



راهنمای نصب ONT

U-TEL G442



راهنمای نصب U-TEL G442 ONT

تاریخ تنظیم: دی ۱۴۰۲

گروه شرکت‌های شاتل

فهرست مطالب

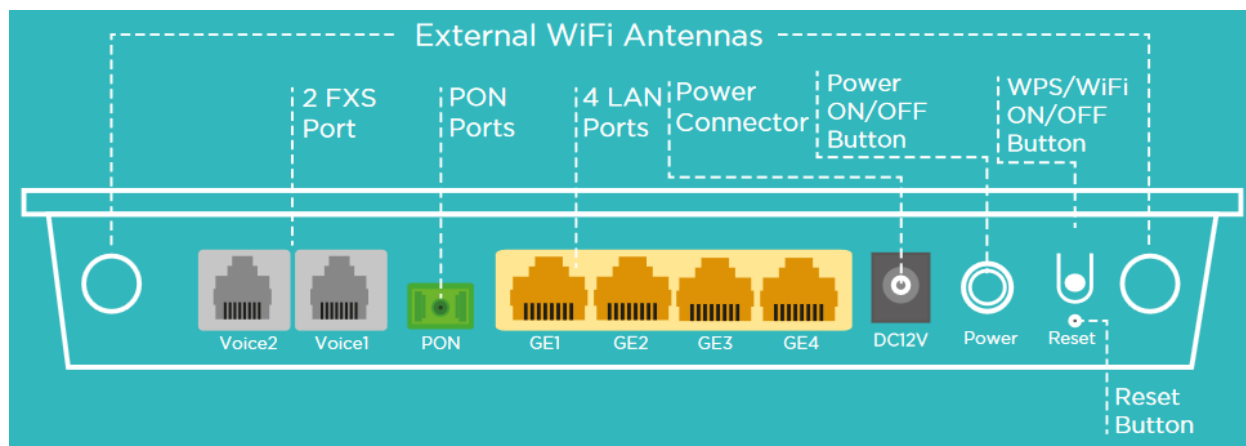
مشخصات فیزیکی ONT
ورود به تنظیمات ONT
صفحه Status
مشاهده Receive Power
تنظیمات اینترنت
تنظیمات وایرلس باند ۲/۴ گیگاهرتز
پیدا کردن کانال های خلوت تر روی باند ۲/۴
تنظیمات وایرلس باند ۵ گیگاهرتز
تنظیمات LAN
تنظیمات DHCP
تنظیمات Port Forward
تنظیمات DMZ
PING گرفتن از داخل کنسول
trace گرفتن از داخل کنسول
ریبوت کردن ONT
ریست کردن و بک آپ گرفتن تنظیمات از داخل کنسول
تغییر رمز پیش فرض کنسول ONT
تنظیمات ACS
Upgrade کردن ONT

مشخصات فیزیکی ONT



پورت های ONT از سمت راست به شرح زیر هستند :

- آداپتور برق برای اتصال دستگاه به برق
- پورت های LAN برای اتصال سیستم کامپیوتری به ONT از طریق کابل شبکه
- پورت PON برای اتصال کابل فیبر نوری به ONT
- پورت voice در صورتی که سرویس voip استفاده میکنید از این پورت استفاده کنید .



تصویر راهنمای تنظیمات ONT موجود در جعبه:





ورود به تنظیمات ONT

به صورت وایرلسی یا با کابل Lan به مودم متصل شوید و ادرس ۱۹۲/۱۶۸/۱/۱ را داخل مرورگر سرچ کنید و با یوزرنیم admin و پسورد admin داخل ONT لاگین کنید.

Tel U.Tel-G442 Login

admin

.....

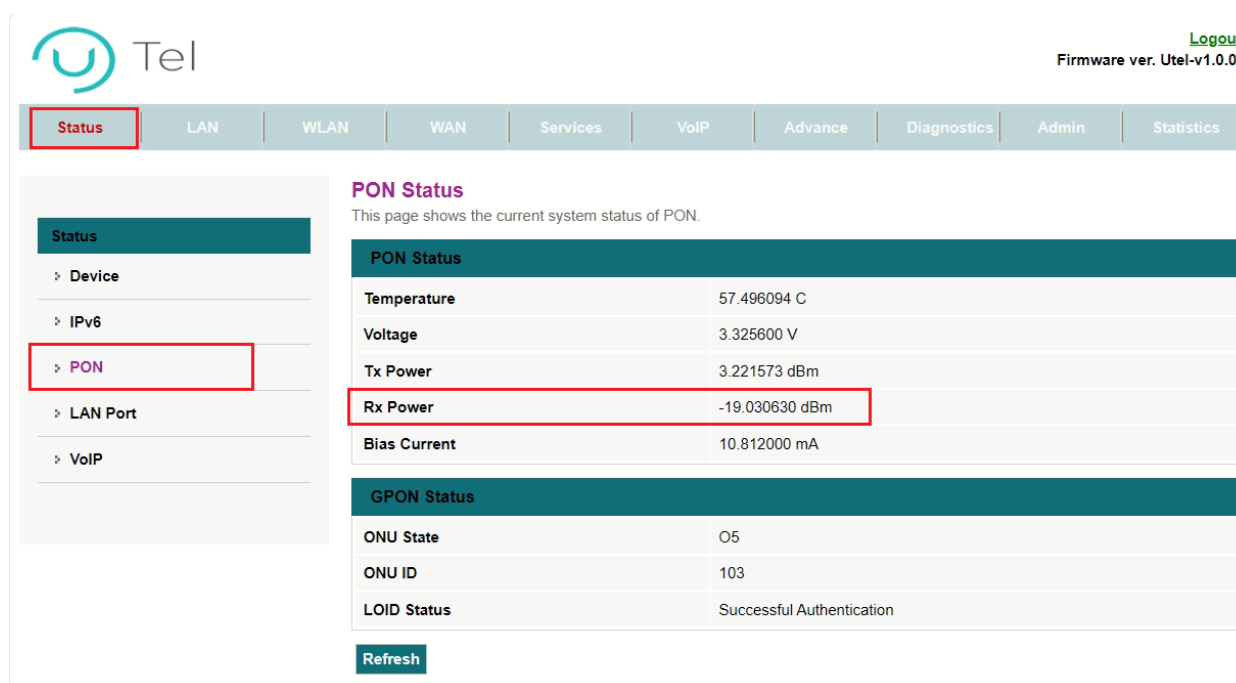
Login

صفحه: Status

در صفحه Status امکان مشاهده وضعیت کلی ONT شامل وضعیت پورت های LAN و دستگاه های متصل به ONT و وضعیت اتصال فیبر وجود دارد.

مشاهده Receive Power

برای مشاهده مقدار Receive Power در صفحه status روی گزینه PON در سمت چپ صفحه کلیک کنید عبارت RX Power پاور دریافتی فیبر را نشان میدهد که این عدد باید بزرگتر از -27 dbm باشد .



PON Status
This page shows the current system status of PON.

PON Status	
Temperature	57.496094 C
Voltage	3.325600 V
Tx Power	3.221573 dBm
Rx Power	-19.030630 dBm
Bias Current	10.812000 mA

GPON Status	
ONU State	O5
ONU ID	103
LOID Status	Successful Authentication

[Refresh](#)

تنظیمات اینترنت

برای انجام تنظیمات اینترنت از منوی بالا گزینه WAN و منوی سمت چپ گزینه PON WAN را انتخاب و موارد زیر را تکمیل نمایید و سپس گزینه apply Changes را بزنید

Channel mode:PPPOE

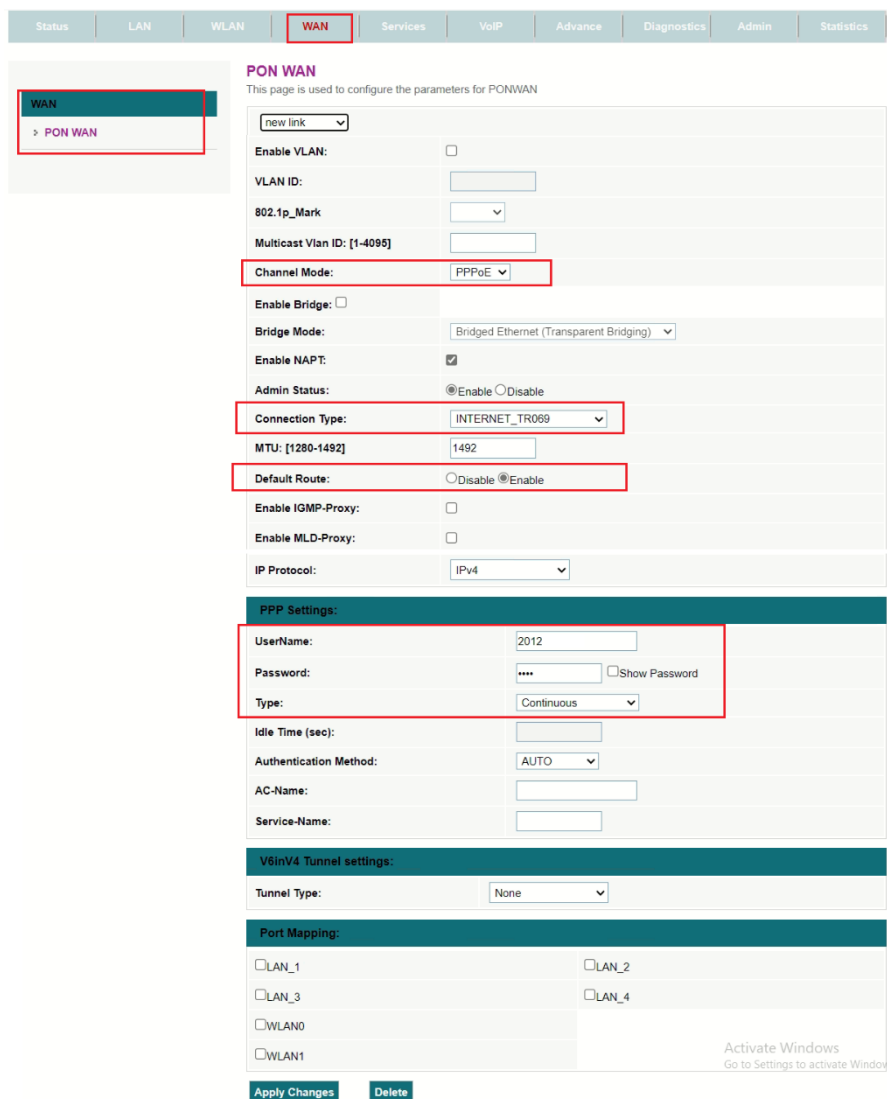
Connection Type: Internet_tr069

Default Route:Enable

Username: شناسه کاربری شاتل

PPPOE پسورد: Password:

Type: continuous



تنظیمات وایرلس باند 2.4GHZ

برای انجام تنظیمات وایرلس از منوی بالا گزینه Wlan را انتخاب کنید و از منوی سمت چپ گزینه Wlan(2.4GHZ) زیر منو Basic settings را انتخاب کنید با زدن دکمه Disable Wlan interface امکان غیر فعال کردن وایرلس وجود دارد تغییرات زیر را انجام دهید و سپس گزینه Apply changes را بزنید

اسم وایرلس مورد نظر SSID:

امکان تغییر کانال وایرلس وجود دارد Channel:

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	------	-----	----------	------	---------	-------------	-------	------------

wlan0 (5GHz)

wlan1 (2.4GHz)

Basic Settings

Advanced Settings

Security

Access Control

Site Survey

WPS

Status

Easy Mesh

WLAN Basic Settings

This page is used to configure the parameters for WLAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

☐ Disable WLAN Interface

Band:

2.4 GHz (B+G+N)

Mode:

AP

Multiple AP

SSID:

UTELB56C

Channel Width:

20/40MHz

Control Sideband:

Upper

Channel Number:

Auto

Radio Power (%):

100%

TX restrict:

0

Mbps (0:no restrict)

RX restrict:

0

Mbps (0:no restrict)

Associated Clients:

Show Active WLAN Clients

☐ Enable Universal Repeater Mode (Acting as AP and client simultaneouly)

SSID of Extended Interface:

repeater_ssid2

Apply Changes

برای انجام تنظیمات امنیتی روی ONT از منوی بالا گزینه Wlan انتخاب و زیر منوی Security انتخاب کنید

رمز وایرلس حداقل ۸ کاراکتر Preshared key:

در تنظیمات security گزینه encryption به صورت پیش فرض wpa3 انتخاب شده برای اتصال مناسب تر همه دستگاه ها ، این گزینه را تغییر ندهید.

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	------	-----	----------	------	---------	-------------	-------	------------

wlan0 (5GHz)

wlan1 (2.4GHz)

Basic Settings

Advanced Settings

Security

Access Control

Site Survey

WPS

Status

WLAN Security Settings

This page allows you setup the WLAN security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Type:

Root AP - UTELB56C

Encryption:

WPA3

H2E:

Capable

Required

IEEE 802.11w:

None

Capable

Required

Cipher Suite:

AES

Group Key Update Timer:

300

Pre-Shared Key:

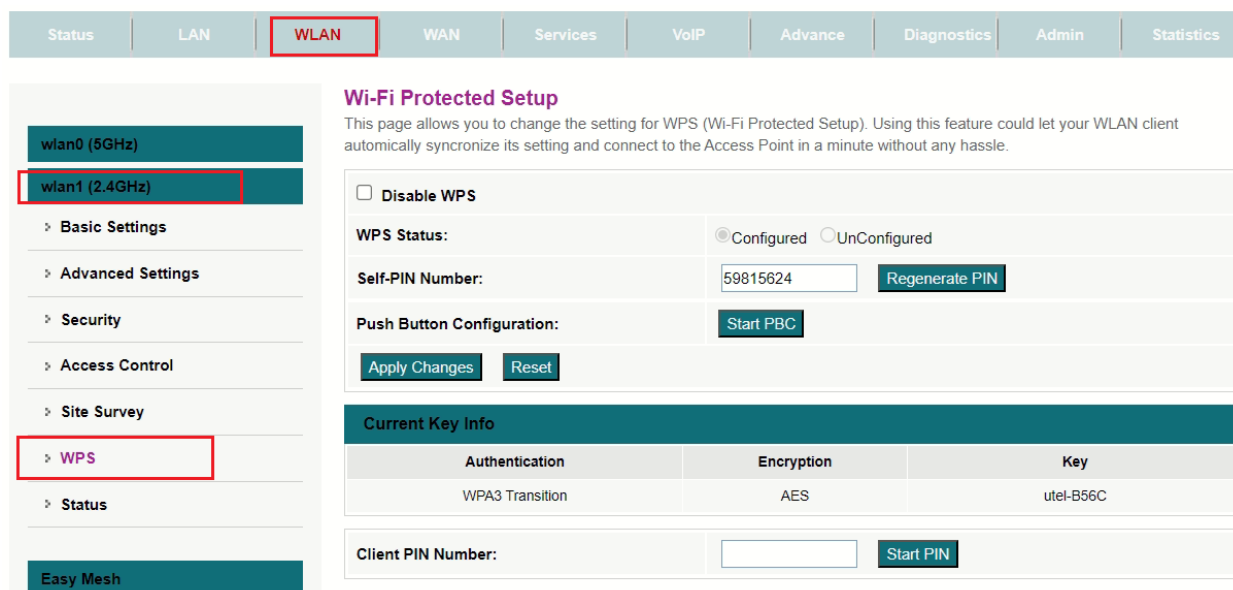
.....

Show Password

Apply Changes

تنظیمات wps باند 2.4GHZ

برای غیر فعال کردن WPS از منوی بالای صفحه گزینه Wlan را انتخاب کنید و از منوهای سمت چپ گزینه WPS انتخاب کنید و گزینه Disable wps را تیک بزنید و سپس Apply Changes را بزنید .



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

WPS Status: ☒ Configured ☐ UnConfigured

Self-PIN Number: 59815624 [Regenerate PIN](#)

Push Button Configuration: [Start PBC](#)

[Apply Changes](#) [Reset](#)

Current Key Info		
Authentication	Encryption	Key
WPA3 Transition	AES	utel-B56C

Client PIN Number: [Start PIN](#)

پیدا کردن کانال های خلوت تر روی باند 2.4GHZ

برای پیدا کردن کانال خلوت تر در محدوده ای که هستید گزینه Wlan بالای صفحه را انتخاب سپس از منوی سمت چپ گزینه Site Survey را انتخاب کنید از روی گزینه Channel در جدول میتوانید خلوت ترین کانال وایرلسی را انتخاب کنید .

Status

LAN

WLAN

WAN

Services

VoIP

Advance

Diagnostics

Admin

Statistics

wlan0 (5GHz)

wlan1 (2.4GHz)

Basic Settings

Advanced Settings

Security

Access Control

Site Survey

WPS

Status

Easy Mesh

WLAN Site Survey

This page provides tool to scan the wireless network. If any Access Point or IBSS is found, you could choose to connect it manually when client mode is enabled.

SSID	BSSID	Channel	Type	Encryption	Signal(%)
DELSAD4D7B0	5c:f4:ab:d4:d7:b0	5 (B+G+N) 20MHz	AP	WPA-PSK/WPA2-PSK	71
shatel-public-wifi	60:31:97:85:0e:3d	1 (B+G+N) 20MHz	AP	WPA2-PSK	64
CTS-Fiber	9c:9d:7e:ea:3c:c2	11 (B+G+N) 20MHz	AP	WPA-PSK/WPA2-PSK	55
Serenti	88:83:22:5d:88:2e	6 (B+G+N) 20MHz	AP	WPA2-PSK	52
shatel-public-wifi	1c:74:0d:ff:b1:71	6 (B+G+N) 20MHz	AP	WPA2-PSK	37
shatel-public-wifi	60:31:97:85:0e:3d	6 (B+G+N) 20MHz	AP	WPA2-PSK	28
Afsane	f4:12:6d:91:96:8d	1 (B+G+N) 20MHz	AP	WPA2-PSK	27
shatel-public-wifi	1c:74:0d:ff:b1:6b	11 (B+G+N) 20MHz	AP	WPA2-PSK	26
saqafi	3c:1e:04:83:58:26	11 (B+G+N) 20MHz	AP	WPA2-PSK	25
Mina	90:8d:78:1f:0c:c3	8 (B+G+N) 20MHz	AP	WPA2-PSK	25
shatel-public-wifi	60:31:97:85:0e:4c	1 (B+G+N) 20MHz	AP	WPA2-PSK	25
shatel-public-wifi	1c:74:0d:ff:b0:69	1 (B+G+N) 20MHz	AP	WPA2-PSK	19

Refresh

Next Step

مک فیلتر روی باند 2.4 GHZ

برای انجام تنظیمات مک فیلتر روی باند 2.4GHZ بعد از پیدا کردن مک دستگاه ها از منوی بالای صفحه گزینه Wlan را انتخاب و از منوهای سمت چپ گزینه Wlan(2.4GHZ) را بزنید. وزیر منوی Access Control را انتخاب کنید Mode: Allow Listed را انتخاب و Apply Changes را بزنید در قسمت Mac Address ادرس مک مورد نظر را بدون : وارد کنید و گزینه Add را بزنید.

Status

LAN

WLAN

WAN

Services

VoIP

Advance

Diagnostics

Admin

Statistics

wlan0 (5GHz)

wlan1 (2.4GHz)

Basic Settings

Advanced Settings

Security

Access Control

Site Survey

WPS

Status

Easy Mesh

WLAN Access Control

If you choose 'Allowed Listed', only those WLAN clients whose MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these WLAN clients on the list will not be able to connect the Access Point.

Mode:

Disabled

Apply Changes

MAC Address:

(ex. 00E086710502)

Add

Reset

Current Access Control List

MAC Address	Select

Delete Selected

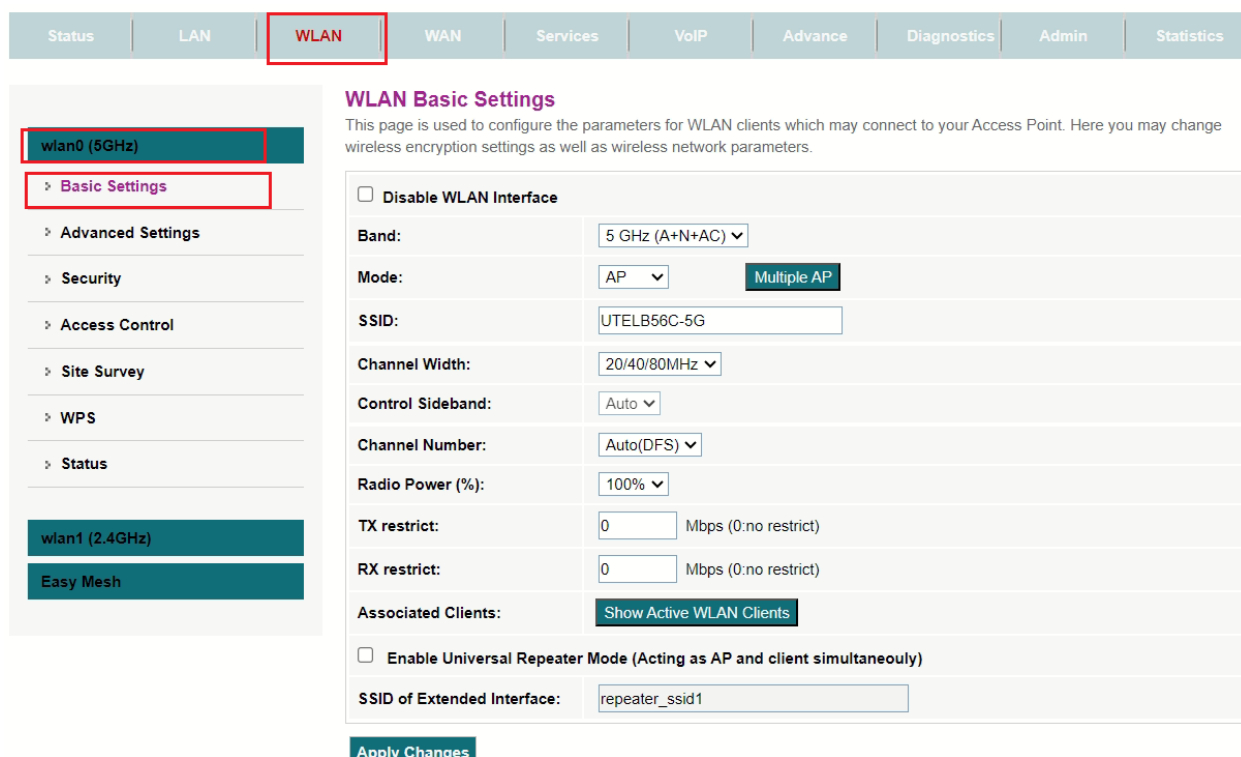
Delete All

تنظیمات وایرلس باند 5GHZ

برای انجام تنظیمات وایرلس از منوی بالا گزینه wlan را انتخاب کنید و از منوی سمت چپ گزینه Wlan(5GHZ) زیر منوی Basic settings را انتخاب کنید با زدن دکمه Disable Wlan interface امکان غیر فعال کردن وایرلس وجود دارد تنظیمات زیر را تغییر دهید و در نهایت برای ذخیره کردن اطلاعات دکمه Apply Changes را بزنید .

اسم وایرلس مورد نظر: SSID:

امکان تغییر کانال وایرلس وجود دارد: Channel:



برای انجام تنظیمات امنیتی روی مودم از منوی بالا گزینه Wlan انتخاب و زیر منوی Security انتخاب کنید

رمز وایرلس حداقل ۸ کاراکتر: Preshared key:

در تنظیمات security گزینه encryption به صورت پیش فرض wpa3 انتخاب شده برای اتصال مناسب تر همه دستگاه ها ، این گزینه را تغییر ندهید.

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	-------------	-----	----------	------	---------	-------------	-------	------------

wlan0 (5GHz)

Basic Settings

Advanced Settings

Security

Access Control

Site Survey

WPS

Status

wlan1 (2.4GHz)

Easy Mesh

WLAN Security Settings

This page allows you setup the WLAN security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

SSID Type:	Root AP - TEST-5G
Encryption:	WPA3
H2E:	<input type="radio"/> Capable <input checked="" type="radio"/> Required
IEEE 802.11w:	<input type="radio"/> None <input type="radio"/> Capable <input checked="" type="radio"/> Required
Cipher Suite:	<input checked="" type="checkbox"/> AES
Group Key Update Timer:	86400
Pre-Shared Key: <input type="checkbox"/> Show Password

Apply Changes

مک فیلتر روی باند 5GHZ

برای انجام تنظیمات مک فیلتر روی باند 5GHZ بعد از پیدا کردن مک دستگاه ها از منوی بالای صفحه گزینه Wlan را انتخاب و از منوهای سمت چپ گزینه Wlan(5GHZ) را بزنید وزیر منوی Access Control را انتخاب کنید Mode: Allow Listed را انتخاب و Apply Changes را بزنید در قسمت Mac Address آدرس مک مورد نظر را بدون : وارد کنید و گزینه Add را بزنید .

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	-------------	-----	----------	------	---------	-------------	-------	------------

wlan0 (5GHz)

Basic Settings

Advanced Settings

Security

Access Control

Site Survey

WPS

Status

wlan1 (2.4GHz)

Easy Mesh

WLAN Access Control

If you choose 'Allowed Listed', only those WLAN clients whose MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these WLAN clients on the list will not be able to connect the Access Point.

Mode:	Allow Listed	Apply Changes
MAC Address:		(ex. 00E086710502)

Add

Reset

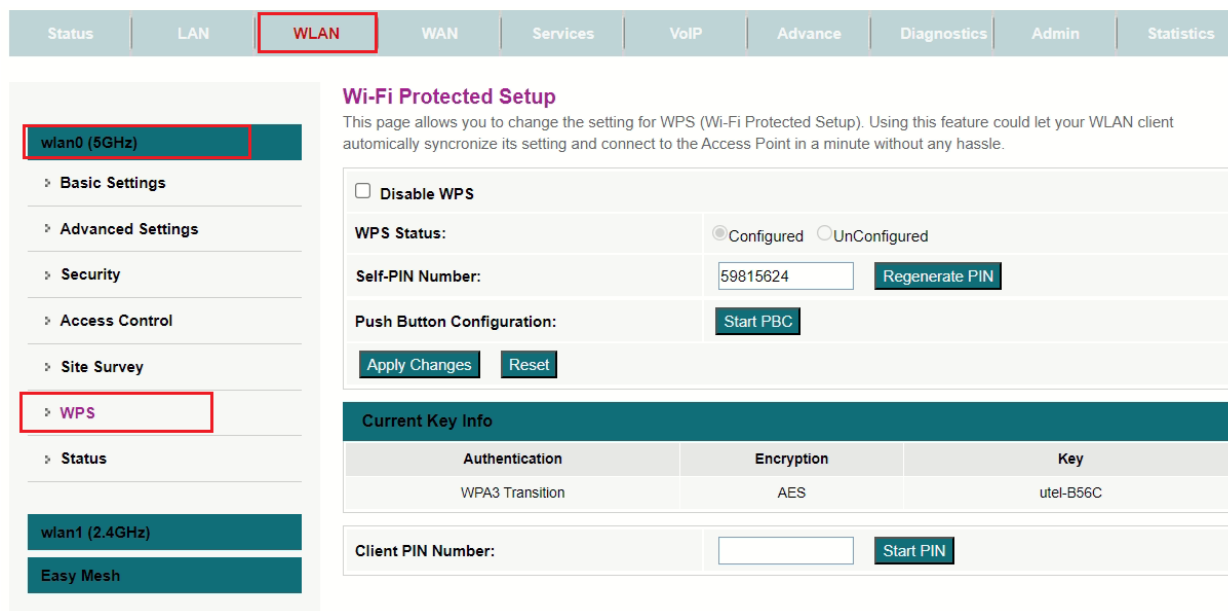
Current Access Control List	
MAC Address	Select

Delete Selected

Delete All

wps روی باند ۵ گیگاهرتز

برای فعال یا غیر فعال کردن Wps در ONT از منوی بالای صفحه گزینه Wlan را انتخاب از منوی سمت چپ گزینه WPS را انتخاب کنید با زدن گزینه Disable WPS و Apply Changes این گزینه غیر فعال میشود .



Wi-Fi Protected Setup

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your WLAN client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

☐ Disable WPS

WPS Status: ☒ Configured ☐ UnConfigured

Self-PIN Number: [Regenerate PIN](#)

Push Button Configuration: [Start PBC](#)

[Apply Changes](#) [Reset](#)

Current Key Info		
Authentication	Encryption	Key
WPA3 Transition	AES	utel-B56C

Client PIN Number: [Start PIN](#)

تنظیمات LAN :

از این قسمت میتوانیم پورت های LAN دستگاه ها Enable و Disable کنیم ، در قسمت پایین صفحه مقابل LAN1 و ... گزینه های Enable و Disable وجود دارد . برای این منظور از منوی بالای صفحه گزینه LAN را انتخاب و سپس از منوهای سمت چپ گزینه Lan Interface Settings را انتخاب میکنیم .

[Status](#) | **[LAN](#)** | [WLAN](#) | [WAN](#) | [Services](#) | [VoIP](#) | [Advance](#) | [Diagnostics](#) | [Admin](#) | [Statistics](#)

LAN

> LAN Interface Settings

LAN Interface Settings

This page is used to configure the LAN interface of your Device. Here you may change the setting for IP addresses, subnet mask, etc..

InterfaceName:	br0
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
IPv6 Link-Local Address Mode:	Static
IPv6 Link-Local Address:	fe80::1
IPv6 DNS Mode:	HGWPProxy
Prefix Mode:	WANDelegated
WAN Interface:	

IGMP Snooping:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Ethernet to Wireless Blocking:	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled

LAN1:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
LAN2:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
LAN3:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
LAN4:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled

Activate Windows
Go to Settings to activate Window

از قسمت status بخش Lan port می‌توانید وضعیت اتصال کابل های Lan رو سرعت اتصال را نیز مشاهده فرمایید:

[Status](#) | [LAN](#) | [WLAN](#) | [WAN](#) | [Services](#) | [VoIP](#) | [Advance](#) | [Diagnostics](#)

Status

- > Device
- > IPv6
- > PON
- > LAN Port**
- > VoIP

LAN Port Status

This page shows the current LAN Port status.

LAN Port Status	
LAN1	not-connected
LAN2	not-connected
LAN3	not-connected
LAN4	Up, 1000Mb, Full

[Refresh](#)

تنظیمات DHCP

برای انجام تنظیمات DHCP از منوی بالای صفحه گزینه Services را انتخاب و از منوهای سمت چپ گزینه DHCP را انتخاب کنید در این صفحه امکان تعریف رنج ای پی های داخلی وجود دارد.

Services

DHCP
Dynamic DNS
IGMP Proxy
UPnP
RIP

Firewall

DHCP Settings

This page is used to configure DHCP Server and DHCP Relay.

DHCP Mode:
☐ NONE
☐ DHCP Relay
☒ DHCP Server
☐ DHCP Client

Enable the DHCP Server if you are using this device as a DHCP server. This page lists the IP address pools available to hosts on your LAN. The device distributes numbers in the pool to hosts on your network as they request Internet access.

LAN IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0

IP Pool Range:	192.168.1.2 - 192.168.1.254	Show Client
Subnet Mask:	255.255.255.0	
Max Lease Time:	86400 seconds (-1 indicates an infinite lease)	
DomainName:	bwrouter	
Gateway Address:	192.168.1.1	
DNS option:	<input checked="" type="radio"/> Use DNS Proxy <input type="radio"/> Set Manually	

Apply Changes
Port-Based Filter
MAC-Based Assignment

تنظیمات Port Forwarding

برای انجام Port Forwarding از منوی بالای صفحه گزینه Services را انتخاب و از منوهای سمت چپ گزینه Firewall را بزنید از زیر منوهای آن Port Forwarding را انتخاب کنید تنظیمات زیر را انجام دهید و add در نهایت را بزنید

Port Forwarding : Enable

Comment: نام دلخواه وارد کنید

Local Ip: آی پی داخلی

Local Port From: پورت مورد نظر:

Local Port to: پورت مورد نظر:

Remote Ip: آی پی مورد نظر:

Remote Port: پورت مورد نظر

Services

Firewall

- IP/Port Filtering
- MAC Filtering
- Port Forwarding**
- URL Blocking
- Domain Blocking
- Parental Control
- DMZ

Port Forwarding

Entries in this table allow 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: ☒ Disable ☐ Enable [Apply Changes](#)

Enable ☒ Application:

Comment	Local IP	Local Port from	Local Port to	Protocol	Remote IP	Remote Port from	Remote Port to	Interface
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Both <input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Any <input type="text"/>

[Add](#)

تنظیمات DMZ

برای انجام تنظیمات DMZ از منوی بالای صفحه گزینه Services را انتخاب و از منوهای سمت چپ گزینه Firewall را انتخاب کنید و وارد زیر منو DMZ شوید و تنظیمات زیر را انجام دهید و در نهایت Apply Changes را بزنید

DMZ Host: Enable

DMZ Host Ip Address: آدرس آی پی داخلی که قصد فعال سازی آن را دارید وارد کنید

Services

Firewall

- IP/Port Filtering
- MAC Filtering
- Port Forwarding
- URL Blocking
- Domain Blocking
- Parental Control
- DMZ**

DMZ Configuration

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

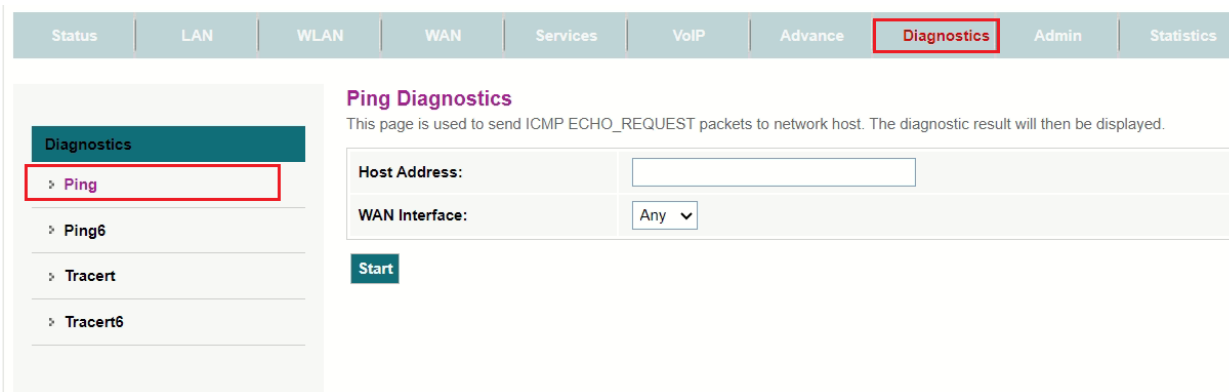
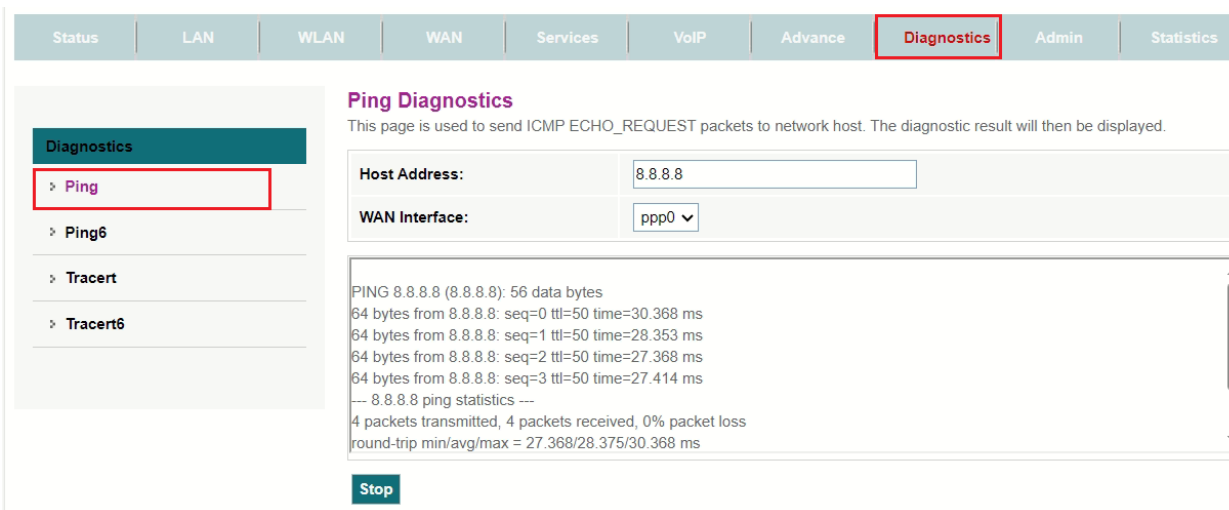
DMZ Host: ☒ Disable ☐ Enable

DMZ Host IP Address:

[Apply Changes](#)

PING گرفتن از داخل کنسول

برای بررسی پینگ از کنسول ONT از منوی بالای صفحه عبارت Diagnostics را انتخاب و از منوهای سمت چپ گزینه Ping را انتخاب کنید در قسمت Host Address مقصدی که قصد دارید پینگ آن را بررسی کنید وارد نمایید و گزینه Start را بزنید .

Trace گرفتن از داخل کنسول:

برای بررسی Trace از داخل ONT از بالای صفحه گزینه Diagnostics انتخاب کنید و از منوی سمت چپ گزینه Trace را بزنید در قسمت Host Address مقصدی که قصد تریس آن را دارید وارد نمایید و گزینه Start را بزنید.

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	------	-----	----------	------	---------	--------------------	-------	------------

Diagnostics

- › Ping
- › Ping6
- › Tracert**
- › Tracert6

Traceroute Diagnostics

This page is used to print the route packets trace to network host. The diagnostic result will then be displayed.

Protocol:	ICMP ▾
Host Address:	<input type="text"/>
Number Of Tries:	<input type="text" value="3"/>
Time out:	<input type="text" value="5"/> s
Data Size:	<input type="text" value="56"/> Bytes
DSCP:	<input type="text" value="0"/>
Max HopCount:	<input type="text" value="30"/>
WAN Interface:	Any ▾

Start

ONT کردن Reboot

برای Reboot کردن Ont از منوی بالای صفحه عبارت Admin را انتخاب از منوی سمت چپ عبارت commit/Reboot را بزنید.

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	------	-----	----------	------	---------	-------------	--------------	------------

Admin

- › Commit/Reboot**
- › Backup/Restore
- › System Log
- › Password
- › Time Zone
- › Logout

Commit and Reboot

This page is used to commit changes to system memory and reboot your system.

Commit and Reboot:	Commit and Reboot
--------------------	--------------------------

backup گرفتن از تنظیمات و ریست کردن ONT

در صورتی که قصد یک آپ گرفتن از تنظیمات ONT را دارد از منوی بالای صفحه گزینه Admin را انتخاب و از منوهای سمت چپ گزینه Backup/Restore را انتخاب کنید تنظیمات گزینه های این صفحه به شرح زیر است :

Backup Settings to File: Backup ONT گرفته می شود

Backup: Restore Settings from File گرفته شده را Restore میکند

ONT: Reset Settings Default را به تنظیمات کارخانه بر میگرداند

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	------	-----	----------	------	---------	-------------	--------------	------------

Admin

Commit/Reboot

Backup/Restore

System Log

Password

Time Zone

Logout

Backup and Restore Settings

This page allows you to backup current settings to a file or restore the settings from the file which was saved previously. Besides, you could reset the current settings to factory default.

Backup Settings to File:

Restore Settings from File:
 No file chosen

Reset Settings to Default:

تغییر رمز پیش فرض کنسول ONT

برای تغییر رمز پیش فرض ورود به تنظیمات ONT از منوی بالای صفحه گزینه Admin را انتخاب و سپس از منوی سمت چپ عبارت Password را انتخاب کنید و تنظیمات زیر را تغییر دهید در نهایت گزینه Apply Changes را بزنید

Old Password: رمز قدیمی

New Password: رمز جدید

Confirmed Password: تکرار رمز جدید

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	------	-----	----------	------	---------	-------------	--------------	------------

Admin

Commit/Reboot

Backup/Restore

System Log

Password

Time Zone

Logout

Password

This page is used to set the account to access the web server of ADSL Router. Empty user name and password will disable the protection.

Login User:	admin
Old Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirmed Password:	<input type="password"/>

تنظیمات ACL

در صورتی که با یوزر Root وارد تنظیمات شویم ، منوی تنظیمات ACL را مشاهده خواهیم کرد:

دقت داشته باشید ، برای تعریف کردن acl روی ONT حتما باید رنج ip مبدا را مشخص کنیم ، در صورتی که تصمیم داریم دسترسی acl برای باز کردن کنسول ONT از شرکت را فراهم کنیم ، به صورت زیر تنظیم کنید:

از بالای صفحه منوی Admin را انتخاب و از زیر منوها گزینه ACL را انتخاب کنید و گزینه های زیر را تغییر دهید و در نهایت گزینه Add را بزنید.

interface : wan

start ip : 192.168.0.0

end ip : 192.168.255.255

Status

LAN

WLAN

WAN

Services

VoIP

Advance

Diagnostics

Admin

Statistics

Admin

GPON Settings

OMCI Information

Commit/Reboot

Backup/Restore

System Log

DOS

Password

Firmware Upgrade

ACL

Time Zone

TR-069

Logout

ACL Configuration

This page is used to configure the IP Address for Access Control List. If ACL is enabled, only the IP address in the ACL Table can access CPE. Here you can add/delete the IP Address.

ACL Capability:

☐ Disable
 ☒ Enable

Apply Changes

Enable:

☒

Interface:

WAN

LAN

WAN

Start IP Address:

End IP Address:

ServiceName	WAN
TELNET	<input type="checkbox"/>
FTP	<input type="checkbox"/>
TFTP	<input type="checkbox"/>
HTTP	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>
SSH	<input type="checkbox"/>
PING	<input type="checkbox"/>

Add

Update Edited

ACL Table					
Select	State	Interface	IP Address	Services	Port
<input type="radio"/>	Enable	LAN	192.168.1.1-192.168.1.255	web,https,ping	80,443,--
<input type="radio"/>	Enable	WAN	192.168.0.0-192.168.255.255	telnet,web,ping	23,80,--

Delete Selected

تنظیمات ACS

از بالای صفحه منوی Admin را انتخاب کرده و از منوهای کنار صفحه گزینه TR-069 را انتخاب کرده و مطابق با تصویر تنظیمات را انجام دهید.

ACS URL: <http://tr069-delsa.net>:9675

Connection Requested path: /tr069

Connection Requested port: 7548

Inform interval: 3600

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	------	-----	----------	------	---------	-------------	-------	------------

Admin

- GPON Settings
- OMCI Information
- Commit/Reboot
- Backup/Restore
- System Log
- DOS
- Password
- Firmware Upgrade
- ACL
- Time Zone
- TR-069**
- Logout

TR-069 Configuration

This page is used to configure the TR-069 CPE. Here you may change the setting for the ACS's parameters.

TR069 Daemon:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Enable CWMP Parameter:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

ACS

URL:	<input type="text" value="http://tr069-delsa.net9675"/>
UserName:	<input type="text" value="username"/>
Password:	<input type="text" value="password"/>
Periodic Inform:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Periodic Inform Interval:	<input type="text" value="3600"/>

Connection Request

Authentication:	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
UserName:	<input type="text" value="My9dQKxLrNw"/>
Password:	<input type="text" value="dUDrwDQgviGZ"/>
Path:	<input type="text" value="/tr069"/>
Port:	<input type="text" value="7548"/>

Certificate Management

CPE Certificate Password:	<input type="text" value="client"/> <input type="button" value="Apply"/> <input type="button" value="Undo"/>
---------------------------	--

Upgrade کردن ONT

جهت Upgrade کردن ONT می‌توانید از منوی بالای صفحه گزینه Admin را انتخاب کرده و پس از انتخاب گزینه FirmWare Upgrade با انتخاب فایل مورد نظر ONT را Upgrade نمایید.

Firmware ver. Utel-V1.0.0

Status	LAN	WLAN	WAN	Services	VoIP	Advance	Diagnostics	Admin	Statistics
--------	-----	------	-----	----------	------	---------	-------------	-------	------------

Admin

- › GPON Settings
- › OMCI Information
- › Commit/Reboot
- › Backup/Restore
- › System Log
- › DOS
- › Password
- › Firmware Upgrade
- › ACL
- › Time Zone
- › TR-069
- › Logout

Firmware Upgrade

This page allows you upgrade the firmware to the newer version. Please note that do not power off the device during the upload because this make the system unbootable.

Browse... No file selected.

Upgrade
Reset