WiNG 5.7.1.0-019R Release Notes

Overview

WiNG 5.7.1 is a maintenance release that continues to build on the innovative WiNG 5 architecture across the Zebra Technologies 802.11n and 802.11ac Enterprise WLAN portfolio and provides critical fixes and enhancements for customer reported issues.

1. Platforms Supported

WiNG 5.7.1 supports the following platforms with the corresponding firmware images. Note: Virtual Machine capability is supported on NX 45XX, NX 65XX and NX 95XX controllers only.

Controller Platform	Firmware Image
RFS 4010 / RFS 4011	RFS4000-5.7.1.0.0-019R.img, RFS4000-LEAN-5.7.1.0.0-019R.img
RFS 6000	RFS6000-5.7.1.0.0-019R.img, RFS6000-LEAN-5.7.1.0.0-019R.img
RFS 7000	RFS7000-5.7.1.0.0-019R.img, RFS7000-LEAN-5.7.1.0.0-019R.img
NX 9000	NX9000-5.7.1.0.0-019R.img (image without VM support)
NX 9500/ NX 9510	NX9000-5.7.1.0.0-019R.img (image without VM support)
NX 9500/ NX 9510	NX9500-5.7.1.0.0-019R.img (image with VM support)

Controller Platform	Firmware Image
NX 75XX	NX7500-5.7.1.0.0-019R.img
NX 45XX/ NX 65XX	NX65XX-5.7.1.0.0-019R.img

Virtual Platform	Firmware Image
VX 9000–production iso/img image	VX9000-INSTALL-5.7.1.0.0-019R.iso, VX9000--5.7.1.0.0-019R.img
VX 9000 – demo iso image	VX9000-DEMO-INSTALL-5.7.1.0.0-019R.iso[1]

Note 1: The VX demo image is a 60-day trial image of the VX-9000 software VM that can be used for demos and in the lab environments. This image does not need any additional licenses; it comes with 16 AAP licenses built-in. There is no migration from the demo image to the production image.

WiNG Express Manager	Firmware Image
NX 7510E	NX7500E-5.7.1.0.0-019R.img
VX 9000E	VX9000E-INSTALL-5.7.1.0.0-019R.iso

AP Platforms	Firmware Image
Dependent APs	
AP 621	AP621-5.7.1.0.0-019R.img (included in all Controller images)
AP 622	AP622-5.7.1.0.0-019R (included in all Controller images)
AP 650	AP650-5.7.1.0.0-019R.img (included in all Controller images)
Independent /Adaptive APs	
AP 6511 / AP 6511E	AP6511-5.7.1.0.0-019R.img (included in NX controller images)
AP 6521 / AP 6521E	AP6521-5.7.1.0.0-019R.img (included in all Controller images)
AP 6522 / AP 6522E	AP6522-5.7.1.0.0-019R.img (included in all Controller images)
AP 6532	AP6532-5.7.1.0.0-019R.img (included in all Controller images)
AP 6562 / AP 6562E	AP6562-5.7.1.0.0-019R.img (included in all Controller images)
AP 7131 / AP7161 / AP 7181	AP71XX-5.7.1.0.0-019R.img (included in NX controller images)
AP 7532	AP7532-5.7.1.0.0-019R.img (included in the NX controller images)
AP 7522 / AP 7522E	AP7522-5.7.1.0.0-019R.img (included in the NX controller images)
AP 7562	AP7562-5.7.1.0.0-019R.img (included in the NX controller images)
AP 7502 / AP 7502E	AP7502-5.7.1.0.0-019R.img (included in the NX controller images)
AP 8132 / AP 8122 / AP 8163	AP81XX-5.7.1.0.0-019R.img (included in NX controller images)
AP 8222 / AP 8232	AP82XX-5.7.1.0.0-019R.img (included in NX controller images)
Independent /Adaptive Wall Switch	
ES 6510	AP6511-5.7.1.0.0-019R.img (ES 6510 uses AP 6511 image)

2. New Features in WiNG 5.7.1

WiNG 5.7.1 introduces support for the following new features:

AP 7562

WiNG 5.7.1 introduces support for AP 7562 is WiNG enabled outdoor rugged 802.11ac Mesh Access Point. It provides high performance 802.11ac wireless networks to unlock network capacity particularly in the harshest outdoor environments. The AP-7562 is a Dual

Radio 3x3:3 802.11ac Access Point utilizing one 2.4 GHz 802.11n radio and one 5 GHz 802.11ac radio to give you the power and flexibility to handle today's bandwidth-heavy applications and secure your data — without purchasing and managing an additional layer of equipment. The AP-7562 is optimized with WiNG intelligence, extending QoS, security, and mobility services to the access point to support better capacity and performance.

Following SKUs will be supported for AP 7562:

Model No	Part No	Description
AP 7562	AP-7562-67040-US	802.11ac Outdoor IP67 Dual radio External antennas US
AP 7562	AP-7562- 67040-EU	802.11ac Outdoor IP67 Dual radio External antennas EU
AP 7562	AP-7562-67040-WR	802.11ac Outdoor IP67 Dual radio External antennas WR
AP 7562	AP-7562-67040-APME	802.11ac Outdoor IP67 Dual radio External antennas APME

MCX support for AP 7522, 7532, 7562

WiNG 5.7.1 adds support for MCX feature for AP 7522, 7532 and 7562. WiNG 5.7.1 also adds GUI support for this feature with SWiFT UI.

CRM enhancements

Critical resource monitoring functionality prior to WiNG 5.7.1 utilized ICMP or ARP packets to monitor configured resources causing increased network traffic with increase in the number of devices monitoring. WiNG 5.7.1 enhances CRM functionality to address the scalability issues as below:

1) Use firewall flows instead of using ICMP or ARP packets.
2) Designate one device (rf-domain-manager or cluster-master) to perform CRM and update the rest of the devices with the state changes.

Captive Portal enhancements

- Adds support for mobile friendly captive portal pages.
- Adds ability to redirect the user to an external Success url while hosting the landing page on the AP.
- Adds ability to customize the captive portal page sections for background color and font color.
- Adds following GUI configuration enhancements – this is to simplify the configuration for common use cases.
    a) Email Access
    b) Mobile Access
    c) Other Access (Customizable field, Ex:- Loyalty number)

AP 7502 MSTP support

WiNG 5.7.1 enables MSTP support for AP 7502. MSTP can be configured and supported on all FE and GE ports of AP 7502 in the same way as it's supported on WING 5 controllers.

AP 8163 Scan Ahead

In the ETSI domain this feature enables the third radio to constantly scan ahead for channels that are free and clear of radar interference. In the event the 5 GHz data radio is hit by radar, the channel can then be changed in milliseconds, eliminating any network outage due to radar interference.

In ETSI domain countries that only allow 5 bonded 5Ghz DFS Channels (100-140) to be selected for backhaul, the radios first need to perform a Channel Availability Check (CAC) before operating on it. While this check is performing there is an in-activity period that could range between 1 to 10mins. By Using a Scan-Ahead radio this in-activity period can be avoided.

WiNG 5.5.6 features and fixes fully included in WiNG 5.7.1 release.

3. Firmware Upgrade / Downgrade – Controllers and Dependent APs

3.1 Important Notes on Upgrade / Downgrade

1. Prior to upgrading to WiNG 5.7.1, if you have Onboard-Radius Server with LDAP Authentication configured, please note the following:

   "(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})" – is not supported.

   “(sAMAccountName=%{Stripped-User-Name})" – is supported.

   Configurations using "(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})" need to be updated to “(sAMAccountName=%{Stripped-User-Name})" prior to performing the upgrade process.

2. When downgrading from WiNG 5.7.x to WiNG 5.5.5 or WiNG 5.5.4 on AP 7532/7522, the user needs to apply patch **AP75XX-CPU-Bringup-1.0.patch**.
   AP7532/AP7522 running wing 5.5.6/5.7.x has an updated kernel version and the patch is required when the AP downgrades to a firmware with a prior kernel version.
   Steps to apply the patch:
   - Load the kernel patch for AP7522 and AP7532 device models on controller using device-upgrade load-image option:
     - “device-upgrade load-image ap7522 tftp://<server ip address >/AP75XX-CPU-Bringup-1.0.patch”
   - Execute “device-upgrade all force no-reboot” from the controller to upgrade the APs with the patch.
   - Use “boot system primary” or “boot system secondary" based on the WiNG 5.5.5/5.5.4 image location on the APs and reload the APs from the controller.

3. AP 300 support has been removed with WiNG 5.7.x release.
4. The “Lean Controller image” introduced with ONEVIEW in WiNG 5.5, does not include AP images.
5. Upgrading WiNG v4.x networks to WiNG v5.7 will not retain the 4.x configuration. Please use the configuration migration utility to convert a 4.x configuration to a 5.7 based configuration. This is an offline tool that assists with config migration.
6. When downgrading from WiNG 5.7.x to a version prior to WING 5.4.x through rf-domain, the user needs to downgrade without reloading APs and then do a manual reload on the rf-domain. The following are the CLI commands for this procedure:
   device-upgrade rf-domain <RF domain name> all no-reboot … this downgrades all APs (including the RF domain manager) without rebooting them
   reload on <RF domain name> … this reboots the entire RF domain.
   Staggered reboot option is not supported in this downgrade scenario.

7. AP 622 v5.2.3.0-008R must be first upgraded to v5.2.3.0-040R before it can be upgraded to v.5.7.x.
8. Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP or controller. Please allow time for devices to complete the upgrade. Where APs are powered through PoE connections to WLAN controllers, the controller needs to stay up during the upgrade process.
9. Both the controller and the AP should be upgraded to the same versions – a firmware mismatch can cause network disruptions and should be avoided. When upgrading, the controllers should be upgraded first and then the APs. When downgrading, the APs should be downgraded first, and then the controller.
10. Upgrade for AP 650 from WiNG 4.x to WiNG 5.4.x or later is NOT seamless and requires additional steps. AP should first be updated to any WiNG 5.2.x or 5.3.x image.
    Please set in the controller profile "service wireless ap650 legacy-auto-update-image <PATH:/ap.img> to point to WiNG 5.2.x or WiNG 5.3.x AP 650/6532 image.
    For example:
    1. Copy AP 650/6532 5.2 image on the RFS flash

    rfs4000-22A1B8#copy tftp://<Server IP>/AP6532-5.2.0.0-069R.img flash:/AP6532-5.2.0.0-069R.img
    2. User the below command to first upgrade the AP650s to a 5.2 image

    rfs4000-22A1B8#configure terminal
    Enter configuration commands, one per line. End with CNTL/Z.
    rfs4000-22A1B8(config)#self
    rfs4000-22A1B8(config-device-XXX)#service wireless ap650 legacy-auto-update-image flash:/AP6532-5.2.0.0-069R.img
    3. If auto upgrade is enabled AP650 will get upgraded to 5.4.x once it adopts to the controller, else use the below command to upgrade the AP650 to 5.4.x or later

    rfs4000-22A1B8#device-upgrade ap650 <DEVICE> .
11. In Virtual Controller deployments, APs running version 5.4.x will not adopt to a virtual controller running WiNG v5.7.x. First upgrade APs to WiNG v5.7.x (manually) and then upgrade the Virtual Controller. New APs need to be upgraded to 5.5.x manually before connecting to a WiNG 5.7.x Virtual Controller network.
12. Downgrade to WiNG 4 is not recommended in countries following ETSI regulations as WiNG 4 is not compliant with current ETSI DFS regulations.

3.2 Upgrade/Downgrade Matrix

This section documents allowed upgrade/ downgrade combinations. Please ensure that the controller and AP are on the same WiNG version after the upgrade is complete.

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
RFS + AP 650	v4.3.x onwards on the controller	v4.3.x onwards on the controller	AP 650 image is contained within the controller image
RFS + AP 7131/AP 7131N	v4.1.1 onwards on the AP v4.3.x onwards on the controller	v4.1.1 onwards on the AP v4.3.x onwards on the controller	AP 7131/AP 7131N v5.x image is not within the controller image

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
RFS + AP 6532	v5.1 onwards	v5.1 onwards	AP 6532 image is contained within the controller image
RFS + AP 6511	v5.1 onwards	v5.1 onwards	AP 6511 image is not contained within the controller image
RFS + ES 6510	v5.4 and higher	v5.4 and higher	ES 6510 uses the same image file as the AP 6511. The image is not contained within the controller image
RFS 4011 with AP 650	v5.1 onwards	v5.1 onwards	
RFS/NX 9XXX + AP 7181 Controllers need to be on 5.4 to be able to adopt AP 7181.	v5.4 onwards	v5.4 onwards	Controller assistance is not available for upgrade from 3.2.2 to 5.4. This can be performed standalone or with Wireless Manager.
RFS/NX 9XXX + AP 7161	v5.1.1, v5.1.4, v5.2 onwards	v5.1.1, v5.1.4, v5.2 onwards	
RFS/NX 9XXX + AP 6521/AP 621	v5.2 onwards	v5.2 onwards	AP 6521 image is contained within the controller image
RFS/NX 9XXX + AP 6522	v5.4 onwards	v5.4 onwards	AP 6522 image is contained within the controller image
RFS/NX 9XXX + AP 6562	v5.4.4 onwards	v5.4.4 onwards	AP 6562 image is contained within the controller image
RFS/NX 9XXX + AP 622	v5.2.3, v5.2.13 or 5.4 and higher.	v5.2.3, v5.2.13 or 5.4 and higher.	AP 622 image is contained within the controller image. WiNG 5.3.x does not support AP 622
NX 45XX/NX 65XX + AP 7131, AP 6532, AP 650, AP 6511, AP 6521, AP 621	v5.2.4, 5.4.2 and higher	v5.2.4	AP images are contained within the controller image
NX 45XX/NX 65XX + AP 7181, AP 7161, AP 6522, AP 622, AP 6562, AP 8132	v5.4.4 and higher	v5.4.4	AP images are contained within the controller image

Dependent/Adaptive with the RFS controller	Upgrade from	Downgrade to	Notes
RFS/ NX + AP 8132	v5.2.6, 5.4.2 and higher	v5.2.6, 5.4.2 and higher	AP 8132 image is not within the RFS controller image, but is contained within NX controller image
RFS/ NX + AP 82XX	v5.5.3 and higher	v5.5.3 and higher	AP 82XX image is not within the RFS controller image, but is contained within NX controller image
RFS/ NX + AP 8122	v5.5.2 and higher	v5.5.2 and higher	AP 8122 image is not within the RFS controller image, but is contained within NX controller image
NX7500	v5.5.2 and higher	v5.5.2 and higher	Note: WiNG 5.6 doesn't support NX 7500.
RFS/NX + AP 7532/AP 7522	v5.5.3.1 and higher, excluding v5.6.x	v5.5.3.1 and higher, excluding v5.6.x	AP image is contained within the NX controller image in v5.5.4
RFS/NX + AP 7562	v5.7.1 and higher	v5.7.1 and higher	AP image is contained within the NX controller image in v5.7.1
RFS/NX + AP 7502	v5.5.4.1 and higher, excluding v5.6.x	v5.5.4.1 and higher, excluding v5.6.x	AP image is contained within the NX controller image in v5.5.5
RFS/ NX + AP 8163	v5.6 and higher	v5.6 and higher	AP 8163 images are not within the controller image
VX + all supported APs	v5.6 and higher	v5.6 and higher	
NX 7510E/VX 9000E + AP 6511E / AP 6521E / AP 6522E / AP 6562E / AP 7502E / AP 7522E	v5.5.3 and higher	-	NX 7510E and VX 9000E are supported starting with v5.7

3.3 Upgrade/Downgrade Procedure for WLAN Controllers

Customers upgrading from an earlier WiNG 5 release not requiring ONEVIEW, the procedure is the same as before.

Customers using ONEVIEW in WiNG 5.5, please see the WiNG 5.5 training for details of upgrade/ downgrade***. Note in particular the use of the "Lean Controller image" which does not include AP image***s – since the controller image size is now significantly larger than WiNG 5.4.x release.

The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

IMPORTANT: Always create config back-up before upgrade.

3.3.1 Upgrade from WiNG v5.x to WiNG v5.7.x

1. Copy the RFSX000-5.7.X.X-0XXR.img or NXXX00-5.7.X.X-0XXR.img to your tftp/ftp server.

2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the controller. From CLI the command is —reload.

3.3.2 Upgrade from WiNG v4.3.x (or higher) to WiNG v5.7.X

1. Copy the RFSX000-5.7.X.X-0XXR.img to your tftp/ftp server.

2. Use the —**upgrade ftp://<ip address of server>/<name of file>** command from CLI or **Switch->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the controller. From CLI the command is —reload.

Note: *Please use ftp to upgrade to WiNG v5.5.x on an RFS 6000, and not tftp, if using GE1.*

3.3.3 Downgrade to a WiNG v4.3.X (or higher) from WiNG v5.7.X

1. Copy the RFSX000-4.3.X.X-XXXR.img to your tftp/ftp server.

2. Use the —**upgrade ftp://<ip address of server>/<name of file>** command from CLI or **Operations>Device Detail>Load Firmware** option from the GUI. You may need to specify the username and password for your ftp server.

3. Restart the Controller. From CLI the command is —reload.

Please note: due to hardware refresh changes on controllers RFS7000, RFS6000 and RFS40XX, downgrade/upgrade to version that doesn't support new hardware components will be prevented. Following currently released version don't support new hardware: v5.0.x, v5.1.x. v5.2.0, v5.2.1, v5.2.2, v5.2.11, v5.2.3, v5.3.0, all versions prior to v4.4.1.
Configuration Restoration
On upgrade from 4.x to 5.x the 5.x controller will save the configuration from 4.x in another file on flash (so that 'startup-config' will point to the 5.x default startup-config). The configuration file from 4.x is renamed to startup-config-wing4. The password encryption file is also moved to /etc2/encrypt-passwd-wing4.

On downgrade from 5.x to 4.x the controller will save the 5.x configuration and it is moved to hidden files of the same name (/etc2/.encrypt-passwd-wing5 and /etc2/nvram/.startup-config-wing5). Any previously saved wing4 config if present (ie. startup-config-wing4) is restored back.

3.4 Upgrade/Downgrade Procedure for dependent APs connected to RFS controllers

3.4.1 AP 650 upgrade

Note: If upgrading from any of the following releases 4.x, 5.0.x, 5.1.x, 5.2.0.x, 5.2.1.x, 5.2.3.x, 5.2.4.x, 5.2.6.x, 5.2.11.x, 5.2.12.x, 5.2.21.x or 5.3.x, you need to upgrade to 5.2.13 or 5.4.x before upgrading to 5.7

A WiNG 5.x controller can upgrade an AP 650 running 4.x code to 5.x using the WISPe upgrade. This capability is enabled using "legacy-auto-update" command for the controller, either under the device or profile. The controller will first adopt the access point using the standard WISPE protocol messages (just as a 4.x controller would adopt it) and then download the new image to it, which would convert the AP to WiNG 5.x version of code.
Legacy-auto-update is enabled by default. If legacy-auto-update is disabled, use the following CLI instructions to enable the Legacy-auto-update feature:

rfs4000-22A136#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
rfs4000-22A136(config)#profile rfs4000 default-rfs4000
rfs4000-22A136(config-profile-default-rfs4000)#legacy-auto-update
rfs4000-22A136(config-profile-default-rfs4000)#commit
rfs4000-22A136(config-profile-default-rfs4000)#

Important: In WiNG 5.4.x – please enable FTP server on the controller for legacy-auto-update to work.
The AP 650 can be automatically downgraded to a 4.x version of the AP by connecting it to a controller running the version 4.x. The AP tries to discover both 4.x as well as 5.x controllers by default, and if it does not find a 5.x controller, but does find a 4.x controller, then it will adopt to it, and as part of the adoption the 4.x controller will download a 4.x image to it.
Important: See also Section 4.1 Important Note #7

3.4.2 AP 7131 upgrade from AP 4.x

For AP 7131's running 4.x firmware the released 5.x firmware (AP71XX-5.7.X.X-0XXR.img) should not be used to upgrade the AP to 5.x. Instead for every 5.x release, there is a corresponding migration image to 5.x (AP7131-5.7.0.0-0XXR.bin).

3.5 Device upgrade options

WiNG 5.x supports device firmware upgrade from the controller. For firmware upgrade through controller, firmware image needs to be loaded onto a controller and the same can be used for the upgrade of all the corresponding devices.
Available firmware on the controller can be checked using the below command:
nx9500-6C8647#show device-upgrade versions

If device firmware is not part of controller image, a new image can be uploaded using following command:

nx9500-6C8647# device-upgrade load-image

Once device firmware is loaded on the controller, below are the different options that are available for device firmware upgrade:

- **Manual Upgrade**

Firmware upgrade can be initiated on a single or a list of Aps using the below command.

nx9500-6C8647# device-upgrade ap71xx-16C7B4 ?

```
 no-reboot       No reboot (manually reboot after the upgrade)
 reboot-time     Schedule a reboot time
 upgrade-time    Schedule an upgrade time
```

nx9500-6C8647# device-upgrade ap71xx all ?

```
 force           Force upgrade on all devices
 no-reboot       No reboot (manually reboot after the upgrade)
 reboot-time     Schedule a reboot time
 staggered-reboot  Reboot one at a time without network being hit
 upgrade-time    Schedule an upgrade time
```

- **Scheduling Firmware upgrade**

Firmware upgrade can be scheduled on a controller, that is upgrade time and reboot time can be configured. Firmware upgrade on the Aps follows the configured upgrade time.

nx9500-6C8647# device-upgrade all ?

```
 no-reboot     No reboot (manually reboot after the upgrade)
 reboot-time   Schedule a reboot time
 staggered-reboot  Reboot one at a time without network being hit
 upgrade-time  Schedule an upgrade time
```

- **Upgrade through RF Domain manager**

Manual Firmware upgrade can be initiated through a domain manager

nx9500-6C8647# #device-upgrade rf-domain ?

```
 DOMAIN-NAME  RF-Domain name
 all          Upgrade all RF Domains
 containing   Specify domains that contain a sub-string in the domain name
 filter       Specify additional selection filter
```

3.6 Auto Upgrade

Auto firmware upgrade can be enabled on the controller using the below command. When enabled, any AP with a firmware version different than the controller will be upgraded to the controller's version on adoption.

rfs4000-22A1B8(config-device-XXX)# device-upgrade auto

The number of concurrent firmware upgrades can be configured using the below command based on the bandwidth available between the controller and the Aps.

rfs4000-22A1B8(config-device-XXX)# device-upgrade count ?

```
 <1-20>  Number of concurrent AP upgrades
```

Note: Auto upgrade on the APs always happens through the controller.

3.7 AutoInstall

AutoInstall in v5.4.x and later works via the DHCP server. This requires the definition of Vendor Class and three sub-options that can be either sent seperately, or under option 43:

Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to enter as a string: —ftp://admin:admin123@192.168.1.10)

Option 187 - defines the firmware path and file name

Option 188 - defines the config path and file name

Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable "ip dhcp client request options all" on the vlan interface which is being used to perform the above autoinstall.
DHCP vendor class for platforms is noted below:

- WingRFS.RFS4000
- WingRFS.RFS6000
- WingRFS.RFS7000
- WingNX.NX4500
- WingNX.NX4524
- WingNX.NX6500
- WingNX.NX6524
- WingNX.NX7500
- WingNX.NX9000
- WingNX.VX

3.8 Virtual Machine Installation on NX 95xx

The ADSP VM can be installed on NX 95XX Integrated Services Controllers; it does not come pre-installed with WiNG 5.7.
The procedure to upgrade the VMs on these controllers is similar to the example below, except that it will always require first uninstalling the pre-installed VM.

Note: *The VM upgrade will not impact the currently installed/running VM. However, the "uninstall" will cause the VM's configuration and database entries to be wiped out. Please be sure to export and save the configuration and database prior to uninstalling.*

If the NX 95xx is running an image without VM support, first upgrade to the NX 95xx image with VM support.

Note: When upgrading from WiNG 5.6/WiNG 5.5.4 or earlier versions to WiNG 5.7.x with ADSP VM installed - due to ADSP MAC fix and memory fix, you first you need uninstall ADSP VM, upgrade and then install again on WiNG 5.7.x. There is no issue when upgrading from WiNG 5.5.5/WiNG 5.6.1 to WiNG 5.7.x with ADSP VM installed.

The following outlines the steps to install ADSP VM image on NX95XX integrated series controllers:

1. Download the ADSP image and place it onto an FTP/TFTP server or USB key
2. Set WiNG memory to allow for VM image:
   virtual-machine set wing-memory 16384
3. Reload the controller
4. Using the ***upgrade*** CLI command or ***Firmware Upgrade*** option in the Web-UI, download the ADSP image onto the NX 95XX. Note if using the CLI it is recommended that you transfer the ADSP image to the NX 95XX using the background option! This will install the image in the /vmarchive partition.
5. Using the CLI ("virtual machine install") or App Center Install ADSP. The installation will take approximately 20 minutes to complete. Once installed the ADSP Virtual Machine will automatically start!

To upgrade a VM (instead of a first time install), you need to uninstall the currently installed VM and then install the new one. i.e. replace step (3) above with

NX9500#virtual-machine uninstall adsp # Uninstalls the ADSP-VM
NX9500#virtual-machine install adsp # Installs the new ADSP-VM

4. Firmware Upgrade/Downgrade – Independent APs

4.1 Important Notes on Upgrade / Downgrade

1. When downgrading from WiNG 5.7.x to WiNG 5.5.5 or WiNG 5.5.4 on AP 7532/7522, the user needs to apply kernel patch **AP75XX-CPU-Bringup-1.0.patch**.
   AP7532/AP7522 running wing 5.5.6/5.7.x has an updated kernel version and the patch is required when the AP downgrades to a firmware with a prior kernel version.
   Steps to apply the patch:
   - Copy AP75XX-CPU-Bringup-1.0.patch to your tftp server.
   - Apply the patch using upgrade command:
     - "upgrade tftp://<server ip address >/AP75XX-CPU-Bringup-1.0.patch"
   - Use "boot system primary" or "boot system secondary" based on the WiNG 5.5.5/5.5.4 image location on the AP and reload.

2. AP 8XXX new NAND:
   WiNG 5.5.2 added support for hardware refresh NAND component on AP 81XX and AP 82XX. Following restrictions will apply when using those APs with new hardware component:
   - New revision of hardware - downgrade/upgrade will only be supported to releases that also support those components. Downgrade/upgrade to all other releases will be prevented.
   - Older revision of hardware - downgrade/upgrade procedure is unchanged.
3. Upon upgrade to v5.5.3 or above – AP 6511, AP 6521, AP 6522, AP 6562 will have a new web UI.
4. When downgrading from WiNG 5.5.x to a lower WiNG 5.x version through rf-domain, the user needs to downgrade without reloading APs and then do a manual reload on the rf-domain. The following are the CLI commands for this procedure:
   device-upgrade rf-domain <RF domain name> all no-reboot … this downgrades all APs (including the RF domain manager) without rebooting them
   reload on <RF domain name> … this reboots the entire RF domain.
   Staggered reboot option is not supported in this downgrade scenario.
5. Firmware upgrades can take several minutes; aborting an update by removing power may damage the AP. Please allow time for devices to complete the upgrade.
6. Upgrade for AP 6532 from release prior to v5.2.13 directly to v5.4.x or later is NOT seamless and requires additional steps. AP should first be updated to any WiNG 5.2.13 image.
7. Downgrade to WiNG 4 is not recommended in countries following ETSI regulations as WiNG 4 is not compliant with current ETSI DFS regulations.

4.2 Upgrade/Downgrade Matrix

This section documents allowed upgrade/ downgrade combinations.

Independent/Adaptive Access Point	Upgrade from	Downgrade to	Notes
AP 6511	v5.1 onwards	v5.1 onwards	
ES 6510	v5.4 onwards	v5.4 onwards	
AP 6521	v5.2.x onwards	v5.2.x onwards	
AP 6522	v5.4 onwards	v5.4 onwards	
AP 6532	v5.1 onwards	v5.1 onwards	See Note 2
AP 6562	v5.4.4 onwards	v5.4.4 onwards	
AP 7131	v4.1.1 onwards	v4.1.1 onwards	

Independent/Adaptive Access Point	Upgrade from	Downgrade to	Notes
AP 7161	v5.1.1 (adaptive) v5.1.4 (adaptive) v5.2 onwards	v5.1.1 (adaptive) v5.1.4 (adaptive) v5.2 onwards	
AP 7181	v5.4 onwards	v5.4 onwards	See Note 1.
AP 7502	v5.5.5 onwards	v5.5.5 onwards	No support in v5.6.x
AP 7532/ AP 7522	v5.5.3.1 onwards	v5.5.3.1 onwards	No support in v5.6.x
AP 7562	v5.7.1 onwards	v5.7.1 onwards	
AP 8132	v5.2.6, 5.4.2 onwards	v5.2.6	
AP 8122	v5.5.2 onwards	v5.5.2 onwards	
AP 8222/AP 8232	v5.5.3 onwards	v5.5.3 onwards	
AP 8163	v5.6 onwards	v5.6 onwards	
AP 6511E / AP 6521E / AP 6522E / AP 6562E / AP 7502E / AP 7522E	V5.5.3 onwards	V5.5.3 onwards	

Note:

1. AP 7181 - WLAN Controller assistance is not available for upgrade from 3.2.3 to 5.4.x. This upgrade can be performed standalone or with Wireless Manager. The migration process will convert the necessary settings/configuration to maintain mesh connectivity. Please refer to section 4.3.3.
2. Note: If upgrading from any of the following releases 5.0.x, 5.1.x, 5.2.0.x, 5.2.1.x, 5.2.3.x, 5.2.4.x, 5.2.6.x, 5.2.11.x, 5.2.12.x, 5.2.21.x or 5.3.x, you need to upgrade to 5.2.13 or 5.4.x before upgrading to 5.5.x.

4.3 AP Upgrade/Downgrade Procedure

The method described in this section uses the Command Line Interface (CLI) procedures. To log into the CLI, either SSH, Telnet or serial access can be used.

4.3.1 Upgrade from WiNG v5.1.x or higher to WiNG v5.7.X

1. Copy the APXXXX-5.7.X.X-0XXR.img to your tftp/ftp server.
2. Use the —**upgrade ftp://<username>:<password>@<ip address of server>/<name of file>**, or —**upgrade tftp://<ip address of server>/<name of file>** command from CLI or **AccessPoint->Firmware->Update Firmware** option from the GUI. You may need to specify the username and password for your ftp server.
3. Restart the Access Point. From CLI the command is —reload.

Note: WiNG 5.1.3 added support for the new NAND for AP 7131N. WiNG 5.1.4 added support for the new NAND for AP 7161. Hardware revs with the new NAND will be unable to downgrade below these versions or version 4.1.5 – as these support the new NAND, but previous versions do not.

Note: WiNG 5.5.2 added support for new NAND for AP 8XXX platforms. Downgrade to prior releases on hardware with new NAND will be prevented.

4.3.2 Upgrade/Downgrade for AP 7131/AP 7131N from WiNG v4.x to WiNG v5.x

Upgrade from WiNG v4.x to WiNG v5.x

If an AP 7131 has a firmware release version 3.2.0 or earlier, it is mandatory to upgrade the access point to release version 3.2.1.0 before an upgrade to release version 4.x or later can be attempted. Users on AP 7131 release version 3.2.2 need not downgrade to version 3.2.1 and can directly upgrade to a release version 4.x or later.
Users are strongly cautioned against upgrading from the AP 7131 System Boot OS prompt. Upgrading from the Boot OS prompt is not a recommended and supported upgrade methodology on the AP 7131.

To conduct a firmware update on the AP 7131 from the run-time system software from GUI:

1. Select 'System Configuration', 'Firmware Update' from the AP 7131 menu tree of the GUI.
2. Specify the name of the target firmware file within the 'Filename' field.
3. If the target firmware file resides within a directory, specify a complete path for the file within the 'Filepath (optional)' field.
4. Enter an IP address for the FTP or TFTP server used for the update.
5. Select either the FTP or TFTP button to define whether the firmware file resides on a FTP or TFTP server.
6. Set the following FTP parameters if applicable:
    a. *Username* - Specify a username for the FTP server login.
    b. *Password* - Specify a password for FTP server login.
7. Click 'Apply'.

Click the 'Perform Update' button to initiate the update. Upon confirming the firmware update, the AP reboots and completes the update. This step may take several minutes. After this upgrade the access point will reload and come up with wing 5.x firmware.

Note: *Please use the special "migration image" (**AP7131-5.7.X.X-0XXR.bin**) when upgrading from 4.x to 5.x.*

If the user upgrades an AP 7131/AP 7131N running a version of code older than 4.1.1.0 using the AP migration image, there is a possibility of the AP getting "stuck" on coming up with 5.x. If this occurs, the following error message is seen on the console after bootup:
cpu not running at correct speed. Expected(500Mhz) current> Speed(600MHz)
To work-around this issue, the administrators need to type the following command after the error message: 'achip fix-cpu-speed'
When the AP comes up to runtime, upgrade again using the 'upgrade' command to the latest 5.3 release.

Downgrading from WiNG v5.x to AP v4.x for AP 7131/AP 7131N

To downgrade an access point running 5.x back to 4.x the reverse migration image (AP7131-5.7.0.0-0XXR-040402000004R.img) needs to be used. This image is installed on the AP just as a regular 5.x firmware is installed using ap-upgrade/ device-upgrade from CLI or UI. Please refer to the AP 7131 v4.1.5 release notes for downgrade to an earlier version.

Downgrade the access points using the AP-upgrade/device-upgrade command from CLI of the AP and put all APs back to 4.x. All configurations from 5.x is lost as the AP is reverted to 4.x. However the original 4.x configuration, if any, could still be present on the AP.

Configuration Restore

Some of the configuration items from a 4.X AP 7131 are translated and migrated over to the 5.x version of the configuration after update. The items of configuration that are migrated are:

- Hostname
- Port phy configuration (speed, duplex)
- Port L2 configuration (trunking info)
- IP address of controller if available (translated to 'controller host' in 5.x)
- WAN interface IP addressing
- LAN interface /subnet1 IP address

If the configuration could not be read properly then the AP will come up with default 5.x configuration and create a logfile called legacyapn_<version>.dump.tar.gz in flash:/crashinfo indicating what was translated, what was the error etc, for post-analysis.

4.3.3 Upgrade/Downgrade for AP 7181 from v3.2.3 to WiNG v5.7.x

To upgrade an AP 7181 from v 3.2.3 to v 5.7.x, it must first be upgraded to v 5.4.x.
Likewise for downgrading AP 7181's from v5.7.x, it must be downgraded to 5.4.x before downgrading to 3.2.3.
Please see the WiNG 5.4 release notes and "WiNG 5.4 How-To Guide AP7181 Migration" on support central for the procedure.

4.4 AutoInstall

AutoInstall in v5.7 works via DHCP. This requires the definition of Vendor Class and three sub-options that can be either sent separately, or under option 43:

Option 186 - defines the tftp/ftp server and ftp username, password information (IP address and protocol need to be entered as a string: —ftp://admin:admin123@192.168.1.10)
Option 187 - defines the firmware path and file name
Option 188 - defines the config path and file name
Autoinstall of firmware and autoinstall of configuration can be enabled or disabled. Ensure to enable "ip dhcp client request options all" on the vlan interface which is being used to perform the above autoinstall.
DHCP vendor class for platforms is noted below:

- WingAP.AP6511
- WingAP.AP6521
- WingAP.AP6522
- WingAP.AP6562
- WingAP.AP6532
- WingAP.AP7131
- WingAP.AP7161
- WingAP.AP7181
- WingAP.AP7502
- WingAP.AP7522
- WingAP.AP7532
- WingAP.AP7562
- WingAP.AP8122
- WingAP.AP8132
- WingAP.AP8222
- WingAP.AP8232
- WingAP.AP8163

6. Important Notes

New in v5.7.1

1. AP 622, 6522, 6562 - Default value for radio lna control on 2.4GHz has been changed to improve receive sensitivity and range in low/medium AP density environments.

2. DHCP Vendor Class Identifier has been changed use "Wing" instead of Motorola (5.7)/Zebra (5.5.6) to be consistent with rest of re-branding changes, e.g. WingAP.AP7532, WingAP8132, WingRFS.RFS4000 and etc.

3. Captive Portal internal web-page templates are enhanced for mobile friendly rendering. Existing WiNG5.x deployments using internally hosted web-pages for captive portal will automatically get this functionality on upgrading to WiNG5.7.1. Please note that there will be slight changes to pages – page style, background color, font color etc.

4. AP 7562 sensor functionality will be supported in later ADSP release.

New in v5.7

1. The AP 6521 will include support for configuration and management of the on-board AAA server in the HTTP User Interface. This UI is found on the standard WiNG OS for the AP 6521, and the AP 6521 Express. Please note that the Virtual Controller function will be disabled when the on-board AAA server is enabled on a standalone AP 6521. To use the Virtual Controller function, you must disable the on-board AAA server.

2. Web Filtering : URLs in custom category will get priority over standard/predefined category irrespective of precedence configured

3. Web Filtering is not supported on the NX65xx/NX45xx platforms

4. Wired captive portal – to support clients with MAC authentication, 802.1x configuration is also required on the controller

5. OpenDNS
   - the dhcp server/pool policy configuration is required to include the OpenDNS IP (*208.67.220.220, 208.67.222.222* **)** as the dns-server
   - The ip access-list is required to include the following firewall rules to prevent clients from using any unauthorized DNS server
     permit udp any host 208.67.222.222 eq dns rule-precedence 1 rule-description "allow dns queries only to OpenDNS"
     deny udp any any eq dns rule-precedence 10 rule-description "block all other dns queries"

6. VX 9000 – MAC address of the device should not be changed once installed/configured.

7. WiNG Express Manager

   a. Express Manager (NX 7510E) can be accessed using default IP 192.168.0.1 and 'admin' is the supported user role.
   b. Smart-RF is enabled by default with channel override capabilities on individual APs. Any Smart-RF channel list change will take effect after the device reboot.
   c. RADIUS services will not be supported on AP 6511 and AP 6521.

d. DHCP service should be started at the site-level and APs have to adopted to the Express Manager before starting the DHCP service.
e. VLAN 1 and 2200 are reserved VLANs – they are not available for user configuration
f. GUI will be supported on the following browsers/version
    i. IE10 and above
    ii. Chrome
    iii. Firefox
g. Country code should be configured at the site-level for the AP radios to function.
h. Auto-provisioning policy must be created before adopting APs to a site. Express Manager needs to be reloaded for any changes to the auto-provisioning policy to take effect.
i. Event history page may experience slow to refresh when the event table size is large
j. Default profile configuration (inherited from the system) can be modified at the site-level, however needs manual reconfiguration to revert to defaults
k. Disable DFS checkbox under Advanced Smart-RF tab removes DFS channels from the available channel list
l. Floor maps should be loaded independently on the standby in a cluster scenario
m. Firmware upgrade for the Express Manager should be administered through the System basic configuration screen. Upgrading through the devices screen is not supported.
n. Access to the NX 7510E USB port is not available from the Express Manager UI
o. There is no periodic auto-refresh for the UI charts, tables and map. Needs manual page refresh using refresh button.
p. Site icon can be removed from the Dashboard map only after the corresponding site profile has been deleted from the system.
q. AP upgrade status is shown on the Active Express Manager while the upgrade is initiated from the Standby in a cluster setup
r. Site connectivity to the Express Manager needs to be active for the mac-registration feature to function.
s. For infinite lease option on the dhcp pool configuration, the user needs to set “0” for the day, hours and minutes.

8. ETSI 1.7.1 Adaptivity Limitation on AP 622, AP 6522, AP 6562
   This note applies to the following APs that end with “-EU”. These APs are sold to countries that comply with the EU directives - AP 622, AP 6522, and AP 6562. This does not apply to APs that end in “-US” or “-WR”
   - Radio 1 will support operation as a 2.4Ghz data radio compliant with ETSI 1.7.1 adaptivity directive
   - Radio 2 cannot be enabled for operation as a 2.4Ghz data radio. Radio 2 will support operation as a 5Ghz data radio only
     - If using Radio 2 in 2.4Ghz, please enable Radio 1 for data access in 2.4Ghz
   - When Radio 2 is configured as a dual-band security sensor with an ADSP appliance;
     - Radio 2 will not support Air Termination, AP Test, and Network Assurance at 2.4Ghz band
     - Radio 2 will support receive packet and forensic security analysis at 2.4Ghz band
     - Radio 2 will support Air Termination, AP Test, Network Assurance and all packet receive functions on the 5Ghz band

9. The following defaults and CLI commands / help-strings have been changed as part of the de-branding :

	WiNG 5.7.x	Older versions
Default username / password	admin / admin123	admin / motorola
Default DNS name	“WiNG-wlc”	“Motorola-wlc”
Default WLAN name	“WLAN-1”	“Motorola”
CLI command	“wing-extensions”	“motorola-extensions”
	“wing-ie”	“symbol-ie”
CLI help string	WiNG	Motorola or Symbol
802.1x default username / password	admin / admin123	admin / motorola

10. AP 6522/6532/6562/71xx - VRRP and OSPF feature support have been removed

New in v5.6.x

1. AP 6511 – Firewall is disabled by default starting with WiNG 5.6 in order to meet the requirements for WiFi certification. Some features such as Captive Portal require firewall to be enabled.

2. IPV6 ACLs do not support the object oriented firewall feature in this release.
3. IPv6 implementation does not support IPsec VPNs in this release.

4. IPv6 – MLD snooping is not supported on the ethernet switch ports on the NX 4524 and NX 6524 platforms. It is supported only on UP1, UP2 ports.

5. IPv6 – When there are multiple DHCP servers (one for IPv4 and another for IPv6) that respond to option 191, ensure that both provide valid IP addresses/ hostnames. Otherwise, with both servers responding the later response will override the previous response. If the later response does not contain valid information, AP will not be able to adopt to the controller.

6. VX 9000 - Only 1 GE1 interface is supported on the VX platform

7. VX 9000 instances running in Amazon EC2 must use "Elastic IP" to retain the public IP when the instance is stopped and restarted.

8. VX 9000 - VMWare and other hypervisors need to be configured in promiscuous mode for features like VRRP to work correctly.

9. When creating a cluster between multiple VX 9000’s, all instances should use identical resources (e.g. replication from one instance with higher memory to a smaller one can lead the smaller instance to run out of memory).

10. VX 9000 – Ipv6 is not supported when using Microsoft HyperV as the virtualization platform. Dataplane support does not work correctly with Microsoft HyperV. It works fine with other supported hypervisors.

11. Captive Portal Time Based Voucher is only supported with Active: Standby configurations. Active: Active based clusters are not supported. The database gets replicated from the Active Controller to the Standby Controller periodically (default is 5 min).

12. eBGP Scaling by platform is as follows:
    a. RFS 4000/RFS 6000 – 6000 routes

b. NX 9510 – 9000 routes
c. NX 4500/NX 6500 – 12 routes

13. T5 adoption – https must be enabled on the WiNG controller for T5 adoption to work

14. Wired Captive Portal
    a. If wired captive portal is being used along with wireless captive portal on the same controller, then same captive portal policy needs to be used for both wired and wireless captive portal enforcement.
    b. If Wired captive portal is being implemented for a particular bridged vlan on the controller's physical interface that receives APs traffic, then applying wireless captive portal for the same bridge vlan is not valid, since the wireless client will then be subjected to captive portal enforcement twice.

15. The following default values have been changed/ corrected:
    a. *route-limit num-routes 12288 retry-count 5 retry-timeout 60 reset-time 1| route -limit num-routes 12288 retry-count 5 retry-timeout 60 reset-time 3* ….. reset time was changed from 1 to 3.
    b. vrrp-state-check command previously present in "router ospf" context, has been moved to device/profile context
    c. min-misconfiguration-recovery-time 120 …. Was increased from 60 to 120.

New in v5.5.6

1. Currently, for all events, forward-to-switch is on by default. Due to this setting a controller adopting many APs gets too many events sometimes. So for certain events, forward-to-switch setting will be off by default. This will apply whether event-system-policy is used on not. The events being changed are:
"dot11 client-associated", "dot11 client-disassociated", and "dot11 client-info".

2. **Vulnerability updates in WiNG 5.5.6:**
NTP v4.2.8p1 that addresses the following security vulnerabilities outlined in CVE-2014-9297, CVE-2014-9298, CVE-2014-9295, CVE-2014-9295, CVE-2014-9295, CVE-2014-9296 .
CVE-2015-0235 - GHOST Linux Vulnerability.
CVE-2014-4877 - wget updated to v1.16.

3. Flow control on AP 6511 has been disabled to prevent transmission and receive of pause packets.

4. AP discovery tool will work on windows 7 laptop only with static IP.

New in v5.5.5

1. When upgrading to WiNG 5.5.5 – AP statistics will not be available on the controller until APs have also been upgraded to WiNG 5.5.5.

2. CPLD images on AP 7131/7161/7181 have been updated. AP 7131N CPLD image is without change.

3. When upgrading to WiNG 5.5.5 with ADSP VM installed - due to ADSP MAC address fix for SPR 26107 and memory fix, you first you need uninstall ADSP VM, upgrade and then install again on WiNG 5.5.5.

4. "No service" page for captive portal enhancements:
   WiNG 5.5 has introduced support for "no service" page support. However - the failure page was ONLY displayed if the Access Point (or Wireless Client) can reach a DNS server. WiNG 5.5.5 addresses the issue with DNS reachability and provides option to configure "service monitor dns crm <crm-name> vlan <failover-vlan>". This service command will monitor DNS server reachability. When DNS server is not reachable, the clients are moved to failover-vlan. In the failover-vlan every time DNS request comes from captive portal clients, they are redirected to No-service page since DNS server is not reachable.
   In case of extended VLAN, CRM for service monitor should be configured on the controller with sync-adoptees option. Any CRM state changes would be forwarded to the adopted devices which would redirect the wireless clients on the WLAN to no-service page in case the monitored CRM is down.

5. AP 622/6522/6562 enhancement for radio 1 – New configuration option to improve receive sensitivity of Radio 1 (2.4GHz) on AP622/AP6522/AP6562 platform. Useful for deployments with low AP density, high ceilings (warehouses), VOIP services etc.

   Under radio configuration (profile/device → interface radio 1):
   service radio-lna ms
   Default is "service radio-lna ang".

6. WiNG 5.5.5 includes updated GNU bash program for NX series of controllers that fixes the Shellshock family of security vulnerabilities outlined in CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277 and CVE-2014-6278.

7. WiNG 5.5.5 includes ability to disable/enable sslv3 for https module under management policy context. This is to address CVE-2014-3566 aka Poodle attack. New command is " https sslv3". Default setting is "no https sslv3".

8. MCD devices with Jedi radios can have connectivity issues when 5.5 and 11 mpbs rates configured on infrastructure. Impacted devices are: MC1790, MC5590, MC7590, MC7594, MC9590, MC9596, MC3190, MC75, MC9190, MC55, VC6090, VC6096, MT2090, MK3900, MK4900, MK590.
   If SSID/band is used exclusively for 802.11g or 802.11gn devices (i.e. no 802.11b devices), configure the data-rates on the SSID/radio to be "g-only" or "gn" or custom with 5.5 and 11 Mbps excluded from the basic rate set.
   If SSID/band is used by 802.11b-only devices as well, configure the data-rates on the SSID/radio to be custom with 1 Mbps and/or 2 Mbps as basic and exclude 5.5 Mbps and 11 Mbps from the supported rates.

New in v5.5.4

1. New event was added to track down IP address of associated client. All events are enabled by default in the system.
   Rfs4000(config-event-policy)#event dot11 client-info

2. One can now configure SNMP community strings for SNMP traps. Previously it was using default community string – public.
   Rfs4000(config-management-policy-default)#snmp-server host <ip> <ver> <port>
   changed to

Rfs4000(config-management-policy-default)##snmp-server host <ip> <ver> <port> community ?
WORD Enter Trap Community Name

Host and Version is mandatory parameters while port (default 162) and community (default public) is optional parameters. Default community string is public.

New in v5.5.3

1. The command - "device-upgrade load-image <image-type> URL" changed to "device-upgrade load-image <image-type> <URL> <on device or domain name>". When on device or domain name is given then the image will be loaded on remote device or RF domain manager respectively. If URL is missing then location of the image will be images loaded on the self device.
2. The command - "show device-upgrade versions on rf-domain-manager" changed to "show device-upgrade versions on <device or domain name>".
3. New web UI:
   a. When upgrading existing installations of controller managed AP 6522, AP 6521, AP 6511, AP 6562 – it's not recommended to use new UI on the APs.
   b. When using new web UI to configure Aps – use of CLI at the same time is not recommended as it can lead to configuration corruption.
   c. New web UI configuration can't be done though Nexus 7 chrome browser as all the fields are misplaced in UI.
   d. New web UI doesn't have option to configure MCX feature.
4. Currently device upgrade on multiple rf-domains does not work from NOC controller when the RFDs are all controller managed. Each domain needs to be upgrade separately.
5. Smart-rf calibration has been removed in this release.
6. NX 9xxx controller will not reboot correctly if USB flash drive is mounted. Please remove the USB when rebooting the controller.
7. CDP and LLDP protocols are enabled by default on WiNG devices. If the wired infrastructure has a combination of managed and unmanaged switches and some are not CDP protocol aware, then CDP protocol needs to be disabled on AP profiles to avoid the L2 switch flooding the packets to all ports.
   WiNG 5.5.x release introduced an enhancement to learn the APs wired side connected port through CDP or LLDP packet processing, so the CDP packet flooding needs to be avoided to eliminate the excessive packet flooding from the APS to controller.
8. WiNG 5.5.4 does NOT include support for ADSP unified mode for NX 7500 series.

New in v5.5.2

1. Change in behavior for "show wireless xxxxx" cli commands and techsupport for centralized controller deployments:

   For centralized controller deployments (multiple RF-Domains across distributed locations), all "show wireless xxxxx" commands will resolve only to the local rf-domain. This will prevent a "show wireless xxxxx" cli command without any rf-domain specified or a techsupport dump operation initiated on the centralized controller from collecting statistics information from all the distributed locations (rf-domains). New mechanisms have been added to collect rf-domain specific statistics individually or globally.

2. New Display Mode in the CLI to view RF-Domain specific or global (across all rf-domains) wireless statistics:
   From the CLI (in EXEC mode/privileged EXEC mode):
   "on rf-domain <rf-domain_name>" sets the display mode for wireless statistics show commands to resolve to a particular rf-domain, all "show wireless xxxxx" commands executed in this mode will automatically return the output corresponding to that rf-domain without the user specifying the "on <rf-domain_name>" extension to every command.

   "on rf-domain all" sets the display mode for wireless statistics show commands to run in global mode – i.e. for each "show wireless xxxxx" command that you run, the controller will display statistics across all rf-domains.

3. Ability to generate wireless stats summary report on a per rf-domain basis or globally (across all rf-domains):

   From the CLI (in privileged EXEC mode) –

   "service copy stats-report rf-domain <rf-domain-name> <URL>"

   "service copy stats-report global <URL>"

   Note: The above option could be utilized for generating inventory/reporting at a system level.

4. **Deprecating the usage of TKIP Encryption:**
   From January 1st , 2014, the WPA TKIP is no longer allowed for Wi-Fi Alliance product certification. For AP/STA products wishing to support a legacy device that is capable of supporting only TKIP encryption, they are required to implement mixed mode with WPA/WPA2.

   Following changes are enforced from WiNG 5.5.3 release onwards to comply with the above Wi-Fi Alliance requirement:

   a) Configuring encryption type as TKIP for a wlan will no longer be supported; wlans requiring to support TKIP clients should use tkip-ccmp as the encryption type.
   b) Upgrading from a prior WiNG 5.x to release to WiNG 5.5.3 will automatically modify the configurations for wlans using 'tkip' as encryption type to 'tkip-ccmp' and will add "service wpa-wpa2 exclude-ccmp" command to avoid any post upgrade incompatibility issues.

   For new configurations, to handle certain legacy/non-Wi-Fi compliant client situations where the client driver is incompatible or does not operate properly in a mixed mode TKIP-CCMP configuration, add the following command "service wpa-wpa2 exclude-ccmp" to the wlan configuration. This configuration allows the wlan to operate in TKIP only mode until the non-compliant wireless clients are phased out of the network.

5. Change in terminology for adoption/upgrade related action commands/events/traps:
   With WiNG 5.5 One View deployment scenarios supporting controllers to be adopted and managed by a centralized controller cluster, existing "ap-xxxxx" action commands have been replaced with "device-xxxxx" action commands. For example: ap-upgrade xxxx will now be referred to as device-upgrade xxxxx.
   All adoption related events and traps are modified to reflect the "device" terminology instead of "ap".

6. Ability to optionally include 'dhcp client-identifier' as part of DHCP Discover/Request packets:
   If your DHCP server uses dhcp client identifier for static bindings (dhcp lease reservations) and responds only to DHCP Discover/Requests with dhcp client identifier present, then the client identifier can be included by configuring the following command "dhcp client include client-identifier" under the SVI (interface vlan X) which is configured as DHCP client.
7. Auto-provisioning policy: 'reevaluate-everytime' command is modified to 'evaluate-always' and moved to 'auto-provisioning-policy' from device/profile context. Upgrade from 5.5.1 to 5.5.3 or later versions should work in accordance with location and syntax changes. However, downgrade from 5.5.3 to former versions would cause the command to disappear from all contexts.
8. Advanced WIPS feature is deprecated in this release. WiNG 5.6 will provide enhance WIPS functionality to replace deprecated feature.

New in v5.5.1

1. NIST SP 800-131A regulation made 1028 bit certificates obsolete as of January 1, 2014. All self-signed on-board certificates which are 1028 bits will be regenerated upon upgrade. Customers need to upgrade all third party certificates to be compliant to new regulations.
2. "show global domain managers" will show incorrect values for number of APs if domain has APs on version below WiNG 5.5.

New in v5.5

1. New images are introduced in WiNG 5.5 for the RFSxxx platforms. These images are labeled RFSxxx-LEAN-5.5.0.0-yyy.img. Where xxx is the target platform and yyy is the build version number. The new controller images do not include any AP images and are intended to be utilized on a site controller operating in a hierarchical typology.

   For a controller operating in a non-hierarchical setup, the upgrade process doesn't involve copying the controller firmware to flash but rather it's copied to RAM. In this scenario, the traditional image (containing the AP images) can be used. However, in a hierarchical typology, during device-upgrade operation the controller image must be copied to flash. In this scenario the "lean" image must be used since the normal image does not fit in flash.
2. ONEVIEW – Site Controller and access points must be in the same RF domain.

3. New notation has been introduced for channel width for all APs in WING 5.5. The new model is to specify the primary channel followed by 'w' or 'ww' to indicate 40MHz or 80MHz. Please see the product documentation for details.

4. ADSP-WiNG Integration:
   - The ADSP release 9.1 Unified mode image (released separately) that corresponds with WiNG 5.5 supports 1500 sensors by default. The administrator can run ADSP with fewer sensors per the table below to free resources for additional VMs, if required.

Sensor Count	CPU (vCPUs)	RAM	HDD	Total WLAN devices (BSS/Station)	Total Active WLAN devices
1500	12	16 GB	400GB	600,000	70,000

- When ADSP is in Unified Mode, it periodically synchronizes with WiNG tree hierarchy. If there are no Areas or Floors under an RF-domain it will create an Area and Floor under that RF-domain automatically in the ADSP scope tree. If later, an Area and Floor are created under that RF-domain within WiNG, they are automatically synchronized into ADSP (including synchronization of device placements).
- WiNG auto-provisioning rules have been expanded to include auto-placement of generic non-WiNG 5 devices. These rules are consumed by ADSP running in Unified mode to auto-place non-WiNG 5 and third party devices.

5. Leverage Level 2 MINT links when building out large multi-site deployments. This is not new in 5.5, but is a common issue when scaling large deployments. WiNG 5 uses Level 1 MINT links by default. There is direct communication between all Level 1 MINT neighbors increasing network traffic and database sizes on the WiNG nodes. Using level 2 MINT links summarizes this information, thereby creating a more efficient network design. Please see the NOC deployment guide for details.

6. WLAN controller does not retain saved auto upgrade configuration when downgrading from 5.5 to pre-5.5 release. This is because “ap-upgrade” commands were renamed to “device-upgrade” in 5.5. When upgrading to 5.5, the conversion happens automatically, however, when downgrading from 5.5 the previous firmware release does not understand “device-upgrade”. The workaround is to manually fix the configuration.
7. Mesh Connex Migration – With the introduction of Auto Channel Select, Mesh Connex Configuration will be migrated when the WLAN controller reboots. The following parameters get migrated:
    - Channel list from smart-rf is copied on to the rf-domain.
    - Priority meshpoint name and root recovery parameters are copied to the meshpoint-device configuration under device context or profile of the APs.
    - For Per-Area Smart RF, the channel list configured for that “Area” is directly configured to the device context of the APs which are part of that area.

8. Open up management access only to those subnets that the administrator will access the devices from. Leaving the management access open in general poses a risk to the network. This will also help eliminate known (medium/ low) vulnerabilities and unknown vulnerabilities that may be discovered in the future. At the time of the release there are no known high vulnerabilities (tested with Nessus/Qualys Guard/Tripwire-Purecloud).
9. Voice enterprise, Hotspot2.0, 802.11w and WIPS sensor features are currently not supported on AP 82xx Access Points. WiNG 5.7.x release supports the MOD-8132 3rd radio sensor module on the AP-8232 platform. LTE module is not supported.

10. Following is a list of clients that were validated for use with 11ac access points

MODEL	CONNECTIVITY	BAND	PHY
Macbook Air(2013)	PCIe	ac+abgn	3x3:3
ASUS PCE-AC66	PCIe	ac+abgn	3x3:3
Broadcom 11n - Asus G750J	PCIe	ac+abgn	2x2:2
Edimax EW-7822UAC	USB 3.0	ac+abgn	2x2:2
Belkin F9L1106 v1	USB 2.0	ac+abgn	2x2:2
Netgear A6200	USB 2.0	ac+abgn	2x2:2
D-Link DWA-182 rev A1	USB 2.0	ac+abgn	2x2:2

MODEL	CONNECTIVITY	BAND	PHY
Buffalo WI-U2-866D	USB 2.0	ac+abgn	2x2:2
Linksys AE6000	USB 2.0	ac+abgn	1x1:1
Asus AC1200	USB 2.0	ac+abgn	2x2:2
Zyxel NWD 6505	USB 2.0	ac+abgn	1x1:1
TRENDnet TEW-805UB	USB 3.0	ac+abgn	2x2:2

11. WiNG 5.5 extended L2tpv3 support for AP 6521, AP 621 and AP 6511. In addition on configuring l2tpv3 settings on those APs – following is required to be set in AP profile for l2tpV3 to work – "service l2tpv3 enable".

12. WiNG 5.5 introduced addition of precedence to ip nat rules.
    ip nat inside source list mylist ?
      precedence Set precedence of access list
    For example: ip nat inside source list mylist precedence 1 interface vlan2 overload

13. In WiNG 5.5 legacy mesh related show commands have been replaced with 'mint' to remove confusion with meshpoint functionality. Use "show wireless mint links" to see the legacy mesh links.

14. **Captive Portal Deployments using External (or) Advanced pages:**
    Captive portal query string delimiter has been changed to '&' instead of '?' from WiNG 5.5 onwards. When upgrading to a 5.5.x based firmware, the JavaScript embedded in the external or advanced webpage(s) needs to be updated to parse the new style of query stings.

    Following line needs to be modified under function **getQueryVariable(variable),**

    var vars = query.split("?"); === change it to ==➔ var vars = query.split(/[?&]/);

    Please ensure that this function gets updated in all the captive portal pages that uses it.

New in version 5.4.x

1. Following vulnerabilities were addressed:
   CVE-2010-4478 - OpenSSH J-PAKE Session Key Retrieval Vulnerability
   CVE-2012-0814 - OpenSSH Commands Information Disclosure Vulnerability
   Note: even though vulnerabilities were addressed – some vulnerability scan firmware that only checks the version number of the component as opposed to testing the actual vulnerability – might still report issue being present.
2. Transmit power adjustments for following platforms:
   a. AP 6532 – Adjustments to FCC, ETSI, and Japan
   b. AP 8132 – Adjustments to FCC, ETSI, and Japan
   c. AP 622/AP 6522 – Adjustments to FCC & ETSI
   d. AP 6562 – Adjustments to FCC & ETSI

3. When upgrading from prior versions – new profiles for newly supported platforms will not be present in the startup-config. User can either create a default profile or do “erase startup-config”.
4. Mismatch in controller and AP version (v5.4.2 and below) will cause extended VLANs not to work properly.
5. ADSP SA cannot be run through a mesh with AP7131N tri radio; non root AP has 3rd radio as sensor
6. Interoperability with Samsung S2 devices:
   A Samsung Galaxy S2 device sometimes fails to connect using EAP-MAC authentication and WEP64 encryption. It’s recommended to reduce the number of attempts (authentication eap wireless-client attempts) from default 3 to 2.
7. With 802.11r enabled WLAN – some clients might have problems associating. Please create a different WLAN for non 802.11r enabled clients.
8. ADSP Spectrum Analysis doesn’t work over a mesh connection.
9. MCX max range feature – the maximum range is 25 km except for 5Ghz 40Mhz channels where range is 24km.
10. WiNG 5.4 and above enforces the limit of policies on standalone APs. Current limit for DHCP, L2TPv3 policy and etc. is one policy per AP. When upgrading from WiNG 5.3 where the limit was not enforced – only one policy will be maintained.
11. VMM – please use following recommendations when configuring VMM feature:
    - Disable L2 Stateful Packet Inspection in Firewall Policy
    - Disable Dynamic Chain Selection on the radio
    - Use Opportunistic Rate Selection on the radio
    - Disable A-MPDU Aggregation if vehicular speed is greater than 30 mph
    - Set RTS-Threshold to 1 on all mesh devices

    Note: for more detail use case scenarios see AP 7161 VMM How-To guide.
12. It’s recommended disabling IP DoS attacks in firewall policy when configuring IGMP snooping.
13. 10 GbE support on the NX 9510 is limited to SFP+ SR interfaces that are included in the controller. LR or XR SFP+ are not supported.
14. NX 9510 only supports extended VLANs in version 5.4.2. L2TPv3 tunneling, IPsec VPN, are not supported in v 5.4.2. These features will be supported in a future release.
15. When downgrading from WiNG 5.4 to a lower WiNG 5.x version through rf-domain, the user needs to downgrade without reloading APs and then do a manual reload on the rf-domain. The following are the CLI commands for this procedure:
    ap-upgrade rf-domain <RF domain name> all no-reboot … this downgrades all APs (including the RF domain manager) without rebooting them
    reload on <RF domain name> … this reboots the entire RF domain.
    Staggered reboot option is not supported in this downgrade scenario.
16. The Firewall has been enhanced in 5.4 to a per-VLAN firewall which can be enabled or disabled on a per-VLAN basis. Per VLAN Firewall is enabled by default. It can be enabled using “firewall” cli command and disabled using the “no firewall” command.
17. WiNG 5.4 adds support for the new USB chip for RFS6000. Previously support was added for the new power supervisor chip.

18. Number of CRM policies is limited to 1 for AP 6511, ES 6510, AP 6521, and AP 621. Number of CRM policies is limited to 4 for AP 6522, AP 6532, AP 650, AP 71x1, AP 622 and RFS 4011.
19. There is a single profile for AP71XX. However, for AP 7161 and AP 7181 placement is set to "outdoor" at the device level. So even though the profile in the controller doesn't have the "outdoor" setting, when configuration is pushed to the AP, the outdoor placement is automatically enforced.
20. Telnet is disabled on AP 621, AP 6521, ES 6510 and AP 6511, since these have limited memory.
21. On AP 6511, AP 6521, ES 6510 or AP 621, when adopted by a controller, the GUI is disabled, to make the memory available for other core functions such as additional mint routes. It is assumed that when an AP is adopted to a controller the controllers' GUI will be used for its configuration. To re-enable the GUI on these APs - use the "memory profile" parameter. Note that when an adopted AP (6521, 6511) or ES 6510 is separated from a controller to operate in standalone mode, the GUI will remain disabled due to this feature, unless the above command is used.
    If APs are already separated from the controller:
    a) Connect to AP CLI.
    b) Set memory profile to 'standalone' under device override or profile context.

    If APs are adopted to controller then memory profile configuration change can be applied from controller CLI:
    a) Connect to Controller CLI.
    b) Set memory profile to 'standalone' under AP profile context.

    Changing the memory profile reboots the AP which then comes up with GUI.

    e.g. CONTROLLER(config-profile-default-ap6511)#memory-profile (adopted | standalone).

From previous releases (prior to 5.4.0.0):

1. Wireless Controller Access protocols
    - HTTPS/SSHv2/SNMP enabled by default
    - HTTP/Telnet Disabled is by default
2. Only two (2) controllers in a cluster are supported in WiNG 5.2 and higher, the same as in WiNG v5.1.x. Cluster creation changed in WiNG v5.2 as compared to WiNG v5.1.x To create a cluster, please do the following:
    a. Controller 1 needs to be fully configured and functional
    b. For controller 2 to be added:
        - Login to Controller 1. Configure "cluster name" if not already configured.
        - Log in to Controller 2, setup an SVI with a static IP address and make sure you can ping Controller 1 IP address. DHCP is not recommended for clustering since the IP address may change later on and the cluster may not form.
        - From Controller 2, execute "join-cluster <Controller 1 IP> username "admin" and the admins' password
          rfs4000-22A3DE#cluster-join 10.10.1.1 username "admin" password <admin-password>
          Joining cluster at 10.10.1.1... Done
          Please execute "write memory" to save cluster configuration.

The requirement that user has to know the admin user name and pass word of Controller 1 makes sure that only the admin can add new controllers to the cluster. To make sure cluster config persists across reboots, user should do "write mem" explicitly after cluster is formed. The command "joincluster" changes only running-config, not startup-config.

3. When using Juniper ex2200-24p-4g or related models when connecting Zebra Access Points – either disable IGMP snooping on the Juniper switches to ensure AP adoption or configure firewall policy filter that will allow the flow of traffic to specified destination-mac-address – 01:A0:F8:00:00:00/48.
4. If using an 802.3af 10/100 power injector to power up the 802.11n APs, when plugged into a Gig E wired switch, please set link speed to 100 full, or user a GigE Power Injector.
5. Important Default Configuration Changes from 4.x to 5.x on the RFS

Description	4.x	5.x
ME1 default IP address	10.1.1.100	192.168.0.1
Auto upgrade enabled	On	On for all other platforms – controllers and AP. Disabled for the NX 9000 by default
HTTP enabled	On	Off
Default User Name/Password	admin/superuser	admin/motorola

6. APs (& ES) have a shadow or secondary IP for gaining access to the AP if the IP address of the AP is not known but the MAC address is known. To derive the shadow IP address of an AP, use the last two hex bytes of the AP's MAC address to determine the last two octets of the IP address.

   AP MAC address - 00:C0:23:00:F0:0A
   AP IP address equivalent – 169.254.240.10

   To derive the AP's IP address using its factory assigned MAC address
   a. Open the Windows calculator by selecting Start>All Programs>Accessories>Calculator. This menu path may vary slightly depending on your version of Windows.
   b. With the Calculator displayed, selct View>Scientific. Select the Hex radio button.
   c. Enter a hex byte of the AP's MAC address. For example, F0.
   d. Select the Dec radio button. The calculator converts the F0 to 240. Repeat this process for the last AP MAC address octet.
7. Default mode for a WLAN is tunnel. For Local bridging, please change config to "local bridging".
8. AP adoption: APs are adopted based on valid SKUs, once discovered under the Auto provisioning policy. AP's with mismatched SKU still get adopted to the controller, but their radio does not turn on.
9. If the system flash is full from packet traces, crash files or ap-images, then there may not be enough space left on the device to create hotspot pages. If this happens, users must clear enough space from flash to allow hotspot pages to be created.
10. Radius authentication of management users uses a different configuration model from 5.0. So if upgrading from 5.0 to 5.2 or higher and you are using radius authentication for management access, you need to either change it to local authentication before upgrade, or

make the mode 'fallback' and then reconfigure after upgrade using the new config model (configuring under aaa-policy).

11. Client load balancing makes decisions based on the average load in a band, in a channel within a band and average AP load. Client load balancing ignores differences in what wlans APs are beaconing. Running client-load-balancing amongst APs with different wlan config, will lead to decisions that may cause clients to NOT associate on a certain wlan
12. Install wizard is available only on the RFS 40XX, among the controller platforms.
13. In WiNG 5.x, antenna power table for the AP 650 has been updated. User should confirm power settings for the AP 650s. In 5.3, the power table for AP 6521 has been updated.
14. Multicipher support: Some of clients keep on sending deauthentication request when associated to WEP security WLAN in multicipher configuration. Please use different BSSIDs with the same WLAN, with different ciphers.
15. Commit is not allowed with radio configuration having two WLANs mapped with different data rates, as this is not a supported configuration.
16. Mesh and SMART RF – please exclude the Mesh APs from the SMART RF domain, as there may be channel changes due to RF interference that could disrupt the mesh link.
17. VPN feature has been re-implemented in WiNG 5.3 to provide a common, more optimized implementation on controllers and APs. Please use the config migration utility when upgrading from a WiNG 4.x release to WiNG 5.4.0. It is recommended that you save your old VPN config to assist in possible downgrades. Please see Note 2 on which VPN configurations cannot be converted using the migration utility, as they are not supported in 5.3. In particular, note that configurations containing AH and DES as IKE encryption algorithm cannot be migrated. For upgrades from WiNG 5.1.x or 5.2.x to WiNG 5.4.0, the VPN config migration is performed automatically (tool is not required).
18. IPsec VPN – In comparison to VPN implementation on RFS controllers on WiNG 4.x or WiNG v5.x, here are the primary differences.
    a. Authentication Header (AH) is not supported in v5.x, but was supported in WiNG 4.x VPN. Use ESP instead of AH.
    b. L2TP over IPsec is not supported in v5.x, but was supported in WiNG4.x VPN. WiNG 5.x supports XAUTH and can be used with a IPsec VPN clients. XUATH has been tested with Cisco and Safenet VPN clients.
    c. IKEv2 was not supported in WiNG 4.x, but is supported in WiNG 5.x.
    d. DES encryption is not supported in the IKE proposal.
    e. Transport mode is only supported for host-to-host rule, in other cases it will fall back to Tunnel mode.
    f. Transport mode NAT-Traversal not supported for IKEv1 and IKEv2 in 5.x. This is supported in tunnel mode.
    g. In the case of IKEv1, if PFS option for IPSec SA (under crypto map entry) is configured on both peers, then the value requested by the initiator is used for the tunnel. If the configured PFS value on the initiator end is lower than that configured on the responder, the lower value is used. If PFS is required, please configure the same PFS value in both the peers.
    h. The value of Kilobyte expiry of an IPSec SA (security-association lifetime kilobytes) can be configured to as low as 500KB. This has to be used with caution. If there is a lot of traffic on the tunnel and the value is set to very low value, the tunnel will end up in an indefinite rekeying IPSec SA state. This value has to be arrived at based on the maximum traffic that is expected on the tunnel and set such that there is an

interval of at least a few minutes between rekeys. It is recommended that this value be set to a minimum of 512000 (500MB).
Impact from lack of the above 4.x features if any, is expected to be minimal.

19. IPsec VPN statistics - following SNMP tables are not available for VPN statistics via SNMP – they will be implemented in a future release – wingStatsDevVpnIpsecSaTable, wingStatsDevVpnIpsecSaTrafficSelectorTable, wingStatsDevVpnIkesaTable.
20. Built-in RADIUS server is available as a demo capability on AP 6521 and can be configured via CLI.
21. Auto-tunnel for VPN
    a. A single group id/PSK is supported on RFS controllers. All APs use same group id/PSK.
    b. When APs are behind NAT (e.g. two remote sites), it is required that the AP IP address are different.
    c. Auto IPsec tunnel termination has been verified on Cisco Gateways with PSK/RSA authentication.
22. VRRP
    a. VRRP version 3.0 (RFC 5798) and 2.0 (RFC 3768) are supported. Default is version 2 to support interoperability. Please note that only version 3 supports sub-second failover.
    b. Services like DHCP, RADIUS, NAT, and VPN running on the virtual IP are supported
    c. For DHCP relay, you can point to the DHCP server as virtual IP
    d. For VPN, on the initiator side, remote peer can be configured as virtual IP
23. If using TFTP to upgrade an AP 6521, AP 6511, ES 6510 or AP 621, on the TFTP server please configure the following settings:
    a. Per packet timeout in seconds: 15
    b. Maximum retries: 20
24. When using iPods as clients, you may see WPA2 group key rotation handshake failures while MUs are idle (2.4GHz band). Change the handshake timeout to 2 sec to correct this problem. From the wlan config, the cli command is: wpa-wpa2 handshake timeout X (where X is the timeout in ms, within a range of 10-5000)
25. Auto assign sensor is not available for AP 6511, AP 6521, ES 6510 or AP 621 – since this feature requires a reboot on low memory devices, which cannot be done with Smart RF enabled.
26. For IGMP Snooping version v2, v3, source specific multicast is not supported, this will be addressed in a future release.
27. To safeguard against unknown attacks, it is recommended that management access be restricted to authorized hosts/subnets. This can be done using the restrict-mgmt-access host/subnet cli command under management-policy.
28. RFS 7000 - Compact flash card will not work on pre-Rev F RFS 7000 hardware.
29. NX 9XXX:
    - NX 9000 requires a laptop with a minimum of 4GB RAM for viewing GUI with greater than 3000 AP.
    - Extended VLANs are not supported on the NX 9000/NX 9500. Only Local VLANs are supported.
    - There is no VPN, or Advanced WIPS support on the NX 9000/NX 9500.
30. AP 7131: PoE and Gigabit Ethernet Ports:

The AP 7131 family features upgraded Gigabit Ethernet (GE) ports. These ports are labeled as follows:

- GE1/PoE: GE1 is the LAN Port and supports 802.3af, 802.3at (draft) PoE.
- GE2: GE2 is the WAN port.

Single radio models can operate fully with 802.3af power sources. Dual radio models and tri-radio models can also power up two radios and GE1 interface with 802.3af power sources. At higher power levels, 2 radios and both Ethernet interfaces are fully functional in the dual and tri-radio models. Single, dual and tri- radio models can also operate using an A/C power supply. The third radio (dedicated WIPS sensor radio or a future modular off-the-shelf 3G WAN Express Card) on the tri-radio model requires 802.3at power levels, A/C power supply or a Gigabit Ethernet PoE+ injector.
The following table shows the radio and LAN resources available under various power configuration modes for the AP 7131 family:

Available Power	Radio Resources	Ethernet Port Configuration
Power Status: 3af (12.95W)	2 Radios	GE1 10/100/1000
Power Status: 3at (24W)	3 Radios (Express Card option supported with radios at lower power)	GE1 10/100/1000 GE2 10/100/1000
Power Status: Full Power (30W)	3 Radios (with Express Card)	GE1 10/100/1000 GE2 10/100/1000

When a Zebra 802.3af power injector (AP-PSBIAS-1P2-AFR) is used with AP- 7131 or AP 7131N, then the GE1 or LAN1 port will be limited to 10/100 Mbps. Zebra recommends the 802.3at (Draft) power injector (AP-PSBIAS-1P3-AFR) to be used with AP 7131/AP 7131N configurations.

31. When AP adopts to Controller, the clock is not getting sync with controller clock immediately. It happens over period of time depending on time delta.

7. DFS Tables, Sensor and Radio Share

1. Following is the DFS support in WiNG 5.7.1 for the supported radio platforms:

Product	Master DFS FCC	Master DFS ETSI	Master DFS Japan	Client DFS FCC	Client DFS ETSI	Client DFS Japan
AP 650 /6532	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7131	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7161	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7181	Disabled	Enabled	Enabled	Disabled	Enabled	Enabled
AP 6511	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 621 /6521	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 622/6522 /6562	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 8132	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 8122	Enabled	Enabled	Disabled	Enabled	Enabled	Disabled
AP 8163	Enabled	Enabled	Disabled	Enabled	Enabled	Disabled

Product	Master DFS FCC	Master DFS ETSI	Master DFS Japan	Client DFS FCC	Client DFS ETSI	Client DFS Japan
MOD-8132-6001S-WW	NA	NA	NA	Enabled	Enabled	Enabled
AP 8222/8232	Enabled	Enabled	Enabled	Disabled	Disabled	Disabled
AP 7502	Disabled	Enabled	Disabled	Disabled	Enabled	Disabled
AP 7532/7522	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
AP 7562	Disabled	Enabled	Disabled	Disabled	Enabled	Disabled
RFS 4011	Disabled	Disabled	Enabled	Disabled	Disabled	Enabled

2. Air Defense sensor capabilities are supported on the 802.11n/802.11ac APs in this release, and are available for enabling the WIPS functionality as well as the Network Assurance Capabilities. There are some caveats on managing the AP directly via ADSP, for certain AP platforms:

Network Assurance Toolset when Radio is dedicated as a sensor	**AP 621 6511 6521** (Note 1)	**AP 650 6532**	**AP 622 6522 6562**	**AP 7131 7161 7181**	**AP 7532 7522 (Note 4)**	**AP 8132 8122**	**AP 8232 82f22**	**AP 7502**
Spectrum Analysis	No	Yes	No	Yes	No	No	No	No
Advanced Spectrum Analysis	Yes	No	Yes	No	Yes	Yes	No	No
Live RF	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Live View	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AP Testing	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Connectivity Testing	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Note 1: GUI is disabled and number of SSH sessions is limited to 1

3. Radio Share functionality (allows for enabling the Network Assurance toolkit in ADSP, without dedicating a radio as a sensor) is available on the 802.11n/802.11ac APs with some caveats – please see details below:

Network Assurance Toolset with Radio Share	**AP 6511 621 6521** (Note 1)	**AP 650 6532**	**AP 622 6522 6562**	**AP 7131 7161 7181**	**AP 7532 7522 (Note 4)**	**AP 8132 8122 8163**	**AP 8232 8222**	**AP 7502**
Spectrum Analysis (Note 2)	No	No	No	No	No	No	No	No
Advanced Spectrum Analysis((Note 3)	Yes	No	Yes	No	No	Yes	No	No
Live RF	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Live View	Yes	Yes	Yes	Yes	Yes	Yes	No	No
AP Testing	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Network Assurance Toolset with Radio Share	AP 6511 621 6521 (Note 1)	AP 650 6532	AP 622 6522 6562	AP 7131 7161 7181	AP 7532 7522 (Note 4)	AP 8132 8122 8163	AP 8232 8222	AP 7502
Connectivity Testing	Yes	Yes	Yes	Yes	Yes	Yes	No	No

Note 1: GUI is disabled when Radio Share is enabled.
Note 2: Spectrum Analysis is not supported with Radio share enabled.
Note 3: Advanced Spectrum Analysis in RadioShare mode may impact WLAN performance.
Note 4: ADSP support for AP 7532/ AP 7522 will be available in v9.1.2.

9. Issues Fixed

Following issues have been fixed in WiNG 5.7.1 release:

SPR#	Description
26535	MCX-ACS scanning loop when radio bands swapped (R1:5GHz/R2:2.4GHz)
26970	When meshpoint name != meshid, mcx-acs will not settle on channel and the mesh never forms
26975	vmif command not available in NX profile via VX9000 cli interface
27068	NX 7500 fails to respond to IP MIB in MIB II.
27113	Passwords containing HTML special characters cannot be used to login to web GUI interface
27153	WiNG 5 permits entering underscore character in the hostname which cause rim cores.
27195	WiNG 5.7 adopts AP although AP adoption is disabled in GUI
27196	Unable to select ACS in the GUI. Configuring ACS via CLI generates error when modifying that radio in the GUI.
27220	Invalid error msg when more than 32 characters are entered for WPA2-PSK through Initial Startup Wizard
27224	When msdu rx-tx is configured on the radio - large frame MSDU packets received over mesh are discarded
27235	Dropdown menu buttons are not clickable under configuration tab after upgrade to 5.7.
27251	CFGD service can crash when controller receives a message from an AP that is incorrectly formatted
27289	"Event Systems Policy" create or edit buttons not click-able in GUI under profile or override.
27328	Radio1 remains in calibrate state, if channel and power is marked smart,with no smart-rf policy mapped
27335	NX9500 with 5.5.6.0-019R firmware abnormal reboot when the command "reload force on AP Device/RF-Domain Manager
27352	Import of custom captive portal pages fail to extract files.
27358	Webpage-location advanced not configured if APPLY button is not entered first after configuring Upload Files param
27362	RIM crashes found on couple of AP71XX on every 1 hour interval , when clients roam from one ap to another
27428	Not able to set Country code in Initial Setup Wizard
27470	Hawaii-Aleutian Time Zone not available
27489	GUI access (HTTPS) disabled when upgrading to WiNG 5.7.0
27502	Adding more than one subnet in the management policy restrict-access gives invalid input message

CQ 205618	show wireless meshpoint tree command not displaying output with low network connectivity
CQ 200239	Critical Resource Monitoring to Shut off a WLAN triggers a DOS attack
CQ 205708	Cfgd error - event_bus writer cannot send on socket
CQ 206477	Wireless Client that is idle will lose network connectivity when roaming
CQ 204461	IPX: Add support for new traps being added to the T5 5.3.2 release
CQ 206925	AP 7532 dumps a rim core when executing "show wireless radio detail" command
CQ 206052	AP 7131N crashes with message: rhal_process_radarevent
CQ 205851	DNS request is not sent once the time to live gets expired for previously resolved dns cache for AAA server name.
CQ 205314	Occasional panic observed with AP7522/AP7532 while reloading after upgrading to 5.7 with PPPoE configuration
CQ 204641	Custom data rate configuration on the AP8232 profile via the GUI is missing

9. Known Issues

Following issues are known issue in WiNG 5.7.x:

CQ/ SPR	Headline	Comments
CQ 202258	CP Bandwidth voucher: User is not getting configured data limit for bandwidth based voucher	This is seen for the upstream traffic which is the opposite of the general traffic in a hotspot, and TCP based applications will anyway back off once they are throttled
CQ 203121	FIPS: Encrypted parts of configuration are lost when downgrading from WiNG 5.7	Workaround: - disable password encryption before the downgrade #no password-encryption secret 2 <password> - perform the downgrade - enable password encryption #password-encryption secret 2 <password>
CQ 200221	Even after disabling routing "show ip route" has all static route entry and traffic between two network is not dropped	
CQ 204497	'no ip dhcp trust' functionality does not working on the AP 7502 FE ports	FE port on AP 7502 will not drop the packet because switch on AP 7502 is not configured to drop. FE port will pass discover packets from dhcp server irrespective of " no ip dhcp trust" to ge1. We can configure GE1 to drop.
CQ 204643	WiNG Express Manager – terminate rogue device function may not work in certain conditions	
CQ 204465	WiNG Express Manager – Cluster license count is not displayed on the UI page	

CQ 206839	MCX Swift UI: Mesh is not applied on either of the radio if bss 2 is already been assigned to wlan	Create mesh point first and them WLANs.
CQ 200297	Slight reduction in throughput when using MacBooks and DCS is enabled on the radios for AP 7532/7522/7562	