Brocade Mobility Software Release v5.5.5

Release Notes v1.0

November 19, 2014

Document History

Document Title	Summary of Changes	Publication Date
Brocade Mobility Software Release v5.5.5 – Release Notes v1.0	New document	November 2014

Contents

Quick Look

Mobility is an architecture that encompasses wireless controllers and associated Access Points (AP). The Mobility software runs on the Brocade Mobility wireless controllers and the Brocade Mobility APs. These release notes apply to version v5.5.5.0 of the Mobility software. This software is fully described in the manual titled: "Brocade Mobility v5.5 System Reference Guide" dated January 2014 and available on the Knowledge Portal and at my.Brocade.com.

Mobility v5.x provides an innovative architecture across the Brocade 802.11n Enterprise WLAN portfolio. This maintenance software release provides critical fixes and enhancements for customer-reported issues. See the Introduction to New Features section below for more details.

Supported Devices

Most devices require their own unique software image. Images from a different product will be rejected during any installation attempt. These images are consistent in release numbering, supported capabilities whenever possible, as well as look and feel.

Mobility v5.5.5 supports the following products using the following image file names:

Product	Image File Name
Controllers	
Mobility RFS4000	BR-RFS4000-5.5.5.0-018R.img
Mobility RFS6000	BR-RFS6000-5.5.5.0-018R.img
Mobility RFS7000	BR-RFS7000-5.5.5.0-018R.img
Mobility RFS9510	BR-NX9510-5.5.5.0-018R.img
Dependent APs	
Mobility 300	(Image is bundled in the controller images)
Mobility 650	(Image is bundled in the controller images)
Independent/Adaptive APs	
Mobility 6511	BR6511-5.5.5.0-018R.img
Mobility 7131 and Mobility 7131N	BR71XX-5.5.5.0-018R.img
Mobility 1220	BR1220-5.5.5.0-018R.img
Mobility 1240	BR124X-5.5.5.0-018R.img

Notes:

(1) The Mobility 5181 access points are not supported by the Mobility v5.x software releases.

(2) The software images for the dependent access points are embedded within the controller images and do not require any specific installation step.

(3) Virtual Machine capability is supported on Mobility RFS9510 controllers only.

Adaptive APs are configured by a controller but retain their configuration and survive the loss of connectivity to their parent controller.

Dependent APs are configured by a controller but must maintain connection to their parent controller (or be adopted by a standby controller) to remain operational.

Independent APs are Adaptive APs that operate without a wireless controller.

The following table provides a software compatibility matrix for deployments of the Mobility RFS controller with the adaptive APs:

Mobility RFS Controller (and Dependent APs)	**Mobility 5181 802.11 a/b/g AP**	**Mobility 7131/7131N 802.11 a/b/g/n APs**	**Mobility 6511 802.11 a/b/g/n AP**	**Mobility 1220 and 1240 802.11 a/b/g/n APs**
5.5.5.0-018R	N/A	5.5.5.0-018R	5.5.5.0-018R	5.5.5.0-018R
5.5.4.0-018R	N/A	5.5.4.0-018R	5.5.4.0-018R	5.5.4.0-018R
5.5.3.0-041R	N/A	5.5.3.0-041R	5.5.3.0-041R	5.5.3.0-041R
5.5.2.0-011R	N/A	5.5.2.0-011R	5.5.2.0-011R	5.5.2.0-011R
5.5.1.0-017R	N/A	5.5.1.0-017R	5.5.1.0-017R	5.5.1.0-017R
5.5.0.0-090R	N/A	5.5.0.0-090R	5.5.0.0-090R	5.5.0.0-090R
5.4.4.0-008R	N/A	5.4.4.0-008R	5.4.4.0-008R	5.4.4.0-008R
5.4.3.0-018R	N/A	5.4.3.0-018R	5.4.3.0-018R	5.4.3.0-018R
5.4.2.0-030R	N/A	5.4.2.0-030R	5.4.2.0-030R	5.4.2.0-030R
5.4.1.0-020R (4000/6000/7000 only)	N/A	5.4.1.0-020R	5.4.1.0-020R	N/A
5.4.0.0-047R (4000/6000/7000 only)	N/A	5.4.0.0-047R	5.4.0.0-047R	N/A
5.3.1.0-009R (4000/6000/7000 only)	N/A	5.3.1.0-009R	5.3.1.0-009R	N/A
5.2.13.0-015R (4000/6000/7000 only)	N/A	5.2.13.0-015R	5.2.13.0-015R	N/A
5.2.12.0-010R (4000/6000/7000 only)	N/A	5.2.12.0-010R	5.2.12.0-010R	N/A
5.2.0.0-069R (4000/6000/7000 only)	N/A	5.2.0.0-069R	5.2.0.0-069R	N/A
5.1.0.0-074R (4000/6000/7000 only)	N/A	5.1.0.0-074R	5.1.0.0-074R	N/A
4.4.2.0-003R (4000/6000/7000 only)	2.6.3.0-002R	4.4.2.0-003R	N/A	N/A
4.4.0.0-034R (4000/6000/7000 only)	2.6.0.0-034R	4.4.0.0-034R	N/A	N/A

4.3.4.0-014R (4000/6000/7000 only)	2.5.3.0-003R	4.1.4.0-002R	N/A	N/A
4.3.1.0-018R (4000/6000/7000 only)	2.5.1.0-016R	4.1.1.0-018R	N/A	N/A
4.3.0.0-059R (4000/6000/7000 only)	2.5.0.0-041R	4.1.0.0-072R	N/A	N/A
4.2.1.0-006R (6000/7000 only)	2.4.1.0-006R	4.0.3.0-006R (7131 AP only)	N/A	N/A
4.0.2.0-012R (6000/7000 only)	2.3.2.0-011R	3.2.2.0-011R (7131 AP only)	N/A	N/A

Supported Wireless WAN cards

The 3G wireless WAN feature is available on the Mobility RFS4000 and RFS6000 controllers, and Mobility 7131N access point (via the ExpressCard™ slot). Selection of an ExpressCard™ 3G wireless WAN card is dependent on the offerings of the local service providers in the area of operation of the controller. Driver support is provided for one of the following wireless cards:

- AT&T (NALA) – Option GT Ultra Express, Sierra Wireless Aircard 890
- Verizon (NALA) – Verizon Wireless V740, PC770 Express Cards
- Sprint (NALA) - Sprint Novatel Merlin C777 Express card
- Vodaphone (EMEA) – Novatel Merlin XU870
- Vodaphone (EMEA) – Vodaphone Mobile Connect E3730 3G Expresscard
- Telstra (Australia) – Telstra Turbo 7 series Expresscard (Aircard 880E)
- General Use (NALA/APAC) – Novatel Merlin XU870, Sierra Wireless Aircard 503, 504

Supported Web Browsers

The Graphical User Interface (GUI) of the devices requires the browser to be capable of running **Adobe Flash Player v10**. The following browsers have been validated:

- Internet Explorer 6.0 to 10.0
- Firefox 3.5 to 21.x
- Chrome 10.0 to 27.x
- Safari 5.0 to 6.0

ADSP Software Compatibility

Motorola's AirDefense Services Platform (ADSP) is a system designed to manage, monitor and protect WLAN networks. ADSP has tight out-of-the-box integration with the Mobility software. It combines the information collected from your network of sensors or access points with the analytical power of an intelligent central console to provide network monitoring, automate security, and enable regulatory compliance, multi-vendor management, remote troubleshooting and locationing services.

Mobility v5.5.x is compatible with the Motorola Air Defense Services Platform (ADSP) software v9.1 and later releases.

Introduction to New Features

Support for ETSI EN 300 328 v1.8.1 and ETSI EN 301 893 v1.7.1
ETSI EN 300 328 v1.8.1 and ETSI EN 301 893 v1.7.1 have an effective date of December 31, 2014. Therefore APs shipped, deployed and installed in Europe as of January 1, 2015 need to be compliant with new regulations. Do not change the firmware to a non-compliant version.

The following APs will comply with new ETSI regulations in WiNG 5.5.5 release:
AP 6511, AP 1220, AP 1240.

The following WiNG APs will not comply with new ETSI regulations:
AP 650, AP 7131.

Vulnerability updates:
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.

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"

Controller Licensing

The supported licenses on the controllers in Mobility v5.5.5.0-018 are:

	Mobility RFS4000	**Mobility RFS6000**	**Mobility RFS7000**	**Mobility RFS9510**
"Adaptive AP" licenses Applicable to Mobility 650, 7131/7131N, 6511, 1220, 1240	Up to 144	Up to 256	Up to 1024	Up to 10,240
"AP" licenses Applicable to Mobility 300, 650, 7131/7131N, 6511, 1220, 1240	6	Up to 48	Up to 256	N/A

Advanced Security (for Role Based firewall)	Included in the software	On/Off license – not shareable in a cluster
Advanced IDS/IPS		On/Off license – not shareable in a cluster (license is applied on controller to enable functionality on both controller and adopted APs)

Please note that that the Mobility 300 continues to require the AP license type and follows the AP license capacity. It is only supported by the RFS4000/6000/7000 controllers.

A key difference with v5.x from prior v4.x releases is that the Mobility 650 Dependent Access Points also follow the maximum capacity per controller as the Adaptive APs (Mobility 7131/ 7131N, 6511, 1220, 1240) since it can now locally bridge and locally forward traffic securely. However, the Mobility 650 APs are not site-survivable APs, i.e. they will stop operation if they lose connection to the controller.

Virtual Controller Capability

Independent Access Points (BR7131/BR7131N, BR6511, BR1220, and BR1240) can be deployed in controller-less environments with one Access Point being configured as the "Virtual Controller" (VC) for the others APs. The maximum capacity of a Virtual Controller Access Point to be able to manage other APs is 24 APs of the same model.

Virtual controller provides controller-like features such as:

- Firmware Updates for the other like APs on that location
- Configuration Management for the other APs
- Statistics collection and aggregation
- Troubleshooting for all the other APs on that location.

In addition to the above, an AP acting as a virtual controller supports all the features of an Independent AP. Enabling VC mode on an AP does not require a license. An AP when in VC mode can have one RF Domain and one profile. Any AP specific configurations that do not conform to that common profile will need to be configured as "device overrides" for that particular AP.

Upgrading and Downgrading the Software

This section outlines the upgrade procedure applicable if the controller had a prior release or a beta image version installed. The sections below cover installation from the CLI or GUI from controllers or APs. Additional information may be found in the "Brocade Mobility v5.5 CLI Reference Guide" for CLI installation and the "Brocade Mobility v5.5 System Reference Guide" for GUI installation.

- Upon upgrade to v5.5.3 – AP 6511, AP 1220 will have a new web UI.
- Upgrading WiNG v4.x networks to WiNG v5.5.x will not retain the 4.x configuration. Please use the configuration migration utility to convert a 4.x configuration to a 5.5 based configuration. This is an offline tool that assists with config migration.
- When downgrading from WiNG 5.5.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 rfdomain. 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.

- 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.
- 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.
- 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 image. For example:
  - Copy AP 650 5.2 image on the RFS flash rfs4000-22A1B8#copy tftp://<Server IP>/AP650-5.2.0.0-069R.img flash:/AP650-5.2.0.0- 069R.img
  - 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
    - 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>
- In Virtual Controller deployments, APs running version 5.4.x will not adopt to a virtual controller running version 5.5.x. First upgrade APs to version 5.5.x (manually) and then upgrade the Virtual Controller. New APs need to be upgraded to 5.5.x manually before connecting to a WiNG 5.5.x Virtual Controller network.
- Downgrade to WiNG 4 is not recommended in countries following ETSI regulations as WiNG 4 is not compliant with current ETSI DFS regulations.

Note: **Users are strongly cautioned against upgrading any Mobility device from the Boot OS prompt at the serial console. Upgrading from the Boot OS prompt is not a recommended and supported upgrade methodology.**

Controller/AP Upgrade/Downgrade Matrix

Following is the supported Upgrade/Downgrade Matrix for the various platforms:

Controller and AP Combination	Upgrade from	Downgrade to	Notes
Mobility RFS controller + Mobility 650/300	v4.3.1 onwards on the controller	Downwards to v4.3.3 on the controller	Mobility 300 and 650 images are contained within the controller image
Mobility RFS controller + Mobility 7131/7131N	v4.1.1 onwards on the AP v4.3.1 onwards on the controller	Downwards to v4.1.5 on the AP Downwards to	Mobility 7131/7131N image is not contained within the controller

		v4.3.3 on the controller	image
Mobility RFS controller + Mobility 6511	v5.1 onwards, on the AP v4.3.x onwards on the controller	Downwards to v5.1 on the AP and controller	Mobility 6511 image is not contained within the controller image
Mobility RFS controller + Mobility 1220	v5.4.2 onwards, on the AP and controller	Downwards to v5.4.2 on the AP and controller	Mobility 1220 image is not contained within the controller image
Mobility RFS controller + Mobility 1240	v5.4.2 onwards, on the AP and controller	Downwards to v5.4.2 on the AP and controller	Mobility 1240 image is not contained within the controller image
Independent/Adaptive AP	**Upgrade from**	**Downgrade to**	**Notes**
Mobility 6511	v5.1 onwards	Downwards to v5.2	BR6511 v5.1 is not supported for the independent mode of operation
Mobility 7131/7131N	v4.1.1 onwards	Downwards to v4.1.5	
Mobility 1220	V5.4.2 onwards	Downwards to v5.4.2	
Mobility 1240	V5.4.2 onwards	Downwards to v5.4.2	

When operating with controllers, please ensure that the controller and APs are running the same Wireless Mobility version after the upgrades are complete.

When upgrading a Mobility 300 access port (BR300 or AP300) from old Mobility v4.x to v5.x, please make sure to upgrade to v4.3 or later prior to upgrading to v5.x.

Mobility Wireless Controllers

The methods described in this section use the Command Line Interface (CLI), the Graphical User Interface (GUI) or the Auto-Install procedure. To log into the CLI, either SSH, Telnet or serial access can be used. A TFTP/FTP network upgrade scenario with the RFS4000 controller is used in the examples below. Additional protocols or mass storage options are supported by the CLI upgrade command or the GUI.

Important: Always create a backup of your configuration prior to upgrade.

Controller Upgrade/Downgrade between v5.x Versions

1. Copy the **BR-RFS4000-5.5.5.0-018R.img** controller image 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**.

Controller Upgrade from v4.3.x (or Higher v4.x)

1. Copy the **BR-RFS4000-5.5.5.0-018R.img** controller image 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**.

Note*:** When upgrading from v4.x to v5.x, ***the configuration is not retained or converted. All configuration items will be set to factory defaults. You may use the offline CFGCV configuration migration tool to convert a v4.x configuration to a v5.4.x configuration. The configuration must otherwise be rebuilt.

Note: Please use FTP to upgrade to v5.x on a Mobility RFS6000, and not TFTP, if using the "ge1" port.

Controller Downgrade to v4.3.x (or Higher v4.x)

1. Copy the **BR-RFS4000-4.3.X.X-XXXR.img** controller image 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**.

On downgrade from v5.x to v4.x, any saved v4.x configuration file (if available from an earlier upgrade from v4.x to v5.x) is restored back.

Note: Due to necessary hardware refresh changes on the Mobility controllers, older versions of software may not support the newer hardware revisions. Downgrade/upgrade to a version that does not support the new hardware components on the unit will be automatically prevented. Any version of software prior to v5.2.12 may not support the newest controller revisions.

Configuration Restoration

On upgrade from v4.x to v5.x, the controller will save the v4.x configuration file in another file on flash (in 'nvram:/startup-config-wing4') and the 'startup-config' will then point to the v5.x default startup-config. The password encryption file is also moved to /etc2/encrypt-passwd-WiNG4. No v4.x configuration is automatically migrated. Please use the off-line CFGCV configuration migration tool to convert a v4.x configuration to a v5.4.x configuration.

On downgrade from v5.x to v4.x, any previously saved v4.x config if present is restored back.

Access Point Upgrade Options

Mobility v5.x supports AP firmware upgrade from the controller. With the AP firmware image loaded on a controller, the same AP image can then be used for the upgrade of all the corresponding APs.

Available firmware on the controller can be checked using the below command:

```
br-rfs4000-22A1B8#show ap-upgrade versions
```

If the AP image is not already part of the controller image, a new image can be uploaded to the controller using following command:

```
br-rfs4000-22A1B8#ap-upgrade load-image ?
  br650   Upgrade an BR650 device
  br6511  Upgrade an BR6511 device
  br1220  Upgrade an BR1220 device
  br71xx  Upgrade an BR71XX device
  br124x  Upgrade an BR124X device
```

Once AP firmware is loaded on the controller, different options are available for AP firmware upgrade:

Manual Upgrade

Firmware upgrade can be initiated on a single AP or a list of APs using the following command:

```
br-rfs4000-22A1B8#ap-upgrade br71xx-16C7B4 ?
  no-reboot     No reboot (manually reboot after the upgrade)
  reboot-time   Schedule a reboot time
  upgrade-time  Schedule an upgrade time
```

or

```
br-rfs4000-22A1B8#ap-upgrade ap71xx all ?
  no-reboot     No reboot (manually reboot after the upgrade)
  reboot-time   Schedule a reboot time
  upgrade-time  Schedule an upgrade time
```

Scheduling AP Firmware Upgrade

AP firmware upgrade can be scheduled on a controller, that is upgrade time and reboot time can be configured. The controller performs the firmware upgrade on the APs following the configured upgrade time.

```
br-rfs4000-22A1B8#ap-upgrade all ?
  no-reboot     No reboot (manually reboot after the upgrade)
  reboot-time   Schedule a reboot time
  upgrade-time  Schedule an upgrade time
```

Upgrade through RF Domain Manager

A firmware upgrade can be initiated from a controller to be performed through an RF domain manager. The RF domain manager is a Mobility device that is elected within each RF domain to assist with some statistics data collection and some management or control tasks at a local level. Upgrading via the RF domain manager results in pushing a firmware image once from the controller to the RF domain manager and then having the RF domain manager further push this image to the appropriate devices for that image within its RF domain.

```
br-rfs4000-22A1B8#ap-upgrade rf-domain default ?
  all     Upgrade all access points in rf domain
  br650   Upgrade an BR650 device
  br6511  Upgrade an BR6511 device
  br1220  Upgrade an BR1220 device
  br71xx  Upgrade an BR71XX device
  br124x  Upgrade an BR124X device
```

Auto Upgrade

Auto firmware upgrade can be enabled on the controller to force any AP that is being adopted by the controller to be updated to the version present on the controller if its firmware version is different. The following CLI command should be used:

```
br-rfs4000-22A1B8(config-device-XXX)#ap-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.

```
br-rfs4000-22A1B8(config-device-XXX)#ap-upgrade count ?
  <1-20>  Number of concurrent AP upgrades
```

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

Mobility 300 / 650 Dependent Access Points

Upgrade/Downgrade for Mobility 300 and Mobility 650 access points from/to v4.x-compatible firmware to/from v5.4-compatible firmware is seamless, and done automatically by the controller.

Dependent AP Upgrade from v4.x

Upgrade for Mobility 650 from v4.x to v5.x prior to v5.4 release is seamless, and done automatically by the controller as described in the next paragraph. However, upgrade from v4.x to v5.4.x or later is NOT seamless and requires that the Mobility 650 be first updated to any v5.2.x or v5.3.x image.

The v5.x controller can upgrade the Mobility 650 from v4.x to v5.2.x or v5.4.x using the WISPe protocol upgrade facility. This capability is enabled using "**`legacy-auto-update`**" command for the controller, either in the device or profile configuration files. The controller will first adopt the access point using the WISPe protocol messages (just as a v4.x controller would do) and then download the new image to it, which upgrades the AP firmware to v5.x.

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:

br-rfs4000-22A136#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

br-rfs4000-22A136(config)#profile br-rfs4000 default-br-rfs4000

br-rfs4000-22A136(config-profile-default-br-rfs4000)#**legacy-auto-update**

br-rfs4000-22A136(config-profile-default-br-rfs4000)#**commit**

br-rfs4000-22A136(config-profile-default-br-rfs4000)#

Note: The FTP server on the controller must be enabled for successful operation of this feature.

The BR650 v5.2.x or v5.3.x image should be available on the RFS controller:

```
br-rfs4000-22A136#copy tftp://<Server IP>/BR650-5.2.0.0-069R.img
flash:/BR650-5.2.0.0-069R.img
```

In the controller profile context, set the legacy auto-update image pointer to the v5.2.x or v5.3.x image Mobility 650 image:

```
br-rfs4000-22A136(config-profile-default-br-rfs4000)#service wireless
br650 legacy-auto-update-image flash:/BR650-5.2.0.0-069R.img
```

With auto update enabled, BR650 will get upgraded to the designated image upon adoption to the controller. Without auto update enabled, use the ap-upgrade command to upgrade individual Mobility 650 devices:

```
br-rfs4000-22A136#ap-upgrade br650 <DEVICE>
```

Dependent AP Downgrade to v4.x

The Mobility 650 can be automatically downgraded to a v4.x version of the AP firmware by connecting it to a controller running the desired v4.x version. The AP tries to discover both v4.x as well as v5.x controllers by default, and if it does not find a v5.x controller, but does find a v4.x controller, it will initiate adoption to it. As part of the adoption process, the v4.x controller will download a corresponding v4.x image to it.

Dependent AP Adoption after Upgrade

If the Access point was adopted at layer 2 or was using DHCP options to get adopted by the controller, there is no change in the adoption process following the upgrade. The AP connects back to the controller in the same way.

Mobility Independent/Adaptive APs

Independent APs include Mobility 7131, 7131N, 6511, 1220, and 1240 APs. A Mobility 7131 AP is used in the examples below.

Adaptive AP Upgrade/Downgrade Between v5.x versions

1. Copy the **BR71XX-5.5.4.0-018R.img** controller image 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**.

Mobility 7131/7131N Upgrade from v4.x

Please use the special "migration image" **BR7131-5.5.5.0-018R.bin** when upgrading from v4.x (v4.1.1.0-018R or later) to v5.4. After upgrade with this migration image, the access point will reload, running the v5.4 software.

For automatic upgrades from the controller, the migration image must first be copied to flash:/ on the v5.4 controller which must be configured with the '**legacy-auto-update br71xx image flash:/**' CLI command (see example above for Mobility 650).

For a manual upgrade of the AP from its v4.x Graphical User Interface (GUI), follow these steps:

1. On the Mobility 7131/7131N running v4.1.1.0-018R (or later), open the GUI and log in as "admin".
2. Select 'System Configuration' > 'Firmware Update' from the BR7131 menu tree of the GUI.
3. Specify the name of the target firmware file within the 'Filename' field: BR71XX-5.5.2.0-011R.bin
4. If the target firmware file resides within a directory, specify a complete path for the file within the 'Filepath (optional)' field.
5. Enter an IP address for the FTP or TFTP server used for the update.
6. Select either the FTP or TFTP button to define whether the firmware file resides on a FTP or TFTP server.
7. 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.
8. Click the 'Perform Update' button to initiate the update.
9. Click 'Yes' to confirm. The update may take several minutes.

Alternatively, for a manual upgrade of the AP via its Command Line Interface, follow these steps:

1. Log in as "admin" into the BR7131 running v4.1.1.0-018R (or later).
2. Go to the firmware update context and enter file name "BR7131-5.5.4.0-018R.bin" for upgrade:

```
admin(system.fw-update)>set file BR7131-5.5.5.0-018R.bin
admin(system.fw-update)>sh

automatic firmware upgrade        : disable
automatic config upgrade          : enable

firmware filename                 : BR7131-5.5.5.0-018R.bin
firmware filepath                 :
ftp/sftp/tftp server ip address   : 192.168.0.5
ftp/sftp user name                : lap
ftp/sftp password                 : ********
```

```
admin(system.fw-update)>
```

3. Start the upgrade with the below command.

```
admin(system.fw-update)>upgrade tftp
```

Mobility 7131/7131N Downgrade to v4.1.5

To downgrade a Mobility 7131/7131N access point running v5.4.x to v4.1.5 the reverse migration image **BR7131-5.5.5.0-018R-04010500004R.img** must be used. This image is installed on the AP just as a regular v5.x image is installed using the controller CLI (**`ap-upgrade`**) or the AP CLI (**`upgrade`**). After this downgrade the AP runs v4.1.5; further upgrade/downgrades may be required if a different v4.x version is required.

When adopted by a controller, first downgrade all APs to v4.1.5. Then downgrade the controller to the corresponding v4.x and the APs come back and get adopted.

All configurations from v5.x are lost as the AP is downgraded to v4.1.5. However the original v4.x configuration file, if any was left over from a prior v4.x to v5.x migration, is automatically restored.

Mobility 7131/7131N Limited Configuration Restoration

Some of the configuration items from a v4.1 BR7131/7131N are translated and migrated over to the v5.x version of the config during update. These help ensure connectivity back to the controller. The items of configuration that are migrated are:

- Hostname
- Port PHY configuration (speed, duplex)
- Port L2 configuration (trunking information)
- IP address of controller (translated to ‘controller host’ in v5.x)
- WAN interface IP addressing
- LAN interface /subnet1 IP address

If the v4.x configuration could not be read properly (bad blocks, any exceptions while reading the flash memory, etc) then the AP will come up with the default v5.5.x configuration and create a log file called ‘legacyapn_<version>.dump.tar.gz’ in ‘flash:/crashinfo’ indicating what was translated and additional details on the error for post-analysis.

AutoInstall

AutoInstall works via the DHCP server. This requires the definition on the DHCP server of a 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. For example: ‘ftp://admin:admin123@192.168.1.10’)

Option 187 - defines the firmware path and file name

Option 188 - defines the configuration file path and file name

The DHCP vendor class parameters for the various platforms are:

Mobility Device	DHCP Vendor Class Parameter
Mobility RFS7000	BrocadeRFS.br-rfs7000
Mobility RFS6000	BrocadeRFS. br-rfs6000
Mobility RFS4000	BrocadeRFS. br-rfs4000
Mobility RFS9510	BrocadeRFS.br-rfs9510
Mobility 7131/7131N	BrocadeAP. br7131
Mobility 650	BrocadeAP. br650
Mobility 6511	BrocadeAP. br6511
Mobility 1220	BrocadeAP. br6522
Mobility 1240	BrocadeAP. br1240

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.

ADSP Virtual Machine Installation on RFS9510

The ADSP VM can be installed on RFS9510 controllers; it does not come pre-installed with Mobility 5.5. The installation procedure is as follows:

1. Download the ADSP image and place it onto an FTP/TFTP server or USB key.

2. Using the **`upgrade`** CLI command or **Firmware Upgrade** option in the Web-UI, download the ADSP image onto the RFS9510. Note if using the CLI it is recommended that you transfer the ADSP image to the RFS9510 using the background option! This will install the image in the /vmarchive partition.

3. 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

#**`virtual-machine uninstall adsp`** # Uninstalls the ADSP-VM

#**`virtual-machine install adsp`** # Installs the new ADSP-VM

Note: "**`uninstall`**" will cause the VM configuration and database entries to be erased. Please be sure to export and save the configuration and database prior to uninstalling.

Technical Support

Contact your supplier for the hardware, firmware, and software support, including product repairs and part ordering. To expedite you call, have the following information immediately available:

General Information:

- Technical Support contract number, if applicable
- Device model
- Software release version
- Error numbers and messages received
- Detailed description of the problem, including the controller or network behavior immediately following the problem, and specific questions
- Description of any troubleshooting steps already performed, with the results
- Controller Serial Number

Getting Help or Reporting Errors

Brocade is committed to ensuring that your investment in our products remains cost-effective. If you need assistance, or find errors in the manuals, contact Brocade. Go to http://www.brocade.com/services-support/index.page for e-mail and telephone contact information.

Additional Resources

For more information about the products supported in this software release, refer to the following publications.

- Brocade Mobility RFS4000 Installation Guide
- Brocade Mobility RFS6000 Installation Guide
- Brocade Mobility RFS7000 Installation Guide
- Brocade Mobility RFS9510 Installation Guide
- Brocade Mobility 7131/7131N Installation Guide
- Brocade Mobility 650 Installation Guide
- Brocade Mobility 6511 Installation Guide
- Brocade Mobility 1220 Installation Guide
- Brocade Mobility 1240 Installation Guide
- Brocade Mobility v5.5 CLI Reference Guide
- Brocade Mobility v5.5 System Reference Guide

Important Notes

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 7131have 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. Roaming assist changes: WiNG 5.5.5 adds new configuration options for controlling the aggressiveness of roaming assist functionality.

6. AP 1220 enhancement for radio 1 – New configuration option to improve receive sensitivity of Radio 1 (2.4GHz) on AP1220 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".

7. 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.

8. 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".

9. 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 Notes for Release 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 Notes for Release v5.5.3

1. The command - "device-upgrade load-image <image-type> URL" changed to "deviceupgrade 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 1220, AP 6511 – 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 is 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. WiNG 5.4.4 adds support for Analytics feature on NX 7500.

New Notes for Release 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 Mobility v5.5.2 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 v5.x release to v5.5.2 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 Mobility v5.5 OneView deployment scenarios that support controllers 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 v5.5.1 to v5.5.2 or later versions should work in accordance with location and syntax changes. However, downgrade from v5.5.2 to former versions would cause the command to disappear from all contexts.

8. Advanced WIPS feature is deprecated in this release.

Notes for Release v5.5.1

1. NIST SP 800-131A regulation made 1024 bit certificates obsolete as of January 1, 2014. All self-signed on-board certificates which are 1024 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 v5.5.

Notes for Release v5.5

3. ONEVIEW – Site Controller and access points must be in the same RF domain.

4. New notation has been introduced for channel width for all APs in Mobility v5.5. 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.

5. Mobility allows users to download the ADSP toolkit. The link to this toolkit is http://docs.symbol.com/downloads/AirDefense/MotorolaADSP-install.exe. Downloading of this toolkit is a one-time process. This requires internet connectivity.

6. Mobility-ADSP integration:

   - The ADSP release 9.1 Unified mode image (from Motorola Solutions) that corresponds with Mobility 5.5 supports 2000 sensors by default. The administrator can run ADSP with fewer sensors per the table below to free resources, if required.

Sensor Count	CPU (vCPUs)	RAM	HDD	Total WLAN devices (BSS/Station)	Total Active WLAN devices
2000	12	16 GB	400GB	400,000	70,000
1500	8	12 GB	300GB	270,000	60,000
1000	6	10 GB	200GB	200,000	40,000
500	4	8 GB	100GB	200,000	20,000

- When ADSP is in Unified Mode, it periodically synchronizes with Mobility 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 Mobility, they are automatically synchronized into ADSP (including synchronization of device placements).
- Mobility auto-provisioning rules have been expanded to include auto-placement of generic non-Mobility v5 devices. These rules are consumed by ADSP running in Unified mode to auto-place non-Mobility v5 and third party devices.

7. Make use of "Level 2 MINT links" when building out large multi-site deployments. This recommendation (not new with v5.5) is important when scaling to large deployments. Mobility v5 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 Mobility nodes. Using Level 2 MINT links summarizes this information, thereby creating a more efficient network design. Please see the NOC deployment guide for details.
8. The WLAN controller does not retain the saved auto upgrade configuration when downgrading from v5.5 to pre-v5.5 release. This is because "ap-upgrade" commands were renamed to "device-upgrade" in v5.5. When upgrading to v5.5, the conversion happens automatically, however, when downgrading from v5.5 the previous firmware release does not understand "device-upgrade". The workaround is to manually fix the configuration.
9. 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.
10. Open 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).

11. Analytics:

- When working in cluster – following firewall ports need to be opened:

  tcp - 8020, 50010, 50020, 60000, 60020, 2181 (proprietary protocol)
  tcp - 50070, 50090 (http is used on these ports)
  tcp - 50075, 60010, 60030 (also via http, carry debug related traffic)

- The nodes in a cluster must be configured to use NTP. The skew must be not less than 15 seconds

- Take a backup of the analytics database on each controller before upgrade and on a regular basis. If for any reason data becomes corrupted – it can be restored from last back up.

  To back up everything including database:

  service copy analytics-support ftp://<ip address of server>/<name of file>

  To restore database:

  archive tar /xtract ftp://<ip address of server>/<name of file> /

- When upgrading from Mobility v5.4.x to v5.5, data from v5.4.x is migrated over to v5.5. When downgrading from v5.5 to v5.4.x, the system does NOT bring back data from v5.5 to v5.4.x. This means the user will revert to the previous v5.4.x backup data.

- To configure your new Mobility RFS9510 systems after the upgrade:

  ✓ On the Primary controller
    - service analytics stop (*if analytics was configured and running previously)*
    - service analytics primary <primary_ip>
    - service analytics start

  ✓ On the Standby controller:
    - service analytics stop (*if analytics was configured and running previously)*
    - service analytics clear-data
    - service analytics secondary <secondary_ip> <primary_ip>
    - service analytics start

  Note: If you do not enter the above CLI commands, then Analytics starts as Standalone on both systems.

12. Maximum number of WLANs and RF domains supported per controller:

Controller Platform	WLAN capacity	RF Domains
Mobility RFS9510	1024	4096
Mobility RFS7000	256	1024
Mobility RFS6000	32	256
Mobility RFS4000	24	144

Notes From v5.4.x Releases

13. AP300 default setting changed to ACS instead of SMART which is not supported on AP300 platform.

14. Transmit power adjustments for following platforms:

    Mobility 1240 – Adjustments to FCC, ETSI, and Japan

    Mobility 1220 – Adjustments to FCC & ETSI

15. 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".
16. Mismatch in controller and AP version (5.4.2 and below) will cause extended VLANs not to work properly.
17. 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.
18. With 802.11r enabled WLAN – some clients might have problems associating. Please create a different WLAN for non 802.11r enabled clients.
19. ADSP Spectrum Analysis doesn't work over a mesh connection.
20. MCX mesh max range feature – the maximum range is 25 km except for 5Ghz 40Mhz channels where range is 24km.
21. Mobility v5.4 and above enforce the limit of policies on standalone APs. Current limit for DHCP, L2TPv3 policy etc. is one policy per AP. When upgrading from v5.3 where the limit was not enforced, only one policy will be maintained.
22. It is recommended to disable IP DoS attacks in the firewall policy when configuring IGMP snooping.
23. 10 GbE support on the RFS9510 is limited to SFP+ SR interfaces that are included in the controller. LR or XR SFP+ are not supported.
24. The Firewall has been enhanced in v5.4 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.
25. Following is the DFS support for the supported radio platforms:

Product	Master DFS FCC	Master DFS ETSI	Master DFS Japan	Client DFS FCC	Client DFS ETSI	Client DFS Japan
BR650	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
BR7131/BR7131N	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
BR6511	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
BR1220	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
BR1240	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled

26. Maximum number of clients per AP platform is as follows:

AP Platforms	Client Association Capacities
Dependent APs	
Mobility 300	256
Mobility 650	256
Independent APs	
Mobility 6511	128
Mobility 7131/7131N	256
Mobility 1220	256
Mobility 1240	256

The client association capacities are the same per radio and per AP.

27. Air Defense sensor capabilities are supported on all the 802.11n 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 the Air Defense ADSP appliance, for certain AP platforms:

Network Assurance Toolset when Radio is dedicated as a sensor	**Mobility 6511** ***Note:*** **GUI is disabled and number of SSH sessions is limited to 1**	**Mobility 650**	**Mobility 7131/7131N**	**Mobility 1220, 1240**
Spectrum Analysis	Yes	Yes	Yes	No
Advanced Spectrum Analysis	Yes	No	No	Yes
Live RF	Yes	Yes	Yes	Yes
Live View	Yes	Yes	Yes	Yes
AP Testing	Yes	Yes	Yes	Yes
Connectivity Testing	Yes	Yes	Yes	Yes

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

Network Assurance Toolset with Radio Share	Mobility 6511 *Note:* GUI is disabled when Radio Share is enabled	Mobility 650	Mobility 7131/7131N	Mobility 1220, 1240
Spectrum Analysis	No AP needs to be dedicated to Spectrum Analysis	No AP needs to be dedicated to Spectrum Analysis	No AP needs to be dedicated to Spectrum Analysis	No BR1220 needs to be dedicated to Spectrum Analysis
Advanced Spectrum Analysis	Yes	No	No	Yes
Live RF	Yes	Yes	Yes	Yes
Live View	Yes	Yes	Yes	Yes
AP Testing	Yes	Yes	Yes	Yes
Connectivity Testing	Yes	Yes	Yes	Yes

29. Customers migrating from multi-hop STP mesh in Mobility v4.x to MeshConnex with Mobility v5.x using auto-channel must enable Smart RF. Smart RF must be appropriately configured in this case. The Firewall has been enhanced in v5.4 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 the "**`firewall`**" cli command and disabled using the "**`no firewall`**" command.
30. The number of Critical Resource Monitoring (CRM) policies is limited to 1 for the Mobility 6511 AP and to 4 for the other APs.
31. Due to memory limitations, Telnet is disabled on the Mobility 6511 AP.
32. On the Mobility 6511 AP, when adopted by a controller, the GUI is disabled to make the memory available for other core functions. It is assumed that when an AP is adopted to a controller the controller GUI will be used for its configuration. To re-enable the GUI on these APs - use the "**`memory-profile`**" CLI command. Note that when an adopted BR6511 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: connect to the AP CLI, and set the memory profile to 'standalone' under device override or profile context.

    If APs are currently adopted to controller, then the memory profile configuration change can be applied from controller CLI: connect to Controller CLI, and set the 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-br6511)#**`memory-profile`** (**`adopted`** | **`standalone`**)

General and Multi-Platform Notes From Previous v5.x Releases

33. Wireless controller or AP access protocols are:
    - HTTPS/SSHv2/SNMP -- enabled by default
    - HTTP/Telnet – disabled is by default

34. Important Default Configuration Changes from v4.x to v5.x

Description	v4.x	v5.x
Controller "me1" port default IP address	10.1.1.100 or 192.168.0.1 depending on device	192.168.0.1 for all devices
Auto upgrade enabled	On	Off for RFS9510, On for all other devices
HTTP enabled	On	Off
802.1X AP authentication	On	Off

35. Only two (2) controllers in a cluster are supported in v5.x. Cluster creation has changed in v5.4 as compared to v5.1. To create a cluster in v5.4, 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 the join-cluster <Controller 1 IP> CLI command with username "admin" and the admin password:

    ```
    br-rfs4000-22A3DE#join-cluster 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 the user has to know the admin username and password of Controller 1 makes sure that only the admin can add new controllers to the cluster. To make sure the cluster configuration persists across reboots, enter "`write mem`" explicitly after cluster is formed. The command "`join-cluster`" changes only running-config, not startup-config.

36. APs have a shadow IP address that allows gaining access to the AP if the normal IP address of the AP is not 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. For example:

    AP MAC address - 00:04:96:00:**F0:0A** ➔ AP IP address equivalent – 169.254.**240.10**

    To convert hexadecimal to decimal, you may use the Windows calculator as follows:

    Open the Windows calculator by selecting Start>All Programs>Accessories>Calculator. This menu path may vary slightly depending on your version of Windows.

    With the Calculator displayed, select View>Scientific. Select the Hex radio button.

    Enter a hex byte of the AP's MAC address. For example, F0.

    Select the Dec radio button. The calculator converts the F0 to 240. Repeat this process for the last AP MAC address octet.

37. The default mode for a WLAN is tunnel. For local bridging, please change the configuration to "local bridging".

38. If using an 802.3af 10/100 power injector to power up the 802.11n APs, when plugged into a Gigabit Ethernet wired switch, use a Gigabit Ethernet Power Injector; else, set the link speed to 100 full.
39. WLANs created using Initial Setup Wizard are not applied to the AP300 devices. Workaround: User needs to subsequently map these WLANs for AP300 devices.
40. When experiencing high number of handshake failures with AP300s, it is recommended to set "`wpa-wpa2 handshake priority normal`" in the WLAN.
41. Features available/not available on a Mobility 300 AP, when in a v5.x deployment:
    a. It is not a site survivable Access Point, and will operate as a thin port without any mesh, local bridging or forwarding capabilities- similar to Mobility v4.x.
    b. Roaming will work in a mixed AP environment – should be on the same L2 segment.
    c. To make bulk changes to adopted Mobility 300 APs, please use config-ap300 {} from the CLI.
    d. Multi-country support is available for the Mobility 300.
    e. AP300 is not seen as a device in the tree hierarchy, but under the controllers, when the controller is the RF Domain Manager. The AP300 cannot be an RF Domain Manager.
    f. Sensor conversion from the controller is not support. However, if the deployment is being upgraded, and the APs were previously converted to dedicated WIPS sensors for Air Defense WIPS, then they will continue to function as sensors.
    g. **AP license type** is required for AP 300 adoption, with the following capacities per controller:

       RFS 4000: 6

       RFS 6000: 48

       RFS 7000: 256
    h. Features not supported:
        i. Unlike the .11n APs in Mobility v5, AP300 continues to be a thin port with all traffic being tunneled through the controller. It is not able to forward traffic locally.
        ii. L3 Mobility
        iii. SMART RF/ Self Healing
        iv. SMART Band Control will not be available
        v. No Secure WiSPe
        vi. Dual Image bank
        vii. Does not have a profile
        viii. Does not have the L2/L3 firewall on the AP, it resides on the controller.
        ix. Sensor conversion is not available through the controller. However, if upgrading an existing installation where the AP300 was a sensor, it would continue to be sensor, as long as it is not plugged into controller for adoption.
        x. Will not support the remote packet capture like the .11n APs in Mobility v5
42. AP adoption: APs are adopted based on valid SKU identification strings, once discovered under the Auto-provisioning policy. The SKU identification string is a manufacturing-programmed string that most typically is a combination of the model number and authorized regulatory domain. An AP with a mismatched identification string still gets adopted by the controller, but its radio(s) are not enabled.

43. If the system flash is full (from either packet traces, crash files or ap-images), there may not be enough space left on the device to create hotspot pages. In this case, users must clear enough space from flash to allow hotspot pages to be created. Use the '`service clear crash-info`' or '`delete <filename>`' CLI commands.
44. RADIUS authentication of management users uses a different configuration model from v5.0. So if upgrading from 5.0 to 5.2 or higher and radius authentication for management access is used, 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).
45. 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 configurations may lead to decisions that could cause clients to NOT associate on a certain WLAN.
46. The controller install wizard is available only on the Mobility RFS4000 controller.
47. Multi-cipher support: Some clients keep on sending de-authentication requests when associated to WEP security WLAN in multi-cipher configuration. Please use different BSSIDs for different ciphers with the same WLAN.
48. Commit is not allowed with a radio configuration having two WLANs mapped with different data rates, as this is not a supported configuration.
49. 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.
50. AP radios will not beacon unless a country code setting is provided. Please use the GUI wizard, the GUI, or the CLI of the controller, if any, or of the AP to enable country code and change password.
51. When using the 3G WWAN functionality on the Mobility RFS4000 or Mobility 7131N (via an Express Card adapter):
    - Hot-swapping of the 3G cards, once plugged in and operational is not recommended, as it may cause a system panic.
    - Before unplugging the card, please make sure you "shutdown".
    - If you encounter a panic doing hotplug, power off the device for one minute.
    - To troubleshoot 3G issues from the AP CLI:
        - Enter "**`debug nsm all`**" to see more detailed debugging messages about 3G.
        - If the card does not connect within a couple of minutes after "**`no shutdown`**", check syslog for "`detected ttyUSB0 No such file`". If that's the case, reseating the card should clear the issue.
        - If the card has difficulty connecting to the ISP, i.e. syslog shows that it retries LCP ConfReq for a long time: Check if the SIM card is still valid and is plugged in correctly.
    - To configure:

      Verizon PC770 & Sprint C777: `at$nwautoinstall=0`

      Option Ultra Express & Vodafone 3730: `at_oifc=3,1,1,0`
    - To query/verify:

      Verizon PC770 & Sprint C777: `at$nwautoinstall?`

Option Ultra Express & Vodafone 3730: `at_oifc?`

52. Role Based Firewall configuration is not available on the Standalone APs or on the Virtual Controller APs.
53. The VPN feature has been re-implemented in Mobility v5.3 to provide a common, more optimized implementation on controllers and APs. Please use the offline CFGCV configuration migration utility when upgrading from a v4.x release to v5.4.x. It is recommended that you save your old VPN configuration to assist in possible downgrades. Please see the follow-on note on which VPN configurations cannot be converted using the migration utility, as they are not supported in v5.3. In particular, note that configurations containing AH and DES as IKE encryption algorithm cannot be migrated. For upgrades from v5.1.x or v5.2.x to v5.4.x, the VPN configuration migration is performed automatically – the offline configuration migration tool is not required.
54. IPsec VPN – The primary VPN implementation differences in comparison to controllers on v4.x or v5.2.x are:
    a. Authentication Header (AH) is not supported in v5.3.x, but was supported in v4.x VPN. Use ESP instead of AH.
    b. L2TP over IPsec is not supported in v5.3.x, but was supported in v4.x VPN. v5.3.x supports XAUTH and can be used with IPsec VPN clients. XAUTH has been tested with Cisco and Safenet VPN clients.
    c. IKEv2 was not supported in v4.x, but is now supported in v5.3.x.
    d. Transport mode is only supported for host-to-host rule, in other cases it will fall back to Tunnel mode.
    e. Transport mode NAT-Traversal is not supported for IKEv1 and IKEv2 in v5.3.x. This is supported in tunnel mode.
    f. 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.
    g. The value of Kilobyte expiry of an IPSec SA (security-association lifetime kilobytes) can be configured to be 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 a very low value, the tunnel will end up in an indefinite rekeying IPSec SA state. This value has to be determined 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 v4.x features is expected to be minimal.
55. IPsec VPN statistics: The following SNMP tables are not available for VPN statistics via SNMP – they will be implemented in a future release – wingStatsDevVpnIpsecSaTable, wingStatsDevVpnIpsecSaTrafficSelectorTable, wingStatsDevVpnIkesaTable
56. Auto-tunnel for VPN:
    a. A single group id/PSK is supported on 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.

57. 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
58. If using TFTP to upgrade a Mobility 6511, please configure the following settings on the TFTP server:
    a. Per packet timeout in seconds: 15
    b. Maximum retries: 20
59. 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)
60. Auto assign sensor is not available for BR6511 – since this feature requires a reboot on low memory devices, which cannot be done with Smart RF enabled.
61. For IGMP Snooping version v2, v3, source specific multicast is not supported; this will be addressed in a future release.
62. 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.
63. When AP gets adopted by a controller, the clock is not getting synchronized with the controller clock immediately. It happens over period of time which may vary based on time difference.

Mobility RFS7000 Notes

64. The CF card slot of the Mobility RFS7000 controller is enabled for controllers with a hardware revision that is Rev C or later and disabled for earlier hardware revisions. The two USB ports on the controller can be used for directly attached external storage devices with all revision of the controller hardware.

Mobility RFS6000 Notes

65. A license key is no longer required to enable the Express Card 3G WWAN radio support on the controller.

Mobility 650 Notes

66. The antenna power table has been updated. Users should confirm power settings.
67. After upgrade to v5.4, both the amber and green LEDs of the Mobility 650 will be ON solid while the AP is adopted and not yet configured.

Mobility 7131/7131N Notes

68. The Mobility 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.

69. For the Mobility 7131/7131N, the ge1 and ge2 ports are mapped to vlan1 and vlan1 has its primary IP configured for DHCP and its secondary IP configured for zeroconfig. In addition, unlike with v4.x, a Mobility 7131/7131N with v5.x can bridge traffic between ge1 and ge2. Other important default configuration changes from v4.x to v5.x for Mobility 7131/7131N are:

Description	4.x	5.x
GE2(WAN) default IP address	10.1.1.1	Zeroconfig with DHCP client
GE1 (LAN)	DHCP client	Zeroconfig with DHCP client
Auto upgrade (Upgrade f/w, apply config)	Enabled	Enabled
.1x authentication	Enabled	Disabled. Enabled once username/password are configured.
Firewall	Enabled	Disabled for L2 and L3
Link Aggregation	N/A	Disabled

70. 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, 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 dual radio models:

Available Power Radio	Resources	Ethernet Port Configuration
Power Status: 3af (12.95W)	2 Radios	GE1 10/100/1000
Power Status: Mid Power (18W)	2 Radios	GE1 10/100/1000 GE2 10/100
Power Status: Full Power (24W)	2 Radios	GE1 10/100/1000 GE2 10/100/1000

The following table shows the radio and LAN resources available under various power configuration modes for the tri-radio models:

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	GE1 10/100/1000 GE2 10/100/1000

	radios at lower power)	
Power Status: Full Power (30W)	3 Radios (with Express Card)	GE1 10/100/1000 GE2 10/100/1000

Defects

Closed Defects

SPR #	Description
26060	Cisco ISE posture validation and provisioning with eap as authentication
26107	MAC address of the VM installed on primary NX95XX is the same as the Base MAC of the secondary NX9510 in cluster.
26119	Mobile users will not be redirected to the captive portal "no service page" if DNS server is unreachable.
26126	Failure to configure critical resource with space in the name thru GUI
26238	Override-wlan wpa-wpa2-psk command under RF-domain will not accept pre-shared key in clear text format
26245	Add for Controller Hostnames under AP profile is not present, unless "allow adoption of this controller" is enable
26247	Rim process memory leak on a standalone AP7131 (no mint links), when at least 9 MUs roam from a particular AP to 9 different APs.
26337	Receiving AP is failing to install the migrated snoop entries on client roaming.
26361	When AP has more than 16 aliases configured – CFGD process on the AP fails to start and AP can’t adopt fully.
26383	SWiFT UI: not able to edit WLAN
26426	command http_analyze doesn't accept URL with more than 64 characters
26440	With the me1 link up, when the controller boots - me1 interface by default shows a high value of output
26443	Active-Standby LED state change is not in sync with the cluster status
26444	AP 6511 is showing large output unicast statistics.
26448	ID Theft Out of Sequence alarm on AP sensor after upgrade to 5.5.x
26470	Corrupted bonjour packets are leading to a reboot of controller.
26479	When modifying Alias ACL statement, unmodified ACLs gets corrupted
26481	Factory defaulting NX 95xx controller does not delete unified mode ADSP VM instance.
26484	Multicast frames going out before beacon with DTIM 0 goes out due to which clients fail to get all multicast frames
26524	Random RIM cores on the AP when processing bad DHCP request/renew with illegal option fields.
26582	AP 71xx: Maximum radio power not tied to radio band but tied to radio number
26592	WEP 128 legacy pre-share key authentication fails
26594	POODLE SSL v3 exploit in WING WEB interface
26595	Unauthorized access to captive portal.
26649	When interesting traffic is defined by a network using VLSM, on the NX controllers, the tunnel comes up with a wrong subnet value.
CQ 203140	NX controllers: Remote exploit vulnerability in bash program.

SPR #	Description
CQ 203158	MiNT packet corruption in AP discovery can prevent AP from adopting to the controller
CQ 203136	When WLAN is removed and added - data is not forwarded to external analytics.
CQ 201666	Roam-assist policy enhancements - added roaming aggressiveness
CQ 203362	"show wireless meshpoint neighbor statistics rf" causes rim core
CQ 202259	Introduce device list confirmation for the exectution of command 'service clear wireless dns-cache on <rf-domain>'
CQ 202977	Captive portal: no service page AP doesn't need direct connection to the DNS, CRM can be on the controller
CQ 203156	When radio 1 on AP 1220 configured as WLAN and radio 2 as sensor - sensor only scans on 2.4Ghz.
CQ 201757	Smart-rf report should include interfering AP and neighbor information.
CQ 203262	Windows 7/8 when acting as 802.1x clients has 20 minute hold time which can cause AP not finish authentication
CQ 201222	Device upgrade issued for a site through rf-domain, selects only APs when the site controller image is not present.
CQ 201135	Date and time options added to reload command
CQ 201834	Acct-session-time drifts during roaming.
CQ 203050	Wipsd core dump when sensor frequently is re-connecting to appliance.

Open Defects

While these defects are still formally "open", they are unlikely to impede Brocade customers in their deployment of this release, and have been deferred to a later release.

CQ/ SPR	Headline	Comments
25851	FREE_RAM_DISK Free system: file system space, 8.9% is less than limit 90.0%	No operational impact. Added additional information for tech support dump in WiNG 5.5.5 to better understand the issue.
26180	AP 1240 fails to boot properly off Cisco POE only switch like 3560G when LLDP is configured	Disable LLDP on Cisco ports, allow APs to boot and then disable LLDP in AP profile as well as set the power to 3af mode.
CQ 203477	GUI can't read default event policy values	When creating modifying events in the event policy – mark state for each event as most events are enabled by default.