

May 2012
Revision 1

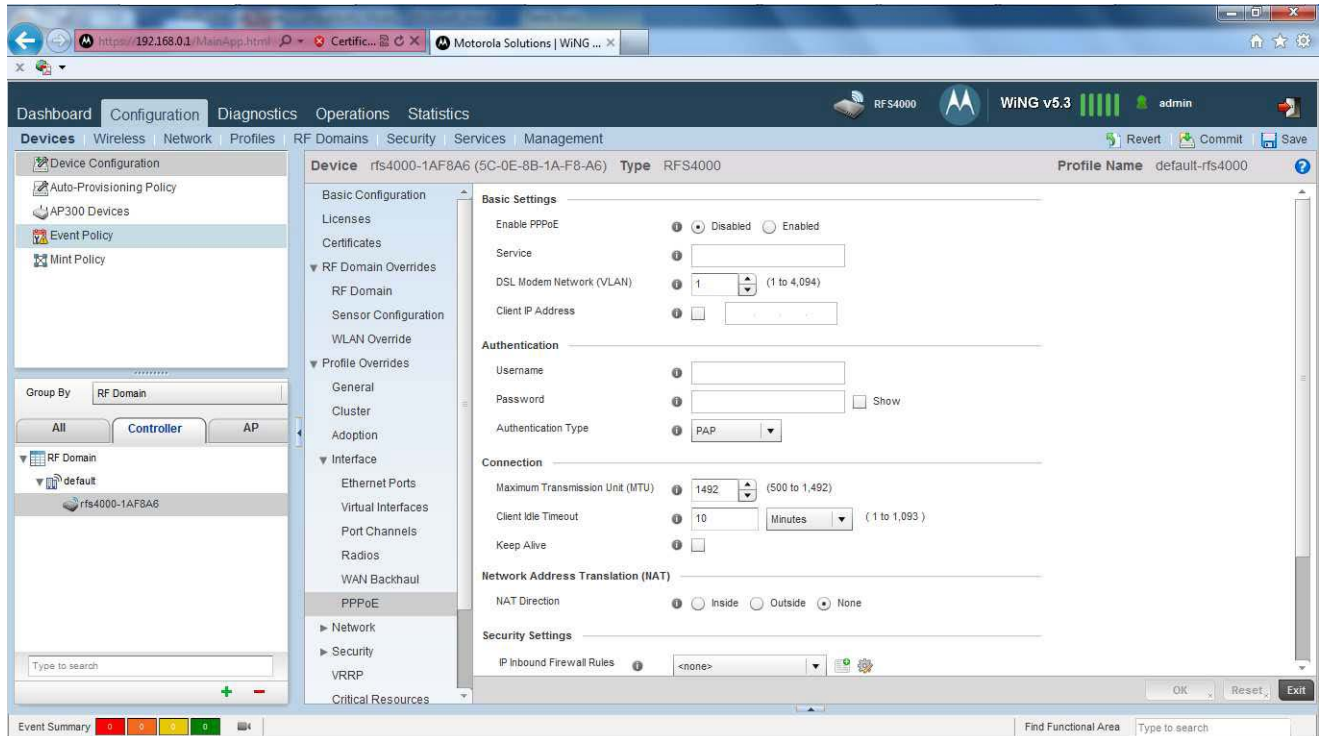
1. Overview

Many Internet service providers use the Point-to-Point Protocol over Ethernet (PPPoE) to provide Digital Subscriber Link (DSL) broadband Internet access. PPPoE uses a standard method of encryption, authentication, and compression specified by the Point-to-Point Protocol. With the release of WING 5.3, a PPPoE client was implemented. Implementing a PPPoE client allows a WiNG 5.X device to connect to the ISP over an Ethernet interface.

As with other interfaces, a PPPoE client interface can be defined within a Device Profile or directly to a device as a Device Override. In the command console, the PPPoE client uses the interface name `pppoe1`. The interface also supports Firewall and Crypto policies as well as NAT. Keep in mind that the interface configuration **MUST** include the VLAN ID the DSL modem is connected to.

1.1 Configuring PPPoE parameters

1. Log in to the WING 5 GUI of the controller. In the WiNG GUI of your Wireless Controller, select Configuration > Devices > [your controller name] > [Edit]. Then expand Interface section and click on PPPoE.



The PPPoE configuration page will appear:

(5C-0E-8B-1A-F8-A6) Type RFS4000

Basic Settings

Enable PPPoE Disabled Enabled

Service

DSL Modem Network (VLAN) (1 to 4,094)

Client IP Address

Authentication

Username

Password Show

Authentication Type

Connection

Maximum Transmission Unit (MTU) (500 to 1,492)

Client Idle Timeout Minutes (1 to 1,093)

Keep Alive

Network Address Translation (NAT)

NAT Direction Inside Outside None

Security Settings

IP Inbound Firewall Rules

2. Begin entering all the relevant parameters. Under the Basic Settings section, choose the Enable PPPoE :: Enabled option. You can also enter the name of your DSL service provider in the Service field. Next enter the VLAN ID of your network into the DSL Modem Network (VLAN) field. Finally, enter the Client IP Address if your ISP assigns you a static IP address. Otherwise, leave it unchecked.
3. Under Authentication, put in your username and password in the appropriate fields and select your ISP's authentication type. There is a choice of CHAP, MSCHAP, mschap-v2, and PAP for authentication.

The screenshot shows a configuration page with two main sections: Authentication and Connection. In the Authentication section, there are input fields for Username (containing 'YourUserName') and Password (containing 'YourPassword'), with a 'Show' checkbox next to the password field. Below these is a dropdown menu for Authentication Type, currently set to 'PAP'. The Connection section includes fields for Maximum Transmission Unit (MTU) with a range of 0 to 1,492, Client Idle Timeout with a range of 1 to 1,093 minutes, and a Keep Alive checkbox. At the bottom, there is a section for Network Address Translation (NAT) with a dropdown menu currently set to 'PAP'.

4. In Connection, you can choose to change the default Maximum Transmission Unit (MTU) parameter from 1492 to another value if you know the optimum setting. You can also choose to increase or decrease the Client Idle Timeout from the default of 10 minutes as well as enable Keep Alive to maintain connectivity.
5. You can configure the Network Address Translation to be Inside, Outside, or None. For the majority of network configurations, Outside will need to be selected.
6. Finally, you can choose the Crypto and Firewall policies to apply to the PPPoE interface.

Example Configuration

Basic Settings

Enable PPPoE Disabled Enabled

Service

DSL Modem Network (VLAN) (1 to 4,094)

Client IP Address

Authentication

Username

Password Show

Authentication Type

Connection

Maximum Transmission Unit (MTU) (500 to 1,492)

Client Idle Timeout Minutes (1 to 1,093)

Keep Alive

Network Address Translation (NAT)

NAT Direction Inside Outside None

Authentication

Username

Password Show

Authentication Type

Connection

Maximum Transmission Unit (MTU) (500 to 1,492)

Client Idle Timeout Minutes (1 to 1,093)

Keep Alive

Network Address Translation (NAT)

NAT Direction Inside Outside None

Security Settings

IP Inbound Firewall Rules

- When you're done, save your changes to the running configuration on the switch by clicking the Commit command at the upper right-hand corner of the main window:



- Save your changes to the startup configuration on the switch by clicking the Save command at the upper right-hand corner of the main window.

