



A *RF45-PRO*

Wi-Fi b/g Modem



User Guide

No part of this document may be reproduced or transmitted (in electronic or paper version, photocopy) without Adeunis RF consent.

This document is subject to change without notice.

All trademarks mentioned in this guide are the property of their respective owner.

ADEUNIS RF

283, rue Louis Néel

38920 Crolles

France

Phone +33 (0)4 76 92 07 77

Fax +33 (0)4 76 08 97 46

Ref. 09-03-V0-jcs

Table of contents

About this document	3
Declaration of conformity	4
Feature's Overview	5
Power supply	8
Serial link wiring	9
<i>Connection during serial configuration phase</i>	9
<i>Connection for data transmission</i>	9
ARF45-PRO Configuration	10
<i>ARF45-PRO WLAN PROFILES</i>	11
<i>ARF45-PRO default configuration</i>	19
<i>Web-based configuration</i>	20
<i>Command mode configuration</i>	22
Configuration using Telnet session	22
Configuration using a Serial Port connection	23
Navigating the command line interface (CLI)	24
<i>Summary: Configuration How-To</i>	27
<i>Duplicating configuration</i>	27
Duplicating configuration through the Web-based interface	28
Duplicating configuration through the Command Line Interface	30
Duplicating configuration through an FTP connection	31
Duplicating configuration with Adeunis-RF configuration application	31
XML group	32
Network Communication mode	43
<i>Connect mode</i>	43
<i>Accept mode</i>	45

<i>Port numbers</i>	48
<i>Modem emulation mode</i>	49
<i>Entering Command mode on the ARF45-PRO</i>	51
Security modes in details	53
<i>Features overview</i>	53
<i>EAP methods supported</i>	54
<i>Security mode deployment</i>	54
<i>RADIUS authentication server: configuration</i>	55
<i>Wireless Access Point: configuration</i>	63
<i>EAP-TLS based deployment</i>	64
<i>PEAP based deployment</i>	79
Roaming capability	82
COM port redirector	83
Firmware Upgrade	84
Specifications	86

About this document

This guide describes the A^{RF45-PRO} devices, their options and accessories.

Declaration of conformity



Manufacturer's name: **ADEUNIS R.F.**
 Manufacturer's address: Parc Technologique PRE ROUX IV
 283 rue Louis NEEL
 38920 CROLLES - FRANCE

declares that the product if used and installed according to the user guide available on our web site www.adeunis-rf.com

Product Name: **ARF45**
 Product Number(s): **ARF7532A**
 Product options:

Complies with the RTTE Directive 99/5/EC:

EMC: conformity to the harmonized standard EN 301 489
 Safety: conformity to the standard EN 60950-1/2001
 Radio: conformity to harmonized standard EN 300-328 covering essential radio requirements of the RTTE directive.

Exposure to radio frequency signals: Regarding the 1999/519/EC recommendation, when using the device, keep the product at least 3 cm from your body.

Notes: - Conformity has been evaluated according to the procedure described in Annex III of the RTTE directive.
 - Receiver class (if applicable): 3.

Crolles, November 12th, 2008
 VINCENT Hervé / Quality manager

A handwritten signature in black ink, appearing to be 'VINCENT', is written over the printed name.

Download of the user guide

Thank you for having chosen the ADEUNIS RF products.
 User guides can be uploaded directly on our web site www.adeunis-rf.com

Index **Products**
 Paragraph **Modems > WIFI modem**
 Print version available upon request

✓ Tel : +33 4 76 92 07 77
 ✓ Email : arf@adeunis-rf.com

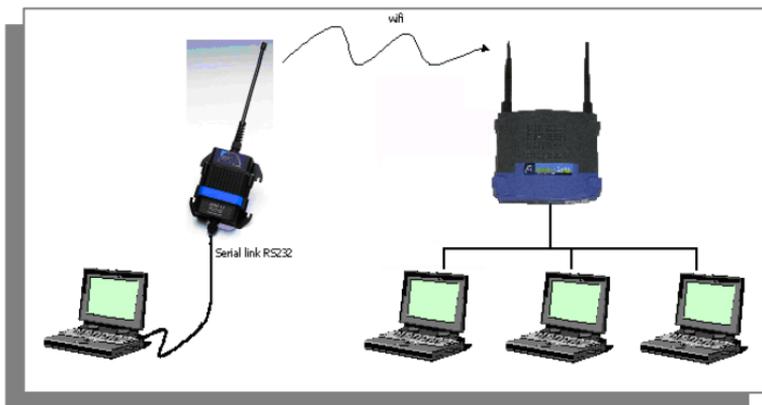
Feature's Overview

- ARF45-PRO is a device that adds secure wireless 802.11 b/g (Wi-Fi) networking capability to any device with a serial interface. Basically the ARF45-PRO can be seen as a RS232/WIFI gateway.
- The ARF45-PRO enables remote access to a serial port over a wireless network. The data from the serial link is encapsulated into TCP or UDP packets which can travel through any IP based wireless network.

By the same token, the ARF45-PRO converts TCP or UDP packets from any IP based wireless network onto serial data.

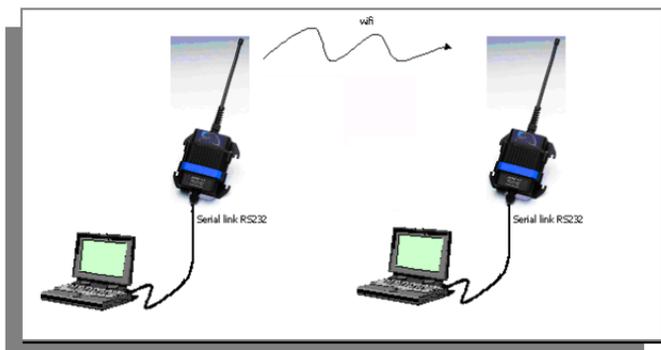
- From a functional point of view, the major difference between the ARF42/45 and the ARF45-PRO is the addition of the WPA2/802.11i enterprise-grade security and authentication protocols (based on the EAP/802.1X framework).
- The ARF45-PRO's integrated web server transforms a standalone device into a networked product that can be managed remotely via a standard web browser.
- The ARF45-PRO operates as a WI-FI station and can thus be part of an Infrastructure network (communication with other WI-FI station through an Access Point) or an Ad-hoc network (direct Point to Point communication with another WI-FI station).

Infrastructure mode: The ARF45-PRO is connected to an Access Point

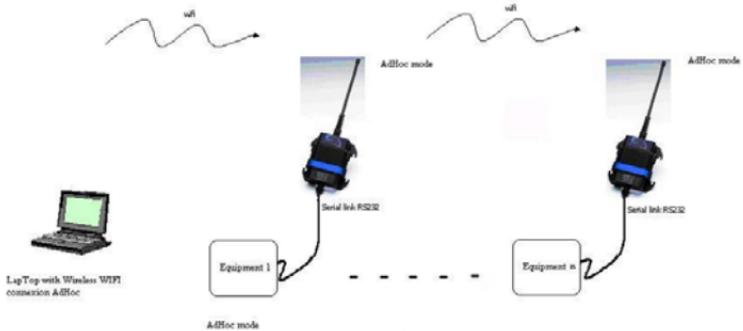


Ad-hoc mode: The ARF45-PRO is directly connected to another WI-FI station.

In this mode, point to point communication between two ARF45-PRO modems is also possible.



The following topology is also possible using Wi-Fi Ad-hoc mode:



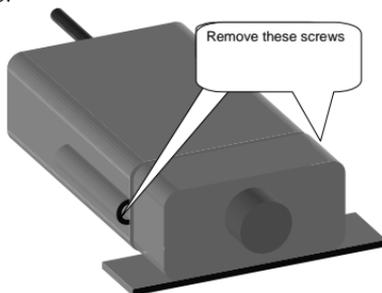
- The ARF45-PRO contains a full-featured TCP/IP stack and supports the following communication and management protocols:

ARP, IP, TCP, UDP, ICMP, BOOTP, DHCP AutoIP, Telnet, FTP, TFTP, HTTP(S), SSH, SSL/TLS, SNMP, DNS, PPP, as well as the complete suite of 802.1X Enterprise Authentication Protocols (EAP) including EAP-TLS, EAP-TTLS, PEAP and LEAP.

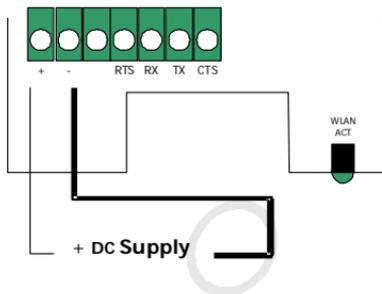
- The configuration of the ARF45-PRO (that is the Serial link, Network, WLAN/Ethernet interfaces, Security mode...parameters) can be achieved in 2 ways:
 - 1) Through a terminal software using a PC serial port.
 - 2) Over the network, through a browser-based interface (which is accessing the embedded web server) or a Telnet connection.

Power supply

To perform wiring of these products, the bottom part of the housing (part with stuffing box) has to be opened by unscrewing the two stainless steel screws on each side.



The ARF45PRO product must be supplied from a **DC voltage** source. This voltage source must be 8V minimum and must not exceed 36 V_{DC}.

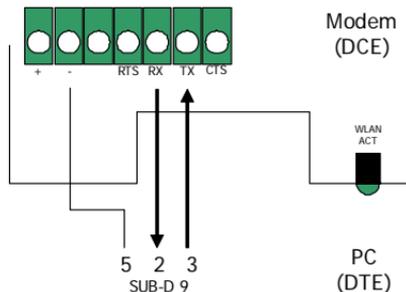


Serial link wiring

The WIFI modem serial interface wiring is a two-step connection process: First connect the modem to a PC to set up the modem configuration, Then connect the modem to the final equipment for data transmission.

Connection during serial configuration phase

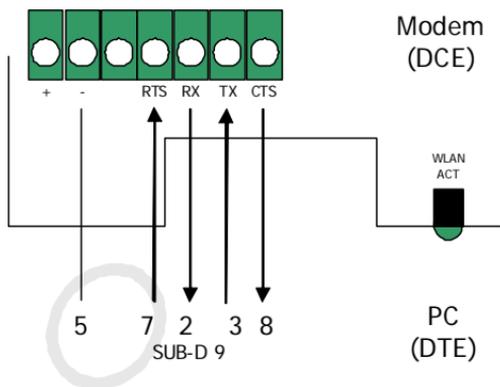
For the initial configuration phase, the WIFI modem has to be connected on to a PC COM port. The set-up configuration software does not require RTS/CTS wiring. The following scheme is an example of connection with a PC:



Connection for data transmission

For the data transmission phase, the WIFI modem is attached by its serial port to the final transmission equipment. If the hardware flow control has been selected during modem configuration phase, RTS and CTS lines have to be connected between both pieces of equipment.

The following scheme is an example where the modem is connected as a piece of DCE equipment to a DTE with hardware flow control handshake:



ARF45-PRO Configuration

The ARF45-PRO comes with a default configuration.

The configuration is then modifiable through access to a set of parameters that are detailed further below.

In order to fit the application, the ARF45-PRO's configuration parameters can easily be modified using two different methods.

Here are listed below the two methods for configuring the ARF45-PRO:

- Through a **web browser** (by making a network connection to the embedded web server, also called the **Web Manager**, of the ARF45-PRO): the advantage of this method is that it offers a user-friendly graphical interface. However this method requires the user to know what the WLAN interface settings (Network, Basic and Security settings) of the ARF45-PRO are. Indeed in order to make a network connection to the ARF45-PRO, the user needs to configure an Access Point (or a Wireless network card) with the same WLAN settings as the ones contained in the ARF45-PRO.

- Through the **Command Line Interface** (accessible either over the network by making a Telnet connection or locally by connecting a terminal to the ARF45-PRO's serial port): the advantage of this method is that the user can access the ARF45-PRO configuration without having the knowledge of its WLAN settings (for instance in order to perform the very first configuration of the product which contains the factory settings). However the drawback of this method is that the command line interface is not user friendly and thus requires the user to navigate through the parameters structure tree and handle commands (it is actually a Cisco –like CLI). However this burden can be avoided by using the Adeunis configuration application which is a user-friendly application tool enabling the configuration of the ARF45-PRO from the serial interface. The purpose of this application is also to assist the user in configuring the ARF45-PRO by providing him with a step by step procedure.

Please refer to the “ARF45-PRO_CommandSet.html” file which presents the parameters structure tree as well as all the available commands and their definition.

The configuration parameters are organised in several groups, based on their function: for instance the parameters pertaining to the network settings are put together into a group of parameters named *Network*.

ARF45-PRO WLAN PROFILES

The ARF45-PRO may have up to four WLAN profiles active at the same time.

A profile corresponds to the configuration of a WLAN link on the ARF45-PRO. In other words, a profile defines the parameters for the connection between an ARF45-PRO and the wireless network.

Those parameters are of 3 types:

- Basic parameters: Network name (also called SSID), network Topology and frequency channel (applicable only in Ad-hoc topology).
- Advanced parameters: TX data rate, TX power settings.
- Security parameters: Parameters pertaining to the encryption and authentication methods.

When using the web-based interface method for configuring the ARF45-PRO, the WLAN profiles are listed in order of precedence under the page Network-> Network 2-> Link-> Configuration (see figure 1 below):

Note: The ARF45-PRO can support 2 network interfaces: one 802.11 b/g wireless network interface (which corresponds to "Network 2") and one Ethernet network interface (which corresponds to "Network 1"). **However, as of now, the Ethernet network interface is not available on the product!**

The screenshot shows the ARF45-PRO web interface. The left sidebar contains a navigation menu with the following items: Status, CLI, CPM, CPU Power Mgmt, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Network (highlighted), ppp, Protocol Stack, Query Port, RSS, SNMP, SSH, SSL, Syslog, System, Terminal, TFTP, Tunnel, WLAN Profiles, and XML.

The main content area is titled "Network 2 (wlan0) WLAN Link Configuration". At the top, there are tabs for "Network 1" and "Network 2", with "Network 2" selected. Below these are tabs for "Interface" and "Link", with "Link" selected. At the bottom of this section are buttons for "Status", "Configuration", and "Scan".

The configuration table is as follows:

Choice 1 Profile:	<input type="text" value="default_infrastructure_profile"/>
Choice 2 Profile:	<input type="text" value="default_adhoc_profile"/>
Choice 3 Profile:	<input type="text" value="PEAP_secured_profile"/>
Choice 4 Profile:	<input type="text" value="EAP_TLS_secured_profile"/>
Out of Range Scan Interval:	<input type="text" value="1"/> seconds
Roaming:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

The right-hand sidebar contains the following text:

This page shows configuration of a WLAN Link on the device.

The configuration details are stored in one or more **WLAN Profile**. List the selected WLAN Profiles in order of preference here.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

Figure 1

By default, the ARF45-PRO product comes with two default profiles: one which enables the connection to an Infrastructure Network (profile name is: *default_infrastructure_profile*) and another one which enables the connection to an Ad-Hoc network (profile name is: *default_adhoc_profile*).

Both of these profiles are set up with default network names (respectively *Lantronix Initial Infra Network* and *Lantronix Initial Adhoc Network*) and no security level activated.

The benefit from having these two default profiles activated is that by default (which means when the product contains the factory settings) the ARF45-

PRO can be configured over the network through an AP (Infrastructure) or a Wireless Network Card (Ad-Hoc). The prerequisite for this is to apply the ARF45-PRO's default WLAN settings to the AP or the Wireless Card. On top of this, a DHCP server must be present in the network in order to be able to proceed to the very first configuration of the product over the network!!

The ARF45-PRO also gives the possibility to create new WLAN profiles. For instance, the figures below (figure 2 to figure 5) show the four active WLAN profiles contained in an ARF45-PRO device: the two default profile (which have been kept) and two WLAN profiles which have been created for different purpose.

Important Point:

The ARF45-PRO can be used to connect to another ARF45-PRO in Ad-Hoc mode (for instance in order to establish a direct network connection between 2 ARF45-PRO).

If such a topology is to be used, the user must make sure that the *AdHoc merging* setting is enabled (if not, trouble during the connection may occur)!!!

The screenshot displays the configuration page for a WLAN Profile named "default_infrastructure_profile". The interface includes a left-hand navigation menu with various system settings, a main configuration area, and a right-hand help section.

Navigation Menu: Status, CLI, CPM, CPU Power Mgmt, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Network, ppp, Protocol Stack, Query Port, RSS, SNMP, SSH, SSL, Syslog, System, Terminal, TFTP, Tunnel, **WLAN Profiles**, XML.

WLAN Profile "default_infrastructure_profile" Configuration:

Basic Configuration	
Network Name:	test
Topology:	<input checked="" type="radio"/> Infrastructure <input type="radio"/> Adhoc
Advanced Configuration	
TX Data Rate Maximum:	54 Mbps
TX Data Rate:	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto-reduction
TX Power Maximum:	14 dBm
TX Power:	<input type="radio"/> Fixed <input checked="" type="radio"/> Adaptation
TX Retries:	7
Power Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Security Configuration	
Suite:	None

Help Text:

This page shows configuration of a WLAN Profile on the device.

In the **Basic Configuration** section, choice of **Topology** affects the makeup of configurables in that section and in the **Advanced Configuration** section.

In the **Advanced Configuration** section, if **Power Management** is enabled, specify the **Power Management Interval**.

In the **Security Configuration** section, choice of **Suite**, **Key Type**, **Authentication**, and **IEEE 802.1X** (when visible) affect the makeup of other configurables in that section.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

Figure 2





- Status
- CLI
- CPM
- CPU Power Mgmt
- Diagnostics
- DNS
- Email
- Filesystem
- FTP
- Host
- HTTP
- IP Address Filter
- Line
- LPD
- Network
- ppp
- Protocol Stack
- Query Port
- RSS
- SNMP
- SSH
- SSL
- Syslog
- System
- Terminal
- TFTP
- Tunnel
- WLAN Profiles
- XML

WLAN Profile "default_adhoc_profile"

Basic Configuration	
Network Name:	<input type="text" value="Lantronix Initial Adhoc Network"/>
Topology:	<input type="radio"/> Infrastructure <input checked="" type="radio"/> Adhoc
Channel:	<input type="text" value="1"/>
Advanced Configuration	
Adhoc Merging:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
TX Data Rate Maximum:	<input type="text" value="54"/> Mbps
TX Data Rate:	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto-reduction
TX Power Maximum:	<input type="text" value="14"/> dBm
TX Power:	<input type="radio"/> Fixed <input checked="" type="radio"/> Adaptation
TX Retries:	<input type="text" value="7"/>
Power Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Security Configuration	
Suite:	<input type="text" value="None"/>

This page shows configuration of a WLAN Profile on the device.

In the **Basic Configuration** section, choice of **Topology** affects the makeup of configurables in that section and in the **Advanced Configuration** section.

In the **Advanced Configuration** section, if **Power Management** is enabled, specify the **Power Management Interval**.

In the **Security Configuration** section, choice of **Suite**, **Key Type**, **Authentication**, and **IEEE 802.1X** (when visible) affect the makeup of other configurables in that section.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

Figure 3





- Status
- CLI
- CPM
- CPU Power Mgmt
- Diagnostics
- DNS
- Email
- Filesystem
- FTP
- Host
- HTTP
- IP Address Filter
- Line
- LPD
- Network
- PPP
- Protocol Stack
- Query Port
- RSS
- SNMP
- SSH
- SSL
- Syslog
- System
- Terminal
- TFTP
- Tunnel
- WLAN Profiles
- XML

WLAN Profile "PEAP_secured_profile"

Basic Configuration

Network Name:	<input type="text" value="test"/>
Topology:	<input checked="" type="radio"/> Infrastructure <input type="radio"/> Adhoc

Advanced Configuration

TX Data Rate Maximum:	<input type="text" value="54"/> Mbps
TX Data Rate:	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto-reduction
TX Power Maximum:	<input type="text" value="14"/> dBm
TX Power:	<input type="radio"/> Fixed <input checked="" type="radio"/> Adaptation
TX Retries:	<input type="text" value="7"/>
Power Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Security Configuration

Suite:	<input type="text" value="WPA"/>
Authentication:	<input type="radio"/> PSK <input checked="" type="radio"/> IEEE 802.1X
IEEE 802.1X:	<input type="text" value="PEAP"/>
PEAP Option:	<input type="text" value="EAP-MSCHAPV2"/>
Username:	<input type="text" value="arf45Pro"/>
Password:	<input type="text" value="<Configured>"/>
Encryption:	<input checked="" type="checkbox"/> CCMP <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> WEP

This page shows configuration of a WLAN Profile on the device.

In the **Basic Configuration** section, choice of **Topology** affects the makeup of configurables in that section and in the **Advanced Configuration** section.

In the **Advanced Configuration** section, if **Power Management** is enabled, specify the **Power Management Interval**.

In the **Security Configuration** section, choice of **Suite**, **Key Type**, **Authentication**, and **IEEE 802.1X** (when visible) affect the makeup of other configurables in that section.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

Figure 4

The screenshot displays the configuration page for a WLAN Profile named "EAP_TLS_secured_profile". The interface includes a left-hand navigation menu with various system settings, a main configuration area, and a right-hand help section.

WLAN Profile
"EAP_TLS_secured_profile"

Basic Configuration

Network Name:	test
Topology:	<input checked="" type="radio"/> Infrastructure <input type="radio"/> Adhoc

Advanced Configuration

TX Data Rate Maximum:	54 Mbps
TX Data Rate:	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto-reduction
TX Power Maximum:	14 dBm
TX Power:	<input type="radio"/> Fixed <input checked="" type="radio"/> Adaptation
TX Retries:	7
Power Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Security Configuration

Suite:	WPA
Authentication:	<input type="radio"/> PSK <input checked="" type="radio"/> IEEE 802.1X
IEEE 802.1X:	EAP-TLS
Username:	arf45Pro
Encryption:	<input checked="" type="checkbox"/> CCMP <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> WEP

Help Text:
This page shows configuration of a WLAN Profile on the device.
In the **Basic Configuration** section, choice of **Topology** affects the makeup of configurables in that section and in the **Advanced Configuration** section.
In the **Advanced Configuration** section, if **Power Management** is enabled, specify the **Power Management Interval**.
In the **Security Configuration** section, choice of **Suite, Key Type, Authentication, and IEEE 802.1X** (when visible) affect the makeup of other configurables in that section.
Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
Use the **Submit** button to both update the WLAN settings and save them to Flash.

Figure 5

The "EAP_TLS_secured_profile" and "PEAP_secured_profile" WLAN profiles are profiles with the EAP authentication mode enabled. From figure 1, we can see that the "default infrastructure profile" has precedence over the EAP_TLS profile which means that the ARF45-PRO will first search for a wireless Access Point with the same SSID, Channel number and Security mode as the ones contained in the "default infrastructure profile" profile. If such a profile is not found, then the ARF45-PRO will search for a profile matching the settings of the "PEAP secured profile" profile and so on.

Ref. 09-03-V0-jcs

In the case where more than one of the active profiles is available in the surrounding environment, it is important to note that the signal strength (from the Access Point) also comes into play when selecting the profile to which the ARF45-PRO is going to connect to.

ARF45-PRO default configuration

The ARF45-PRO default configuration is as follows:

- 1) Two default profiles:
 - Infrastructure Mode SSID: *Lantronix Initial Infra Network*
 - Ad hoc mode SSID: *Lantronix Initial Adhoc Network*

Note: Both of these profiles are enabled by default. Infrastructure Mode is the first choice, then Ad-Hoc mode. You can set your AP to match an SSID of *Lantronix Initial Infra Network* or connect with another wireless card in Ad-hoc mode with an SSID of *Lantronix Initial Adhoc Network*.

- 2) No encryption
- 3) BOOTP, DHCP, and AutoIP enabled.

Note: AutoIP generates a random default IP address in the range 169.254.0.1 to 169.254.255.254 if no BOOTP or DHCP server is found.

 In case the user wish to configure the ARF45-PRO using the Web-based method, he has to make sure that the computer from which he is going to launch the web-browser (or open a Telnet session) is connected to an AP or have access to a wireless card with the **same settings !!!**

Note that during the very first configuration, if no DHCP server is found, the AutoIP server (running on the ARF45-PRO) is going to assigned a default (and random) IP address to the ARF45-PRO. As a consequence the user does not know the IP address of the ARF45-PRO and thus he has to make use of the Command Line Interface method (over the serial port!) in order to carry Ref. 09-03-V0-jcs

out the very first configuration of the product (either using directly the CLI command mode or through the Adeunis configuration application).

Here are described below on figure 6 the steps to follow when the ARF45-PRO device contains the default factory settings:

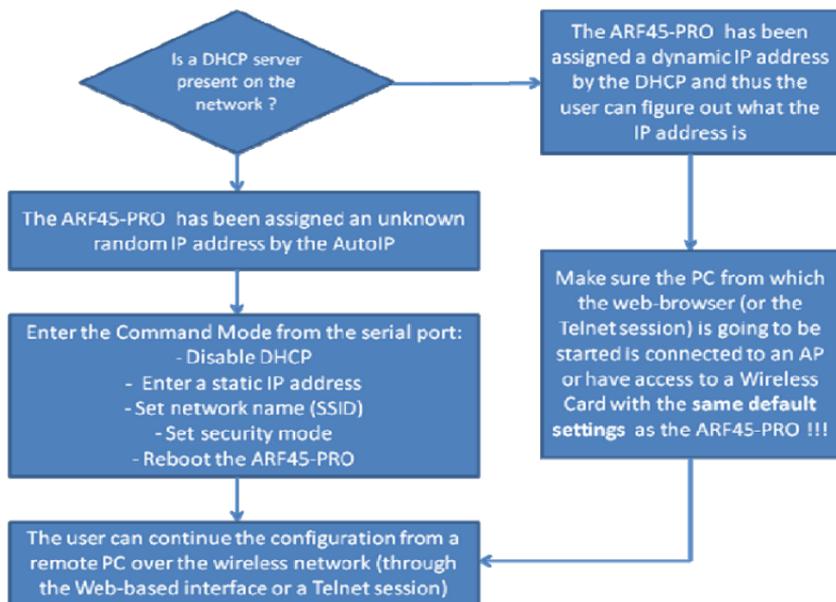


Figure 6

Web-based configuration

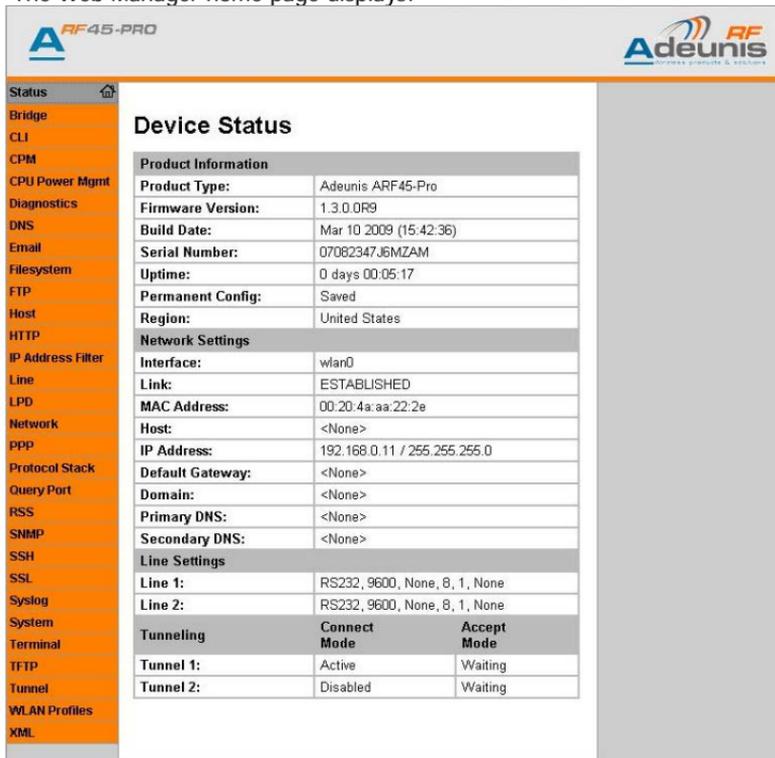
To access the Web Manager:

1. Open a standard web browser (such as Netscape Navigator, Internet Explorer, Mozilla Firefox).

2. Enter the IP address of the ARF45-PRO in the address bar.
3. Enter your user name and password.

Note: The factory-default user name is *admin* and the factory-default password is *PASS*.

The Web Manager home page displays:



The screenshot shows the Web Manager interface for the ARF45-PRO device. The top header includes the 'A^{RF45-PRO}' logo on the left and the 'Adeunis' logo on the right. A navigation menu on the left lists various system functions such as Status, Bridge, CLI, CPM, CPU Power Mgmt, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Network, PPP, Protocol Stack, Query Port, RSS, SNMP, SSH, SSL, Syslog, System, Terminal, TFTP, Tunnel, WLAN Profiles, and XML. The main content area is titled 'Device Status' and contains the following information:

Product Information			
Product Type:	Adeunis ARF45-Pro		
Firmware Version:	1.3.0.0R9		
Build Date:	Mar 10 2009 (15:42:36)		
Serial Number:	07082347J6MZAM		
Uptime:	0 days 00:05:17		
Permanent Config:	Saved		
Region:	United States		
Network Settings			
Interface:	wlan0		
Link:	ESTABLISHED		
MAC Address:	00:20:4a:aa:22:2e		
Host:	<None>		
IP Address:	192.168.0.11 / 255.255.255.0		
Default Gateway:	<None>		
Domain:	<None>		
Primary DNS:	<None>		
Secondary DNS:	<None>		
Line Settings			
Line 1:	RS232, 9600, None, 8, 1, None		
Line 2:	RS232, 9600, None, 8, 1, None		
Tunneling		Connect Mode	Accept Mode
Tunnel 1:	Active	Waiting	
Tunnel 2:	Disabled	Waiting	

Figure 7

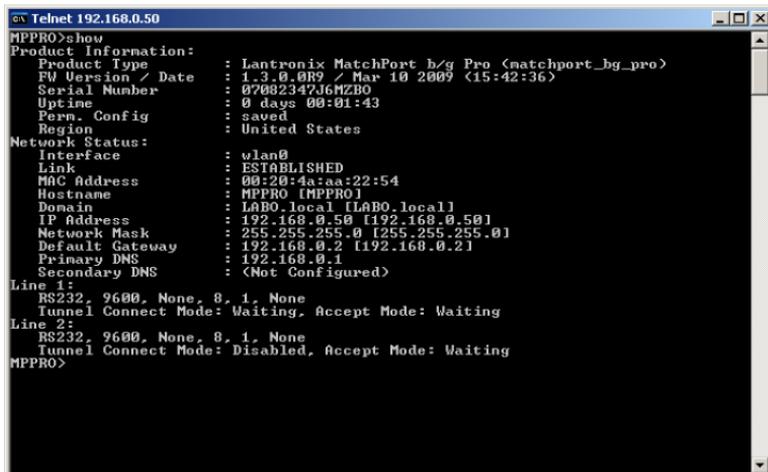
Command mode configuration

As an alternative to using the Web Manager, you can configure the ARF45-PRO through the command line interface (CLI) using a series of commands. The command mode interface can be accessed through a Telnet session or a direct connection to a serial port.

Configuration using Telnet session

To configure the ARF45-PRO device using a Telnet session over the network, establish a Telnet connection:

1. From the Windows Start menu, click Run. The Run dialog box appears.
2. In the Run dialog box, type the following command, where x.x.x.x is the IP address of the ARF45-PRO device: telnet x.x.x.x
=> The command mode prompt shows up.



```

MPPRO>show
Product Information:
  Product Type       : Lantronix MatchPort b/g Pro <matchport_bg_pro>
  FW Version / Date  : 1.3.0.0R9 / Mar 10 2009 <15:42:36>
  Serial Number      : 07002347J6MZD0
  Uptime             : 0 days 00:01:43
  Perm. Config       : saved
  Region             : United States
Network Status:
  Interface          : vlan0
  Link               : ESTABLISHED
  MAC Address        : 00:20:4a:aa:22:54
  Hostname           : MPPRO [MPPRO]
  Domain             : LAB0.local [LAB0.local]
  IP Address         : 192.168.0.50 [192.168.0.50]
  Network Mask       : 255.255.255.0 [255.255.255.0]
  Default Gateway    : 192.168.0.2 [192.168.0.2]
  Primary DNS        : 192.168.0.1
  Secondary DNS      : <Not Configured>
Line 1:
  RS232, 9600, None, 8, 1, None
  Tunnel Connect Mode: Waiting, Accept Mode: Waiting
Line 2:
  RS232, 9600, None, 8, 1, None
  Tunnel Connect Mode: Disabled, Accept Mode: Waiting
MPPRO>

```

Figure 8

At boot time, executing the following sequence enables to enter the command mode:

Press and hold down the exclamation point (!) key.

Then, when an exclamation point (!) appears on the terminal or PC screen, type xyz within 5 seconds to display the command mode prompt.

At any time: There is also the possibility for the ARF45-PRO device to enter the command mode at any time, even while a connection with a remote device is set up.

To enter the Command mode, execute the following sequence at any time:

- Enter the string "---" (this causes the ARF45-PRO to reset).
- Then press and hold down the exclamation point (!) key until an exclamation point (!) appears on the terminal or PC screen and then type "xyz" within 5 seconds to display the command mode prompt.

 Entering the command mode through a serial port connection causes the ARF45-PRO device to be reset!

An alternative (to enter the command mode at any time) to using the above procedure consists of using the modem emulation mode.

See in subsequent chapters how to configure this mode. Using this method does not reset the ARF45-PRO.

Navigating the command line interface (CLI)

The CLI is organized into a hierarchy of levels. When you first start a command line session, you are in the login level. Commands at the login level of the CLI do not affect current configuration settings; these commands provide diagnostic and status information only. To configure the device server running on Evolution, you must be in the enable level or any of its sub-levels. The level structure is depicted in the following figure:

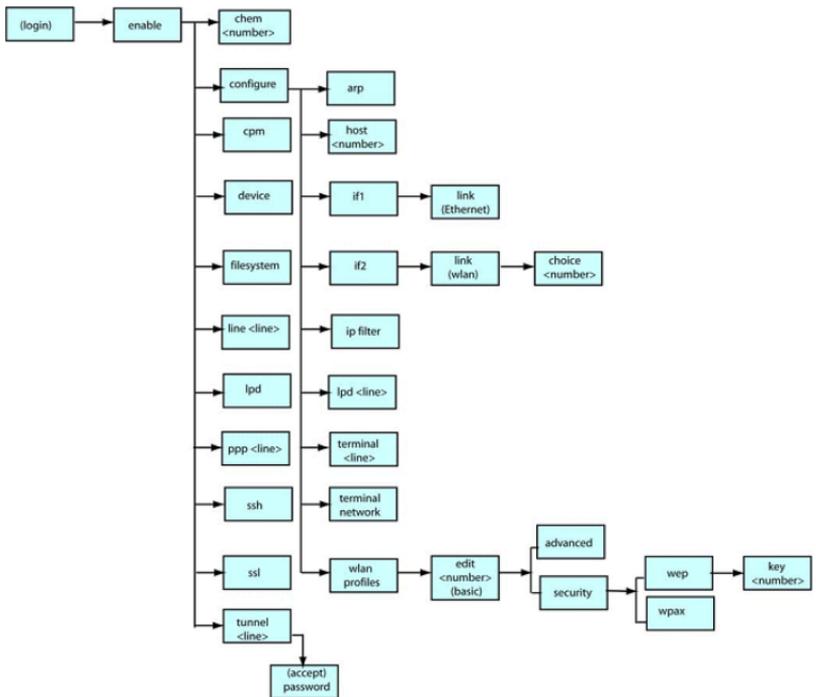


Figure 10

To move to a different level: Enter the name of that level from within its parent level.

For example:

```
>enable (enable)#tunnel 2
```

Note: Some levels require a number to indicate one of several level instances. In the example above the number 2 indicates that we would like to configure the settings for tunneling on serial port 2.

To exit and return to one level higher: Type **exit** and press the Enter key.

Note: Typing exit at the login level or the enable level will close the CLI session.

To view the current configuration at any level: Type **show**. The configuration for that level displays.

To view the list of commands available at the current level: At the command prompt, type the question mark "**?**". The list of current commands displays. (There is no need to press Enter.)

Note: Items within < > (e.g. <string>) are required parameters.

To view the available commands and their explanations: At the command prompt, type ***** and press Enter. The list of commands for that level and their description displays.

To view the list of commands available for a partial command: At the command prompt, type the partial command followed by the question mark "**?**". The list of current commands displays. (There is no need to press Enter.)

For example: <tunnel-1>#accept? displays a list of all accept commands at the tunnel level.

To view the available commands and their explanations for a partial command: At the command prompt, type the partial command followed by ***** and press Enter. The list of partial commands and descriptions displays.

For example: <tunnel-1>#accept* displays a list of all accept commands and descriptions at the tunnel level.

Summary: Configuration How-To

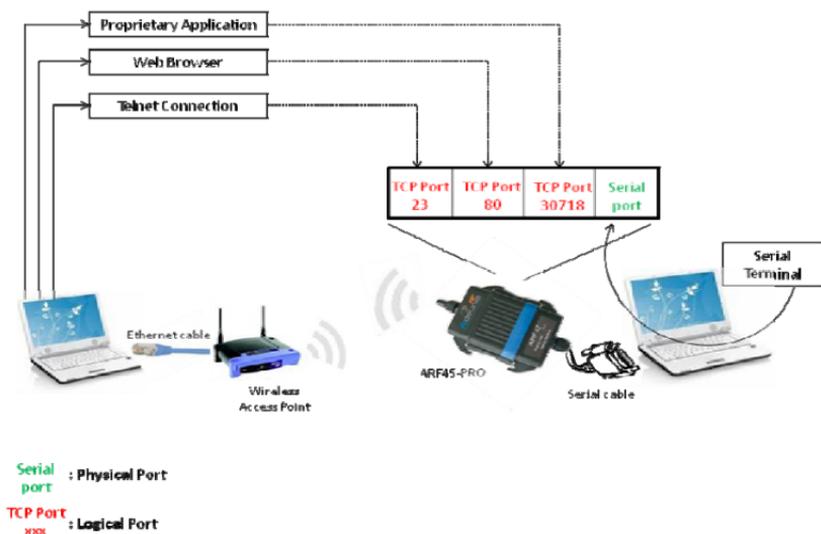


Figure 11

Duplicating configuration

The ARF45-PRO device supports XML-based configuration which make device configuration transparent to users. The XML is easily editable with a standard text or XML editor.

Using XML-based configuration file provide a straightforward and flexible way to manage the configuration of multiple devices.

The ARF45-PRO allows for the configuration of units using an XML configuration file making it possible to easily export a current configuration for use on other ARF45-PRO devices or import a saved configuration file.

Exporting/Importing XML configuration file from/to an ARF45-PRO device is possible both through the use of the web-based interface or the use of the command mode interface.

When exporting the current system configuration in XML format, the generated XML file can be imported later to restore a configuration. It can also be modified and imported to update the configuration on this ARF45-PRO device or another ARF45-PRO device. The XML data can be exported to the browser window or to a file on the file system.

Duplicating configuration through the Web-based interface

The Web interface can be used to import (figure 13) and export (figure 12) an XML configuration file to the ARF45-PRO file system. It can also be used to import an XML configuration file from an external source such as your local hard drive.

Export Configuration **Export Status** **Import Configuration**

XML: Export Configuration

Export to browser

Export to local file

Export secrets (use only with extreme caution)

Lines to Export: [\[Clear All\]](#) [\[Select All\]](#)

1 2 network

Groups to Export: [\[Clear All\]](#) [\[Select All but Networking\]](#)

<input checked="" type="checkbox"/> arp	<input type="checkbox"/> bridge: bridge0
<input checked="" type="checkbox"/> cli	<input checked="" type="checkbox"/> cp group
<input checked="" type="checkbox"/> device	<input checked="" type="checkbox"/> email
<input checked="" type="checkbox"/> ethernet: eth0	<input checked="" type="checkbox"/> ftp server
<input checked="" type="checkbox"/> host	<input checked="" type="checkbox"/> http authentication uri
<input checked="" type="checkbox"/> http server	<input checked="" type="checkbox"/> icmp
<input type="checkbox"/> interface: eth0	<input type="checkbox"/> interface: wlan0
<input checked="" type="checkbox"/> ip	<input checked="" type="checkbox"/> ip filter
<input checked="" type="checkbox"/> line	<input checked="" type="checkbox"/> lpd
<input checked="" type="checkbox"/> power management	<input checked="" type="checkbox"/> ppp
<input checked="" type="checkbox"/> query port	<input checked="" type="checkbox"/> rss
<input checked="" type="checkbox"/> serial command mode	<input checked="" type="checkbox"/> snmp
<input checked="" type="checkbox"/> ssh client	<input checked="" type="checkbox"/> ssh command mode
<input checked="" type="checkbox"/> ssh server	<input checked="" type="checkbox"/> ssl
<input checked="" type="checkbox"/> syslog	<input checked="" type="checkbox"/> tcp
<input checked="" type="checkbox"/> telnet command mode	<input checked="" type="checkbox"/> terminal
<input checked="" type="checkbox"/> tftp server	<input checked="" type="checkbox"/> tunnel accept
<input checked="" type="checkbox"/> tunnel connect	<input checked="" type="checkbox"/> tunnel disconnect
<input checked="" type="checkbox"/> tunnel modem	<input checked="" type="checkbox"/> tunnel packing
<input checked="" type="checkbox"/> tunnel serial	<input checked="" type="checkbox"/> tunnel start

Caution: The "wlan profile" and "http authentication uri" groups must be exported with **export secrets** enabled if they are to be used to later restore the configuration.

The exported XML file can be modified and imported to update the configuration on this device or another.

The XML data can be exported to the browser window or to a file on the filesystem.

Caution: Only **export secrets** over a secure connection and make sure that the data goes only to secure locations.

Notice that by default, all **Groups to Export** are checked except some pertaining to the network configuration; this is so that if you later "paste" the entire XML configuration, it will not break your network connectivity. You may check or uncheck any group to include or omit that group from export.

Selection of **Lines to Export** filters instances to be exported in the line, lpd, ppp, serial, tunnel, and terminal groups.

Figure 12

By default the network interface settings are not exported. This is so that if you later export the entire XML configuration, it will not break your network connectivity.

The screenshot displays the 'XML: Import Configuration' page in the Adeunis RF45-PRO web interface. The left sidebar lists various system management functions, with 'XML' selected. The main content area features three tabs: 'Export Configuration', 'Export Status', and 'Import Configuration'. The 'Import Configuration' tab is active, showing the title 'XML: Import Configuration' and an 'Import:' section with three radio button options: 'Configuration from External file', 'Configuration from Filesystem', and 'Line(s) from single line Settings on the Filesystem'. On the right side, there is explanatory text about importing from external files and filesystems, and a section for 'Text List' with an example string: '<q>: <i> <q>: <i> . . .'. Below this, it explains that each group name is followed by a colon and the instance value, and each instance value is separated by a semi-colon.

Figure 13

Duplicating configuration through the Command Line Interface

An XML configuration file can be imported (captured) or exported (dumped) directly to a Telnet or serial line session. Capturing an XML configuration record can be started by pasting a valid XML configuration file directly into the Command line interface.

To dump the current configuration, use the following command:

xcr dump <param>

By default *param* is empty and the whole configuration is dumped and displayed on the terminal window.

The user may choose to export only part of the configuration by setting *param* to the group's names that have to be exported:

Example:

xcr dump *interface:2,arp,ppp* will export and display the content of the *arp* group, the content of the *ppp* group and the content of the instance 2 of the *interface* group.

Duplicating configuration through an FTP connection

An XML configuration file can be exported or imported to or from the PC's filesystem by setting up a connection to the FTP server of the ARF45-PRO.

By default the FTP server is running and the default username/pwd is: admin/none.

Export: type the command: **get** *matchport_bg_pro.xcr* onto the FTP client window. As a result, the current configuration of the ARF45-PRO is exported onto a file named *matchport_bg_pro.xcr* created in the FTP directory, which is the directory from which you ftp'ed.

Import: type the command: **put** *matchport_bg_pro.xcr* onto the FTP client window. As a result, the content of the *matchport_bg_pro.xcr* configuration file (that should be located in the FTP directory, which is the directory from which you ftp'ed) is loaded in the ARF45-PRO.

For this to take effect, the ARF45-PRO must be rebooted!

Duplicating configuration with Adeunis-RF configuration application

Using the Adeunis-RF application enables the user to export and import configuration over the serial port.

XML group

Here is below the list of XML group. This table indicates whether each item can be imported, exported, or exported with the placeholder "<!--configured and ignored-->":

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information	
arp	arp timeout			import/export		
	arp entry	ip address		import	Add a dynamic entry to the ARP table.	
		Mac address		import		
	arp delete			import	Remove an entry from the ARP table. Specify the entry by its IP address.	
dl	enable level password			import/export	Placeholder	
	login password			import/export	Placeholder	
	quit connect line			import/export		
cp group	state		enable	import/export		
			disable			
	cp	cp		import/export	CP number from 1 to 7	
		bit		import/export	Bit number from 0 to 6	
		type	input		import/export	
output						
	assert low		enable	import/export		
			disable			
device	long name			import/export		
	serial number			export		
	short name			import/export		
email	to			import/export	Multiple to addresses may be separated with semicolons or input as separate "to" items.	
	From			import/export		
	reply to			import/export		
	cc			import/export	Multiple cc address may be separated with semicolons or input as separate "cc" items.	
	subject			import/export		
	message file			import/export		
	local port			import/export		
	server port			import/export		
	priority			Very Low	import/export	
				Low		
			Normal			
			High			
			Urgent			
overriding domain				import/export		

Figure 14

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information				
	cp	group		import/export					
		trigger value		import/export					
ethernet	duplex		auto	import/export					
			full						
			half						
	speed		auto	import/export					
10									
		100							
exit cli	state		enable	import					
			disable						
firmware	version			export					
ftp server	state		enable	import/export					
			disable						
	admin		import/export						
	username		import/export	Exports as "!-- configured and ignored -->".					
	admin		import/export	Placeholder					
	password		import/export	Placeholder					
host	name			import/export					
	protocol		telnet	import/export					
			ssh						
	remote			import/export					
	address								
	remote port			import/export					
ssh			import/export	Username must correspond to a configured ssh client user.					
http authentication uri	realm			import/export	Attribute of "instance" specifies the uri.				
	type			import/export					
	user	username		import/export					
		password		import/export	Placeholder	Exports as "!-- configured and ignored -->".			
	user delete			import	Delete the HTTP Authentication URI user. The value element is used to specify the user for deletion.				
	Uri delete			import	Delete the HTTP Authentication URI. The value of the element is used to specify the URI for deletion.				
http server	state		enable	import/export					
			disable						
	port			import/export					
	secure port			import/export					
	secure protocols	ssl/3		enable	import/export				
				disable					
				ttl/s 1.0			enable	import/export	
				disable					
				ttl/s 1.1			enable		
		disable							
max timeout			import/export						
max bytes			import/export						
bgging state			import/export						

Figure 15

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	<i>bg format</i>			<i>import/export</i>	
	<i>max log entries</i>			<i>import/export</i>	
<i>icmp</i>	<i>state</i>		<i>enable</i> <i>dsable</i>	<i>import/export</i>	
<i>interface</i>	<i>state</i>		<i>enable</i>	<i>import/export</i>	
			<i>dsable</i>		
	<i>bootp</i>		<i>enable</i> <i>dsable</i>	<i>import/export</i>	
	<i>dhcp</i>		<i>enable</i> <i>dsable</i>	<i>import/export</i>	
	<i>dhcp client id</i>			<i>import/export</i>	Set the identity of the client device.
	<i>domain</i>			<i>import/export</i>	
	<i>hostname</i>			<i>import/export</i>	
	<i>p address</i>			<i>import/export</i>	
	<i>default gateway</i>			<i>import/export</i>	
	<i>primary dns</i>			<i>import/export</i>	
	<i>secondary dns</i>			<i>import/export</i>	
<i>ip filter</i>	<i>filter entry</i>	<i>p address</i>		<i>import/export</i>	
		<i>net mask</i>			
	<i>filter delete</i>	<i>p address</i> <i>Net mask</i>		<i>import</i>	Delete an IP filter entry.
<i>line</i>	<i>state</i>		<i>enable</i>	<i>import/export</i>	
			<i>dsable</i>		
	<i>baud rate</i>			<i>import/export</i>	Any value from 300 to 230400.
	<i>data bits</i>		7	<i>import/export</i>	
			8		
	<i>parity</i>		<i>none</i>	<i>import/export</i>	
			<i>even</i>		
			<i>odd</i>		
	<i>stop bits</i>		1	<i>import/export</i>	
			2		
	<i>flow control</i>		<i>hardware</i>	<i>import/export</i>	
			<i>software</i>		
				<i>none</i>	
	<i>xon char</i>			<i>import/export</i>	Set the x-on character. Enter as a hexadecimal byte.
	<i>Xoff char</i>			<i>import/export</i>	Set the x-off character. Enter as a hexadecimal byte.
	<i>interface</i>		<i>rs232</i>	<i>import/export</i>	rs485 option is only available on EDS4100 ports 1 and 3????
			<i>rs485</i>		
	<i>name</i>			<i>import/export</i>	
	<i>protocol</i>		<i>lpd</i>	<i>import/export</i>	
			<i>none</i>		
			<i>ppp</i>		
			<i>tunnel</i>		
			<i>dsable</i>		
<i>lpd</i>	<i>banner</i>		<i>enable</i>	<i>import/export</i>	lpd settings cannot be imported for a console port (if applicable)
			<i>dsable</i>		
	<i>binary</i>		<i>enable</i>	<i>import/export</i>	
			<i>dsable</i>		
<i>convert</i>			<i>enable</i>	<i>import/export</i>	

Figure 16

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	newline		disable	import/export	
	ecj		enable		
			disable	import/export	
	ecj text		enable		
	formfeed		disable	import/export	
	queue name			import/export	
	soj		enable	import/export	
		disable			
power management	soj text			import/export	
	state		enable	import/export	
ppp			disable		
	lcal ip			import/export	
	peer ip			import/export	
	network mask			import/export	
	authentication mode		none	import/export	
			pap		
			chap		
	username		import/export	Exports as "!-> configured and ignored ->".	
	password		import/export		
query port	state		enable	import/export	
			disable		
			Disable		
rss	feed		enable	import/export	
			disable		
			enable	import/export	
			disable		
	max entries			import/export	
clear data			import		
serial command mode	mode		enable	import/export	
			disable		
			always		
			serial string		
	echo serial string		enable	import/export	
			disable		
	serial string			import/export	
	signon message			import/export	
wait time			import/export		
cp	group		import/export		
	trigger value				
snmp	state		enable	import/export	
			disable		
	system name			import/export	
	system contact			import/export	
	system description			import/export	
	system location			import/export	
	traps	state		enable	
			disable		

Figure 17

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
		<i>primary destination</i>		<i>import/export</i>	
		<i>secondary destination</i>		<i>import/export</i>	
	<i>read community</i>			<i>import/export</i>	<i>Exports as "!-- configured and ignored -->"</i>
	<i>write community</i>			<i>import/export Placeholder</i>	<i>Exports as "!-- configured and ignored -->"</i>
<i>ssh client</i>	<i>known host</i>	<i>public dsa key</i>		<i>import/export</i>	
		<i>server</i>			
		<i>public rsa key</i>			
	<i>client users</i>	<i>username</i>		<i>import/export</i>	
		<i>password</i>		<i>import/export</i>	<i>Exports as "!-- configured and ignored -->"</i>
		<i>remote command</i>		<i>import/export</i>	
		<i>public rsa key</i>		<i>import/export</i>	<i>Exports as "!-- configured and ignored -->"</i>
		<i>private rsa key</i>		<i>import/export</i>	
		<i>public dsa key</i>		<i>import/export</i>	<i>Exports as "!-- configured and ignored -->"</i>
		<i>private dsa key</i>		<i>import/export</i>	
	<i>known host delete</i>			<i>import</i>	<i>Specify the server host for deletion.</i>
	<i>Client users delete</i>			<i>import</i>	<i>Specify the username for deletion.</i>
	<i>Client rsa key delete</i>			<i>import</i>	<i>Specify the username.</i>
	<i>Client dsa key delete</i>			<i>import</i>	<i>Specify the username.</i>
<i>ssh command mode</i>	<i>max sessions</i>			<i>import/export</i>	
	<i>state</i>		<i>enable</i>	<i>import/export</i>	
			<i>disable</i>		
	<i>port</i>			<i>import/export</i>	
<i>ssh server</i>	<i>host rsa keys</i>	<i>public key</i>		<i>import/export</i>	
		<i>private key</i>		<i>import/export</i>	<i>Exports as "!-- configured and ignored -->"</i>
	<i>host dsa keys</i>	<i>public key</i>		<i>import/export</i>	<i>Exports as "!-- configured and ignored -->"</i>
		<i>private key</i>		<i>import/export</i>	<i>Exports as "!-- configured and ignored -->"</i>
	<i>authorized users</i>	<i>username</i>		<i>import/export</i>	
		<i>password</i>		<i>import/export</i>	<i>Exports as "!-- configured and ignored -->"</i>
		<i>public rsa key</i>		<i>import/export</i>	
		<i>public dsa key</i>		<i>import/export</i>	
	<i>authorized users delete</i>			<i>import</i>	<i>Delete an SSH authorized user.</i>

Figure 18

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
ssl	host keys delete	key type	rsa	import	Delete the SSH host keys.
			dsa		
	certificate	certificate		import/export	Enter the text of the certificate.
			private key		import/export
	rsa certificate	certificate		import/export	Enter the text of the certificate.
			private key		import/export
	dsa certificate	certificate		import/export	Enter the text of the certificate.
			private key		import/export
	delete		certificate	import	Deletes the current SSL certificate.
	syslog	trusted ca			import/export
host				import/export	
local port				import/export	
remote port				import/export	
severity log level			emergency	import/export	
			alert		
			critical		
			error		
	warning				
notice					
information					
debug					
state		enable	import/export		
tcp	resets		enable	import/export	
			disable		
telnet command mode	max sessions			import/export	
	state		enable		
			disable		
port					
terminal	break			import/export	milliseconds
	duration				
	echo		enable	import/export	
			disable		
	exit connect menu		enable	import/export	
disable					
bgln connect menu		enable	import/export		
		disable			

Figure 19

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	send break			import/export	control character
	terminal type			import/export	
fttp server	state		enable	import/export	
			disable		
	allow file creation		enable	import/export	
			disable		
tunnel accept	accept mode		enable	import/export	
			disable		
			any character		
			start character		
			modem control asserted		
			modem		
	aes decrypt key			import/export Placeholder	
	aes encrypt key			import/export Placeholder	
	bcpl port			import/export	
	protocol		tcp	import/export	
		tcp aes			
		ssh			
		ssl			
		telnet			
	flush serial		enable	import/export	
			disable		
	block serial		enable	import/export	
			disable		
	block network		enable	import/export	
			disable		
	tcp keep alive			import/export	
	email connect			import/export	
	email disconnect			import/export	
	cp set group	cp		import/export	cp name or cp group name
		connection value		import/export	
		disconnect value		import/export	
	password	prompt	enable	import/export	
			disable		
		password		import/export	Exports as "!-- configured and ignored -->".
tunnel connect	connect mode		enable	import/export	
			disable		
			any character		
			start character		
			modem control asserted		

Figure 20

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
	aes decrypt key		modem	import/export	
	aes encrypt key			Placeholder	
	bcast port			import/export	
	remote address			import/export	
	remote port			import/export	
	protocol		tcp	import/export	
			udp		
			ssh		
			ssl		
			tcp aes		
			udp aes		
			telnet		
	reconnect time			import/export	
	flush serial		enable	import/export	
			dsable		
	ssh username			import/export	Username must correspond to a configured ssh client user.
	Block serial		enable	import/export	
			dsable		
	block network		enable	import/export	
			dsable		
	tcp keep alive			import/export	
	email connect			import/export	
	email disconnect			import/export	
	cp set group	cp		import/export	cp name or cp group name
		connection value		import/export	
		dsconnection value		import/export	
tunnel disconnect	character stop		enable	import/export	
			dsable		
	flush serial		enable	import/export	
			dsable		
	modem control		enable	import/export	
			dsable		
	timeout			import/export	A value of 0 disables the timeout feature.
tunnel modem	echo pluses		enable	import/export	
			dsable		
	echo commands		enable	import/export	
			dsable		
	verbose response		enable	import/export	
			dsable		
	response type		text	import/export	
			numeric		
	error unknown commands		enable	import/export	
			dsable		
tunnel	connect string			import/export	
	packing mode		dsable	import/export	

Figure 21

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information	
packng			<i>timeout</i>			
			<i>send character</i>			
	<i>timeout</i>			<i>import/export</i>		
	<i>threshold</i>			<i>import/export</i>		
	<i>send character</i>			<i>import/export</i>		
	<i>trailing character</i>			<i>import/export</i>		
tunnel serial	<i>buffer size</i>			<i>import/export</i>		
	<i>ctr</i>		<i>asserted while connected continuously asserted</i>	<i>import/export</i>		
	<i>read timeout</i>			<i>import/export</i>		
	<i>wait read timeout</i>			<i>import/export</i>		
tunnel start	<i>start character</i>			<i>import/export</i>		
	<i>echo</i>		<i>enable</i> <i>disable</i>	<i>import/export</i>		
tunnel stop	<i>stop character</i>			<i>import/export</i>		
	<i>echo</i>		<i>enable</i> <i>disable</i>	<i>import/export</i>		
wan	<i>choice</i>	<i>profile</i>		<i>import/export</i>	<i>Value is the name of a WLAN profile. Up to 30 characters.</i>	
	<i>out of range scan interval</i>			<i>import/export</i>	<i>Time interval in seconds. Default: 30 seconds.</i>	
wan profile	<i>basic</i>	<i>network name</i>		<i>import/export</i>	<i>Value is the name of the network. Up to 32 characters.</i>	
		<i>topology</i>	<i>infrastructure</i> <i>adhoc</i>	<i>import/export</i> <i>import/export</i>	<i>Default.</i>	
		<i>channel</i>		<i>import/export</i>	<i>Value is the channel number. Applies only if topology is adhoc. Default: 1.</i>	
	<i>advanced</i>	<i>adhoc merging</i>		<i>enable</i> <i>disable</i>	<i>import/export</i> <i>import/export</i>	<i>Applies only if topology is adhoc. Default.</i> <i>Applies only if topology is adhoc.</i>
			<i>tx data rate minimum</i>	<i>1 Mbps</i> <i>2 Mbps</i> <i>5.5 Mbps</i> <i>6 Mbps</i> <i>9 Mbps</i> <i>11 Mbps</i> <i>12 Mbps</i> <i>18 Mbps</i> <i>24 Mbps</i> <i>36 Mbps</i> <i>48 Mbps</i> <i>54 Mbps</i>	<i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i> <i>import/export</i>	
					<i>import/export</i>	<i>Default.</i>

Figure 22

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
		tx data rate	fixed auto-reduction	import/export	Default.
		tx power maximum		import/export	Value is the number of dBm. Default: 14 dBm.
		tx power	fixed adaptation	import/export	Default.
		tx retries			Value is the number of retries. Default: 4.
		power management	enable disable	import/export	Default.
		power management interval		import/export	Value is number of "beacons". One beacon per 100 ms. Applies only if "power management" is enabled. Default: 1.
	security	suite	none	import/export	Default.
			wep	import/export	
			wpa	import/export	
			wpa2	import/export	
		key type	passphrase hex	import/export	Default.
		passphrase		import/export	Exports as "- configured and ignored -->". Up to 63 characters.
		wep authentication	open shared	import/export	Default.
		wep key size	40 104	import/export	Default.
		wep tx key index	1	import/export	Default.
			2	import/export	
			3	import/export	
			4	import/export	
		wep key 1		import/export	Hexadecimal, up to 26 digits. Exports as "- configured and ignored -->".
		wep key 2		import/export	Hexadecimal, up to 26 digits. Exports as "- configured and ignored -->".
		wep key 3		import/export	Hexadecimal, up to 26 digits. Exports as "- configured and ignored -->".
		wep key 4		import/export	Hexadecimal, up to 26 digits. Exports as "- configured and ignored -->".
		wpa authentication	psk 802.1x	import/export	Default.
		wpa key		import/export	Hexadecimal, up to 64 digits. Exports as "- configured and ignored -->".
		wpa ieee 802.1x	802.1x 802.11s	import/export	import/export

Figure 23

Group Name	Item Name	Value Name	Value	Import/Export	Additional Information
			eap-tls	import/export	Default.
			peap	import/export	
	wpax eap-tls option		eap-mschapv2	import/export	Default.
			mschapv2	import/export	
			mschap	import/export	
			chap	import/export	
			pap	import/export	
			eap-md5	import/export	
	wpax peap option		eap-mschapv2	import/export	Default.
			eap-md5	import/export	
	wpax username			import/export	Up to 63 characters.
	wpax password			import/export	Exports as " <i>!~</i> - configured and ignored <i>--></i> ". Up to 63 characters.
	wpax encryption			import/export	Set to any combination of "ccmp", "tkip", and "wep". For example, "ccmp, wep" selects both CCMP and WEP.
Notes:					
Group "wan" instance is the network name, such as "wan0".					
Group "wan" item "choice" instance is the choice number, from 1 to 4.					
xml import control	restore factory configuration		enable	import/export	
			disable		
	delete cpm groups		enable	import/export	
			disable		
	delete wlan profiles		enable	import/export	Deletes existing profiles before importing new ones.
			disable		
	reboot		enable	import/export	Reboots after importing.
			disable		
xml paste passwords	passwords	cli login		import	Used with the CLI capture feature. If pasting XML into the CLI login password prompt, this field must be the correct CLI login password.
		cli enable level		import	Used with the CLI capture feature. If pasting XML into the CLI enable level password prompt (or CLI login password prompt), this value must be the correct CLI enable level password.

Figure 24

Network Communication mode

A serial tunneling communication is a communication between two serial devices connected over an IP-based network.

Two ARF45-PRO modem devices can be used to create a “serial tunnel” over an IP network (it does not matter whether the connection is a point to point connection, in the case of ad-hoc network, or a connection via an AP, in case of infrastructure network). This can be thought of as cable replacement.

The ARF45-PRO supports two tunneling connections simultaneously on its serial port. One of these connections is Connect Mode and the other connection is Accept Mode.

When any character comes in through the serial port, it gets copied to both the Connect Mode connection and the Accept Mode connection (if both are active). See the figures on the next pages.

Connect mode

In this mode, the ARF45-PRO actively makes a connection. In other words, the ARF45-PRO behaves like an IP client. The receiving node on the network must listen for the Connect Mode's connection.

Note: Connect Mode is disabled by default!

For Connect Mode to function, it must be enabled, have a remote station (node) configured, and a remote port configured (TCP or UDP).

Enter the remote station as an IP address or DNS name. The ARF45-PRO will not make a connection unless it can resolve the address.

The screenshot shows the 'Tunnel 1 - Connect Mode' configuration page. At the top, there are tabs for 'Tunnel 1' and 'Tunnel 2'. Below these are buttons for 'Statistics', 'Serial Settings', 'Start/Stop Chars', 'Accept Mode', 'Connect Mode', and 'Disconnect Mode'. Further down are 'Packing Mode' and 'Modem Emulation' buttons.

Tunnel 1- Connect Mode

Mode:	Always
Remote Address:	192.168.0.1
Remote Port:	20
Local Port:	20
Protocol:	TCP
TCP Keep Alive:	45000 milliseconds
Reconnect Timer:	15000 milliseconds
Flush Serial Data:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Network:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Output:	Group:

Mode: Always

Remote Address: 192.168.0.1

Remote Port: 20

Local Port: 20

Protocol: TCP

TCP Keep Alive: 45000 milliseconds

Reconnect Timer: 15000 milliseconds

Flush Serial Data: Enabled Disabled

Block Serial: Enabled Disabled

Block Network: Enabled Disabled

Email on Connect: <None>

Email on Disconnect: <None>

CP Output: Group:

A Tunnel in Connect Mode can be started in a number of ways:

- Disabled:** never started.
- Always:** always started.
- Any Character:** started when any character is read on the Serial Line.
- Start Character:** started when the Start Character is read on the Serial Line.
- Modem Control Asserted:** started when the Modem Control pin is asserted on the Serial Line.
- Modem Emulation:** started by an ATD command.

Figure 25

Connect Mode supports the following protocols:

- TCP
- AES encryption over UDP
- AES encryption over TCP
- SSH (the ARF45-PRO is the SSH client)
- UDP (available only in Connect Mode because it is a connectionless protocol).

Connect Mode has five states:

- Disabled (no connection)
- Enabled (always makes a connection)
- Active if it sees any character from the serial port
- Active if it sees a specific (configurable) character from the serial port.
- Modem emulation

Accept mode

In this mode, the ARF45-PRO listens for a connection. In other words, the ARF45-PRO behaves like an IP server. A node on the network initiates the connection.

Note: Accept Mode is enabled by default!

In Accept Mode, the ARF45-PRO waits for a connection. The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. The default local port is 10001.

The screenshot displays the configuration interface for Tunnel 1. The sidebar on the left lists various system functions, with 'Tunnel' highlighted. The top navigation bar includes the 'A^{RF45-PRO}' logo and the 'Adeunis' logo. The main content area is divided into three sections: a top navigation bar for 'Tunnel 1' and 'Tunnel 2', a central configuration table, and a right-hand help text box.

Tunnel 1 - Accept Mode

Mode:	Always
Local Port:	10001
Protocol:	TCP
TCP Keep Alive:	45000 milliseconds
Flush Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Serial:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Block Network:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Password:	<None>
Email on Connect:	<None>
Email on Disconnect:	<None>
CP Output:	Group:

Tunnel Accept Mode controls how a tunnel behaves when a connection attempt originates from the network.

Figure 26

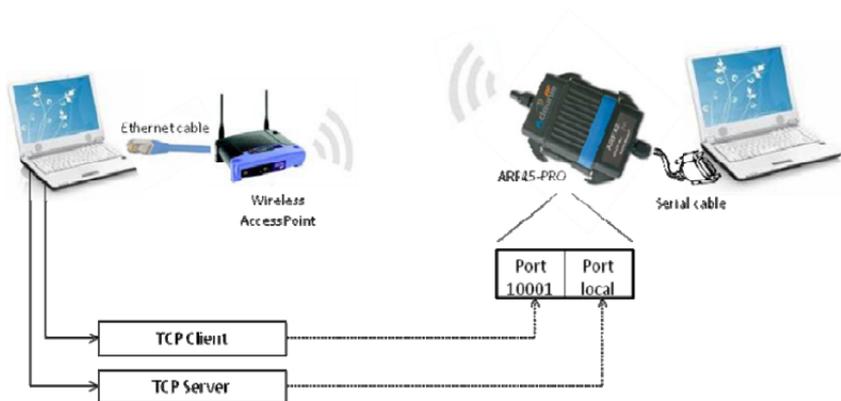


Figure 27

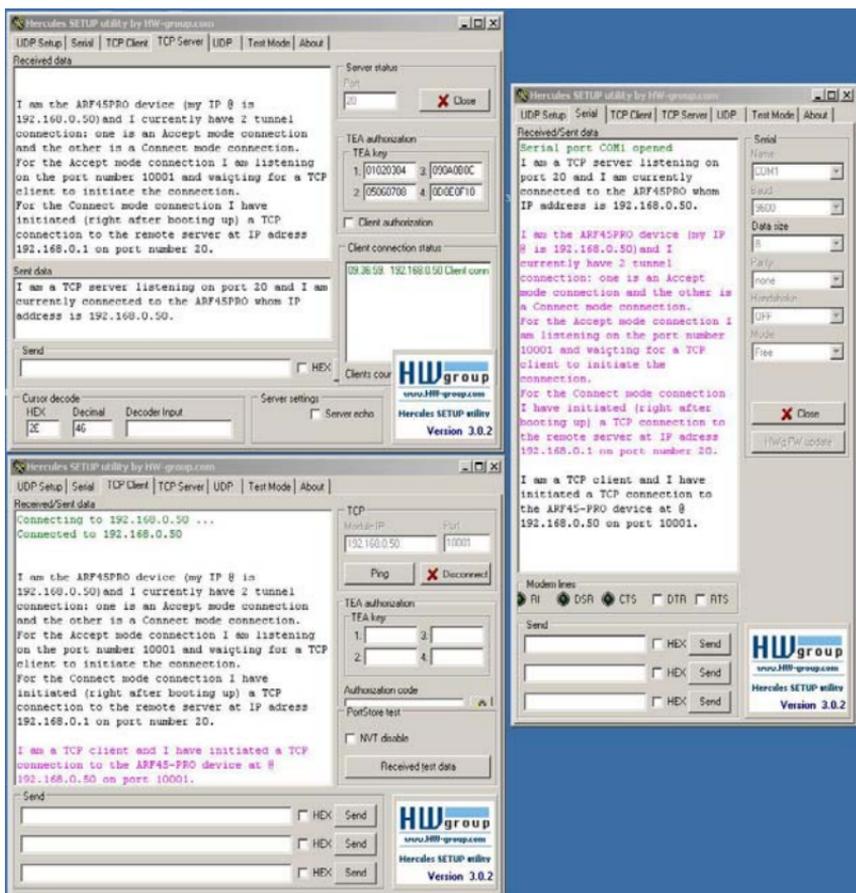


Figure 28

Port numbers

Every TCP connection and every UDP datagram is defined by a destination and source IP address, and a destination and source port number.

Ref. 09-03-V0-jcs

For example, a Telnet server commonly uses port number 23.

The following is a list of the default (and thus reserved) server port numbers running on the ARF45-PRO:

- TCP Port 22: SSH Server (Command Mode configuration)
- TCP Port 23: Telnet Server (Command Mode configuration)
- TCP Port 80: HTTP (Web Manager configuration)
- TCP Port 443: HTTPS (Web Manager configuration)
- UDP Port 161: SNMP
- TCP Port 21: FTP
- UDP Port 69: TFTP
- UDP Port 30718: Query port
- TCP/UDP Port 10001: Tunnel 1

Modem emulation mode

The ARF45-PRO supports Modem Emulation mode for devices that send out modem signals. There are two different modes supported:

Command Mode: sends back verbal response codes.

Data Mode: information transferred in is also transferred out.

Command mode

The Modem Emulation's Command Mode supports the standard AT command set. For a list of available commands from the serial or Telnet login, enter AT?

Command	Description
+++	Switches to Command Mode if entered from serial port during connection.
AT?	Help.
ATDT<Address Info>	Establishes the TCP connection to socket (<IP>/<port>).
ATDP<Address Info>	See ATDT.
ATD	Like ATDT. Dials default Connect Mode remote address and port.
ATD<Address Info>	Sets up a TCP connection. A value of 0 begins a command line interface session.
ATO	Switches to data mode if connection still exists. Vice versa to '+++'.
ATEn	Switches echo in Command Mode (off - 0, on - 1).
ATH	Disconnects the network session.
ATI	Displays modem information.
ATQn	Quiet mode (0 - enable results code, 1 - disable results code.)
ATVn	Verbose mode (0 - numeric result codes, 1 - text result codes.)
ATXn	Command does nothing and returns OK status.
ATUn	Accept unknown commands. (n value of 0 = off, n value of 1 = on.)
AT&V	Display current and saved settings.
AT&F	Reset settings in NVR to factory defaults.
AT&W	Save active settings to NVR.
ATZ	Restores the current state from the setup settings.
ATS0=n	Accept incoming connection. n value of 0 = disable n value of 1 = connect automatically n value of 2+ = connect with ATA command.
ATA	Answer incoming connection (if ATS0 is 2 or greater).
A/	Repeat last valid command.

Figure 29

All of these commands behave like a modem. For commands that are valid but not applicable to the ARF45-PRO, an "OK" message is sent (but the command is silently ignored).

The ARF45-PRO attempts to make a Command Mode connection as per the IP/DNS/port numbers defined in Connect Mode. It is possible to override the remote address, as well as the remote port number.

When using ATD, enter 0.0.0.0 to switch to Command Mode.

Entering Command mode on the ARF45-PRO

Like mentioned previously in this document, the modem emulation mode can be used to enter the command mode at any time. In order for this to work, both the Accept and Connect mode has to be set with the Modem emulation mode. Then entering the "+++" string enables to switch to command mode at any time without resetting the device.

For the Accept tunnel connection, the connection can be established automatically (initiated from a remote node on the network) if configured. However for the Connect tunnel connection, the ATD command has to be entered in order to establish the connection with the remote node on the network.

The screenshot displays the configuration page for Tunnel 1 - Modem Emulation. At the top, there are tabs for Tunnel 1 and Tunnel 2. Below the tabs, there are three main sections: Statistics, Serial Settings, and Start/Stop Chars. The Serial Settings section is active, showing options for Accept Mode, Connect Mode, and Packing Mode. The Start/Stop Chars section shows options for Disconnect Mode and Modem Emulation.

Tunnel 1- Modem Emulation

Configuration	Status
Echo Pluses: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	
Echo Commands: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
Verbose Response: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
Response Type: <input checked="" type="radio"/> Text <input type="radio"/> Numeric	Text
Error Unknown Commands: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Enabled
Incoming Connection: <input type="radio"/> Disabled <input checked="" type="radio"/> Automatic <input type="radio"/> Manual	Automatic
Connect String: <input type="text"/>	
Display Remote IP: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	

A Tunnel in Connect Mode can be initiated using Modem commands incoming from the Serial Line.

With **Echo Pluses** enabled, pluses will be echoed during a "pause +++ pause" escape sequence on the Serial Line.

With **Echo Commands** enabled (ATE1), characters read on the Serial Line will be echoed while the Line is in Modem Command Mode.

With **Verbose Response** enabled (ATQ0), Modem Response Codes are sent out on the Serial Line.

Response Type selects either Text (ATV1) or Numeric (ATV0) representation for the Modem Response Codes sent out on the Serial Line.

With **Error Unknown Commands** enabled (ATU0), ERROR is returned for unrecognized AT commands. Otherwise (ATU1) OK is returned for unrecognized AT commands.

Incoming Connection requests may be disabled (ATS0=0), answered automatically (ATS0=1), or answered manually via the ATA command after an incoming RING (ATS0=2).

The **Connect String** is a customized string that is sent with the CONNECT Modem Response Code.

With **Display Remote IP** enabled, the incoming RING is followed by the IP address of the caller.

Figure 30

Security modes in details

Features overview

The ARF45-PRO device enables to add Wi-Fi networking capability to devices with the highest WPA2/802.11i enterprise-grade security and authentication protocols.

Like the ARF45, the ARF45-PRO supports the WPA/WPA2 Personal mode which is a security mode that uses pre-shared key (PSK) for authentication.

On top of that, the ARF45-PRO also supports the WPA/WPA2 Enterprise mode which enables to meet the rigorous requirement of enterprise security by leveraging the 802.1X authentication framework which in turns relies on EAP and an authentication server (RADIUS server) to provide strong mutual authentication between the client and the authentication server via an access point.

The picture below depicts the deployment scheme in which are involved three components: the WIFI client (for instance an ARF45-PRO) also called the supplicant, the Access Point also called the authenticator and the authentication RADIUS server in charge of performing the client authentication.

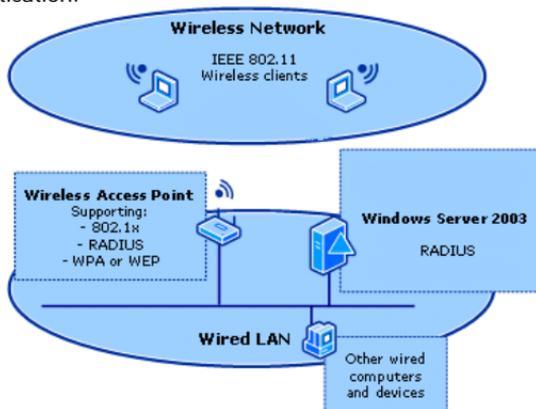


Figure 31

Note: WPA and WPA2/IEEE 802.11i are not available for Ad-hoc topology.

EAP methods supported

Here are the EAP methods that are supported by the ARF45-PRO:

LEAP = Lightweight Extensible Authentication Protocol.

EAP-TLS = Extensible Authentication Protocol - Transport Layer Security: requires authentication certificates on both the network side and the ARF45-PRO side.

EAP-TTLS = Extensible Authentication Protocol - Tunneled Transport Layer Security.

PEAP = Protected Extensible Authentication Protocol.

EAP-TTLS and PEAP have been developed to avoid the requirement of certificates on the client side which makes deployment more cumbersome. Both make use of EAP-TLS to authenticate the server (network) side and establish an encrypted tunnel. This is called the outer-authentication. Then a conventional authentication method (MD5, MSCHAP, etc.) is used through the tunnel to authenticate the ARF45-PRO. This is called inner-authentication.

Security mode deployment

This chapter describes how to deploy the WPA/WPA2 Enterprise security mode using the PEAP and EAP-TLS authentication methods.

The deployment has been carried out using a Windows Server 2003 authentication server running Authentication services, a Certificate Authority and a RADIUS server.

 When using EAP-TLS, EAP-TTLS or PEAP authentication methods at least one authority certificate will have to be installed on the ARF45-PRO that is
Ref. 09-03-V0-jcs

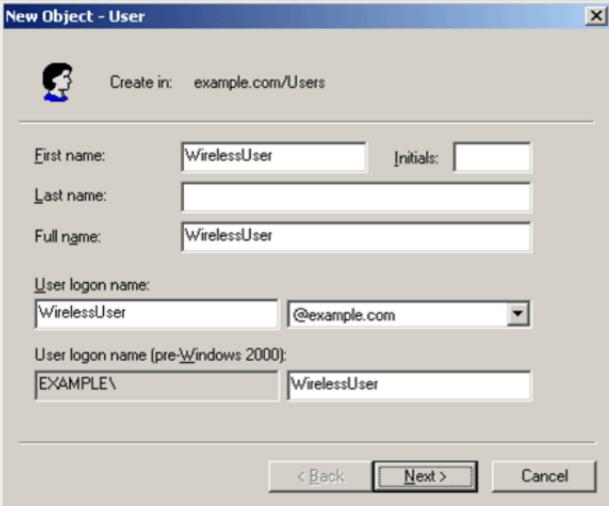
able to verify the Radius server's certificate. In case of EAP-TLS also a certificate and matching private key need to be configured to authenticate the ARF45-PRO to the Radius server (that is to identify itself) and sign its messages.

Prior to embark on the configuration of the ARF45-PRO, both EAP-TLS and PEAP based authentication methods require the RADIUS server and the access point (which is also called the RADIUS client) to be correctly configured.

RADIUS authentication server: configuration

Add users to the domain:

- In the **Active Directory Users and Computers** console tree, right-click **Users**, click **New**, and then click **User**.
- In the New Object – User dialog box, type WirelessUser in First name and type WirelessUser in User logon name. This is shown in the following figure.



The screenshot shows a dialog box titled "New Object - User". At the top, it says "Create in: example.com/Users". Below this, there are several input fields:

- First name: Initials:
- Last name:
- Full name:
- User logon name: - User logon name (pre-Windows 2000):

At the bottom, there are three buttons: "< Back", "Next >" (which is highlighted with a black border), and "Cancel".

Figure 32

- Click Next. In the New Object – User dialog box, type a password of your choice in Password and Confirm password. Clear the User must change password at next logon check box, and then click Next. This is shown in the following figure.

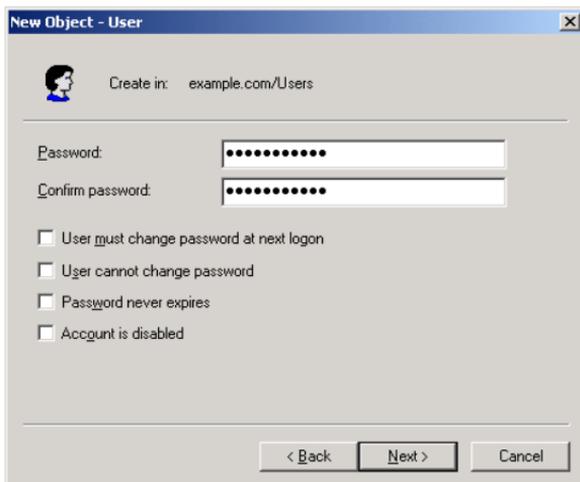


Figure 33

- In the final New Object – User dialog box, click Finish.

Allow wireless access to users:

- In the Active Directory Users and Computers console tree, click the Users folder, right-click WirelessUser, click Properties, and then click the Dial-in tab.
- Select Allow access, and then click OK.

Add groups to the domain:

- In the Active Directory Users and Computers console tree, right-click Users, click New, and then click Group.
- In the New Object – Group dialog box, type WirelessUsers in Group name, and then click OK. This is shown in the following figure.

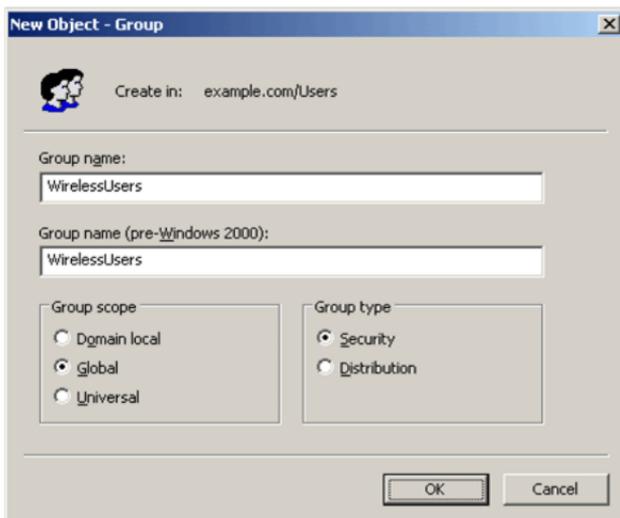


Figure 34

Add users to the WirelessUsers group :

- In the details pane of the Active Directory Users and Computers, double-click WirelessUsers.
- Click the Members tab, and then click Add.
- In the Select Users, Contacts, Computers, or Groups dialog box, type wirelessuser in Enter the object names to select.
- Click OK. In the Multiple Names Found dialog box, click OK. The WirelessUser user account is added to the WirelessUsers group.
- Click OK to save changes to the WirelessUsers group.

Add a Wireless AP as RADIUS client :

- In the console tree of the Internet Authentication Service snap-in, right-click RADIUS Clients, and then click New RADIUS Client.
- On the Name and Address page of the New RADIUS Client wizard, in Friendly name, type WirelessAP. In Client address (IP or DNS), type the IP address of the AP on the network, and then click Next. This is shown in the following figure.

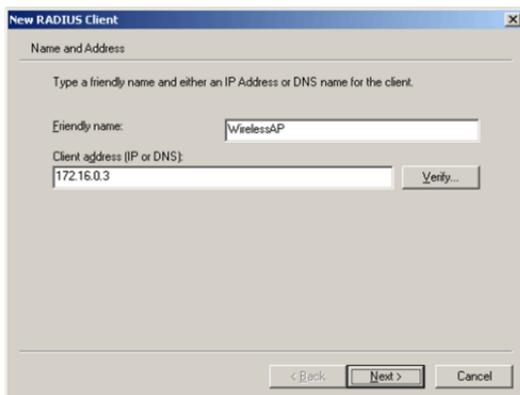


Figure 35

- Click Next. On the Additional Information page of the New RADIUS Client wizard, for Shared secret, type a RADIUS shared secret for the wireless AP, and then type it again in Confirm shared secret. This is shown in the following figure. The shared secret entered here needs to match the RADIUS shared secret on the configuration of the wireless AP.

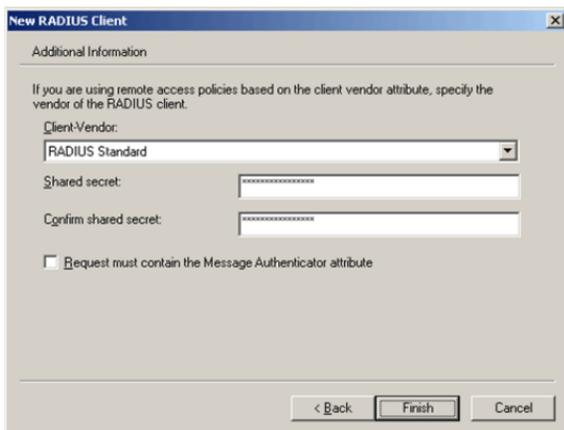


Figure 36

- Click Finish.

Create and configure remote access policy :

- In the console tree of the Internet Authentication Service snap-in, right-click Remote Access Policies, and then click New Remote Access Policy.
- On the Welcome to the New Remote Access Policy Wizard page, click Next.
- On the Policy Configuration Method page, type Wireless access to intranet in Policy name. This is shown in the following figure.

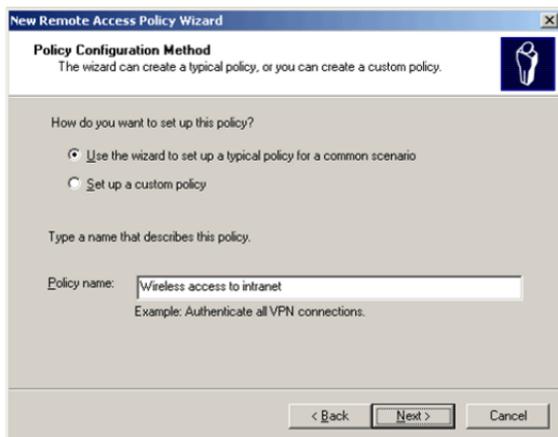


Figure 37

- Click Next. On the Access Method page, select Wireless. This is shown in the following figure.

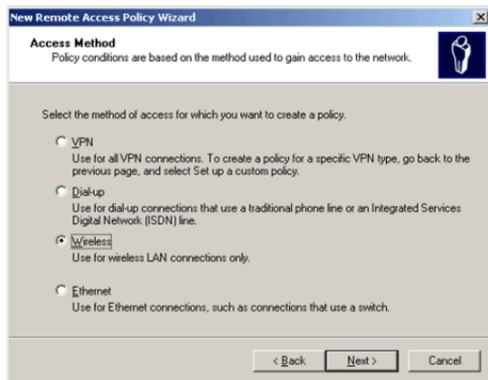


Figure 38

- Click Next. On the User or Group Access page, select Group. This is shown in the following figure.

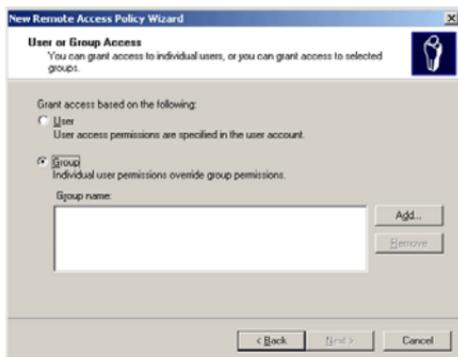


Figure 39

- Click Add. In the Select Groups dialog box, click Locations, select example.com, and then click OK.
- Type wirelessusers in the Enter the object names to select box. This is shown in the following figure.

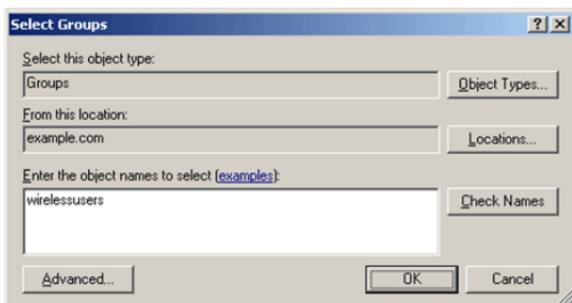


Figure 40

- Click OK. The WirelessUsers group in the example.com domain is added to the list of groups on the User or Group Access page. This is shown in the following figure.



Figure 41

- Click Next. On the Authentication Methods page, select "Smart card or other certificate" (for EAP-TLS deployment) or "Protected EAP" (for PEAP deployment). In case of PEAP deployment, the user also has to choose the inner-authentication method (MS-CHAP v2, CHAP ...) to be used.
- Click Next. On the Completing the New Remote Access Policy page, click Finish.

Wireless Access Point: configuration

On the AP side there is only a few things to do:

- In the advance security settings, select the WPA/WPA2 802.1X authentication and security protocols.
- Entering the IP address of the RADIUS server.
- Entering the authentication port of the RADIUS server (1812 by default).

- Entering the shared secret, which must match the shared secret previously entered on the RADIUS server.

EAP-TLS based deployment

There are several steps that have to be carried out in order to deploy the EAP-TLS based security mode on the ARF45-PRO device.

The EAP-TLS method requires authentication certificates on both the network side (that is on the authentication RADIUS server) and the ARF45-PRO side.

Certificate generation

So the very **first step** (after having configured the RADIUS server and the Access Point) consists of generating two certificates: the user/client certificate (along with its private key) and the Certificate Authority (CA) root certificate.

Here are described below the steps to follow in order to generate the **client certificate**:

- Make sure that Certificate Services are running on the Windows server. Open the Services program through the Start Menu (Start->Administrative Tools->Services). Find the Certificate Services line and check if the status shows up as "Started". If not, right click on the Certificate Services line and select Start.

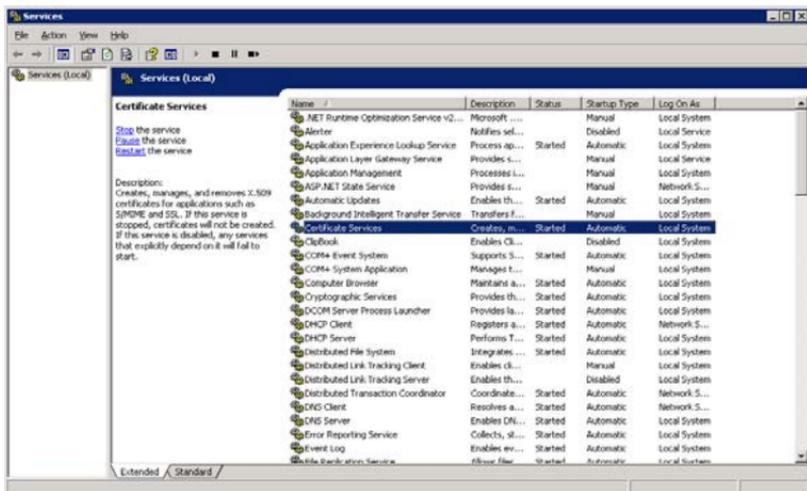


Figure 42

- On the Windows server, open a web browser (e.g. Internet Explorer), and enter <http://127.0.0.1/certsrv> for the address. If prompted for user name and password, enter those configured for the EAP authentication user.

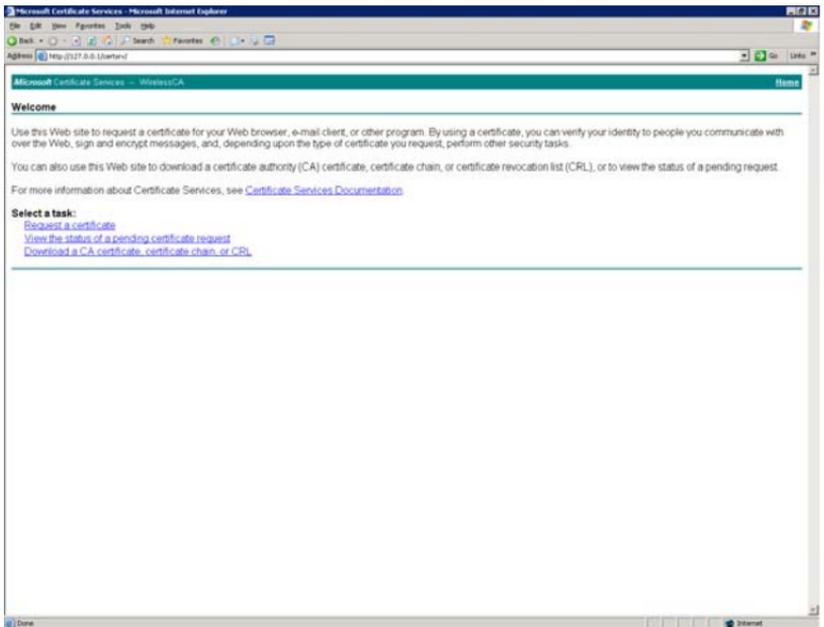


Figure 43

- Click on "Request a certificate". On the page that loads, click on "advanced certificate request".

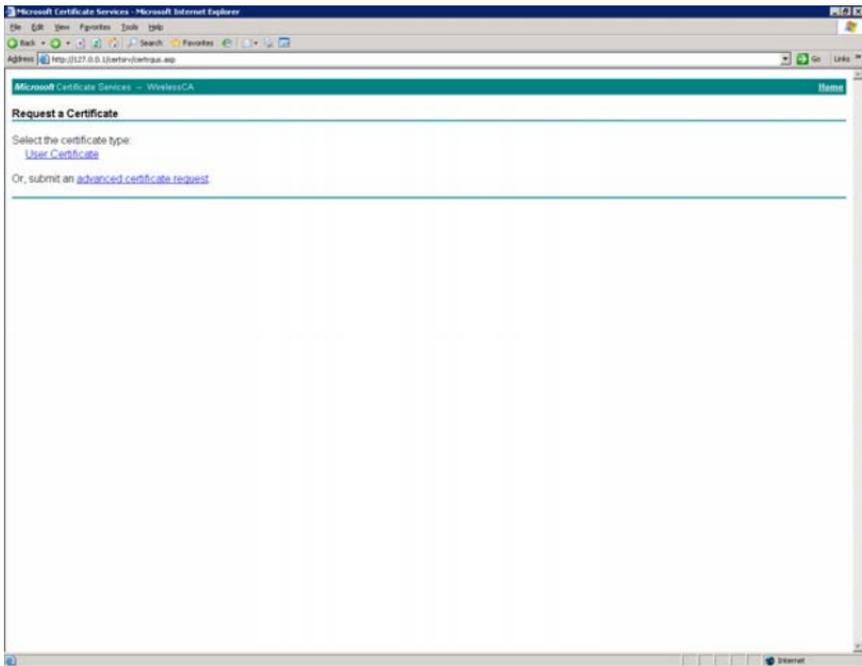


Figure 44

- On the next page click on "Create and submit a request to this CA".

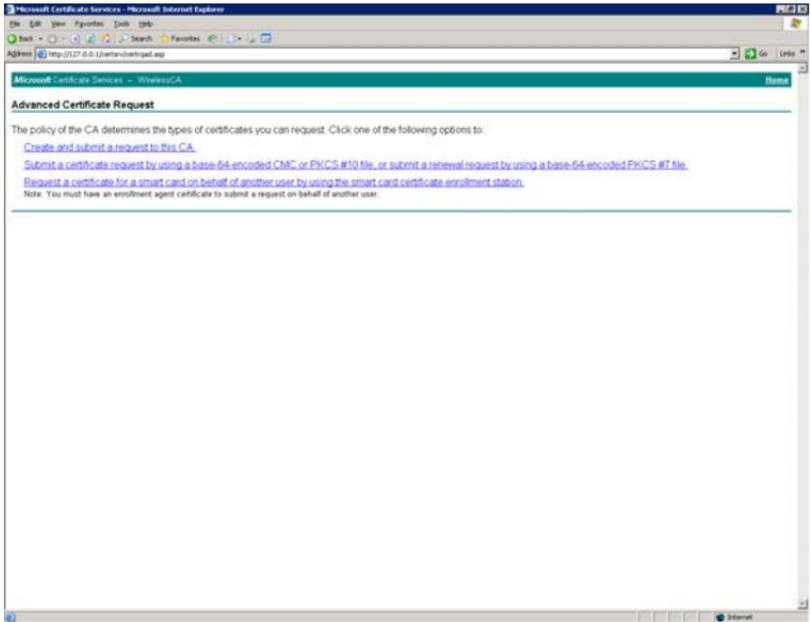


Figure 45

- On the page that loads select “User” under Certificate Template. Make sure “Mark keys as exportable” is selected, and also select “Export keys to file”. Then select a full path name to save the private key to under “Full path name:” The request format should be set to CMC. Select a Friendly name in the box provided. Once completed, click on the “Submit” button. If prompted whether or not you want to request a certificate now, click “Yes”.

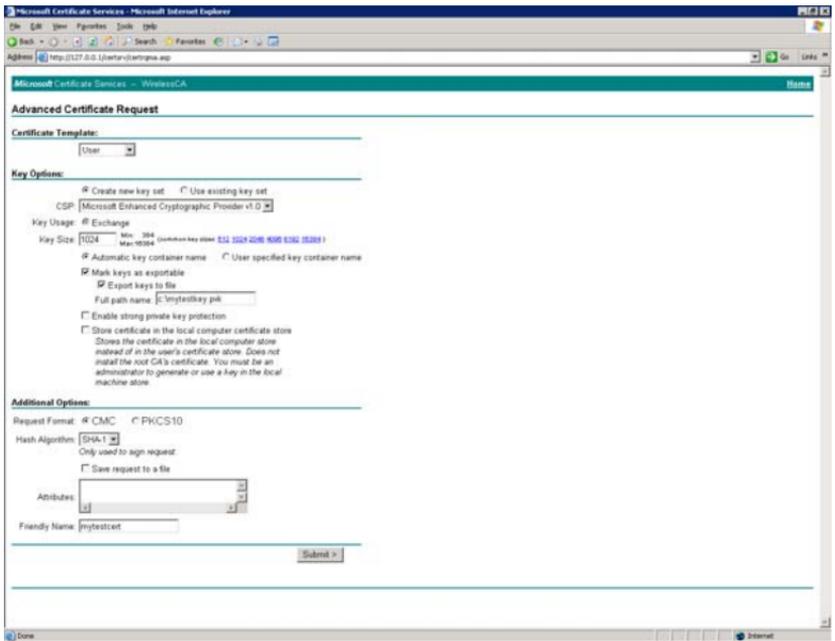


Figure 46

- When prompted to create a private key password, select “None”.



Figure 47

- On the next page, make sure that "DER encoded" is selected, and click on "Download certificate".

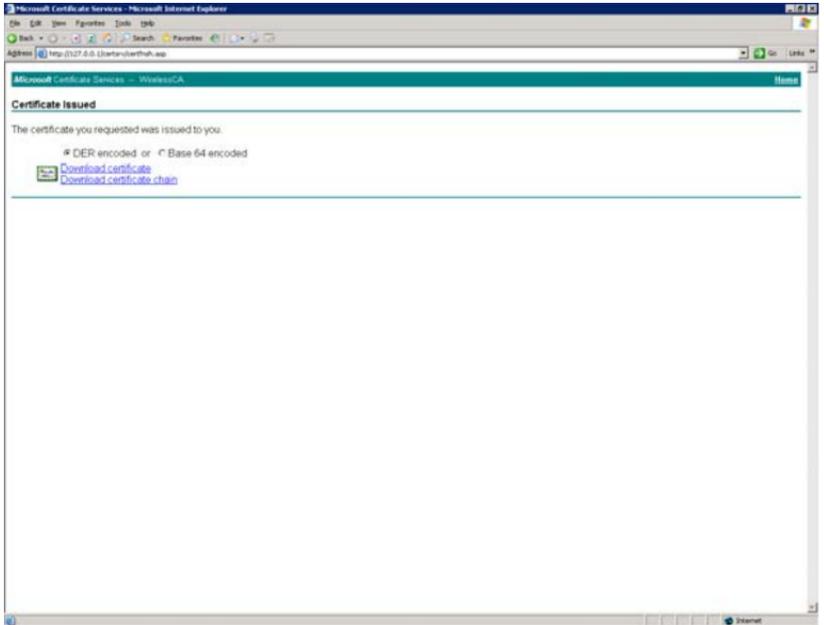


Figure 48

Here are described below the steps to follow in order to generate the CA root certificate:

- Open the Certificate Authority Program (assumes certificate authority is already setup). You can find the CA in Start Menu/Administrative Tools/Certificate Authority.

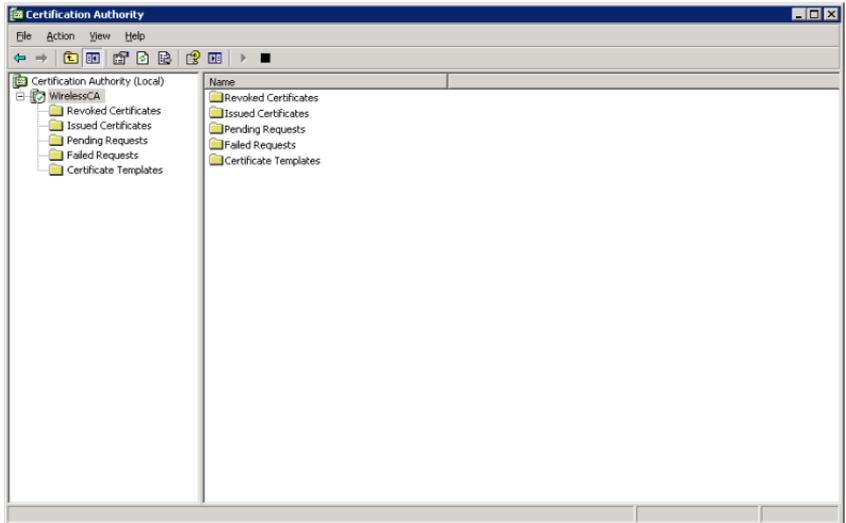


Figure 49

- Right click on the CA and select "Properties". Then click on "View Certificate".

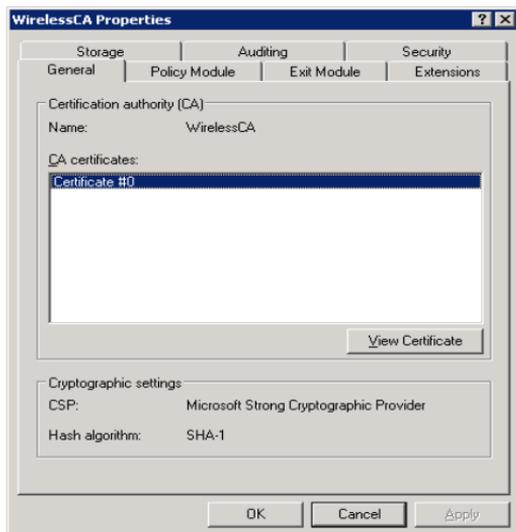


Figure 50

- Click on the Details tab, and then the "Copy to File" button.

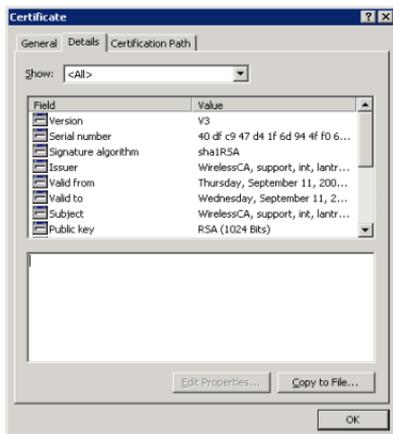


Figure 51

- Click "Next" on the initial certificate export wizard window. Then select "DER encoded binary X.509 (.CER)" and click the "Next" button.

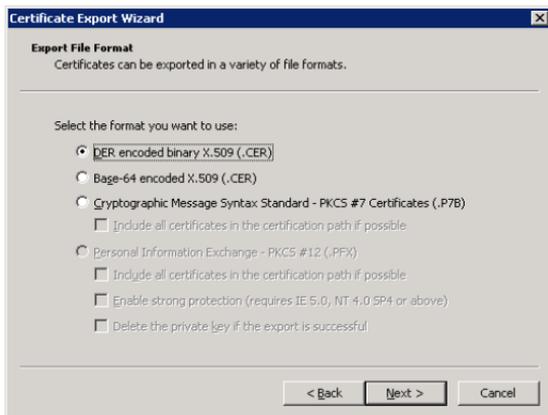


Figure 52

- Select a file path to export to by clicking on the browse button, name the file and click save. Then click "Next".

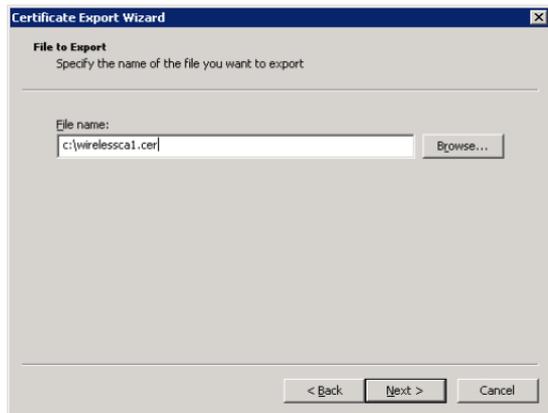


Figure 53

- Now click Finish. You will see “The Export was successful.” Window and click OK. Then click OK twice more to exit all windows and close the CA program.



Figure 54

Certificate conversion

Then the **second step** consists in converting the certificates's format onto a format that is supported by the ARF45-PRO, that is the PEM format.

Certificates and private keys can be stored in several file formats. Best known are PKCS12, DER and PEM. Certificate and key can be in the same file or in separate files. The key can be encrypted with a password or not.

⚠ The ARF45-PRO currently only accepts separate PEM files and the key needs to be unencrypted!!

The user certificate as well as the CA certificate have been generated in the DER format.

However the ARF45-PRO only supports for certificate in PEM format => thus a conversion has to be performed in order for the certificates to be uploaded onto the ARF45-PRO.

For this purpose two utility tools are required: *openssl* and *pvktool*.

Openssl enables to convert the certificate file from DER format onto PEM format, whereas *pvktool* enables to convert the private key file from the PVK format onto the PEM format.

Those tools as well as a procedure explaining how to carry out the conversion can be downloaded from Adeunis web site.

Certificate upload

The **third step** consists in uploading the certificates onto the ARF45-PRO.

Login to the ARF45-PRO and go to the SSL page:

SSL

Upload Certificate

New Certificate:

New Private Key:

Upload Authority Certificate

Authority:

Create New Self-Signed Certificate

Country (2 Letter Code):

State/Province:

Locality (City):

Organization:

Organization Unit:

Common Name:

Expires: mm/dd/yyyy

Key length: 512 bit 768 bit 1024 bit

Type: RSA DSA

Current SSL Certificates

An SSL Certificate must be configured in order for the HTTP Server to listen on the HTTPS Port. This certificate can be created elsewhere and uploaded to the device or automatically generated on the device. A certificate generated on the device will be self-signed.

If uploading an existing SSL Certificate, take care to ensure the Private Key will not be compromised in transit. This implies the data is uploaded over some kind of secure private network.

WARNING: When generating a new self-signed SSL Certificate, using a large key size can result in a VERY LONG key generation time. Tests on this hardware have shown it can take upwards of:

- 10 seconds for a 512 bit RSA Key
- 30 seconds for a 768 bit RSA Key
- 1 minute for a 1024 bit RSA Key
- 30 seconds for a 512 bit DSA Key
- 2 minutes for a 768 bit DSA Key
- 6 minutes for a 1024 bit DSA Key

Figure 55

User Certificate and private key:

Under Upload Certificate set the paths where the converted PEM encoded certificate and private key are stored. Once complete, click on the Submit button to commit the changes.

CA certificate:

Under “Upload Authority Certificate”, select browse to the path where the converted PEM encoded certificate is stored and click “Submit”.

Current SSL Certificates	
[Delete]	
Type:	RSA
Version:	3 (0x02)
Serial Number:	61 1c 3a 9f 00 02 00 00 00 16
Signature Algorithm:	sha1WithRSAEncryption
Issuer:	C: ST: L: O: OU: CN: LABO
Validity:	Issued On: Mar 24 14:55:31 2009 GMT Expires On: Mar 24 14:55:31 2010 GMT
Subject:	C: ST: L: O: OU: CN: arf45Pro
Subject Public Key:	1024-bit e5 9f 56 5d 0a 36 65 51 60 2b b5 fd e1 23 e2 2b 90 ea 4b b5 54 56 2f 5f 06 40 17 4b 00 0f ea 8e 44 4e 7a 60 0b de 81 6e 9f 2e a9 5f 75 40 3c f6 ac 68 ff 50 40 06 10 e5 fc d0 b5 a7 1e 9a 7c 9c 13 f6 49 0e 55 c4 ad da 7a 69 02 dd d4 0c d3 5a b6 69 4b d4 3a d9 11 92 30 ec a0 25 ef 1e e5 b4 54 87 45 23 26 16 0b 94 0e 44 6d 23 ee 92 63 2b 42 a0 ea 87 46 66 88 9e 74 f2 0a b0 8e 2a 20 3d
Current Certificate Authorities	
Trusted Authority [Delete]	C: ST: L: O: OU: CN: LABO

Figure 56

Setting the security suite

The **last step** consists in setting the security parameters on the ARF45-PRO side

Login to the ARF45-PRO and go to the WLAN Profile page.

Click on the existing profile you want to use for EAT-TLS security deployment or you can create a new profile dedicated to EAP-TLS deployment.

The screenshot displays the configuration page for a WLAN Profile named "EAP_TLS_secured_profile". The interface includes a left-hand navigation menu with various system settings, a main configuration area, and a right-hand help section.

WLAN Profile "EAP_TLS_secured_profile"

Basic Configuration

Network Name:	test
Topology:	<input checked="" type="radio"/> Infrastructure <input type="radio"/> Adhoc

Advanced Configuration

TX Data Rate Maximum:	54 Mbps
TX Data Rate:	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto-reduction
TX Power Maximum:	14 dBm
TX Power:	<input type="radio"/> Fixed <input checked="" type="radio"/> Adaptation
TX Retries:	7
Power Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

Security Configuration

Suite:	WPA
Authentication:	<input type="radio"/> PSK <input checked="" type="radio"/> IEEE 802.1X
IEEE 802.1X:	EAP-TLS
Username:	arf45Pro
Encryption:	<input checked="" type="checkbox"/> CCMP <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> WEP

Help Text:

This page shows configuration of a WLAN Profile on the device.

In the **Basic Configuration** section, choice of **Topology** affects the make-up of configurables in that section and in the **Advanced Configuration** section.

In the **Advanced Configuration** section, if **Power Management** is enabled, specify the **Power Management Interval**.

In the **Security Configuration** section, choice of **Suite**, **Key Type**, **Authentication**, and **IEEE 802.1X** (when visible) affect the make-up of other configurables in that section.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

Figure 57

Choose EAP-TLS from the drop down box for the IEEE 802.1X Configuration. Check the boxes for CCMP & TKIP for Encryption and click submit. If the profile is a newly created one, don't forget to add it in the list of active profile in the network page:

The screenshot shows the ARF45-PRO web interface. The navigation menu on the left includes: Status, CLI, CPM, CPU Power Mgmt, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Network (highlighted), ppp, Protocol Stack, Query Port, RSS, SNMP, SSH, SSL, Syslog, System, Terminal, TFTP, Tunnel, WLAN Profiles, and XML.

The main configuration area is titled "Network 2 (wlan0) WLAN Link Configuration". It features a breadcrumb trail: Network 1 > Network 2 > Interface > Link > Status > Configuration > Scan. The configuration table is as follows:

Choice 1 Profile:	default_infrastructure_profile
Choice 2 Profile:	default_adhoc_profile
Choice 3 Profile:	PEAP_secured_profile
Choice 4 Profile:	EAP_TLS_secured_profile
Out of Range Scan Interval:	1 seconds
Roaming:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

The right sidebar contains the following text:

This page shows configuration of a WLAN Link on the device.

The configuration details are stored in one or more **WLAN Profile**. List the selected WLAN Profiles in order of preference here.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

Figure 58

You are now ready to use your ARF45-PRO to authenticate to the RADIUS server and get access to your wireless network.

PEAP based deployment

There are several steps that have to be carried out in order to deploy the PEAP based security mode on the ARF45-PRO device.

Ref. 09-03-V0-jcs

PEAP have been developed to avoid the requirement of certificates on the client side which makes deployment more cumbersome.

So PEAP methods requires only one authority certificate to be installed on the ARF45-PRO so to be able to verify the Radius server's certificate.

All the steps (listed on the previous chapter) that apply to the EAP-TLS method also apply to the PEAP method.

The only differences are:

- The user does not need to generate a user/client certificate and thus only the CA root certificate is uploaded in the ARF45-PRO (on the SSL page).
- On the WLAN Profile page choose PEAP from the drop down box for the IEEE 802.1X Configuration.
Also, select the PEAP option (MS-CHAP v2, CHAP ...) and check the boxes for CCMP & TKIP for Encryption.
Enter the *username* and *password* that are used for identifying the ARF45-PRO to the RADIUS server on the network.
Username and *Password* correspond to the username and password entered when creating the user account on the authentication RADIUS server.

Then click submit.





Status

CLI

CPM

CPU Power Mgmt

Diagnostics

DNS

Email

Filesystem

FTP

Host

HTTP

IP Address Filter

Line

LPD

Network

PPP

Protocol Stack

Query Port

RSS

SNMP

SSH

SSL

Syslog

System

Terminal

TFTP

Tunnel

WLAN Profiles

XML

WLAN Profile "PEAP_secured_profile"

Basic Configuration	
Network Name:	<input type="text" value="test"/>
Topology:	<input checked="" type="radio"/> Infrastructure <input type="radio"/> Adhoc
Advanced Configuration	
TX Data Rate Maximum:	<input type="text" value="54"/> Mbps
TX Data Rate:	<input type="radio"/> Fixed <input checked="" type="radio"/> Auto-reduction
TX Power Maximum:	<input type="text" value="14"/> dBm
TX Power:	<input type="radio"/> Fixed <input checked="" type="radio"/> Adaptation
TX Retries:	<input type="text" value="7"/>
Power Management:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Security Configuration	
Suite:	<input type="text" value="WPA"/>
Authentication:	<input type="radio"/> PSK <input checked="" type="radio"/> IEEE 802.1X
IEEE 802.1X:	<input type="text" value="PEAP"/>
PEAP Option:	<input type="text" value="EAP-MSCHAPV2"/>
Username:	<input type="text" value="arf45Pro"/>
Password:	<input type="text" value="<Configured>"/>
Encryption:	<input checked="" type="checkbox"/> CCMP <input checked="" type="checkbox"/> TKIP <input type="checkbox"/> WEP

This page shows configuration of a WLAN Profile on the device.

In the **Basic Configuration** section, choice of **Topology** affects the makeup of configurables in that section and in the **Advanced Configuration** section.

In the **Advanced Configuration** section, if **Power Management** is enabled, specify the **Power Management Interval**.

In the **Security Configuration** section, choice of **Suite**, **Key Type**, **Authentication**, and **IEEE 802.1X** (when visible) affect the makeup of other configurables in that section.

Use the **Apply** button to try out settings on the WLAN without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.

Use the **Submit** button to both update the WLAN settings and save them to Flash.

Figure 59

Roaming capability

The ARF45-PRO provides roaming capability across WLAN networks. When WPA2 is enabled, pre-authentication enables smooth and automatic transition to an access point with a stronger signal.

The roaming feature of the ARF45-PRO can be enabled from the Network-> Network 2-> configuration pages using the web-based method.

The screenshot displays the web-based configuration interface for the ARF45-PRO device. The left sidebar contains a navigation menu with categories like Status, CLI, CPM, CPU Power Mgmt, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Network (highlighted), PPP, Protocol Stack, Query Part, RSS, SNMP, SSH, SSL, System, System, Terminal, TFTP, Tunnel, WLAN Profiles, and XML. The main content area is titled 'Network 2 (wlan0) WLAN Link Configuration'. At the top, there are tabs for 'Network 1' and 'Network 2', and sub-tabs for 'Interface' and 'Link'. Below these are 'Status', 'Configuration', and 'Scan' buttons. The configuration table is as follows:

Choice 1 Profile:	<input type="text" value="default_infrastructure_profile"/>
Choice 2 Profile:	<input type="text" value="default_adhoc_profile"/>
Choice 3 Profile:	<input type="text" value="PEAP_secured_profile"/>
Choice 4 Profile:	<input type="text" value="EAP_TLS_secured_profile"/>
Out of Range Scan Interval:	<input type="text" value="1"/> seconds
Roaming:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

On the right side of the configuration area, there is explanatory text: 'This page shows configuration of a WLAN Link on the device. The configuration details are stored in one or more WLAN Profile. List the selected WLAN Profiles in order of preference here. Use the Apply button to try out settings on the WLAN without saving them to flash. If the settings do not work, when you reboot the device, it will still have the original settings. Use the Submit button to built update the WLAN settings and save them to flash.'

Figure 60

Checking *Enabled* enables roaming to other Access Points with the same SSID.

COM port redirector

A COM Port Redirector (CPR) is application software that enables COM Port-based applications to communicate over a network to remote equipment.

The main purpose is to enable the control of COM port-based equipment over an IP-based network.

Com Port Redirector maps 'virtual COM' ports on a PC platform. It redirects application data destined to an attached device via the PC's local serial (COM) port: Rather than going out the local port, the data is transmitted across the IP-based wireless network using TCP/IP.

An ARF45-PRO attached to the wireless network receives the data and transfers it from its own serial port to the attached equipment.

Conversely, data sent from the networked equipment to the serial port of an ARF45-PRO is transmitted back to the application software on the PC via the wireless IP-based network.

Com Port Redirector receives the data and presents it to the control application as if it came from a COM port via a local serial connection.

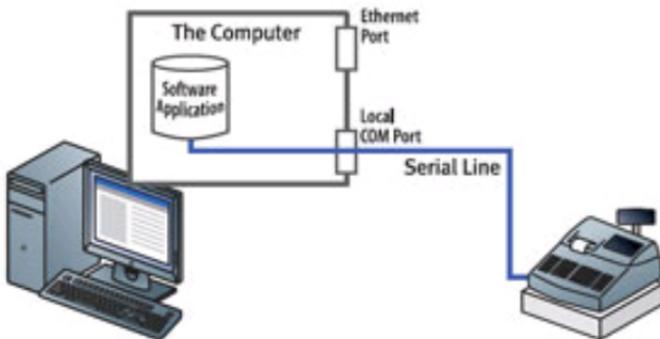


Figure 61

Firmware Upgrade

There exists several way for upgrading the firmware of the ARF45-PRO modem. In every case, the firmware is written into a RAM memory (as a zipped file) as it is being downloaded. Then once the download is completed the firmware is unzipped and written to flash memory=> so in case the download process does not run until completion (for instance: because of a failure on the radio link), there are no impact at all on the current firmware.

From remote connection using FTP protocol:

Simply do a **put** of the firmware **.romz** file.

The **.romz** file is a compressed file which contains both the ARF45-PRO WLAN firmware and the web manager application.

From the ARF45-PRO Web Manager's File system page:

1. Click System in the menu bar. The File system page opens.
2. In the Upload New Firmware section, click Browse. A pop-up page displays; locate the firmware file.
3. Click Upload to install the firmware on the ARF45-PRO. The device automatically reboots upon the installation of new firmware.

The screenshot displays the web interface for the A^{RF45-PRO} device. The left sidebar contains a navigation menu with the following items: Status, CLI, CPM, CPU Power Mgmt, Diagnostics, DNS, Email, Filesystem, FTP, Host, HTTP, IP Address Filter, Line, LPD, Network, ppp, Protocol Stack, Query Port, RSS, SNMP, SSH, SSL, Syslog, System (highlighted), Terminal, TFTP, Tunnel, WLAN Profiles, and XML. The main content area is titled "System" and contains several sections:

- System**: A header section.
- Reboot Device**: A section with a "Reboot" button.
- Restore Factory Defaults**: A section with a "Factory Defaults" button.
- Upload New Firmware**: A section with a text input field, a "Parcourir..." button, and an "Upload" button.
- Name**: A section with "Short Name:" and "Long Name:" labels, each followed by a text input field, and a "Submit" button.
- Current Configuration**: A table showing the current settings.

Firmware Version:	1.3.0.0R9
Short Name:	matchport_bg_pro
Long Name:	Lantronix MatchPort b/g Pro

The right-hand sidebar contains the following text:

When the device is rebooted, your browser should be refreshed and redirected to the main status page after 30 seconds. Note that the redirect will not work as expected if the IP Address of the device changes after reboot.

After setting the configuration back to the factory defaults, the device will automatically be rebooted.

Be careful not to power off or reset the device while uploading new firmware. Once the upload has completed and the new firmware has been verified and flashed, the device will automatically be rebooted.

Figure 62

Specifications

RF	
Frequency range :	2.412 – 2.484 GHz
Radiated RF power :	+ 15 dBm
Sensitivity :	- 91 dBm @ 1 Mbps
Range :	200 m in open field
Standards compliance :	EN 300-328 – EN301-489
WIFI	
Network standard :	802.11b; 802.11g
Security :	WEP 64, WEP 128, WPA/WPA2-Personal (PSK), WPA/WPA2-Enterprise (EAP-TLS, EAP-TTLS, PEAP, LEAP)
Radio data rate :	Up to 54 Mbps
Supported LAN Protocols :	TCP-IP, DHCP, BOOTP, ICMP, ARP, UDP, SMTP, TFTP, ICMP, SNMP, AutoIP
Modem interface	
Serial data rate :	From 300 bps to 250 Kbps
Serial ports :	TxD, RxD.
Flow control :	RTS, CTS
Set-up and configuration :	Through menus (by serial link or telnet or web manager)
Mode :	Transparent
General information	
Power supply :	8 to 36 Volts (integrated regulator)
Transmission consumption	740 mW
Listening consumption	250 mW
Operating temperature :	-30 to +70 °C
Size :	145x100x40 mm
Packaging :	IP65 box with integrated antenna

References

[ARF75321 : IP65 box version](#)