

Dell™ Networking X1000 / X4012 Series Switches

# Dell™ Networking X1000 / X4012 Series Release Notes

**Date: Dec 2018**  
**System Firmware Version 3.0.1.1**



**Information in this document is subject to change without notice.**

**© 2018 Dell Inc. All rights reserved.**

Reproduction in any manner without the written permission of Dell Inc is strictly forbidden.

Trademarks used in this text: Dell, the DELL logo and PowerConnect are trademarks of Dell Computer Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entity claiming the marks and names or their products. Dell Computer Corporation disclaims any proprietary interest in trademarks and trade names other than its own. All rights reserved. This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without the prior written consent of Dell. Dell reserves the right to make changes without further notices to any products or specifications referred to herein to improve reliability, functionality or design. Reproduction, adaptation or translation without prior written permission is prohibited, except as allowed under the copyright laws.



## Table of Contents

<b>Introduction</b>	<b>4</b>
<b>GLOBAL SUPPORT</b>	<b>4</b>
<b>Firmware Specifications</b>	<b>4</b>
<b>Supported Firmware Functionality</b>	<b>5</b>
<b>Functionality Change in Current Release</b>	<b>5</b>
<b>Functionality Change in Previous Release</b>	<b>5</b>
Turn off cross site scripting restrictions in the Go Web service .....	5
Updated boot for X10xx Series Switches .....	5
Support for latest browser versions .....	5
<b>Issues Resolved in Current Version</b>	<b>6</b>
<b>Issues Resolved in Previous Versions</b>	<b>7</b>
X10xxP - Stops powering up PDs with POE ERRORS (“HAL_config_poe-A-POEFailDetected: POE ERROR(send_recieve_msg. Send Msg [13] HALP_config_poe_691xx_msg_GetPortMeasurements_E With Echo 124, Received Msg [1]: err no_recieve) was detected” and “HAL_config_poe-A-POEFailDetected: POE ERROR(***** Poe Fail Detected ***** ) was detected”).....	9
After a few weeks of system uptime, no power is provided to PDs connected to the switch. Required switch reload to restore the PoE functionality back. ....	9
FATAL ERROR: GOAH: ABORT DATA exception after multiple login to device on the same time via UI.....	9
In some cases, the switch would crash with the message “GOAH: ABORT DATA exception”. Device would reload and not forward traffic .....	9
DNSE/X-Series - Bandwidth gauge displays incorrectly on dashboard .....	9
Wrong bandwidth info presented by dashboard – especially with 10G interfaces .....	9
DNSE/3.0.0.90 - Crypto RSA key-generate option missing. ....	9
The option to generate a certificate with key (command “crypto certificate 1 generate key-generate” in CLI) is missing in version 3.0.0.90 .....	9
DNSE/X1018 - 3.0.0.90: First EAP Identity Request packet is dropped in switch. ....	10
Switch does NOT send an ‘EAP Identity Request’ directly on link-up. Only after ‘Resending EAP Identity Request (Sec)’ timer which has minimum value of 30 seconds. This is a problem for certain supplicants (like MAC) which will not send an EAPOL start until switch sends the request.....	10
DNSE/3.0.0.90 - X-Series - Security vulnerabilities.....	10
DNSE/X1052/3.0.0.90/crash @ BRMN task.....	10
Switch crash and reboot – losing connectivity and not forwarding traffic. ....	10
DNSE/3.0.0.91 - X-Series - Security vulnerability CVE-2016-2183 .....	10
Found during Retina System Vulnerability scanner. Remote attackers can obtain clear text data via a birthday attack against a long-duration encrypted session .....	10
DNSE/3.0.0.90 - X0152P - LLDP info fails to show up via WebUI.....	10
On some browser GUI does not display LLPD neighbor information .....	10
DNSE/X4012: GUI Statistics displays different % of utilization for 10Gbps interfaces. ....	11
Utilization shows only 30% of traffic on 10G ports running at 10Gbps .....	11
Dell-1127 - DNSE/3.0.0.64 - X-Series Vulnerability Check CVE ID: CVE-2008-5161 .....	11



The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the cipher text .....	11
Dell-1136 - DNSE/3.0.0.90 - X4012 - Interface Utilization Percentage Shows 100 .....	11
Interface Utilization Percentage shows as 100% incorrectly in the WebUI of X4012 switches.....	11
Dell-1140 - DNSE/3.0.0.90 - X-Series - High CPU Utilization of GOAH task .....	11
Performed PCI Security scan on X-Series switches, It leads to port-channel flaps after the CPU spikes to 100% utilization. .	11
Dell-1111 - DNSE/X-Series - SHA1 Trusted Certificate issues starting January 1, 2017.....	11
Google Chrome will completely stop supporting SHA-1 (not including self-signed). So is it right to interpret that trusted SHA1 certificates will not be supported .....	11
Dell-1120 - 3.0.0.90 - Default settings in running-config shows 32 Po intfs while only 12 is supported.....	12
CLI the “default settings” in show run shows 32 port-channel interfaces.....	12
Dell-1122 - 3.0.0.90 - X1000 GUI displays the LAG Type as eth1000M for 10G ports .....	12
“LAG Type” displayed as ‘eth1000M’ instead of ‘eth10G’ for the X1052 platform. ....	12
Dell-1116 - DNSE/X-Series - Bandwidth gauge displays incorrectly on dashboard.....	12
Incorrect display of Bandwidth at dashboard page .....	12
Dell-1125 - DNSE/3.0.0.90 - X-Series - STP Port Settings "Designated Cost" Display issue.....	12
Incorrect display of Designated Cost for Lag interface. ....	12
Dell-1128 - DNI/30082/X1008/X1008P - Copper ports ACT LED issue under unmanaged mode .....	12
X1008/X1008P copper ports ACT LED issue under unmanaged mode. ....	12
The “ACT” LED shows incorrect color with “Amber”, not correct color “Green” when X1008/X1008P set at unmanaged mode and ports are linked up at 100M speeds only .....	12
DELL-1016 – DNSE/X-series - 3.0.0.64: WebGui "Optical Transceiver Diagnostic" incorrect info for FCLF-8521-3-DL 1000Base-T.....	13
In some scenarios when an qualified Cable will be displayed as “Generic Unqualified Transceiver”.....	13
It’s a cosmetic issue and all cables functionality is working as expected .....	13
DELL-1009 - X4012 WebUI - Incorrect link utilization .....	13
Link Utilization is incorrectly shown in WebUI of X4012 switches.....	13
The following two issues are seen with link utilization.....	13
1. Utilization is shown to be 200% for minimal ingress unicast/multicast traffic. ....	13
2. Utilization is blank when there is traffic egressing the port. ....	13
DELL-1098 - DNSE/X1052/3.0.0.80/Configuration loss after downloading the configGUI .....	13
Trunk port configurations the interface is getting lost after the downloading the configuration via GUI and reboot. ....	13
The issue happens only when that interface has "switchport trunk native vlan none" configured.....	13
DELL-1088 - DNSE/X1052P - 3.0.0.80 : WebGUI SNMP community access mode settings doesn't match with CLI output	13
If a new SNMP community is created with 'Read Only' access rights and DefaultSuper view map, then it appears as 'SNMP Admin' in the GUI instead. The configuration Web will be applied to the running-config correctly .....	13

## Known Issues 13

DELL-1104 DNSE/X1026P/3.0.0.80 /Management access via http result in switch being unresponsive.....	13
-----------------------------------------------------------------------------------------------------	----

## Known Restrictions and Limitations 14

X4012 – Some link flap logs on the console when shut/no-shut peer switch interface(s).....	14
--------------------------------------------------------------------------------------------	----

## Documentation updates 14

Introduction .....	14
N/A .....	14

## Addendum 14

Port Profile Description.....	14
-------------------------------	----





## Introduction

This document provides specific information for the Dell networking X1000 / X4012 series switching systems, firmware version 3.0.1.1.

It is recommended that this release note be thoroughly reviewed prior to installing or upgrading this product.

## GLOBAL SUPPORT

For information regarding the latest available firmware, recent release revisions or if requiring additional assistance, please visit <http://support.dell.com> Support Web Site.

## Firmware Specifications

### Firmware Version Details


Model	Boot PROM Name	Version No.	Release Date
X10xx	X10xx_boot-10025.rfb	1.0.0.25	April, 2017
X4012	X4012_boot-10010.rfb	1.0.0.10	Oct, 2014

Model	Firmware Image Name	Version No.	Release Date
X10xx	x10xx-3011.ros	3.0.1.1	Dec 2018
X4012	x4012-3011.ros	3.0.1.1	Dec 2018

The firmware image version should be 3.0.1.1

When using the X10xx series, the boot prom image should be 1.0.0.25.

When using the X4012 series, the boot prom image should be 1.0.0.10.

 **NOTE:** Administrators upgrading Dell Networking X1008, X1008P, X1018, X1018P, X1026, X1026P, X1052, X1052P switches to firmware-image version 3.0.1.1 and Boot-code/PROM version 1.0.0.25 MUST follow the upgrade instructions documented in the “X10xx\_X4012\_CLI\_Software\_Upgrade\_Instructions.pdf” procedure. Failure to follow the procedures described in that document when upgrading firmware may result in an inoperable switch!

Version Numbering Convention					
Version number					Description
X10xx X4012	3	0	1	1	Four part version number
				□	Denotes the build number.
			□		Denotes an ad hoc release of the product software.
		□			Denotes a scheduled maintenance release of the product software.
	□				Denotes a major version number.



## Supported Firmware Functionality


For more details regarding the functionalities listed, please refer to the X1000 / X4012 series Switching User's Guide.

## Functionality Change in Current Release

None

## Functionality Change in Previous Release

Summary	Description
Turn off cross site scripting restrictions in the Go Web service	Relevant for All X10xx and X4012 platforms
Updated boot for X10xx Series Switches	Relevant for X10xx Series only: As of image version 3.0.0.94, updated boot is provided: 1.0.0.25
Support for latest browser versions	Chrome - Release 56.0.2924.87 Firefox - Release 51.0.1 Internet Explorer - Release 11.0.38 Safari - Release 10.0.3 / Windows 5.1.7

 **WARNING:** The relevant X-Series switches will automatically update CPLD to the latest version (X1018/P: Rev07, X1026/P: Rev08, X1052/P: Rev0B) on boot up after updating the firmware version to 3.0.0.82 and later (3.0.1.1) and boot-code version 1.0.0.21 and later (1.0.0.25). CPLD update will take at least 10 to 15 minutes to complete. Power cycling the switch during the CPLD update is likely to cause the switch to become inoperable and requires the switches to be RMA'ed for factory re-installation of the firmware.



## Issues Resolved in Current Version

The following issues have been resolved in current firmware release 3.0.1.1

Summary	User Impact	Resolution
DELL-1184 DNSE/3.0.0.98 - X4012 - LAG Creation wizard from dashboard of GUI doesn't allow for removal of LAG config.	User can't remove assigned ports to LAG from the dashboard wizard, still could be done via Network administration menu	Fixed
DELL-1185 DNSE/3.0.0.98/X4012 - Switch stuck in boot loop	Switch reboots when adding ports to LAG and then disable negotiation with module connected.	Fixed
DELL-1186 X series: VLAN configuration lost if "switchport trunk native vlan none" configured.	Configuration lost when configuring with the command "switchport trunk allowed vlan remove 1-99,101-199..."	Fixed
DELL-1189 DNSE/X- Series - 3.0.0.99 - FATAL Switch Crash when attempt to download configuration from HTTPS session	Switch crashes when connected to device via HTTPS and tried to download configuration via HTTP.	Fixed



DELL-1191 DNSE/2.0.0.74 - R1-2210 - Switch_FATAL ERROR crash Reporting Task: SSHU.	Switch crashes when connected to device via SSH session and then tried to connect with cloned session.	Fixed
DELL-1195 DNSE/X4000/3.0.0.99 - Unable to remove reserved vlan for a port	When configured Reserve VLAN for Internal Use, it wasn't possible to remove that configuration.	Fixed

### Issues Resolved in Previous Versions

The following issues have been resolved in version 3.0.0.98

Summary	User Impact	Resolution
DELL-1180 - DNSE/3.0.0.95 - X1052P - GOAH FATAL crash with OSMEMG_rn_free: Memory magic is corrupt	During Nmap toll multiple scans - device crash	Fixed
DELL-1181 - X-Series/RADIUS & TACACS key is not encrypted showing in clear text	Running configuration and files show Radius and Tacacs in clear text	Fixed





DELL-1173 - Xseries/3.0.0.95/VLAN configuration lost if "switchport trunk native vlan none" configured	The following interface configuration was deleted after copy running to startup and reload – "switchport trunk allowed vlan remove 10,20-22"	Fixed
--------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------	-------

The following issues have been resolved between version 3.0.0.95 and 3.0.0.97:

Summary	User Impact	Resolution
DELL-1164 - DNSE/X1000/X4000 - version 3.0.0.94 : Web GUI displays wrong system up time	System Up Time is getting reset every 6th minute in GUI	Fixed
DELL-1162 - FATAL ERROR: GOAH: ABORT DATA exception after configure more than 256 character on SNMP Community String	on page: SNMP Monitoring>Edit Notification Recipients user could edit string to 162 characters which caused device crash	Fixed
DELL-1030 X1026P/52P - Stops powering up PDs with POE ERRORs	On some cases no power is provided to PDs connected to the switch. Required switch reload to restore the PoE functionality back.	Reduce Poe error prints. Added delays in polling commands. In case of connection problem – wait 12 Seconds and try again. In case Poe still not responding the recovery process will be triggered.



The following issues have been resolved between version 3.0.0.92 and 3.0.0.94:

Summary	User Impact	Resolution
<b>X10xxP - Stops powering up PDs with POE ERRORS</b> ("HAL_config_poe-A-POEFailDetected: POE ERROR(send_recieve_msg. Send Msg [13] HALP_config_poe_691xx_msg_GetPortMeasurements_E With Echo 124, Received Msg [1]: err no_recieve) was detected" and "HAL_config_poe-A-POEFailDetected: POE ERROR(***** Poe Fail Detected ***** ) was detected")  DELL-1030/FIELD-1731 ,1450, 2352,2333,2295,2288,2237,1854,2245	After a few weeks of system uptime, no power is provided to PDs connected to the switch. Required switch reload to restore the PoE functionality back.	When issue occurs – PoE process will restart to allow power to be provided to PD.  Notes: PD ports will still be without power for a minimum of 20 seconds during PoE restart process; It may take up to 1:30 minutes for all PDs to come up (depend on PD power up process) Failure and recovery process will be accompanied by log messages.
<b>FATAL ERROR: GOAH: ABORT DATA exception after multiple login to device on the same time via UI.</b>  DELL-1152/FIELD-2417	In some cases, the switch would crash with the message "GOAH: ABORT DATA exception". Device would reload and not forward traffic	Fixed
<b>DNSE/X-Series - Bandwidth gauge displays incorrectly on dashboard</b>  DELL-1116/FIELD-2211	Wrong bandwidth info presented by dashboard – especially with 10G interfaces	Fixed
<b>DNSE/3.0.0.90 - Crypto RSA key-generate option missing.</b>  DELL-1147/FIELD-2340	The option to generate a certificate with key (command "crypto certificate 1 generate key-generate" in CLI) is missing in version 3.0.0.90	Fixed



## X1000/X4012 Series – Release Notes

<b>DNSE/X1018 - 3.0.0.90: First EAP Identity Request packet is dropped in switch.</b> DELL-1148/FIELD-2358	Switch does NOT send an 'EAP Identity Request' directly on link-up. Only after 'Resending EAP Identity Request (Sec)' timer which has minimum value of 30 seconds. This is a problem for certain supplicants (like MAC) which will not send an EAPOL start until switch sends the request	Fixed
<b>DNSE/3.0.0.90 - X-Series - Security vulnerabilities.</b> DELL-1144/FIELD-2337	RC4 Ciphers CVE-2013-2566. - disabled the use of RC4 based ciphers  CBC mode ciphers CVE-2014-3566 - disabled SSLv3.0 and below protocols  Use of weak hash CVE-2012-4929 - disabled SSL compression	Fixed
<b>DNSE/X1052/3.0.0.90/crash @ BRMN task.</b> DELL-1151/FIELD-2373	Switch crash and reboot – losing connectivity and not forwarding traffic.	Fixed
<b>DNSE/3.0.0.91 - X-Series - Security vulnerability CVE-2016-2183</b> DELL-1154/FIELD-2434	Found during Retina System Vulnerability scanner. Remote attackers can obtain clear text data via a birthday attack against a long-duration encrypted session	Fixed - disabled DES & 3DES based ciphers in the SSL cipher list
<b>DNSE/3.0.0.90 - X0152P - LLDP info fails to show up via WebUI.</b> DELL-1150/FIELD-2372	On some browser GUI does not display LLDP neighbor information	Fixed



<b>DNSE/X4012: GUI Statistics displays different % of utilization for 10Gbps interfaces.</b> DELL-1157/FIELD-2410	Utilization shows only 30% of traffic on 10G ports running at 10Gbps	Fixed
----------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------	-------

The following issues have been resolved between version 3.0.0.90 and 3.0.0.91:

Summary	User Impact	Resolution
<b>Dell-1127 - DNSE/3.0.0.64 - X-Series Vulnerability</b> <b>Check CVE ID: CVE-2008-5161</b>	The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the cipher text	Fixed
<b>Dell-1136 - DNSE/3.0.0.90 - X4012 - Interface Utilization Percentage Shows 100</b>	Interface Utilization Percentage shows as 100% incorrectly in the WebUI of X4012 switches.	Fixed
<b>Dell-1140 - DNSE/3.0.0.90 - X-Series - High CPU Utilization of GOAH task</b>	Performed PCI Security scan on X-Series switches, It leads to port-channel flaps after the CPU spikes to 100% utilization.	Fixed
<b>Dell-1111 - DNSE/X-Series - SHA1 Trusted Certificate issues starting January 1, 2017</b>	Google Chrome will completely stop supporting SHA-1 (not including self-signed). So is it right to interpret that trusted SHA1 certificates will not be supported	Fixed



<b>Dell-1120 - 3.0.0.90 - Default settings in running-config shows 32 Po intfs while only 12 is supported</b>	CLI the “default settings” in show run shows 32 port-channel interfaces	Fixed
<b>Dell-1122 - 3.0.0.90 - X1000 GUI displays the LAG Type as eth1000M for 10G ports</b>	“LAG Type” displayed as ‘eth1000M’ instead of ‘eth10G’ for the X1052 platform.	Fixed
<b>Dell-1116 - DNSE/X-Series - Bandwidth gauge displays incorrectly on dashboard</b>	Incorrect display of Bandwidth at dashboard page	Partially fixed
<b>Dell-1125 - DNSE/3.0.0.90 - X-Series - STP Port Settings "Designated Cost" Display issue</b>	Incorrect display of Designated Cost for Lag interface.	Fixed
<b>Dell-1128 - DNI/30082/X1008/X1008P - Copper ports ACT LED issue under unmanaged mode</b>	X1008/X1008P copper ports ACT LED issue under unmanaged mode.  The “ACT” LED shows incorrect color with “Amber”, not correct color “Green” when X1008/X1008P set at unmanaged mode and ports are linked up at 100M speeds only	Fixed



## X1000/X4012 Series – Release Notes

The following issues have been resolved between version 3.0.0.82 and 3.0.0.90

Summary	User Impact	Resolution
<b>DELL-1016 – DNSE/X-series - 3.0.0.64: WebGui "Optical Transceiver Diagnostic" incorrect info for FCLF-8521-3-DL 1000Base-T</b>	In some scenarios when an qualified Cable will be displayed as “Generic Unqualified Transceiver”.  It’s a cosmetic issue and all cables functionality is working as expected	Fixed
<b>DELL-1009 - X4012 WebUI - Incorrect link utilization</b>	Link Utilization is incorrectly shown in WebUI of X4012 switches.  The following two issues are seen with link utilization.  1. Utilization is shown to be 200% for minimal ingress unicast/multicast traffic.  2. Utilization is blank when there is traffic egressing the port.	Fixed
<b>DELL-1098 - DNSE/X1052/3.0.0.80/Configuration loss after downloading the configGUI</b>	Trunk port configurations the interface is getting lost after the downloading the configuration via GUI and reboot.  The issue happens only when that interface has "switchport trunk native vlan none" configured	Fixed
<b>DELL-1088 - DNSE/X1052P - 3.0.0.80 : WebGUI SNMP community access mode settings doesn't match with CLI output</b>	If a new SNMP community is created with 'Read Only' access rights and DefaultSuper view map, then it appears as 'SNMP Admin' in the GUI instead. The configuration will be applied to the running-config correctly	Fixed

### Known Issues

The following issues are known in current firmware release 3.0.0.91

Summary	User Impact	Workaround
<b>DELL-1104 DNSE/X1026P/3.0.0.80 /Management access via http result in switch being unresponsive.</b>	When facing this problem experience locking out the user from remote access via https/telnet/SSH, while all device data traffic is working as expected.	Reboot the switch.



## Known Restrictions and Limitations

Summary	User Impact	Workaround
<b>X4012 – Some link flap logs on the console when shut/no-shut peer switch interface(s)</b>	Momentary link flap logs on the console when shut/no-shut peer switch interfaces.	None. Ignore console logs since it brings the link UP eventually.

## Documentation updates

### Introduction

This document lists the changes from the X1000 / X4012 series switching User's Guide. The modifications are due to instances discovered in various user environments.

Summary	Description	Relevant Documents
N/A	N/A	

## Addendum

### Port Profile Description

The Port Profile Wizard provides a convenient way to save and share common port profile configurations. When a profile is applied to a port(s) the configuration commands are executed and added to the Running Configuration File.

Port Profiles can be applied to specific interfaces, a range of interfaces, or the global configuration using the Port Profile Wizard. The Port Profiles are predefined macros which cannot be changed or deleted from the software system image.

The software system image includes 7 built-in profiles: profile-global-4, profile-global-8, profile - desktop, profile -phone, profile -switch, profile-router, profile- wireless. The following sections define the configuration information for each of the built-in profiles.

### profile-global-4:

When a port profile is configured the profile-global-4 is automatically loaded on X Series models X1008/P, X1018/P and X1026/P. When a port profile is cleared, the profile-global-4 configuration will remain.

Macro name : profile-global-4  
Macro type : default global  
macro description Global  
# Spanning Tree RSTP mode for rapid convergence  
spanning-tree mode rstp  
#QoS



```
#
qos advanced
qos map policed-dscp 24 26 46 to 0
wrr-queue bandwidth 10 10 35 45
#
# CoS to Queue Mapping
#
wrr-queue cos-map 4 0
wrr-queue cos-map 4 1
wrr-queue cos-map 3 2
wrr-queue cos-map 2 3
wrr-queue cos-map 1 5
wrr-queue cos-map 2 6
wrr-queue cos-map 2 7
#
# DSCP to Queue Mapping
#
qos map dscp-queue 40 41 42 43 44 45 46 47 to 1
qos map dscp-queue 24 25 26 27 28 29 30 31 to 2
qos map dscp-queue 48 49 50 51 52 53 54 55 to 2
qos map dscp-queue 56 57 58 59 60 61 62 63 to 2
qos map dscp-queue 16 17 18 19 20 21 22 23 to 3
qos map dscp-queue 32 33 34 35 36 37 38 to 3
qos map dscp-queue 39 to 3
qos map dscp-queue 0 1 2 3 4 5 6 7 to 4
qos map dscp-queue 8 9 10 11 12 13 14 15 to 4
#
priority-queue out num-of-queues 0
#
# MAC Access Lists
#
# IP Access Lists
#
ip access-list extended permit-all
permit ip any any
exit
#
ip access-list extended voip-data
permit ip any any dscp 46    #rfc4594: ef 101110 IP Telephony bearer
exit
#
ip access-list extended voip-control
permit ip any any dscp 24    #rfc4594: cs3 011000 Broadcast TV & live events
permit ip any any dscp 26    #rfc4594: af3 011010 Streaming video and audio on demand
exit
#
# Classes
#
class-map general-class match-any
match access-group permit-all
exit
#
class-map switch-class match-any
match access-group permit-all
exit
```





```
#
class-map router-class match-any
match access-group permit-all
exit
#
class-map voice-class match-any
match access-group permit-all
exit
#
class-map VoIP-data-class match-any
match access-group voip-data
exit
#
class-map VoIP-Control-class match-any
match access-group voip-control
exit
#
# Police Maps
#
policy-map general-map
class general-class
set dscp 7
exit
#
policy-map switch-map
class switch-class
trust
exit
#
policy-map router-map
class router-class
trust
exit
#
policy-map voice-map
class VoIP-data-class
trust
police 320 8000 exceed-action policed-dscp-transmit
exit
class VoIP-Control-class
trust
police 32 8000 exceed-action policed-dscp-transmit
exit
class voice-class
set dscp 0
exit
#
```

### profile-global-8:

When a port profile is configured the profile-global-8 is automatically loaded on X Series models X1052/P and X4012. When a port profile is cleared, the profile-global-8 configuration will remain.

Macro name : profile-global

Macro type : default global



```
macro description Global
# Spanning Tree RSTP mode for rapid convergence
spanning-tree mode rstp
#QoS
#
qos advanced
qos map policed-dscp 24 26 46 to 0
wrr-queue bandwidth 40 40 240 80 1 1
#
# CoS to Queue Mapping
#
wrr-queue cos-map 4 0
wrr-queue cos-map 4 1
wrr-queue cos-map 2 3
wrr-queue cos-map 3 4
wrr-queue cos-map 7 5
wrr-queue cos-map 2 6
wrr-queue cos-map 2 7
#
# DSCP to Queue Mapping
#
qos map dscp-queue 40 41 42 43 44 45 46 47 to 7
qos map dscp-queue 24 25 26 27 28 29 30 31 to 2
qos map dscp-queue 48 49 50 51 52 53 54 55 to 2
qos map dscp-queue 56 57 58 59 60 61 62 63 to 2
qos map dscp-queue 16 17 18 19 20 21 22 23 to 3
qos map dscp-queue 32 33 34 35 36 37 38 to 3
qos map dscp-queue 39 to 3
qos map dscp-queue 0 1 2 3 4 5 6 7 to 4
qos map dscp-queue 8 9 10 11 12 13 14 15 to 4
#
# MAC Access Lists
#
# IP Access Lists
#
ip access-list extended permit-all
permit ip any any
exit
#
ip access-list extended voip-data
permit ip any any dscp 46    #rfc4594: ef 101110 IP Telephony bearer
exit
#
ip access-list extended voip-control
permit ip any any dscp 24    #rfc4594: cs3 011000 Broadcast TV & live events
permit ip any any dscp 26    #rfc4594: af3 011010 Streaming video and audio on demand
exit
#
priority-queue out num-of-queues 2
#
# Classes
#
class-map general-class match-any
match access-group permit-all
exit
```



```
#
class-map switch-class match-any
match access-group permit-all
exit
#
class-map router-class match-any
match access-group permit-all
exit
#
class-map voice-class match-any
match access-group permit-all
exit
#
class-map VoIP-data-class match-any
match access-group voip-data
exit
#
class-map VoIP-Control-class match-any
match access-group voip-control
exit
#
# Police Maps
#
policy-map general-map
class general-class
set dscp 7
exit
#
policy-map switch-map
class switch-class
trust
exit
#
policy-map router-map
class router-class
trust
exit
#
policy-map voice-map
class VoIP-data-class
trust
police 320 8000 exceed-action policed-dscp-transmit
exit
class VoIP-Control-class
trust
police 32 8000 exceed-action policed-dscp-transmit
exit
class voice-class
set dscp 0
exit
#
```

### profile-desktop

Used for port interface configuration for increased network security and reliability when connecting a desktop device, such as a PC, to a switch port.



Macro name : profile-desktop  
macro description profile-desktop  
# macro keywords \$access\_vlan  
# Basic interface - Enable data VLAN only  
# Recommended value for access vlan should not be 1  
switchport access vlan \$access\_vlan  
switchport mode access  
# Port Security is enabled to limit to 1 MAC address  
# (desktop MAC) on the port  
port security max 1  
port security mode max-addresses  
port security discard  
# Configure port as an edge network port  
spanning-tree portfast  
spanning-tree bpduguard enable

### profile-phone

Used for port interface configuration when connecting a desktop device, such as a PC with an IP Phone, to a switch port.

Macro name : profile-phone  
macro description profile-phone  
# macro keywords \$access\_vlan \$voice\_vlan  
# Data vlan (access\_vlan) and voice vlan (voice\_vlan)  
# are both active for a VoIP enabled interface  
  
# Recommended value for access vlan should not be 1  
switchport general pvid \$access\_vlan  
switchport general allowed vlan add \$access\_vlan untagged  
switchport mode general  
# Update the Voice VLAN value which should be  
# different from data VLAN  
# Recommended value for voice vlan should not be 1  
switchport general allowed vlan add \$voice\_vlan tagged  
# Port Security is enabled to limit to 2 MAC addresses on the port  
#(desktop mac and phone mac)  
port security max 2  
port security mode max-addresses  
port security discard  
# qos configuration to extend trust to attached IP phone  
service-policy input voice-map  
# Configure port as an edge network port  
spanning-tree portfast  
spanning-tree bpduguard enable

### profile-switch

Used for interface configuration when connecting an access switch and a distribution switch, or between access switches.

Macro name : profile-switch  
macro description profile-switch  
# macro keywords \$native\_vlan  
# Define unique Native VLAN on trunk ports



```
# Recommended value for native vlan should not be 1
switchport trunk native vlan $native_vlan
# Update the allowed VLAN range such that it
# includes data, voice and native VLANs
switchport trunk allowed vlan ALL
switchport mode trunk
# Configure qos to trust this interface
service-policy input switch-map
# 802.1w defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point
```

### profile-router

Used for interface configuration when connecting the switch to a WAN router.

```
Macro name : profile-router
macro keywords $native_vlan
macro description profile-router
# Native VLAN defaults to 1 if not specifically defined
switchport trunk native vlan $native_vlan
# Include all VLANs on Trunk
switchport trunk allowed vlan ALL
switchport mode trunk
# Configure qos to trust this interface
service-policy input router-map
# Ensure that switch devices cannot become active on the interface.
spanning-tree bpduguard enable
```

### profile-wireless

Used for interface configuration when connecting the switch to a wireless access point.

```
Macro name : profile-wireless
macro description profile-wireless
# macro keywords $native_vlan
# Native VLAN defaults to 1 if not specifically defined
switchport trunk native vlan $native_vlan
# Include all VLANs on Trunk
switchport trunk allowed vlan ALL
switchport mode trunk
# Configure qos to trust this interface
service-policy input router-map
# Ensure that switch devices cannot become active on the interface.
spanning-tree bpduguard enable
```

<b>End of Release Notes</b>
-----------------------------