



A5/A5c User Guide

Mimosa Access Points

copyright © Mimosa. All rights reserved.
<http://backhaul.help.mimosa.co/>

The information contained in this document is subject to change without notice.
This document contains proprietary information which is protected by copyright.
All rights are reserved. No part of this document may be photocopied, reproduced,
or translated to another language without the prior written consent of Mimosa.

Table of Contents

FAQ's	1
Setup	1
Default IP Address	1
Reset Process	3
Reset A5	3
Serial Number Location	4
Unlock Process	6
Change Unlock Country	6
No CLI	10
Performance	11
Maximum Tx Power	11
SNR Required for each MCS	13
Error Vector Magnitude (EVM)	14
Quality of Service (QoS)	15
Spectrum Analysis	17
Auto Channel	18
Compatibility	20
Client Compatibility	20
Specifications	21
Supported Frequencies	21
Supported Channel Widths	24
Receiver Sensitivity	25
Power over Ethernet (PoE)	26
Hardware & Materials	28
Installation Guide	29
Installation Overview	29
Radio Unlock Process	30
A5 Installation	32
A5c Installation	34
PoE Connections	37
Access Point Setup	39
User Guide	41
Overview	41
General	41
Accessing the Interface	42
Logging In	43
User Interface Overview	44
Dashboard	46
Dashboard Overview	46
Status Bar	47
Connected Clients	48
Airtime Usage	49
Configured SSIDs	50

Performance	51
Device Details	52
Access Point Settings	53
Wireless	54
Clients	54
Client List	54
SSID	56
SSID Management	56
Site Survey	58
Survey Results	58
Channel & Power	59
Spectrum Analyzer	59
5 GHz Channel & Power	60
2.4 GHz Management Interface	61
Exclusions & Restrictions	62
Location	63
Local Satellite Signals	63
Satellite Information	64
Location Data	65
Traffic	66
Access Control Lists	66
Traffic Shaping Plans	67
Fixed Clients	68
Preferences	69
General	69
Naming	69
Session Management	70
Miscellaneous	71
System Log Notifications	72
Set Password	73
Management	74
Management IP	74
Rogue DHCP Server Protection	75
Application Prioritization	76
VLAN Management	77
Miscellaneous	78
Firmware & Reset	79
Device Firmware	79
Reset & Reboot	80
Backup & Restore	81
Backup & Restore	81
Diagnostics	82
Tests	82
Tests	82
Ping	83
Traceroute	84

Logs	85
Log Overview	85
Troubleshooting Guide	86
A5 LED Status	86
GPS Signals	89
Testing Throughput with iPerf	90
Firmware	91
A5 Firmware Roadmap	91
A5	93
A5 Firmware Downloads	93
A5 Release Notes	94
White Papers & Application Notes	97
ACL Traffic Optimization	97

Default IP Address

Wired Ethernet

Mimosa Access Points are assigned the static IP Address 192.168.1.10. This value can either be set manually, or by an external DHCP server.

Wireless 2.4 GHz (Normal Operation)

Two 2.4 GHz management SSID's are broadcast at boot up. The "MimosaM###" SSID is used to distinguish between Access Points if multiple AP's at the same site advertise the same SSID. Clients of the AP will be assigned DHCP addresses if an external DHCP server is present. If not, their IP addresses must be configured manually.

SSID Name*	Purpose	SSID Availability	AP IP Address	Client IP Address
"MimosaM###"	Management	10 minutes	Static (192.168.1.10)	Manual
			External DHCP	External DHCP
"Mimosa2G"	Management	Always on	Static (192.168.1.10)	Manual
			External DHCP	External DHCP

Wireless 2.4 GHz (Reset/Recovery)

Applying power to the radio without populating the PoE Data port initiates the reset/recovery process. Since no external DHCP server is available, the Access Point assigns a DHCP address to the client.

SSID Name*	Purpose	SSID Availability	AP IP Address	Client IP Address
"MimosaR###"	Reset/Recovery	5 minutes	Static (192.168.26.1)	AP assigns DHCP

* ### = the last three digits of the serial number

IP Address Discovery

Run the following command from the command line to discover the IP addresses of any directly connected Mimosa devices. The string "20:B5:C6" is an Organizationally Unique Identifier (OUI), which is the first half of the MAC address assigned to Mimosa devices. After executing the command, the IP address will be shown for each device.

Windows / DOS:

```
arp -a | findstr 20:B5:C6
```

Mac / Linux:

```
arp -a | grep 20:B5:C6
```

No CDP / LLDP Support

Mimosa radios do not respond to either CDP or LLDP at this time.

Related:

[Access Point Setup Overview](#) - Detailed process for configuring your device

[Accessing the Mimosa Cloud](#) - Firewall adjustments for cloud monitoring (no NAT required)

[Reset Process](#) - Explains how to recover/reset a device if needed

Reset A5

Product Applicability: A5/A5c

This process is to restore the device to the factory state when the device is physically available. It replaces a physical reset button and allows recovery without the need to climb a tower.

Follow these steps to reset the radio:

1. Unplug both Ethernet cables from the POE. Leave unplugged for about 3 seconds.
2. Plug in only the data + power cable to the radio. Do not plug in the LAN cable.
3. Immediately connect to the "mimosaR###" SSID (where ### = the last three digits of the serial number) with a PC or mobile device. The SSID and total recovery window expires after 5 minutes.
4. With a web browser, navigate to 192.168.26.1
5. Enter the device serial number located on back of device and click enter.
6. Click the reset button to factory reset the device. This action will remove all configuration settings and passwords.
7. The radio will then reboot for about 90 seconds.

After factory reset, access the device with the default IP address, then follow the device unlock process again before reuse.

It is also good practice to create a configuration backup such that it can be restored in the case of lost passwords.

Finding the Serial Number

The Mimosa serial number is a 10-digit number used to differentiate radios. This unique number is used as part of the unlock process to ensure genuine product assurance.

There are two ways to find the Serial number on a Mimosa radio:

1. On the bottom of the radio, you can find the serial number next to the QR code (see images below).
2. Within the user interface, you can find the serial number on the Dashboard under Device Details.

A5 Serial Number Label



A5c Serial Number Label



Changing the Unlock Country

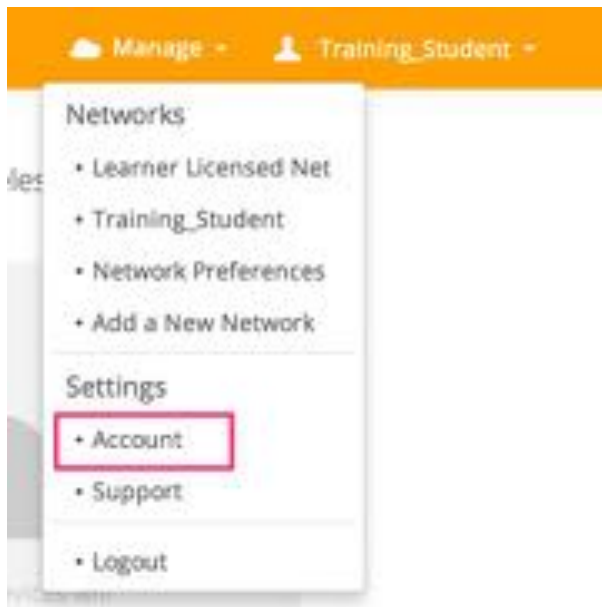
Background

During the unlock process, a country must be selected to obtain an unlock code. The country can be changed later, but a new unlock code is required to do so. Unlock codes are specific to both the serial number of the device and the country selected.

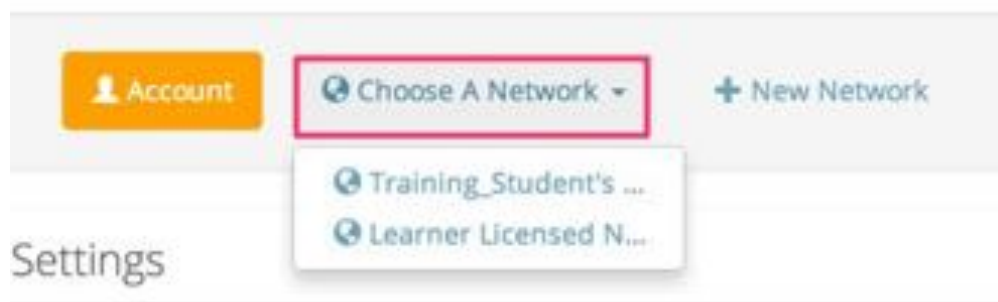
Process

This process describes how to obtain an unlock code for another country if the device is moved outside of the original country, or if licensed mode is used:

1. Log into manage.mimosa.co
2. Click on your network name in the upper right hand corner.
3. Select **Settings > Account**.



4. Click on the "Choose a Network" drop-down list and select your network name.



5. Click on the **Add Country Code to Network** button.



6. In the dialog box that opens, select the new country to add.

7. Complete additional contact information.

8. If changing to a country with licensed operation ("[Country Name] Licensed"), agree to the Terms of Use and click **Add**.

Add a country to this network

To add another country to this network, you must provide a valid business address.

Country * Address 1 *

Company Name * Address 2

City *

Optional Code *

State/Province

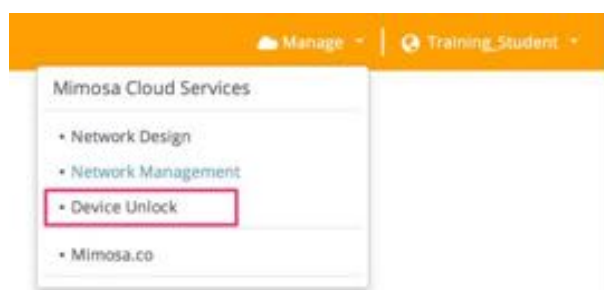
LICENSED FREQUENCY TERMS-OF-USE

Use of this Mimosa device in any licensed frequency is subject to your legal authorization to do so. By checking this box, you hereby represent and warrant that you (as person) the required government approvals to operate this device within the licensed frequency, and (ii) agree to provide the requisite supporting documentation promptly upon request by Mimosa to do so. Mimosa retains the right to deactivate the license on this device in the event you fail to comply with either of these requirements.

☒ Agree to Terms of Use

Cancel

9. Click the "Manage" drop-down box, and select **Device Unlock**.



10. Choose the new unlock country from the "Country" drop-down list.



Enter the 10 digit serial number of the device(s) you would like to unlock. This will generate unlock key(s) that must be entered into each device before first use.

[Need help finding your serial number?](#)

Network:
Training_Student

Country:
United States

Colombia Licensed
United States

☒ If your network operates in multiple countries, you can add them in Account Settings.

☒ I agree to the License and Privacy Policy *

Submit

11. Enter the device serial number.

12. Once you accept the terms and submit, the new unlock code will be shown.

Network:
Training_Student

Country:
Colombia Licensed

Serial Number:
12 - 3456 - 7890

☒ I agree to the Licensed Frequency TOS *

☒ I agree to the TOS and Privacy Policy *

Submit

13. Reset the unlock code and enter the new unlock code to complete the process.

No Command Line Interface (CLI) Access

There is no user-accessible method for SSH or telnet to Mimosa devices. Mimosa Support is the only party capable of accessing the shell, and only after installation of an RSA certificate.

Mimosa disables the CLI by default due to security, support, and regulatory compliance concerns:

- Prevents installation of non-Mimosa operating systems that can lead to unsupported configuration changes - especially related to regulatory compliance.
- Protects devices, and data passing across them, from unauthorized access.
- Deters counterfeiting and reverse engineering of Mimosa's intellectual property.

Maximum Tx Power and EIRP

Product Applicability: A5/A5c

The maximum transmit power that you can select is limited by product specifications and maximum EIRP limits.

Maximum Transmitter Power

Mimosa Access Points are capable of transmitting at the power levels in the table below. Total power is divided equally between all four antennas or antenna outputs.

		Maximum Tx Power (dBm)	
Product	Channels	Total Power	Per Antenna
A5/A5c	1	30	24

Calculating EIRP

A5/A5c EIRP calculations are a bit different from traditional omni or sectors. To account for the A5's unique quad-sector design with one radio chain per sector and circular polarization, several additional factors must be considered when calculating EIRP:

- Tx Power (dBm) is the total system power.
- To account for the quad-sector design, the total system power is split over the four sector antennas, a -6 dBi gain at each sector.
- To account for the +3 dBi gain of circular polarization, the power must be normalized to linear polarization, the way EIRP is measured. This is represented by a -3 dBi gain.

Here is an example of computing EIRP for the A5-14 on a U-NII-2 channel with a maximum linear EIRP of 30 dBm (FCC).

Maximum Tx Power (dBm)	Per Chain Power (dBm)	Antenna Gain (dBi)	Linear Polarization Normalization (dBi)	EIRP (dBm)
25	-6	+14	-3	30

Maximum EIRP Limits (5 GHz)

Local laws may restrict maximum EIRP for certain frequency ranges. The chart below shows restrictions in the United States.



SNR Required for Each MCS

The table below shows the SNR required for each MCS index as well as the modulation, coding and data rate per stream based on channel width in MHz. Note that each channel uses up to two streams.

Examples:

- 1 x 80 MHz channels operating at MCS 9 with 2 streams would yield 866 Mbps (433 Mbps * 2 streams).
- 1 x 40 MHz channel operating at MCS 8 with 2 streams would yield 360 Mbps (180 Mbps * 2 streams).
- 1x 20 MHz channel operating at MCS 7 with 2 streams would yield 144 Mbps (72.2 Mbps * 2 streams).

Modulation and Coding Scheme (MCS)				PHY Data Rate (Mbps/stream)		
Index	Modulation	Coding	Required SNR (dB)	20 MHz	40 MHz	80 MHz
0	BPSK	1/2	5	7.2	15	32.5
1	QPSK	1/2	7.5	14.4	30	65
2	QPSK	3/4	10	21.7	45	97.5
3	16-QAM	1/2	12.5	28.9	60	130
4	16-QAM	3/4	15	43.3	90	195
5	64-QAM	2/3	17.5	57.8	120	260
6	64-QAM	3/4	20	65	135	292.5
7	64-QAM	5/6	22.5	72.2	150	325
8	256-QAM	3/4	25	86.7	180	390
9	256-QAM	5/6	27.5	n/a	200	433

Throughput measured at each client will be lower due to MAC protocol overhead and the division of total capacity amongst all associated clients.

Related:

Access Point FAQ: What is the sensitivity for each MCS index?

Error Vector Magnitude (EVM)

The error vector magnitude or EVM describes how well the receiver can detect symbols (data) within a constellation of symbols on the I-Q plane for a particular modulation. It is the difference in RMS power between the point where a symbol is received and where the symbol should be. This difference is caused by noise.

When analyzing EVM, the lower the number the better.

EVM (dB)	EVM (%)	Assessment
0	100.0	Poor
-5	56.2	Poor
-10	31.6	Poor
-15	17.8	OK
-20	10.0	Good
-25	5.6	Good
-30	3.2	Excellent
-35	1.8	Excellent

Quality of Service (QoS) Support

Mimosa backhaul radios support four different L2/L3 QoS queues for traffic prioritization. Typically, an upstream router sets values for CoS (L2), or DSCP/TOS (L3) for specific traffic on the post-routing chain. After packets leave the router, they enter the radio where the traffic is queued and sent according to the packet marking. While the radio does not function as a router, it does respect packet markings assigned by the upstream router.

The table below lists the four QoS queues and corresponding prioritization values for various traffic marking standards.

Traffic Queue	IEEE P802.1p (VLAN CoS Priority)	TOS	DSCP	Mimosa Weighting (% of capacity)
BE	0	0-31	0-7	20
BK	1	32-63	8-15	10
BK	2	64-95	16-23	10
BE	3	96-127	24-31	20
VI	4	128-159	32-39	30
VI	5	160-191	40-47	30
VO	6	192-223	48-55	40
VO	7	224-255	56-63	40

where,

BK = Background (lowest priority)

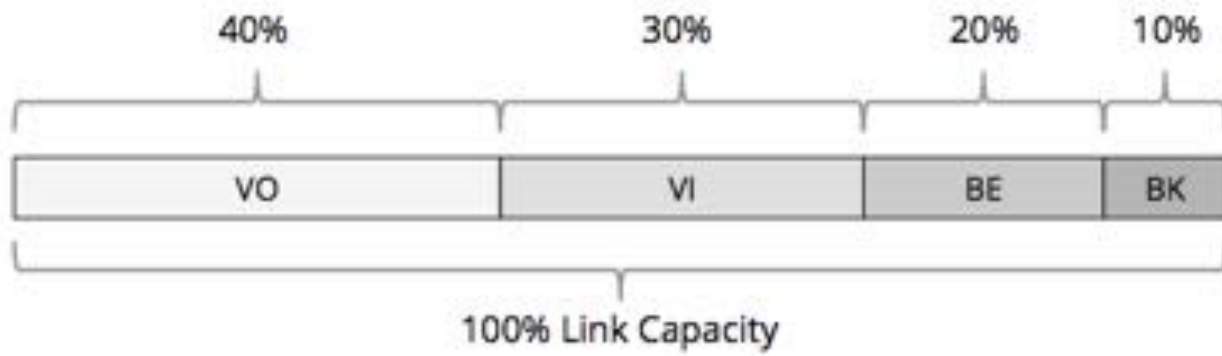
BE = Best Effort

VI = Video

VO = Voice (highest priority)

Mimosa QoS Weighting

Mimosa radios dynamically allocate link capacity by expanding or contracting each traffic queue based on the current mix of marked traffic. If there is no traffic in a particular queue, that capacity is divided between the other queues according to their relative weights. Unmarked traffic is processed in the Best Effort (BE) queue by default.



Access Point Spectrum Analyzer

Mimosa Access Points continuously scan the entire operating spectrum in a background task without disturbing client connections.

In addition, Mimosa Cloud Services can record historical spectrum analysis for all of your Mimosa devices. The spectrum data can be visually played back to identify trends and gain insight into how the RF environment impacts your customers.

Mimosa provides storage of up to 24 hours of spectrum data for all your Mimosa devices as a free service.

Communication between your devices and Mimosa Cloud Services is optional, but you will not be able to gain access to cloud features such as spectrum playback without Mimosa Cloud Services.

Auto Channel

Product Applicability: A5/A5c

Auto Channel is a feature that makes automatic adjustments to AP settings (channel, primary channel, channel width, and transmit power) to improve the average PHY rate for all connected clients by considering the following values over time:

- Available channels and power in compliance with regulatory restrictions
- Noise data from spectrum analysis
- AP PHY Errors: SPF/LPF, CRC, Retries, and Backoffs
- Client PHY Statistics: Average RSSI, EVM, MCS, and spatial streams
- Site Surveys before channel changes to avoid interfering with other Mimosa AP's

Auto Channel arbitrarily selects a channel when it starts for the first time after boot up, and then uses client data to make change decisions. For this reason, we recommend manually selecting the channel with the least interference for the AP, connecting a few clients, and then turning on Auto Channel. The last known configuration, either auto or manual, is used after subsequent reboots.

100% Mimosa Deployments

If every client connected to the AP is another Mimosa device (C5/C5c), each client's received signal is excluded from the AP's spectrum analysis results, providing a clear view of interference.

Mixed Client Deployments

Decision logic varies when non-Mimosa clients are connected to the AP. This is because non-Mimosa clients show up in spectrum analysis data as noise, so spectrum analysis data is ignored, and AP PHY errors are used instead.

Time Scale and Change Frequency

The time range for channel changes is 8-12 minutes, but high PER can accelerate this to as little as 3 minutes. A reduction in channel width takes 2 minutes.

Hysteresis is applied based on recent channel change history such that higher thresholds are required for subsequent changes. The threshold limits depend on whether the AP has all Mimosa clients, non-Mimosa clients, or a mix of both. The penalty applied based on history is reset every 6 hours.

Channel and channel width changes take 2 minutes per each additional A5 detected in site survey results. When multiple A5's are detected in site survey results, a hashing algorithm is employed to allow each AP to self organize and divide spectrum across all available channels.

Optimized for Uptime

Pending changes are communicated to clients via wireless beacons such that (non-DFS) channel changes and Tx power changes do not require client re-association. Changes to DFS channels, or to channel width require re-association, so each carry lower priority within the decision-making algorithm.

Operating on DFS Channels

By default, non-DFS channels are favored over DFS channels considering the time cost of the CAC period, ranging from 60 seconds to 10 minutes depending on regulatory domain, but there are cases where DFS channels offer the cleanest spectrum.

When moving from a non-DFS channel to a DFS channel, Tx power may be reduced depending on the regulatory domain. In this case, the Auto Channel algorithm would have already considered the SNR impact to each client, and each client would reduce its own Tx power settings when required. If moving from a DFS channel to a non-DFS channel, Tx power may be increased if regulations allow.

A best alternate channel is identified when operating on a DFS channel, such that channel changes after a radar detection result in the best possible performance.

Adjustment for EIRP Compliance

Auto Channel will recalculate the maximum allowed transmit power based upon the regulatory domain and antenna gain. Any change to antenna gain (Wireless > Channel & Power > Channel & Power Settings > Antenna Gain) will cause Auto Channel to recalculate the new maximum allowed transmit power.

Turning Off Auto Channel

Auto Channel can be turned off by selecting "Off" in the toggle control. If turned off, Auto Channel will no longer make changes to channel, primary channel, channel width or Tx power.

Auto Channel and Excluded Channels

Prior to enabling Auto Channel, specific frequency range(s) can be excluded from use by adding them to the exclusion list on the AP (Wireless > Channel & Power > Exclusions & Restrictions), and then saving.

To exclude the current channel, you must first turn off Auto Channel, make a manual channel change outside of the exclusion range, add the exclusion, and then turn Auto Channel back on.

Removing channels from the exclusion list will make those new channels available to Auto Channel. Note that "WiFi Interop" mode is limited to standard Wi-Fi channels.

Mimosa Access Point Product Family Compatibility

The Mimosa A5/A5c Access Point supports clients that are compatible with the standards in the table below.

5 GHz Clients	2.4 GHz Management
• 802.11a • 802.11n • 802.11ac	• 802.11b • 802.11g • 802.11n

Access Point Supported Frequencies

Product	Frequencies*
A5	4900-6200 MHz
A5c	4900-6200 MHz

* Your regulatory domain may limit allowable frequency ranges. 4.9 GHz and >5.8 GHz not available in WiFi Interop mode; requires firmware upgrade.

U-NII-2 and DFS Support

Product Applicability: A5/A5c

Mimosa 5 GHz radios support U-NII-2 operation and comply with DFS requirements. When a DFS channel is selected, there is a mandatory 60-second waiting period where the device listens for radar before association on that particular channel. In the EU, there is a mandatory 10-minute waiting period for the 5600-5650 TDWR band.

If a qualifying radar signature is detected, the radio will comply with DFS requirements by vacating the channel for 30 minutes. For this reason, Mimosa recommends the use of Dual-Channel mode with the secondary channel on a non-DFS channel (U-NII-1 or U-NII-3) so that traffic will be routed over the second channel and no link down time is incurred.

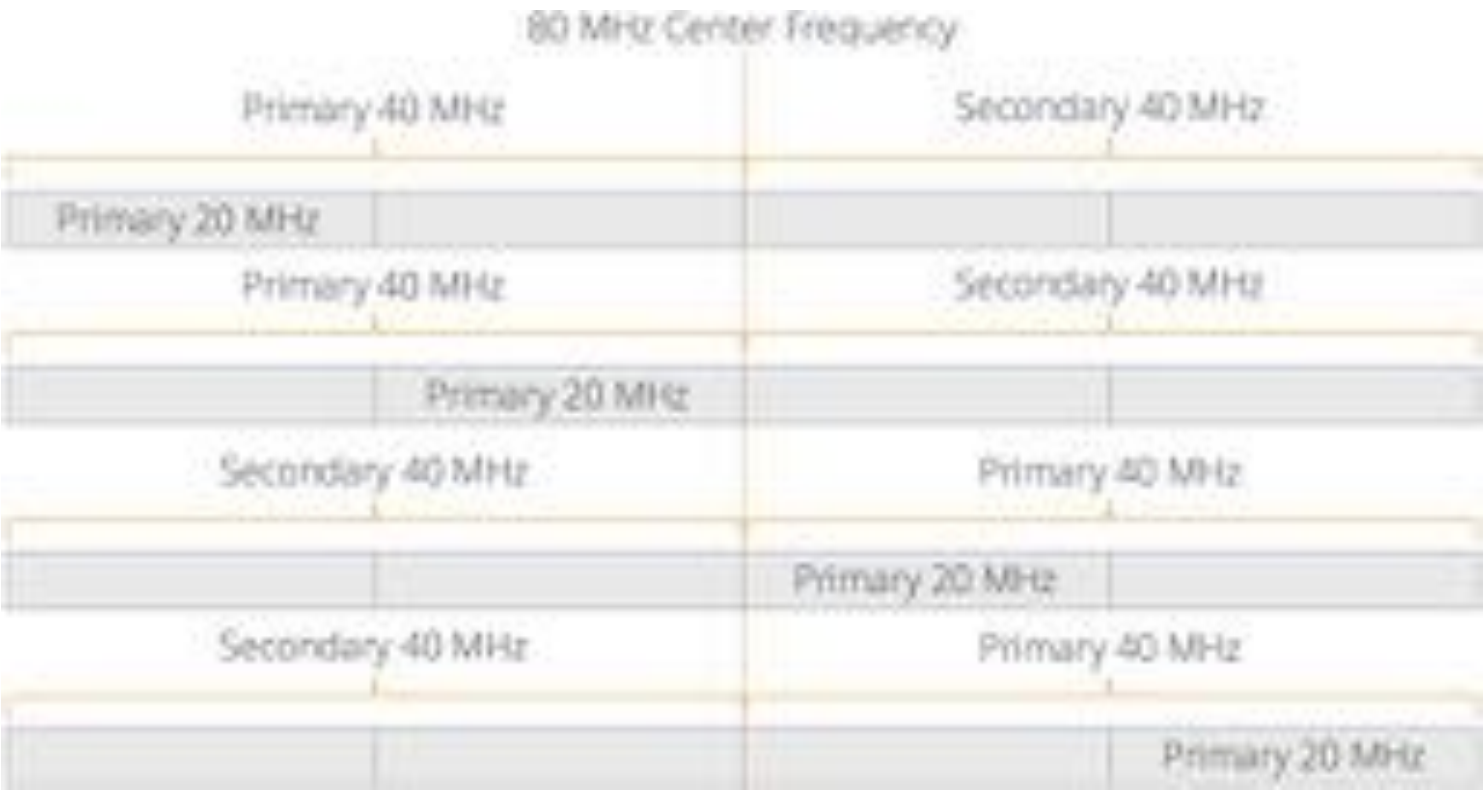
Instead of specifying alternate frequency selections in the case of a DFS hit, Mimosa implemented frequency "Exclusions" that are set on the Channel & Power page. Exclusions are used to mark frequencies that should be avoided, leaving the remainder of the spectrum available for automatic selection based on favorable RF conditions.

WiFi Interop Mode

The WiFi Interop Mode is limited to defined Wi-Fi channels. The graphic below shows the frequencies and channel numbers for 20, 40 and 80 MHz channel sizes.



This allows clients that only support 20 or 40 MHz to connect to an AP that supports up to 80 MHz. Devices with different channel widths can associate and pass traffic as part of the protocol. It is important to choose the primary 20 MHz in the portion of spectrum with the least noise.



Related:

Managing Exclusions and Restrictions - Setting Exclusions and Viewing Restrictions for a Regulatory Domain

Supported Channel Widths

Mimosa Access Points support the following channel widths:

Channel Width (MHz)*	Total Channel Width (MHz)	A5	A5c
1x20	20	Yes	Yes
1x40	40	Yes	Yes
1x80	80	Yes	Yes

* Your regulatory domain may limit allowable channel widths.

Access Point Receiver Sensitivity

Product Applicability: A5/A5c

The table below shows sensitivity in dBm for each MCS index.

MCS Index	Channel Width		
	20 MHz	40 MHz	80 MHz
9	-70.5	-67.5	-64.5
8	-73.0	-70.0	-67.0
7	-75.5	-72.5	-69.5
6	-78.0	-75.0	-72.0
5	-80.5	-77.5	-74.5
4	-83.0	-80.0	-77.0
3	-85.5	-82.5	-79.5
2	-88.0	-85.0	-82.0
1	-90.5	-87.5	-84.5
0	-93.0	-90.0	-87.0

Power over Ethernet Specifications

Product Applicability: A5/A5c

Radio Voltage Input Specifications

Mimosa backhaul radios comply with the 802.3at PoE+ standard. While the radio's nominal operating voltage is 48 volts, it accepts an input voltage range of 44 to 57 volts on a wide variety of pin combinations. An input voltage of -48 Vdc is also acceptable.

The included PoE injector was designed to compensate for voltage drops even over the longest cable runs allowed by the CAT6 standard, less protection circuit losses which net to 100 m (328 feet).

PoE Injector Output Specifications

Mimosa backhaul radios will work with most 802.3at-compliant, 48V PoE adapters. Mimosa recommends the use of the Mimosa provided PoE adapter in order to ensure maximum throughput¹, protection in the event of lightning strike, and to maintain product warranty.

Input Surge Protection

The Mimosa POE is designed to protect connected equipment against voltage and current surges in two ways:

- Transformer isolation between the two Ethernet ports; and
- Gas Discharge Tubes (GDTs) on the DATA+POE port.

In case of lightning, GDTs become a virtual short, diverting surge current and voltage to ground and away from connected equipment. Other PoE's may not have these protections which could lead to equipment damage during a lightning event.

We do not recommend any additional surge protection devices placed between the Mimosa POE and radio because the increased capacitance may cause port flapping between 100BaseT and 1000BaseT.

Input Voltage Range

The Mimosa PoE provides power over all four pairs of wires so there is less voltage drop over a long cable run. Voltage is provided from the Mimosa PoE at 56 Vdc instead of the nominal 48 Vdc for the same reason, although B5/B5c Backhaul radios accept a wider input voltage range (44-57 Vdc). An input voltage of -48 Vdc is also acceptable (see below).

Reverse Polarity Protection

All Mimosa radios include a diode bridge circuit which corrects for reverse polarity on the power inputs, and improves compatibility with 3rd-party 802.3at-compliant PoE injectors and switches that meet the radio's input power specifications.

Table 1 below shows valid combinations of +VE and -VE to the radio on either 2 or 4 wire pairs. All of the combinations below will work so long as the Ethernet signal pairs are connected per the wiring standard.

Ethernet Wiring and Signals	4-Pair PoE Options	2-Pair PoE Options
-----------------------------	--------------------	--------------------

Ethernet Pin	T568A Pair	T568B Pair	1000BASE-T Signal ID	1	2	3	4	5	6	1	2	3	4	5	6	7	8	9	10	11	12
1	3	2	DA+	+	+	+	-	-	-	+	+	+	-	NA	NA	-	NA	NA	-	NA	NA
2	3	2	DA-	+	+	+	-	-	-	+	+	+	-	NA	NA	-	NA	NA	-	NA	NA
3	2	3	DB+	+	-	-	+	-	+	-	NA	NA	+	+	+	NA	-	NA	NA	-	NA
4	1	1	DC+	-	+	-	-	+	+	NA	-	NA	NA	-	NA	+	+	+	NA	NA	-
5	1	1	DC-	-	+	-	-	+	+	NA	-	NA	NA	-	NA	+	+	+	NA	NA	-
6	2	3	DB-	+	-	-	+	-	+	-	NA	NA	+	+	+	NA	-	NA	NA	-	NA
7	4	4	DD+	-	-	+	+	+	-	NA	NA	-	NA	NA	-	NA	NA	-	+	+	+
8	4	4	DD-	-	-	+	+	+	-	NA	NA	-	NA	NA	-	NA	NA	-	+	+	+

Table 1 – Radio Input Voltage Polarization Compatibility

Notes:

1. Performance will be limited if a 10/100BASE-T PoE is used. Mimosa backhaul radios are designed for speeds that exceed the capability of these standards.
2. Some 3rd-party PoE injectors may not have a sufficient power budget to deliver full power to all of their ports depending on how many other PoE-powered devices are installed and how much power each device draws.

Related:

Product Specifications: A5-14, A5-18

Enclosure Ratings

Product Applicability: A5/A5c

The IP is short for International Protection Marking described in IEC standard 60529. This standard classifies and rates the degree of protection provided against the intrusion of solid objects and liquids into electrical enclosures. The two numbers that follow are used to specify the degree of protection. The higher the number, the better the protection. The first number refers to protection against solid objects. The second number refers to protection against liquids.

IP67

- The 6 rating means that the enclosure is totally protected against dust.
- The 7 rating means that the enclosure is protected against the effect of immersion between 15 cm and 1m, although Mimosa does not recommend submerging any of its products.

Protective Vent

The protective vent on the bottom of the radio is designed to reduce stress on the enclosure seals by constantly equalizing the difference in pressure between the inside of the enclosure and the immediate environment. The vent works by allowing air and other gases to pass through its microporous ePTFE membrane freely but stops liquids, dirt and other contaminants from entering the enclosure.

Mounting Hardware

The provided hardware is made from stainless steel, including the hose clamps, ground screw, and cover screws.

Gasket Materials

The black gaskets inside the IP67 gland are made of EPDM (also a synthetic rubber). EPDM also has excellent weatherability characteristics, and is commonly used in weather seals and roofing membranes.

Access Point Installation Overview

A5/A5c

1. Follow the Radio Unlock process.
2. Follow the A5 Installation process.
3. Follow the POE Connection process.
4. Follow the Access Point Setup process.

Radio Unlock Process

Important: An unlock key must be obtained online prior to operation or unlock of the Mimosa Access Point radio. Do not attempt installation in remote locations with limited Internet access without completing the following instructions to obtain an unlock key.

The unlock process provides genuine product assurance and provides the ability to track and monitor your radio easily over the web.

Follow these steps to unlock a radio:

1. Create a Mimosa Cloud account (or log in if already registered)
2. Scan the QR-code on the box, or visit mimosa.co/start from any device (PC or mobile device).
3. Enter the device serial number at mimosa.co/start to obtain an unlock code.*
4. Log into the radio using the default IP address.
5. Type the unlock code (without dashes) on the radio, and then click the Unlock button.
6. Repeat steps 2-5 for each radio. Note that Unlock codes are unique for each serial number.

A5 Unlock Example



Note: The unlock code is unique and reusable for one radio. If a radio is reset to factory defaults, the same code can be entered again on the same radio to unlock it without having to visit mimosa.co/start.

Related:

Change Unlock Country - Replacing an existing unlock code for another regulatory domain

A5 Installation

Follow these steps to mount and ground the A5.

1. Using the included pole mount clamps, tightly attach the bracket to the top section of your mounting pole with a flathead screwdriver.



2. Ground: Use minimum 10 AWG (5.26 mm²) ground wire, less than 1 meter in length.



3. Use only shielded CAT 6 cabling and seal the system with the IP67 gland as shown:



Related:

A5 Specifications - See specification sheet section entitled, "Physical" for additional mounting hardware details.

Hardware & Materials - Details about what materials are used in each provided part.

A5c Installation

Follow these steps to mount and ground the A5c.

1. Option A: Insert the included pole mount clamps through the 2 mounting slots, attach to your mounting pole, and tighten with a flathead screwdriver.

Option B: For antennas with Mimosa A5c quick mount compatible brackets, remove the mounting plate, slide onto the antenna bracket, and tighten.



2. Ground: Use minimum 10 AWG (5.26 mm²) ground wire with a ring terminal connector. The wire should be no longer than 1 meter in length.



3. Using N-type connector jumper cables, connect the antenna to the A5c connectors labeled 1/2/3/4. Connect polarizations in an alternating sequence (e.g. 1-V, 2-H, 3-V, 4-H).



4. Properly seal the four N-connectors using the included mastic tape. Wrap in an upward direction.



5. Use only shielded CAT 6 cabling and seal the system with the IP67 gland as shown:



Related:

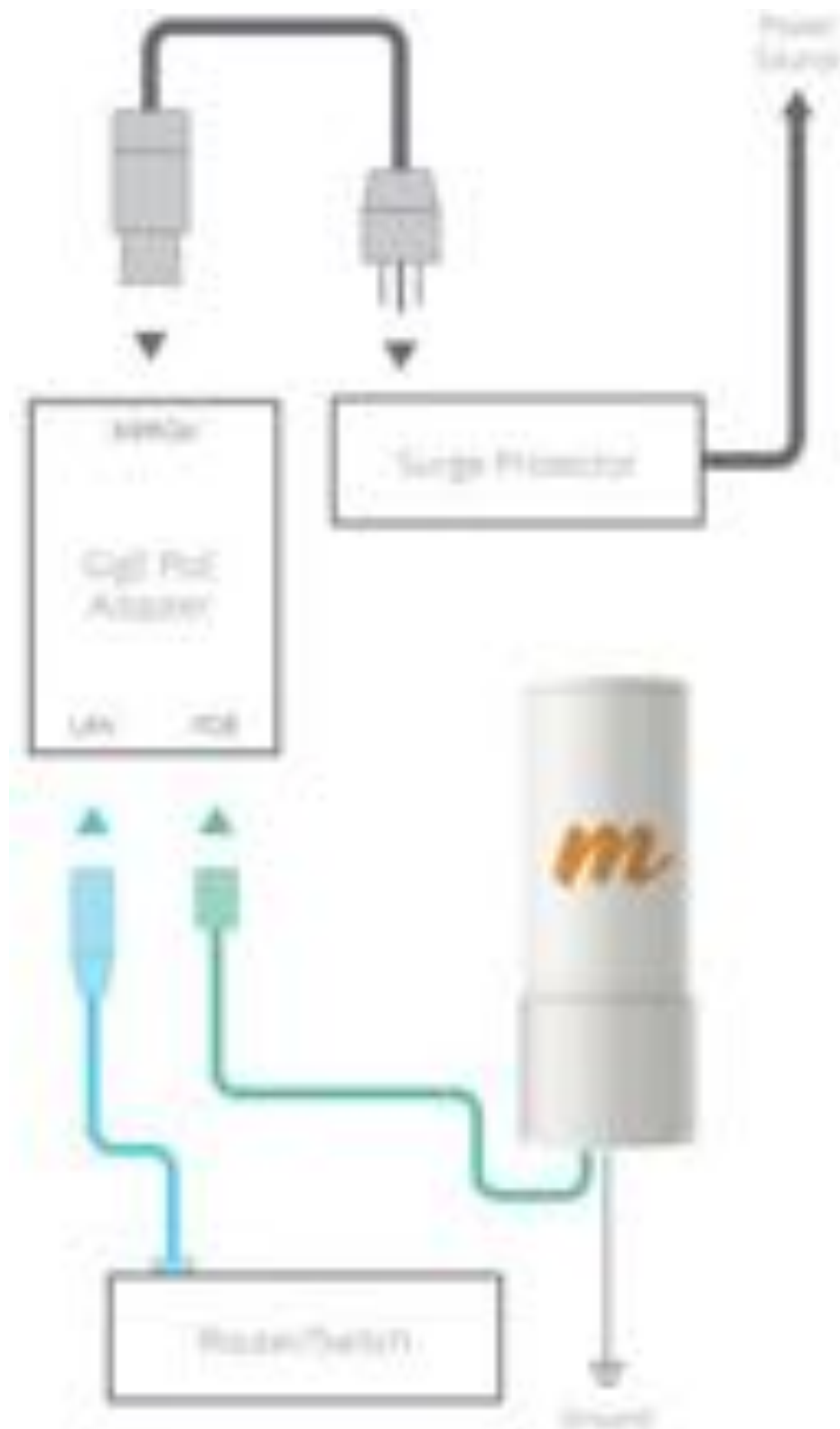
A5c Specifications - See specification sheet section entitled, "Physical" for additional mounting hardware details.

Hardware & Materials - Details about what materials are used in each provided part.

PoE Connections

This process ensures the proper PoE connection to a power source, the radio and the LAN.

1. Connect the provided power cable between the power over Ethernet (PoE) adapter and a power source. A surge protector can be installed between the PoE and the power source, but it is not required.
2. Connect a shielded CAT6 Ethernet cable between the Ethernet port labeled "POE" on the GigE PoE adapter and the radio.
3. Connect a shielded CAT6 Ethernet cable between the Ethernet port labeled "LAN" on the GigE PoE adapter and the LAN side of your network, which is typically a switch or router.



Related:

LED Status Indicators - External LED behavior based on device status.

Access Point Setup

This overview is intended to assist the user with preliminary radio setup prior to deployment.

Notes:

- Internet access is required to access firmware, unlock codes, and online help resources.
- If the radio is connected to a DHCP server, the default IP addresses shown below will be different.

1. Log in or create a Mimosa Cloud account.
2. Download latest Firmware for your device.
3. Connect the PoE to the Radio.
4. Prepare your computer for use.
 - Connect an Ethernet cable between your computer and the PoE port labeled DATA.
 - Ensure that your computer's IP address is different from that of the radio (192.168.1.10), but in the same network. The subnet mask should be the same for both devices (255.255.255.0). Consult operating system documentation for instructions about how to change your computer's IP address.
5. Access the radio in a browser.
 - Open a browser and enter 192.168.1.10 in the address bar.
 - Enter a password that will be used to administer the device.
6. Install firmware image.
 - Select the firmware image from your computer downloaded in step 1 for upload. The radio will validate and install the firmware, and then reboot.
7. Assign a friendly radio name.
 - Navigate to Preferences > General > Device Friendly Name to enter a meaningful radio name.
8. Configure the radio's IP address.
 - Navigate to Preferences > Management > Management IP to ensure the settings match your existing network configuration.
 - After changing the radio's IP address adjust your computer's IP address to operate on the same network.
9. Configure the 5 GHz SSID to which clients will connect.
 - Navigate to Wireless > SSID.
 - Give the SSID a name.
 - Select a type: CPE.
 - Enter an Encryption Key (Passphrase) for the SSID.
 - Ensure that the Broadcast slider is in the ON position.
10. Choose operating frequencies within the 5 GHz Channel & Power panel.
 - Navigate to Wireless > Channel & Power > Channel & Power Settings.
 - Select a desired Channel Width: 20, 40 or 80 MHz.

- Select a desired Center Frequency.
- Set Tx Power to desired level.
- Select a Primary Channel.
- Select a Wireless Protocol.

General

Product Applicability: A5/A5c

FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The radiated output power of this device is below the FCC radio frequency exposure limits. Nevertheless, the device should be used in such a manner that the potential for human contact during the normal operation is minimized. In order to avoid the possibility of exceeding the FCC radio frequency exposure limit, human proximity to the antenna should be more than 9.53m.

Any changes or modifications not expressly approved by Mimosa could void the user's authority to operate this device.

Industry Canada Compliance

This device complies with Industry Canada's license-exempt RSSs. Operation is subject to the following two conditions:

- (1) This device may not cause interference; and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Follow all safety precautions as dictated by your local regulator in installation.

Accessing the Graphical User Interface

Accessing the graphical user interface (GUI) requires that the radio first be connected to power. The Power over Ethernet (PoE) connection process describes the steps to do this. Note that the GUI will be available approximately one minute after applying power.

The GUI can be accessed in three ways to facilitate set-up and management.

1. Locally through the 2.4 GHz or 5 GHz wireless SSID
2. Through the local Ethernet interface (LAN)

Via 2.4 GHz Management Network

On any device with 2.4 GHz 802.11n capability, go to the wireless network listing and connect to the Local Network Management wireless network (SSID): "mimosaMXXX". The default passphrase for the 2.4 GHz connection is "mimosanetworks". Once connected, type 192.168.1.10 into your browser. Please note that both the Local Network Management SSID and passphrase are configurable by the user, so their values could be different from the default values.

Via Ethernet interface or in-band over the 5 GHz Wireless link

By default, the device IP address is 192.168.1.10 and can be accessed via the Ethernet port using this IP address in any standard Web browser. To access the device via a locally connected computer initially (on the same LAN or directly to the Ethernet port), the computer's IP address must be on the same subnet as the above address. Once you have modified the device IP address (static or DHCP) for management purposes, the new IP address must be used to access the device.

Logging In

After connecting via one of the three access methods, the GUI will prompt you to log-in with a password. The default password is "mimosa", and should be changed immediately after login to protect your network since it gives the user read / write privileges. The password can be changed within the Preferences > General > Set Password panel of the GUI.



If you are looking for the Mimosa Cloud Log In process, please see [Manage User Guide: Logging In](#).

User Interface Overview

When you first log in, you'll notice that there is a title bar with the device name shown in the top-right corner, a navigation pane on the left, and a large content pane on the right. The default page shown in the content pane is the Dashboard, which shows a summary of overall performance at a glance, and highlights both radio and link parameters that affect link health.



On the left navigation pane, there are four prominent sections: Overview, Wireless, Preferences, and Diagnostics. Each of these sections contains one or more links to pages containing task-related data, controls, and tools used to administer the radio...and you can return the Dashboard at any time by clicking on the Dashboard link in the Overview section.

The pin in the top corner of the left navigation pane allows you to "pin" open the navigation menu for easier access. Else, the menu contracts to provide more workspace within the GUI. Note that the 2.4 GHz Console menu item is not present on the B5-Lite.



The Dashboard

The Dashboard contains several panels used to group related items. The status panel at the top of the page shows the device name, the number of connected clients, GPS signal quality, and Device Uptime since the last reboot. Detailed help text can be found by clicking on the information icon in the upper right hand corner.



Dashboard Status Bar

The Dashboard Status bar summarizes the following important metrics:

- Device Name - Friendly name of the device.
- Connected Clients - The number of currently connected clients.
- Satellite Signal - Qualitative assessment of GPS/GLONASS signal strength.
- Device Uptime - The elapsed time since the last reboot.

mimosa

A5-360-18 MimosaSth | Logout

MimosaSth

21

Good

14d 6h 4m 47s

Device Name

Connected Clients

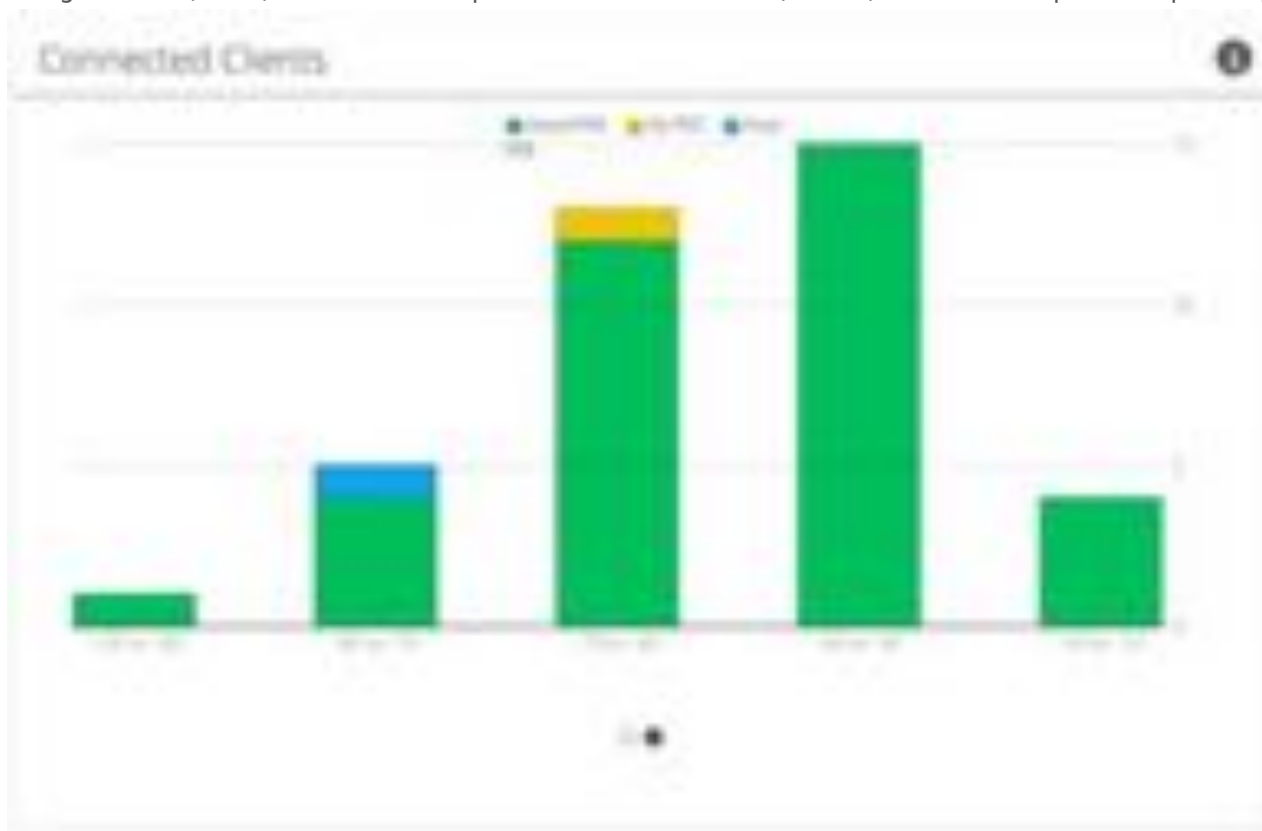
Satellite Signal

Device Uptime

Connected Clients Graph

Clients Graph

This stacked bar graph shows the number of connected clients grouped by their signal strength (dBm). Further, each bar is grouped into 1-3 color-coded segments which represent the packet error rate (PER %). Green color represents low/good PER (0-7%). Yellow color represents moderate PER (7-10%). Blue color represents poor/high PER (>10%).



Airtime Usage

The Airtime Usage chart shows client utilization of total airtime, idle time, and the number of errors. Clients are indicated within the graph based on device name, IP or MAC address.



Configured SSIDs

This table lists both 2.4 GHz and 5 GHz SSIDs

- Name - The SSID name.
- Security - The type of security applied to the SSID.
- Enabled - If checked, indicates that the SSID is active.
- Broadcast - If checked, indicates that the SSID broadcast is on.
- Clients - Number of clients connected to the SSID.

Configured SSIDs 				
Name	Security	Enabled	Broadcast	Clients
5 GHz SSID				
Mimosa	Pre-Shared-Key	✓	✓	28
2.4 GHz SSID				
Mimosa2G	Pre-Shared-Key	✓	✓	0

Reading the Performance Chart

IP Throughput is charted over 60 seconds in 5-second intervals. The newest data shows up on the right and scrolls to the left over time.

The IP Throughput graph plots three lines representing transmit, receive, and total (summed) throughput.



Device Details

The Device Details panel shows a summary of status and identification details for the AP:

- Device Name - The friendly name given to each device. (Set in *Preferences > General > Naming*)
- Serial Number - The unique identifier for the device assigned at the factory.
- CPU Temp 1 - Temperature on the first CPU (operating range: -40 °C to +110 °C).
- Ethernet MAC - The unique identifier for the physical Ethernet interface.
- Latitude - GPS derived latitude coordinate in signed decimal format.
- Altitude - GPS derived altitude in meters and feet.
- Device Time - GPS derived time.
- Firmware Version - The installed firmware version on the AP. (Set in *Preferences > Firmware & Reset*)
- CPU Temp 2 - Temperature on the second CPU (operating range: -40 °C to +110 °C).
- Ethernet Speed - Data rate and duplex mode of the wired Ethernet interface in Mbps.
- Longitude - GPS derived longitude coordinate in signed decimal format.
- Last Reboot - The date and time at which the device was last rebooted.

Device Details			
Device Name	Mimosa5th	Device Time	3/30/16 5:43 PM
Serial Number	2000000043	Firmware Version	2.0.0
CPU #1 Temp	67°C / 153°F	CPU #2 Temp	69°C / 156°F
Ethernet MAC	20-B5-C6-00-F6-14	Ethernet Speed	1000 Mbps
Latitude	37.3515	Longitude	-121.9341
Altitude	26.40 m / 86.61 ft	Last Reboot	3/29/16 9:57 PM

Access Point Settings

The Access Point Settings panel shows a summary of status and identification details for the AP:

- 5 GHz Center Frequency - Center frequency of the current channel in MHz.
- 5 GHz Bandwidth - The selected channel width for 5 GHz operation.
- 5 GHz Tx Power - The current transmit power level of the 5 GHz radio.
- 5 GHz Primary Channel - The primary channel that corresponds with the operating frequency.
- 5 GHz MAC - The unique identifier for the 5 GHz radio.
- 5 GHz Wireless Mode - The 5 GHz radio operating mode: WiFi Interop or GPS+GNSS Sync (Future).
- 2.4 GHz Center Frequency - Center frequency of the current channel in MHz.
- 2.4 GHz Bandwidth - The selected channel width for 2.4 GHz operation.
- 2.4 GHz Tx Power - The current transmit power level of the 2.4 GHz radio.
- 2.4 GHz Wireless Mode - The wireless protocol is fixed for compatibility with 802.11b/g/n.
- 2.4 GHz MAC - The unique identifier for the 2.4 GHz radio.
- IP Address - The network address used to manage the device. (Set in *Preferences > Management*)

Access Point Settings			
5 GHz Center Freq.	5090 MHz	2.4 GHz Center Freq.	2437 MHz
5 GHz Bandwidth	80 MHz	2.4 GHz Bandwidth	20 MHz
5 GHz Tx Power	22 dBm	2.4 GHz Tx Power	16 dBm
5 GHz Primary Channel	140	2.4 GHz Wireless Mode	802.11b/g/n
5 GHz MAC	20:85:C8:00:F6:D4	2.4 GHz MAC	20:85:C8:00:F6:0C
5 GHz Wireless Mode	WiFi Interop	IP Address	10.1.0.3

Client List

The Client List shows settings and metrics between the AP and each client device.

- Client - The name assigned to the client device, or the device MAC address if the device name is unknown.
- MAC - The unique identifier for the client radio.
- IP - The IP address assigned to the client radio.
- SSID - The SSID to which the client is connected.
- BW (MHz) - The Channel Width setting (20/40/80 MHz) used by the client.
- Throughput (Tx/Rx Mbps) - The IP throughput in both directions averaged over the past 10 seconds.
- PHY Rate (Tx/Rx Mbps) - Capacity in both directions
- Streams (Tx/Rx) - Number of data streams in both directions
- MCS (Tx/Rx) - The modulation coding scheme in both directions indicate how well each radio can receive data from the other.
- PER % - The Packet Error Rate (PER) is the number of packets with errors divided by the total number of packets sent within a 5-second period. Ideally, this value should be below 2%, while higher values indicate the presence of interference.
- RSSI (dBm) - Receive Signal Strength Indicator for each of the four RF chains. Larger values are better (e.g. -30 dBm is better than -60 dBm).
- EVM (dB) - Error Vector Magnitude for each of the four RF streams. EVM indicates the difference between the actual and expected amplitude and phase of an incoming signal. Smaller values are better (e.g. -30 dB is better than -10 dB).

To force client disassociation (kick client), click the "x" at the far right end of the client row.

Rate Adaptation dynamically adjusts both the MCS and the number of streams depending on RF conditions.

Poor RF conditions (i.e. interference) cause PER to increase.

PER and MCS are inversely correlated. As PER increases, MCS decreases and vice versa.

Client List												
Client	Mac	IP	SSID	Ch	Channel Width	Max Throughput	Throughput Tx/Rx	MCS Tx/Rx	PER %	RSSI dBm	EVM dB	Kick
Client 1	XXXXXXXXXX	192.168.1.101	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.102	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 2	XXXXXXXXXX	192.168.1.103	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.104	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 3	XXXXXXXXXX	192.168.1.105	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.106	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 4	XXXXXXXXXX	192.168.1.107	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.108	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 5	XXXXXXXXXX	192.168.1.109	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.110	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 6	XXXXXXXXXX	192.168.1.111	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.112	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 7	XXXXXXXXXX	192.168.1.113	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.114	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 8	XXXXXXXXXX	192.168.1.115	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.116	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 9	XXXXXXXXXX	192.168.1.117	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.118	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
Client 10	XXXXXXXXXX	192.168.1.119	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	
	XXXXXXXXXX	192.168.1.120	WiFiNet	20	20.0 MHz	86.7 Mbps	0.00	0.00	0.0	-50.0	-10.0	

Related:

Access Point FAQ: What SNR is required for each MCS?

Access Point FAQ: What is the sensitivity for each MCS index?

Access Point FAQ: What's a good EVM?

SSID Configuration Settings

The SSID Management panel contains controls for configuring how client devices will connect to the access point. To add a new SSID, click on the plus "+" button at the upper right hand corner.

To delete an SSID, click on the blue X icon at the top of the SSID panel. The default 2.4 and 5 GHz SSIDs can not be deleted, and both appear at the top of their respective sections.

SSID Values

- Name - Enter a name for the SSID.
- Band - Select an operating band for this SSID:
 - 2.4 GHz - Compatible with older, roaming clients.
 - 5 GHz - Compatible with newer clients and fixed Mimosa Clients.
 - SSID Type - This field is shown if the 5 GHz band is selected. Select CPE (fixed), or Hotspot (mobile devices), to define the type of clients that will connect to this SSID.
- Enable - Click the slider to turn this SSID on or off. The default 5 GHz SSID can not be disabled.
- Broadcast - Click the slider to turn broadcast of this SSID on or off. When turned on, this feature does not broadcast the name of the SSID in the beacon. Wireless clients will need to manually enter the SSID name and security settings when operating in this mode. Note, while referred to as a hidden SSID, it is still possible to detect the presence of a non-broadcast SSID.
- Client Isolation - Click the slider to turn client isolation on or off. When on, clients are prevented from communicating with each other through the AP in the Layer 2 domain.
- VLAN ID - Enter a non-zero VLAN ID to enable VLAN tagging for this SSID. Enter zero (0) to disable VLAN tagging. VLANs must be unique per SSID.
- Security - Select from the following security options:
 - Open - No authentication or encryption is used. This operational mode is not secure.
 - Enterprise - Users are authenticated and encrypted using radius.
 - Server IP - Enter the IP address of the RADIUS server. This field is shown if the Enterprise option is selected in the Security field.
 - Encryption Key - Enter the secret for the RADIUS server. This field is shown if the Enterprise option is selected in the Security field.
 - Auth. Port - Enter the port number for RADIUS authentication messages (typically 1812).
 - Acct. Port - Enter the port number for RADIUS accounting messages (typically 1813).
 - Pre-Shared Key - There is no user authentication but the link is encrypted using a pre-shared key.
 - Encryption Key - Enter a passphrase to connect to this SSID. This field is shown when the Pre-Shared-Key option is selected in the Security field.
 - Show Encryption Key - Check the box to show the Encryption Key value in clear text, or uncheck it to show asterisks instead.
- RTS/CTS - Configure Request to Send Threshold in bytes: 1-65536 (enter 0 to disable, default is 500).

Pre-Shared Key

The screenshot shows the SSID Configuration Settings panel with the following fields and values:

Name	Type	Enabled	Broadcast	Client Isolation	VLAN ID	Security	Encryption Key	RTS Threshold
Mimosa	CPE	ON	ON	ON	0	Pre-Shared		500

Open

Name	Type	Enabled	Broadcast	Client Isolation	VLAN ID
Mimosa	CPE	ON	ON	ON	0
Security	RTS Threshold				
Open	500				

Enterprise

Name	Type	Enabled	Broadcast	Client Isolation	VLAN ID
Mimosa	CPE	ON	ON	ON	0
Security	Server IP	Encryption Key	Auth Port	Acct Port	RTS Threshold
Enterprise	192.168.1.30		1812	1813	500

Site Survey Results

The Survey Results status table summarizes the results of a site survey, including each SSID broadcast by other devices, their configuration and capabilities.

The table provides the following data per device found:

- SSID - The wireless link name advertised by each detected AP.
- Vendor - The name of the device manufacturer (if known).
- MAC - The device's unique identifier.
- Capability - Indicates which 802.11 (Wi-Fi technology standard) is supported by the device. Options include 802.11a, g, n, ac.
- Channel - Lists the channel on which the device operates.
- Channel Width (MHz) - The size of the channel on which the device operates.
- Frequency Range (MHz) - The frequency range within which the device operates.
- Security - The security or encryption method offered by an AP: Open, Enterprise, or Pre-Shared-Key.
- Signal (dBm) - The received power level from each detected AP.

Use the Start Survey button to place the radio into the scan mode to search for 802.11-compatible access points.

NOTE: It is important to note that running a site survey may temporarily take down your 5 GHz access point. Once activated, this process can not be stopped until complete. Please plan accordingly.

Start

The site survey may take up to 30 seconds to complete.
Your site will be unavailable during this time.

Survey Results

SSID	Vendor	MAC	Capabilities	Channel	Channel Width (MHz)	Frequency Range	Security	Signal
SSID1-2345	Vendor	00:00:00:00:00:00	71g, 71a, 71ac	36	40	5180 - 5220	Pre-Shared-Key	-57
SSID2-6789	Vendor	00:00:00:00:00:00	71g, 71a, 71ac	149	40	5755 - 5795	Pre-Shared-Key	-61
SSID3-1234	Vendor	00:00:00:00:00:00	71g, 71a	36	40	5180 - 5220	Pre-Shared-Key	-65
SSID4-5678	Vendor	00:00:00:00:00:00	71g, 71a	36	40	5180 - 5220	Pre-Shared-Key	-69
SSID5-9012	Vendor	00:00:00:00:00:00	71g, 71a	36	40	5180 - 5220	Enterprise	-71
SSID6-3456	Vendor	00:00:00:00:00:00	71g, 71a, 71ac	40	40	5180 - 5220	Pre-Shared-Key	-75
SSID7-7890	Vendor	00:00:00:00:00:00	71g, 71a	149	40	5755 - 5795	Enterprise	-80
SSID8-2345	Vendor	00:00:00:00:00:00	71g, 71a	149	40	5755 - 5795	Enterprise	-85

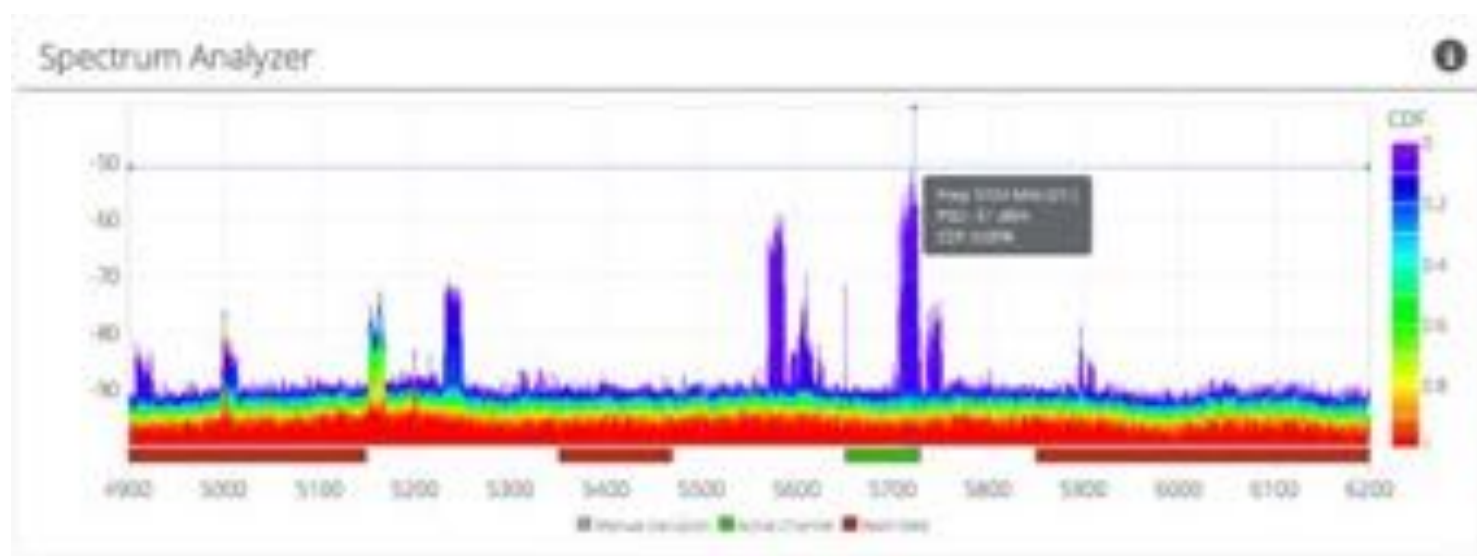
Reading the Spectrum Analyzer

The Spectrum Analyzer actively scans the 5 GHz band in the background to report on interference sources that may impact link performance.

Channels in use have higher Power Spectral Density (PSD), or amplitude, on the vertical axis, and are shaded in different colors to represent how often the signals are likely to be on the same frequency at the same amplitude. The legend to the right of the graph explains the color code for the Cumulative Distribution Function (CDF). The color red suggests the highest probability (1 = 100%), while purple represents the lowest probability (0 = 0%). Cross hairs appear on the graph beneath the mouse pointer along with an information box containing the frequency (channel), PSD, and CDF values.

There are three types of markings, or bars, immediately beneath the graph's horizontal axis that indicate frequency ranges that are restricted, manually excluded, or in active use by this link. Note that traffic from the Active Channel is excluded from the display so that noise can be detected.

NOTE: Viewing Remote or Combined Spectrum View is not supported on the A5/A5c at this time.



5 GHz Channel & Power

The 5 GHz Channel & Power panel allows for changing the channel, channel width, power and Automatic Gain Control (AGC) values.

- Auto Channel Selection - Click the slider to turn Auto Channel Selection on or off. This function selects the channel that results in the best RF performance.
- Channel Width (MHz) - Choose the channel width for access point operation: 20 MHz, 40 MHz or 80 MHz.
- Center Frequency (MHz) - Select the center frequency of the channel used on the access point. The center frequency represents the absolute center of the selected channel width without any offset.
- Tx Power (dBm) - Set the desired transmit power level. The allowed options are determined by a combination of country and chosen frequency.
- Primary Channel - Select the primary channel number that corresponds with the operating frequency.
- Wireless Mode - Select the wireless mode that the AP should support.
 - WiFi Interop - Select for compatibility with newer 3rd party Access Points.
 - GPS+GNSS Sync (Future) - Mimosa proprietary TDMA protocol for fixed Clients.
- Traffic Optimization - This feature improves throughput at higher client counts. The default value is on. Changing this value requires a reboot.
- AGC Mode - The Automatic Gain Control (AGC) feature is used to set the signal level below which the radio ignores incoming RF interference. The choices are Off or Manual.
- AGC Minimum Rx Power (dBm) - In Manual mode, select an Rx power level below your expected signal, but above other interference (-90 to -10 dBm).
- Antenna Gain (dBi) - On an A5c, set the gain according to antenna specifications and subtract out any cable/connector loss.

5 GHz Channel & Power

Auto Channel Selection	OFF	Channel Width (MHz)	20
Center Frequency (MHz)	5210	Tx Power (dBm)	18
Primary Channel	36	Wireless Mode	WiFi Interop
Traffic Optimization	ON		
AGC Mode	Manual	AGC Minimum Rx Power (dBm)	-85
Antenna Gain (dBi)	16		

2.4 GHz Management Interface

The 2.4 GHz Management Interface panel allows changes to channel, channel width, and power.

- Channel Width (MHz) - The channel width for access point operation is fixed for 20 MHz operation.
- Center Frequency (MHz) - Select the center frequency of the channel used on the access point. The center frequency represents the absolute center of the selected channel width without any offset.
- Tx Power (dBm) - Set the desired transmit power level. The allowed options are determined by a combination of country and chosen frequency.
- Wireless Protocol - The wireless protocol is fixed for compatibility with 802.11b/g/n.

2.4 GHz Management Interface i

Channel Width (MHz)	20	Center Frequency (MHz)	2437
Tx Power (dBm)	16	Wireless Mode	802.11b/g/n

Managing Exclusions & Restrictions

Exclusions list the frequency ranges in which the device should not operate. The excluded bands will be shown as shaded regions on the Spectrum Analyzer.

- Start Frequency - Specify the lower limit for the exclusion range, not including this frequency.
- End Frequency - Specify the upper limit for the exclusion range, not including this frequency.
- Add New Exclusion - Click the button to add the Start and End Frequency range to the exclusion list.
- Existing Exclusions and Restrictions - Exclusions can be removed from the list by clicking on the trash icon. The restricted bands with the lock icon cannot be removed. They are protected because of regulatory requirements.
- Regulatory Domain - The country in which the device has been configured to operate.

In the United States, if either the AP or Clients are within a 60 km radius of a Terminal Doppler Weather Radar (TDWR) location, one or more 30 MHz restrictions are automatically created to avoid the TDWR operating frequencies.

Exclusions & Restrictions

Add a New Exclusion (MHz)

Start Frequency End Frequency

+ Add New Exclusion

Exclusion Start (MHz)	Exclusion End (MHz)
5000	5100

Regulatory Domain: US

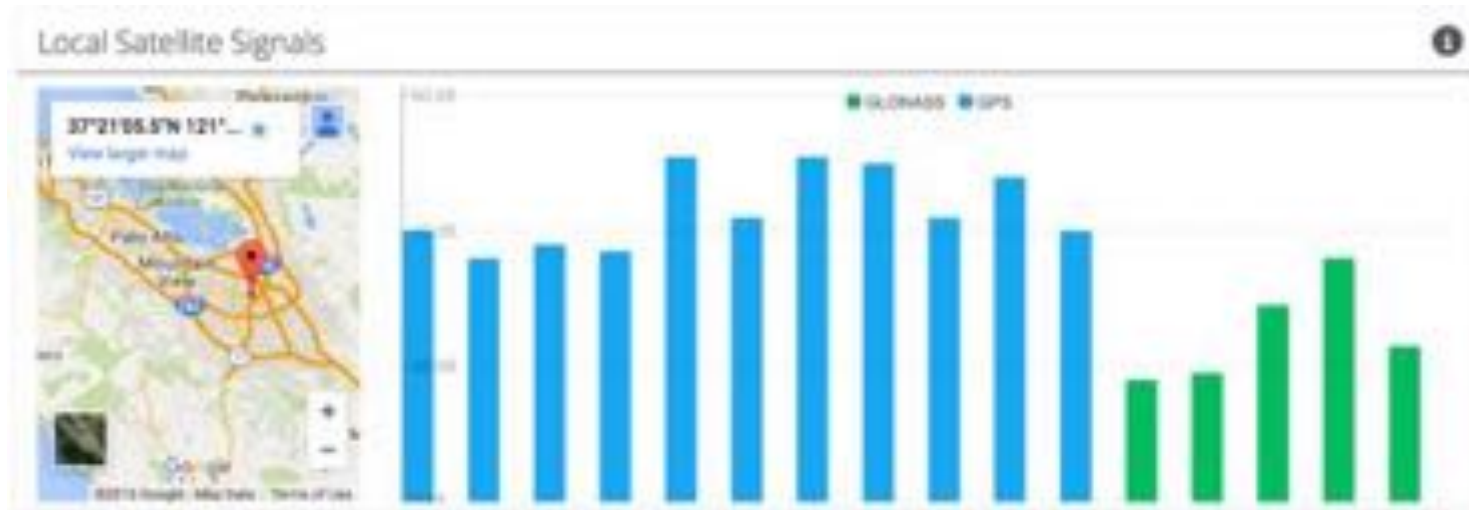
Related:

Change Unlock Country - Replace an existing unlock code to enable another regulatory domain

Interpreting Local Satellite Signals

The Local Satellite Signals panel contains a chart showing both GPS and GLONASS satellites in blue and green, respectively, from which the radio can obtain position and timing data used for synchronization. Each numbered column represents a unique satellite with the columns' amplitude representing the signal to noise ratio of the satellite's signal at the radio's receiver. The number of satellites the radio detects and the SNR of each both contribute to clock accuracy.

If GPS location is detected, a Google location image of the access point location will be shown on the leftmost portion of the Satellite Signal page. If no GPS signals are detected the Google location map will be blank.



Reading Satellite Information

The Satellite Information panel contains values that represent and contribute to clock accuracy. Good GPS signal strength is required for maximum performance, as the GPS is used to synchronize timing between devices.

- Satellite Signal Strength - Qualitative assessment based on all items below; also displayed on the Dashboard.
- Satellite Avg SNR - Average signal to noise ratio (dB) amongst satellites.
- Total Satellites - Sum of detected GPS and GLONASS satellites.
 - GPS - Number of GPS satellites detected.
 - GLONASS - Number of GLONASS satellites detected.

Satellite Information				
Satellite Signal Strength	Good	Total Satellites	16	
Satellite Avg SNR	37.25 dB	GPS	1, 6, 7, 11, 13, 15, 17, 19, 24, 28, 30	
		GLONASS	67, 68, 77, 86, 87	

Viewing Location Data

Status table showing coordinates and altitude for both the local device.

Location Data	
Latitude	37.3515
Longitude	-121.9341
Altitude	27.40 m / 89.90 ft

Access Control Lists

Access Control Lists remark QoS settings and control the flow of traffic by allowing or denying network traffic based on matching criteria for MAC or IP address, and network protocol. The ACL is also used to specify traffic priority by remarking the TC or DSCP header.

Click the "Add a New Rule" button to add a new rule.

Click the trash can icon to the right of each row to remove rules.

- Unique Name - Enter a friendly name to describe the rule.
- Direction - Select Inbound or Outbound (from the Ethernet port).
- Match Type - Select IP or MAC.
- Source Address - Enter the IP address or MAC of the source device.
- Source Mask - Enter the subnet or MAC mask of the source device.
- Destination Address - Enter the IP Address or MAC of the destination device.
- Destination Mask - Enter the subnet or MAC mask of the destination device.
- Protocol - Select an IP protocol from the list: TCP, UDP, ICMP.
- Permit - Select Allow or Deny; applies to traffic that matches the rule criteria.
- TC - ToS QoS Mark. Enter a number from 0 (lowest priority) to 7 (highest priority).
- DSCP - QoS Mark. Enter a number from 0 (lowest priority) to 63 (highest priority).

Access Control List

Use the Access Control List to specify which ports, MAC addresses, and IP address combinations are permitted to access and use this device.

Unique Name	Direction	Match Type	Source Address	Source Address Mask	Dest. Address	Dest. Mask	Protocol	Permit	TC	DSCP
HighPriority	Inbound	IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	TCP	Allow	0-7	63
HighPriorityOut	Outbound	IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	TCP	Allow	0-7	63

Traffic Shaping Plans

The Traffic Shaping Plans panel is used to manage plans and to control the maximum rate limit and committed rate shaping for each fixed client. By default a new fixed client that connects to a Fixed Client SSID will be assigned to the default plan. Editing an existing plan may impact its existing subscribers. You must first remove all fixed clients from a traffic shaping plan before deleting or renaming it.

Click on the "+" icon in the top right corner to add a new plan.

Click the trash can icon to the right of each row to remove the plan. The default plan can not be deleted.

- Name - Friendly name of the traffic shaping plan.
- Downlink Max (Mbps) - Enter the maximum download capacity to the client.
- Downlink Commit (Mbps) - Enter the minimum download capacity. During times of throughput contention, the access point will attempt to maintain this capacity for the client. Other traffic above the commit will be de-prioritized.
- Uplink Max (Mbps) - Enter the maximum upload rate to the client.
- Uplink Commit (Mbps) - Enter the minimum upload capacity. During times of throughput contention, the access point will attempt to maintain this capacity for the client. Other traffic above the commit will be de-prioritized.
- Clients - The number of clients currently subscribed to the traffic shaping plan.

Traffic Shaping Plans

Editing an existing Traffic Shaping Plan may impact its existing subscribers. A plan's name cannot be changed unless there are no connected clients.

Name	Downlink Max (Mbps)	Downlink Commit (Mbps)	Uplink Max (Mbps)	Uplink Commit (Mbps)	Clients	
default	1000	1000	1000	1000	166	
Change Test	5	5	5	5	0	
Side Test	25	5	25	5	1	

Fixed Clients

The Fixed Clients panel is used to identify and assign plans and SSID's to each client. Click the "+" button at the top right corner of the panel to add fixed clients. Click the trash can icon at the right of each row to remove a client/subscriber.

- Friendly Name - The name of the fixed client.
- Brand - Enter the manufacturer of the client device.
- Model - Enter the model number of the client device.
- MAC - Enter the MAC address of the client device.
- SSID - Enter the SSID to which the client will connect.
- Plan - Select from the list of traffic shaping plans defined in the Traffic Shaping Plans panel.

Some values are automatically learned, but each can be manually overridden.

Fixed Clients

+

i

Friendly Name	Brand	Model	MAC	SSID	Plan
sub_name	non-mimosa	c5	00:00:00:00:00:00	Mimosa	default
sub_name	non-mimosa	c5	00:00:00:00:00:00	Mimosa	default
sub_name	non-mimosa	c5	00:00:00:00:00:00	Mimosa	default
sub_name	non-mimosa	c5	00:00:00:00:00:00	Mimosa	default
sub_name	non-mimosa	c5	00:00:00:00:00:00	Mimosa	default

Setting a Device Name

The device name is a local identifier for administrative purposes, and is not used as part of the wireless link.

- Device Friendly Name - Name for the local device displayed on the Dashboard.

Naming

Device Friendly Name

SysTestA5

Session Management

- Session Timeout - Set the number of minutes (0-60) of inactivity that will be allowed on the interface before automatic log-out for browser sessions when accessing the device GUI. If set to "0", the browser session will have no timeout.

Session Management

Session Timeout

Time in minutes. 0 is infinite. 60 minutes max.

General Miscellaneous Settings

The Miscellaneous panel contains general functionality not described elsewhere.

- Unlock Code - Displays the code used to unlock the device.

Miscellaneous

Unlock Code

MZN-SFR-Q7L

Related:

Change Unlock Country - Replace an existing unlock code to enable another regulatory domain

Enabling System Log Notifications

Enable Syslog service on the local device to send traps to a remote Syslog server.

- Enable - Enable or disable Syslog service on the local device.
- Protocol - Choose the desired protocol for the Syslog connection. Note that most devices send UDP messages by default. UDP is an unreliable transmission protocol, thus messages may get lost. Choose TCP for higher reliability if any message loss is unacceptable.
- Remote Log IP Address - List the IP Address of the remote Syslog server to which Notifications will be sent.
- Remote Log Port - List the Port on the remote Syslog server to which Notifications will be sent.

System Log Notifications

Enable

OFF

Protocol

TCP

Remote Log IP Address

Remote Log Port

514

Setting a Password

Enter the new password in both the New Password and Verify New Password input boxes to validate that they were typed correctly. To finalize the change, enter the existing password and then save. By default, the password is "mimosa", and it should be changed during device configuration to protect your network.

- New Password - Enter the new password.
- Verify New Password - Re-enter the new password (to confirm).
- Current Password - Enter the existing password (as a security measure).

The Password rules are as follows for choosing a password:

- It must be between 6 to 64 characters.
- It can use capital (A-Z) or lower case (a-z) characters, excluding space.
- The password cannot contain a space.
- The password cannot be blank.
- There is no complexity required for the password.



The image shows a web form titled "Set Password". It contains three input fields: "New Password", "Confirm New Password", and "Current Password". The "Current Password" field is preceded by the text "To change password, you must enter your current password below:". The form is styled with a light gray background and rounded corners.

Set Password	
New Password	
Confirm New Password	
To change password, you must enter your current password below.	
Current Password	

Setting the Management IP Address

The Management IP panel contains controls for setting the device's network address, subnet, gateway and DNS servers.

- IP Mode - Select the preferred mode of network addressing: Static or DHCP+Static Failover. If Static is chosen, the device will always use the IP address that has been assigned. If DHCP+Static Failover is chosen, and a DHCP server is available, then the addresses are automatically assigned by the DHCP server. If a DHCP server is unavailable, the device will use the static IP address listed below.
- IP Address - The network address used to manage the device.
- Netmask - The subnet mask that defines the network subnet.
- Gateway - The gateway address for the subnet.
- Primary DNS - The first DNS server IP Address. Default is 8.8.8.8.
- Secondary DNS - The backup DNS server IP Address. Default is 8.8.4.4.



The screenshot shows a web interface titled "Management IP" with a help icon in the top right corner. The interface contains several configuration fields, each with a label, a current value, and a text input box for modification. The fields are: IP Mode (set to Static), IP Address (192.168.1.10), Netmask (255.255.255.0), Gateway (192.168.1.1), Primary DNS (8.8.8.8), and Secondary DNS (8.8.4.4). Each field has a "Current" value displayed below the label.

Field	Current Value	Input Box Value
IP Mode	Static	Static
IP Address	192.168.1.10	192.168.1.10
Netmask	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.1.1
Primary DNS	8.8.8.8	8.8.8.8
Secondary DNS	8.8.4.4	8.8.4.4

Rogue DHCP Server Protection

The Rogue DHCP Server protection feature prevents DHCP servers other than the ones you specify from assigning IP addresses.

Click the "+" icon in the upper right corner of the panel to add up to 5 servers.

Click the "x" icon next to a DHCP server to remove it from the list.

Click the edit icon (to the left of "x") to edit a server's IP address.

- Rogue DHCP Protection - Turn Rogue DHCP server protection on or off.
- DHCP Server # - Enter the IP address of one or more allowed DHCP servers.

The screenshot shows a configuration panel titled "Rogue DHCP Server Protection". In the top right corner, there is a "+" icon and an information icon "i". Below the title, there is a toggle switch for "Rogue DHCP Protection" which is currently set to "OFF". Below the toggle, there is a table with two rows of DHCP servers. Each row has a label "DHCP Server #1" and "DHCP Server #2", an input field containing the IP addresses "32.2.55.1" and "1.1.1.21", and two action buttons: an edit icon (pencil) and a delete icon (x).

Rogue DHCP Server Protection		
Rogue DHCP Protection		OFF
DHCP Server #1	32.2.55.1	[Edit] [X]
DHCP Server #2	1.1.1.21	[Edit] [X]

Application Prioritization

The Application Prioritization feature adjusts performance for certain types of traffic by changing the QoS priority for each. When enabled, these settings override Traffic Shaping Plans.

- Prioritize Traffic - Turn application prioritization on or off.
- Application Name - Select a value for each application: Off, Low, Medium, High, or Highest.

Application Priority	DSCP Value	WMM Queue
Low	0	0
Medium	16	1
High	32	2
Highest	47	3



VLAN Management

The VLAN Management panel allows the administrator to enable a VLAN (Virtual Local Area Network) for management traffic by entering a VLAN ID. When a value is entered, all Web Management traffic must originate from a device on that VLAN.

- Management VLAN - Upon activating the Management VLAN, the GUI of this device will become inaccessible over Ethernet, unless connecting over a network configured with a matching VLAN number.
- Management VLAN ID - The VLAN ID tag can range from 2 to 4094. Leave blank to disable VLAN tagging.
- VLAN Passthrough - This feature allows all VLANs to pass through from A5 to C5. This feature is not compatible with per-SSID VLANs, so they must first be disabled before enabling this feature.



The screenshot shows the 'VLAN Management' configuration panel. It has a title bar with the text 'VLAN Management' and an information icon (i) on the right. Below the title bar, there are three settings:

- Management VLAN:** A toggle switch that is currently turned 'ON' (blue).
- Management VLAN ID:** A text input field containing the value '96'.
- VLAN Passthrough:** A toggle switch that is currently turned 'ON' (blue).

Miscellaneous Management

The Miscellaneous panel contains controls to enable Mimosa Cloud Management.

- Mimosa Cloud Management - Enables the device to use Mimosa Cloud Management tools. Data will be collected and stored the Mimosa Cloud.

Performing a Firmware Update

The Firmware Update panel displays the current firmware version and date, and allows the user to upload a new firmware image. The latest firmware image may be downloaded from help.mimosa.co. Alternately, firmware can be pushed to the device automatically through the Manage application at manage.mimosa.co.

- Installed Version - The currently installed firmware version.
- Update Firmware - Update to the latest firmware. Click the Browse File button to select a file for upload the file.



The firmware update process occurs in four phases:

1. Upload - Selecting a firmware image and uploading to the radio
2. Verification - Ensuring that the firmware image is complete and without errors
3. Upgrade - Writing the new firmware image to flash memory
4. Reboot - Restarting with the new firmware image

Reset & Reboot the Device

Reboot the device or reset it to its original factory settings.

- Factory Reset Device - Clears all configuration settings and locks the device. WARNING: This will delete ALL saved configuration settings and return the device to the locked factory state. You will be required to re-enter your unlock key upon device reset. The current version of firmware will remain, however.
- Reset Device Configuration - Clears all configuration settings. The device will remain unlocked.
- Reset Device Unlock - Locks the device and resets the country code. WARNING: You will be required to re-enter your unlock key upon reset.
- Reboot Device - Restarts the device.



Backup or Restore Configuration Settings

The Backup and Restore Configuration panel contains controls for managing configuration settings files.

Configuration files have the format: config.<devicename>.tar.gz

- Backup Current Configuration - Perform a backup by downloading the configuration file.
- Restore Configuration - Click the Choose File button to upload a previously saved configuration file.

Backup & Restore

Backup Current Configuration

Download File

Restore Configuration

Choose File

Diagnostic Tests

Two types of tests are available within the Diagnostics section: Ping and Traceroute.

Ping Test

A low level ICMP test which indicates whether the target host is reachable from the local device.

- Destination Host - The destination IP Address of the device to ping.
- Packet Count - The number of packets to transmit during a ping.
- Packet Size (kB) - The size of each packet to transmit during a ping.
- Run Test - Click on the Run Test button to ping the destination IP address. Results are shown in the corresponding table.

Traceroute Test

A network utility used to display the path and transit delay between the local device and a given destination across an IP network.

- Destination Host - The destination IP address for traceroute to send packets.
- Max Number of Hops - Choose the maximum number of intermediate devices (e.g. routers) through which packets must pass between source and destination.
- Run Test - Click on the Run Test button to begin the traceroute test. Results are shown in the corresponding table.

Running a Ping Test

A low level ICMP test which indicates whether the target host is reachable from the local device.

- Destination Host - The destination IP Address of the device to ping.
- Packet Count - The number of packets to transmit during a ping.
- Packet Size (kB) - The size of each packet to transmit during a ping.
- Run Test - Click on the Run Test button to ping the destination IP address. Results are shown in corresponding table.



The screenshot shows a web interface for running a Ping test. It features two tabs: 'Ping' (selected) and 'Traceroute'. Below the tabs, there are three input fields: 'Destination Host' with the value '8.8.8.8', 'Packet Count' with the value '20', and 'Packet Size' with the value '64'. Each input field has a small up/down arrow icon to its right. At the bottom of the form is a button labeled 'Run Test' with a circular arrow icon to its left.

Running a Traceroute Test

A network utility used to display the path and transit delay between the local device and a given destination across an IP network.

- Destination Host - The destination IP address for traceroute to send packets.
- Max Number of Hops - Choose the maximum number of intermediate devices (e.g. routers) through which packets must pass between source and destination.



The image shows a web-based configuration interface for running a Traceroute test. At the top, there are two tabs: 'Ping' and 'Traceroute', with 'Traceroute' being the active tab. Below the tabs, there are two input fields. The first is labeled 'Destination Host' and contains the IP address '127.0.0.1'. The second is labeled 'Maximum Hops' and contains the number '30'. To the right of the 'Maximum Hops' field is a small downward arrow icon. Below these fields is a button labeled 'Run Test' with a play icon to its left.

Diagnostic Logs

View Events and download diagnostic information to share with Mimosa Support.

- Logging - This is a persistent (non-volatile) log of all significant events that occur.
- Support Info - Download a single file containing all information required by Mimosa Support to help with troubleshooting.

LoggingSupport Info

Mar 21 15:09:34	:	CPE with MAC		added with plan default
Mar 21 15:31:03	:	CPE with MAC		added with plan default
Mar 21 15:38:41	:	CPE with MAC		added with plan default
Mar 21 15:59:48	:	CPE with MAC		added with plan default
Mar 21 16:17:43	:	CPE with MAC		added with plan default
Mar 21 16:17:53	:	CPE with MAC		added with plan default
Mar 21 17:17:06	:	CPE with MAC		added with plan default

LoggingSupport Info

Customer Support

Download the support file and send it to Mimosa if requested. This file is encrypted and can only be read by Mimosa.

Download

A5 External LED Status Indicators

Product Applicability: A5/A5c

Three LED indicators on the outside of the case communicate operational status: Power, Ethernet, and Wireless.

A5 Status LED Indicators



●  Power ●  Ethernet ●  Wireless

A5c Status LED Indicators



Power On LED Sequence

The tables below describe the boot sequence for the A5. The A5 is operational approximately 10 seconds after Step 5 is reached.

Step	Sequence Name			
1	Power Initialization - Phase 1			
2	Power Initialization - Phase 2			
3	System Initialization (All LEDs are off for 8 seconds)			
4	System Loading			
5	Ready (Operational)			

Power Status LED Table

The Power Status LED indicates the presence of power.

State	LED	Description
-------	-----	-------------

Off		No Power to Device
Solid Green		Ready (Operational)

Ethernet Status LED Table

The Ethernet Status LED indicates the negotiated port speed for the wired network connection. The device is designed to perform best with a 1000BASE-T connection. While other port speeds are possible, they are not recommended because they create a data bottleneck that reduces end-to-end throughput.

State	LED	Description
Off		No Ethernet Connection
Solid Green		1000BASE-T
Blinking Green		1000BASE-T with Traffic
Solid Yellow		100BASE-T
Blinking Yellow		100BASE-T with Traffic
Solid Red		10BASE-T
Blinking Red		10BASE-T with Traffic

Wireless Status LED Table

The Wireless Status LED indicates at least one client is connected to the access point.

State	LED	Description
Off		Not clients associated
Solid Blue		Associated client (one or more)

Troubleshooting GPS Signal Strength

The A5 and A5c Access Points utilize high-precision GPS and GLONASS timing sources to synchronize their communication and facilitate collocation. Up to 48 satellites are detectable: 24 from GPS and 24 from GLONASS. The Dashboard and Wireless > Location pages display the number of satellites, signal strength, and timing quality. If these timing sources are unavailable (such as while indoors or when GPS signals are otherwise blocked), the wireless links will still associate and operate but with lower performance. In this case, a Time Synchronization Function (TSF) is used to exchange timing information between radios in the same link. This mode is represented on the Dashboard as "No GPS" whenever GPS/GLONASS signals are absent.

GPS performance can usually be improved by relocating the radio physically, and there are several considerations depending on the installed conditions:

- Verify there are satellites present in the graph on the Wireless > Location page. There may be only a small number of satellites, or only satellites with low SNR present in the graph.
- Ensure that the top of the radio has an unobstructed view to the sky. Even when located outdoors, GPS signals can still be blocked by physical objects for a portion of time. Note any patterns such as specific times when GPS signals are degraded.
- Relocate the radio away from any high-power transmitters (TV, LTE cellular/mobile, or FM) that are mounted on the same tower or nearby.

Testing Throughput with iPerf

Mimosa has found that iPerf, a tool for active measurements of the maximum achievable bandwidth on IP networks, provides the most reliable measure of TCP performance. Instructions for downloading iperf, building the executable for your environment, and usage are available at this link: <https://github.com/esnet/iperf>

Example Test Topologies

- Computer 1 - Mimosa 1 - Mimosa 2 - Computer 2
- Computer 1 - Switch 1 - Mimosa 1 - Mimosa 2 - Switch 2 - Computer 2

Example Commands

The iPerf (version 2) commands below send 10 TCP streams for 100 seconds with 64k TCP window size in one direction. Open separate terminal windows and reverse the commands to create bidirectional traffic.

Command to make Computer 1 (192.168.1.22) the *listener*:

```
iperf -s -f m -i 60
```

Command to make Computer 2 (192.168.1.23) the *sender*:

```
iperf -c 192.168.1.22 -P 10 -t 100 -w 64k
```

Note: Mimosa radios do not contain iPerf. For accurate measurement, the device under test should not generate traffic because the test would impair the ability of the device by occupying the CPU and skewing the test result. Please see the link below for more information about the Mimosa bandwidth test.

Access Point Firmware Roadmap

Firmware Version 2.0.2

July, 2016 (Planned)

Product Applicability: A5, A5c

New Features

Long Distance Support for Mimosa Clients

Auto ranging for Mimosa clients up to 40 km (25 miles) away, limited only by SNR. This feature is targeted for A5c, and also works for A5 when SNR is sufficient, but does not yet work for third-party clients. Note: large SNR differences between client(s) and AP reduce overall performance.

VLAN Passthrough

Pass all VLAN tagged traffic from A5 to C5 and beyond. VLAN Passthrough is not compatible with per-SSID VLANs, so they must first be disabled before enabling this feature. This firmware version allows SSID edits, except for the per-SSID VLAN field.

Application Prioritization

Easy QoS controls for specific types of traffic: HTTP/HTTPS, VPN, ICMP, Torrents, and video streaming services. When enabled, these settings override Traffic Shaping Plans.

Rogue DHCP Server Protection

Prevents DHCP servers other than the ones you specify from assigning IP addresses.

Compliance

- Updated regulatory database: Netherlands

User Interface

- Added Mimosa client distances to client page
- Primary channel number now shown in spectrum graph
- Removed 2.4 GHz SSID Type (CPE/Hotspot) option
- Special characters now allowed in GUI password (except for space)
- Synchronized Tx power on Dashboard after power change
- Added Tx power compression threshold warning

Performance Management

- Support for G2 network-wide health monitoring
- Resolved periodic drops in cloud connectivity

Traffic Management

- Improved throughput for VPN/PPPoE traffic
- Updated ACL L2 input validation

PHY and MAC Improvements

- Resolved A5-C5 channel width discrepancies
- Increased Tx gain table dynamic range for A5c

Access Point Firmware

Updating your device firmware enables the latest product enhancements and provides improvements to stability and performance. To ensure the highest quality experience, only the latest two versions are available here for download. Firmware can be downloaded from this page and uploaded to each radio manually (Preferences > Firmware & Reset > Firmware Update).

Alternately, firmware can be installed directly from the Manage application, either in bulk to your entire network, or to select devices in an order that you specify.

A5 Production Firmware

Version	Date	Firmware Download	Release Notes
2.0.1	May 13, 2016	Mimosa-A5-2.0.1.img.signed	

Firmware 2.0.1 Release Notes

May 13, 2016

Product Applicability: A5-14, A5-18, A5c

New Features

- Support for cloud management enhancements
- Added GPS/GLONASS satellite count and SNR to cloud data

Compliance

- Updated regulatory database: Russia, US (higher Tx power in U-NII-3)

User Interface

- Added Management VLAN Enable/Disable slider control
- Added validation for IP and MAC address masks in ACL rules
- Added Syslog controls

Resolved Issues

- Resolved high PER when changing channel width from 40 to 80 MHz
- Resolved per-SSID VLAN issues that prevent VLAN resets, high PER, and missing client details
- Fixed client traffic shaping entries can now be deleted before client association
- Static IP address now persistent after changing from Static to DHCP+failover
- Memory management and system stability improvements

Known Issues

- Spectrum analysis sometimes becomes unavailable requiring a reboot
- No option to turn off 2.4 GHz management radio
- Ranging issues with clients at long distance
- Low performance with 20 MHz channel sizes in certain conditions

Firmware 2.0.0 Release Notes

March 31, 2016

Product Applicability: A5-14, A5-18

The Mimosa A5 access point delivers cutting-edge multipoint technology for service providers to affordably deliver the industry's first scalable gigabit wireless broadband network. Our small form-factor hardware leverages years of engineering protocol development to provide operators with high performance connectivity to both Mimosa C5 and 3rd party clients.

Performance Features

- Supports WiFi Interoperability mode. SSIDs in CPE Mode utilize RTS/CTS frame control technology and account for longer distance CPE links. This optimizes network throughput, reduces collisions and prevents re-transmissions. Mimosa GPS Sync utilizing TDMA will be a software update in a later release.
- Up to 750 Mbps delivered to connected clients
- Supports up to 100 5 GHz clients
- Quad directional smart sector transmits and receives only on the antennas required to maximize SNR in both directions
- Advanced network processing unit provides controls for capacity and subscriber management
- Traffic shaping plans to set committed and maximum rates per client
- Supports four pre-configured levels of QoS for prioritizing voice, video, best effort and background traffic.
- Broad frequency range spans 4900 – 6200 MHz, restricted by country of operation
- Smart spectrum management actively scans, monitors and logs ongoing RF interference across all channels with no service impact
- Auto Channel Selection picks the optimum channel and channel width for highest performance and avoids severe interference.
- Automatic Gain Control (AGC) to squelch RF signals providing high immunity to lower powered, nearby WiFi and planned self-interference

Security Features

- WPA2 or Enterprise 802.1x for user/password authentication
- Wireless Client Isolation to prohibit wireless clients from communicating with one another
- Access Control Lists to permit, deny and remark Layer 2 and Layer 3 traffic flows
- VLAN to SSID mapping

Management Features

- HTML5 based web UI
- Mimosa Cloud monitoring and management
- Support for up to 8 SSID's on 5 GHz
- GPS location for accurate device position and timing utilizing GNSS1 (GPS + GLONASS)
- 2.4 GHz 802.11b/g/n radio for local management
- DHCP Snooping and OUI mapping for detecting client name and type
- Management VLAN

Known Issues

- Static IP address may be overwritten after changing from Static to DHCP+failover
- C5 channel width is sometimes misreported on the A5
- No cancel buttons on traceroute or ping
- Setting a per-SSID VLAN may reset another per-SSID VLAN
- Client name and IP address is sometimes not visible after per-SSID VLAN is set
- Enabling and then disabling per-SSID VLANs may cause high PER on some clients

Roadmap Items

- Mimosa GPS Sync mode (TDMA) for synchronization and collocation
- Advanced MU-MIMO
- Hotspot Support
- HTTPS
- SNMP and REST
- Syslog
- Auto exclusions for TDWR
- Ping watchdog

Optimizing Traffic with Access Control Lists

Certain types of traffic, such as video or management, may require special Quality of Service (QoS) settings. The Access Control List (ACL) within the A5 provides the ability to re-tag traffic to (re)assign priority based upon a set of specified criteria.

Example - Add a rule to increase the priority for ICMP (ping) traffic

1. Click the "+ Add a New Rule" button.
2. Enter a descriptive name, such as "ICMP-DL". In this case, "DL" stands for downlink. Traffic from an A5 to a C5 is considered "downlink", while traffic from a C5 to an A5 is considered "uplink".
3. Select "Inbound" as the traffic Direction, which is from the perspective of the Ethernet port. Inbound traffic on Ethernet is destined for a C5 with the exception of management traffic to the A5.
4. Select "ICMP" in the Protocol drop down.
5. Select "Allow" in the Permit drop down.
6. Enter a number in the DSCP input box between 0 (lowest priority) and 63 (highest priority). In this case, we have selected 63 which is the highest priority.

The screenshot shows the 'Access Control List' configuration page. At the top, there is a '+ Add a New Rule' button and a descriptive text: 'Use the Access Control List to specify which ports, MAC addresses, and IP address combinations are permitted to access and use this device.' Below this is a table with columns: Unique Name, Direction, Match Type, Source Address, Source Address Mask, Dest. Address, Dest. Mask, Protocol, Permit, TC, and DSCP. Three rules are listed:

Unique Name	Direction	Match Type	Source Address	Source Address Mask	Dest. Address	Dest. Mask	Protocol	Permit	TC	DSCP
ICMP-DL	Inbound	IP	0.0.0.0	0.0.0.0	192.168.1.*	255.255.255.255	ICMP	Allow	0.7	63
UDP-DL	Inbound	IP	0.0.0.0	0.0.0.0	192.168.1.*	255.255.255.255	UDP	Allow	0.7	63
TCP-DL	Inbound	IP	0.0.0.0	0.0.0.0	192.168.1.*	255.255.255.255	TCP	Allow	0.7	63