

Enterprise



**Driving Operational Efficiency: A Guide
to Using AirWave Wireless Management
Suite™ for Service Desk Troubleshooting**

Table Contents

Introduction	2
Problem #1: “I can’t get onto the network”	3
2.1 Step 1: Has the user ever connected?	3
2.2 Step 2: Has the user connected recently?	3
2.3 Step 3: Check the user’s AP association history.....	4
2.4 Step 4: Check the usual AP’s status	5
2.5 Step 5: Check the SSID	5
2.6 Step 6: Look at the network status in the user’s work area.....	6
2.7 Step 7: Look for alerts on AP or authentication issues	6
Problem #2: “The network is slow”	7
3.1 Step 1: Verify the work location	7
3.2 Step 2: Check the SSID	7
3.3 Step 3: Examine the signal quality	7
3.4 Step 4: Look at bandwidth usage	8
3.5 Step 5: Check that the user is connected to the usual AP	9
3.6 Step 6: Confirm coverage at the user’s physical location	9
3.7 Step 7: Check AP usage levels	11
3.8 Step 9: Look for IDS alerts	12
Problem #3: “My connection keeps dropping”	13
Using AirWave to Escalate to Network Engineering	13
Summary	14

1. Introduction

In a typical IT organization, the service desk takes incoming user support calls and determines whether the problem is an individual user or device issue or a broader network issue that might affect multiple users. The service desk itself usually handles the individual user problems and escalates broader network issues to the network engineering or network operations team.

With wireless networks, most user complaints boil down to one of three observable problems:

- "I cannot connect to the wireless network."
- "The wireless network is slow."
- "My connection keeps dropping."

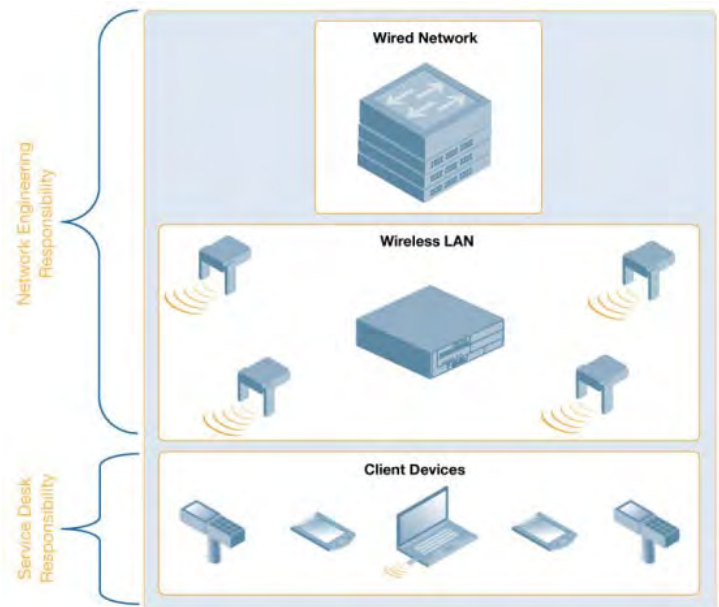
There are dozens of different potential root causes for any of these three symptoms. Many, if not most, of these problems are related to client device settings or authentication issues — issues that the service desk should be able to resolve quickly over the phone. Problems, such as issues with wireless controllers or APs or issues in wired infrastructure, require direct involvement from various teams within network engineering. Unfortunately, when the service desk does not have the tools and diagnostic capabilities to perform a first-level triage, most issues are escalated directly to network engineering. No one likes the result. Users are unhappy because their problems are not resolved quickly. The service desk staff becomes frustrated because they cannot do their jobs. Network engineers suffer because they are swamped with calls related to the wireless LAN (WLAN).

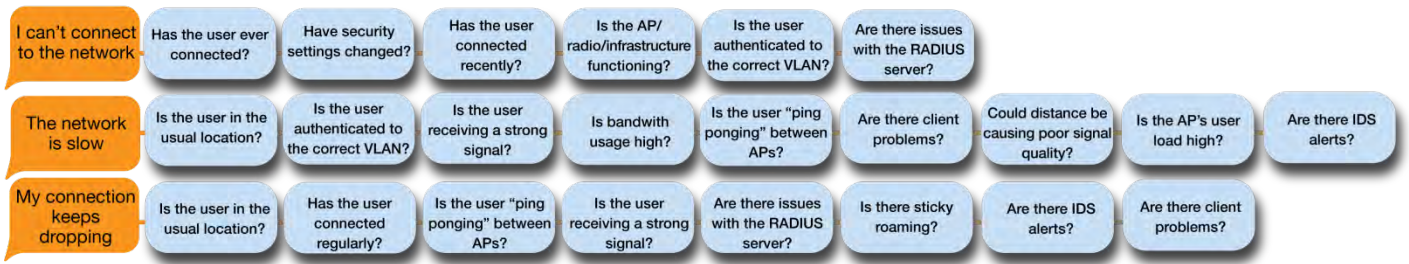
AirWave Wireless Management Suite™ from Aruba Networks, consists of AirWave Management Platform™ (AMP), AirWave RAPIDS™ Rogue Detection and AirWave VisualRF™ Location and Mapping, gives the IT organization a more efficient way to handle all aspects of wireless support. With its easy-to-use interface and user-centric approach, AirWave is designed to let the service desk do triage and troubleshooting, so that the network engineering staff can focus on the real Level 3 problems.

This white paper provides a step-by-step guide explaining how service desk staff can use AirWave to:

- Distinguish between common user and device problems and network issues
- Diagnose and resolve client issues
- Gather useful information to enable faster problem resolution when issues must be escalated to network engineering

The figure at the right depicts the basic troubleshooting workflow process for the service desk. Most of its steps can be performed in minutes with read-only access to AirWave, usually while the user is still on the telephone. By following this process, you start with the problem reported by the user and work your way through the most common root causes, including client device configuration problems, AP/load issues and RF coverage issues.





The AirWave troubleshooting process for the service desk.

2. Problem #1: "I can't get onto the network"

When a user cannot connect to the network at all, the problem often relates to security or configuration settings on the device with which he or she is trying to connect. Therefore, the troubleshooting process starts by ascertaining the likelihood of improper settings.

2.1 Step 1: Has the user ever connected?

When a user has never connected to the network, the first step is to check security and configuration settings. Talk the user through a checklist of the proper security and configuration settings until you are sure that the device is set up appropriately. If the user still cannot connect, continue through the steps described below.

2.2 Step 2: Has the user connected recently?

Because AirWave automatically tracks every user and device that associates with your network, you can easily verify whether the user has recently connected by entering his or her username in the search box available in the top right-hand corner of every page of the AirWave Management Platform (AMP). Anyone who has recently connected, whether or not he or she is currently on the network, will appear in the search results. (The length of time during which past user associations appear in these search results depend on how your organization has configured AMP.) It is possible to search for a user via MAC address, although few users would have this information available during a service desk interaction.

Users:

1-6 of 6 Users Page 1 of 1 Choose Columns

Username	Role	MAC Address ▲	AP/Device	SSID	VLAN	AP Radio	Connection Mode	Association Time
ARUBANETWORKS\pthormycroft	employee	00:05:4E:4D:9D:6A	AL37	ethersphere-wpa2	65	802.11an	802.11a	2/27/2009 2:09 PM
ARUBANETWORKS\peter	-	00:11:F5:53:AE:0F	Cisco1200-Airwave	trampledrose	0	802.11a	802.11a	11/3/2009 2:41 AM
ARUBANETWORKS\dpeterson	employee	00:19:7E:4C:EB:7A	AL27	ethersphere-wpa2	65	802.11an	802.11a	11/6/2009 3:41 PM
Peter Lane-ext5172	vocera	00:1D:6A:49:C2:5B	AL1	ethersphere-vocera	66	802.11bgn	802.11g	11/3/2009 2:44 AM
ARUBANETWORKS\peter	employee	00:1F:3B:79:EF:E3	AL1	ethersphere-wpa2	65	802.11an	802.11n (5GHz)	11/9/2009 8:59 AM
ARUBANETWORKS\pthormycroft	employee	00:21:6A:02:44:8C	AL37	ethersphere-wpa2	65	802.11an	802.11n (5GHz)	11/9/2009 8:24 AM

The search summary results page shows the MAC address, AP and SSID, association time and other relevant information. Notice that the users who are currently connected are highlighted in green. For users who aren't connected, you see information about the most recent connection.

If the user has not connected recently, determine whether he or she has changed hardware recently. Also, consider whether there have been changes to security policies that may have made the user's device configuration obsolete. For example, some organizations are still transitioning parts of the WLAN from Wired Equivalent Privacy (WEP) to Wi-Fi Protected Access (WPA) and WPA2. In either case, you may have to take the user through all or part of the security and configuration checklist described above.

If the user has connected recently, it is more efficient to complete Steps 3–7 before considering device-level problems.

2.3 Step 3: Check the user's AP association history

First, log into the AirWave Management Platform (AMP) and find the user via search. Click on his or her MAC address to access the user's individual details. At the bottom of the user details page, you will find a table displaying the user's association history. It will tell you if the user always connects to the same AP so that you can check its status. Verify verbally that the user is in his or her usual location. If the user is not in his or her usual location, you will want to skip to Step 6; otherwise, continue to Step 4.

Device Information

Username: ARUBANETWORKS\pthornycroft
 Vendor: Intel Corporate
 First Seen: 2/26/2009 3:44 PM on AL19 for 2 mins
 Last Seen: 11/11/2009 12:49 PM on AL37 for 30 mins
 Classification: Unclassified

Alert Summary at 11/11/2009 12:49 PM

Type	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-
Incidents	0	0	0	-
RADIUS Authentication Issues	0	0	0	-

Signal Quality for 00:21:6A:02:44:8C Last 2 hours

Maximum Average
 Signal Quality 45 38.8

Bandwidth for 00:21:6A:02:44:8C Last 2 hours

Maximum Average
 Bits Per Second In 2.1 Mbps 237.8 kbps
 Bits Per Second Out 81 kbps 17.3 kbps

Association History

1-20 of 115 Past Associations Page 1 of 6 > | Choose Columns

Username	AP/Device	SSID	VLAN	Connection Mode	Association Time	Duration	Auth. Type	Cipher
ARUBANETWORKS\pthornycroft	00:0b:86:c3:68:fa	ethersphere-wpa2	2360	802.11g	11/9/2009 6:48 AM	45 mins	EAP	-
ARUBANETWORKS\pthornycroft	00:0b:86:c3:68:fa	ethersphere-wpa2	2360	802.11g	11/6/2009 5:25 PM	45 mins	EAP	-
ARUBANETWORKS\pthornycroft	AL37	ethersphere-voip	66	802.11n (5GHz)	11/6/2009 2:40 PM	1 hr 56 mins	WPA2	AES
host/peter-x200.arubanetworks.c	AL37	ethersphere-voip	66	802.11n (5GHz)	11/6/2009 2:10 PM	30 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL37	ethersphere-voip	66	802.11n (5GHz)	11/6/2009 12:29 PM	1 hr 40 mins	WPA2	AES
host/peter-x200.arubanetworks.c	AL37	ethersphere-voip	66	802.11n (5GHz)	11/6/2009 12:14 PM	15 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL33	ethersphere-wpa2	65	802.11n (5GHz)	11/6/2009 12:04 PM	10 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL37	ethersphere-wpa2	65	802.11n (5GHz)	11/6/2009 8:28 AM	3 hrs 36 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	00:0b:86:c3:68:fa	ethersphere-wpa2	2360	802.11g	11/6/2009 6:46 AM	50 mins	EAP	-
host/peter-x200.arubanetworks.c	AL37	ethersphere-voip	66	802.11n (5GHz)	11/5/2009 5:05 PM	1 hr 5 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL37	ethersphere-wpa2	65	802.11n (5GHz)	11/5/2009 8:16 AM	8 hrs 49 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	00:0b:86:c3:68:fa	ethersphere-wpa2	2360	802.11g	11/5/2009 6:48 AM	50 mins	EAP	-
ARUBANETWORKS\pthornycroft	00:0b:86:c3:68:fa	ethersphere-wpa2	2360	802.11g	11/4/2009 5:35 PM	25 mins	EAP	-
ARUBANETWORKS\pthornycroft	AL37	ethersphere-voip	66	802.11n (5GHz)	11/4/2009 4:07 PM	49 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL37	ethersphere-voip	66	802.11n (5GHz)	11/4/2009 3:07 PM	40 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL37	ethersphere-voip	66	802.11n (2.4GHz)	11/4/2009 2:32 PM	35 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL33	ethersphere-voip	66	802.11n (2.4GHz)	11/4/2009 1:41 PM	50 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL37	ethersphere-voip	66	802.11n (2.4GHz)	11/4/2009 12:11 PM	1 hr 30 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL40	ethersphere-wpa2	65	802.11n (5GHz)	11/4/2009 12:06 PM	5 mins	WPA2	AES
ARUBANETWORKS\pthornycroft	AL33	ethersphere-wpa2	65	802.11n (5GHz)	11/4/2009 12:01 PM	5 mins	WPA2	AES

1-20 of 115 Past Associations Page 1 of 6 > |

2.4 Step 4: Check the usual AP's status

You can click directly into the AP itself using the hyperlink in the association history table and view the appropriate AP monitoring page. At the top of the page, you will see the status as well as a quick view of the overall situation on the AP. When the user can't connect, you need only be concerned about whether the AP is up or down and whether the configuration status is good or somehow out of policy. We visit this page again when we review the steps to troubleshoot a slow connection.

Monitoring **AL1** in group **Ethersphere-lms3** in folder **Top > Sunnyvale H**

This Device is in monitor-only-with-firmware-upgrades mode.

Status: Up (OK)
Configuration: Good

Controller: Ethersphere-lms3

LAN MAC Address:	Aruba AP 125	Remote AP:	No	Last Contacted:	11/9/2009 9:36 AM	Uptime:	31 days 15 hrs 32 mins
IP Address:	10.6.1.222	Serial:	AJ0000138	Total Users:	10	Bandwidth:	1615 kbps
First Radio:	802.11bgn	MAC Address:	00:1A:1E:25:94:D0	Users:	5	Bandwidth:	3 kbps
Second Radio:	802.11an	MAC Address:	00:1A:1E:25:94:C0	Users:	5	Bandwidth:	1612 kbps
Wired Interface:	Enet0 (uplink only)	MAC Address:	00:1A:1E:CA:59:4C	Users:	0	Channel:	11
Wired Interface:	Enet1	MAC Address:	00:1A:1E:CA:59:4D	Users:	0	Channel:	36

Notes:

Your network engineering team has set up AMP to poll the network infrastructure at a predetermined interval, usually every 5 to 10 minutes. If you want up-to-the-second information, you can click the polling buttons on the AP monitoring page. (Depending on the infrastructure deployed on your WLAN, this button may say "Poll Controller Now" or "Poll Now.") If you do identify a down AP or one that's out of policy, go to Section 5 of this document and follow the steps for escalating to network engineering.

If the AP is down, the AP monitoring page provides explanatory text that can be useful in escalating the problem to the appropriate resource. For example, in the situation depicted below, the root cause of the problem appears to be a downed switch. In many organizations, different engineering teams handle wired and wireless infrastructure. By escalating to the appropriate resource, you can get your user's problem fixed more quickly.

Monitoring **AP001d.4591.141a** in group **Cisco Gear** in folder **Top**

This Device is in monitor-only-with-firmware-upgrades mode.

Status: Down (AP is No Longer Associated with Controller - Upstream Device **switch10.dev.airwave.com** is Down)
Configuration: Mismatched (The settings on the device do not match the desired configuration policy.)

Firmware: 6.0.182.0 (IOS: 12.4(21a)JA)

Controller: Airespace-5500

Type:	Cisco Aironet 1250 LWAPP	Controller Interface:	1	Last Contacted:	11/9/2009 6:03 PM	Uptime:	-
LAN MAC Address:	00:1D:45:91:14:1A	Serial:	FTX1151901E	Location:	some location	Bandwidth:	-
IP Address:	10.51.1.98	Total Users:	-	Bandwidth:	-	Users:	-
First Radio:	802.11an (Statistics)	MAC Address:	00:17:DF:A1:1E:70	Users:	-	Bandwidth:	-
SSIDs:	123 (123), 5500 8021x (5500 8021x), 5500 CKIP (5500 CKIP lab la la), 5500 guest (5500 guest_bundle), 5500 wep short ascii 3 (5500 wep short ascii 3), 5500 WPA2 PSK (5500 WPA2 PSK), 5500 WPA2 WEB (5500 WPA2 WEB), 5500 WPA2C RADIUS (5500 WPA2C RADIUS), 5500-wpa-psk-hex (5500-wpa-psk-hex), 5500-wpa2-psk-hex (5500-wpa2-psk-hex)						

Second Radio: None

Notes:

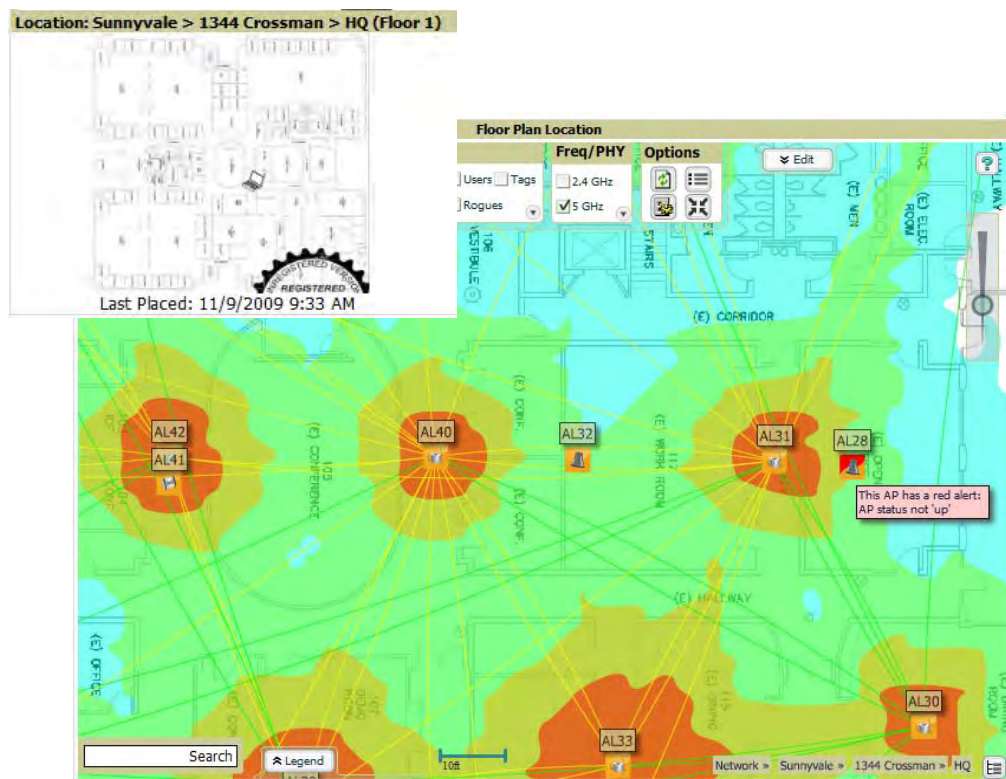
2.5 Step 5: Check the SSID

The user details page shows the SSID to which the user is connected. In some cases, the user may have connected to the wrong network (for example, a guest network or voice network). The user may report a problem such as "I can't connect to the Internet" or "I can't access my file servers." You can quickly remedy the problem by correcting the SSID setup in the user's wireless network connection.

NOTE: If AMP does not show a user being connected to your network but he or she reports network access, the user may be connected to a rogue access point or other unauthorized ad hoc network. In this case, the service desk should contact network engineering immediately and offer the user assistance in reconfiguring the connection.

2.6 Step 6: Look at the network status in the user's work area

If you suspect that another AP is involved, you can click on the floor plan thumbnail on the user details page to get a visual view of the network. You may see another down AP in the user's work area. Depending on how your organization has configured the system, these APs may be depicted with a red background in the floor plan. Alternatively, if your network engineering team has used AMP to set up folders or groups that correspond to physical locations (for example, a "New Jersey Warehouse Facility" folder), you can navigate to the folder (Home-APs/Devices- <Foldername>) to check the status of APs in the user's location.



2.7 Step 7: Look for alerts on AP or authentication issues

The user details page contains an Alerts section that shows AMP alerts (generally notifications that an AP is going up and down, incidents (trouble tickets set up in AMP, which are described in Section 4 of this white paper), and alerts on RADIUS authentication issues).

RADIUS authentication issues are common causes of connectivity problems. AMP might show these alerts when:

- A client is misconfigured
- The user is entering an incorrect password
- The back-end RADIUS server did not respond to an authentication request, either due to network issues causing timeouts or because the server is down

Alert Summary at 12/17/2009 10:57 AM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	23	219	412	12/17/2009 10:57 AM
IDS Events	280	3616	10055	12/17/2009 10:55 AM
Incidents	0	0	11	11/6/2009 7:55 AM
RADIUS Authentication Issues	6	73	195	12/17/2009 10:23 AM

3. Problem #2: “The network is slow”

As with connectivity problems, slow network connections have a variety of causes. Always start by asking the user how he or she knows that the network is slow. The subjective information that he or she provides, such as “When I’m in my office it’s always much faster!” may save you some steps in the troubleshooting process described below.

3.1 Step 1: Verify the work location

Determine whether this user connects regularly and whether he or she is in the usual work location. You can ask the user and verify his or her responses via the user details page in AMP (see Steps 3 and 4).

3.2 Step 2: Check the SSID

Many organizations have guest networks that leverage the same APs as their internal networks but that are configured to run at a slower data rate. When a user inadvertently connects to the guest network, the problem may present itself as a slow connection. You can check the SSID to which your user is connected through the search summary results or on the user details page.

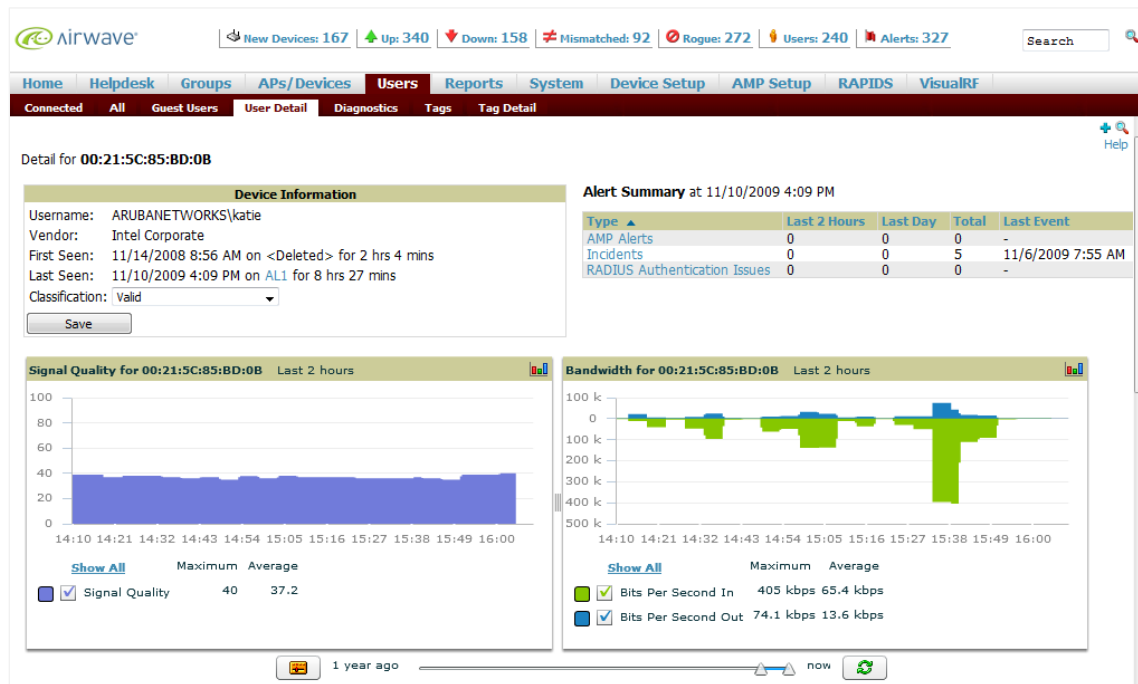
Users:

1-6 of 6 Users Page 1 of 1 Choose Columns

Username	Role	MAC Address ▲	AP/Device	SSID	VLAN	AP Radio	Connection Mode	Association Time
ARUBANETWORKS\pthornycroft	employee	00:05:4E:4D:9D:6A	AL37	ethersphere-wpa2	65	802.11an	802.11a	2/27/2009 2:09 PM
ARUBANETWORKS\peter	-	00:11:F5:53:AE:0F	Cisco1200-Airwave	trampledrose	0	802.11a	802.11a	11/3/2009 2:41 AM
ARUBANETWORKS\dpeterson	employee	00:19:7E:4C:EB:7A	AL27	ethersphere-wpa2	65	802.11an	802.11a	11/6/2009 3:41 PM
Peter Lane-ext5172	vocera	00:1D:6A:49:C2:5B	AL1	ethersphere-vocera	66	802.11bgn	802.11g	11/3/2009 2:44 AM
ARUBANETWORKS\peter	employee	00:1F:38:79:EF:E3	AL1	ethersphere-wpa2	65	802.11an	802.11n (5GHz)	11/9/2009 8:59 AM
ARUBANETWORKS\pthornycroft	employee	00:21:6A:02:44:8C	AL37	ethersphere-wpa2	65	802.11an	802.11n (5GHz)	11/9/2009 8:24 AM

3.3 Step 3: Examine the signal quality

In the next set of steps, you will use the rich set of information available on the user details page as well as the diagnostics tab for the user. On the middle of the page, you will see a chart showing current signal quality to historical levels. You can use the slider at the bottom of the chart to adjust its time scale to include data for up to one year in the past, so that it reflects a relevant picture of the user’s network usage.



The numbers on this chart represent raw signal strength. While >20 generally represents an ideal value across wireless networks, actual values vary significantly across infrastructure vendors and customer environments. Therefore, it's more important to look at trends — comparing the user's signal strength to his or her previous experience on the network — than to absolute values.

3.4 Step 4: Look at bandwidth usage

To the right of the signal quality chart, the user details page includes a chart showing the user's bandwidth usage. Again, you can use the slider at the bottom of the chart to adjust its time scale to include historical data for up to one year. Note that this graph shows bandwidth usage from the perspective of the AP. Bandwidth "in" from the device to the AP is at the bottom of the chart, while bandwidth "out" from the AP to the device is at the top. Look for deviations from historical bandwidth usage rates. If you see anything unusual, you can click to the user diagnostics page for further evaluation.

The screenshot shows the AirWave interface for a user. At the top, there are status indicators: New Devices: 167, Up: 341, Down: 157, Mismatched: 92, Rogue: 272, Users: 161, Alerts: 348. The navigation menu includes Home, Helpdesk, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, and VisualRF. The current page is 'Users' with sub-tabs for Connected, All, Guest Users, User Detail, Diagnostics, Tags, and Tag Detail. The main content area is titled 'Diagnostics for 00:17:3F:20:99:6B' and contains a 'Possible Issues' table, a 'Diagnostic Summary' table, and a 'Current User Counts' table.

Issue	Ideal	Actual
Low signal quality:	>= 20	-
Excessive roaming in last two hours:	<= 10 roams	0
High user bandwidth:	<= 50% of radio capacity	-
Unauthenticated user:	Authenticated	Not Authenticated
High user load on AP/radio:	<= 15	6
High AP/radio bandwidth:	<= 75% of radio capacity	3 kbps (0.01%)
802.11b users associated to 802.11bg radio:	None	0
802.11bg or 802.11a users associated to 802.11n radio:	None	-
High FCS error rate:	<= 100	51

	Current	Last Hour	Last 2 Hours	Last 4 Hours	Last 8 Hours	Last Day	Last Week
User Bandwidth	-	0 kbps (0.00%)	0 kbps (0.00%)	0 kbps (0.00%)	0 kbps (0.00%)	0 kbps (0.00%)	0 kbps (0.00%)
Radio Bandwidth	3 kbps (0.01%)	11 kbps (0.03%)	11 kbps (0.03%)	17 kbps (0.05%)	20 kbps (0.06%)	20 kbps (0.06%)	37503 kbps (109.73%)
AP Bandwidth	3 kbps (0.00%)	11 kbps (0.02%)	11 kbps (0.02%)	18 kbps (0.03%)	21 kbps (0.03%)	21 kbps (0.03%)	57054 kbps (83.46%)
Radio User Count	6	6	6	6	6	6	7
AP User Count	6	6	6	6	6	7	10
Signal Quality	-	0	0	0	0	0	0

	User Count on AP	User Count on Radio
802.11bg	6	6
Total	6	6

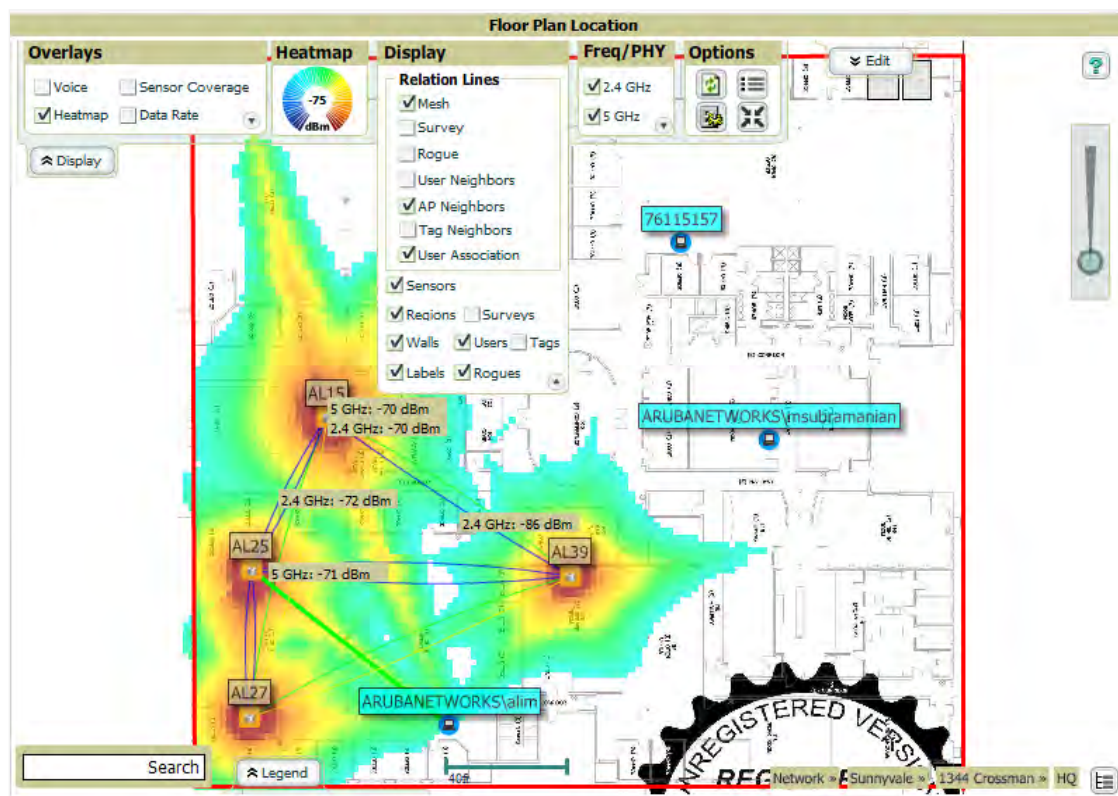
At the top of this page, you will see a table that shows a snapshot of the user's connection and a list of possible connectivity problems. It compares actual values to ideal values based on industry norms. Any possible cause that deviates from the norm will be shown in bold red text. If high user bandwidth appears to be an issue, you can go down to the diagnostic summary table and compare usage over the last few hours, day and week. Then, ask the user what he or she has been doing. It may be a specific task such as a file transfer that's causing the problem. Certain viruses also may cause a user's machine to consume large quantities of bandwidth.

3.5 Step 5: Check that the user is connected to the usual AP

Confirm that the user is in his or her normal location. Look at the Association History table on the user details page. If you see frequent roams that don't seem to correlate to actual movements, the user might be ping-ponging between neighboring APs. AP problems, RF interference or a client problem on the user's device can cause this condition. Look for AP problems by examining any AMP alerts (shown at the top right portion of the user details page). We will provide instructions for how to identify RF interference in Step 8 below. The next step covers client problems.

3.6 Step 6: Confirm coverage at the user's physical location

The user's location relative to the associated AP has a significant effect on signal quality and network performance. The easiest way to troubleshoot for location-dependent problems is with the AirWave VisualRF™ Location and Mapping feature. VisualRF gives you an accurate real-time view of your network. You can access VisualRF by clicking on the building floor plan thumbnail on the user details page.

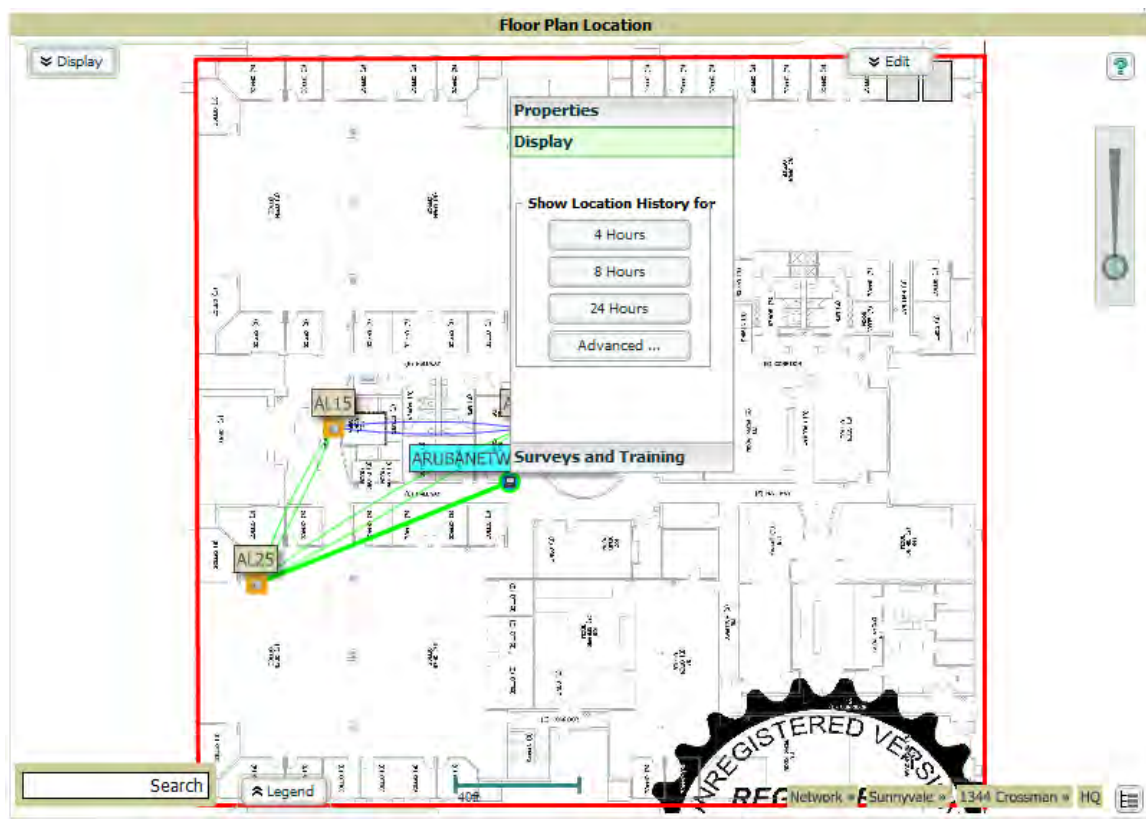


When VisualRF loads, you can see the actual location of the user and a line to the AP to which he or she is associated. If you check the “AP Neighbors” box in the display options, you will see the physical location of the AP and calculated signal strength, along with calculated signal strengths to other, unassociated APs. This view can quickly show you if you have a “sticky roaming” problem, where the user has moved but his device is staying associated with a distant AP. AirWave customers have seen this problem most frequently with handheld scanners and other Windows Mobile or Windows CE devices.

If signal strength looks questionable, ask the user to move closer to the AP and report performance.

- If performance improves noticeably when the user is closer to the AP, poor RF signal strength is a likely cause of the problem. You can check the “Heatmap” view in VisualRF to see if any neighboring access points might provide a stronger, clearer signal to the user. In our example, the areas with the strongest signal are depicted in red, while areas with the weakest (or no) signal are in light blue or white.
- If performance does not improve when the user is closer to the AP, RF interference may still affect performance even when the user is receiving a strong signal from a nearby AP. You will learn how to check whether RF interference is likely to be a cause of the problem in Step 8 below.

If you want to look at the user’s movements, VisualRF can play back user locations over the past 24 hours. From the VisualRF interface, click on the user’s icon. A pop-up will come up, from which you select the “Display” tab and click on the period of time (4, 8 or 24 hours) for which you want to view data.



3.7 Step 7: Check AP usage levels

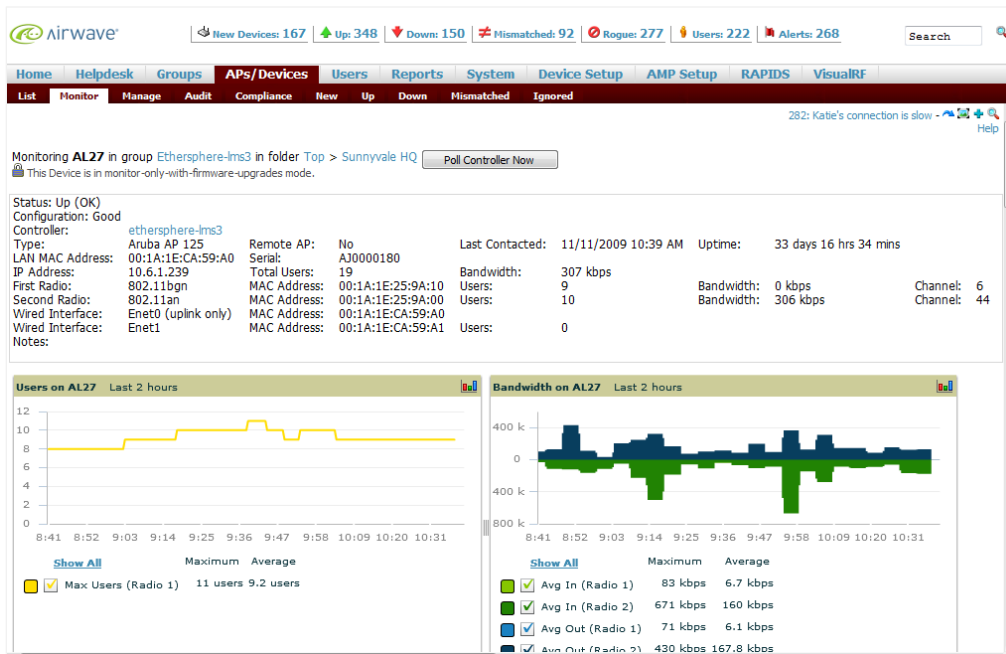
The top of the user diagnostics page contains several pieces of information to help you find possible problems relating to overall AP usage:

- *High user load on AP/radio and high AP/radio bandwidth:* The AP could simply be overloaded. If you have multiple APs at the user's location, you may be able to suggest that the user connect to another AP.
- *802.11b users associated to 802.11bg radio and 802.11b/g or 802.11a users associated to 802.11n radio:* Both of these conditions cause slow service for all users associated to the AP. If you see this as a persistent problem, your organization may choose to upgrade those users.

Diagnostics for 00:05:4E:4D:9D:6A

Possible Issues		
Issue	Ideal	Actual
Low signal quality:	>= 20	-
Excessive roaming in last two hours:	<= 10 roams	0
High user bandwidth:	<= 50% of radio capacity	-
Unauthenticated user:	Authenticated	Not Authenticated
High user load on AP/radio:	<= 15	1
High AP/radio bandwidth:	<= 75% of radio capacity	2 kbps (0.00%)
802.11b users associated to 802.11bg radio:	None	0
802.11b or 802.11a users associated to 802.11n radio:	None	1
High FCS error rate:	<= 100	0

Also look at the AP Bandwidth line on the Diagnostic Summary table (depicted in Step 4). Clicking on the “AP Bandwidth” hyperlink brings up a series of charts. If bandwidth looks high compared to historical norms, you can navigate to the AP monitoring page for a deeper review.



Below the summary charts of user load and bandwidth usage, you can see a list of actual users associated with the AP. Sort the user list by bandwidth consumption to quickly see if another user is consuming excessive amounts of bandwidth. If this is the case, contact that user and go through Step 4 described above.

Connected Users

1-20 ▾ of 20 Connected Users Page 1 ▾ of 1 Choose Columns

Username	MAC Address	SSID	VLAN	Connection Mode	Association Time	Duration	Sig. Qual. BW ▾
ARUBANETWORKS\mfager	00:16:CF:BC:08:15	ethersphere-wpa2	65	802.11a	11/11/2009 8:13 AM	2 hrs 33 mins	51 137 kbps
ARUBANETWORKS\tespinosa	00:16:CF:AB:4A:A9	ethersphere-wpa2	65	802.11a	11/10/2009 10:15 AM	1 day 0 hrs 30 mins	44 105 kbps
ARUBANETWORKS\mcollins	00:05:4E:50:13:17	ethersphere-wpa2	65	802.11a	11/11/2009 7:53 AM	2 hrs 53 mins	41 30 kbps
ARUBANETWORKS\abean	00:1D:D9:01:C4:70	ethersphere-wpa2	65	802.11a	11/11/2009 10:38 AM	7 mins	45 3 kbps
ARUBANETWORKS\dboles	00:19:7D:3A:99:8E	ethersphere-wpa2	65	802.11a	11/11/2009 9:43 AM	1 hr 2 mins	40 1 kbps
ARUBANETWORKS\stsung	00:16:CE:2C:85:18	ethersphere-wpa2	65	802.11a	11/11/2009 8:48 AM	1 hr 58 mins	29 1 kbps
ARUBANETWORKS\stomlinson	00:1F:3B:91:36:91	ethersphere-wpa2	65	802.11a	11/11/2009 8:13 AM	2 hrs 33 mins	47 1 kbps
ARUBANETWORKS\jghidinelli	00:19:7E:4C:EA:E5	ethersphere-wpa2	65	802.11a	11/11/2009 8:53 AM	1 hr 53 mins	49 0 kbps
ARUBANETWORKS\jmlies	00:1E:4C:3A:02:52	ethersphere-wpa2	65	802.11a	11/11/2009 9:58 AM	47 mins	46 0 kbps
ARUBANETWORKS\jchavez	00:21:6A:51:E2:74	ethersphere-voip	66	802.11n (5GHz)	11/11/2009 9:08 AM	1 hr 37 mins	48 0 kbps
wifiphone	00:03:2A:02:6B:14	ethersphere-voip	66	802.11g	11/10/2009 9:07 AM	1 day 1 hr 39 mins	56 0 kbps
wifiphone	00:03:2A:02:52:8C	ethersphere-voip	66	802.11g	11/10/2009 10:35 AM	1 day 0 hrs 10 mins	64 0 kbps
wifiphone	00:03:2A:02:6A:63	ethersphere-voip	66	802.11g	11/10/2009 9:07 AM	1 day 1 hr 39 mins	55 0 kbps
wifiphone	00:03:2A:02:6A:F8	ethersphere-voip	66	802.11g	11/10/2009 2:42 PM	20 hrs 3 mins	57 0 kbps
wifiphone	00:03:2A:02:6B:0F	ethersphere-voip	66	802.11g	11/11/2009 9:08 AM	1 hr 37 mins	54 0 kbps
wifiphone	00:03:2A:02:6A:65	ethersphere-voip	66	802.11g	11/11/2009 10:43 AM	2 mins	42 0 kbps
wifiphone	00:03:2A:02:6A:05	ethersphere-voip	66	802.11g	11/10/2009 4:30 PM	18 hrs 15 mins	54 0 kbps
wifiphone	00:03:2A:02:69:D4	ethersphere-voip	66	802.11g	11/10/2009 8:32 AM	1 day 2 hrs 14 mins	60 0 kbps
wifiphone	00:03:2A:02:6B:51	ethersphere-voip	66	802.11g	11/9/2009 6:44 PM	1 day 16 hrs 2 mins	57 0 kbps
lmlies@arubanetworks.com	04:1E:64:40:68:DF	ethersphere-voip	66	802.11g	11/11/2009 9:23 AM	1 hr 22 mins	46 0 kbps

1-20 ▾ of 20 Connected Users Page 1 ▾ of 1

3.8 Step 9: Look for IDS alerts

IDS alerts may indicate man-in-the-middle or denial-of-service attacks on your network — both of which can disrupt service to users. If you see a large number of IDS events showing in the Alert Summary section of your AirWave home page, be sure to alert network engineering.

Alert Summary at 12/17/2009 10:57 AM				
Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	23	219	412	12/17/2009 10:57 AM
IDS Events	280	3616	10055	12/17/2009 10:55 AM
Incidents	0	0	11	11/6/2009 7:55 AM
RADIUS Authentication Issues	6	73	195	12/17/2009 10:23 AM

5. Problem #3: “My connection keeps dropping”

When a user’s connection is dropping repeatedly, the troubleshooting process is very similar to the steps described above for no connection or a slow connection. Typically, this situation happens because of RF interference, ping-ponging, sticky roaming, or a bad driver in a client device.

You can take the following steps to narrow down the problem:

1. Verify that the user is in his or her usual location.
2. Determine whether he or she connects regularly. If the user connects infrequently, troubleshoot the device settings first.
3. Check that he or she is connected to the usual AP.
4. Examine the AP association history for signs of ping-ponging.
5. Look for changes in signal quality, using the chart on the user details page.
6. Use VisualRF’s user location playback feature to see if the user’s movements could have affected signal quality and to look for sticky roaming.
7. Look for IDS alerts.
8. Troubleshoot device settings, and if necessary, reinstall drivers.

6. Using AirWave to Escalate to Network Engineering

AirWave customers have found that they can resolve the majority of service desk calls just by taking the steps above. Other problems, however, require working with your network engineering team. While escalation processes vary from organization to organization, using AirWave Wireless Management Suite makes the handover significantly more efficient.

Many organizations already have a system in place for managing user trouble tickets. However, if no such system exists, you can use the HelpDesk function in the AirWave Management Platform to track issues. You use this function to create an incident as soon as you begin working with the user, or you can wait until you have isolated the problem.

HelpDesk incidents include a name and description. More importantly, you can “relate” any AMP page to the incident simply by clicking on an incident link as you navigate through the system during troubleshooting. In addition, you can click on a “picture” item to incorporate a snapshot of the page — a picture of exactly what you saw at the point in time when the user was experiencing the problem. You should take snapshots of any page where you saw anomalies so that network engineering can make an informed assessment after escalation.

The screenshot displays the AirWave user diagnostics interface. At the top, there are status indicators for New Devices (76), Up (396), Down (226), Mismatched (96), Rogue (342), Users (250), and Alerts (15). The navigation menu includes Home, Helpdesk, Groups, APs/Devices, Users, Reports, System, Device Setup, AMP Setup, RAPIDS, and VisualRF. The current view is 'Users' > 'Diagnostics' > 'Tags' > 'Tag Detail' for the MAC address 00:1F:3B:8C:3A:15.

Possible Issues

Issue	Ideal	Actual	Description
Low signal quality:	>= 20	39	State: Open, Last updated on 12/17/2009 11:57 AM
Excessive roaming in last two hours:	<= 10 roams	0	Description:
High user bandwidth:	<= 50% of radio capacity	7 kbps	Bryan called to report a slow connection. He is working in his office today.
Unauthenticated user:	Authenticated	EAP	History:
High user load on AP/radio:	<= 15	19	Thu Dec 17 11:57:33 2009 Snapshot added: Snapshot 625 Isonne
High AP/radio bandwidth:	<= 75% of radio capacity	1348 kb	
802.11b users associated to 802.11bg radio:	None	0	<input type="button" value="Edit"/>
802.11bg or 802.11a users associated to 802.11n radio:	None	1	<input type="button" value="Unselect Current Incident"/>
High FCS error rate:	<= 100	0	

Diagnostic Summary

	Current	Last Hour	Last 2 Hours	Last 4 Hours	Last 8 Hours	Last Day	Last Week
User Bandwidth	7 kbps (0.00%)	306 kbps (0.12%)	306 kbps (0.12%)	428 kbps (0.17%)	428 kbps (0.17%)	707 kbps (0.29%)	2966 kbps (1.20%)
Radio Bandwidth	1348 kbps (0.54%)	5690 kbps (2.29%)	6075 kbps (2.45%)	9943 kbps (4.01%)	9943 kbps (4.01%)	10466 kbps (4.22%)	45950 kbps (18.53%)
AP Bandwidth	1352 kbps (0.27%)	5703 kbps (1.15%)	6142 kbps (1.24%)	9947 kbps (2.01%)	9947 kbps (2.01%)	10564 kbps (2.13%)	46020 kbps (9.28%)
Radio User Count	13	17	17	17	17	17	17
AP User Count	19	23	24	24	24	24	24
Signal Quality	39	43	43	43	43	46	44

Current User Counts

	User Count on AP	User Count on Radio
802.11n (5GHz)	12	12
802.11g	6	0
802.11a	1	1
Total	19	13

7. Summary

The troubleshooting process described in this white paper, supported by the valuable data captured in AirWave, drives operational efficiency for the service desk and the entire IT organization. AirWave customers have been able to get service desk personnel ready to perform troubleshooting activities with a two- to four-hour training session. In doing so, they offload routine troubleshooting from their network engineering resources, who can then work more strategically and proactively to improve service quality for all users. The benefits of this approach include:

- Faster trouble ticket resolution
- Lower support costs
- Higher service quality
- More satisfied users

About Aruba Networks

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services - regardless of the user's device, location, or network. This dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at arubanetworks.com. For real-time news updates follow Aruba on twitter.com/ArubaNetworks, or greenislandnews.blogspot.com.



1344 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. 408.227.4500 | Fax. 408.227.4550 | 1-866-55-ARUBA
info@arubanetworks.com | <http://www.arubanetworks.com>