UBIQUITI NETWORKS

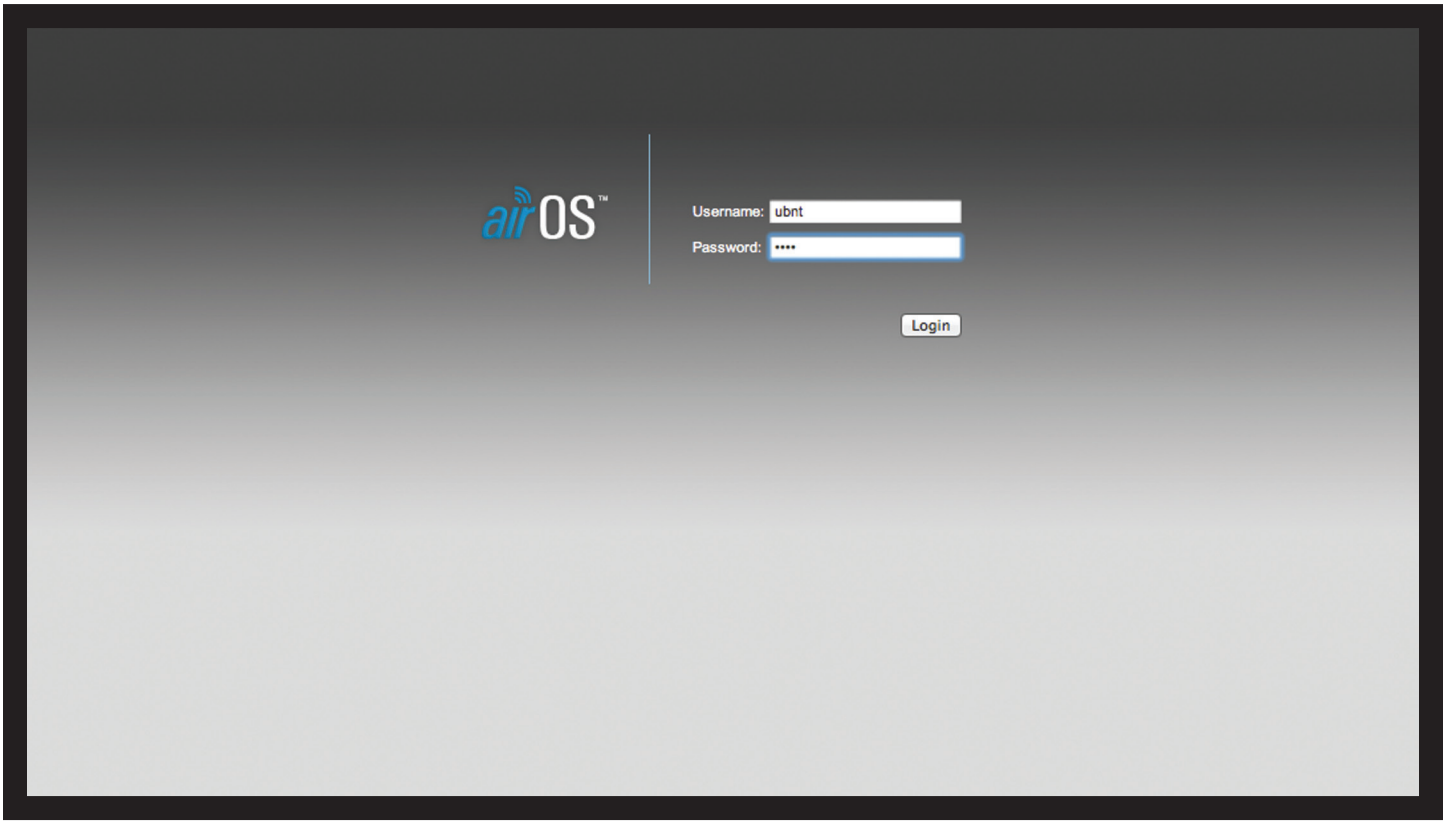
airOS™

Sistemul de operare pentru produsele din seria M

Versiunea: 5.5

USER GUIDE

Cuprins



Capitoulul 1: Noțiuni Introductive

Introducere

airOS v5.5 – ultima versiune a interfeței de configurare airOS furnizată de Ubiquiti Network™. airOS v5.5 oferă noi facilități, ca:

- Suport pentru Rețele Virtuale Multiple (VLAN)
- Facilitate Dynamic Access Control List (ACL)
- Autentificare la Distanță Dial-In User Service (RADIUS) și autentificare după MAC (Media Access Control)
- Suport airSync™
- Suport airMAX™ pentru alte aparate existente

Notă: Pentru compatibilitate, aparatele existente sau 802.11 a/b/g trebuie să folosească firmware cu suport airMAX (cum ar fi airOS firmware v4.0). Aparatele existente vor funcționa ca și clienți airMAX din seria M setate ca AP airMAX.

- Lățimi de bandă personalizate
- Funcționalitate DHCP relay
- Suport Universal Plug and Play (UPnP)
- Versiune Linux kernel actualizată

airOS este un sistem de operare avansat cu capabilități wireless puternice, funcții de routare și o interfață simplă și intuitivă.

Acest ghid descrie sistemul de operare airOS versiunea 5.5, folosit de toate produsele din seria M.

Produse Suportate

airOS v5.5 suportă noile versiuni ale produselor din seria M:

- Rocket™M
- Rocket™M GPS
- NanoStation™M/NanoStation loco™M
- NanoBridge™M
- Bullet™M
- PicoStation™M
- PowerBridge™M
- airGrid™M
- WispStation™M

Modurile de rețea airOS v5.5

airOS suportă următoarele moduri de rețea:

- Conexiune transparentă Layer 2
- Router
- SOHO Router

Moduri Wireless airOS v5.5

airOS suportă următoarele moduri wireless:

- Access Point
- Station / Client
- AP-Repeater

Cerințe de Sistem

- Microsoft Windows XP, Windows Vista, Windows 7, Linux, sau Mac OS X
- Java Runtime Environment 1.6 (sau mai nou)
- Browser Web : Mozilla Firefox, Apple Safari, Google Chrome, sau Microsoft Internet Explorer 8 (sau mai nou)

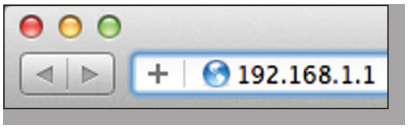
Noțiuni de bază

Pentru a accesa configurările airOS, indepliniți următorii pași:

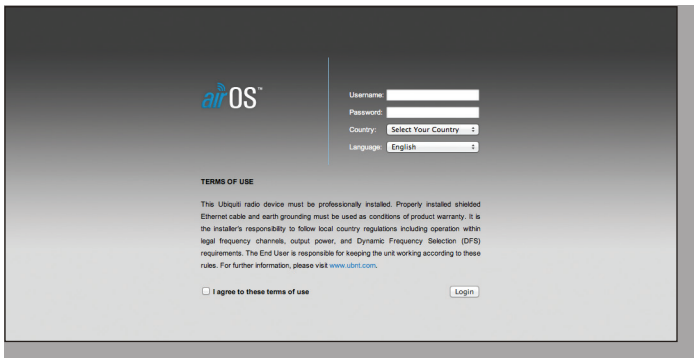
1. Configurați adaptorul Ethernet cu o adresă IP statică 192.168.1.x din subrețea (de examplu, adresa IP: 192.168.1.100 și masca de rețea: 255.255.255.0).
2. Porniți browser-ul Web. Introduceți IP-ul implicit addresei de pe aparatul dumneavoastră în câmpul de adresă. Apăsați *Enter* (PC) sau *Return* (Mac).

Device	Default IP Address
airRouter	192.168.1.1
Other Devices	192.168.1.20

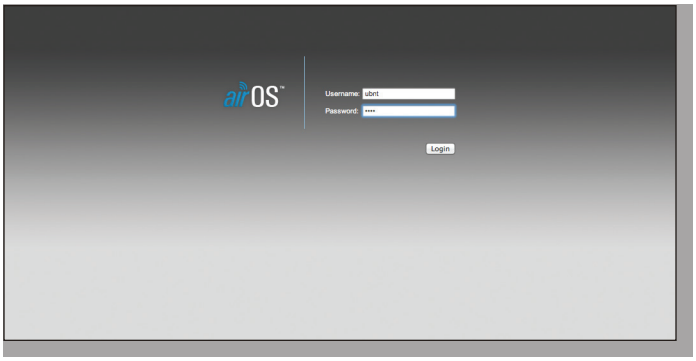
De exemplu, introduceți 192.168.1.1 pentru a accesa aparatul airRouter.



3. La prima logare, pe ecran vor apărea *Condițiile de folosință*. Introduceți **ubnt** în câmpurile *Username* și *Password*, apoi selectați țara și limba dorită. Bifați căsuța *I agree to these terms of use*, apoi apăsați *Login*.



4. După prima logare, va aparea fereastra standard de logare. Introduceți **ubnt** în câmpurile *Username* și *Password*, apoi apăsați *Login*.



Verificarea Produsului

Începând cu modelele introduse în 2012, airOS va verifica dacă produsul este original sau contrafăcut.

Înainte de 2012

Pentru modelele introduse înainte de 2012, airOS NU va afișa nici un logo în colțul din stânga jos al ecranului.

După 2012

Începând cu modelele introduse în 2012, airOS va afișa logo-ul *Genuine Product* în colțul din stânga jos al ecranului.

În cazul unui produs contrafăcut se va afișa un avertisment. Referitor la aceste produse, contactați Ubiquiti la support@ubnt.com.

Navigarea

Interfața airOS conține 7 meniuri principale, fiecare setând un anumit aspect al aparatului:

- Logo-ul Ubiquiti "Meniul Logo Ubiquiti" (pagina 4) controlează tehnologiile specifice Ubiquiti, ca airMAX, airView, airSelect și airSync (numai aparatele din seria GPS).

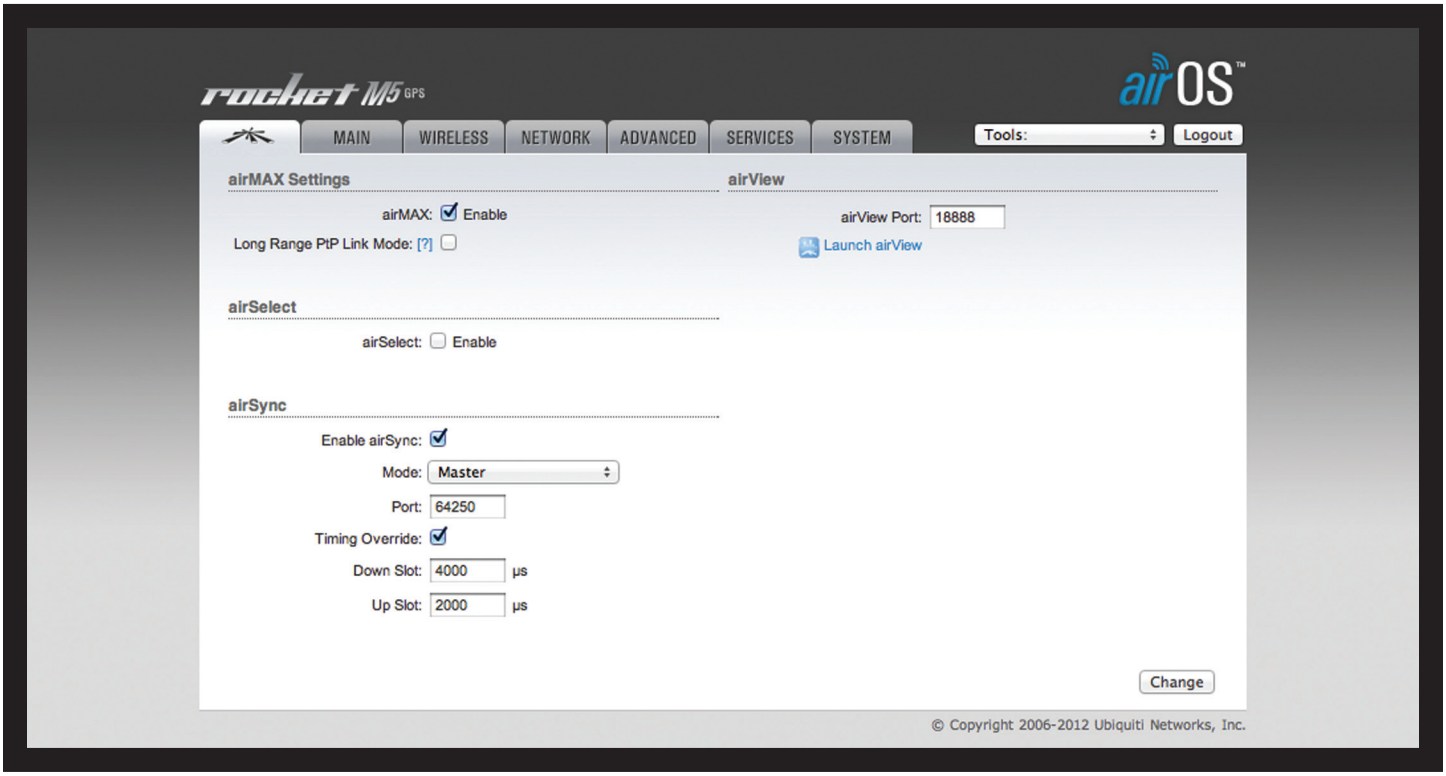
  Nota: Implicit aparatele pentru interior, ca airRouter, nu vor afișa meniul *logo Ubiquiti*. Totuși puteți activa acest meniu prin accesarea: System tab > Miscellaneous > airMAX Technology Features. Pentru mai multe informații citiți "Miscellaneous" (pagina 55).

- Main The "Meniul Main" (pagina 10) afișează statusul, statisticile și link-urile pentru monitorizarea rețelei.

- Wireless “Meniul Wireless” (pagina 18) afișează setările wireless de bază, ca: modul de wireless, numele rețelei (SSID), modul 802.11, canalul și frecvența, puterea de transmisie și securitatea wireless.
- Network În “Meniul Network” (pagina 25) se configurează modul de rețea, setările IP; aliating mode; aliasurile IP, rețelele VLAN; filtrarea de pachete, setările de bridging și rutele statice; și setările de traffic shaping.
- Advanced “Meniul Advanced” (pagina 47) furnizează setări wireless mai precise (advanced wireless settings, advanced Ethernet settings și signal LED thresholds).
- Services “Meniul Services” (pagina 50) configurează serviciile pentru managementul sistemului: Ping Watchdog, Simple Network Management Protocol (SNMP), servers (Web, SSH, telnet), Network Time Protocol (NTP) client, Dynamic Domain Name System (DDNS) client, system log și device discovery.
- System “Meniul System” (pagina 54) se află setările pentru întreținerea sistemului (administrator account management, location management, device customization, firmware update și configuration backup). De aici puteți schimba limba interfeței Web.

Fiecare pagină conține și uneltele pentru administrarea și monitorizarea rețelei:

- “Align Antenna” pagina 57
- “Site Survey” pagina 58
- “Discovery” pagina 58
- “Ping” pagina 58
- “Traceroute” pagina 58
- “Speed Test” pagina 59
- “airView” pagina 59



Capitolul 2: Meniul Ubiquiti Logo

Meniul Ubiquiti logo afișează setările pentru a porni, lansa și modifica funcțiile specifice Ubiquiti, cum ar fi:

- airMAX™ Oferă performanțe wireless superioare, mai mulți clienți Access Point (AP) și latență redusă.
- airSelect™ Schimbă canalul wireless în mod dinamic pentru a evita interferențele.
- airView™ Analizor de spectru oferit de Ubiquiti.
- airSync™ Sincronizează transmisiile aparatelor din seria GPS pentru eliminarea interferențelor de transmisie.

Nota: Implicit aparatele pentru interior, ca airRouter, nu vor afișa meniul *logo Ubiquiti*. Totuși puteți activa acest meniu prin accesarea: System tab > Miscellaneous > airMAX Technology Features. Pentru mai multe informații citiți “Miscellaneous” (pagina 55).

Change Pentru a salva sau testa setările apăsați **Change**.

Apare un mesaj nou cu trei opțiuni:

- Apply Pentru salvarea setărilor apasați **Apply**.
- Test Pentru a testa setările fără a salva apăsați **Test**. Pentru a păstra setările apăsați **Apply**. Dacă nu se apasă **Apply** timp de 180 secunde (cronometrul este afișat), atunci se revine la ultimele setări salvate.
- Discard Pentru a renunța la setări apăsați **Discard**.

Setările airMAX

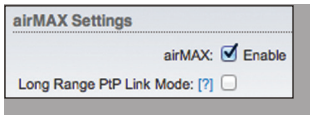
airMAX este tehnologie specifică Ubiquiti pentru sondare Time Division Multiple Access (TDMA). airMAX îmbunătățește performanțele în structură Punct la Punct (PtP) și Punct la Multipunct (PtMP) în mediile cu interferențe deoarece reduce latența, mărește viteza de transfer și oferă toleranță mai mare la interferență. Datorită acestor avantaje, airMAX mărește și numărul maxim de utilizatori care pot fi asociați unui AP care folosește airMAX.

airMAX atribuie intervale de timp pentru fiecare aparat pentru a evita problema “hidden node”, care apare atunci când un nod este vizibil de către AP, dar nu și de alte noduri care comunică cu AP-ul original.

Pentru compatibilitate, aparatele existente sau 802.11 a/b/g trebuie să folosească firmware cu suport airMAX (cum ar fi airOS firmware v4.0). Aparatele existente vor funcționa ca și clienți airMAX din seria M setate ca AP airMAX.

Notă: Pentru a suporta clienți existenți care folosesc airMAX, aparatele din seria M trebuie sa folosească airOS v5.5 sau mai nou.

Setările airMAX includ:



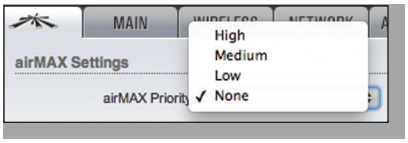
- airMAX (Disponibil numai în modul *AP-Repeater* sau *Access Point*) Dacă opțiunea airMAX este bifată, aparatul funcționează în modul airMAX și acceptă conexiuni numai de la aparate airMAX.

  Notă: Dacă opțiunea airMAX este bifată, la AP nu se pot conecta aparate Wi-Fi standard ca laptop-uri, tablete sau smartphone-uri.

  Dacă aparatul funcționează în modul *Station* (Meniul *Wireless* > *Wireless Mode*), aparatul va activa automat opțiunea airMAX când se conectează la un AP airMAX.
- Long Range PtP Link Mode (Disponibil numai în modul *AP-Repeater* sau *Access Point*) Setarea timpul de confirmare (ACK) este limitată de specificațiile hardware. Folosiți această opțiune dacă aveți un singur client (PtP) și distanța link-ului depășește limitările hardware ACK:
  - 27 km sau 17 miles (modul 40 MHz)
  - 51 km sau 32 miles (modul 20 MHz)

  Dacă folosiți modul *Long Range PtP Link Mode*, atunci opțiunea *Auto Adjust* din meniul *Advanced* nu este disponibilă.

  Dacă aveți mai mulți clienți atunci folosiți setările automate. Activați opțiunea *Auto Adjust* din meniul *Advanced* (vezi "**Advanced Wireless Settings**" pagina 47). Dacă activați opțiunea *Auto Adjust*, atunci *Long Range PtP Link Mode* nu este disponibil.
- airMAX Priority (Disponibil numai în modul *Station*) Definește numărul intervalelor de timp alocat fiecărui client. În mod implicit AP-ul alocă intervale de timp egale pentru clienți. Totuși dacă clienții sunt configurați cu diferite priorități, AP-ul va aloca timpi diferiți în funcție de prioritate.



Notă: Prioritățile airMAX funcționează numai când sunt activi mai mulți clienți.

Opțiunile pentru *airMAX Priority* includ:

- High 4 intervale de timp (rație 4:1)
- Medium 3 intervale de timp (rație 3:1)
- Low 2 intervale de timp (rație 2:1)
- None 1 interval de timp (Setare implicită pentru clienți; rație 1:1)

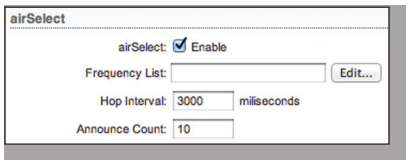
Clienții cu prioritate mai mare au acces la mai mult din timpul AP-ului, oferind o viteză de transfer mai mare și o latență mai mică față de alți clienți activi.
De exemplu dacă există 3 clienți cu prioritățile: 1 setat ca *None*, 1 setat ca *Medium* și 1 setat ca *High*, clinetul cu opțiunea *None* va primi 1 interval de timp, clientul cu opțiunea *Medium* va primi 3 intervale de timp, iar clientul cu opțiunea *High* va primi 4 intervale de timp.

airSelect

Notă: Dacă activați opțiunea *airSelect*, atunci airSync nu este disponibil.

(Disponibil numai în modul *Access Point*) airSelect este o tehnologie care evită interferențele și crește viteza de transfer. Schimbă în mod dinamic canalul wireless, sărind periodic, la intervale definite de utilizator în milisecunde (ms), la cel mai puțin folosit canal din listă (*Frequency List,* definită de utilizator*)*. airSelect urmărește nivelul de interferență pentru fiecare canal folosit, sărind în mod frecvent la canalele cu cele mai mai mici interferențe.

Opțiunile airSelect includ:

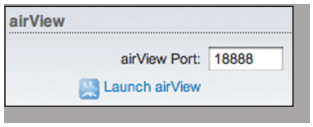


- airSelect Bifați pentru a activa airSelect. Când airSelect este activat, AP-ul și clienții asociați schimbă rapid între frecvențe pentru a evita interferențele.
- Frequency List Disponibil numai când airSelect este activat. Apasați **Edit** pentru a selecta frecvențele folosite de AP pentru airSelect. Frecvențele disponibile diferă în funcție de aparat.
- Hop Interval Disponibil numai când airSelect este activat. Durata (în milisecunde) pentru care AP-ul va rămâne pe o frecvență înainte de a se tranfera la alta. Valoarea inițială este de 3000 ms.
- Announce Count Disponibil numai când airSelect este activat. Numărul de dăți în care AP-ul anunță clienții desapre informațiile următoarei schimbări (de exemplu frecvența). De examplu, dacă *Hop Interval* este setat de la 10000 ms și *Announce Count* la 10, AP-ul va transmite clienților informațiile despre următoarea schimbare la fiecare 1000 ms. Cu cât perioada între anunțuri și salturi este mai mare, cu atât crește riscul decalării (salturile nu mai sunt sincronizate), de aceea se recomandă păstrarea setării *Hop Interval* la 100 ms (sau rația între *Announce Count* și *Hop Interval* sa fie 1:100). Valoarea inițială este 10.

airView

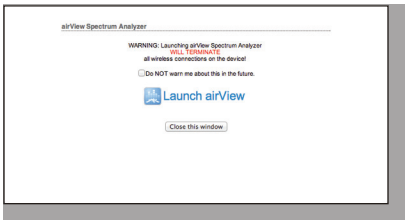
Folosiți *airView Spectrum Analyzer* pentru a analiza zgomotul din spectrul radio și pentru a selecta frecvența optimă în cazul instalării unui link PtP airMAX.

Opțiunile airView includ:

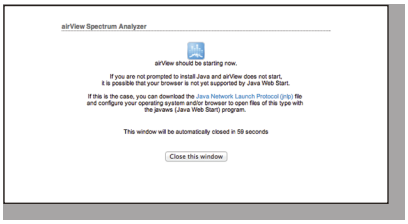


- airView Port Definește portul TCP folosit de airView pe aparat. Setarea implicită este 18888.
- Launch airView Există două cerințe de sistem pentru folosirea airView Spectrum Analyzer:
  - Sistemul dumneavoastră trebuie conectat la aparat prin cablu deoarece după lansarea airView se vor întrerupe toate conexiunile wireless.
  - Pe sistem trebuie sa aveți instalat Java Runtime Environment 1.6 (sau mai nou).

  Apăsați **Launch airView** pentru a folosi airView Spectrum Analyzer. La prima folosință va apărea următoarea fereastră:



- Do NOT warn me about this in the future Bifați căsuța pentru a evita această fereastră în viitor.
- Launch airView Apăsați **Launch airView** pentru a descărca fișierul Java Network Launch Protocol (jnlp) și pentru a lansa aplicația airView.



Fereastra Principală

Device Afișează numele, adresa MAC (Media Access Control) și adresa IP a aparatului care rulează airView.

Total RF Frames Afișează numărul total de cadre RF (Radio Frequency) adunate de la pornirea sesiunii airView sau de când a fost apăsat ultima dată butonul *Reset All Data*.

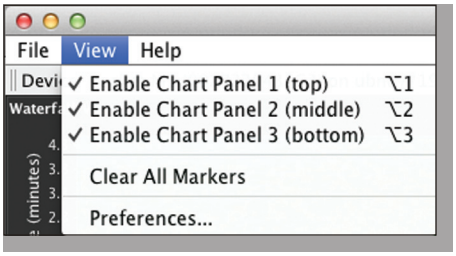
FPS Afișează numărul total de cadre pe secundă (FPS) adunate de la pornirea sesiunii airView sau de când a fost apăsat ultima dată butonul *Reset All Data*.

Reset All Data Apăsați pentru a reseta toate informațiile adunate.Folosiți această opțiune pentru a analiza spectrul dintr-o altă locație sau adresă.

Meniul File

Apăsați **Exit** pentru a incheia sesiunea airView.

Meniul View



Enable Chart Panel 1 (top) Afișează utilizarea canalelor (Waterfall) în panoul 1, în funcție de opțiunea selectată în meniul *Preferences*. Acest grafic afișează în funție de timp energia colectată pentru fiecare frecvență de la începutul sesiunii airView.

Enable Chart Panel 2 (middle) Afișează graficul cu forma de undă în panoul 2. Graficul arată semnătura RF a zgomotului în funcție de timp de la începutul sesiunii airView. Culoarea energiei indică amplitudinea. Culorile reci reprezintă nivele mici de energie (albastru reprezintă cel mai mic ninel) și culorile calde (galben, portocaliu sau roșu) reprezintă nivele de energie mai mari.

Enable Chart Panel 3 (bottom) Afișează tabelul în timp real (modul tradițional de afișare) în panoul 3. Energia (în dBm) este indicată în timp real în funcție de frecvență.

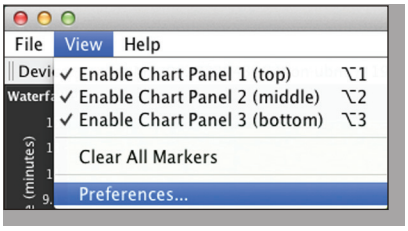
Notă: Energia este rația dintre decibelii (dB) puterii măsurate luată ca referință față de un miliwatt (mW).

Clear All Markers Resetează toate marker-ele anterioare. Un marker se crează prin selectarea unui punct, care corespunde unei frecvențe în tabelul Real-time.

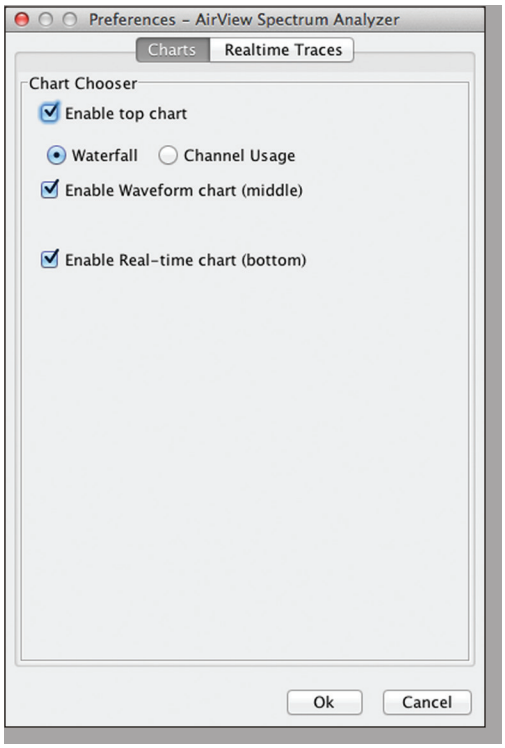
Preferences Modifică setările airView, pornind sau oprind panouri sau urme, sau specificând intervalul de frecvență.

Preferences

Selectați **View > Preferences** pentru a afișa fereastra cu preferințele airView Spectrum Analyzer.



Charts



Enable top chart Bifați pentru a porni panoul 1. Selectați tipul de tabel afișat în panoul 1. Există două opțiuni:

- Waterfall Este un grafic în funcție de timp a energiei colectate pe fiecare frecvență de la începutul sesiunii airView. Culoarea energiei indică amplitudinea. Culorile reci reprezintă nivele mici de energie (albastru reprezintă cel mai mic ninel) și culorile calde (galben, portocaliu sau roșu) reprezintă nivele de energie mai mari.

  Legenda vederii Waterfall (colțul din dreapta sus) furnizează un ghid al valorilor numerice asociate culorilor în funcție de nivelul de putere (în dBm). Partea inferioară a legendei (stânga) este întotdeauna ajustată la limita inferioară a zgomotului, iar partea superioară (dreapta) este setată la nivelul de putere maxim detectat de la începutul sesiunii airView.
- Channel Usage Pentru fiecare canal Wi-Fi, o bară afișează procentajul relativ de aglomerare. Pentru calcularea procentajului, airView Spectrum Analyzer analizează atât popularitatea, cât și puterea energiei RF a respectivului canal de la începutul sesiunii airView.

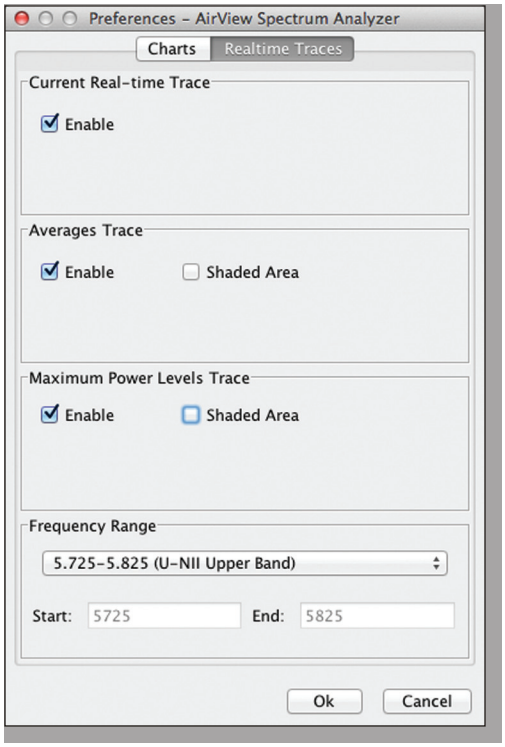
Enable Waveform chart (middle) Bifați pentru a porni panoul 2. Panoul afișează printr-un grafic în funcție de timp, semnătura zgomotului RF de la pornirea sesiunii airView. Culoarea energiei indică amplitudinea. Culorile reci reprezintă nivele mici de energie (albastru reprezintă cel mai mic ninel) și culorile calde (galben, portocaliu sau roșu) reprezintă nivele de energie mai mari.

Vederea spectrală va afișa starea stabilă a semnăturii energiei RF de-a lungul timpului întrun anumit mediu.

Enable Real-time chart (bottom) Bifați pentru a porni panoul 3. Graficul afișează analizatorul de spectru tradițional, în care energia (în dBm) este afișată în timp real în funcție de frecvență. Sunt trei urme pentru această vedere:

- Current (Galben) Arată energia în timp real văzută de aparat în funcție de frecvență.
- Average (Verde) Afișează energia medie în funție de frecvență.
- Maximum (Albastru) Afișează nivelul maxim de putere în funcție de frecvență.

Realtime Traces



Următoarele setări se aplică numai pentru graficul în timp real:

Current Real-time Trace Bifați pentru a activa urma în timp real. Când este activată, conturul galben din graficul Real-time reprezintă nivelul de putere în timp real în funcție de frecvență. Viteza de actualizare depinde de FPS.

Averages Trace Bifați pentru a activa urma de medie. Când este activată, zona verde din graficul Real-time afișează media nivelului de putere de la începutul sesiunii airView. Pentru a activa o zonă verde umbrită, bifați *Shaded Area*. Pentru a afișa numai un contur verde, debifați *Shaded Area*.

Maximum Power Levels Trace Bifați pentru a activa urma puterii maxime. Când este activată, zona albastră din graficul Real-time afișează nivelul puterii maxime de la începutul sesiunii airView. Pentru a activa o zonă albastră umbrită, bifați *Shaded Area*. Pentru a afișa numai un contur albastru, debifați *Shaded Area*.

Frequency Range Selectați intervalul de frecvențe care va fi scanat din lista *Frequency Range*. Frecvențele disponibile diferă în funcție de aparat. Există intervale predefinite pentru cele mai populare benzi. Puteți introduce și un interval personalizat; selectați **Custom Range** din lista *Frequency Range* și introduceți valorile dorite în câmpurile *Start* și *End*.

Help

Apăsați **About** pentru a vedea versiunea și numărul de compilare a airView Spectrum Analyzer.

airSync (Numai seria GPS)

Notă: Dacă activați opțiunea airSync, atunci airSelect nu este disponibil.

(Disponibil numai în modul *Access Point*) airSync (disponibil numai pentru aparatele din seria GPS) sincronizează AP-urile airMAX cu un semnal satelit pentru referință de timp. Când este activ, airSync elimină erorile de recepție (RX) datorate interferențelor de transmisie.

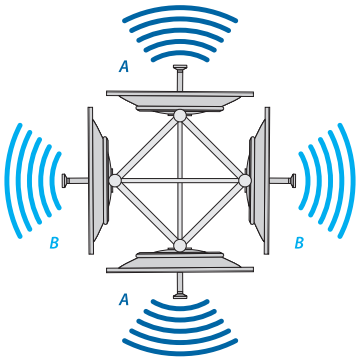
Notă: Pentru a folosi airSync, toate stațiile trebuie să funcționeze cu airOS v5.5 sau mai nou; altfel, acestea nu se pot conecta la AP.

Vă recomandăm următoarele:

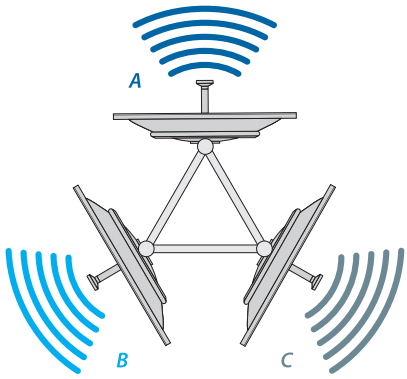
- Sectoarele alăturate ar trebui să folosească frecvențe diferite.
- Sectoarele spate în spate pot folosi aceeași frecvență.
- Nu folosiți aceeași frecvență pentru toate AP-urile din aceeași locație. Unele AP-uri dintr-o locație pot folosi aceeași frecvență în funcție de poziționare. Vedeți exemplele: Patru AP-uri și două AP-uri.
- Numărul de frecvențe folosite depinde de numărul de AP-uri de pe un singur turn, deoarece un client se poate deruta dacă primește semnale pe aceeași frecvență de la două AP-uri diferite.
- Dacă folosiți mai mult de o frecvență, asigurațivă că există o separare de 20 MHz între marginea frecvențelor. De exemplu: dacă intervalul A se sfârșește la 5815 MHz, atunci intervalul B poate începe la 5835 MHz sau mai mare.

Vă oferim următoarele exemple:

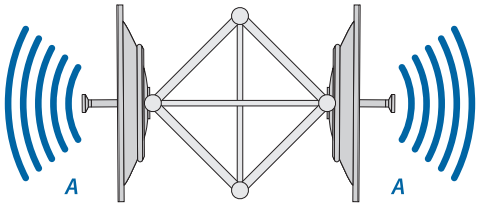
- Patru AP-uri Folosiți două frecvențe diferite. Setați aceeași frecvență pe AP-urile spate în spate (acesta este un model ABAB). De exemplu, dacă un client este situat egal între două AP-uri (unul setat pe frecvența A și celălalt pe frecvența B), acesta va recepționa semnalul numai de la AP-ul cu aceeași frecvență.



Trei AP-uri Setați frecvențe diferite pentru fiecare AP (acesta este un model ABC). De exemplu, dacă un client este situat egal între două AP-uri (unul setat pe frecvența A și celălalt pe frecvența B), acesta va recepționa semnalul numai de la AP-ul cu aceeași frecvență. Dacă un alt client este situat egal între o altă pereche de AP-uri (unul setat pe frecvența B și celălalt pe frecvența C), acesta va recepționa semnalul numai de la AP-ul cu aceeași frecvență.



- Două AP-uri Setați aceeași frecvență pe ambele AP-uri spate în spate (acesta este un model AA).



Pentru a sincroniza mai multe AP-uri, acestea sunt cerințele:

- AP-ul principal trebuie să aibă conectivitate IP (mai precis UDP) cu AP-urile secundare.
- Toate AP-urile trebuie să aibă semnal GPS activ.
- Trebuie să configurați duratele de transmisie și recepție pe AP-ul principal.

După ce configurați aceste durate pe AP-ul principal, acestea trebuie transmise către toate AP-urile secundare. Folosirea aceleași durate de transmisie și recepție, permite fiecărui AP să determine când să transmită și când să recepționeze.

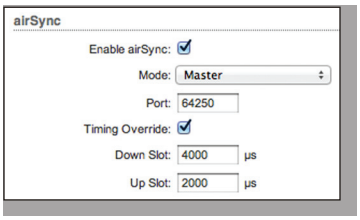
Duratele sunt configurate în microsecunde (µs) și specifică perioada de timp în care AP-ul va transmite și va recepționa. Setarea *Down Slot* specifică timpul de descărcare (download) pentru clienți, în timp ce setarea *Up Slot* specifică timpul de încărcare (upload).

Puteți să vă gândiți la timpii de descărcare și încărcare ca la o rație. Dacă *Down Slot* este setat la 4000 µs și *Up Slot* setat la 2000 µs, atunci AP-ul alocă 66% [4000/(4000+2000)] din timp pentru descărcare și 33% pentru încărcare. În mod implicit, *Down Slot* este setat la 4000 µs, iar *Up Slot* este setat la 2000 µs.

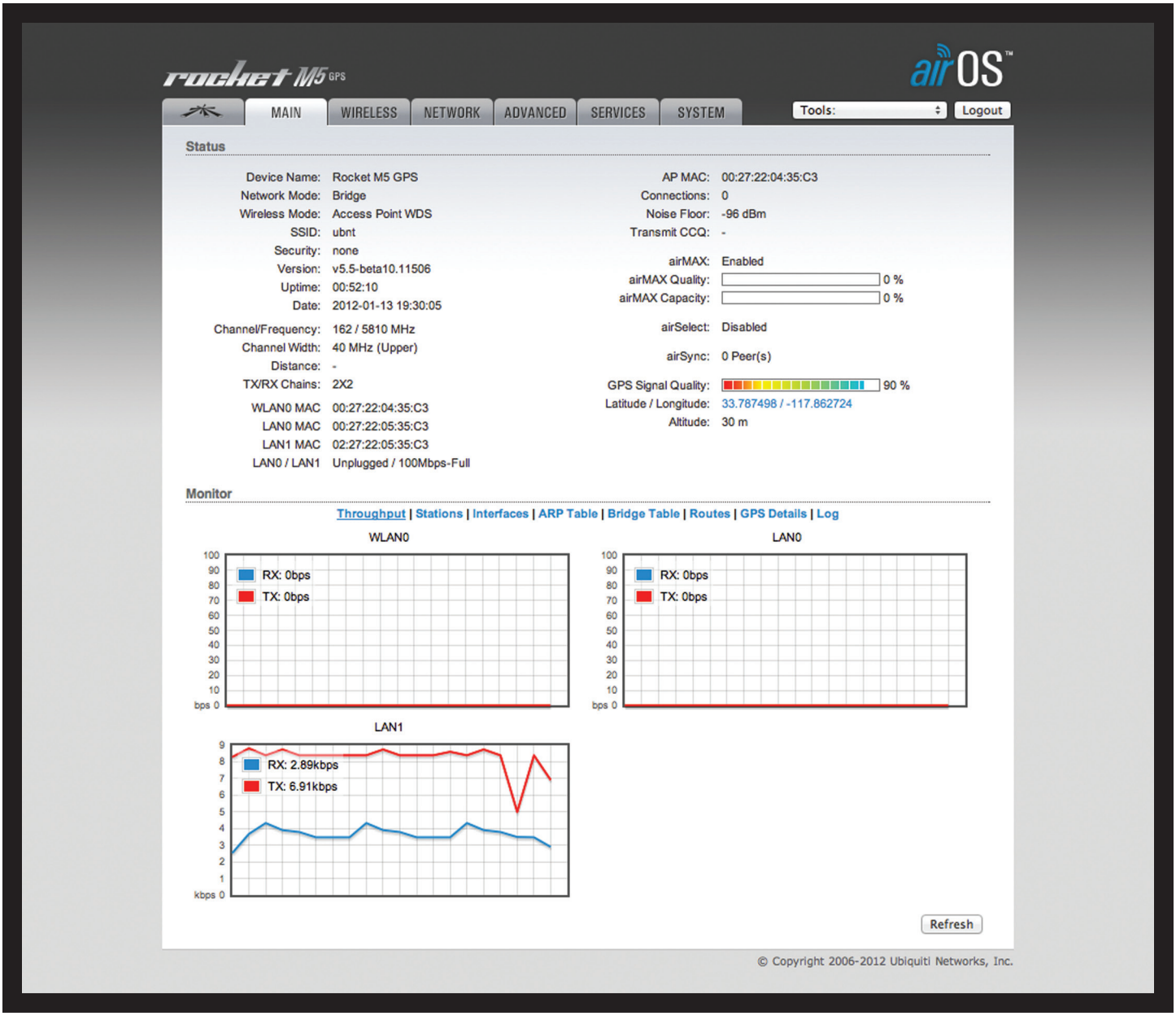
În unele cazuri este necesară funcția *Timing Override*, în funcție de traficul utilizatorilor. Dacă clienții unui AP descarcă excesiv, măriți rația între *Down Slots* și *Up Slots*.

Similar, dacă un AP are clienți business și care au nevoie de viteze mai mari de upload folosiți o rație egală *Down Slot/ Up Slot*. În funcție de modelul de trafic, ajustați rația *Down Slot/Up Slot*.

Opțiunile airSync includ:



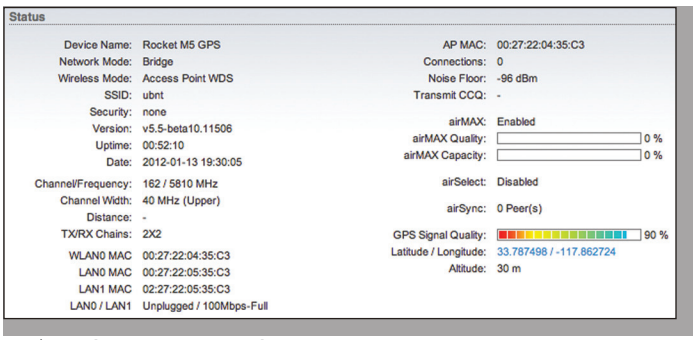
- Enable airSync Bifați pentru a activa airSync.
- Mode Disponibil numai când airSync este activ. Selectați **Master** sau **Slave** în funcție de modul în care este configurat aparatul. Aparatul setat în mod *Master* se sincronizează cu toți clienții setați în modul *Slave.*
- Port Disponibil numai când airSync este activ. Implicit, portul este 64250, dar aceasta se poate modifica.
- Timing Override (Master) Disponibil numai când airSync este activat pe AP-ul principal. Bifați căsuța pentru a activa *Timing Override*. Debifați căsuța pentru a dezactiva *Timing Override* și pentru a reveni la setările implicite.
  - Down Slot Implicit este setat la 4000 µs.
  - Up Slot Implicit este setat la 2000 µs.
- Master IP (Slave) Disponibil numai când airSync este activat pe AP-ul secundar. Introduceți adresa IP a AP-ului principal.



Capitolul 3: Meniul Main

Meniul Main afișează rezumatul cu statusul link-ului, setările de bază curente (în funcție de modul de operare), informațiile și setările despre rețea și statisticile despre trafic.

Status



Device Name Arată numele sau identificatorul aparatului, care poate fi schimbat. Numele aparatului (cunoscut și ca numele host-ului) este afișat în ecranele de înregistrare și de uneltele de descoperire.

Network Mode Afișează modul de operare în rețea. airOS suportă trei moduri de operare: *Bridge, Router* și *SOHO Router*. Setarea implicită depinde de aparat. Configurați *Network Mode* în meniul *Network*.

Wireless Mode Afișează modul de operare a interfeței wireless. airOS suportă trei moduri de operare: *Station, Access Point* și *AP-Repeater*. etarea implicită depinde de aparat. Configurați *Wireless Mode* în meniul *Wireless*. Dacă este activat modul *Station* sau *Access Point* atunci se poate selecta **WDS** (Wireless Distribution System) dacă este nevoie.

De asemenea, airOS suportă modul airView (spectrum analyzer), un mod temporar care întrerupe toate conexiunile wireless. Pentru a selecta modul airView, apăsați **Tools > airView** sau **Launch** în m

Ubiquiti Logo. În timpul sesiunii airView, toate conexiunile wireless vor fi întrerupte. Închideți fereastra airView, pentru a reveni la modul wireless anterior. session. Orice aparat din seria M poate opera într-un singur mod în același timp. De exemplu, dacă aparatul funcționează în modul *Access Point*, nu poate funcționa în același timp și în modul *Station*.

SSID Afișează numele rețelei wireless (SSID). Numele rețelei wireless depinde de modul wireless selectat:

- În modul Station mode, afișează SSID-ul AP-ului cu care este asociat.
- În modul Access Point mode, afișează SSID-ul aparatului, configurat in meniul *Wireless*.

Security Afișează metoda de securitate wireless folosită. Dacă este afișat *None* atunci securitatea este dezactivată, totuși puteți folosi autentificarea RADIUS MAC.

Version Afișează versiunea softului airOS.

Uptime Afișează timpul total de la ultimul reboot (când aparatul a fost pornit) sau ultima actualizare software. Timpul este afișat în zile, ore, minute și secunde.

Date Afișează data și ora curentă, în formatul AN-LUNĂ-ZI-ORĂ:MINUTE:SECUNDE. Data și ora sunt preluate de la un server folosind protocolul NTP (Network Time Protocol). Clientul NTP este activ în mod implicit în meniul *Services*. Aparatul nu are ceas intern, de aceea data și ora pot fi greșite dacă clientul NTP este dezactivat sau aparatul nu este conectat la internet.

Channel/Frequency Afișează numărul canalului și frecvența corespunzătoare. Aparatul folosește canalul și frecvența specificată pentru a transmite și primii date. Intervalele de canale și frecvențe pot varia în funcție de reglementările din fiecare țară.

Channel Width Afișează lățimea de bandă a canalului folosit de aparat. airOS v5.5 suportă lățime de bandă de 2, 3, 5, 8, 10, 20, 25, 30, și 40 MHz; totuși, acestea pot varia în funcție de aparat. În modul *Station* setarea implicită este *Auto 20/40 MHz.*

Distance Afișează distanța între aparate în km și mile pentru cadrele de confirmare (ACK). Modificarea distanței va schimba și timpul de confirmare (ACK). Setarea ACK specifică cât timp va aștepta aparatul confirmarea de recepționare a pachetului de la un alt aparat, înainte de a concluziona că a apărut o eroare și de a retrimite pachetul. Puteți seta valoarea distanței din meniul ”**Advanced Wireless Settings**” pagina 47.

TX/RX Chains Afișează numărul de strimuri de date independente pe care dispozitivul de transmite (TX) și primește (RX) în același timp în cadrul unui canal. Abilitatea este specifică aparatelor 802.11n care se bazează pe tehnologia MIMO (Multiple-Input Multiple-Output). Mai multe lanțuri cresc semnificativ rata de transfer. Numărul de lanțuri folosit de aparatele Ubiquiti depind de dispozitiv, deoarece fiecare lanț TX/RX necesită o antenă separată.

Antenna (Aplicabil numai pentru NanoStationM900 loco) Este afișat tipul de antenă (*Internal, External,* sau *External + Internal*). Vedeți opțiunile *Antenna* în meniul “**Basic Wireless Settings**” pagina 18.

WLAN0 MAC Afișează adresa MAC a aparatului văzută pe rețeaua wireless.

LAN0 MAC Afișează adresa MAC a aparatului văzută pe LAN.

LAN1 MAC Afișează adresa MAC a aparatului văzută pe interfața WAN. Aceasta este adresa MAC văzută pe internet.

LAN0/LAN1 Indică statusul curent al conexiunii porturilor WAN și LAN Ethernet. Poate indica dacă un cablu a fost deconectat sau nu există conexiune Ethernet activă.

AP MAC În modul *Access Point* sau *AP-Repeater*, afișează adresa MAC a aparatului. În modul *Station*, afișează adresa MAC a AP-ului cu care este asociat.

Signal Strength (Disponibil numai în modul *Station*) Afișează nivelul de semnal wireless recepționat. Valoarea afișată coincide cu graficul. Folosiți unealta *antenna alignment* pentru a ajusta poziția aparatului pentru obținerea unei conexiuni mai bune. Antena clientului wireless trebuie ajustată pentru obținerea puterii de semnal maxim. Puterea semnalului este măsurată în dBm (decibeli în referință cu 1 miliwatt). Conversia este definită ca dBm=10log10(P/1mW). Deci, 0 dBm înseamnă 1 mW și -72 dBm înseamnă 0.0000006 mW.
Pentru un link stabil, se recomandă o putere a semnalului de -80 dBm sau mai bună (-50 la -70 dBm).

Chain or Horizontal/Vertical or External/Internal (Vertical) (Disponibil numai în modul *Station*) Afișează nivelul de semnal wireless (în dBm) a fiecărui semnal. Aparatele cu antenă fixă afișează *Horizontal/Vertical* în loc de *Chain*. Când sunt afișate lanțuri (chains), numărul de lanțuri diferă în funcție de aparat.

NanoStationM900 loco afișează *External/Internal (Vertical)* dacă opțiunea *Antenna* din meniul *Wireless* este setat ca *External + Internal (2x2)*. Vedeți opțiunea *Antenna* din meniul “**Basic Wireless Settings**” pagina 18.

Connections (ADisponibil numai în modul *Access Point* sau *AP-Repeater*) Afișează numărul de clienți conectați la aparat.

Noise Floor Afișează valoarea curentă a zgomotului în dBm (de la interferențe) pe care aparatul o recepționează pe frecvența de operare. airOS ia în considerare valoarea Noise Flool în timp ce evaluează calitatea semnalului (Raportul semnal/Zgomot SNR, RSSI). Valoarea medie depinde de puterea semnalului peste cea a Noise Floor.

Transmit CCQ Afișează nivelul wireless CCQ (Client Connection Quality). Nivelul are o valoare procentuală, 100% corespunzând unei conexiuni perfetce.

TX Rate/RX Rate (Disponibil numai în modul *Station*) Afișează rata actuală de transmisie (TX) și recepție (RX).

airMAX Indică statusul airMAX. Dacă airMAX este activ, atunci aparatul va accepta doar clienți airMAX. De asemenea, airMAX oferă funcții avansate de autodedectare a setărilor QoS (Quality of Service).

Notă: Pentru compatibilitate, aparatele existente sau 802.11 a/ b/g trebuie să folosească firmware cu suport airMAX (cum ar fi airOS firmware v4.0). Aparatele existente vor funcționa ca și clienți airMAX din seria M setate ca AP airMAX.

airMAX Priority Disponibil numai în modul *Station* cu *airMAX* activ. Indică prioritatea airMAX setată în meniul *Ubiquiti logo*. Implicit, toți clienții AP-ului au aceeași prioritate. Totuși dacă clienții sunt configurați cu diferite priorități, AP-ul va seta timpii de transmisie/recepție în funcție de prioritate.

airMAX Quality Disponibil dacă *airMAX* este activ. airMAX Quality (AMQ) este bazat pe numărul de încercări și pe calitatea conexiunii. Dacă această valoare este mică, este posibil să aveți interferențe și trebuie să schimbați frecvența. Dacă AMQ este peste 80% și nu observați nici o problemă, atunci nu trebuie să faceți nici o modificare.

airMAX Capacity Disponibil dacă *airMAX* este activ. airMAX Capacity (AMC) este bazat pe eficiența aparatului. De exemplu, dacă aveți un singur client cu o rată de transfer mică sau folosiți aparate 1x1 (ca Bullet sau airGrid) împreună cu clienți 2x2, atunci va folosi mai mult timp (sloturi) pentru a trimite aceleași date, reducând timpul pentru alți clienți. Cu cât AMC este mai mic, cu atât AP-ul este mai ineficient. Dacă aveți un singur client, acest lucru nu contează, dar în cazul mai multor clienți (mai mult de 30), atunci AMC devine foarte important și veți dori să fie cât mai mare posibil.

Dacă vă uitați la un client, AMC arată capacitatea teoretică a acestuia, bazate pe ratele TX/RX și calitate. Procentajul AMC este bazat pe care ar fi performața maximă în cazul unei conexiuni perfecte. Clienții cu AMC slab pot afecta negativ alți clienți, prin ocuparea timpului cu transmisii lente. De exemplu, clientul A are viteza MCS 12 (78 Mbps) din cauza semnalului slab. Clientul teoretic ar putea avea viteza de MCS 15 (130 Mbps), deci AMC-ul este bazat pe rația între rata curentă/rata maximă (78 Mbps divizat la 130 Mbps), adică 60%. În mod similar, un aparat 1x1 va avea un AMC maxim de 50%, deoarece furnizează jumătate din performanța 2x2. Dacă vă uitați la AP, atunci AMQ și AMC sunt medii a valorilor tuturor clienților.
Pentru a descoperii de ce aveți valorile mici pe un AP, căutați clienții slabi. Puteți folosi airControl™ (recomandat) sau puteți merge la fiecare client în parte. Încercați să folosiți antene cu câștig mai mare (pentru a permite rate de transfer mai mari) sau treceți la un aparat 2x2 dacă folosiți un aparat 1x1.

airSelect Indică statusul airSelect. Dacă airSelect este activ, atunci airSync nu este disponibil. Accesați setările airSelect în meniul *Ubiquiti Logo > airSelect*.

Hop Interval Disponibil numai când airSelect este activ. Durata (în milisecunde) pentru care AP-ul va rămâne pe o frecvență înainte de a se tranfera la alta.

airSync (numai seria GPS) Indică statusul airSync. Dacă airSync este activ, airSelect nu este disponibil și aparatul principal arată numărul de clienți secundari cu airSync activ. Accesați setările airSync prin meniul *Ubiquiti Logo airSync*.

GPS Signal Quality (numai seria GPS) Afișează calitatea semnalului GPS în valoare procentuală pe o scală 0-100%.

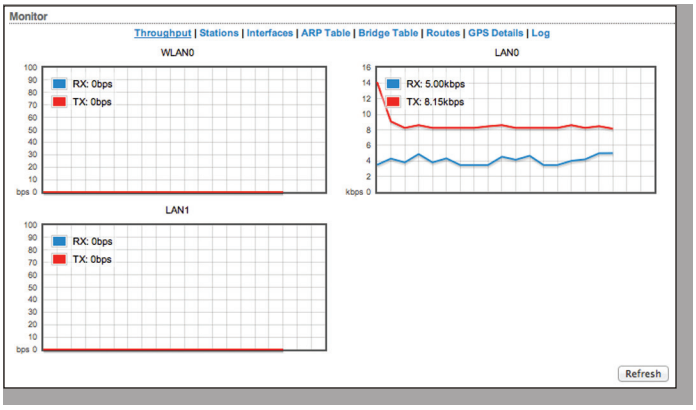
Latitude/Longitude (numai seria GPS) Bazat pe poziționare GPS, afișează latitudinea și longitudinea aparatului. Dacă apăsați pe link, poziționarea va fi afișată în browser folosind Google Maps™ (http://maps.google.com).

Altitude (numai seria GPS) Bazată pe poziționare GPS, afișează altitudinea aparatului.

Monitor

Există o varietate de unelte pentru monitorizare, accesibile prin link-uri în meniul Main. Implicit, în meniul Main, este afișat *Throughput*.

Throughput

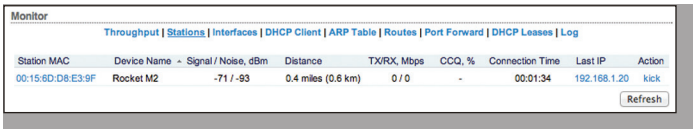


Throughput afișează rata de transfer curentă pentru LAN și WLAN în formă numerică și sub formă de grafic. Scala se schimbă dinamic (Bps, Kbps, Mbps) în funcție de media ratei de transfer. Statisticile se actualizează automat.

Refresh Dacă apar întarzieri de actualizare, apăsați **Refresh** pentru actualizarea manuală a statisticilor.

Stations

(Disponibil numai în modul *Access Point* sau *AP-Repeater*) Submeniul afișează lista cu clienții conectați la aparat.



Sunt afișate următoarele informații despre clienți:

Station MAC Afișează adresa MAC a clientului. Acesta este un link care afișează informații suplimentare despre client.

Device Name Afișează numele clientului. Numele aparatului client poate fi schimbat în meniul *System.*

Signal/Noise, dBm Valoarea *Signal* reprezintă nivelul semnalului wireless recepționat și valoarea *Noise* reprezintă nivelul de zgomot.

Distance (Disponibilă dacă setarea *Auto Adjust* este activă în meniul *Advanced Wireless tab > Advanced Wireless Settings*) Afișează distanța dintre aparate, în kilometri și mile, pentru cadrele de confirmare (ACK). Cu opțiunea Auto Adjust activă, aparatul ajustează automat valoarea timpului de confirmare, fără intervenția utilizatorului.

TX/RX, Mbps Valoarea TX afișează rata de transfer, în Mbps, a ultimelor pachete transmise și valoarea RX afișează rata de transfer, în Mbps, a ultimelor pachete recepționate.

CCQ, % Evaluează calitatea conexiunii clientului (CCQ). Este o valoare procentuală, 100% corespunzând unei conexiuni perfecte.

Connection Time Afișează durata conexiunii pentru fiecare client conectat la aparat, sub forma zile, ore, minute și secunde.

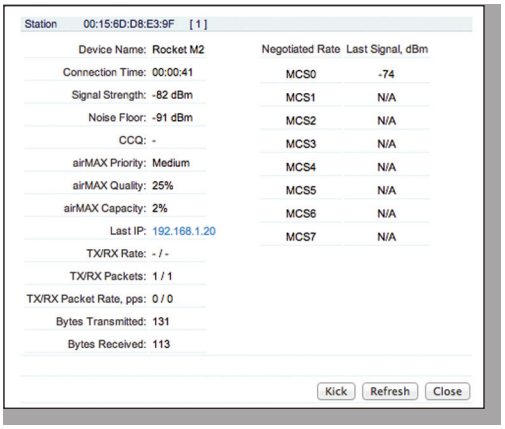
Last IP Afișează ultima adresă IP a clientului.

Action Afișează opțiunile disponibile pentru client. De exemplu, apăsați **KicK** pentru întreruperea conexiunii cu clientul.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

Detalii despre client

Când apăsați pe o adresă MAC, sunt afișate următoarele informații:

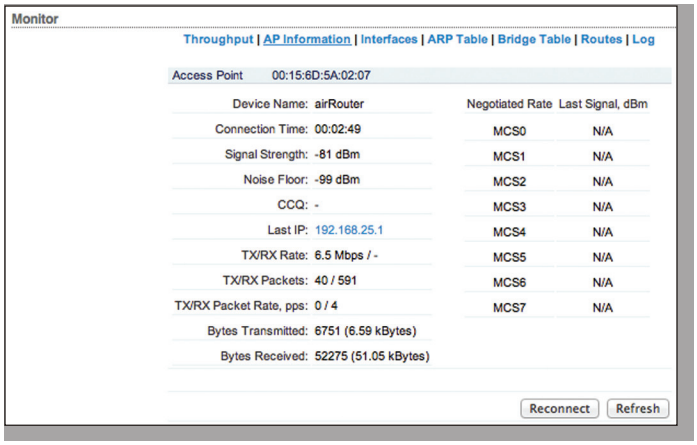


- Station Afișează adresa MAC a clientului.
- Device Name Afișează numele clientului.
- Connection Time Afișează durata conexiunii pentru fiecare client conectat la aparat, sub forma zile, ore, minute și secunde.
- Signal Strength Afișează valoarea în dBm a ultimului semnal wireless recepționat.
- Noise Floor Afișează valoarea curentă a zgomotului în dBm (de la interferențe) pe care aparatul o recepționează pe frecvența de operare. airOS ia în considerare valoarea Noise Flool în timp ce evaluează calitatea semnalului (Raportul semnal/Zgomot SNR, RSSI). Valoarea medie depinde de puterea semnalului peste cea a Noise Floor.
- Distance (Disponibilă dacă setarea *Auto Adjust* este activă în meniul *Advanced Wireless tab > Advanced Wireless Settings*) Afișează distanța dintre aparate, în kilometri și mile, pentru cadrele de confirmare (ACK). Cu opțiunea Auto Adjust activă, aparatul ajustează automat valoarea timpului de confirmare, fără intervenția utilizatorului.
- CCQ Valoarea reprezintă calitatea conexiunii cu AP-ul. Evaluează calitatea conexiunii clientului (CCQ). Este o valoare procentuală, 100% corespunzând unei conexiuni perfecte.
- airMAX Priority Prioritatea airMAX a clientului în comparație cu alți clienți.
- airMAX Quality Nivelul calității conexiunii airMAX este bazat pe un nivel de 100% care corespunde unei conexiuni perfecte.
- airMAX Capacity Este un indicator al nivelului de operare comparativ cu capacitatea maximă. Un număr mai mic indică o unitate care încetinește sistemul.
- Last IP Afișează adresa IP a clientului.
- TX/RX Rate Afișează rațelele de transfer în Mbps a ultimelor pachete transmise/recepționate.

- TX/RX Packets Afișează numărul total de pachete transmise și recepționate pe durata conexiunii.
- TX/RX Packet Rate, pps Afișează valoarea medie a ratei pachetelor transmise și recepționate.
- Bytes Transmitted Afișează cantitatea totală de date (în bytes) transmis pe durata conexiunii.
- Bytes Received Afișează cantitatea totală de date (în bytes) recepționate pe durata conexiunii.
- Negotiated Rate/Last Signal, dBm Valorile reprezintă nivelul semnalului wireless cu rata de transfer corespunzătoare pachetelor de date recepționate recent. Este afișat N/A dacă nu s-au primit pachete cu respectiva rată de transfer.
- Kick Pentru întreruperea conexiunii cu clientul apăsați **Kick**.
- Refresh Pentru actualizarea informațiilor apăsați **Refresh**.
- Close Pentru închiderea ferestrei apăsați **Close**.

AP Information

(Disponibil numai în modul *Station*) În acest submeniu se afișează informațiile despre AP-ul care este asociat aparatului.



Access Point Afișează adresa MAC a AP-ului.
Device Name Afișează numele AP-ului.

Connection Time Afișează durata conexiunii cu AP-ul, sub forma: zile, ore, minute și secunde.

Signal Strength Afișează valoarea în dBm a ultimului semnal wireless recepționat.

Noise Floor Afișează valoarea curentă a zgomotului în dBm (de la interferențe) pe care aparatul o recepționează pe frecvența de operare. airOS ia în considerare valoarea Noise Flool în timp ce evaluează calitatea semnalului (Raportul semnal/Zgomot SNR, RSSI). Valoarea medie depinde de puterea semnalului peste cea a Noise Floor.

CCQ Valoarea reprezintă calitatea conexiunii cu AP-ul. Evaluează calitatea conexiunii AP-ului (CCQ). Este o valoare procentuală, 100% corespunzând unei conexiuni perfecte.

Last IP Afișează adresa IP a AP-ului.

TX/RX Rate Afișează rațelele de transfer în Mbps a ultimelor pachete transmise/recepționate.

TX/RX Packets Afișează numărul total de pachete transmise și recepționate pe durata conexiunii.

TX/RX Packet Rate, pps Afișează valoarea medie a ratei pachetelor transmise și recepționate.

Bytes Transmitted Afișează cantitatea totală de date (în bytes) transmis pe durata conexiunii.

Bytes Received Afișează cantitatea totală de date (în bytes) recepționate pe durata conexiunii.

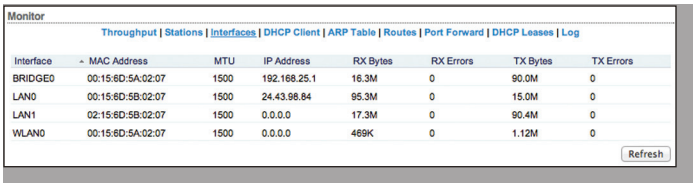
Negotiated Rate/Last Signal, dBm Valorile reprezintă nivelul semnalului wireless cu rata de transfer corespunzătoare pachetelor de date recepționate recent. Este afișat N/A dacă nu s-au primit pachete cu respectiva rată de transfer.

Reconnect Pentru restabilirea conexiunii cu AP-ul, apăsați **Reconnect**.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

Interfaces

Afișează numele, adresa MAC, MTU, adresa IP și informații despre trafic pentru interfețele aparatului.



Name Afișează numele interfeței.

MAC Address Afișează adresa MAC a interfeței

MTU Afișează valoarea MTU (Maximum Transmission Unit), care reprezintă mărimea maximă a unui pachet (în bytes) care poate fi transmisă de către interfață. Implicit este 1500.

IP Address Afișează adresa IP a interfeței.

RX Bytes Afișează cantitatea totală de date (în bytes), recepționată de interfață.

RX Errors Afișează numărul de erori de recepție.

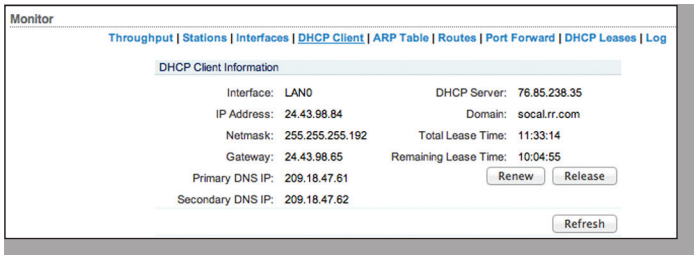
TX Bytes Afișează cantitatea totală de date (în bytes), transmisă de interfață.

TX Errors fișează numărul de erori de transmisie.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

DHCP Client

(Disponibil numai în modul *Router* sau *SOHO Router*) Afișează adresa IP WAN, masca de rețea, serverele DNS și gateway-ul aparatului, în timp ce funcționează ca și client DHCP al unui server DHCP.



Interface Afișează interfața care se conectează la un WAN.

IP Address Afișează adresa IP atribuită de un server DHCP conectat la interfața WAN. Dacă nu se găsește un server DHCP extern, se va folosi adresa IP definită în câmpul DHCP Fallback IP aflate în setările WAN Network Settings. Vedeți "**WAN Network Settings**" pagina 31.

Netmask Afișează masca de rețea atribuită de un server DHCP conectat la interfața WAN. Dacă nu se găsește un server DHCP extern, se va folosi adresa IP definită în câmpul DHCP Fallback Netmask aflate în setările WAN Network Settings. Vedeți "**WAN Network Settings**" pagina 31.

Gateway Afișează adresa Gateway atribuită de un server DHCP conectat la interfața WAN.

Primary/Secondary DNS IP DNS-ul (Domain Name System) este o carte de contacte a internetului care traduce numele de domenii în adrese IP. În aceste câmpuri se completează adresele IP ale serverelor pe care aparatul le folosește pentru traducere.

DHCP Server Afișează adresa IP a serverului DHCP extern, care atribuie adresa IP WAN aparatului.

Domain Afișează numele domeniului.

Total Lease Time Afișează timpul total (valabilitatea) pentru adresa IP atribuită de serverul extern DHCP.

Remaining Lease Time Afișează timpul de valabilitate rămas a adresei IP, atribuite de serverul DHCP extern.

Renew Pentru a cere noi setări IP de la serverul DHCP extern, apăsați **Renew**.

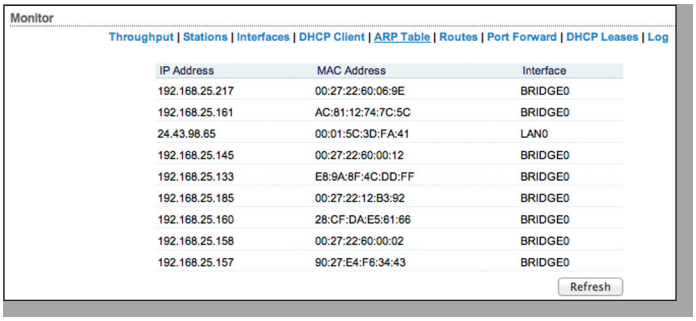
Release Pentru a elibera setările IP curente, apăsați **Release**.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

ARP Table

Afișează un tabel cu lista tuturor intrărilor ARP (Address Resolution Protocol) din aparat.

ARP este folosit pentru asocierea fiecărei adrese IP cu o adresă unică hardware MAC a fiecărui aparat din rețea. Este important ca fiecare adresă MAC să aibă o adresă IP unică, deoarece altfel pot apărea rute ambigue pe rețea.



IP Address Afișează adresa IP atribuită unui aparat.

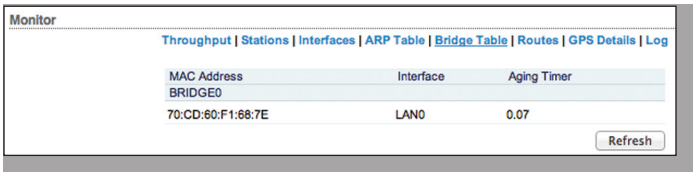
MAC Address Afișează adresa MAC atribuită unui aparat.

Interface Afișează interfața conectată la aparat.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

Bridge Table

(Disponibilă numai în modul *Bridge*) afișează toate intrările în tabelul *Bridge*.



MAC Address Un aparat în rețea este identificat după adresa MAC.

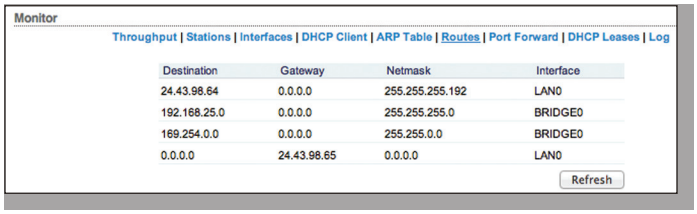
Interface Tabelul *Bridge* afișează cu care port sau interfață, LAN (Ethernet) sau WLAN (Wireless), aparatul de rețea este asociat. airOS poate transmite pachete numai către portul specificat, eliminând can forward packets only to the specified port of the device, eliminând transmisiile și copiile excesive.

Aging Timer Afișează timpul de îmbătrânire a unei adrese (în secunde). Dacă după un anumit timp aparatul nu a mai primit nici un pachet de la o anumită adresă, o va șterge din tabelul *Bridge*.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

Routes

Afișează toate intrările din tabelul de routare.



airOS examinează adresa IP de destinație a fiecărui pachet care tranzitează aparatul și alege interfața prin care să îl transmită. Alegerea depinde de rutele statice, intrări din tabelul de routare. Rutele statice pentru anumiți clienți, rețele sau gateway-ul implicit se crează automat în funcție de configurația tuturor interfețelor airOS.

Destination Afișează adresa IP a aparatului destinatar.

Gateway Afișează adresa IP a gateway-ului potrivit.

Netmask Afișează masca de rețea a aparatului destinatar.

Interface Afișează interfața pe care se află aparatul destinatar.

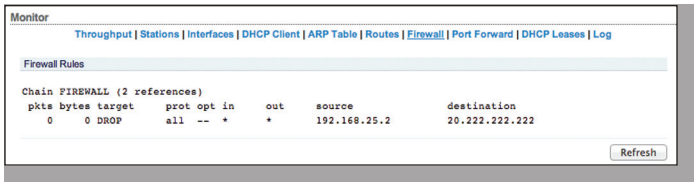
Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

Firewall

Această opțiune este disponibilă când firewall-ul este activ în meniul *Network*. Implicit nu există reguli firewall.

Dacă aparatul funcționează în modul *Bridge*, intrările firewall active sunt afișate în lanțul firewall a tabelului de filtrare ebtables.

Dacă aparatul funcționează în modul *Router* sau *SOHO Router*, intrările firewall active sunt afișate în lanțul firewall a tabelului de filtrare iptables.



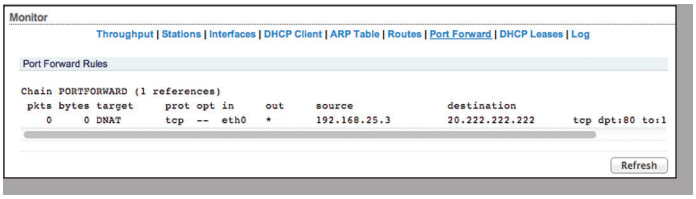
Firewall Rules În airOS, controlul accesului și filtrarea pachetelor IP și MAC, sunt implementate folosind firewall ebtables (bridging) sau iptables (routing), care protejează resursele rețelei private de amenințări externe, prin prevenirea accesului neautorizat și filtrarea unor tipuri de comunicare specifice.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

Configurați regulile firewall în meniul *Network*. Vedeți “**Firewall**” pagina 29.

Port Forward

(Disponibil numai în modul *Router* sau *SOHO Router*) Port forwarding vă permite să vă conectați la un serviciu specific ca un server FTP sau server Web. Port forwarding crează un tunel transparent prin firewall/NAT, permițând accesul dinspre WAN la un serviciu anume care rulează în LAN.



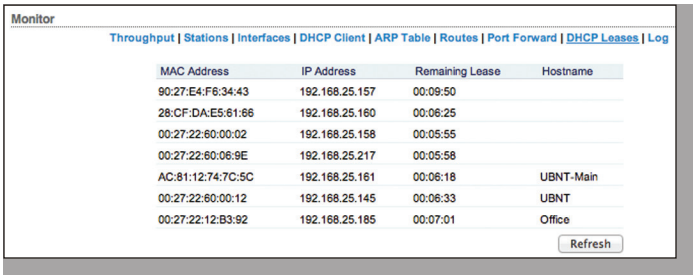
Port Forward Rules Afișează regulile de port forwarding active în lanțul PREROUTING al tabelului iptables nat, în timp ce aparatul funcționează în modul *Router* sau *SOHO Router*.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

Configurați regulile port forwarding în meniul *Network*. Vedeți “Port Forwarding” pagina 37.

DHCP Leases

(Disponibil numai în modul *Router* sau *SOHO Router* cu funcția server DHCP activă) Afișează status-ul adreselor IP atribuite de serverul DHCP clienților DHCP locali.



MAC Address Afișează adresa MAC a clienților.

IP Address Afișează adresa IP a clienților.

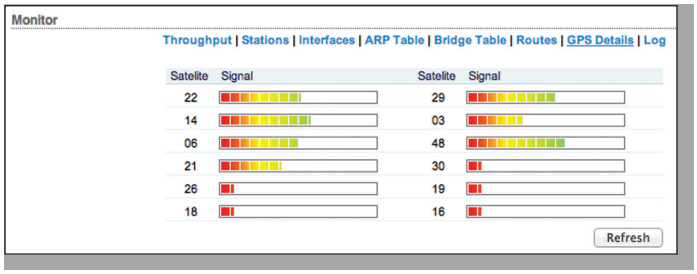
Remaining Lease Afișează timpul de valabilitate rămas a adresei IP atribuite de serverul DHCP.

Hostname Afișează numele clientului.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

GPS Details (Numai pentru seria GPS)

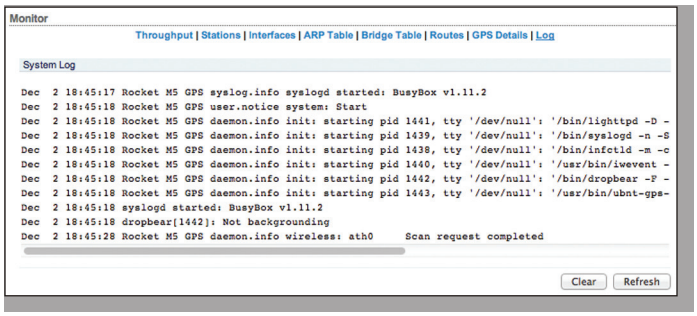
GPS Details (disponibil numai pentru aparatele din seria GPS) afișează detalii despre sateliți și calitatea semnalului.



Refresh Pentru actualizarea informațiilor apăsați **Refresh**.

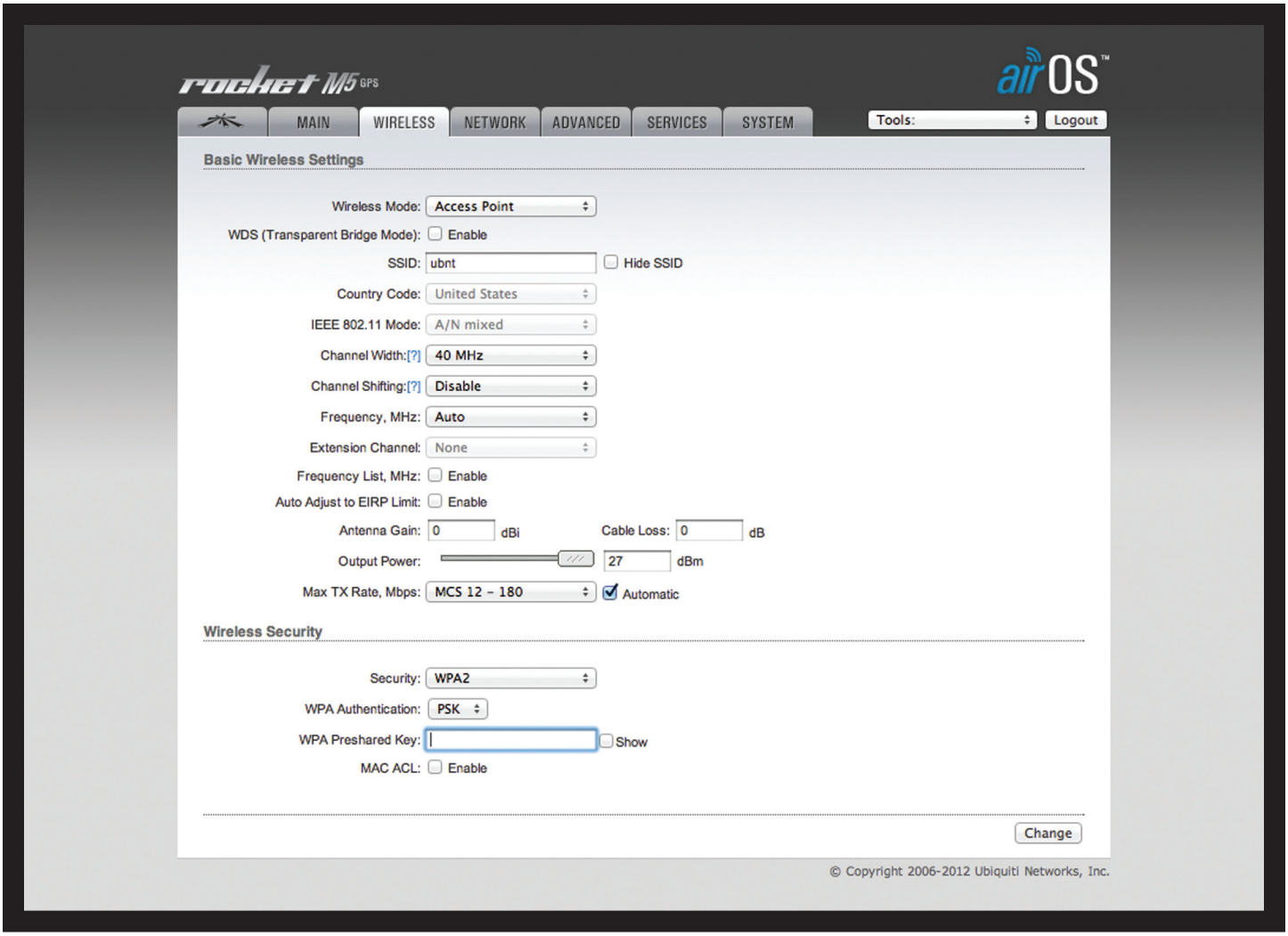
Log

Când logarea este activă (vezi "**System Log**" pagina 52 pentru activarea logării) afișează toate evenimentele înregistrate. Implicit logarea nu este activă.



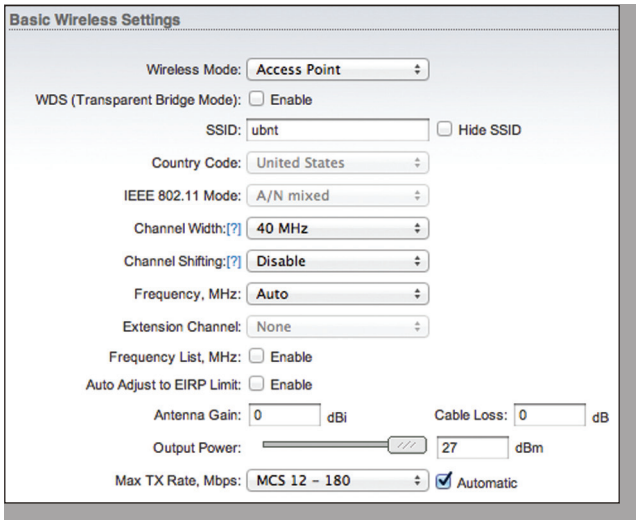
Clear Pentru a șterge toate intrările din *system log*, apăsați **Clear**.

Refresh Pentru actualizarea informațiilor apăsați **Refresh**.



Capitolul 4: Meniul Wireless

Meniul “Wireless” conține toate setările necesare configurării conexiunii wireless. Printre acestea se numără: SSID, canalul și frecvența, modul de funcționare, rata de transfer și setările de securitate.



Change Pentru a salva sau a testa modificările făcute apasați **Change**.
Apare un mesaj nou cu trei opțiuni:
Apply Pentru salvarea setărilor apăsați **Apply**.
Test Pentru a testa setările fără a salva apăsați **Test**. Pentru a păstra setările apăsați **Apply**. Dacă nu se apasă *Apply* timp de 180 secunde (cronometrul este afișat), atunci se revine la ultimele setări salvate.
Discard Pentru a renunța la setări apăsați **Discard**.

Basic Wireless Settings (Setări Wireless de bază)

În această secțiune se configurează setările de wireless de bază ca: tipul de conexiune wireless, numele rețelei (SSID), codul țării, tipul de protocol 802.11, puterea de emisie și rata de transfer.

Wireless Mode Specificați tipul de conexiune a aparatului. Tipul depinde de topologia rețelei. airOS oferă următoarele opțiuni:

Station Dacă aparatul dumneavoastră se conecteaza la un AP, atunci selectați modul *Station*. Aparatul devinde client al AP-ului. Se folosește numele AP-ului (SSID) și tot traficul dispozitivelor conectate la rețea este transmis AP-ului.

Nota: Dacă WDS (Tipul de Conexiune Transparentă) este dezactivat, atunci rețeaua folosește *arpnat*, care reprezintă o conexiune netransparentă. Pentru o conexiune transparentă selectați *Station* și activați WDS-ul.

- Access Point Dacă aparatul dumneavoastră se comportă ca un AP, atunci selectați *Access Point*. La un AP se pot conecta mai mulți clienți. În cazul mai multor AP-uri care nu sunt conectate Ethernet, selectează modul *AP-Repeater*.

Nota: Pentru a activa modul *Access Point* (WDS), selectați Access Point și apoi activați WDS.

- AP-Repeater Dacă aveți mai multe AP-uri selectați modul *AP-Repeater* pentru a creea o infrastructură wireless, WDS. Dacă opțiunea *Auto* este activă, toate AP-urile setate ca AP-Repeater și care au același SSID, se vor conecta în mod WDS. (Clienții se pot conecta în continuare la un AP setat ca AP-Repeater).

Nota: În modul *AP-Repeater*, nu vor funcționa metodele de securitate WPA/WPA2; se poate utiliza securitatea WEP sau nici un tip de securitate (acest lucru poate compromite securitatea rețelei). Există în continuare posibilitatea utilizării autentificării de tip RADIUS MAC și MAC ACL.

WDS (Tipul de conexiune transparentă) (Disponibil doar în modul *Access Point* sau *Station*) În majoritatea cazurilor este recomandată folosirea WDS, deoarece folosește traficul layer 2 transparent. Pentru activare, bifați căsuța **Enable**.

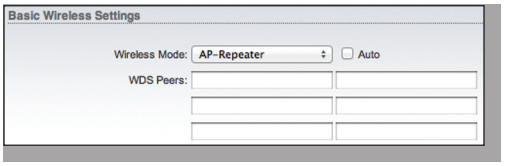
Protocolul WDS nu este definit ca standard, deci pot exista probleme de compatibilitate între echipamentele diferiților producători.

- Station (WDS) Station (WDS) trebuie folosit dacă AC-ul este configurat ca Access Point (WDS).
- Access Point (WDS) Access Point (WDS) permite conectarea Layer 2 între aparatele configurate ca Station (WDS).

Nota: Dacă se conectează un aparat configurat ca Station (WDS) la un aparat configurat ca Access Point (WDS), atunci pot fi folosite toate metodele de securitate (inclusiv WPA/WPA2)

Auto (Disponibil doar în modul *AP-Repeater*) Bifați căsuța **Auto** pentru stabilirea automată a conexiunii WDS între AP-uri în modul *AP-Repeater*. Dacă opțiunea Auto este activă, aparatul își va alege perechi WDS în funcție de setările SSID. În modul *AP-Repeater* nu se poate activa opțiunea Auto dacă folosiți tipurile de securitate WPA/WPA2, deoarece acestea necesită roluri diferite pentru AP-uri (autentificator sau solicitator).

Notă: Toate AP-urile configurate ca AP-Repeater, trebuie să funcționeze frecvență/canal și să folosească aceeași lățime de banda și aceleași setări de securitate.



WDS Peers (Disponibil numai în modul *AP-Repeater*) Dacă nu se bifează opțiunea Auto, atunci trebuie specificată lista de AP-uri în modul *AP-Repeater*. Introduceți adresa MAC a fiecărui AP în câmpul WDS Peers. În cazul unei conexiuni Punct la Punct (PtP) se va specifica doar o adresă MAC. În cazul unei conexiuni Punct la Multipunct (PtMP) se pot specifica până la șase perechi WDS.

SSID Dacă aparatul este configurat ca *Access Point* sau *AP-Repeater* se va specifica numele rețelei wireless sau SSID-ul (Service Set Identifier) folosit pentru identificarea rețelei dumneavoastră. AP-ul va fi vizibil pentru toate aparatele client aflate în raza acestuia.

În cazul aparatelor configurate ca *Station,* trebuie specificat SSID-ul AP-ului asociat. Pot mai multe AP-uri cu același SSID.

Select (disponibil numai în modul *Station*) Pentru afișarea listei cu AP-urile disponibile apăsați **Select**.

Unealta *Site Survey* va căuta rețelele wireless disponibile pe toate canalele suportate și va permite selectarea unei rețele pentru asociere. Dacă rețeaua selectată folosește criptare, este necesară configurarea setărilor de securitate wireless și salvarea acestora înainte de folosirea uneltei Site Survey.

- Lock to AP Selectați AP-ul din listă. Apăsați **Lock to AP** pentru a menține o conexiune permanentă cu AP-ul, în funcție de adresa MAC a acestuia.
- Select Selectați AP-ul din listă apoi apăsați **Select** pentru asociere.
- Scan Apasați **Scan** pentru actualizarea rețelelor wireless disponibile.

Puteți schimba lista frecvențelor scanate de Site Survey folosind opțiunea Frequency Scan List.

Lock to AP MAC (disponibil numai în modul *Station*) Această opțiune permite menținerea unei conexiuni permanante cu un AP, folosind o adresă MAC specifică. Acest lucru este util atunci când exista mai multe AP-uri cu același SSID. Intorduceți adresa MAC în câmpul **Lock to AP** MAC, pentru a bloca clientul pe un anumit AP.

Hide SSID (Disponibil numai în modul *AP-Repeater* sau *Access Point*) Când Hide SSID este activat, SSID-ul (wireless network name) nu este vizibil de către clienți.

Country Code Fiecare țară are propriile reglementări privind puterea de emisie și frecvență. Pentru a fi siguri că respectați reglementările, specificați corect țara în care folosiți aparatul. Modul IEEE 802.11, setările de canal, frecvența și limita puterii de emisie vor fi setate automat conform reglementărilor din țara aleasă. Pentru mai multe detalii despre reglementările internaționale, consultați RF Compliance Guide.

IEEE 802.11 Mode Se referă la standardul radio folosit de aparat. 802.11b, 802.11a, si 802.11g sunt vechile standarde, în timp ce 802.11n este un standard mai nou care oferă capacitate și performanață superioară. Opțiunile includ:

- A/N mixed Se poate conecta la o rețea 802.11a sau 802.11n. Acest mod oferă o mai bună compatibilitate. Modul A/N mixed este selectat ca implicit pentru următoarele aparate:
  - Seria M900
  - Seria M3
  - Seria M365
  - Seria M5
- B/G/N mixed Se poate conecta la o rețea 802.11b, 802.11g, sau 802.11n. Acest mod oferă o mai bună compatibilitate. Modul B/G/N mixed este selectat ca implicit pentru următoarele aparate:
  - Seria M2

Channel Width Afișează lățimea de bandă a canalului radio. Cu această opțiune puteți controla lățimea de bandă a conexiunii.

Folosirea unei lățimi de banda mai mare crește viteza de transfer. Folosirea unei lățimi de bandă mai mică:

- Reduce viteza de transfer proporțional cu lățimea canalului. De exemplu, o lățime de 40 MHz oferă o viteza de 2x mai mare decât cea de 20 MHz, iar lățimea de 10 MHz scade viteza de 2x față de 20 MHz.
- Mărește numărul de canale disponibile, neintercalate, pentru o dezvoltare mai bună a rețelelor.
- Mărește densitatea de putere (Power Spectral Density-PSD) a canalului, pentru obținerea unor conexiuni robuste pe distanțe mai mari.

În funcție de aparat, se pot selecta diferite lățimi de bandă:

- 2 MHz Canalul are o lățime de bandă de 2 MHz.
- 3 MHz Canalul are o lățime de bandă de 3 MHz.
- 5 MHz Canalul are o lățime de bandă de 5 MHz (cunoscut și ca modul Quarter-Rate).
- 8 MHz Canalul are o lățime de bandă de 8 MHz.
- 10 MHz Canalul are o latime de banda de 10 MHz (cunoscut și ca modul Half-Rate).
- 20 MHz Canalul standard cu o lățime de bandă de 20 MHz (acesta este selectat implicit).

  Notă: Pentru a conecta un aparat Wi-Fi care funcționează pe frecvența de 2.4 GHz, verificați că ați selectat lățimea de bandă 20 MHz.
- 25 MHz Canalul are o lățime de bandă de 25 MHz.
- 30 MHz Canalul are o lățime de bandă de 30 MHz.
- 40 MHz Canalul are o lățime de bandă de 40 MHz.
- Auto 20/40 MHz (Disponibil numai în modul *Station*) Oferă o compatibilitate mai bună.

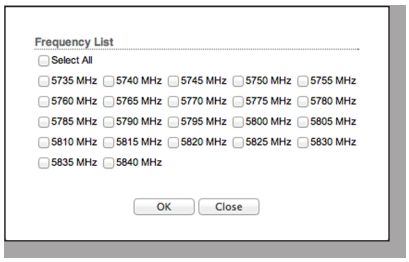
Channel Shifting Crează canale speciale cu o frecvență decalată față de canalele standard ale 802.11b/g/n și 802.11a. Această opțiune este dezvoltată și oferită doar de Ubiquiti Networks. În timp ce rețelele 802.11 au canale standard (de exemplu, canalul 36 (5180 MHz), canalul 40 (5200 MHz), etc, cu o distanță de 5 MHz între ele), channel shifting folosește canale nestandardizate (non-802.11) decalate de canalele standard. Toate canalele pot fi decalate cu 5 MHz (in 802.11a/n) sau 2 MHz (in 802.11b/g/n) de la frecvența standard.

Notă: Channel Shifting nu este compatibil cu produsele standard.

Channel Shifting oferă posibilitatea creării unei rețele private și implicit o securitate suplimentara deoarece este puțin probabil ca rețeaua sa fie detectată de alte aparate Wi-Fi.

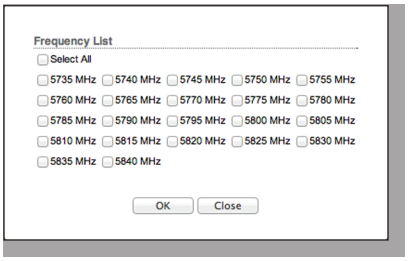
Extension Channel (Disponibil numai în modul *AP-Repeater* sau *Access Point* cu lățimea de banda 40 MHz) Un canal de 40 MHz este compus din două canale de 20 MHz. Extension Channel instruiește dispozitivul să adauge un canal suplimentar peste sau sub canalul standard existent. De exemplu, dacă selectați 5805 MHz (canal de 40 MHz) și Below, dispozitivul va folosi (de la 5775 la 5795 MHz) + (de la 5795 la 5815 MHz), dar dacă selectați 5805 MHz (canal de 40 MHz) și Above, dispozitivul va folosi (de la 5795 la 5815 MHz) + (de la 5815 la 5835 MHz).

Frequency List, MHz (Disponibil numai în modul *AP-Repeater* sau *Access Point*) Sunt disponibile mai multe frecvențe pentru a evita interferențele între AP-uri apropiate. Lista de frecvențe variază în funcție de țara selectată, modul IEEE 802.11, lățimea de bandă și de opțiunea Channel Shifting. Odată bifat *enabled*, apăsați **Edit** pentru a deschide fereastra cu lista de frecvențe.



Selectați frecvențele dorite și apăsați **OK** sau apăsați **Close** pentru a închide fereastra fără a face modificări.

Frequency Scan List, MHz (Disponibil numai în modul Station) Această opiune restricționează scanarea doar la frecvențele selectate. Ajută la o scanare mai rapidă și la filtrarea AP-urilor nedorite. Unealta *Site Survey* va căuta AP-uri doar în frecvențele selectate. Odată bifat enabled, apasați Edit pentru a deschide fereastra cu lista de frecvențe.



Selectati frecvențele dorite și apasați OK, sau apasați Close pentru a închide fereastra fără a face modificări.

Auto Adjust to EIRP Limit (Nu se aplică la NanoStation M900 loco.) Această opțiune ar trebui lăsată activa pentru a limita puterea de trasmisie conform reglementărilor țării selectate. Dacă opțiunea este activă nu se pot seta puteri de ieșire (EIRP) mai mari decât cele legale.(puterea de transmisie maximă și câștigul maxim al antenei diferă pentru fiecare standard IEEE 802.11b/g/n sau țară).

Pentru a putea dezactiva opțiunea *Auto Adjust to EIRP Limit*, trebuie bifată setarea *Installer EIRP Control* din meniul *Advanced*.

Antenna (disponibil numai pentru NanoStationM900 loco) Selectați opțiunea adecvată pentru dumneavoastră: I*nternal (2x2), External (1x1)*, sau *External + Internal (2x2)*. Conectorul RP-SMA extern va transmite lantul de date 0, ceea ce reprezintă polaritatea orizontală internă.

Antenna Gain (aplicabil doar aparatelor cu conector pentru antenă extern) Introduceți câștigul antenei în dB. Cu opțiunea *Auto Adjust to EIRP* Limit activată, *Antenna Gain* calculează reducerea puterii de transmisie necerară pentru a se menține în reglementări. Setarea *Antenna Gain* se folosește împreună cu setarea *Cable Loss*, ambele afectând puterea de transmisie.

Cable Loss (aplicabil doar aparatelor cu conector pentru antenă extern) Introduceți pierderea cablului în dB. Cu opțiunea *Auto Adjust to EIRP* Limit activată, *Cable Loss* afectează puterea de transmisie. În cazul pierderilor mari *pe cablu se mărește puterea de transmisie pentru încadrarea în reglementări.* Setarea Cable Loss se folosește împreună cu setarea Antenna Gain, ambele afectând puterea de transmisie.

Output Power Definește puterea de transmisie medie maximă (în dBm). Pentru a specifica puterea folosiți slider-ul sau introduceți manual valoarea puterii. Puterea de transmisie maximă este reglementată în funcție de tară. (Dacă aparatul are antenă internă atunci puterea de transmisie este aceeași cu puterea folosită de antena internă).

Max TX Rate, Mbps Definește rata de transfer (în Mbps) la care aparatul transmite pachetele. Puteți seta o rată de transfer specifică între MCS 0 și MCS 7 (sau MCS 15 pentru aparate cu lanțuri de date 2x2). Se recomandă folositea opțiunii *automatic*, în special dacă aveți probleme cu conexiunea sau aveți pierderi de pachete la viteze mari. În acest caz se vor folosi automat rate de transfer mai mici. Dacă selectați o lățime de bandă de 20 MHz, rata de transfer maximă este MCS 7 (65 Mbps) sau MCS 15 (130 Mbps). Dacă selectați o lățime de bandă de 40 MHz, rata de transfer maximă este MCS 7 (150 Mbps) sau MCS 15 (300 Mbps).

Automatic Dacă este bifată opțiunea, ajustează automat rata de transfer optimă în funcție de calitatea conexiunii. Se recomandă folositea opțiunii *automatic*, în special dacă aveți probleme cu conexiunea sau aveți pierderi de pachete la viteze mari. Pentru mai multe informații despre ratele de transfer studiați setările Wireless avansate.

Wireless Security (Securitatea rețelei Wireless)

În modul *Access Point* sau *AP-Repeater,* setările de securitate wireless vor fi folosite de toate aparatele din rețea.

În modul *Station*, introduceți setările de securitate folosite de AP-ul cu care este asociat.

În tabelul următor sunt prezentate metodele de securitate pentru fiecare mod de funcționare:

Security Method	Access Point	AP-Repeater	Station
none	X[1]	X[1]	X
WEP	X[2]	X[2]	X
WPA	X		X
WPA-TKIP	X		X
WPA-AES	X		X
WPA2	X		X
WPA2-TKIP	X		X
WPA2-AES	X		X

1 Dacă selectați *none* ca metodă de securitate se poate compromite securitatea rețelei, totuși puteți folosi autentificarea RADIUS MAC și MAC ACL.

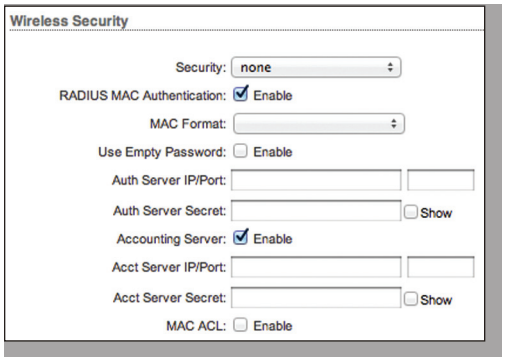
2 Dacă selectați WEP ca metodă de securitate se poate compromite securitatea rețelei, totuși puteți folosi MAC ACL.

Security airOS suportă urmatoarele setări de securitate wireless:

- none Dacă nu doriți nici un tip de securitate selectați **none**. Aveți în continuare opțiunea folosirii autentificării RADIUS MAC și MAC ACL.
- WEP WEP (Wired Equivalent Privacy) este cel mai vechi și puțin sigur algoritm de securitate. Când este posibil, folosiți WPA or WPA2.
- WPA WPA (Wi-Fi Protected Access) a fost dezvoltată ca o alternativă de criptare mai puternică decât WEP.

- WPA-TKIP WPA (Wi-Fi Protected Access) mod de securitate cu suport numai pentru TKIP (Temporal Key Integrity Protocol). TKIP folosește algoritmul de criptare RC4. Folosind TKIP există o limitare de performanță, de aceea se recomandă folosirea AES.
- WPA-AES WPA mod de securitate numai cu suport AES (Advanced Encryption Standard). AES mai este cunoscut ca CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), care folosește algoritmul AES.
- WPA2 WPA2 a fost dezvoltat pentru îmbunătățirea securității wireless și este mai puternic decât WEP și WPA.
- WPA2-TKIP mod de securitate WPA2 numai cu suport TKIP. TKIP uses RC4 encryption algorithm. TKIP folosește algoritmul de criptare RC4. Folosind TKIP există o limitare de performanță, de aceea se recomandă folosirea AES.
- WPA2-AES mod de securitate WPA2 numai cu suport AES. Este cea mai puternică opțiune de securitate disponibilă. Vă recomandăm să folosiți acest tip de securitate, dacă toate aparatele din rețea îl suportă.

None



RADIUS MAC Authentication Puteți autentifica aparatele folosind adresa lor MAC.

MAC Format Selectați formatul adreselor MAC.

Use Empty Password Pentru a salva o adresă MAC fără parolă bifați căsuța *Enable*.

Auth Server IP/Port În primul câmp introduceți adresa IP a serverului de autentificare RADIUS. RADIUS este un protocol de rețea, care furnizează Autentificare, Autorizare și Contabilizare centralizată, pentru calculatoarele ce folosesc servicii de rețea.

În al doilea câmp introduceți portul UDP al serverului de autentificare RADIUS. În mod uzual se folosește portul 1812, dar acesta poate varia în funcție de serverul RADIUS folosit.

Auth Server Secret Introduceți parola. Un șir de caractere secret și case-sensitive folosit pentru validarea locației dintre două aparate RADIUS.

Show Bifați căsuța dacă doriți să vizualizați caracterele din câmpul Auth Server Secret.

Accounting Server Dacă folosiți server de contabilizare separat, bifați căsuța *Enable*.

Acct Server IP/Port Dacă serverul de contabilizare este activat introduceți adresa IP a acestuia.

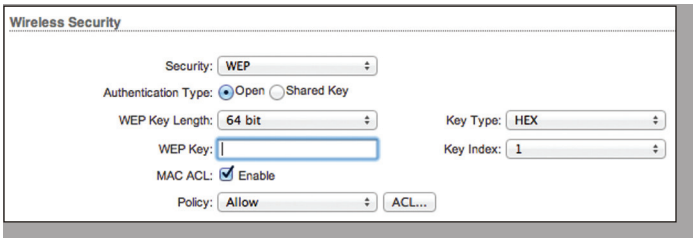
În al doilea câmp introduceți portul UDP al serverului de contabilizare RADIUS. În mod uzual se folosește portul 1813, dar acesta poate varia în funcție de serverul RADIUS folosit.

Acct Server Secret Dacă serverul de contabilizare este activat introduceți parola acestuia. Un șir de caractere secret și case-sensitive folosit pentru validarea locației dintre două aparate RADIUS.

Show Bifați căsuța dacă doriți să vizualizați caracterele din câmpul Acct Server Secret.

Mac ACL Citiți secțiunea "MAC ACL".

WEP



Authentication Type Selectați una din metodele de autentificare:

- Open Această opțiune este selectată implicit. Clientul este autentificat automat de către AP.
- Shared Key Clientul este autentificat după provocarea generată de AP.

WEP Key Length Specifică lungimea cheii de securitate WEP. Selectați una din cele două opțini:

- 64-bit Această opțiune este selectată implicit. O cheie de 64-biti are o lungime de 10 caractere HEX sau 5 caractere ASCII.
- 128-bit Opțiunea de 128-biti furnizează o securitate sporită și are o lungime de 26 caractere HEX sau 13 caractere ASCII.

Key Type Specifică tipul de caractere din care este formată cheia WEP:

- HEX Este opțiunea implicită și folosește caractere hexazecimale. 0-9, A-F, sau a-f sunt caractere valide.
- ASCII ASCII folosește alfabetul standard englezesc și caractere numerice.

WEP Key Introduceți o cheie WEP adecvată:

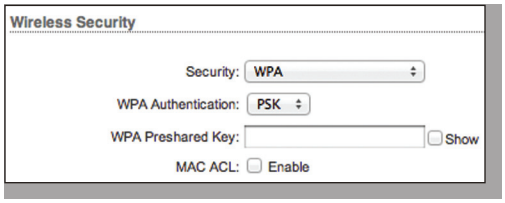
Type	HEX	ASCII
64-bit	10 hexadecimal characters (0-9, A-F or a-f) Example: **00112233AA**	5 ASCII characters Example: **ubnt1**
128-bit	26 hexadecimal characters (0-9, A-F or a-f) Example: **00112233445566778899AABBCC**	13 ASCII characters Example: **ubntproducts1**

Key Index Specifică indexul cheii WEP folosite. Se pot configura 4 chei WEP în același timp, dar numai una poate fi folosită. Pentru a activa cheia dorită selectați **1**, **2**, **3**, sau **4**.

Mac ACL Citiți secțiunea "MAC ACL".

WPA or WPA2

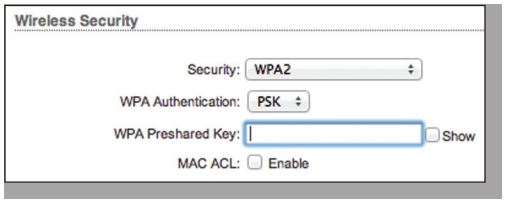
Opțiunile de configurare sunt identice atât pentru WPA cât și pentru WPA2. WPA2-AES este cea mai puternică metodă de securitate. Vă recomandăm să folosiți acest tip de securitate, dacă toate aparatele din rețea îl suportă.



WPA Authentication Specificați una din următoarele metode de selectare a cheii WPA:

- PSK Metoda cheii pre-distribuite (selectată implicit).
- EAP EAP (Extensible Authentication Protocol) Metodă de autentificare IEEE 802.1x. Această metodă se folosește în special în rețelele enterprise.

PSK



WPA Preshared Key Specificați parola. Cheia pre-distribuită este formată din 8-63 caractere alpha-numerice.

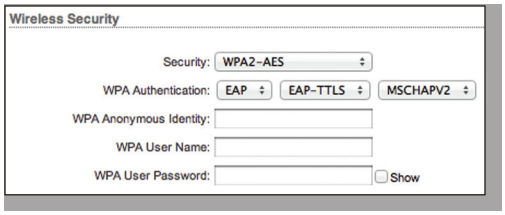
Show Bifați căsuța dacă doriți să vizualizați caracterele din câmpul WEP Preshared Key.

Mac ACL Citiți secțiunea "MAC ACL".

EAP

EAP - Station Mode

Următoarele opțiune sunt aplicabile numai în modul Station.



EAP-TTLS / EAP-PEAP Selectați protocolul de autentificare folosit de AP-ul dumneavoastră.

MSCHAPV2 Protocol de autentificare intern.

WPA Anonymous Identity Introduceți datele de identificare folosite de client pentru autentificarea EAP în forma necriptată.

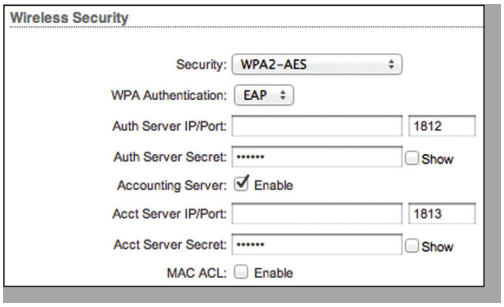
WPA User Name Introduceți datele de identificare folosite de client pentru autentificarea EAP.

WPA User Password Introduceți datele de identificare folosite de client pentru autentificarea EAP.

Show Bifați căsuța dacă doriți să vizualizați caracterele din câmpul WPA User Password.

EAP- Access Point Mode

Următoarele opțiune sunt aplicabile numai în modul Access Point sau AP-Repeater.



Auth Server IP/Port În primul câmp introduceți adresa IP a serverului de autentificare RADIUS. RADIUS este un protocol de rețea, care furnizează Autentificare, Autorizare și Contabilizare centralizată, pentru calculatoarele ce folosesc servicii de rețea.

În al doilea câmp introduceți portul UDP al serverului de autentificare RADIUS. În mod uzual se folosește portul 1812, dar acesta poate varia în funcție de serverul RADIUS folosit.

Auth Server Secret ntroduceți parola. Un șir de caractere secret și case-sensitive folosit pentru validarea locației dintre două aparate RADIUS.

Show Check the box if you want to view the characters of the Auth Server Secret.

Accounting Server Bifați căsuța dacă doriți să vizualizați caracterele din câmpul Auth Server Secret.

Acct Server IP/Port Dacă serverul de contabilizare este activat introduceți adresa IP a acestuia.

În al doilea câmp introduceți portul UDP al serverului de contabilizare RADIUS. În mod uzual se folosește portul 1813, dar acesta poate varia în funcție de serverul RADIUS folosit.

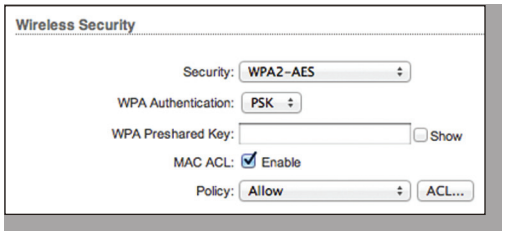
Acct Server Secret Dacă serverul de contabilizare este activat introduceți parola acestuia. Un șir de caractere secret și case-sensitive folosit pentru validarea locației dintre două aparate RADIUS.

Show Bifați căsuța dacă doriți să vizualizați caracterele din câmpul Acct Server Secret.

Mac ACL Citiți secțiunea "MAC ACL".

MAC ACL

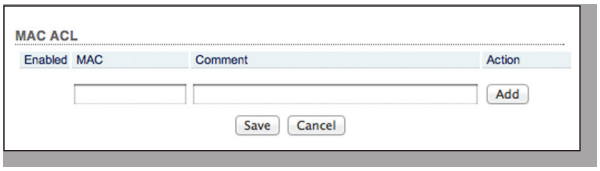
Următoarele opțiune sunt aplicabile numai în modul Access Point sau AP-Repeater.



MAC ACL MAC ACL vă oferă posibilitatea de a permite clienților accesul la aparat sau de a-i bloca. Când este activ aveți următoarele opțiuni:

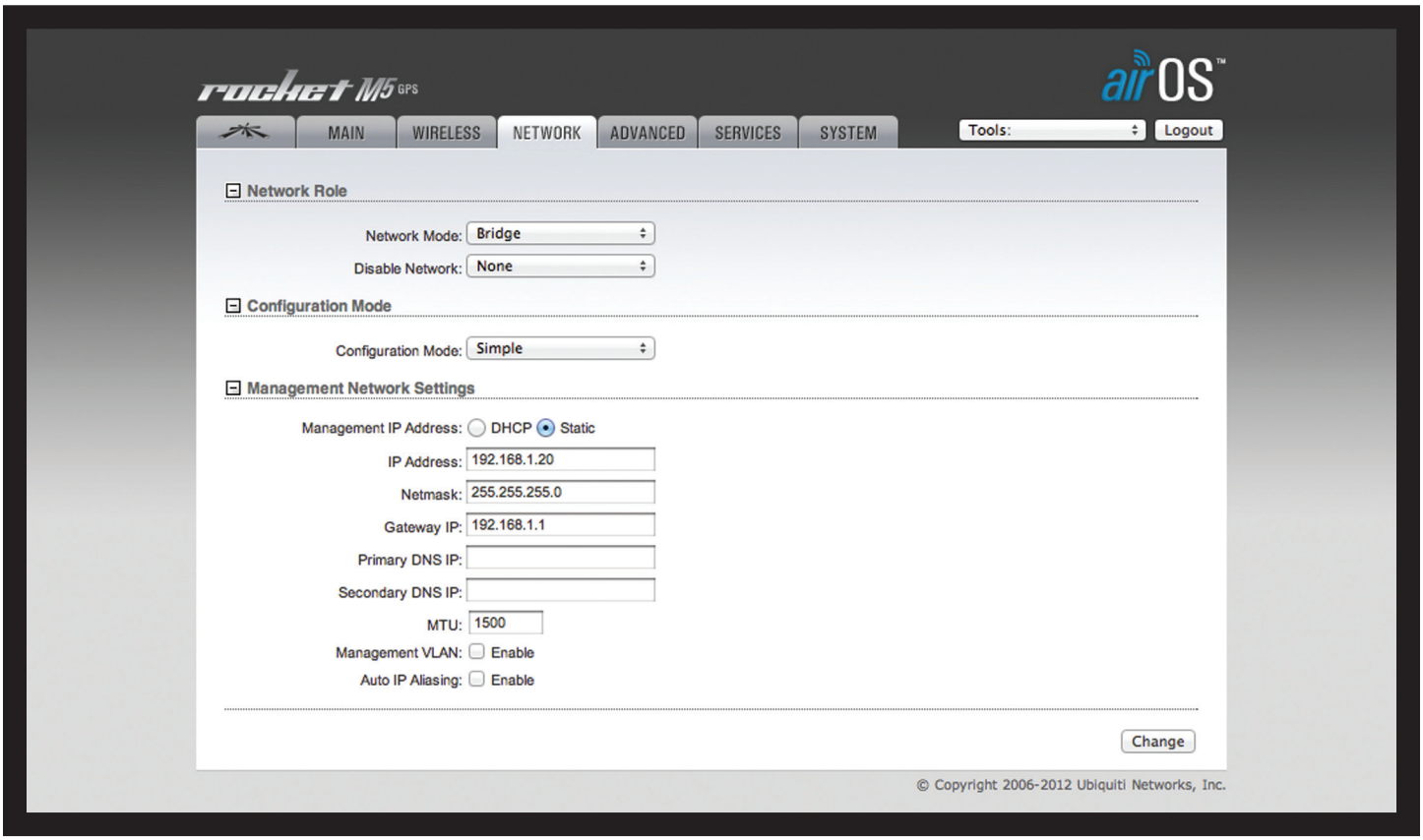
Policy Selectați una dintre tipurile de politică:

- Allow Clienții aflați pe listă pot accesa aparatul. Orice client ce nu se afla pe listă are accesul blocat la aparat.
- Deny Clienții aflați pe listă au accesul blocat la aparat. Orice client ce nu se află pe listă poate accesa aparatul.
- ACL Pentru a adăuga adresele MAC ale clienților wireless apăsați ACL.



- Enabled Politica se va aplica acestui client.
- MAC Introduceți adresa MAC sub acest format: XX:XX:XX:XX:XX:XX (fiecare X reprezintă un caracter hexazecimal: 0-9, A-F, sau a-f).
- Comment Introduceti o descriere a clientului wireless.
- Action Apăsați Add pentru a adăuga adresa MAC a unui client wireless. Apăsați Del pentru a șterge adresa MAC a unui client wireless. Apăsați Edit pentru a face modificări la un câmp.

Nota: MAC ACL ar trebui folosit în combinație cu o metodă de securitate ca WPA sau WPA2. Nu ar trebui folosit ca singura metodă de securitate a rețelei.



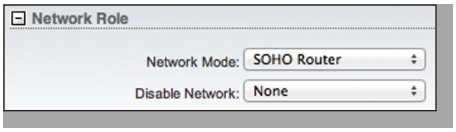
Capitolul 5: Meniul Network

Meniul Network vă permite să configurați aparatul în modul bridge sau routing și să configurați setările IP.

Change Pentru a salva sau a testa modificările făcute apasați **Change**.
Apare un mesaj nou cu trei opțiuni:
Apply Pentru salvarea setărilor apăsați **Apply**.
Test Pentru a testa setările fără a salva apăsați **Test**. Pentru a păstra setările apăsați **Apply**. Dacă nu se apasă *Apply* timp de 180 secunde (cronometrul este afișat), atunci se revine la ultimele setări salvate.
Discard Pentru a renunța la setări apăsați **Discard**.

Network Role

airOS suportă următoarele moduri de funcționare: *Bridge, Router* și *SOHO Router*. Numai router-ele suportă modurile router.



Network Mode Specifați modul de rețea al aparatului. Setarea inițială diferă în funcție de aparat. Modul depinde structura rețelei.

Modul *Bridge* este potrivit pentru rețelele foarte mici. Totuși, o rețea mare cu mult trafic, necesită setarea aparatului în modul *Router* sau *SOHO Router*. Modul *Router* sau *SOHO Router* păstrează traficul broadcast în domeniul propriu pentru ca acesta să nu încarce traficul întregii rețele.

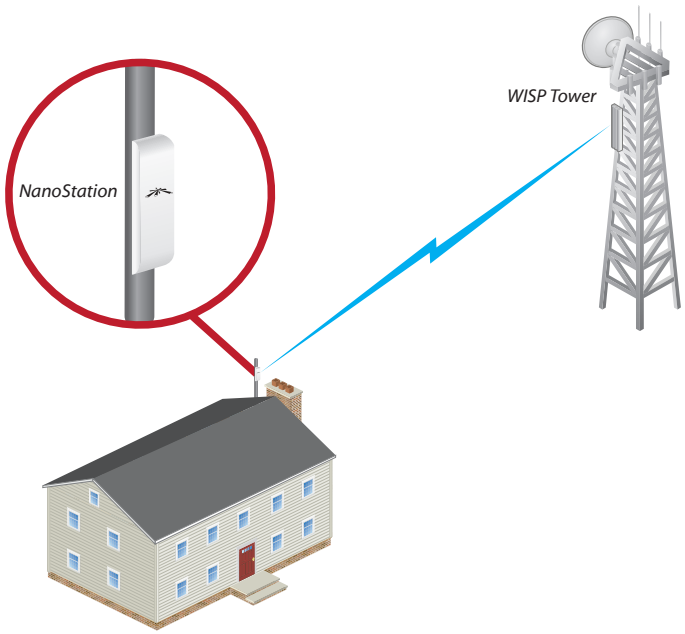
- Bridge Aparatul oferă o conexiune transparentă Layer 2, similară cu cea oferită de un switch neadministrat.

  În modul Bridge se setează o singură adresă IP pentru aparat.

- Router Aparatul este separat în două rețele sau subrețele (una WAN și una LAN). În modul *Router*, interfața wireless funcționează ca WAN (Wide Area Network). Porturile Ethernet funcționează ca LAN. Fiecare interfață wireless sau cu fir din rețeaua WAN sau LAN are o adresă IP.

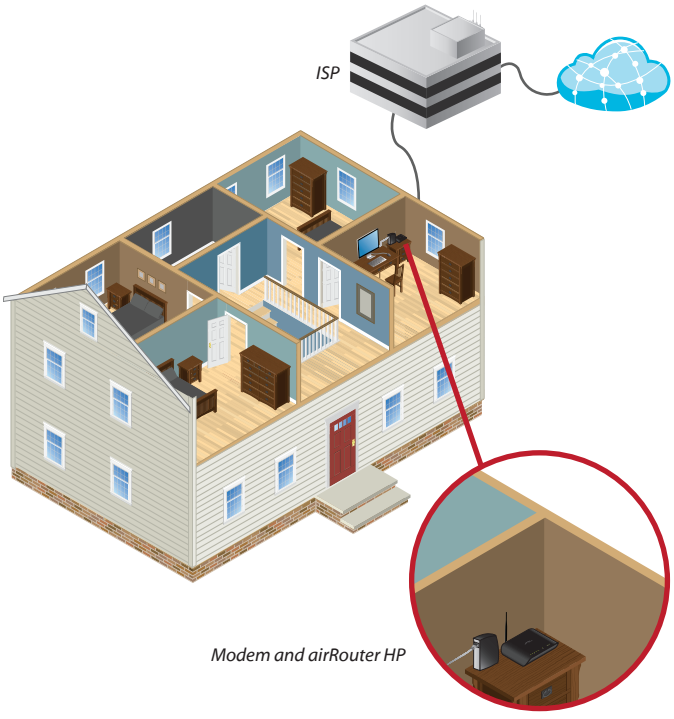
  De exemplu, modul *Router* este folosit în special în instalările CPE (Customer Premises Equipment). Aparatul se comportă ca un punct de separație între CPE și WISP (Wireless Internet Service Provider) cu interfața wireless conectată la WISP.

Următoarea imagine arată un aparat NanoStation rezidențial conectat la un turn WISP.



- SOHO Router Modul *SOHO* (Small Office/Home Office) *Router* este derivat din modul *Router*. În modul *SOHO Router*, portul Ethernet principal marcat cu <⋯> funcționează ca port WAN. Interfața WLAN și alte porturi Ethernet funcționează ca LAN. Fiecare interfață wireless sau cu fir de pe WAN or LAN are o adresă IP.

  De exemplu, modul *SOHO Router* este folosit într-o instalare în care portul principal Ethernet se conectează la ISP (Internet Service Provider). Următoarea imagine arată aparatul airRouter HP conectat la un modem, care este conectat la ISP.



Disable Network Dezactivează interfața WLAN, LAN, sau WAN. Folosiți această setare cu grijă, deoarece pe interfața conectată nu veți putea realiza nici o conexiune pe Layer 2 sau Layer 3. Nu veți putea accesa aparatul dinspre rețeaua wireless sau cu fir conectată la interfața dezactivată.

Pentru mai multe informații despre modurile de rețea, citiți:

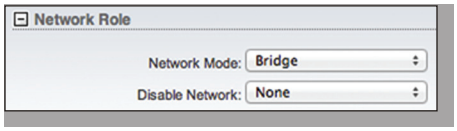
- "**Bridge**" pagina 26
- "**Router**" pagina 30
- "**SOHO Router**" pagina 38

Bridge

În modul *Bridge*, aparatul retransmite toate pachetele de date și management de la o interfață la alta, fără routare inteligentă. Pentru aplicații simple, acesta oferă o soluție de rețea transparentă eficientă.

Nu există o divizare a rețelei, iar domeniul broadcast este același. Modul *Bridge* nu blochează nici un fel de trafic broadcast sau multicast. Puteți configura setări firewall adiționale pentru filtrarea pachetelor Layer 2 și pentru controlul accesului.

Interfețele WLAN și LAN fac parte din aceeași rețea și împart același grup de adrese IP. Acestea formează o interfață bridge virtuală, comportându-se ca porturi bridge. Setările IP sunt disponibile numai în scopul de management al aparatului.



Configuration Mode

Meniul Network dispune de două moduri de vizualizare: Simple și Advanced.

Simple Sunt disponibile setările de configurare de bază. Setările avansate sunt ascunse.

Advanced Afișează setările avansate de configurare:

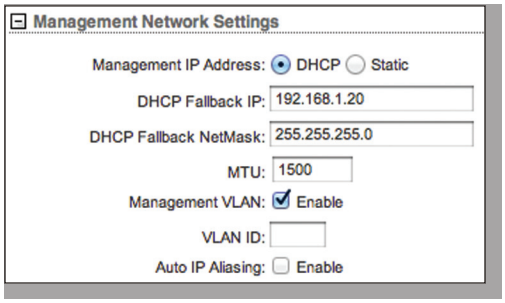
- "**Management Network Settings**" pagina 26
- "**Interfaces**" pagina 27
- "**IP Aliases**" pagina 28
- "**VLAN Network**" pagina 28
- "**Bridge Network**" pagina 28
- "**Firewall**" pagina 29
- "**Static Routes**" pagina 29
- "**Traffic Shaping**" pagina 29

Management Network Settings

Management Interface (Disponibil în vederea *Advanced*) Selectați interfacța folosită pentru management.

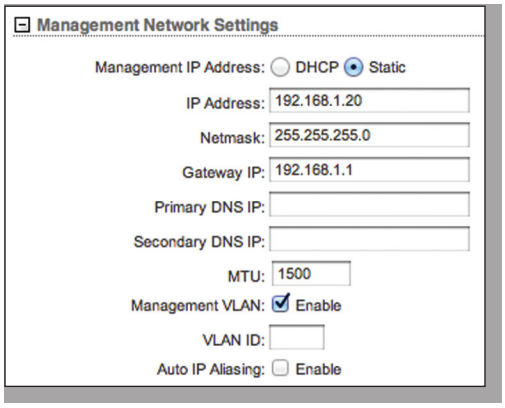
Management IP Address Aparatul poate folosi o adresă IP statică sau să obțină adresă IP de la un

- DHCP Serverul local DHCP atribuie aparatului adrese IP dinamice, adrese IP gateway și adrese DNS.



  - DHCP Fallback IP Specifați o adresă IP pentru aparat pentru când nu se găsește server DHCP.
  - DHCP Fallback Netmask Specifați o mască de rețea pentru aparat pentru când nu se găsește server DHCP.
- Static Specificați o adresă IP statică pentru aparat.

Notă: Setările IP trebuie să fie corespunzătoare segmentului de rețea din care aparatul face parte.



  - IP Address Specifați adresa IP a aparatului. IP-ul va fi folosit în scopul configurării aparatului.
  - Netmask Masca de rețea în formă binară furnizează informații pentru definirea unui interval de adrese IP folosit de aparatele din rețea. Masca de rețea definește segmentul de rețea al aparatului. Masca 255.255.255.0 (sau "/24") este folosită de obicei în cazul rețelelor IP de clasă C.
  - Gateway IP De obicei, este o adresă IP a router-ului care furnizează conexiunea la internet. Acesta poate fi un modem DSL, modem de cablu sau router WISP. Aparatul treimite pachetele care nu sunt destinate rețelei locale către gateway.

Notă: În modul *Bridge*, adresa IP gateway trebuie să fie în același segment de rețea ca aparatul.

  - Primary DNS IP Specifați adresa IP a serverului DNS (Domain Name System) principal.
  - Secondary DNS Specifați adresa IP a serverului DNS (Domain Name System) secundar. Acest câmp este opțional și este folosit numai dacă serverul DNS principal nu răspunde.

MTU (Disponibil în vederea *Simple*) Mărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Implicit este 1500.

Management VLAN (Disponibil în vederea *Simple*) Dacă este activat, apare automat un submeniu Virtual Local Area Network (VLAN).

- VLAN ID Introduceți un ID VLAN unic între 2 și 4094.

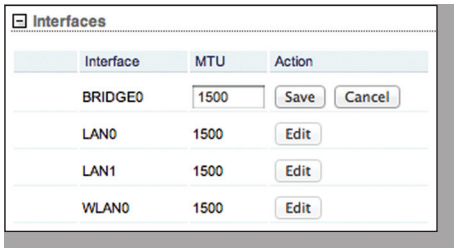
Auto IP Aliasing Dacă este activat, va genera automat o adresă IP corespunzătoare interfeței WLAN/LAN. Adresa IP generată este o adresă unică de clasă B din intervalul 169.254.X.Y (netmask 255.255.0.0), destinată folosirii în același segment de rețea. IP-ul generată începe întotdeauna cu 169.254.X.Y, unde X și Y sunt ultimii doi octeți din adresa MAC a aparatului. De exemplu, dacă adresa MAC este 00:15:6D:A3:04:FB, atunci adresa generată va fi 169.254.4.251.

Setarea *Auto IP Aliasing* este folosită deoarece puteți accesa și configura aparatul chiar dacă pierdeți, configurați greșit sau uitați adresa IP a acestuia. Puteți determina adresa IP a aparatului dacă cunoașteți adresa MAC, deoarece adresa generată se bazează pe ultimii doi octeți a adresei MAC.

Interfaces

(Disponibil în vederea *Advanced*) Mărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Puteți seta un MTU diferit pentru fiecare interfață

Apăsați butonul **+** pentru a afișa secțiunea *Interfaces*.



Interface Afișează numele interfeței.

MTU Implicit este 1500.

Action Apăsați **Edit** pentru a schimba valoarea MTU. Apoi, apăsați **Save** pentru a salva modificările.

IP Aliases

(Disponibil în vederea *Advanced*) Puteți configura un alias IP pentru interfețele locale și externe în scopul managementului aparatului. De exemplu, puteți avea nevoie de mai multe adrese IP pentru un singur aparat (o adresă privată și una publică). Dacă un CPE folosește PPPoE, acesta obține o adresă publică PPPoE, dar administratorul rețelei atribuie aparatului un alias IP intern. Astfel, administratorul rețelei poate accesa aparatul intern și nu prin intermediul serverului PPPoE.

Apăsați butonul **+** pentru a afișa secțiunea *IP Aliases*.

Enabled Activează un alias IP specific. Toate alias-urile IP adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

IP Address Adresa IP alternativă a interfeței. Aceasta poate fi folosită pentru routare sau pentru administrarea aparatului.

Netmask Masca de rețea pentru alias-ul IP.

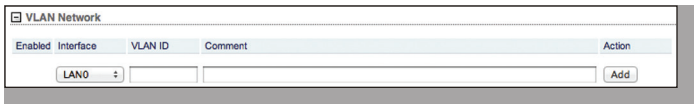
Comment Puteți introduce o scurtă descriere a alias-ului IP.

Action Aveți următoarele opțiuni:

- Add Adaugă un alias IP.
- Edit Modifică un alias IP. Apăsați **Save** pentru a salva modificările.
- Del Șterge un alias IP.

VLAN Network

(Disponibil în vederea *Advanced*) Puteți creea mai multe rețele virtuale (VLAN). Apăsați butonul **+** pentru a afișa secțiunea *VLAN Network.*



Enabled Activează un VLAN specific. Toate VLAN-urile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

VLAN ID VLAN ID este o valoare unică atribuită fiecărui VLAN de pe aparat. Fiecare VLAN ID reprezintă un VLAN diferit. Poate avea valori între 2 și 4094. Este permis un singur VLAN ID per aparat.

Comment Puteți introduce o scurtă descriere a VLAN-ului.

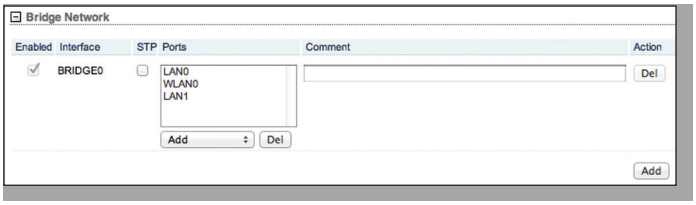
Action Aveți următoarele opțiuni:

- Add Adaugă un VLAN.
- Edit Modifică un VLAN. Apăsați **Save** pentru a salva modificările.
- Del Șterge un VLAN.

Bridge Network

(Disponibil în vederea *Advanced*) Puteți creea una sau mai multe bridge-uri dacă aveți nevoie de tranparență completă Layer 2. Este similar folosirii unui switch – tot traficul tranzitează bridge-ul, intră pe un port și iese pe altul, indiferent de adresa IP sau VLAN. De exemplu, dacă vreți să folosiți aceeași sub rețea pe ambele părți ale aparatului, atunci puteți creea un bridge. Sunt multe situații care necesită folosirea unui bridge, deci secțiunea *Bridge Network* oferă flexibilitate.

Apăsați butonul **+** pentru a afișa secțiunea *Bridge Network*.



Enabled Activează un bridge specific. Toate bridge-urile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Interfața este afișată automat.

STP Mai multe bridge-uri interconectate crează o rețea mai mare, care folosește protocolul STP-IEEE 802.1d (Spanning Tree Protocol), care găsește cea mai scurtă cale prin rețea, eliminând buclele din structură.

Dacă este activ, bridge-ul aparatului comunică cu alte aparate din rețea prin protocolul BPDU (Bridge Protocol Data Units). STP ar trebui dezactivat (setare implicită) când dispozitivul este singurul bridge din rețea pe rețea nu există bucle, deoarece setarea STP nu este necesară.

Ports Selectați porturile potrivite pentru crearea bridge-ului (Se pot selecta si porturi virtuale dacă ați creat rețele VLAN).

- Add Selectați un port.
- Del Ștergeți un port.

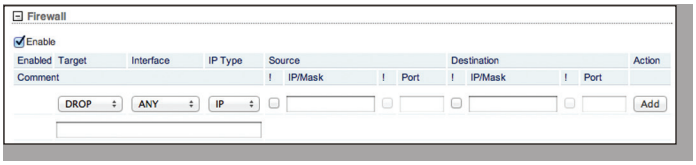
Comment Puteți introduce o scurtă descriere a bridge-ului.

Action Aveți următoarele opțiuni:

- Add Adaugă un bridge.
- Del Șterge un bridge.

Firewall

(Disponibil în vederea *Advanced*) Puteți configura regulile firewall ale interfeței rețelei locale sau externe. Apăsați butonul **+** pentru a afișa secțiunea Firewall.



Enable Activează firewall-ul.

Enabled Activează o regulă specifică a firewall-ului. Toate regulile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Target Pentru a permite trecerea pachetelor prin firewall, selectați **ACCEPT**. Pentru a bloca pachetele și a nu răspunde, selectați **DROP**.

Interface Selectați interfața potrivită pentru care se aplică regula firewall. Pentru a aplica regula firewall la toate interfețele, selectați **ANY**.

IP Type Specifică ce tip de protocol Layer 3 (IP, ICMP, TCP, UDP) trebuie filtrat.

! Poate fi folosit pentru inversarea criteriilor de filtrare Source IP/Mask, Source Port, Destination IP/Mask, și/sau Destination Port. De exemplu, dacă activați *!* (Not) pentru portul de destinație 443 (folosit de obicei de HTTPS), atunci criteriul de filtrare va fi aplicat pachetelor trimise către toate porturile de destinație, cu excepția portului 443.

Source IP/Mask Bifați căsuța apoi specificați sursa IP a pachetului (aflat în antetul pachetului). De obicei este adresa IP a sistemului care trimite pachetul.
Masca se notează sub forma "/xy". De exemplu, dacă introduceți 192.168.1.0/24, vă referiți la intervalul 192.168.1.0 - 192.168.1.255.

Source Port Bifați căsuța apoi specificați portul sursă a pachetului (aflat în antetul pachetului). De obicei este portul sistemului care trimite pachetul.

Destination IP/Mask Bifați căsuța apoi specificați IP-ul de destinație a pachetului (aflat în antetul pachetului). De obicei este adresa IP a sistemului căruia îi este destinat pachetul. Masca se notează sub forma "/xy". De exemplu, dacă introduceți 192.168.1.0/24, vă referiți la intervalul 192.168.1.0 - 192.168.1.255.

Destination Port Bifați căsuța apoi specificați portul de destinație a pachetului (aflat în antetul pachetului). De obicei este portul sistemului căruia îi este destinat pachetul.

Comment Puteți introduce o scurtă descriere a regulii firewall-ului.

Toate intrările firewall active sunt stocate în lanțul FIREWALL din tabelul ebtables filter.

Action Aveți următoarele opțiuni:

- Add Adaugă o regulă firewall.
- Edit Modifică o regulă firewall. Apăsați **Save** pentru a salva modificările.
- Del Șterge o regulă firewall.

Static Routes

(Disponibil în vederea *Advanced*) Puteți adăuga manual reguli statice de routare în tabelul de routare; puteți creea o regulă pentru ca o anume adresă IP (interval de adrese IP) să tranziteze către un anume gateway. Apăsați butonul **+** pentru a afișa secțiunea *Static Routes*.

Enabled Activează o rută statică specifică. Toate rutele adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Target Network IP Specificați adresa IP de destinație.

Netmask Specificați masca de rețea de destinație.

Gateway IP Specificați adresa IP a gateway-ului.

Comment Puteți introduce o scurtă descriere a rutei statice.

Action Aveți următoarele opțiuni:

- Add Adaugă o rută statică.
- Edit Modifică o rută statică. Apăsați **Save** pentru a salva modificările.
- Del Șterge o rută statică.

Traffic Shaping

(Disponibil în vederea *Advanced*) Traffic Shaping controlează lățimea de bandă din perspectiva clientului (care este conectat la interfața Ethernet). Facilitatea Bursting oferă viteze mari de descărcare atunci când utilizatorul descarcă fișiere mici (de exemplu, vizionarea unui pagini web), dar previne utilizatorul să folosească excesiv lățime de bandă atunci când descarcă fișiere mari (de exemplu, vizualizează un film).

Ca la Layer 3 QoS, puteți limita traficul unui aparat la nivel de port în funcție de rata maximă pe care o definiți. Fiecare port are două tipuri de trafic:

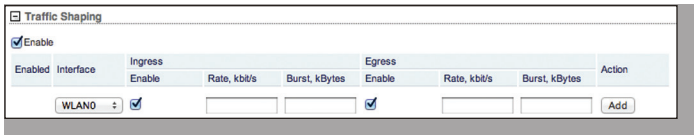
- Ingress traficul care intră în port
- Egress traficul care iese din port

Vă recomandăm sa folosiți Traffic Shaping pentru controlarea traficului egress, deoarece este mai eficient în direcția egress. Atunci când un port acceptă trafic ingress, nu poate controla cât de repede ajunge traficul – când transmite, aparatul poate controla traficul. Totuși, când portul transmite trafic egress, poate controla viteza de transmisie.

Funcția Bursting permite creșterea ratei de transfer peste valoarea maximă configurată în câmpurile *Ingress Rate* și *Egress Rate* – pentru o scurtă perioadă de timp. După folosirea rației Ingress sau Egress Burst (volum de date), rata de transfer scade la valorile pe care le-ați setat în câmpurile *Ingress Rate* sau *Egress Rate* (maximum bandwidth).

De exemplu, dacă folosiți următoarele setări:

- Ingress Burst este 2048 kBytes.
- Ingress Rate este 512 kbit/s.
- Rata de transfer reală este 1024 kbit/s. Bursting permite trecerea a 2048 kBytes cu rata de 1024 kbit/s, înainte de a o limita la 512 kbit/s.



Enable Activează controlul ratei de transfer pe aparat.
Enabled Activează o regulă specifică. Toate regulile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

Ingress

- Enable Activează valoarea ingress.
- Rate, kbit/s Specificați valoarea ratei de transfer maxime (în kilobits pe secundă) pentru traficul dinspre interfața wireless spre interfața Ethernet.
- Burst, kBytes Specificați volumul de date (în kilobytes) permis înainte ca valoarea ingress să fie limitată la valoarea maximă setată.

Egress

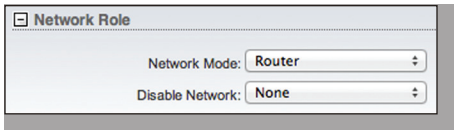
- Enable Activează valoarea egress.
- Rate, kbit/s Specificați valoarea ratei de transfer maxime (în kilobits pe secundă) pentru traficul dinspre interfața Ethernet spre interfața wireless.
- Burst, kBytes Specificați volumul de date (în kilobytes) permis înainte ca valoarea egress să fie limitată la valoarea maximă setată.

Action Aveți următoarele opțiuni:

- Add Adaugă o regulă.
- Edit Modifică o regulă. Apăsați **Save** pentru a salva modificările.
- Del Șterge o regulă.

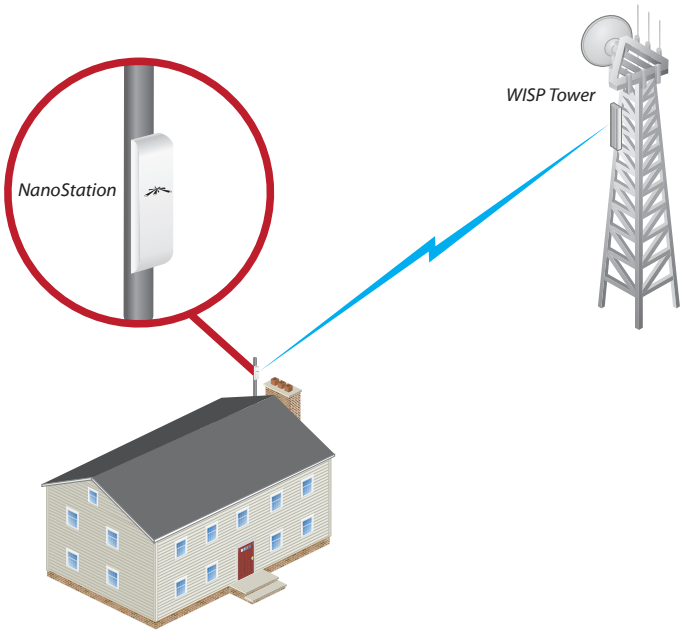
Router

În modul *Router*, aparatul operează în Layer 3 pentru efectuarea rutării și se activează segmentarea de rețea – clienții wireless sunt pe o subrețea diferită. Modul *Router* blochează traficul broadcast și poate trece prin traficul multicast. Puteți configura reguli firewall suplimentare pentru filtrarea pachetelor Layer 3 și pentru controlul accesului.



Aparatul poate funcționa ca server DHCP și poate folosi NAT (Network Address Translation - Masquerading), care este des folosit de AP-uri. NAT-ul se comportă ca un firewall între LAN și WAN.

În modul *Router*, interfața wireless funcționează ca WAN (Wide Area Network). Porturile Ethernet funcționează ca LAN. Fiecare interfață wireless sau cu fir din rețeaua WAN sau LAN are o adresă IP. De exemplu, următoarea imagine arată un aparat NanoStation rezidențial conectat la un turn WISP.



Configuration Mode

Meniul Network dispune de două moduri de vizualizare:

Simple și Advanced.

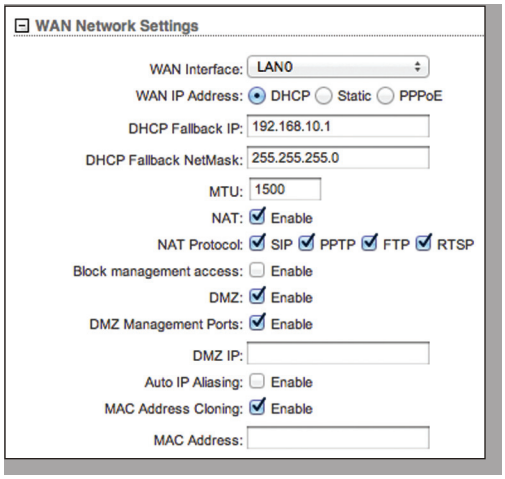
Simple Afișează setările de bază de configurare:

- "**WAN Network Settings**" pagina 31
- "**LAN Network Settings**" pagina 34
- "**Port Forwarding**" pagina 37
- "**Multicast Routing Settings**" pagina 37

Setările avansate sunt ascunse.
Advanced Afișează setările avansate de configurare:

- "**Management Network Settings**" pagina 35
- "**Interfaces**" pagina 35
- "**IP Aliases**" pagina 35
- "**VLAN Network**" pagina 35
- "**Bridge Network**" pagina 36
- "**Firewall**" pagina 36
- "**Static Routes**" pagina 37
- "**Traffic Shaping**" pagina 38

WAN Network Settings



WAN Interface Selectați interfața folosită pentru management.

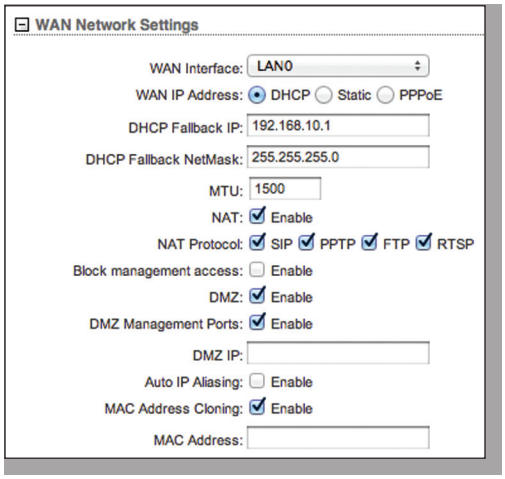
WAN IP Address Adresa IP a interfeței WAN este conectată la rețeaua externă. Puteți folosi această adresă IP pentru rutare sau pentru managementul aparatului.

Aparatul poate folosi următoarele:

- "**DHCP**" pagina 31
- "**Static**" pagina 32
- "**PPPoE**" pagina 33

DHCP

Serverul DHCP extern atribuie aparatului adrese IP dinamice, adrese IP gateway și adrese DNS.



DHCP Fallback IP Specifați o adresă IP pentru aparat pentru când nu se găsește server DHCP.

DHCP Fallback Netmask Specifați o mască de rețea pentru aparat pentru când nu se găsește server DHCP.

MTU (Disponibil în vederea *Simple*) Mărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Implicit este 1500.

NAT NAT-ul (Network Address Translation) permite expedierea pachetelor de la rețeaua externă (WAN) către adresa IP a interfeței locale și apoi subrutarea către un alt aparat client pe rețeaua locală, în timp ce aparatul airOS funcționează în modul *Access Point* sau *AP-Repeater*. Pachetele sunt rutate în direcția opusă față de modul *Station*.

NAT este implementat folosind reguli firewall de tip masquerade. Intrările NAT firewall sunt stocate în tabelul nat al iptables. Specificați rute statice pentru a permite pachetelor să traversese aparatul când NAT este dezactivat.

- NAT Protocol Dacă NAT este activ, puteți modifica pachetele de date pentru a le permite trecerea prin aparat. Pentru a evita modificarea unor pachete specifice ca: SIP, PPTP, FTP sau RTSP, debifați căsuțele respective.

Block management access Bifați căsuța pentru a bloca managementul aparatului dinspre interfața WAN. Această facilitate crește securitatea în modul *Router* dacă aparatul are o adresă IP publică.

DMZ DMZ (Demilitarized Zone) permite unui calculator/aparat din spatele NAT-ului să devină "demilitarizat", pentru ca toate porturile din rețeaua publică să fie transmise către porturi din această rețea privată, similar cu NAT 1:1.

- DMZ Management Ports Portul de management Web, (implicit portul TCP/IP 80) al aparatului airOS va fi folosit pentru acesta. Aparatul airOS va răspunde cererilor din rețeaua externă ca și când ar fi aparatul specificat ca DMZ. Dacă opțiunea *DMZ Management Ports* este activă, toate porturile vor fi transmise către aparatul DMZ, deciveți putea accesa aparatul doar dispre LAN.

• DMZ IP Specificați adresa IP a aparatului DMZ. Aparatul DMZ va fi complet expus la rețeaua externă.

Auto IP Aliasing Dacă este activat, va genera automat o adresă IP corespunzătoare interfeței WLAN/LAN. Adresa IP generată este o adresă unică de clasă B din intervalul 169.254.X.Y (netmask 255.255.0.0), destinată folosirii în același segment de rețea. IP-ul generată începe întotdeauna cu 169.254.X.Y, unde X și Y sunt ultimii doi octeți din adresa MAC a aparatului. De exemplu, dacă adresa MAC este 00:15:6D:A3:04:FB, atunci adresa generată va fi 169.254.4.251.

Setarea *Auto IP Aliasing* este folosită deoarece puteți accesa și configura aparatul chiar dacă pierdeți, configurați greșit sau uitați adresa IP a acestuia. Puteți determina adresa IP a aparatului dacă cunoașteți adresa MAC, deoarece adresa generată se bazează pe ultimii doi octeți a adresei MAC.

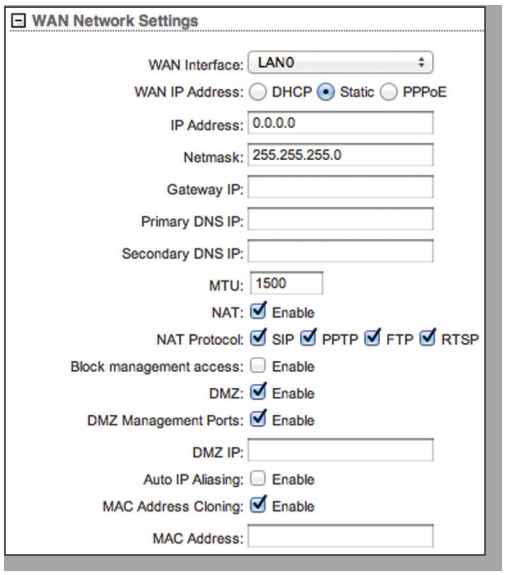
MAC Address Cloning Când este activă, vă permite să schimbați adresa MAC a respectivei interfețe. Opțiunea este folositoare atunci când ISP-ul asociază adresa IP cu o adresă MAC specifică. Această metodă este folosită în special de operatorii prin cablu sau unii operatori WISP.

- MAC Address Introduceți adresa MAC pentru interfața respectivă. Acesta devine noul MAC al interfeței.

Static

Specificați o adresă IP statică pentru aparat.

Notă: Setările IP trebuie să fie corespunzătoare segmentului de rețea din care aparatul face parte.



IP Address Specifați adresa IP a aparatului. IP-ul va fi folosit în scopul configurării aparatului.

Netmask Masca de rețea în formă binară furnizează informații pentru definirea unui interval de adrese IP folosit de aparatele din rețea. Masca de rețea definește segmentul de rețea al aparatului. Masca 255.255.255.0 (sau "/24") este folosită de obicei în cazul rețelelor IP de clasă C.

Gateway IP De obicei, este o adresă IP a router-ului care furnizează conexiunea la internet. Acesta poate fi un modem DSL, modem de cablu sau router WISP. Aparatul treimite pachetele care nu sunt destinate rețelei locale către gateway.

Primary DNS IP Specifați adresa IP a serverului DNS (Domain Name System) principal.

Secondary DNS IP Specifați adresa IP a serverului DNS (Domain Name System) secundar. Acest câmp este opțional și este folosit numai dacă serverul DNS principal nu răspunde.

MTU (Disponibil în vederea *Simple*) Mărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Implicit este 1500.

NAT NAT-ul (Network Address Translation) permite expedierea pachetelor de la rețeaua externă (WAN) către adresa IP a interfeței locale și apoi subrutarea către un alt aparat client pe rețeaua locală, în timp ce aparatul airOS funcționează în modul *Access Point* sau *AP-Repeater*. Pachetele sunt rutate în direcția opusă față de modul *Station*.

NAT este implementat folosind reguli firewall de tip masquerade. Intrările NAT firewall sunt stocate în tabelul nat al iptables. Specificați rute statice pentru a permite pachetelor să traversese aparatul când NAT este dezactivat.

- NAT Protocol Dacă NAT este activ, puteți modifica pachetele de date pentru a le permite trecerea prin aparat. Pentru a evita modificarea unor pachete specifice ca: SIP, PPTP, FTP sau RTSP, debifați căsuțele respective.

Block management access Bifați căsuța pentru a bloca managementul aparatului dinspre interfața WAN. Această facilitate crește securitatea în modul *Router* dacă aparatul are o adresă IP publică.

DMZ DMZ (Demilitarized Zone) permite unui calculator/aparat din spatele NAT-ului să devină "demilitarizat", pentru ca toate porturile din rețeaua publică să fie transmise către porturi din această rețea privată, similar cu NAT 1:1.

- DMZ Management Ports Portul de management Web, (implicit portul TCP/IP 80) al aparatului airOS va fi folosit pentru acesta. Aparatul airOS va răspunde cererilor din rețeaua externă ca și când ar fi aparatul specificat ca DMZ. Dacă opțiunea *DMZ Management Ports* este activă, toate porturile vor fi transmise către aparatul DMZ, deciveți putea accesa aparatul doar dispre LAN.

• DMZ IP Specificați adresa IP a aparatului DMZ. Aparatul DMZ va fi complet expus la rețeaua externă.

Auto IP Aliasing Dacă este activat, va genera automat o adresă IP corespunzătoare interfeței WLAN/LAN. Adresa IP generată este o adresă unică de clasă B din intervalul 169.254.X.Y (netmask 255.255.0.0), destinată folosirii în același segment de rețea. IP-ul generată începe întotdeauna cu 169.254.X.Y, unde X și Y sunt ultimii doi octeți din adresa MAC a aparatului. De exemplu, dacă adresa MAC este 00:15:6D:A3:04:FB, atunci adresa generată va fi 169.254.4.251.

Setarea *Auto IP Aliasing* este folosită deoarece puteți accesa și configura aparatul chiar dacă pierdeți, configurați greșit sau uitați adresa IP a acestuia. Puteți determina adresa IP a aparatului dacă cunoașteți adresa MAC, deoarece adresa generată se bazează pe ultimii doi octeți a adresei MAC.

MAC Address Cloning Când este activă, vă permite să schimbați adresa MAC a respectivei interfețe. Opțiunea este folositoare atunci când ISP-ul asociază adresa IP cu o adresă MAC specifică. Această metodă este folosită în special de operatorii prin cablu sau unii operatori WISP.

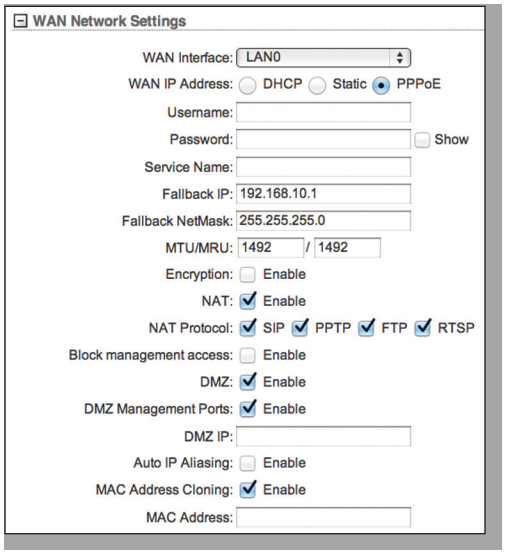
- MAC Address Introduceți adresa MAC pentru interfața respectivă. Acesta devine noul MAC al interfeței.

PPPoE

Protocolul PPPoE (Point-to-Point Protocol over Ethernet) este o conexiune sigură și privată, între două sisteme, care permite încapsularea datelor transportat. Clienții uneori folosesc PPPoE pentru conectarea la ISP (Internet Service Providers), în special la furnizorii DSL.

Selectați **PPPoE** pentru a configura un tunel PPPoE. Puteți configura o singură interfață externă de rețea, deoarece ca și client PPPoE va fi trimis prin acest tunel. După realizarea conexiunii PPPoE, aparatul va primi de la serverul PPPoE adresa IP, adresa Gateway și adresa serverului DNS. Adresa broadcast este folosită pentru descoperirea serverului PPPoE și realizarea tunelului.

Dacă există o conexiune PPPoE activă, atunci adresa interfeței PPP va fi afișată în meniul *Main* lângă statisticile interfeței PPP; altfel va fi afișat mesajul *Not Connected* și va fi activ butonul *Reconnect*. Pentru a reconecta tunelul PPPoE, apăsați **Reconnect**.



Username Specifați numele de utilizator pentru conectarea la serverul PPPoE; trebuie să fie identic cu cel configurat pe serverul PPPoE.

Password Specifați parola pentru conectarea la serverul PPPoE; trebuie să fie identică cu cea configurată pe serverul PPPoE.

Show Bifați căsuța pentru a vedea caracterele parolei.

Service Name Specificați numele serviciului PPPoE.

Fallback IP Specifați o adresă IP pentru aparat pentru când nu se găsește server DHCP.

DHCP Fallback Netmask Specifați o mască de rețea pentru aparat pentru când nu se găsește server DHCP.

MTU/MRU Mărimea (în bytes) pachetelor MTU (Maximum Transmission Unit) și MRU (Maximum Receive Unit) folosite pentru încapsularea datelor în timpul transferului prin tunel. Valoarea implicită este 1492.

Encryption Activează criptarea Microsoft Punct la Punct (Microsoft Point-to-Point Encryption - MPPE).

NAT NAT-ul (Network Address Translation) permite expedierea pachetelor de la rețeaua externă (WAN) către adresa IP a interfeței locale și apoi subrutarea către un alt aparat client pe rețeaua locală, în timp ce aparatul airOS funcționează în modul *Access Point* sau *AP-Repeater*. Pachetele sunt rutate în direcția opusă față de modul *Station*.

NAT este implementat folosind reguli firewall de tip masquerade. Intrările NAT firewall sunt stocate în tabelul nat al iptables. Specificați rute statice pentru a permite pachetelor să traversese aparatul când NAT este dezactivat.

- NAT Protocol Dacă NAT este activ, puteți modifica pachetele de date pentru a le permite trecerea prin aparat. Pentru a evita modificarea unor pachete specifice ca: SIP, PPTP, FTP sau RTSP, debifați căsuțele respective.

Block management access Bifați căsuța pentru a bloca managementul aparatului dinspre interfața WAN. Această facilitate crește securitatea în modul *Router* dacă aparatul are o adresă IP publică.

DMZ DMZ (Demilitarized Zone) permite unui calculator/aparat din spatele NAT-ului să devină "demilitarizat", pentru ca toate porturile din rețeaua publică să fie transmise către porturi din această rețea privată, similar cu NAT 1:1.

- DMZ Management Ports Portul de management Web, (implicit portul TCP/IP 80) al aparatului airOS va fi folosit pentru acesta. Aparatul airOS va răspunde cererilor din rețeaua externă ca și când ar fi aparatul specificat ca DMZ. Dacă opțiunea *DMZ Management Ports* este activă, toate porturile vor fi transmise către aparatul DMZ, deciveți putea accesa aparatul doar dispre LAN.

• DMZ IP Specificați adresa IP a aparatului DMZ. Aparatul DMZ va fi complet expus la rețeaua externă.

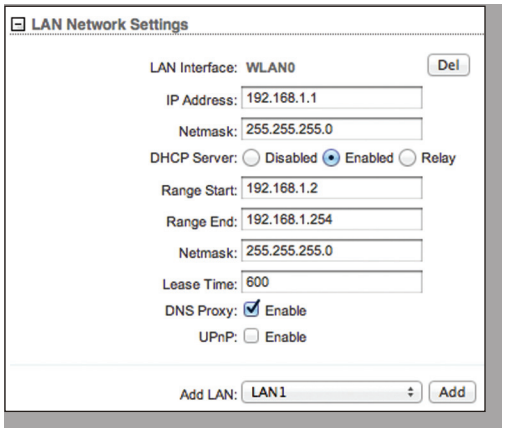
Auto IP Aliasing Dacă este activat, va genera automat o adresă IP corespunzătoare interfeței WLAN/LAN. Adresa IP generată este o adresă unică de clasă B din intervalul 169.254.X.Y (netmask 255.255.0.0), destinată folosirii în același segment de rețea. IP-ul generată începe întotdeauna cu 169.254.X.Y, unde X și Y sunt ultimii doi octeți din adresa MAC a aparatului. De exemplu, dacă adresa MAC este 00:15:6D:A3:04:FB, atunci adresa generată va fi 169.254.4.251.

Setarea *Auto IP Aliasing* este folosită deoarece puteți accesa și configura aparatul chiar dacă pierdeți, configurați greșit sau uitați adresa IP a acestuia. Puteți determina adresa IP a aparatului dacă cunoașteți adresa MAC, deoarece adresa generată se bazează pe ultimii doi octeți a adresei MAC.

MAC Address Cloning Când este activă, vă permite să schimbați adresa MAC a respectivei interfețe. Opțiunea este folositoare atunci când ISP-ul asociază adresa IP cu o adresă MAC specifică. Această metodă este folosită în special de operatorii prin cablu sau unii operatori WISP.

- MAC Address Introduceți adresa MAC pentru interfața respectivă. Acesta devine noul MAC al interfeței.

LAN Network Settings



LAN Interface Interfața este afișată. Apăsați **Del** pentru a șterge interfața. Dacă nu există nici o interfață selectată, selectați una din lista *Add LAN* și apăsați **Add**.

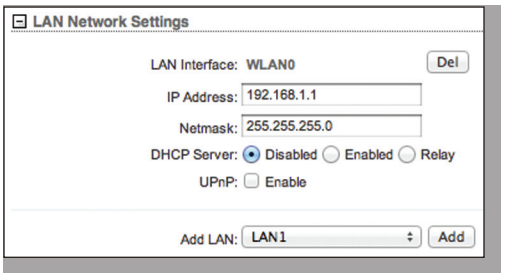
IP Address Adresa IP a interfeței LAN (inclusiv WLAN) conectată la rețeaua locală. Acest IP va fi folosit pentru rutarea rețelei locale; va fi IP-ul gateway pentru toate aparatele din rețeaua locală. Acest IP este folosit pentru managementul aparatului.

Netmask Definește clasa IP pentru intervalul IP ales. 255.255.255.0 este clasa de rețea obișnuită pentru rețelele de clasă C, care suportă intervalul de adrese IP de la 192.0.0.x până la 223.255.255.x. Masca unei rețele în clasă C, folosește 24 biți pentru identificarea rețelei (notare alternativă "/24") și 8 biți pentru identificarea unui aparat.

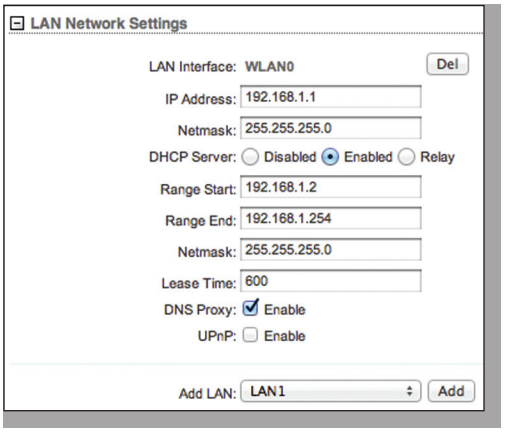
MTU (Disponibil în vederea *Simple*) Mărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Implicit este 1500.

DHCP Server Serverul DHCP integrat, atribuie adrese IP clienților conectați la interfața wireless și la interfața LAN când funcționează în modul *Access Point* sau *AP-Repeater*. Serverul DHCP integrat, atribuie adrese IP clienților conectați la interfața LAN când funcționează în modul *Station*.

- Disabled Aparatul nu atribuie adrese IP.

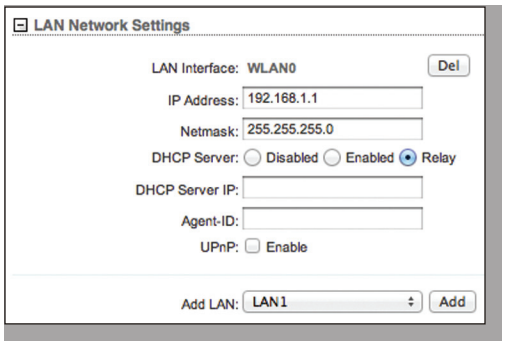


- Enabled Aparatul atribuie adrese IP clienților din rețeaua locală.



  - Range Start and End Determină intervalul de adrese IP atribuite de serverul DHCP.
  - Netmask Definește clasa IP pentru intervalul IP ales. 255.255.255.0 este clasa de rețea obișnuită pentru rețelele de clasă C, care suportă intervalul de adrese IP de la 192.0.0.x până la 223.255.255.x. Masca unei rețele în clasă C, folosește 24 biți pentru identificarea rețelei (notare alternativă "/24") și 8 biți pentru identificarea unui aparat.
  - Lease Time Adresele IP atribuite de serverul DHCP sunt valide o durată specifică de timp (lease time). Creșterea perioadei asigură o operare a clientului neîntreruptă, dar poate creea conflicte. Scăderea timpului evită potențialele conflicte de adresă, dar poate cauza mai multe întreruperi pentru client în timpul obținerii unei noi adrese IP de la serverul DHCP. Timpul este exprimat în secunde.
  - DNS Proxy Serverul DNS (Domain Name System) proxy, transmite cererile DNS de la clienții din rețeaua locală către serverul DNS.

- Relay Transmite mesajele dintre clienții DHCP și serverele DHCP din rețele IP diferite.



  - DHCP Server IP Specificați adresa IP a serverului DHCP care va primi mesaje DHCP.
  - Agent-ID Specificați identificatorul agentului *DHCP relay*.

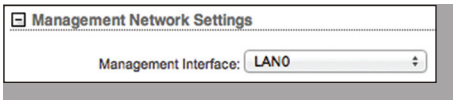
UPnP Permite folosirea UPnP (Universal Plug-and-Play) pentru jocuri, conferințe, chat și alte aplicații.

Add LAN (Available in Advanced view.) Select an interface, and then click Add.

Management Network Settings

Management Interface (Disponibil în vederea *Advanced*)

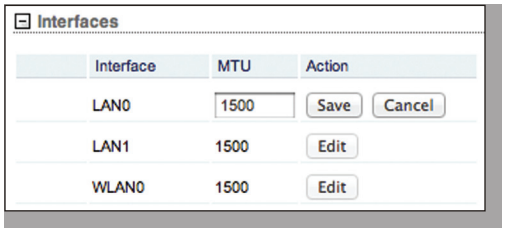
Selectați interfața folosită pentru management.



Interfaces

(Disponibil în vederea *Advanced*) ărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Puteți seta un MTU diferit pentru fiecare interfață

Apăsați butonul **+** pentru a afișa secțiunea *Interfaces.*



Interface Afișează numele interfeței.

MTU Implicit este 1500.

Action Apăsați **Edit** pentru a schimba valoarea MTU. Apoi, apăsați **Save** pentru a salva modificările.

IP Aliases

(Disponibil în vederea *Advanced*) Puteți configura un alias IP pentru interfețele locale și externe în scopul managementului aparatului. De exemplu, puteți avea nevoie de mai multe adrese IP pentru un singur aparat (o adresă privată și una publică). Dacă un CPE folosește PPPoE, acesta obține o adresă publică PPPoE, dar administratorul rețelei atribuie aparatului un alias IP intern. Astfel, administratorul rețelei poate accesa aparatul intern și nu prin intermediul serverului PPPoE.

Apăsați butonul **+** pentru a afișa secțiunea *IP Aliases*.

Enabled Activează un alias IP specific. Toate alias-urile IP adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

IP Address Adresa IP alternativă a interfeței. Aceasta poate fi folosită pentru routare sau pentru administrarea aparatului.

Netmask Masca de rețea pentru alias-ul IP.

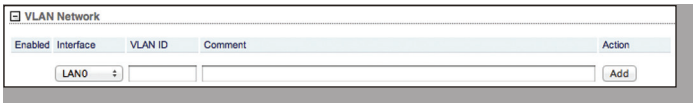
Comment Puteți introduce o scurtă descrierere a alias-ului IP.

Action Aveți următoarele opțiuni:

- Add Adaugă un alias IP.
- Edit Modifică un alias IP. Apăsați **Save** pentru a salva modificările.
- Del Șterge un alias IP.

VLAN Network

(Disponibil în vederea *Advanced*) Puteți creea mai multe rețele virtuale (VLAN). Apăsați butonul **+** pentru a afișa secțiunea *VLAN Network.*



Enabled Activează un VLAN specific. Toate VLAN-urile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

VLAN ID VLAN ID este o valoare unică atribuită fiecărui VLAN de pe aparat. Fiecare VLAN ID reprezintă un VLAN diferit. Poate avea valori între 2 și 4094. Este permis un singur VLAN ID per aparat.

Comment Puteți introduce o scurtă descrierere a VLAN-ului.

Action Aveți următoarele opțiuni:

- Add Adaugă un VLAN.
- Edit Modifică un VLAN. Apăsați **Save** pentru a salva modificările.
- Del Șterge un VLAN.

Bridge Network

(Disponibil în vederea *Advanced*) Puteți creea una sau mai multe bridge-uri dacă aveți nevoie de tranparență completă Layer 2. Este similar folosirii unui switch – tot traficul tranzitează bridge-ul, intră pe un port și iese pe altul, indiferent de adresa IP sau VLAN. De exemplu, dacă vreți să folosiți aceeași sub rețea pe ambele părți ale aparatului, atunci puteți creea un bridge. Sunt multe situații care necesită folosirea unui bridge, deci secțiunea *Bridge Network* oferă flexibilitate.

Apăsați butonul **+** pentru a afișa secțiunea *Bridge Network*.

Enabled Activează un bridge specific. Toate bridge-urile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Interfața este afișată automat.

STP Mai multe bridge-uri interconectate crează o rețea mai mare, care folosește protocolul STP-IEEE 802.1d (Spanning Tree Protocol), care găsește cea mai scurtă cale prin rețea, eliminând buclele din structură.

Dacă este activ, bridge-ul aparatului comunică cu alte aparate din rețea prin protocolul BPDU (Bridge Protocol Data Units). STP ar trebui dezactivat (setare implicită) când dispozitivul este singurul bridge din rețea pe rețea nu există bucle, deoarece setarea STP nu este necesară.

Ports Selectați porturile potrivite pentru crearea bridge-ului (Se pot selecta si porturi virtuale dacă ați creat rețele VLAN).

- Add Selectați un port.
- Del Ștergeți un port.

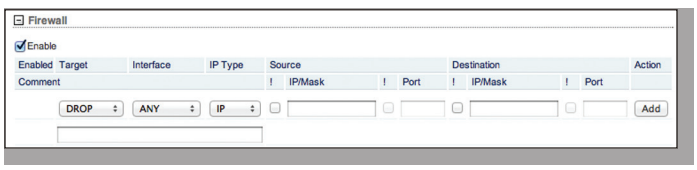
Comment Puteți introduce o scurtă descrierere a bridge-ului.

Action Aveți următoarele opțiuni:

- Add Adaugă un bridge.
- Del Șterge un bridge.

Firewall

(Disponibil în vederea *Advanced*) Puteți configura regulile firewall ale interfeței rețelei locale sau externe. Apăsați butonul **+** pentru a afișa secțiunea Firewall.



Enable Activează firewall-ul.

Enabled Activează o regulă specifică a firewall-ului. Toate regulile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Target Pentru a permite trecerea pachetelor prin firewall, selectați **ACCEPT**. Pentru a bloca pachetele și a nu răspunde, selectați **DROP**.

Interface Selectați interfața potrivită pentru care se aplică regula firewall. Pentru a aplica regula firewall la toate interfețele, selectați **ANY**.

IP Type Specifică ce tip de protocol Layer 3 (IP, ICMP, TCP, UDP) trebuie filtrat.

! Poate fi folosit pentru inversarea criteriilor de filtrare Source IP/Mask, Source Port, Destination IP/Mask, și/sau Destination Port. De exemplu, dacă activați *!* (Not) pentru portul de destinație 443 (folosit de obicei de HTTPS), atunci criteriul de filtrare va fi aplicat pachetelor trimise către toate porturile de destinație, cu excepția portului 443.

Source IP/Mask Bifați căsuța apoi specificați sursa IP a pachetului (aflat în antetul pachetului). De obicei este adresa IP a sistemului care trimite pachetul.
Masca se notează sub forma "/xy". De exemplu, dacă introduceți 192.168.1.0/24, vă referiți la intervalul 192.168.1.0 - 192.168.1.255.

Source Port Bifați căsuța apoi specificați portul sursă a pachetului (aflat în antetul pachetului). De obicei este portul sistemului care trimite pachetul.

Destination IP/Mask Bifați căsuța apoi specificați IP-ul de destinație a pachetului (aflat în antetul pachetului). De obicei este adresa IP a sistemului căruia îi este destinat pachetul. Masca se notează sub forma "/xy". De exemplu, dacă introduceți 192.168.1.0/24, vă referiți la intervalul 192.168.1.0 - 192.168.1.255.

Destination Port Bifați căsuța apoi specificați portul de destinație a pachetului (aflat în antetul pachetului). De obicei este portul sistemului căruia îi este destinat pachetul.

Comment Puteți introduce o scurtă descrierere a regulii firewall-ului.

Toate intrările firewall active sunt stocate în lanțul FIREWALL din tabelul ebtables filter.

Action Aveți următoarele opțiuni:

- Add Adaugă o regulă firewall.
- Edit Modifică o regulă firewall. Apăsați **Save** pentru a salva modificările.
- Del Șterge o regulă firewall.

Static Routes

(Disponibil în vederea *Advanced*) Puteți adăuga manual reguli statice de routare în tabelul de routare; puteți creea o regulă pentru ca o anume adresă IP (interval de adrese IP) să tranziteze către un anume gateway. Apăsați butonul **+** pentru a afișa secțiunea *Static Routes.*

Enabled Activează o rută statică specifică. Toate rutele adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Target Network IP Specificați adresa IP de destinație.

Netmask Specificați masca de rețea de destinație.

Gateway IP Specificați adresa IP a gateway-ului.

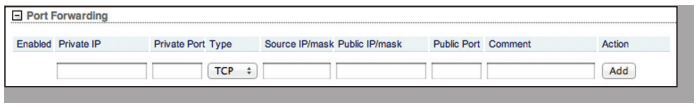
Comment Puteți introduce o scurtă descrierere a rutei statice.

Action Aveți următoarele opțiuni:

- Add Adaugă o rută statică.
- Edit Modifică o rută statică. Apăsați **Save** pentru a salva modificările.
- Del Șterge o rută statică.

Port Forwarding

Port forwarding permite unor porturi specifice ale aparatelor din rețeaua locală să fie transmise către rețeaua externă (WAN). Este folositoare pentru un număr de aplicații (ca servere FTP, VoIP, jocuri), care necesită ca aparatul să fie văzut folosind o adresă IP/port comun. Apăsați butonul **+** pentru a afișa secțiunea *Port Forwarding.*



Enabled Activează o rută de forwarding specifică. Toate rutele adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Private IP Adresa IP a clientului care trebuie să fie accesibil din rețeaua externă.

Private Port Portul TCP sau UDP a aplicației care rulează pe aparatul client. Portul specificat, va fi accesibil din rețeaua externă.

Type Tipul de protocol Layer 3 care trebuie transmis de la rețeaua locală.

Source IP/mask Adresa IP și masca de rețea a aparatului sursă.

Public IP/mask Adresa IP și masca de rețea a aparatului care va accepta și transmite conexiunile de la rețeaua externă către client.

Public Port Portul TCP sau UDP al aparatului care va accepta și transmite conexiunile de la rețeaua externă către client.

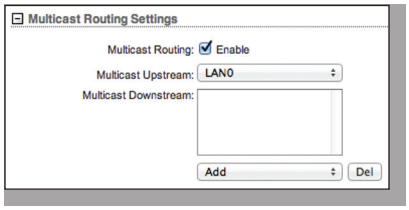
Comment Puteți introduce o scurtă descrierere a regulii de forwarding.

Action Aveți următoarele opțiuni:

- Add Adaugă o regulă de port forwarding.
- Edit Modifică o regulă de port forwarding. Apăsați **Save** pentru a salva modificările.
- Del Șterge o regulă de port forwarding.

Multicast Routing Settings

Cu un design multicast, aplicațiile pot trimite o singură copie a unui pachet, adresată unui grup de calculatoare care vor sa îl primească. Această tehnică adresează pachetele unui grup de receptori, în locul unui singur receptor. Se bazează pe rețea pentru a trimite pachetele calculatoarelor care trebuie să le recepționeze. Ruterele tradiționale izolează tot traficul broadcast (și cel multicast) între rețeaua locală și cea externă; totuși, aparatul oferă opțiunea trecerii pachetelor *multicast*.



Multicast Routing Permite trecerea pachetelor multicast între rețeaua locală și externă, în timp ce aparatul funcționează în modul *Router*. Comunicarea multicast se bazează pe protocolul IGMP (Internet Group Management Protocol).

Multicast Upstream Specifică sursa traficului multicast.

Multicast Downstream Specifică destinația (destinațiile) traficului multicast.

Add Adaugați o destinație.

Del Ștergeți o destinație.

Traffic Shaping

(Disponibil în vederea *Advanced*) Traffic Shaping controlează lățimea de bandă din perspectiva clientului (care este conectat la interfața Ethernet). Facilitatea Bursting oferă viteze mari de descărcare atunci când utilizatorul descarcă fișiere mici (de exemplu, vizionarea unui pagini web), dar previne utilizatorul să folosească excesiv lățime de bandă atunci când descarcă fișiere mari (de exemplu, vizualizează un film).

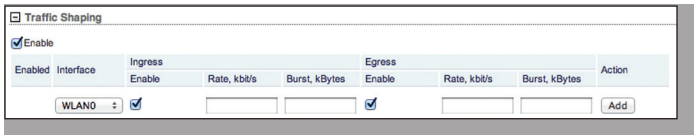
Ca la Layer 3 QoS, puteți limita traficul unui aparat la nivel de port în funcție de rata maximă pe care o definiți. Fiecare port are două tipuri de trafic:

- Ingress traficul care intră în port
- Egress traficul care iese din port

Vă recomandăm sa folosiți Traffic Shaping pentru controlarea traficului egress, deoarece este mai eficient în direcția egress. Atunci când un port acceptă trafic ingress, nu poate controla cât de repede ajunge traficul – când transmite, aparatul poate controla traficul. Totuși, când portul transmite trafic egress, poate controla viteza de transmisie.

Funcția Bursting permite creșterea ratei de transfer peste valoarea maximă configurată în câmpurile *Ingress Rate* și *Egress Rate* – pentru o scurtă perioadă de timp. După folosirea rației Ingress sau Egress Burst (volum de date), rata de transfer scade la valorile pe care le-ați setat în câmpurile *Ingress Rate* sau *Egress Rate* (maximum bandwidth).

De exemplu, dacă folosiți următoarele setări:
- Ingress Burst este 2048 kBytes.
- Ingress Rate este 512 kbit/s.
- Rata de transfer reală este 1024 kbit/s. Bursting permite trecerea a 2048 kBytes cu rata de 1024 kbit/s, înainte de a o limita la 512 kbit/s.



Enable Activează controlul ratei de transfer pe aparat.
Enabled Activează o regulă specifică. Toate regulile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

Ingress

- Enable Activează valoarea ingress.
- Rate, kbit/s Specificați valoarea ratei de transfer maxime (în kilobits pe secundă) pentru traficul dinspre interfața wireless spre interfața Ethernet.
- Burst, kBytes Specificați volumul de date (în kilobytes) permis înainte ca valoarea ingress să fie limitată la valoarea maximă setată.

Egress

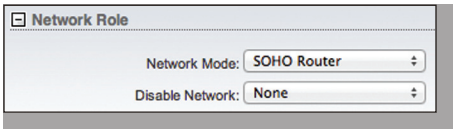
- Enable Activează valoarea egress.
- Rate, kbit/s Specificați valoarea ratei de transfer maxime (în kilobits pe secundă) pentru traficul dinspre interfața Ethernet spre interfața wireless.
- Burst, kBytes Specificați volumul de date (în kilobytes) permis înainte ca valoarea egress să fie limitată la valoarea maximă setată.

Action Aveți următoarele opțiuni:

- Add Adaugă o regulă.
- Edit Modifică o regulă. Apăsați **Save** pentru a salva modificările.
- Del Șterge o regulă.

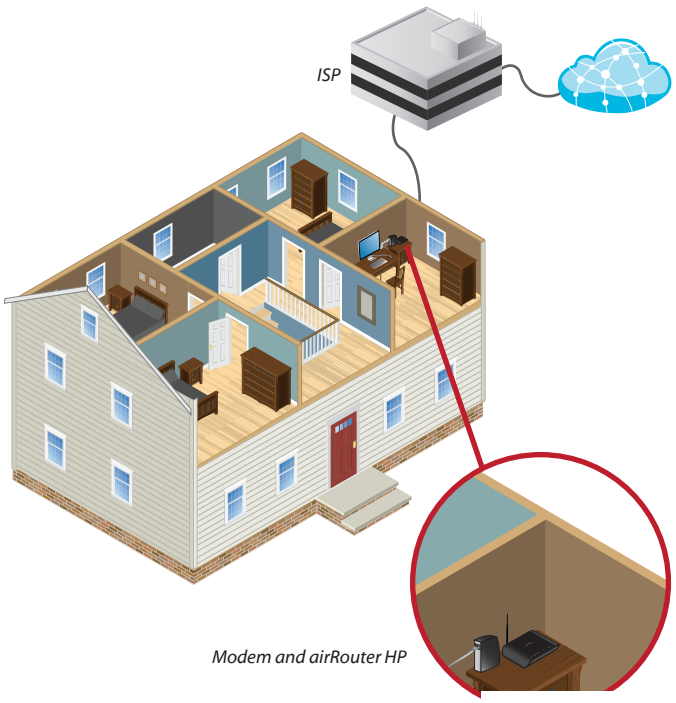
SOHO Router

În modul *SOHO Router*, aparatul operează în Layer 3 pentru efectuarea rutării și se activează segmentarea de rețea – clienții wireless sunt pe o subrețea diferită. Modul *SOHO Router* blochează traficul broadcast și poate trece prin traficul multicast. Puteți configura reguli firewall suplimentare pentru filtrarea pachetelor Layer 3 și pentru controlul accesului.



Aparatul poate funcționa ca server DHCP și poate folosi NAT (Network Address Translation - Masquerading), care este des folosit de AP-uri. NAT-ul se comportă ca un firewall între LAN și WAN.

În modul *SOHO Router*, portul Ethernet principal marcat cu <···> funcționează ca port WAN. Interfața WLAN și alte porturi Ethernet funcționează ca LAN. Fiecare interfață wireless sau cu fir de pe WAN or LAN are o adresă IP. De exemplu, următoarea imagine arată aparatul airRouter HP conectat la un modem, care este conectat la ISP.



Modem and airRouter HP

Modul *SOHO Router* funcționează corect numai în modul wireless *Access Point* sau *AP-Repeater*, deoarece nu a fost proiectat pentru a se comporta ca și client wireless.

La aparatele cu un singur port Ethernet (În timp ce funcționează ca *Access Point* sau *AP-Repeater*), modul *SOHO Router* funcționează ca modul *Router*, cu excepția că portul LAN funcționează ca port WAN și WLAN ca rețea locală.

Notă: Nu folosiți modul *SOHO Router* în combinație cu modul *wireless Station*; aparatul poate deveni inaccesibil. Dacă se întâmplă acest lucru, resetați aparatul la setările implicite; țineți apăsat butonul **Reset** timp de 8 secunde apoi eliberați-l.

Configuration Mode

TMeniul Network dispune de două moduri de vizualizare:

Simple și Advanced.

Simple Afișează setările de bază de configurare: •

"**WAN Network Settings**" pagina 39

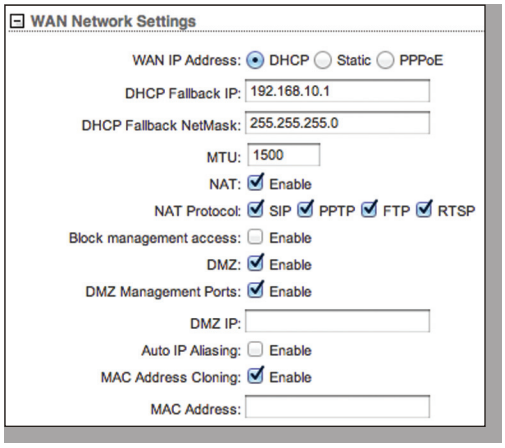
- "**LAN Network Settings**" pagina 42
- "**Port Forwarding**" pagina 45
- "**Multicast Routing Settings**" pagina 46

Setările avansate sunt ascunse.

Advanced Afișează setările avansate de configurare:

- "**Management Network Settings**" pagina 43
- "**Interfaces**" pagina 43
- "**IP Aliases**" pagina 43
- "**VLAN Network**" pagina 43
- "**Bridge Network**" pagina 44
- "**Firewall**" pagina 44
- "**Static Routes**" pagina 45
- "**Traffic Shaping**" pagina 46

WAN Network Settings



WAN Interface (Disponibil în vederea *Advanced*) Selectați interfața folosită pentru management.

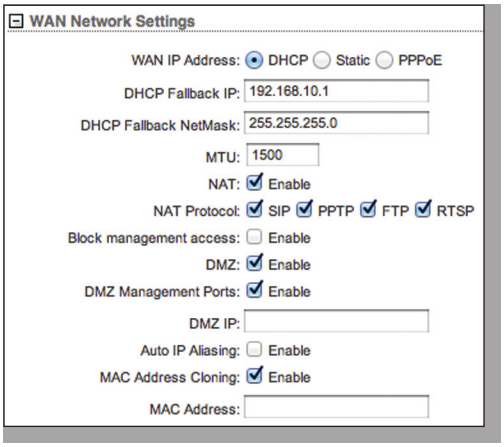
WAN IP Address Adresa IP a interfeței WAN este conectată la rețeaua externă. Puteți folosi această adresă IP pentru rutare sau pentru managementul aparatului.

Aparatul poate folosi următoarele:

- "**DHCP**" pagina 39
- "**Static**" pagina 40
- "**PPPoE**" pagina 41

DHCP

Serverul DHCP extern atribuie aparatului adrese IP dinamice, adrese IP gateway și adrese DNS.



DHCP Fallback IP Specifați o adresă IP pentru aparat pentru când nu se găsește server DHCP.

DHCP Fallback Netmask Specifați o mască de rețea pentru aparat pentru când nu se găsește server DHCP.

MTU (Disponibil în vederea *Simple*) Mărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Implicit este 1500.

NAT NAT-ul (Network Address Translation) permite expedierea pachetelor de la rețeaua externă (WAN) către adresa IP a interfeței locale și apoi subrutarea către un alt aparat client pe rețeaua locală, în timp ce aparatul airOS funcționează în modul *Access Point* sau *AP-Repeater*. Pachetele sunt rutate în direcția opusă față de modul *Station*.

NAT este implementat folosind reguli firewall de tip masquerade. Intrările NAT firewall sunt stocate în tabelul nat al iptables. Specificați rute statice pentru a permite pachetelor să traversese aparatul când NAT este dezactivat.

- NAT Protocol Dacă NAT este activ, puteți modifica pachetele de date pentru a le permite trecerea prin aparat. Pentru a evita modificarea unor pachete specifice ca: SIP, PPTP, FTP sau RTSP, debifați căsuțele respective.

Block management access Bifați căsuța pentru a bloca managementul aparatului dinspre interfața WAN. Această facilitate crește securitatea în modul *Router* dacă aparatul are o adresă IP publică.

DMZ DMZ (Demilitarized Zone) permite unui calculator/ aparat din spatele NAT-ului să devină “demilitarizat”, pentru ca toate porturile din rețeaua publică să fie transmise către porturi din această rețea privată, similar cu NAT 1:1.

- DMZ Management Ports Portul de management Web, (implicit portul TCP/IP 80) al aparatului airOS va fi folosit pentru acesta. Aparatul airOS va răspunde cererilor din rețeaua externă ca și când ar fi aparatul specificat ca DMZ. Dacă opțiunea *DMZ Management Ports* este activă, toate porturile vor fi transmise către aparatul DMZ, deciveți putea accesa aparatul doar dispre LAN.

• DMZ IP Specificați adresa IP a aparatului DMZ. Aparatul DMZ va fi complet expus la rețeaua externă.

Auto IP Aliasing Dacă este activat, va genera automat o adresă IP corespunzătoare interfeței WLAN/LAN. Adresa IP generată este o adresă unică de clasă B din intervalul 169.254.X.Y (netmask 255.255.0.0), destinată folosirii în același segment de rețea. IP-ul generată începe întotdeauna cu 169.254.X.Y, unde X și Y sunt ultimii doi octeți din adresa MAC a aparatului. De exemplu, dacă adresa MAC este 00:15:6D:A3:04:FB, atunci adresa generată va fi 169.254.4.251.

Setarea *Auto IP Aliasing* este folosită deoarece puteți accesa și configura aparatul chiar dacă pierdeți, configurați greșit sau uitați adresa IP a acestuia. Puteți determina adresa IP a aparatului dacă cunoașteți adresa MAC, deoarece adresa generată se bazează pe ultimii doi octeți a adresei MAC.

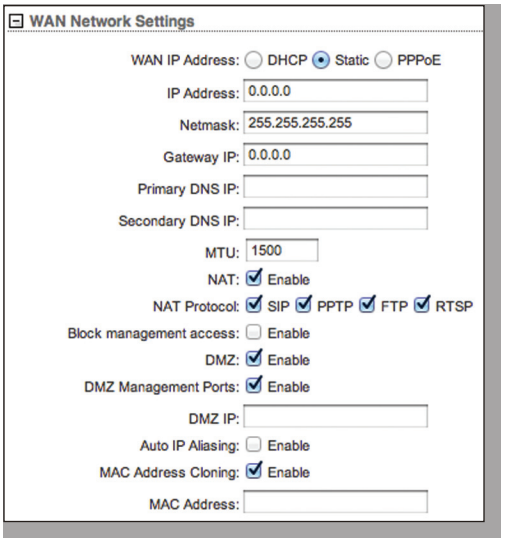
MAC Address Cloning Când este activă, vă permite să schimbați adresa MAC a respectivei interfețe. Opțiunea este folositoare atunci când ISP-ul asociază adresa IP cu o adresă MAC specifică. Această metodă este folosită în special de operatorii prin cablu sau unii operatori WISP.

- MAC Address Introduceți adresa MAC pentru interfața respectivă. Acesta devine noul MAC al interfeței.

Static

Specificați o adresă IP statică pentru aparat.

Notă: Setările IP trebuie să fie corespunzătoare segmentului de rețea din care aparatul face parte.



IP Address Specifați adresa IP a aparatului. IP-ul va fi folosit în scopul configurării aparatului.

Netmask Masca de rețea în formă binară furnizează informații pentru definirea unui interval de adrese IP folosit de aparatele din rețea. Masca de rețea definește segmentul de rețea al aparatului. Masca 255.255.255.0 (sau “/24”) este folosită de obicei în cazul rețelelor IP de clasă C.

Gateway IP De obicei, este o adresă IP a router-ului care furnizează conexiunea la internet. Acesta poate fi un modem DSL, modem de cablu sau router WISP. Aparatul treimite pachetele care nu sunt destinate rețelei locale către gateway.

Primary DNS IP Specifați adresa IP a serverului DNS (Domain Name System) principal.

Secondary DNS IP Specifați adresa IP a serverului DNS (Domain Name System) secundar. Acest câmp este opțional și este folosit numai dacă serverul DNS principal nu răspunde.

MTU (Disponibil în vederea *Simple*) Mărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Implicit este 1500.

NAT NAT-ul (Network Address Translation) permite expedierea pachetelor de la rețeaua externă (WAN) către adresa IP a interfeței locale și apoi subrutarea către un alt aparat client pe rețeaua locală, în timp ce aparatul airOS funcționează în modul *Access Point* sau *AP-Repeater*.

NAT este implementat folosind reguli firewall de tip masquerade. Intrările NAT firewall sunt stocate în tabelul nat al iptables. Specificați rute statice pentru a permite pachetelor să traversese aparatul când NAT este dezactivat.

- NAT Protocol Dacă NAT este activ, puteți modifica pachetele de date pentru a le permite trecerea prin aparat. Pentru a evita modificarea unor pachete specifice ca: SIP, PPTP, FTP sau RTSP, debifați căsuțele respective.

Block management access Bifați căsuța pentru a bloca managementul aparatului dinspre interfața WAN. Această facilitate crește securitatea în modul *Router* dacă aparatul are o adresă IP publică.

DMZ DMZ (Demilitarized Zone) permite unui calculator/aparat din spatele NAT-ului să devină "demilitarizat", pentru ca toate porturile din rețeaua publică să fie transmise către porturi din această rețea privată, similar cu NAT 1:1.

- DMZ Management Ports Portul de management Web, (implicit portul TCP/IP 80) al aparatului airOS va fi folosit pentru acesta. Aparatul airOS va răspunde cererilor din rețeaua externă ca și când ar fi aparatul specificat ca DMZ. Dacă opțiunea *DMZ Management Ports* este activă, toate porturile vor fi transmise către aparatul DMZ, deciveți putea accesa aparatul doar dispre LAN.

• DMZ IP Specificați adresa IP a aparatului DMZ. Aparatul DMZ va fi complet expus la rețeaua externă.

Auto IP Aliasing Dacă este activat, va genera automat o adresă IP corespunzătoare interfeței WLAN/LAN. Adresa IP generată este o adresă unică de clasă B din intervalul 169.254.X.Y (netmask 255.255.0.0), destinată folosirii în același segment de rețea. IP-ul generată începe întotdeauna cu 169.254.X.Y, unde X și Y sunt ultimii doi octeți din adresa MAC a aparatului. De exemplu, dacă adresa MAC este 00:15:6D:A3:04:FB, atunci adresa generată va fi 169.254.4.251.

Setarea *Auto IP Aliasing* este folosită deoarece puteți accesa și configura aparatul chiar dacă pierdeți, configurați greșit sau uitați adresa IP a acestuia. Puteți determina adresa IP a aparatului dacă cunoașteți adresa MAC, deoarece adresa generată se bazează pe ultimii doi octeți a adresei MAC.

MAC Address Cloning Când este activă, vă permite să schimbați adresa MAC a respectivei interfețe. Opțiunea este folositoare atunci când ISP-ul asociază adresa IP cu o adresă MAC specifică. Această metodă este folosită în special de operatorii prin cablu sau unii operatori WISP.

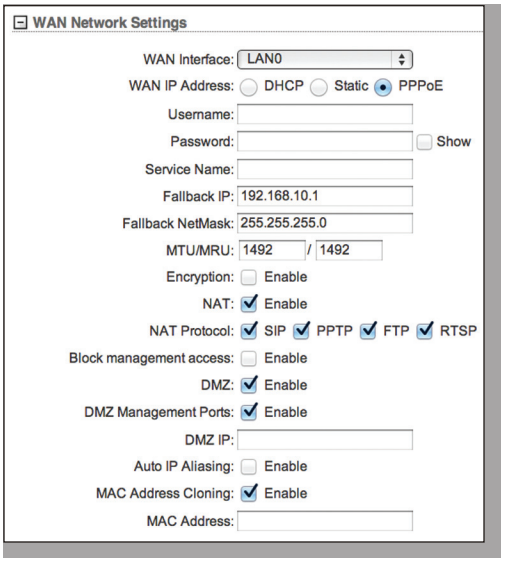
- MAC Address Introduceți adresa MAC pentru interfața respectivă. Acesta devine noul MAC al interfeței.

PPPoE

Protocolul PPPoE (Point-to-Point Protocol over Ethernet) este o conexiune sigură și privată, între două sisteme, care permite încapsularea datelor transportat. Clienții uneori folosesc PPPoE pentru conectarea la ISP (Internet Service Providers), în special la furnizorii DSL.

Selectați **PPPoE** pentru a configura un tunel PPPoE. Puteți configura o singură interfață externă de rețea, deoarece ca și client PPPoE va fi trimis prin acest tunel. După realizarea conexiunii PPPoE, aparatul va primi de la serverul PPPoE adresa IP, adresa Gateway și adresa serverului DNS. Adresa broadcast este folosită pentru descoperirea serverului PPPoE și realizarea tunelului.

Dacă există o conexiune PPPoE activă, atunci adresa interfeței PPP va fi afișată în meniul *Main* lângă statisticile interfeței PPP; altfel va fi afișat mesajul *Not Connected* și va fi activ butonul *Reconnect*. Pentru a reconecta tunelul PPPoE, apăsați **Reconnect**.



Username Specifați numele de utilizator pentru conectarea la serverul PPPoE; trebuie să fie identic cu cel configurat pe serverul PPPoE.

Password Specifați parola pentru conectarea la serverul PPPoE; trebuie să fie identică cu cea configurată pe serverul PPPoE.

Show Bifați căsuța pentru a vedea caracterele parolei.

Service Name Specificați numele serviciului PPPoE.

Fallback IP Specifați o adresă IP pentru aparat pentru când nu se găsește server DHCP.

DHCP Fallback Netmask Specifați o mască de rețea pentru aparat pentru când nu se găsește server DHCP.

MTU/MRU Mărimea (în bytes) pachetelor MTU (Maximum Transmission Unit) și MRU (Maximum Receive Unit) folosite pentru încapsularea datelor în timpul transferului prin tunel. Valoarea implicită este 1492.

Encryption Activează criptarea Microsoft Punct la Punct (Microsoft Point-to-Point Encryption - MPPE).

NAT NAT-ul (Network Address Translation) permite expedierea pachetelor de la rețeaua externă (WAN) către adresa IP a interfeței locale și apoi subrutarea către un alt aparat client pe rețeaua locală, în timp ce aparatul airOS funcționează în modul *Access Point* sau *AP-Repeater*. Pachetele sunt rutate în direcția opusă față de modul *Station*.

NAT este implementat folosind reguli firewall de tip masquerade. Intrările NAT firewall sunt stocate în tabelul nat al iptables. Specificați rute statice pentru a permite pachetelor să traverseze aparatul când NAT este dezactivat.

- NAT Protocol Dacă NAT este activ, puteți modifica pachetele de date pentru a le permite trecerea prin aparat. Pentru a evita modificarea unor pachete specifice ca: SIP, PPTP, FTP sau RTSP, debifați căsuțele respective.

Block management access Bifați căsuța pentru a bloca managementul aparatului dinspre interfața WAN. Această facilitate crește securitatea în modul *Router* dacă aparatul are o adresă IP publică.

DMZ DMZ (Demilitarized Zone) permite unui calculator/aparat din spatele NAT-ului să devină "demilitarizat", pentru ca toate porturile din rețeaua publică să fie transmise către porturi din această rețea privată, similar cu NAT 1:1.

- DMZ Management Ports Portul de management Web, (implicit portul TCP/IP 80) al aparatului airOS va fi folosit pentru acesta. Aparatul airOS va răspunde cererilor din rețeaua externă ca și când ar fi aparatul specificat ca DMZ. Dacă opțiunea *DMZ Management Ports* este activă, toate porturile vor fi transmise către aparatul DMZ, deciveți putea accesa aparatul doar dispre LAN.

• DMZ IP Specificați adresa IP a aparatului DMZ. Aparatul DMZ va fi complet expus la rețeaua externă.

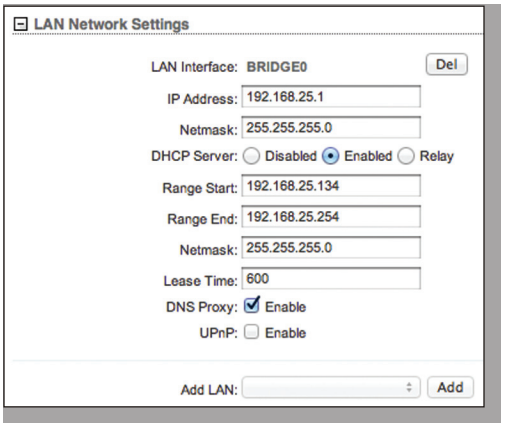
Auto IP Aliasing Dacă este activat, va genera automat o adresă IP corespunzătoare interfeței WLAN/LAN. Adresa IP generată este o adresă unică de clasă B din intervalul 169.254.X.Y (netmask 255.255.0.0), destinată folosirii în același segment de rețea. IP-ul generată începe întotdeauna cu 169.254.X.Y, unde X și Y sunt ultimii doi octeți din adresa MAC a aparatului. De exemplu, dacă adresa MAC este 00:15:6D:A3:04:FB, atunci adresa generată va fi 169.254.4.251.

Setarea *Auto IP Aliasing* este folosită deoarece puteți accesa și configura aparatul chiar dacă pierdeți, configurați greșit sau uitați adresa IP a acestuia. Puteți determina adresa IP a aparatului dacă cunoașteți adresa MAC, deoarece adresa generată se bazează pe ultimii doi octeți a adresei MAC.

MAC Address Cloning Când este activă, vă permite să schimbați adresa MAC a respectivei interfețe. Opțiunea este folositoare atunci când ISP-ul asociază adresa IP cu o adresă MAC specifică. Această metodă este folosită în special de operatorii prin cablu sau unii operatori WISP.

- MAC Address Introduceți adresa MAC pentru interfața respectivă. Acesta devine noul MAC al interfeței.

LAN Network Settings



LAN Interface Interfața este afișată. Apăsați **Del** pentru a șterge interfața. Dacă nu există nici o interfață selectată, selectați una din lista *Add LAN* și apăsați **Add**.

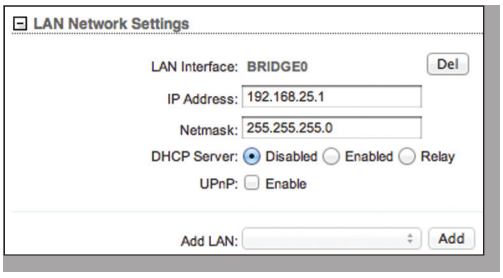
IP Address Adresa IP a interfeței LAN (inclusiv WLAN) conectată la rețeaua locală. Acest IP va fi folosit pentru rutarea rețelei locale; va fi IP-ul gateway pentru toate aparatele din rețeaua locală. Acest IP este folosit pentru managementul aparatului.

Netmask Definește clasa IP pentru intervalul IP ales. 255.255.255.0 este clasa de rețea obișnuită pentru rețelele de clasă C, care suportă intervalul de adrese IP de la 192.0.0.x până la 223.255.255.x. Masca unei rețele în clasă C, folosește 24 biți pentru identificarea rețelei (notare alternativă "/24") și 8 biți pentru identificarea unui aparat.

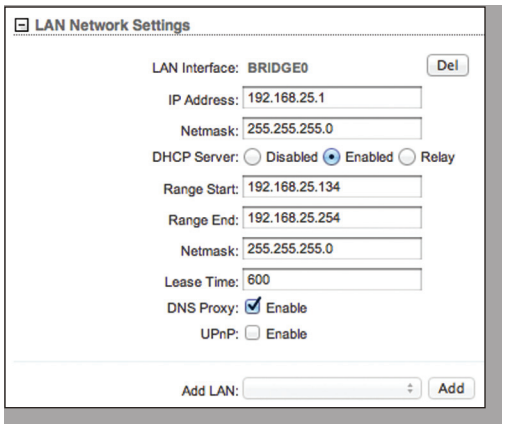
MTU (Disponibil în vederea *Simple*) Mărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Implicit este 1500.

DHCP Server Serverul DHCP integrat, atribuie adrese IP clienților conectați la interfața wireless și la interfața LAN când funcționează în modul *Access Point* sau *AP-Repeater*. Serverul DHCP integrat, atribuie adrese IP clienților conectați la interfața LAN când funcționează în modul *Station*.

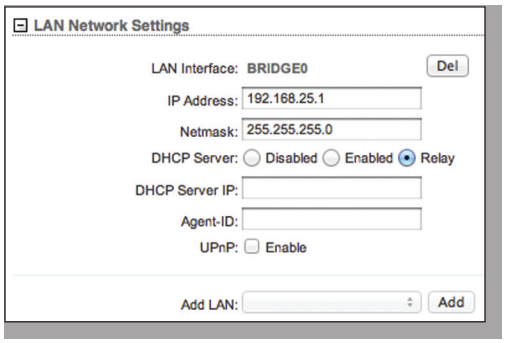
- Disabled Aparatul nu atribuie adrese IP.



- Enabled Aparatul atribuie adrese IP clienților din rețeaua locală.



- Range Start and End Determină intervalul de adrese IP atribuite de serverul DHCP.
- Netmask Definește clasa IP pentru intervalul IP ales. 255.255.255.0 este clasa de rețea obișnuită pentru rețelele de clasă C, care suportă intervalul de adrese IP de la 192.0.0.x până la 223.255.255.x. Masca unei rețele în clasă C, folosește 24 biți pentru identificarea rețelei (notare alternativă "/24") și 8 biți pentru identificarea unui aparat.
- Lease Time Adresele IP atribuite de serverul DHCP sunt valide o durată specifică de timp (lease time). Creșterea perioadei asigură o operare a clientului neîntreruptă, dar poate creea conflicte. Scăderea timpului evită potențialele conflicte de adresă, dar poate cauza mai multe întreruperi pentru client în timpul obținerii unei noi adrese IP de la serverul DHCP. Timpul este exprimat în secunde.
  - DNS Proxy Serverul DNS (Domain Name System) proxy, transmite cererile DNS de la clienții din rețeaua locală către serverul DNS.
  - Primary DNS IP Specifați adresa IP a serverului DNS (Domain Name System) principal.
  - Secondary DNS IP Specifați adresa IP a serverului DNS (Domain Name System) secundar. Acest câmp este opțional și este folosit numai dacă serverul DNS principal nu răspunde.
- Relay Transmite mesajele dintre clienții DHCP și serverele DHCP din rețele IP diferite.



  - DHCP Server IP Specificați adresa IP a serverului DHCP care va primi mesaje DHCP.
  - Agent-ID Specificați identificatorul agentului *DHCP relay*.

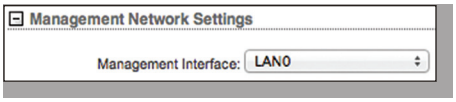
UPnP Permite folosirea UPnP (Universal Plug-and-Play) pentru jocuri, conferințe, chat și alte aplicații.

Add LAN (Available in Advanced view.) Select an interface, and then click Add.

Management Network Settings

Management Interface (Disponibil în vederea *Advanced*)

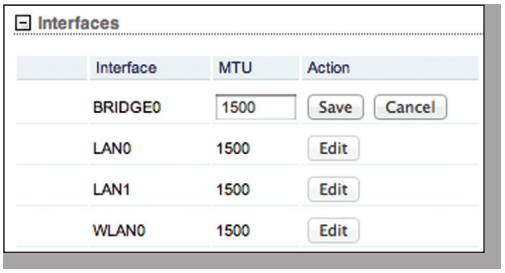
Selectați interfața folosită pentru management.



Interfaces

(Disponibil în vederea *Advanced*) ărimea maximă a pachetului MTU (Maximum Transmission Unit), în bytes, care se poate transmite în rețea. Puteți seta un MTU diferit pentru fiecare interfață

Apăsați butonul **+** pentru a afișa secțiunea *Interfaces*.



Interface Afișează numele interfeței.

MTU Implicit este 1500.

Action Apăsați **Edit** pentru a schimba valoarea MTU. Apoi, apăsați **Save** pentru a salva modificările.

IP Aliases

(Disponibil în vederea *Advanced*) Puteți configura un alias IP pentru interfețele locale și externe în scopul managementului aparatului. De exemplu, puteți avea nevoie de mai multe adrese IP pentru un singur aparat (o adresă privată și una publică). Dacă un CPE folosește PPPoE, acesta obține o adresă publică PPPoE, dar administratorul rețelei atribuie aparatului un alias IP intern. Astfel, administratorul rețelei poate accesa aparatul intern și nu prin intermediul serverului PPPoE.

Apăsați butonul **+** pentru a afișa secțiunea *IP Aliases*.

Enabled Activează un alias IP specific. Toate alias-urile IP adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

IP Address Adresa IP alternativă a interfeței. Aceasta poate fi folosită pentru routare sau pentru administrarea aparatului.

Netmask Masca de rețea pentru alias-ul IP.

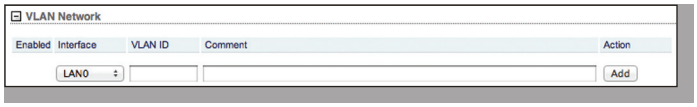
Comment Puteți introduce o scurtă descrierere a alias-ului IP.

Action Aveți următoarele opțiuni:

- Add Adaugă un alias IP.
- Edit Modifică un alias IP. Apăsați **Save** pentru a salva modificările.
- Del Șterge un alias IP.

VLAN Network

(Disponibil în vederea *Advanced*) Puteți creea mai multe rețele virtuale (VLAN). Apăsați butonul **+** pentru a afișa secțiunea *VLAN Network.*



Enabled Activează un VLAN specific. Toate VLAN-urile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

VLAN ID VLAN ID este o valoare unică atribuită fiecărui VLAN de pe aparat. Fiecare VLAN ID reprezintă un VLAN diferit. Poate avea valori între 2 și 4094. Este permis un singur VLAN ID per aparat.

Comment Puteți introduce o scurtă descrierere a VLAN-ului.

Action Aveți următoarele opțiuni:

- Add Adaugă un VLAN.
- Edit Modifică un VLAN. Apăsați **Save** pentru a salva modificările.
- Del Șterge un VLAN.

Bridge Network

(Disponibil în vederea *Advanced*) Puteți creea una sau mai multe bridge-uri dacă aveți nevoie de tranparență completă Layer 2. Este similar folosirii unui switch – tot traficul tranzitează bridge-ul, intră pe un port și iese pe altul, indiferent de adresa IP sau VLAN. De exemplu, dacă vreți să folosiți aceeași sub rețea pe ambele părți ale aparatului, atunci puteți creea un bridge. Sunt multe situații care necesită folosirea unui bridge, deci secțiunea *Bridge Network* oferă flexibilitate.

Apăsați butonul **+** pentru a afișa secțiunea *Bridge Network*.

Enabled Activează un bridge specific. Toate bridge-urile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Interfața este afișată automat.

STP Mai multe bridge-uri interconectate crează o rețea mai mare, care folosește protocolul STP-IEEE 802.1d (Spanning Tree Protocol), care găsește cea mai scurtă cale prin rețea, eliminând buclele din structură.

Dacă este activ, bridge-ul aparatului comunică cu alte aparate din rețea prin protocolul BPDU (Bridge Protocol Data Units). STP ar trebui dezactivat (setare implicită) când dispozitivul este singurul bridge din rețea pe rețea nu există bucle, deoarece setarea STP nu este necesară.

Ports Selectați porturile potrivite pentru crearea bridge-ului (Se pot selecta si porturi virtuale dacă ați creat rețele VLAN).

- Add Selectați un port.
- Del Ștergeți un port.

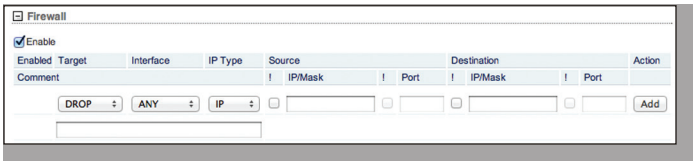
Comment Puteți introduce o scurtă descrierere a bridge-ului.

Action Aveți următoarele opțiuni:

- Add Adaugă un bridge.
- Del Șterge un bridge.

Firewall

(Disponibil în vederea *Advanced*) Puteți configura regulile firewall ale interfeței rețelei locale sau externe. Apăsați butonul **+** pentru a afișa secțiunea Firewall.



Enable Activează firewall-ul.

Enabled Activează o regulă specifică a firewall-ului. Toate regulile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Target Pentru a permite trecerea pachetelor prin firewall, selectați **ACCEPT**. Pentru a bloca pachetele și a nu răspunde, selectați **DROP**.

Interface Selectați interfața potrivită pentru care se aplică regula firewall. Pentru a aplica regula firewall la toate interfețele, selectați **ANY**.

IP Type Specifică ce tip de protocol Layer 3 (IP, ICMP, TCP, UDP) trebuie filtrat.

! Poate fi folosit pentru inversarea criteriilor de filtrare Source IP/Mask, Source Port, Destination IP/Mask, și/sau Destination Port. De exemplu, dacă activați *!* (Not) pentru portul de destinație 443 (folosit de obicei de HTTPS), atunci criteriul de filtrare va fi aplicat pachetelor trimise către toate porturile de destinație, cu excepția portului 443.

Source IP/Mask Bifați căsuța apoi specificați sursa IP a pachetului (aflat în antetul pachetului). De obicei este adresa IP a sistemului care trimite pachetul.
Masca se notează sub forma "/xy". De exemplu, dacă introduceți 192.168.1.0/24, vă referiți la intervalul 192.168.1.0 - 192.168.1.255.

Source Port Bifați căsuța apoi specificați portul sursă a pachetului (aflat în antetul pachetului). De obicei este portul sistemului care trimite pachetul.

Destination IP/Mask Bifați căsuța apoi specificați IP-ul de destinație a pachetului (aflat în antetul pachetului). De obicei este adresa IP a sistemului căruia îi este destinat pachetul. Masca se notează sub forma "/xy". De exemplu, dacă introduceți 192.168.1.0/24, vă referiți la intervalul 192.168.1.0 - 192.168.1.255.
Destination Port Bifați căsuța apoi specificați portul de destinație a pachetului (aflat în antetul pachetului). De obicei este portul sistemului căruia îi este destinat pachetul.

Comment Puteți introduce o scurtă descriere a regulii firewall-ului.

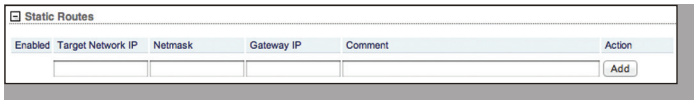
Toate intrările firewall active sunt stocate în lanțul FIREWALL din tabelul ebtables filter.

Action Aveți următoarele opțiuni:

- Add Adaugă o regulă firewall.
- Edit Modifică o regulă firewall. Apăsați **Save** pentru a salva modificările.
- Del Șterge o regulă firewall.

Static Routes

(Disponibil în vederea *Advanced*) Puteți adăuga manual reguli statice de routare în tabelul de routare; puteți creea o regulă pentru ca o anume adresă IP (interval de adrese IP) să tranziteze către un anume gateway. Apăsați butonul **+** pentru a afișa secțiunea *Static Routes*.



Enabled Activează o rută statică specifică. Toate rutele adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Target Network IP Specificați adresa IP de destinație.

Netmask Specificați masca de rețea de destinație.

Gateway IP Specificați adresa IP a gateway-ului.

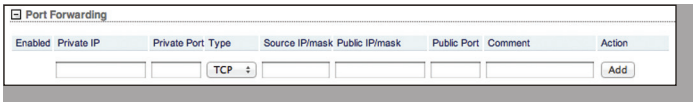
Comment Puteți introduce o scurtă descriere a rutei statice.

Action Aveți următoarele opțiuni:

- Add Adaugă o rută statică.
- Edit Modifică o rută statică. Apăsați **Save** pentru a salva modificările.
- Del Șterge o rută statică.

Port Forwarding

Port forwarding permite unor porturi specifice ale aparatelor din rețeaua locală să fie transmise către rețeaua externă (WAN). Este folositoare pentru un număr de aplicații (ca servere FTP, VoIP, jocuri), care necesită ca aparatul să fie văzut folosind o adresă IP/ port comun. Apăsați butonul **+** pentru a afișa secțiunea *Port Forwarding*.



Enabled Activează o rută de forwarding specifică. Toate rutele adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Private IP Adresa IP a clientului care trebuie să fie accesibil din rețeaua externă.

Private Port Portul TCP sau UDP a aplicației care rulează pe aparatul client. Portul specificat, va fi accesibil din rețeaua externă.

Type Tipul de protocol Layer 3 care trebuie transmis de la rețeaua locală.

Source IP/mask Adresa IP și masca de rețea a aparatului sursă.
Public IP/mask Adresa IP și masca de rețea a aparatului care va accepta și transmite conexiunile de la rețeaua externă către client.

Public Port Portul TCP sau UDP al aparatului care va accepta și transmite conexiunile de la rețeaua externă către client.

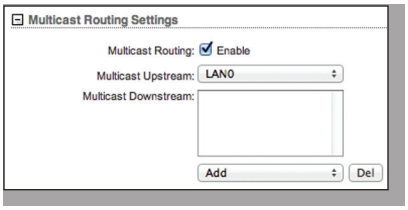
Comment Puteți introduce o scurtă descriere a regulii de forwarding.

Action Aveți următoarele opțiuni:

- Add Adaugă o regulă de port forwarding.
- Edit Modifică o regulă de port forwarding. Apăsați **Save** pentru a salva modificările.
- Del Șterge o regulă de port forwarding.

Multicast Routing Settings

Cu un design multicast, aplicațiile pot trimite o singură copie a unui pachet, adresată unui grup de calculatoare care vor sa îl primească. Această tehnică adresează pachetele unui grup de receptori, în locul unui singur receptor. Se bazează pe rețea pentru a trimite pachetele calculatoarelor care trebuie să le recepționeze. Ruterele tradiționale izolează tot traficul broadcast (și cel multicast) între rețeaua locală și cea externă; totuși, aparatul oferă opțiunea trecerii pachetelor *multicast*.



Multicast Routing Permite trecerea pachetelor multicast între rețeaua locală și externă, în timp ce aparatul funcționează în modul *Router*. Comunicarea multicast se bazează pe protocolul IGMP (Internet Group Management Protocol).

Multicast Upstream Specifică sursa traficului multicast.

Multicast Downstream Specifică destinația (destinațiile) traficului multicast.

Add Adaugați o destinație.

Del Ștergeți o destinație.

Traffic Shaping

(Disponibil în vederea *Advanced*) Traffic Shaping controlează lățimea de bandă din perspectiva clientului (care este conectat la interfața Ethernet). Facilitatea Bursting oferă viteze mari de descărcare atunci când utilizatorul descarcă fișiere mici (de exemplu, vizionarea unui pagini web), dar previne utilizatorul să folosească excesiv lățime de bandă atunci când descarcă fișiere mari (de exemplu, vizualizează un film).

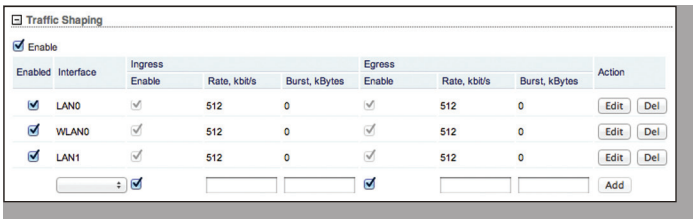
Ca la Layer 3 QoS, puteți limita traficul unui aparat la nivel de port în funcție de rata maximă pe care o definiți. Fiecare port are două tipuri de trafic:

- Ingress traficul care intră în port
- Egress traficul care iese din port

Vă recomandăm sa folosiți Traffic Shaping pentru controlarea traficului egress, deoarece este mai eficient în direcția egress. Atunci când un port acceptă trafic ingress, nu poate controla cât de repede ajunge traficul – când transmite, aparatul poate controla traficul. Totuși, când portul transmite trafic egress, poate controla viteza de transmisie.

Funcția Bursting permite creșterea ratei de transfer peste valoarea maximă configurată în câmpurile *Ingress Rate* și *Egress Rate* – pentru o scurtă perioadă de timp. După folosirea ratiei Ingress sau Egress Burst (volum de date), rata de transfer scade la valorile pe care le-ați setat în câmpurile *Ingress Rate* sau *Egress Rate* (maximum bandwidth).

De exemplu, dacă folosiți următoarele setări:
- Ingress Burst este 2048 kBytes.
- Ingress Rate este 512 kbit/s.
- Rata de transfer reală este 1024 kbit/s. Bursting permite trecerea a 2048 kBytes cu rata de 1024 kbit/s, înainte de a o limita la 512 kbit/s.



Enable Activează controlul ratei de transfer pe aparat.

Enabled Activează o regulă specifică. Toate regulile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.

Interface Selectați interfața potrivită.

Ingress

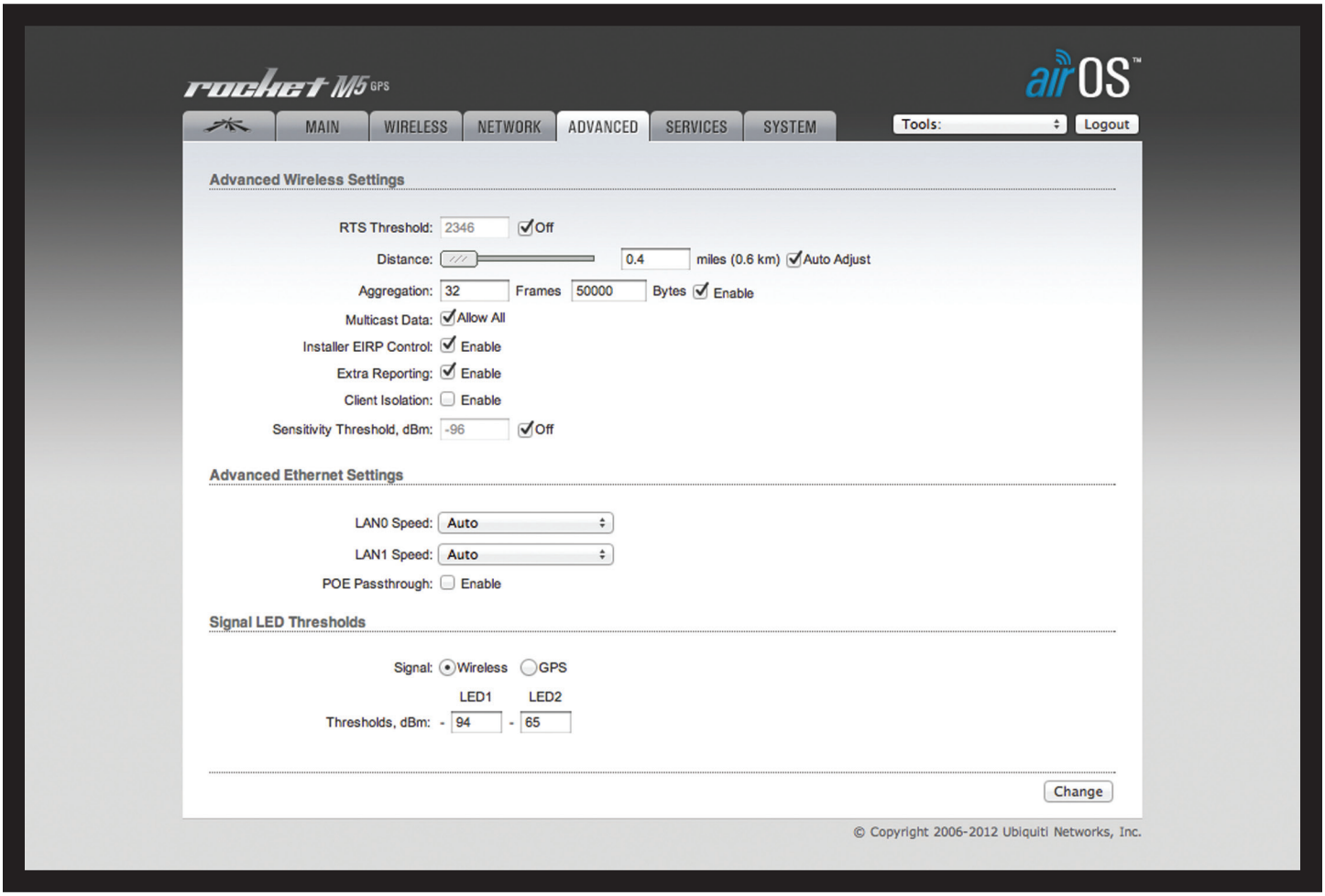
- Enable Activează valoarea ingress.
- Rate, kbit/s Specificați valoarea ratei de transfer maxime (în kilobits pe secundă) pentru traficul dinspre interfața wireless spre interfața Ethernet.
- Burst, kBytes Specificați volumul de date (în kilobytes) permis înainte ca valoarea ingress să fie limitată la valoarea maximă setată.

Egress

- Enable Activează valoarea egress.
- Rate, kbit/s Specificați valoarea ratei de transfer maxime (în kilobits pe secundă) pentru traficul dinspre interfața Ethernet spre interfața wireless.
- Burst, kBytes Specificați volumul de date (în kilobytes) permis înainte ca valoarea egress să fie limitată la valoarea maximă setată.

Action Aveți următoarele opțiuni:

- Add Adaugă o regulă.
- Edit Modifică o regulă. Apăsați **Save** pentru a salva modificările.
- Del Șterge o regulă.



Capitolul 6: Meniul Advanced

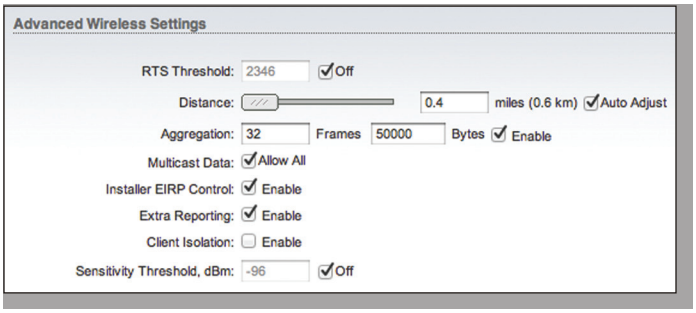
Meniul Advanced conține setările avansate de rutare și wireless. Setările wireless avansate ar trebui folosite doare de către utilizatorii avansați care au suficiente cunoștințe despre tehnologia WLAN. Aceste setări nu trebuiesc modificate decât dacă știți ce efecte vor avea asupra aparatului.

Change Pentru a salva sau a testa modificările făcute apasați **Change**.
Apare un mesaj nou cu trei opțiuni:
Apply Pentru salvarea setărilor apăsați **Apply**.
Test Pentru a testa setările fără a salva apăsați **Test**.
Pentru a păstra setările apăsați **Apply**. Dacă nu se apasă *Apply* timp de 180 secunde (cronometrul este afișat), atunci se revine la ultimele setări salvate.
Discard Pentru a renunța la setări apăsați **Discard**.

Advanced Wireless Settings

Următorul tabel afișează ratele de transfer disponibile pentru 802.11n:

Devices with Chains	Data Rates
1x1	MCS 0, MCS 1, MCS 3, MCS 4, MCS 5, MCS 6, MCS 7
2x2	MCS 8 MCS 9, MCS 10, MCS 11, MCS 12, MCS 13, MCS 14, MCS 15



RTS Threshold (Dacă este activat airMAX, *RTS Threshold* nu este necesar) Determină mărimea pachetului unei transmisii și (cu ajutorul unui AP) ajută la controlul traficului. Intervalul de valori este 0-2346 bytes. Setarea implicită este 2346; aceasta înseamnă că RTS este dezactivat.

Notă: Ca alternativă, puteți selecta **Off** pentru a dezactiva opțiunea.

Protocolul de rețea wireless 802.11 folosește mecanisme wireless 802.11 de tipul *Request to Send (RTS)*/*Clear to Send (CTS)* pentru reducerea coliziunii pachetelor introdusă de terminale ascunse. Mărimea maximă pachetelor RTS/CTS poate fi cuprinsă între 0-2346 bytes. Dacă mărimea pachetului pe care aparatul vrea să îl transmită este mai mare decât limita, este activat protocolul *RTS/CTS handshake*. Dacă pachetul este mai mic sau egal cu limita, atunci este transmis imediat.

Sistemul folosește pachete RTS/CTS pentru acord; aceasta reduce coliziunile AP-urilor cu stații ascunse. Stația trimite prima un pachet RTS, iar AP-ul răspunde cu un pachet CTS. După acordul cu AP-ul a fost finalizat, stația transmite datele. Managementul controlului coliziunilor CTS are un interval de timp stabilit; în acest interval nici o stație nu va transmite și așteaptă până stația inițială termină transmisia.

Distance Pentru a specifica distanța în mile (sau kilometri), folosiți slider-ul sau introduceți valoarea manual. Puterea semnalului și rata de transmisie scad proporțional cu distanța. Modificarea distanței va schimba și timpul de confirmare (ACK).

Auto Adjust Vă recomandăm activarea acestei opțiuni. De fiecare dată când stația primește un pachet de date, transmite un pachet de confirmare (ACK) AP-ului (dacă nu există erori de transmisie). Dacă AP-ul nu primește pachetul ACK în timpul stabilit, atunci retransmite datele. Dacă prea multe pachete de date sunt retransmise (din cauza unui timp ACK prea scurt sau prea lung), atunci există o conexiune prea slabă și rata de transfer scade.

Aparatul are un nou algoritm de auto-confirmare, care modifică automat valoarea timpului ACK. Această facilitate esențială este necesară pentru stabilizarea conexiunilor pe distanță lungă.

Dacă două sau mai multe stații sunt amplasate la distanțe mult diferite față de AP, se va seta pe AP distanța celei mai îndepărtate stații.

Aggregation Standardul 802.11n permite transmiterea mai multor pachete într-un singur timp de acces, prin combinarea pachetelor într-un pachet mai mare. Combină pachetele cu aceeași sursă, destinație și clasă de trafic (QoS) într-un pachet mare cu antet MAC comun.

- Frames Determină numărul de cadre combinate într-un pachet mai mare.
- Bytes Determină mărimea (în bytes) a pachetului mai mare.
- Enable Bifați căsuța pentru activarea funcției *Aggregation*.

Multicast Data Permite trecerea pachetelot multicast. Implicit, această opțiune, este dezactivată.

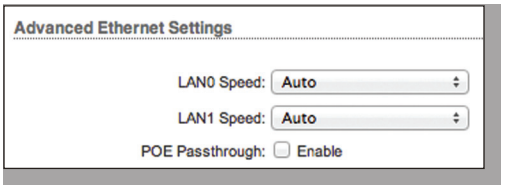
Installer EIRP Control Permite modificarea setării *Auto Adjust to EIRP Limit* din meniul *Wireless*.

Extra Reporting Comunică informații adiționale (ca numele aparatului) în pachetele de management 802.11. Această informație este în general folosită pentru identificarea sistemului și verificarea statusului de către utilitățile de descoperire și de softul router-elor.

Client Isolation (Disponibil numai în modul *Access Point* sau *AP-Repeater*) Permite transmiterea pachetelor numai dinspre rețeaua externă către CPE și invers. Dacă este activă, clienții wireless conectați la același AP nu se pot interconecta nici Layer 2 (MAC) și nici Layer 3 (IP). Opțiunea afectează atât clienții cât și perechile WDS.

Sensitivity Threshold, dBm Definește nivelul minim de semnal acceptat de către AP pentru conectarea unui client. Dacă după conectare nivelul semnalului scade, clientul rămâne conectat la AP.

Advanced Ethernet Settings



LAN0/1 Speed Setarea implicită este *Auto*. Aparatul negociază automat parametrii transmisiei, ca viteaza și duplexul, cu perechea sa. Procesul constă în comunicarea capabilităților fiecărui aparat, apoi alegerea modului cel mai rapid de transmisie pe care îl suportă ambele aparate.

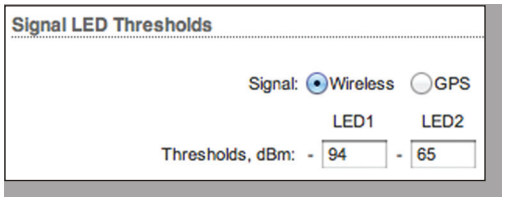
Pentru a specifica manual rata de transmisie și modul duplex, selectați una din opțiuni: **1000 Mbps-Full, 1000 Mbps-Half, 100 Mbps-Full, 100 Mbps-Half, 10 Mbps-Full** sau **10 Mbps-Half** (Aparatele Gigabit oferă opțiunea 1000 Mbps). Dacă folosiți cabluri Ethernet foarte lungi, o rată de transfer de Mbps poate ajuta la obținerea unei stabilități sporite.

Modul *Full-duplex* permite comunicarea simultană în ambele sensuri. Modul *Half-duplex* permite comunicarea în ambele sensuri, dar nu în același timp.

POE Passthrough (Disponibilitatea depinde de aparat) Când este activă, aparatul permite puterii PoE (Power over Ethernet) să treacă de la portul principal la portul secundar, astfel alimentând încă un aparat (de exemplu, o cameră IP compatibilă).

Signal LED Thresholds

(Opțiunea nu este disponibilă pe toate aparatele) Puteți configura ledurile aparatului să se aprindă când semnalul ajunge la valorile speciificate în câmpurile următoare. Facilitatea permite unui tehnician să monteze cu ușurință un aparat airOS CPE fără a se loga la acesta (de exemplu, pentru alinierea antenei).



Signal Tipul de semnal (wireless sau GPS).

Thresholds, dBm Numărul de leduri depinde de aparat, iar valorile implicite depind de numărul de leduri (vedeți tabelele). Fiecare led se aprinde dacă semnalul atinge valoarea setată în câmpul aferent.

De exemplu, dacă aparatul are patru leduri și puterea semnalului (din meniul *Main*) fluctuează în jurul valorii de -63 dBm, atunci valorile limită pentru leduri pot fi setate: -70, -65, -62, și -60.

Notă: Caracterul "-" se află în afara câmpului și nu trebuie folosit la scrierea valorii.

Următoarele tabele afișează setările implicite pentru aparatele cu două, trei, patru sau șase leduri.

Două leduri

LED	Default Threshold Value
1	-94 dBm
2	-65 dBm

Trei leduri

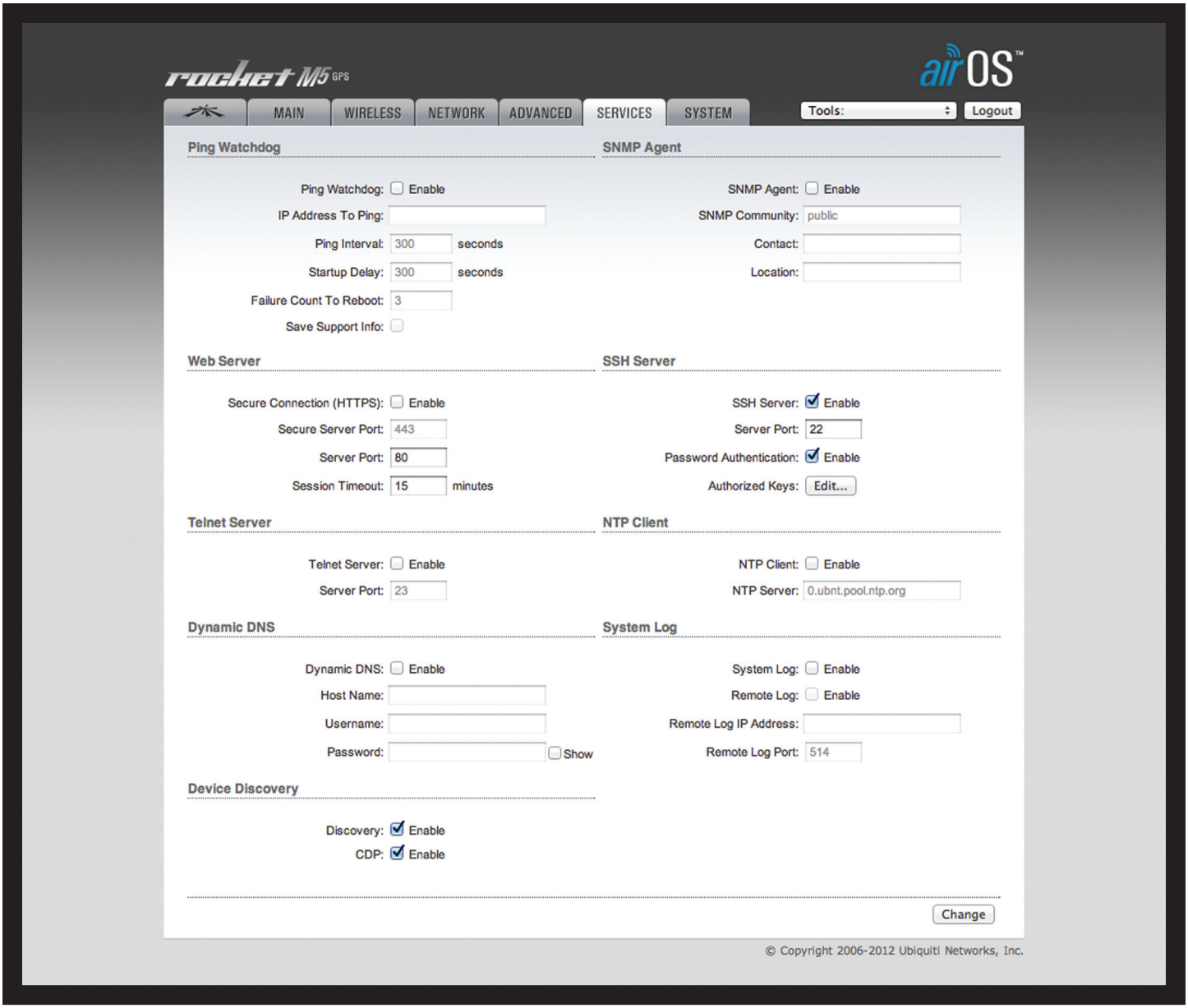
LED	Default Threshold Value
1	- 94 dBm
2	-77 dBm
3	-65 dBm

Patru leduri

LED	Default Threshold Value
1	-94 dBm
2	-80 dBm
3	-73 dBm
4	-65 dBm

Șase leduri

LED	Default Threshold Value
1	-94 dBm
2	-88 dBm
3	-82 dBm
4	-77 dBm
5	-71 dBm
6	-65 dBm



Capitolul 7: Meniul Services

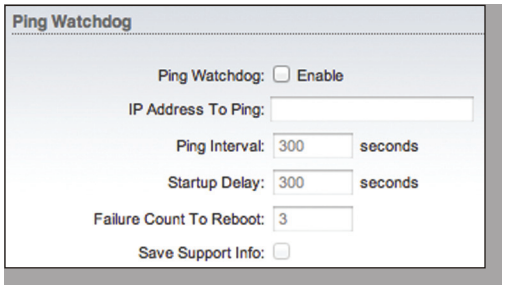
În meniul *Services* se configurează serviciile de management: Ping Watchdog, SNMP, servers (Web, SSH, telnet), NTP, DDNS, system log și device discovery.

Change Pentru a salva sau a testa modificările făcute apasați **Change**.
Apare un mesaj nou cu trei opțiuni:
Apply Pentru salvarea setărilor apăsați **Apply**.
Test Pentru a testa setările fără a salva apăsați **Test**. Pentru a păstra setările apăsați **Apply**. Dacă nu se apasă *Apply* timp de 180 secunde (cronometrul este afișat), atunci se revine la ultimele setări salvate.
Discard Pentru a renunța la setări apăsați **Discard**.

Ping Watchdog

Ping Watchdog instruiește aparatul să dea ping la o adresă IP specificată de utilizator (poate fi adresa gateway-ului). Dacă operațiunea de ping nu reușește, aparatul se va restarta automat. Această opțiune crează un mecanism împotriva cedării aparatului.

Ping Watchdog monitorizează continuu o conexiune specifică cu un aparat, folosind unealta Ping. Unealta Ping funcționează prin trimiterea unui pachet ICMP echo, unui aparat și așteptarea răspunsului ICMP echo. Dacă nu se primește un număr minim definit de răspunsuri, unealta restartează aparatului.



Ping Watchdog Activează funcția Ping Watchdog.

- IP Address To Ping Specificați adresa IP monitorizată de Ping Watchdog.
- Ping Interval Specificați intervalul de timp (în secunde) între cererile ICMP echo trimise de Ping Watchdog. Valoarea implicită este 300 de secunde.
- Startup Delay Specificați timpul inițial (în secunde) până la prima cerere ICMP echo trimisă de Ping Watchdog. Valoarea implicită este 300 de secunde.

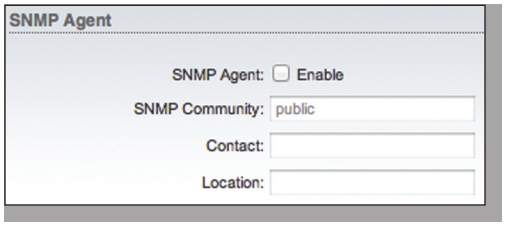
  Valoarea Startup Delay ar trebui să fie cel puțin 60 de secunde pentru a permite reinițializarea interfeței de rețea și a conexiunii wireless, dacă aparatul a fost restartat.
- Failure Count to Reboot Specificați numărul de răspunsuri ICMP echo. Dacă numărul de pachete specificat de ICMP echo nu este primit continuu, atunci Ping Watchdog va restarta aparatul. Valoarea implicită este 3.
- Save Support Info Generează un fișier cu informații pentru suport.

SNMP Agent

Protocolul SNMP (Simple Network Monitor Protocol) este o aplicație care facilitează schimbul de informație pentru management între aparatele rețelei. Administratorii de rețea folosesc SNMP pentru monitorizarea aparatelor conectate la rețea în cazul problemelor ce necesită atenție.

Aparatul conține un agent SNMP care realizează următoarele:

- Furnizează o interfață pentru monitorizarea aparatului folosind SNMP
- Comunică cu aplicațiile de management SNMP pentru întreținerea rețelei.
- Permite administratorilor de rețea să monitorizeze performanța rețelei și să rezolve problemele.

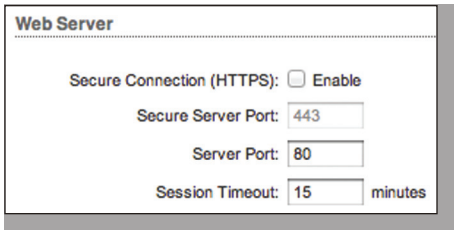


Pentru identificarea echipamentului, configurați agentul SNMP cu datele de contact și locație:

SNMP Agent Activează agentul SNMP.

- SNMP Community Specificați numele comunității SNMP. Este necesar pentru a permite autentificarea la obiectele MIB (Management Information Base) și funcționează ca o parolă integrată. Aparatul suportă comunități read-only; stațiile de management autorizate pot citi obiectele MIB, cu excepția numelui comunității, dar nu pot face operații de scriere. Aparatul suportă SNMP v1. Numele implicit a comunității SNMP este *public*.
- Contact Specificați datele de contact în cazul unei urgențe.
- Location Specificați locația aparatului.

Web Server



Pentru *Web Server*, se pot seta următorii parametrii:

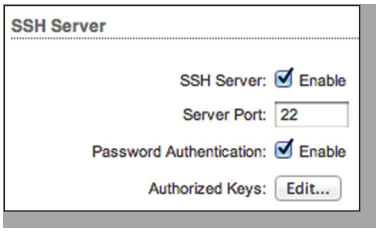
Secure Connection (HTTPS) Dacă este activ, serverul Web folosește modul securizat HTTPS.

- Secure Server Port Dacă este folosit modul secure HTTPS, specificați portul TCP/IP pentru serverul Web.

Server Port Dacă este folosit modul HTTP, specificați portul TCP/IP pentru serverul Web.

Session Timeout Specifică durata de timp după care o sesiune expiră. După ce o sesiune expiră, trebuie să vă reautentificați folosind numele și parola.

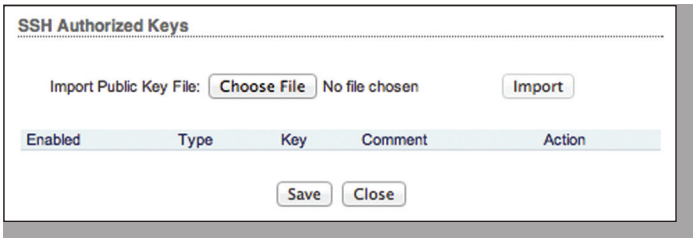
SSH Server



Pentru SSH Server, se pot seta următorii parametrii:

SSH Server Această opțiune activează accesul SSH la aparat.

- Server Port Specificați portul TCP/IP pentru serverul SSH.
- Password Authentication Dacă este activată, trebuie să vă autentificați ca administrator pentru a primi acces SSH la aparat; altfel trebuie să aveți o cheie autorizată.
- Authorized Keys Apăsați **Edit** pentru importa o cheie publică pentru a accesa prin SSH aparatul, în locul folosirii unei parole de administrator.

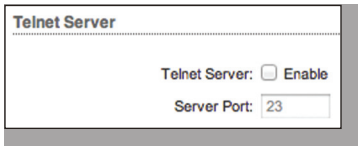


- Choose File Apăsați **Choose File** pentru a alege fișierul cu noua cheie. Selectați fișierul și apăsați **Open**.
- Import Importă fișierul pentru accesul SSH.
- Enabled Activează o anumită cheie. Toate cheile adăugate sunt salvate în fișierul de configurare, dar numai cele activate afectează aparatul.
- Type Afișează tipul de cheie.
- Key Afișează cheia.
- Comment Puteți introduce o scurtă descrierere a cheii.

Action Aveți următoarele opțiuni:

- Add Adaugă o cheie.
- Edit Modifică o cheie. Apăsați **Save** pentru a salva modificările.
  - Del Șterge o cheie.
- Save Salvați modificările.
- Close Anulați modificările.

Telnet Server



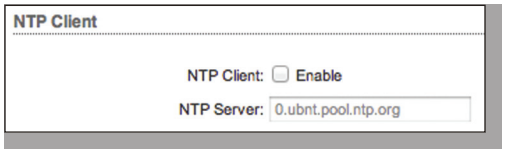
Pentru *Telnet Server*, se pot seta următorii parametrii:

Telnet Server Activează accesul Telnet către aparat.

- Server Port Specificați portul TCP/IP pentru serverul Telnet

NTP Client

NTP (Network Time Protocol) este un protocol care sincronizează ceasurile sistemelor într-o rețea cu latență variabilă și cu comutare de pachete. Îl puteți folosii pentru setarea orei pe aparat. Dacă opțiunea *Log* este activă, atunci lângă fiecare intrare se va specifica ora.

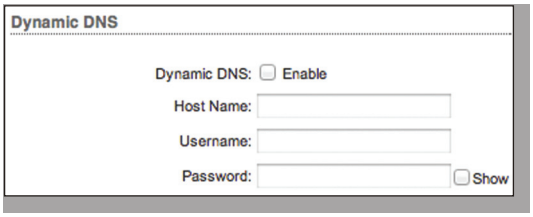


NTP Client Instruiește aparatul să obțină ora de la un server NTP de pe internet.

- NTP Server Specificați adresa IP sau numele de domeniu a serverului NTP.

Dynamic DNS

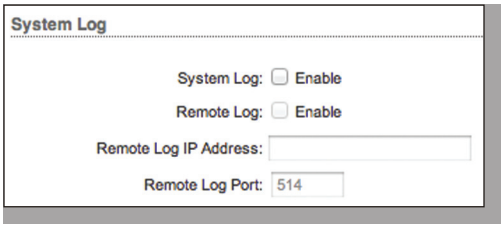
DNS (Domain Name System) traduce numele de domenii în adrese IP; Fiecare server DNS din internet păstrează aceste înregistrări în baza de date DNS. DDNS (Dynamic Domain Name System) este un serviciu de rețea care înștiințează serverul DNS în timp real despre modificarea adresei IP a aparatului. Chiar dacă adresa IP a aparatului se modifică, tot îl puteți accesa folosind numele de domeniu.



Dynamic DNS Dacă este activ, aparatul permite comunicarea cu serverul DDNS.

- Host Name Introduceți numele/adresa serverului DDNS.
- Username Introduceți numele de utilizator DDNS
- Password Introduceți parola utilizatorului DDNS.
- Show Bifați pentru a afișa parola.

System Log

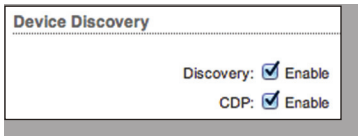


System Log Opțiunea activează logarea mesajelor de sistem (syslog). Implicit, opțiunea este dezactivată.

- Remote Log Activează funcția de trimitere a mesajelor de sistem către alt server. Mesajele de sistem sunt trimise către un server din altă locație specificat în câmpurile *Remote Log IP Address* și *Remote Log Port*.
  - Remote Log IP Address Adresa IP a serverului care recepționează mesajele de sistem. Configurați serverul corespunzător pentru a primi aceste mesaje.
  - Remote Log Port Portul TCP/IP a serverului care recepționează mesajele de sistem. Portul folosit implicit de utilitățile pentru logarea mesajelor de sistem este 514.

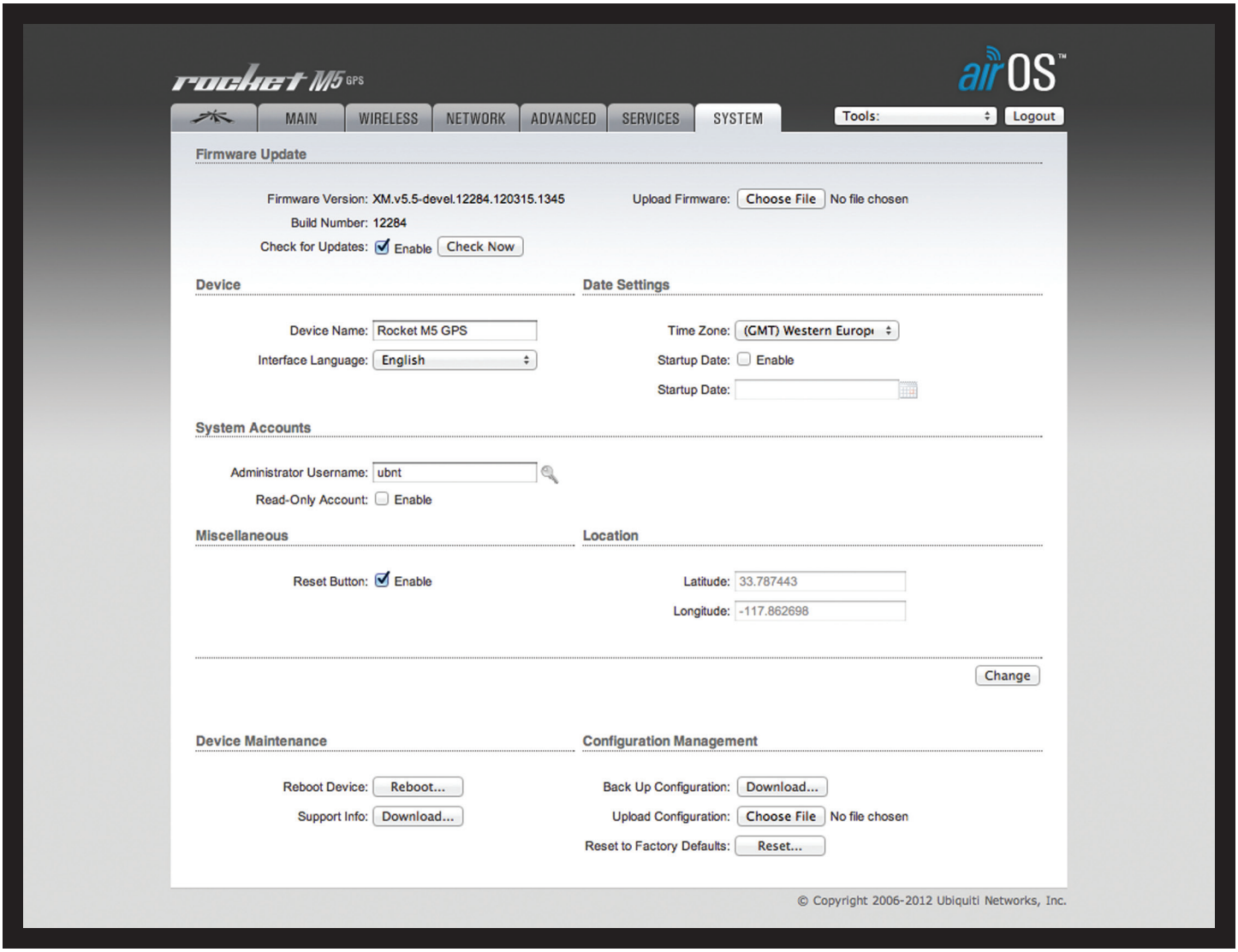
Fiecare mesaj logat conține cel puțin ora și numele aparatului. De obicei, numele unui serviciu care a generat un eveniment de sistem este de asemenea specificat în mesaj. Mesajele diferitelor servicii au contexte și nivele de detaliere diferite. De obicei, sunt raportate erorile, avertismentele sau informațiile despre un serviu al sistemului, totuși se pot raporta și mesașe mai detaliate pentru depanare. Cu cât mesajele sunt mai detaliate, cu atât este mai mare volumul mesajelor generate.

Device Discovery



Discovery Activează serviciul *device discovery*, pentru ca aparatul să poată fi descoperit de alte aparate Ubiquiti prin unealta *Discovery*.

CDP Activează comunicarea CDP (Cisco Discovery Protocol), pentru ca aparatul să poată trimite pachete CDP cu informațiile sale.



Capitolul 8: Meniul System

Meniul *System* conține setările administrative. Permite administratorului să restarteze aparatul, să reseteze aparatul la setările implicite, să actualizeze firmware-ul, să actualizeze sau să salveze configurațiile și să configureze contul de administrator.

Change Pentru a salva sau a testa modificările făcute apasați **Change**.
Apare un mesaj nou cu trei opțiuni:
Apply Pentru salvarea setărilor apăsați **Apply**.
Test Pentru a testa setările fără a salva apăsați **Test**. Pentru a păstra setările apăsați **Apply**. Dacă nu se apasă *Apply* timp de 180 secunde (cronometrul este afișat), atunci se revine la ultimele setări salvate.
Discard Pentru a renunța la setări apăsați **Discard**.

Firmware Update

Setările din această secțiune sunt pentru întreținerea firmware-ului.

Firmware Version Afișează versiunea curentă a firmware-ului.

Build Number Afișează numărul de compilare a firmware-ului.

Check for Updates Implicit, firmware-ul caută automat actualizări. Pentru a căuta manual actualizări, apăsați **Check Now**.

Upload Firmware Apăsați acest buton pentru a actualiza firmware-ul.

Actualizarea firmware-ului se poate face indiferent de setările de pe aparat. La actualizarea firmware-ului se mențin setările precedente. Totuși vă recomandăm să salvați setările aparatului înainte de actualizarea firmware-ului.

Este o procedură în trei pași:

1. Apăsați **Choose File** pentru a localiza fișierul noului firmware. Selectați fișierul și apăsați **Open**.
2. Apăsați **Upload** pentru a încărca noul firmware în aparat.
3. Este afișată versiunea firmware-ului aîncărcat. Pentru a confirma, apăsați **Update**.

În timpul procesului de actualizare, puteți închide fereastra de actualizare, dar acest lucru nu va întrerupe actualizarea. Fiți răbdători, deoarece procesul de actualizare poate dura între 3 și 7 minute. Nu puteți accesa aparatul până la finalizarea procesului de actualizarea a firmware-ului.

Notă: Nu opriți și nu deconectați aparatul de la sursa de tensiune în timpul procesului de actualizare, deoarece puteți avaria aparatul.

Device

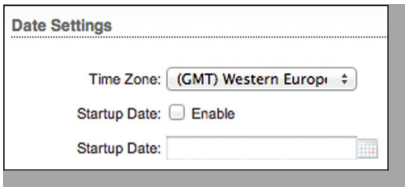
Numele aparatului (host name) este identificatorul întregului sistem. Agentul SNMP, îl transmite soluțiilor de management autorizate. Numele aparatului apare pe ecranele de logare, în uneltele de descoperire și în sistemele de operare populare pentru rutere.

Device Name Specificați numele aparatului.

Interface Language Vă permite selectarea limbii pentru afișarea interfeței de management. Setarea implicită este *English.*

Puteți încărca profile de limbă suplimentare. Vizitați pagina wiki la adresa: www.ubnt.com/wiki/How_to_import_Language_Profile

Date Settings



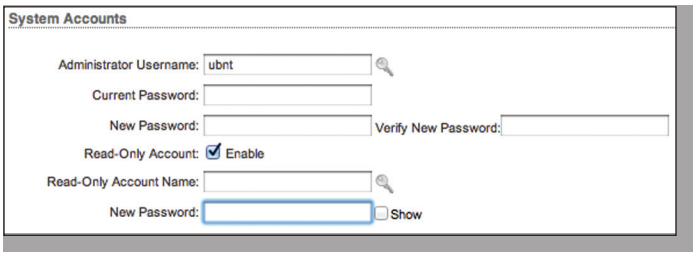
Time Zone Specificați fusul orar în funcție de GMT (Greenwich Mean Time).

Startup Date Când este activată, puteți modifica data de pornire a aparatului.

- Startup Date Specificați data de pornire a aparatului. Apăsați icoana **Calendar** sau introduceți data manual în următorul format: XX/YY/ZZZZ (lună/zi/an). De exemplu, pentru 20 decembrie 2011, introduceți 12/20/2011.

System Accounts

Puteți schimba parola de administrator pentru a vă proteja de accesări neautorizate. Vă recomandăm schimbarea parolei de administrator încă de la prima accesare a aparatului:



Administrator Username Specificați numele administratorului.

Key button Apăsați pentru schimbarea parolei de administrator.

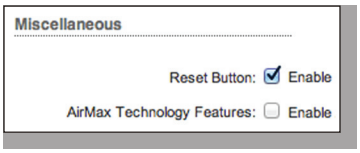
- Current Password Introduceți parola curentă. Este necesară pentru modificarea numelui sau parolei de administrator.
- New Password Introduceți noua parolă pentru contul de administrator.
- Verify New Password Reintroduceți noua parolă pentru contul de administrator.

Notă: Parola poate avea maxim 8 caractere; parolele peste 8 caractere vor fi scurtate.

Read-Only Account Bifați căsuța pentru a activa contul de utilizator, care poate vedea numai meniul *Main.* Configurați numele și parola pentru a proteja aparatul de modificări neautorizate.

- Read-Only Account Name Specificați numele utilizatorului.
- Key button Apăsați butonul pentru a modifica parola utilizatorului.
  - New Password Introduceți noua parolă pentru utilizator.
  - Show Bifați pentru a afișa caracterele parolei.

Miscellaneous



Reset Button Bifați căsuța pentru a permite folosirea butonului *reset* de pe aparat. Pentru a preveni resetarea accidentală, debifați căsuța (dezactivează și funcția de resetare prin POE).

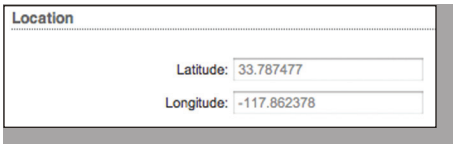
Notă: Puteți reseta aparatul la setările implicite prin accesarea meniului *System* > *Reset to Defaults.*

airMAX Technology Features (Disponibil în meniul *System* dacă nu este afișat meniul *Ubiquiti logo*) airMAX este tehnologie specifică Ubiquiti pentru sondare Time Division Multiple Access (TDMA). airMAX oferă toleranță mai mare la interferență. Datorită acestor avantaje, airMAX mărește și numărul maxim de utilizatori care pot fi asociați unui AP care folosește airMAX.

După ce ați activat această opțiun e în meniul *System*, va apărea meniul *Ubiquiti.* Vezi "**airMAX Settings**" pagina 4.

Location

Latitudinea și longitudinea definesc coordonatele aparatului; sunt folosite pentru a actualiza automat locația aparatului în airControl.

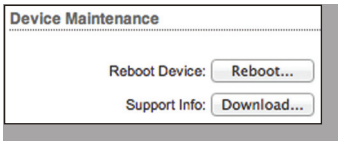


Latitude Este afișată latitudinea aparatului.

Longitude Este afișată longitudinea aparatului.

Device Maintenance

În această secțiune se realizează setările de mentenanță: restartare și rapoartele cu informații pentru suport.



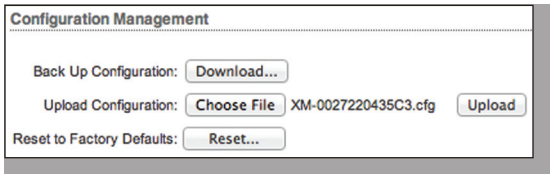
Reboot Device Funcția este similară cu întreruperea alimentării și apoi reconectarea acesteia. După ciclul de restartare, setările aparatului se mențin. Orice modificare nesalvată se va pierde.

Support Info Generează un fișier cu informații pentru suport, pe care inginerii Ubiquiti îl poate folosi pentru acordarea de suport. Acest fișier trebuie generat doar dacă vi se cere.

Configuration Management

În această secțiune se află setările pentru managementul configurărilor și opțiunea pentru resetarea aparatului la setările implicite.

Configurarea aparatului este stocată într-un fișier text (fișier .cfg). Puteți selva, restaura sau actualiza un fișier de configurare:



Back Up Configuration Apăsați **Download** pentru a descărca fișierul cu configurările de sistem curente.

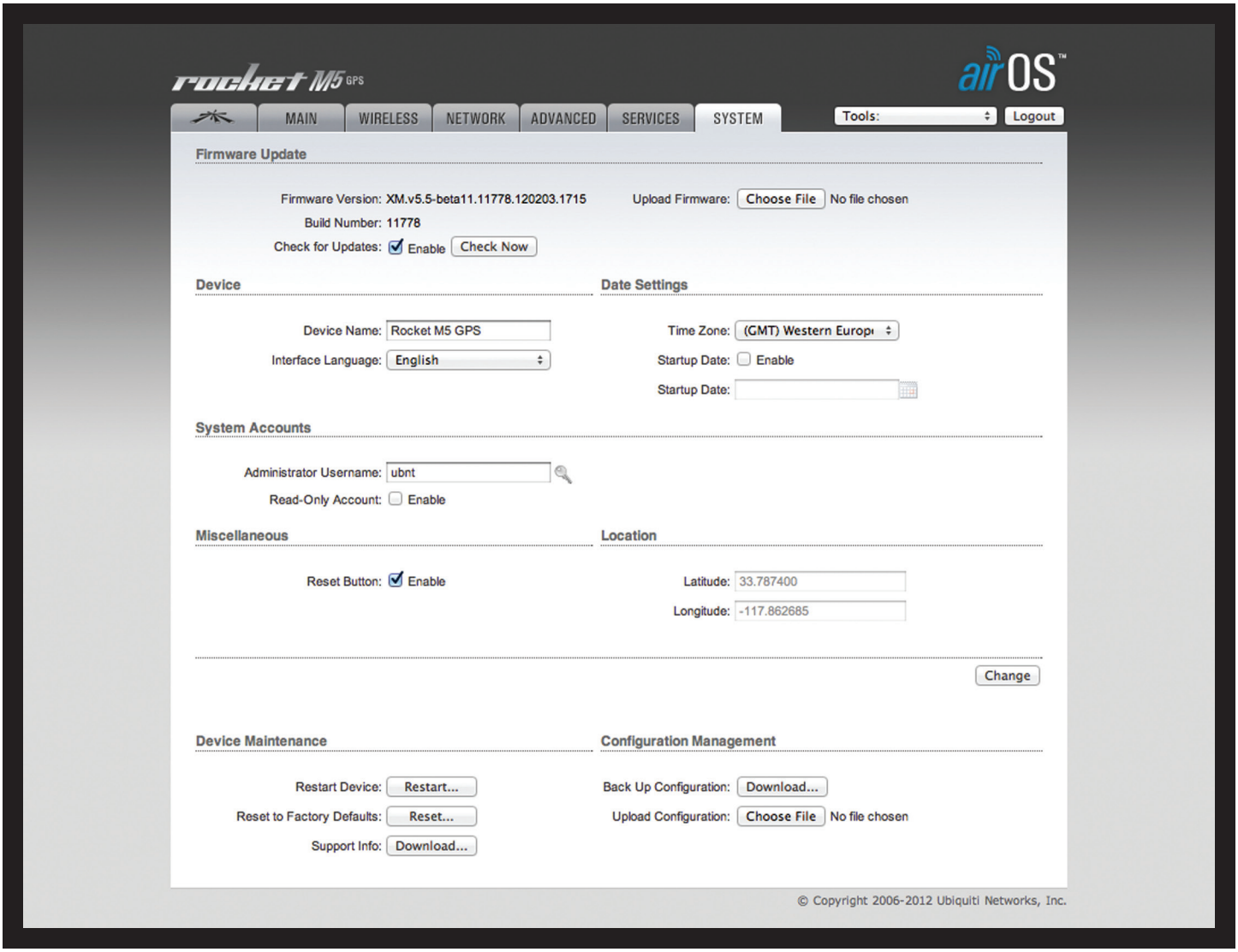
Upload Configuration Apăsați **Choose File** pentru a localiza fișierul cu noile configurări. Selectați fișierul și apăsați **Open**. Vă recomandăm să salvați setările curente înainte de a încarca noile configurări.

Notă: Folosiți numai acele fișiere destinate aparatului dumneavoastră. În cazul folosirii fișierelor de la alte aparate, comportamentul acestuia poate deveni imprevizibil (de exemplu, încărcați un fișier cu setările pentru RocketM5 pe un aparat RocketM5; NU încărcați fișiere cu setările pentru BulletM5 pe un aparat RocketM5).

Upload Apăsați butonul pentru a încărca în aparat fișierul cu noile configurări. Apăsați **Apply** pentru confirmare.

După ce aparatul se restartează, în meniurile *Wireless, Network, Advanced, Services* și *System,* vor fi afișate noile setări.

Reset to Factory Defaults Apăsați pentru resetarea aparatului la setările implicite. Aparatul se va restarta și vor fi restaurate toate setările implicite. Înainte de a face acest lucru, vă recomandăm să salvați setările curente.

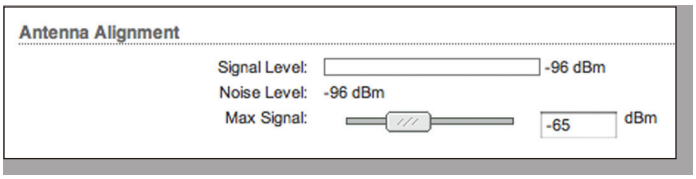


Capitolul 9: Tools

Fiecare meniu din airOS conține uneltele pentru administrarea și monitorizarea rețelei. Apăsați pe **Tools** din colțul din dreapta sus al paginii pentru afișarea uneltelor disponibile.

Align Antenna

Folosiți unealta *Align Antenna* pentru a regla poziția antenei în direcția cu semnal maxim. Fereastra *Antenna Alignment* se reînprospătează în fiecare secundă.



Signal Level Afișează puterea semnalului a ultimului pachet recepționat.

Chain Afișează nivelul semnalului wireless (în dBm) a fiecărui lanț, dacă există mai mult de un lanț (numărul de lanțuri diferă în funcție de aparat)

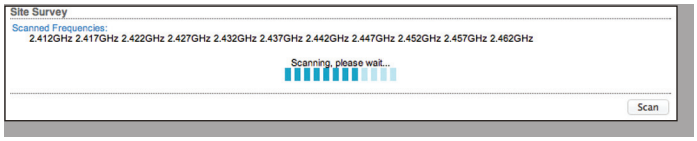
Noise Level Afișează nivelul de zgomot (în dBm) a semnalului wireless recepționat.

Max Signal Afișează puterea maximă a semnalului (în dBm). Pentru a ajusta valoarea, folosiți sliderul sau introduceți valoarea manual. Dacă reduceți intervalul afișat, schimbarea culorii va fi mai sensibilă la fluctuația semnalului, indicând diferența maximă între nivele și scala.

Site Survey

Unealta *Site Survey* caută rețelele wireless pe toate canalele suportate. În modul *Station,* puteți modifica lista de frecvențe; pentru detalii vedeți ”**Basic Wireless Settings**” pagina 18.

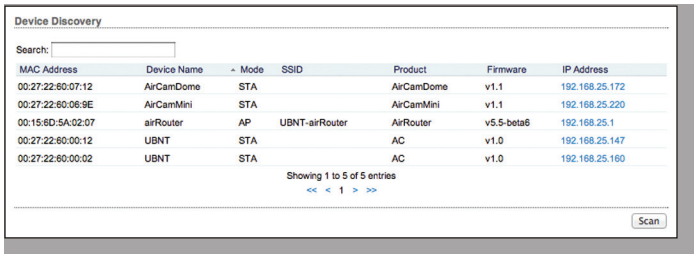
Unealta *Site Survey,* afișează pentru fiecare AP descoperit, următoarele informații: adresa MAC, SSID-ul, numele aparatului, tipul de criptare (dacă există), puterea și zgomotul semnalului (în dBm), frecvența în GHz și canalul Wireless.



Pentru a reîncărca fereastra, apăsați **Scan**.

Discovery

Unealta *Device Discovery,* caută toate aparatele Ubiquiti de pe rețeaua dumneavastră. Câmpul *Search* filtrează automat aparatele care conțin numele sau numerele introduse de dumneavoastră.

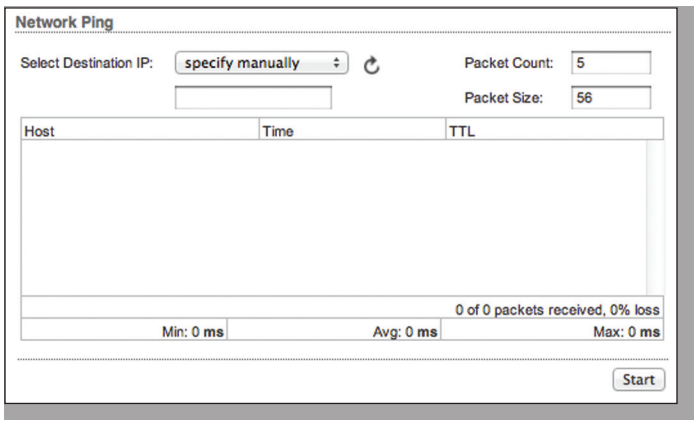


Pentru fiecare aparat Ubiquiti, afișează: adresa MAC, SSID-ul, numele aparatului, modul de funcționare, tipul produsului, versiunea firmware-ului și adresa IP. Pentru a accesa aparatul prin interfața de management, apăsați adresa IP a acestuia.

Pentru a reîncărca fereastra, apăsați **Scan**.

Ping

Puteți da ping direct de pe aparat altor aparate din rețea. Unealta *Ping* folosește pachete ICMP pentru o verificare preliminară a calității link-ului și pentru estimarea latenței dintre două aparate.



Network Ping

Select Destination IP Aveți două opțiuni:

- Selectați un IP din lista generată automat.
- Selectați **specify manually** și introduceți adresa IP în câmpul de dedesubt.

Packet Count Introduceți numărul de pachete trimise de testul ping.

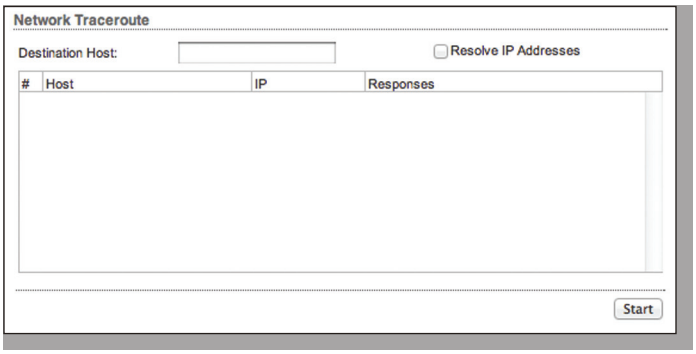
Packet Size Specificați mărimea pachetului.

Start Apăsați **start** pentru începerea testului.

După finalizarea testului se afișează statisticile despre pierderea de pachete și latența.

Traceroute

Unealta *Traceroute* afișează numărul de hopuri între aparat și o adresă IP specificată. Folosiți această unealtă pentru a descoperii ruta pe care o au pachetele ICMP prin rețea până la destinație.



Destination Host Introduceți adresa IP de destinație.

Resolve IP Addresses Selectați această opțiune pentru afișarea numelor DNS în locul adresei IP.

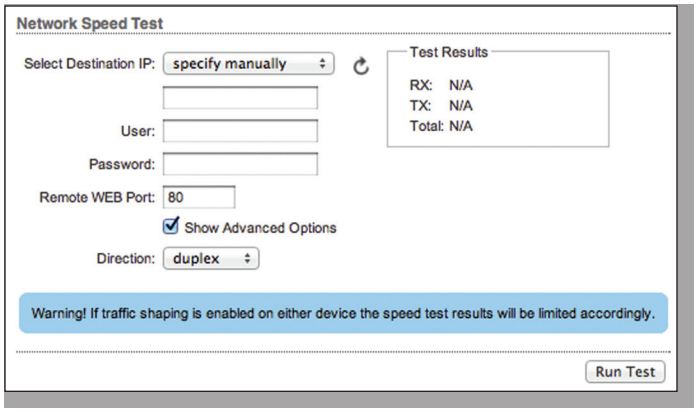
Start Apăsați **start** pentru a începerea testului.

Rezultatele sunt afișate după finalizarea testului.

Speed Test

Utilitatea vă permite testarea conexiunii dintre două aparate airOS care folosesc versiunea firmware 5.2 (sau mai nou). Puteți folosi *Speed Test* pentru estimare preliminară a ratei de transfer între două aparate.

Notă: Dacă *traffic shaping* este activ, atunci rezultatele vor fi limitate corespunzător.



Select Destination IP Aveți două opțiuni:

- Selectați un IP din lista generată automat.
- Selectați **specify manually** și introduceți adresa IP în câmpul de dedesubt.

User Introduceți numele de administrator.

Notă: Pentru comunicarea între două aparate airOS trebuie să introduceți datele de logare a celuilalt aparat. Informațiile sunt necesare pentru realizarea testului de rată de transfer bazat pe TCP/IP.

Password Introduceți parola de administrator.

Remote WEB port Introduceți portul Web al aparatului airOS pentru realizarea testului de rată de transfer bazat pe TCP/IP (de exemplu, specificați portul 443 dacă pe celălalt aparat este activat HTTPS). Dacă portul Web al celuilalt aparat nu este corect, se va inițializa testul de rată de transfer ICMP.

Show Advanced Options Afișează opțiuni suplimentare pentru testul de viteză.

Direction Selectați una din cele trei direcții:

- duplex Estimează, în același timp, rata de transfer de descărcare (RX) și încărcare (TX).
- receive Estimează rata de transfer de descărcare (RX).
- transmit Estimează rata de transfer de încărcare (TX).

Run Test Apăsați **start** pentru a începerea testului.

Test Results Afișează rezultatele pe trei categorii:

- RX Afișează rata de transfer de descărcare (estimată).
- TX Afișează rata de transfer de încărcare (estimată).
- Total Afișează rata de transfer totală.

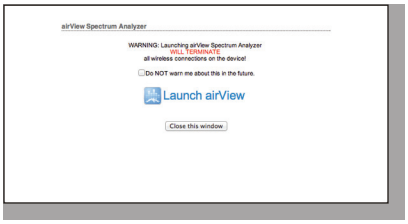
airView

Folosiți unealta *airView Spectrum Analyzer* pentru a analiza zgomotul din spectrul radio și pentru a selecta frecvența optimă pentru instalarea unui link PtP airMAX.

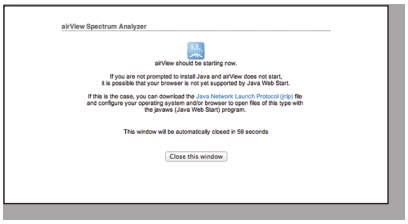
Există două cerințe de sistem pentru folosirea airView Spectrum Analyzer:

- Sistemul dumneavoastră trebuie conectat la aparat prin cablu deoarece după lansarea airView se vor întrerupe toate conexiunile wireless.
- Pe sistem trebuie sa aveți instalat Java Runtime Environment 1.6 (sau mai nou).

La prima folosire va apărea următoarea fereastră:



- Do NOT warn me about this in the future Bifați căsuța pentru a evita această fereastră în viitor.
- Launch airView Apăsați **Launch airView** pentru a descărca fișierul Java Network Launch Protocol (jnlp) și pentru a lansa aplicația airView.



Fereastra Principală

Device Afișează numele, adresa MAC (Media Access Control) și adresa IP a aparatului care rulează airView.

Total RF Frames Afișează numărul total de cadre RF (Radio Frequency) adunate de la pornirea sesiunii airView sau de când a fost apăsat ultima dată butonul *Reset All Data*.

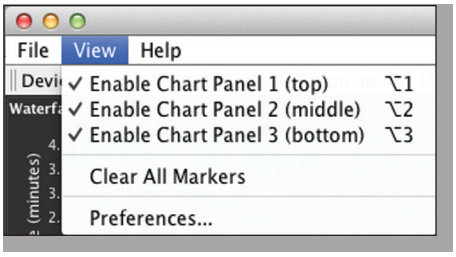
FPS Afișează numărul total de cadre pe secundă (FPS) adunate de la pornirea sesiunii airView sau de când a fost apăsat ultima dată butonul *Reset All Data*.

Reset All Data Apăsați pentru a reseta toate informațiile adunate.Folosiți această opțiune pentru a analiza spectrul dintr-o altă locație sau adresă.

Meniul File

Apăsați **Exit** pentru a incheia sesiunea airView.

Meniul View



Enable Chart Panel 1 (top) Afișează utilizarea canalelor (Waterfall) în panoul 1, în funcție de opțiunea selectată în meniul *Preferences*. Acest grafic afișează în funție de timp energia colectată pentru fiecare frecvență de la începutul sesiunii airView.

Enable Chart Panel 2 (middle) Afșează graficul cu forma de undă în panoul 2. Graficul arată semnătura RF a zgomotului în funcție de timp de la începutul sesiunii airView. Culoarea energiei indică amplitudinea. Culorile reci reprezintă nivele mici de energie (albastru reprezintă cel mai mic ninel) și culorile calde (galben, portocaliu sau roșu) reprezintă nivele de energie mai mari.

Enable Chart Panel 3 (bottom) Afișează tabelul în timp real (modul tradițional de afișare) în panoul 3. Energia (în dBm) este indicată în timp real în funcție de frecvență.

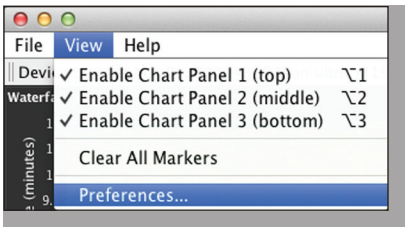
Notă: Energia este rația dintre decibelii (dB) puterii măsurate luată ca referință față de un miliwatt (mW).

Clear All Markers Resetează toate marker-ele anterioare. Un marker se crează prin selectarea unui punct, care corespunde unei frecvențe în tabelul Real-time.

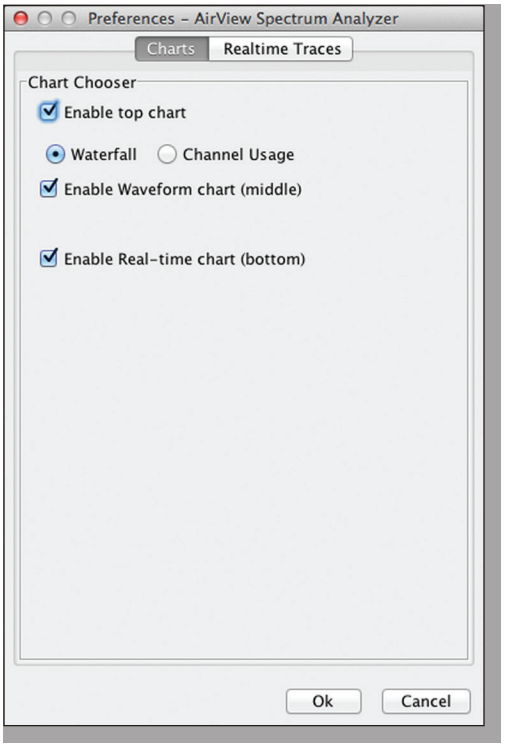
Preferences Modifică setările airView, pornind sau oprind panouri sau urme, sau specificând intervalul de frecvență.

Preferences

Selectați **View > Preferences** pentru a afișa fereastra cu preferințele airView Spectrum Analyzer.



Charts



Enable top chart Bifați pentru a porni panoul 1. Selectați tipul de tabel afișat în panoul 1. Există două opțiuni:

- Waterfall Este un grafic în funcție de timp a energiei colectate pe fiecare frecvență de la începutul sesiunii airView. Culoarea energiei indică amplitudinea. Culorile reci reprezintă nivele mici de energie (albastru reprezintă cel mai mic ninel) și culorile calde (galben, portocaliu sau roșu) reprezintă nivele de energie mai mari.

  Legenda vederii Waterfall (colțul din dreapta sus) furnizează un ghid al valorilor numerice asociate culorilor în funcție de nivelul de putere (în dBm). Partea inferioară a legendei (stânga) este întotdeauna ajustată la limita inferioară a zgomotului, iar partea superioară (dreapta) este setată la nivelul de putere maxim detectat de la începutul sesiunii airView.

- Channel Usage Pentru fiecare canal Wi-Fi, o bară afișează procentajul relativ de aglomerare. Pentru calcularea procentajului, airView Spectrum Analyzer analizează atât popularitatea, cât și puterea energiei RF a respectivului canal de la începutul sesiunii airView.

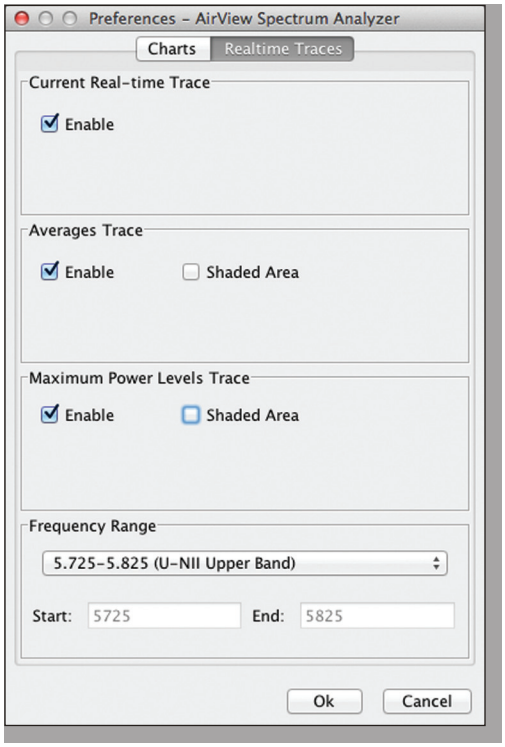
Enable Waveform chart (middle) Bifați pentru a porni panoul 2. Panoul afișează printr-un grafic în funcție de timp, semnătura zgomotului RF de la pornirea sesiunii airView. Culoarea energiei indică amplitudinea. Culorile reci reprezintă nivele mici de energie (albastru reprezintă cel mai mic ninel) și culorile calde (galben, portocaliu sau roșu) reprezintă nivele de energie mai mari.

Vederea spectrală va afișa starea stabilă a semnăturii energiei RF de-a lungul timpului întrun anumit mediu.

Enable Real-time chart (bottom) Bifați pentru a porni panoul 3. Graficul afișează analizatorul de spectru tradițional, în care energia (în dBm) este afișată în timp real în funcție de frecvență. Sunt trei urme pentru această vedere:

- Current (Galben) Arată energia în timp real văzută de aparat în funcție de frecvență.
- Average (Verde) Afișează energia medie în funție de frecvență.
- Maximum (Albastru) Afișează nivelul maxim de putere în funcție de frecvență.

Realtime Traces



Următoarele setări se aplică numai pentru graficul în timp real:

Current Real-time Trace Bifați pentru a activa urma în timp real. Când este activată, conturul galben din graficul Real-time reprezintă nivelul de putere în timp real în funcție de frecvență. Viteza de actualizare depinde de FPS.

Averages Trace Bifați pentru a activa urma de medie. Când este activată, zona verde din graficul Real-time afișează media nivelului de putere de la începutul sesiunii airView. Pentru a activa o zonă verde umbrită, bifați *Shaded Area*. Pentru a afișa numai un contur verde, debifați *Shaded Area*.

Maximum Power Levels Trace Bifați pentru a activa urma puterii maxime. Când este activată, zona albastră din graficul Real-time afișează nivelul puterii maxime de la începutul sesiunii airView. Pentru a activa o zonă albastră umbrită, bifați *Shaded Area*. Pentru a afișa numai un contur albastru, debifați *Shaded Area*.

Frequency Range Selectați intervalul de frecvențe care va fi scanat din lista *Frequency Range*. Frecvențele disponibile diferă în funcție de aparat. Există intervale predefinite pentru cele mai populare benzi. Puteți introduce și un interval personalizat; selectați **Custom Range** din lista *Frequency Range* și introduceți valorile dorite în câmpurile *Start* și *End*.

HELP

Apăsați **About** pentru a vedea versiunea și numărul de compilare a airView Spectrum Analyzer.