UBWH Australia

Wi-Tek
Communication Solution

Managed, Auto PoE Switch

WI-PMS310GF-Alien
8GE + 2 SFP
Layer 2 Managed Auto PoE Switch

Quick Start Guide
V2108

Table of Contents

1. Introduction

The WI-PMS310GF-Alien is an Auto-PoE, Managed, Layer 2 (L2), POE (24 & 48V) IP Switch, with Gigabit Ethernet (GbE), Small Form-factor Pluggable (SFP), and serial Console interfaces.

This document supplements the Wi-TeK Managed Industrial PoE Switch User Manual, available for download from:
http://www.wireless-tek.com/Uploads/download/1583371174.pdf

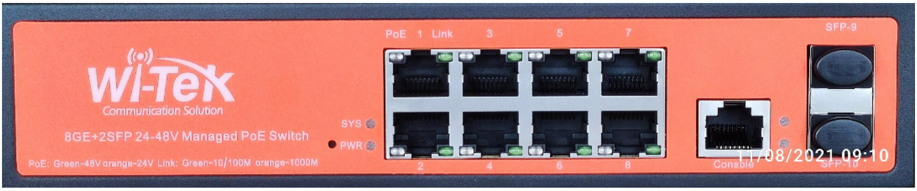
2. Package Contents

WI-PMS310GF-Alien

3. System Requirements

Web Browser: e.g. Mozilla Firefox, Google Chrome, Safari, Microsoft Edge, or Microsoft Internet Explorer.

4. LEDs


Wi-Tek
Communication Solution
8GE+2SFP 24-48V Managed PoE Switch
PoE: Green-48V orange-24V Link: Green-10/100M orange-1000M
SYS
PWR
PoE
1
Link
3
5
7
2
4
6
8
Console
SFP-9
SFP-10
11/08/2021 09:10

4.1 System LEDs

LED	State	Status
SYS	Blinking (slow)	Normal Operation
	Flashing (Fast)	Initializing (boot up)
PWR	On	Steady on if power applied

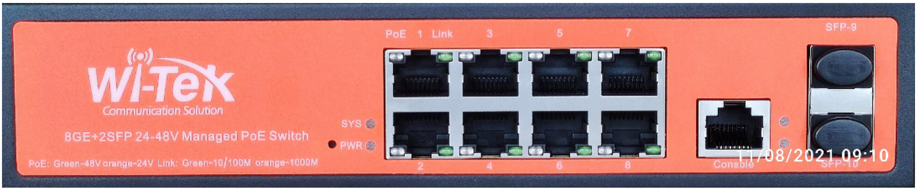
4.2 RJ45 LEDs

LED	State	Status
PoE	Off	No Power applied
	Green	48 V PoE applied
	Orange	24 V PoE applied
Link	Green	10/100/1000 Mbps connection. Flashes with activity.
	Off	No Ethernet connection

4.3 SFP LEDs

LED	State	Status
9 10	Off	No link
	Green	Link established at 1000 Mbps (1 Gbps) Flashing Indicates Activity

5. Front Panel


Wi-Tek
Communication Solution
8GE+2SFP 24-48V Managed PoE Switch
PoE: Green-48V orange-24V Link: Green-10/100M orange-1000M
SYS
PWR
PoE 1 Link
3
5
7
2
4
6
8
Console
SFP-9
SFP-10
11/08/2021 09:10

Port	Description
Note	Active PoE means that PoE voltage is applied only if a device is connected.
RJ45 1-8	LAN: 10/100/1000 bps Ethernet connection PoE Out. 2-Pair, Pins: 48V=1,2(+) 3,6 (-), 24V=4,5(+) 7,8 (-) Software selectable: • Off • 24 V Active • 48 V Active 802.3af 15 W max • 48 V Active 803.3at 30 W max • Auto Active, Auto selection Off/24/48V PoE • 24V Forced On • 48V Forced On
SFP 9-10	Hot-swappable Small Form-factor Pluggable (SFP) ports supporting 1 Gbps connections.
Console	This port is compatible with Cisco part number 72-3383-01 (Console Cable). The serial settings are: Baud rate: 38400 Data bits: 8 Stop bits: 1 Parity: None Flow control: None

RESET	Button to the left of the PWR LED. To reset the Switch to factory defaults: The Switch should be running after bootup is complete and the SYS LED is blinking. Press and hold the **Reset** button until the SYS LED starts flashing rapidly. Release the **Reset** button.

6. Configuration

This section covers some tasks that are not fully covered in the User Manual (see section Introduction, page 3).

6.1 Accessing the Configuration Interface

There are two configuration options:

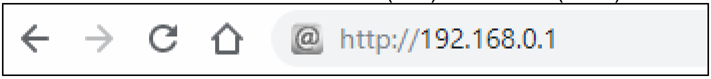
1. Graphical User Interface (GUI), using an Ethernet connection.
2. Command Line Interface (CLI), using a console cable.

6.1.1. Graphical User Interface

For full details, download this document:
http://www.wireless-tek.com/Uploads/download/1583371174.pdf

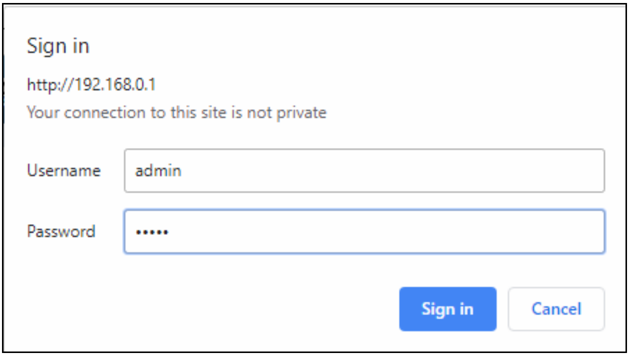
When in Factory Reset state, the Switch is set to use the default IP address of **192.168.0.1**.

1. Make sure that your host system is connected via Ethernet to the Switch.
2. Configure the Ethernet adapter on your host system with a static IP address in the 192.168.0.x subnet.
   e.g. 192.168.0.10
3. Launch your web browser and type **`http://192.168.0.1`** in the address field. Press enter (PC) or return (Mac).



http://192.168.0.1

4. Enter the login credentials.
   The default credentials are:
   Username: admin
   Password: admin



Sign in

http://192.168.0.1

Your connection to this site is not private

Username: admin

Password: •••••

6.1.2. Command Line Interface

For full details, download these documents:

- `https://ubwh.com.au/documents/WI-TEK_CLI.pdf`
- `https://ubwh.com.au/documents/WI-TEK_CLI_POE.pdf`
  (additional CLI commands for POE switches)

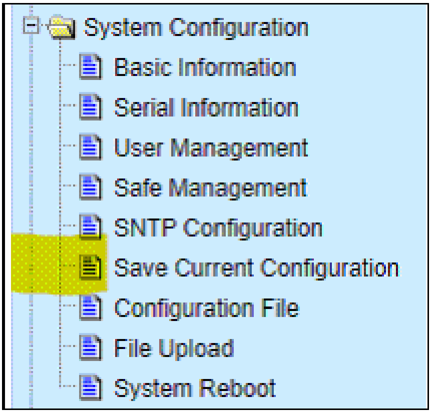
See an example session below, with many lines deleted for clarity.

```
Username:admin
Password:admin
Switch>?
Exec commands:
  show      Show running system information

Switch>show ?
  ip                 Internet Protocol (IP)

Switch>show ip ?
  interface  IP interface status and configuration

Switch>show ip interface brief
Interface     IP-Address    Status        Protocol
ge1/1         unassigned    up            down
```

6.2 Saving Current Configuration

Configuration changes are not permanent, unless saved.

To preserve a configuration change to be used on the next boot-up, save the current configuration using the ***System Configuration / Save Current Configuration*** menu option.

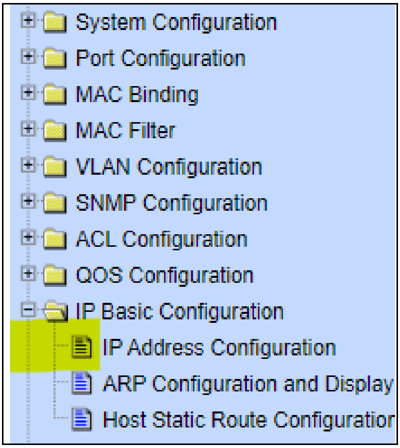


6.3 DHCP IP Address

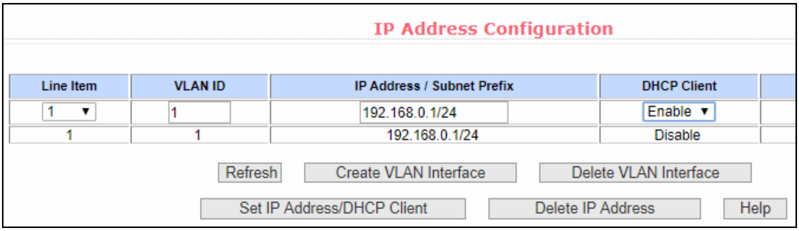
These instructions are to configure the device to obtain its network configuration (IP address, subnet mask, gateway address) from a DHCP server on the same LAN.

After this has been done, consult the DHCP server's list of leases to learn the IP address of the device.

1. Select the ***IP Basic Configuration / IP Address Configuration*** menu selection.



2. Set Line Item to **1**
   Set DHCP Client to **Enable**
   Click **Set IP Address/DHCP Client**



IP Address Configuration

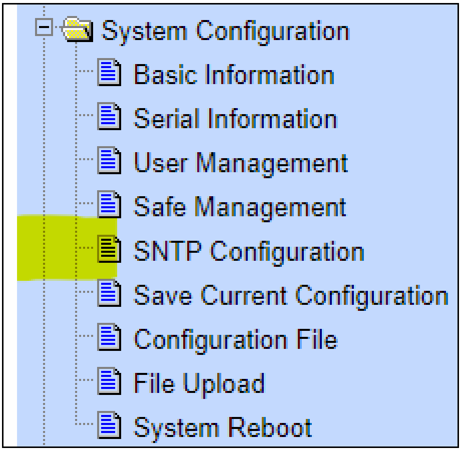
Line Item	VLAN ID	IP Address / Subnet Prefix	DHCP Client	
1 ▼	1	192.168.0.1/24	Enable ▼	
1	1	192.168.0.1/24	Disable	

3. The Switch will now query the LAN DHCP server and move to a new IP address. Consult the DHCP server's list of leases to learn the new IP address of the Switch.

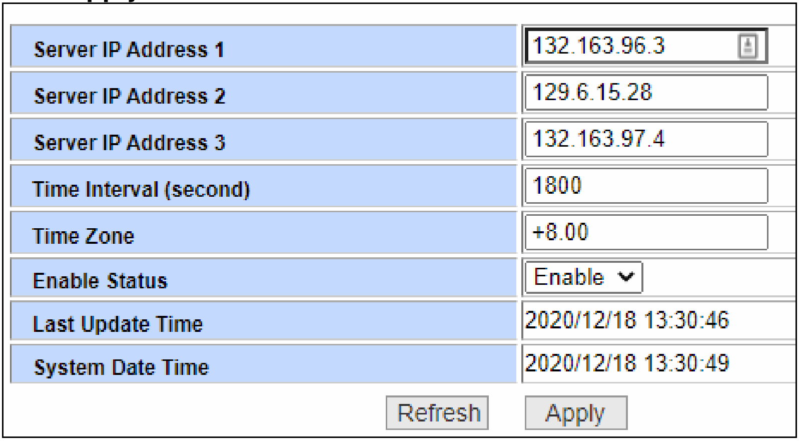
6.4 Network Time Client Setup

By default the Simple Network Time Protocol (SNTP) client is disabled. To enable:

1. Select the ***System Configuration*** / ***SNMP Configuration*** menu selection.



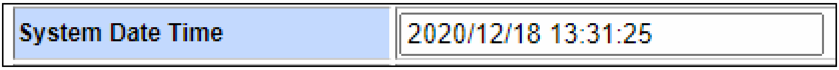
2. Set ***Enable Status*** to ***Enable***,
Set the ***Time Zone***
Enter one or more of the Server IP addresses shown below.
Click **Apply**



Server IP Address 1	132.163.96.3
Server IP Address 2	129.6.15.28
Server IP Address 3	132.163.97.4
Time Interval (second)	1800
Time Zone	+8.00
Enable Status	Enable
Last Update Time	2020/12/18 13:30:46
System Date Time	2020/12/18 13:30:49

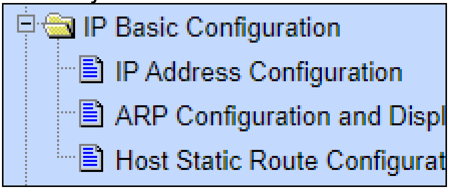
3. Select the ***System Configuration*** / ***Basic Information*** menu option

   You should see the correct time.



System Date Time: 2020/12/18 13:31:25

If the time is incorrect, that indicates the Switch is unable to connect to the Internet. Start by checking the IP Basic Configuration settings to check the IP address, subnet mask, and default gateway are set correctly.



6.5 AAA

Authentication, Authorization and Accounting (AAA) features in the switch can be used as follows:

- **TACACS+:** External authentication for switch **management logins**.
- **802.1x:** External authentication for **user network access**.

6.5.1. TACACS+

The default behaviour is that switch management interface logins are authenticated against the internal switch database, as configured in ***System Configuration*** / ***User Management.***

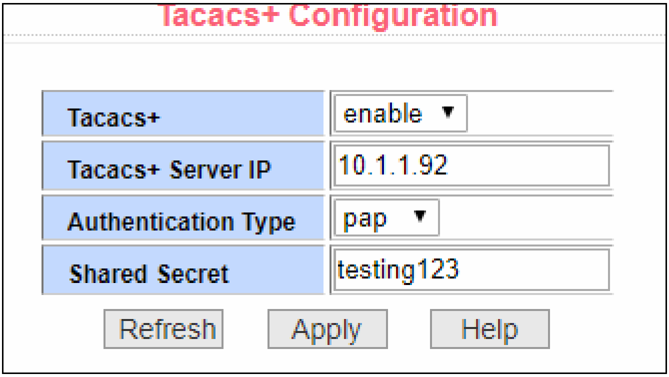
Alternatively, these logins can be authenticated against an external TACACS+ server.

> **WARNING:**
> When you enable & apply TACACS+ authentication, management login to the switch will ONLY use TACACS+. Only save the configuration after confirming you can still login.

1. Setup a TACACS+ server accessible by the switch. Shown below is a simple TACACS+ configuration file that will authenticate switch management logins with Username/Password credentials of admin/admin.

```
# Created by Henry-Nicolas Tourneur(henry.nicolas@tourneur.be)
# See man(5) tac_plus.conf for more details

# Define where to log accounting data, this is the default.
accounting file = /var/log/tac_plus.acct

# This is the key that clients have to use to access Tacacs+
key = testing123

# We also can define local users and specify a file where data
is stored.
# That file may be filled using tac_pwd

group = admins {
  cmd = enable { permit .* }
  cmd = show   { permit .* }
  cmd = ping   { permit .* }
}

user = admin {
    member  = admins
    pap     = des tColoimj9QXZc
    chap    = cleartext admin
    enable  = des tColoimj9QXZc
}
```

2. Select the ***AAA Configuration / Tacacs+ Configuration*** menu option and setup similar to as below and click **Apply**.



Tacacs+ Configuration

Tacacs+	enable
Tacacs+ Server IP	10.1.1.92
Authentication Type	pap
Shared Secret	testing123

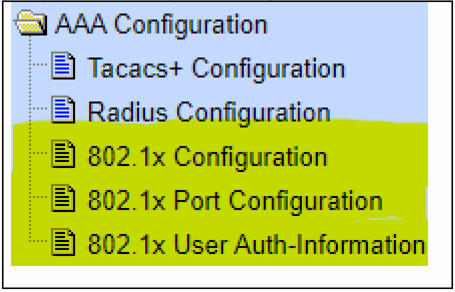
3. In a new browser window, go to the URL of your switch and confirm you can still login.

   If OK: Then select the ***System Configuration*** / ***Save Current Configuration*** menu option and click ***Save***.

   Otherwise: Resolve the TACACS+ problem.

6.5.2. 802.1x (EAP)

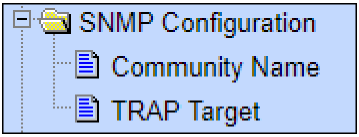
The default switch behaviour can be changed such that devices (e.g. PCs) plugged into specified ports have no network connectivity until authorized.



6.6 SNMP and MIBs

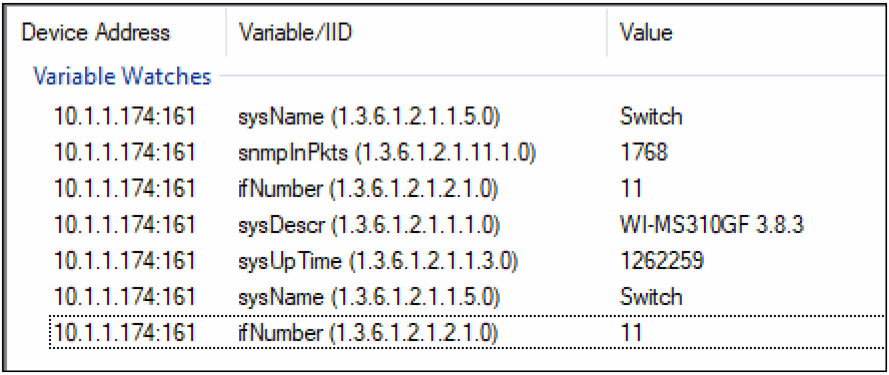
The Switch supports the Simple Network Management Protocol (SNMP). The Management Information Base (MIB) definition files are available from: `https://ubwh.com.au/documents/WiTek-MIBs.zip`

In addition, the Switch can send alerts to a TRAP server.



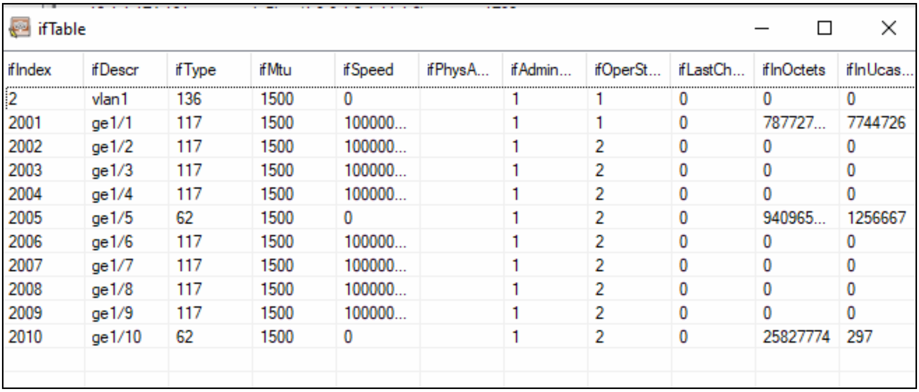
- SNMP Configuration
  - Community Name
  - TRAP Target

Shown below are some example screen captures from a Windows program called ***PowerSNMP Free Manager*** available from `https://www.dart.com/pages/powersnmp-free-manager`



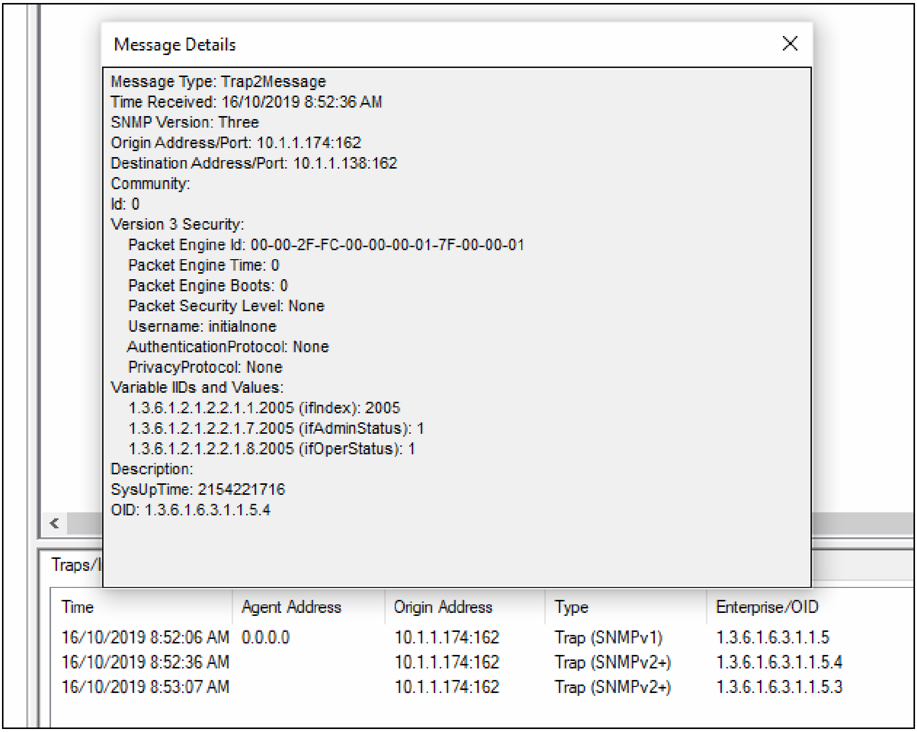
Device Address	Variable/IID	Value
Variable Watches		
10.1.1.174:161	sysName (1.3.6.1.2.1.1.5.0)	Switch
10.1.1.174:161	snmpInPkts (1.3.6.1.2.1.11.1.0)	1768
10.1.1.174:161	ifNumber (1.3.6.1.2.1.2.1.0)	11
10.1.1.174:161	sysDescr (1.3.6.1.2.1.1.1.0)	WI-MS310GF 3.8.3
10.1.1.174:161	sysUpTime (1.3.6.1.2.1.1.3.0)	1262259
10.1.1.174:161	sysName (1.3.6.1.2.1.1.5.0)	Switch
10.1.1.174:161	ifNumber (1.3.6.1.2.1.2.1.0)	11

Figure 1 - Basic SNMP queries



ifIndex	ifDescr	ifType	ifMtu	ifSpeed	ifPhysA...	ifAdmin...	ifOperSt...	ifLastCh...	ifInOctets	ifInUcas...
2	vlan1	136	1500	0		1	1	0	0	0
2001	ge1/1	117	1500	100000...		1	1	0	787727...	7744726
2002	ge1/2	117	1500	100000...		1	2	0	0	0
2003	ge1/3	117	1500	100000...		1	2	0	0	0
2004	ge1/4	117	1500	100000...		1	2	0	0	0
2005	ge1/5	62	1500	0		1	2	0	940965...	1256667
2006	ge1/6	117	1500	100000...		1	2	0	0	0
2007	ge1/7	117	1500	100000...		1	2	0	0	0
2008	ge1/8	117	1500	100000...		1	2	0	0	0
2009	ge1/9	117	1500	100000...		1	2	0	0	0
2010	ge1/10	62	1500	0		1	2	0	25827774	297

Figure 2 Interface Table Query



```
Message Type: Trap2Message
Time Received: 16/10/2019 8:52:36 AM
SNMP Version: Three
Origin Address/Port: 10.1.1.174:162
Destination Address/Port: 10.1.1.138:162
Community:
Id: 0
Version 3 Security:
   Packet Engine Id: 00-00-2F-FC-00-00-00-01-7F-00-00-01
   Packet Engine Time: 0
   Packet Engine Boots: 0
   Packet Security Level: None
   Username: initialnone
   AuthenticationProtocol: None
   PrivacyProtocol: None
Variable IIDs and Values:
   1.3.6.1.2.1.2.2.1.1.2005 (ifIndex): 2005
   1.3.6.1.2.1.2.2.1.7.2005 (ifAdminStatus): 1
   1.3.6.1.2.1.2.2.1.8.2005 (ifOperStatus): 1
Description:
SysUpTime: 2154221716
OID: 1.3.6.1.6.3.1.1.5.4
```

Time	Agent Address	Origin Address	Type	Enterprise/OID
16/10/2019 8:52:06 AM	0.0.0.0	10.1.1.174:162	Trap (SNMPv1)	1.3.6.1.6.3.1.1.5
16/10/2019 8:52:36 AM		10.1.1.174:162	Trap (SNMPv2+)	1.3.6.1.6.3.1.1.5.4
16/10/2019 8:53:07 AM		10.1.1.174:162	Trap (SNMPv2+)	1.3.6.1.6.3.1.1.5.3

Figure 3 Example Received TRAP messages

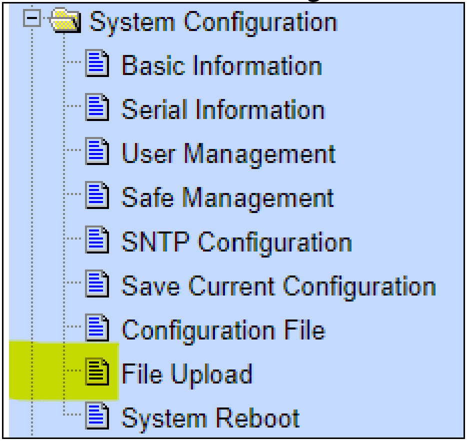
7. Firmware Update

Firmware updates are available from:
`http://www.wireless-tek.com/Support/download`

If there is no firmware there for your product, that means there have been no firmware updates.

7.1 Update using GUI

1. Select the ***IP Basic Configuration*** / ***File Upload*** menu selection.



2. Click **Choose file** and select the *xx.img* file downloaded in section 7.
3. Click **Upload**.
4. Wait until you see:
   File uploaded successfully, please reset switch.
5. Select the ***IP Basic Configuration*** / ***System Reboot*** menu selection
6. Click **Reboot**

7.2 Update using TFTP

See https://ubwh.com.au/documents/WI-TEK_CLI.pdf