Tunnel 6to4

Enable IPv6: Connection Type:	Tunnel Stad
WAN Connection:	

• WAN Connection - Display the available wan connection.

4.15.3. IPv6 LAN

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to IPv6 > IPv6 LAN and configure the IPv6 LAN settings as needed.

IPv6 LAN Settings	
The parameters of IPv6 LAN can be configured on this page when IPv	6 enabled.
Group:	Default
Address Auto-Configuration Type:	RADVD DHCPv6 Server
Enable RDNSS:	
Enable ULA Prefix:	
Site Prefix Configuration Type:	Delegated Static
Prefix Delegated WAN Connection:	No available interface.
	Save

- Address Auto-Configuration Type Select a type to assign IPv6 addresses to the computers in your LAN. RADVD and DHCPv6 Server are provided. I
- Site Prefix Configuration Type The type of IPv6 address prefix.
 - Delegated Get the IPv6 address prefix from the ISP automatically, and the device will delegate it to the LAN.
 - Static Configure the Site Prefix and Site Prefix Length manually. Please contact your ISP to get more information before you configure them.

Note:

If your IPv6 wan connection type is "Tunnel 6to4", the Site Prefix Configuration Type should be "Static" to make sure "Tunnel 6to4" works properly.

4.16. System Tools

4.16.1. Time Settings

This page allows you to set the time manually or to configure automatic time synchronization. The router can automatically update the time from an NTP server via the internet.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Time Settings.

Settings								
Time Jame	(GM7-0	8.00) Pa	the The	+(05.8.0)	enada) 1	Tijuaka		(*
Dates	1970	Year	1	(Marity	*	(Det)		
Time	8	Hand	41	Mille	40	Second	Get ture PC	71
NIP Aniver 1					in the second	1		
ATP Server 2					in presented			
Get GMT	littere	then the i	oternet a	onnection is	INCOME:			

• To set time manually:

- 1. Select your local Time Zone.
- 2. Enter the Date in Month/Day/Year format.
- 3. Enter the Time in Hour/Minute/Second format.
- 4. Click Save.

• To set time automatically:

- 5. Select your local Time Zone.
- 6. Enter the address or domain of the NTP Server 1 or NTP Server 2.
- 7. Click Get GMT to get time from the internet if you have connected to the internet.

• To set Daylight Saving Time:

- 1. Select Enable Daylight Saving.
- 2. Select the start time from the drop-down list in the Start fields.
- 3. Select the end time from the drop-down list in the End fields.
- 4. Click Save.

Note:

This setting will be used for some time-based functions such as firewall. You must specify your time zone once you log in to the router successfully; otherwise, time-based functions will not take effect.

4.16.2. Diagnostic

Diagnostic is used to test the connectivity between the router and the host or other network devices.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Diagnostic.

Diagnostic Tools		
Diagnostic Parameters		
Diagnority Text	a regi	Tracardulle Start
if addressDomain same		
Phy Lints	4	pingc1 - 991
Prog Pachal State	61	(0-105520-@ytex)
Prog Tennetar.	t	(1-03 (lectricit)
Tracements Mar 175	70	(T - 30)

- Diagnostic Tool Select one diagnostic tool.
 - Ping This diagnostic tool troubleshoots connectivity, reachability, and name resolution to a given host or gateway.
 - Tracerouter This diagnostic tool tests the performance of a connection.

Note:

You can use ping/traceroute to test both numeric IP address or domain name. If pinging/tracerouting the IP address is successful, but pinging/tracerouting the domain name is not, you might have a name resolution problem. In this case, ensure that the domain name you are specifying can be resolved by using Domain Name System (DNS) queries.

- IP Address/Domain Name Enter the destination IP address (such as 192.168.0.1) or Domain name (such as www.tp-link.com).
- Pings Count The number of Ping packets for a Ping connection.
- Ping Packet Size The size of Ping packet.
- Ping Timeout Set the waiting time for the reply of each Ping packet. If there is no reply in the specified time, the connection is overtime.
- Traceroute Max TTL The max number of hops for a Traceroute connection.
- 3. Click Start to check the connectivity of the internet.
- 4. The Diagnostic Results page displays the diagnosis result. If the result is similar to the following figure, the connectivity of the internet is fine.

Diagnostic Results					
Pinging 192.168.0.1 with	64 bytes	of data:			
Reply from 192.168.0.1:	bytes=64	time=1	TTL=64	seq=1	
Reply from 192.168.0.1:	bytes=64	time=1	TTL=64	seq=2	
Reply from 192.168.0.1:	bytes=64	time=1	TTL=64	seq=3	
Reply from 192.168.0.1:	bytes=64	time=1	TTL=64	seq=4	
Ping statistics for 192. Packets: Sent = 4, Rece	168.0.1 ived = 4,	Lost = O	(0% loss)		
Approximate round trip t Minimum = 1, Maximum =	imes in mi 1, Average	llisecond: = l	3:		

4. 16. 3. Firmware Upgrade

TP-Link is dedicated to improving and richening the product features, giving users a better network experience. We will release the latest firmware at TP-Link official website <u>www.tp-link.com</u>. You can download the lastest firmware file from the <u>Support</u> page of our website and upgrade the firmware to the latest version.

- 1. Download the latest firmware file for the router from our website www.tp-link.com.
- 2. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 3. Go to System Tools > Firmware Upgrade.
- 4. Click Choose File to locate the downloaded firmware file, and click Upgrade.

Firmware Upgrade	
Firmware File Path:	Choose File No file chosen
Firmware version:	
Hardware version:	
	Upgrade

4. 16. 4. Factory Defaults

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Factory Defaults. Click Restore to reset all settings to the default values.

Construction of setting other for many lists is being being the second bullet for an excitation of period on the second bullet.
Therein (

- Default Username: admin
- Default Password: admin

- Default IP Address: 192.168.0.1
- Default Subnet Mask: 255.255.255.0

4.16.5. Backup & Restore

The configuration settings are stored as a configuration file in the router. You can backup the configuration file in your computer for future use and restore the router to the previous settings from the backup file when needed.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Backup & Restore.

Backup and Restore	
Backup	
You can restore a previously saved configuration bin file.	

• To backup configuration settings:

Click Backup to save a copy of the current settings in your local computer. A ".bin" file of the current settings will be stored in your computer.

• To restore configuration settings:

1. Click Choose File to locate the backup configuration file stored in your computer, and click Restore.

2. Wait a few minutes for the restoring and rebooting.

Note:

During the restoring process, do not power off or reset the router.

4.16.6. Reboot

Some settings of the router will take effect only after rebooting, including:

- Change the LAN IP Address (system will reboot automatically).
- Change the DHCP Settings.
- Change the Working Modes.
- Change the Web Management Port.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router to its factory defaults (system will reboot automatically).
- Update the configuration with the file (system will reboot automatically).

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Reboot.
- To reboot manually

Click Reboot, and wait a few minutes for the router to rebooting.

System Reboot	
Click Reboot to restart the device without applying any changes to	your current settings.
	Reboot

- To reboot automatically
 - Select Timeout in the drop-down list of Enable Auto Reboot and specify a time period (1-72hours), then the router will reboot automatically after every this interval.

Enable Auto Reboot:	Timeout ~			
	1 Hours 0			Minutes
	Remaining Th	me		

• Select Schedule in the drop-down list of Enable Auto Reboot and specify the Time when the router reboots and Day which to decide how often it reboots.

Schedule
O Everyday 🔿 Select Days
Man Tue Wed Thu Pri Sat Sun
00~ 00~ (Hour:Minute)
The Schedule is based on the time of the Router.

4.16.7. Account Management

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Administrator, and focus on the Account Management section. You can change the factory default username and password of the router.

Account Management	
The username and password must not exce	ed 15 characters in length!
Old Password:	
New User Name:	
New Password:	
Confirm password:	

It is strongly recommended that you change the default username and password of the router, for all users that try to access the router's web-based utility or Quick Setup will be prompted for the router's username and password.

Note:

The new username and password must not exceed 15 characters and not include any spacing.

3. Click Save.

4. 16. 8. Local Management

This feature allows you to block computers on the LAN from accessing the router by using the MAC/IP-based authentication.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Administrator, and focus on the Service Configuration section.

	HTTP: Service	UTSPS Service	Average fixed (PRAC)
Local Nanopenett	Pate	Energia Part - 1	
Suma Management	Numeric Children in	from C Feet	() () () () () () () () () ()

- Allow all LAN conencted devices to manage the router locally
- 1. Keep the Available Host (IP/MAC) empty, which means you don't specify any host to manage the router.
- 2. If you want to access the router via both HTTPS and HTTP, please tick the Enable checkbox in HTTPS Service column. Otherwise, keep it disbled.
- 3. Keep the local management port as default if you don't know which port to use.
- 4. Click Save.

Note:

If the web management port conflicts with the one used for Virtual Server entry, the entry will be automatically disabled after the setting is saved.

Allow a specific device to manage the router locally

- 2. If you want to access the router via both HTTPS and HTTP, please tick the Enable box in HTTPS Service column. Otherwise, keep it disbled.
- 3. Keep the Port as default if you don't know which port to use.
- 4. Click Save.

Note:

If your PC is blocked but you want to access the router again, press and hold the Reset button to reset the router to the factory defaults.

Certificate

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

Certificate Download

4.16.9. Remote Management

This feature allows you to manage your router from a remote location via the internet.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Administrator, and focus on the Service Configuration section.

		WTSt Service	HTSPS Service	Average fixed (PRAC)
Local Nanoperson	PAGE .	111111	Even () Per (-1)	
Names Strengtown	Reason (1)	des	Francis Co Frank	() () () () () () () () () ()

• Forbid all devices to manage the router remotely

Do not tick the Enable checkbox in both HTTP Service and HTTPS Service.

• Allow all devices to manage the router remotely

- 1. Tick the Enable checkbox in HTTP Service.
- 2. If you want to access the router via both HTTPS and HTTP, please tick the Enable checkbox in HTTPS Service column. Otherwise, keep it disbled.
- 3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.
- 4. Click Save.

• Allow a specific device to manage the router remotely

- 1. Tick the Enable checkbox in HTTP Service.
- 2. If you want to access the router via both HTTPS and HTTP, please tick the Enable checkbox in HTTPS Service column. Otherwise, keep it disbled.
- 3. For higher security, you can change the remote management web port by entering a number between 1024 and 65534.
- 5. Click Save.

Certificate

Download and install the certificate for management via HTTPS if you need it. Once the certificate is installed, warnings will not pop up when you access the router via HTTPS.

Certificate Download

Note:

- To access the router, enter your router's WAN IP address in your browser's address bar, followed by a colon and the custom port number. For example, if your router's WAN address is 202.96.12.8, and the port number used is 8080, please enter http://202.96.12.8:8080 in your browser. Later, you may be asked for the router's password. After successfully entering the username and password, you will be able to access the router's web management page.
- Be sure to change the router's default password for security purposes.

4. 16. 10. System Log

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > System Log, and you can view the logs of the router.

:04	e from ALL		Lighteel	dang +	
inter a	line	hie	Louis	fame)	
1.	1479-01-0120-00-00	140/0	hibe	10md ACR to 102 108 (108	
	1070-01-01-02-00	DHORD	1000	Provide Add and a state of the second and a state of the second and the second an	

- Loge Type -By selecting the log type, only logs of this type will be shown.
- Log Level By selecting the log level, only logs of this level will be shown.
- Refresh Refresh the page to show the latest log list.
- Clear Log All the logs will be deleted from the router permanently, not just from the page.

4.16.11. Statistics

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to System Tools > Traffic Statistics.
- 3. Select Enable and click Save. You can view the network traffic of each PC on the LAN, including total traffic and the value of the last Packets Statistic interval in seconds.

Sale Sales								
Talk Salahiri - Litt								
Thefford Last	eti tarrez é los	Ne (1010) Name	Nava Percel 33 4 or		1			
WARNER	Parmin	States .	Pachets	3994	KNO D	10111	118.74	((paiption)
			Gyett	11.695				
		fac	e vill 🛛 🖂 Cele		lakarb -			

4.17. Log out

Click Logout at the bottom of the main menu, and you will log out of the web management page and return to the login window.

Chapter 5

Configure the Router in WISP Mode (Hotspot Mode)

This chapter presents how to configure the various features of the router working as a WISP router (Hotspot router).

It contains the following sections:

- Status
- Operation Mode
- <u>Network</u>
- <u>Wireless</u>
- Guest Network
- <u>DHCP</u>
- Forwarding
- Security
- Parental Controls

- <u>Access Control</u>
- Advanced Routing
- Bandwidth Control
- IP&MAC Binding
- Dynamic DNS
- <u>IPv6</u>
- System Tools
- Log out

5.1. Status

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Status. You can view the current status information of the router.

Status		
	Firmware Version:	1.4.7.3.17 e001.03449 (1912) T-hu 20000
	Hardware Version:	T, MINISTER of BERNINS
LAN		
	MAC Address:	65.FF.78.06.1A.F0
	IP Address:	192,168.0.1
	Subnet Mask:	255.255.255.0
Wireless 2.4GHz	6	
	Operation Mode:	WESP
	Wireless Radio	Enabled
	Name(BSRD):	TP-Link_tAF0
	Mode	11bgn mixed
	Charriet.	8
	Channel Width:	Auto
	MAC Address:	66 FF 78.06-1A.FD
WAN		
	MAC Address	68.FF.70.06.1A:F1
	IP Address:	(Dynamic IP)
	Subnet Mask:	255.255.255.0
	Default Gateway:	192.168.1.1
	DNS Server:	192.368.1.1 0.0.0.0
	System Up Time:	0 diry(s) 00:10:00 Refresh

- Firmware Version The version information of the router's firmware.
- Hardware Version The version information of the router's hardware.
- LAN This field displays the current settings of the LAN, and you can configure them on the Network > LAN page.
 - MAC address The physical address of the router.

- IP address The LAN IP address of the router.
- Subnet Mask The subnet mask associated with the LAN IP address.
- Wireless This field displays the basic information or status of the wireless function, and you can configure them on the Wireless > Basic Settings page.
 - Operation Mode The current wireless working mode in use.
 - Wireless Radio Indicates whether the wireless radio feature of the router is enabled or disabled.
 - Name(SSID) The SSID of the router.
 - Mode The current wireless mode which the router works on.
 - Channel The current wireless channel in use.
 - Channel Width The current wireless channel width in use.
 - MAC Address The physical address of the router.
- WAN This field displays the current settings of the WAN, and you can configure them on the Network > WAN page.
 - MAC Address The physical address of the WAN port.
 - IP Address The current WAN (Internet) IP Address. This field will be blank or 0.0.0.0 if the IP Address is assigned dynamically and there is no internet connection.
 - Subnet Mask The subnet mask associated with the WAN IP Address.
 - Default Gateway The Gateway currently used is shown here. When you use Dynamic IP as the internet connection type, click Renew or Release here to obtain new IP parameters dynamically from the ISP or release them.
 - DNS Server The IP addresses of DNS (Domain Name System) server.
- System Up Time The length of the time since the router was last powered on or reset.

Click Refresh to get the latest status and settings of the router.

5.2. Operation Mode

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Operation Mode.
- 3. Select the working mode as needed and click Save.

Select an Operation Mode:		
O Wireless Router		
O WISP		
O Access Point		
C Range Extender		
Client.		

5.3. Network

5.3.1. WAN

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Network > WAN.
- 3. Configure the IP parameters of the WAN and click Save.

Dynamic IP

If your ISP provides the DHCP service, please select Dynamic IP, and the router will automatically get IP parameters from your ISP.

Click Renew to renew the IP parameters from your ISP.

Click Release to release the IP parameters.

Liniwithin from	Byranni M. • Datur
of Addison-	10.00
There we have a second se	8.0.8.0
(among	8448
	Teres Distant
Million:	[1000] C1000 as select, in relations must be selected as
Franke Kall Franci	*
0.00° value	0 m # 4
Qui P with Drought	20 Win study we required.
that DWD answer manualty.	14
deniel beinner	

- MTU(Bytes) The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- Enable IGMP Proxy IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- Get IP with Unicast A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP address normally, you can choose this option. (It is rarely required.)
- Set DNS server manually If your ISP gives you one or two DNS addresses, select Set DNS server manually and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned automatically from your ISP.
- Host Name -This option specifies the name of the router.

Static IP

If your ISP provides a static or fixed IP address, subnet mask, default gateway and DNS setting, please select Static IP.

WAN Settings	
Connection Type:	Static IP
#* Address	0.0.0
Bubnet Mask:	0.0.0
Gateway:	0.0.0
Primary DNS Server:	0.0.0.0
Secondary DNS Server.	0.0.0 topfore()
MTU(8)N40	1500 (1508 as default, do not change unless necessary)
Enable IGMP Prony:	2
IGMP Version:	0.42 (8.43
	Save

- IP Address Enter the IP address in dotted-decimal notation provided by your ISP.
- Subnet Mask Enter the subnet mask in dotted-decimal notation provided by your ISP. Normally 255.255.255.0 is used as the subnet mask.
- Gateway Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- Primary/Secondary DNS Server (Optional) Enter one or two DNS addresses in dotted-decimal notation provided by your ISP.
- MTU (Bytes) The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. It is not recommended that you change the default MTU size unless required by your ISP.

• Enable IGMP Proxy - IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.

PPPoE

If your ISP provides PPPoE connection, select PPPoE.

WAN Server.	
farindan law	PPTvd: • Denot
THE CONTRACT	
OVO Padjanci	
Confere passesses	
Becordia) Consultant	$\#$ Transet $\hat{\rho}$ (transit Ψ). This Ψ , for that masses
Convertien Made	# man m
	© Senidar Interest
	© Carriel Salary
ter de los	T5 entrude+ (2 meaning connection-service active of all terms)
Aphenistan Type	AUTO_AUTW .
	(invest)
	CEN
the set of	(in an party share server)
Farvet foarter	[106 and total discontinues and a constraints]
PTTL Dome.	1400 11400 as persual, the unit stange primes excenses(s)
Evanis ADAP Provid	*
COMP VALUE	2.12.8.17
tria P antimus sonthad to the	14 III III III III III III III III III I
Rate request mercer	10 10+12 seconds, 3-beaming to begand;
fait 2445 served regrandly	8
	1ee

- PPP Username/Password Enter the user name and password provided by your ISP. These fields are case-sensitive.
- Confirm Password Enter the Password provided by your ISP again to ensure the password you entered is correct.
- Secondary Connection It's available only for PPPoE connection. If your ISP provides an extra connection type, select Dynamic IP or Static IP to activate the secondary connection.
- Connection Mode
 - Always On In this mode, the internet connection will be active all the time.
 - Connect on Demand In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be reestablished when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the Max Idle Time

field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.

- Connect Manually You can click Connect/Disconnect to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.
- Authentication Type Choose an authentication type.

Note:

Sometimes the connection cannot be terminated although you have specified the Max Idle Time because some applications are visiting the internet continually in the background.

- Service Name/Server Name The service name and server name should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- MTU(Bytes) The default MTU size is 1480 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- Enable IGMP Proxy IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- ISP Specified IP Address If your ISP does not automatically assign IP addresses to the router, please select Use IP address specified by ISP and enter the IP address provided by your ISP in dotted-decimal notation.
- Echo Request Interval The router will detect Access Concentrator online at every interval. The default value is 0. You can input the value between 0 and 120. The value 0 means no detect.
- DNS Server/Secondary DNS Server If your ISP does not automatically assign DNS addresses to the router, please select Set DNS server manually and enter the IP address in dotted-decimal notation of your ISP's primary DNS server. If a secondary DNS server address is available, enter it as well.

L2TP

Committee Type	L2TP + Datast
Containe	
Passes	
	Damast 1 Discound 1
Approximp Type	Borance P ← State P
Neve # Address Name	
P Addmin	8.8.8.9
Talenar Much	83.8.8
liamony	8848
CNS Server	8.8.8 9.0.0
Education Address	8384
innerier Disb	8888 9209
SETU: Bylani	1402 S1403 as defeat, so norcharge unexp terminary
Emailes (GHAP Frenz	C 2
(DRF-) wheel	0 # 10 0
Elemented Music	· Advantan
	Canadia bened
	 Carrent elancely
Mat tille Time	15 Manufact 10 reasoning companition termine active at all female

If your ISP provides L2TP connection, please select L2TP.

- Username/Password Enter the username and password provided by your ISP. These fields are case-sensitive.
- Addressing Type Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.
- MTU(Bytes) The default MTU size is "1460" bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- Enable IGMP Proxy IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- Connection Mode
 - Always On In this mode, the internet connection will be active all the time.
 - Connect on Demand In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be reestablished when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.

 Connect Manually - You can click Connect/Disconnect to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

Note:

Sometimes the connection cannot be terminated although you have specified the Max Idle Time because some applications are visiting the internet continually in the background.

PPTP

If your ISP provides PPTP connection, please select PPTP.

WAN Settings	
Connection Type:	PPTP • Detect
Usemame:	
Password:	
	Connect Disconnect
Addressing Type:	Dynamic IP Distatic IP
Server IP Address/Name:	
IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Gateway:	0.0.0.0
DNS Server:	0.0.0.0, 0.0.0.0
Internet IP Address:	0.0.0.0
Internet DNS:	0.0.0. 0.0.0
MTU(Bytes):	1420 (1420 as default, do not change unless necessary)
Enable IGMP Prony.	2
10htlP Version:	0.12 @13
Connection Mode:	Always on
	Connection demand
	Connect manually
Max idle Time:	15 minutes (0 meaning connection remains active at all times)

- Username/Password Enter the username and password provided by your ISP. These fields are case-sensitive.
- Addressing Type Choose the addressing type given by your ISP, either Dynamic IP or Static IP. Click the Connect button to connect immediately. Click the Disconnect button to disconnect immediately.
- MTU(Bytes) The default MTU size is "1420" bytes, which is usually fine. It is not recommended that you change the default MTU Size unless required by your ISP.
- Enable IGMP Proxy IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.

- Connection Mode
 - Always On In this mode, the internet connection will be active all the time.
 - Connect on Demand In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be reestablished when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - Connect Manually You can click Connect/Disconnect to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

Note:

Sometimes the connection cannot be terminated although you have specified the Max Idle Time because some applications are visiting the internet continually in the background.

BigPond Cable

If your ISP provides BigPond cable connection, please select BigPond Cable.

WAN Settings	
Connection Type:	RieBurd Cable R Detect
	Digrono Cable * Direct
Usemane:	
Password:	
Auth Server.	
Auth Domain:	
MTU(Bytes):	1500 (1500 as default, do not change unless necessary)
Enable (GMP Proxy:	2
IOMP Version:	© v2 ⊛ v3
Connection Mode:	Always on
	Connect on demand
	Connect manually
Max Idle Time:	15 minutes (0 meaning connection remains active at all times)
	Connect Disconnect
	Seve

- Username/Password Enter the username and password provided by your ISP. These fields are case-sensitive.
- Auth Server Enter the authenticating server IP address or host name.
- Auth Domain Type in the domain suffix server name based on your location.

- MTU(Bytes) The default MTU size is 1500 bytes. It is not recommended that you change the default MTU size unless required by your ISP.
- Enable IGMP Proxy IGMP (Internet Group Management Protocol) is used to manage multicasting on TCP/IP networks. Some ISPs use IGMP to perform remote configuration for client devices, such as the modem router. The default value is enabled, and if you are not sure, please contact your ISP or just leave it.
- Connection Mode
 - Always On In this mode, the internet connection will be active all the time.
 - Connect on Demand In this mode, the internet connection can be terminated automatically after a specified inactivity period (Max Idle Time) and be reestablished when you attempt to access the internet again. If you want to keep your internet connection active all the time, please enter 0 in the Max Idle Time field. Otherwise, enter the number of minutes you want to have elapsed before your internet access disconnects.
 - Connect Manually You can click Connect/Disconnect to connect/disconnect immediately. This mode also supports the Max Idle Time function as Connect on Demand mode. The internet connection can be disconnected automatically after a specified inactivity period (Max Idle Time) and not be able to re-establish when you attempt to access the internet again.

5.3.2. LAN

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Network > LAN.
- 3. Configure the IP parameters of the LAN and click Save.

	10 FE 70 AL 14 FA	
MAG Address:	08:FF:78:00:1A:F0	
IP Address:	192.168.0.1	
Subnet Mask:	255.255.255.0	

- MAC Address The physical address of the LAN ports. The value can not be changed.
- IP Address Enter the IP address in dotted-decimal notation of your router (the default one is 192.168.0.1).

• Subnet Mask - An address code that determines the size of the network. Normally 255.255.255.0 is used as the subnet mask.

Note:

- If you have changed the IP address, you must use the new IP address to log in.
- If the new IP address you set is not in the same subnet as the old one, the IP address pool in the DHCP Server will be configured automatically, but the Virtual Server and DMZ Host will not take effect until they are re-configured.

5. 3. 3. MAC Clone

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Network > MAC Clone.
- 3. Configure the WAN MAC address and click Save.

ire Factory MAC
e MAC Address

- WAN MAC Address This field displays the current MAC address of the WAN port. If your ISP requires you to register the MAC address, please enter the correct MAC address in this field. Click Restore Factory MAC to restore the MAC address of WAN port to the factory default value.
- Your PC's MAC Address This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click Clone MAC Address and this MAC address will be filled in the WAN MAC Address field.

Note:

- You can only use the MAC Address Clone function for PCs on the LAN.
- If you have changed the WAN MAC address when the WAN connection is PPPoE, it will not take effect until the connection is re-established.

5.4. Wireless

5. 4. 1. Basic Settings

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Wireless > Basic Settings.
- 3. Configure the basic settings for the wireless network and click Save.

Worked Settings	
Clern Belling	
WHERE is integral.	
100.C destinantio as insignals	A & B 10 00 F 11 20 31 (Loss to M
	- Ann
Res Turn	weat-rac
WOT holes:	(t)
Automation Type	rises fareer
Erreption	H2 2
Works Passeril	()
AP Setting	
Western Marco	[] Alter called TERTS
Children of Childr	
	Annual Control of Cont

- Client Settings The settings of the public Wi-Fi your router is going to connect to.
 - SSID(to be bridged) The SSID of the public Wi-Fi your router is going to connect to as a client.
 - MAC Address(to be bridged) The MAC address of the public Wi-Fi your router is going to connect to as a client.
 - Lock to AP If selected, the device's connection will be restricted to only the network with this specific MAC address.
 - Scan Click this button to search the public Wi-Fi.
 - Key type Select the key type according to the public Wi-Fi's security configuration. It is recommended that the key type is the same as the public Wi-Fi's security type.
 - WEP Index Select which of the four keys will be used if the key type is WEP (ASCII) or WEP (HEX).
 - Authentication Type Select the authorization type if the key type is WEP (ASCII) or WEP(HEX).
 - Encryption Select the encryption type is the key type is WPA-PSK or WPA2-PSK.
 - Password Enter the public Wi-Fi's password if required.
- AP Settings The wireless settings of your router.
 - Local Wireless Network Name Enter a string of up to 32 characters. It is strongly recommended that you change your network name (SSID). This value is case-sensitive. For example, TEST is NOT the same as test.
 - Mode You can choose the appropriate "Mixed" mode.

- Channel This field determines which operating frequency will be used. The default channel is set to Auto. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- Channel Width This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point. If you select auto, then AP will choose the best channel automatically.
- Enable SSID Broadcast If enabled, the router will broadcast the wireless network name (SSID).

5.4.2. WPS

WPS (Wi-Fi Protected Setup) can help you to quickly and securely connect to a network. This section will guide you to add a new wireless device to your router's network quickly via WPS.

Note:

The WPS function cannot be configured if the wireless function of the router is disabled. Please make sure the wireless function is enabled before configuration.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Wireless > WPS.
- 3. Follow one of the following three methods to connect your client device to the router's Wi-Fi network.

Method ONE: Press the WPS Button on Your Client Device

1. Keep the WPS Status as Enabled and click Add Device.

WPE (W/F) Protected Setup)			
	Enabled	Disable	
Correct Pile	12345678	Restore PM	Generate New PIN
Add a base during	Add dev	ice .	

2. Select Press the WPS button of the new device within the next two minutes and click Connect.

 Enter 	mew device	PIN				
FIN:						
· Press	the WPS b	uttan of the new	r device within	the next two min	2995	

- 3. Within two minutes, press the WPS button on your client device.
- 4. A success message will appear on the WPS page if the client device has been successfully added to the router's network.

Method TWO: Enter the Client's PIN

1. Keep the WPS Status as Enabled and click Add Device.

WPS (W-F) Protoclast Setup)			
WE	Enabled	Disable	
Current Pite	12345678	Restore Pill	Generate New PIN
Add a twee devices	Add dev	ica 🔄	

2. Select Enter new device PIN, enter your client device's current PIN in the PIN filed and click Connect.

· Tribe	new device PIN				
PINE					
© Presi	the WPS button	of the new device	e within the pert larg	minutes.	

3. A success message will appear on the WPS page if the client device has been successfully added to the router's network.

Method Three: Enter the Router's PIN

1. Keep the WPS Status as Enabled and get the Current PIN of the router.

(APS (W/7) Protected Setup)			
WE	Enabled	Disable	
Current Pite	12345678	Restore PM	Generate New PIN
Add a turn during	Add devi		

2. Enter the router's current PIN on your client device to join the router's Wi-Fi network.

5. 4. 3. Wireless Security

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Wireless > Wireless Security.
- 3. Configure the security settings of your wireless network and click Save.

when the provide the second statement of the second s	and 35.8" sharpplices are pro-	of pages and with WFS eventsed	
Provide Managers Sciences			
Contraction of the local			
a WARRAD Personal Reconstruction			
Weiter	10PA2-P58. •		
Gertariae	AEI •		
Witnesser Parameter	#7336003		
Would Key Linkson Perfort	8		
WINAWAY LINEARS			
Wow	A41		
Compton	And a		
BARNUS Same P			
RADIAL Server Part	DEC LIGHT	Linear in default and 19121	
RADIUS Deven Passent			
Group Key Garlete Period			
	374		
o wer	10012 A 10022 - 10		
ALTERNITION THE	Geen System .		
INCO AND FATTURE	Haadecingi •		
Deserved Puty	WEP-may	day t	1940
Far 1		Disate	Acf. +
649.1 U		Devado	- 1n
Pag 2		Divet	411 +
Page 4. (1)		Datable	101 + 310

• Disable Wireless Security - The wireless security function can be enabled or disabled. If disabled, wireless clients can connect to the router without a password. It's strongly recommended to choose one of the following modes to enable security.

- WPA-PSK/WPA2-Personal It's the WPA/WPA2 authentication type based on preshared passphrase.
 - Version Select Auto, WPA-PSK or WPA2-PSK.
 - Encryption Select Auto, TKIP or AES.
 - Wireless Password Enter ASCII or Hexadecimal characters. For Hexadecimal, the length should be between 8 and 64 characters; for ASCII, the length should be between 8 and 63 characters.
 - Group Key Update Period Specify the group key update interval in seconds. The value can be 0 or at least 30. Enter 0 to disable the update.
- WPA /WPA2-Enterprise It's based on Radius Server.
 - Version Select Auto, WPA or WPA2.
 - Encryption Select Auto, TKIP or AES.
 - RADIUS Server IP Enter the IP address of the Radius server.
 - RADIUS Server Port Enter the port that Radius server used.
 - RADIUS Server Password Enter the password for the Radius server.
 - Group Key Update Period Specify the group key update interval in seconds. The value should be 30 or above. Enter 0 to disable the update.
- WEP It is based on the IEEE 802.11 standard.
 - Authentication Type The default setting is Auto, which can select Shared Key or Open System authentication type automatically based on the wireless client's capability and request.
 - WEP Key Format Hexadecimal and ASCII formats are provided here. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
 - WEP Key Select which of the four keys will be used and enter the matching WEP key. Make sure these values are identical on all wireless clients in your network.
 - Key Type Select the WEP key length (64-bit, 128-bit or 152-bit) for encryption. Disabled means this WEP key entry is invalid.
 - 64-bit Enter 10 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 5 ASCII characters.
 - 128-bit Enter 26 hexadecimal digits (any combination of 0-9, a-f and A-F. Null key is not permitted) or 13 ASCII characters.

5. 4. 4. Wireless MAC Filtering

Wireless MAC Filtering is used to deny or allow specific wireless client devices to access your network by their MAC addresses.

I want to:

Deny or allow specific wireless client devices to access my network by their MAC addresses.

For example, you want the wireless client A with the MAC address 00:0A:EB:B0:00:0B and the wireless client B with the MAC address 00:0A:EB:00:07:5F to access the router, but other wireless clients cannot access the router

How can I do that?

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Wireless > Wireless MAC Filtering.
- 3. Click Enable to enable the Wireless MAC Filtering function.
- 4. Select Allow the stations specified by any enabled entries in the list to access as the filtering rule.
- 5. Delete all or disable all entries if there are any entries already.
- 6. Click Add New and fill in the blank.

You can configure Wireless MAC Filterity	j which allows you to control sensions accous on the network
trafar.	
MAC Amireur	00 NA 58-90:00 08
Description	Client A
Status	Enabled ~

- 1) Enter the MAC address 00:0A:EB:B0:00:0B / 00:0A:EB:00:07:5F in the MAC Address field.
- 2) Enter wireless client A/B in the Description field.
- 3) Select Enabled in the Status drop-down list.
- 4) Click Save and click Back.
- 7. The configured filtering rules should be listed as the picture shows below.

WEIGHT BUILT	following trained Dr	uitte			
Printing Treasure					
(1.00m) THE IS	tony specified to any analysis	without in the last to assume	66.		
and the second s					
	much through the sound to	errites in the Distribution			
	MAL Address	Andreas in Frankrike proce	war.	Description	14
	MAI Astron	Police Follow Encount	wer Tripp, bar	Generation: start.6	i de Edit
	 WAL Address Architel Scheme Architel Scheme Architel Scheme 	Printer in Fre Solite pros Pallan Ensemen Filosofie	NUM THEORY, DATE THEORY, DATE	Description start A Title B	Lat Lat

Done!

Now only client A and client B can access your network.

5. 4. 5. Wireless Advanced

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Wireless > Wireless Advanced.

3. Configure the advanced settings of your wireless network and click Save.

Note:

If you are not familiar with the setting items on this page, it's strongly recommended to keep the provided default values; otherwise it may result in lower wireless network performance.

Wireless Advanced		
Transmit Power:	High •	
Beacon Interval:	100	(40-1000)
RTS Threshold:	2346	(1-2346)
Fragmentation Threshold:	2345	(256-2346)
D'TIM Interval:	1	(1-15)
	🗷 Enable Shi	ort Gi
	🔲 Enable Clie	ent Isolation
	Enable Wi	IM .
		Save

- Transmit Power Select High, Middle or Low which you would like to specify for the router. High is the default setting and recommended.
- Beacon Interval Enter a value between 40-1000 milliseconds for Beacon Interval here. Beacon Interval value determines the time interval of the beacons. The beacons are the packets sent by the router to synchronize a wireless network. The default value is 100.

- RTS Threshold Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the router will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2346.
- Fragmentation Threshold This value is the maximum size determining whether packets will be fragmented. Setting a low value for the Fragmentation Threshold may result in poor network performance because of excessive packets. 2346 is the default setting and is recommended.
- DTIM Interval This value determines the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. You can specify the value between 1-255 Beacon Intervals. The default value is 1, which indicates the DTIM Interval is the same as Beacon Interval.
- Enable Short GI It is recommended to enable this function, for it will increase the data capacity by reducing the guard interval time.
- Enable Client Isolation This function isolates all connected wireless stations so that wireless stations cannot access each other through WLAN. This function will be disabled if WDS/Bridge is enabled.
- Enable WMM WMM function can guarantee the packets with high-priority messages being transmitted preferentially. It is strongly recommended to enable this function.

5. 4. 6. Wireless Statistics

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Wireless > Wireless Statistics to check the data packets sent and received by each client device connected to the router.

Wrei	ess Stations Currently Conne	cted: 1 Refresh			
(D)	MAC Address	Current Status	Received Packets	Sent Packets	\$\$ID
1	44.00.10/07/38/A7	Associated	29	19	101-1000, 1107, 3 Household

- MAC Address The MAC address of the connected wireless client.
- Current Status The running status of the connected wireless client.
- Received Packets Packets received by the wireless client.
- Sent Packets Packets sent by the wireless client.
- SSID SSID that the station associates with.

5.5. Guest Network

Guest Network allows you to provide Wi-Fi access for guests without disclosing your host network. When you have guests in your house, apartment, or workplace, you can create a guest network for them. In addition, you can customize guest network settings to ensure network security and privacy.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Guest Network.
- 3. Enable the Guset Network function.
- 4. Create a network name for your guest network.
- 5. Select the Security type and create the Password of the guest network.
- 6. Select Schedule from the Access Time drop-down list and customize it for the guest network.
- 7. Click Save.

inter line	in the Access by Level Meleont.	Cautte	- S-				
	Date Testsork yaraba.	Obsattle					
1.00	errietun Semant Cartor	Cluttle					
		2.252.5	1				
	Superior Management		nume				
	Transient married	11-13-6 16	anc 3900				
	No. No. 10 Ave.	1					
	2624	WEAVER,	J-Petral	•			
	Advertisation Type	Auto					
	Tecolulu	Add	٠				
	Wesseld, Passessing	01234567					
		-0 mile 442.0	Destro M	mit 3 and	55 (c + inc)	decimal d	Considers failement
	Group Kiru Lipsien Perint	0	(Hecteria)	line-	120.2	******	199
	Li Cale		_				
	- The second sec	1 Million and Million and Million and Million					
The Review of States	tions for last home in the same if	Schedon		a manufactor			
Old To printing this is birthin is based on the line	Total Res Teld Lattice (s. 12 percent)	a president and other	att in head to	-	out of an	-	
Cital Pay antisakan Arbis in Intelain is knowed on Rachter	river for field builty is 10 years if of the Reader The loss and in the	e period air old I in Thomas To	nti pon teant liv	a pand bat	and of last	-	
This We consider table to ballely is bound on the little	inee Box Teld Landso (n. 22 hours B of the Vender The Vene Lan be of Witerwei Telfandere	Contraction a previously with the line "Receiver for the Receiver	ett over tened for m - Jana Jan # Donation	r pand het	est of ad	-	
Appg To	name for both tenter in these if of the booter the two-car is of the booter the two-car is of the booter Start fails	Contraction in product on other the Theorem Ton the Theorem Ton	nti proy honed the min - Jama (pert min Docations and Falsan	r pand had	and of and	and all	
Apply 14 Card Day	Name and other lead families in attempt of other Name The Nove Last into or Ultimeters Schweiser States Familie States Familie States Familie	Catendaria e period ai alt for Taxent for to Examine 1 1 24	anti pera menal de mi - Jana, Jana - Donativa - Manalita - Manalita - Manalita - Manalita - Manalita			Att	
Appin To Cash Day	noo ike ladi kalis la itana ik ofte kale Ta kesi lai is o tilena fakis kan faki bi bi -	Schebn e pelad al alt de "honere fu i) fonder j.j.	nti pro scali de m - Jum jet e Donation mai Palen 20				
Appin To Cash Day	March and South So	Surfacebox e period on oth for Thomas for () Fromber () 24 () 24 (nti per send la - Juni Jett - Donative and Rose 00 100 Juni 100	- panel (ref			
Appin Fe	Normal Sectors of the Sectors of the Order Texa Sector Texa Sectors Texa Sectors of Texa Sectors of Texas Se	Suffeedan e period an off die Thomas for O Thomas (34) al anni Sout	nti ony kenditi - Juni Jett + Donative Ind False Ind False			44	
Agen fo Each Day	Normal Sea of the black balls in the statement is of the blacker. The break sea is an University Schweizer. State Land Sea 2000 - 1000 2000 200 Date State	Collection a product of the collection for the "Scorestor (24) all a real (244)	 A second design of the second design o	, panel 144		in an	
Appin Fit	Normal and other hands the bost and an or other handler. The bost and the of Historic Tables Bill 20 • These Bill 20 • These Bill 20 • These Bill 20 • These Bill 20 •	Columbas e period of off the "horsen for () founder () () () () () () () () () () () () ()	n par sent te - <u>Jan be</u> + Dentite Ind Fate DI •			4.9	
Apply To Catholic is bound on the little Apply To Catholic is the second of the little Apply To	Normal Sea of the field factor in a constraint of the field of the fi	Collection a previous of the tile "therefore for Collection for (34) 134 134 134 134 134 134 134 134	nti sen teni te m - Juni teni e Drontes and Fans 01	i kan si		44	
Apply 14 East Day	Normal Sea of the field factor is a comparison of of the field of the last is a comparison of the mean of the field of the last Sea of the last is a comparison of the last Sea of the last is a comparison of the last Sea of the last is a comparison of the last Sea of the last is a comparison of the last is a comparison of the last Sea of the last is a comparison of the last is a compa	Echeba a print of the fire the set for \odot from the \odot from the from the \odot from the from the from the \odot from the from the from the from the from the from the from	ati per send to a - Juni Jati 4 Doutes nel fram 10	i kan si			
Apply 14 (Each Day)	Normal Series (Series Series Ser	Extension in the theorem for the the theorem for the the theorem for the the the theorem for the the the the theorem for the the theorem for the the the the the theorem for the the the the the the the the the the	att inn weat (b w - Juni (et w Doutin nd Flow the 2-94 (b)			44	
Apply 14 Each Day	Normal Sector Se	Extension in the theorem for the the theorem for the the theorem for the theorem for the theorem for the the the theorem for the the the the the theorem for the the the the the the the the the the	etti one senet da se - Juna juetti se Donation one Proce tille 2-24 (1994)				
Apply 14 Each Day	Normal Sectors II of the North Field Sectors II of the North Person Sectors II Sector Tables Bill 20 Normal Sectors II Sector 19 Sector	Extension in the theorem for the the theorem for the theorem for the the theorem for the theorem for the the the theorem for the theorem for the the the theorem for the the theorem for the the theorem for the the the the the theorem for the the the the the the the the the the	etti one venetti to • Juna junta • Donation ned Flows 101				

- Allow Guest To Access My Local Network If enabled, guests can access the local network and manage it.
- Guest Network Isolation If enabled, guests are isolated from each other.
- Enable Guest Network Bandwidth Control If enabled, the Guest Network Bandwidth Control rules will take effect.

Note:

The range of bandwidth for guest network is calculated according to the setting of Bandwidth Control on the Bandwidth Control page.

5. 6. DHCP

By default, the DHCP (Dynamic Host Configuration Protocol) Server is enabled and the router acts as a DHCP server; it dynamically assigns TCP/IP parameters to client devices from the IP Address Pool. You can change the settings of DHCP Server if necessary, and you can reserve LAN IP addresses for specified client devices.

5. 6. 1. DHCP Settings

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to DHCP > DHCP Settings.
- 3. Specify DHCP server settings and click Save.

Concer Solution			
DHCP Server	0.044	a # Endra	
That IP Address	192.004	0.100	
End IP Address	192,164	0.199	
Lasse Time.	129	minuted	11-2888 mouses, the default verse is 1281
Dyfault Gatewite	192.168	8.1	(optional)
Deleat Domain			institutial
DHS Server	0.0.00		ropheriali
Geconitary DNR Derver	0.0.0.0		(cquintere)
		Seve	

- DHCP Server Enable or disable the DHCP server. If disabled, you must have another DHCP server within your network or else you must configure the computer manually.
- Start IP Address Specify an IP address for the DHCP Server to start with when assigning IP addresses. 192.168.0.100 is the default start address.
- End IP Address Specify an IP address for the DHCP Server to end with when assigning IP addresses. 192.168.0.199 is the default end address.

- Address Lease Time The Address Lease Time is the amount of time a network user will be allowed to connect to the router with the current dynamic IP Address. When time is up, the user will be automatically assigned a new dynamic IP address. The range of the time is 1 ~ 2880 minutes. The default value is 120.
- Default Gateway (Optional) It is suggested to input the IP address of the LAN port of the router. The default value is 192.168.0.1.
- Default Domain (Optional) Input the domain name of your network.
- DNS Server (Optional) Input the DNS IP address provided by your ISP.
- Secondary DNS Server (Optional) Input the IP address of another DNS server if your ISP provides two DNS servers.

Note:

To use the DHCP server function of the router, you must configure all computers on the LAN as Obtain an IP Address automatically.

5. 6. 2. DHCP Clients List

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to DHCP > DHCP Clients List to view the information of the clients connected to the router.

DHCP Client	ls List				
This page display	s information of a	II DHCP clients on the network.			
	ID	Client Name	MAC Address	Assigned IP	Lease Time
	1	Camille	48/80/5C/89/74/85	192.168.0.100	00.00.32
	2	Phone	34/E2/F0:14:10:00	192.168.0.101	00.00.55

- Client Name The name of the DHCP client.
- MAC Address The MAC address of the DHCP client.
- Assigned IP The IP address that the outer has allocated to the DHCP client.
- Lease Time The time of the DHCP client leased. After the dynamic IP address has expired, a new dynamic IP address will be automatically assigned to the user.

You cannot change any of the values on this page. To update this page and show the current attached devices, click Refresh.

5. 6. 3. Address Reservation

You can reserve an IP address for a specific client. When you specify a reserved IP address for a PC on the LAN, this PC will always receive the same IP address each time when it accesses the DHCP server.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to DHCP > Address Reservation.
- 3. Click Add New and fill in the blanks.

CP Addres Reenador	
The static IP address of the DHCP Server can be cooligan	ed to this tage.
MAC ORFERS	
(P Address)	
20shut	Disabled •
	Save Bask

- 1) Enter the MAC address (in XX:XX:XX:XX:XX format.) of the client for which you want to reserve an IP address.
- 2) Enter the IP address (in dotted-decimal notation) which you want to reserve for the client.
- 3) Leave the Status as Enabled.
- 4) Click Save.

5.7. Forwarding

The router's NAT (Network Address Translation) feature makes the devices on the LAN use the same public IP address to communicate on the internet, which protects the local network by hiding IP addresses of the devices. However, it also brings about the problem that external hosts cannot initiatively communicate with the specified devices in the local network.

With the forwarding feature, the router can traverse the isolation of NAT so that clients on the internet can reach devices on the LAN and realize some specific functions.

The TP-Link router includes four forwarding rules. If two or more rules are set, the priority of implementation from high to low is Virtual Servers, Port Triggering, UPNP and DMZ.

5.7.1. Virtual Server

When you build up a server in the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to internet users. At the same time virtual servers can keep the local network safe as other services are still invisible from the internet. Virtual Servers can be used to set up public services in your local network, such as HTTP, FTP, DNS, POP3/SMTP and Telnet. Different service uses different service port. Port 80 is used in HTTP service, port 21 in FTP service, port 25 in SMTP service and port 110 in POP3 service. Please verify the service port number before the configuration.

I want to:

Share my personal website I've built in local network with my friends through the internet.

For example, the personal website has been built in my home PC (192.168.0.100). I hope that my friends on the internet can visit my website in some way. My PC is connected to the router with the WAN IP address 218.18.232.154.



- 1. Set your PC to a static IP address, for example 192.168.0.100.
- 2. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- **3.** Go to Forwarding > Virtual Server.
- Click Add New. Select HTTP from the Common Service Port list. The service port, internal port and protocol will be automatically filled in. Enter the PC's IP address 192.168.0.100 in the IP Address field.



5. Leave the status as Enabled and click Save.

Note:

- It is recommended to keep the default settings of Internal Port and Protocol if you are not clear about which port and protocol to use.
- If the service you want to use is not in the Common Service Port list, you can enter the corresponding parameters manually. You should verify the port number that the service needs.
- You can add multiple virtual server rules if you want to provide several services in a router. Please note that the Service Port should not be overlapped.

Done!

Users on the internet can enter http:// WAN IP (in this example: http:// 218.18.232.154)

to visit your personal website.

Note:

- If you have changed the default Service Port, you should use http:// WAN IP: Service Port to visit the website.
- Some specific service ports are forbidden by the ISP, if you fail to visit the website, please use another service port.

5.7.2. Port Triggering

Port triggering can specify a triggering port and its corresponding external ports. When a host in the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The router can record the IP address of the host. When the data from the internet return to the external ports, the router can forward them to the corresponding host. Port triggering is mainly applied to online games, VoIPs, video players and common applications including MSN Gaming Zone, Dialpad, Quick Time 4 players and more.

Follow the steps below to configure the port triggering rules:

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Forwarding > Port Triggering.
- 3. Click Add New. Select the desired application from the Common Applications list. The trigger port amd incoming ports will be automatically filled in. The following picture takes application MSN Gaming Zone as an example.

Port Trigger		
Trigger Port:	47624) <i>20</i> 0)
Trigger Protocol:	ALL •	
Open Port:	2300-2400,28800-29	(XX,XX,XX or XX-XX,XX)
Open Protocol:	ALL •	
Status:	Enabled •]
Common Service Port:	MSN Gaming Zone •]
	Save	Back

4. Leave the status as Enabled and click Save.

Note:

- You can add multiple port triggering rules as needed.
- The triggering ports can not be overlapped.
- If the application you need is not listed in the Common Service Port list, please enter the parameters manually. You should verify the open ports the application uses first and enter them in Open Port field. You can input at most 5 groups of ports (or port sections). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.

5.7.3. DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host in the local network, it is totally exposed to the internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the PC to be a DMZ host.

Note:

DMZ is more applicable in the situation that users are not clear about which ports to open. When it is enabled, the DMZ host is totally exposed to the internet, which may bring some potential safety hazards. If DMZ is not in use, please disable it in time.

I want to:

Make the home PC join the internet online game without port restriction.

For example, due to some port restriction, when playing the online games, you can log in normally but cannot join a team with other players. To solve this problem, set your PC as a DMZ host with all ports opened.

How can I do that?

- 1. Assign a static IP address to your PC, for example 192.168.0.100.
- 2. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- **3.** Go to Forwarding > DMZ.
- 4. Select Enable and enter the IP address 192.168.0.100 in the DMZ Host IP Address filed.

Current DMZ Status:	Enable Disable	
CONTRACTOR CONTRACTOR	a crane o crane	
DMZ Host IP Address:	192.168.0.100	

5. Click Save.

Done!

You've set your PC to a DMZ host and now you can make a team to game with other players.

5.7.4. UPnP

The UPnP (Universal Plug and Play) protocol allows the applications or host devices to automatically find the front-end NAT device and send request to it to open the

corresponding ports. With UPnP enabled, the applications or host devices on the local network and the internet can freely communicate with each other realizing the seamless connection of the network. You may need to enable the UPnP if you want to use applications for multiplayer gaming, peer-to-peer connections, real-time communication (such as VoIP or telephone conference) or remote assistance, etc.

Tips:

- UPnP is enabled by default in this router.
- Only the application supporting UPnP protocol can use this feature.
- UPnP feature needs the support of operating system (e.g. Windows Vista/ Windows 7/ Windows 8, etc. Some of operating system need to install the UPnP components).

For example, when you connect your Xbox to the router which is connected to the internet to play online games, UPnP will send request to the router to open the corresponding ports allowing the following data penetrating the NAT to transmit. Therefore, you can play Xbox online games without a hitch.



If necessary, you can follow the steps to change the status of UPnP.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Forwarding > UPnP.
- 3. Click Disable or Enable according to your needs.

UPnP						
	Current UPnP Status	Enabled Disable				
		Current UPr	P Settings List			
10	App Description	External Port	Protocol	Internal Port	IP Address	Status
		- Pa	itech			

5.8. Security

This function allows you to protect your home network from cyber attacks and unauthorized users by implementing these network security functions.

5.8.1. Basic Security

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Security > Basic Security, and you can enable or disable the security functions.

Basic Security	
Firewall	
Enable SPI Firewalt	×
VPN	
PPTP Pass-through:	Enable Disable
L2TP Pass-brough:	Enable Disable
IPSec Pass-through:	Enable Disable
ALG	
FTP ALO:	Enable Disable
TFTP ALC:	Enable Disable
H323 ALG:	Enable Disable
SIP ALC:	Enable Disable
RTSP ALG:	Enable Disable
	Save

- Firewall A firewall protects your network from internet attacks.
 - Enable SPI Firewall SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by default.
- VPN VPN Passthrough must be enabled if you want to allow VPN tunnels using IPSec, PPTP or L2TP protocols to pass through the router's firewall.
 - PPTP Pass-through Point-to-Point Tunneling Protocol (PPTP) allows the Pointto-Point Protocol (PPP) to be tunneled through an IP network. If you want to allow PPTP tunnels to pass through the router, you can keep the default (Enabled).
 - L2TP Pass-through Layer 2 Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the internet on the Layer 2 level. If you want to allow L2TP tunnels to pass through the router, you can keep the default (Enabled).
 - IPSec Pass-through Internet Protocol Security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. If you want to allow IPSec tunnels to pass through the router, you can keep the default (Enabled).
- ALG It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

- FTP ALG To allow FTP clients and servers to transfer data across NAT, keep the default Enable.
- TFTP ALG To allow TFTP clients and servers to transfer data across NAT, keep the default Enable.
- H323 ALG To allow Microsoft NetMeeting clients to communicate across NAT, keep the default Enable.
- SIP ALG To allow some multimedia clients to communicate across NAT, click Enable.
- RTSP ALG To allow some media player clients to communicate with some streaming media servers across NAT, click Enable.

3. Click Save.

5.8.2. Advanced Security

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Security > Advanced Security, and you can protect the router from being attacked by ICMP-Flood, UDP Flood and TCP-SYN Flood.

DoS Protection: @ Enable # Dinable		
Enable ICWP-Flood Attack Filtering		
ICMP-Flood Packets Threshold (5-3600)	50.	packetshecund
Enable UDP-Flood Attack Fittering		
UDF-Field Packets Threshold (8-3600)	\$00	packets/second
Enable TCP-SVN-Flood Adack Fillering		
TCP-STN-Flood Packets Threshold (5-3885)	34	packett/becomd
EForbid Ping Packet Fixon WAN Port		
Forbid Fing Facket From LAN Port		

 DoS Protection - Denial of Service protection. Select Enable or Disable to enable or disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.

Note:

Dos Protection will take effect only when the Statistics in System Tools > Statistics is enabled.

 Enable ICMP-FLOOD Attack Filtering - Tick the checkbox to enable or disable this function.

- ICMP-FLOOD Packets Threshold (5~3600) The default value is 50. Enter a value between 5 ~ 3600. When the number of the current ICMP-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- Enable UDP-FLOOD Filtering Tick the checkbox to enable this function.
- UDP-FLOOD Packets Threshold (5~3600) The default value is 500. Enter a value between 5 ~ 3600. When the number of the current UPD-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- Enable TCP-SYN-FLOOD Attack Filtering -Tick the checkbox to enable or disable this function.
- TCP-SYN-FLOOD Packets Threshold (5~3600) The default value is 50. Enter a value between 5 ~ 3600. When the number of the current TCP-SYN-FLOOD packets is beyond the set value, the router will startup the blocking function immediately.
- Ignore Ping Packet From WAN Port The default setting is disabled. If enabled, the ping packet from the internet cannot access the router.
- Forbid Ping Packet From LAN Port The default setting is disabled. If enabled, the ping packet from LAN cannot access the router. This function can be used to defend against some viruses.
- 3. Click Save.
- 4. Click Blocked DoS Host List to display the DoS host table by blocking.

5.9. Parental Controls

Parental Controls allows you to block inappropriate and malicious websites, and control access to specific websites at specific time for your children's devices.

For example, you want the children's PC with the MAC address 00:11:22:33:44:AA can access www.tp-link.com on Saturday only while the parent PC with the MAC address 00:11:22:33:44:BB is without any restriction.

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Parental Controls.
- 3. Tick the Enable Parental Controls checkbox, enter the MAC address 00:11:22:33:44:BB in the MAC Address of Parental PC field and then click Save.

Parental Controls	Parental Controls					
Parential Controls can be used to administer all internet activity including limiting usage and/or access to specific websites to all clients on the network for a specified period of the Subedule is based on the time of the Router. The time can be set in "Bystem Tools ~ <u>Time Setting</u> ".						
2 Enable Parental Controls						
MAC Address Of Parental PC: 0	00 11 22 33 44 88					
MAC Address of Current PC	C0 4A 02 1A C3 45	Copy to Above				
Save						

4. Enter 00:11:22:33:44:AA in the MAC Address 1 field.

MAC Address - 1:	00-11-22-33-44-AA	
MAC Address - 2:		
MAC Address - 3:		
MAC Address - 4:		
MAC Address in current LAN:	C0:4A:00:1A:C3:45	Copy toPlease Select-

5. Select Each Week from the Apply To drop-down list, and select Sat. Select 00:00 as the Start Time and Select 24:00 as the End Time. And then click Add.

MIRIN 10		Served 1.8	CHP .		East 10	and .	
Each Week •	0	1:00			24.00		Add
Mon 💠 Tues. 🔛 Wed	iii The	UR	2.54	L) fun			
	Time	R.00 11	00 2 00	310 410	2.00 2.00		00 1000110012001200140
	Then,						
	sten-						
	Tent:						
	Well:						
	Thur.						
	FR	-					
	34						
		1					

6. Enter www.tp-link.com in the Add URL field. Click Add.

	ANURE	www.tp-link.com	inA
12		Details	

7. Click Save.

5.10. Access Control

Access Control is used to deny or allow specific client devices to access your network with access time and content restrictions.

I want to:

Deny or allow specific client devices to access my network with access tiem and content restrictions.

For example, If you want to restrict the internet activities of host with MAC address 00:11:22:33:44:AA on the LAN to access www.tp-link.com only, please follow the steps below:

How can I do that?

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Access Control > Host and configure the host settings:
 - 1) Click Add New.
 - 2) Select MAC Address as the mode type. Create a unique description (e.g. host_1) for the host in the Description field and enter 00-11-22-33-44-AA in the MAC Address filed.

bhatter	MAC ANDERS *	
Depoturium		
MAL, Autowski		

- 3) Click Save.
- 3. Go to Access Control > Target and configure the target settings:
 - 1) Click Add New.
 - 2) Select URL Address as the mode type. Create a unique description (e.g. target_1) for the target in the Target Description field and enter the domain name, either the full name or the keywords (for example TP-Link) in the Add URL Address field. And then Click Add.

Note:

Any URL address with keywords in it (e.g. www.tp-link.com) will be blocked or allowed.

	auto (DEE Villant)	
Dece	Anne (AN
100.1		Getal
	Dates 1 years	NUTLING OTHER AND DALL DAVE THERE IT AND

- 3) Click Save.
- 4. Go to Access Control > Schedule and configure the schedule settings:
 - 1) Click Add New.
 - 2) Create a unique description (e.g. schedule_1) for the schedule in the Schedule Description field and set the day(s) and time period. And then click Add.

	Description Tarba	lin_1	
Apply Inc.	(Auger) Talase	Englisher	
Each Day •	00.00	24.18 *	- AR
	Name and Address of the	way have must from \$155 miles	walking Charles
	44. 2 3 4 5 5		
	Set. BERRERE		
	11		
Clear behicket			

- 3) Click Save.
- 5. Go to Access Control > Rule and add a new access control rule.
 - 1) Click Add New.
 - 2) Give a name for the rule in the Description field. Select host_1 from the LAN host drop-down list; select target_1 from the target drop-down list; select schedule_1 from the schedule drop-down list.

Description:	rule_1		
LAN Host:	host_1	\sim	Add LAN Host
Target:	Target_1	\sim	Add Target
Schedule:	Any Time	\sim	Add Schedule
Rule:	Deny	\sim	
Status:	Enabled	\sim	
Direction:	OUT		

3) Leave the status as Enabled as click Save.

Note:

When Target is set to be URL Address mode, the Direction field is OUT and not editable, which means the host can only visit or is not allowed to visit the URL address you set.

- 6. Select Enable Internet Access Control to enable Access Control function.
- 7. Select Allow the packets specified by any enabled access control policy to pass through the Router as the default filter policy and click Save.

Acces	Orma Ras Menagement
The store of	on order training where his product 200 hours. You are instant promine access control care in placebark, manage you restrictly.
	Tauta General access access
	elsali Filmeng Raine. Alloni Re-patters oni genalari in, any titering nanyis pandhonggi disi tenan Titere Re-patters stat gazifilat bujan Bieneg salai in sandhonggi titer devere.
24	•

Done!

Now only the specific host(s) can visit the target(s) within the scheduled time period. Note:

When LAN Host and Target are both set to be the MAC Address mode, you need to set Protocol: ALL, TCP, UDP, ICMP. The default setting is ALL and it is recommended to keep the default setting.

5.11. Advanced Routing

Static Routing is a form of routing that is configured manually by a network administrator or a user by adding entries into a routing table. The manually-configured routing information guides the router in forwarding data packets to the specific destination.

5. 11. 1. Static Route List

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Advanced Routing > Static Route List.
- To add static routing entries:
- 1. Click Add New.
- 2. Enter the following information.

Destination IF Address		
Subnet Mack:		
Gatematy		
tviterface:		 (approximit)
Status	Enabled	

• Destination IP Address - The Destination Network is the address of the network or host that you want to assign to a static route.

- Subnet Mask The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway This is the IP address of the default gateway device that allows the contact between the router and the network or host.
- 3. Select Enabled or Disabled for this entry on the Status drop-down list.
- 4. Click Save.

5. 11. 2. System Routing Table

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Advanced Routing > System Routing Table, and you can view all the valid route entries in use.

stern Ro	ding Table			
10	Destination Network	Subnet Masik	Geteway	Interface
1	192.168.0.0	255,255,255,0	0.0.0.0	LAN & WLAN

- Destination Network The Destination Network is the address of the network or host to which the static route is assigned.
- Subnet Mask The Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion.
- Gateway This is the IP address of the gateway device that allows for contact between the Router and the network or host.
- Interface This interface tells you whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), or the WAN (Internet).

Click Refresh to refresh the data displayed.

5.12. Bandwidth Control

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to Bandwidth Control.
- 3. Tick the Enable Bandwidth Control checkbox, and configure the Egress Bandwidth and Ingress Bandwidth, and then click Save. The Egress/Ingress Bandwidth is the upload/download speed through the WAN port. The value should be less than 100,000Kbps.

Bandwidth Control			
REnable Bandwidth Control			
	Egress Bandwidth:	512	Kbps
	Ingress Bandwidth:	2048	Kbps
Save			

4. Click Add New, fill in the blanks and click Save.

Enable: W Review	
Part Range	
Probati	ALL +
Poorty	E • (1 meaning highest prests)
	Mit Bandwidt(Raps) Biox Bandwidt(Rizes)
Lipson Ramporth.	
Highest Bandworth.	

- IP Range Interior PC address range. If both are blank or 0.0.0.0, the domain is noneffective.
- Port Range The port range which the Interior PC access the outside PC. If all are blank or 0, the domain is noneffective.
- Protocol Transport layer protocol, here there are ALL, TCP, UDP.
- Priority Priority of Bandwidth Control rules. '1' stands for the highest priority while '8' stands for the lowest priority. The total Upstream/ Downstream Bandwidth is first allocated to guarantee all the Min Rate of Bandwidth Control rules. If there is any bandwidth left, it is first allocated to the rule with the highest priority, then to the rule with the second highest priority, and so on.
- Egress Bandwidth The max and the min upload speed through the WAN port.
- Ingress Bandwidth The max and the min download speed through the WAN port.

5.13. IP & MAC Binding

IP & MAC Binding, namely, ARP (Address Resolution Protocol) Binding, is used to bind a network device's IP address to its MAC address. This will prevent ARP spoofing and other ARP attacks by denying network access to a device with a matching IP address in the ARP list, but with an unrecognized MAC address.

5. 13. 1. Binding Settings

- 1. Visit <u>http://tplinkwifi.net</u>, and log in with the username and password you set for the router.
- 2. Go to IP & MAC Binding > Binding Settings.
- 3. Select Enable for ARP Binding and click Save.

Binding Settings			
	ARP Binding:	Enable Disable	Save

- To add IP & MAC Binding entries:
- 1. Click Add New.
- 2. Enter the MAC address and IP address.
- 3. Tick the Bind checkbox and click Save.

- control of the second s		
tus page allows you to set IP-MAC Binding entities.		
MAC Abdress		
F Address		
Sint	æ	

- To modify or delete an existing entry:
- 1. Select the desired entry in the table.
- 2. Click Edit or Delete Selected.

5.13.2. ARP List

To manage a device, you can observe the device on the LAN by checking its MAC address and IP address on the ARP list, and you can also configure the items. This page displays the ARP list which shows all the existing IP & MAC Binding entries.

MAX: PUBLICAS	1P.848455	Martin.
 10122-40 00 07 00	10 10 A	Butt.
	14(2 164 6 10) G	International