araknis NETWORKS

DUAL-WAN GIGABIT VPN ROUTER

PRODUCT MANUAL

Models:
AN-300-RT-4L2W

FCC Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

- This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
  - Reorient or relocate the receiving antenna.
  - Increase the separation between the equipment and receiver.
  - Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
  - Consult the dealer or an experienced radio/TV technician for help.

CE Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

UL

This device is intended for indoor use only. It should not be connected to an Ethernet network with outside plant routing.

© 2015 Araknis Networks®

About this Manual

This manual was created to provide a reference for installers and end users of Araknis Networks products. It provides all known information regarding the installation, setup, use, and maintenance of the product. The symbols below are used to identify important information:

Pro Tip – Pro tips are included in sections of the manual to add information that provides extra value, utility, or ease-of-use for the installer or end user of the product. Pro tips may also link to extra information that will provide a better understanding of application, technology or use of the product or feature in question. These items are not required, but have been added for your convenience.

Note – Notes emphasize information important to the installation, setup, or use of the product that is not essential to follow for safety of the equipment or user. Notes may be located before or in the midst of the section to which they apply, depending on the type of information. These items usually contain essential information, like the size or dimension of a separate part required, or a critical step in the process, that, if missed, would cause the installer or end user extra work to overcome.

Caution – The caution symbol is used to indicate information vital to the safety of the equipment in use with the product, or the product itself. Cautions are always provided before the information they relate to. Not following a caution will almost always result in permanent damage to equipment that is not covered by warranty.

Warning – Warnings indicate information vital to the safety of the installer or end user of the product. Warnings are always provided before the information they relate to. Not following a warning may result in permanent damage to equipment and serious injury or death of the installer or end user.

© 2015 Araknis Networks®

Table of Contents

FCC Warning 2
CE Warning 2
UL 2
About this Manual 3
1 - Welcome to Araknis Networks 10
1.1 - Features 10
2 - Package Contents 10
3 - Hardware Overview 11
3.1 - Front Panel Layout 11
3.2 - Rear Panel Layout 11
4 - Wiring Requirements 12
4.1 - Network Cable Requirements 12
4.2 - Power Requirements 12
4.3 - Wiring Diagram 12
5 - Mounting Options 13
5.1 - Rack Mount 13
5.1.1 - Rack Mounting Guidelines 13
5.2 - Wall Mount 14
5.3 - Shelf Mount 14
6 - Installation Instructions 14
7 - Logging Into the Web Interface 15
8 - Quick Setup 15
9 - OvrC™ Access 16
10 - Menu Overview 17
11 - Status 18
11.1 - System 18
11.1.1 - System Information 19
11.1.2 - Port Status Display 19
11.1.3 - Port Status 20
11.1.4 - WAN Status 20
11.1.5 - System Log 21
11.2 - Clients and Services 22
11.2.1 - Firewall Status 22
11.2.2 - VPN Status 23
11.2.3 - DHCP Status 23
11.2.4 - Client Table 24
11.2.5 - Forwarded Ports 24
11.3 - Ports 25
11.3.1 - Port Status 25
12 - Settings 26
12.1 - System 26
12.1.1 - System Information 27
12.1.2 - Time Setting 28
12.1.3 - Auto-Reboot 29
12.2 - WAN 30
12.2.1 - WAN Status 31
12.2.2 - Interface Setting 32
12.2.3 - WAN Setting 33

© 2015 Araknis Networks®

12.2.3.1 - Understanding WAN Connection Types and Setup 34
12.2.3.2 - Understanding Load Balancing 34
12.2.4 - Network Service Detection 35
12.3 - LAN 36
12.3.1 - Port Settings 37
12.3.2 - DHCP Server Settings 38
12.3.3 - DHCP Reservation Table 39
12.4 - Firewall 40
12.4.1 - General Settings 41
12.4.1.1 - Configuring Remote Management 42
12.4.1.2 - Using Remote Management 42
12.4.2 - Content Filter 43
12.4.3 - General Settings 43
12.4.3.1 - Configuring the Content Filter 43
12.5 - DDNS 44
12.5.1 - Dynamic DNS Settings 44
12.5.1.1 - Configuring DDNS Accounts 45
12.6 - Port Forwarding 46
12.6.1 - Port Forwarding Menu 47
12.6.2 - Port Forwarding Setup Instructions 48
12.6.2.1 - Adding a New Port Forwarding Rule 48
12.6.2.2 - Editing or Deleting an existing Port Forwarding Rule 48
12.7 - Security 49
12.7.1 - Email Alert 49
12.7.1.1 - Configuring Email Alerts 50
13 - Maintenance 51
13.1 - Ping 51
13.1.1 - Ping Test Results 51
13.2 - DNS Lookup 52
13.3 - File Management 53
13.3.1 - Configuration File 53
13.3.1.1 - Backup Current Configuration 53
13.3.1.2 - Upload New Configuration File 53
13.3.1.3 - Restore Factory Defaults 53
13.3.2 - Firmware 54
13.4 - Restart 55
13.5 - Logout 55
14 - Advanced Menus 56
15 - Routing 57
15.1 - Static Route 57
15.1.1 - Routing Table 57
15.1.2 - Static Route Setting 58
15.2 - Port Triggering 59
15.2.1 - Configuring Port Triggering 60
15.3 - DMZ 61
15.4 - One-to-One NAT 62
15.4.1 - Configuring One-to-One NAT 63
16 - VLANs 64
16.1 - Benefits of VLANs 65
16.2 - Why Set up VLANs? 65
16.3 - Basic VLAN Setup Recommendations 66

© 2015 Araknis Networks®

16.4 - Configuring VLANs 66
17 - VPN 68
17.1 - VPN Status 68
17.1.1 - Tunnel Status 69
17.1.2 - Group VPN Status 70
17.2 - OpenVPN 71
17.2.1 - OpenVPN Menu 72
17.2.2 - OpenVPN Client Status 72
17.2.3 - Configuring OpenVPN Accounts in the Router 73
17.3 - PPTP 74
17.3.1 - IP Address Range 74
17.3.2 - PPTP Server 74
17.3.3 - Connection List 74
17.4 - VPN Passthrough 75
17.5 - Gateway to Gateway 76
17.5.1 - Add a New Tunnel 77
17.5.2 - Local Group Setup 77
17.5.3 - Remote Group Setup 78
17.5.4 - IPSec Setup 79
17.6 - Client to Gateway 81
17.6.1 - Add a New Tunnel 83
17.6.1.1 - Local Group Setup 83
17.6.1.2 - Remote Client Setup 84
17.6.1.3 - IPSec Setup 85
17.7 - IPv6 87
17.7.1 - IP Mode 87
17.7.1.1 - WAN Setting 88
17.7.1.2 - LAN Setting 89
17.8 - Local DNS 90
17.8.1 - Configuring Local DNS 91
17.9 - SNMP 92
17.9.1.1 - SNMP Global Settings 92
17.10 - ACLs 93
17.10.1 - Service Management 93
17.10.2 - Access Control List Settings 94
17.10.3 - Adding a New Access Control Rule 95
18 - Troubleshooting 96
18.1 - Resetting the Router 96
20 - Specifications 97
21 - 2-Year Limited Warranty 99
22 - Contacting Technical Support 99

© 2015 Araknis Networks®

Table of Figures

Figure 1. EIA/TIA 568B Termination Pattern 12
Figure 2. Network Wiring Connection Diagram 12
Figure 3. Rack Mounting Ear Installation 13
Figure 4. Installing the Router in a Rack 13
Figure 5. Connecting Mounting Ears for Wall Mount Installation 14
Figure 6. Shelf Mounting Diagram 14
Figure 7. Quick Setup 15
Figure 8. OvrC Diagram 16
Figure 9. Menu Overview (System Status Screen) 17
Figure 10. System Status Screen 18
Figure 11. System Information 19
Figure 12. Port Status Display 19
Figure 13. Port Status 20
Figure 14. System Information 20
Figure 15. System Information 21
Figure 16. Clients and Services Status Screen 22
Figure 17. Firewall Status 22
Figure 18. VPN Status 23
Figure 19. DHCP Status 23
Figure 20. Client Table 24
Figure 21. Forwarded Ports 24
Figure 22. Ports Status Screen 25
Figure 23. System Settings Menu 26
Figure 24. System Information 27
Figure 25. Time Setting Menu 28
Figure 26. Manual Time Setting 28
Figure 27. Auto Reboot Menu 29
Figure 28. WAN Settings Menu 30
Figure 29. WAN Status 31
Figure 30. System Information 32
Figure 31. WAN Settings 33
Figure 32. Network Service Detection Menu 35
Figure 33. LAN Settings Menu 36
Figure 34. Port Settings Menu 37
Figure 35. DHCP Server Settings Menu 38
Figure 36. DHCP Server Settings Menu 39
Figure 37. Firewall Settings Menu 40
Figure 38. General Firewall Settings Menu 41
Figure 39. Remote Management Setup 42
Figure 40. Remote Router Access 42
Figure 41. Firewall Settings Menu 43
Figure 42. Dynamic DNS Settings Menu 44
Figure 43. DDNS Configuration 45

© 2015 Araknis Networks®

Figure 44. Port Forwarding Menu 47
Figure 45. New Port Forwarding Rule 48
Figure 46. Security Email Alert Menu 49
Figure 47. Common Email Client Ports 50
Figure 48. Ping Menu 51
Figure 49. Ping Menu 51
Figure 50. DNS Lookup Menu 52
Figure 51. File Management Menu 53
Figure 52. Firmware Menu 54
Figure 53. Restart Menu 55
Figure 54. Logout Menu 55
Figure 55. Static Route Configuration Example 57
Figure 56. Static Routing Menu 57
Figure 57. Adding a new Static Route 58
Figure 58. Port Triggering Setup Menu 59
Figure 59. Adding a New Port Trigger Rule 59
Figure 60. DMZ Setup Menu 61
Figure 61. One-to-One NAT Setup Menu 62
Figure 62. Adding a New One-to-One NAT Entry 62
Figure 63. One-to-One NAT Setup 63
Figure 64. One-to-One NAT Operation Example 63
Figure 65. VLANs Setup Menu 64
Figure 66. VLAN Network Topography Example 65
Figure 67. AN-300-RT-4L2W VLANs Menu 66
Figure 68. New VLAN Entry 66
Figure 69. LAN Menu – New VLAN 20 67
Figure 70. VPN Status Screen 68
Figure 71. VPN Status Table 68
Figure 72. VPN Tunnel Status 69
Figure 73. VPN Tunnel Status 70
Figure 74. OpenVPN Operation Diagram 71
Figure 75. OpenVPN Setup Page 72
Figure 76. Adding a New OpenVPN Client 73
Figure 77. OpenVPN Configuration File Saved 73
Figure 78. PPTP Setup Menu 74
Figure 79. VPN Passthrough Settings Screen 75
Figure 80. Gateway to Gateway 76
Figure 81. Add a New Tunnel 77
Figure 82. Local Group Setup 77
Figure 83. Remote Group Setup 78
Figure 84. IPSec Setup 79
Figure 85. Gateway to Gateway Advanced Settings 80
Figure 86. Tunnel Mode 81
Figure 87. Group Mode 82

© 2015 Araknis Networks®

Figure 88. Add a New Tunnel 83
Figure 89. Local Group Setup 83
Figure 90. Remote Client Setup 84
Figure 91. Add a New Tunnel 85
Figure 92. Tunnel Mode Advanced 86
Figure 93. IPv6 Setup Menu 87
Figure 94. IP Mode 87
Figure 95. WAN Setting 88
Figure 96. LAN Setting 89
Figure 97. Local DNS Setup Page 90
Figure 98. Local DNS Configuration 91
Figure 99. SNMP Settings Menu (SNMPv12 & SNMPv3 enabled to show available settings) 92
Figure 100. SNMPv2 & SNMPv3 Settings 92
Figure 101. Access Control Lists (ACLs) Menu 93
Figure 102. Access Control List Settings 94
Figure 103. Add New Access Control List Entry 95
Figure 105. Reset Button 96

© 2015 Araknis Networks®

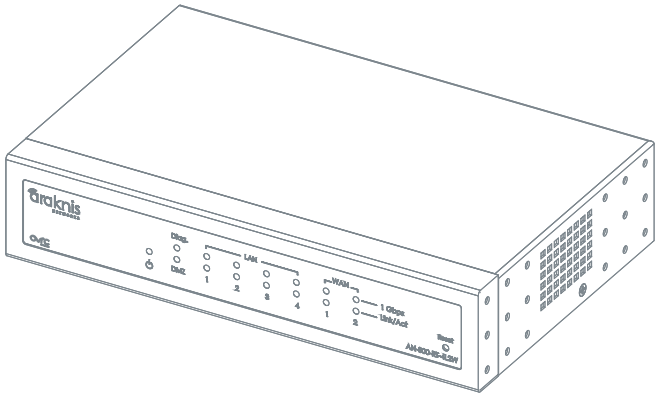
1 - Welcome to Araknis Networks

Thank you for choosing an Araknis router. With gigabit connectivity on all ports, dual-WAN capabilities, and support for a plethora of advanced features such as QoS, VLANs, VPNs and port forwarding, the Araknis 300-series router is ideal for use in both residential and commercial applications.

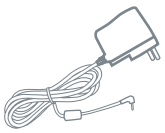
1.1 - Features

Feature	AN-300-RT-4L2W
Gigabit Ethernet	Yes
Number of LAN Interfaces	4
Number of WAN Interfaces	2
802.1Q VLANs	Yes
VPN & OpenVPN Support	Yes
Firewall	Yes
OvrC Enabled	Yes
Clients & Services Reports	Yes
Port Forwarding	Yes

2 - Package Contents

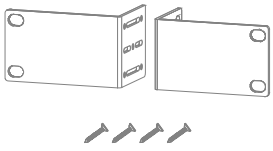


AN-300-RT-4L2W (Router)



DC Power Supply

Rubber Feet for Flat Surfaces (4)



Rack-Mount Kit (1)

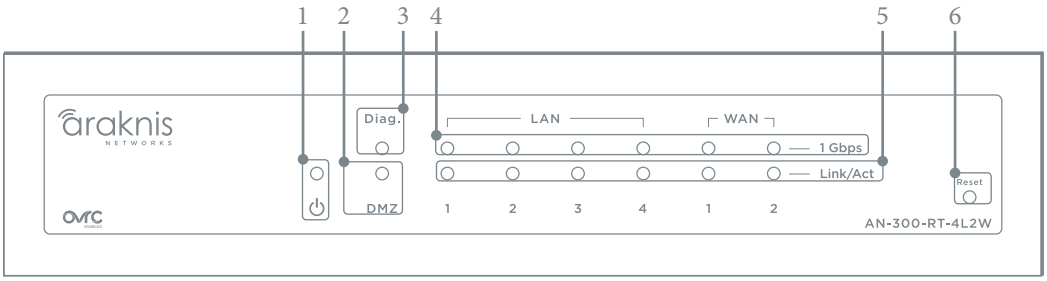
Quick Start Guide

© 2015 Araknis Networks®

3 - Hardware Overview

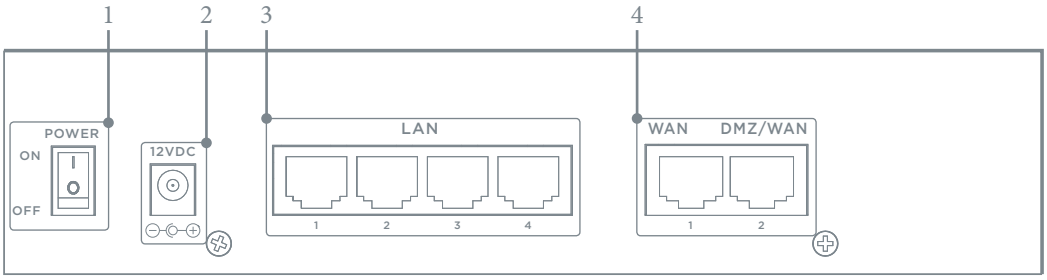
Use these images to familiarize yourself with the physical layout of the AN-300-RT-4L2W router.

3.1 - Front Panel Layout



1. **Power LED (Blue) –** Solid: system is up. Off: system is down.
2. **DMZ LED (Blue)–** Solid: WAN2 interface is configured as DMZ. Off: DMZ feature is disabled.
3. **Diag. LED (Red) –** Solid: system self-test is running. Blinking: system error. Off: system self-test successfully completed.
4. **1Gbps LED (Blue)–** Solid: port connected at 1000Mbps speed. Off: port is connected at 10/100Mbps speed.
5. **Link/Act LED (Blue)–** On: port is connected to another device. Blinking: packets are running through the port. Off: port is not connected to a device.
6. **Reset Button –** Perform a basic or full reset on the router. See section *18.1 - Resetting the Router (page 96)* for instructions.

3.2 - Rear Panel Layout



7. **Master Power Switch –** Toggle Switch for master power control.
8. **Power Jack –** Attach the included 12V DC power supply.
9. **LAN Ethernet Ports (RJ45) –** Connect Ethernet network cables routed to equipment.
10. **WAN and DMZ/WAN Ports (RJ45) –** Connect cables from the modem(s) and/or secondary network.

© 2015 Araknis Networks®

4 - Wiring Requirements

4.1 - Network Cable Requirements

Use Cat5e/6 straight-through cables throughout the installation. 568B termination is recommended

Figure 1. EIA/TIA 568B Termination Pattern

(Gold Pins Facing Up)

Pin 1	White/Orange	Pin 5	White/Blue
Pin 2	Orange	Pin 6	Green
Pin 3	White/Green	Pin 7	White/Brown
Pin 4	Blue	Pin 8	Brown

Note – Maximum cable length is 328′ (100m). A repeater device is required for longer runs.

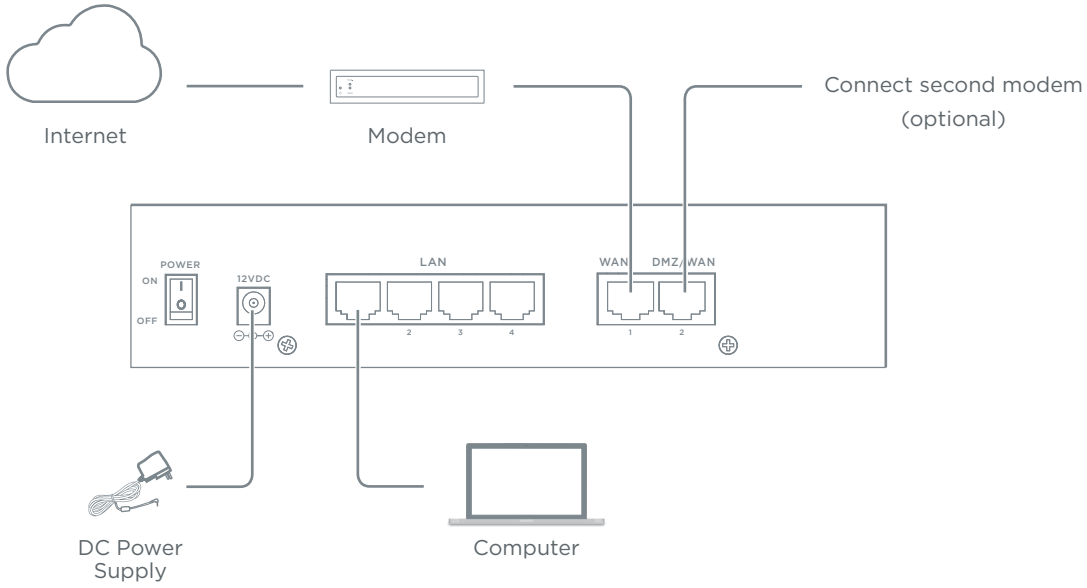
4.2 - Power Requirements

Use only the included power supply. Specifications:

- **AC Outlet –** 100-240V AC, 50/60Hz
- **DC Input –** 12V DC 1A

4.3 - Wiring Diagram

Figure 2. Network Wiring Connection Diagram



© 2015 Araknis Networks®

5 - Mounting Options

5.1 - Rack Mount

Figure 3. Rack Mounting Ear Installation

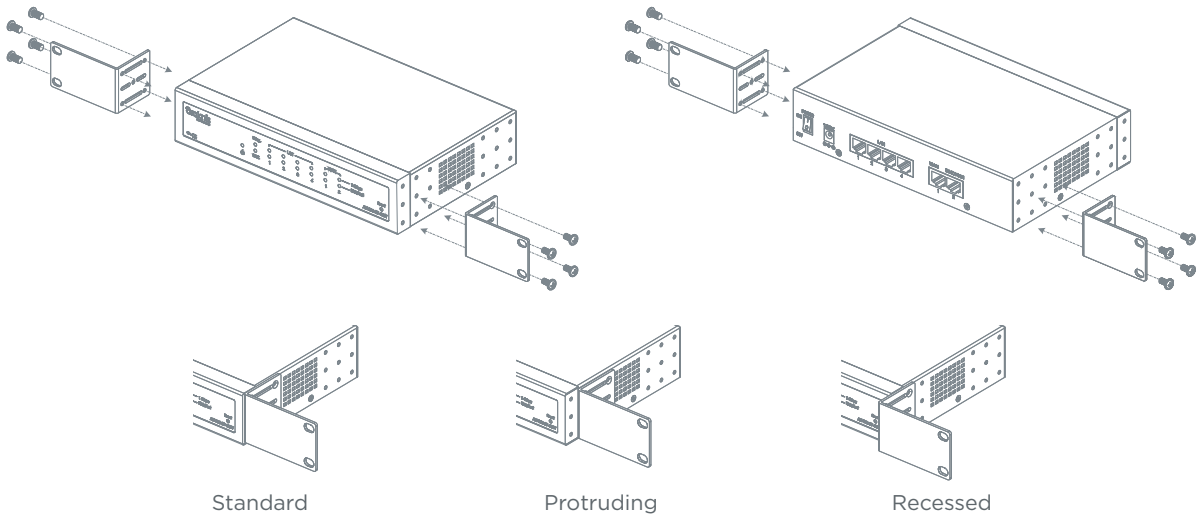
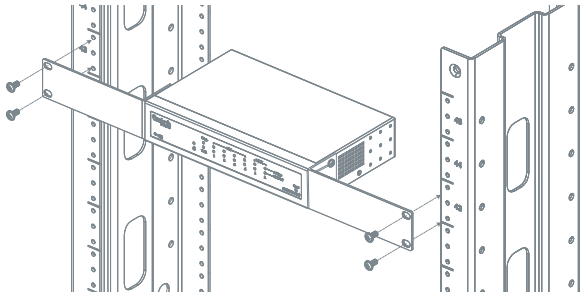


Figure 4. Installing the Router in a Rack



5.1.1 - Rack Mounting Guidelines

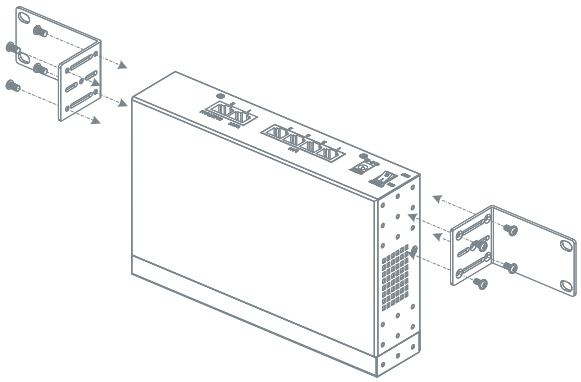
- **Elevated Operating Ambient –** If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the operating ambient temperature of 104°F.
- **Reduced Airflow –** Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- **Mechanical Loading –** Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- **Circuit Overloading –** Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing –** Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

© 2015 Araknis Networks®

5.2 - Wall Mount

The rack mounting ears can be used for wall mounting. Secure the router to the wall using fasteners rated for the wall material (not included).

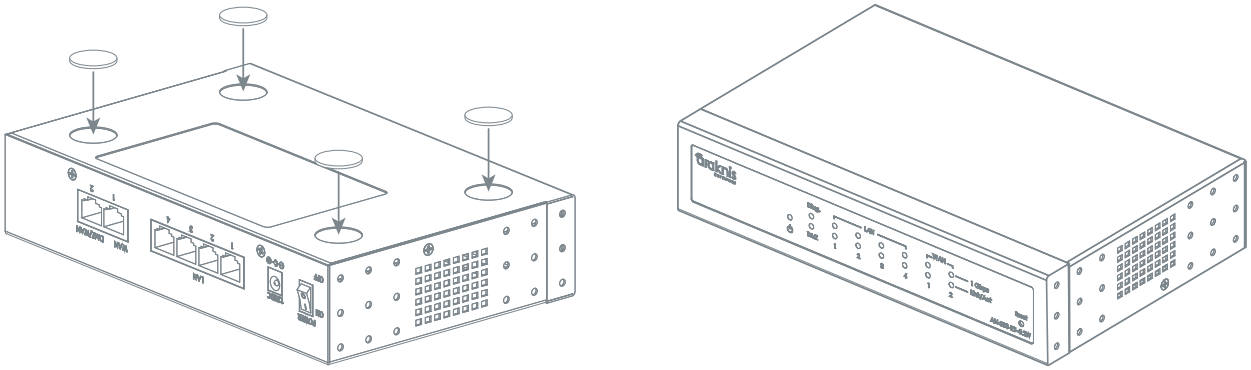
Figure 5. Connecting Mounting Ears for Wall Mount Installation



5.3 - Shelf Mount

Attach the included rubber feet to the bottom of the router for shelf mounting. The feet will prevent unwanted vibration and movement of the router.

Figure 6. Shelf Mounting Diagram



6 - Installation Instructions

1. Unpack the router. Confirm that all contents are included (see *2 - Package Contents (page 10)*).
2. Mount the router in the desired location (see *5 - Mounting Options (page 13)*)
3. Connect the router to the network wiring (see *4 - Wiring Requirements (page 12)*).
4. Connect your computer to the network and complete quick setup (see next section).

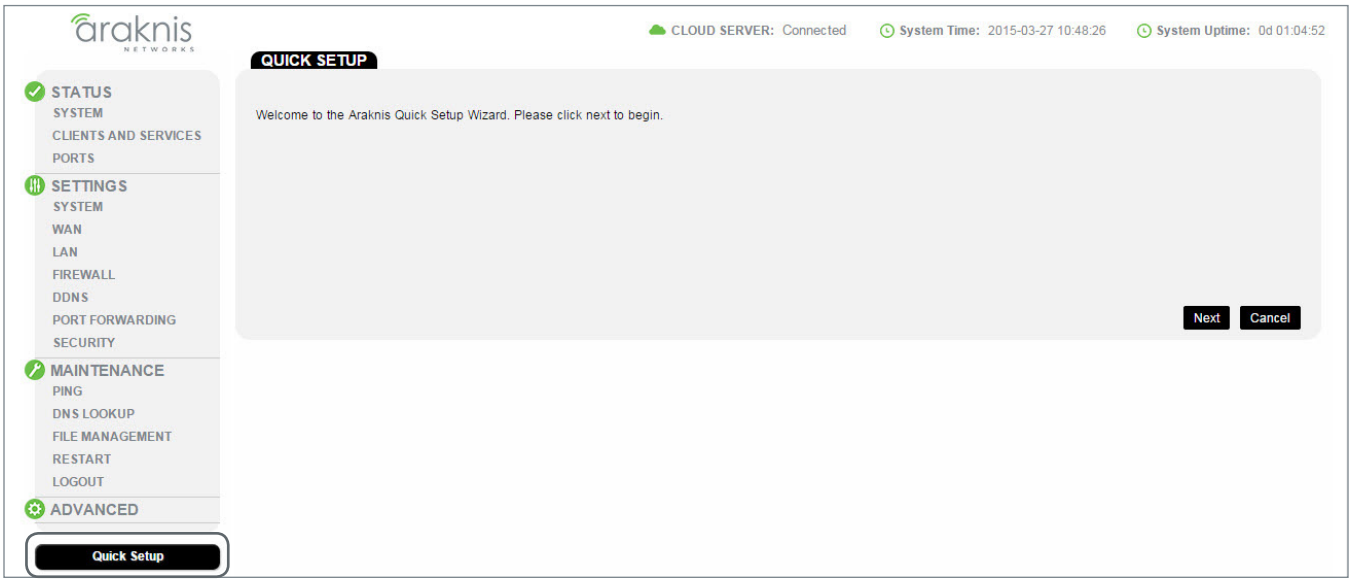
© 2015 Araknis Networks®

7 - Logging Into the Web Interface

1. Set the Ethernet adapter on your computer to DHCP mode or configure the adapter with a static IP address:
   - **IP Address:** ***192.168.1.x***
     (x=any number from 2 to 99)
   - **Subnet Mask:** ***255.255.255.0***
2. Open a web browser and enter ***http://192.168.1.1*** in the address bar.
3. Log in using the default credentials:
   - **Username:** araknis
   - **Password:** araknis

8 - Quick Setup

Figure 7. Quick Setup



Click the Quick Setup button in the left bar to begin. Use Quick Setup to configure:

- System name
- System IP address
- WAN 1 and WAN 2 settings
- DHCP servers
- Port forwarding

Use the menus in the web interface to change additional settings.

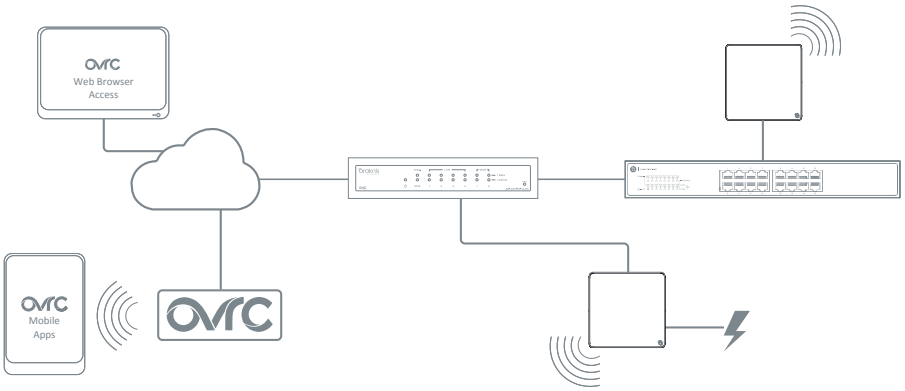
© 2015 Araknis Networks®

9 - OvrC™ Access

OvrC provides remote device management, real-time notifications, and intuitive customer management, right from your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS required. To add this device to your OvrC account:

1. Connect the router to the Internet.
2. Log into OvrC (www.ovrc.com) or load the OvrC app, available for iOS and Android.
3. Add the device (MAC address and Service Tag number is needed for authentication).

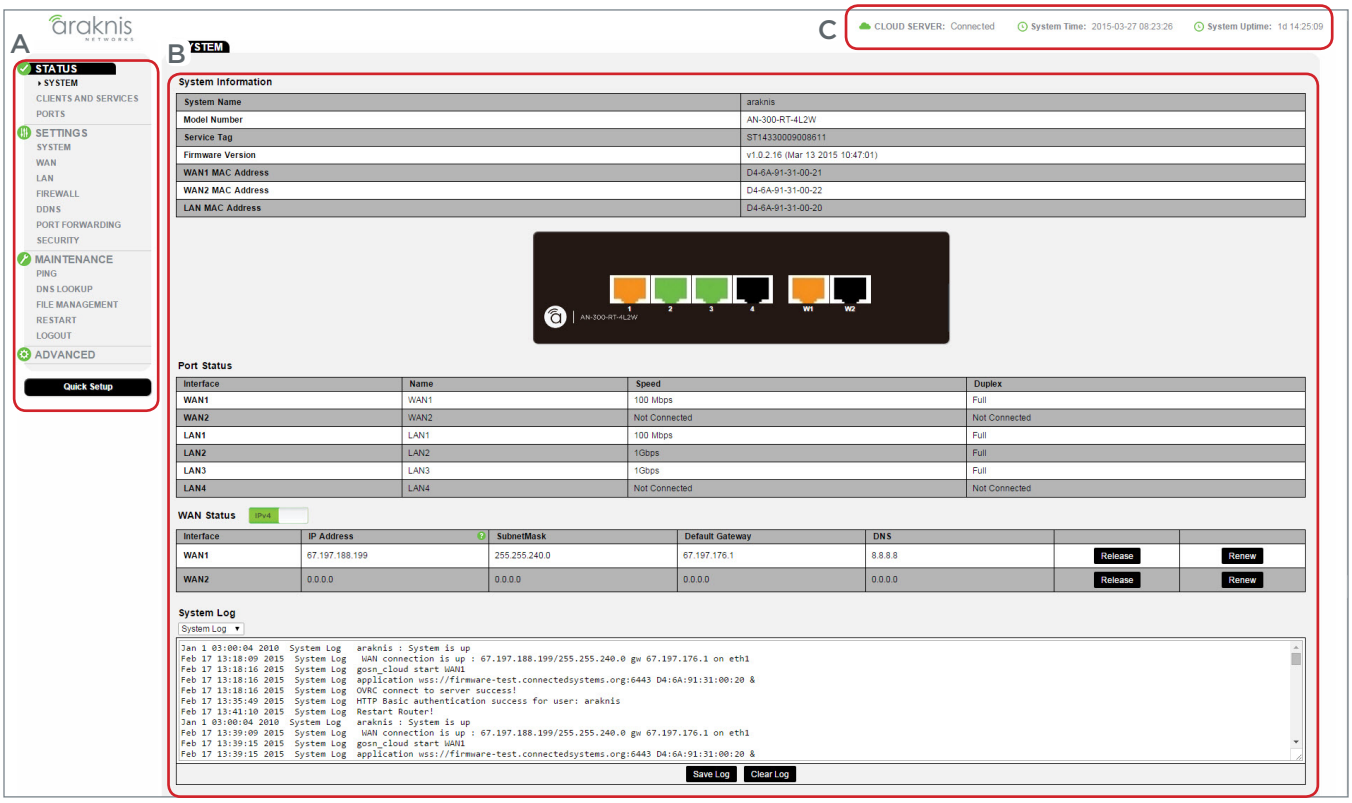
Figure 8. OvrC Diagram



© 2015 Araknis Networks®

10 - Menu Overview

Figure 9. Menu Overview (System Status Screen)



- **A - Main Navigation Menu**
  Use the submenus under the Status, Settings, Maintenance, and Advanced headings to configure and maintain the router. Click **Quick Setup** to configure basic settings (see *8 - Quick Setup (page 15)*).

- **B - Main Window**
  The main window displays the currently selected submenu.

- **C - Top Bar**
  The top bar displays the current connection status to the OvrC server, the current system time, and the current system uptime in DAYS:HOURS:MINUTES.

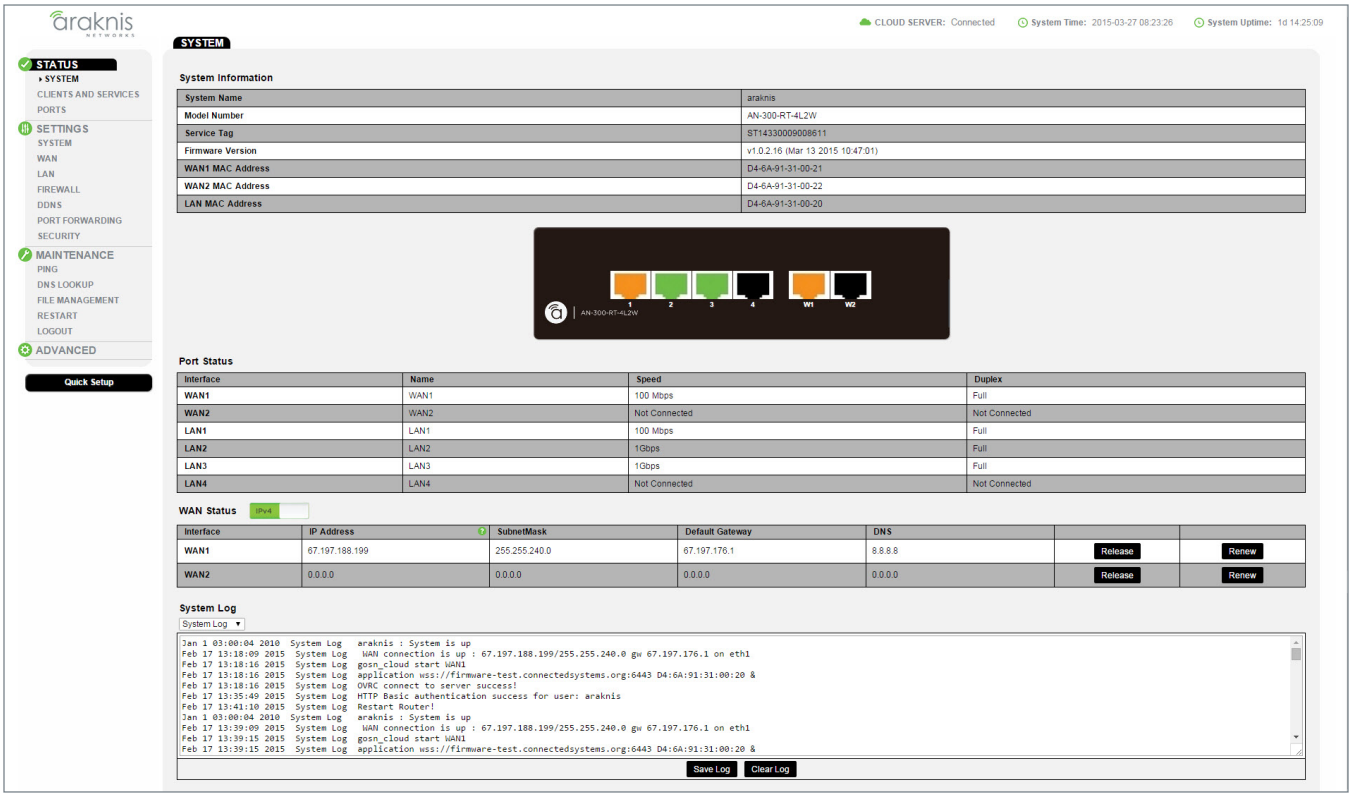
© 2015 Araknis Networks®

11 - Status

The System Status screen provides a real-time summary of router system information, and is the first screen that appears when you log into the router web interface. Use the screen to verify settings and operation of your device.

11.1 - System

Figure 10. System Status Screen



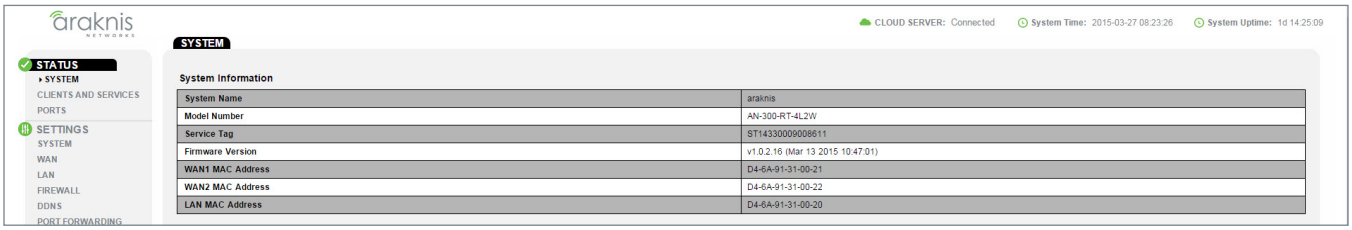
Path – Status, System

© 2015 Araknis Networks®

11.1.1 - System Information

See current information for identifying the router.

Figure 11. System Information



Path – Status, System, System Information

Parameters –

- **System Name –** Name assigned to the system. Used for configured name access.
- **Model Number –** Router part number (AN-300-RT-4L2W).
- **Service Tag –** Internal tracking number used to track every product sold by Araknis Networks. The service tag number must be used to configure OvrC access.
- **Firmware Version –** Current version of firmware installed on the router.
- **WAN1 MAC Address –** Media Access Control (MAC) address for WAN1 port.
- **WAN2 MAC Address –** MAC address for WAN2 port.
- **LAN MAC Address –** MAC address of the device. The MAC address must be used to configure OvrC access.

11.1.2 - Port Status Display

Use the image to quickly determine the status of each port on the router.

Figure 12. Port Status Display

Path – Status, System

Parameters –

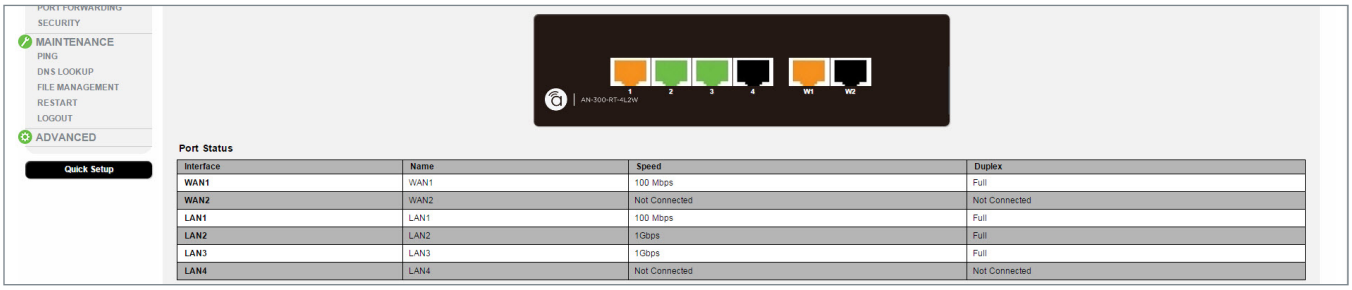
- **Black –** Not in use or the connected device is not linking to the network.
- **Orange –** 100Mbps connection is active.
- **Green –** 1Gbps connection is active.
- **Red –** Port has been disabled by the user in the web interface settings (see *12.3.1 - Port Settings (page 37)*).

© 2015 Araknis Networks®

11.1.3 - Port Status

See current information about the status of each router port.

Figure 13. Port Status



Path – Status, System

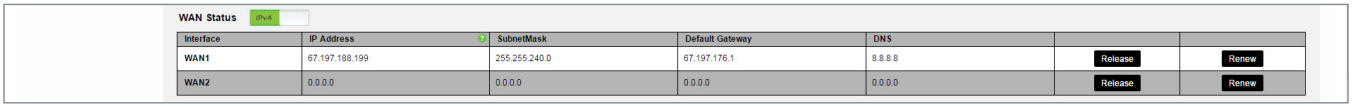
Parameters –

- **Interface –** List of all ports on the router.
- **Name –** Name used to identify each port.
- **Speed –** User-selected or device-negotiated port speed.
- **Duplex –** Displays the duplex mode of the port.

11.1.4 - WAN Status

See current information about the WAN interface status.

Figure 14. System Information



Path – Status, System, System Information

Parameters –

> **Note –** Click the green IPv4 button to toggle the table to IPv6 mode.

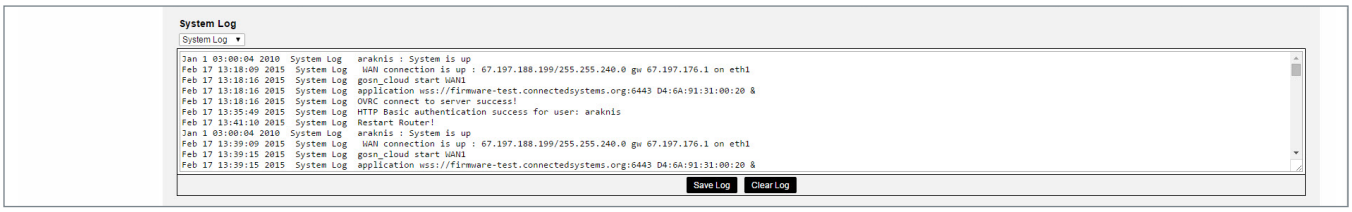
- **Interface –** WAN1 or WAN2.
- **IP Address–** WAN IP address of the connection.
- **SubnetMask –** WAN subnet mask.
- **Default Gateway –** WAN gateway IP address.
- **DNS –** WAN Domain Name Server.

© 2015 Araknis Networks®

11.1.5 - System Log

See recorded activities and status changes. Use the dropdown box to select from ALL, System Log, Access Log, Firewall Log, or VPN Log.

Figure 15. System Information



Path – Status, System, System Information

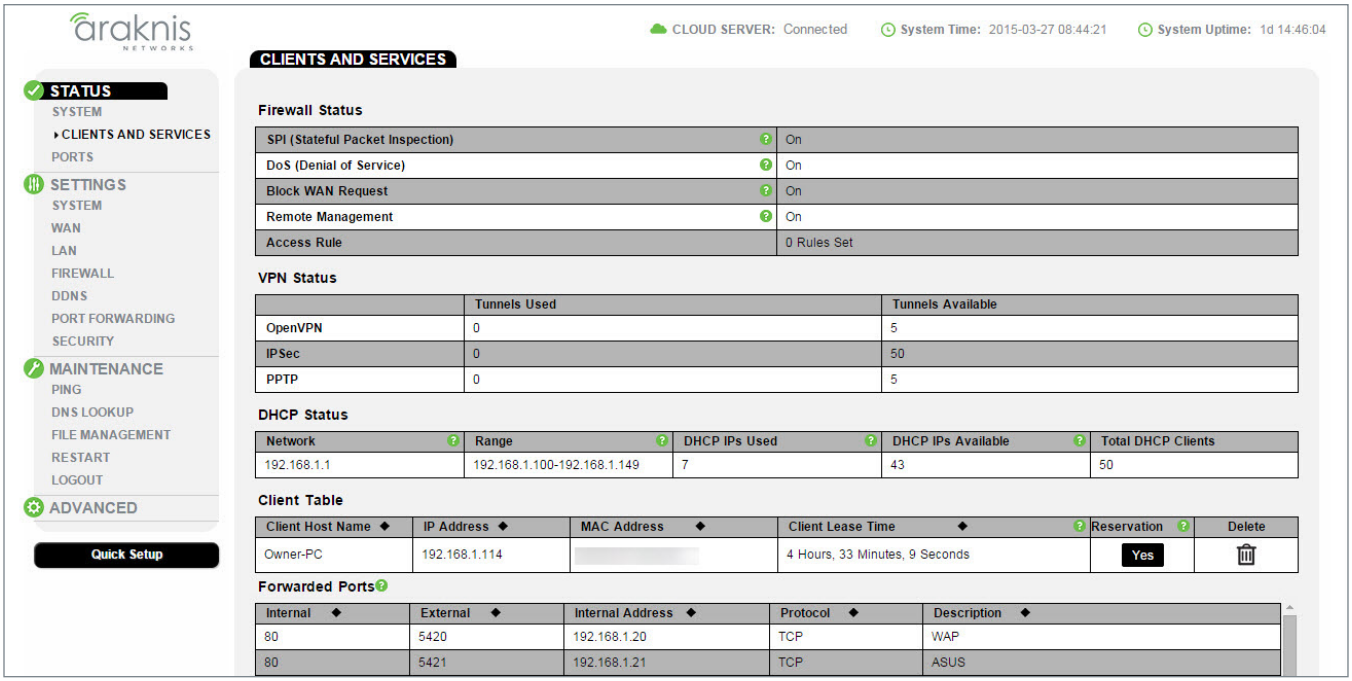
Parameters –

- **Save Log –** Click to save a copy of the currently viewed log to your PC.
- **Clear Log –** Click to clear all current log entries.

© 2015 Araknis Networks®

11.2 - Clients and Services

Figure 16. Clients and Services Status Screen

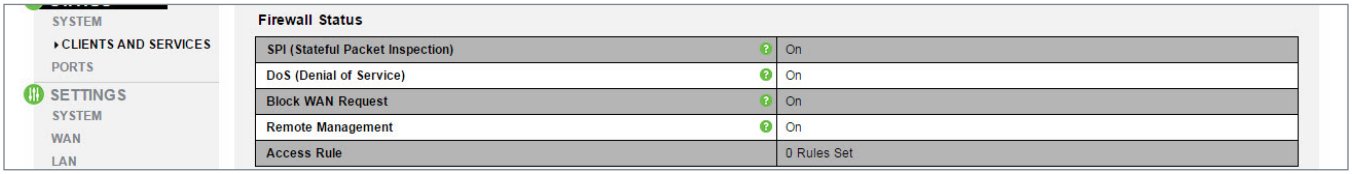


Path – Status, Clients and Services

11.2.1 - Firewall Status

See the current basic firewall security settings in use.

Figure 17. Firewall Status



Path – Status, Clients and Services

Parameters –

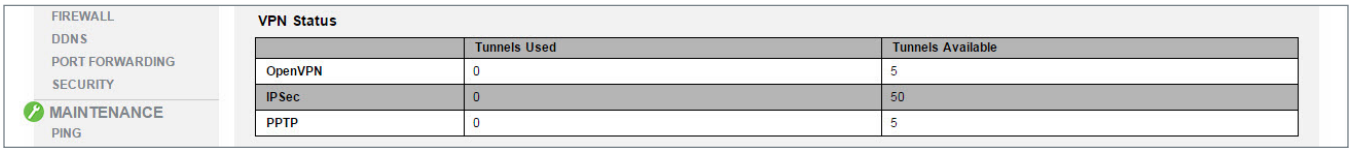
- **SPI (Stateful Packet Inspection) –** See whether the SPI firewall setting is on or off.
- **DoS (Denial of Service) –** See whether the DoS firewall setting is on or off.
- **Block WAN Request –** See whether the Block WAN Request firewall setting is on or off.
- **Remote Management –** See whether the Remote Management firewall setting is on or off.
- **Access Rule –** See how many access rules are currently enabled.

© 2015 Araknis Networks®

11.2.2 - VPN Status

See information about current VPN availability and usage.

Figure 18. VPN Status



	Tunnels Used	Tunnels Available
OpenVPN	0	5
IPSec	0	50
PPTP	0	5

Path – Status, Clients and Services

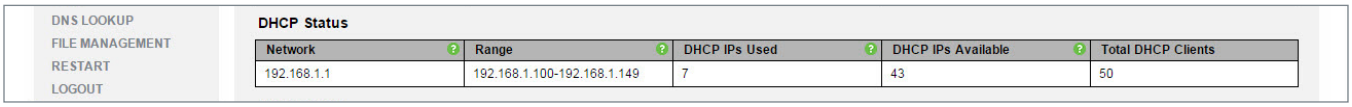
Parameters –

- **Tunnels Used –** Number of OpenVPN, IPSec, and PPTP tunnels currently in use.
- **Tunnels Available –** Total number of tunnels currently available. The router can support a maximum of five OpenVPN, fifty IPSec, and five PPTP tunnels.

11.2.3 - DHCP Status

See current information about the router's DHCP server.

Figure 19. DHCP Status



Network	Range	DHCP IPs Used	DHCP IPs Available	Total DHCP Clients
192.168.1.1	192.168.1.100-192.168.1.149	7	43	50

Path – Status, Clients and Services

Parameters –

- **Network –** Gateway IP address for the network.
- **Range –** IP address range configured for the DHCP server.
- **DHCP IPs Used –** Number of DHCP IP addresses currently assigned to LAN clients.
- **DHCP IPs Available –** Number of DHCP IP addresses currently available and not assigned to clients.
- **Total DHCP Clients –** Sum of available DHCP IP addresses (used + available).

© 2015 Araknis Networks®

11.2.4 - Client Table

See information about clients currently connected to the router's DHCP server. Each entry line displays the status of a client.

Figure 20. Client Table

Path – Status, Clients and Services

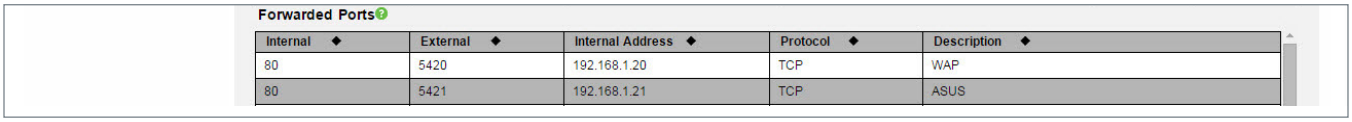
Parameters –

- **Client Host Name –** Name of the connected device.
- **IP Address –** IP address assigned to the connected device.
- **MAC Address –** MAC address of the connected device.
- **Client Lease Time –** Amount of time the client has been assigned its IP address.
- **Reservation –** Indicates whether the IP address has been reserved for the client. The field will display *Reserved* or a **Yes** button. Click the **Yes** button to reserve the address.
- **Delete –** Click the **Trashcan** to remove an entry. The client will lose its current lease.

11.2.5 - Forwarded Ports

See all of the ports currently forwarded in the router.

Figure 21. Forwarded Ports



Path – Status, Clients and Services

Parameters –

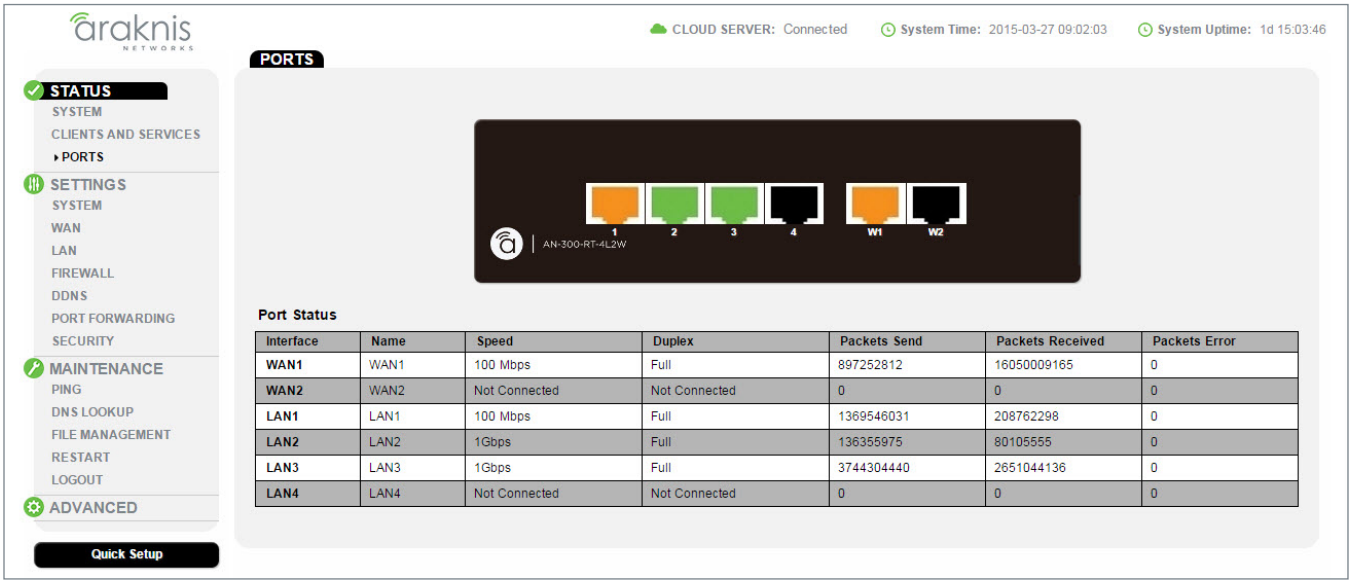
- **Internal –** Port assigned to the LAN device.
- **External –** Port that WAN devices connect to in order to communicate to the devices Internal port.
- **Internal Address –** IP address of the port-forwarded device.
- **Protocol –** Configured protocols for the rule (TCP, UDP, or Both).
- **Description –** Used to easily identify the port.

© 2015 Araknis Networks®

11.3 - Ports

See detailed information about the physical ports on the router.

Figure 22. Ports Status Screen



Path – Status, Ports

11.3.1 - Port Status

Parameters –

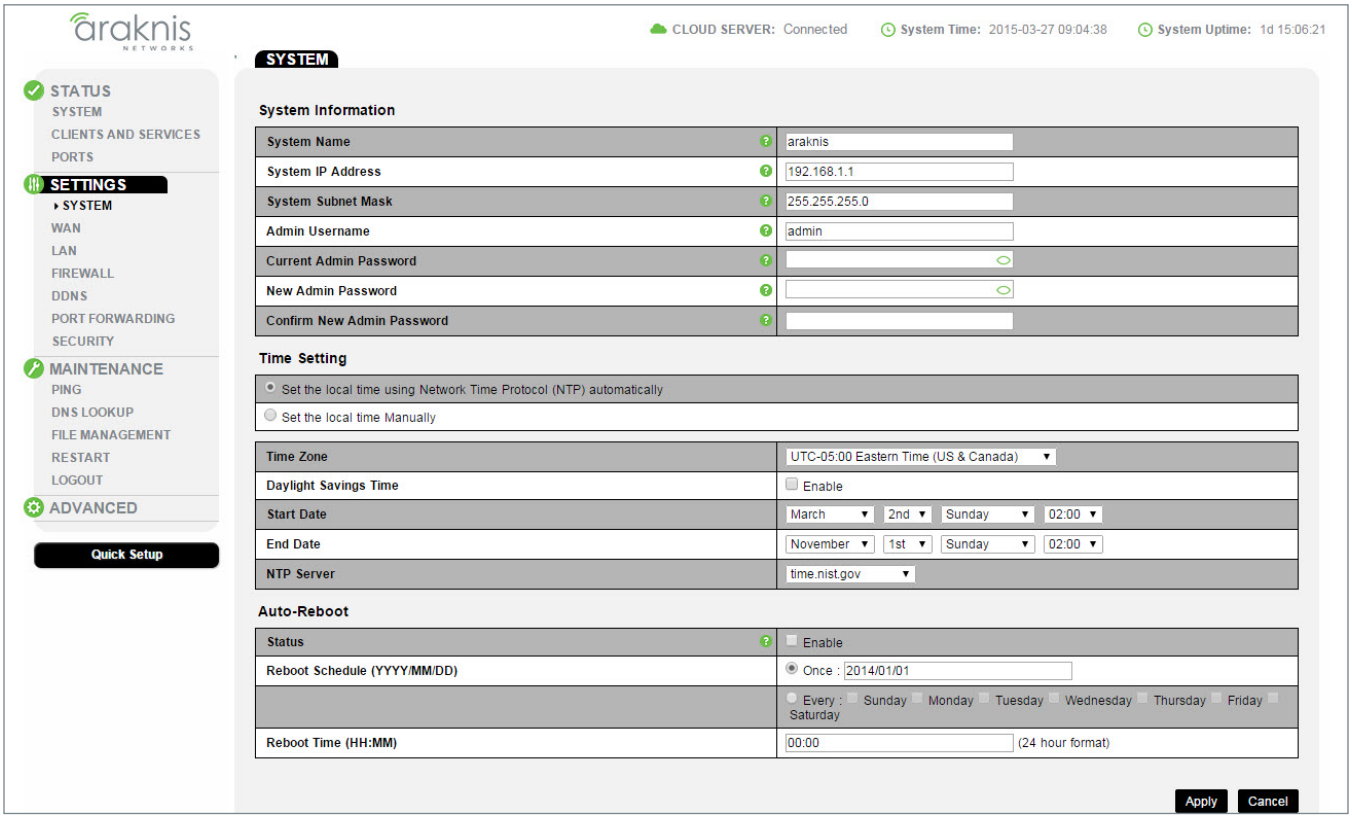
- **Interface –** List of all ports on the router.
- **Name –** Name used to identify each port.
- **Speed –** Traffic speed on the port.
- **Duplex –** Displays the duplex mode of the port.
- **Packets Send –** Total packets sent on the port.
- **Packets Received –** Total packets received on the port.
- **Packets Error –** Total number of packet errors on the port. Packet errors indicate that the router is dropping packets (not reading them), or that they are being discarded by the router.

© 2015 Araknis Networks®

12 - Settings

12.1 - System

Figure 23. System Settings Menu

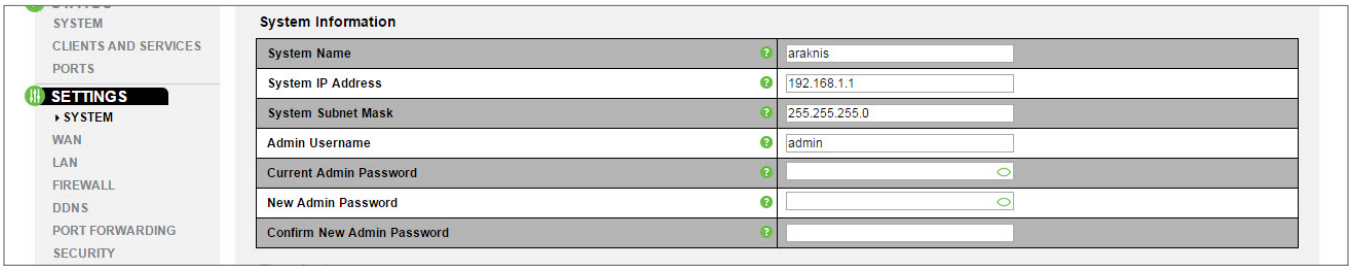


Path – Setting, System

© 2015 Araknis Networks®

12.1.1 - System Information

Figure 24. System Information



Path – Status, System, System Information

Parameters –

- **System Name –** Enter a meaningful name such as ***SmithRouter***. Limited to 32 characters, including spaces.
  Default: araknis
- **Admin Username –** Enter a new username for logging into the router. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.
  Default: araknis
- **Admin Current Password –** Enter the current login password when changing the password.
  Default: araknis
- **Admin New Password –** Enter a new login password. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.
- **Confirm Admin New Password –** Confirm a new login password (enter same password as above).

> **Note –** Place your mouse on the eye icon to the right of the field to display the hidden password characters.

Parameters –

Configuration Instructions –

1. Change the desired settings.
2. Enter the current administrator password.
3. Click Apply to save the new settings. You may be prompted to log back into the router after making changes in this menu.

© 2015 Araknis Networks®

12.1.2 - Time Setting

Figure 25. Time Setting Menu

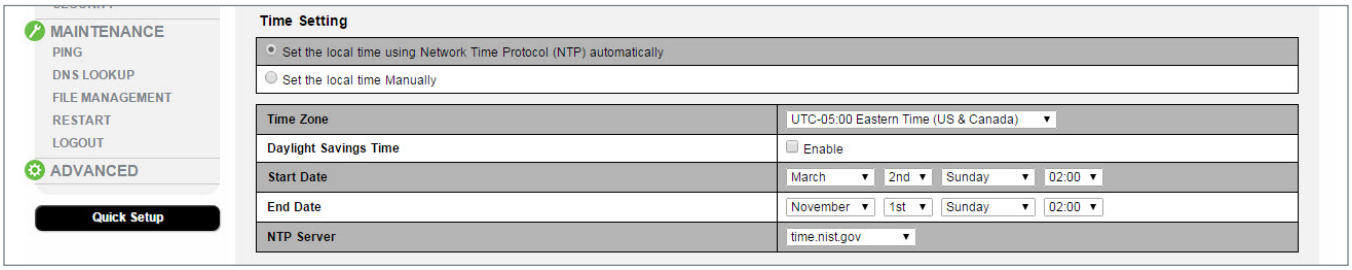
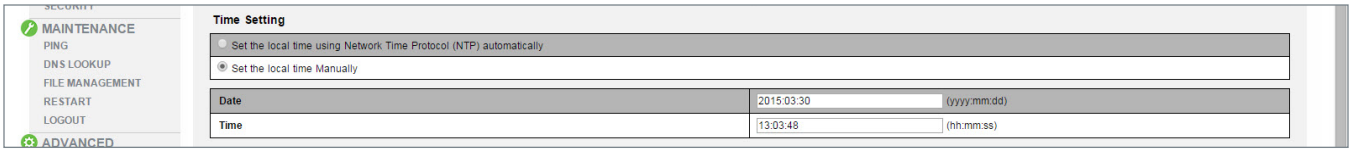


Figure 26. Manual Time Setting



Path – Status, System, System Information

Parameters –

- **Auto/Manual Time Setting –** Select whether to set the local time using Network Time Protocol (NTP) (automatically) or manually.
  Default: Set the local time using Network Time Protocol (NTP) automatically
  - **Set the local time Manually –** Select to manually set date and time.
    - **Date –** Enter the year, month and date.
    - **Time –** Enter the hour and minutes for the correct current time. Use a mobile device or satellite clock for accuracy.
- **Time Zone –** Select the appropriate time zone from the drop-down.
- **Enable Daylight Saving –** Select to enable. DST start/end can change from year to year. Be sure to update this information.
  - **Start** – Select the month, date, day and time Daylight Saving Time starts.
  - **End** – Select the month, date, day and time Daylight Saving Time ends.
- **NTP Server –** Server providing time updates for automatic time setting. The default setting is sufficient for most applications.
  Default: time.nist.gov

Configuration Instructions –

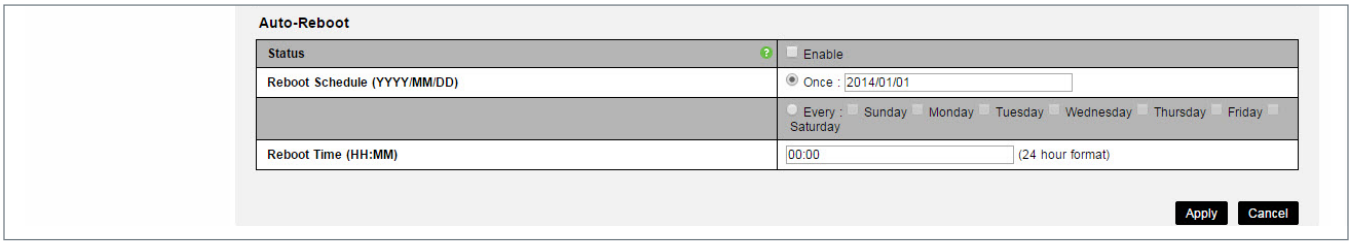
1. Change the desired settings.
2. Click Apply to save the new settings.

© 2015 Araknis Networks®

12.1.3 - Auto-Reboot

Use the auto-reboot feature to reset your router on a regular basis. This will help ensure trouble-free operation.

Figure 27. Auto Reboot Menu



Path – Status, System, System Information

Parameters –

- **Status –** Click to check the box and enable auto-reboot.
  Default: Disabled (unchecked).
- **Reboot Schedule (YYYY/MM/DD) –** Once : Every : Sunday Monday Tuesday Wednesday Thursday Friday Saturday
- **Reboot Time (HH:MM) –** (24 hour format)

Configuration Instructions –

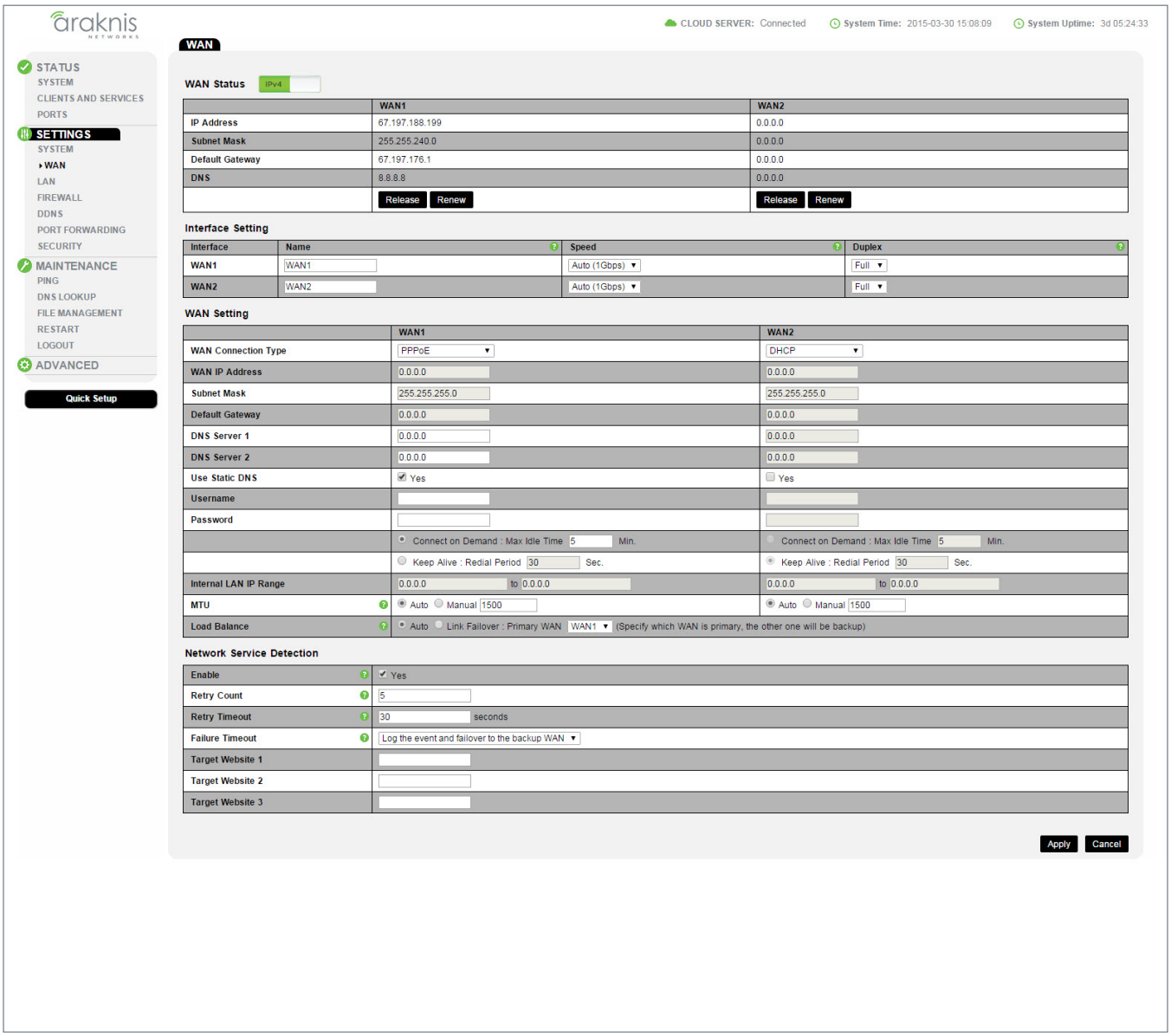
1. Change the desired settings.
2. Click Apply to save the new settings.

© 2015 Araknis Networks®

12.2 - WAN

Use the WAN Settings menu to configure the router's connection(s) to the Internet through WAN ports 1 and 2.

Figure 28. WAN Settings Menu

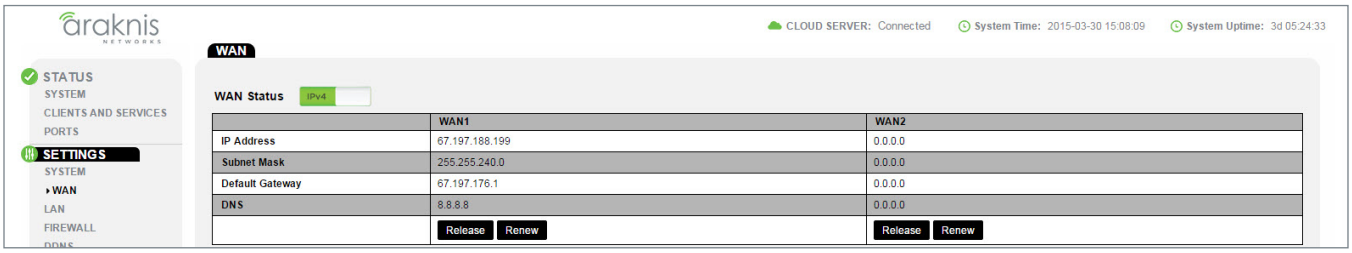


Path – Setting, WAN

© 2015 Araknis Networks®

12.2.1 - WAN Status

Figure 29. WAN Status



Path – Status, System, System Information

Parameters –

> **Note –** Click the green IPv4 button to toggle the table to IPv6 mode.

- **IP Address –** IP address issued to the WAN interface.
- **Subnet Mask –** Subnet mask of the WAN interface.
- **Default Gateway –** Default gateway of the WAN interface.
- **DNS –** Domain Name Server of the WAN interface.
- **Release –** Click to release the current WAN IP address back to the DHCP pool and receive a new one.
- **Renew –** Click to renew the current WAN DHCP connection. The WAN IP address may or may not change.

Configuration Instructions –

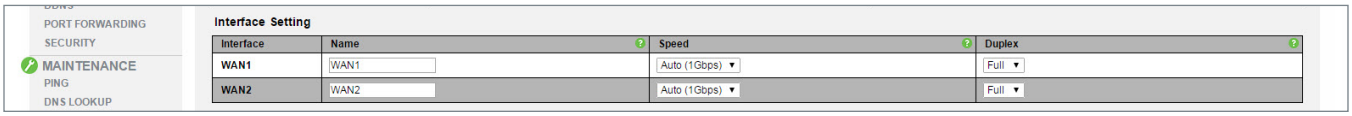
1. Click the associated button to **Release** or **Renew** the IP address for the interface.
2. Click **Confirm** or **Cancel** in the confirmation box.
3. Click Apply to save the new settings.

© 2015 Araknis Networks®

12.2.2 - Interface Setting

Set the speed and duplex mode for each WAN interface.

Figure 30. System Information



Path – Status, System, System Information

Parameters –

- **Interface –** WAN1 or WAN2.
- **Name –** Change the name of the interface for easier identification.
  Default: WAN1/WAN2.
- **Speed –** Select a speed for the interface. Options: Auto (1Gbps), 100 Mbps, 10 Mbps, Disabled
  Default: Auto (1Gbps).
- **Duplex –** Select whether the port is set to full- or half-duplex mode. Cannot be changed when Speed is set to Auto.
  Default: Full.

> **Note –** A full-duplex port can both transmit and receive data on the port simultaneously. A half-duplex port can only receive or transmit data in sequence.

Configuration Instructions –

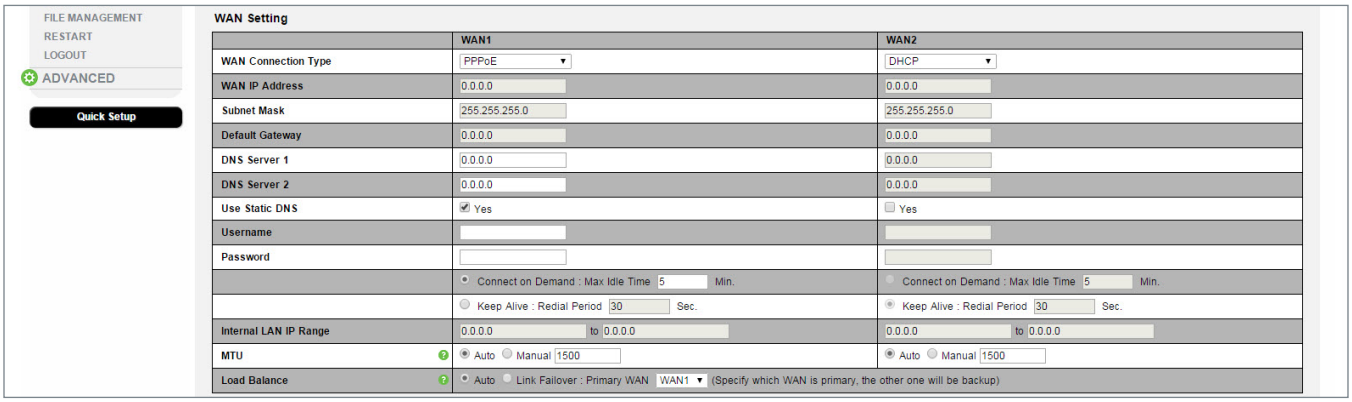
1. Change the desired settings.
2. Click Apply to save the new settings.

© 2015 Araknis Networks®

12.2.3 - WAN Setting

Configure each WAN connection.

Figure 31. WAN Settings



Path – Status, System, System Information

Parameters –

- **WAN Connection Type –** Set the connection type for the interface. Options: DHCP, Static IP, PPPoE, PPTP, Transparent Bridge. See section *12.2.3.1 - Understanding WAN Connection Types and Setup (page 34)* for more information about WAN connection types.
  Default: DHCP
- **WAN IP Address –** Set the WAN IP address of the interface. Not used in DHCP or PPPoE mode.
- **Subnet Mask –** Set the subnet mask for the interface. Not used in DHCP or PPPoE mode.
  Default: 255.255.255.0
- **Default Gateway –** Set the default gateway IP address for the interface. Not used in DHCP or PPPoE mode.
- **DNS Server 1 –** Set the primary Domain Name Server for the interface.
- **DNS Server 2 –** Set the secondary Domain Name Server for the interface.
- **Use Static DNS –** Select if static DNS is used. Only for DHCP and PPPoE modes.
  Default: Enabled
- **Username –** Enter the username for the connection. Only for PPPoE and PPTP modes.
- **Password –** Enter the password for the connection. Only for PPPoE and PPTP modes.
- **Connect on Demand/Keep Alive –** Select whether the WAN connection opens when needed or is connected at all times. Only for PPPoE and PPTP modes.
  Default: 5 minutes
- **Internal LAN IP Range –** LAN IP addresses given access to the WAN connection. Only for Transparent Bridge mode.
- **MTU–** Maximum Transmission Unit specifies the largest packet or frame size that can be transmitted across the WAN interface. Use the Auto setting unless the ISP specifies to use a certain MTU value.
  Default: Auto

© 2015 Araknis Networks®

- **Load Balance –** Configure traffic spillover for each WAN interface. Only for installations utilizing both WAN connections. See section *12.2.3.2 - Understanding Load Balancing (page 34)* for explanation and configuration instructions.
  Default: Auto

12.2.3.1 - Understanding WAN Connection Types and Setup

- **DHCP (default) –** The ISP issues a dynamic WAN IP address to the modem and router that can change at any time. Standard for most residential Internet connections. This connect type is usually "set and forget"; no additional WAN setup is required after connecting the modem to router port WAN 1 or WAN 2.
- **Static IP –** The ISP issues a static IP address for the modem and router that will not change. This connection type is standard in most commercial Internet connections and anywhere the user has purchased an IP address. The ISP provides the IP address to the network administrator, who configures the address in the router.
- **PPPoE –** Point-to Point Protocol over Ethernet is most applicable in situations with DSL providers. The system pings the DSL server to gather the IP settings. The ping comes with username and password authentication.
- **PPTP –** Point-to-Point Tunneling Protocol establishes a static connection to a WAN address using a VPN service.
- **Transparent Bridge –** Setting the router's WAN port to Transparent Bridge mode causes the incoming WAN connection to bypass the router's network address translation (NAT). Transparent bridge mode is important to use when there are multiple routers in one network because it reduces NAT complexity.

12.2.3.2 - Understanding Load Balancing

- **Auto –** The router balances the traffic across both ports. This combines the upload/download of both ports together for faster overall throughput. If one connection goes down, the network will remain connected to the Internet on the remaining connection. This is the default and recommended setting.

> **Pro Tip –** VLANs can be configured to remain connected to one WAN connection even when Load Balancing is to ***auto***. See section *16 - VLANs (page 64)* for more information about configuring VLANs.

- **Link Failover –** The router uses a single WAN port. If Internet access is lost on that port, traffic is switched to the other port. This setting is useful, for example, if the backup Internet connection is more expensive to operate like a backup satellite service for a hardwired primary connection. Network service detection is used to monitor the ports for operation. See section *12.2.4 - Network Service Detection (page 35)* for more information.

Configuration Instructions –

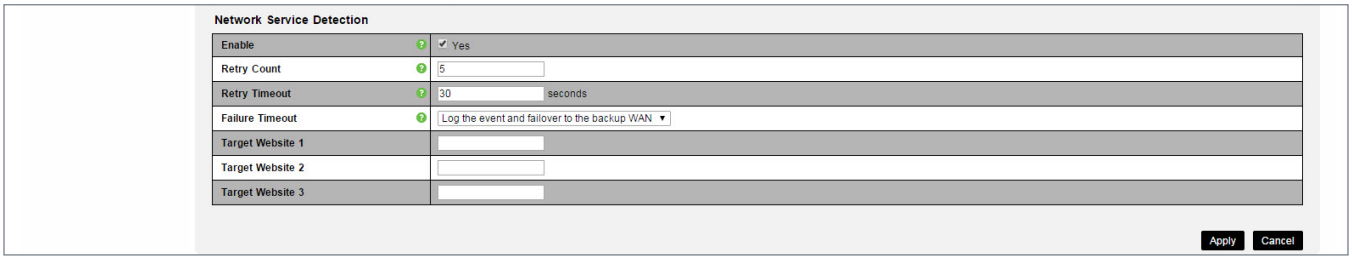
1. Select the connection mode for the WAN interface being configured.
2. Enter additional settings for the selected mode as required.
3. Click Apply to save the new settings. The router may need to reboot for the new settings to take effect.

© 2015 Araknis Networks®

12.2.4 - Network Service Detection

This feature monitors the connection from the router to three target websites on the Internet. If the router cannot ping all three sites, you can set the device to either log the event in the system log or log it and switch over to the backup WAN if both WAN1 and WAN2 ports are connected.

Figure 32. Network Service Detection Menu



Path – Status, System, System Information

Parameters –

- **Enable –** Check the box to enable detection.
  Default: Disabled
- **Retry Count –** Retry Timeout seconds – Set how many times the router will attempt to ping after a failed attempt before acting.
  Default: 5
- **Failure Timeout –** Set how long the router waits between pings.
  Default: 30 seconds
- **Target Website 1/2/3 –** Set the three websites the router will ping. Configure three sites for the best performance. The feature will work with less, but this is not recommended.

Configuration Instructions –

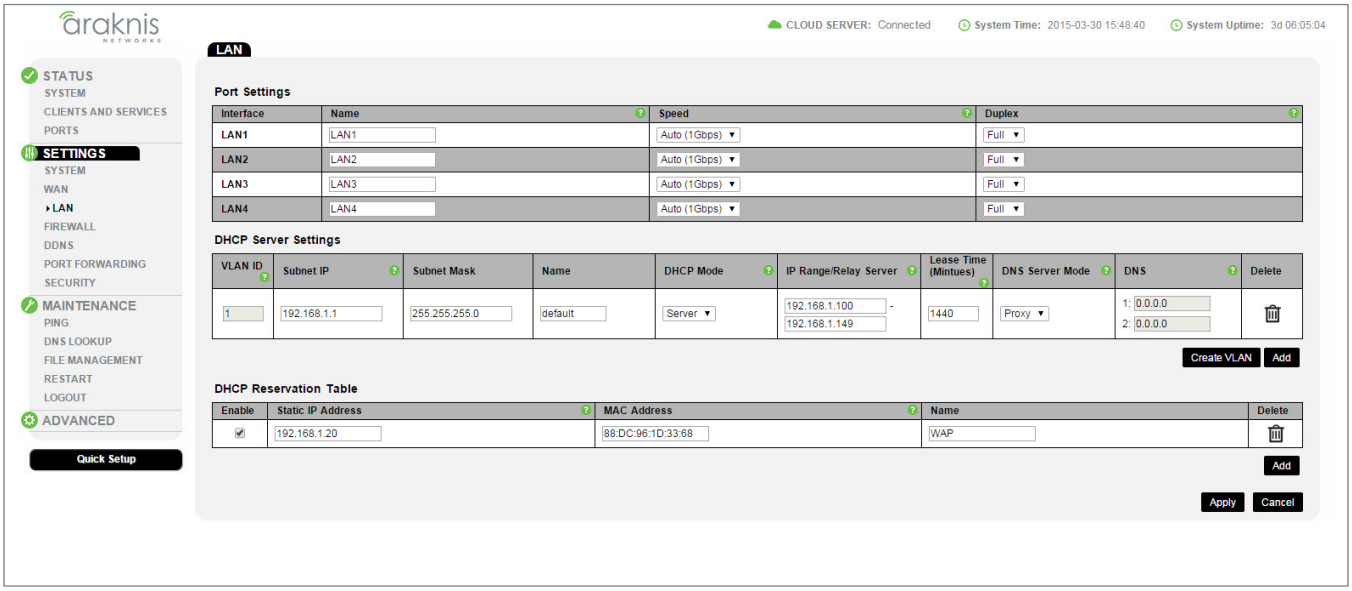
1. Change the desired settings.
2. Click Apply to save the new settings.

© 2015 Araknis Networks®

12.3 - LAN

Use the LAN menu page to configure settings for the four local area network ports on the router.

Figure 33. LAN Settings Menu

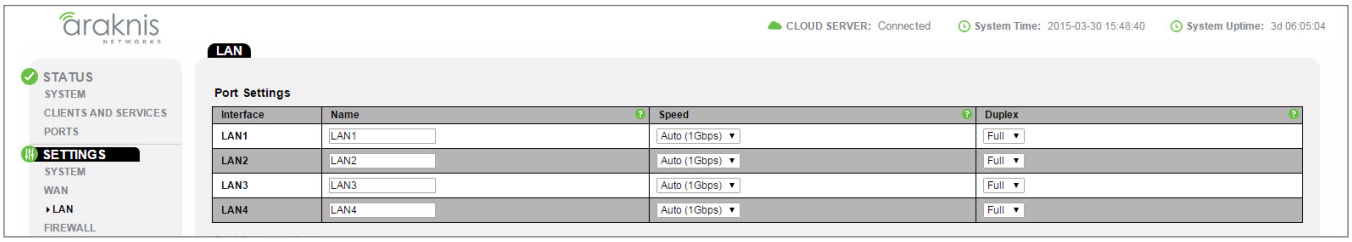


Path – Settings, LAN

© 2015 Araknis Networks®

12.3.1 - Port Settings

Figure 34. Port Settings Menu



Path – Status, System, LAN

Parameters –

- **Interface –** LAN port being configured.
- **Name –** Change the name of the interface for easier identification.
  Default: LAN1/LAN2/LAN3/LAN4.
- **Speed –** Select a speed for the interface. Options: Auto (1Gbps), 100 Mbps, 10 Mbps, Disabled
  Default: Auto (1Gbps).
- **Duplex –** Select whether the port is set to full or half duplex mode. Cannot be changed when Speed is set to Auto.
  Default: Full.

> **Note –** A full-duplex port can both transmit and receive data on the port simultaneously. A half-duplex port can only receive or transmit data in sequence.

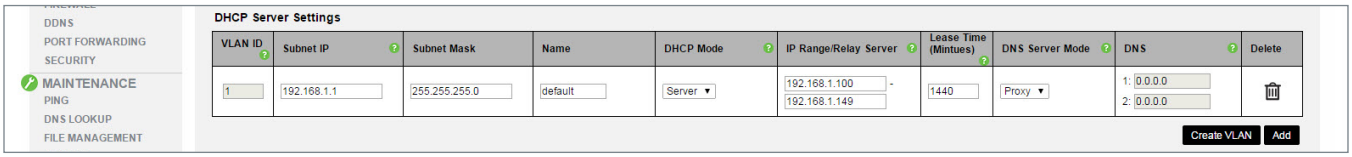
Configuration Instructions –

1. Change the desired settings.
2. Click Apply to save the new settings.

© 2015 Araknis Networks®

12.3.2 - DHCP Server Settings

Figure 35. DHCP Server Settings Menu



Path – Status, System, System Settings

Parameters –

- **VLAN ID –** Set the ID of the specified VLAN.
  Default: VLAN 1.
- **Subnet IP –** Set the IP address of the sunet.
- **Subnet Mask –** Set the subnet mask of the VLAN. Usually 255.255.255.0.
  Default: 255.255.255.0
- **Name –** Enter a custom name for the VLAN for easy identification.
  Default: Default.
- **DHCP Mode –** Options: None, Server, Relay.
  - **None (default) –** Devices are not automatically assigned IP addresses.
  - **Server –** Creates a server inside the router to assign IP addresses to clients requesting one on the particular VLAN.
  - **Relay –** Takes the requests on a particular VLAN and forwards them to a centralized DHCP server that handles all requests from all VLANs.
- **IP Range/Relay Server –** Set the range of IP addresses that may be issued within the VLAN.
  Default: 192.168.1.100 - 192.168.1.149
- **Lease Time –** Number of minutes that a DHCP address lease will last.
  Default: 1440 (24 hours)
- **DNS Server Mode –** Options: Proxy, ISP, Static.
  Default: Proxy
- **DNS –** Set the DNS server 1 and 2 for the new subnet.
- **Delete –** Click the **Trashcan** to delete an entry.
- **Create VLAN –** Click to create a new subnet.

Configuration Instructions –

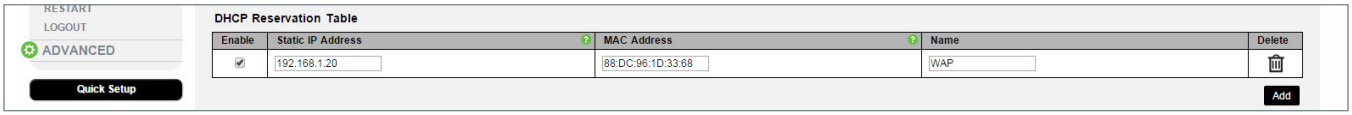
1. Change the desired settings.
2. Click Apply to save the new settings.

© 2015 Araknis Networks®

12.3.3 - DHCP Reservation Table

Use the DHCP Reservation table to reserve IP addresses for devices on the network. This method is similar to setting a static IP address in a device's IP settings, except that with reservations, the device will receive the same IP address based on it MAC address.

Figure 36. DHCP Server Settings Menu



Path – Status, System, System Settings

Parameters –

- **Enable –** Check the box to enable the reservation. Use this to deactivate reservations temporarily without having to delete them.
- **Static IP Address –** Enter the IP address to reserve for the device. May be inside or outside of the DHCP range.
- **Name –** Enter a unique name for the reservation for easy identification.
- **Delete –** Click the **Trashcan** to delete an entry.
- **Add –** Click to add a new DHCP reservation.

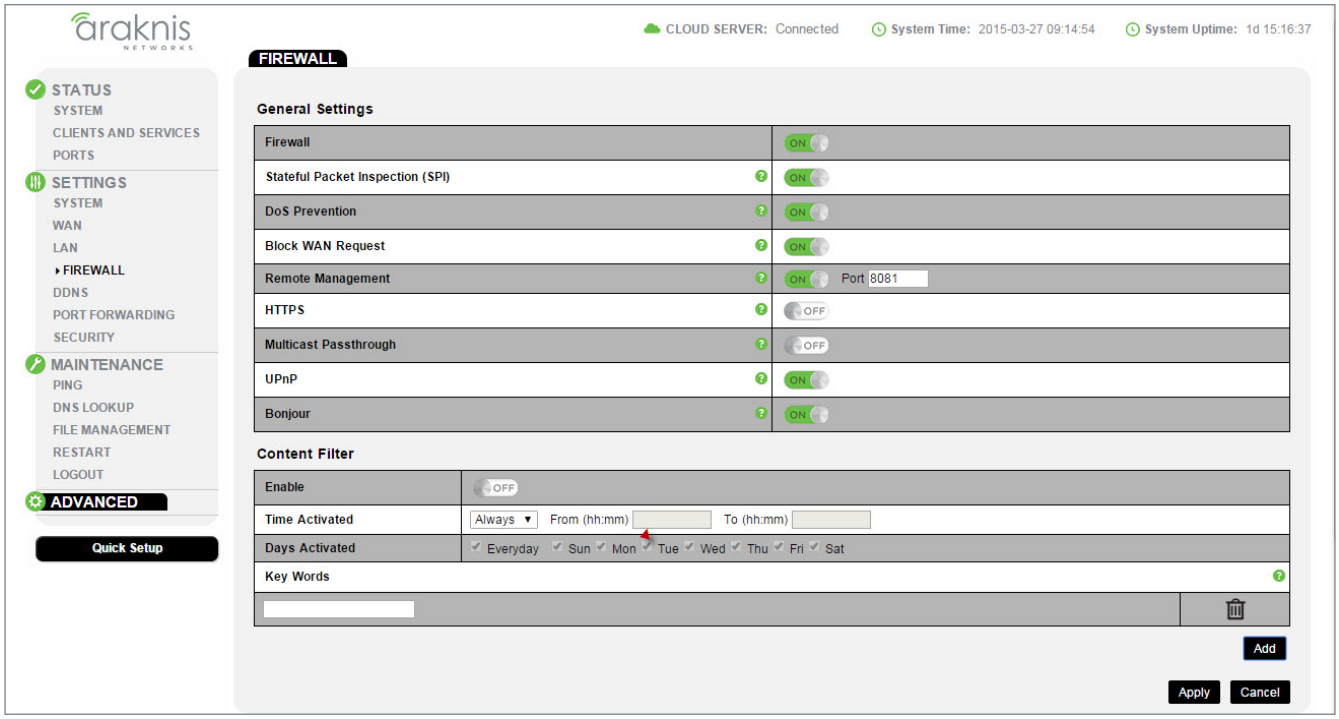
Configuration Instructions –

1. Change the desired settings.
2. Click Apply to save the new settings.

© 2015 Araknis Networks®

12.4 - Firewall

Figure 37. Firewall Settings Menu

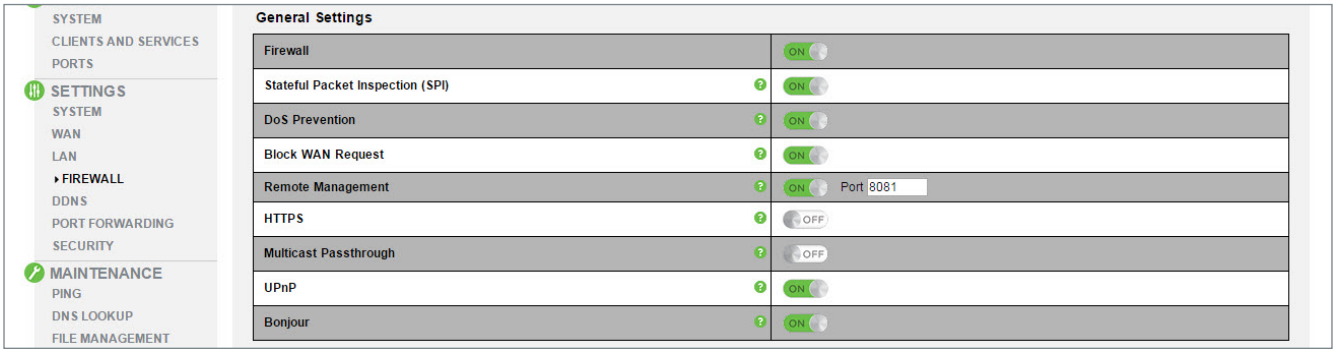


Path – Setting, Firewall

© 2015 Araknis Networks®

12.4.1 - General Settings

Figure 38. General Firewall Settings Menu



Path – Settings, Firewall

Parameters –

- **Firewall –** Turn the firewall on or off.
  Default: On.

> **Note –** Disabling the firewall causes sever network threats and is not recommended.

- **Stateful Packet Inspection (SPI) –** SPI inspects packets to determine their validity by comparing them to existing sessions and rejects those that do not fit the profile. SPI is useful for defending against IP spoofing attacks.
  Default: On.
- **DoS Prevention –** Turn Denial of Service Prevention on or off. DoS Prevention blocks bogus requests that clog the network during a DoS attack.
  Default: On.
- **Block WAN Request –** Prevents the WAN ports from responding to outside pings and makes the network seem invisible to others on the Internet.
  Default: On.
- **Remote Management –** With this feature enabled, access the router's web interface from outside the local network by connecting to the WAN IP address and remote management port. See *12.4.1.1 - Configuring Remote Management (page 42)* for setup and use instructions.
  Default: Off.
- **HTTPS –** Enabling HTTPS creates a more secure connection to the router web interface. HTTPS uses port 443 by default, in the same manner that HTTP uses port 80 by default. No port forwarding is required.
- **Multicast Passthrough –** Enable to allow the router to forward multicast packets to the correct clients simultaneously.
  Default: Off
- **UPnP –** Enable Universal Plug and Play to allow UPnP network devices to automatically see and communicate on the network. UPnP opens ports as needed. Monitor UPnP port activity in the ports status table. See *11.3 - Ports (page 25)*
  Default: Off

© 2015 Araknis Networks®

- **Bonjour –** Enable or Disable Apple's Bonjour. Bonjour is Apple's implementation of Zero Configuration networking, which allows users to search, locate and set up Apple Access Points. *Default: On*

> **Note –** Bonjour is accessible through Safari once it is enabled in Safari's Preferences. It shows up in your Bookmarks Menu and Bookmarks Menu Bar on both Mac and PC.

Configuration Instructions –

1. Change the desired settings.
2. Click Apply to save the new settings.

12.4.1.1 - Configuring Remote Management

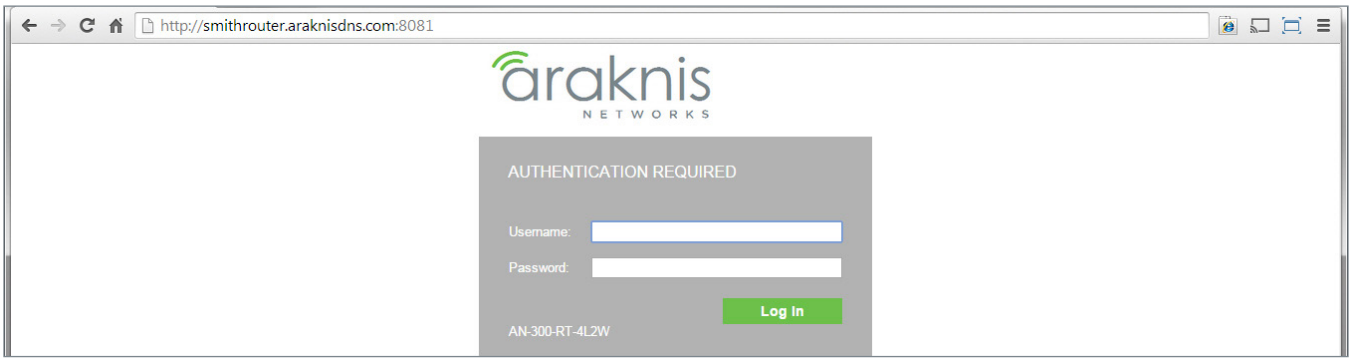
Figure 39. Remote Management Setup

1. Navigate to Settings, Firewall.
2. Set Remote Management to **On**, and enter a port for remote access. The default port 8081 is fine for most applications.
3. Click Apply at the bottom right of the page to save the settings.
4. If the WAN IP address of the router is dynamic, a DDNS address should be configured when remote management is enabled. For complete details and configuration instructions, see section *12.5 - DDNS (page 44).*
5. Record the port and DDNS/WAN IP address. This information must be entered in the web browser for remote access.

12.4.1.2 - Using Remote Management

To connect to the router interface from the Internet, users must enter the DDNS or WAN IP address and remote management port of the router, then log in using their account credentials. See the figure below. In the example, the DDNS address is smithrouter.araknisdns.com, and the port is set to 8081.

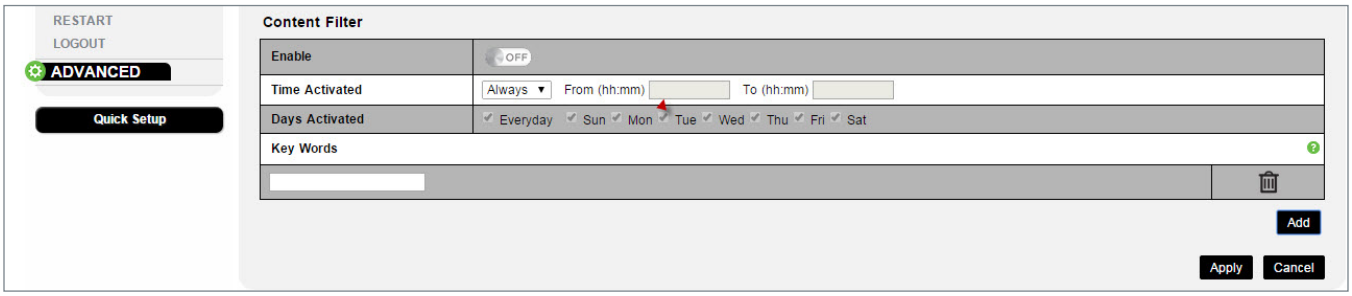
Figure 40. Remote Router Access



© 2015 Araknis Networks®

12.4.2 - Content Filter

Figure 41. Firewall Settings Menu



Path – Setting, Firewall

12.4.3 - General Settings

Parameters –

- **Enable –** Click to enable the Content Filter feature.
  Default: Off
- **Time Activated –** Set the time schedule for the Content Filter.
- **Days Activated –** Set the days the Content Filter is enabled (during the time specified above).
- **Keywords –** When content filtering is enabled, you can add a new rule and put IP addresses or URLs in this field. It will prevent the router from accessing these sites.
- **Delete –** Delete an entry from the Content Filter list.
- **Add –** Add a new entry to the Content Filter list.

12.4.3.1 - Configuring the Content Filter

1. Enable the Content Filter.
2. Select a schedule for the filter to be enabled:
   - **Always On –** Select **Always** from the Time Activated dropdown, and select the check box for **Everyday** in the Days Activated field.
   - **Interval –** Select **Interval** from the Time Activated dropdown, enter the desired time for the filter to turn on and turn off, and select the check box for the desired active days in the Days Activated field.
3. Click the **Add** button and enter an IP address or URL to block access too. Click **Add** again to add more rules.
4. Click **Apply** to save the new settings. Check the filter settings by attempting to access the listed sites from a computer on the LAN during the time the filter is active.

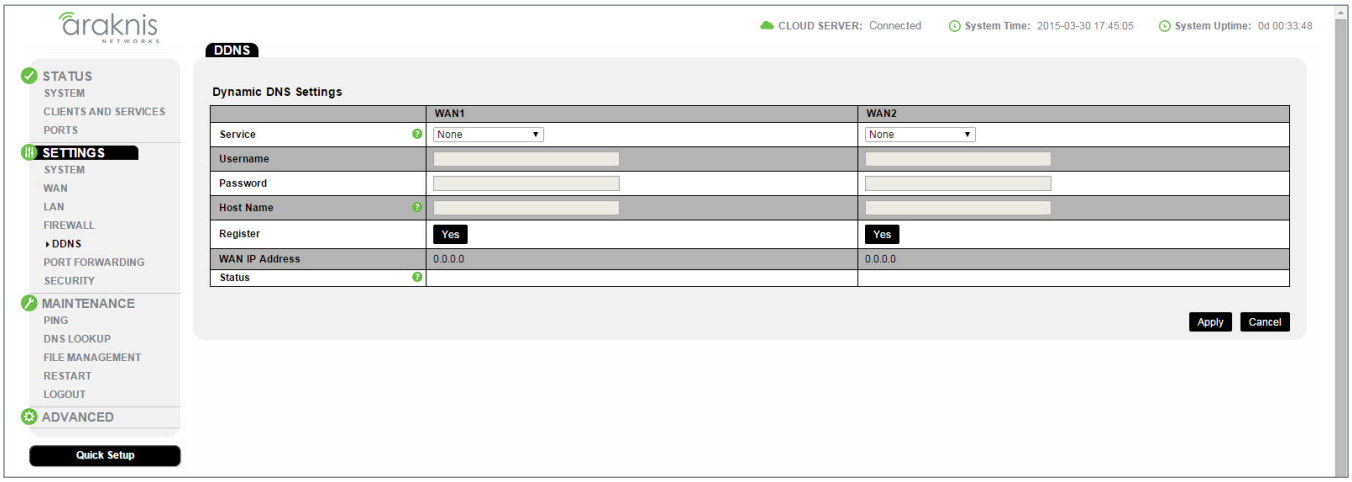
© 2015 Araknis Networks®

12.5 - DDNS

Use Dynamic DNS to access the router web interface and network devices from the Internet using a standard web address instead of the WAN IP address.

> **Note –** DDNS is commonly used to access the router for remote management. See section *12.4.1.1 - Configuring Remote Management (page 42)* for details.

Figure 42. Dynamic DNS Settings Menu



Path – Setting, DDNS

12.5.1 - Dynamic DNS Settings

Parameters –

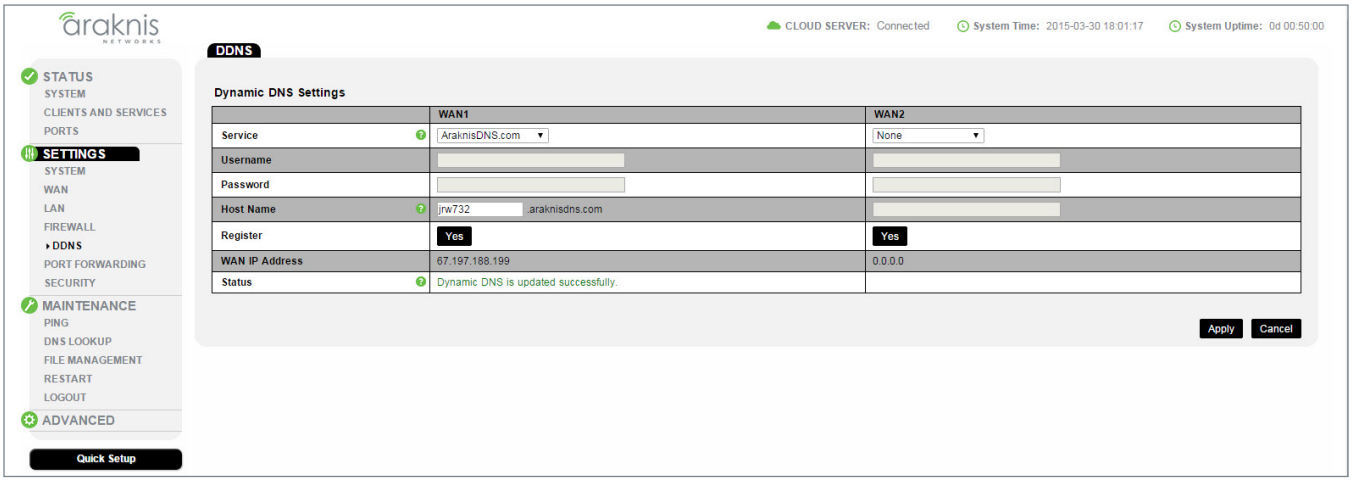
- **Service –** Select the DDNS service to be used from the dropdown. Options: None, DynDNS.org, 3322.org, WattBoxDNS.com, AraknisDNS.com, WirepathDNS.com, NO-IP.org.
  Default: None (DDNS disabled by default).
- **Username –** DDNS account username.
- **Password –** DDNS account password.
- **Host Name –** Prefix for the DDNS account appended to the front of the address. For example, Host Name ***smith*** would equal DDNS address ***smith.AraknisDNS.com***.
- **Register –** Click to register an account using entered credentials.
- **WAN IP Address –** WAN IP address currently on record with the DDNS account.
- **Status –** Current status of the DDNS account.

© 2015 Araknis Networks®

12.5.1.1 - Configuring DDNS Accounts

> **Note –** Other devices on the LAN may offer DDNS service features. However, only one DDNS address is needed for all devices on the network. Save time and effort by using the router's DDNS feature to access all devices.

Figure 43. DDNS Configuration



1. Select a service from the dropdown. ***AraknisDNS.com*** is the recommended choice.
2. Enter a host name for the account.
3. Click **Apply** to register the new DDNS account. The Status bar will update once the registration is completed.
4. If the host name is rejected, enter a new one and apply the settings again.

© 2015 Araknis Networks®

12.6 - Port Forwarding

Network ports are used to direct traffic between individual software applications running on network devices. Port numbers are always associated with a host IP address and a protocol type, usually either TCP, UDP, or both (TCP/UDP).

Most HTTP traffic on the network communicates using TCP port 80. When an address is entered in the web browser, the request is automatically sent to port 80 unless a different port is added to the end of the address. For example, if you access a device at IP address *192.168.1.20*, the request actually processes as if you entered *192.168.1.20:80*.

When software from LAN devices need access to and from the Internet, additional ports may be forwarded to the device to allow communication through the router firewall. Common uses for port forwarding include:

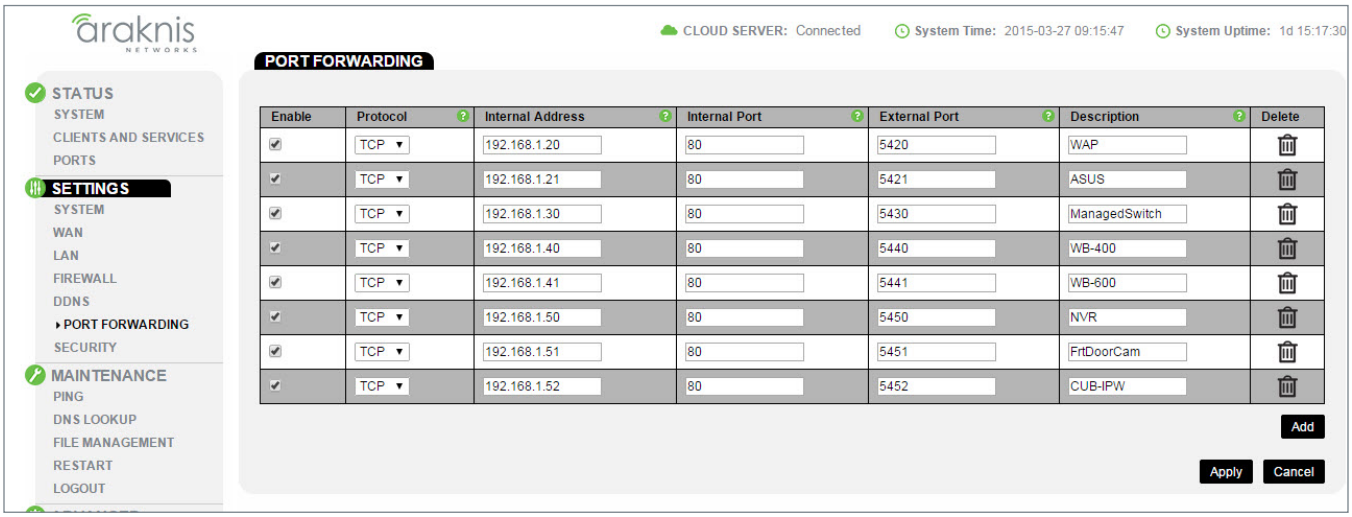
- Remote access for surveillance cameras and recorders
- Computer games and server applications
- Remote storage devices
- Remote access for network device setup menus (WAPs, managed switches, power monitoring devices)

Note – Many popular programs and protocols are set to use specific port numbers by default. For instance, HTTPS services typically use port 443, and SMTP mail services typically use port 25.

© 2015 Araknis Networks®

12.6.1 - Port Forwarding Menu

Figure 44. Port Forwarding Menu



Path – Settings, Port Forwarding

Parameters –

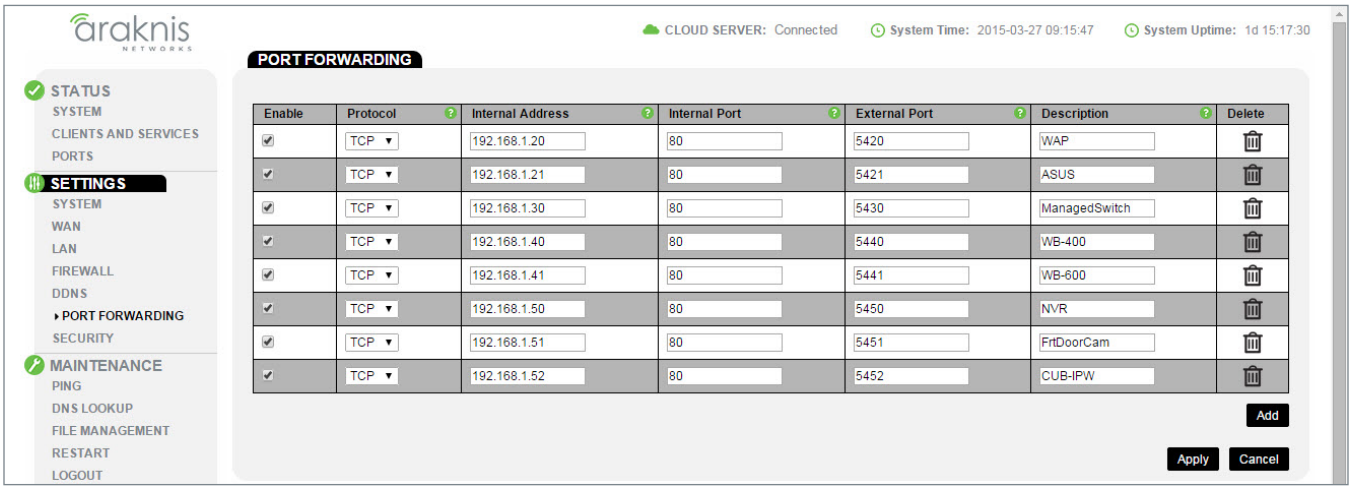
- **Enable –** Check to enable a port forwarding rule entry.
- **Protocol –** Select the protocol for the port. Options: TCP, UDP, Both.
- **Internal Address –** IP address of the device the port will forward to.
- **Internal Port –** Port configured for use in the device. Usually port 80.
- **External Port –** External port(s) that will connect to the internal port. Single numbers (example: 5400), or ranges (example: 5401-5410) may be entered.
- **Description –** Enter a name to identify the purpose of the forwarded port.

© 2015 Araknis Networks®

12.6.2 - Port Forwarding Setup Instructions

12.6.2.1 - Adding a New Port Forwarding Rule

Figure 45. New Port Forwarding Rule



> **Note –** When configuring port forwarding, internal ports may be assigned to one or more IP addresses without issue. External ports can only be forwarded to one IP address at a time.

1. Click **Add** to create a new entry line. Leave Enable checked to keep the new entry active.
2. Select the desired protocol from the dropdown (TCP, UDP, or both).
3. Enter the LAN IP address of the device into the Internal Address field.
4. Enter the device port in the Internal Port Field.
5. Enter the external port in the field.
6. Add a description to note the purpose of the forwarded port.
7. Click **Add** to configure additional ports, or **Apply** to save the newly configured settings.

12.6.2.2 - Editing or Deleting an existing Port Forwarding Rule

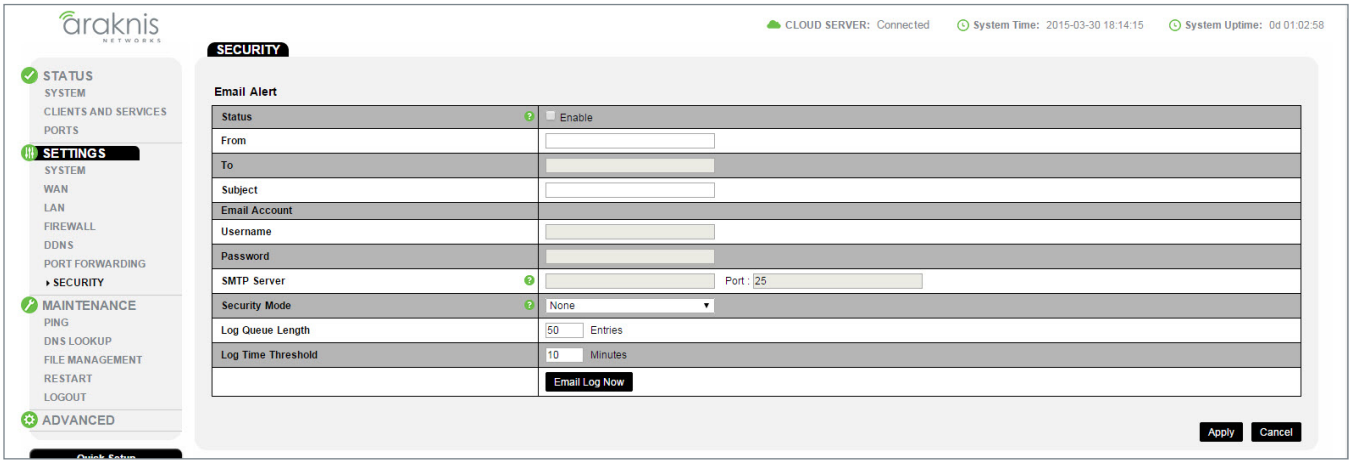
Uncheck the Enable box to deactivate a port forwarding rule without deleting it. Edit fields or click the **Trashcan** to delete existing rules, then click **Apply** to save the new settings.

© 2015 Araknis Networks®

12.7 - Security

Use the security menu to set up email. Send system logs and VPN configuration files using an email server.

Figure 46. Security Email Alert Menu



Path – Setting, Security

12.7.1 - Email Alert

Parameters –

- **Status –** Select Enable to send email notifications in the event of certain abnormal conditions.
  Default: Not selected
- **From –** Enter the email address of the configured sending email account.
- **To –** Enter the email address of the recipient.
- **Subject –** Enter a value for the subject line of sent emails.
- **Email Account –**
  - **Username –** Enter the username for the email account (Outlook, Gmail, etc.) sending the alert.
  - **Password –** Enter the password for the email account (Outlook, Gmail, etc.) sending the alert.
  - **SMTP Server –** Enter the SMTP Server and Port Number of the email client sending emails. For example, to configure a Gmail account, enter ***smtp.gmail.com***.
    Default: SMTP Server Blank; Port: 25
- **Security Mode –** Select the security mode used for communicating with the email server. Most connections require the ***SSL/TLS*** setting.
  Default: None.
- **Log Queue Length –** Number of most current entries to send in the log file.
  Default: 50.
- **Log Time Threshold –** How often (in minutes) the router emails a log. To get a report once a day, change the setting to ***1440*** minutes.
  Default: 10.
- **Email Log Now –** Click to email a copy of the system log to the email address in the To field.

© 2015 Araknis Networks®

12.7.1.1 - Configuring Email Alerts

Figure 47. Common Email Client Ports

Email Client	Ports(TLS)	Ports(SSL)
Gmail	587	465
Outlook	25 or 587	-
Microsoft Exchange	25	465
Yahoo	-	465
Office 365	587	-

Configuration Instructions –

1. Go to Settings, Security.
2. Specify the email alert settings.
3. Click **Apply** to save the new settings.
4. Click **Email Log Now** to ensure the new settings work correctly.

© 2015 Araknis Networks®

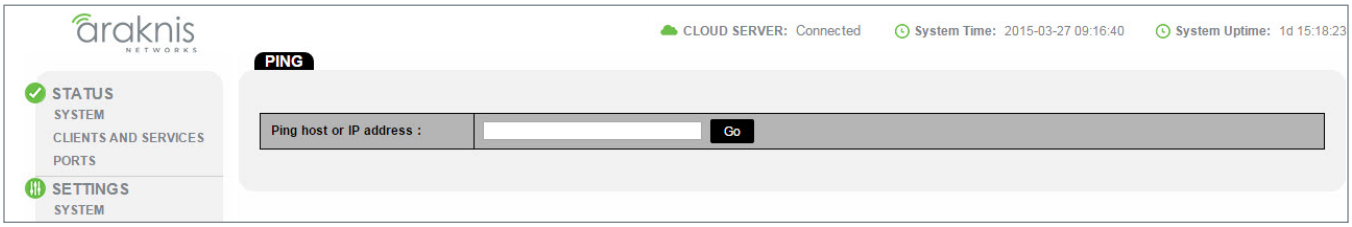
13 - Maintenance

Use the maintenance menu functions to troubleshoot network issues, maintain backup configuration files, and upgrade the router's firmware.

13.1 - Ping

The Ping Test screen is used to determine if a particular IP address can be reached from the router.

Figure 48. Ping Menu



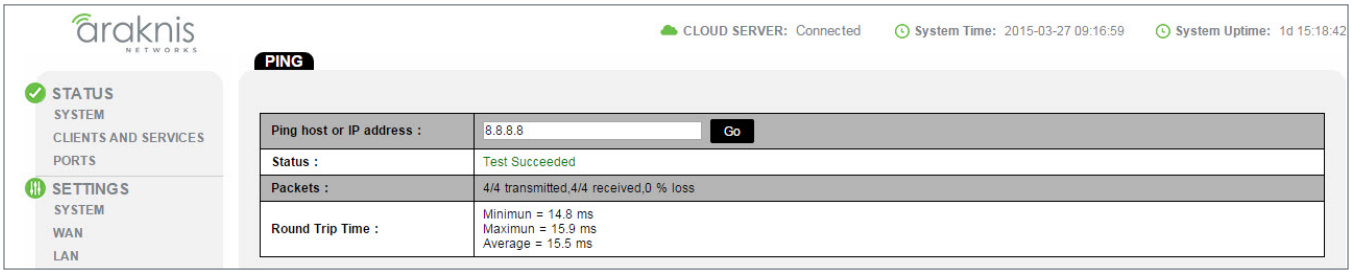
Path – MAINTENANCE , Ping

Parameters –

- **Ping host or IP address –** Enter the address to ping. Click **Go** to begin the test.

13.1.1 - Ping Test Results

Figure 49. Ping Menu



Parameters –

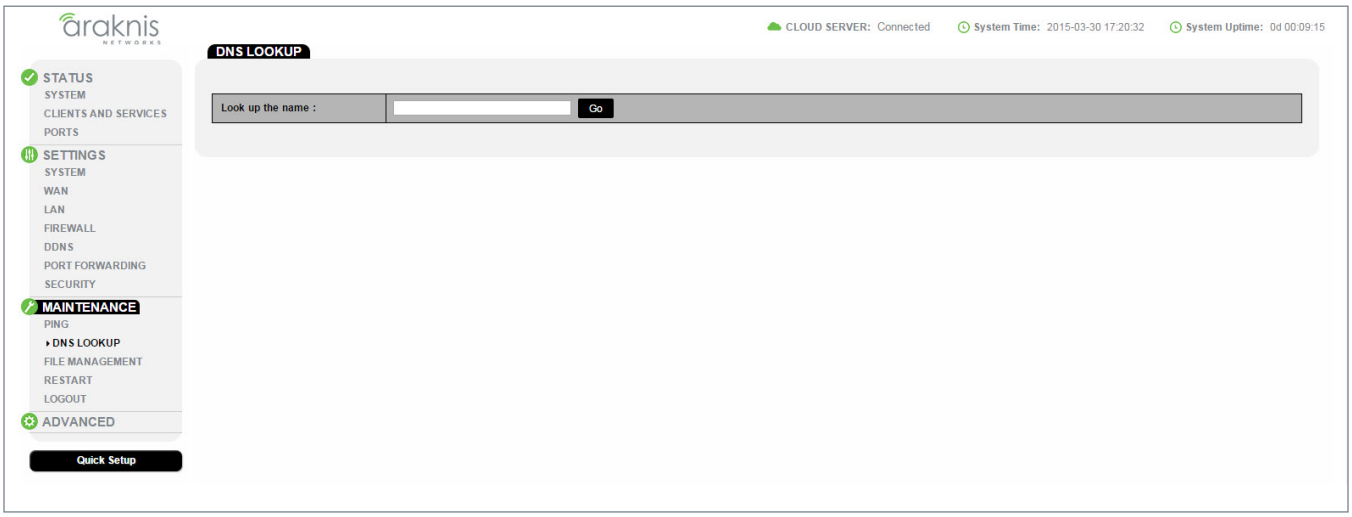
- **Status –** Current stage or summary of the test.
- **Packets –** Detailed information about the ping packets.
- **Round Trip Time –** Minimum, maximum, and average time for the packets to travel to and from the site the router pinged.

© 2015 Araknis Networks®

13.2 - DNS Lookup

Use the DNS Lookup feature to troubleshoot issues with a DNS server and also to make sure that the DNS server referenced in the IP settings is up and running.

Figure 50. DNS Lookup Menu



Path – MAINTENANCE , DNS Lookup

Parameters –

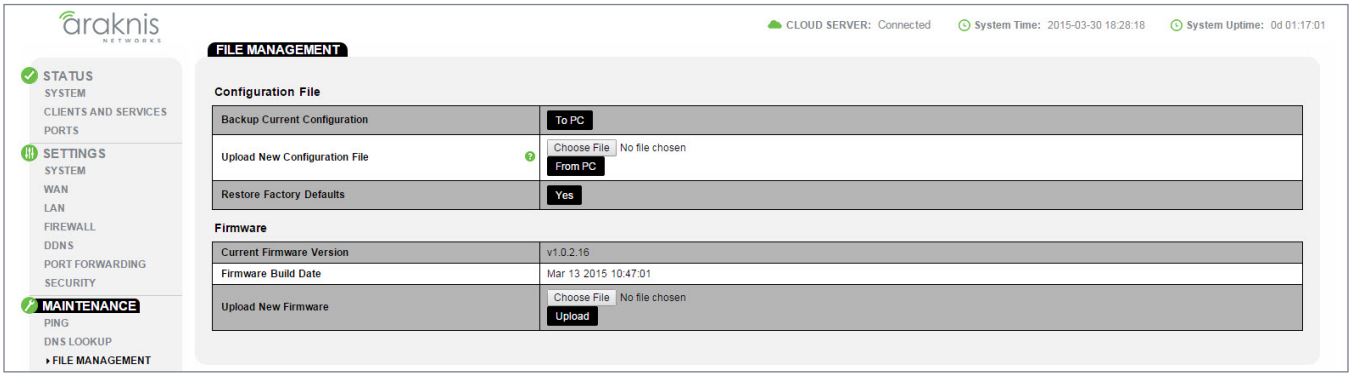
- **Look up the name –** Enter a website name and click the **Go** button to look up the

© 2015 Araknis Networks®

13.3 - File Management

Backup and upload settings and manage firmware.

Figure 51. File Management Menu



Path – Maintenance , File Management

13.3.1 - Configuration File

Use the Configuration File menu to back up or restore settings to the router.

13.3.1.1 - Backup Current Configuration

Save the router's current configuration settings to a *.tar* format compressed archive on your computer.

1. Click the **To PC** button and select a location to save the file.
2. Name the file and save it to your computer.

13.3.1.2 - Upload New Configuration File

Restore previously saved configuration settings to the router to restore settings.

1. Click the **Choose File** button and select a configuration file (*.tar* file type) from the Open window.
2. The file name will appear to the right of the **Choose File** button.
3. Click the **From PC** button to upload the configuration file. Wait while the Rebooting screen opens and loads the selected configuration. When the upload is finished, the Log In window will open.
4. Log in and confirm the new configuration settings.

13.3.1.3 - Restore Factory Defaults

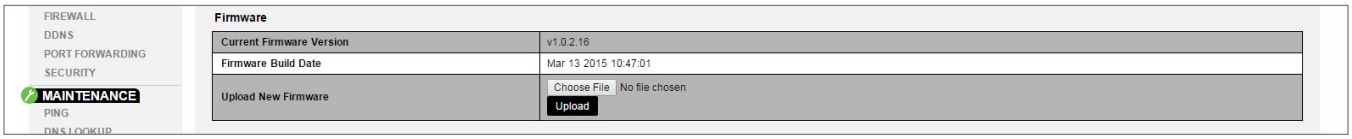
1. Click the **Yes** button to restore the router to factory default settings. The red ALERT message will appear.
2. Click **Confirm** and wait while the rebooting screen is open and loading the selected configuration. When the configuration upload is finished, the login window will appear.
3. Enter the username and password. (***araknis***; ***araknis***)
4. Confirm the new configuration settings.

© 2015 Araknis Networks®

13.3.2 - Firmware

Use the Firmware menu to upload new firmware to the router.

Figure 52. Firmware Menu



Path – Maintenance, File Management, Firmware

Parameters –

- **Current Firmware Version –** Indicates the current running firmware version.
- **Firmware Build Date –** Date the current firmware was released to the public
- **Upload New Firmware –** See configuration instructions below.

Configuration Instructions –

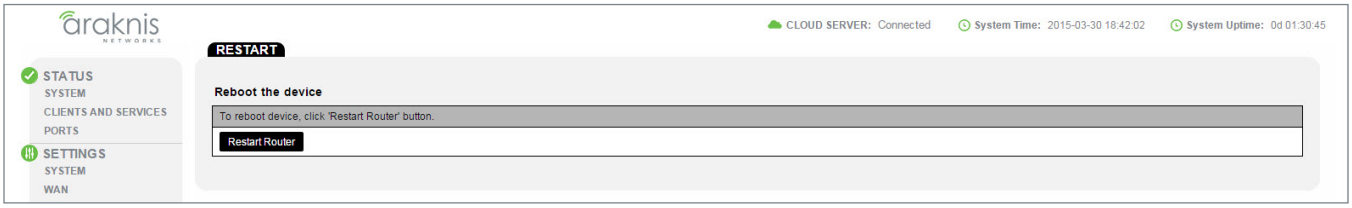
1. Click the **Browse** button to navigate to where the firmware file is saved.
2. Select the file and then press Enter/Return on the computer keyboard or click **Open** on the Upload menu. (The firmware file name should appear next to the Upload New Firmware File **Browse** button.)
3. Click **Upload**. The Upload Firmware Information screen will open.
4. Click **Upgrade**. Wait while the new firmware loads. When the configuration upload is finished, the login screen will appear.
5. Enter the username and password.
6. Confirm the firmware version.

© 2015 Araknis Networks®

13.4 - Restart

Restart the router.

Figure 53. Restart Menu



Path – Maintenance, Restart

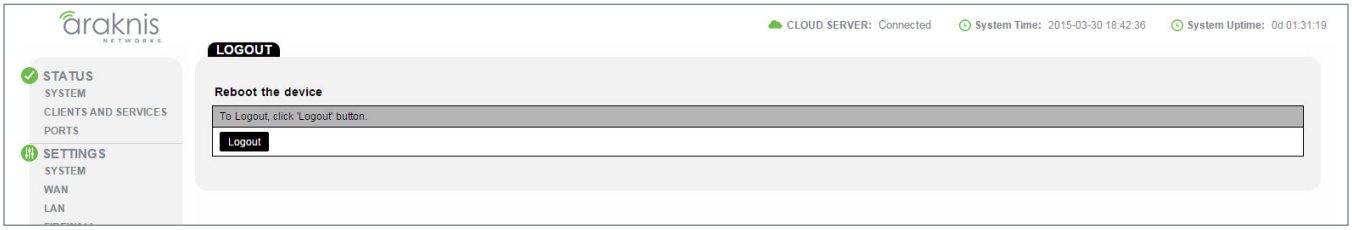
Configuration Instructions –

1. Click the **Restart Router** button. The following message will appear: "This will reboot the device and may take a few seconds..."
2. Click **OK** to reboot (or **Cancel** to return to the Restart Screen).
3. Wait while the router reboots. When the device has rebooted, the login screen will appear.
4. Enter the username and password and log in.
5. Confirm the firmware and configuration.

13.5 - Logout

Sign out of the router.

Figure 54. Logout Menu



Path – Maintenance, Logout

Configuration Instructions –

1. Click the **Logout** button.
2. Click **Confirm** to log out, or **Cancel** to the menu.
3. If you clicked **Logout**, the login screen will appear with a message stating you have logged out.

© 2015 Araknis Networks®

14 - Advanced Menus

Caution – The advanced menus include features that will not be used by most. Use caution when changing advanced settings to avoid interrupting network traffic or losing access to the router interface.

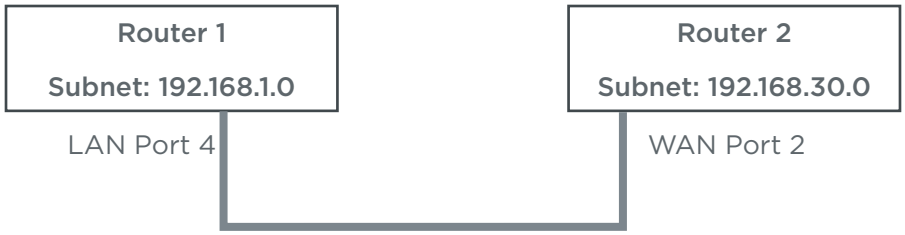
© 2015 Araknis Networks®

15 - Routing

Static routing is used to create routes to other subnets using a fixed routing table.

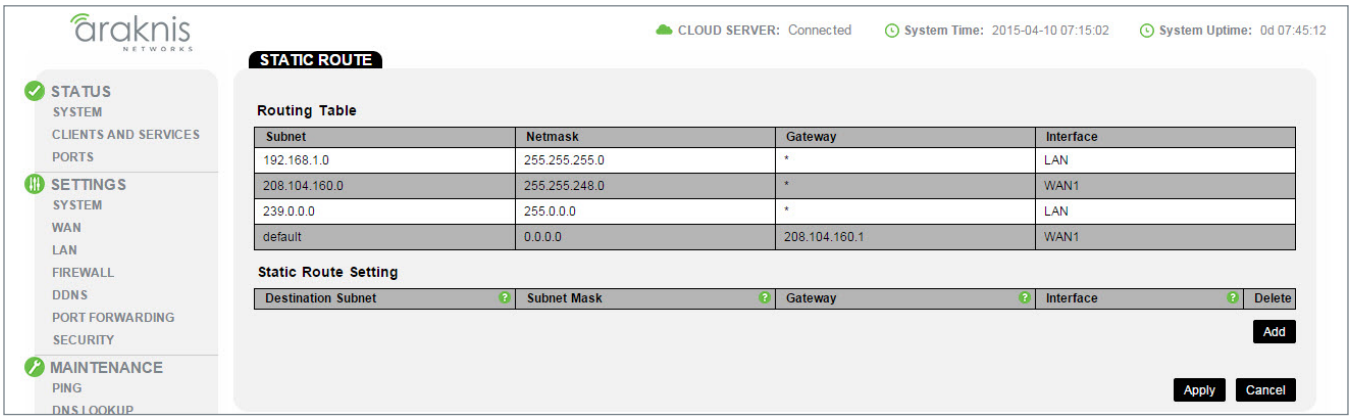
Static routes are commonly used to allow traffic between subnets on different routers. For example, in a large office network, there is a subnet configured for the first floor inside of Router 1 with the IP address 192.168.1.0. Computers on the third floor are connected to Router 2 using subnet 192.168.30.0, and they need to communicate with the 192.168.1.0 subnet. A static route is configured in each router to the port connecting them.

Figure 55. Static Route Configuration Example



15.1 - Static Route

Figure 56. Static Routing Menu



15.1.1 - Routing Table

The routing table displays default routing information for the router. Use this information to troubleshoot and set up static routes.

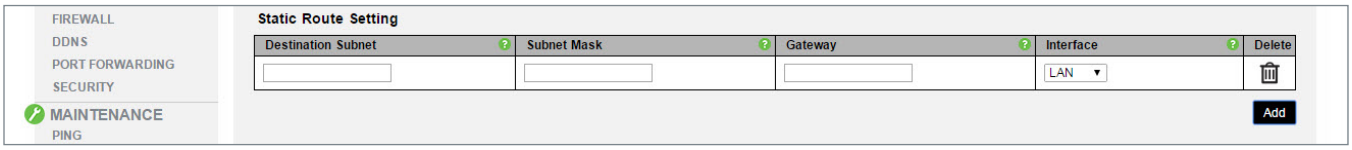
Parameters –

- **Subnet –** Subnet used on the specified interface.
- **Netmask –** Subnet mask of the specified interface.
- **Gateway –** Gateway IP address of the specified interface. The asterisk symbol (*) indicates a wild card.
- **Interface –** Interface using the routing table entry, either the LAN (1/2/3/4) or one of the WAN ports (WAN 1/WAN 2).

© 2015 Araknis Networks®

15.1.2 - Static Route Setting

Figure 57. Adding a new Static Route

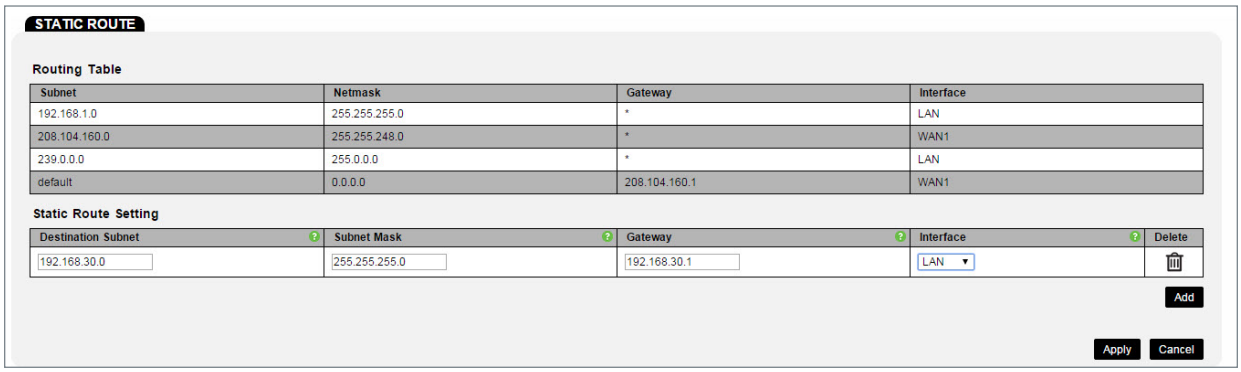


Parameters –

- **Destination Subnet –** Enter the network address of the destination subnet. The destination could be internal or external. Usually ends in zero, for example, ***192.168.1.0***.
- **Subnet Mask –** Enter the subnet mask of the destination subnet. Usually 255.255.255.0.
- **Gateway –** Specify a gateway IP address for the subnet destination.
- **Interface –** Physical port the static route will use.
- **Delete –** Click the **Trashcan** to delete an existing static route.
- **Add –** Click to add a new static route.

Configuration Instructions –

1. Add a static route in Router 1:



© 2015 Araknis Networks®

15.2 - Port Triggering

Use port triggering to enable ports only when needed by watching internal ports for activity.

Figure 58. Port Triggering Setup Menu

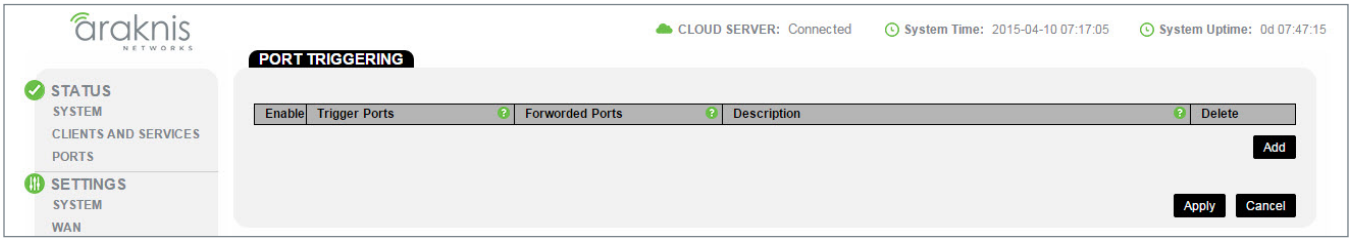
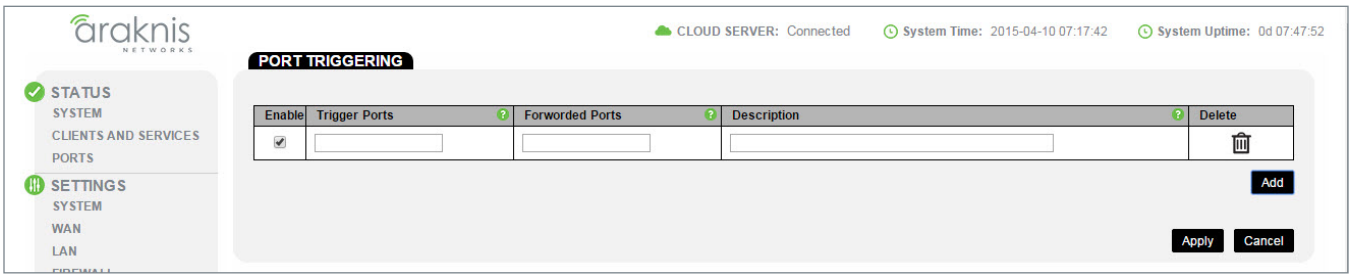


Figure 59. Adding a New Port Trigger Rule



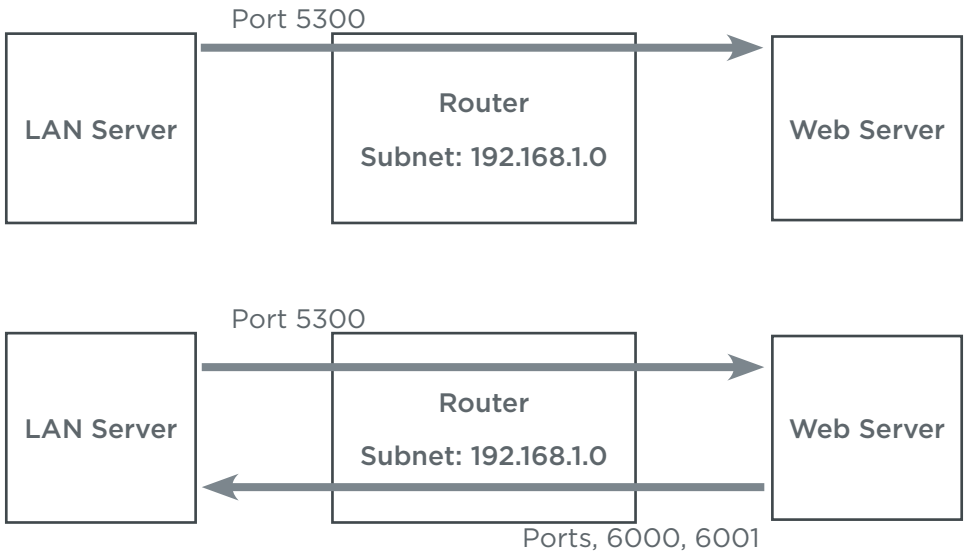
Parameters –

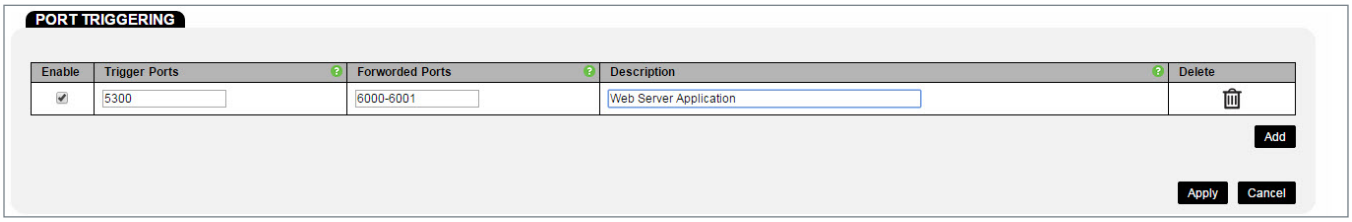
- **Add –** Click to add a new port triggering rule.
- **Edit –** Edit an existing rule.
- **Delete –** Delete an existing rule.
- **Enable –** Check the box to enable the port trigger rule. New entries are enabled by default.
- **Trigger Ports –** Enter the port(s) to be triggered when the specified forwarded ports are in use. Single numbers (example: 5400), multiple numbers (example: 5400,5405), or ranges (example: 5401-5410) may be entered.
- **Forwarded Ports –** Specify the forwarded port(s) that will enable the trigger ports. Single numbers (example: 5400), multiple numbers (example: 5400,5405), or ranges (example: 5401-5410) may be entered.
- **Description –** Add a description to detail the use of the rule.
- **Delete –** Click the **Trashcan** to delete an existing static route.
- **Add –** Click to add a new static route.

© 2015 Araknis Networks®

15.2.1 - Configuring Port Triggering

1. Click the **Add** button.
2. Enter the trigger ports that the router will monitor for activity.
3. Enter the ports to be forwarded when a trigger port is active.
4. Click **Add** again to start a new rule, or click **Apply** to save the new rule.





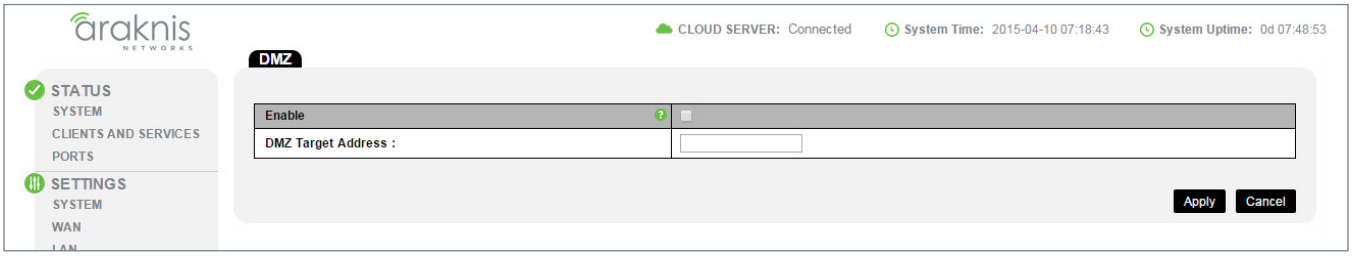
© 2015 Araknis Networks®

15.3 - DMZ

Use DMZ to enable all ports to one IP address, negating the need to forward individual ports to that device. DMZ is typically used for web servers running their own firewall for protection from WAN attacks.

> **Note –** Devices configured for DMZ access are vulnerable to attack...

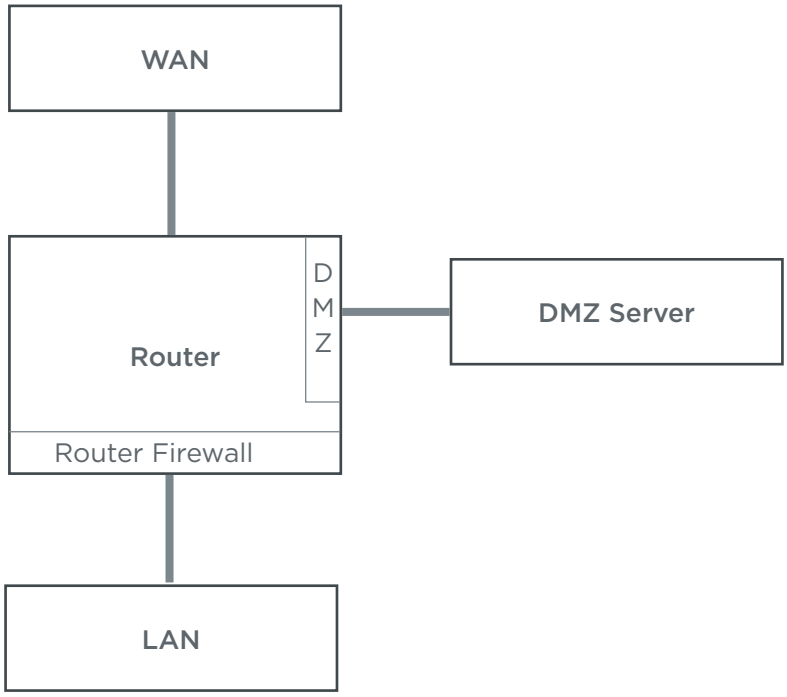
Figure 60. DMZ Setup Menu



Path – Advanced, Forwarding, DMZ

Parameters –

- **Enable –** Check the box to enable the DMZ feature.
- **DMZ Target Address –** IP address of the device being forwarded to.



© 2015 Araknis Networks®

15.4 - One-to-One NAT

Configure devices on the LAN to appear as having a specific public (WAN) IP address.

Figure 61. One-to-One NAT Setup Menu

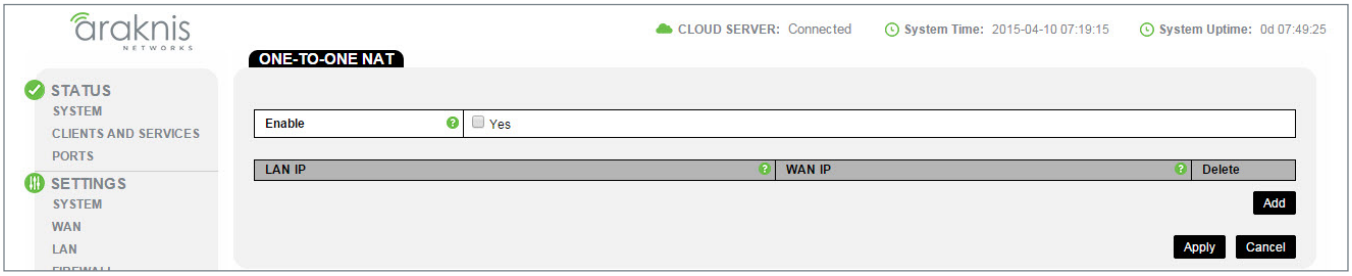
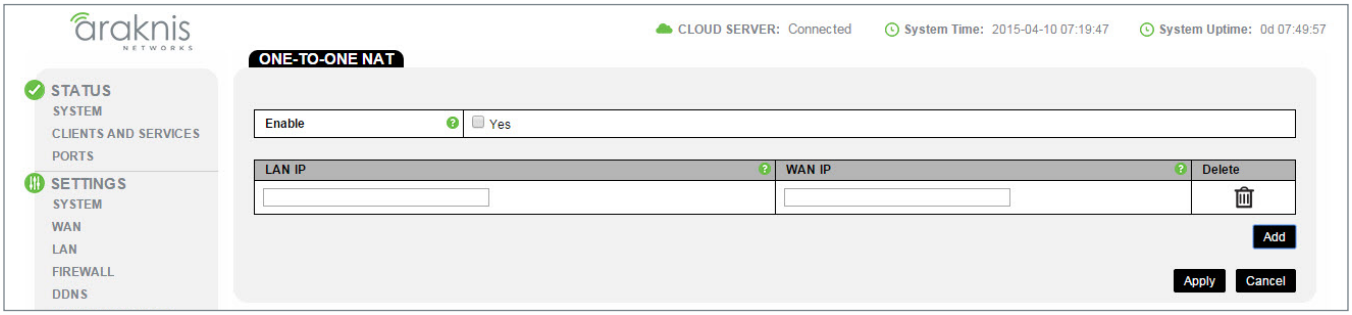


Figure 62. Adding a New One-to-One NAT Entry



Path – Advanced, Forwarding, One-to-One NAT

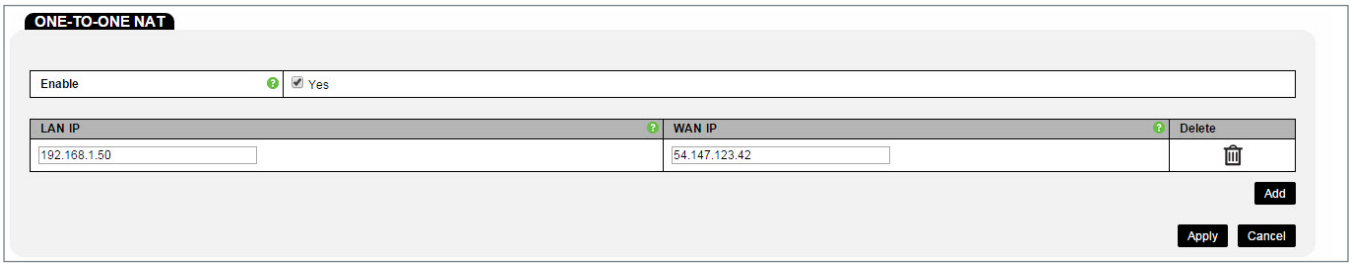
Parameters –

- **Enable –** Check the box to enable one-to-one NAT.
- **LAN IP –** Enter a single IP address or a range of IP addresses to be represented by the specified WAN IP address.
- **WAN IP –** Enter the desired public IP address for use.
- **Delete –** Click the **Trashcan** to delete an existing static route.
- **Add –** Click to add a new static route.

© 2015 Araknis Networks®

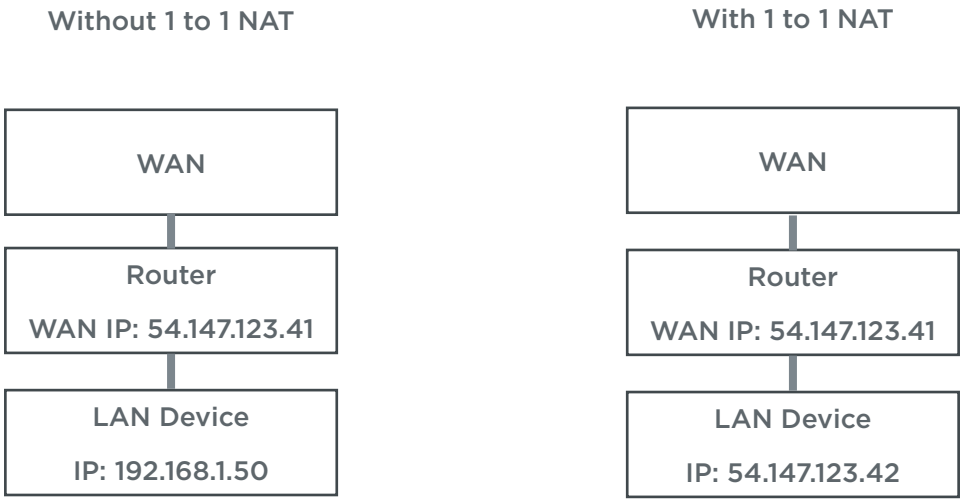
15.4.1 - Configuring One-to-One NAT

Figure 63. One-to-One NAT Setup



1. Enable One-to-One NAT and click the **Add** button to create a new entry field.
2. Enter the LAN IP address.
3. Enter the WAN IP address.
4. Click Apply to save the new entry.

Figure 64. One-to-One NAT Operation Example

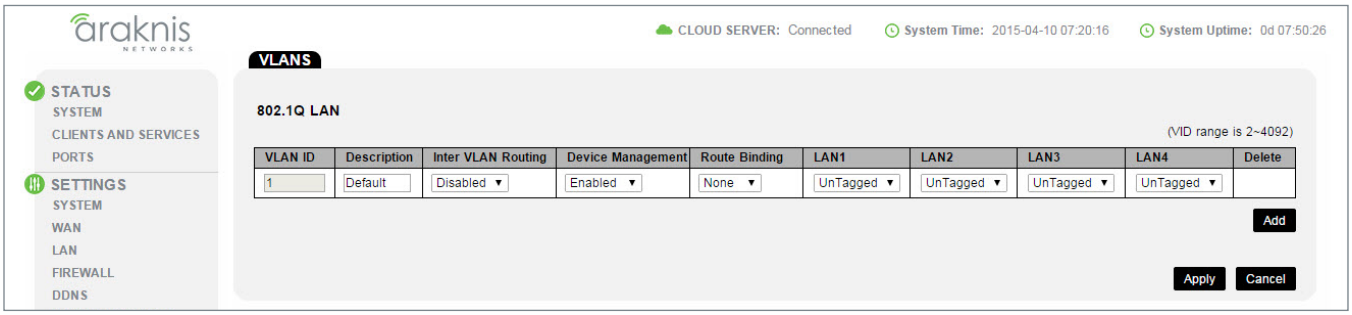


© 2015 Araknis Networks®

16 - VLANs

Virtual Local Area Networks (VLANs) are used to segment traffic on the LAN. Proper setup of VLANs will increase the reliability, speed and security of the network.

Figure 65. VLANs Setup Menu



Path – Advanced, VLANs

Parameters –

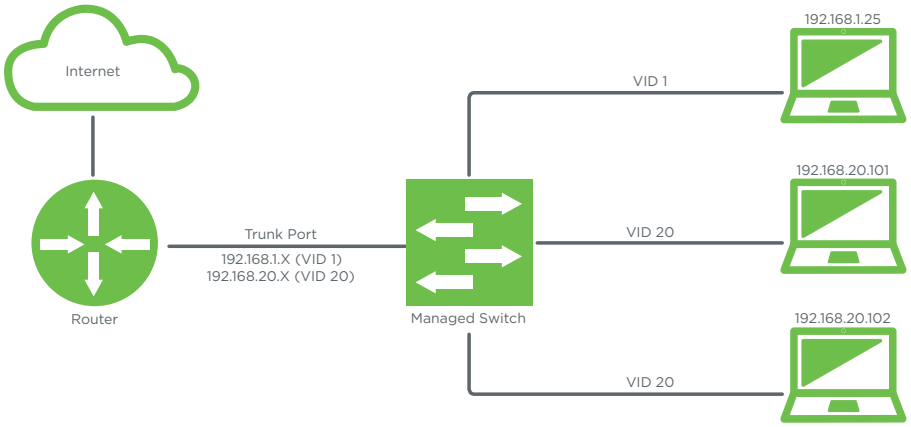
- **VLAN ID –** Identification number for the VLAN. The default VLAN is always set to 1.
- **Description –** Enter a description to help easily identify the VLAN's purpose.
- **Inter VLAN Routing –** Select whether routing between VLANs is enabled or disabled.
  Default: Disabled.
- **Device Management –** Select whether to enable or disable device management.
- **Route Binding –** Set whether routes use the WAN1 or WAN2 port.
  Default: None.
- **LAN1/2/3/4 –** Configure the LAN ports on the router for the VLAN. A port may be configured as one of the following options:
  - **Untagged –** The port is a member of the specified VLAN. VLAN frames handled through this port are not tagged with a VLAN ID.
  - **Tagged –** The port is a member of the specified VLAN. VLAN frames handled through the port are tagged with a VLAN ID.
  - **Excluded (Default) –** The port is not a member of the specified VLAN.
- **Add –** Click to add a new VLAN.
- **Delete –** Click the **Trashcan** to delete an existing static route.

© 2015 Araknis Networks®

16.1 - Benefits of VLANs

- VLANs are created and managed by the network admin using managed network devices with VLAN capability.
- VLANs structure communication between network devices:
  - Without VLANs, network broadcast traffic (packets) from any device is sent to all devices.
  - With VLANs, broadcast packets are tagged with a VLAN ID when they pass through an assigned VLAN port. Tagged packets are only sent to other devices that are members of the same VLAN.
- VLANs break a LAN into smaller sub-networks. For example, VLANs may be used to segment the LAN traffic in a large home network, based on the type of user:
  - VLAN 1 is used for entertainment and end user devices (phones, computers, tablets).
  - VLAN 20 is only for surveillance systems (NVRs, IP cameras).
  - VLAN 30 is only for home automation/control system equipment.
  - VLAN 40 is restricted Wi-Fi for guests.
- Devices can be part of a VLAN based on either:
  - Physical port number on a managed switch or router that connects to a network device.
  - MAC address of device (VLAN is configured with a list of MAC addresses that are allowed or not allowed to connect to it).
- VLANs can be totally restricted (only devices in the same VLAN can talk to each other) or allow access from/to other VLANs. Inter-VLAN communication is controlled by the router or other Layer 3 devices.

Figure 66. VLAN Network Topography Example



16.2 - Why Set up VLANs?

- **Increased Security –** Unknown users can connect to a guest network but can't get access to other parts of the network unless you give them access.
- **Minimize Network Equipment –** Instead of needing multiple switches to make multiple subnets, you can use one switch and assign each port to a VLAN as needed.

© 2015 Araknis Networks®

16.3 - Basic VLAN Setup Recommendations

Planning is the key to success with VLANs. List equipment by the way you want to split up a network, then record what devices are connected to what ports. You need managed switches located correctly to ensure that configuration can be completed, and cables between switches and the router to move data efficiently.

After you have the network organized, you can begin configuring VLANs in the router. We recommend setting up the router before any switches to ensure you don't set the wrong VLAN and lose access to a device.

Use different subnets for different VLANs to make it clear in which VLAN a device is located. Example:

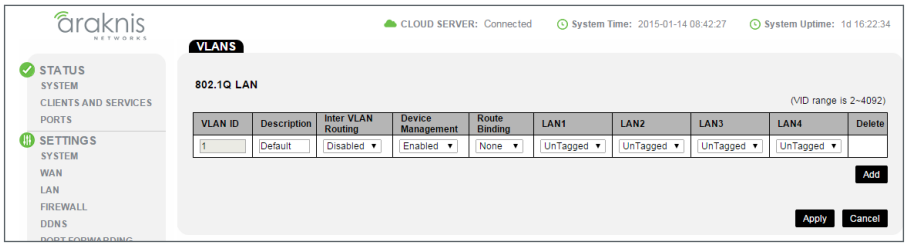
- VLAN 1 uses *192.168.1.XXX* addresses.
- VLAN 20 uses *192.168.20.XXX* addresses.
- VLAN 30 uses "192.168.30.XXX" addresses.

16.4 - Configuring VLANs

By default, the entire network is on VLAN 1. Follow these instructions to configure new VLANs in the Araknis router.

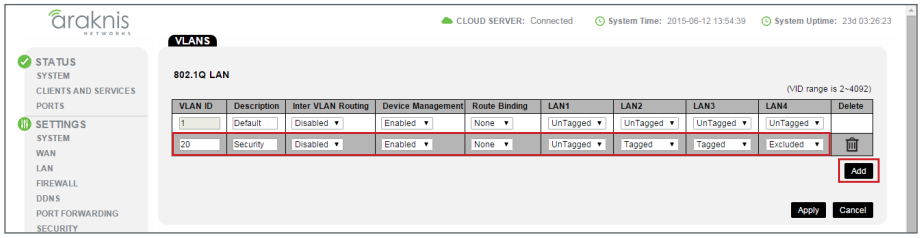
1. Log into the router web interface as an administrator, and navigate to Advanced, VLANs.

Figure 67. AN-300-RT-4L2W VLANs Menu



2. Click the **Add** button to the right and enter a new VLAN ID in the field. For this example, we will add new VLAN 20. *If you add a new entry and do not use it, delete the entry using the* **Trashcan** *button before applying other changes.*

Figure 68. New VLAN Entry

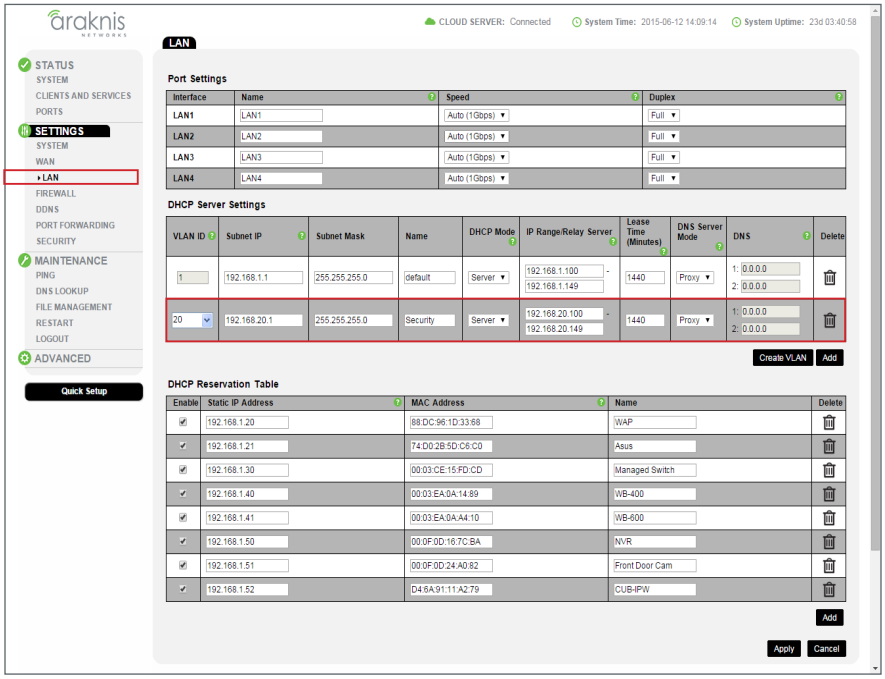


3. Configure the VLAN description, settings, and port assignments as desired.
4. Click **Apply** in the bottom-right corner to save the new entry. Now that the VLAN has been added in this menu, a new DHCP server and subnet has automatically been enabled in the LAN menu.

© 2015 Araknis Networks®

5. Navigate to the **LAN** menu and review the settings for the new VLAN. *Note the new subnet and DHCP server settings entries listed for VLAN 20.*

Figure 69. LAN Menu – New VLAN 20



6. The default settings for the DHCP server are ideal for most VLANs that require it. Change these settings if desired, then click **Apply** in the bottom-right to save the changes. Your router is now configured to issue DHCP IP addresses and handle traffic on VLAN 20.

© 2015 Araknis Networks®

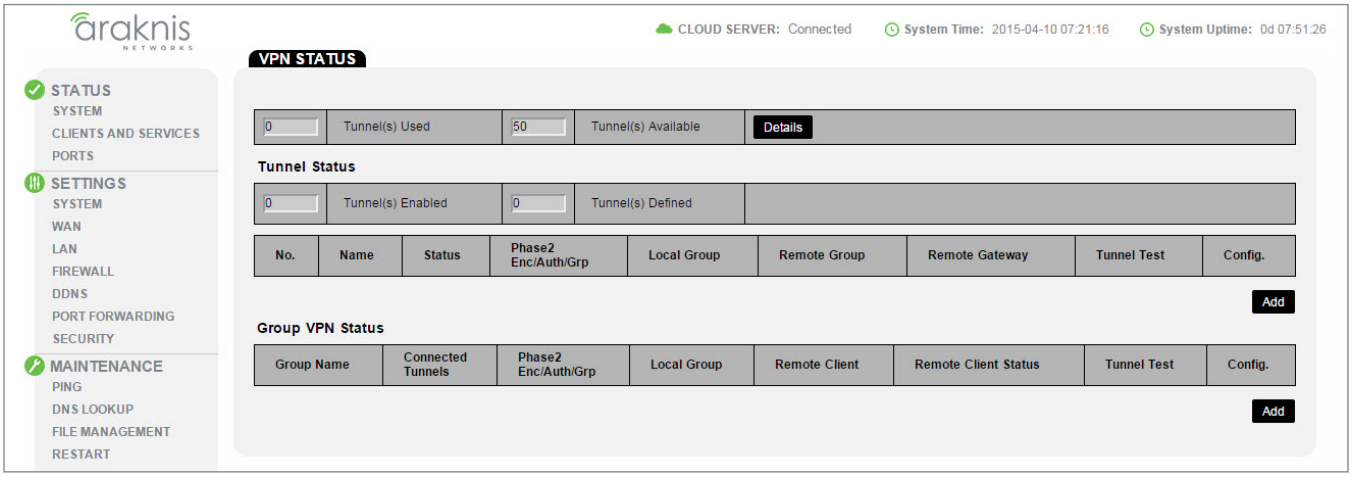
17 - VPN

A Virtual Private Network (VPN) provides a connection between different networks through a secure tunnel over the Internet. Data sent through the VPN tunnel is encrypted for privacy even when connected to a public or shared network that isn't secure. VPNs are commonly used to send data between networks in different geographical locations without requiring a dedicated physical connection between the networks.

VPNs may be configured the OpenVPN, PPTP, L2TP, or IPSec standard.

17.1 - VPN Status

Figure 70. VPN Status Screen

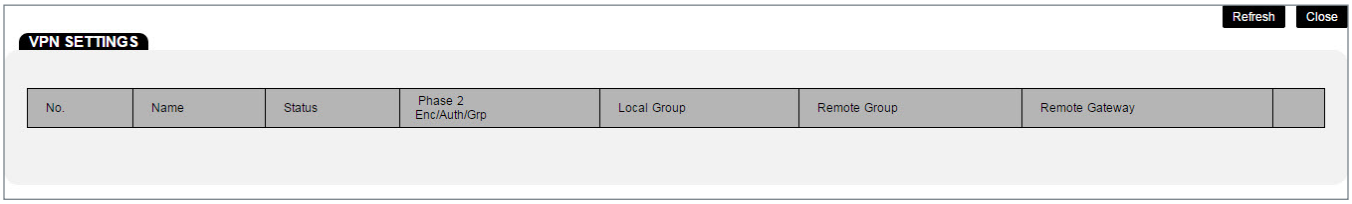


Path – Advanced, VPN, Status

Parameters –

- **Tunnel(s) Used –** Total number of available tunnels currently in use.
- **Tunnel(s) Available –** Free tunnels available for use.
- **Details –** Click the button to view the VPN Status table.

Figure 71. VPN Status Table

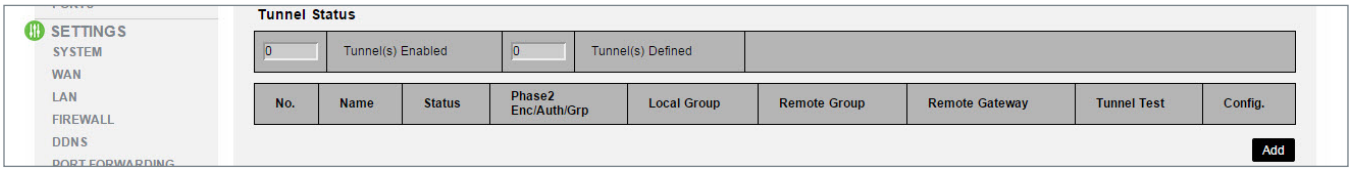


© 2015 Araknis Networks®

17.1.1 - Tunnel Status

See what type of tunnels are currently in use and what network devices they are communicating with.

Figure 72. VPN Tunnel Status



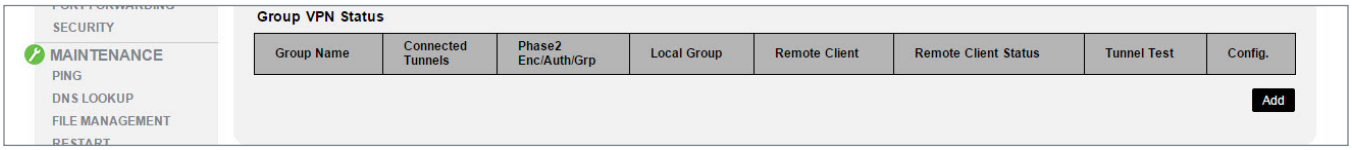
Parameters –

- **Tunnel(s) Enabled –** Number of tunnels currently available.
- **Tunnel(s) Defined –** Number of currently defined tunnels.
- **No. –** VPN tunnel number.
- **Name –** Custom name assigned to the tunnel for easy identification.
- **Status –** Status of the current VPN tunnel.
- **Phase2 Enc/Auth/Grp –** IPSec settings.
- **Local Group –** IP settings for the Local Group.
- **Remote Group –** IP settings for the Remote Group.
- **Remote Gateway –** Remote Gateway IP address.
- **Tunnel Test –** Click the button to test the connection.
- **Config. –** Click the **Paper** icon to edit the tunnel settings or the **Trashcan** to delete the entry.
- **Add –** Click to add a new VPN tunnel.

© 2015 Araknis Networks®

17.1.2 - Group VPN Status

Figure 73. VPN Tunnel Status



Parameters –

- **Group Name –** Custom name assigned to the group for easy identification.
- **Conected Tunnels –** Number of tunnels currently in use.
- **Phase2 Enc/Auth/Grp –** IPSec settings.
- **Local Group –** IP settings for the Local Group.
- **Remote Group –** IP settings for the Remote Group.
- **Local Group –** IP settings for the Local Group.
- **Remote Client –** IP settings for the Remote Client.
- **Remote Client Status –** Click to view the remote client connection list.
- **Tunnel Test –** Click the button to test the connection.
- **Config. –** Click the **Paper** icon to edit the tunnel settings or the **Trashcan** to delete the entry.
- **Add –** Click to add a new VPN tunnel.

© 2015 Araknis Networks®

17.2 - OpenVPN

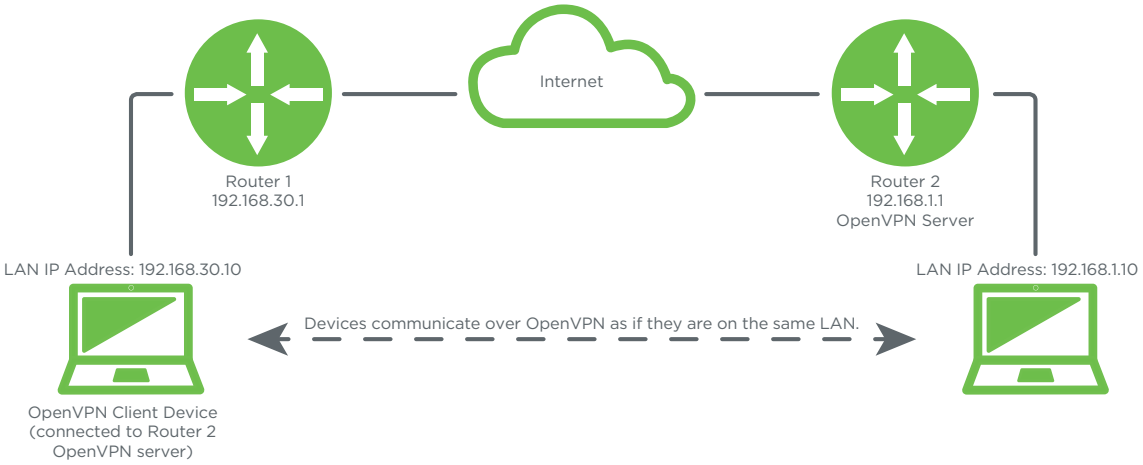
The AN-300-RT-4L2W router features a built-in OpenVPN server for secure, easily configured access to the network from the Internet using devices with an OpenVPN client application. Use OpenVPN to access local network devices like shared drives and home network servers as if you were on the local network.

OpenVPN communicates using encrypted SSL/TLS channels between networks that hide traffic from other devices on the Internet. The OpenVPN server runs on the router to control access to the tunnels, and users connect using a client application installed on their computer.

VPN users are provided with a configuration file generated by the OpenVPN server. This file is used as a key for the client application to communicate with the server and open a connection. The router must be configured for each OpenVPN account that will be used.

Client applications are available for PC and Mac computers and iOS and Android mobile devices.

Figure 74. OpenVPN Operation Diagram



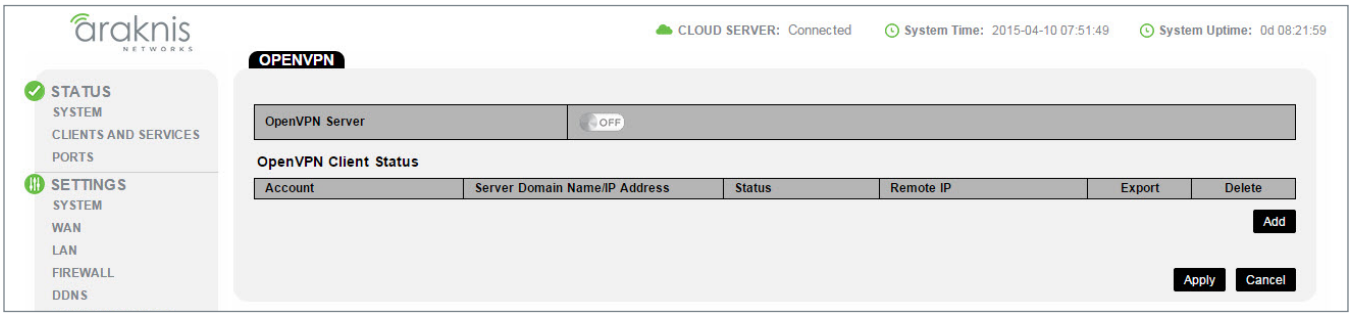
Note – When the PC client is connected to the VPN server, there will be one network adapter controlling the connection to the physical network the PC is on, and one running the VPN tunnel connection. The router's internal DHCP server will issue an IP address in the 172.0.0.XXX range to the PC network adapter for the VPN tunnel. The device will not appear in the router's DHCP list.

Also, local DNS addresses configured in the router will not function from VPN client-connected devices.

© 2015 Araknis Networks®

17.2.1 - OpenVPN Menu

Figure 75. OpenVPN Setup Page



Path – Advanced, VPN, OpenVPN

Parameters –

- **OpenVPN Server –** Click the button to turn the OpenVPN Server feature on or off.
  Default: Off.

17.2.2 - OpenVPN Client Status

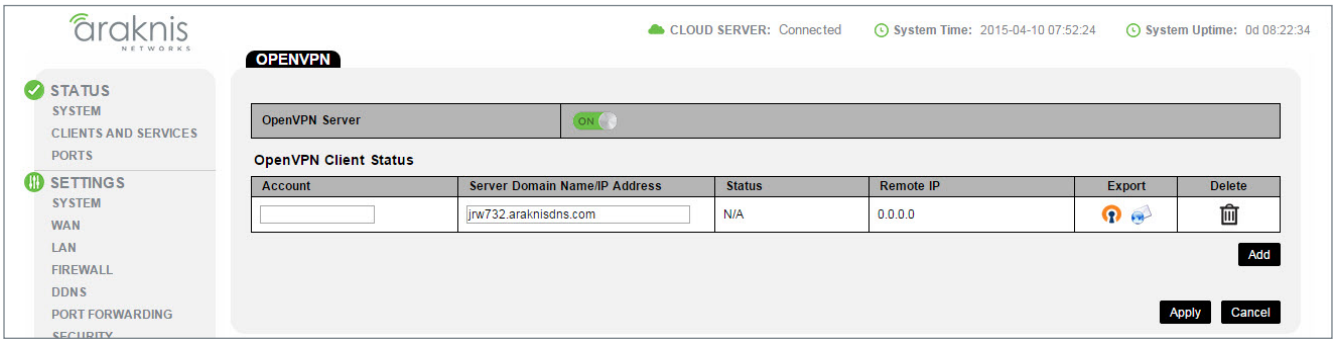
Parameters –

- **Account –** Username for the account.
- **Server Domain Name/IP Address –** WAN IP address of the server. This field should only be changed if a different DDNS service is being used, or if a static IP has been purchased for the Internet connection.
  Default: Displays current router DDNS address (if DDNS is configured)
- **Status –** Shows the current status of the account connection.
- **Remote IP –** Remote IP address of the device connecting to the account.
- **Export –** Save or email a copy of the client configuration file used to configure remote devices.
- **Delete –** Click the **Trashcan** to delete an existing static route.
- **Add –** Click to add a new client account entry.

© 2015 Araknis Networks®

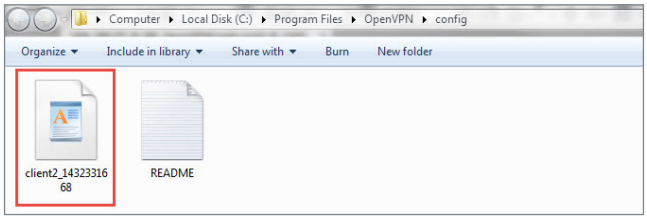
17.2.3 - Configuring OpenVPN Accounts in the Router

Figure 76. Adding a New OpenVPN Client



1. Log in to the router web interface and click Advanced, VPN, OpenVPN.
2. Click the **On/Off** button to turn the OpenVPN server ON.
3. Click **Add** to create a new account entry.
4. Enter a username in the Account field to identify the account user.
5. Do not change the Server Domain Name/IP Address field.
6. Click **Add** to create additional accounts or click **Apply** and confirm the new settings. Account setup in the router is now complete.
7. A configuration file must be exported and given to the OpenVPN client program on each device that will use an account. Click the button to export a copy of the configuration file to save, or click the button to email the file to a recipient. (The email server in the Security menu must be enabled to email OpenVPN files. See section *12.7.1.1 - Configuring Email Alerts (page 50)*for setup instructions.

Figure 77. OpenVPN Configuration File Saved



Guides for help with configuring client applications are available on the router product support tab for the following popular systems:

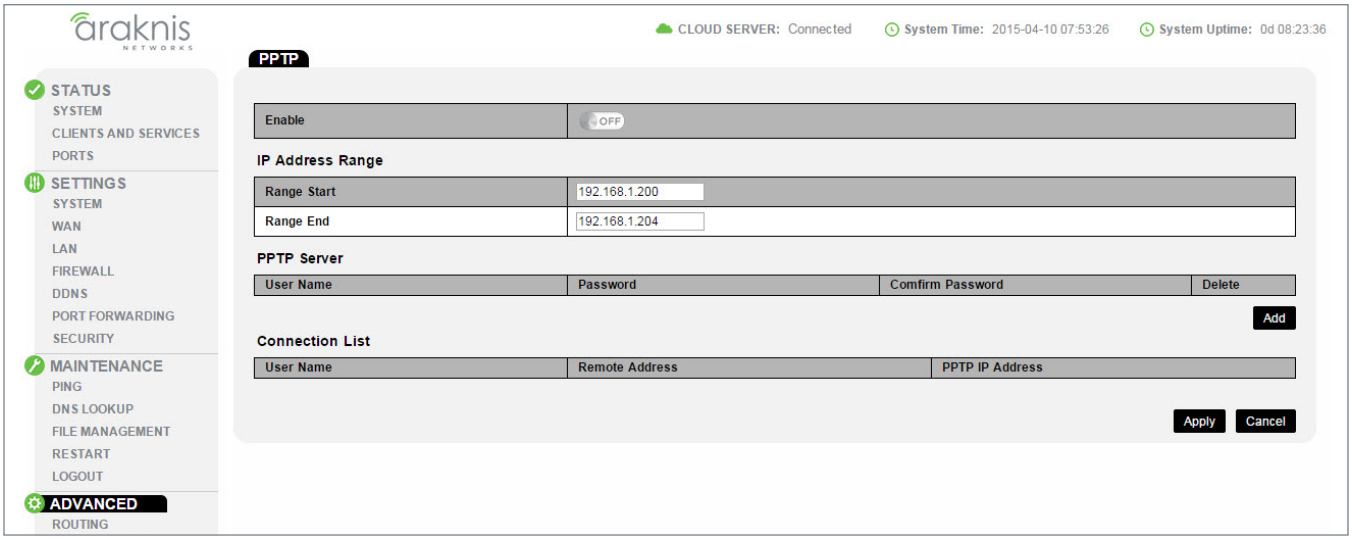
- Windows PC OpenVPN client
- iOS smartphone/tablet OpenVPN client
- Mac computer OpenVPN client

Note – When using a Windows-based OpenVPN client, always open the client by right-clicking and choose to *Run as Administrator*. The client program will not be able to access the remote network if this step is not taken.

© 2015 Araknis Networks®

17.3 - PPTP

Figure 78. PPTP Setup Menu



Path – Advance, VPN, PPTP

Parameters –

- **Enable –** Click the button to turn the PPTP feature on or off.
  Default: Off.

17.3.1 - IP Address Range

Parameters –

- **Range Start –** Enter the starting IP address in the range for PPTP configuration.
- **Range End –** Enter the ending IP address in the range for PPTP configuration.

17.3.2 - PPTP Server

Parameters –

- **User Name –** Enter the username for the account.
- **Password –** Enter the password for the account.
- **Confirm Password –** Re-enter the password to confirm it for the account.

17.3.3 - Connection List

Parameters –

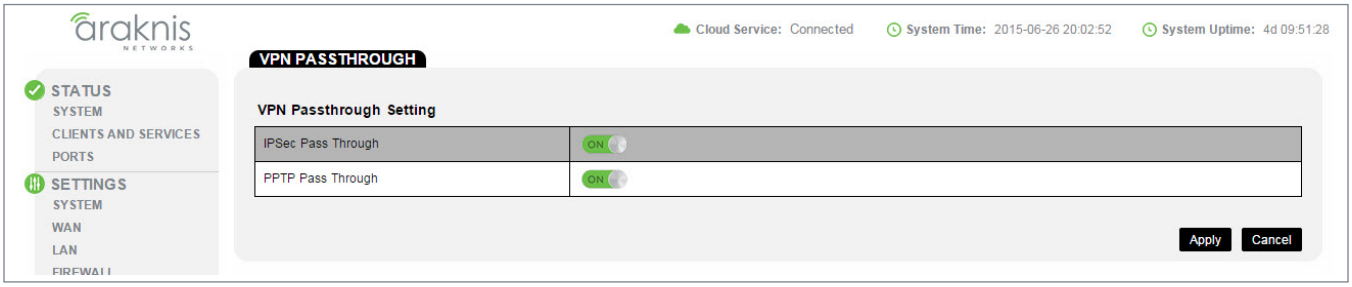
- **User Name –** Username of the user active on the connection.
- **Remote Address –** IP address where the connection is originating from.
- **PPTP IP Address –** LAN IP address assigned for use to the account.

© 2015 Araknis Networks®

17.4 - VPN Passthrough

Enable passthrough to allow IPSec and PPTP VPN traffic to cross the firewall.

Figure 79. VPN Passthrough Settings Screen



Path – Advance, VPN, VPN Passthrough

Parameters –VPN Passthrough Setting

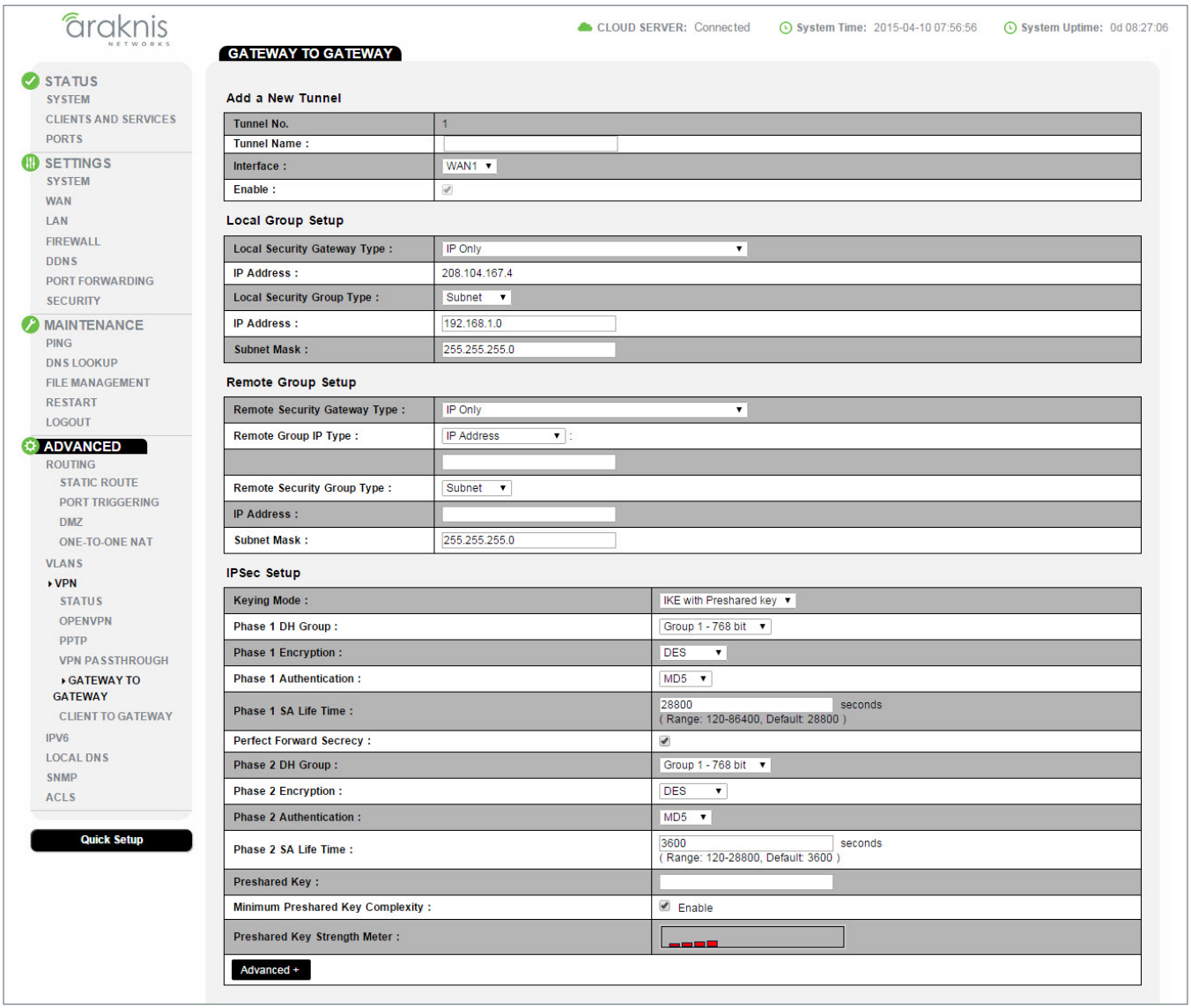
- **IPSec Pass Through –** Click the button to toggle IPSec passthrough on and off.
- **PPTP Pass Through –** Click the button to toggle PPTP passthrough on and off.

© 2015 Araknis Networks®

17.5 - Gateway to Gateway

Configure a VPN between two routers so that devices on each network can communicate through the VPN tunnel.

Figure 80. Gateway to Gateway

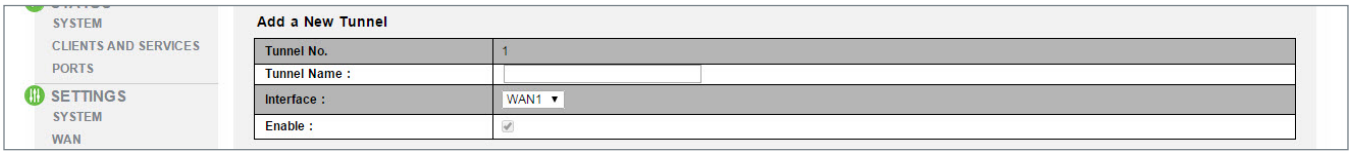


Path – Advanced, VPN, Gateway to Gateway

© 2015 Araknis Networks®

17.5.1 - Add a New Tunnel

Figure 81. Add a New Tunnel



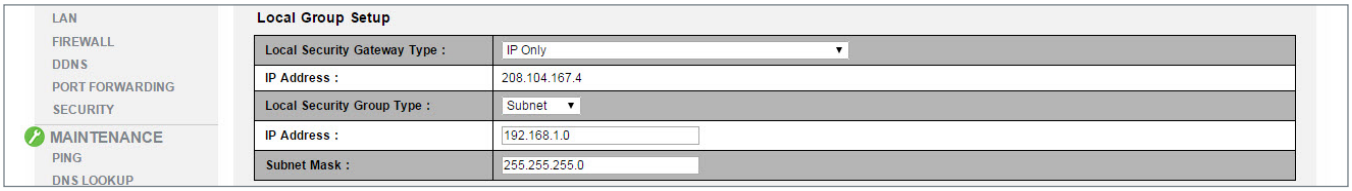
Path – Advanced, VPN, Gateway to Gateway

Parameters –

- **Tunnel No. –** Number identifying the tunnel being configured.
- **Tunnel Name –** Name for the tunnel to make it easily identifiable.
- **Interface –** Port the VPN will connect through. Options: WAN1, WAN2.
- **Enable –** Check the box to enable the new tunnel.

17.5.2 - Local Group Setup

Figure 82. Local Group Setup



Path – Advanced, VPN, Gateway to Gateway

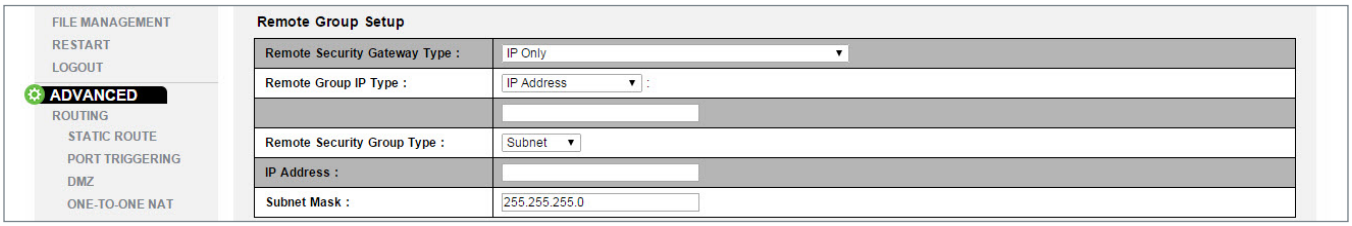
Parameters –

- **Local Security Gateway Type –** Set the Local Security Gateway Type.
- **IP Address –** IP address for the local group.
- **Local Security Group Type –** Set the security type from the dropdown.
- **IP Address –** IP address for the network device connecting to the local group.
- **Subnet Mask –** Subnet mask for the connection.

© 2015 Araknis Networks®

17.5.3 - Remote Group Setup

Figure 83. Remote Group Setup



Path – Advanced, VPN, Gateway to Gateway

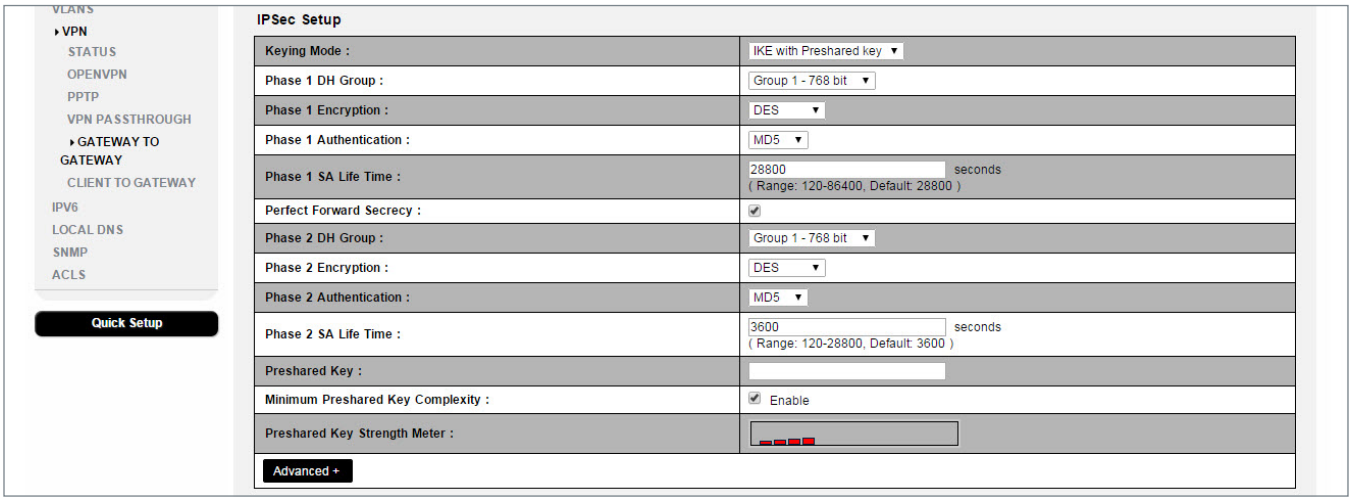
Parameters –

- **Remote Security Gateway Type –** Set the Remote Security Gateway Type.
- **Remote Group IP Type –** Set the IP type for the remote group.
- **Remote Security Group Type –** Set the Remote Security Group Type.
- **IP Address –** IP address of the remote group.
- **Subnet Mask –** Subnet mask of the remote group.

© 2015 Araknis Networks®

17.5.4 - IPSec Setup

Figure 84. IPSec Setup



Path – Advanced, VPN, Gateway to Gateway

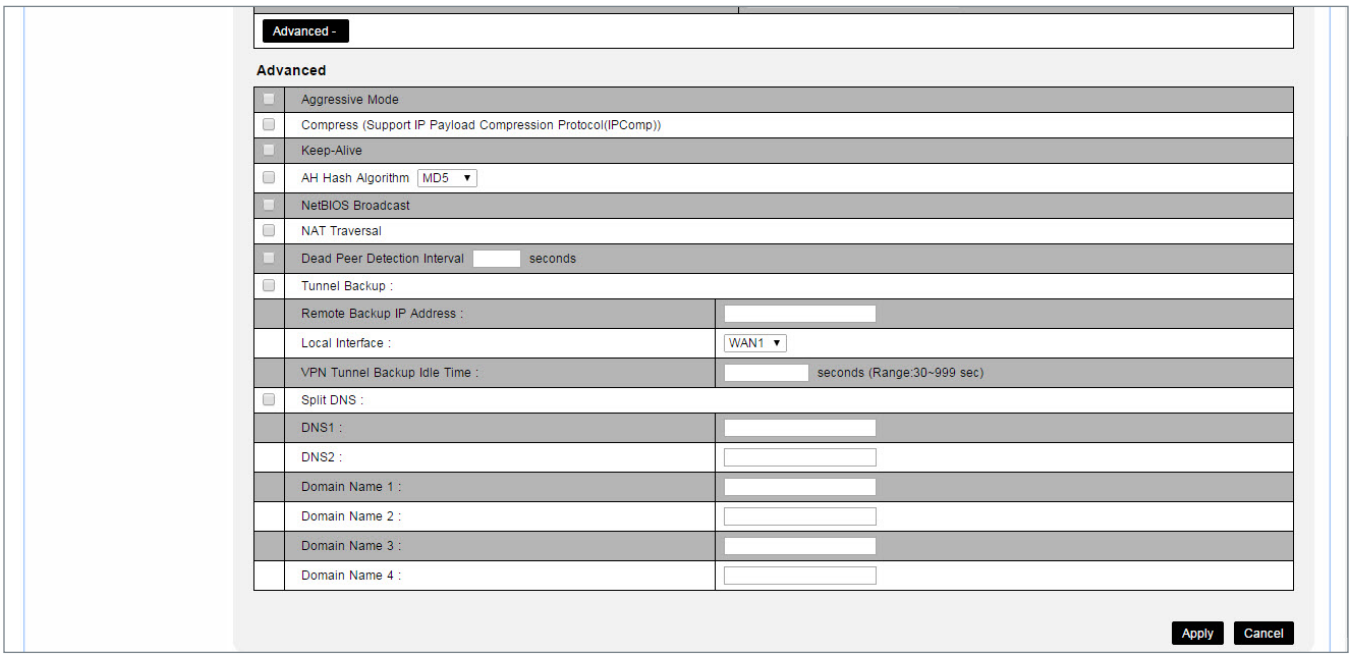
Parameters –

- **Keying Mode –** Select a mode from the dropdown. Options: Manual, IKE with Preshared key.
- **Phase 1 DH Group –** Select a group from the dropdown. Options, Group 1 – 768 Bit, Group 2 – 1024 Bit, Group 5 – 1536 Bit.
- **Phase 1 Encryption –** Select a type from the dropdown. Options: DES, 3DES, AES-128, AES-192, AES-256.
- **Phase 1 Authentication –** Select a mode from the dropdown. Options: MD5, SHA1.
- **Phase 1 SA Life Time –** Enter a range between 120 and 86400.
  Default: 28800.
- **Perfect Forward Secrecy –** Check to enable secrecy.
- **Phase 2 DH Group –** Select a group from the dropdown. Options, Group 1 – 768 Bit, Group 2 – 1024 Bit, Group 5 – 1536 Bit.
- **Phase 2 Encryption –** Select a type from the dropdown. Options: DES, 3DES, AES-128, AES-192, AES-256.
- **Phase 2 Authentication –** Select a mode from the dropdown. Options: MD5, SHA1.
- **Phase 2 SA Life Time –** Enter a range between 120 and 28800.
  Default: 3600.
- **Preshared Key –** Shared password for accessing the connection.
- **Minimum Preshared Key Complexity –** Enable this setting to enforce a minimum level of pre-shared key complexity.
- **Preshared Key Strength Meter –** Indicated the strength of the pre-shared key. Use a combination of letters, number, and symbols to make the key more secure.
- **See advanced features on the next page.**

© 2015 Araknis Networks®

Advanced IPSec Setup Options

Figure 85. Gateway to Gateway Advanced Settings



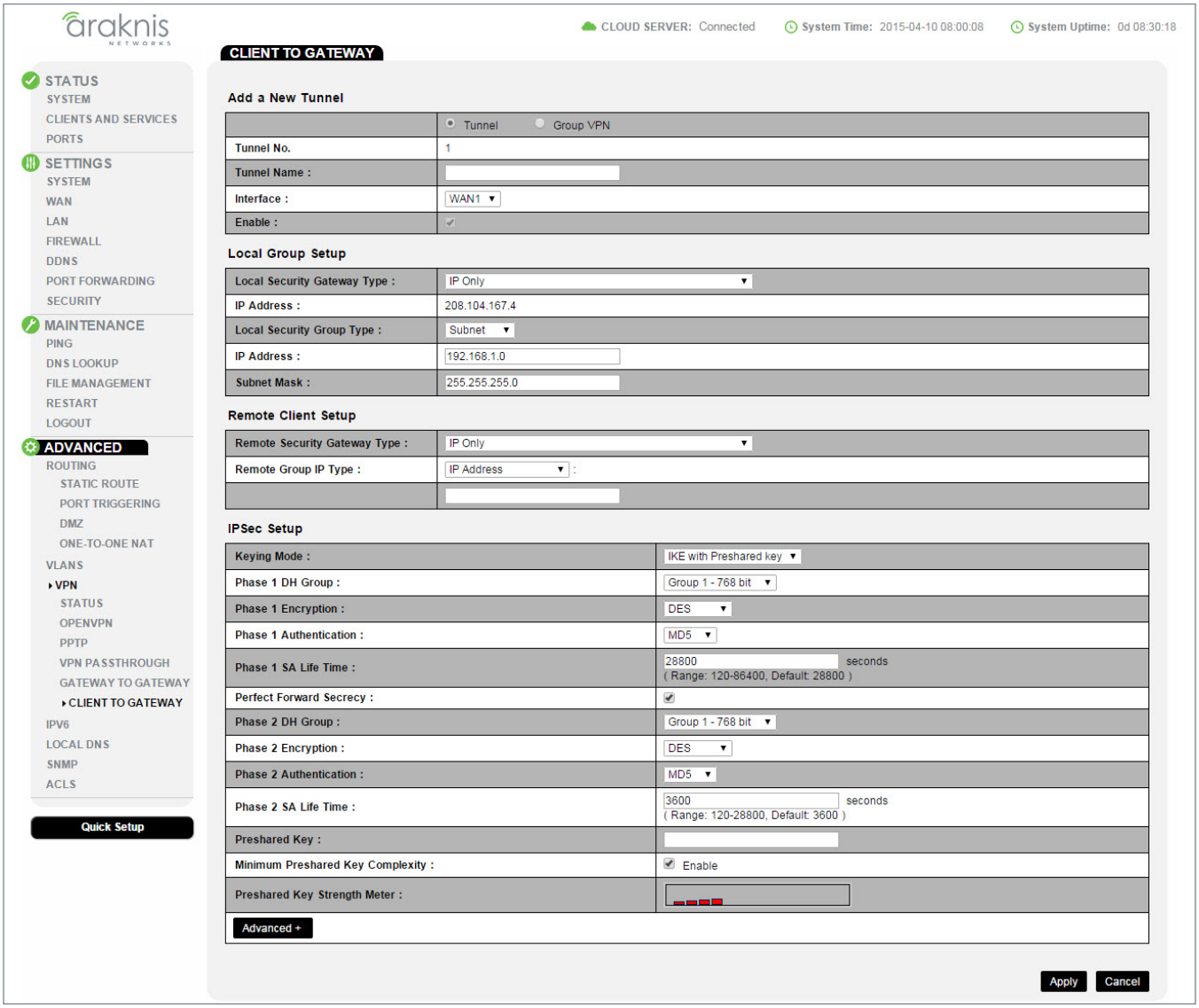
- **Aggressive Mode –** Check the box to enable Aggressive Mode.
- **Compress (Support IP Payload Compression Protocol(IPComp)) –** Check to enable Compress.
- **Keep-Alive –** Check to enable Keep-Alive.
- **AH Hash Algorithm –** Check to enable AH Hash Algorithm Select the type from the dropdown.
- **NetBIOS Broadcast –** Check to enable NetBIOS Broadcast.
- **NAT Traversal –** Check to enable NAT Transversal.
- **Dead Peer Detection Interval (Seconds) –** Check to enable and set the Dead Peer Detection Interval.
- **Tunnel Backup –** Check to enable Tunnel Backup. Enter the following values to configure the setting:
  - **Remote Backup IP Address –** Enter the IP address of the backup tunnel.
  - **Local Interface –** Select which port to use for connecting the backup tunnel.
  - **VPN Tunnel Backup Idle Time (seconds) –** Set the amount of time to wait before switching to the backup tunnel. (Range: 30~999)
- **Split DNS –** Check to enable Split DNS.
  - **DNS1/DNS2 –** Enter the Split DNS addresses.
  - **Domain Name 1/2/3/4 –** Enter up to four domain names.

© 2015 Araknis Networks®

17.6 - Client to Gateway

Set up a custom VPN tunnel between a client device and the router.

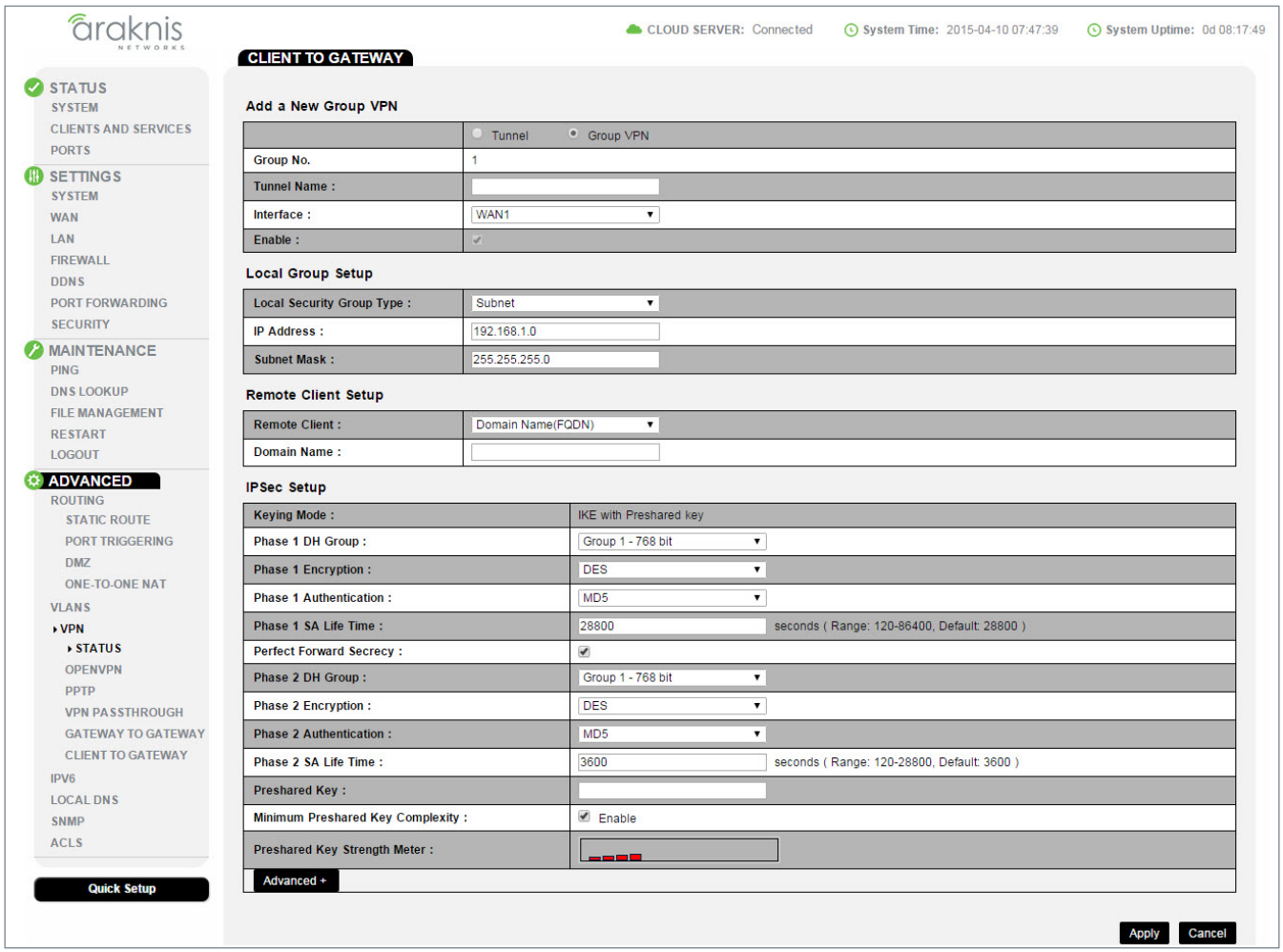
Figure 86. Tunnel Mode



Path – Advanced, VPN, Client to Gateway

© 2015 Araknis Networks®

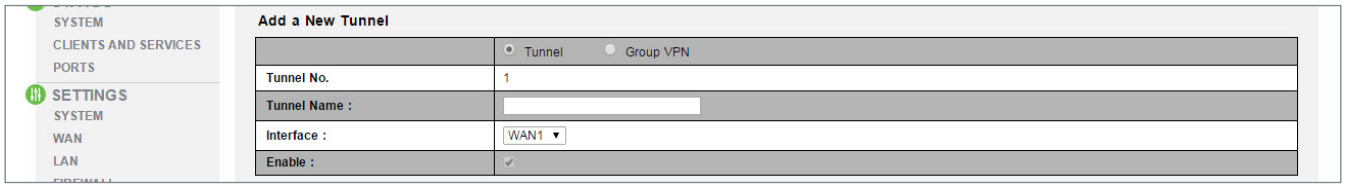
Figure 87. Group Mode



© 2015 Araknis Networks®

17.6.1 - Add a New Tunnel

Figure 88. Add a New Tunnel



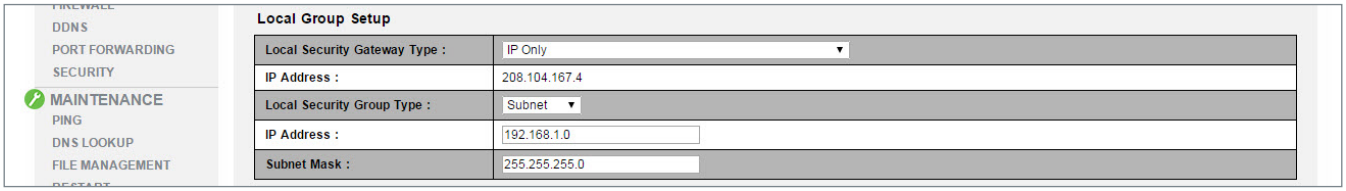
Path – Advanced, VPN, Client to Gateway

Parameters –

- **Tunnel No. –** Number identifying the tunnel being configured.
- **Tunnel Name –** Name for the tunnel to make it easily identifiable.
- **Interface –** Port the VPN will connect through. Options: WAN1, WAN2.
- **Enable –** Check the box to enable the new tunnel.

17.6.1.1 - Local Group Setup

Figure 89. Local Group Setup



Path – Advanced, VPN, Client to Gateway

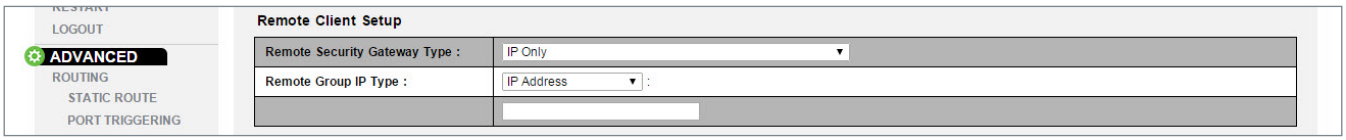
Parameters –

- **Local Security Gateway Type –** Set the Local Security Gateway Type.
- **IP Address –** IP address for the local group.
- **Local Security Group Type –** Set the security type from the dropdown.
- **IP Address –** IP address for the network device connecting to the local group.
- **Subnet Mask –** Subnet mask for the connection.

© 2015 Araknis Networks®

17.6.1.2 - Remote Client Setup

Figure 90. Remote Client Setup



Path – Advanced, VPN, Client to Gateway

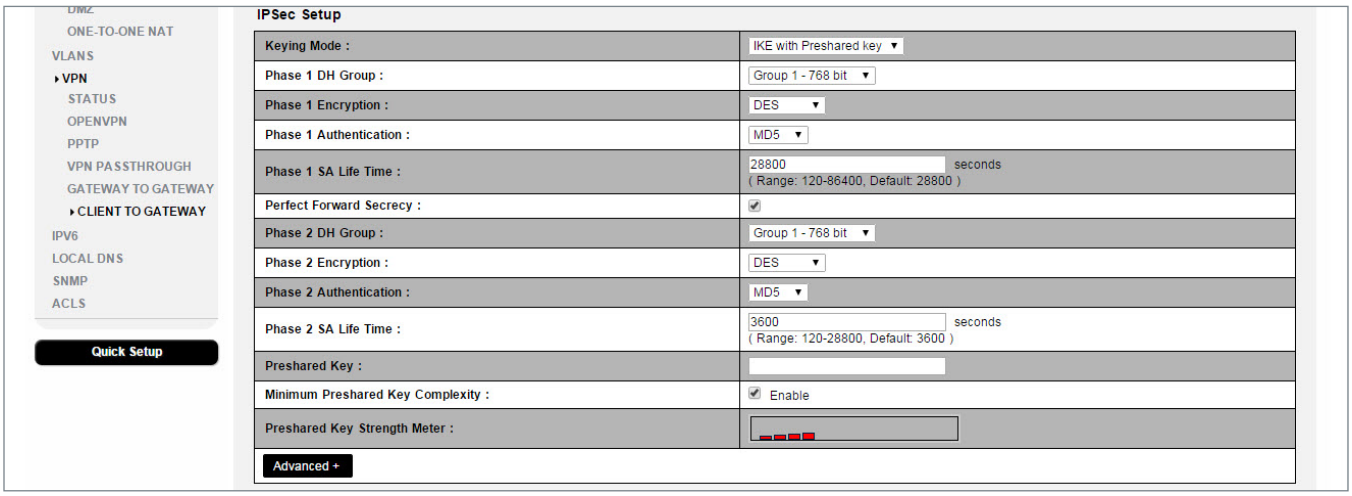
Parameters –

- **Remote Security Gateway Type –** Set the Remote Security Gateway Type.
- **Remote Group IP Type –** Set the IP type for the remote group.
- **<field left blank> –** Enter the remote IP address.

© 2015 Araknis Networks®

17.6.1.3 - IPSec Setup

Figure 91. Add a New Tunnel



Path – Advanced, VPN, Client to Gateway

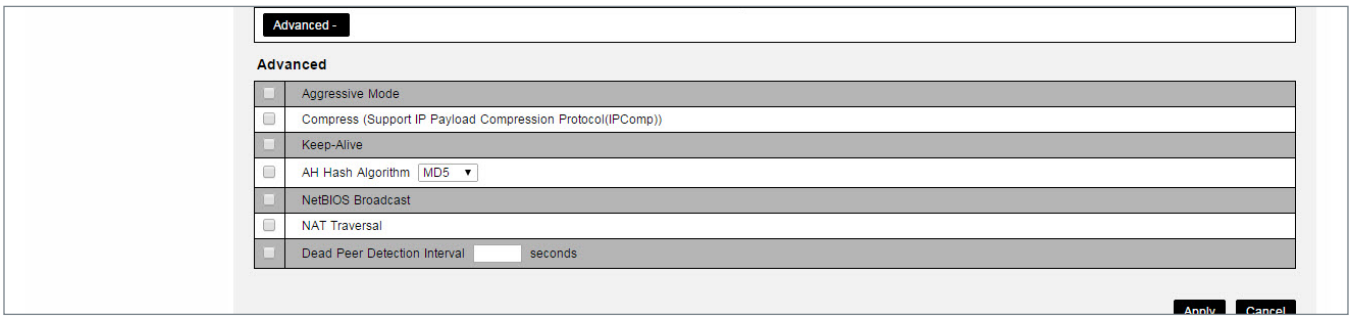
Parameters –

- **Keying Mode –** Select a mode from the dropdown. Options: Manual, IKE with Preshared key.
- **Phase 1 DH Group –** Select a group from the dropdown. Options, Group 1 – 768 Bit, Group 2 – 1024 Bit, Group 5 – 1536 Bit.
- **Phase 1 Encryption –** Select a type from the dropdown. Options: DES, 3DES, AES-128, AES-192, AES-256.
- **Phase 1 Authentication –** Select a mode from the dropdown. Options: MD5, SHA1.
- **Phase 1 SA Life Time –** Enter a range between 120 and 86400.
  Default: 28800.
- **Perfect Forward Secrecy –** Check to enable secrecy.
- **Phase 2 DH Group –** Select a group from the dropdown. Options, Group 1 – 768 Bit, Group 2 – 1024 Bit, Group 5 – 1536 Bit.
- **Phase 2 Encryption –** Select a type from the dropdown. Options: DES, 3DES, AES-128, AES-192, AES-256.
- **Phase 2 Authentication –** Select a mode from the dropdown. Options: MD5, SHA1.
- **Phase 2 SA Life Time –** Enter a range between 120 and 28800.
  Default: 3600.
- **Preshared Key –** Shared password for accessing the connection.
- **Minimum Preshared Key Complexity –** Enable this setting to enforce a minimum level of pre-shared key complexity.
- **Preshared Key Strength Meter –** Indicated the strength of the pre-shared key. Use a combination of letters, number, and symbols to make the key more secure.
- **See advanced features on the next page.**

© 2015 Araknis Networks®

Advanced IPSec Setup Options

Figure 92. Tunnel Mode Advanced



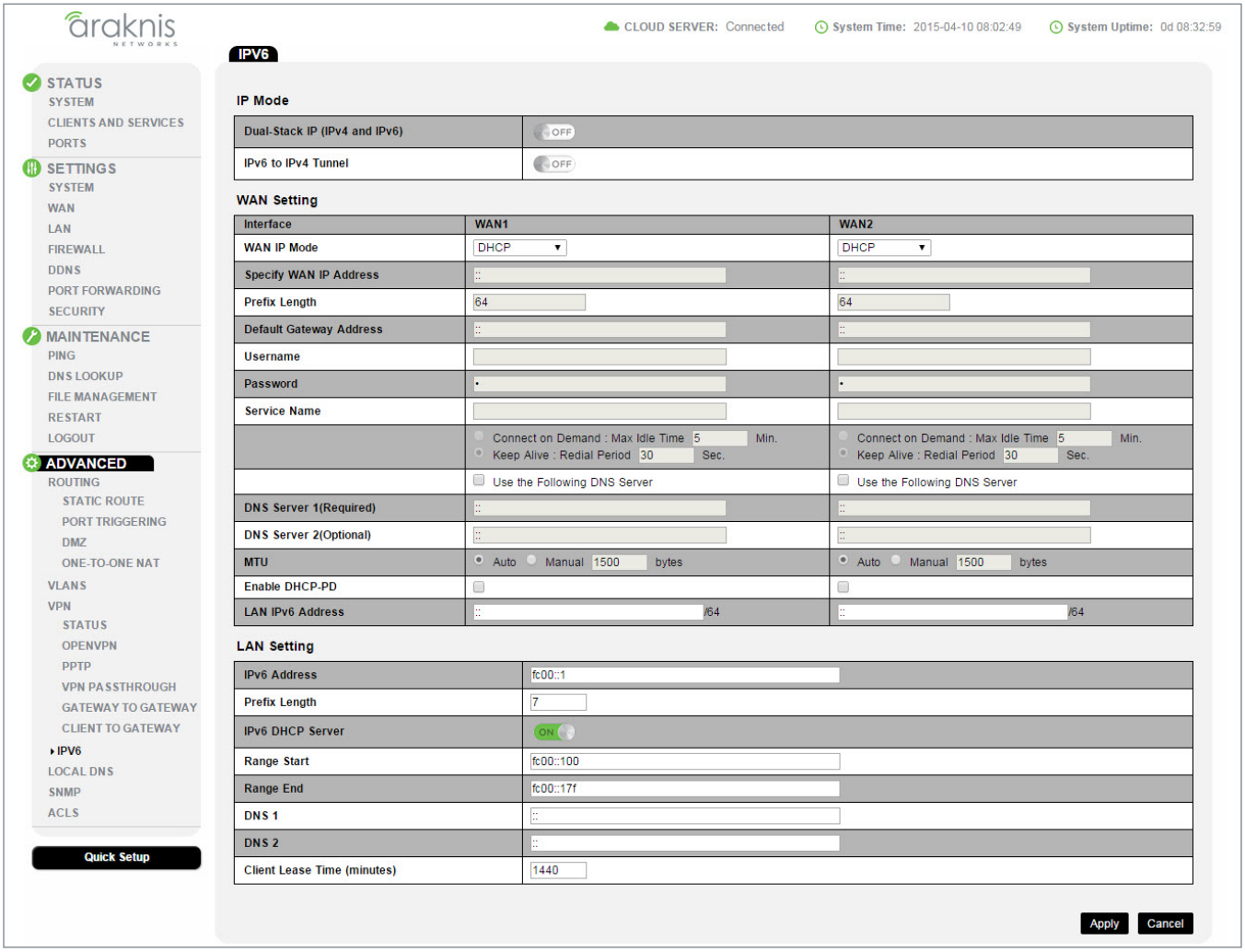
- **Aggressive Mode –** Check the box to enable Aggressive Mode.
- **Compress (Support IP Payload Compression Protocol(IPComp)) –** Check to enable Compress.
- **Keep-Alive –** Check to enable Keep-Alive.
- **AH Hash Algorithm –** Check to enable AH Hash Algorithm Select the type from the dropdown.
- **NetBIOS Broadcast –** Check to enable NetBIOS Broadcast.
- **NAT Traversal –** Check to enable NAT Transversal.
- **Dead Peer Detection Interval (Seconds) –** Check to enable and set the Dead Peer Detection Interval.

© 2015 Araknis Networks®

17.7 - IPv6

Enable and configure IPv6 network addressing.

Figure 93. IPv6 Setup Menu



Path – Advanced, IPv6

17.7.1 - IP Mode

Figure 94. IP Mode

Path – Advanced, IPv6

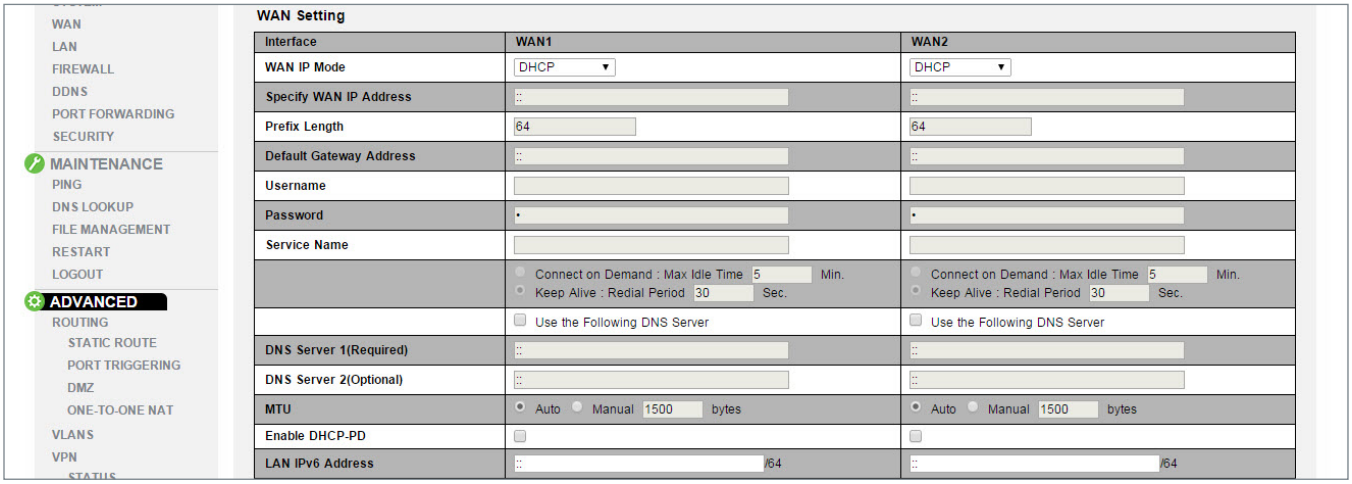
Parameters –

- **Dual-Stack IP (IPv4 and IPv6) –** Toggle Dual-Stack mode on and off.
  Default: Off
- **IPv6 to IPv4 Tunnel –** Toggle the IPv6 to IPv4 tunnel on and off.
  Default: Off

© 2015 Araknis Networks®

17.7.1.1 - WAN Setting

Figure 95. WAN Setting



Path – Advanced, IPv6

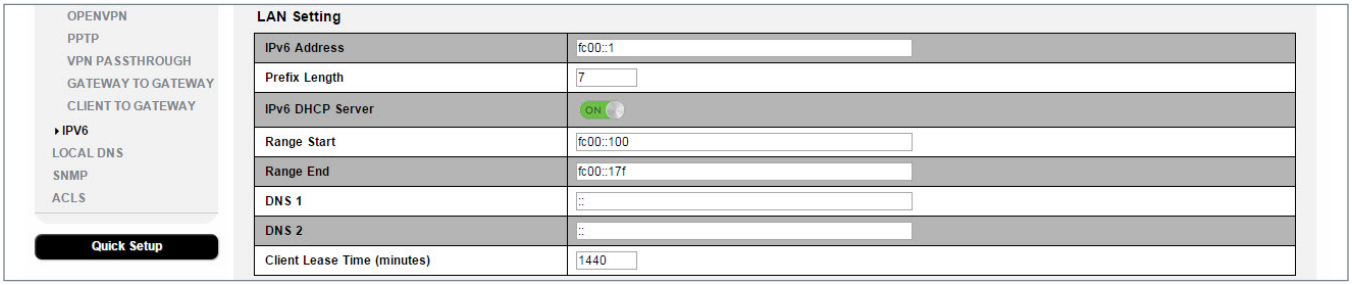
Parameters –

- **Interface –** Settings listed for the WAN1 and WAN2 interfaces.
- **WAN IP Mode –** Select the connection IP mode. Options: DHCP, Static IP, PPPoE.
  Default: DHCP
- **Specify WAN IP Address –** Enter the WAN IP address for the interface. Only for Static IP addresses.
- **Prefix Length –** Length of the prefix.
  Default: 64
- **Default Gateway Address –** Default gateway address. Only for Static IP mode.
- **Username –** Username for PPPoE connections.
- **Password –** Password for PPPoE connections.
- **Service Name –** Service name for PPPoE mode.
- **Connect on Demand –** Set a PPPoE connection to disconnect after the specified amount of idle time.
  Default: 5 minutes
- **Keep Alive –** Set a PPPoE account to reconnect after the time set, in the event of a disconnection.
  Default: 30 seconds
- **Use the Following DNS Server –** Check to enable custom DNS settings for a PPPoE connection.
  - **DNS Server 1(Required) –** Enter the primary DNS Server for the connection.
  - **DNS Server 2(Optional) –** Enter the secondary DNS Server for the connection.
- **MTU –** Maximum Transmission Unit specifies the largest packet or frame size that can be transmitted across the WAN interface. Use the Auto setting unless the ISP specifies to use a certain MTU value.
  Default: Auto
- **Enable DHCP-PD –** Check to enable prefix delegation.
- **LAN IPv6 Address/64 –** Enter the LAN IPv6 address.

© 2015 Araknis Networks®

17.7.1.2 - LAN Setting

Figure 96. LAN Setting



Path – Advanced, IPv6

Parameters –

- **IPv6 Address –** Enter the LAN IPv6 Address.
- **Prefix Length –** Set how many bits represent the network part of the address.
- **IPv6 DHCP Server –** Enable or disable the IPv6 DHCP Server.
- **Range Start –** Enter a starting IPv6 address for the DHCP server address range.
- **Range End –** Enter an ending IPv6 address for the DHCP server address range.
- **DNS 1 –** Enter the primary IPv6 DNS address.
- **DNS 2 –** Enter the secondary IPv6 DNS address.
- **Client Lease Time –** Number of minutes that a DHCP address lease will last.
  Default: 1440 (24 hours)

© 2015 Araknis Networks®

17.8 - Local DNS

Configure the Local DNS server to assign unique domain addresses to connected LAN devices. Use the domain address to access a device without having to remember the IP address.

Note – Before configuring Local DNS, complete these steps for each device being configured:

- Reserve an IP address for each device being configured, or set each device to have a static IP address. Using a DHCP address could cause the domain name to point to a different device if the address is reissued after setup. See *12.3.3 - DHCP Reservation Table (page 39)*.
- Set the DNS server setting in each device to the same IP address as the router (default: 192.168.1.1).

Figure 97. Local DNS Setup Page

Path – Advanced, Local DNS Database

Parameters –

- **Domain Name –** Enter a domain name for local DNS server addresses. Local DNS domains usually end in ***.local***, and may contain anything that a website URL can contain and be up to 40 characters in length.
  Default: router<MAC address>.com
- **Host Name –** Enter a host name for the device. The router will auto-fill the full address after moving to the next field. For example, if you entered ***Router1***, the local DNS address for that device would be ***Router1.smithrouter.local***.
- **IP Address –** Enter the LAN IP address of the device being configured.
- **IP Mode –** Select the IP mode of the connection. Options: IPv4, IPv6.
  Default: IPv4

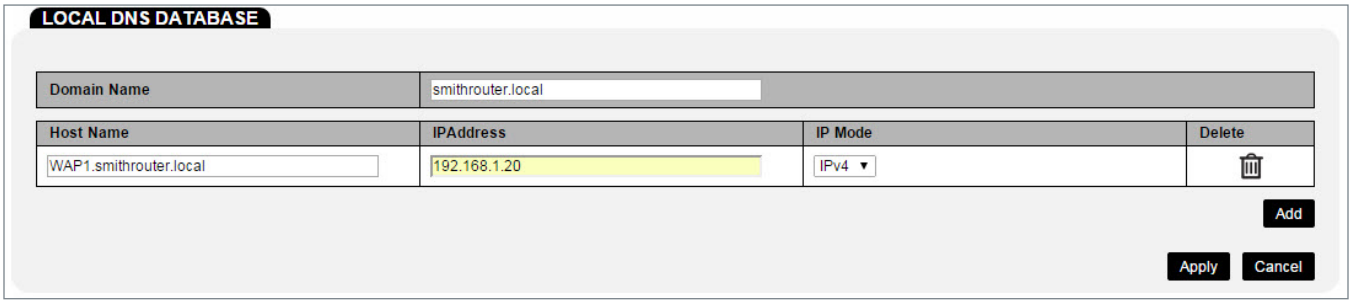
© 2015 Araknis Networks®

17.8.1 - Configuring Local DNS

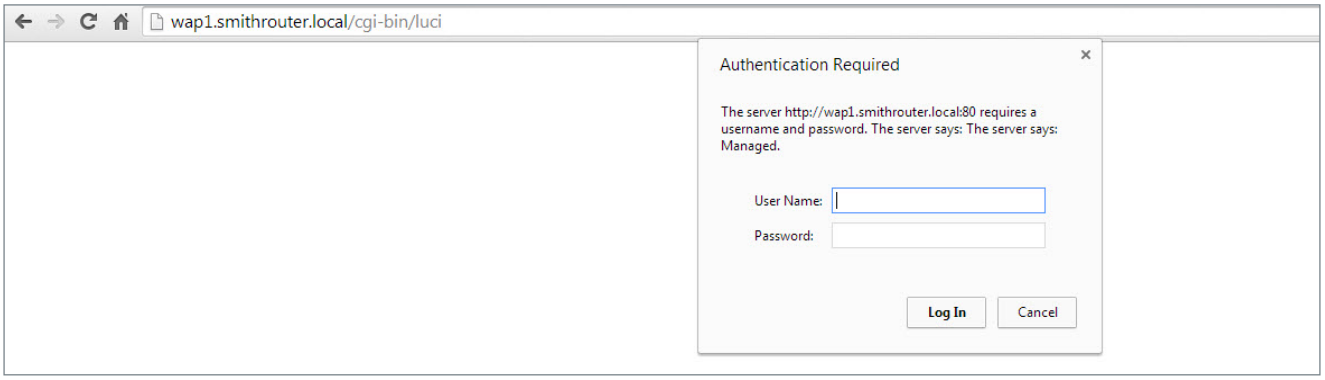
Note – Before configuring Local DNS, complete these steps for each device being configured:

- Reserve an IP address for each device being configured or set each device to have a static IP address. Using a DHCP address could cause the domain name to point to a different device if the address is reissued after setup. See *12.3.3 - DHCP Reservation Table (page 39)*.
- Set the DNS server setting in each device to the same IP address as the router (default: 192.168.1.1).

Figure 98. Local DNS Configuration



1. Log into the router and navigate to Advanced, Local DNS using the navigation menu.
2. Enter a Domain Name in the field for device addresses.
3. Click **Add** to create a new entry field.
4. Enter a Host Name and the IP address of the network device being configured. Do not change the IP mode unless the network is configured for IPv6.
5. Click **Add** to create additional entries, or **Apply** to save the new settings.
6. Test the new entries by entering the domain name for each device into a web browser (computer must be on the same network with the devices).



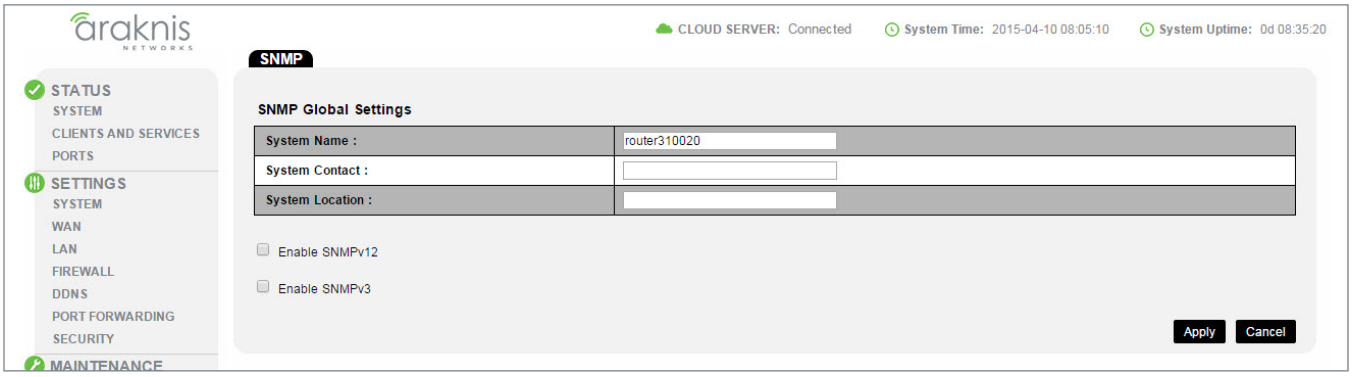
7. If you can't connect to a device, try accessing it using the IP address. If that works, there is an issue with the DNS settings. If the IP address does not work, the IP address of the device has changed.

© 2015 Araknis Networks®

17.9 - SNMP

Simple Network Management Protocol is used by network administrators to monitor the performance and settings of network devices. Configure SNMP to communicate with management devices in place on the network.

Figure 99. SNMP Settings Menu (SNMPv12 & SNMPv3 enabled to show available settings)



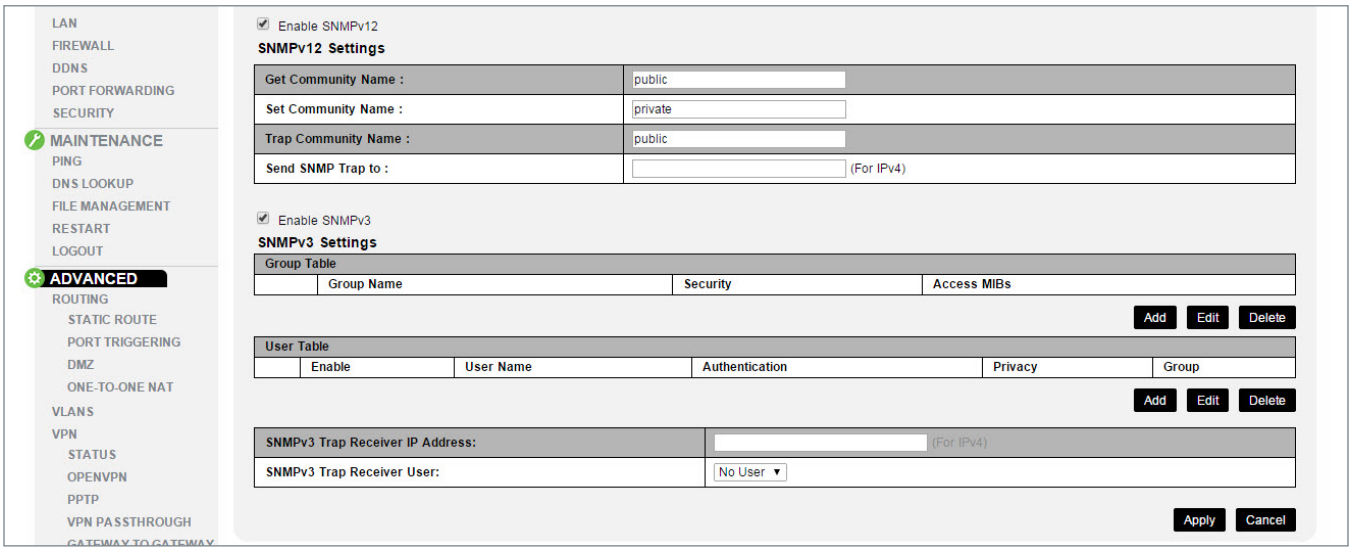
Path – Advanced, SNMP

17.9.1.1 - SNMP Global Settings

Parameters –

- **System Name –** Enter the system name required for SNMP configuration.
- **System Contact –** Enter the system contact required for SNMP configuration.
- **System Location –** Enter the system location required for SNMP configuration.
- **Enable SNMPv2 –** Check the box to enable SNMPv12.
- **Enable SNMPv3 –** Check the box to enable SNMPv3.

Figure 100. SNMPv2 & SNMPv3 Settings

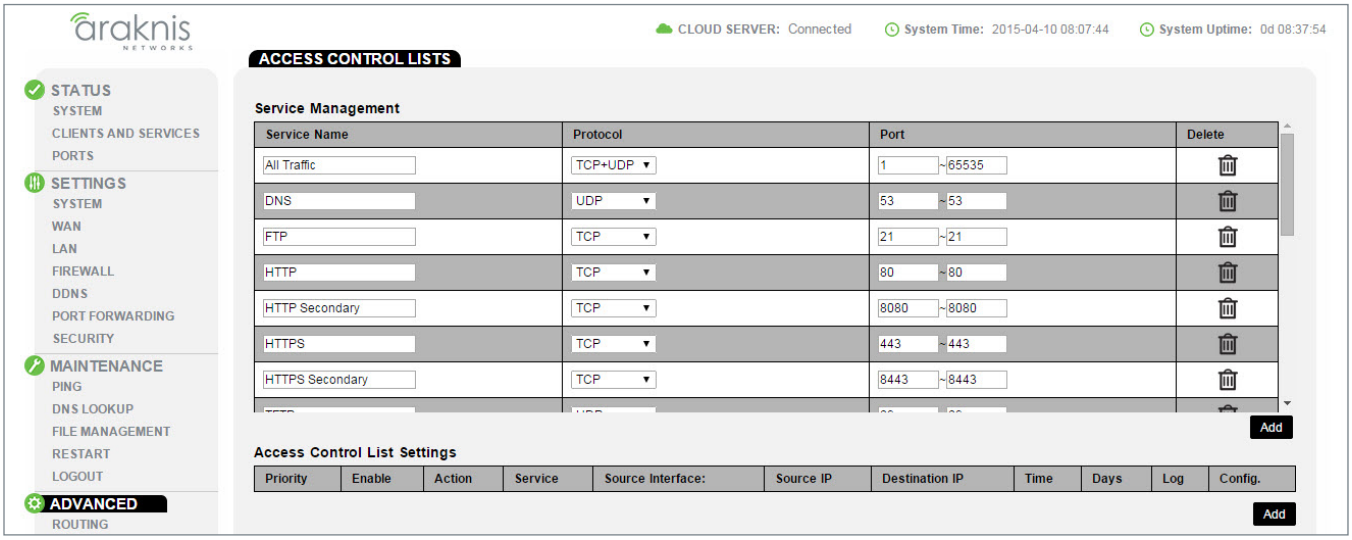


© 2015 Araknis Networks®

17.10 - ACLs

Use Access Control List entries to restrict undesired port use.

Figure 101. Access Control Lists (ACLs) Menu



Path – Advanced, Access Control Lists

17.10.1 - Service Management

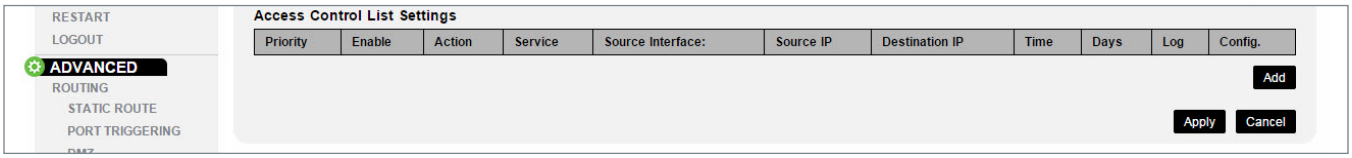
Parameters –

- **Service Name –** Enter a name to identify the service rule.
- **Protocol –** Set the protocol the service rule affects.
- **Port –** Set the start and end port to enforce the service rule on.
- **Delete –** Click the **Trashcan** to delete a service rule.

© 2015 Araknis Networks®

17.10.2 - Access Control List Settings

Figure 102. Access Control List Settings



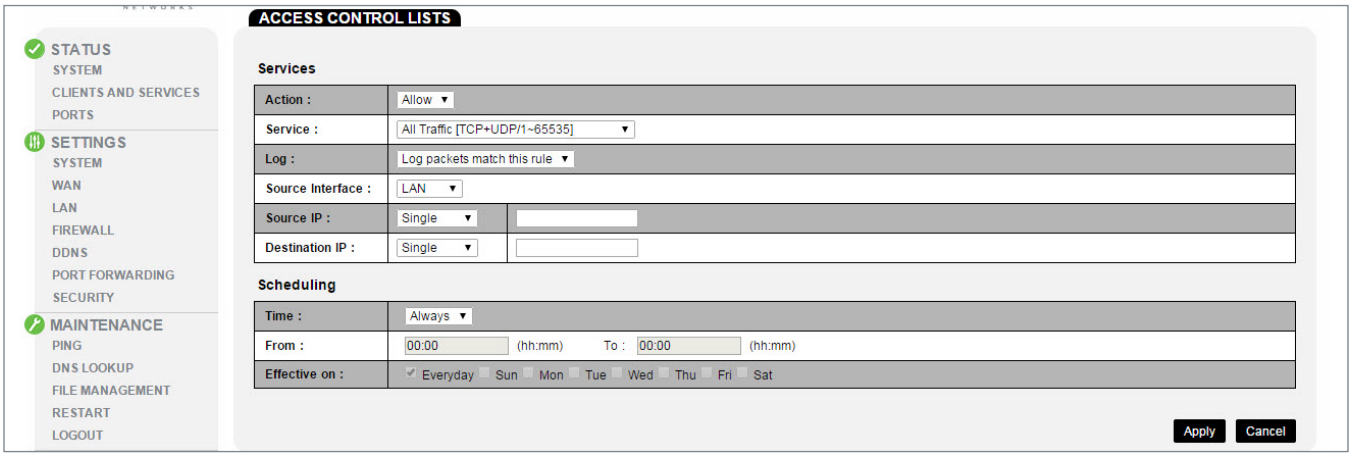
Parameters –

- **Priority –** Select the priority of the rule from the drop down. The rules are enforced in order: ***Priority 1*** takes precedence over all other rules (2, 3, 4...).
- **Enable –** Check the box to enable the rule.
- **Action –** Displays whether the rule is set to allow or disallow traffic.
- **Service –** Describes the traffic and ports enforced by the rule.
- **Source Interface –** Displays whether the source interface is WAN or LAN-based.
- **Source IP –** Displays the source IP address controlled by the rule.
- **Destination IP –** Displays the destination IP address controlled by the rule.
- **Time –** Describes when the rule is in effect.
- **Days –** Describes what days the rule will be active.
- **Log –** Describes whether activity based on the rule will be recorded in the system log.
- **Config. –** Click the **Note** icon to edit the settings for a rule or the **Trashcan** to delete a rule.
- **Add –** Click to add a new Access Control Rule.

© 2015 Araknis Networks®

17.10.3 - Adding a New Access Control Rule

Figure 103. Add New Access Control List Entry



1. Click Add to open the **Services** and **Scheduling** page.
2. Set the desired Action, Service, and Log settings using the dropdowns.
3. Select the source of the traffic to control from the dropdown.
4. Enter a Source IP address or range the traffic will come from.
5. Enter a Destination IP address or range the traffic will be traveling toward.
6. Set up scheduling for when the rule will be active. If the rule needs to be active at all times, leave **Time** set to ***Always***.
7. Click **Apply** to enable the newly created rule.

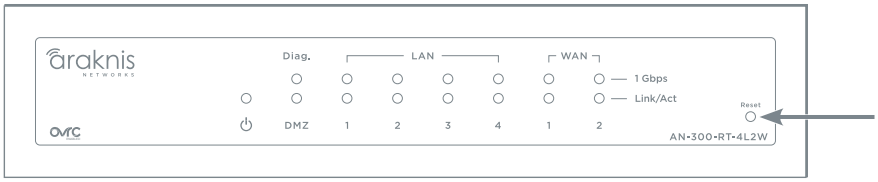
© 2015 Araknis Networks®

18 - Troubleshooting

18.1 - Resetting the Router

> **Note –** Use a ballpoint pen or a pencil to press the reset button.

Figure 105. Reset Button



Configuration Instructions –

- **Basic Reset –** Press for 10 seconds. The Diag. LED will flash slowly until the procedure is complete. The router will reboot and no settings will be changed.
- **Factory Reset –** Press for 20 seconds. The Diag. LED will flash rapidly until the procedure is complete. All settings will be reset to default. The current firmware version will not change.

© 2015 Araknis Networks®

20 - Specifications

Features	
WAN - RJ45 10/100/1000 Base-T	2
LAN - RJ45 10/100/1000 Base-T	4
Performance	
LAN - LAN Throughput	1 Gbps
WAN - LAN Throughput	492 Mbps
IPSec Throughput	75 Mbps
SDRAM	256 MB DDR2
Flash ROM	32 MB
L3 Features	
WAN Load-balancing	Yes
WAN Link Failover	Yes
Static Routing	Yes
Inter-VLAN Routing	Yes
DHCP Server	Yes
DHCP Client	Yes
DHCP Relay	Yes
DNS Relay	Yes
DDNS	Yes
1:1 NAT	Yes
PAT (Port Address Translation)	Yes
Port Trigger	Yes
DMZ Host	Yes
IPv6	Yes
L2 Features	
VLANs	Yes - 802.1Q
RJ45 Auto-sensing	Yes
RJ45 Auto-negotiation	Yes
Security	
Stateful Firewall	Yes
Stateful Packet Inspection (SPI)	Yes
DoS Prevention	Yes
Ping of Death	Yes
SYN Flood	Yes
IP Spoofing	Yes
Port Forwarding	Yes
Content Filtering (URL & Keyword)	Yes
Access Control List	Yes
UPnP	Yes
Bonjour	Yes
Auto Reboot	Yes

© 2015 Araknis Networks®

VPN Features	
IPSec	Yes
PPTP Server	Yes
PPPoE	Yes
OpenVPN	Yes
Encryption	DES, 3DES, AES-128, AES-192, AES-256
Authentication	MD5/SHA-1
Management	
Web Management	Yes
SNMP v1,2c,3	Yes
E-mail Alert	Yes
Download/Upload Config File	Yes
System Log	Yes
HTTP & HTTPs	Yes
System Time	NTP/Manually
Cloud Management	Yes
Environmental & Physical	
Product Dimensions (W x H x D) in inches	8.1 x 1.7 x 5.2
External Power Supply	12V 1A DC
Operating Temperature	0ºC to 40ºC (32ºF to 104ºF)
Storage Temperature	0ºC to 70ºC (32ºF to 158ºF)
Operating Humidity	10% to 85% non-condensing
Storage Humidity	5% to 90% non-condensing
Certifications	CE, FCC, UL

© 2015 Araknis Networks®

21 - 2-Year Limited Warranty

Araknis Networks products have a 2-Year Limited Warranty. This warranty includes parts and labor repairs on all components found to be defective in material or workmanship under normal conditions of use. This warranty shall not apply to products that have been abused, modified, or disassembled. Products to be repaired under this warranty must be returned to SnapAV or a designated service center with prior notification and an assigned return authorization number (RA).

22 - Contacting Technical Support

P: (866) 838-5052

E: techsupport@araknisnetworks.com

© 2015 Araknis Networks®

© 2015 Araknis Networks®

150629-1345