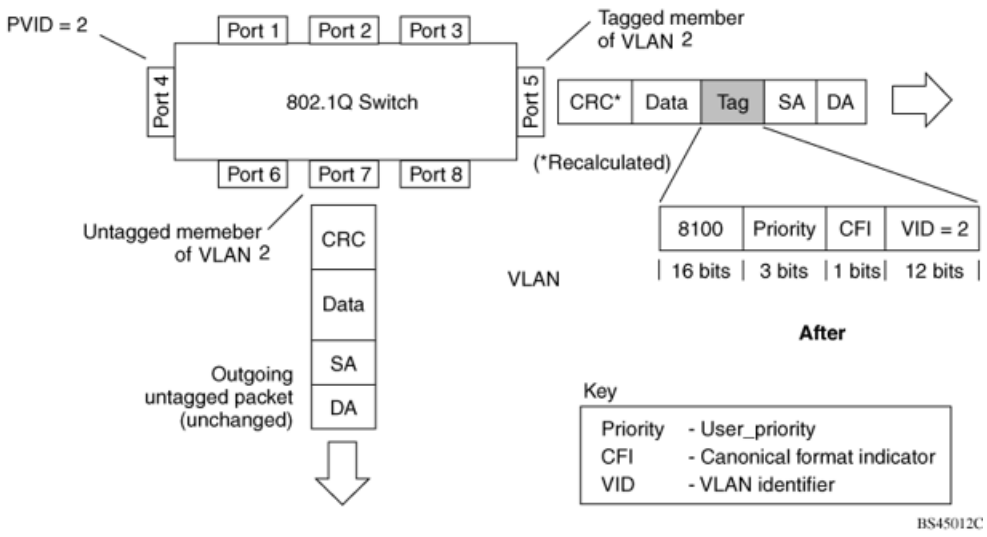

Figure 8: 802.1Q tagging (after 30–bit 802.1Q tag assignment)

VLANs Spanning Multiple Switches

You can use VLANs to segment a network within a switch. When multiple switches are connected, you can connect users of one VLAN with users of that same VLAN in another switch. However, the configuration guidelines depend on whether both switches support 32-bit 802.1Q tagging.

With 32-bit 802.1Q tagging enabled on a port for a VLAN, all frames leaving the port for that VLAN are marked as belonging to that specific VLAN. You can assign specific switch ports as members of one or more VLANs that span multiple switches, without interfering with the Spanning Tree Protocol.

VLANs spanning multiple 802.1Q tagged switches

The figure that follows shows VLANs spanning two Avaya Virtual Services Platform (VSP) 7000 switches. The 32-bit 802.1Q tagging is enabled on S1, port 6 and on S2, port 5 for VLAN 1 and VLAN 2. Both ports are tagged members of VLAN 1 and VLAN 2.

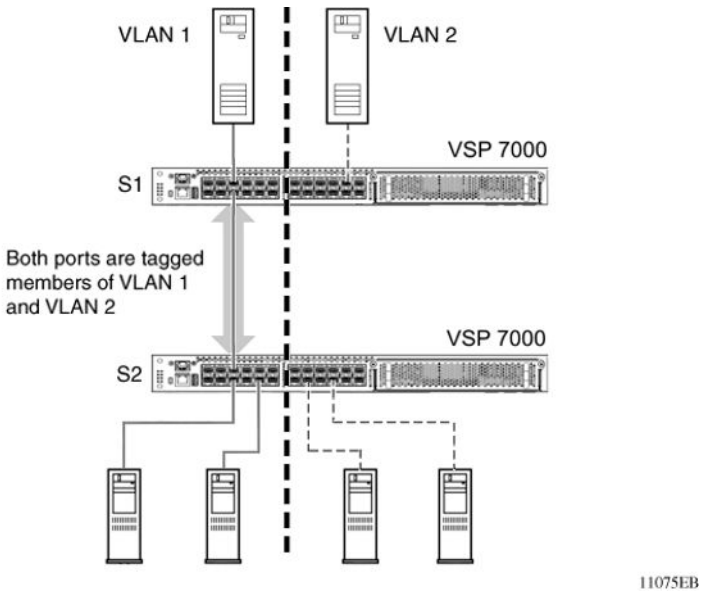

Figure 9: VLANs spanning multiple 802.1Q tagged switches

Because only one link exists between the two switches, the Spanning Tree Protocol (STP) treats this configuration as any other switch-to-switch connection. For this configuration to work properly, both switches must support the 32-bit 802.1Q tagging protocol.

VLANs spanning multiple untagged switches

The following figure shows VLANs spanning multiple untagged switches. In this configuration, Switch S2 does not support 32-bit 802.1Q tagging and you must use a single switch port on each switch for each VLAN.

For this configuration to work properly, you must set spanning tree participation to Disabled (the STP is not supported across multiple LANs).

Comments? infodev@avaya.com

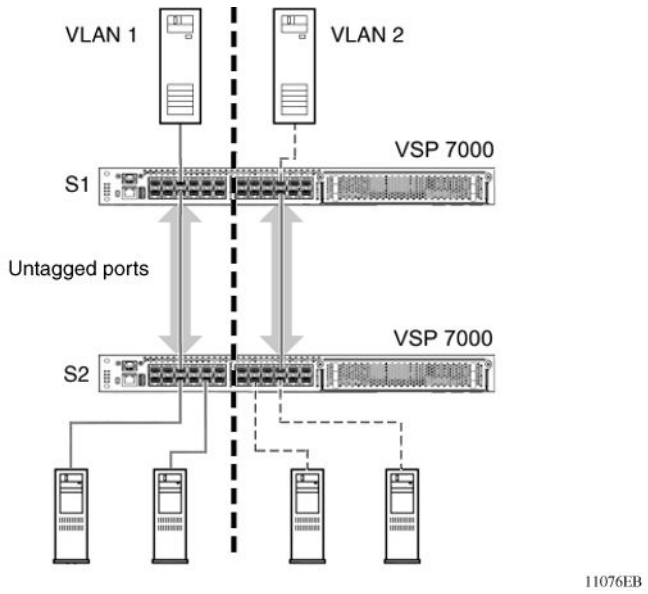

Figure 10: VLANs spanning multiple untagged switches

When the STP is enabled on these switches, only one link between the pair of switches forwards traffic. Because each port belongs to only one VLAN at a time, connectivity on the other VLAN is lost. Exercise care when configuring the switches to ensure that the VLAN configuration does not conflict with spanning tree configuration.

To connect multiple VLANs across switches with redundant links, you must disable the STP on all participating switch ports. The figure on the next page shows possible consequences of enabling the STP when using VLANs between untagged (non-802.1Q tagged) switches.

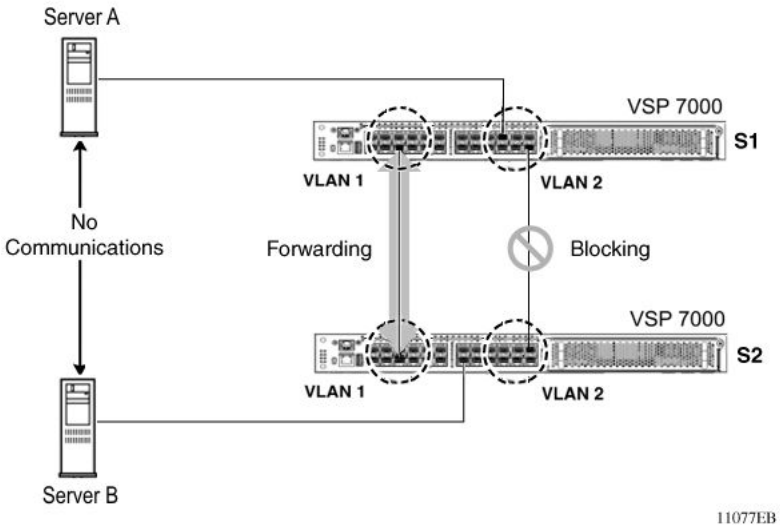

Figure 11: Possible problems with VLANs and Spanning Tree Protocol

As shown in the preceding diagram, with STP enabled, only one connection between Switch S1 and Switch S2 is forwarding at any time. Communications failure occurs between VLAN 2 of S1 and VLAN 2 of S2, blocking communications between Stations A and B.

The STP selects the link connecting VLAN 1 on Switches S1 and S2 as the forwarding link based on port speed, duplex-mode, and port priority. Because the other link connecting VLAN 2 is in Blocking mode, stations on VLAN 2 in Switch S1 cannot communicate with stations in VLAN 2 on Switch S2. With multiple links only one link will be forwarding.

VLAN Summary

This section summarizes the VLAN examples discussed in the previous sections.

As shown in the figure on the next page, Switch S1 (Avaya Virtual Services Platform 7000 Series) is configured with multiple VLANs:

- Ports 5, 8, 13, and 14 are in VLAN 1.
- Ports 4, 6, 7, 9, and 12 are in VLAN 2.
- Port 10 is in VLAN 3.

Because S4 does not support 32-bit 802.1Q tagging, a single switch port on each switch must be used for each VLAN.

The connection to S2 requires only one link between the switches because S1 and S2 are both Avaya Virtual Services Platform Series switches that support 32-bit 802.1Q tagging (see **VLANs spanning multiple untagged switches**).

Comments? infodev@avaya.com

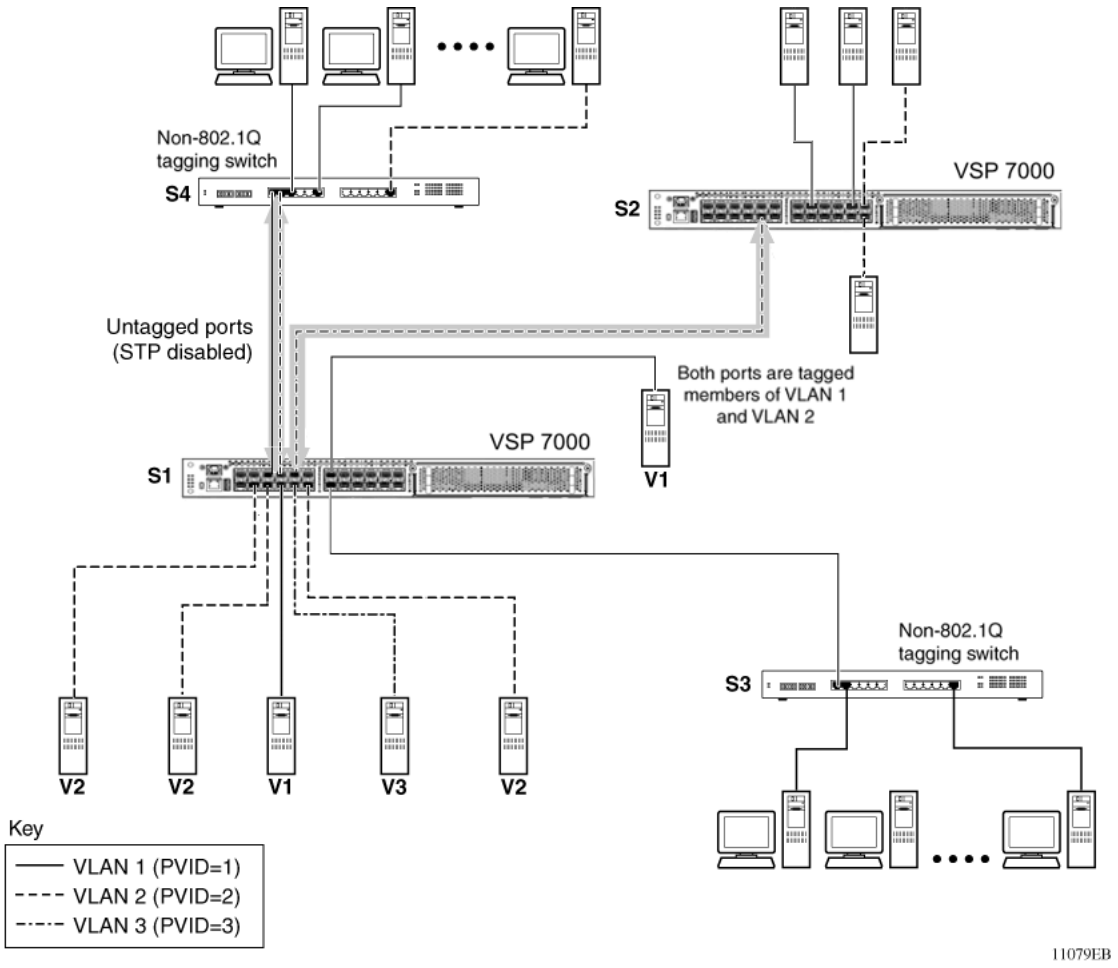

Figure 12: VLAN configuration spanning multiple switches

VLAN Configuration Rules

VLANs operate according to specific configuration rules. When creating VLANs, consider the following rules that determine how the configured VLAN reacts in any network topology:

- If a port is a trunk group member, all trunk members are added or deleted from the VLAN.
- All ports involved in trunking must have the same VLAN configuration.
- VLANs are not dependent on Rate Limiting settings.

VLAN Configuration Control

VLAN Configuration Control (VCC) allows a switch administrator to control how VLANs are modified. VLAN Configuration Control is a superset of the existing AutoPVID functionality and incorporates this functionality for backwards compatibility. VLAN Configuration Control is globally applied to all VLANs on the switch.

VLAN Configuration Control offers four options for controlling VLAN modification:

1. *Strict* — This option restricts the addition of an untagged port to a VLAN if it is already a member of another VLAN. To add an untagged port to a new VLAN, the switch administrator must remove the port from all other VLANs of which it is a member before adding it to the new VLAN. The PVID of the port is changed to the new VID to which it was added.

   Note:
   Strict is the factory default setting.

2. *Automatic* — This option automatically adds an untagged port to a new VLAN and automatically removes it from any previous VLAN membership. The PVID of the port is automatically changed to the VID of the VLAN it joins. Since the port is first added to the new VLAN, and then removed from any previous membership, the Spanning Tree Group participation of the port will not be disabled as long as the VLANs involved are in the same Spanning Tree Group.

3. *AutoPVID* — This option functions in the same manner as previous AutoPVID functionality. When an untagged port is added to a new VLAN, the port is added to the new VLAN and the PVID assigned to the new VID without removing it from any previous VLAN memberships. Using this option an untagged port can have membership in multiple VLANs.

4. *Flexible* —This option functions in a similar manner to disabling AutoPVID functionality. When this option is used, an untagged port can belong to an unlimited number of VLANs. Any new additions of an untagged port to a new VLAN does not change the PVID of that port.

VLAN Configuration Control is only applied to ports with the tagging modes of **Untag All** and **Tag PVID Only**. Ports with the tagging modes of **Tag All** and **Untag PVID Only** are not governed by VLAN Configuration Control. Ports with the tagging modes of **Tag All** and **Untag PVID Only** can belong to multiple VLANs regardless of VLAN Configuration Control settings and must have their PVID manually changed.

Important:
If you disable tagging on tagged ports when VCC is enabled, those ports are removed from all VLANs.

Comments? infodev@avaya.com

Chapter 3: Spanning Tree Protocol Fundamentals

The Avaya Virtual Services Platform (VSP) 7000 Series supports the Spanning Tree Protocol (STP) as defined in IEEE 802.1D. The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. When multiple paths exist, the spanning tree algorithm configures the network so that a bridge or switch uses only the most efficient path. If that path fails, the protocol automatically reconfigures the network to make another path become active, thus sustaining network operations.

The Avaya VSP 7000 platform supports multiple spanning tree groups (STG). It supports a maximum of 8 STGs, either all in one stand-alone switch or across a stack. Multiple STGs provide multiple data paths, which you can use for load-balancing and redundancy. Load balancing is enabled between two switches using multiple STGs by configuring each path with a different VLAN, and then assigning each VLAN to a separate STG. Each STG is independent. Each STG sends its own Bridge Protocol Data Units (BPDU), and each STG must be independently configured.

The STG, or bridge group, forms a loop-free topology that includes one or more virtual LANs (VLAN). The Avaya Virtual Services Platform 7000 supports multiple instances (8) of STGs running simultaneously.

The Avaya VSP 7000 Series supports a maximum of 256 VLANs. With a maximum of 8 STGs, on average, each STG can have 32 VLANs.

In the default configuration of the Avaya VSP 7000 Series, a single STG with the ID of 1 includes all ports on the switch. This STG is the default STG. Although you can add ports to or delet ports from the default STG, you cannot delete the default STG (STG1) itself from the system. Also you cannot delete the default VLAN (VLAN1) from STG1.

The tagging for the BPDUs from STG1, or the default STG, is user-configurable (as are tagging settings for all STGs). However, by default STG1 sends out only untagged BPDUs to operate with all devices that support only one instance of STP. (The default tagging of STG2 through STG8 is tagged.) The tagging setting for each STG is user-configurable.

Note:

If the STG is tagging a BPDU, the BPDU packet is tagged only on a tagged port. Also, ensure that the Filter Unregistered Frames option for the tagged port is disabled for this to function properly.

All other STGs, except the Default STG, must be created by the user. After an STG is created, at least one VLAN must be assigned to the STG before activating it. Also, to become active, each STG must be enabled by the user after the STG is created. Each STG is assigned an ID number from 2 to 8 (the Default STG is assigned the ID number 1). Ports or VLANs can also be assigned to an active STG. However, a port that is not a member of a VLAN is not allowed to join a STG.

When an STG is made active, all ports belonging to any assigned VLAN are automatically added to the STG.

When an STG is no longer needed, disable and delete it. After the STG is disabled, all ports in all VLANs assigned to that STG will have participation disabled. To assure a loop-free topology for these VLANs, move them to another active STG, before their current STG gets disabled.

You can configure a unique multicast address for STGs 1 to 4.

Note:
If a unique multicast address for an STG is configured, each device in that STG must also be configured with the same spanning tree multicast address.

STG Configuration Guidelines

This section provides important information about configuring STGs:

- An STG must be created by following these steps:
    a. Create the STG.
    b. Add the existing VLAN and port memberships
    c. Enable the STG
- When a VLAN is created, that VLAN automatically belongs to STG 1, the default STG. If the VLAN is to be in another STG, it must be moved by assigning it to another STG.
- A newly created VLAN must be moved to an existing STG by following these steps:
    a. Create the VLAN
    b. Add the VLAN to an existing STG
- VLAN1 cannot be moved or deleted from STG1.
- You can create and add VLAN X directly to STG Y with **`vlan create X type port Y`** from ACLI if STG Y exists.
- VLANs must be contained within a single STG; a VLAN cannot span multiple STGs. By confining VLANs within a single STG, you avoid problems with spanning tree blocking ports and causing a loss of connectivity within the VLAN. When a VLAN spans multiple switches, the VLAN must be within the same spanning tree group (have the same STG ID) across all the switches.
- A port that is not a member of any VLAN cannot be added to any STG. The port must be added to a VLAN, and that VLAN added to the desired STG.
- Tagged ports can belong to more than one STG, but untagged ports can belong to only one STG.

- When a tagged port belongs to more than one STG, the egress BPDUs are tagged to distinguish the BPDUs of one STG from those of another STG.
- Because some STP-compliant devices do not support tagging, you can configure whether to send tagged or untagged BPDUs, even from tagged ports. The VLAN ID for the tagged BPDUs is 4000+STG ID.
- The default VLAN ID for tagged BPDUs is as follows:
  - 4001--STG1
  - 4002--STG2
  - 4003--STG3
  - 4004--STG4
  - 4005--STG5
  - 4006--STG6
  - 4007--STG7
  - 4008--STG8
- You can select a VLAN ID for tagged BPDUs for each STG. Valid VLAN IDs are 1 to 4094.
- Tagged BPDUs cannot use the same VID as an active VLAN.
- An untagged port cannot span multiple STGs.
- When a port is removed from a VLAN that belongs to an STG, that port is also removed from the STG. However, if that port belongs to another VLAN in the same STG, the port remains in the STG.
- As an example, assume that port 1 belongs to VLAN1, and that VLAN1 belongs to STG1. When you remove port 1 from VLAN1, port 1 is also removed from STG1.

  However, if port 1 belongs to both VLAN1 and VLAN2 and both VLANs belong to STG1, removing port 1 from VLAN1 does not remove port 1 from STG1 because VLAN2 is still a member of STG1.

  An STG cannot be deleted until you disable it.
- You can configure a unique multicast address for STGs 1 to 4 only.

Spanning Tree Fast Learning

Spanning Tree Fast Learning is an enhanced port mode supported by the Avaya Virtual Services Platform (VSP) 7000 Series. If Spanning Tree Fast Learning is enabled on a port with no other bridges, the port is brought up more quickly after a switch initialization or a spanning tree change. The port goes through the normal blocking and learning states before the

forwarding state, but the hold times for these states is the bridge hello timer (2 seconds by default) instead of the bridge forward delay timer (15 seconds by default).

The port set with Fast Learning can forward data immediately, as soon as the switch learns that the port is enabled.

Fast Learning is intended for access ports in which only one device is connected to the switch (as in workstations with no other spanning tree devices). For these ports, it is not desirable to wait the usual 30 to 35 seconds for spanning tree initialization and bridge learning.

Note:

Use Spanning Tree Fast Learning with caution. This procedure is contrary to that specified in the IEEE 802.1D standard for Spanning Tree Protocol (STP) in which a port enters the blocking state after the initialization of the bridging device, or after a return from the disabled state when the port is enabled through configuration.

STG port membership mode

IEEE 802.1D STGs support two different STP port membership modes: normal and auto. In the normal mode, when a port is assigned to VLAN X and VLAN X is in STP group Y, the port does not automatically become a member of STP group Y. In the auto mode, when a port is assigned to VLAN X and VLAN X is in STP group Y, the port automatically becomes a member of STP group Y.

802.1t path cost calculation

You can set the switch to calculate the STG path cost using either the IEEE 802.1d standard or the IEEE 802.1t standard. The 802.1t standard is a maintenance extension to the 802.1d standard.

Chapter 4: Multi-Link Trunking fundamentals

Multi-Link trunks

With Multi-Link trunks, you can group up to four switch ports together to form a link to another switch or server, thus increasing aggregate throughput of the interconnection between the devices . You can configure up to 12 Multi-Link trunks, with a maximum of 4 links for each trunk. The maximum bandwidth for each trunk is 40 Gigabytes. Multi-Link Trunking software detects misconfigured (or broken) trunk links and redirects traffic on the misconfigured or broken trunk link to other trunk members within that trunk.

You can use the Avaya Command Line Interface (ACLI) to create switch-to-switch and switch-to-server Multi-Link trunk links.

Hierarchical server configuration using Multi-Link trunks

The following figure shows an example of how you can use Multi-Link Trunking in a client/server configuration. In this example, two servers connect directly to Switch S1. FS2 is connected through a trunk configuration. The switch-to-switch connections are through trunks.

Client servers accessing data from the FS1 and FS2 servers are provided with maximized bandwidth through trunks T1, T2, T3, T4, and T5. Trunk members (the ports making up each trunk) do not have to be consecutive switch ports; you can select ports randomly, as shown by T5.

With spanning tree enabled, one of the trunks (T2 or T3) acts as a redundant (backup) trunk to Switch S2. With spanning tree disabled, trunks T2 and T3 must be configured into separate VLANs for this configuration to function properly.

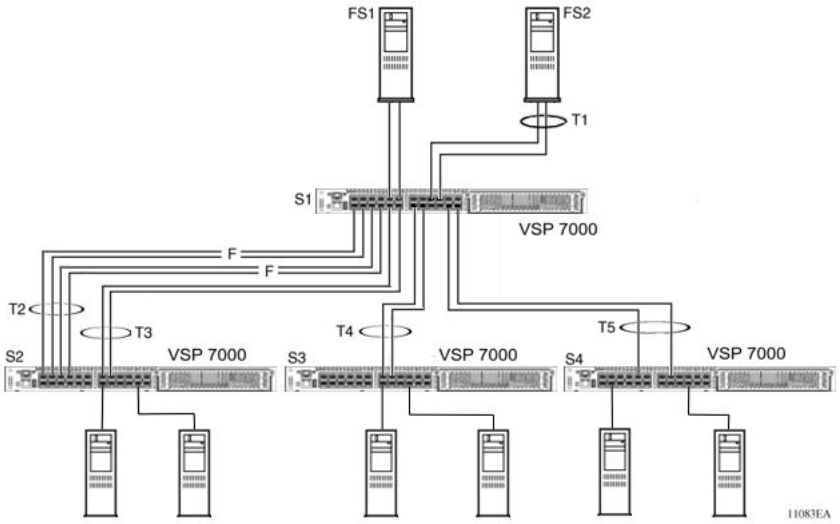

Figure 13: Hierarchical server configuration example

Before configuring trunks

When a trunk is created and enabled, the trunk members (switch ports) take on certain settings necessary for the correct operation of the Multi-Link Trunking feature.

Before configuring a Multi-Link trunk, consider these settings, along with specific configuration rules, as follows:

1. Read the configuration rules provided in Multi-Link Trunking Configuration Rules on page 23.
2. Determine which switch ports (up to four) are to become trunk members (the specific ports making up the trunk). A minimum of two ports are required for each trunk.

   Note:

   Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure they are enabled.
3. Ensure that the trunk member ports have the same VLAN configuration.
4. To avoid configuration errors, all network cabling must be complete and stable before configuring any trunks.

   Note:

   If trunk ports are STP-enabled, ensure that all potential trunk members are connected to their corresponding members; otherwise, STP cannot converge correctly, and traffic loss can result.
5. Consider how the existing spanning tree will react to the new trunk configuration.

Comments? infodev@avaya.com

Note:

If potential trunk ports are connected and STP is disabled on these ports, a loop is formed; to avoid this situation, enable the trunk before you disable STP.

6. Consider how existing VLANs will be affected by the addition of a trunk.

Multi-Link Trunking Configuration Rules

The Multi-Link Trunking feature is deterministic; that is, it operates according to specific configuration rules. When creating trunks, consider the following rules that determine how the Multi-Link trunk reacts in any network topology:

- Disabled ports can belong to MLTs. For traffic to flow to your configured MLT ports, be sure they are enabled (enable ports from interface configuration mode).
- All trunk members must have the same VLAN configuration before the Trunk Status can be set to Enabled using the ACLI.
- When an active port is configured in a trunk, the port becomes a trunk member when the Trunk Status field is set to Enabled. The spanning tree parameters for the port then change to reflect the new trunk settings.
- If the spanning tree participation of any trunk member is changed to Enabled or Disabled, the spanning tree participation of all members of that trunk changes similarly.
- If the VLAN settings of any trunk member is changed, the VLAN settings of all members of that trunk change similarly.
- A trunk member cannot be configured as a monitor port.
- Entire trunks cannot be monitored by a monitor port; however, trunk members can be monitored.
- You can set MLT ports to participate in different STGs. They must have the same spanning tree learning in every group but not necessarily have the same learning between different groups to consistently update their state in the port driver.
- Like normal ports, you can set MLT ports to participate with different spanning tree learning for different spanning tree groups. Trunk ports that are in multiple spanning tree groups must be tagged, and all MLT members must belong to the same spanning tree group.

MLT load-balancing

With the Virtual Services Platform 7000 Series you can choose between MAC-based (basic) or IP-based (advanced) load balancing. You can configure this option using the ACLI.

The variables used in the formula represent different parameters for each load-balancing mode:

- MAC-based (basic) mode uses last 4 bits from each octet of source MAC, destination MAC, ether type, VLAN ID, ports ID, and module ID to perform an XOR function. A MOD is then made between the obtained result and the number of active trunk links. The formula is:

  Index=macsa(43,40)^macsa(35,32)^macsa(27,24)^macsa(19,16)^macsa(11,8)^macsa(3,0)^macda(43,40)^macda(35,32)^macda(27,24)^macda(19,16)^macda(11,8)^macda(3,0)^vlan(11,8)^vlan(3,0)^ether_type(11,8)^ether_type(3,0)^lbid_src_modid(3,0)^lbid_src_port(3,0)

  Link Selected = (Index) MOD (no. active links)

- IP-based (advanced) mode uses last 4 bits from each octet of source IP, destination IP, TCP/UDP source port, and TCP/UDP destination port to perform an XOR function. A MOD is then made between the obtained result and the number of active trunk links. The formula is:

  Index1=sip(123,120)^sip(115,112)^sip(107,104)^sip(99,96)^sip(91,88)^sip(83,80)^sip(75,72)^sip(67,64)^
  sip(59,56)^sip(51,48)^sip(43,40)^sip(35,32)^sip(27,24)^sip(19,16)^sip(11,8)^sip(3,0)^tcp_src_port(11,8)^tcp _src_port(3,0)

  Index2 = dip(123,120) ^dip(115,112) ^dip(107,104) ^dip (99,96) ^dip(91,88) ^ dip(83,80) ^dip(75,72)^dip(67,64)^dip(59,56)^dip(51,48)^dip(43,40)^dip(35,32)^dip(27,24)^dip(19,16)^dip(11,8)^dip(3,0)^tcp_dst_port(11,8)^tcp_dst_port(3,0);

  Link selected = (Index1 ^ Index2) MOD (no. active links)

Removal of MLT restrictions

If any trunk member is set to Disabled (not active) the trunk member is no longer removed from the trunk. The trunk member remains a disabled member of the trunk, and no longer requires reconfiguring to rejoin the trunk. A trunk member can also now be disabled if only two trunk members exist on the trunk.

The lowest numbered port in the trunk can now be disabled as well. However, Avaya does not recommend disabling the lowest numbered port if Spanning Tree is enabled on the trunk.

Adding and deleting links from existing Multi-Link trunks

Ports cannot be added or removed from a VSP 7000 Series switch MLT, unless MLT is first disabled. When MLT is disabled, the ports assigned to the MLT are not disabled. The ports form separate links and create a network loop.

Comments? infodev@avaya.com

Spanning Tree Considerations for Multi-Link trunks

The spanning tree path cost parameter is recalculated based on the aggregate bandwidth of the trunk. For example, the **Path Cost Arbitration** figure shows a two-port trunk (T1) with two port members operating at an aggregate bandwidth of 20 Gbps, with a comparable path cost of **X**. Trunk 2 has two ports at 2 Gbps with a path cost of 1.

802.1t path cost calculation is enabled for both S1 and S2.

When the path cost calculations for both trunks are equal, the software chooses the trunk containing the lowest numbered port as the forwarding path.

Note:

The default spanning tree path cost for all gigabit ports is always equal to 1.

Be careful when configuring trunks so as to not add one gigabit link physically in front of another trunk; the trunk will be blocked because they both have a path cost of 1.

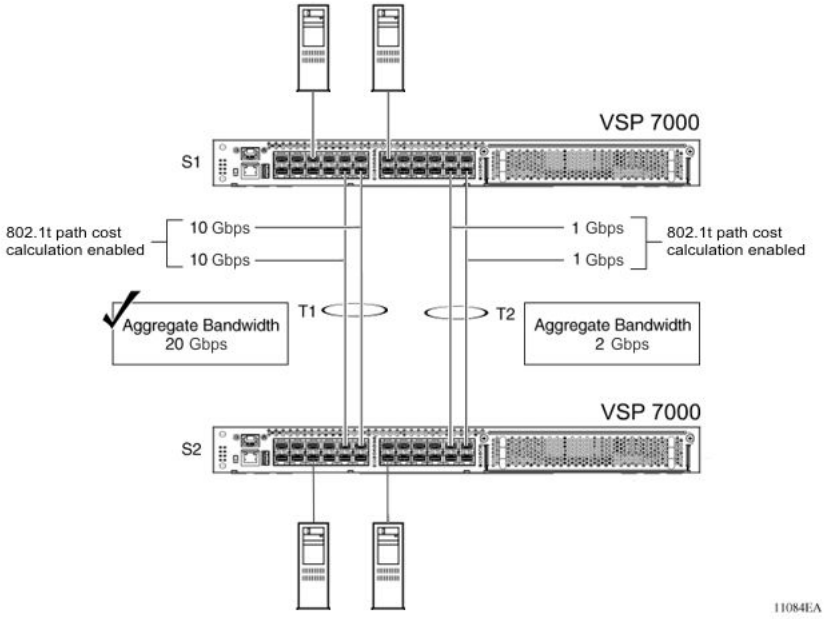

Figure 14: PATH COST ARBITRATION

The switch can also detect trunk member ports that are physically misconfigured. For example, as shown in the following figure, trunk member ports 2, 4, and 6 of Switch S1 are configured correctly to trunk member ports 7, 9, and 11 of Switch S2. The port state for each port is **Forwarding**.

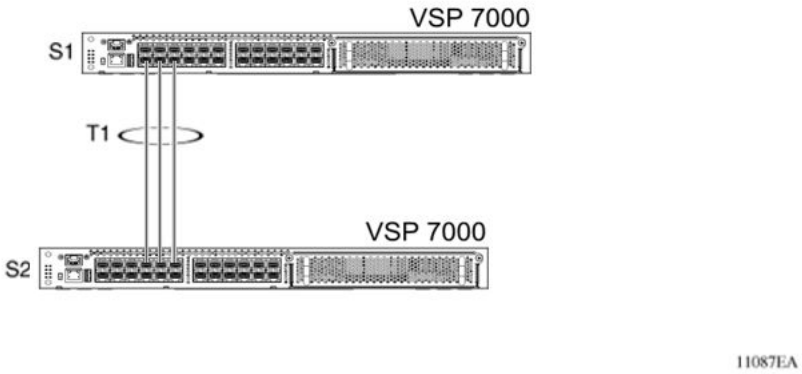

Figure 15: Correctly Configured Trunk

Note:

Path cost varies with port speed. For example, the cost for a 1 Gbps port is 1, while the cost for a 20 Gbps port is **X**.

If trunk member port 11 of root Switch S2 is physically disconnected, and then reconnected to port 13; then port 6 of Switch S1 changes to the Blocking state. See the following figure.

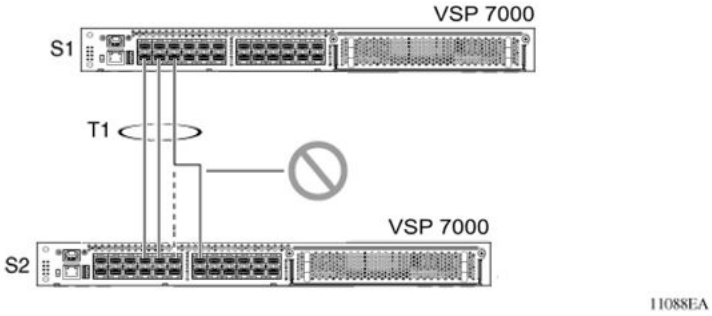

Figure 16: Detecting a Misconfigured Port

Note:

If the port speed is 1 Gbps, the STP cost for trunk members on S2 is 1.

MLT whole trunk enable or disable

The MLT Enable or Disable Whole Trunk feature is configurable globally for the switch. When you the enable or disable MLT or DMLT groups, the operational state of the links that make up the bundle are not changed by default. When you disable MLT or DMLT groups, a traffic loop within a network can occur. The Avaya Virtual Services Platform 7000 Series supports the

ability to change this operational mode using the MLT Enable or Disable Whole Trunk capability.

If you enable the MLT Enable or Disable Whole Trunk functionality, the underlying state of the port changes to reflect the state of the MLT or DMLT bundle irrespective of their previous status. Similarly, if you disable the MLT or DMLT, all links that are part of the MLT group are disabled, except the Destination Lookup Failure (DLF) link. The DLF link is typically the lowest numbered port of a MLT or DMLT link.

You can enable or disable individual links of a MLT or DMLT when you enable the MLT Enable or Disable Whole Trunk functionality.

MLT Enable or Disable Whole Trunk is disabled by default

Important:

For network configuration, Avaya recommends that you set the MLT Enable or Disable Whole Trunk functionality to *enabled*.

Port membership in Multi-Link Trunking

When a Multi-Link trunk is created, the individual trunk members (the specific ports that make up the trunk) logically connect and react as a single entity. For example, if you change spanning tree parameters for any trunk member, the spanning tree parameters for all trunk members change.

To change port membership in Multi-Link Trunking:

1. Disable the trunk.
2. Make the change.
3. Re-enable the trunk.

When you change a Spanning Tree parameter for one trunk member, the modification affects all trunk members.

The trunk is also viewed by management stations as a single spanning tree port. The spanning tree port is represented by the trunk member with the lowest port number. For example, if ports 13, 14, 15, and 16 are trunk members of trunk T1, the management station views trunk T1 as spanning tree port 13.

Comments? infodev@avaya.com

Chapter 5: Virtual Local Area Network configuration using ACLI

This chapter provides information for creating and managing a Virtual Local Area Network (VLAN), using the Avaya Command Line Interface (ACLI).

Displaying VLAN information

Use this procedure to display the number, name, type, protocol, user PID, state of a VLAN, and whether it is a management VLAN.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
show vlan [configcontrol] [id <1-4094>] [interface {info | vids}] [mgmt] [summary] [type port]
```

Variable definitions

The following table describes the parameters for the **`show vlan`** command.

Variable	Value
configcontrol	Displays the VLAN control mode.
id	Enter the number of VLAN to display. RANGE: 1 to 4094

Variable	Value
interface *{info | vids}*	Displays the specific VLAN configuration information for interfaces: • info—Displays the VLAN configuration for ports. • vids—Displays VLAN membership for ports.
mgmt	Displays the management VLAN ID.
summary	Displays a VLAN configuration summary.
type port	Indicates a port-based VLAN type.

Displaying VLAN interface information

Use this procedure to display VLAN settings associated with a port, including tagging information, PVID number, priority, and filtering information for tagged, untagged, and unregistered frames.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
show vlan interface info [<portlist>]
```

Displaying VLAN port membership

Use this procedure to display port memberships in VLANs.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

Comments? infodev@avaya.com

```
show vlan interface vids [<portlist>]
```

Setting the management VLAN

Use this procedure to set a VLAN as the management VLAN.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
vlan mgmt <1–4094>
```

Variable definitions

The following table describes the parameters for the **`vlan mgmt`** command.

Variable	Value
<1–4094>	Specifies the VLAN ID.

Resetting the management VLAN to default

Use this procedure to reset the management VLAN to VLAN1.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
default vlan mgmt
```

Creating a VLAN

Use this procedure to create a VLAN. A VLAN is created by setting the state of a previously nonexistent VLAN.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
vlan create <1-4094> [name <vlan_name>] [type port] [<stg_id>]
```

Variable definitions

The following table describes the parameters for the **`vlan create`** command.

Variable	Value
<1–4094>	Enter the number of the VLAN to create
name <*vlan_name*>	Enter the name of the VLAN to create. If you do not assign a VLAN name, the switch automatically generates a name based on the next sequential VLAN ID that is available.
type port	Specifies a port-based VLAN.
<stg_id>	Enter the STG ID, value of 1–8.

Comments? infodev@avaya.com

Deleting a VLAN

Use this procedure to delete a VLAN.

Before you begin

About this task

Use these commands in the Global Configuration mode.

Procedure

Enter either of the following commands:

```
vlan delete <2–4094>
```

OR

```
no vlan <2–4094>
```

Variable definitions

The following table describes the parameters for the **`vlan delete`** and **`no vlan`** commands.

Variable	Value
<2–4094>	Specifies the ID of the VLAN to delete.

Configuring a VLAN name

Use this procedure to configure or modify the name of an existing VLAN.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
vlan name <1-4094> <name>
```

Variable definitions

The following table describes the parameters for the **vlan name** command.

Variable	Value
<1–4094>	Specifies the number of the VLAN to be configured or modified.
<name>	Specifies a new alphanumeric VLAN name.

Restoring a VLAN name to default

Use this procedure to restore a configured VLAN name to the default value.

Before you begin

Use these commands in the Global Configuration mode.

Procedure

Enter either of the following commands:

```
default vlan name <vlan_list>
```

OR

```
no vlan name <vlan_list>
```

Variable definitions

The following table describes the parameters for the **default vlan name** and **no vlan name** commands.

Variable	Value
<vlan_list>	Specifies an individual VLAN or list of VLANs.

Comments? infodev@avaya.com

Enabling or disabling automatic PVID

Use this procedure to enable or disable automatic Port VLAN Identifier (PVID) feature for all switch ports. Automatic PVID is enabled by default.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
[no] auto-pvid
```

Variable definitions

The following table describes the parameters for the **auto-pvid** command.

Variable	Value
[no]	Disables automatic PVID for all switch ports.

Configuring VLAN port settings

Use this procedure to configure VLAN-related settings for a port.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
vlan ports [<portlist>] [tagging {enable | disable | tagAll |
untagAll | tagPvidOnly | untagPvidOnly}] [pvid <1-4094>]
[filter-untagged-frame {enable | disable}] [filter-
```

```
unregistered-frames {enable | disable}] [priority <0-7>] [name
<line>]
```

Variable definitions

The following table describes the parameters for the **`vlan ports`** command.

Variable	Value
<portlist>	Enter the port numbers to be configured for a VLAN.
tagging *{enable|disable|tagAll| untagAll| tagPvidOnly| untagPvidOnly}*	Enables or disables the port as a tagged VLAN member for egressing packet. DEFAULT: untagAll
pvid *<1–4094>*	Sets the PVID of the port to the specified VLAN. DEFAULT: established based on membership and configcontrol
filter-untagged-frames *{enable| disable}*	Enables or disables the port to filter received untagged packets. DEFAULT: disable
filter-unregistered-frames *{enable| disable}*	Enables or disables the port to filter received unregistered packets. Enabling this feature on a port means that any frames with a VID to which the port does not belong to are discarded. DEFAULT: enable
priority *<0–7>*	Sets the port as a priority for the switch to consider as it forwards received packets. DEFAULT: 0
name *<line>*	Enter the name you want for this port. **Note:** This option can only be used if a single port is specified in the <portlist>.

Comments? infodev@avaya.com

Restoring a VLAN port member name to default

Use this procedure to restore a previously modified VLAN port member name to the default value.

Before you begin

Use these commands in the Global Configuration mode.

Procedure

Enter either of the following commands:

```
no vlan ports name <port_list>
```

OR

```
default vlan ports name <port_list>
```

Variable definitions

The following table describes the parameters for the **`no vlan ports name`** and **`default vlan ports name`** command.

Variable	Value
<port_list>	Specifies a port or list of ports.

Configuring VLAN Members

Use this procedure to add or delete a port from a VLAN.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
vlan members [add | remove] <1-4094> <portlist>
```

Variable definitions

The following table describes the parameters for the **`vlan members`** command.

Variable	Value
add | remove	Adds a port to, or removes a port from a VLAN. **Note:** IF this parameter is omitted, set the exact port membership for the VLAN; the prior port membership of the VLAN is discarded and replaced by the new list of ports.
<1–4094>	Specifies the target VLAN.
portlist	Enter the list of ports to be added, removed, or assigned to the VLAN.

Displaying VLAN Configuration Control settings

VLAN Configuration Control (VCC) allows a switch administrator to control how VLANs are modified. VLAN Configuration Control is a superset of the AutoPVID functionality and incorporates this functionality for backwards compatibility. VLAN Configuration Control is globally applied to all VLANs on the switch.

VLAN Configuration Control is only applied to ports with the tagging modes of **Untag All** and **Tag PVID Only**.

Before you begin

Use this command in the Global Configuration mode.

About this task

VLAN Configuration Control offers four options for controlling VLAN modification:

- Strict
- Automatic
- AutoPVID
- Flexible

Procedure

Enter the following command:

Comments? infodev@avaya.com

```
show vlan configcontrol
```

Modifying VLAN Configuration Control settings

Use this procedure to modify the current VLAN Configuration Control setting. This command applies the selected option to all VLANs on the switch.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
vlan configcontrol <vcc_option>
```

Variable definitions

The following table describes the parameters for the **`vlan configcontrol`** command.

Variable	Value
<vcc_option>	This parameters denotes the VCC option to use on the switch. The value values are: • automatic — Changes the VCC option to Automatic • autopvid — Changes the VCC option to AutoPVID • flexible — Changes the VCC options to Flexible • strict — Changes the VCC option to Strict. DEFAULT: Strict

Displaying the MAC address forwarding table

Use this procedure to display the current contents of the MAC address forwarding database table. You can filter the MAC address table by port number. The MAC address table can store up to 131,070 addresses.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
show mac-address-table [vid <1-4094>] [aging-time] [address
<H.H.H>] [port <portlist>]
```

Variable definitions

The following table describes the parameters for the **`show mac-address-table`** command.

Variable	Value
vid<*1–4094*>	Enter the number of the VLAN for which you want to display the forwarding database. DEFAULT: To display the management VLAN's database
aging-time	Displays the time in seconds after which an unused entry is removed from the forwarding database. DEFAULT: 300 seconds
address<*H.H.H*>	Displays a specific MAC address if it exists in the database. Enter the MAC address you want displayed.
port <*portlist*>	Specifies a port or list of ports.

Comments? infodev@avaya.com

Configuring MAC address retention

Use this procedure to set the time during which the switch retains unseen MAC addresses.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
mac-address-table aging-time <10–1000000>
```

Variable definitions

The following table describes the parameters for the **`mac-address-table aging-time`** command.

Variable	Value
<10–1000000>	Enter the aging time in seconds that you want for MAC addresses before they expire. DEFAULT: 300 seconds

Setting MAC address retention time to default

Use this procedure to set the retention time for unseen MAC addresses to 300 seconds.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
default mac-address-table aging-time
```

Comments? infodev@avaya.com

Chapter 6: STP configuration using ACLI

This chapter provides information for creating and managing Spanning Tree Protocol (STP) to detect and eliminate logical loops in bridged or switched networks, using the Avaya Command Line Interface (ACLI).

Configuring path cost calculation mode

Use this procedure to set the path cost calculation mode for all Spanning Tree Groups on the VSP Series switches. Select either IEEE Standard 802.1d or IEEE Standard 802.1t. The IEEE Standard 802.1t is the maintenance extension to the 802.1d standard.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
spanning-tree cost-calc-mode {dot1d | dot1t}
```

Variable definitions

The following table describes the parameters for the **`spanning-tree cost-calc-mode`** command.

Variable	Value
cost-calc-mode *{dot1d* | *dot1t}*	Enter one of the STG path cost calculation modes: • dot1d — IEEE Standard 802.1d • dot1t — IEEE Standard 802.1t DEFAULT: dot1d

Configuring STG port membership mode

Use this procedure to set the STG port membership for all Spanning Tree Groups on the VSP 7000 Series switches.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
spanning-tree port-mode {auto | normal}
```

Variable definitions

The following table describes the parameters for the **`spanning-tree port-mode`** command.

Variable	Value
port-mode *{auto | normal}*	Enter one of the values: • auto — In the auto mode, when a port is assigned to VLAN X and VLAN X is in STP group Y, the port automatically becomes a member of STP group Y. • normal — In the normal mode, when a port is assigned to VLAN X and VLAN X is in STP group Y, the port does not automatically become a member of STP group Y. DEFAULT: normal

Displaying STP configuration information

Use this procedure to display Spanning Tree Configuration information that is specific to either the Spanning Tree Group or to the port. In this procedure, the omission of the parameter that

Comments? infodev@avaya.com

specifies a specific Spanning Tree Group (1 to 8) results in the command operating against the default Spanning Tree Group (Spanning Tree Group 1).

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
show spanning-tree [config <port> | <vlans>] [cost-calc-mode]
[port <port_list>] [port-mode] [stp <1-8>] [vlans] [802dot1d-
port-compliance]
```

Variable definitions

The following table describes the parameters for the **`show spanning-tree`** command.

Variable	Value
config <*port* > | <*vlans*>	Displays Spanning Tree configuration for the switch or specific interfaces. • port — the ports within the Spanning Tree Group • vlans — the VLANs that are members of the specified Spanning Tree Group
cost-calc-mode	Displays the pathcost type.
port <*port_list*>	Displays the Spanning Tree status for a specific port or list of ports.
port-mode	Displays the Spanning Tree port membership mode
stp <*1–8*>	Displays specified Spanning Tree Group configuration. Enter the ID number of the group to be displayed. Values range from 1 to 8.
vlans	Displays Spanning Tree group VLAN members.
802dot1d-port-compliance	Displays the 802dot1d port compliance mode.

Creating a Spanning Tree Group

Use this procedure to create a Spanning Tree Group.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
spanning-tree stp <1-8> create
```

Variable definitions

The following table describes the parameters for the **`spanning-tree create`** command.

Variable	Value
stp <*1–8*>	Enter the number of the Spanning Tree group to be created.

Deleting a Spanning Tree Group

Use this procedure to delete a Spanning Tree Group.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
spanning-tree stp <1-8> delete
```


Comments? infodev@avaya.com

Variable definitions

The following table describes the parameers for the **`spanning-tree delete`** command.

Variable	Value
stp <*1–8*>	Enter the number of the Spanning Tree group to be deleted.

Enabling or disabling a Spanning Tree Group

Use this procedure to enable or disable a Spanning Tree Group.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
spanning-tree stp <1-8> {enable | disable}
```

Variable definitions

The following table describes the parameters for the **`spanning-tree`** command.

Variable	Value
stp <*1–8*>	Enter the number of the Spanning Tree group to be enabled or disabled.
enable	Enables the Spanning Tree group.
disable	Disables the Spanning Tree group.

Configuring STP values

Use this procedure to set STP values such as forward time, hello time, max age, priority and multicast address by Spanning Tree Group. You can set the BDPU to tagged or untagged. set

the tagged BPDU VLAN ID (VID) for STGs 1 to 8, and add a VLAN to or remove a VLAN from the Spanning Tree Group.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
spanning-tree [add-vlan] [forward-time <4-30>] [hello-time
<1-10>] [max-age <6-40>] [multicast-address <H.H.H>] [priority
{0x000 | 0x1000 | 0x2000 | 0x3000 | .... | 0xE000 | 0xF000}]
[remove-vlan] [stp <1-8>] [tagged-bpdu {enable | disable}]
[tagged-bpdu-vid <1-4094>] [802dot1d-port-compliance enable]
```

Variable definitions

The following table describes the parameters for the **`spanning-tree`** command.

Variable	Values
add-vlan	Adds a VLAN to the Spanning Tree Group.
forward-time *<4–30>*	Enter the forward time of the STG in seconds. DEFAULT: 15 seconds RANGE: 4–30 seconds
hello-time *<1–10>*	Enter the hello time of the STG in seconds. DEFAULT: 2 seconds RANGE: 1–10 seconds
max-age *<6–40>*	Enter the max-age of the STG in seconds. DEFAULT: 20 seconds RANGE: 6–40 seconds
multicast-address *<H.H.H>*	Sets the spanning tree multicast address.
priority *{0x000 | 0x1000 | 0x2000 | 0x3000 | .... | 0xE000 | 0xF000}*	Sets the spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000.
remove-vlan	Removes a VLAN from the Spanning Tree Group.
stp *<1–8>*	Specifies the Spanning Tree Group; enter the STG ID.
tagged-bpdu *{enable | disable}*	Sets the BPDU as tagged or untagged.

Comments? infodev@avaya.com

Variable	Values
	DEFAULT: Untagged for STG 1 (default group) and Tagged for the other groups.
tagged-bpdu-vid *<1–4094>*	Sets the VLAN ID (VID) for the tagged BPDU. DEFAULT: 4001–4008 for STG 1–8 , respectively
802dot1d-port-compliance enable	Enables 802dot1d port compliance mode.

Restoring default Spanning Tree values

Use this procedure to restore default spanning tree values for the Spanning Tree Group.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
default spanning-tree [stp <1-8>] [forward-time] [hello-time]
[max-age] [priority] [tagged-bpdu] [multicast address]
```

Variable definitions

The following table describes the parameters for the **`default spanning-tree`** command.

Variable	Value
stp *<1–8>*	Disables the Spanning Tree Group; enter the STG ID.
forward-time	Sets the forward time to the default value. DEFAULT: 15 seconds
hello-time	Sets the hello time to the default value. DEFAULT: 2 seconds
max-age	Sets the maximum age time to the default value. DEFAULT: 20 seconds

Variable	Value
priority	Sets spanning tree priority (in Hex); if 802.1T compliant, this value must be a multiple of 0x1000. DEFAULT: 0x8000
tagged-bpdu	Sets the tagging to the default value. DEFAULT: For Spanning Tree Group 1 (default group) is untagged; the default for the other groups is tagged.
multicast address	Sets the spanning tree multicast MAC address to the default. DEFAULT: 01-80-C2-00-00-00

Adding a VLAN to a Spanning Tree Group

Use this procedure to add a VLAN to a specific Spanning Tree Group.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
spanning-tree [stp <1-8>] add-vlan <1-4094>
```

Variable definitions

The following table describes the parameters for the **`spanning-tree add-vlan`** command.

Variable	Value
stp <*1–8*>	Enter the STG ID. RANGE: 1–8
add-vlan <*1–4094*>	Enter the ID of the VLAN to be added. RANGE: 1–4094

Comments? infodev@avaya.com

Removing a VLAN from a Spanning Tree Group

Use this procedure to remove a VLAN from a specific Spanning Tree Group.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
spanning-tree [stp <1-8>] remove-vlan <1-4094>
```

Variable definitions

The following table describes the parameters for the **`spanning-tree remove-vlan`** command.

Variable	Value
stp <*1–8*>	Enter the STG ID. RANGE: 1–8
remove-vlan <*1–4094*>	Enter the ID of the VLAN to be removed. RANGE: 1–4094

Configuring STP learning

Use this procedure to configure the Spanning Tree learning type for one or more ports.

Before you begin

Use this command in the Interface Configuration mode.

Procedure

Enter the following command:

```
spanning-tree learning [disable | normal | fast]
```

Variable definitions

The following table describes the parameters for the **spanning-tree learning** command.

Variable	Value
disable	Disables Spanning Tree for the port or ports on the specified STG.
fast	Sets fast learning for one or more ports on the specified STG.
normal	Sets normal learning for one or more ports on the specified STG.

Resetting Spanning Tree values for ports to default

Use this procedure to set the spanning tree values for the ports within the specified Spanning Tree Group to the factory default settings

Before you begin

Use this command in the Interface Configuration mode.

Procedure

Enter the following command:

```
default spanning-tree [port <portlist> ] [stp <1-8>] [learning]
[cost] [priority]
```

Variable definitions

The following table describes the parameters for the **default spanning-tree** command.

Variable	Value
port <*portlist*>	Enables spanning tree for the specified port or ports; enter the port or ports to be set to factory spanning tree default values.

Comments? infodev@avaya.com

Variable	Value
	Note: If you omit this parameter, the system uses the port number you specified when you issued the interface command to enter the Interface Configuration mode.
stp <*1–8*>	Specifies the spanning tree group to set to factory default values; enter the STG ID. DEFAULT: This command places the port into STG 1.
learning	Sets the STP learning mode to the factory default value. DEFAULT: Normal mode
cost	Sets the path cost to the factory default value. DEFAULT: Depends on the type of port.
priority	Sets the spanning tree priority to the factory default value. DEFAULT: 0x8000 hexadecimal or 128 decimal

Comments? infodev@avaya.com

Chapter 7: Multi-Link Trunking configuration using ACLI

This chapter provides information for creating and managing a Multi-Link Trunk (MLT) to form a link to another switch or server, using the Avaya Command Line Interface (ACLI).

Configuring an MLT

Use this procedure to group a maximum of four switch ports together to form a link to another switch or server, which increases the aggregate throughput of the link.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
mlt <id> [name <trunkname>] [enable | disable] [member
<portlist>] [learning {disable | fast | normal}] loadbalance
{basic | advance}
```

Variable definitions

The following table describes the parameters for the **mlt** command.

Variable	Value
id	Specifies the MLT ID. Values range from 1 to 12.
name <*trunkname*>	Specifies a unique, alphanumeric identifier for the MLT, with a maximum of 16 characters.
enable | *disable*	Enables or disables the trunk.
member <*portlist*>	Specifies a port or list of ports to assign as members of the MLT.

Variable	Value
learning *{disable | fast | normal}*	Sets STP learning mode.
loadbalance *{basic | advance}*	Specifies the MLT load balancing mode. Values include: • basic—MAC address-based load balancing • advance—IP-based load balancing

Disabling an MLT

Use this procedure to disable an MLT and clear all the MLT port members.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
no mlt [<id>]
```

Variable definitions

The following table describes the parameters for the **`auto-pvid`** command.

Variable	Value
[no]	Disables automatic PVID for all switch ports.

Comments? infodev@avaya.com

Configuring STP participation for MLTs

Use this procedure to configure Spanning Tree Protocol (STP) participation with MLTs.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
mlt spanning-tree <1-12> [stp <1-8, ALL>] [learning {disable |
normal | fast}]
```

Variable definitions

The following table describes the parameters for the **`mlt spanning-tree`** command.

Variable	Value
<1-12>	Specifies the ID of the MLT to associate with the STP. Values range from 1 to 12.
stp *<1-8, ALL>*	Specifies the STG to participate with the MLT. • 1-8—selects a specific STG ID. Values range from 1 to 8. • ALL—selects all configured STGs.
learning *{disable | normal | fast}*	Specifies the STP learning mode: • disable—disables STP learning • normal—sets the STP learning mode to normal • fast—sets the STP learning mode to fast

Enabling disabled trunk loop prevention

Use this procedure to prevent traffic loops within a network by enabling the MLT Enable or Disable Whole Trunk feature.

Before you begin

Use this command in the Global Configuration mode.

About this task

By enabling MLT Enable or Disable Whole Trunk, you enable the ability for the switch to enable all MLT member ports simultaneously when you enable the associated MLT, or disable all MLT member ports simultaneously, except the first active link, when you disable the associated MLT.

Procedure

Enter the following command:

```
mlt shutdown-ports-on-disable enable
```

Disabling disabled trunk loop prevention

Use this procedure to disable the MLT Enable or Disable Whole Trunk feature.

Before you begin

Use these commands in the Global Configuration mode.

About this task

By disabling MLT Enable or Disable Whole Trunk, you disable the ability for the switch to enable all MLT member ports simultaneously when you enable the associated MLT, or disable all MLT member ports simultaneously, except the first active link, when you disable the associated MLT.

Procedure

Enter either of the following commands:

```
[no] shutdown-ports-on-disable enable
```

OR

```
[default] shutdown-ports-on-disable enable
```


Comments? infodev@avaya.com

Displaying MLT information

Use this procedure to view information about MLTs configured on your switch.

Before you begin

Use this command in the Privileged EXEC Configuration mode.

Procedure

Enter the following command:

```
show mlt [shutdown-ports-on-disable] [spanning-tree <1–12>]
[utilization <1-12>]
```

Variable definitions

The following table describes the parameters for the **`show mlt`** command.

Variable	Value
shutdown-ports-on-disable	Displays the status of disabled trunk loop prevention.
spanning-tree <*1–12*>	Displays MLT spanning-tree group and learning information. <*1–12*> specifies the MLT ID.
utilization <*1-12*>	Displays MLT utilization information. <*1–12*> specifies the trunk ID.

Comments? infodev@avaya.com