

WR7802-XT Series

Industrial Managed PoE Cellular Router

2 - Gigabit PoE Plus Ports

2 - Gigabit SFP Ports

User Guide

Beta Version

Copyright Notice

Control and RocketLinx are trademarks of Control Corporation.

Microsoft and Windows are trademarks of Microsoft Corporation.

FireFox is a trademark of Mozilla Foundation.

PuTTY is a copyright of Simon Tatham.

Other product names mentioned herein may be trademarks and/or registered trademarks of their respective owners.

First Edition, June 27, 2018

Copyright © 2017-2018. Control Corporation.

All Rights Reserved.

Control Corporation makes no representations or warranties with regard to the contents of this document or to the suitability of the Control product for any particular purpose. Specifications are subject to change without notice. Some software or features may not be available at the time of publication. Contact your reseller for current product information.

Beta Version

Table of Contents

Introduction	5
Basic Factory Default Settings	5
R&TTE Directive 1999/5/EC	6
Federal Communications Commission (FCC) Statement	6
FCC Radiation Exposure Statement	7
Safety Precautions	7
General Notification	7
Environment and Housing	8
Installation.....	8
Hardware Installation	9
Safety Precautions	9
General Notifications.....	9
Environment and Housing Notifications.....	10
Installation Notifications	10
Insert the SIM Card	11
Connect the Antenna	11
Mounting an SMA-Type External Antenna	12
Mounting an N-Type External Antenna	12
How to Select an External Antenna	12
Antenna Alignment	13
Lightning Arrestor.....	13
Connect the Power	13
Connect the Digital Output (Dry Relay Output)	14
Ground the WR7802-XT	14
Connect the Ethernet Ports	15
Connect SFP Transceivers (Ports 3-4)	16
Mount the WR7802-XT	16
LED Descriptions	17
Reset Button	17
Using PortVision DX	19
PortVision DX Overview	19
PortVision DX Requirements	20
Installing PortVision DX	20
Configuring the Network Settings	21
Checking the Firmware Version	23
Uploading the Latest Firmware	25
Uploading Firmware to Multiple WR7802-XT Switches	26
Adding a New Device in PortVision DX	27
Using Configuration Files	28
Saving a Configuration File	28
Loading a Configuration File	28
Using the LED Tracker	29
Customizing PortVision DX	30

Accessing RocketLinux Documentation from PortVision DX.....	30
How to Download Documentation	31
How to Open Previously Downloaded Documents	32
Configuration Using the Web User Interface.....	33
System Requirements.....	33
How to Log Into the WR7802-XT	33
Web User Interface.....	33
Secure Web User Interface.....	36
Diagnosing a Login Failure.....	39
Introduction to the Web Interface.....	39
Status Web Pages.....	41
Status Information Page	42
Status Network Flow Page	44
Status ARP Table Page	45
Status DHCP Client List Page	45
System Web Pages	46
System Basic Settings Page.....	46
System IP Settings Page	47
System DHCP Server Page	49
System Time Settings Page	50
System Relay Settings Page	51
System DDNS Settings Page	51
System Traffic Shaping Page.....	53
System Outbound Firewall Submenu	53
System Outbound Firewall Src (Source) IP Filtering Page.....	54
System Outbound Firewall Dest (Destination) IP Filtering Page	54
System Outbound Firewall Src (Source) Port Filtering Page	55
System Outbound Firewall Dest (Destination) Port Filtering Page.....	55
System Inbound Filtering Page.....	56
System NAT Settings Submenu	57
System NAT Settings Port Forwarding Page.....	57
System NAT Settings DMZ Page.....	58
System NAT Settings Advanced Page.....	59
Power Over Ethernet Pages.....	59
Power over Ethernet PoE Control Page	59
Power over Ethernet PoE Schedule Page.....	62
Power over Ethernet PoE Status Page.....	63
Switch Configuration Pages	64
Switch Configuration Port Status Page	64
Switch Configuration Port Control Page.....	65
Switch Configuration VLAN Configuration Page.....	66
System Configuration Rate Control Page	68
Switch Configuration Port Statistics Page.....	69
Traffic Prioritization Pages.....	70
Traffic Prioritization QoS Setting Page	70
Traffic Prioritization CoS-Queue Mapping Page.....	71
Traffic Prioritization DSCP-Queue Mapping Page.....	72
Multicast Filtering Pages	73
Multicast Filtering IGMP Snooping Page.....	74
Multicast Filtering IGMP Query Page.....	75

Network Redundancy Pages.....	76
Network Redundancy STP Configuration Page.....	77
Network Redundancy STP Port Configuration Page	79
Network Redundancy STP Information Page.....	80
Network Redundancy Redundant Ring Configuration Page.....	81
Network Redundancy Redundant Ring Information Page.....	82
Network Redundancy Redundant Gateway Page.....	83
Network Redundancy VRRP Page.....	85
Cellular Pages.....	87
Cellular Cellular Basic Settings Page	87
Cellular SIM Security Settings Page.....	89
Cellular Mobile Manager Settings Page	90
VPN Pages	91
VPN VPN Status Page	92
VPN OpenVPN Client Settings Page	93
VPN OpenVPN Server Settings Page	95
VPN VPN Port Forwarding Page	97
VPN VPN Certificate Page	98
VPN IPsec Settings Page	98
Security - Port Security Page	101
Management Pages.....	102
Management OPCUA Settings Page.....	103
Management Remote Settings Page.....	104
Management SMTP Settings Page.....	107
Management Login Settings Page.....	108
Management Firmware Upgrade Page	110
Management Configuration File Page	111
Management LLDP Configuration Page.....	112
Tools Pages.....	113
Tools System Log Page.....	113
Tools Ping Watchdog Page.....	114
Tools Ping Page.....	115
Save Page.....	115
Logout Page	115
Reboot Page	115
Configuration Using the Command Line Interface (CLI)	116
Overview	116
Accessing the CLI through an SSH Client.....	116
Accessing the CLI through PortVision DX	117
CLI Introduction.....	118
Command List.....	118
Using SHOW Commands	120
Using SET Commands	123
How to Set the Device Name.....	123
Set the Cellular Settings	124
Set the PoE Settings.....	124
Set the Switch Settings	125
Using DELETE Commands.....	126

Beta Version

Introduction

The RocketLinx WR7802-XT Series is an industrial grade Cellular LTE router with two PoE and two SFP fiber Ethernet ports. The WR7802-XT contains a Long Term Evolution (LTE) module with two SIM slots, which supports for up to 100M DL and 50M DL. In addition, the two Gigabit 802.3at PoE ports support up to 30W to PoE devices. The two 100/1000BASE-X SFP fiber ports provide great flexibility for field installations.

The WR7802-XT supports Cellular communications features, such as multiple ports to LTE NAT routings, dual SIM standby, SNMP, LLDP and Mobile Manager Server for remote monitoring. The OPC UA is designed for industrial machine to machine (M2M) communication, a popular protocol for industrial automation and M2M applications.

The WR7802-XT also provides different types of VPN Client technology and 1-1 OpenVPN Server for secure M2M connectivity. The WR7802-XT supports dual 54V (48-57VDC) input, Digital Output and a wide operating temperature of -40~75° with an IP30 enclosure.

Standard	Details
Cellular Standard	3GPP Release 9 Long Term Evolution (LTE), 2x2 DL-MIMO LTE category 3: Maximum 100 Mbps DL, 50 Mbps UL Backward compatible with UMTS/HSPA+/GSM/GPRS/EDGE
WR7802-XT-E Bands	LTE: 800/900/1800/2600/2100 MHz, FDD-Band (20,8,3,7, 1) UMTS/HSPA+: 900/1800/2100 MHz, FDD-Band (8,3,1) GSM/GPRS/EDGE: 900/1800 MHz
WR7802-XT-X Bands	LTE: 700/700/850/AWS (1700/2100)/1900 MHz; FDD-Band (13,17,5,4,2)Tri Band UMTS/HSPA+: 850/AWS (1700/2100)/1900 MHz; FDD-Band (5,4,2);Quad Band GSM/GRPS/EDGE: 850/900/1800/1900 MHz

Basic Factory Default Settings

The following table provides an overview of the default settings on the WR7802-XT.

Features	Factory Default Settings
Username	admin
Password	admin
Model Name	WR7802-XT
LAN IP Address (Default)	
IP Address	192.168.250.250
Subnet Mask	255.255.255.0
IP Gateway Address	192.168.250.1
DHCP Server Settings	
DHCP Server	Enable
DHCP IP Range Start	192.168.250.100

Features	Factory Default Settings
DHCP IP Range End	192.168.250.200
DHCP Subnet Mask	255.255.255.0
DHCP Gateway Address	192.168.250.1
Diagnostic CLI (Reserved for Engineering Diagnostics)	
Console Type	3-pin (Tx, Rx, GND)
Baud Rate	115200
Cellular (3G/LTE)	
SIM Socket	Default is SIM 1
Cellular Redundancy	Disabled by default. This feature is only available when two SIM cards are inserted.
Cellular Connect	Automatically after the SIM is inserted and the WR7802-XT is receiving power.
Others SIM Settings	Determined by your SIM card settings.
SIM Security	None

Detailed specifications for the RocketLinX WR7802-XT Series are available on the Control [web site](#).

R&TTE Directive 1999/5/EC

The product may be operated in all European Union countries. The R&TTE (1999/5/EC) Directive requires that the apparatus bears the CE mark as conformation of compliance with the R&TTE Directive.

A formal declaration of R&TTE for wireless products is available on our web site. Different products may conform to different standards of Health & Safety, EMC, Radio and other specific standards. You can download the formal document for the product from the Web site or request it from our Sales/Technical staff.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To avoid the possibility of exceeding radio frequency exposure limits, you shall keep a distance of at least 100cm between you and the antenna of the installed equipment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Safety Precautions

General Notification

- Only operate the device according to the technical specifications. You can find this information in the product data sheet, Quick Installation Guide, and the User Guide.
- Read the installation instructions before connecting the system to the power source.
- Only trained and qualified personnel should be allowed to install, replace, or service this device.
- This device is designed for operation with extra-low voltage (SELV). Connect the unit only to DC power source 54V (50-57VDC) that complies with the safety extra-low voltage (SELV) requirements in IEC/EN 60950 based safety standards. (Not supported on the 110V input model.)

Connect a power supply that corresponds to the type of your device. For power connection, make sure the following requirements are met:

- The DC power circuit of the product is usually not an isolated design circuit. In practice, it is suggested to use an isolated DC power design PSU for field installations. Besides the PSU selection, good digital/earth grounding is also important before powering on the system.
- The Power Supply conforms to the over-voltage category I or II.
- The output voltage of the AC/DC to DC Power Supply conforms to the range of the input voltage of the device.
- The connection cables used are permitted for the specified electronic voltage, current, wire diameter and temperature range. (Wire Diameter of AC voltage is at least 0.75mm, AWG18. For DC voltage, it is at least 1.0mm, AWG16.)
- Follow the power installation instructions in this guide, which indicates the input voltage, pin assignment, connection circuit and notices.
- The Power Supply must be properly installed, including grounding and other notices which are defined in the User Guide.
- Only power on the supply voltage to the device if the housing is closed, the terminal blocks are wired up correctly and the terminal blocks are connected.
- The equipment must be grounded. Ground the device before connecting the cables, antennas and power supply. The grounding of the equipment and DC Power Supply may be different in some applications, if this is case, you must ground them separately.
- Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Environment and Housing

- **Hot surface.** Avoid touching the device while it is operating.
- Only operate the device at the specified ambient temperature and humidity. The temperature of the surrounding air means a distance of up to 5cm from the device. When installing multiple devices within the cabinet, leaving space between the devices is mandatory for better heat dispersement.
- Install the device in the vertical position, with the antenna connections pointing upward.
- Install the device in a cabinet or in an operating site with limited access. The metal cabinet will filter the radio signals. Use an extended antenna cable and install the external antenna in a free space that helps provide a better radio signal.
- Only technicians authorized by the manufacturer are permitted to open the housing. Without the manufacturer permission, opening the housing means the product is not covered under warranty and not responsible for any unexpected risk.

Installation

If you are installing the wireless equipment in the field box or outdoor area, for your safety as well as others', please seek assistance from a professional installer who has received safety training on the hazards involved. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.

Please note the following things as well:

- Do not use a metal ladder;
- Do not work on a wet or windy day;
- Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
- If you are installing the equipment in an indoor office or factory, make sure that the device and power source are properly grounded. A professional wireless IT Engineer can provide advice for the AP location, channel and field plan to get better performance and coverage.
- Connect the equipment after verifying that the cabinet meets the appropriate IP degree of protection.
- Read the radio output power, receiver sensitivity, antenna gain specifications before installation. The shipped product and antenna conforms to the R&TTE Directive and is allowed for use in all European countries. You can read the related technical specifications from the product data sheet or User Guide.
- When installing external antennas, the Radio Output power and antenna gain value must meet the regulations of the country.
- When the system is operational with a high gain antenna, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.
- When the system is operational with a high gain antenna for short distance transmission, adjust the radio output lower. Strong output power with a high gain antenna is not a proper installation method for short distance transmission.
- You are responsible for undertaking suitable lightning protection.
- Install over voltage protector devices on every outdoor Ethernet cable.
- Protect each antenna installed outside with lightening protection devices, for example, a lightening arrester.

Note that Field EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

Hardware Installation

There are two models available that support different areas of the world:

- WR7802-XT-E, which supports GSM bands
- WR7802-XT-X, which supports US bands

Note: Both models are simply referred to as the WR7802-XT unless there is information for a specific model.

You can use the following subsections to install the RocketLinx WR7802-XT Series.

- [Safety Precautions](#)
- [Insert the SIM Card](#) on Page 11
- [Connect the Antenna](#) on Page 11
- [Connect the Power](#) on Page 13
- [Connect the Digital Output \(Dry Relay Output\)](#) on Page 14
- [Ground the WR7802-XT](#) on Page 14
- [Connect the Ethernet Ports](#) on Page 15
- [Connect SFP Transceivers \(Ports 3-4\)](#) on Page 16
- [Mount the WR7802-XT](#) on Page 16
- [LED Descriptions](#) on Page 17
- [Reset Button](#) on Page 17

Safety Precautions

Please read the following safety precautions before installing the WR7802-XT.

- [General Notifications](#)
- [Environment and Housing Notifications](#) on Page 10
- [Installation Notifications](#) on Page 10

General Notifications

Adhere to the these general notifications:

- Only operate the WR7802-XT according to the technical specifications. You can find this information in the product data sheet on the [web site](#), Quick Installation Guide, and this User Guide.
- Read the installation instructions before connecting the WR7802-XT to the power source.
- Only trained and qualified personnel should be allowed to install, replace, or service the WR7802-XT.
- The WR7802-XT is designed for operation with extra-low voltage (SELV). Connect the unit only to DC power source 54V (48-57VDC) that complies with the safety extra-low voltage (SELV) requirements in IEC/EN 60950 based safety standards. (Not supported on the 110V input model.)

Connect an appropriate power supply that meets the WR7802-XT power specifications. Before connecting and applying power to the WR7802-XT, make sure the following requirements are met:

- The DC power circuit of the WR7802-XT is not an isolated design circuit. In practice, we recommend using an isolated DC power design PSU for field installations. Do not power on the WR7802-XT without an appropriate PSU and following proper grounding methods.
- The power supply conforms to the Over-Voltage Category I or II.

Hardware Installation

- The output voltage of the AC/DC to DC power supply conforms to the input voltage range of the WR7802-XT.
- Cables (wire) must be appropriate for the specified electronic voltage, current, wire diameter and temperature range. Remember, the minimum wire diameter of AC voltage is at least 0.75mm(AWG18). The minimum for DC voltage is at least 1.0mm (AWG16)).
- Follow the power installation instructions in this guide, which indicates the input voltage, pin assignment, connection circuit and notices.
- Only power on the supply voltage to the WR7802-XT if the WR7802-XT housing is closed, the terminal blocks are wired correctly and the terminal blocks are connected.
- The WR7802-XT **MUST** be grounded. Ground the WR7802-XT before connecting the cables, antennas and power supply. The grounding WR7802-XT and DC power supply may be different in some applications, if this is case, you must ground them separately.
- Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Environment and Housing Notifications

- **Hot surface.** Avoid touching the WR7802-XT while it is operating.
- Only operate the WR7802-XT at the specified ambient temperature and humidity. The temperature of the surrounding air means a distance of up to 5cm from the WR7802-XT. When installing multiple devices within the cabinet, leaving space between the devices is mandatory for better heat dispersment.
- Install the WR7802-XT in the vertical position, with the antenna connections pointing upward.
- Install the WR7802-XT in a cabinet or at an operating site with limited access. A metal cabinet will filter the radio signals. Use an extended antenna cable and install the external antenna in a free space that helps provide a better radio signal.
- Only technicians authorized by the manufacturer are permitted to open the WR7802-XT housing. Without the manufacturer's permission, opening the housing means the product is not covered under warranty and not responsible for any unexpected risk.

Installation Notifications

If you are installing the WR7802-XT in a field box or outdoor area, for your safety as well as others', seek assistance from a professional installer who has received safety training on the hazards involved. Keep safety as well as performance in mind when selecting your installation site, especially where there are electric power and phone lines.

Please note the following things as well:

- Do not use a metal ladder;
- Do not work on a wet or windy day;
- Wear shoes with rubber soles and heels, rubber gloves, long sleeved shirt or jacket.
- If you are installing the WR7802-XT in an indoor office or factory, make sure that the WR7802-XT and power source are properly grounded. A professional wireless IT Engineer can provide advice on the AP location, channel, and field plan to get the best performance and coverage.
- Connect the WR7802-XT after verifying that the cabinet meets the appropriate IP degree of protection.
- Read the radio output power, receiver sensitivity, antenna gain specifications before installation. The shipped product and antenna conforms to the R&TTE Directive and is allowed for use in all European countries. You can read the related technical specifications from the product data sheet found on the web site or User Guide.
- When installing external antennas, the radio output power and antenna gain value must meet the regulations of the country.
- When the system is operational with a high gain antenna, avoid standing directly in front of it. Strong RF fields are present when the transmitter is on.

- When the system is operational with a high gain antenna for short distance transmission, adjust the radio output lower. Strong output power with a high gain antenna is not a proper installation method for short distance transmission.
- You are responsible for undertaking suitable lightning protection.
- Install over-voltage protector devices on every outdoor Ethernet cable.
- Protect each antenna installed outside with lightning protection devices, for example, a lightning arrester.

Note: FIELD EMD (LIGHTNING) DAMAGE IS NOT COVERED UNDER WARRANTY.

Insert the SIM Card

The WR7802-XT provides dual external SIM (Subscriber Identity Module) sockets to store the Cellular Nano SIM card. The WR7802-XT only supports the Nano SIM card, which fits into the Nano SIM carrier tray that slides into the SIM slots. The illustration shows the types of SIM cards available.

If you want to use both SIM sockets, you should insert both SIM cards into the WR7802-XT before applying power. After applying power, you can enable the Cellular Redundant option and configure SIM 2 as startup or backup SIM socket using the *Cellular Basic Settings* web page.

Note: The Cellular Redundant option is only available if you insert two SIM cards into the sockets. If you only insert one, DO NOT enable Cellular Redundant.

Use the following procedure to insert the SIM card.

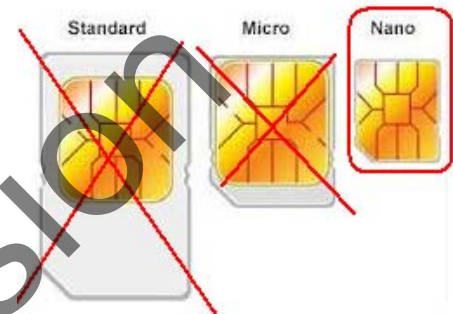
Note: The WR7802-XT cannot be powered on when inserting the SIM cards. Later when you power on the WR7802-XT it takes approximately 1 minute to start up and searches for SIM card in SIM slot 1.

1. Remove the two screws that secure the front plate of dual SIM socket.
2. Remove the SIM carrier tray.

Note: The SIM 1 is the default SIM socket.

3. Place SIM card into the carrier, aligning the angled corner with the angled corner of the tray.
4. Gently insert the SIM card into the SIM slot.

After completing the installation, if the Cellular connection is not connected, go to the *Status | Information* web page to check the Cellular status and settings.



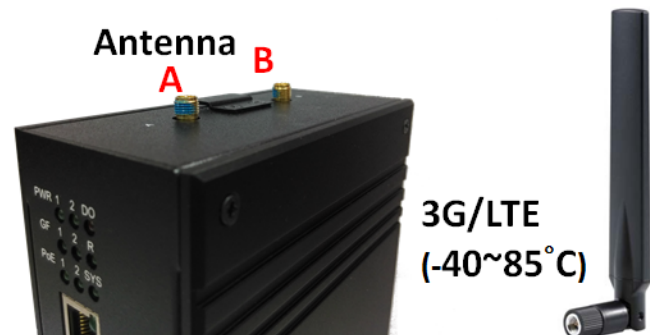
Connect the Antenna

The WR7802-XT supports up to two antenna sockets and two LTE antennas are shipped with the product.

- Antenna A is the LTE-Aux antenna
- Antenna B is the LTE-Main antenna

Note: Leave the dust cap on unconnected antennas.

The antennas shipped with the product are a wide-temperature design; however, they are not water-proof. If you want to install it in outdoor area, use water-proof outdoor antennas.



The antennas meet these specifications.

Frequency Range	824 - 894MHz	900 - 960MHz	1710 - 1880MHz	1910 - 2170MHz
Peak Gain	1.5dBi	1.0dBi	2.0dBi	4.0dBi
Average Gain	-2.5dBi	-3.5dBi	-2.5dBi	-2.0dBi
Voltage Standing Wave Ratio (VSWR)	4.0: 1 maximum			
Polarization	Linear, vertical			
Impedance	50 Ω			
Connector	RP SMA plug (Reverse-Polarity Sub Miniature version A)			

The antennas are easy to connect, simply align the antenna on the connector and turn the antenna clockwise to lock it into place.

Note: To remove the antenna, turn it counter-clockwise.

If you are installing the WR7802-XT in a high vibration environment, you may want to connect it with an extended radio cable antenna.

If installing the WR7802-XT in a weatherproof cabinet to protect it from water, rain or other reasons, we recommend mounting its antennas outside the cabinet.

Mounting an SMA-Type External Antenna

If the default antenna is not suitable for your environment, you can purchase an external antenna for your environment. When selecting an SMA-type external antenna, you must choose an antenna that supports the correct band in your country for radio transmission.

Mounting an N-Type External Antenna

If the default antenna is not suitable for your environment, for example an outdoor area, you can purchase an external water-proof N-Type antenna. When selecting an N-type external antenna, you must choose the correct frequency band of the antenna and it must conform to the radio band you connected.

The WR7802-XT requires an N-Type external antenna, which is an SMA to N-Type connector or RF cable. Remember that the WR7802-XT antenna connector is an RP-SMA female that connects to RP-SMA male cable.

How to Select an External Antenna

Normally, the antenna that is shipped with the WR7802-XT works well in most indoor applications. If you need to install the WR7802-XT in a low signal environment and want to install an external antenna, consult with your system integrator to choose a suitable external antenna. Remember you will need an SMA-type or N-Type connector for your application. Different antennas support different bands, polarization and different ranges of coverage.

Keep the following in mind when selecting an external antenna:

- **Gain:** Affects the system performance.
- **Direction:** Typical types include: Omni-Directional or Directional antenna. Check the antenna zone in its specification.

- Connector: Make sure you choose the correct connection type. is, for example N-Type, SMA Male/Female.

Antenna Alignment

Use the following procedure to align your antenna.

1. Follow the antenna installation guide to install the antenna properly.
2. Connect your laptop to the Ethernet port and if necessary, install a Cellular Speed Test utility on your laptop or connect to the carrier provider's web page, as some carriers provide an utility on their web site.
3. Adjust the antenna location, run the Speed Test utility to check the result after changing the location or direction.

Lightning Arrestor

If you install an external antenna in outside area, we recommend installing a lightning arrestor to avoid an environment attack through the antenna. A lightning arrestor protects the insulation and conductors of the system from the damaging effects of lightning.

Note: Before installing an external antenna, make sure that the antenna can support a 3G connection. Most of the high gain external antennas are installed in higher place than the AP, you should get a low power loss antenna cable in advance. If installing the AP in a metal field box, connect an extended antenna cable to outside the box to avoid the Radio lost.

Connect the Power

The following table provides WR7802-XT electrical specifications.

Electrical Specifications		Value
Power Input Voltage DC1/DC2	IEEE 802.3af	54V (48-57VDC)
	IEEE 802.3at	54V (50-57VDC)
Maximum PoE Power/Port	IEEE 802.3af	15.4W
	IEEE 802.3at	31W
Power Budget	PWR1/PWR2	66W @ 54V
Power Consumption	Without PD load (maximum)	11W
	PoE with PD load (maximum)	76W

The WR7802-XT supports redundant power supplies if you connect both PWR1 and PWR2. The WR7802-XT accepts a positive power source. If both power inputs are connected, the WR7802-XT is powered from the highest connected voltage. The WR7802-XT does not support reverse polarity protection.

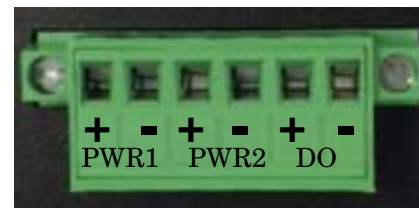
The DC power circuit of the WR7802-XT is not an isolated design circuit. In practice, we recommend using an isolated DC power design PSU for field installations. Do not power on the WR7802-XT without an appropriate PSU and following proper grounding methods.

Note: Power should be disconnected from the power supply before connecting it to the WR7802-XT. Your screw driver blade can inadvertently short the terminal connections to the grounded enclosure.

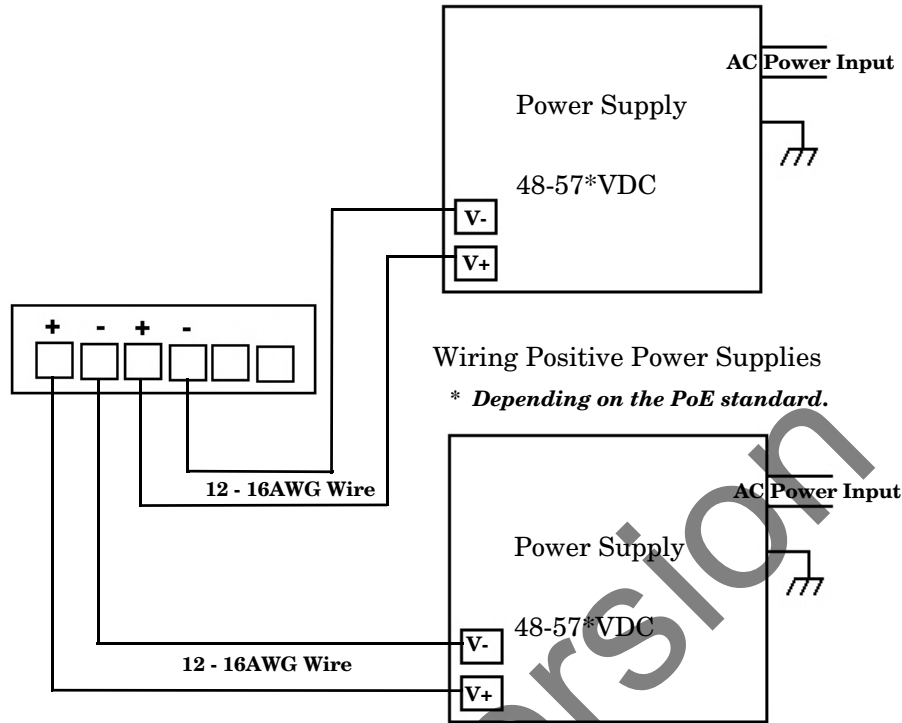
Use the following procedure to connect the power to the WR7802-XT.

1. Connect the DC power inputs by inserting the positive and negative wires (12-16AWG) into the PWR+ and PWR- contacts using the following wiring drawing.

Note: Tighten the wire-clamp screws to prevent the wires from coming loose.



- If you are not going to connect digital output, make sure that you tighten the power connector screws into the housing so that the power connector is secure.



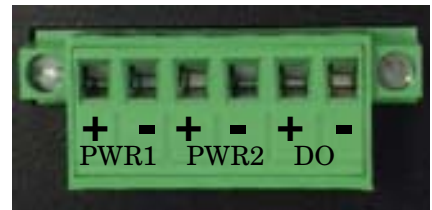
Connect the Digital Output (Dry Relay Output)

The WR7802-XT provides one digital output (dry relay output) on the terminal block connector on the bottom of the WR7802-XT.

You can configure link failure using one of the WR7802-XT user interfaces.

Digital output relay contacts are energized (open) for normal operation and close for fault conditions. The digital output relay contacts support up to 1A at 24VDC. Do not apply voltage and current higher than the specifications.

- Insert the positive and negative wires (12-24 AWG) into V+ and V-.
- Tighten the wire-clamp screws to prevent the wires from coming loose.
- Make sure that you tighten the power connector screws into the housing so that the power connector is secure.



Ground the WR7802-XT

Connect a ground wire between the chassis and earth ground using 12-24AWG wire to ensure that the WR7802-XT is not damaged by noise or electrical shock.

- Loosen the ground screw on the bottom of the WR7802-XT.
- Insert the ground wire.
- Tighten the ground screw after the ground wire is connected.



Note: The WR7802-XT **MUST** be properly grounded. Connect the Ethernet cable, Antenna, extended antenna cable and Ground before powering on the system.

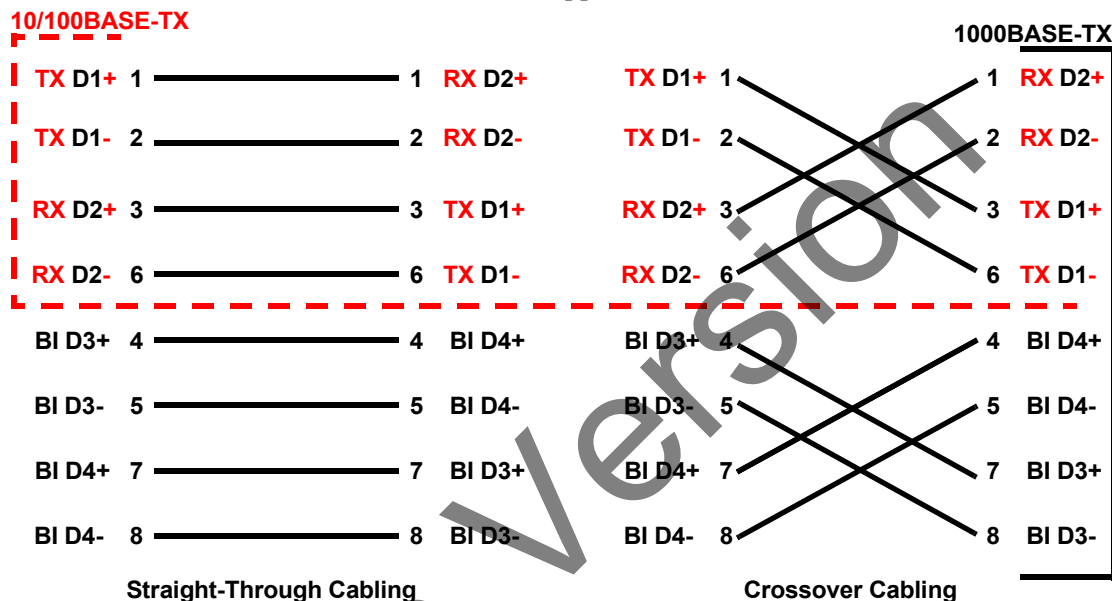
Connect the Ethernet Ports

There are four Gigabit Ethernet ports, two standard RJ45, IEEE802.3 at 30W High Power PoE ports and two SFP Fiber ports for LAN.

You can use the following information to connect Ethernet cables between the WR7802-XT Ethernet ports and the network nodes.

See [Connect SFP Transceivers \(Ports 3-4\)](#) on Page 16 for information about SFP installation.

The RJ45 Ethernet ports automatically detect the signal from the connected devices to negotiate the link speed and duplex mode (half- or full-duplex). Auto MDI/MDIX allows you to connect another switch, hub, or workstation without changing straight-through or crossover cables. Crossover cables cross-connect the transmit lines at each end to the received lines at the opposite end.



Connect one side of an Ethernet cable into any switch port and connect the other side to your attached device. The **LNK/ACT** LED is lit when the cable is correctly connected. Always make sure that the cables between the switches and attached devices (for example, switch, hub, or workstation) are less than 100 meters (328 feet) and meet these requirements.

- **10BASE-T:** Category 3 or higher cable
- **100BASE-TX:** Category 5 or higher cable
- **1000BASE-TX:** Category 5 or higher cable

Note: Control recommends using CAT 5E / CAT 6 cables in harsh environments. STP (Shielded Twisted Pair) cable is preferred. If the WR7802-XT is installed in a harsh environment, part of the EMS protection is based on STP cable.

Connect SFP Transceivers (Ports 3-4)

The WR7802-XT provides two SFP ports that accept standard mini GBIC DDM SFP transceivers that support 100BASE-FX/1000BASE-X.

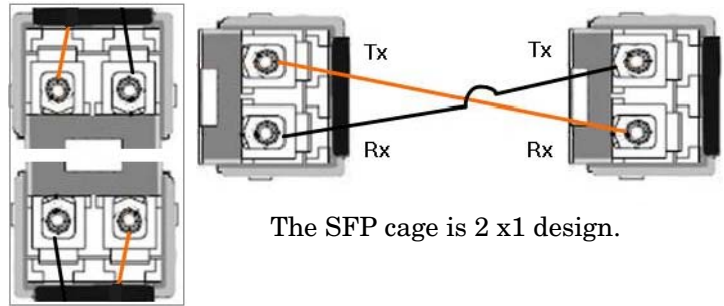
To ensure system reliability, Control recommends using [Control certified SFP Transceivers](#).

1. Plug the SFP transceiver into the SFP fiber transceiver.
2. Connect the transmit channel to the receive channel at each end.
3. Check the direction/angle of the fiber transceiver and the fiber cable.

Note: This is a Class 1 Laser / LED product. Do not stare at the Laser / LED Beam.

The default speed setting is 1000Mbps. If you want to use a 100M SFP Fiber transceiver, you MUST change the speed to 100Mbps in management interface first.

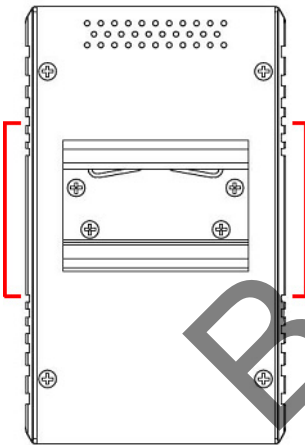
Multi-Mode cables should not exceed 2KM and Single-Mode cables should not exceed 30km.



The SFP cage is 2 x1 design.

Mount the WR7802-XT

You can use the following procedure to mount the WR7802-XT on a DIN rail or on the wall. The DIN rail clip is already attached to the WR7802-XT. If the DIN rail clip is not screwed onto the WR7802-XT, follow the instructions and the figure below to attach DIN rail clip to the WR7802-XT.



DIN Rail Mounting

1. Insert the upper end of DIN rail clip into the back of DIN rail track from its upper side.
2. Lightly push the bottom of DIN rail clip into the track.
3. Verify that the DIN rail clip is tightly attached on the track.
4. To remove the WR7802-XT from the track, reverse the steps above.

LED Descriptions

This subsection provides information about the WR7802-XT LEDs.

LED	Indication	Blinking	On	Off
PWR	PWR1/PWR2 Status	N/A	Valid power applied	No power
GF	Fiber Port GF1/GF2 Status	GF is activating	GF is linked up	No link
PoE	PoE Output Status	N/A	Delivering PoE power	No PD is attached
ETH	Eth1/Eth2 Status	Port is activating	Port is linked up	Port not linked up
DO	Digital Output Status	N/A	The Relay is ON. It may indicate the alarm of specific events.	The Relay is OFF
R	Boot Status	Booting	LTE connected	Boot finished
SYS	System Status	N/A	Power on	Power off

Reset Button

The WR7802-XT has a reset button that you can use to reboot the WR7802-XT or reset the configuration to the factory default.

Reset Button	Description
Depress 0-3 Seconds	This reboots the WR7802-XT without changing the configuration.
Depress > 7 Seconds	This loads the factory default configuration values into the WR7802-XT including the IP address.

The **Reset** button is located on the front panel of the WR7802-XT below the second SFP port.

Beta Version

Using PortVision DX

There are several ways to configure network information. Control Technical Support recommends connecting the WR7802-XT to a PC or laptop running [Windows](#) and installing *PortVision DX* for initial configuration.

This section shows how to use PortVision DX for initial network configuration and discusses how to:

- Install PortVision DX ([Page 20](#))
- Configure the network address ([Page 21](#))
- Check the firmware and bootloader version on the WR7802-XT to verify that the latest versions are loaded ([Page 23](#)) before configuration
- Download the latest version firmware and bootloader and upload it to the WR7802-XT ([Page 25](#))
- Perform other PortVision DX tasks, such as:
 - Uploading firmware to multiple WR7802-XT switches ([Page 26](#))
 - Adding a new RocketLinx (managed or unmanaged) or a third party device to PortVision DX to maintain device information on your network ([Page 27](#))
 - Using configuration files for use in configuring multiple installations with the same features ([Page 28](#))
 - Using the LED Tracker ([Page 29](#))
- Organize how PortVision DX displays your Control Ethernet attached products ([Page 28](#))
- Access the latest documentation for your Control Ethernet attached product

PortVision DX Overview

PortVision DX automatically detects Control Ethernet attached products physically attached to the local network segment so that you can configure the network address, upload firmware, and manage the following products:

- RocketLinx (managed) switches
- DeviceMaster family
 - DeviceMaster DM series
 - DeviceMaster PRO
 - DeviceMaster LT
 - DeviceMaster RTS
 - DeviceMaster Serial Hub
- DeviceMaster Industrial Gateway family
 - DeviceMaster EIP
 - DeviceMaster MOD
 - DeviceMaster PNIO
 - DeviceMaster UP
- IO-Link Master family

In addition to identifying Control Ethernet attached products, you can use PortVision DX to display any third-party switch and hardware that may be connected directly to those devices. All non-Control products and unmanaged RocketLinx switches are treated as non-intelligent devices and have limited feature support. For example, you cannot configure or update firmware on a third-party switch.

PortVision DX Requirements

Use PortVision DX to identify, configure, update, and manage the WR7802-XT on Windows 7 through Windows 10 operating systems (at the time of publication).

PortVision DX requires that you connect the Comtrol Ethernet attached product to the same network segment as the Windows host system if you want to be able to scan and locate it automatically during the configuration process.

Installing PortVision DX

During initial configuration, PortVision DX automatically detects and identifies WR7802-XT switches, if they are in the same network segment.

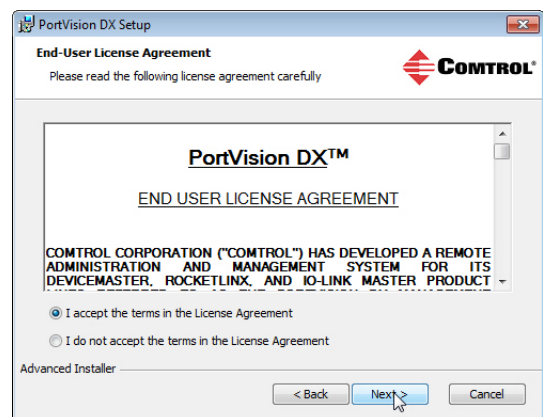
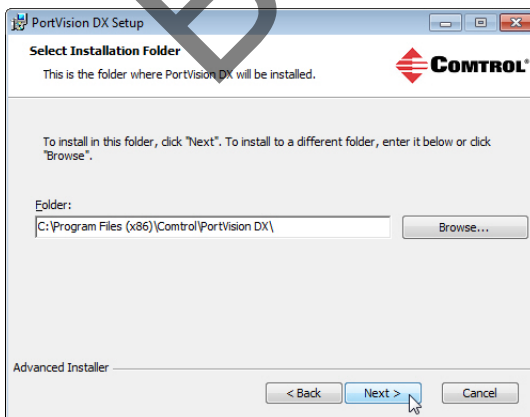
You can download the latest version of PortVision DX from: http://downloads.comtrol.com/rocketlinx/portvision_dx.

1. Execute the **PortVision_DX[version].msi** file.

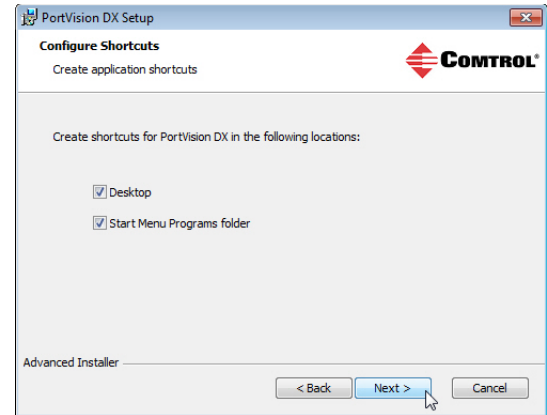
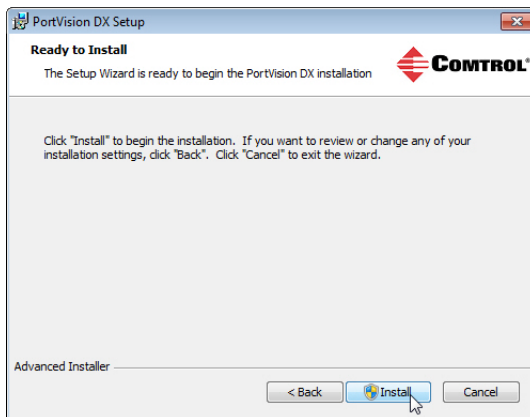


Note: Depending on your operating system, you may need to respond to a Security Warning to permit access.

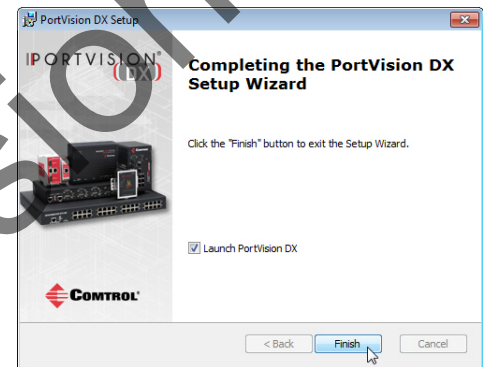
2. Click **Next** on the *Welcome* screen.
3. Click **I accept the terms in the License Agreement** and **Next**.
4. Click **Next** or optionally, browse to a different location and then click **Next**.



5. Click **Next** to configure the shortcuts.
6. Click **Install**.



7. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to install software on this computer?* query.
8. Click **Launch PortVision DX** and **Finish** in the last installation screen.
9. Depending on the operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.
10. Go the next subsection to use PortVision DX to program the network information.



Configuring the Network Settings

The WR7802-XT has the following default values for the LAN IP address when shipped from the factory:

- IP address: 192.168.250.250
- Subnet mask: 255.255.255.0
- Gateway address: 192.168.250.1

Use the following procedure to change the default network settings on the WR7802-XT for your network.

1. If necessary, start PortVision DX using the **PortVision DX** desktop shortcut or from the **Start** button, click **Control | PortVision DX**.

Note: Depending on your operating system, you may need to click **Yes** to the *Do you want to allow the following program to make changes to this computer?* query.

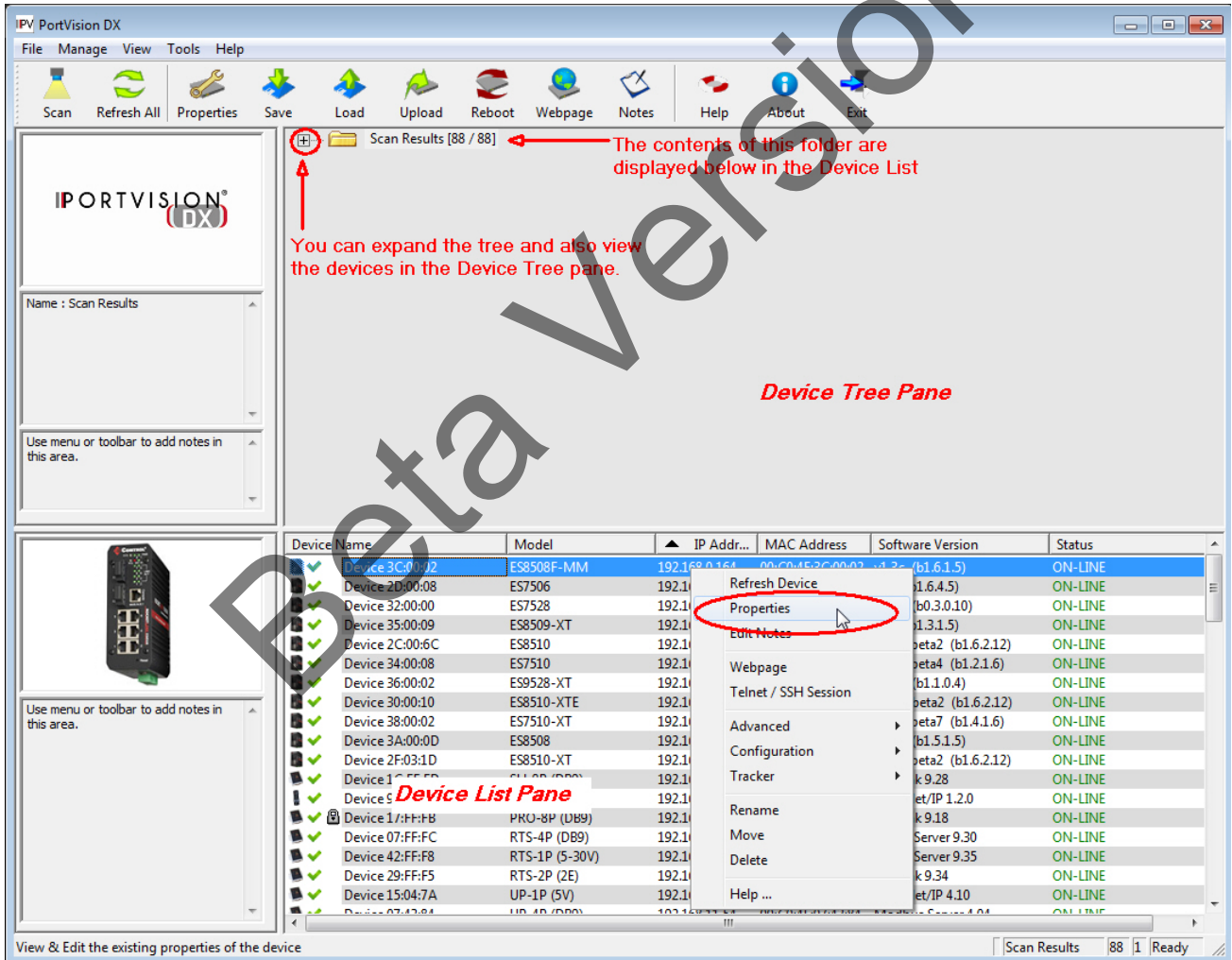
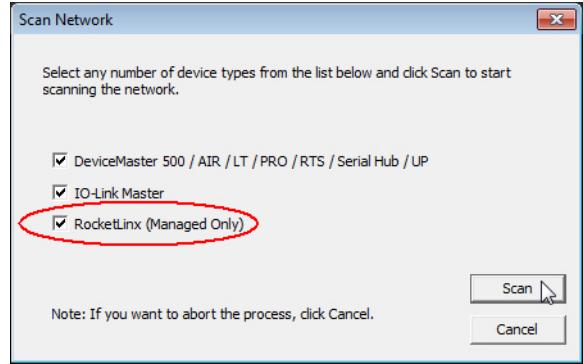
2. Click the **Scan** button in the *Toolbar*.

- Select the Control Ethernet attached products that you want to locate and then click **Scan**.

Note: *If the Control Ethernet attached product is not on the local segment and it has been programmed with an IP address, it will be necessary to manually add the Control Ethernet attached product to PortVision DX.*

- Highlight the WR7802-XT for which you want to program network information and open the **Properties** screen using one of these methods.

- Double-click the WR7802-XT in the *Device Tree* or *Device List* pane.
- Highlight the WR7802-XT in the *Device Tree* or *Device List* pane and click the **Properties** button.
- Right-click the WR7802-XT in the *Device Tree* or *Device List* pane and click **Properties** in the popup menu
- Highlight the WR7802-XT, click the **Manage** menu and then **Properties**.



- Optionally, rename the WR7802-XT in the **Device Name** field for a PortVision DX friendly name. The default name displays as *Device* and the last three sets of hex numbers from the MAC address.

Note: *The MAC address and Device Status fields are automatically populated and you cannot change these values.*

6. Optionally, enter the serial number, which is on a label on the WR7802-XT.
7. Select **DHCP IP** or **Static IP** for the *IP Mode*.
 - If you select **DHCP IP**, go to [Step 8](#).
 - If you select **Static IP**:
 - Enter a unique **IP address** as required for your site.
 - Enter a valid **Subnet Mask** value for your network.
 - Enter a valid **Default Gateway** value for your network.
8. Optionally, select the **Network Topology** type, which is an informational field.
9. Click **Apply Changes** to update the network information on the WR7802-XT.

Note: *If you are deploying multiple WR7802-XT switches that share common values, you can save the configuration file and load that configuration onto other WR7802-XT switches. See [Using Configuration Files](#) on Page 28 for more information.*
10. Click **Close** to exit the *Properties* window.
11. You should verify that you have the latest firmware loaded on the WR7802-XT because a newer version typically includes feature enhancements and bug fixes. Refer to [Checking the Firmware Version](#) on Page 23 and if necessary, [Uploading the Latest Firmware](#) on Page 25.
12. If you have the latest firmware, you can begin feature configuration, see one of these sections:
 - [Configuration Using the Web User Interface](#) on Page 33
 - [Configuration Using the Command Line Interface \(CLI\)](#) on Page 116
 - Right-click the WR7802-XT in the *Device List* pane and click **Webpage** in the popup menu.

Note: *The default User Name and Password are both **admin**.*

Checking the Firmware Version

Checking your web interface version is easy in PortVision DX.

Control recommends loading the latest firmware so that you have all of the latest feature enhancements and bug fixes.

1. If the WR7802-XT is not displayed in PortVision DX, click the **Scan** button.
2. Select the Control Ethernet attached product type and click the **Scan** button.

- Locate the WR7802-XT in the *Device List* pane. Under *Software Version*: The first number reflects the firmware version.

The screenshot shows the PortVision DX application window. The interface includes a menu bar (File, Manage, View, Tools, Help), a toolbar with icons for Scan, Refresh All, Properties, Save, Load, Upload, Reboot, Webpage, Notes, Help, About, and Exit. On the left, there is a sidebar with the IPORVISION DX logo and a text area for notes. The main area is divided into a tree view on the left and a table on the right. The tree view shows a hierarchy of devices under 'PM_Test [29 / 30]', including 'IO-Link Masters [9 / 10]' and 'Testing_01 [0 / 12]'. The table below lists various devices with columns for Device Name, Model, IP Address, MAC Address, Software Version, and Status. One row, 'WR7802-XT_69:00:01', has its 'Software Version' cell highlighted in yellow, containing the text '0.9a6t3'. A red text overlay on the screen reads: 'You can customize and organize your view using PortVision DX. In addition, you can save and reload different sessions.' Another yellow text box points to the highlighted software version, stating: 'This is the firmware version on the WR7802-XT-X'. A large 'Beta' watermark is visible across the center of the image.

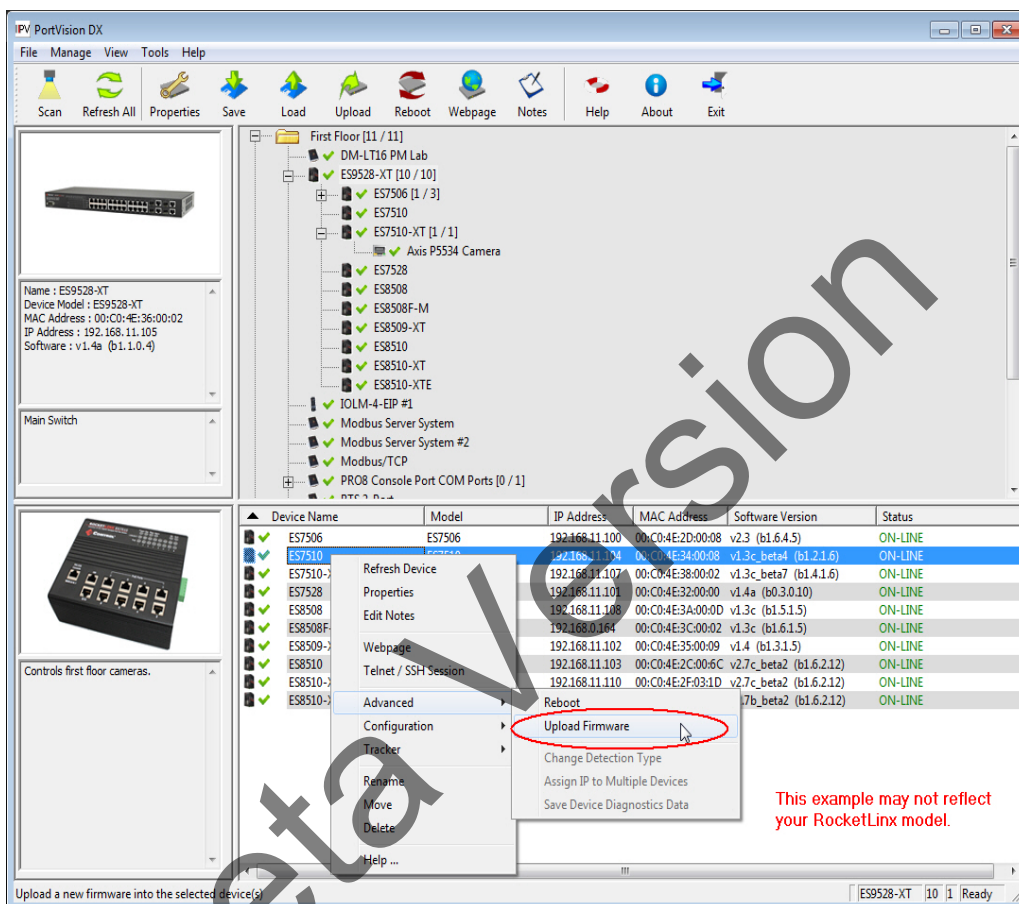
Device Name	Model	IP Address	MAC Address	Software Version	Status
b2	ES8105-GigE				ON-LINE
WR7802-XT_69:00:01	WR7802-XT-X	10.0.0.144	00:C0:4E:69:00:01	0.9a6t3	ON-LINE
RTS2P2E Test	RTS-2P (2E)	10.0.0.52	00:C0:4E:29:FF:F5	SocketServer 11.14	ON-LINE
MP1204-XT	OTHER_SWITCH	10.0.0.203			ON-LINE
Isolated NIC	OTHER_HW	10.0.0.1			ON-LINE
ES9528-XT_v2 #3	ES9528-XT V2	10.0.0.113	00:C0:4E:58:00:00	v2.1 (b2.0.0.6)	ON-LINE
ES9528-XT_v2 #2	ES9528-XT V2	10.0.0.112	00:C0:4E:58:00:01	v2.1 (b2.0.0.6)	ON-LINE
ES8814-XT	ES8814-XT	0.0.0.0	00:C0:4E:60:00:00	v1.0_b10 (b2.1.1.0)	ON-LINE
ES8520-XT	ES8520-XT	10.0.0.116	00:C0:4E:5F:00:68	v1.1a (b2.0.1.1)	ON-LINE
ES8510-XTE_BackBone	ES8510-XTE	192.168.11.106	00:C0:4E:30:00:10	v3.1a_b1 (b1.6.2.12)	ON-LINE
ES8510	ES8510	192.168.11.103	00:C0:4E:2C:00:6C	v3.1 (b1.6.2.12)	ON-LINE
ES8509-XT	ES8509-XT	10.0.0.102	00:C0:4E:35:00:09	v2.1a (b1.3.1.7)	ON-LINE
ES8508F-MM	ES8508F-MM	10.0.0.115	00:C0:4E:3C:00:02	v2.0 (b1.6.1.7)	ON-LINE
ES8508	ES8508	10.0.0.108	00:C0:4E:3A:00:0D	v2.0 (b1.5.1.7)	ON-LINE
ES7810-XT_V1	ES7810-XT	10.0.0.118	00:C0:4E:5E:00:03	v1.0_b10 (b2.1.2.0)	ON-LINE
ES7528	ES7528	10.0.0.101	00:C0:4E:32:00:00	v2.1_b3 (b0.3.0.10)	ON-LINE
ES7510-XT#2	ES7510-XT	10.0.0.111	00:C0:4E:38:00:67	v2.1a_b1 (b1.4.1.8)	OFF-LINE
ES7510-XT#1	ES7510-XT	10.0.0.107	00:C0:4E:38:00:02	v2.1a (b1.4.1.8)	ON-LINE
ES7510	ES7510	10.0.0.104	00:C0:4E:34:00:08	v2.0_b6 (b1.2.1.8)	ON-LINE
Device 36:00:02	ES9528-XT	10.0.0.105	00:C0:4E:36:00:02	v2.0 (b1.1.0.4)	ON-LINE
Device 32:03:5F	ES7528	10.0.0.119	00:C0:4E:32:03:5F	v1.0 (b1.0.0.0)	ON-LINE

- Check the [Control download](#) site for the latest firmware. Simply, click your product type and click the **Software** link and check the latest version against the version on the WR7802-XT. Use the next subsection for procedures to upload the firmware (web interface).

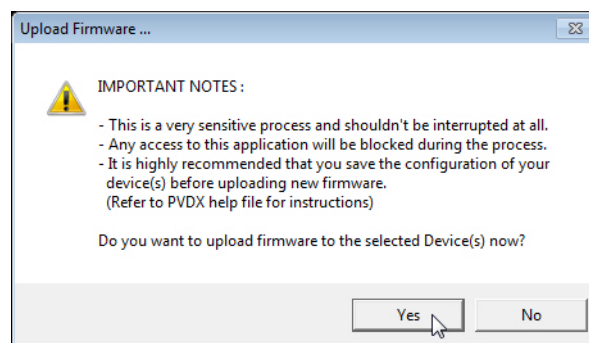
Uploading the Latest Firmware

You can use the following procedure to upload the latest firmware.

1. If you have not done so, download the latest firmware using the previous subsection.
2. Right-click the WR7802-XT in the *Device List* pane that you want to update, click **Advanced | Upload firmware**.



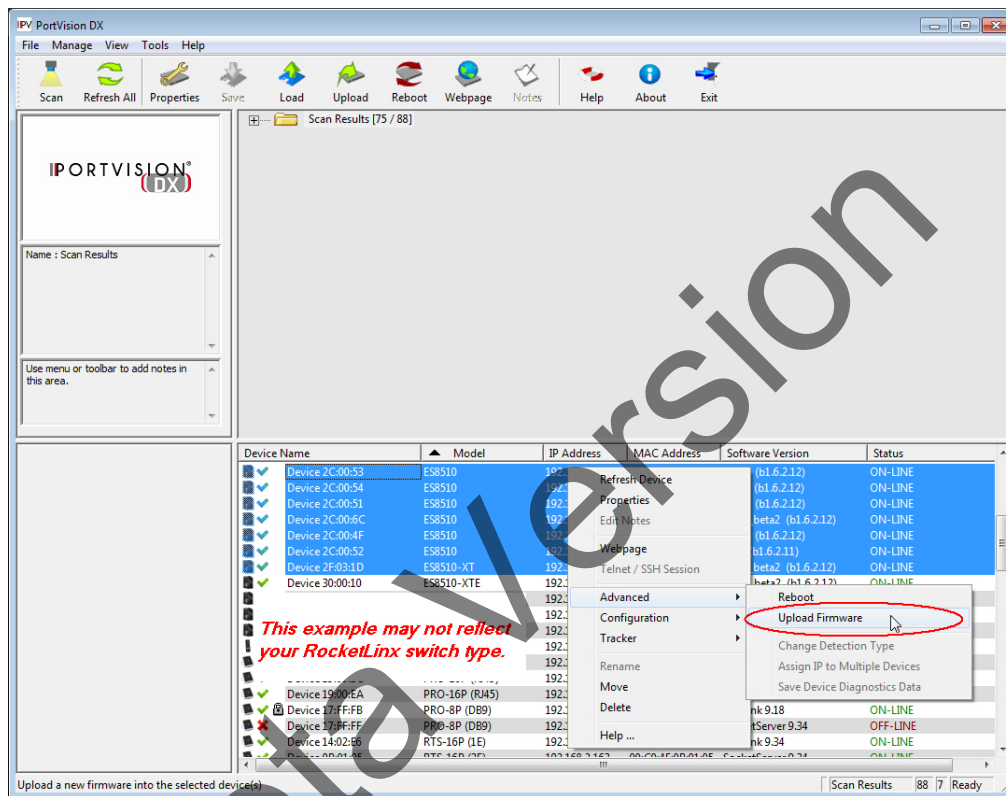
3. Navigate to the location of the firmware files, select the appropriate file, and then click **Open**.
4. Click **Yes** to the *Upload Firmware* message.
5. Click **Ok** to the message notifying you that you should wait to use the WR7802-XT when the status returns to ON-LINE.
6. Right-click the WR7802-XT in the *Device List* pane and click **Refresh**. Optionally, you can click the **Refresh** button in the *Toolbar* and that refreshes all devices in PortVision DX.
7. Verify that the version change is reflected in under the *Software Version*.



Uploading Firmware to Multiple WR7802-XT Switches

You can use this procedure if your WR7802-XT is connected to the host PC, laptop, or if the WR7802-XT resides on the local network segment.

1. If the WR7802-XT is not displayed in PortVision DX, click the **Scan** button.
2. Select the Control Ethernet attached product type and click the **Scan** button.
3. Shift-click the multiple WR7802-XT switches on the **Main** screen that you want to update and right-click and then click **Advanced** | **Upload Firmware**.



4. Browse, click the firmware (.img) file, **Open** (*Please locate the new firmware*), and then click **Yes** (*Upload Firmware*).

It may take a few minutes for the firmware to upload onto all of the WR7802-XT switches. The WR7802-XT reboots itself during the upload process.

5. Click **Ok** to the advisory message about waiting to use the device until the status reads **ON-LINE**.

In the next polling cycle, PortVision DX updates the *Device List* pane and displays the new firmware version.

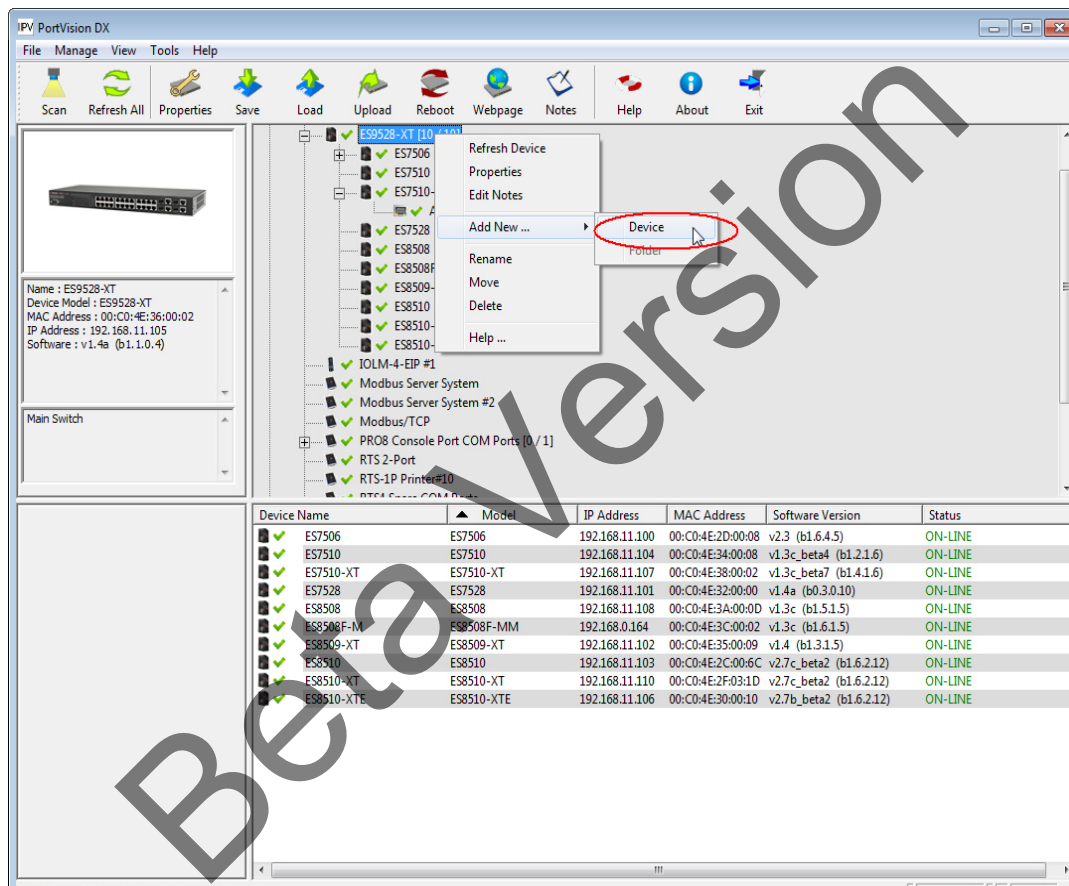
Adding a New Device in PortVision DX

You can add a new WR7802-XT manually, if you do not want to scan the network to locate it or you want to pre-configure an WR7802-XT before connecting it to the network. Optionally, you can also add unmanaged devices or RocketLinux switches to maintain information about devices on the network.

See the PortVision DX help system for additional information about adding unmanaged RocketLinux switches or third party devices or switches.

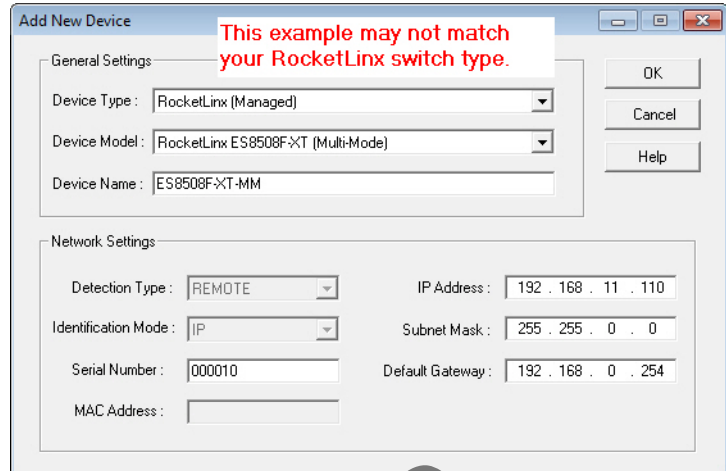
Use the following procedure to add a remote WR7802-XT to PortVision DX.

1. Access the *New Device* window using one of these methods:
 - Click **Add New | Device** in the *Manage* menu.
 - Right-click a folder or a RocketLinux switch in the *Device Tree* pane and click **Add New | Device**.



2. Select the appropriate RocketLinux in the **Device Type** drop list.
3. Select the appropriate model in the **Device Model** drop list.
4. Enter a friendly device name in the **Device Name** list box.
5. Optionally, enter the serial number in the **Serial Number** list box.

6. Enter the IP Address for the WR7802-XT. It is not necessary to enter the Subnet Mask and Default Gateway
7. Click **Ok** to close the *Add New Device* window. It may take a few moments to save the WR7802-XT.
8. If necessary, click **Refresh** for the new RocketLinX to display in the *Device Tree* or *Device List* panes. The RocketLinX shows OFF-LINE if it is not connected to the local network or if an incorrect IP address was entered.



Using Configuration Files

If you are deploying multiple WR7802-XT switches that share common firmware values, you can save the configuration file (.dc) from the *Main* screen in PortVision DX and load that configuration onto other WR7802-XT switches.

Saving a Configuration File

Use this procedure to save a configuration file.

1. Highlight the WR7802-XT in the *Device List* pane and use one of the following methods:
 - Click the **Save** button.
 - Right-click and then click **Configuration | Save**.
2. Browse to the location you want to save the file, enter a file name, and click **Save**.
3. Click **Ok** to close the *Save Configuration Completed* message.

Loading a Configuration File

Use the following procedure to load a previously saved a WR7802-XT configuration file. Load a configuration file and apply it to a selected WR7802-XT switch or switches from the *Device List* pane.

Use this procedure to load a configuration file using the *Device List* pane to one or more WR7802-XT switches.

1. Highlight the device or devices in the *Device List* pane and use one of the following methods:
 - Click the **Load** button
 - Right-click and then click **Configuration | Load**
2. Click **Yes** to the warning that it will take 25 seconds per device and it may also reboot the devices.
3. Browse to the location of the configuration file, click the file name (.dc) and then **Open**.
4. Close the *Load Configuration* popup message.

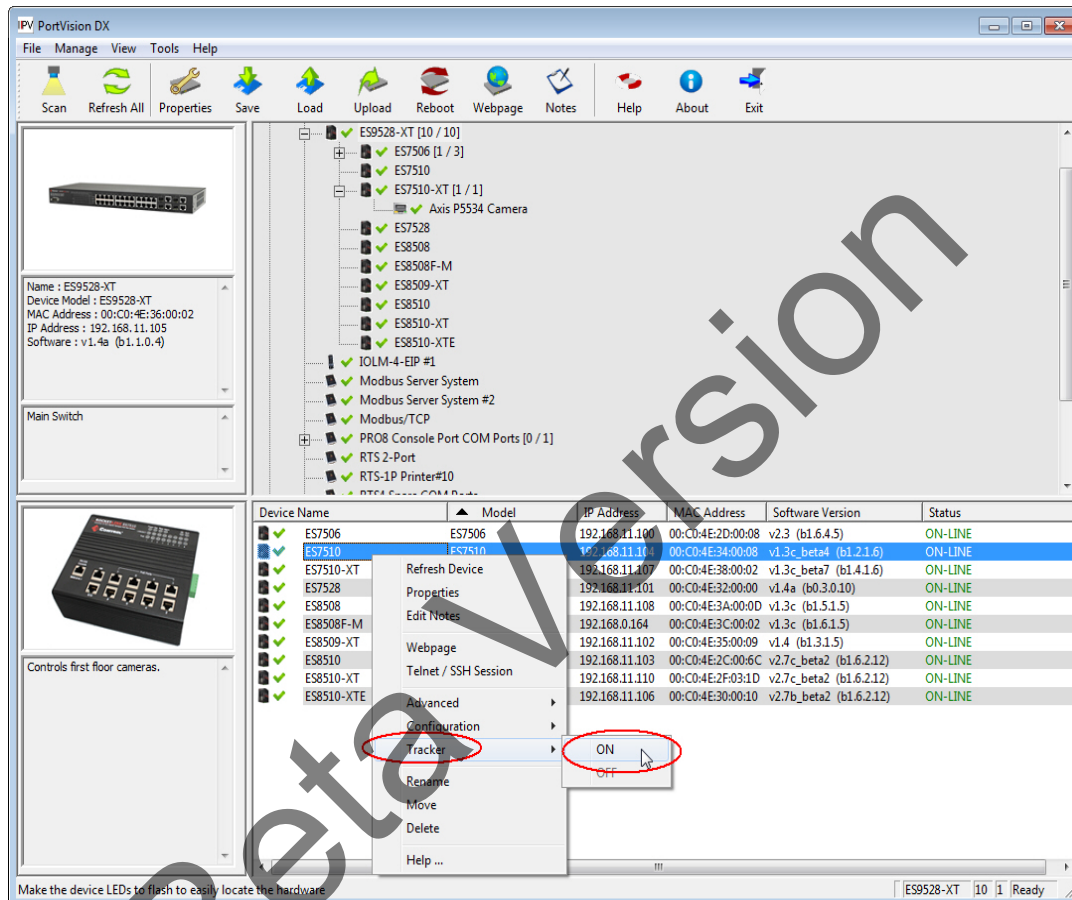
Using the LED Tracker

RocketLinx managed switches support the LED Tracker feature, which allows you to toggle on/off the LEDs on a specific device so that you can locate the physical unit.

Use this procedure to toggle the LED Tracker feature on RocketLinx switches.

1. Right-click the WR7802-XT in the *Device List* pane, click **Tracker**, and then click **ON**.

The WR7802-XT SYS LED will flash for five seconds.

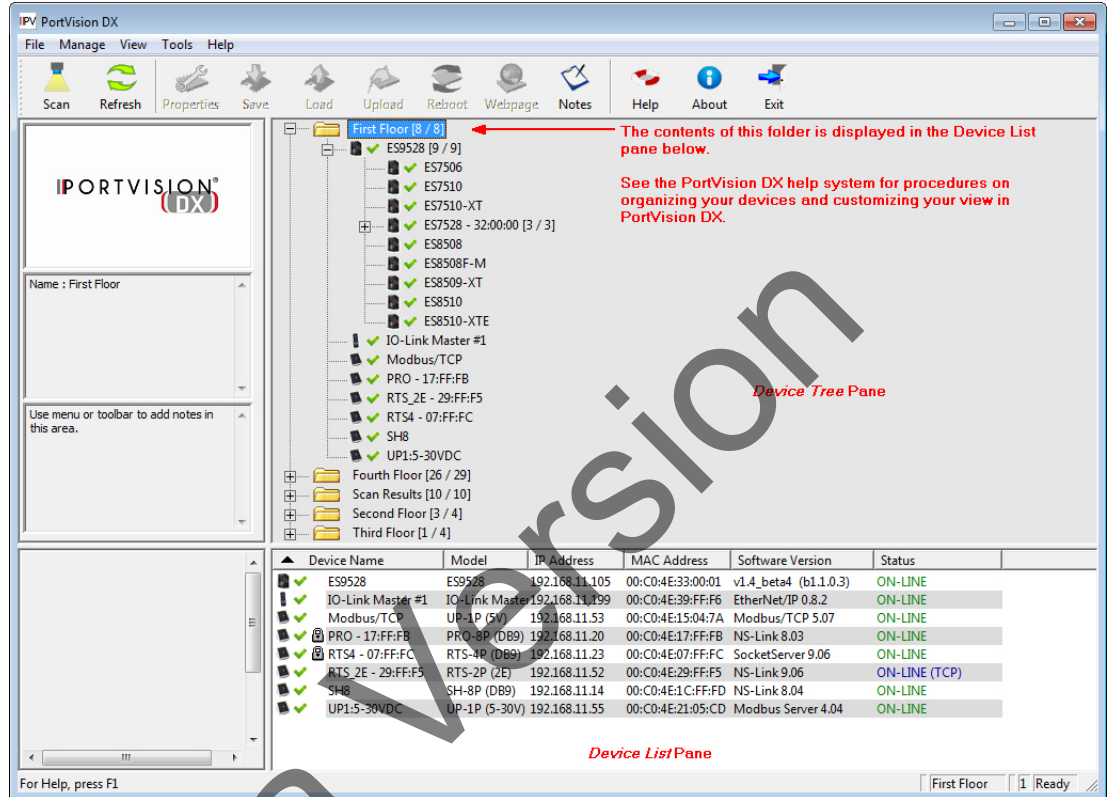


2. If necessary, you may need to click **Tracker** and **ON** several times to catch the flashing **SYS LED**.

Customizing PortVision DX

You can customize how PortVision DX displays the devices. You can even create sessions tailored for specific audiences. You can also add shortcuts to other applications using **Tools | Applications | Customize** feature.

The following illustrates how you can customize your view.



See the PortVision DX Help system for detailed information about modifying the view. For example, the above screen shot illustrates devices layered in folders.

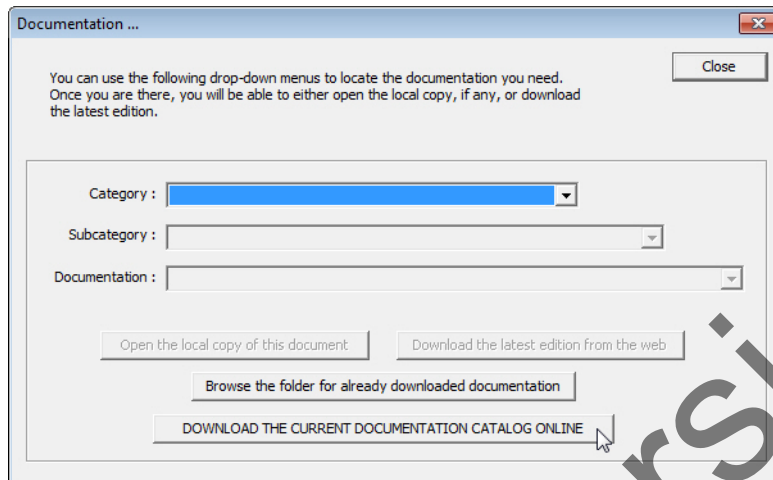
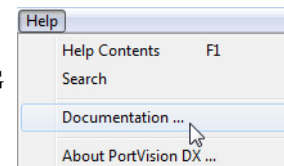
Accessing RocketLinx Documentation from PortVision DX

You can use this procedure in PortVision DX to [download](#) and [open the previously downloaded documents](#) for the RocketLinx.

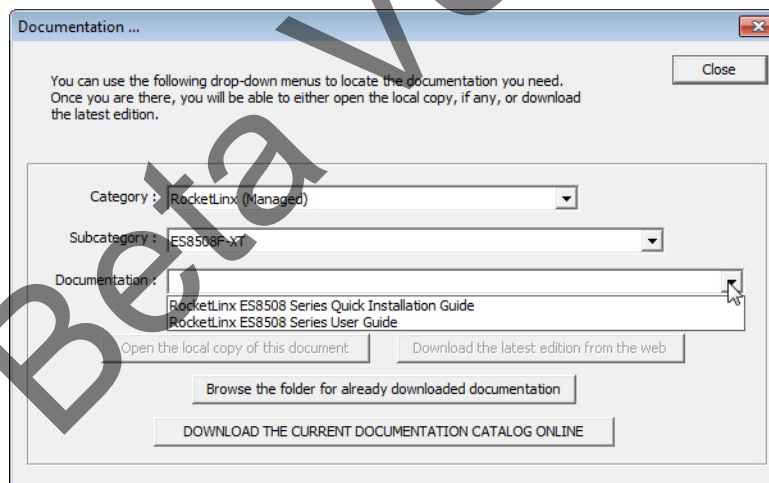
How to Download Documentation

Use this procedure to initially download a document or documents.

1. If necessary, open PortVision DX.
2. Click **Help | Documentation**.
3. Optionally, click the **DOWNLOAD THE CURRENT DOCUMENTATION CATALOG ONLINE** button to make sure that the latest documentation is available to PortVision DX.



4. Select the product **Category** from the drop list.
5. Select the document you want to download from the **Documentation** drop list.



Note: This image may not reflect your RocketLinx.

6. Click the **Download the latest edition from the web** button.

Note: It may take a few minutes to download, depending on your connection speed. The document opens automatically after it has downloaded.

7. Click **Close** if you have downloaded all of the documents that you wanted.

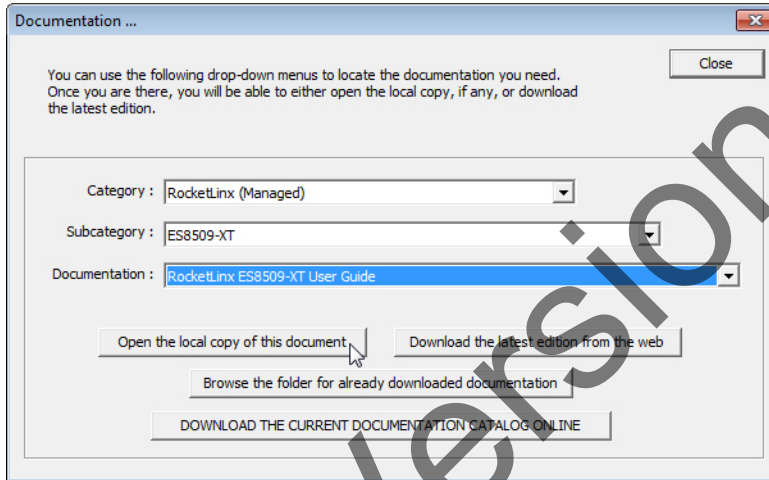
How to Open Previously Downloaded Documents

Use the following procedure to access previously downloaded documents in PortVision DX.

Note: *Optionally, you can browse to the Program Files (x86) | Control | PortVision DX | Docs subdirectory and open the document.*

1. If necessary, open **PortVision DX | Start/Programs | Control | PortVision DX | PortVision DX** or use the desktop shortcut.
2. Click **Help | Documentation**.
3. Click the **Open the local copy of the document** button to view the document.

Note: *This image may not reflect your RocketLinx.*



Note: *If the document fails to open, it may be that your browser has been disabled. You can still access the document by clicking the **Browse the folder for already downloaded documentation** button and opening the document with your custom browser.*

4. Click **Close** in the *Documentation...* popup, unless you want to open or download other documents.

Configuration Using the Web User Interface

The WR7802-XT provides the following methods so that you can connect remotely using the IP address through the network.

- Web user interface (HTTP web user interface ([Page 33](#)) and secure HTTPS web user interface ([Page 36](#)))
- Telnet or SSH console ([Configuration Using the Command Line Interface \(CLI\)](#) on Page 116) and the command line interface (CLI)

System Requirements

Before configuration, make sure your system meets the following requirements:

- A computer/laptop with 10/100/1000 BASE-T(X) adapter
- A web browser for configuration such as Microsoft Internet Explorer or above, Google Chrome or Firefox.

If you choose not to use PortVision DX to configure an IP address, you will need to change the static address of your system to use a static IP address of 192.168.250.x (X cannot be 0, 1, 250, or 255). The WR7802-XT default IP address is 192.168.250.250. Connect the system to one of the LAN ports, GT1 or GT2.

How to Log Into the WR7802-XT

You can log into the WR7802-XT using a standard http connection or through a secure connection https. Use the appropriate discussion for your environment, [Web User Interface](#) on Page 33 (standard http) or [Secure Web User Interface](#) on Page 36 (secure connection).

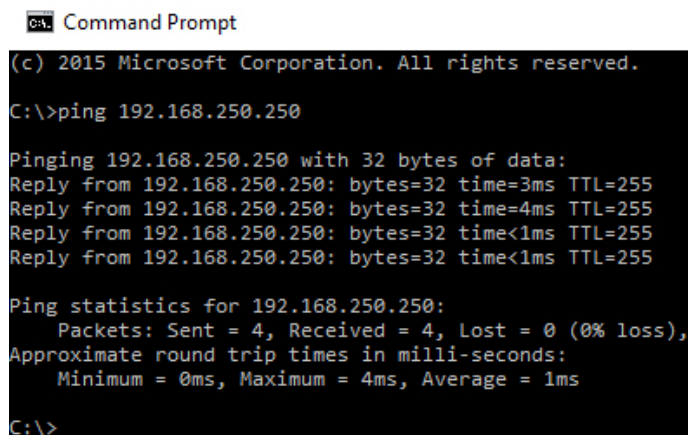
Web User Interface

You can use a standard web browser to configure and communicate with the WR7802-XT from anywhere on the network.

The default IP address for the WR7802-XT is **192.168.250.250**.

1. Open a command prompt window and ping the IP address for the WR7802-XT to verify a normal response time.

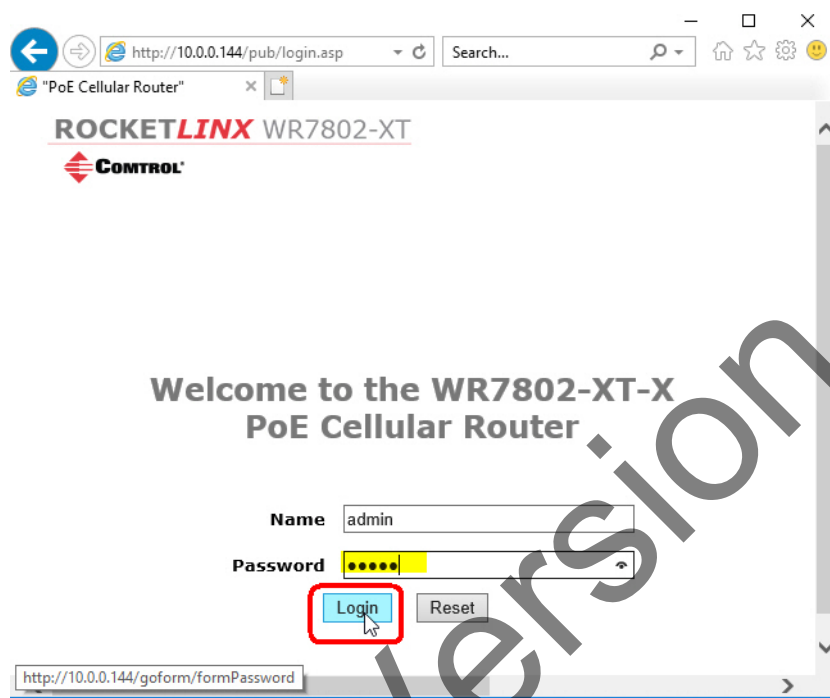
Note: If you did not program the IP address for your network using PortVision DX ([Configuring the Network Settings](#) on Page 21), you need to change your computer IP address to **192.168.250.x** (Network Mask: 255.255.255.0).



```
Command Prompt
(c) 2015 Microsoft Corporation. All rights reserved.
C:\>ping 192.168.250.250
Pinging 192.168.250.250 with 32 bytes of data:
Reply from 192.168.250.250: bytes=32 time=3ms TTL=255
Reply from 192.168.250.250: bytes=32 time=4ms TTL=255
Reply from 192.168.250.250: bytes=32 time<1ms TTL=255
Reply from 192.168.250.250: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.250.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms
C:\>
```

2. Launch the web browser on the PC using one of these methods:
 - Right-click the WR7802-XT in PortVision DX and click **Webpage**.
 - Open your browser, enter the IP address of the switch, and then press **Enter**. For example: **http://10.0.0.140**.



- Enter the user name, the password, and click **OK**. The default user name and password are both **admin**. The first web page that displays is the **Information** page, which provides overall status of the WR7802-XT.

ROCKETLINX WR7802-XT

CONTROL

WR7802-XT-X

- Status
- System
- Power over Ethernet
- Switch Configuration
- Traffic Prioritization
- Multicast Filtering
- Network Redundancy
- Cellular
- VPN
- Security
- Management
- Tools
- Save
- Logout
- Reboot

Information

System Information

Model Name	WR7802-XT-X
Device Name	PM-Lab-690001
Firmware Version	0.9a6f3

LAN Settings

IP Address	10.0.0.144
Subnet Mask	255.0.0.0
Gateway IP Address	0.0.0.0
MAC Address	00:c0:4e:69:00:01

Cellular Settings

SIM	
Provider	Verizon Wireless
APN	mw01.vzwstatic
Service Type	E-UTRAN
IMEI	359677060155738
Signal Strength	-79 dBm(Good)
SIM1 Status	SIM OK
SIM2 Status	SIM Carrier Inserted
Connection Status	Connected
IP Address	166.246.168.172

This illustrates that the cellular network is functioning properly with the SIM

Note: If you cannot log into the WR7802-XT, refer to [Diagnosing a Login Failure](#) on Page 39.

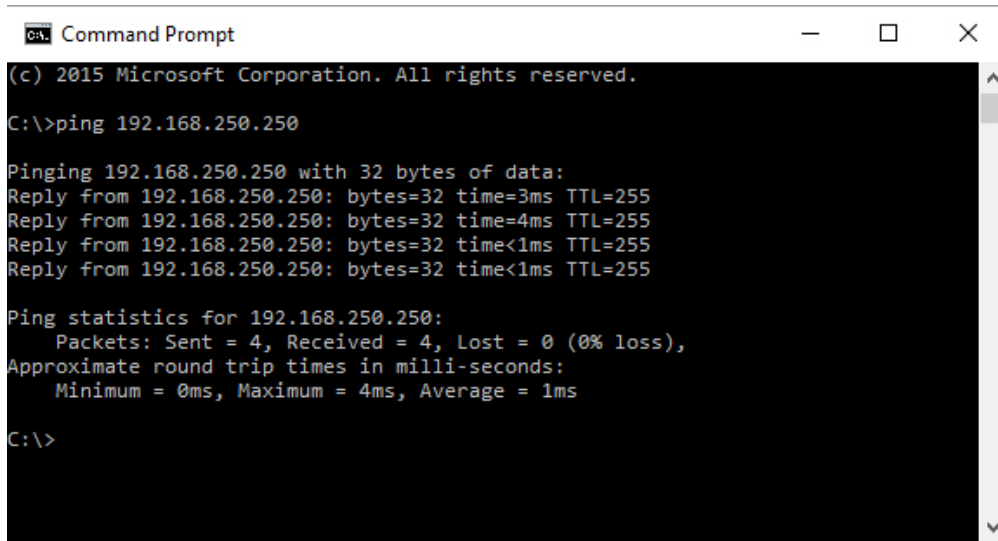
- If you have not done so, you can change the WR7802-XT IP address to meet your network environment using the **System | IP Settings** page.

Secure Web User Interface

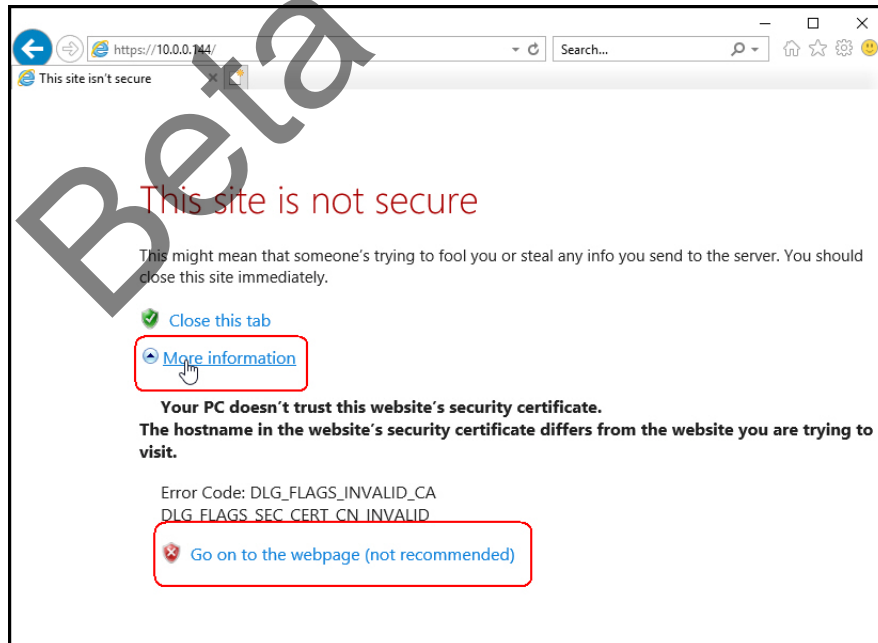
The WR7802-XT web user interface also provides secured management through an HTTPS login so that all of the configuration commands are secure.

If you did not program the IP address for your network using PortVision DX ([Configuring the Network Settings](#) on Page 21), you need to change your computer IP address to **192.168.250.x** (Network Mask: 255.255.255.0). The default IP address for the WR7802-XT is *192.168.250.250*.

1. Open a command prompt window and ping the IP address for the WR7802-XT to verify a normal response time.



2. Launch the web browser and type **https://192.168.250.250** (or the IP address of the WR7802-XT).and then press **Enter**.
3. Expand the **More Information** link and then click the **Go on to the webpage (not recommended)** option.



4. Enter the user name and the password and click **OK**. The default name and password are both **admin**.



The first web page that displays is the **Information** page, which provides overall status of the WR7802-XT.

ROCKETLINX WR7802-XT

CONTROL

- WR7802-XT-X
 - Status
 - System
 - Power over Ethernet
 - Switch Configuration
 - Traffic Prioritization
 - Multicast Filtering
 - Network Redundancy
 - Cellular
 - VPN
 - Security
 - Management
 - Tools
 - Save
 - Logout
 - Reboot

Information

System Information

Model Name	WR7802-XT-X
Device Name	PM-Lab-690001
Firmware Version	0.9a6i3

LAN Settings

IP Address	10.0.0.144
Subnet Mask	255.0.0.0
Gateway IP Address	0.0.0.0
MAC Address	00:c0:4e:69:00:01

Cellular Settings

SIM	1
Provider	Verizon Wireless
APN	mvd01.vzwstatic
Service Type	E-UTRAN
IMEI	359677060155738
Signal Strength	-79 dBm(Good)
SIM1 Status	SIM OK
SIM2 Status	SIM Carrier Inserted
Connection Status	Connected
IP Address	166.246.168.172

This illustrates that the cellular network is functioning properly with the SIM

Note: If you cannot log into the WR7802-XT, refer to [Diagnosing a Login Failure](#) on Page 39.

- If you have not done so, you can change the WR7802-XT IP address to meet your network environment, using the **System | IP Settings** page.

Diagnosing a Login Failure

If you were unable to log into the WR7802-XT, you try the following:

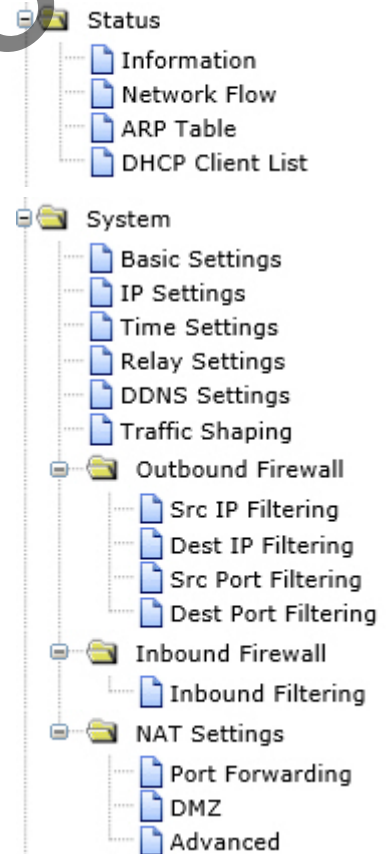
- Try a different web browser.
- Temporally disable the firewall settings for your browser. The firewall setting may block the connection from your PC to the device. Make sure that you re-enable the firewall to protect your system.
- Check the IP configuration on your system. The WR7802-XT must be located within the same subnet.
- Check whether the connected ports are properly connected, or if the ports are assigned to different IP addresses.

Note: The web interface connection session for the WR7802-XT logs out automatically if you do not enter any input after 30 seconds. After being logged out, you should re-login.

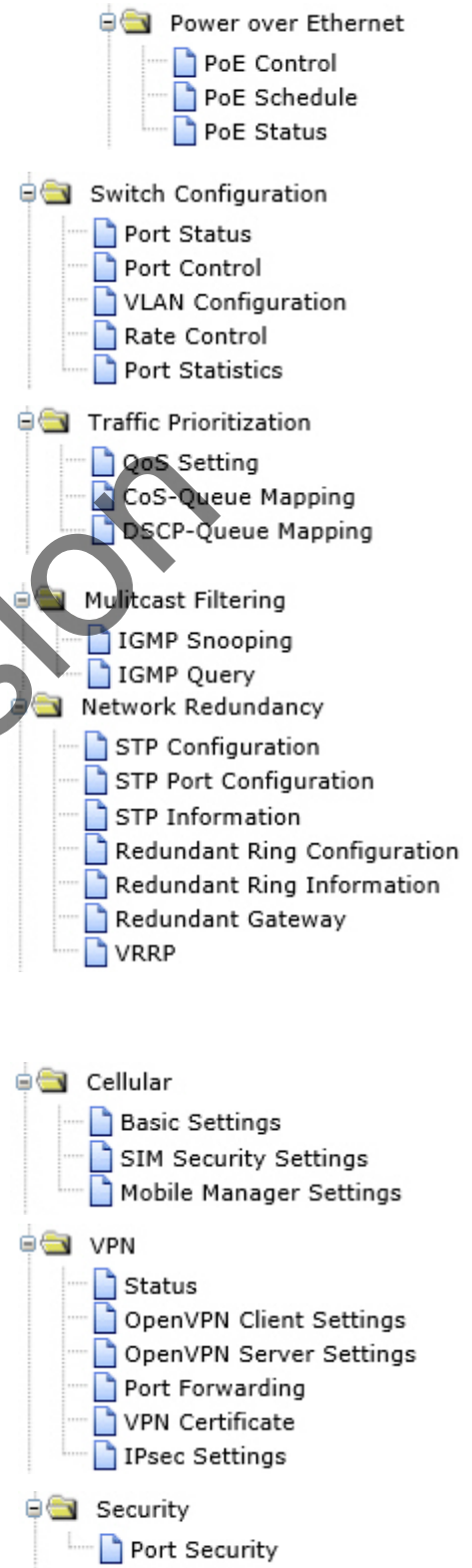
Introduction to the Web Interface

The WR7802-XT provides these top-level menus with the corresponding web pages:

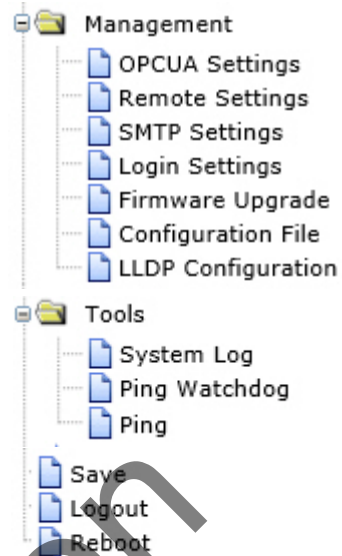
- [Status Web Pages](#) on Page 41
 - [Status | Information Page](#) on Page 42
 - [Status | Network Flow Page](#) on Page 44
 - [Status | ARP Table Page](#) on Page 45
 - [Status | DHCP Client List Page](#) on Page 45
- [System Web Pages](#) on Page 46
 - [System | Basic Settings Page](#) on Page 46
 - [System | IP Settings Page](#) on Page 47
 - [System | Time Settings Page](#) on Page 50
 - [System | Relay Settings Page](#) on Page 51
 - [System | DDNS Settings Page](#) on Page 51
 - [System | Traffic Shaping Page](#) on Page 53
 - [System | Outbound Firewall Submenu](#) on Page 53
 - [System | Outbound Firewall | Src \(Source\) IP Filtering Page](#) on Page 54
 - [System | Outbound Firewall | Dest \(Destination\) IP Filtering Page](#) on Page 54
 - [System | Outbound Firewall | Src \(Source\) Port Filtering Page](#) on Page 55
 - [System | Outbound Firewall | Dest \(Destination\) Port Filtering Page](#) on Page 55
 - [System | Inbound Filtering Page](#) on Page 56
 - [System | NAT Settings Submenu](#) on Page 57
 - [System | NAT Settings | Port Forwarding Page](#) on Page 57
 - [System | NAT Settings | DMZ Page](#) on Page 58
 - [System | NAT Settings | Advanced Page](#) on Page 59



- [Power Over Ethernet Pages](#) on Page 59
 - [Power over Ethernet | PoE Control Page](#) on Page 59
 - [Power over Ethernet | PoE Schedule Page](#) on Page 62
 - [Power over Ethernet | PoE Status Page](#) on Page 63
- [Switch Configuration Pages](#) on Page 64
 - [Switch Configuration | Port Status Page](#) on Page 64
 - [Switch Configuration | Port Control Page](#) on Page 65
 - [Switch Configuration | VLAN Configuration Page](#) on Page 66
 - [System Configuration | Rate Control Page](#) on Page 68
 - [Switch Configuration | Port Statistics Page](#) on Page 69
- [Traffic Prioritization Pages](#) on Page 70
 - [Traffic Prioritization | QoS Setting Page](#) on Page 70
 - [Traffic Prioritization | CoS-Queue Mapping Page](#) on Page 71
 - [Traffic Prioritization | DSCP-Queue Mapping Page](#) on Page 72
- [Multicast Filtering Pages](#) on Page 73
 - [Multicast Filtering | IGMP Snooping Page](#) on Page 74
 - [Multicast Filtering | IGMP Query Page](#) on Page 75
- [Network Redundancy Pages](#) on Page 76
 - [Network Redundancy | STP Configuration Page](#) on Page 77
 - [Network Redundancy | STP Port Configuration Page](#) on Page 79
 - [Network Redundancy | STP Information Page](#) on Page 80
 - [Network Redundancy | Redundant Ring Configuration Page](#) on Page 81
 - [Network Redundancy | Redundant Ring Information Page](#) on Page 82
 - [Network Redundancy | Redundant Gateway Page](#) on Page 83
 - [Network Redundancy | VRRP Page](#) on Page 85
- [Cellular Pages](#) on Page 87
 - [Cellular | Cellular Basic Settings Page](#) on Page 87
 - [Cellular | SIM Security Settings Page](#) on Page 89
 - [Cellular | Mobile Manager Settings Page](#) on Page 90
- [VPN Pages](#) on Page 91
 - [VPN | VPN Status Page](#) on Page 92
 - [VPN | OpenVPN Client Settings Page](#) on Page 93
 - [VPN | OpenVPN Server Settings Page](#) on Page 95
 - [VPN | VPN Port Forwarding Page](#) on Page 97
 - [VPN | VPN Certificate Page](#) on Page 98
 - [VPN | IPsec Settings Page](#) on Page 98
- [Security - Port Security Page](#) on Page 101



- [Management Pages](#) on Page 102
 - [Management | OPCUA Settings Page](#) on Page 103
 - [Management | Remote Settings Page](#) on Page 104
 - [Management | SMTP Settings Page](#) on Page 107
 - [Management | Login Settings Page](#) on Page 108
 - [Management | Firmware Upgrade Page](#) on Page 110
 - [Management | Configuration File Page](#) on Page 111
 - [Management | LLDP Configuration Page](#) on Page 112
- [Tools Pages](#) on Page 113
 - [Tools | System Log Page](#) on Page 113
 - [Tools | Ping Watchdog Page](#) on Page 114
 - [Tools | Ping Page](#) on Page 115
- [Save Page](#) on Page 115
- [Logout Page](#) on Page 115
- [Reboot Page](#) on Page 115



Status Web Pages

The **Status** menu provides these web pages:

- [Status | Information Page](#) on Page 42
- [Status | Network Flow Page](#) on Page 44
- [Status | ARP Table Page](#) on Page 45
- [Status | DHCP Client List Page](#) on Page 45

Status | Information Page

The **Information** page provides current status and some basic settings for the WR7802-XT.

ROCKETLIX WR7802-XT

CONTROL

- WR7802-XT-X
 - Status
 - System
 - Power over Ethernet
 - Switch Configuration
 - Traffic Prioritization
 - Multicast Filtering
 - Network Redundancy
 - Cellular
 - VPN
 - Security
 - Management
 - Tools
 - Save
 - Logout
 - Reboot

Information

System Information

Model Name	WR7802-XT-X
Device Name	PM-Lab-690001
Firmware Version	0.9a613

LAN Settings

IP Address	10.0.0.144
Subnet Mask	255.0.0.0
Gateway IP Address	0.0.0.0
MAC Address	00:c0:4e:09:00:01

Cellular Settings

SIM	1
Provider	Verizon Wireless
APN	mw01.vzwstatic
Service Type	E-UTRAN
IMEI	359677060155738
Signal Strength	-79 dBm(Good)
SIM1 Status	SIM OK
SIM2 Status	SIM Carrier Inserted
Connection Status	Connected
IP Address	166.246.168.172

This illustrates that the cellular network is functioning properly with the SIM

Beta Version

System Information	
Model Name	Displays the product model name.
Device Name	Displays the device name, which can be changed using the System Basic Settings page.
Firmware Version	Displays the firmware version loaded on the router.
LAN Settings	
IP Address	Displays the LAN IP address.
Subnet Mask	Displays the LAN subnet mask.
Gateway IP Address	Displays the LAN gateway address.
MAC Address	Displays the MAC address of the LAN.
Cellular Settings	
SIM	Displays the primary SIM card number, 1 or 2. This is dependent on which SIM you selected on the Cellular Basic Settings page.
Provider	Displays the name of the Cellular carrier or ISP (Internet service provider).
APN	Displays the access point name. Some ISPs require a specific APN, which should be configured on the Cellular Basic Setting page.
Service Type	<p>Displays the type of service.</p> <p>After 3G/LTE connects, the connected ISP updates the service type here. The possible types are GSM, UMTS, GSM w/EGPRS, UMTS w/HSDPA, UMTS w/HSDPA and HSUPA, E-UTRAN, Unknown, No Service (default value)</p> <p>Typically, Cellular service is mainly HSPA/LTE data communications. The rest of services are backward compatible service to avoid losing connection when HSPA/LTE is not available.</p>
IMEI	The unique International Mobile Equipment Identity for this router.
Signal Strength	<p>Displays the signal strength to the remotely connected base station. If the signal strength displays low, you should move the AP/Gateway location or mount an auxiliary antenna in better location.</p> <p>Signal strength definitions:</p> <ul style="list-style-type: none"> • 0 dBm (Default value while no connection, or during a Read the Signal Strength error.) • -113 dBm or less (Low) • -51 dBm or greater (Excellent) • Not known or not detectable

Cellular Settings	
SIM1 Status SIM2 Status	This defines the possible SIM status messages: <ul style="list-style-type: none"> • SIM OK: The SIM card is ready to use. • SIM Carrier Inserted: The SIM card is not inserted. • SIM PIN Locked: The SIM card is locked due to PIN error. It may be caused by error typing PIN password many times. Check with your ISP to resolve the issue. • SIM is deactivated: The SIM card may have some problem. Please check with your ISP to resolve the issue.
Connection Status	<ul style="list-style-type: none"> • Connected: The 3G/LTE interface is connected to the base station. • Not Connected: The 3G/LTE interface is not connected to the base station.
IP Address	This is the Cellular IP address assigned by the ISP.

Status | Network Flow Page

The Network Flow shows the packet counters for transmission and reception for the Cellular interface.(3G or LTE).

Network Flow Help

Poll Interval: (0-65534) sec Set Interval

Stop

	Received	Transmitted
Cellular		
Total Packets	0	2
Total Bytes	0	680

Refresh

Network Flow Page	
Poll Interval	The Poll Interval time setting, ranges from 0~65524 seconds. If you want to change the Poll Interval time, click the Stop button, enter a new value, and click Set Interval to activate.
Set Interval	Click this button to set a new interval time after entering a new polling interval time.
Stop	Click this button to stop polling the associated clients.
Refresh	Click to refresh the table.

Status | ARP Table Page

This displays the ARP (address resolution table).

ARP Table

IP Address	MAC Address	Interface
10.0.0.202	00:40:f4:a8:c3:e7	br0

Refresh

ARP Table Page	
IP Address	The IP Address learnt from the interface.
MAC Address	The MAC Address learnt from the interface.
Interface	The interface that learnt the ARP packet (IP and MAC Address).
Refresh	Click to refresh the table.

Status | DHCP Client List Page

This table shows the assigned IP address, MAC address and expiration timer of the connected DHCP client device.

DHCP Client List

Help

IP Address	MAC Address	Time Expired(s)
10.0.0.37	00:c0:4e:34:00:08	862

Refresh

DHCP Client List Page	
IP Address	The assigned IP address of the connected DHCP client device.
MAC Address	The MAC address of the connected DHCP client device.
Time Expired(s)	The DHCP expiration timer of the connected DHCP client device. The time unit is in seconds. The number can be changed on the System IP Settings page with the DHCP Server Lease Time setting.
Refresh	Click this button to refresh the table.

System Web Pages

The System menu provides these web pages:

- [System | Basic Settings Page](#) on Page 46
- [System | IP Settings Page](#) on Page 47
- [System | DHCP Server Page](#) on Page 49
- [System | Time Settings Page](#) on Page 50
- [System | Relay Settings Page](#) on Page 51
- [System | DDNS Settings Page](#) on Page 51
- [System | Traffic Shaping Page](#) on Page 53
- [System | Outbound Firewall Submenu](#) on Page 53
- [System | Inbound Filtering Page](#) on Page 56
- [System | NAT Settings Submenu](#) on Page 57

System | Basic Settings Page

The System | Basic Settings page allows you to give a name to identify an access point name. It allows maximum 15 characters and no spaces.

The screenshot shows the 'Basic Settings' page with a 'Help' button. Below the title is a section for 'Device Settings'. A text input field is labeled 'Device Name :'. The field contains the text 'PM-Lab-690001'. To the right of the field, there is a note: '(max. 15 characters and no spaces)'. At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

System | IP Settings Page

Use the **IP Settings** page to configure the IP related parameters for LAN interfaces, which connects to the LAN port of your router (Access Point).

IP Settings Help

LAN IP Address Assignment

Use DHCP
 Use Static IP Address

IP Address :	10.0.0.144
Subnet Mask :	255.0.0.0
Gateway IP Address :	0.0.0.0
DNS 1 :	8.8.8.8
DNS 2 :	0.0.0.0

Apply Cancel

IPv6 Address	Prefix Length

Add

IPv6 Default Gateway

Apply

IPv6 Address

<input type="checkbox"/>	fe80::02c0:4e69:feff:0001/64
--------------------------	------------------------------

Remove Reload

IPv6 Neighbor Table

Neighbor	Interface	MAC Address	State

IP Settings Page	
LAN IP Address Settings	
Use DHCP	If you select this option, the router allows a DHCP server to assign an IP address.
Use Static IP Address	If you select this option, enter a valid address in the IP Address field.
IP Address	The IP Address field allows you to set the static IP address on the WR7802-XT. The default IP address is 192.168.250.250.
Subnet Mask	You can change the subnet mask address for the LAN interface. The default subnet mask is a Class C address: 255.255.255.0.
Gateway IP Address	You can change the gateway address. The default gateway address is 192.168.250.1. This is the system gateway IP address when Cellular is not available.
DNS 1/2	The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.
IPv6 Address	This field allows you to enter an IPv6 address to add to the management VLAN. By default the management interface automatically configures with a link-local address. Click the Add button to add the entered address to the management VLAN.
Prefix Length	This field allows you to indicate what part of the IPv6 address is used for routing. Click the Apply button to set the entered default gateway.
IPv6 Default Gateway	The default gateway IP address identifies the gateway (for example, a router) that receives and forwards those packets whose addresses are unknown to the local network. The agent uses the default gateway address when sending alert packets to the management workstation on a network other than the local network.
IPv6 Address	This table shows the IPv6 addresses that have been added to the management VLAN. To remove an entry click the check box next to it and click the Remove button. To reload the list click the Reload button.
IPv6 Neighbor Table	
Neighbor	The IPv6 address of the neighbor.
Interface	The port that the neighbor is connected to.
MAC Address	The MAC address of the neighbor.
State	The Neighbor connection state of the neighbor entry.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

System | DHCP Server Page

Use this page to configure the DHCP server.

DHCP Server

DHCP Settings:	Disabled ▾
DHCP IP Address Range Start :	10.0.0.40
DHCP IP Address Range End :	10.0.0.49
DHCP Subnet Mask:	255.255.0.0
DHCP Gateway:	0.0.0.0
WINS1 :	0.0.0.0
WINS2 :	0.0.0.0
Primary DNS Server :	8.8.8.8
Secondary DNS Server :	0.0.0.0
Lease Time(15-44640 Minutes) :	15

DHCP Server Page	
DHCP Settings	You can Enable or Disable this option. After the DHCP Server option is enabled, you can then assign the starting and ending IP of the DHCP IP address range. The WR7802-XT allows you to assign up to one Class C range which is 255 IP addresses. <i>Note: The maximum connections per session is 64.</i>
DHCP IP Address Range Start	This is the starting IP address that DHCP will assign. The default is 192.168.250.100.
DHCP IP Address Range End	This is the ending IP address that DHCP will assign. The default is 192.168.250.200.
DHCP Subnet Mask	This is the DHCP subnet mask. The default is 255.255.255.0.
DHCP Gateway	This is the DHCP gateway address. The default is 192.168.250.250.
WINS1/2	This is the primary and secondary DNS servers IP addresses.
Primary/Secondary DNS	The DNS server address that you want the DHCP server to distribute.
Lease Time	This is the amount of time of the assigned IP addresses. The range is 15 - 44640 minutes.

System | Time Settings Page

Use the **Time Settings** page to configure the time settings for the WR7802-XT. You can configure current time, time zone, and configure NTP protocol to synchronize system time with a public time server over the Internet.

Time Settings

Current Time:	Yr <input type="text" value="2017"/> Mon <input type="text" value="4"/> Day <input type="text" value="6"/> Hr <input type="text" value="10"/> Mn <input type="text" value="47"/> Sec <input type="text" value="50"/>
	<input type="button" value="Get PC Time"/>
Time Zone :	<input type="text" value="(GMT-06:00)Central Time (US & Canada)"/>
NTP:	<input type="checkbox"/> Enable NTP client update
<input checked="" type="radio"/> NTP server:	<input type="text" value="pool.ntp.org - Global"/>
<input type="radio"/> Manual IP:	<input type="text" value="0.0.0.0"/>

Time Settings Page	
Current Time	<p>You can manually type the current time or get the time from your PC or Cellular module.</p> <ul style="list-style-type: none"> If you click the Get PC Time button, the current time is updated according to your PC's time. If you click Get Cellular Time, the current time is updated according to your module's RTC (real time clock). This button is hidden if a Cellular network is not detected.
Time Zone	Select the time zone of your country from the drop-down list.
NTP	You can select the Enable NTP client update option and then the NTP feature is activated and synchronized from the remote time server.
NTP Server	Select the time server from the NTP Server drop-down list or manually input the IP address of available time server into Manual IP .
Manual IP	You can enter the IP address of server that you want to set the time on the WR7802-XT.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

System | Relay Settings Page

Use the **Relay Settings** page to configure the DO relay.

Relay Settings

Link Failure:	Port <input type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4
----------------------	--

Select the port or ports that want monitor for a link failure and then press **Apply** to activate the settings.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

System | DDNS Settings Page

Use the **DDNS Settings** page to configure the parameters for DDNS (Dynamic Domain Name System) client.

Since not all carrier providers provide a fixed IP service and the dynamic IP address of Cellular interface may change often, making it difficult to remotely manage the WR7802-XT IP address. Optionally, you can use DDNS domain name instead fixed IP address.

DDNS Settings

Enable DDNS Client

Server:	dyndns.org ▼
Domain Name:	<input type="text"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

DDNS Settings	
Enable DDNS Client	Select this option if you want to enable a DDNS domain name instead of a fixed IP address.
Server	The WR7802-XT supports dyndns.org, freedns.afraid.org and no-ip.com services.
Domain Name	This is the domain name provided by the Cellular carrier.
User Name	This is user name provided by the Cellular carrier.
Password	This is the password for the DDNS client.
Confirm Password	You must confirm the DDNS client password before applying the settings.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Beta Version

System | Traffic Shaping Page

Use the **Traffic Shaping** page to specify the incoming and outgoing traffic limit.

Traffic Shaping

Enable Traffic Shaping

Incoming Traffic Limit:	<input type="text" value="1024000"/>	kbit/s
Incoming Traffic Burst:	<input type="text" value="20"/>	kBytes
Outgoing Traffic Limit:	<input type="text" value="1024000"/>	kbit/s
Outgoing Traffic Burst:	<input type="text" value="20"/>	kBytes

Traffic Shaping Page	
Enable Traffic Shaping	Select the item to activate the feature. After enabling traffic shaping, you can configure the Incoming Traffic Limit , Incoming Traffic Burst , Outgoing Traffic Limit and Outgoing Traffic Burst .
Incoming Traffic Limit	If necessary, enter a suitable value for this parameter. The range is 100 to 1024000.
Incoming Traffic Burst	If necessary, enter a suitable value for this parameter. The range is 0 to 1024000.
Outgoing Traffic Limit	If necessary, enter a suitable value for this parameter. The range is 100 to 1024000.
Outgoing Traffic Burst	If necessary, enter a suitable value for this parameter. The range is 0 to 1024000.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

System | Outbound Firewall Submenu

Use the following firewall settings pages to configure the firewall setting. There are different types of firewall settings:

- **Src IP Filtering** ([Page 54](#)): Source IP address filtering from your LAN to Internet through the gateway.
- **Dest IP Filtering** ([Page 54](#)): Destination IP address filtering from the LAN to Internet through the gateway.
- **Src Port Filtering** ([Page 55](#)): Source port filtering from the LAN to Internet through the gateway.
- **Dest Port Filtering** ([Page 55](#)): Destination ports filtering from the LAN to Internet through the gateway.

System | Outbound Firewall | Src (Source) IP Filtering Page

Entries in this table are used to restrict certain types of data packets from your local network to the Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

Select **Enable Source IP Filtering**, type the local IP address and comment (note for the entry) and then press **Apply** to activate the settings.

The table displays each local IP address and the comment for each entry. Use the table to edit or delete any entry as needed.

After selecting **Apply** to activate the settings you can then see the entries you configured in the table below.

Note: You must **Save** (Page 115) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Source IP Filtering

<input type="checkbox"/> Enable Source IP Filtering	
Local IP Address:	<input type="text"/>
Comment:	<input type="text"/>

Apply Cancel

Local IP Address	Comment	Select	Edit

Delete Selected Delete All Refresh

System | Outbound Firewall | Dest (Destination) IP Filtering Page

Entries in this table are used to restrict the computers in the LAN from accessing certain websites in the WAN according to IP address.

Select **Enable Destination IP Filtering**, type the Destination IP address and comment (note for the entry) and then press **Apply** to activate the settings.

The table displays each destination IP address and the comment for each entry. Use the table to edit or delete any entry as needed.

After selecting **Apply** to activate the settings you can then see the entries you configured in the table below.

Note: You must **Save** (Page 115) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Destination IP Filtering

<input type="checkbox"/> Enable Destination IP Filtering	
Destination IP Address:	<input type="text"/>
Comment:	<input type="text"/>

Apply Cancel

Destination IP Address	Comment	Select	Edit

Delete Selected Delete All Refresh

System | Outbound Firewall | Src (Source) Port Filtering Page

Entries in this table are used to restrict certain ports of data packets from your local network to the Internet through the gateway. Use of such filters can be helpful in securing or restricting your local network.

Select **Enable Source Port Filtering**, type the port range, select the Protocol type (UDP, TCP, or Both). You can enter a comment (note for the entry) and then press **Apply** to activate the settings.

The table displays each source port range, protocol, and the comment for each entry. Use the table to edit or delete any entry as needed.

After selecting **Apply** to activate the settings you can then see the entries you configured in the table below.

Note: You must **Save** (Page 115) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Source Port Filtering

Enable Source Port Filtering

Port Range:	-
Protocol:	Both ▾
Comment:	

Source Port Range ↕	Protocol ↕	Comment ↕	Select	Edit

System | Outbound Firewall | Dest (Destination) Port Filtering Page

Use the entries in this table to restrict certain ports of data packets from your local network to the Internet through the gateway. Use of such filters can be helpful in securing or restricting your local network.

Select **Enable Destination Port Filtering**, type the port range, protocol type (UDP, TCP or Both). Type the Comment (note for the entry) and then click **Apply** to activate the settings.

The table displays each destination port range, protocol, and the comment for each entry. Use the table to edit or delete any entry as needed.

After selecting **Apply** to activate the settings you can then see the entries you configured in the table below.

Note: You must **Save** (Page 115) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Destination Port Filtering

Enable Destination Port Filtering

Port Range:	-
Protocol:	Both ▾
Comment:	

Dest Port Range ↕	Protocol ↕	Comment ↕	Select	Edit

System | Inbound Filtering Page

Inbound Filtering is used to restrict any access from Internet to the LAN. Only the applied entries in the Remote Management Exception list can access the LAN from the Internet through the gateway.

Enable Inbound Firewall: After enabled inbound firewall, it means that all the IP address from the Internet can NOT access the LAN through the gateway. You can configure Remote Management Exception for exceptional items that includes Web, Telnet, SSH and SNMP.

Inbound Filtering Help

Enable Inbound Firewall

Remote Management Exception

Web Telnet SSH
 SNMP

Exception	
Src IP Address:	<input style="width: 90%;" type="text"/>
Src Port Range:	<input style="width: 90%;" type="text"/>
Dest Port Range:	<input style="width: 90%;" type="text"/>
Comment:	<input style="width: 90%;" type="text"/>

Apply Cancel

Src IP Address ↕	Src Port Range ↕	Dest Port Range ↕	Comment ↕	Select	Edit

Delete Selected Delete All Refresh

Inbound Filtering Page	
Exception:	The Exception table allows you to configure the exception list.
Src IP Address:	The entry allows you to configure the source IP address from the Internet.
Src Port Range:	The source port range of the above IP address.
Dest Port Range:	The destination port range of the above IP address. Destination port range can NOT be empty! You should set a value between 1~65535.
Comment:	Note for the entry.

After selecting **Apply** to activate the settings you can then see the entries you configured in the table below.
Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

System | NAT Settings Submenu

NAT is the abbreviation of Network Address Translation. NAT is a methodology of modifying network address information in IP packet headers while they are in transit across a gateway/router for the purpose of remapping one IP address space into another. The simple type of NAT provides one to one translation of IP addresses. It can be used to interconnect two IP networks, normally one network is for Local Area Network and the other network is for Wide Area Network/Internet.

Use the NAT **Settings** pages to configure the NAT settings:

- [System | NAT Settings | Port Forwarding Page](#) on Page 57
- [System | NAT Settings | DMZ Page](#) on Page 58
- [System | NAT Settings | Advanced Page](#) on Page 59

[System | NAT Settings | Port Forwarding Page](#)

Entries in the **Port Forwarding** table allows you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your gateway's NAT firewall.

Port Forwarding

Enable Port Forwarding

Public Port Range: -

IP Address:

Protocol:

Port Range: -

Comment:

Public Port Range	Local IP Address	Protocol	Port Range	Comment	Select	Edit
8888	10.0.0.104	TCP	80	HTTP	<input type="checkbox"/>	<input type="button" value="Edit"/>
80	10.0.0.222	TCP+UDP	80	Camera#1	<input type="checkbox"/>	<input type="button" value="Edit"/>

Port Forwarding Page	
Enable Port Forwarding	Select this check box and then type the parameters to create the port forwarding entries.
Public Port Range	Configure the port range that is public to the WAN/Internet. You can configure one or a range of TCP/UDP port numbers.
IP Address	Configure the IP address of the LAN PC. The traffic from the public port range is redirected to this IP address.

Port Forwarding Page (Continued)	
Protocol	Configure the protocol type: TCP, UDP or Both (TCP and UDP).
Port Range	Configure the port range of the LAN, the traffic from the public port is redirected to these port.
Comment	Add supporting information for the entry.

After selecting **Apply** to activate the settings you can then see the entries you configured in the table below.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

[System](#) | [NAT Settings](#) | [DMZ Page](#)

The DMZ (Demilitarized Zone) page is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains device accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers, and DNS servers.

DMZ Page	
Enable DMZ	Select the check box to enable this feature.
DMZ Host IP Address	Enter the IP address of the DMZ host IP address. This is the DMZ computer's IP address. If you configure the DMZ function for your office network, you should get approval from the IT administrator.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

You can use the NAT **Advanced** page to randomize NAT port mapping. Select **Enable** in the drop list and then click the **Apply** button.

NAT Advanced Settings

Random Port :

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Power Over Ethernet Pages

The Power over Ethernet ports is one of the main features of the router. Each PoE port is compliant with both IEEE 802.3af and 802.3at. Use the Power over Ethernet Configuration pages to configure:

- [Power over Ethernet | PoE Control Page](#) on Page 59
- [Power over Ethernet | PoE Schedule Page](#) on Page 62
- [Power over Ethernet | PoE Status Page](#) on Page 63

Power over Ethernet | PoE Control Page

This page is used to configure the Power over Ethernet parameters for the ports.

Note: During the PoE operation, the surface accumulates heat and causes the surface temperature to become higher than the ambient temperature. Remember **NOT** to touch device surface during PoE operation.



DO NOT TOUCH THE DEVICE
SURFACE DURING PoE OPERATION
- HIGH POWER FEEDING.

If Forced mode is selected, power is provided even if no Ethernet cable is plugged in. Only use Forced mode if you are attaching a device that is capable of receiving power through its Ethernet connection.

You can use these steps to configure PoE settings. Refer to the following table if you need more detailed information.

1. Select **Enable** from the drop list.
2. Enter an appropriate **Power Budget**, the maximum is 62W.
3. Enter an appropriate **Power Budget Warning Level**.
4. Click the **Apply** button.
5. Select **Enable** for the port or ports that you want to use as PoE ports..
6. Select the **Powering Mode** for the attached device.
7. Enter the power **Budget** for the port. The range is 1 to 31W.
8. Set the port **Priority**.
9. Click the **Apply** button.

PoE Control Help

System Configuration

PoE System Enable ▾

Power Budget (W) :	<input style="width: 90%;" type="text" value="62"/>
Power Budget Warning Level (%) :	<input style="width: 90%;" type="text" value="90"/>

Apply Cancel

Port Configuration

Port	Mode	Powering Mode	Budget(W)	Priority
1	Enable ▾	802.3af ▾	<input style="width: 50%;" type="text" value="15"/>	Critical ▾
2	Disable ▾	<div style="border: 1px solid black; padding: 2px;"> 802.3af 802.3at(2-Event) Forced </div>	<input style="width: 50%;" type="text" value="31"/>	Critical ▾

Apply Cancel

10. If desired, configure **PD Status Detection** for the attached PoE devices.
 - a. Enter the **IP Address** of the device attached to the port.
 - b. Enter the **Cycle Time**, which is the time reserved per duration of the PD reboot. The range is from 10~3600 seconds.
 - c. Click the **Apply** button.

Note: You must **Save** (Page 115) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

PD Status Detection

Enable PD Status Detection

PD	IP Address	Cycle Time(s)	Delete
1	<input style="width: 80%;" type="text" value="10.0.0.116"/>	<input style="width: 50%;" type="text" value="20"/>	<input type="checkbox"/>
2	<input style="width: 80%;" type="text"/>	<input style="width: 50%;" type="text"/>	<input type="checkbox"/>

Apply Cancel

PoE Control	
System Configuration	
PoE System	Enable or Disable the system's PoE power output function. This budget must less than the input power. You must first enable this option before you can configure the PoE characteristics.
Power Budget (W)	This is the maximum output budget of the PoE function. The router supports two IEEE 802.3at PoE ports with a maximum power budget of 62W.
Power Budget Warning Level(%)	The warning level is for system warning to alert the user when the PoE system is drawing power that meets the warning level.

PoE Control (Continued)	
Port Configuration	
Mode	Enable/Disable the port's PoE function.
Powering Mode	IEEE 802.3af, 802.3at(2-event), and forced mode are supported. Forced mode ignores the classification behaviors and delivers power to the connected device. When using Forced mode, be careful and verify that your connected device can support the power that you configure.
Budget (W)	Assign the PoE budget of the port. The valid values range from 1~31W.
Power priority	You can set one of the three levels, Critical, High and low. If the system PoE consumption is over the budget, the PoE system turns off the low priority port first, then high and critical are the last.
PD Status Detection	
Enable PD Status Detection	You can detect the connected PD status. If the connected device is failing, the system resets the PoE of the port as the first step to assist the field engineer.
IP address	The IP address of the connected PD of the port.
Cycle time(s)	This is the time reserved per duration of PD reboot in seconds, the range is from 10~3600. You can measure the PD reboots duration time first. Normally, an IP camera will take at least 40~50 seconds. Once you define this function, the PoE router turns off PoE power when the connected PD does not echo the request. After the cycle time, the PoE router starts the PD again. This function also referred to as link partner line detection (LPLD).
Delete	Click Delete and Apply can delete the settings.

Beta Version

Power over Ethernet | PoE Schedule Page

The scheduling PoE functionality can help you save power and money. You need to configure PoE Scheduling and select a target port manually to enable this function

The Power over Ethernet schedule supports hourly and weekly base PoE schedule configuration.

PoE Schedule Help

PoE Schedule Disable on Port 1

Time	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
01:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
02:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
03:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
04:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
05:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
06:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
07:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
08:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
09:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
17:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply Cancel Refresh

Select the target port and select the time frames, and then click **Apply** to activate the PoE scheduling function. The PoE port works with the predefined behavior and follows the system clock. As this result, be sure the system clock have configured as your local time for the reference of scheduling control.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Power over Ethernet | PoE Status Page

The **PoE Status** page shows the operating status of each PoE Port. The information includes PoE mode, Powering Status, PD class, Power Budget (W), Power Consumption (W), Voltage and Current of the connected device. The following screen illustrates that there is a PoE IP camera on Port 1.

PoE Status

Help

Port	Mode	Status	Class	Budget (W)	Consumption (W)	Voltage (V)	Current (mA)
1	Enable	Powering	Class4	31	3.32	46.8	71.0
2	Disable	Searching	---	---	0.0	0.0	0.0

Refresh

Beta Version

Switch Configuration Pages

The **Switch Configuration** group helps you to enable/disable port status, configure port auto-negotiation, speed, and duplex, flow control, rate limit control and VLAN. It also allows you to view port status and port statistics.

This category includes these pages:

- [Switch Configuration | Port Status Page](#)
- [Switch Configuration | Port Control Page](#)
- [Switch Configuration | VLAN Configuration Page](#)
- [System Configuration | Rate Control Page](#)
- [Switch Configuration | Port Statistics Page](#)

Switch Configuration | Port Status Page

This page displays the current status of the ports.

Port Status

[Help](#)

Port	Link	Speed/Duplex	Flow Control	SFP Vendor	Wavelength	Distance
1	Up	100 Full	Disable	---	---	---
2	Up	1000 Full	Disable	---	---	---
3	Up	1000 Full	Disable	Control	1310 nm	10000 m
4	Down	1000 Full	Disable	---	---	---

[Refresh](#)

Port Status Page	
Link	This is the link status with is either Up or Down.
Speed/Duplex	This is the port speed (10, 100 or 1000) and duplex (Full or half).
Flow Control	The status of flow control.
SFP Vendor	Vendor name of the SFP transceiver connected to the port. Most SFP transceivers provide vendor information, which allows your switch to read it. The web page displays the vendor name, wavelength and distance of all SFP transceiver family. If you see <i>Unknown info</i> , it may mean that the vendor did not provide their information or that the information of their transceiver cannot be read.
Wavelength	The wave length of the SFP transceiver connected to the port.
Distance	The distance of the SFP transceiver connected to the port.

Port Status Page (Continued)	
Refresh	Reloads the all of the port information.

Switch Configuration | Port Control Page

Use this page to configure the router.

Port Control

Port	State	Speed/Duplex	Flow Control
1	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>
2	Enable <input type="button" value="v"/>	AutoNegotiation <input type="button" value="v"/>	Disable <input type="button" value="v"/>
3	Enable <input type="button" value="v"/>	1000 <input type="button" value="v"/>	Disable <input type="button" value="v"/>
4	Enable <input type="button" value="v"/>	1000 <input type="button" value="v"/>	Disable <input type="button" value="v"/>

Port Control Page	
State	Enable or disable the state of this port. The default setting is Enable which means all the ports are workable when you receive the device.
Speed/Duplex	<p>You can configure port speed and duplex mode at each port.</p> <p>Ports 1 and 2: The factory default is AutoNegotiation, it will based on transmission to auto negotiate the speed and duplex mode. You can also select 10 Full, 10 Half, 100 Full or 100 Half.</p> <p>Ports 3 and 4: The ports represent the SFP fiber ports. Factory default is 1000, which means that the port is in Gigabit speed. You will need to configure to 100 if you use 100M SFP transceiver.</p> <p><i>Note: It is necessary to reset system, if the SFP configuration was changed.</i></p>
Flow Control	<p>This enables or disables flow control.</p> <p>Enable means that you need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the router to work.</p> <p>Disable means that you do not need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the router works anyway.</p>

Click the **Apply** button to activate the settings.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Switch Configuration | VLAN Configuration Page

The WR7802-XT supports IEEE 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows a VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame's tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.

VLAN Configuration group enables you to Add/Remove static VLAN, configure Management VLAN ID, Port PVID, Egress parameters and view VLAN table.

VLAN Configuration

[Help](#)

PVID Setting

Port	1	2	3	4
PVID	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<input type="text" value="1"/>

[Apply](#)

Management VLAN ID : (1-4094)

[Apply](#)

Add Static VLAN

VLAN ID	1	2	3	4
<input type="text"/>	<input type="text" value="Untag"/> ▾	<input type="text" value="Untag"/> ▾	<input type="text" value="Untag"/> ▾	<input type="text" value="Untag"/> ▾

[Apply](#)

[Cancel](#)

Static VLAN Overview

Vlan ID	1	2	3	4	Select	Edit
1	Untag	Untag	Untag	Untag	<input type="checkbox"/>	Edit

[Delete Selected](#)

[Delete All](#)

[Refresh](#)

VLAN Configuration Page	
PVID Setting	<p>PVID is the abbreviation of the Port VLAN ID.</p> <p>Enter the port VLAN ID in this field. PVID allows the switches to identify which port belongs to which VLAN.</p> <p>To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The values of PVIDs are from 1 to 4095.</p> <p>1 (default value) and 4095 are reserved and you cannot enter these two PVIDs.</p> <p>Click the Apply button to activate the PVID settings.</p>
Management VLAN ID	<p>The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the router. The default management VLAN ID is 1.</p>
Add Static VLAN	<p>Assign VLAN ID for a new VLAN and specify the egress (outgoing) rule to be Untag or Tag on each port.</p> <p>Untag: Indicates that egress/outgoing frames are not VLAN tagged.</p> <p>Tag: Indicates that egress/outgoing frames are to be VLAN tagged.</p> <p>-- : Not available</p> <p>Press the Apply button to activate settings.</p>
Static VLAN Overview	<p>The table shows static VLAN status.</p> <p>Check Select if you want to use the Delete Selected button to delete the selected entry.</p> <p>Edit: Edit entries for the Route Entry.</p> <p>Delete all: Delete the all entries.</p> <p>Refresh: Reload the table.</p>

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

System Configuration | Rate Control Page

Limit Packet Type and Rate is a form of flow control used to enforce a strict bandwidth limit on a port. You can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types.

Rate Control

Limit Packet Type and Rate

Port	Ingress Rule		Egress Rule	
	Packet Type	Rate (Mbps)	Packet Type	Rate (Mbps)
1	Broadcast Only	10	All	0
2	Broadcast Only	10	All	0
3	Broadcast Only	10	All	0
4	Broadcast Only	10	All	0

Rate Control	
Packet type	You can select the packet type that you want to filter. The packet types of the Ingress Rule listed here include: All , Broadcast Only , Broadcast/Multicast and Broadcast/ Multicast/ Unknown Unicast . The packet types of the Egress Rule (outgoing) only support all packet types.
Rate	This column allows you to manually assign the limit rate of the port. Valid values are from 1Mbps-1000Mbps, and Zero means no limit.
Ingress Rate	Increments of 1Mbps.
Egress Rate	1 Mbps to 100 Mbps, increments of 1Mbps. 100 Mbps to 1000 Mbps, increments of 10Mbps.

Click the **Apply** button to apply the configuration changes.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Switch Configuration | Port Statistics Page

You can use this page to view the port statistics. The statistics that can be viewed include Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision. Rx means the received packet while Tx means the transmitted packets.

Port Statistics

Help

Port	Link	Rx Good	Rx Bad	Rx Abort	Tx Good	Tx Bad	Collision	Select
1	Up	13388234	0	0	6730495	0	0	<input type="checkbox"/>
2	Up	2426433	0	0	4793231	0	0	<input type="checkbox"/>
3	Up	4327807	0	0	8624059	0	0	<input type="checkbox"/>
4	Down	0	0	0	0	0	0	<input type="checkbox"/>

Clear Selected

Clear All

Refresh

Port Statistics	
Port	This is the port identifier.
Link	Indicates the link status, Up or Down.
RX Good	The count of good frames received, which is the total number of received unicast, broadcast, multicast, and pause frames.
RX Bad	The count of bad frames received, which is the total number of undersize, fragment, oversize, jabber, RXErr, and FCSErr frames.
RX Abort	The count of aborted frames received, which is the total number of discarded and filtered frames.
TX Good	The count of good frames transmitted, which is the total number of transmitted unicast, broadcast, multicast, and pause frames.
TX Bad	The count of FCSErr frames transmitted.
Collision	The count of collision frames. Collision is the collisions frames (including: single, multiple, excessive, and late collisions frames).
Select	Click Select on a row (port) and you can click Clear Selected to delete the selected entry or entries.
Clears All	Click this button to clear all information from the table.
Refresh	Reload to refresh the counts.

Note: If you see many Bad, Abort or Collision counts increased, that may mean your network cable is not properly connected, the network performance of the port is poor, and so forth. Check your network cable, Network Interface Card of the connected device, the network application, or reallocate the network traffic.

Traffic Prioritization Pages

Quality of Service (QoS) provides a traffic prioritization mechanism which allows users to deliver better service to certain flows. QoS can also help to alleviate congestion problems and ensure high-priority traffic is delivered first. This subsection allows you to configure Traffic Prioritization settings for each port with regard to setting priorities. The WR7802-XT supports 4 physical queues, weighted fair queuing (WRR) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

This group includes these page:

- [Traffic Prioritization | QoS Setting Page](#) on Page 70
- [Traffic Prioritization | CoS-Queue Mapping Page](#) on Page 71
- [Traffic Prioritization | DSCP-Queue Mapping Page](#) on Page 72

Traffic Prioritization | QoS Setting Page

The **QoS Setting** page provides a method to queue scheduling: You can select one of the Queue Scheduling rules.

QoS Setting Help

Queue Scheduling

8,4,2,1 weighted fair queuing scheme
 Strict priority scheme

Port Setting

Port	CoS	Trust Mode
1	0	CoS Only
2	0	CoS Only
3	0	CoS Only
4	0	CoS Only

Apply Cancel

QoS Setting	
8,4,2,1 weighted fair queuing scheme	This is also known as WRR (Weight Round Robin). The WR7802-XT follows the 8:4:2:1 rate to process the packets in a queue from the highest priority to the lowest. For example, the system processes 8 packets with the highest priority in the queue, 4 with the middle priority, 2 with low priority, and 1 with the lowest priority at the same time.
Strict priority scheme	Packets with higher priority in the queue are always processed first, as long as there is no packet with a higher priority.

QoS Setting (Continued)	
Port Settings	
CoS	This column indicates the default port priority value for untagged or priority-tagged frames. When the WR7802-XT receives the frames, it attaches the value to the CoS field of the incoming VLAN-tagged packets. You can select 0,1,2,3,4,5,6 or 7 for the port.
Trust Mode	<p>Indicates the Queue Mapping types for you to select.</p> <p>CoS Only: Port priority only follows CoS-Queue Mapping that you have assigned.</p> <p>DSCP Only: Port priority only follows DSCP-Queue Mapping that you have assigned.</p> <p>CoS first: Port priority follows CoS-Queue Mapping first, and then the DSCP-Queue Mapping rule. The default priority type is CoS First. The system provides a default CoS-Queue table for which you can refer to the next command.</p> <p>DSCP first: Port priority follows DSCP-Queue Mapping first, and then the CoS-Queue Mapping rule.</p>

After configuration, press **Apply** to update the configuration changes.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Traffic Prioritization | CoS-Queue Mapping Page

Use this page is to change the CoS values to Physical Queue mapping table. Since the switch fabric of the WR7802-XT supports four physical queues, **Lowest**, **Low**, **Middle**, and **High**.

You should therefore assign how to map CoS value to the level of the physical queue. You can freely assign the mapping table or follow the suggestion of the IEEE 802.1p standard.

CoS values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS values 6 and 7 are mapped to physical Queue 3, the high physical queue.

CoS-Queue Mapping Help

CoS	0	1	2	3	4	5	6	7
Queue	1 ▾	0 ▾	0 ▾	1 ▾	2 ▾	2 ▾	3 ▾	3 ▾

Note : Queue 3 is the highest priority queue in using Strict Priority scheme.

Apply
Cancel

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Traffic Prioritization | DSCP-Queue Mapping Page

Use this page is to change DSCP (Differentiated Services Code Point) values for the Physical Queue mapping table. The switch fabric of the WR7802-XT supports 4 physical queues, Lowest, Low, Middle and High. You should therefore assign how to map DSCP value to the level of the physical queue. You can freely change the mapping table to follow the Upper Layer 3 switch or routers' DSCP setting.

DSCP-Queue Mapping

Help

DSCP	0	1	2	3	4	5	6	7
Queue	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾
DSCP	8	9	10	11	12	13	14	15
Queue	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾
DSCP	16	17	18	19	20	21	22	23
Queue	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾	0 ▾
DSCP	24	25	26	27	28	29	30	31
Queue	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾	1 ▾
DSCP	32	33	34	35	36	37	38	39
Queue	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾
DSCP	40	41	42	43	44	45	46	47
Queue	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾	2 ▾
DSCP	48	49	50	51	52	53	54	55
Queue	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾
DSCP	56	57	58	59	60	61	62	63
Queue	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾	3 ▾

Note : Queue 3 is the highest priority queue in using Strict Priority scheme.

Apply

Cancel

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Multicast Filtering Pages

For multicast filtering, the WR7802-XT uses IGMP Snooping technology. IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for an Internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the Internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data. Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership. In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

Multicast Filtering	
Query	A message sent from the querier (an IGMP router or a switch) that asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You will see the information of the IGMP Snooping function in this section, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255. In this subsection, Force filtering can determined whether the switch flooding unknown multicast or not. Following web page are included in this group:

- [Multicast Filtering | IGMP Snooping Page](#) on Page 74
- [Multicast Filtering | IGMP Query Page](#) on Page 75

Multicast Filtering | IGMP Snooping Page

Use this page is to enable the IGMP Snooping feature, assign IGMP Snooping for specific VLAN, and view IGMP Snooping table from dynamic learnt or static manual key-in.

IGMP Snooping Help

Enable IGMP Snooping Apply

VLAN Overview

Vlan ID	IGMP Snooping	Select
1	Disabled	<input type="checkbox"/>

Select All

Enable
Disable

IGMP Snooping Table

IP Address	VID	1	2	3	4

Refresh

IGMP Snooping	
Enable IGMP Snooping	Click the check box and the Apply button to enable the IGMP Snooping feature.
VLAN Overview	You can assign IGMP Snooping to for specific VLAN. You can enable IGMP Snooping for some VLANs so that some of the VLANs will support IGMP Snooping and others will not. Click the check box in the Select column and then select the Enable or Disable button.
IGMP Snooping Table	The table shows the multicast group IP Address, VID and member ports of the current working multicast stream in this device.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Multicast Filtering | IGMP Query Page

Use this page to configure the IGMP Query feature. Since the router can only be configured by member ports of the management VLAN, IGMP Query can only be enabled on the management VLAN.

If you want to run IGMP Snooping feature in several VLANs, you should check whether each VLAN has its own IGMP Querier first. The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.

IGMP Query

Help

IGMP Query on Management VLAN

Version :	Disable ▾
Query Interval(s):	125
Query Maximum Response Time(s):	10

Apply

Cancel

IGMP Query	
IGMP Query Version	You can select V1, V2 or Disable. V1 means IGMP V1 General Query. V2 means IGMP V2 General Query. The query is forwarded to all multicast groups in the VLAN. Disable allows you to disable IGMP Query.
Query Interval(s)	The period of query sent by querier. This value determines how frequently in seconds IGMP query messages are sent out. This value should be greater than or equal to the Query Maximum Response Time(s) . Valid values are 1 to 65535.
Query Maximum Response Time	The span querier detected to confirm there are no more directly connected group members on a LAN. Valid values are 1 to 25. Once you finish configuring the settings, click the Apply button to apply your configuration changes.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Network Redundancy Pages

It is critical for industrial applications that network remains non-stop. The WR7802-XT supports STP, RSTP and Redundant Ring technology with these web pages:

- [Network Redundancy | STP Configuration Page](#) on Page 77
- [Network Redundancy | STP Port Configuration Page](#) on Page 79
- [Network Redundancy | STP Information Page](#) on Page 80
- [Network Redundancy | Redundant Ring Configuration Page](#) on Page 81
- [Network Redundancy | Redundant Ring Information Page](#) on Page 82
- [Network Redundancy | Redundant Gateway Page](#) on Page 83
- [Network Redundancy | VRRP Page](#) on Page 85

If you are unsure as to whether to configure Redundant Gateway or VRRP (Virtual Router Redundant Protocol) to provide a gateway failure backup mechanism, you may want to review the following information.

- *VRRP* requires all gateway participants to run VRRP protocol and it detects a gateway failure using IP multicast.
- *Redundant Gateway* detects a gateway failure with Redundant Ring status and ICMP packets.

Since VRRP and Redundant Gateway use different protocols, you can use one or the other but not both.

	Redundant Gateway	VRRP
Protocol	RocketLinx Redundant Ring	IEEE Standard
Role	One master and all other routers are backups	One master and all other routers are backups
Instance	One ring group	Multiple VRRP groups with a maximum of 5
How it is implemented	RocketLinx with the smallest ARP Miss Count on the Redundant Gateway web page	RocketLinx with the highest priority on the VRRP web page
IP	Real router IP	Virtual IP or real router IP
Detection Interval	Configurable ping loss, the default is 5	3 Advertise Intervals, the default is 1 second
Ring Recovery Time	Failover time 5ms and 0 restoration time	

Network Redundancy | STP Configuration Page

Use this page to select the STP mode and configure the global STP/RSTP Bridge Configuration.

STP Configuration

STP Mode ▼

Bridge Configuration

Bridge Address	<input type="text"/>
Bridge Priority	<input type="text" value="0"/> ▼
Max Age	<input type="text" value="6"/> ▼
Hello Time	<input type="text" value="1"/> ▼
Forward Delay	<input type="text" value="4"/> ▼

STP Configuration	
STP Modes	You can choose from STP , RSTP and Disable . You must select the STP Mode for your system first.
Bridge Configuration	
Bridge Address	This shows the router's MAC address.
Bridge Priority (0-61440)	<p>RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of the bridge priority and the bridge MAC address. The bridge with the highest priority becomes the highest bridge ID.</p> <p>If all the bridge IDs have the same priority, the bridge with the lowest MAC address will then become the root bridge.</p> <p><i>Note: The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority. Ex: 4096 is higher than 32768. Note: The Web GUI allows you to select the priority number directly. If you configure the value through the CLI or SNMP, you may need to type the value directly. Make sure that you follow the $n \times 4096$ rules for the Bridge Priority.</i></p>
Max Age (6-40)	<p>Enter a value from 6 to 40 seconds. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.</p> <p>If the device is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then device reconfigures itself as a root bridge.</p> <p>Once two or more devices on the network are recognized as a root bridge, the devices renegotiates to set up a new spanning tree topology.</p>

STP Configuration (Continued)	
Hello Time (1-10)	<p>Enter a value from 1 to 10 seconds. This is a periodic timer that drives the router to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status.</p> <p>The root bridge of the spanning tree topology periodically sends out a hello message to other devices on the network to check if the topology is healthy. The hello time is the amount of time the root has waited during sending hello messages.</p>
Forward Delay Time (4-30)	<p>Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state. This is the amount of time the device waits before checking to see if it should be changed to a different state.</p>

Once you have completed your configuration, click on **Apply** to apply your settings.

Note: You must observe the following rule to configure Hello Time, Forwarding Delay, and Max Age parameters.

$$2 \times (\text{Forward Delay Time} - 1 \text{ sec}) \leq \text{Max Age Time} \leq 2 \times (\text{Hello Time value} + 1 \text{ sec})$$

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Beta Version

Network Redundancy | STP Port Configuration Page

The Spanning Tree Protocol as defined by IEEE 802.1D provides loop free topologies for any Local Area Network (LAN). The Rapid Spanning Tree Protocol as defined by IEEE 802.1w is an evolution of the STP that provides faster spanning tree convergence after a topology change. This page allows you to configure the port parameter after you enable STP or RSTP.

STP Port Configuration

Port	STP State	Path Cost	Port Priority
1	Enable <input type="button" value="v"/>	20000	128 <input type="button" value="v"/>
2	Enable <input type="button" value="v"/>	20000	128 <input type="button" value="v"/>
3	Enable <input type="button" value="v"/>	20000	128 <input type="button" value="v"/>
4	Enable <input type="button" value="v"/>	20000	128 <input type="button" value="v"/>

STP Port Configuration	
Port	This is the port number.
STP State	Enable or Disable the STP/RSTP of the port. The default is Enabled . Use the STP Configuration page to enable and set the STP or RSTP mode.
Path Cost	Enter a number between 1 and 200,000,000. This value represents the cost of the path to the other bridge from the transmitting bridge at the specified port. The default value for 100Mbps ports is 200000. The default value for 1000Mbps ports is 20000.
Priority	Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Network Redundancy | STP Information Page

This page allows you to see the information of the root switch and port status.

Root Information: You can see Root Bridge Address, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

Port Information: You can see Port Role, Port State, Path Cost and Port Priority of the STP ports.

STP Information

Help

Root Information

Root Address	00c0.4e2c.006c
Root Priority	32768
Root Port	3
Root Path Cost	420000
Max Age	20 second(s)
Hello Time	2 second(s)
Forward Delay	15 second(s)

Port Information

Port	Role	Port State	Path Cost	Port Priority
1	Designated	Forwarding	20000	128
2	Designated	Forwarding	20000	128
3	Root	Forwarding	20000	128
4	Disabled	Blocking	20000	128

Refresh

Beta Version

Network Redundancy | Redundant Ring Configuration Page

Use this page to create new Ring configurations and edit existing Ring configurations. Typically, managed switches /routers are connected in series and the last switch is connected back to the first one. In such connection, you can implement Redundant Ring technology.

To create a new ring ID, type a Ring ID and Name and select the characteristics from the table, click **Apply** when done.

Note: You must **Save** (Page 115) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Redundant Ring Configuration Help

Add New Ring

Ring ID	Name	Priority	Ring Port 1	Path Cost	Ring Port 2	Path Cost	Status
<input type="text"/>	<input type="text"/>	128	Port 1 ▼	128	Port 2 ▼	128	Disable ▼

Apply
Cancel

Ring Configuration

ID	Name	Priority	Ring Port 1	Path Cost	Ring Port 2	Path Cost	Status	Select	Edit
1	Ring1	128	Port 3	128	Port 4	128	Disable	<input type="checkbox"/>	Edit

Delete Selected
Delete All
Refresh

Redundant Ring Configuration	
Add New Ring:	
Ring ID	Ring1 with an Ring ID of 1 is created by default and cannot be deleted. The valid range is from 0 to 31 with a maximum 32 rings.
Name	Type the name of the Ring. If it is not filled in when creating, it is automatically named Ring and the Ring ID number, for example: Ring2.
Priority	The switch with highest priority (highest value) is automatically selected as the Ring Master. If all of the switches have the same priority, then the switch with the highest MAC address is selected as the Ring Master.
Ring Port 1/ Ring Port 2	In a Ring, two ports should be selected to be Ring Ports. For the Ring Master, one of the ring ports becomes the forwarding port and the other one becomes the blocking port.
Path Cost	Change the Path Cost of Ring Port. If this switch is the Ring Master of a Ring, then it determines the blocking port. The Port with higher Path Cost in the two ring ports becomes the blocking port, If the Path Cost is the same, the port with larger port number becomes the blocking port.
Status	To enable/disable the Ring. Remember to enable the ring after you add it.
Select	Click the Select check box if you want to Edit or delete the selected row.

Network Redundancy | Redundant Ring Information Page

The table on the Redundant Ring Information page shows the Multiple Super Ring information.

Redundant Ring Information

Help

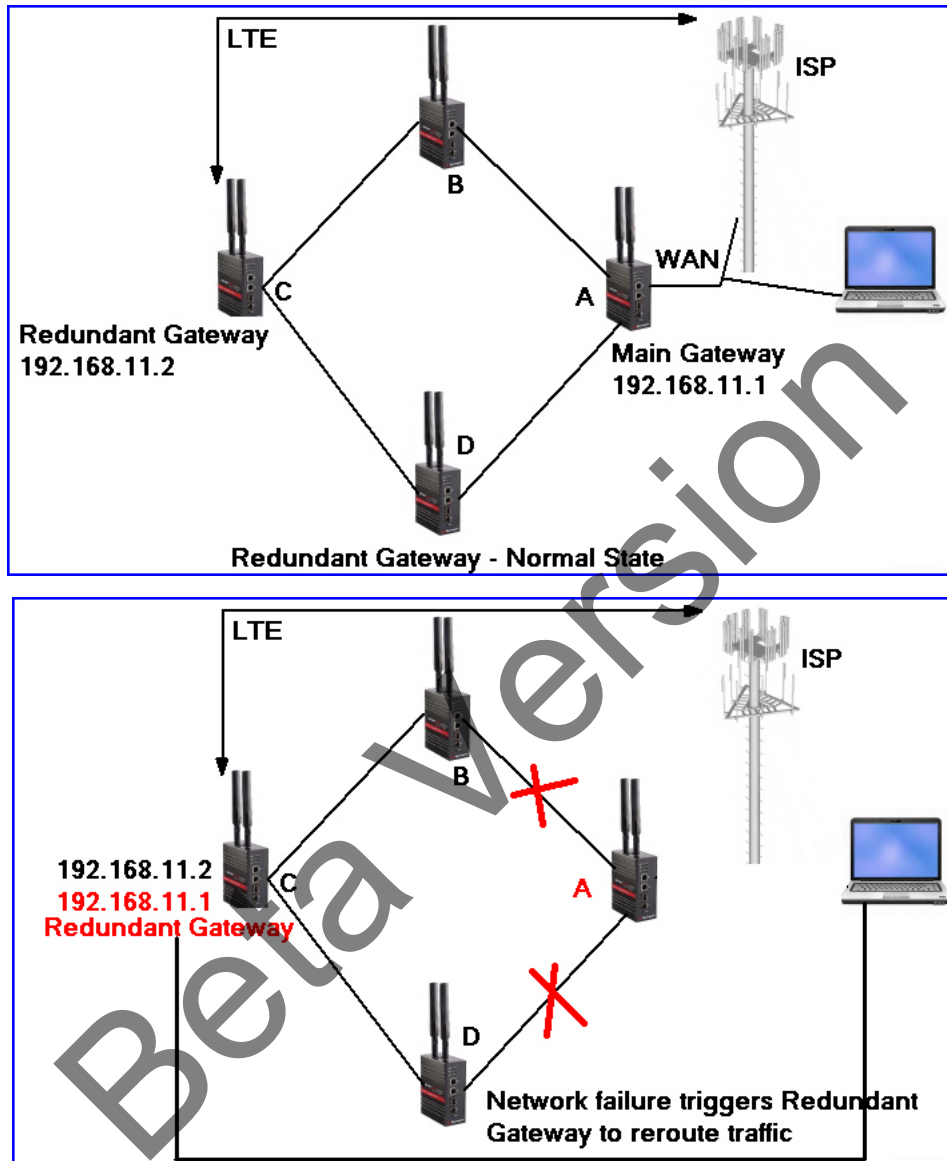
ID	Role	Status	RM MAC	Blocking Port	Role Transition count	Ring State Transition count
1	Disabled	Abnormal	0000.0000.0000	---	0	0

Refresh

Redundant Ring Information	
ID	This is the Ring ID.
Role	This device is the RM, not the Ring Master (nonRM), Emigrant or Disabled.
Status	If this field is Normal which means the redundancy is approved. If any one of the link in this Ring is broken, then the status will be Abnormal .
RM MAC	The MAC address of Ring Master of this Ring. It helps to find the redundant path.
Blocking Port	This field shows which is blocked port of RM.
Role Transition count	This means how many times this switch has changed its Role from nonRM to RM or from RM to nonRM.
Ring State Transition count	This number means how many times the Ring status has been transformed between Normal and Abnormal state.

Network Redundancy | Redundant Gateway Page

Redundant Gateway is a Ring redundancy feature that you can implement for backup if two links fail in a Ring.



In the images above, the Redundant Ring, IP:192.168.11.1 is the main gateway, and there are other devices in the same ring which provides a Cellular interface for external network transmission.

If there are two link failures, this would mean that the other devices cannot transmit data to the external network. You would manually need to change the settings on each device to recover external access.

To solve this problem, you can use the *Redundant Gateway*. If two links fail, the Redundant Gateway device creates an internal virtual gateway (the same as original main gateway) so for other devices, the main gateway still exists and these devices can transmit data to external network via Cellular interface of the Redundant Gateway device.

Redundant Gateway Help

Status:	Disabled
Redundant gateway:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Gateway Address:	<input type="text" value="0.0.0.0"/>
Ring ID :	<input type="text" value="1"/> (1-31)
ARP Miss Count (Default:5):	<input type="text" value="5"/> (0-65535)

Apply Cancel

Redundant Gateway	
Status	Backup or Master. Backup mode means that the Ring status is normal. If two links fail, the Redundant Gateway function is triggered and it is changed to Master mode.
Redundant gateway	You can Enable or Disable the Redundant Gateway function.
Gateway Address	Type the IP address of the main gateway of the Redundant Ring.
Ring ID	The redundant gateway checks the ring status of this Ring ID.
ARP Miss Count(Default:5)	Type the number of ARP missed packets count. When Ring status is abnormal, system transmits ARP packets in the Ring to check whether the main gateway still alive or not. If the ARP miss count is higher than the value that you set, the Redundant Gateway status changes to Master and replaces the original gateway.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Network Redundancy | VRRP Page

The WR7802-XT provides the VRRP (Virtual Router Redundant Protocol) feature, which allows the host to continuously direct traffic to the default gateway without changing the default gateway configuration.

In a VRRP domain, the VRRP device should have the same Virtual Router ID, Virtual IP and Advertisement Interval time and choose one of the VRRP devices as the VRRP Master. The other becomes the VRRP Backup that takes over the VRRP Master immediately.

VRRP

Enable VRRP

Virtual Router ID:	<input type="text"/>
Virtual IP:	<input type="text"/>
Priority:	<input type="text"/>
Adv. Interval:	<input type="text"/>
Preempt Mode:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Virtual Router Interface Status

Select	Virtual ID	Virtual IP	Priority	Adv. Interval	Preempt	VRRP Status	VRRP Mac	Edit
<input type="checkbox"/>								

VRRP	
Virtual Router ID	This is a virtual ID range from 1-255. The device within the same VRRP domain should have the same Virtual Router ID.
Virtual IP	This is the virtual IP of the VRRP domain. This is the Gateway IP of the clients.
Priority	VRRP priority is 0 to 255. The greater the number, the higher the priority. In a VRRP domain, the VRRP device should have the same Virtual Router ID and Virtual IP and choose who should be the VRRP Master. The device with the highest priority is selected as the VRRP Master. The priority setting can be manually changed and the range is 1 to 254. Priority 0 is reserved for special uses and priority 255 for the Virtual owner.
Adv. Interval	This field indicates how often the VRRP devices exchange the VRRP settings. The time unit is seconds and the default setting is 1 second. In a VRRP domain, the VRRP devices should have the same Adv. Interval as well.

VRRP (Continued)	
Preempt Mode	<p>If the VRRP Master link fails, the VRRP Backup takes over its job immediately. However, if the VRRP master link is recovered, who should be the Master?</p> <p>The preempt mode determines whether the VRRP master should be recovered or not. If the Preempt is Enabled and the interface is the VRRP Master, the interface is recovered.</p> <p>If the Preempt is Disabled and the interface is VRRP Master, there is no change while the link is recovered. The VRRP Backup acts as the Master before restarts the device.</p>

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Beta Version

Cellular Pages

The Cellular feature set pages allow you to see the 3G/LTE Status, configure the Basic Setting, SIM Security, Connection Watchdog, Debug Mode and Mobile Manager Server Settings.

- [Cellular | Cellular Basic Settings Page](#) on Page 87
- [Cellular | SIM Security Settings Page](#) on Page 89
- [Cellular | Mobile Manager Settings Page](#) on Page 90

Cellular | Cellular Basic Settings Page

The WR7802-XT supports a dual SIM socket. You can select SIM 1 or SIM 2 as the startup SIM socket, and configure whether the second SIM socket will function redundantly with each other or not.

For Cellular SIM settings, normally, you can connect the Cellular Gateway to the ISP Cellular network without configuring Cellular settings. However, in some countries, before the Cellular gateway can access the ISP's Cellular data network, you may need to enter the APN settings, User Name, Password, Authentication type on the device. You can use this page to configure the parameters.

Cellular Basic Settings

Help

Disable Cellular Interface

SIM Selection:	<input checked="" type="radio"/> SIM1 <input type="radio"/> SIM2
Cellular Redundant:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
SIM1 Settings	
APN:	<input type="text" value="mw01.vzwstatic"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Authentication Type:	<input checked="" type="radio"/> CHAP <input type="radio"/> PAP
SIM2 Settings	
APN:	<input type="text" value="teammobile"/>
User Name:	<input type="text"/>
Password:	<input type="text"/>
Authentication Type:	<input checked="" type="radio"/> CHAP <input type="radio"/> PAP
Connection	
Connect:	Disconnect

Apply
Cancel

Cellular Basic Settings	
Disable Cellular Interface	You can disable the Cellular interface manually.
SIM Selection	<p>SIM 1 means the SIM Socket 1, you can see the ID in the front panel. SIM 2 means the SIM Socket 2.</p> <p>Select one of SIM sockets as the startup SIM socket. SIM 1 is the default settings. Make sure that you insert the SIM card to the SIM socket you select.</p> <p>Note: <i>The LTE module only can check the selected SIM slot. Thus the unselected SIM2 slot shows as inserted because the SIM holder is inserted.</i></p>
Cellular Redundant	<p>If you enable Cellular Redundant, you must insert both SIM cards into the two SIM sockets before powering on the system or you should reboot the WR7802-XT.</p> <p>If enabled, the two SIMs are redundant with each other if the primary Cellular connection fails. The selected SIM number is the primary SIM, the other one is backup SIM. The redundant timer is based on your settings of Reconnection Delay and Retries.</p> <p>Note: <i>Adjust the Reconnection Delay and Retires based on your application, if you requests shorter redundant time, you can modify the delay time or retires times.</i></p>
APN	<p>Every ISP has a specific APN (Access Point Name) assigned to its Cellular network. If necessary, check with your ISP to determine the APN and correctly enter the value on this page.</p> <p>If you fail to connect to the Cellular network, this should be the first setting that you verify.</p>
User Name	The user name for the Cellular connection. If applicable, this is normally provided by your ISP.
Password	The password for the Cellular connection. If applicable, this is normally provided by your ISP.
Authentication Type	You can select CHAP or PAP per your ISP request. If applicable, this is normally is provided by your ISP.
Connection	You can select Connect to re-connect the Cellular connection of the selected SIM card. This progress may take 30 seconds. You will see a pop-up message notifying that you need to wait 30 seconds.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Cellular | SIM Security Settings Page

This page allows you to assign the SIM security. If you (or ISP) already apply the PIN number to your SIM card, you need to configure the correct PIN number for the WR7802-XT. After correctly enter the PIN number, you can start the Cellular connection or change the new PIN settings.

SIM Security Settings Help

SIM	1
SIM Status	SIM OK
Number of Retries Remaining:	3
SIM1 PIN:	<input type="text"/>
Confirm SIM1 PIN:	<input type="text"/>
Remember PIN:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
PIN Protection: Disable	Disable PIN ▼

Apply Cancel

SIM Security Settings	
SIM	The currently selected SIM slot.
SIM Status	The current SIM status of the selected SIM slot.
Number of Retries Remaining	Displays how many retries of entering the PIN on a SIM card before it locks out.
SIM PIN	This is a pin code that locks the SIM card until you enter the correct code. Use the pin to protect your account. The default code is set by the Service Provider.
Remember PIN	Save the PIN code on this device. The system uses the saved PIN code to unlock the SIM card automatically. Make sure that you use the Enable PIN pin protections with this option.
PIN Protection	The following options are available: <ul style="list-style-type: none"> Disable PIN: The PIN code is removed from the SIM card. Enable PIN: Select this option when your SIM card is set with a PIN code. Change PIN: Select this option when you need to change the PIN code on your SIM card.

Press **Apply** to activate the new settings.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Cellular | Mobile Manager Settings Page

The Mobile Manager Utility can help you collect IP addresses after you install the WR7802-XT in the remote field site.

Refer to [Mobile Manager Utility](#) on Page 117 for information about downloading the Mobile Manager and how to use it.

The device acts as the Cellular router device, you can assign the target Server IP Address and specific port (TCP port), then the device will automatically update the current IP address and the new IP address once it is changed to the server.

Mobile Manager Settings Help

Server:	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled	
Server Address:	<input style="width: 100%;" type="text" value="0.0.0.0"/>	
Server Port:	<input style="width: 80%;" type="text" value="2310"/>	(1-65535)
Control Port (Auto:0):	<input style="width: 80%;" type="text" value="0"/>	(0-65535)

Apply
Cancel

Mobile Manager	
Server	You can Enable or Disable this function. The default value is disabled.
Server Address	Enter the Mobile Manager's IP address in this field, which must be a public IP address (accessible through the Internet).
Server Port	The device updates information to server through this port. You can assign specific TCP port number.
Control Port	The Control Port (TCP port) allows you to connect to the device. You can assign specific TCP port number.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

VPN Pages

The VPN feature set of web pages allow you to configure the WR7802-XT as a VPN client that you want to connect to a VPN server. It also allows you to configure one-to-one VPN Server service for one VPN client. You can use both the OpenVPN Server and OpenVPN Client pages to build the one-to-on connection between two devices.

OpenVPN is a full-featured SSL VPN:

- Implements OSI Layer 2 or 3 secure network extensions using the industry standard SSL/TLS protocol.
- Supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials.
- Allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface.

The first step to building an OpenVPN 2.x configuration is to establish a PKI (public key infrastructure). PKI consists of a separate certificate (also known as a public key) and private key for the server and each client, and a master Certificate Authority (CA) certificate and key that are used to sign each of the server and client certificates.

In static encryption mode, each VPN client shares the same static key with OpenVPN server.

In TLS encryption mode, each VPN client needs 3 keys, while VPN server needs 4 keys. The description of the 7 keys listed below.

Filename	Needed By	Purpose	Secret
ca.crt	Server and All Clients	Root CA Certificate	No
ca.key	Key Signing Machine Only	Root CA Key	Yes
dh{n}.pem	Server Only	Diffie Hellman Parameters	No
server.crt	Server Only	Server Certificate	No
server.key	Server Only	Server Key	Yes
client.crt	Client Only	Client1 Certificate	No
client.key	Client Only	Client Key	Yes

If the WR7802-XT acts as an OpenVPN client the **ca.crt**, **client.crt** and **client.key** are needed to establish the OpenVPN tunnel as the OpenVPN client.

Note: The file names of these keys are pre-defined and cannot be changed.

Use the **VPN | VPN Certificate** web page to upload these keys. Import the keys one by one on the page. In addition, use this page to delete old certificates. Refer to [VPN | VPN Certificate Page](#) on Page 98.

Use the **VPN | OpenVPN Client** web page to configure the OpenVPN client ([VPN | OpenVPN Client Settings Page](#) on Page 93).

Note: The settings should be consistent with OpenVPN server.

VPN | VPN Status Page

The **VPN Status** page provides: OpenVPN Client Information, OpenVPN Server Information, and IPsec Information.

VPN Status

Help

VPN Status	
OpenVPN Client Information	
Enabled	<ul style="list-style-type: none"> yes: The VPN function is enabled. no: The VPN function not enabled.
Connection Status	<ul style="list-style-type: none"> Connected: The VPN connection is successfully connected. Disconnected: The VPN has not connected.
Remote Server IP	The remote server IP displays after the VPN client connection is successful.
Tx / Rx Bytes	The transmission data volume in bytes displays <i>after</i> the VPN client connects.
OpenVPN Server Information	
Enabled	<ul style="list-style-type: none"> yes: The VPN function is enabled. no: The VPN function not enabled.
Connection Status	<ul style="list-style-type: none"> Connected: The VPN connection is successfully connected. Disconnected: The VPN has not connected.
Tx / Rx Bytes	The transmission data volume in bytes displays <i>after</i> the VPN client connects.
IPsec Information	
Enabled	<ul style="list-style-type: none"> yes: The VPN function is enabled. no: The VPN function not enabled.
Connection Status	<ul style="list-style-type: none"> Connected: The VPN connection is successfully connected. Disconnected: The VPN has not connected.
Left IP/ Right IP	The IP address of IPsec's left and right endpoint displays <i>after</i> the VPN connects.
Tx / Rx Bytes	The transmission data volume in bytes displays <i>after</i> the VPN client connects.

OpenVPN Client Information

Enabled	no
Connection Status	Disconnected

OpenVPN Server Information

Enabled	no
---------	----

IPsec Information

Enabled	no
Connection Status	Disconnected

Refresh

Note: Click the **Refresh** button to update the information on the page.

VPN | OpenVPN Client Settings Page

Use this page to configure the OpenVPN client settings. For the WR7802-XT to act as the VPN client, it must match the VPN server settings for most parameters. Check with the administrator of the VPN server to determine the parameters for this web page.

OpenVPN Client Settings Help

Enable OpenVPN Client Connection

Encryption Mode :	<input checked="" type="radio"/> Static <input type="radio"/> TLS	
Server Address (1) :	<input type="text" value="192.168.10.1"/>	(IP or Domain Name)
Server Address (2) :	<input type="text" value="0.0.0.0"/>	
Port :	<input type="text" value="1194"/>	(1-65535)
Tunnel Protocol :	UDP ▾	
Encryption Cipher :	Blowfish CBC ▾	
Hash Algorithm :	SHA1 ▾	
ping-timer-rem :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
persist-tun :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
persist-key :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Use LZO Compression :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Keepalive :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Ping Interval :	<input type="text" value="10"/>	(1-99999 seconds)
Retry Timeout :	<input type="text" value="60"/>	(1-99999 seconds)
nobind :	<input checked="" type="checkbox"/>	
ifconfig :	Local : <input type="text" value="10.8.0.2"/>	Remote : <input type="text" value="10.8.0.1"/>
Route :	IP : <input type="text" value="0.0.0.0"/>	MASK : <input type="text" value="0.0.0.0"/>
Enable NAT :	<input type="checkbox"/>	
Save Log File :	<input type="button" value="Save..."/>	

OpenVPN Client Settings	
Encryption Mode	Select the encryption mode: Static or TLS . <ul style="list-style-type: none"> • Static: Use a pre-shared static key. • TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server IP (1)	Enter the IP address of the remote VPN server.
Server IP (2)	Optionally, enter the second IP address of the remote VPN server.

OpenVPN Client Settings (Continued)	
Port	Enter the port number that your VPN service uses. <i>Note: You may need check your VPN server to verify the port settings.</i>
Tunnel Protocol	Select TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish or AES .
Hash Algorithm	Select the hash algorithm from these selections: SHA1 , SHA256 , SHA512 , and MDS .
Ping-timer-rem	Select enable or disable this function to prevent unnecessary restarts of the server/client when the network fails. The default is Enable .
Persist-tun	Select enable or disable the persist-tun function that keeps tun(Layer 3)/ tap(Layer 2) device linked up after the Keepalive timeout occurs. The default value is Enable .
Persist-key	Select enable or disable the persist-key function that keeps the first key to use if the VPN restarts after the Keepalive timeout occurs. The default value is Enable .
Use LZO Compression	You can choose to select LZO Compression or not. This function compresses data to decrease the traffic but it also needs more CPU. The default value is Disable .
Keepalive	Select enable or disable the keepalive function, which is used to detect the status of connection. The default value is Enable .
Ping Interval	Enter the ping interval. The range is from 1~99999 seconds.
Retry Timeout	Enter the retry timeout. The range is from 1~99999 seconds.
nobind	If nobind is enabled, the VPN client does not need to bind to a specific local port number.
ifconfig	Enter the tunnel IP address that VPN should use.
Route	Enter the route IP and MASK. This is the target IP domain you can access through the VPN tunnel.
Enable NAT	Enable NAT (Network Address Translation).
Save Log File	Save an OpenVPN Client log file.

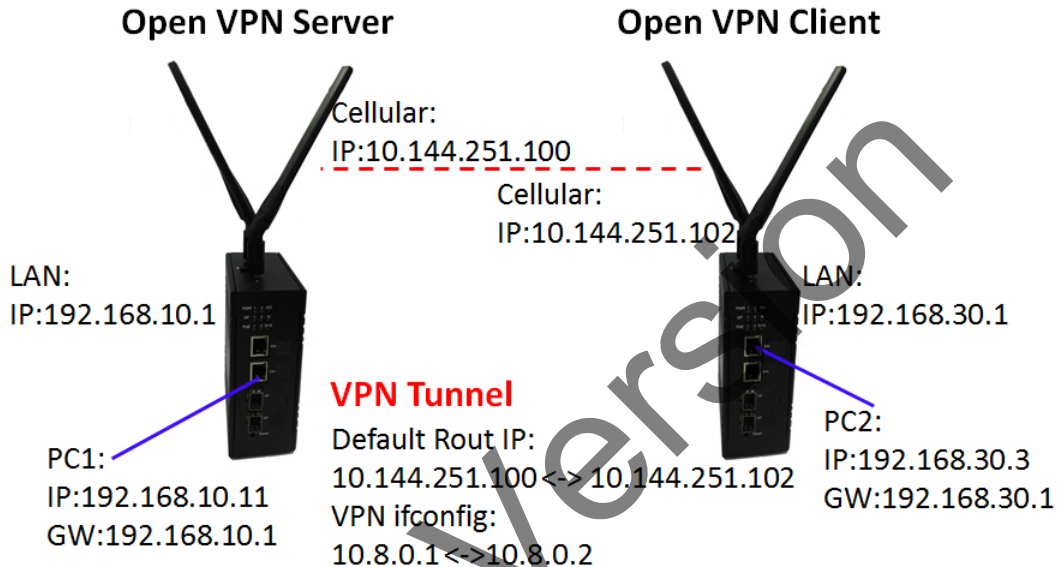
Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

VPN | OpenVPN Server Settings Page

To help you easier create the One-to-One secure M2M (machine to machine) connection for remote devices. The WR7802-XT supports both OpenVPN Server and OpenVPN Client. The server configuration allows you to configure the secure M2M connection for one remote client.

The following image illustrates a simple test setup for your reference. The red color line becomes a VPN tunnel and the transmission data are secured. Before configuration, you need to have the IP plan of the two sites and the routing/VPN paths.

Configure the device as Router mode and give the Ethernet ports specific IP as the default gateway for the connected devices (for example: PCs). For VPN Tunnel, you can choose Cellular interface. Enter the connected IP in the **ifconfig** field and apply/save the settings.



You can use the following steps to create the one-to-one VPN Tunnel:

1. Define the IP of both ends and secure tunnel.
2. Select the general VPN settings:
 - a. Encryption Mode, Port, Tunnel protocol (required)
 - b. Select the Encryption Cipher, Hash Algorithm (required)
 - c. Keepalive, Ping Interval, Retry Timeout (optional)
3. Enter the ifconfig / Route of the tunnel and both ends:
 - a. Tunnel: ifconfig (VPN Tunnel)
 - b. Route: Target Route behind the Client/Server
4. Generate a key and upload the key using the **VPN | VPN Certificate** web page ([VPN | VPN Certificate Page](#) on Page 98).

Note: Generate the key with the VPN Server or 3rd party key generation tool.
5. Enable VPN and **Apply** to activate.
6. Check the status.

7. Save Settings

OpenVPN Server Settings	
Encryption Mode	Select the encryption <ul style="list-style-type: none"> • Static: Use a pre-shared static key. • TLS: Use SSL/TLS + certificates for the authentication and key exchange.
Port	Enter the port number that your VPN service uses.
Tunnel Protocol	You can choose use to TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish to AES .
Hash Algorithm	Select the hash algorithm: SHA1 , SHA256 , SHA512 , or MD5 .
Ping-timer-rem	Select to enable or disable the ping-timer-rem function, which prevents unnecessary restarts at the server/client when the network fails.
Persist-tun	Select to enable or disable the persist-tun function, which keeps the tun(Layer 3)/tap(Layer 2) device linked up after the Keepalive timeout occurs. The default value is Enable .
Persist-key	Select to enable or disable the persist-key function, which keeps the first key to use if VPN restart after Keepalive timeout, default value is Enable .
Use LZO Compression	Select whether to use the LZO Compression function to compress data to decrease the traffic but it also needs more CPU. The default value is Disable .
Keepalive	Select to enable or disable the keepalive function, which is used to detect the status of connection. The default value is Enable .
Ping Interval	Enter the ping interval. The range is from 1~99999 seconds.
Retry Timeout	Enter the retry timeout. The range is from 1~99999 seconds.
Ifconfig	Enter the tunnel IP address that VPN uses.
Route	Enter the route IP and Mask. This is the target IP domain you can access through the VPN tunnel.
Save Log File	You can save an OpenVPN Server log file.

Press **Apply** to activate settings.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

VPN | VPN Port Forwarding Page

Use this page to configure Port Forwarding rules for the OpenVPN Client tunnel.

VPN Port Forwarding Help

Enable VPN Port Forwarding

Protocol:	Both ▾
Source IP Address:	<input style="width: 90%;" type="text"/>
Destination Port or Range:	<input style="width: 40%;" type="text"/> - <input style="width: 40%;" type="text"/>
Forwarding IP Address:	<input style="width: 90%;" type="text"/>
Forwarding Port or Range:	<input style="width: 40%;" type="text"/> - <input style="width: 40%;" type="text"/>

Apply Cancel

Protocol	Source IP	Destination Port Range	Forwarding IP	Forwarding Port Range	Select	Edit

Delete Selected Delete All Refresh

VPN Port Forwarding	
Enable VPN Port Forwarding	Select the Enable VPN Port Forwarding check box if you want to configure this feature. Complete the remaining fields and click Apply .
Protocol	Configure Both (TCP and UDP), TCP or UDP protocol type.
Source IP Address	Enter a specific source IP address.
Destination Port or Range	Configure the destination port range. The destination is WR7802-XT that you plan on using.
Forwarding IP Address	Enter the specific forwarding IP address.
Forwarding Port or Range	Configure the port or range for forwarding device.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted. After configuring VPN port forwarding, you can see the entries you configured in the table below.

- Select **Edit** to modify settings.
- Click **Select** and then click **Delete Selected** to delete selected entries.
- Click **Delete All** to delete all entries.
- Press **Refresh** to update the table.

VPN | VPN Certificate Page

Use this page to upload or delete the VPN certificates.

The filename of the VPN certificate files **MUST** be uploaded using the following file names.

Open VPN Mode	VPN Certificate File Name
OpenVPN Server TLS Mode	ca.crt, server.key, server.crt, dh1024.pem
OpenVPN Client TLS Mode	ca.crt, client.key, client.crt
Static Mode	static.key

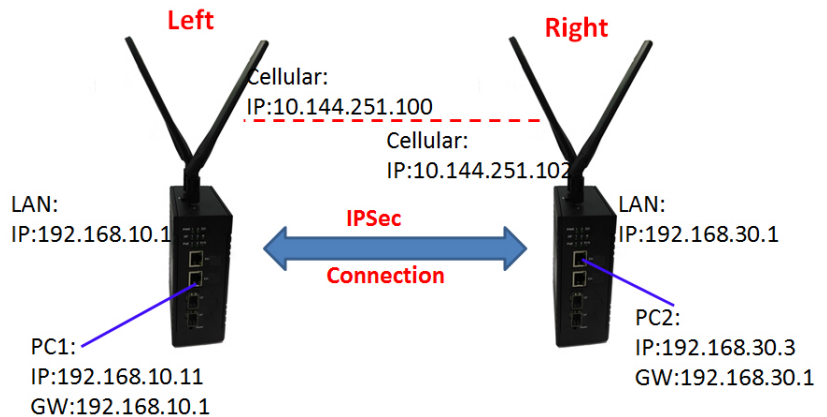
The following table provides information about using this page.

VPN Certificate Management	
Delete VPN Certificate	Press the Delete to delete the selected certificate file.
Import VPN Certificates	Click the Browse button to select the certificate file. After locating the file, click the Import button. <i>Note: Make sure the file names listed in the table above.</i>

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

VPN | IPsec Settings Page

Use this page to configure the parameters for an IPsec Connection. The VPN tunnel has two participants on its ends, called the left and right. Which participant is considered the left or the right is arbitrary. You can configure various parameters for these two ends using this page. The following image shows a simple example of an IPsec connection.



IPsec Settings

Help

Public Key Management

Generate Public Key:	Generate Key...
Current Public Key:	<pre>0sAQNz9k+Zx3fR3jwF+nywiDOMXjJXW +YTpqYf8BZTLwlav5Dw5WBIXDjJpycW Y1/a41e4u8ZZ4gtmMsfO1woX11btiWPK u/px/Mp+J3L6gMzDkOW9wBbSfpVmb2 mIIH3mQpoKmxL0ALL5x15b+9Je/RafxE XxqeMYglw+Bjp/5cdZ4R2c9wu6d6RDQg ul5nD8tGlXaMXnTV5kDUXAGl3kAnIJ3pc Tgp0okpCxrjgZF6U8hWX8M50Fleg3Cn7 UiqUg6RgHb+Dks1b3DMF1hDS4Z3S0Uf 3vnHmY/IH3pNcO68Poe+SktpQp3EoEL</pre>

Enable IPsec Connection

Interfaces for IPsec to Use :	LAN
Authentication Method :	RSA Key
ESP Algorithm :	AES
Left - IP of network interface :	192.168.1.1
Left Source IP Address :	0.0.0.0
Left Subnet (network/netmask) :	(Ex : 192.168.10.0/24)
Left RSA Key :	
Right - IP of network interface :	192.168.1.2
Right Source IP Address :	0.0.0.0
Right Subnet (network/netmask) :	(Ex : 192.168.20.0/24)
Right RSA Key :	

Apply Cancel

IPsec Settings	
Generate Public Key	Generate a new public key by pressing the Generate key... button. The Public key is used when the authentication method set to RSA key in the configuration (below).
Current Public Key	The content of the current public key is displayed.
Enable IPsec Connection	Use this check box to enable or disable the IPsec function. Configure the appropriate fields below.

IPsec Settings (Continued)	
Interfaces for IPsec to Use	Select the interface that you want to use communicate with the VPN peer.
Authentication Method	Select the authentication method, RSA key or Shared secret . <ul style="list-style-type: none"> • Shared secret: Use a static shared secret key. The maximum length is 25. • RSA key: Use an RSA digital signature authentication. The public key for RSA authentication can be generated on the top-half of this page.
ESP Algorithm	Select the algorithm (AES , DES , or 3DES) to encrypt an ESP (Encapsulating Security Payload) payload.
Left - IP of network interface	Left corresponds to the right in an IPsec point-to-point connection. The left and right IP settings should be the same in both IPsec endpoints. Enter the interface IP address of the left endpoint that can directly connect to the right endpoint. For example, a WAN port IP address or Cellular IP address.
Left Source IP Address	As Left - IP of network interface, enter the LAN port interface IP address of the left endpoint.
Left Subnet (network/netmask)	Enter the subnet mask of the left endpoint in CIDR notation, for example, 192.168.10.0/24.
Left RSA Key	The attribute is only required when using the RSA key authentication method using the public key which was generated from the top-half of this page.
Right - IP of network interface	Right corresponds to the left in an IPsec point-to-point connection. The right IP settings should be the same in both IPsec endpoints. Enter the interface IP address of the right endpoint that can directly connected to the left endpoint. For example, a WAN port IP address or Cellular IP address.
Right Source IP Address	As Right - IP of network interface, enter the LAN port interface IP address of the right endpoint.
Right Subnet (network/netmask)	Enter the subnet mask of the right endpoint in CIDR notation, for example, 192.168.20.0/24.
Right RSA Key	The attribute is only required when using the RSA key authentication method using the public key which was generated from the top-half of this page.

Click the **Apply** button to apply the configuration changes.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Security - Port Security Page

The Port Security feature allows you to stop the MAC address learning for a specific port. After stopping MAC learning, only the MAC address listed in the **Port Security List** can access the switch and transmit/receive traffic.

Port Security Help

Port Security State

Port	1	2	3	4
State	Disable ▾	Disable ▾	Disable ▾	Disable ▾

Apply

Add Port Security Entry

Port	VID	MAC Address
Port 1 ▾	<input style="width: 50px;" type="text"/>	<input style="width: 150px;" type="text"/>

Add

Port Security Entry List All ▾

Port	VID	MAC Address	Select

Delete Selected
Delete All
Refresh

Beta Version

Port Security	
Port Security State	
Port	The port identifier.
State	Enable or disable port security on the corresponding port. Click the Apply button to apply the configuration changes.
Add Port Security Entry	
Port	The port ID. Select the appropriate from the Port drop list.
VLAN ID	The VLAN ID. If you want to insert a new MAC entry, the VLAN ID must be correct when creating a new entry.
MAC Address	MAC address of the entry. Click the Add button to add a Port Security Entry.
Show Port Security List	
Port	The port ID of the entry.
VID	The VLAN ID of the entry.
MAC Address	MAC address of the entry.
Delete Selected	Click the Delect Selected button to remove the selected Port Security Entry.
Delete All	Click the Delete All button to remove all Port Security Entry.
Refresh	Click the Refresh button to refresh all Port Security Entry.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Management Pages

The Management group includes the following pages:

- [Management | OPCUA Settings Page](#) on Page 103
- [Management | Remote Settings Page](#) on Page 104
- [Management | SMTP Settings Page](#) on Page 107
- [Management | Login Settings Page](#) on Page 108
- [Management | Firmware Upgrade Page](#) on Page 110
- [Management | Configuration File Page](#) on Page 111
- [Management | LLDP Configuration Page](#) on Page 112

Management | OPCUA Settings Page

OPCUA (Open Platform Communications Unified Architecture) is an industrial M2M (machine-to-machine) communication protocol developed for interoperability. This page allows the user to configure the parameters for an OPCUA Server.

OPCUA Server Settings

Enable OPCUA Server

Clear Certificate Key :	<input type="checkbox"/>
Port :	<input type="text" value="48020"/> (1-65535)
Change Password :	<input type="checkbox"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>

OPC UA Server Settings	
Enable OPCUA Server	Click the check box to enable the OPC UA Server function.
Clear Certificate Key	Click to clear the certificate key saved on the system.
Port	Specifies the port number range, which is from 1 to 65535. The default value is 48020.
Change Password	Click the check box to change the password and then type the new password in the New Password and Confirm Password fields.
Apply	Click the Apply button to apply the configuration changes.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Management | Remote Settings Page

Use the **Remote Settings** page to set the Remote Management Privacy settings, select Event Warning Types, and the configure SNMP settings (V2c and V3). Make sure that the SNMP configuration matches between the device and SNMP server.

Remote Settings
Help

Remote Management Privacy

Telnet
 SSH
 PortVision DX

SNMP
 Force HTTPS

SNMP Trap
 Email Alert

Event Warning Type

Authentication Fail
 Config Changed

SNMP Settings

Protocol Version:	V2c v
Server Port:	161
Get Community:	public
Set Community:	private
Trap Destination:	0.0.0.0
Trap Community:	public

[Configure SNMPv3 User Profile](#)

Click to access
SNMPv3 configuration

Apply
Cancel

Remote Settings	
Remote Management Privacy	Select which remote services are permitted to be opened in your environment. The services include Telnet, SNMP, SNMP Trap, SSH, and Force HTTPS, E-mail Alert and PortVision DX.
Event Warning Type	
Authentication Fail	The failure of authentication event.
Config Changed	The configuration of this device has changed.

Remote Settings (Continued)	
SNMP Settings	
Protocol Version	Select the SNMP version, and make sure that it identical between the device and the SNMP client software. If you chose SNMPv3 and apply it, you must configure the SNMPv3 settings below in the SNMPv3 User Profile .
Server Port	Change the server port for a service if needed; however, you have to use the same port to use that service for remote management.
Get Community	Specify the password for the incoming Get and GetNext requests from the management station. By default, it is set to public and allows all requests.
Set Community	Specify the password for the incoming Set requests from the management station. By default, it is set to private.
Trap Destination	Specify the IP address of the station to which to send the SNMP traps.
Trap Community	Specify the password sent with each trap to the manager. By default, it is set to public and allows all requests.
Apply	Click the Apply button to apply the configuration changes.

Beta Version

Configure SNMPv3 User Profile

<input checked="" type="checkbox"/> Enable SNMPv3Admin	
User Name:	SNMPv3Admin
Password:	••••••••
Confirm Password:	••••••••
Access Type:	Read/Write ▾
Authentication Protocol:	MD5 ▾
Privacy Protocol:	None ▾
<input checked="" type="checkbox"/> Enable SNMPv3User	
User Name:	SNMPv3User
Password:	••••••••
Confirm Password:	••••~•••
Access Type:	Read Only ▾
Authentication Protocol:	MD5 ▾
Privacy Protocol :	None ▾

Apply Cancel

Configure SNMPv3 User Profile	
Configure SNMPv3 User Profile	For SNMP protocol version 3, click the Configure SNMPv3 User Profile link (in blue) to configure the details of the SNMPv3 user.
Enable SNMPv3 Admin/User	Click the check box to enable the SNMPv3 user profile.
User Name	Specify a user name for the SNMPv3 administrator or user. Only the SNMP commands carrying this user name are allowed to access the device.
Password	Specify a password for the SNMPv3 administrator or user. Only the SNMP commands carrying this password are allowed to access the device.
Access Type	Select Read Only or Read and Write accordingly.
Authentication Protocol	Select an authentication algorithm. SHA authentication is stronger than MD5 but it is slower.
Privacy Protocol	Specify the encryption method for SNMP communications. None and DES are available, the default is None .
Apply	Click the Apply button to apply the configuration changes.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Beta Version

Management | SMTP Settings Page

Sends the events that have occurred to the remote E-mail server. The receiver can then receive notification by E-mail.

SMTP Settings

SMTP Server IP:	<input type="text"/>
Email Account:	<input type="text"/>
Authentication Protocol:	None ▾
User Name:	<input type="text"/>
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Rcpt Email Address 1:	<input type="text"/>
Rcpt Email Address 2:	<input type="text"/>

SMTP Settings	
SMTP Server IP	The IP address of the SMTP Server.
Email Account	The sender's Email Account.
Authentication Protocol	If the SMTP server requires authentication, select the Authentication Protocol and enter the User Name and Password.
User Name	The User Name of the Sender Email account.
Password	The Password of the Sender Email account.
Rcpt Email Address	The Receiver's email address.
Apply	Click the Apply button to apply the configuration changes.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Management | Login Settings Page

Use this page to set the user name and password for this device.

Login Settings Help

User Name:	admin
New Password:	
Confirm Password:	

Apply Cancel

Guest Name:	guest
New Password:	
Confirm Password:	

Apply Cancel

Login Settings Help

User Name:	admin
New Password:	
Confirm Password:	

Apply Cancel

Guest Name:	guest
New Password:	
Confirm Password:	

Apply Cancel

Authentication Mode

Authentication Mode: RADIUS->Local

RADIUS Server

RADIUS Server IP:	0.0.0.0
Shared Key:	
Server Port:	1812

Secondary RADIUS Server

RADIUS Server IP:	0.0.0.0
Shared Key:	
Server Port:	1812

Apply

Authentication Mode

Authentication Mode: TACPLUS

TACPLUS Authentication Setting

Authentication Type:	ASCII
Authentication Timeout:	5

TACPLUS Server

TACPLUS Server IP:	0.0.0.0
Shared Key:	
Server Port:	49

Secondary TACPLUS Server

TACPLUS Server IP:	0.0.0.0
Shared Key:	
Server Port:	49

Apply

Login Settings	
User Name	The username to login to this device.
Password	The password to login to this device.
Authentication Mode	
Local	The local account to login to this device.

Login Settings (Continued)	
RADIUS	Use RADIUS (Remote Authentication Dial In User Service) account to login to this device.
RADIUS --> Local	The RADIUS account or local account to login to this device. The RADIUS account will be tried first.
TACPLUS	
TACPLUS -->Local	
RADIUS Server and Secondary RADIUS Server	
RADIUS Server IP	Sets the IP address of an external RADIUS server as the authentication database.
Shared Key	Sets specific characters for server authentication verification.
Server Port	Sets the communication port of an external RADIUS server as the authentication database.
TACPLUS Authentication Setting	
Authentication Type	Choose the authentication protocol (ASCII/PAP/CHAP).
Authentication Timeout	Set the length of time, in seconds, that the device waits for a response from the primary server before sending the request to the secondary server.
TACPLUS Server	
TACPLUS Server IP	Sets the IP address of an external TACPLUS server as the authentication database.
Shared Key	Sets specific characters for server authentication verification.
Server Port	Sets the communication port of an external TACPLUS server as the authentication database.
Apply	Click the Apply button to apply the configuration changes.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Management | Firmware Upgrade Page

You can use this page to update the firmware image. The latest firmware is on our download site. The new firmware may include new features, bug fixes or other software changes. You can review the release notes before installing the latest firmware version.

Technical support recommends uploading the latest firmware version before installing the router at a customer site.

Note: The system automatically reboots after you finish upgrading the firmware. You notify the attached users before upgrading the firmware.

Firmware Upgrade Help

Local file

Select File: Browse...

Upgrade Cancel

TFTP

IP	
File Name	

Upgrade Cancel

Firmware Upgrade	
Local File	
Select File	Type the path of the firmware in Select File field, or click Browse... to browse the firmware file. Press Upgrade to upload the firmware file to the AP. After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash. Note: During the progress, DO NOT power off your system.
TFTP	
IP	This is the IP address of the TFTP server where the firmware image resides.
File Name	This is the file name of the firmware image. Click the Upgrade button to begin upgrading the firmware or click the Cancel button to clear the entered IP address and firmware file name. After the firmware has upgraded, the router reboots automatically.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Management | Configuration File Page

The WR7802-XT provides Configuration File Backup (Save Setting to File), Restore (Load Setting from File) and Reset Setting to Default features.

You can save the current configuration file that is currently saved in the router's flash to a PC. This allows you to execute a Restore command later to restore the configuration file back to the router. Before you restore the configuration file, you must place the backup configuration file to specific folder on the PC. Users can also browse the target folder and select the existing configuration file. The WR7802-XT can then download this file back to the flash.

Configuration File

Help

Local Files

Load Settings from File:	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>
Save Settings to File:	<input type="button" value="Save..."/>		
Reset Settings to Default:	<input type="button" value="Reset"/>	<input type="checkbox"/>	Include IP Settings

TFTP

IP	<input type="text"/>
File Name	WR7802-XT-00C04E670
Load/Save Settings	<input type="button" value="Load"/> <input type="button" value="Save"/> <input type="button" value="Submit"/>

Configuration File	
Local	
Load Setting from File (Restore)	Either enter the path of the configuration file or click Browse... to browse the configuration file. Press the Upload button after selecting the configuration file.
Save Setting to File (Backup)	Press Save... to backup the configuration file to specific path/folder in your computer.
Reset Settings to Default	If you select the Reset button, this resets all the configuration settings except the default IP address to their default settings unless you also select the Include IP Settings option.
TFTP	
IP	Enter the IP address of the TFTP server where your configuration file has been previously saved or can be saved.
File Name	This is the file name of the configuration file that you want to save.
Load/Save Settings	Select the Load option to load the configuration from the TFTP server onto the router. Select the Save option to save the configuration on the router to the TFTP server. Click the Submit button to load or save the configuration.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Management | LLDP Configuration Page

The WR7802-XT supports topology discovery or LLDP (IEEE 802.1AB Link Layer Discovery Protocol) which can help you to discovery a multi-vendor's network device on same segment with an NMS (Network Management System) device which supports LLDP function.

When the LLDP function is enabled, the NMS can easier maintain the topology map, display port ID, port description, system description, VLAN ID, and so forth. Once a link failure occurs, the topology event change can be updated to the NMS as well. The **LLDP Port State** displays the neighbor ID and IP learnt from the connected devices.

LLDP Configuration

Help

Enable LLDP

LLDP Timer:	30	seconds
LLDP Hold Time :	120	seconds

Apply Cancel

LLDP Port State

Local Port	Neighbor ID	Port Description	Neighbor IP	Neighbor VID

Refresh

LLDP Configuration	
Enable LLDP	Set this to Enable to enable LLDP on the router or to Disable to disable the LLDP function.
LLDP Timer	This setting determines how frequently (in seconds) the router sends out LLDP discovery packets. Valid values are 5 to 254 and default is 30.
LLDP Holdtime	This setting determines how long in seconds the WR7802-XT retains LLDP neighbor information. Valid values are 10 to 255 and the default is 120.
Apply	Click the Apply button to apply the configuration changes or click the Cancel button to discard any changes.
LLDP Port State	This table shows the LLDP neighbors for which the router is currently aware.
Local Port	The router port to which the neighbor is connected.
Neighbor ID	The MAC address of the LLDP neighbor.
Port Description	A description of the what is connected to a port.
Neighbor IP	The IP address of the LLDP neighbor
Neighbor VID	The VLAN to which the LLDP neighbor is connected.
Refresh	Click the Refresh button to update the information in the table.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Tools Pages

The **Tools** pages include the following pages:

- System Log
- Ping Watchdog
- Ping

Tools | System Log Page

System log is used for recording events occurred on the WR7802-XT, including connection, disconnection, system reboot, and so forth.

System Log

Enable Remote Syslog Server

IP Address:	0.0.0.0
Port:	514

#	Time	Source	Message
1	2017-04-30 22:13:16	system	TZ: GMT-6

System Log	
Enable Remote Syslog Server	Select this check box to enable the remote system log. The default is to log locally.
IP Address	Specify the IP address of the remote server
Port	Specify the port number of the remote server.
Apply/Cancel	Click the Apply button to apply the configuration changes or click Cancel to cancel the change.

The table displays a local version of the log file. You can do the following with the local log file.

- Click the **Refresh** button to reload the log table.
- Click the **Clear** button to delete log information.
- Click the **Save** button to download log information to your PC.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Tools | Ping Watchdog Page

You can use this feature to ping a specific IP address and if it reaches the failure count, the router automatically reboots itself.

Ping Watchdog

<input checked="" type="checkbox"/> Enable Ping Watchdog	
IP Address to Ping:	<input type="text" value="192.168.11.202"/>
Ping Interval:	<input type="text" value="300"/> seconds
Startup Delay:	<input type="text" value="120"/> seconds(>120)
Failure Count To Reboot:	<input type="text" value="300"/>

Ping Watchdog	
Enable Ping Watchdog	If you select this check box, the ping watchdog feature is enabled.
IP Address to Ping	This is the target IP address that you want to ping.
Ping Interval	Ping this IP every ping interval (in second).
Startup Delay	System boot up time. The startup delay uses to buffer to prevent it continue to reboot itself.
Failure Count To Reboot	When the ping failed time reaches the failure count that you entered, the device will be rebooted.
Apply/Cancel	Click the Apply button to apply the configuration changes or click Cancel to cancel changes to the settings.

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Tools | Ping Page

This feature allows you to check the status of remote station.

Enter the target IP address in the **Destination** field then press **Ping**.

The system pings the remote station four times and lists the ping results in the web GUI.

Ping

Destination:

```

PING 10.0.0.202 (10.0.0.202): 56 data bytes
64 bytes from 10.0.0.202: icmp_seq=0 ttl=128 time=0.8 ms
64 bytes from 10.0.0.202: icmp_seq=1 ttl=128 time=0.6 ms
64 bytes from 10.0.0.202: icmp_seq=2 ttl=128 time=0.5 ms
64 bytes from 10.0.0.202: icmp_seq=3 ttl=128 time=0.6 ms

--- 10.0.0.202 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.5/0.6/0.8 ms
    
```

Note: You must **Save** ([Page 115](#)) settings, if you want to maintain these settings if the WR7802-XT is rebooted.

Save Page

Use this page to save configuration to flash. Every time you finish changing the WR7802-XT configuration, you must save the changes to flash if you want the changes to be permanent.

Save

Do you want to save configuration to flash?

Logout Page

After you completed configuration and have saved the configuration (if desired), you should logout the system.

If you do not log out of the system, the login session does not timeout for couple minutes. There is a risk that other user may login the system without a password. Another side affect is that you cannot access the WR7802-XT at the same time if someone already login the system.

Use this page to logout. Press **Yes** to logout.

Logout

Do you want to logout?

Reboot Page

Use this page to reboot the WR7802-XT.

Reboot

Do you want to reboot?

Configuration Using the Command Line Interface (CLI)

Overview

The RocketLinx WR7802-XT Series provides a Command Line Interface (CLI) that you can access through a Telnet or SSH connection. The SSH connection can secure all the configuration commands you send to the WR7802-XT. SSH is a client/server architecture while the WR7802-XT is the SSH server. When you want to make SSH connection with the WR7802-XT, you can use PortVision DX or download an SSH client tool.

After accessing the CLI, you can view system information, show the status, configure the WR7802-XT and receive a response back from the system by keying in commands.

If you have not done so, you need to program the WR7802-XT IP address to meet your network requirements. The easiest way to configure the IP address is using a Windows system and PortVision DX, which is discussed in [Configuring the Network Settings](#) on Page 21.

This section provides the following information:

- [Accessing the CLI through an SSH Client](#) (below)
- [Accessing the CLI through PortVision DX](#) on Page 117
- [CLI Introduction](#) on Page 118
- [Using SHOW Commands](#) on Page 120
- [Using SET Commands](#) on Page 123
- [Using DELETE Commands](#) on Page 126

Accessing the CLI through an SSH Client

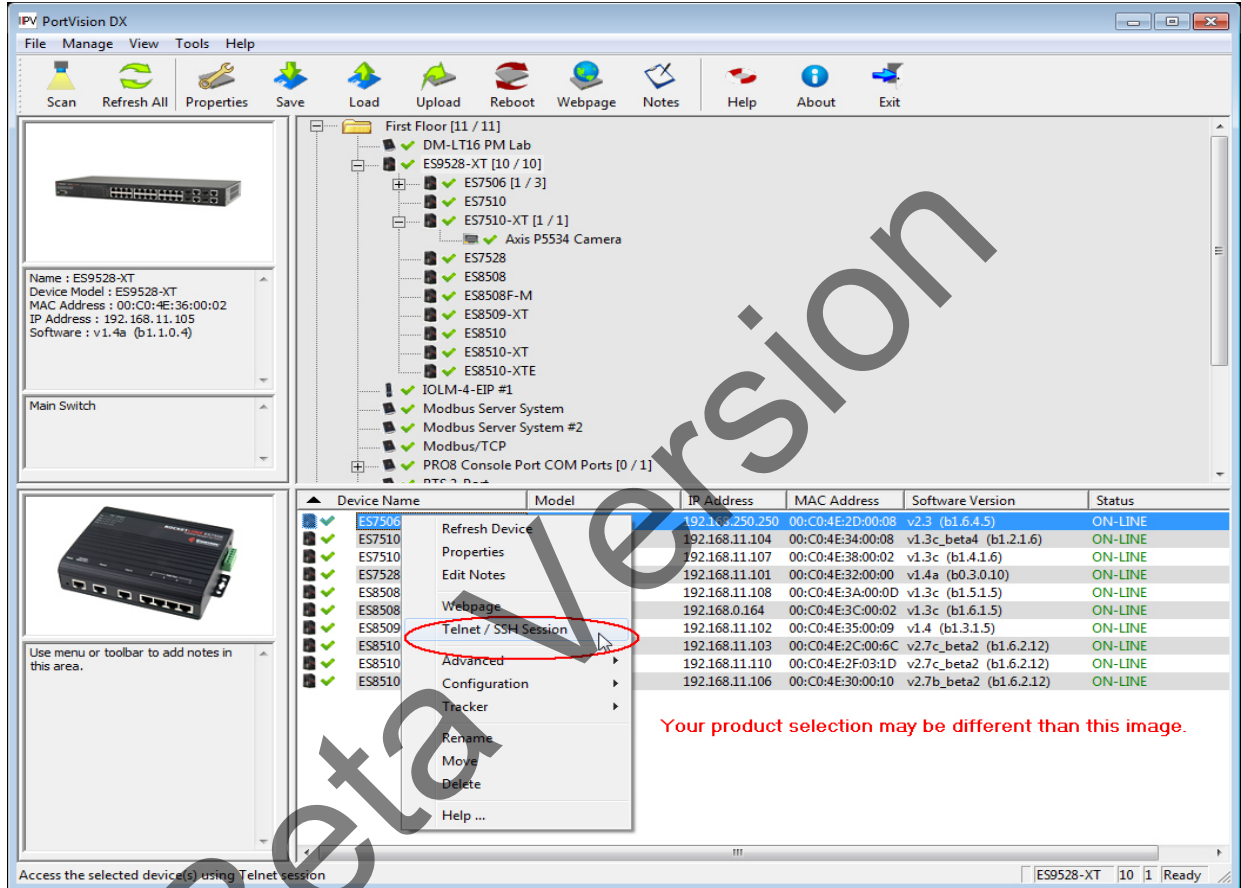
If you want to use your own SSH client to access the CLI, you need the following default information about the WR7802-XT:

- IP address: 192.168.250.250
- Subnet mask: 255.255.255.0
- IP gateway: 192.168.250.1
- Login: admin
- Password: admin (default)

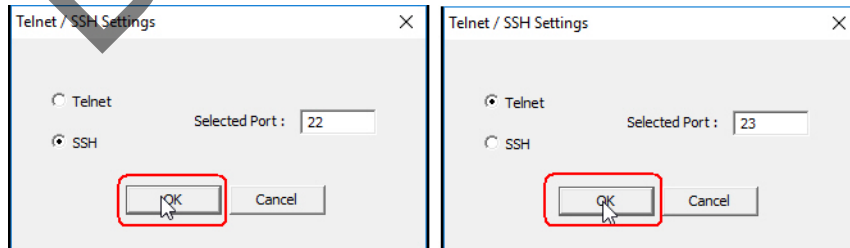
Accessing the CLI through PortVision DX

The next discussion provides procedures to use PortVision DX with a Telnet or SSH connection to access the CLI.

1. If you have not done so, install PortVision DX ([Installing PortVision DX](#) on Page 20).
2. Start PortVision DX.
3. Right-click the WR7802-XT in the *Device List* pane (lower) and click **Telnet/SSH**.

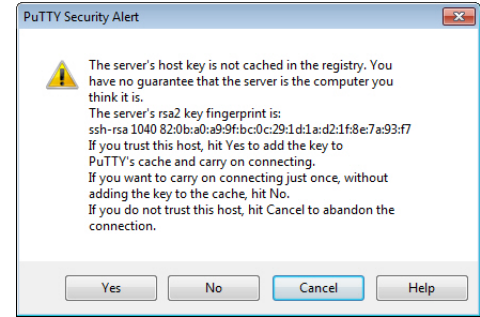
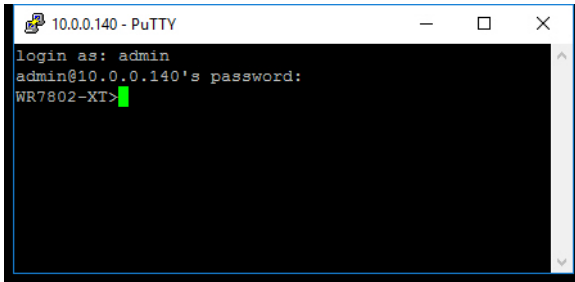


4. Select either Telnet or SSH and leave the default port number.



If you selected SSH, click **Yes** to the security alert.

- Enter the user name (default = **admin**).
- Enter the password (default = **admin**).



CLI Introduction

There are several different command sets. Each command set has its own access ability and available command lines. These command sets are:

list: Use this read-only command to list the available commands.

show: Use this is read-only command to show the current setting and status of the WR7802-XT.

set: This is the write command to change the current setting.

del: This is Delete command to delete the applied settings.

exit: To exit the CLI.

Note: Use the **TAB** key can help you find the correct command and complete the command to make the read or write easier.

Command List

You can view the available command by pressing the **TAB** key.



The commands have these definitions:

- **archive downloads-sw** - upgrades the firmware on the WR7802-XT
- **config** - backup or restore the WR7802-XT configuration file
- **del** - delete settings for one or more of these configuration settings: IPSEC settings, log list (system log), OPCUA settings, OPENVPN settings, or remote settings
- **exit** - exits the CLI

- **list** - displays the available commands and provides information their usage

```

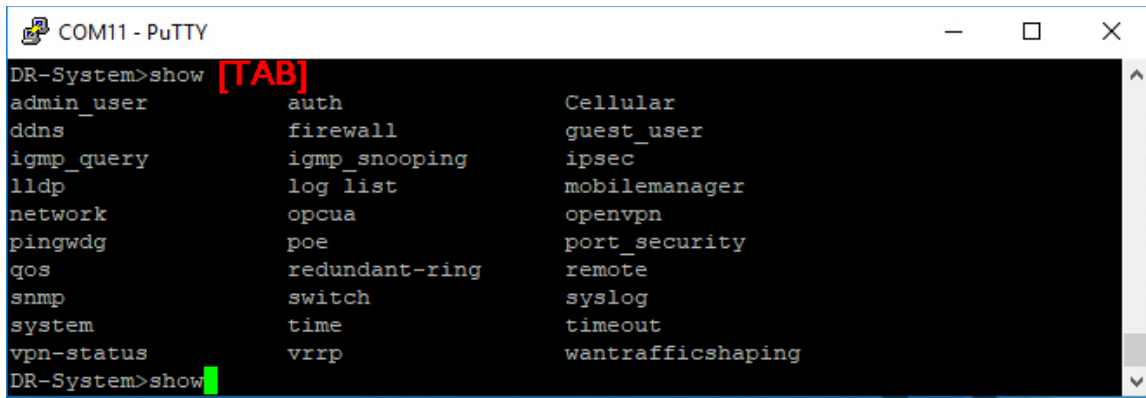
COM11 - PuTTY
DR-System>list [TAB]
admin_user      archive download-sw  auth
Cellular        config                ddns
exit            firewall              guest_user
igmp_query      igmp_snooping        ipsec
lldp            log list              mobilemanager
network         opcua                 openvpn
ping            ping6                 pingwdg
poe             port_security         qos
reboot          redundant-ring        remote
reset           snmp                  switch
syslog          system                time
timeout         vrrp                  wantraffichaping
write

DR-System>list network [TAB]
bridge          dhcpserver            ipv6neighbor
DR-System>list network bridge [ENTER]
show set del keyword                Description
-----
[X] [X]          |-iptype                --fixed/dynamical ip(dhcp client)
[X] [X]          |-ipaddr                --ip address
[X] [X]          |-netmask               --subnet mask
[X] [X]          |-gateway               --gateway ip address
[X] [X]          |-dns1                  --dns1
[X] [X]          |-dns2                  --dns2
[X] [X] [X]       |-ipv6addr              --add ipv6 address
[X] [X] [X]       |-ipv6gw                --config ipv6 gateway
DR-System>
  
```

- **ping** - standard IPv4 ping command
- **ping6** - ping IPv6 address
- **reboot** - this reboots the WR7802-XT
- **reset** - this resets the WR7802-XT back to the factory defaults, including the IP address
- **set** - sets the setting in the WR7802-XT, refer to [Using SET Commands](#) on Page 123 for more information
- **show** - shows you the current settings a configuration setting, refer to [Using SHOW Commands](#) on Page 120 for more information

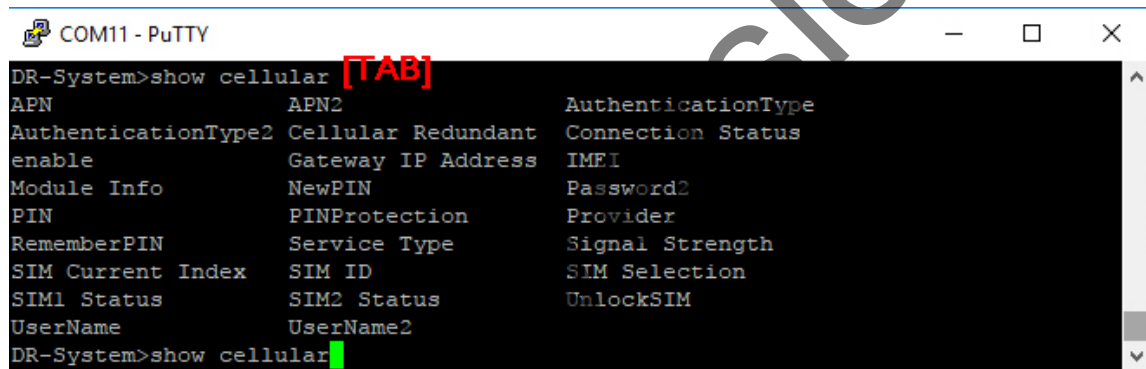
Using SHOW Commands

Type **Show** and press the **TAB** key to see the **show** command sets. The following command lines are available.



```
COM11 - PuTTY
DR-System>show [TAB]
admin_user      auth            Cellular
ddns            firewall        guest_user
igmp_query      igmp_snooping  ipsec
lldp            log_list        mobilemanager
network         opcua           openvpn
pingwdg         poe             port_security
qos             redundant-ring remote
snmp            switch          syslog
system         time            timeout
vpn-status      vrrp           wantrafficsaping
DR-System>show
```

Next, we will examine how to find out more information about one of the supported commands (cellular). Type **show cellular** and the **TAB** key to see all the show cellular command lines.



```
COM11 - PuTTY
DR-System>show cellular [TAB]
APN              APN2           AuthenticationType
AuthenticationType2 Cellular Redundant Connection Status
enable           Gateway IP Address IMEI
Module Info      NewPIN         Password2
PIN              PINProtection  Provider
RememberPIN      Service Type   Signal Strength
SIM Current Index SIM ID         SIM Selection
SIM1 Status      SIM2 Status    UnlockSIM
UserName         UserName2
DR-System>show cellular
```

Type **show cellular** and press the **Enter** key to see all of the cellular information. The console prints all the information for reference.

```

10.0.0.140 - PuTTY
WR7802-XT>show cellular
Cellular SIM Current Index : 1
Cellular Provider : NONE
Cellular Service Type : No Service
Cellular IMEI : 358709050691298
Cellular Signal Strength : 0 dBm
Cellular SIM1 Status : SIM is deactivated
Cellular SIM2 Status : Inserted
Cellular Connection Status : Disconnected
Cellular Gateway IP Address :
Cellular Module Info : Cinterion
                        PLS8-E
                        REVISION 02.011

Cellular SIM ID : No ID
Cellular enable : Enabled
Cellular SIM Selection : 1
Cellular Cellular Redundant : Disabled
Cellular APN : internet
Cellular UserName :
Cellular AuthenticationType : CHAP
Cellular APN2 : internet
Cellular UserName2 :
Cellular Password2 :
Cellular AuthenticationType2 : CHAP
Cellular PIN :
Cellular NewPIN :
Cellular RememberPIN : Disabled
Cellular PINProtection : Disabled
Cellular UnlockSIM : Disabled
WR7802-XT>
    
```

Illustrates the show cellular command followed by the Enter key, which provides the cellular configuration settings.

The following example illustrates how to use the **TAB** key to complete a command.

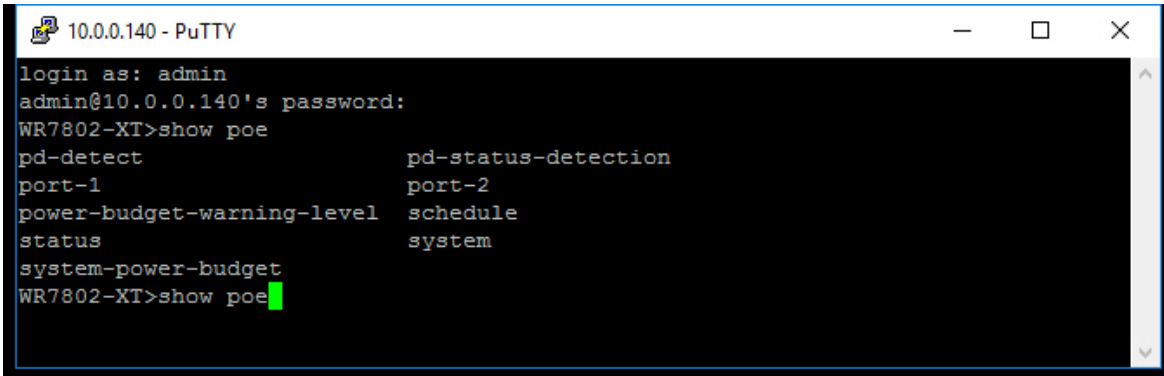
1. Type **show Cellular A** and the **TAB** key to complete the command, which displays the following result.
2. Type **show Cellular AP** and the **TAB** key.
3. Type **show Cellular APN** and the **Enter** key. The command responds with *internet*.

```

10.0.0.140 - PuTTY
WR7802-XT>show cellular a [Press the TAB key]
APN          APN2          AuthenticationType
AuthenticationType2
WR7802-XT>show cellular AP [Press the TAB key]
APN          APN2
WR7802-XT>show cellular APN [Press the ENTER key]
Cellular APN : internet
WR7802-XT>
    
```

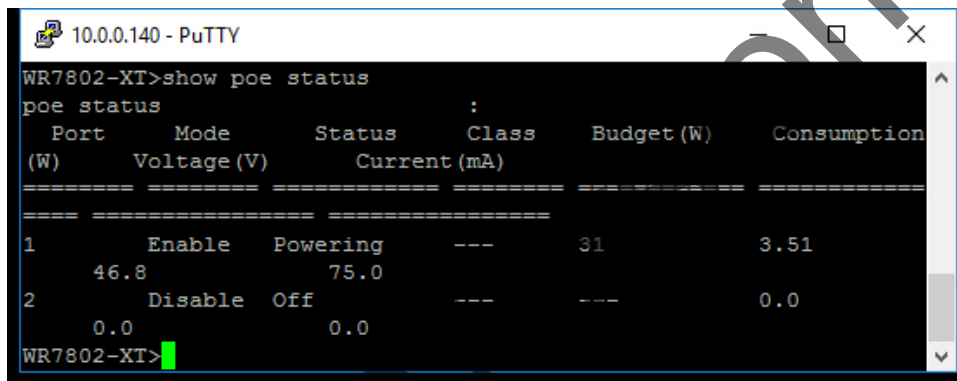
The following examples illustrate how to use the `show poe` command set to view the current settings.

1. Type `show poe` and the **TAB** key.



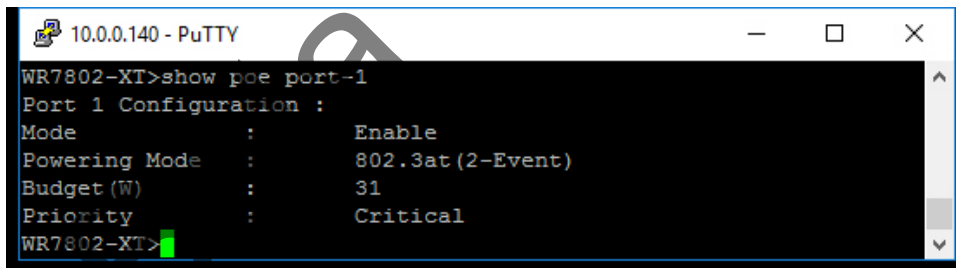
```
10.0.0.140 - PuTTY
login as: admin
admin@10.0.0.140's password:
WR7802-XT>show poe
pd-detect                pd-status-detection
port-1                   port-2
power-budget-warning-level  schedule
status                   system
system-power-budget
WR7802-XT>show poe
```

2. Type `show poe status` and press the **ENTER** key.



```
WR7802-XT>show poe status
poe status
  Port      Mode      Status      Class      Budget (W)      Consumption
  (W)      Voltage (V)      Current (mA)
-----
1          Enable    Powering    ---        31              3.51
  46.8
2          Disable   Off         ---        ---             0.0
  0.0      0.0
WR7802-XT>
```

3. Type `show poe port-1` and press the **ENTER** key.



```
WR7802-XT>show poe port-1
Port 1 Configuration :
Mode      :      Enable
Powering Mode :      802.3at (2-Event)
Budget (W) :      31
Priority   :      Critical
WR7802-XT>
```

Using SET Commands

This subsection shows how to use the set command to configure settings.

To determine commands associated to the set command, type set and the **TAB** key to see all the write command sets. The following command lines are available.

```

10.0.0.140 - PuTTY
WR7802-XT>set
archive download-sw auth Cellular
config ddns exit
firewall igmp_query igmp_snooping
ipsec lldp mobilemanager
network opcu openvpn
password ping pingwdg
poe port_security qos
reboot redundant-ring remote
reset snmp switch
syslog system time
timeout vrrp wantrafficsaping
write
WR7802-XT>set
    
```

Most set command lines have the same functionality as the Web GUI.

How to Set the Device Name

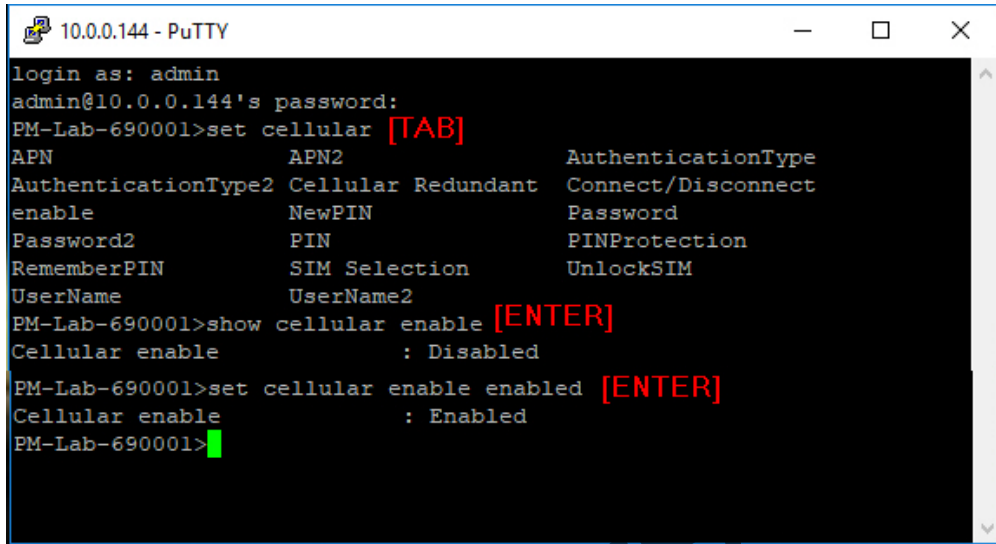
This screen shot shows how to change the device name.

```

10.0.0.140 - PuTTY
login as: admin
admin@10.0.0.140's password:
Control670000>set [TAB]
archive download-sw auth Cellular
config ddns exit
firewall igmp_query igmp_snooping
ipsec lldp mobilemanager
network opcu openvpn
password ping pingwdg
poe port_security qos
reboot redundant-ring remote
reset snmp switch
syslog system time
timeout vrrp wantrafficsaping
write
Control670000>set system [TAB]
devname relay stp stpBridgePrio
stpForwardDelay stpHelloTime stpMaxage stpMode
stpPortCost stpPortPriority stpPortStp
Control670000>set system devname WR7802-XT [ENTER]
system devname : WR7802-XT
WR7802-XT>
    
```

Set the Cellular Settings

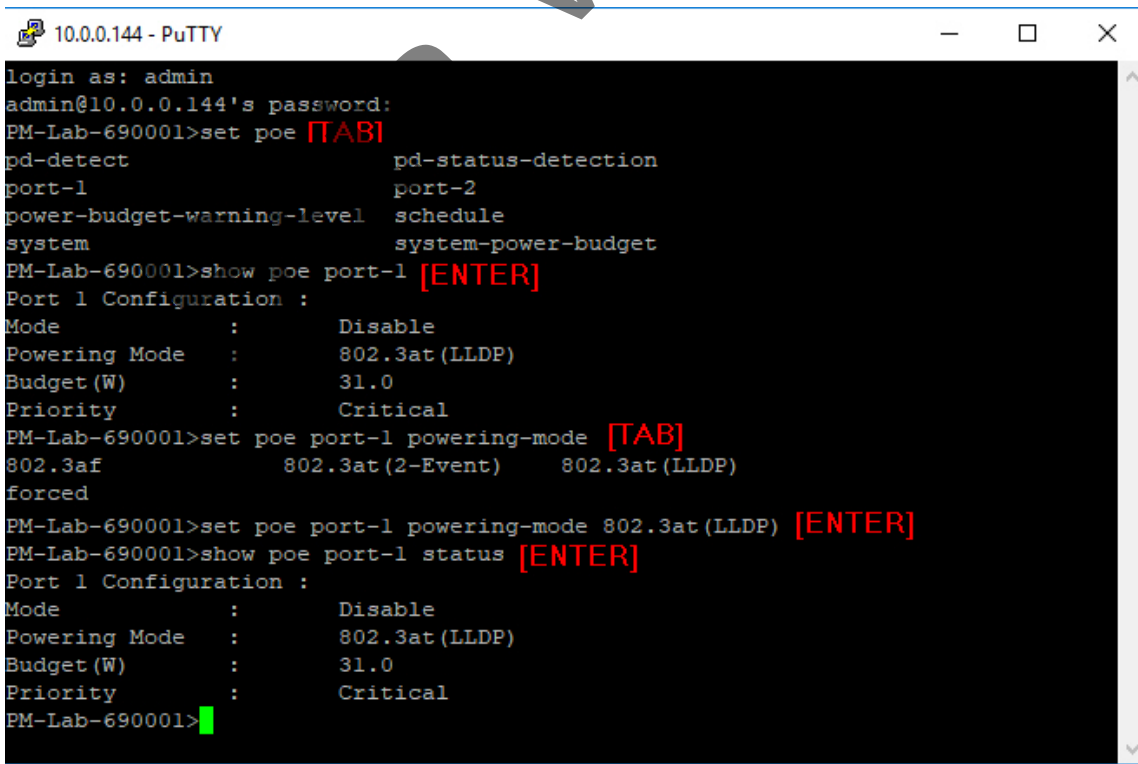
This example shows how to use the **set cellular** command set. The first entry shows the **set cellular** commands, the second entry shows applicable **cellular enable** commands and third entry shows enabling the cellular interface.



```
10.0.0.144 - PuTTY
login as: admin
admin@10.0.0.144's password:
PM-Lab-690001>set cellular [TAB]
APN                APN2                AuthenticationType
AuthenticationType2 Cellular Redundant Connect/Disconnect
enable             NewPIN                Password
Password2         PIN                PINProtection
RememberPIN       SIM Selection        UnlockSIM
UserName          UserName2
PM-Lab-690001>show cellular enable [ENTER]
Cellular enable    : Disabled
PM-Lab-690001>set cellular enable enabled [ENTER]
Cellular enable    : Enabled
PM-Lab-690001>
```

Set the PoE Settings

This example shows how to use the **set poe** command set. The first entry shows the **set poe** commands, the second entry displays the settings for Port 1, the third entry shows how to set the powering mode, and the last entry verifies that the change was made.



```
10.0.0.144 - PuTTY
login as: admin
admin@10.0.0.144's password:
PM-Lab-690001>set poe [TAB]
pd-detect          pd-status-detection
port-1            port-2
power-budget-warning-level schedule
system            system-power-budget
PM-Lab-690001>show poe port-1 [ENTER]
Port 1 Configuration :
Mode                :      Disable
Powering Mode       :      802.3at (LLDP)
Budget (W)          :      31.0
Priority             :      Critical
PM-Lab-690001>set poe port-1 powering-mode [TAB]
802.3af            802.3at (2-Event)    802.3at (LLDP)
forced
PM-Lab-690001>set poe port-1 powering-mode 802.3at (LLDP) [ENTER]
PM-Lab-690001>show poe port-1 status [ENTER]
Port 1 Configuration :
Mode                :      Disable
Powering Mode       :      802.3at (LLDP)
Budget (W)          :      31.0
Priority             :      Critical
PM-Lab-690001>
```

Set the Switch Settings

This example illustrates the set switch settings command. The first entry shows the set switch commands, the second entry shows the commands for gi3, the third entry shows the commands for the state command, the fourth entry shows enabling the gi3 port, and the last entry verifies that the change has been made.

```

10.0.0.144 - PuTTY
login as: admin
admin@10.0.0.144's password:
PM-Lab-690001>set switch [TAB]
gil          gi2          gi3          gi4          statistics  vlan
PM-Lab-690001>set switch gi3 [TAB]
egress_rate  flow-control  ingress_rate  ingress_type
pvid         speed         state
PM-Lab-690001>set switch gi3 state [TAB]
Disable Enable
PM-Lab-690001>set switch gi3 state enable [ENTER]
switch gi3 state          : Enable
PM-Lab-690001>show switch gi3 state [ENTER]
switch gi3 state          : Enable
PM-Lab-690001>

```

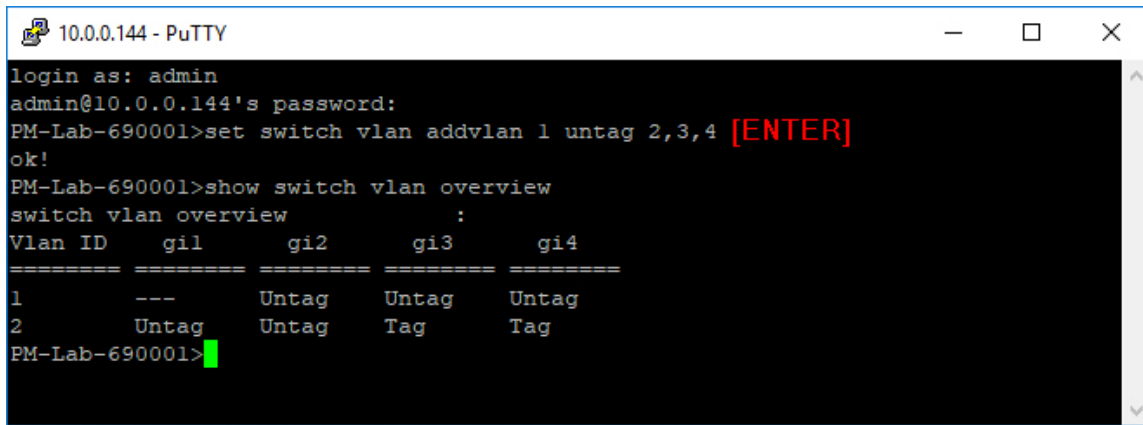
This example shows how to add VLAN 2 to Ports 1 and 2 as untagged and Ports 3 and 5 as tagged.

```

10.0.0.144 - PuTTY
login as: admin
admin@10.0.0.144's password:
PM-Lab-690001>set switch vlan [TAB]
addvlan      delvlan      manageID
PM-Lab-690001>show switch vlan addvlan [ENTER]
String format : vlanid untag port_num tag port_num.
Ex : set switch vlan addvlan 2 untag 1,2 tag 3,4
PM-Lab-690001>set switch vlan addvlan 2 untag 1,2 tag 3,4 [ENTER]
ok!
PM-Lab-690001>show switch vlan [ENTER]
switch vlan manageID      : 1
String format : vlanid untag port_num tag port_num.
Ex : set switch vlan addvlan 2 untag 1,2 tag 3,4
switch vlan overview      :
Vlan ID   gil      gi2      gi3      gi4
=====  =====  =====  =====  =====
1         Untag   Untag   Untag   Untag
2         Untag   Untag   Tag     Tag
PM-Lab-690001>

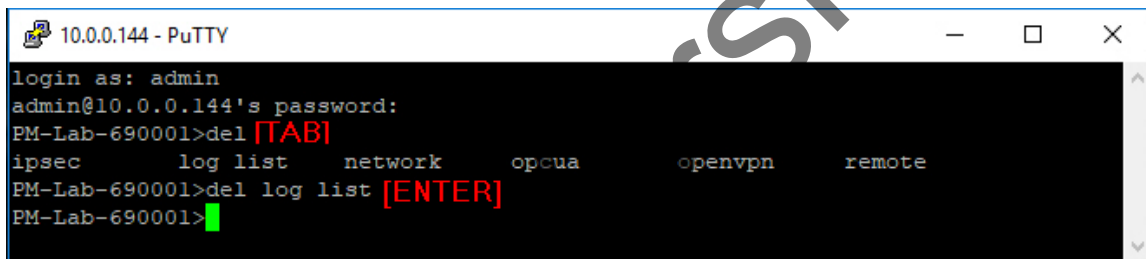
```

The following example shows how to remove Port 1 from VLAN 1.



```
10.0.0.144 - PuTTY
login as: admin
admin@10.0.0.144's password:
PM-Lab-690001>set switch vlan addvlan 1 untag 2,3,4 [ENTER]
ok!
PM-Lab-690001>show switch vlan overview
switch vlan overview
:
Vlan ID   gi1   gi2   gi3   gi4
=====  =====
1         ---   Untag  Untag  Untag
2         Untag  Untag  Tag   Tag
PM-Lab-690001>
```

Using DELETE Commands



```
10.0.0.144 - PuTTY
login as: admin
admin@10.0.0.144's password:
PM-Lab-690001>del [TAB]
ipsec      log list  network  opcua     openvpn   remote
PM-Lab-690001>del log list [ENTER]
PM-Lab-690001>
```