

## **Firmware V5.00 Release Note**

### **ZAP 4.0**

Date: February 03, 2017

## Table of Content

Firmware V5.00 Release Note .....	1
ZAP 4.0 .....	1
1. Overview .....	3
2. What's New in This Release .....	3
3. Supported Platforms: .....	4
4. Supported Utilities:.....	5
5. Files lists contains in the Release ZIP file .....	7
6. Read Me First before Upgrade .....	8
7. Enhancements: .....	8
8. Resolved Issues: .....	11
9. Design Limitations and Known Issues .....	15
Design Limitations.....	15
Zyxel NXC WLAN Controller and Managed AP Mode.....	15
Zyxel Access Points .....	15
Known Issues .....	15
Zyxel NXC WLAN Controller and Managed AP Mode.....	15
Zyxel Access Points in Standalone Mode .....	23
Appendix - A. System Default Setting .....	24
Appendix - B. Firmware Upgrade / Downgrade Procedure .....	25
Appendix - C. SNMPv2 private MIBS support .....	27
Appendix - D. Firmware Recovery .....	28

## **Firmware Release V5.00**

### **1. Overview**

---

This document provides firmware release information on Zyxel NXC WLAN Controller and Unified Access Points platforms, plus new features, enhancements, read-me first before firmware upgrade, known issues and workarounds information for Release V5.00.

### **2. What's New in This Release**

---

Following new features are introduced in this release.

- New AP WAC5302D-S support
- New AP NWA1123-ACv2 support
- Dashboard enhancement for Top N AP by 2.4G or 5G traffic usage
- Monitor Wireless enhancement for SSID Info with 2.4G/5G Station No.
- MAC Authentication fallback to Web Authentication
- Support 802.11r Fast Roaming on NWA5120 series & WAC6000 series
- Dynamic VLAN Assignment by Group
- Managed AP auto save last configuration
- Authentication Primary/Secondary Server fallback
- NXC Internal Captive Portal with FQDN support
- Support computer authentication on Microsoft AD server
- Support Japanese language on controller
- Standalone AP supports Rate Limit
- SNMP MIB Enhancement
- Log enhancement for DFS channel log

## 3. Supported Platforms:

---

### Zyxel WLAN Controller

- NXC2500 V5.00(AAIG.3)
- NXC5500 V5.00(AAOS.3)

### Zyxel Access Points

- NWA3160-N V5.00(UJA.3)
- NWA3550-N V5.00(UJB.3)
- NWA3560-N V5.00(UJC.3)
- NWA5160N V5.00(AAS.3)
- NWA5550-N V5.00(UJD.3)
- NWA5560-N V5.00(UJE.3)
- NWA5121-NI V5.00(AAID.3)
- NWA5123-NI V5.00(AAHY.3)
- NWA5121-N V5.00(AAIF.3)
- NWA5301-NJ V5.00(AANB.3)
- WAC6502D-E V5.00(AASD.3)
- WAC6502D-S V5.00(AASE.3)
- WAC6503D-S V5.00(AASF.3)
- WAC6553D-E V5.00(AASG.3)
- WAC6103D-I V5.00(AAXH.3)
- NWA5123-AC V5.00(AAZY.3)
- WAC5302D-S V5.00(ABFH.3)
- NWA1123-ACv2 V5.00(ABEL.3)

## 4. Supported Utilities:

The exact support release for AP models, please refer to the Utility release note for more details.

### Zyxel One Network (ZON):

Product	Series	Model
Wi-Fi Access Point	WAC6500 series	WAC6502D-E WAC6502D-S WAC6503D-S WAC6553D-E
	WAC5302D-S	WAC5302D-S
	WAC6100 series	WAC6103D-I
	NWA5120 series	NWA5121-NI NWA5121-N NWA5123-NI NWA5123-AC
	NWA5301-NJ	NWA5301-NJ
	NWA1123-ACv2	NWA1123-ACv2
NXC Controller	NXC series	NXC5500 NXC2500

### Zyxel AP Configurator (ZAC):

Series	Access Point
Model	NWA5121-NI NWA5121-N NWA5123-NI NWA5123-AC NWA5301-NJ

	WAC6103D-I WAC6502D-E WAC6502D-S WAC6503D-S WAC6553D-E WAC5302D-S NWA1123-ACv2
--	--

\* ZAC configuration of Access Point is supported with Standalone AP mode.

### Zyxel Wireless Optimizer (ZWO)

Series	Access Point	Wireless LAN Controller
Model	NWA3160-N NWA3560-N NWA3550-N NWA5160N NWA5560-N NWA5550-N NWA5123-AC NWA5121-NI NWA5121-N NWA5123-NI NWA5301-NJ WAC6103D-I WAC6502D-E WAC6502D-S WAC6503D-S WAC6553D-E WAC5302D-S	NXC2500

## 5. Files lists contains in the Release ZIP file

---

### **File name: \*.bin**

Purpose: This binary firmware image file is for normal system update.

Note: The firmware update may take five or more minutes depending on the scale of device configuration. The more complex configuration will take more update time. Do not turn off or reset the NXC2500 while the firmware update is in progress. The firmware might get damaged, if device loss power or you reset the device during the firmware upload. You might need to refer to Appendix D of this document to recover the firmware.

### **File name: \*.conf**

Purpose: This ASCII file contains default system configuration commands.

### **File name: \*.db**

Purpose: This binary file contains default system signatures.

Note: The file is only needed when doing system recovery from damage.

### **File name: \*.ri**

Purpose: This binary firmware recovery image file is for emergent system firmware damage recovery only.

### **File name: \*-MIB.zip**

**Purpose: The MIBs are to collect information on device. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.**

## 6. Read Me First before Upgrade

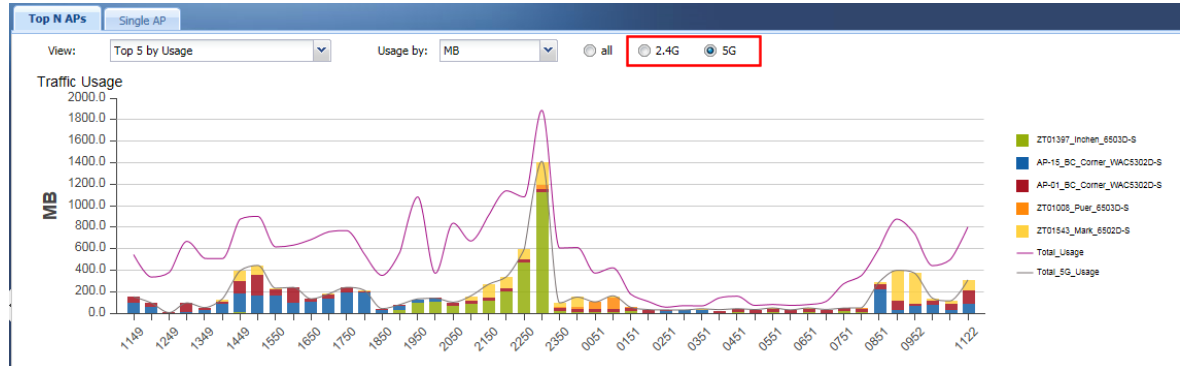
1. The firmware V5.00 supports the latest version of Microsoft *Internet Explorer* and Google *Chrome*.

## 7. Enhancements:

This section includes the enhancements in this firmware V5.00 release.

1. Top N AP by 2.4G or 5G traffic usage

When clicking the color bar, it will drill down to the specific AP information for further setting viewing.



2. SSID Info with 2.4G/5G Station No.

When clicking the number in the 2.4GHz or 5GHz column, it will show the relevant station list information for further viewing

The screenshot shows the 'SSID Info' interface. On the left is a 'MONITOR' sidebar with a tree view containing 'System Status', 'Wireless', 'AP Information', 'ZyMesh', 'SSID Info', 'Station Info', 'Detected Device', and 'Log'. The 'SSID Info' tab is selected. The main area displays a table titled 'Station information for each SSID'. The table has the following columns: '#', 'SSID', '2.4GHz', '5GHz', 'SSID Profile Name', and 'Security Mode'. The '2.4GHz' and '5GHz' columns are highlighted with a red box. The data in the table is as follows:

#	SSID	2.4GHz	5GHz	SSID Profile Name	Security Mode
1	6100 tunnel	0	0	Test_6100_tunnel	wpa2mix
2	ACWL	2	0	ZT01455_ACWL	wpa2-psk
3	ACWL	2	0	ZT02072_ACWL	wpa2-psk
4	ACWL5G	0	0	ZT01455_ACWL5G	wpa2-psk
5	ACWL5G	0	0	ZT02072_ACWL5G	wpa2-psk
6	BearTest5G	0	1	ZT02139_BearTest5G	wpa2-psk
7	BearTest24G	0	0	ZT02139_BearTest24G	wpa2-psk
8	BistroJC	1	0	ZT01613_BistroJC_2G	wpa2-psk
9	BistroJC_5G	0	0	ZT01613_BistroJC_5G	wpa2-psk
10	Brian_5G	0	0	ZT01055_Brian_5G	wpa2-psk

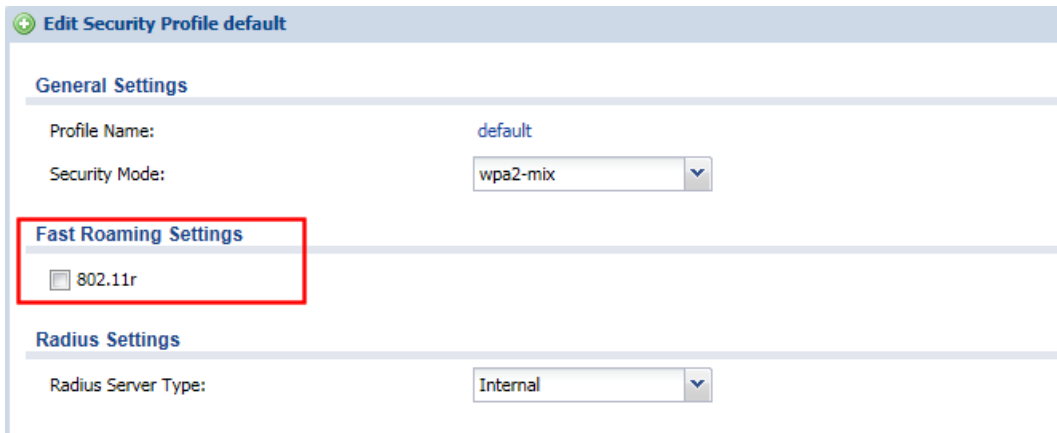


- 3. MAC Authentication fallback to Web Authentication  
This feature enables one SSID supports MAC Auth fallback to Web Auth. Prior to v5.00, MAC Auth and Web Auth require to be different SSID. Note: NWA3000 and NWA5000 series do not support MAC Authentication fallback to Web Authentication feature.
  
- 4. Dynamic VLAN Assignment by Group  
FW v5.00 supports Dynamic VLAN Assignment to wireless clients based on user group information configured in the RADIUS server.

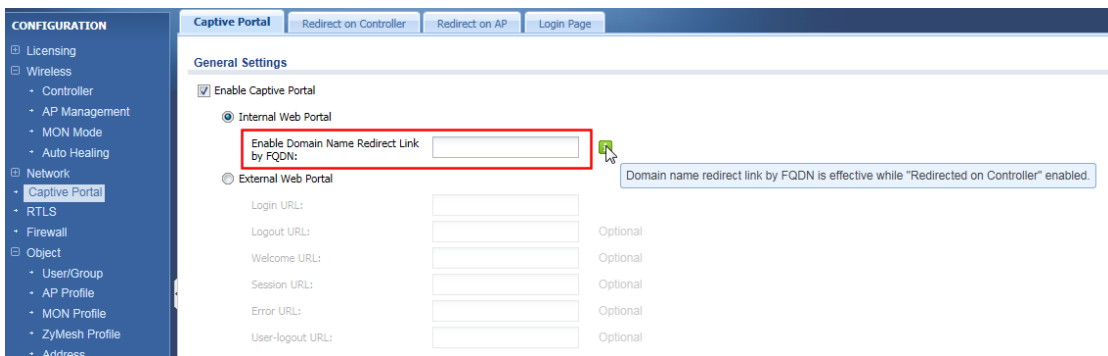
**User Configuration**

User Name :	<input type="text" value="student"/>
User Type:	<input type="text" value="ext-group-user"/> ▼
Group Identifier:	<input type="text" value="student"/>
Associated AAA Server Object:	<input type="text" value="radius"/> ▼
Description:	<input type="text" value="Local User"/>
Authentication Timeout Settings	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> Use Manual Settings
Lease Time:	<input type="text" value="1440"/> minutes
Reauthentication Time:	<input type="text" value="1440"/> minutes
<input checked="" type="checkbox"/> User VLAN ID:	<input type="text" value="102"/> × (1~4094)

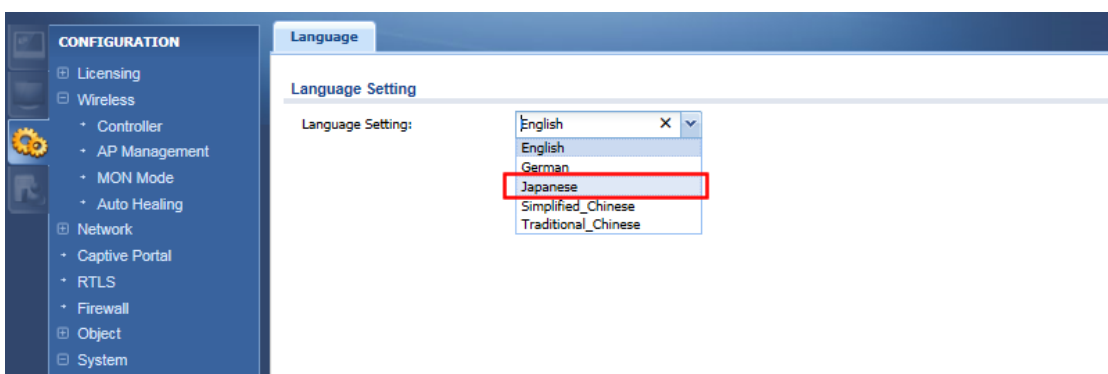
- 5. The V5.00 release supports 802.11r on managed AP NWA5120 series & WAC6000 series for fast roaming. It can be enabled on wpa2/wpa2-mix security mode.



## 6. NXC Internal Captive Portal with FQDN support



## 7. The V5.00 release supports Japanese on controller



## 8. SNMP MIB Enhancement

- AP status on NXC table entry
- Query login user by SNMP

- Per Client TX/RX data bytes
- Total client count per AP(standalone)
- AP TX and RX data byte counters on Controller and AP.  
( Note: Currently only packet count)

## 8. Resolved Issues:

---

1.  
[eITS: 160400957 ]  
[Symptom] Badlock vulnerability on NXC controller, though in normal enterprise switched network environment, it is difficult for an attacker to perform MITM in-between NXC controller and the AD server.
2.  
[eITS: 160500535 ]  
[Symptom] AP and NXC connect through CAPWAP, but can not automatically join default group. The AP group field of the AP is empty
3.  
[eITS: 160500753 ]  
[Symptom] WAC6503DS AP auto reboot randomly.
4.  
[eITS: 160501889 ]  
[Symptom] "realm" and "NetBIOS" support underscore(\_)
5.  
[eITS: 160700570 ]  
[Symptom] When user use 802.1x auth, the system log didn't use prime symbol ( ' ') to include user name.

6.  
[eITS: 160601343 ]  
[Symptom] WAC6502D-S is frequently down.
7.  
[eITS: 160700869 ]  
[Symptom] DHCP reservation from DHCP table in Dashboard does not work after upgrading to firmware 4.30.
8.  
[eITS: 160700992 ]  
[Symptom] The uplink rate limit setting is invalid when the SSID in tunnel mode with VLAN tag.
9.  
[eITS: 160800194 ]  
[Symptom] When AP is changed the IP, but the tunnel rule is still used the original IP address, it cannot be re-created, caused by the connection is lost and the client cannot get the IP address.
10.  
[eITS: 160800370 ]  
[Symptom] The uplink of Rate Limit in tunnel mode doesn't work when the management VLAN and SSID VLAN are different.
11.  
[eITS: 160800371 ]  
[Symptom] A laptop sent some unknown packet cause by the Zylog daemon service is dead.
12.  
[eITS: 160700399 ]  
[Symptom] Captive portal and Redirect on AP doesn't work on repeater AP with ZyMESH .
- 13.

- [eITS: 160800401 ]  
[Symptom] Wireless bridge will be disabled after rebooting.
14.  
[eITS: 160700868 ]  
[Symptom] Add a new feature for NXC drop ICMP unreachable packets in the output chain.
15.  
[eITS: 160800931 ]  
[Symptom] Static route cannot enter IP-0.0.0.0 in the Destination IP on the GUI, but can add via CLI.
16.  
[eITS: 160800931 ]  
[Symptom] LDAP user login fails when upgrading to firmware v4.30
17.  
[eITS: 160900068 ]  
[Symptom] NXC ZySH daemon dead Condition:Socket leak is caused by using debug remoteWTP command
18.  
[eITS: 160900555 ]  
[Symptom] If connecting the devices to the NXC5500, after NXC reboot, the port speed status will be 100M. However, if unplug and re-plug again, the port speed will return to 1000M.
19.  
[eITS: 160900206 ]  
[Symptom] When we do 802.1x for authentication, the account is not able to pass the authentication.
20.  
[eITS: 161100309 ]

[Symptom] NXC controller QRUser fails to pass authentication if its password length is more than 60 characters.

21.

[eITS: 160801219 ]

[Symptom] [MIS field trial] uamd daemon is dead caused by NXC trigger hardware watchdog to reboot the NXC

## 9. Design Limitations and Known Issues

---

This section describes the system behavior or limitations in this firmware release. They will be created into knowledge base.

### Design Limitations

#### **Zyxel NXC WLAN Controller and Managed AP Mode**

N/A

#### **Zyxel Access Points**

NWA5301 does not support SSH version 1.

### Known Issues

#### **Zyxel NXC WLAN Controller and Managed AP Mode**

##### **GUI:**

1. [SPR: 140701012]  
[Symptom] Plug in two USB thumb drives, the GUI shows only one USB Virtual Device in the Dashboard page.
2. [SPR: 150728882]

[Symptom] If creating an ext-group-user in User/Group page, and "Associated AAA Server Object" select AD-Server, the object reference of hyper link will redirect to the wrong page.

3. [SPR: 151103048]

[Symptom] Configure the 2.4GHz channel width as 20/40MHz for NWA3560-N, GUI channel width does not change to 20MHz on the GUI, but it is actually 20MHz configured.

4. [SPR: 151123781]

[Symptom] The value character can't have "\_" in AAA Server' name for AD, LDAP, RADIUS server and cannot exceed 30 characters in RADIUS server.

5. [SPR: 151214770]

[Symptom] NXC Dashboard displays error with Microsoft Internet Explorer 10.

6. [SPR: 160308287]

[Symptom] There is an additional null row at the bottom of AP list.

7. [SPR: 160531033]

[Symptom] The SSID page "Object Name" , the hyperlink cannot be redirected back.

8. [SPR: 160511443]

[Symptom] CONFIGURATION > System > SNMP > SNMPv3 > add User > Select a user with less than 8 passwords (because the password is less than 8, it cannot be added) > User / Group to delete the selected User, it cannot be deleted.

9. [SPR: 161213541]

[Symptom] When enabling MAC auth fallback, the SSID Profile with MAC Cache on the captive portal page, it cannot be added when SSID profile name contains special characters,



## Monitor Mode:

1. [SPR: 140624104]  
[Symptom] Inactivate Mon Mode profile, it will still keep device list in Detected Device.
2. [SPR: 140922844]  
[Symptom] The old SSID data are not cleaned if all aps from MON mode to AP mode in Detected Device.
3. [SPR: 150901039]  
[Symptom] The AP use Mon Mode to monitor 802.11AC SSID, it will be display 802.11n 40MHz WEP.

## Wireless:

1. [SPR: 140820699]  
[Symptom] Wireless client cannot be authorized with EAP TTLS(Mschapv2), if controller uses following settings:
  - i. 802.1X
  - ii. Security: none
  - iii. Authentication method: local database
2. [SPR: 140820701]  
[Symptom] Wireless client cannot be authorized with EAP PEAP(Mschapv2), if Controller uses following settings:
  - i. 802.1X
  - ii. Security: none
  - iii. Authentication method: local database
3. [SPR: 140820702]  
[Symptom] Wireless client cannot be authorized with EAP PEAP(TLS), if controller uses following settings
  - i. 802.1X
  - ii. Security: none

iii. Authentication method: local database

4. [SPR: 141211739]

[Symptom] When SSID name with three spaces sequentially, it causes GUI display incorrectly

### **WDS:**

1. [SPR: 150717134]

[Symptom] If the Repeater AP's Ethernet port is attached to Lan1 port instead of Uplink port, the network will loop.

2. [SPR: 160202129]

[Symptom] In ZyMesh deployment, AP may have mesh disconnect log in some extreme cases due to driver issues, the log is triggered by the workaround embedded in the firmware. When it happens, the AP mesh link will disconnect and reconnect instantly, there is no significant wireless connection impact in general applications.

### **CAPWAP:**

1. [SPR: 150526058]

[Symptom] Some station info will be kept in station info list on the NXC controller even the stations have been dissociated from the AP.

### **System:**

1. [SPR: 140822847]

[Symptom] If user types are "user" or "limited-admin", user is able to perform ftp login on fat AP.

2. [SPR: 140919757]

[Symptom] Power management in WAC6503D-S Standalone mode is incorrect if using PoE 802.3af mode.

3. [SPR: 141111336]

[Symptom] While editing LAN PVID in AP Group Setting > Port Setting, the setting will apply to managed AP immediately even if Cancel button is clicked on AP Group Setting page.

4. [SPR: 141126208]

[Symptom] When VLAN interface gateway does not set, the Metric is not grayed out.

5. [eITS: 140800476]

[Symptom] Many VLANs are configured on the NXC2500. When rebooting the NXC2500, there is possibility that WLAN Clients for example in VLAN 1 getting IPs from DHCP Servers in VLAN 2.

6. [eITS: 150700345]

[Symptom] The Web GUI of NXC indicated the high CPU usage after long system up time.

7. [eITS: 151214794]

[Symptom] When changing the LAN provision for different APs at once, the configuration to the 5301 has no effect.

## **SNMP:**

1. [SPR: 150508405]

[Symptom] The OID value of "station associated time" displays the wrong time format.

## **Configuration Backup/Restore:**

1. [SPR: 150525002]

[Symptom] If the configuration name is started with symbolic characters ".", the GUI will show 'Operation is prohibited'.

## AAA:

1. [SPR: 140818646]  
[Symptom] When client rejects by RADIUS, controller does not show the log of reject reason.
2. [SPR: 150709611]  
[Symptom] When change the default order and priority of the authentication methods on the NXC controller or server IP address, it may occur the users cannot pass the authentication.
3. [SPR: 150821249]  
[Symptom] If the case-sensitive user names are disabled on the AD profile, logging the username by ext-group-user on 802.1X authentication will show the user does not exist in the group.
4. [SPR: 151102017], [SPR: 160511466]  
[eITS: 151001059]  
[Symptom] Computer authentication will fail when the RADIUS server is not on the top of the Authentication Method list.
5. [SPR: 160506735]  
[Symptom] Set up Accounting Max retry count = 3, when the accounting server is not be found, the Radius internal 802.1x will not retry 3 times.
6. [SPR: 160602137]  
[Symptom] If browser is used the Firefox, the account and password will be display on GUI.
7. [SPR: 170125950]  
[Symptom] When there are two APs behind NAT, if one AP was

removed, wireless client via MAC authentication would fail. In normal circumstance, wireless client shall be able to perform MAC authentication without issue while connecting to the other AP which was not removed.

8. [SPR: 170123761]  
[Symptom] For WAC5302D-S, there is possibility that 802.1 X clients may not associate to the AP via either 2.4GHz or 5GHz in certain extreme environment, even though there is a AP reboot workaround in place.

## **Captive Portal:**

1. [SPR: 140820735]  
[Symptom] When wireless client disassociated but login user will not be logout from controller.
2. [SPR: 160601066]  
[Symptom] When enabling the captive portal on AP and Layer 2 isolation together, it needs to add the MAC address of AP into the list of Layer2 isolation.
3. [SPR: 160726983]  
[Symptom] Captive portal request IOS clients to re-log in after disconnect the SSID.
4. [SPR: 161026967]  
[Symptom] WAC5302D-S AP does not support MAC Authentication Fallback to Captive Portal after MAC authentication failure.

## **User / Group / Captive Portal:**

1. [SPR: 150723471]  
[Symptom] The User idle timeout does not work.

## **User / Group / GUI:**

N/A

## **ZON:**

1. [SPR: 151120733]  
[Symptom] If managed AP was enabled LED locator by using ZON utility, the type of icon should be changed to flash icon but managed AP does not.

## **Rate Limit:**

1. [SPR: 160802043]  
[Symptom] Rate limit using tunnel mode with management VLAN (2~4094) cause station upload rate limit can not work.

## **Auto Healing:**

2. [SPR: 150513963]  
[Symptom] NXC2500's Auto Healing Log and console log cannot update AP Description in time.

## **Certificate:**

1. [SPR: 160511432]  
[Symptom] uses SHA1 certificate, the HTTPS connection in Safari does not work with the Web.

## **Zyxel Access Points in Standalone Mode**

1. [SPR: 141204234]  
[Symptom] Using IE11 and Chrome cannot login to Standalone AP when enabling Https and Authenticate Client Certificates.
  
2. [SPR: 140625215]  
[Symptom] The SNMPv1 cannot work on Standalone AP.
  
3. [SPR: 150114622]  
[eITS: 150100208]  
[Symptom] The error message "Do NTP update has failed" shows up when pressing "Sync. Now" button from Date/Time configuration page on Repeater AP.
  
4. [SPR: 160223491]  
[Symptom] If client connect to SSID VLAN(2~4094),daily report does not display radio traffic.
  
5. [SPR: 160330505]  
[Symptom] Accounting Interim Update should be gray out on the GUI when the authentication Settings set as PSK.

## Appendix - A. System Default Setting

### Zyxel NXC WLAN Controller

Following is the system default configuration

- The default device information for NXC controllers  
IP: 192.168.1.1  
Administration username: admin  
Password: 1234
- The default LAN interface is vlan0. The default LAN subnet is 192.168.1.0/24.
- By default, SSH service can only be accessed from LAN subnet.

### Zyxel Access Points

- For AP in Standalone mode, following is the system default configuration:  
The default device information for Unified Access Points  
IP: 192.168.1.2  
Administration username: admin  
Password: 1234
- For AP in Managed AP mode by default, DHCP client enabled is by default.



## Appendix - B. Firmware Upgrade / Downgrade Procedure

The following is the firmware **upgrade** procedure:

1. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:
  - Use Browser to login into NXC2500 as administrator.
  - Click Maintenance > File Manager > Configuration File to open the Configuration File screen. Use the Configuration File screen to backup current configuration file.
  - Find firmware at [www.zyxel.com](http://www.zyxel.com) in a file that (usually) uses the system model name with the .bin extension, for example, "**421AAIG1.bin**".
  - Click Maintenance > File Manager > Firmware Package to open the Firmware Package screen. Browser to the location of firmware package and then click Upload. The NXC2500 automatically reboots after a successful upload.
  - After several minutes, the system is successfully upgraded to newest version.

The following is the firmware **downgrade** procedure:

(We do not recommend user to downgrade f/w of device.)

1. If user has already backup the configuration file before firmware upgrade, please follow the procedures below:
  - Use Console/Telnet /SSH to login into NXC2500.
  - Router>**enable**
  - Router#**configure terminal**
  - Router(config)#**setenv-startup stop-on-error off**
  - Router(config)#**write**
  - Load the older firmware to NXC2500 using standard firmware upload procedure.
  - After system uploads and boot-up successfully, login into NXC2500 via GUI.
  - Go to GUI → "File Manager" menu, select the backup configuration filename, for example, statup-config-backup.conf and press "Apply" button.
  - After several minutes, the system is successfully downgraded to older version.
2. If user did not backup the configuration file before firmware upgrade, please follow the procedures below:

1. Use Console/Telnet /SSH to login into NXC2500.
2. Router>**enable**
3. Router#**configure terminal**
4. Router(config)#**setenv-startup stop-on-error off**
5. Router(config)#**write**
6. Load the older firmware to NXC2500 using standard firmware upload procedure.
7. After system upload and boot-up successfully, login into NXC2500 via Console/Telnet/SSH.
8. Router>**enable**
9. Router#**write**

Now the system is successfully downgraded to older version.

**Note: NXC2500 might lose some configuration settings during this downgrade procedure. It is caused by configuration conflict between older and newer firmware version. If this situation happens, user needs to configure these settings again.**

## **Appendix - C. SNMPv2 private MIBs support**

SNMPv2 private MIBs provides user to monitor NXC2500 platform status. If user wants to use this feature, you must prepare the following step:

1. Have NXC2500 mib file and install to your MIBs application (like MIB-browser).
2. NXC2500 SNMP is enabled.
3. Using your MIBs application connects to NXC2500.

## Appendix - D. Firmware Recovery

In some rare situation, NXC2500 might not boot up successfully after firmware upgrade. The following procedures are the steps to recover firmware to normal condition. Please connect console cable to NXC2500.

If NXC2500 Booting failed, NXC2500 will automatically perform the "Restore Firmware" process. Example: The device show "Bad Data CRC" while uncompressing "Kernel Image".

```
BootModule Version: V1.00 | 2013-03-29 15:39:33
DRAM: Size = 1024 Mbytes

Kernel Version: V2.6.32.27 | 2013-05-23 19:55:22
ZLD Version: V4.00(AAIG.1) | 2013-05-28 09:35:00
CAPWAP Version: V1.00.02

MMC read: dev # 0, block # 2048, count 2048 ... 2048 blocks read: OK

Press any key to enter debug mode within 3 seconds.

BM cmd line: console=ttyS0,115200 numcores=2 mem=1024M
local_args[0]=bootm, local_args[1]=0x20000000
Execute Command (Load Normal Kernel): mmc read 0 0x20000000 0x32801 0x27fff

MMC read: dev # 0, block # 206849, count 163839 ... 163839 blocks read: OK
## Booting kernel from Legacy Image at 20000000 ...
Image Name: Linux Kernel Image
Created: 2013-05-06 8:05:04 UTC
Image Type: MIPS Linux Kernel Image (lzma compressed)
Data Size: 2931281 Bytes = 2.8 MiB
Load Address: 05000000
Entry Point: 80101400
Verifying Checksum ... Bad Data CRC
ERROR: can't get kernel image!
Execute Command (Load Recovery Kernel): mmc read 0 0x20000000 0xa800 0x28000
```

### 1. Restore Firmware

- If "Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file" displays on the screen, you need to recover the firmware by the following procedure.

**Connect a computer to port 1 and FTP to 192.168.1.1 to upload the new file.**

- You will use FTP to upload the firmware package. Keep the console session open in order to see when the firmware recovery finishes.
- Set your computer to use a static IP address from 192.168.1.2 ~ 192.168.1.254. No matter how you have configured the NXC2500's IP addresses, your computer must use a static IP address in this range to recover the firmware.
- Connect your computer to the NXC2500's port 1 (the only port that you can use for recovering the firmware).
- Use an FTP client on your computer to connect to the NXC2500. This example uses the ftp command in the Windows command

prompt. The NXC2500's FTP server IP address for firmware recovery is 192.168.1.1

- Log in without user name (just press enter).
- Set the transfer mode to binary. Use "bin" (or just "bi" in the Windows command prompt).
- Transfer the firmware file from your computer to the NXC2500 (the command is "put 421AAIG1.bin" in the Windows command prompt).

```
c:\users\zt01571\documents\esbu\nxc2500\Patch1C0\400AAIG1C0>ftp 192.168.1.1
Connected to 192.168.1.1.
220-=(<^>)=-.: ( ( Welcome to PureFTPd 1.0.11 )) :.-=(<^>)=
220-You are user number 1 of 50 allowed
220-Local time is now 00:04 and the load is 0.00. Server port: 21.
220-Only anonymous FTP is allowed here
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.1.1:(none)):
230 Anonymous user logged in
ftp> bin
200 TYPE is now 8-bit binary
ftp> put 400AAIG1C0.bin
```

- Wait for the file transfer to complete.

```
200 PORT command successful
150 Connecting to port 61419
226-399.5 Mbytes free disk space
226-File successfully transferred
226 8.191 seconds (measured here), 11.08 Mbytes per second
ftp: 95152648 bytes sent in 8.195seconds 11620.99Kbytes/sec.
ftp>
```

- The console session displays "Firmware received" after the FTP file transfer is complete. Then you need to wait while the NXC2500 recovers the firmware (this may take up to 4 minutes).

```
Firmware received ...
Start to check file system...
/dev/mmcblk0p6: 42/30720 files (4.8% non-contiguous), 47789/122880 blocks
/dev/mmcblk0p7: 132/131072 files (2.3% non-contiguous), 17447/26kjournal starting. Commit interval 5 seconds
2144 blocks
Done
Updating ...
```

- The message here might be "ZLD-current received". Actually, it is equivalent to "Firmware received".

```
ZLD-current received ...
```

```
[Update Filesystem]
  Updating Code
```

- The console session displays "done" when the firmware recovery is complete. Then the NXC2500 automatically restarts.

```

[Updating] /share/wtp_image/NWA5KCN50
.....
[Updating] done.

[Updating] /share/wtp_image/wtpinfo
.
[Updating] done.

rmdir/mkdir /tmp/p6

mount -t ext3 /dev/mmcb1k0p6 /tmp/p6

[Updating] /tmp/p6/compress.img
.....
[Updating] done.

umount/rmdir /tmp/p6
[Updating] touch .fsextract_done is done
mount: mount point /etc/zyxel/ftp/wtp_image/real_wtp_image/ does not exist
Error: We can't mount real_wtp_image partition
md: stopping all md devices.
Restarting system.

```

- The username prompt displays after the NXC2500 starts up successfully. The firmware recovery process is now complete and the NXC2500 is ready to use.
- If one of the following cases occurs, you need to do the “firmware recovery process” again. Note that if the process is done several time but the problem remains, please collect all the console logs and send to Zyxel for further analysis.

If you can't connect to GUI, there is the other way can upload firmware to device.

This method can be used on NXC series and any model APs.

- Use an FTP client on your computer to connect to the device. This example uses the ftp command in the Windows command prompt.
- Log in admin-type user name and enter password
- Set the transfer mode to binary. Use “bin” (or just “bi” in the Windows command prompt).
- Transfer the firmware file from your computer to the device (the command is “put 420AAIF1C0.bin” in the Windows command prompt).

```

C:\>ftp 192.168.1.101
Connected to 192.168.1.101.
220-
220-You are user number 1 of 5 allowed.
220-Local time is now 01:44. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 600 minutes of inactivity.
User (192.168.1.101:(none)): admin
331 User admin OK. Password required
Password:
230 OK. Current restricted directory is /
ftp> bi
200 TYPE is now 8-bit binary
ftp> put C:\421AAXH0C0.bin

```

- Wait for the file transfer to complete.

```
200 PORT command successful
150 Connecting to port 49532
226-File successfully transferred
226-1.230 seconds (measured here), 23.68 Mbytes per second
226-firmware verifying...
226-firmware updating...
226-Please Wait about 5 minutes!!
226-Do not poweroff or reset.
226-system will reboot automatically after finished updating.
226 226 Transfer complete.
ftp: 30540424 bytes sent in 1.23Seconds 24890.32Kbytes/sec.
```

- Device will update firmware after receiving file. Please do not cut off the power supply of device until the LED stop blink.