



Unleashed

Troubleshooting Guide

Part Number: 800-71503-001 Rev A
Published: 20 April 2017

www.ruckuswireless.com

Contents

Copyright Notice and Proprietary Information.....	3
1 Introduction	
About this Guide.....	4
2 Troubleshooting	
Initial Deployment Considerations.....	6
Understanding Master AP Election.....	9
Troubleshooting the Gateway Feature.....	13
Performing Firmware Upgrades.....	16
Troubleshooting Client Authentication Issues.....	17
Wireless Mesh Considerations.....	19
Using the Management Interface.....	21
Configuring DHCP Service.....	22
General Configuration Questions.....	24
Debugging.....	25
Reporting an Unleashed Issue.....	29

Copyright Notice and Proprietary Information

Copyright 2017. Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be used, reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus.

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, BeamFlex, ChannelFly, Dynamic PSK, FlexMaster, Simply Better Wireless, SmartCell, SmartMesh, SmartZone, Unleashed, ZoneDirector and ZoneFlex are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Introduction

1

About this Guide

This document provides basic troubleshooting information for diagnosing common issues with Unleashed APs and Unleashed networks.

For users who are already familiar with Ruckus ZoneDirector systems, the Unleashed troubleshooting methods are generally similar. Where they are different, this guide provides details on the differences.

This guide contains a collection of common questions and answers about Unleashed network deployments. Common issues include initial deployment issues, Master AP selection/election issues, using the Gateway feature, upgrading the network, mesh-related issues and DHCP-related issues.

Initial Deployment Considerations

Q: I just received my Ruckus Unleashed APs. How do I set up my Unleashed network?

A: You can configure one Unleashed AP as your initial Unleashed Master AP by following any of the three methods described below. Once the Unleashed Master is configured, simply connect other Unleashed APs to the same network and they will automatically become member APs and form your Unleashed Network.

Use any of the following options to configure the initial Unleashed Master AP:

Option 1: Using a Wi-Fi client device

1. As soon as the Unleashed AP boots up and is connected to a local network, it begins broadcasting a temporary unencrypted WLAN with an SSID named **Configure.Me-xxxxxx** on both radios. The "xxxxxx" is the last 3 octets of the AP's MAC address.
2. Using your wireless client's Wi-Fi configuration settings, select and associate to the **Configure.Me-xxxxxx** WLAN.
3. Launch a web browser and enter the following into the browser's URL bar: **unleashed.ruckuswireless.com**, and press Enter.

NOTE For Unleashed release 200.5 and later, you can enter any domain name.

4. Select **Create New Unleashed Network** and click **Start** to begin.
5. The **Configuring Unleashed Master** progress screen displays the progress. Wait until the initialization process completes.
6. Once initialization completes, ensure that client device is still connected to the **Configure.Me-[xxxxxx]** WLAN, and click **Next**.
7. The browser will be redirected to the **Unleashed Setup Wizard**. Follow the instructions to configure your initial Unleashed Network.

Option 2: Using a wired client device

If you have some way to learn the Unleashed AP's IP address, or are able to discover the Unleashed AP on your Microsoft Windows network using UPnP, or Apple Mac OS network using Bonjour discovery, you can set up the Unleashed network using a wired client using the following procedure:

1. Connect the client device to the same network as the Unleashed AP with an Ethernet cable. Make sure the client can ping the Unleashed AP's IP address.
2. Launch a web browser and enter the Unleashed AP's IP address, and press **Enter**.
3. Select **Create New Unleashed Network** on the browser screen and click **Start** to begin.

4. The **Configuring Unleashed Master** progress screen displays the progress. Wait until the initialization process completes.
5. Once initialization completes, click **Next** button.
6. The browser screen will be redirected to the **Unleashed Setup Wizard**. Follow the instructions to configure your initial Unleashed network.

NOTE Note: You may be able to find the Unleashed AP's IP address by checking your DHCP server's leased address list. For Unleashed 200.5 and later releases, UPnP and Bonjour services are enabled in an Unleashed AP when it is in factory default state. Windows devices can detect Unleashed APs on the **Window Network**. Apple devices can detect the Unleashed AP using Bonjour service by searching for the service type: **_ruckus-unleashed._tcp**.

Option 3: Using the Unleashed Mobile App on a mobile device

Install the **Ruckus Unleashed Mobile App** on your mobile device, open the app, select **Typical Install**, and follow the instructions.

Q: My Wi-Fi device successfully connects to Configure.Me_XXXXXX WLAN but the device cannot reach the Unleashed AP's web UI. What should I do?

A: The Unleashed AP provides DHCP service on the **Configure.Me_XXXXXX** WLAN, therefore the connected client is expected to receive a dynamically assigned IP address automatically. If the client device is configured to use a static IP address (either configured for this WLAN or for a different WLAN), the client device may be unable to connect to the Unleashed AP. The easiest way is to configure the client's Wi-Fi interface to obtain a dynamic IP address from DHCP.

NOTE Note that different Unleashed AP releases offer IP addresses in different ranges, as shown in the following table. If the wireless device cannot receive an IP address, an alternative is to statically set the IP address to be in the same subnet as the AP, allow the device to connect to the AP, and then proceed with setup troubleshooting steps. Another potential cause of network issues is if the local wired network happens to be in the same subnet as the AP's WLAN IP subnet.

Table 1: Unleashed IP addresses by release

Unleashed release	AP's WLAN interface IP address	Client IP address range	Remarks
200.0	192.168.101.1	192.168.101.31~.253	The LAN network IP addresses cannot overlap with 192.168.101.1/24, otherwise network reachability issues can occur.

Troubleshooting

Initial Deployment Considerations

Unleashed release	AP's WLAN interface IP address	Client IP address range	Remarks
200.1, 200.2, 200.3	169.254.1.1	169.254.1.31~.253	Some Apple devices (incl. iPhone and iPad) don't work well with IP addresses assigned in this subnet. Therefore, the Unleashed Mobile App on these devices may encounter errors when setting up an Unleashed network.
200.4 and later	10.154.231.125	10.154.231.130~.180	Under the assumption that this address most likely will not overlap with customers' LAN IP assignment.

Q: My device can access the Unleashed web interface, but it fails in running the Setup Wizard. What can I do?

A: Try to access the web UI or factory reset the Unleashed AP and restart the initialization process again. If the process still fails, please follow the issue reporting method at the end of this document to report the issue.

Q: Do all Member APs need to be upgraded to join a Master AP that is running a different Unleashed image version?

A: Yes, the member APs must be upgraded to the exact same version as the Master AP to form an Unleashed network. Fortunately, in most cases you can simply connect the member APs to the same subnet as the Master AP, and as long as the Unleashed Master AP can reach the Ruckus firmware image server, firmware upgrades for all connected APs will be performed automatically.

Q: I have multiple Unleashed APs that potentially can have different image versions installed. How do I check their version numbers and perform the firmware upgrades before installation to avoid any potential problems?

A: Before running the Unleashed setup, you can connect to the AP via SSH and run the following CLI commands:

- To check AP version: `get version`.
- To upgrade an image from the AP CLI, one easy way is to load the AP image onto a TFTP server, and then use the following commands:
 - `fw set control <image file name>`
 - `fw set proto tftp`
 - `fw set host <TFTP server address>`
 - `fw update`

Q: I have an Unleashed Network running already and plan to add a new AP to the network. However, the new AP doesn't seem to be able to join the existing Unleashed Network. What should I do?

A: If the new AP is loaded with the same firmware version as the existing Unleashed Master AP, but the new AP cannot be seen on the Master AP's web UI, the issue is most likely caused by one of the following reasons:

- The new AP failed to receive a valid IP address. Check your DHCP server.
- The new AP is connected to a different network from the existing Unleashed network. Make sure the AP is connected to the same subnet as the existing Master AP.
- The new AP already has configuration on it. In this case, factory reset the AP by using a pin to push into the "Reset" hole for 10 seconds while the AP is powered on.
- The total number of APs in the Unleashed AP has reached its maximum. Currently an Unleashed network can have up to 25 APs.

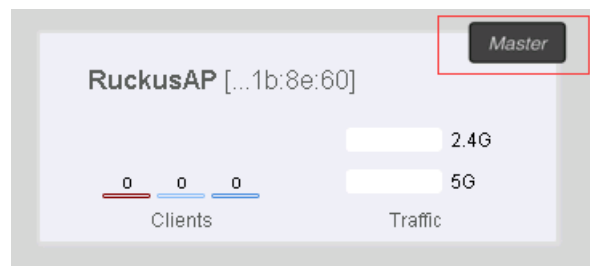
If the new AP is loaded with a different Unleashed image, the Master AP will try to upgrade the new AP's firmware to match that of the Master using images stored on the Ruckus firmware server. In this case, you should check the following:

- Ensure that the AP model of the new AP is supported by the version that the Master AP is running. If not, you will need to upgrade the existing Unleashed Network first, for the new AP to participate.
- Ensure that the Master AP can reach the Ruckus image server so it can locate the appropriate image and instruct the new AP to install it.
- Alternatively, download the desired AP image onto an administrative PC and upgrade the new AP image by using AP CLI in an SSH session.

Understanding Master AP Election

Q: How do I identify which AP is the Master AP?

A: The CTL LED of the Master AP is solid green all the time. On the Unleashed web UI, the Master AP is marked as the following. The similar display is in the Unleashed Mobile app as well.



Q: Is it possible to force an Unleashed AP to be a Member AP?

Troubleshooting

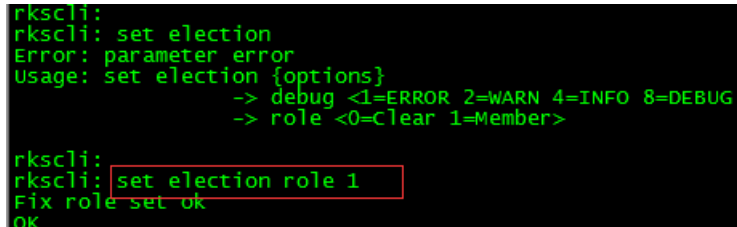
Understanding Master AP Election

A: An AP can be set to never become a Master using the AP CLI. To configure an AP to always assume the role of member, SSH to that AP and issue the following AP CLI command:

```
set election role 1
```

To clear the setting, use the following AP CLI command:

```
set election role 0
```



```
rkscli:
rkscli: set election
Error: parameter error
Usage: set election {options}
       -> debug <1=ERROR 2=WARN 4=INFO 8=DEBUG
       -> role <0=Clear 1=Member>

rkscli:
rkscli: set election role 1
Fix role set ok
OK
```

Q: Is it possible to designate a specific Unleashed AP as the Master AP?

A: Starting with release 200.5, you can configure an AP to be the "preferred Master." Prior to release 200.5, the only option was to set all other APs as Member APs via CLI command. By default, without any specific configuration, Unleashed APs automatically elect the most appropriate AP to be the Master AP.

Q: What will happen if the Master AP is disconnected or goes down?

A: Once Unleashed APs fail to contact the Master for 30 seconds, the election mechanism will start and a new Master AP will be elected. During this period of time, existing wireless clients may remain connected but no new clients can associate with the WLAN.

The exception is if the Gateway function is enabled (only possible on the Master AP). In this case, Master AP election will not happen because the Gateway AP needs a physical WAN connection and no other APs can automatically replace it.

Q: In case the Master AP is disconnected, how long will it take for the Unleashed Network to resume operation?

A: The WLAN service is impacted for about 80 seconds, however Member APs will only have WLAN downtime for a few seconds.

Once APs lose connection to the Master AP for 30 seconds, the new Master AP election starts. Afterwards member APs will join this new Master AP and receives configuration from it. The process takes about 40 seconds. However, even if a Member AP loses its connection to the Master, the existing WLAN service continues, although new clients will not be authenticated during this period of time. When a new Master AP is elected, a Member AP will experience WLAN down time for a few seconds before normal operation is resumed.

Q: Will the old configuration be lost if the Master AP is disconnected from the network?

A: No. For Unleashed 200.2 and later releases, all member AP's keep a copy of the configuration, and when a new AP is elected as the master, it restores the configuration from this copy.

In Unleashed 200.0 and 200.1 releases, the Standby Master AP stores the configuration, and it may take the Master AP role if it loses connection to the Master AP.

Q: What are the Master AP election criteria?

A: The decision factors include the following:

1. Initial setting (the first AP that is configured to be the Master)
2. Manually configured preference (supported in 200.5 and later release)
3. Member AP only role configured by AP CLI command
4. Processing power of the AP model
5. Free memory size
6. Mesh role (only Root mesh AP can be a Master)
7. If mesh is enabled, the number of downlink Mesh nodes (the less the higher the chance to be the Master AP)
8. AP system up time (the longer the higher the chance to be a Master AP)
9. MAC Address as the last arbitrator

Q: Can a Mesh AP be elected as the Master AP?

A: A Mesh AP, which has no Ethernet connection for uplink, cannot assume the role of Master AP.

Q: I cannot see any Unleashed web interface displayed in my browser. It seems there is no AP assuming the role of Unleashed Master AP. How do I investigate the situation?

A: Make sure the administrative PC is on the same network as the Unleashed Network, and enter the following URL <http://unleashed.ruckuswireless.com> in the browser. You should be redirected to the Unleashed Web UI.

Note that if mesh is enabled on your network, only Root APs (i.e., APs connected to the Internet through a wired interface) can become the Unleashed Master AP. One of the criteria to be a Root AP is that the AP can contact its gateway through a wired interface. Therefore, if your network's default gateway becomes unreachable, none of the Unleashed APs can be the Root AP of the mesh network, and then there will be no Unleashed Master on your network. The exception to the above is when the **gateway** function is enabled; in this case the Gateway AP is the Master AP regardless of whether mesh is enabled, or whether its gateway is reachable or not.

If the above doesn't apply to your situation, figure out any AP's IP address, and enter "http://<any AP IP address>" in the URL bar of your browser to access the Unleashed web interface.

If there is still no response (and one of the APs' IP addresses is known), you can SSH into the AP and perform the following:

Type the "get election" AP CLI command. It shows the status of all Unleashed APs, and should display one AP marked as **Master**. Ping that AP's IP address from a device

Troubleshooting

Understanding Master AP Election

connected to the same network. If the AP is not reachable, maybe there is an access denial policy configured on your network in one of your devices. If the AP is responding, type that AP's IP address in a browser's URL bar and check whether the Unleashed web UI can be displayed.

```
kscli:
kscli:
kscli: get election
The local AP's ip address is 172.18.171.3, Election role is master, Fix role is NO, debug level is ERROR
-----
mac_address ipaddress role configID station_rate free_memory mesh_enabled mesh_node mesh_node_type model version bak_version systime
board_type last_seen
f0:b0:52:39:ce:20 172.18.171.3 master 37 48 149868 0 0 0 R500 200.5.10.0.20 200.2.9.13.186 2596 zf7752-3-29-4bss Thu Mar 16 10:35:20
2017
44:68:4d:25:86:70 172.18.171.15 member 37 48 164936 0 0 0 R500 200.5.10.0.20 200.3.9.13.148904240 0 zf7752-3-29-4bss Thu Mar 16 10:3
5:18 2017
#
```

If mesh is enabled, issue `get mesh` to check the mesh status. Only an AP in "ROOT" mesh mode can be the Master AP.

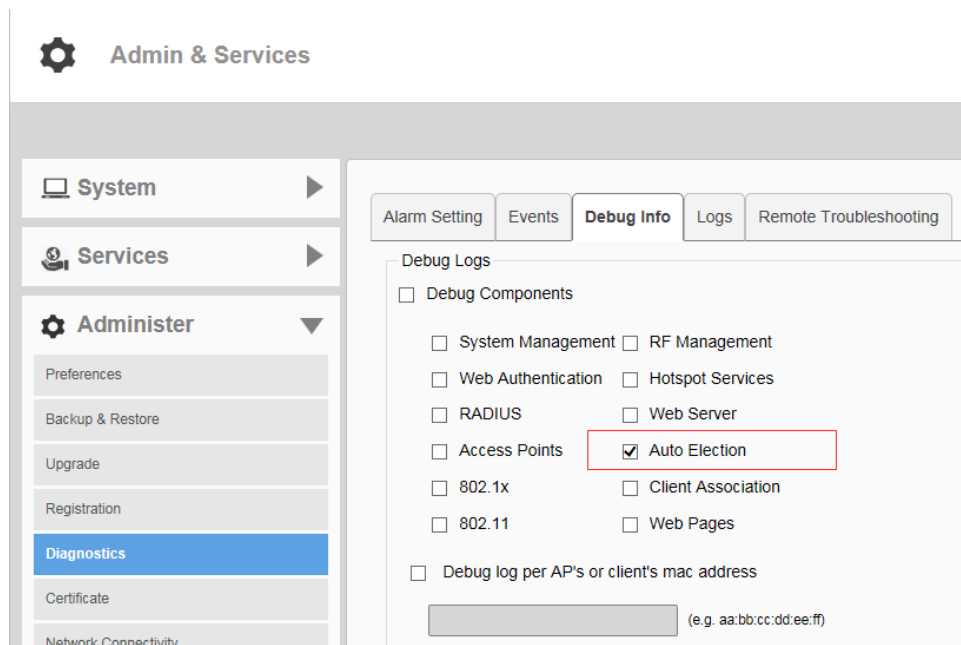
If everything looks fine, but the network still doesn't seem to have an AP assuming the Master role, you may need help from Ruckus customer support. Follow the issue reporting procedure described at the end of this document to report the problem.

Q: What will happen if a disconnected Master AP is reconnected back to the network after a new Master has been elected?

A: The two Master APs will communicate with each other to elect one AP to serve as the Master, and the other AP will become a Member AP and join the master.

Q: How do I enable debugging logs for Master election?

A: Go to **Admin & Services > Administer > Diagnostics > Debug Info**, and enable the **Auto Election** debug component.



Alternatively, SSH to an Unleashed AP and manually turn on election log debugging on that particular AP using the following AP CLI command:

```
set election debug X
```

where X is a number representing the debug level: 1 means to only show messages in case of error. 8 means generate all messages for debugging purposes.

```
rksccli:
rksccli: set election
Error: parameter error
Usage: set election {options}
-> debug <1=ERROR 2=WARN 4=INFO 8=DEBUG
-> role <0=Clear 1=Member>

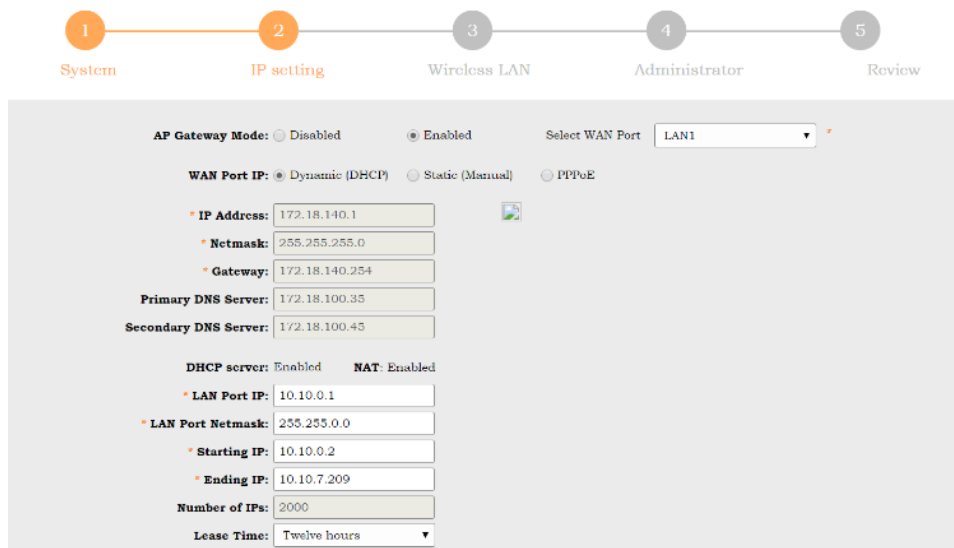
rksccli:
rksccli: set election debug 8
Debug level set ok
OK
```

Troubleshooting the Gateway Feature

Q: How do I setup the Unleashed Gateway Network?

A: There are 2 ways to enable the Gateway feature:

- Option 1: Enable AP Gateway Mode while running the initial **Setup Wizard**:



- Option 2: From the Dashboard, go to **System > IP Settings** and enable **Gateway Mode**.

Troubleshooting

Troubleshooting the Gateway Feature

The screenshot shows a web-based configuration interface. On the left is a sidebar menu with categories: System (containing System Info, IP settings, System Time, Country Code, Roles, Users, Mesh), Services, and Administer. The main content area is titled 'IP Settings' and has sub-tabs for Management Interface, DHCP Client List, and Preserve DHCP Client IPs. A note at the top states: 'If Unleashed was assigned static network addressing, click "Manual" and make the correct entries. If you click "DHCP", the system will automatically configure the network settings.' Below this, there are three radio buttons for 'Gateway Mode': Manual (selected), DHCP, and PPPoE. A 'WAN Port' dropdown menu is set to 'LAN1'. The configuration fields include: IP Address* (172.18.140.3), Netmask* (255.255.255.0), Gateway* (172.18.140.254), Primary DNS Server* (172.18.100.35), Secondary DNS Server (172.18.100.45), DHCP server (Enabled), NAT (Enabled), LAN Port IP Address* (192.169.0.1), LAN Port Netmask* (255.255.0.0), Starting IP* (192.169.0.2), Ending IP* (192.169.7.209), Number of IPs (2000), and Lease Time (Twelve hours).

Q: On the Gateway AP, can I configure more than one port to be the WAN port?

A: No. Only one Ethernet port can be configured as the WAN (wide area network) port for the unleashed gateway.

Q: Once a gateway AP is configured, can I choose a different Unleashed AP to be the Gateway AP?

A: No. The Gateway AP has to be the Master AP, and one Ethernet port should be configured as the WAN port, which acts as the backhaul link for the Unleashed network.

Q: If the Gateway (and Master) AP is down, how do I recover the network?

A: In 200.3 and 200.4 releases, if the Gateway/Master AP is out of service, the user should pick a member AP to serve as the Gateway AP, reset it to factory defaults, and re-configure it as the new Master/Gateway AP.

With release 200.5, a new recovery mechanism has been introduced: If the Master/Gateway AP fails for any reason, the customer can use an existing Member AP to replace the previous Master AP. To do so, connect the previous Master AP's Ethernet cable to this member AP and allow it to set up the desired network topology. This member AP will become the new master after 3 minutes automatically, and will establish an Unleashed network with all of the previous configuration settings. The detailed procedure and screen shots will be provided in a later version of this document, when the implementation is finalized.

Q: My AP only has one Ethernet port. Can it be used as a Gateway AP?

A: Yes, APs such as R310 and T300 that have only one Ethernet port can also be configured in Gateway mode. If mesh is supported on the AP model (such as the T300 series), the AP can also be the gateway for any wired or wireless clients of any downlink mesh APs. The R310 does not support mesh, so it will be unable to serve as a Root AP, and would therefore only be able to service Wi-Fi clients, in this scenario.

Q: Should the DHCP Server function be enabled on the Gateway AP?

A: Yes, the internal DHCP server must be enabled on the Gateway AP. The Gateway AP provides IP addresses for all APs and clients.

Q: How is the IP address of the Gateway AP's WAN interface assigned?

A: There are 3 ways to assign the IP address of a Gateway AP's WAN port:

- By an external DHCP server.
- Manually configured.
- By an external PPPoE server.

Q: Can a Member AP join the Gateway/Master AP through the WAN port of the Gateway/Master AP?

A: No. A member AP can only join a Gateway/Master AP from the Gateway/Master AP's LAN port, and, there should be only one Unleashed network in one IP subnet.

In 200.3 and 200.4 releases, this topology restriction is not enforced; that is, a customer can still set up such an unsupported topology.

Starting from release 200.5, the LWAPP service will be disabled on the WAN port of the Gateway AP. Therefore, all discovery packets coming from a Member AP will be ignored on the Gateway/Master AP.

In either case, the "outer" AP may assume the Master role and cause the Unleashed UI to display confusing information.

Q: Can I set WAN and LAN addresses of the Gateway AP to be in the same subnet?

A: No, the IP address range of the WAN network and the IP address range of the LAN network cannot overlap with each other.

Q: If Gateway mode is enabled, how is the IP addresses assignment accomplished for APs and clients?

A: All Member APs and clients obtain their IP addresses from the Gateway/Master AP's internal DHCP server.

Q: How do I investigate issues with Member APs or clients failing to receive an IP address?

A: You can check the following:

- Ensure that the Gateway feature is enabled and the DHCP service is properly configured.
- Check that the client is configured to use a DHCP-assigned IP address.
- Capture all DHCP packets to better understand the root cause.

Q: Can mesh be enabled while Gateway mode is enabled?

A: Yes. Mesh is supported in gateway mode with the caveat that, in 200.3 and 200.4 releases, if PPPoE is enabled, mesh can be enabled, but the Master AP itself won't enable its mesh downlink. All member APs can serve mesh normally. This restriction will be removed in 200.5 and later releases.

Performing Firmware Upgrades

Q: When should I use online upgrade and when should I use local upgrade to upgrade my system?

A: Online upgrade is the recommended way to upgrade the Unleashed network. However, it requires the Unleashed network to be able to reach to the Ruckus Image server.

Local upgrade can be useful in some situations, including:

1. No or very limited Internet access from the Unleashed network.
2. For some reason a special image version is needed, which is not included in the supported online upgrade images.

Q: How do I know which firmware versions are available for online upgrade?

A: On the Unleashed web UI, go to **Administer** -> **Upgrade**, you will see a version dropdown list.

Current firmware version 200.2.9.13.14685531.

Select upgrade method:

Online Upgrade (Download firmware from Ruckus Wireless) Local Upgrade (Upload firmware from local PC)

Select firmware version:

200.2.9.13.100

Upgrade

Auto reboot the system

AP Role	Name	Mac	Model	Upgrade Progress
Master		6c:aa:b3:3d:64:30	R500	
Member		d4:68:4d:20:02:70	R710	

Q: What is the effect of the "Auto reboot the system" option shown on the Upgrade page?

A: When "Auto reboot" is enabled, all APs will reboot automatically after a successful image upgrade to make the new image version effective. Alternatively, the user can opt to manually reboot all APs at a more convenient time.

Q: Can an Unleashed AP join an Unleashed Network running a different firmware version?

A: If the existing Unleashed network can reach the Ruckus image server and support the new AP model, the new AP's image will be updated to be the same as the image version of the existing network.

If the new AP model is not supported, you will have to upgrade the image version of the existing Unleashed network first to an image that can support the AP model of the new AP.

Q: What do I do if the firmware fails to download during the online upgrade?

A: Make sure your Internet connection is working well, then press the **cancel** button on the Upgrade page to retry. The alternative is to find all required images from Ruckus Support site (support.ruckuswireless.com) and download the images to your administrative PC, and use local upgrade instead.

Q: What should I do if some APs fail to upgrade their images?

A: On the Unleashed Web UI, go to **Access Points** page, make sure the AP is still in **Working** state. Then press **Cancel** to retry. If it still does not work, reboot the AP and retry.

Q: I want to downgrade Unleashed Network to its previous version. How do I do it?

A: Image downgrade is supported only by using the local upgrade method. You will have to download your previous image files, and run local upgrade on each AP. Also note that downgrade sets the system to factory default state to avoid configuration inconsistency.

Q: Where can I find the Unleashed images for local upgrade?

A: You can visit the Ruckus Support website site (support.ruckuswireless.com), login with your customer account, and then search for Unleashed AP images.

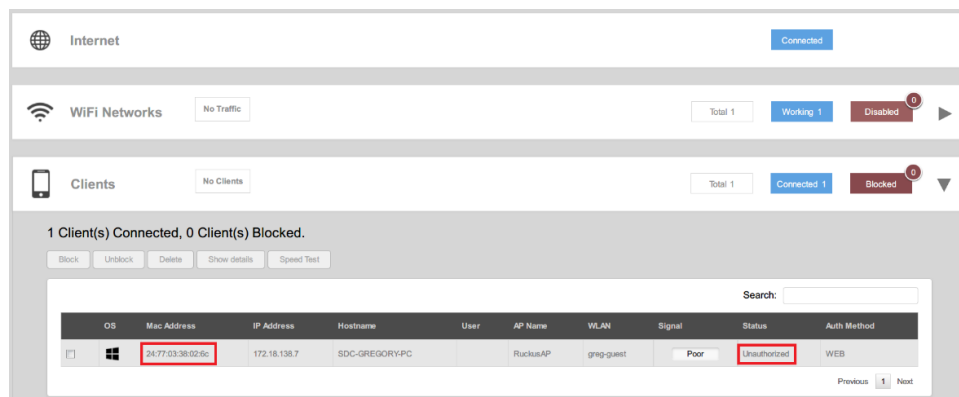
Q: What will happen if in the middle of an image upgrade the network connection on my administrative PC goes down?

A: As long as AP's connection is intact, the upgrade should continue in the background. Simply visit the Upgrade page to see the progress.

Troubleshooting Client Authentication Issues

Q: If the users of Guest or Hotspot (WISPr) WLAN claim their device cannot access the login page, what can I check?

A: First, you can go to the Unleashed web UI and check the Clients list to see whether the client is shown:



The screenshot shows the 'Clients' section of the Unleashed Web UI. It displays a table with one client listed. The client's status is 'Unauthorized', which is highlighted with a red box. The client's Mac Address is also highlighted with a red box. The table has columns for OS, Mac Address, IP Address, Hostname, User, AP Name, WLAN, Signal, Status, and Auth Method.

OS	Mac Address	IP Address	Hostname	User	AP Name	WLAN	Signal	Status	Auth Method
Windows	24:77:03:38:02:fc	172.16.138.7	SDC-GREGORY-PC		RuckusAP	greg-guest	Poor	Unauthorized	WEB

Troubleshooting

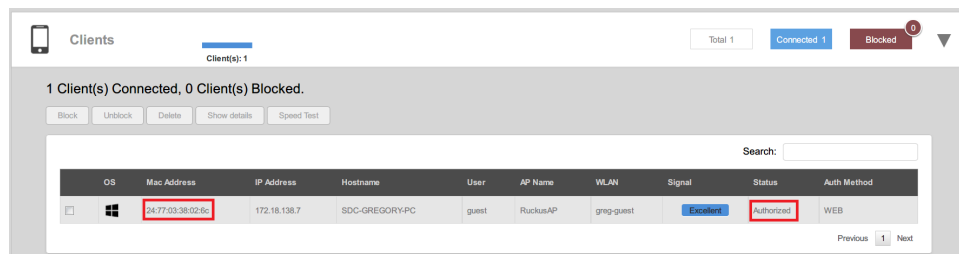
Troubleshooting Client Authentication Issues

If not, check the WLAN configuration, and make sure the client is associated to the correct WLAN.

If client association is fine, for Hotspot/WISPr WLAN, check whether the configured portal server is accessible from the client device. To do so, open a web browser on the client and visit the portal server URL configured on the WLAN configuration directly. If the client cannot visit the portal server, there might be a network issue or an access policy is blocking the client's portal access. Ensure that the portal server's domain name or IP address has been added into the "walled garden" list in the WISPr configuration.

Q: What can I check for reasons why my device still cannot access the Internet after I submitted the username/password on a Hotspot/WISPr WLAN, or a guest key on a Guest WLAN?

A: First, check the Unleashed web UI to confirm that your client status is "Authorized" after submitting credentials.



The screenshot shows the 'Clients' page in the Unleashed web UI. It displays a table with one client connected. The client's status is 'Authorized'.

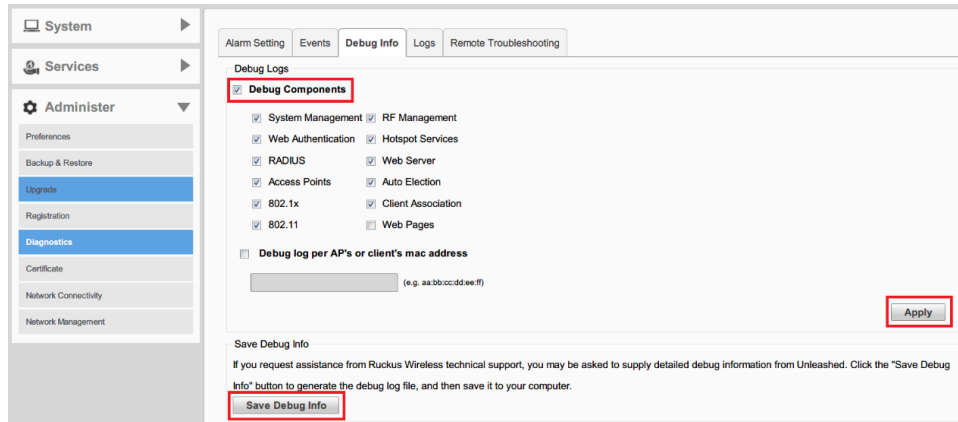
OS	Mac Address	IP Address	Hostname	User	AP Name	WLAN	Signal	Status	Auth Method
Windows	24-77-03-38-02-8c	172.16.138.7	SDC-GREGORY-PC	guest	RuckusAP	grip-guest	Excellent	Authorized	WEB

On a Guest WLAN, if the client is not shown as authorized, the input guest pass key might be incorrect, or the key already expired. You can go to **Services -> Guest Access Services** and check the **Admin Generated Guest Passes** table to check it.

On a Hotspot/WISPr WLAN if the client is not shown as authorized, you need to confirm with the authentication server to check the authentication result.

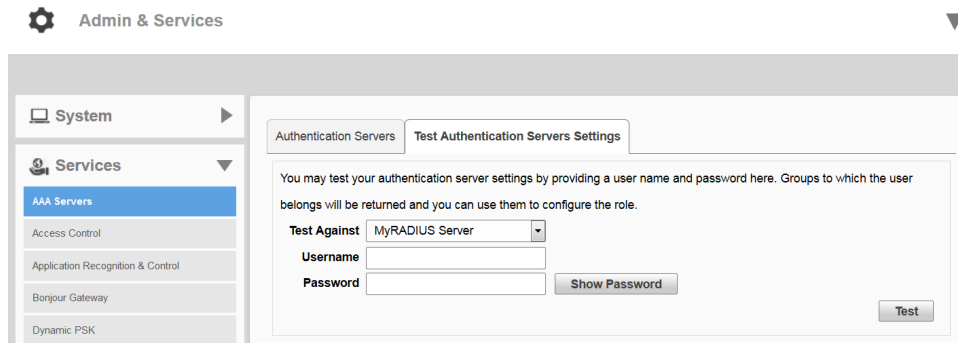
If the problem persists, you can follow the instructions to turn on the debugging log, go through the client connection procedure, and then send the debug file to Ruckus Customer Support for analysis.

On the **Debug Info** tab, check all **Debug Components**, and repeat client login steps, then click **Save Debug Info**. Provide that file to the Customer Support for further diagnostics.



Q: How do I test whether user accounts exist on an AAA (RADIUS or AD) server?

A: You can test RADIUS or Active Directory user entries from the Unleashed web UI: go to **Admin & Services > Services > AAA Servers**, and select the **Test Authentication Servers Settings** tab.



Q: I configured a Guest WLAN for my users but they complained that whenever they use HTTPS to visit a page, the browser pops up a warning message informing the user that the certificate of the portal page cannot be untrusted. How can I enhance the user experience?

A: You can import your own SSL certificate using the web UI: go to **Admin & Services > Administer > Certificate** and follow the instructions to import an SSL certificate.

Wireless Mesh Considerations

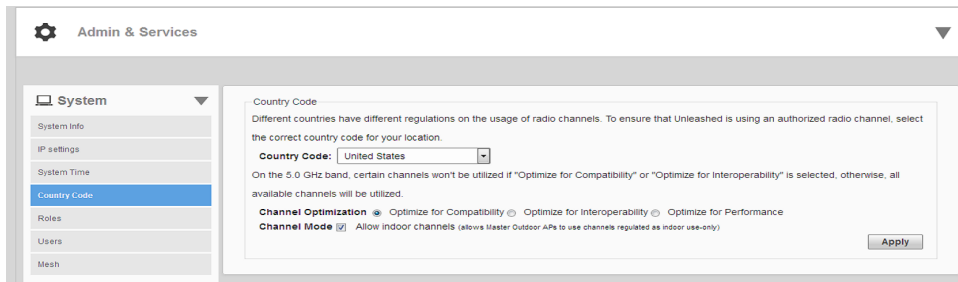
Q: How do I add an AP to an Unleashed Network to make it a wireless mesh AP?

A: First, connect the AP to the same network as the rest of the Unleashed APs via Ethernet. After the AP joins the network and receives the configuration - including the mesh link encryption key - the AP is ready to be used as a wireless mesh AP. You can

disconnect the AP's Ethernet link and move it to the desired location, and it will form a mesh connection to an uplink AP automatically.

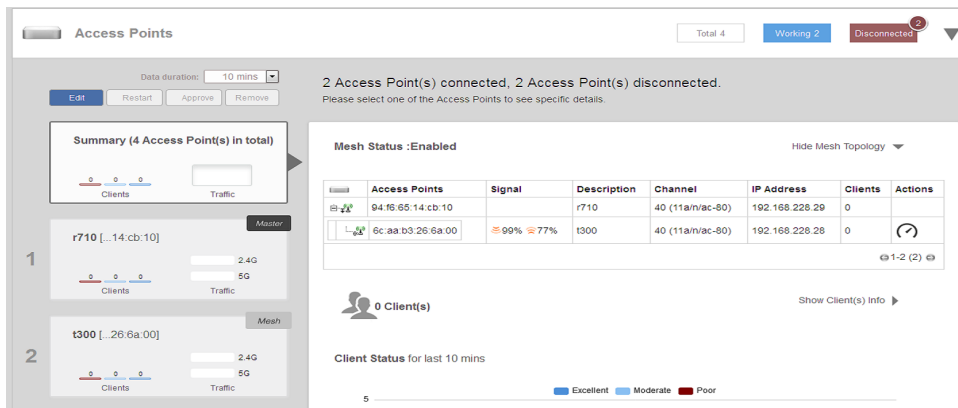
Q: Can a mesh connection be established between an outdoor AP and an indoor AP?

A: Yes, but note that according to the regulations of your country setting, outdoor APs may not be allowed to use certain indoor channels. If the indoor AP stays on an indoor-only channel, the outdoor AP won't be able to connect to it. In this case, you can either fix the channel of the 5 GHz radio on the indoor APs, or, if a statutory permit exists, configure the outdoor AP to allow it to use indoor channels.



Q: How do I see the mesh network topology?

A: You can check the mesh topology on the web interface by clicking the **Access Points** > **Summary** tab. You can choose to display or hide the mesh topology as follows:



Q: What can I do if a mesh AP cannot find an uplink connection?

A: Possible reasons include the following:

- The APs, either the intended mesh AP or the uplink AP, may not support mesh. For example, R310 and H320 do not support mesh.
- The mesh AP may not be properly configured. It is always a good practice to ensure an AP can join an Unleashed network through an Ethernet connection before making it a mesh AP.

- The signal from the uplink AP could be too weak. Try moving the AP to a different location to see whether that is the reason.
- The uplink AP stays on a channel that the mesh AP cannot utilize. Note that an outdoor AP may not be able to utilize certain indoor channels, and, the mesh AP model may not support a DFS channel that the uplink AP is using.
- Check the running release: release 200.0 does not support mesh.
- In release 200.1, there was an issue (ER-3691) reported where the mesh uplink search may not start right after the Ethernet cable is disconnected, until the AP is rebooted. This issue has been resolved in 200.2 and later releases.

If the AP is accessible (through either wired or wireless), SSH into it and type the following CLI debugging commands. If you cannot interpret the results, use the reporting method described at the end of this guide.

- On a root AP:
 - `get mesh`
 - `get channel wifil`
 - `get scanresults wifil`
- On a mesh AP:
 - `get mesh`
 - `get channel wifil`
 - `get scanresults wifil`

Q: Is mesh supported on all Unleashed APs?

A: Mesh has been supported since release 200.1. For Unleashed 200.5 and earlier, mesh is supported on all AP models except R310 and H320.

Q: What will happen if the Master AP becomes a mesh AP?

A: If a Master AP becomes a mesh AP (i.e., its uplink becomes a wireless link), it will give up its master role after a reboot. The new master will be elected among the root APs automatically. Your Unleashed network should be adjusted automatically after a few minutes.

Using the Management Interface

Q: Can the Management interface IP address still be used to access the Master AP if the Master changes?

A: Yes, it can. The Management IP address configuration is shared among all Unleashed APs, and the Master AP is in charge of responding to it.

Q: Does Unleashed support management VLAN on the management interface?

A: No. As of release 200.5, Unleashed APs do not support VLANs, and therefore the management interface cannot be placed into a management VLAN.

Q: Should the management IP address be in the same subnet as the AP's device IP address?

A: Yes, it should. Unleashed APs do not support VLANs, so it is not recommended to configure the management IP in a different subnet.

Q: Can a Member AP utilize the IP address of the Management Interface to connect to the Master AP?

A: No. The Management Interface can only provide web and SNMP services, it is not used for Member APs to connect to the master AP.

Q: Why does the Management interface stop working once I enable Gateway mode?

A: Because if Gateway mode is enabled on an Unleashed Network, the Master AP is fixed. In this situation, the device IP would be the same as a management IP, so the Gateway/Master AP does not support the management IP interface feature.

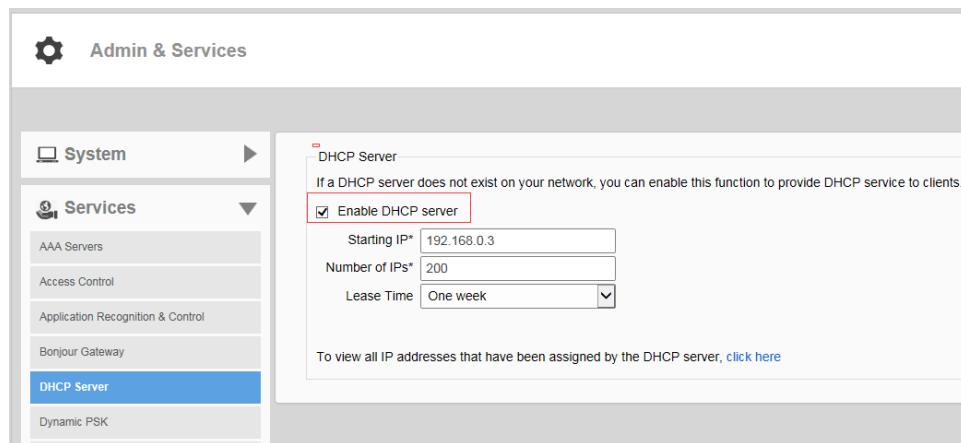
Configuring DHCP Service

Q: How do I enable the internal DHCP server in an Unleashed network?

A: Unleashed DHCP functionality depends on which release you are running.

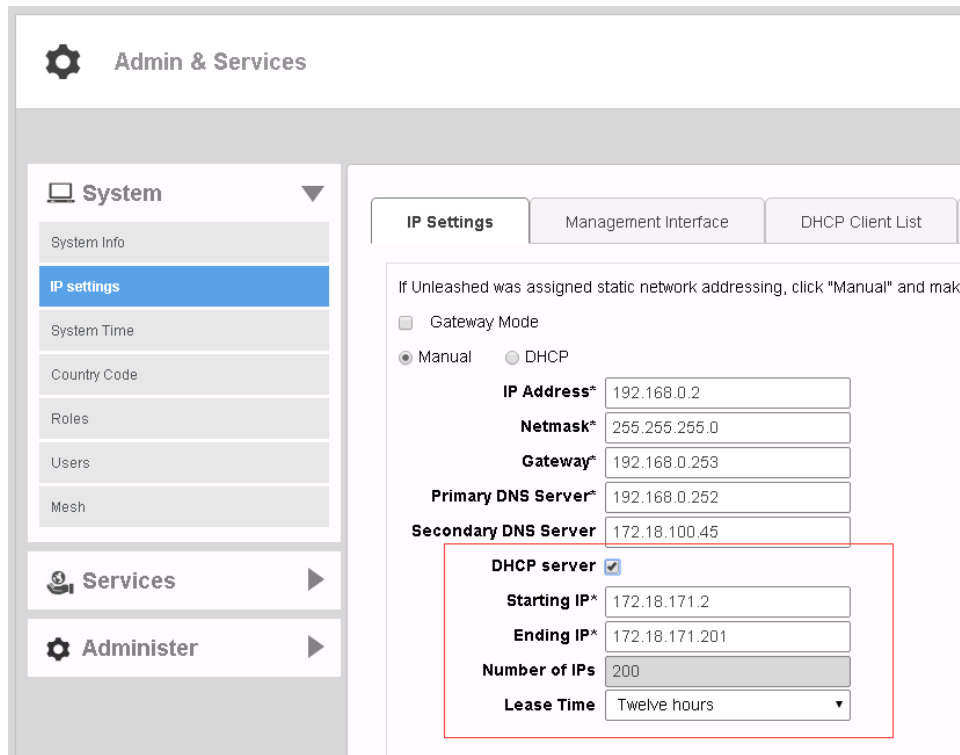
The Gateway mode feature was not supported in releases 200.0, 200.1 and 200.2. In these early releases, the Master AP could be configured with a static IP address and the DHCP server could be enabled.

To enable DHCP server on those Unleashed releases, go to **Admin & Services > Services > DHCP Server** .



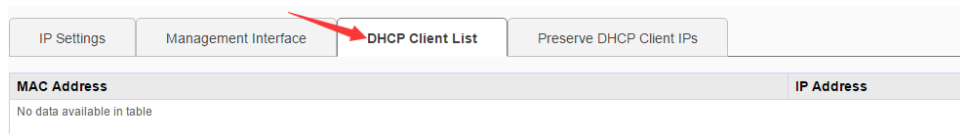
The "Gateway Mode" feature is supported in release 200.3 and later. In later releases, the configuration page has been moved to the following page:

Admin&Services > System > IP settings



Q: How do I check the leased IP addresses from the DHCP server?

A: The list of IP addresses leased by the DHCP server can be seen on the following page: **Admin & Services > System > IP settings** , then select the **DHCP Client List** tab.

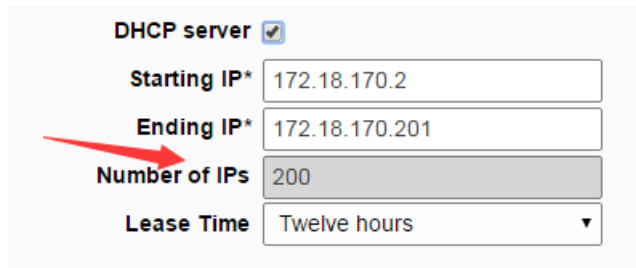


Q: What is the maximum number of IPs addresses supported by the internal DHCP server?

A: The number of IPs is manually configured using the **Number of IPs** and the **Ending IP** address settings on the DHCP server configuration screen.

Troubleshooting

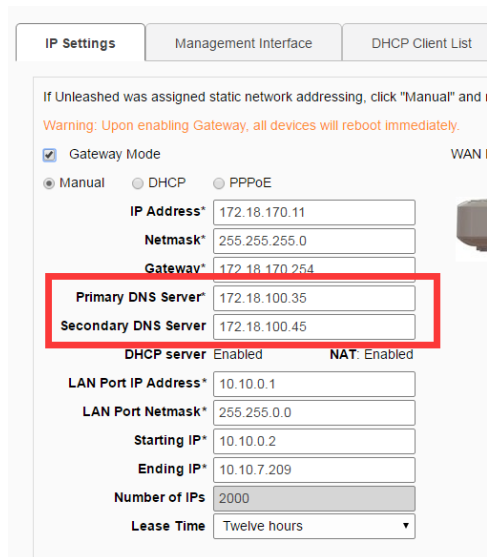
General Configuration Questions



A screenshot of a DHCP server configuration form. The form has a title "DHCP server" with a checked checkbox. Below the title are four input fields: "Starting IP*" with the value "172.18.170.2", "Ending IP*" with the value "172.18.170.201", "Number of IPs" with the value "200", and "Lease Time" with a dropdown menu showing "Twelve hours". A red arrow points to the "Ending IP*" field.

Q: How do I assign DNS server information in the internal DHCP address offers?

A: Go to **Admin & Services > System > IP settings**.



A screenshot of the "IP Settings" form in the Unleashed UI. The form has three tabs: "IP Settings", "Management Interface", and "DHCP Client List". Below the tabs is a warning message: "Warning: Upon enabling Gateway, all devices will reboot immediately." There are three radio buttons for "Gateway Mode": "Manual" (selected), "DHCP", and "PPPoE". Below these are four input fields: "IP Address*" (172.18.170.11), "Netmask*" (255.255.255.0), "Gateway*" (172.18.170.254), and "Primary DNS Server*" (172.18.100.35). The "Secondary DNS Server*" field (172.18.100.45) is highlighted with a red box. Below these fields are two checkboxes: "DHCP server" (Enabled) and "NAT" (Enabled). At the bottom are four more input fields: "LAN Port IP Address*" (10.10.0.1), "LAN Port Netmask*" (255.255.0.0), "Starting IP*" (10.10.0.2), "Ending IP*" (10.10.7.209), "Number of IPs" (2000), and "Lease Time" (Twelve hours).

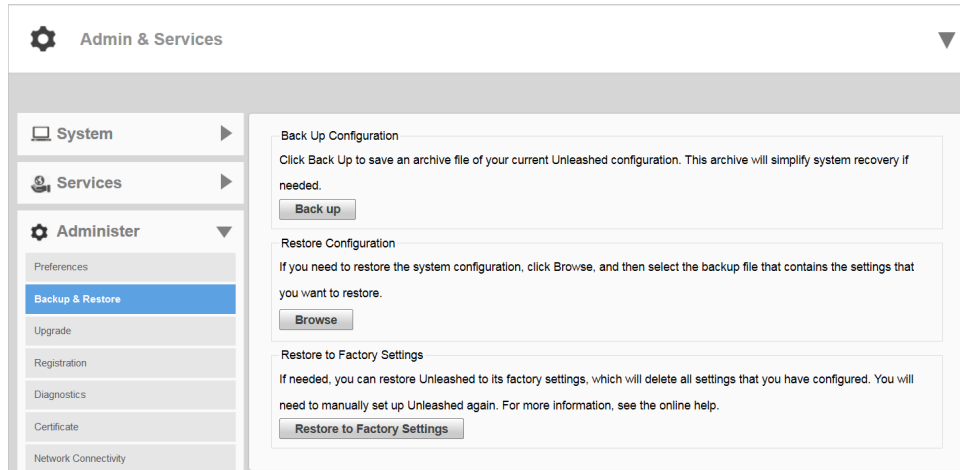
General Configuration Questions

Q: I am familiar with Ruckus ZoneDirector configuration, and I'm curious why I can't find the AP group and WLAN group settings on the Unleashed UI. What am I missing?

A: To simplify Unleashed configuration, AP groups and WLAN groups are not supported.

Q: How do I save an existing configuration or restore my previous configuration?

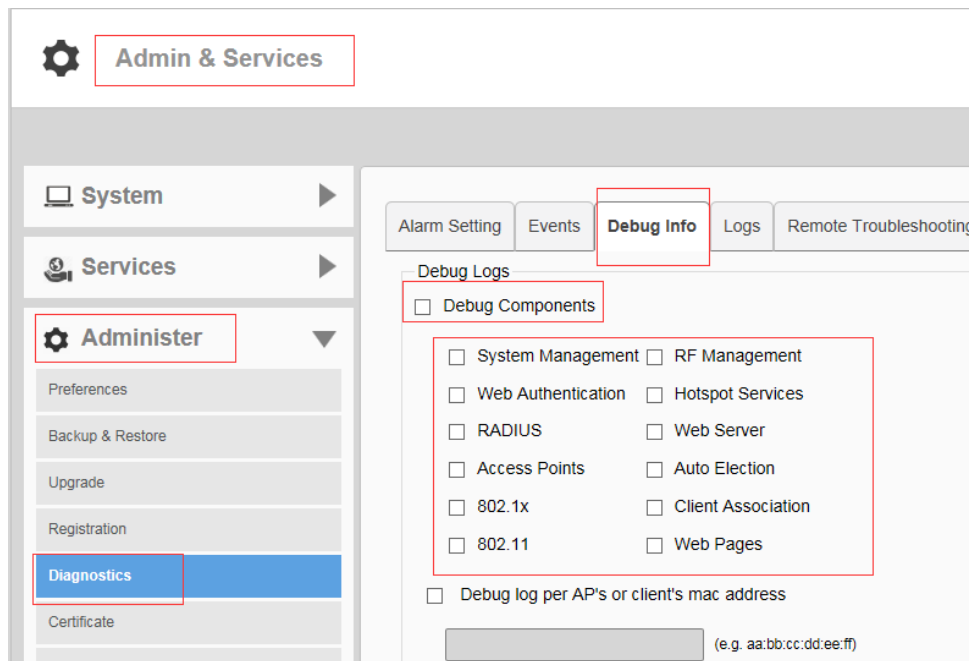
A: You can backup and restore your Unleashed system configuration settings using the **Admin & Services > Administer > Backup & Restore** page.



Debugging

Q: Ruckus Customer Support asked me to turn on debug logging and recreate my problem for diagnosis. How do I enable the logs? And, how do I know which logs need to be enabled?

A: Debug logs can be enabled on the web UI on the following page: **Admin & Services > Administer > Diagnostics > Debug Info** .

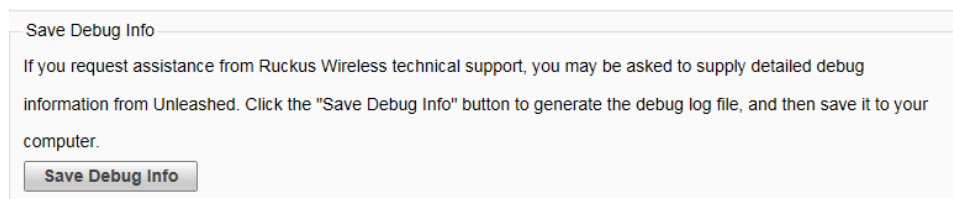


If you are not sure which logs to enable, the recommendation is to enable most of them. One exception is the "Web Pages," component, which generates many log messages. Unless you are analyzing a web UI issue, do not enable this log.

NOTE Generating debug log messages impacts AP performance. Remember to disable debug logs after the logs have been collected.

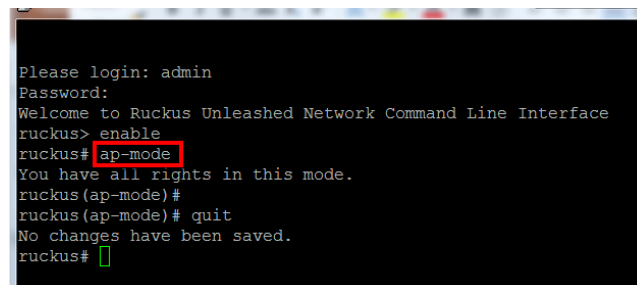
Q: How do I save debug information?

A: Go to **Admin&Services > Administer > Diagnostics > Debug Info**, and click the **Save Debug Info** button. Save the package to your local computer and send it to Ruckus Customer Support.



Q: After SSH into my Master AP, I noticed a different CLI prompt which is not the Ruckus AP CLI. It doesn't take any AP CLI commands either. What's wrong?

A: The Master AP provides a Master-style CLI, closer to the ZoneDirector controller CLI. You can use the **ap-mode** command to enter AP CLI mode, and **quit** to exit back to Master CLI mode.



Q: I suspect that my Master AP may mysteriously crash/reboot at times. But I do not have anything to provide for Ruckus customer support for analysis. What can I do?

A: You can help to collect the debugging information if you know that an AP in the Master role may potentially experience a mysterious crash or reboot. To do so, enable the log reporting mechanism in advance, and, if the AP indeed experiences a problem, it may be able to send its log files out to a preconfigured server before it reboots.

To enable this debug logging feature, go to **Admin&Services > Administer > Diagnostics > debug Info**, and enable **Upload debug logs to remote server**. Enter the **Host IP** address, and click **Apply** to save your changes.

Upload Debug Logs

Enable upload debug logs to remote server

Protocol* TFTP FTP

Host*

Once you have the logs, you can report the issue following the reporting method described at the end of this guide.

Q: One of my member APs has crashed or rebooted. The Ruckus support representative asked me to provide the AP's support information for analysis. How do I collect this information?

A: There are two ways to retrieve an AP's support information:

1. Save the AP support info from the Unleashed web UI: **Access Points** > select the AP > **Show System Overview Info** , and then click the **Save logs** button to save it to your administrative PC.

The screenshot shows the 'Access Points' management interface. At the top, there are status indicators for 'Total 1', 'Working 1', and 'Disconnected 0'. Below this, a summary section shows '1 Access Point(s) connected, 0 Access Point(s) disconnected'. A table lists system overview information for a selected AP:

MAC Address	10:b0:52:39:ce:20
IP Address	172.16.171.3
External IP Port	172.16.171.3:12225
Model	r500
S/N	481464906755
Current Channel(802.11a/n/ac)	40
Current Channel(802.11b/g/n)	11
Max Clients	50
Version	200.2.9.13.186
Log	Save Logs

2. Through AP's CLI: SSH to AP, log in to AP's CLI, execute the following commands and save the console output to a file:

- support
- support show

Q: How do I capture packets on an Unleashed AP?

A: Unleashed APs support remote packet capture using the same methods as a ZoneDirector controller.

You can SSH to the Unleashed AP, and run the following CLI command to enable remote packet capture:

```
set capture wlan100 stream
```

Troubleshooting

Debugging

```
rksccli:
rksccli: set capture wlan100 stream
Capturing in 20 MHz channel BW
OK
rksccli:
```

And replace "stream" with "idle" to stop streaming:

```
set capture wlan100 idle
```

NOTE The above command works in a Member AP. On a Master AP running 200.3 or later image, you need to go to AP CLI mode in SSH session using the `ap-mode` CLI command:

```
Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# ap-mode
You have all rights in this mode.
ruckus (ap-mode)# set capture wlan100 stream
Capturing in 20 MHz channel BW
OK
ruckus (ap-mode)# set capture wlan100 idle

OK
ruckus (ap-mode)# quit
No changes have been saved.
ruckus# █
```

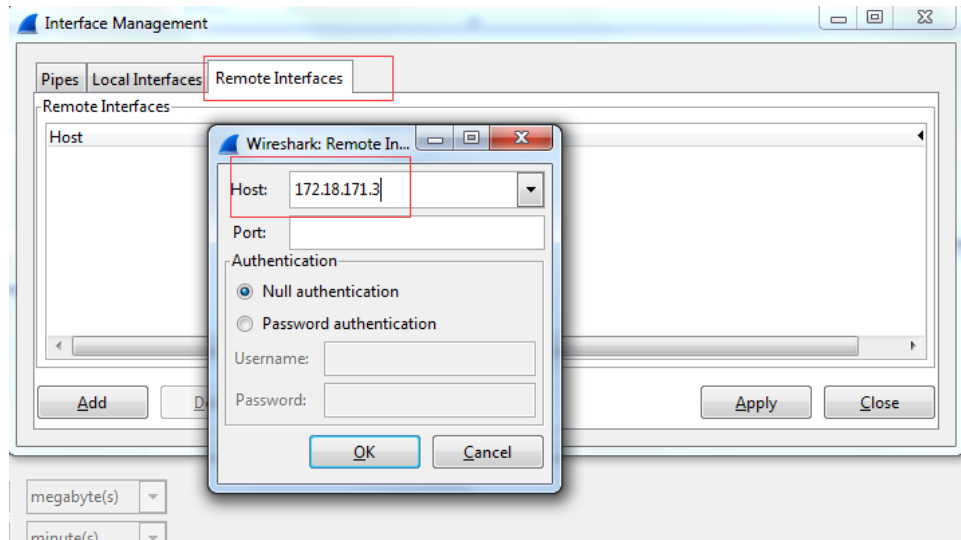
If the Master AP is running 200.2 or earlier version, you can enter the CLI debug mode and use the following `remote_ap_cli` command with the Master AP's MAC address:

```
Please login: admin
Password:
Welcome to Ruckus Unleashed Network Command Line Interface
ruckus> enable
ruckus# debug
You have all rights in this mode.
ruckus (debug)# remote_ap_cli -a f8:e7:1e:0e:ba:c0 "set capture wlan100 stream"
---- Command 'rksccli -c "set capture wlan100 stream"' executed at f8:e7:1e:0e:ba:c0
Stream capture is running on wifi3, please set it to idle mode.
remote_ap_cli "-a" "f8:e7:1e:0e:ba:c0" ""set" "capture" "wlan100" "stream""
ruckus (debug)#
ruckus (debug)# remote_ap_cli -a f8:e7:1e:0e:ba:c0 "set capture wlan100 idle"
---- Command 'rksccli -c "set capture wlan100 idle"' executed at f8:e7:1e:0e:ba:c0
OK
remote_ap_cli "-a" "f8:e7:1e:0e:ba:c0" ""set" "capture" "wlan100" "idle""
ruckus (debug)#
ruckus (debug)# quit
No changes have been saved.
ruckus# █
```

You may also need to use the following AP CLI command to learn the AP's IP address:

```
get ipaddr wan
```

Start Wireshark on a PC, type the AP's IP address to capture the packets:



Reporting an Unleashed Issue

If a customer experiences an issue with their Unleashed network, they can first seek advice from other Unleashed users on the **Ruckus Unleashed Forums**:

https://forums.ruckuswireless.com/ruckuswireless/categories/ruckuswireless_ruckus_unleashed

If the Support forums are unable to provide a solution, customers with a valid support contract can submit a support ticket request for further assistance to **Technical Support** through the Ruckus Support website:

<https://support.ruckuswireless.com/contact-us>

When reporting an issue, please provide the following information:

- Unleashed Release version number
- AP model(s)
- Description of the client device having issues connecting or accessing the Unleashed Network (PC/Web UI, Mobile app, etc.).
- Specific steps that led to the situation
- In most cases, the Master AP's Debug info (saved from **Administer >Diagnostics**) would be helpful for problem analysis.



Copyright © 2017. Ruckus Wireless, Inc.
350 West Java Drive, Sunnyvale, CA

www.ruckuswireless.com