

Step 5: Here you can configure the NAT. If you are not an advanced user, the default settings are recommended and then

#### click Next.

Device Info	Network Address Translation Settings
Advanced Setup	
Layer2 Interface	Network Address Translation (NAT) allows you to share one Wide Area Network (WAN) IP address for multiple computers on your Local Area Network (La
ATM Interface	
ETH Interface	Enable NAT
WAN Service	Proble Firewall
LAN	
NAT	1. March
Security	material as
Parental Control	Enable IGMP Multicast
Bandwidth Control	
Routing	Enable MLD Multicast Proxy
DNS	Back Next

Step 6: To configure the Default Gateway interface when using IPv6, select the interface that you want to configure with

the WAN gateway address in Selected WAN Interface box. Then click Next.

Tend	a	Hore
Device Info	Routing Default Gateway	
Advanced Setup		
Layer2 Interface		
ATM Interface	Default gateway interface list ca	have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the higest and the la
ETH Interface	one the lowest priority if the W	N interface is connected. Priority order can be changed by removing all and adding them back in again.
WAN Service		
LAN	Selected Default	Available Routed WAN
NAT	Gateway Interfaces	Interfaces
Security		
Parental Control	B400.1	
Bandwidth Control		
Routing	->	
DNS	*	
DSL	_	
Storage Service		
Interface Grouping		
IP Tunnel		
Certificate	IPv6: Select a preferred wan inte	face as the system default IPv6 gateway.
Multicast	Selected WAN Interface ipoe_e	0/eth0.1 🗸
IPTV		
Wireless		
Diagnostics		Back Next

Step 7: To configure the WAN DNS address, check the Obtain IPv6 DNS info from a WAN interface option, or select

the Use the following Static IPv6 DNS address option to enter the static DNS server IPv6 addresses provided by your

#### ISP. At last, click Next.

ena	
evice Infa	DNS Server Configuration
dvanced Setup	
Layer2 Interface	Select DNS Server interface from available WAN interfaces CR enter static ENS server IP addresses for the system. In ATM mode, if only a single IVC with IPAA or static IPOE practocol is configured. Static DNS server IP addressas must be enterved.
ATM Interface	DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the lass one the lowest priority if the WAN interface is connected. Priority order can be change
ETH Interface	removing all and adding them back in again.
WAN Service	
AN	🐮 Select DNS Server Interface from available WAN interfaces
TAN	Entertapd DNS Server
ecurity	Interfaces Available WAIN Interfaces
arental Control	
Bandwidth Control	eh(U)
Routing	
DNS	
DSL	
Storage Service	
interface Grouping	
PTunnel	
Certificate	Use the following Static DN5 (P address:
Multicast	Primary DNS server:
PTV	Secondary DNS server
ireless	
agnostics	
anagement	3Pvg: Select the configured WAN interface for IPv6 DNS server information DR enter the static IPv6 DNS server Addresses.
	Note that selecting a WAN interface for Dy-6 DNS anywe will enable DHCPvg Client on that interface.
	Obtain Pré DNS Info from a WAH Interface
	WAN Interface salected: poe_ethOeth0.1 v
	O Lise the following Static IPV6 DINS address:
	Primary IDv6 DNS server:



Step 8: Here you can view your configurations. Click Apply/Save to save your settings if everything is correctly set.

Device Info	WAN Setup - Summ	nary
Advanced Setup Layer2 Interface ATM Interface	Make sure that the s	ettings bel
ETH Interface	Connection Type:	IPoE
WAN Service	NAT:	Disabled
LAN	Full Cone NAT:	Disabled
Security	Firewall:	Enabled
Parental Control	IGMP Multicast:	Disabled
Bandwidth Control Routing	Quality Of Service:	Enabled
DNS		
DSL	Click "Apply/Save" to	o have this
Storage Service		

When the IPoE connection is successful, you can access the Internet.

			Wie	le Area Netw	ork (WAN	I) Service	Setup				
	Chi	oose A	dd, Remove c	r Edit to conf	igure a W/	AN service	e over a se	lected int	terface.		
Interface	Description	Type	V(an802,10	VlanMuotid	lamp	NAT	Firewall	1Pv6	Mid	Remove	Edit
oth0.1	inco othi	iDe5	D(JA)	BC/A	Disabled	Feeblad	Enabled	Enabled	Disabled		Edd
6010.1	ihoeTenin	THOSE	N/A	TW/A	Disabieu	LINADIEU	Chableu	Cilduicu	Disauleu		[ Col
	Interface eth0.1	Chi Interface Description eth0.1 ipoe_eth0	Choose A Interface Description Type eth0.1 ipoe_eth0 IPOE	Chaose Add, Remove of Interface Description Type Vlan802.1p eth0.1 ipoe_eth0 IPoE N/A	Choose Add, Remove or Edit to cont Interface Description Type Vlan802.2p VlanMudd eth0.1 ipoe_eth0 IPoE N/A N/A	Choose Add, Remove or Edit to configure a W/ Interface Description Type Vian802.1p VianMudd Igmp eth0.1 ipoe_eth0 IPoE N/A N/A Disabled	Interface         Description         Type         Vian802.2p         VianMudd         1gmp         NAT           eth0.1         ipoe_eth0         IPoE         N/A         N/A         Disabled         Enabled	Interface         Description         Type         Vian802.1p         Vian802.1p         N/A         NAT         Firewall           eth0.1         ipoe_eth0         IPoE         N/A         N/A         Disabled         Enabled	Interface         Description         Type         VIan802.1p         Vian802.1p         N/A         Disabled         Enabled         Enabled	Interface         Description         Type         Vian802.2.p         Vian802.1.p         N/A         Disabled         Enabled         Enabled         Enabled         Disabled	Mide area retwork (wait) service setup           Choose Add, Remove or Edit to configure a WAN service over a selected interface.           Interface         Description         Type         VIan802.1p         VIan802.1p         NAT         Firewall         TPv6         Mid         Remove or Edit to configure a WAN service over a selected interface.           Interface         Description         Type         VIan802.1p         VIan802.1p         NAT         Firewall         TPv6         Mid         Remove or Edit to configure a WAN service over a selected interface.           eth0.1         ipoe_eth0         IPoE         N/A         N/A         Disabled         Enabled         Enabled         Disabled         Disabled

## Bridging

If you wish to initiate a dialup directly from your PC for Internet access or enjoy the entire Internet connection (instead

of sharing it with others), you can select the Bridging and create a dialup program from your PC.

Step 1: Click Advanced Setup > WAN Service and then click the Add button.

Device Info	Wide Area Network (WAN) Service Setup
Advanced Setup Laver2 Interface	Choose Add, Remove or Edit to configure a WAN service over a selected interface.
ATM Interface	Interface Description Type Vias802 in Viational James NAT Singual 1946 All Dampur Ed
ETH Interface	murranee economication affect annualities annualities faith and the second second con-
WAN Service	





Step 3: Select Bridging. Edit the Enter Service Description. This field is optional. It is recommended that you keep the



default. And click Next.

Device Info	WAN Service Configuration	
Advanced Setup Layer2 Interface ATM Interface ETH Interface	Select WAN service type: O PPP over Ethernet (PPPoE) O IP over Ethernet O Bridging	
WAN Service		
LAN	Enter Service Description: br_eth0	
NAT	The second s	
Security		
Parental Control	For tagged service, enter valid 802.1P Priority and 80.	2.1Q VLAN ID.
Bandwidth Control	For untagged service, set -1 to both 802.1P Priority a	nd 802.1Q VLAN ID.
Routing	Enter 802.1P Priority (0-7):	-1
DNS	Enter 802.1Q VLAN ID [0-4094]:	-1
DSL		1
Storage Service		
Interface Grouping		
IP Tunnel		
Certificate		
Multicast		the stand lar
IPTV		Back

Step 4: Here you can view your configurations. Click Apply/Save to save your settings if everything is correctly set.

Connection Type:     Bridge       AN Service     NAT:       Disabled       Full Cone NAT:     Disabled       Surity     Firewall:       IGMP Multicast:     Disabled       Audity Of Service:     Enabled	Device Info	WAN Setup - Summ	ary
TH Interface     Connection Type:     Bridge       AN Service     NAT:     Disabled       N     Full Cone NAT:     Disabled       Tr     Firewall:     Disabled       curity     Firewall:     Disabled       rental Control     IGMP Multicast:     Disabled       ndwidth Control     Quality Of Service:     Enabled	Advanced Setup Layer2 Interface ATM Interface	Make sure that the s	ettings bei
NN     Disabled       N     Full Cone NAT:     Disabled       Full Cone NAT:     Disabled       curity     Firewall:     Disabled       rental Control     IGMP Multicast:     Disabled       ndwidth Control     Quality Of Service:     Enabled	ETH Interface	Connection Type:	Bridge
N     Full Cone NAT:     Disabled       Tr     Disabled       curity     Firewall:     Disabled       rental Control     IGMP Multicast:     Disabled       uting     Quality Of Service:     Enabled	WAN Service	NATE	Disabled
Firewall:     Disabled       rental Control     IGMP Multicast:     Disabled       ndwidth Control     Quality Of Service:     Enabled	LAN	Full Cone NAT:	Disabled
rental Control IGMP Multicast: Disabled ndwidth Control Quality Of Service: Enabled	Security	Firewall:	Disabled
ndwidth Control Quality Of Service: Enabled	Parental Control	IGMP Multicast:	Disabled
	Bandwidth Control Routing	Quality Of Service:	Enabled
IS	DNS		
	Storage Service		

After the bridging connection is successful, initiate a dialup directly from your PC for Internet access.

Tenda												
Device Info				Wid	le Area Netw	ork (WAN	I) Service	Setup	-			
Advanced Setup Layer2 Interface		Q	hoose A	dd, Remove a	r Edit to conf	igure a W	AN service	over a se	lected inte	erface.		
ATM Interface	Interiare	Description	Type	Man802 To	Vlandavid	lamo	NAT	Firewall	10vs	iddei.	Bernove	Edit
ETH Interface		and an an an	1300	a l'al		et. ht.d	ni di la l	E al la d	at the		-	L Corte
WAN Service	e010.1	pr_etnu	Budge	N/A	N/A	Disableo	Disabled	Enabled	Disabled	Disabled		10001
LAN												
NAT												
Security					A	id Remov	e					



# 4.2.3 LAN Setup

Here you can configure the LAN IP Address and subnet mask. This IP address is to be used to access the device's

settings through a web browser. Be sure to make a note of any changes you apply to this page.

This part includes the following information:

- IPv4
- IPv6 Autoconfig

## IPv4

Device Info	Local Area Network	: (LAN) Setup			
Advanced Setup	Configure the Broad	band Router IP Address and Subnet Mask for LAN interface.			
Layer2 Interface	GroupName Default	<b>T</b>			
WAN Service	IP Address:	192.168.1.1			
LAN	Subnet Mask:	255.255.255.0			
IPv6 Autoconfig	Enable IGMP Snooping				
NAT	Disable DHCP Set	erver			
Security	Enable DHCP Set	rver			
Parental Control	Start IP Address	192.168.1.2			
Bandwidth Control	End IP Address:	192 168 1 254			
Routing	Lessed Time (bo	24			
DNS	Leased Time (no				
DSL	DNS Servers Assign	led by DHCP Server:			
Storage Service	Primary DNS server	192.168.1.1			
Interface Grouping	Secondary DNS ser	ver:			
IP Tunnel	Static IP Lease Li	ist: (A maximum 32 entries can be configured)			
Certificate	MAC Address IP A	ddress Remove			
Multicast	Add Entries Remov	ve Entries			
IPTV	Configure the sec	and ID Address and Subpat Mask for LAN interface			

**IP Address:** The device's LAN IP address. The default setting is 192.168.1.1.

**Subnet Mask:** The LAN subnet mask of the device. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or modem router. You can change the subnet mask to fit your network.

Enable IGMP Snooping: Check to enable the IGMP Snooping. It is recommended to keep the default settings.

Disable DHCP Server: Click to disable the DHCP Server.

Enable DHCP Server: Click to enable the DHCP Server.

Start IP Address: Specify the start of the range for the pool of IP addresses in the same subnet as the router.

End IP Address: Specify the end of the range for the pool of IP addresses in the same subnet as the router.



Leased Time: The lease time is a time length that the IP address is assigned to each device before it is refreshed.

Static IP Lease List: Displays a list of devices with reserved static IP addresses.

Add Entries: Click to add a static IP lease entry. A maximum 32 entries can be configured.

Remove Entries: Click to remove a static IP lease entry.

**Configure the second IP Address and Subnet Mask for LAN interface:** If you want to configure two IP addresses for the LAN interface, you can check this option and enter the second IP Address and Subnet Mask manually.

Apply/Save: After you configure all the needed settings, click this button to apply and save them.

# TIP

DHCP (Dynamic Host Configuration Protocol) assigns an IP address to each device on the LAN/private network. When you enable the DHCP Server, the DHCP Server will automatically allocate an unused IP address from the IP address pool specified in this screen to the requesting device as long as the device is set to "Obtain an IP Address Automatically". By default, DHCP is enabled.

# **IPv6 Autoconfig**



#### Static LAN IPv6 Address Configuration

Interface Address (prefix length is required): Enter the interface address.

# **A**NOTE

1. IPv6 address can only be Aggregatable Global Unicast Addresses and Unique Local Address. Link-Local Unicast

Addresses and Multicast Addresses are not permitted.

2. The IPv6 address must be entered with a prefix length.



#### IPv6 LAN Applications

Enable DHCPv6 Server: Check to enable the DHCPv6 Server.

**Stateless:** If selected, IPv6 clients will generate IPv6 addresses automatically based on the Prefix Delegation's IPv6 prefix and their own MAC addresses.

Stateful: Stateful DHCPv6 is supported based on the assumption of prefix length less than 64. Select this option and configure the start/end interface ID and leased time. The router will automatically assign IPv6 addresses to IPv6 clients.
Leased Time (hour): The lease time is a time length that the IP address is assigned to each device before it is refreshed.
Start interface ID/End interface ID: Specify the start/end interface ID Interface ID does NOT support ZERO
COMPRESSION "::". Please enter the complete information. For example: Please enter "0:0:0:2" instead of "::2".
Enable RADVD: The RADVD (Router Advertisement Daemon) implements link-local advertisements of IPv6 router addresses and IPv6 routing prefixes using the Neighbor Discovery Protocol (NDP) and is used by system administrators in stateless autoconfiguration methods of network hosts on Internet Protocol version 6 networks. Check the checkbox to enable the RADVD.

Enable ULA Prefix Advertisement: If enabled, the router will advertise ULA prefix periodically

Randomly Generate: If selected, address prefix can be automatically generated.

**Statically Configure:** If you select this option, you need to manually configure the address prefix and life time. **Prefix:** Specify the prefix.

Preferred Life Time (hour): Specify the preferred life time in hour.

Valid Life Time (hour): Specify the valid life time in hour.

**Enable MLD Snooping:** MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link. If disabled on layer2 devices, IPv6 multicast data packets will be broadcast on the entire layer2; if enabled, these packets will be multicast to only specified recipient instead of being broadcast on the entire layer2.

# TIF

If you change the LAN IP address of the device, the current connection to the device will be stopped. You must use the new IP address to log in to the device. Be sure to write the new address on a sticky label and attach it to the bottom of the unit. You will need the new address to log in to the device in the future.



# 4.2.4 NAT

This section explains the following:

- Virtual Server
- Port Triggering
- DMZ Host
- UPnP

## **Virtual Server**

The Virtual Server is useful for web servers, ftp servers, e-mail servers, gaming and other specialized Internet

applications. When you enable the Virtual Server, the communication requests from the Internet to your router's WAN

port will be forwarded to the specified LAN IP address.



To enter the virtual server screen, click NAT > Virtual Server and then click the Add button to add rules.

Tenda	Home Page
Device Info	NAT Virtual Servers
Advanced Setup	
Layer2 Interface	Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be
WAN Service	modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as
LAN	"Internal Port Start".
NAT	Remaining number of entries that can be configured: 32
Virtual Servers	
Port Triggering	Use Interface   ipoe_eth0/eth0.1 v
DMZ Host	Service Name:
UPnP	Select a Service: Select One     V
Security	Custom Service:
Parental Control	Sec. 10 Address 400 458 4
Bandwidth Control	Server i P Address: 192.106.1.
Routing	
DNS	External Port Start External Port End Protocol Internal Port Start Internal Port End
DSL	TCP V
Storage Service	TCP •
	TCP •

Use Interface: Select a WAN connection to which you wish to apply the rules. When there is only one WAN connection

available, the rules will be automatically applied to it.

Service Name:

- Select a Service: Allows you to select an existing service from the drop-down list.
- Custom Service: Allows you to customize a service.

Server IP Address: Enter the IP address of your local computer that will provide this service.

External Starting Port and External Ending Port: These are the starting number and ending number for the public



ports at the Internet interface.

Protocol: Select the protocol from the Protocol drop-down list. If you are unsure, select TCP/UDP.

**Internal Starting Port and Internal Ending Port:** These are the starting number and ending number for the ports of a computer on the router's local area network (LAN).

# **A**NOTE

If you have enabled the UPnP functionality on both the router and your PC that is attached to one of the LAN port of the router, you will be prompted on the Virtual Server page that the UPnP interface is being used.

#### Instance

You have set up two servers on your LAN side:

- An FTP server (using the default port number of 21) at the IP address of 192.168.1.100

- A web server (using the default port number of 8080) at the IP address of 192.168.1.110

And want your friends on the Internet to access the FTP server and web server via default ports. To access your FTP or web server from the Internet, a remote user has to know the WAN IP address of your router. In this example, we assume the WAN IP address of your router is 183.37.227.201. Then follow instructions below:

## To configure the router to make your local FTP server public:

## **Procedure**

- 1. Click NAT > Virtual Server to enter it and then click the Add button.
- 2. Select **FTP Server** that you wish to host on your network from the **Select a Service** drop-down list. The port number (21) used by this service will then be automatically populated.

- Or if you wish to define the service yourself, enter a descriptive name in the Custom Service, say My FTP, and

then manually enter the port number (21) used by this service in the Internal Starting Port, Internal Ending Port,

#### **External Starting Port and External Ending Port fields**.

- 3. Select a protocol from the Protocol drop-down list. If you are unsure, select TCP/UDP.
- **4.** In the **Server IP Address** field, enter the last digit of the IP address of your local computer that offers this service. Here in this example, we enter 100.
- 5. Click Apply/Save

Your friends on the Internet will then be able to access your FTP server simply by "ftp://183.37.227.201:21".





#### To configure your router to make your local web server public:

### Procedure

- 1. Click NAT > Virtual Server to enter it and then click the Add button.
- 2. Select **Web Server (HTTP)** that you wish to host on your network from the **Select a Service** drop-down list. The port number (8080) used by this service will then be automatically populated.

- Or if you wish to define the service yourself, enter a descriptive name in the **Custom Service**, say My Web Server (HTTP), and then manually enter the port number (8080) used by this service in the **Internal Starting Port**, **Internal Ending Port, External Starting Port and External Ending Port fields**.

- 3. Select a protocol from the **Protocol** drop-down list. If you are unsure, select **TCP/UDP**.
- **4.** In the **Server IPAddress** field, enter the last digit of the IP address of your local computer that offers this service. Here in this example, we enter 110.
- 5. Click Apply/Save

NAT Virtual Ser	vers							
Select the service I	Select the service name, and enter the server IP address and click "Apply/Save" to forward IP packets for this service to the specified server. NOTE: The "Internal Port End" cannot be							
modified directly	modified directly. Normally, it is set to the same value as "External Port End". However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as							
"Internal Port Sta	"Internal Port Start".							
Remaining numb	Remaining number of entries that can be configured: 32							
,								
🕑 Use Interface	ipoe_eth0/eth0.1	•						
Service Name:								
Select a Service	Web Server (HTT	P)	•					
Custom Service								
Server IP Address	192 168 1 110							
oonton in Addressi	102.100.1110							
External Deut Ctar	t External Dant End	Destacal	Internal Davit Ctart	Internal Dart End				
External Port Star	t External Port End	Protocol	Internal Port Start	Internal Port End				
8080	8080	TCP/UDP V	8080	8080				
		TCP 🔻						

Now you can view your configurations as seen in the screenshot below. Your friends on the Internet will then be able to

access the web server simply by entering "http://183.37.227.201:8080" in his browser.

NAT Virtual Servers Se	tup									
Virtual Server allows you to o	direct incoming traffic t port number used by	from WAN side (identif	ied by Protocol and Ex side A maximum 32	dernal port	to the Internal server be configured	with private IP addre	ess on the LAN side. Th	ie Internal port is i	required on	ly if the external port needs
	e por e number asea by	ale server on the Dav	side, A movinum sz		Add Remove					
	Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove	
	Web Server (HTTP)	8080	8080	тср	8080	8080	192.168.1.110	ppp0.1		
	FTP Server	21	21	тср	21	21	192.168.1.100	ppp0.1		
(¢))	http:	//183.37.22	7.201:8080	)	- م	<b>∂</b> →				

# ANOTE

The "Internal Port End" cannot be modified directly. Normally, it is set to the same value as "External Port End".
 However, if you modify "Internal Port Start", then "Internal Port End" will be set to the same value as "Internal Port

Start".

2. If the service or game you wish to host on your network is not included in the list, manually add it in the Custom Service field and then add the port number used by it to the Internal Starting Port, Internal Ending Port, External Starting Port and External Ending Port fields.



# **Port Triggering**

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'.

Tend	a Home Pa					
Device Info	NAT Port Triggering Setup					
Advanced Setup	Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an					
Layer2 Interface	entre appreciency require data permit permit and relation to a service and accessing with relative permitting permitting operations and relation to a service and relation to a service and relation of the LAN accessing permitting and relative the service and relative the					
WAN Service	application of the Left simulates a feet optic connection of a fertice party long are integrating on the neutron simulation and refers and to connection a fertice party long are integrating and the neutron simulation and refers and to connection a feet of the neutron simulation and the neut					
LAN	to the application on the Data side using the Open Ports. A maximum 32 entries can be configured.					
NAT						
Virtual Servers	Ada Kemove					
Port Triggering	Trigger Open					
DMZ Host	Application Name Port Range Port Range WAN Interface Remove					
UPnP	Protocol Protocol Find Find					
Security	Svars Ena					

To enter the Port Triggering screen, click NAT > Port Triggering and then click the Add button to add rules.

You can configure the port settings from this screen by selecting an existing application or creating your own (Custom

application) and click Save/Apply to add it.

and an Anda	NAT Port Triggering					
evice into	in the magering					
avanced setup	Some applications such as ga	mes video conferencino, remote	access applications and others n	aquire that specific ports in :	the Router's firewall be opened for access by the applics	ations Vo
MAN Comico	can configure the port settin	as from this screen by selecting ar	evisting application or creating	your own (Custom applicati	ion)and click "Save/Apply" to add it	
WAN Service	Remaining number of entri	Remaining number of entries that can be configured: 32				
AN	Kemaning humber of entit	es that can be configured. 52				
NAT		(The second second				
Virtual Servers	Use Interface	ipoe_etnu/etnu.1 ¥				
Port Triggering	Application Name:					
DMZ Host	Select an application:	Select One 🔹				
LIDnD						
UPIIF	Custom application:		-			
ecurity	Custom application:					
ecurity arental Control	Custom application:	ort EndTrigger ProtocolOpen Po	ort StartOpen Port EndOpen Pr	otocol		
Security Parental Control Sandwidth Control	Custom application:	ort End Trigger Protocol Open Po	ort StartOpen Port End Open Pr	otocol		
Security Parental Control Sandwidth Control Routing	Custom application:	ort End Trigger Protocol Open Po	ort Start Open Port End Open Pr	otocol T		
Security Parental Control Sandwidth Control Routing DNS	Custom application:	ort End Trigger Protocol Open Po TCP • TCP •	ort Start Open Port End Open Pr TCP TCP	otocol •		
Security Rearental Control Sandwidth Control touting DNS DSL	Custom application:	TCP V TCP V TCP V TCP V TCP V	TCP	otocol V V		
iecurity Parental Control Isandwidth Control Couting DNS DSL itorage Service	Custom application:	ort End Trigger Protocol Open Pe TCP • TCP • TCP • TCP •	rt Start Open Port End Open Pr TCP TCP TCP TCP TCP	viccol v v v		
iecurity Parental Control Isandwidth Control Itouting INIS ISL Itorage Service Interface Grouping	Custom application:	TCP V TCP V TCP V TCP V TCP V TCP V TCP V	rt StartOpen Port EndOpen P TCP TCP TCP TCP TCP	etocol T T V V V		
ecurity arental Control touting INIS INIS torage Service tterface Grouping P Tunnel	Custom application:	TCP • TCP • TCP • TCP • TCP • TCP • TCP • TCP •	Int Start Open Port End Open P TCP TCP TCP TCP TCP TCP TCP	otocol v v v v v		
ernit arental Control andwidth Control outing INIS SL torage Service torage Service terface Grouping P Tunnel ertificate	Custom application:	Trigger Protocol Open Pe       TCP •       TCP •	Int StartOpen Port End Open Port TCP TCP TCP TCP TCP TCP TCP TCP	v v v v v v v v v v v v v v v v v v v		

**Use Interface:** Select a WAN connection to which you wish to apply the rules. When there is only one WAN connection available, the rules will be automatically applied to it.

Application Name: Two options are available:

Select an application: Select one from the drop-down list directly.

- Custom application: Custom application by yourself.

Trigger Port Start/Trigger Port End: The port range for an application to initiate connections.

Trigger Protocol: Select the protocol from the drop-down list. If you are unsure, select TCP/UDP.

Open Port Start/ Open Port End: These are the starting number and ending number for the ports that will be



automatically opened by the built-in firewall when connections initiated by an application are established.

## **DMZ Host**

The default DMZ (De-Militarized Zone) host feature is helpful when you are using some online games and

videoconferencing applications that are not compatible with NAT (Network Address Translation).

Device Info	NAT DMZ Host
Advanced Setup	
Layer2 Interface	The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer
WAN Service	
LAN	Enter the computer's IP address and click 'Save/Apply' to activate the DMZ host.
NAT	
Virtual Servers	Clear the IP address field and click 'Save/Apply' to deactivate the DMZ host.
Port Triggering	
DMZ Host	DMZ Höst IP Address
UPnP	
Security	Save/Apply
Parental Control	

DMZ Host IP Address: The IP Address of the device for which the router's firewall will be disabled. Be sure to assign a

static IP Address to that device. The DMZ host should be connected to a LAN port of the device. Be sure to assign a

static IP address to that DMZ host.

Device Info	NAT DMZ Host
Advanced Setup	
Layer2 Interface	The Broadband Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host compute
WAN Service	
LAN	Enter the computer's IP address and click 'Save/Apply' to activate the DMZ host.
NAT	
Virtual Servers	Clear the IP address field and click 'Save/Apply' to deactivate the DMZ host.
Port Triggering	
DMZ Host	DMZ Host IP Address: 192.168.1.100
UPnP	
Security	Save/Apply

# Warning!

DMZ servers pose a security risk. A computer designated as the DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet.

## UPnP

UPnP (Universal Plug and Play) allows Windows based systems to configure the device for various Internet applications automatically. UPnP devices can automatically discover the services from other registered UPnP devices on the network. If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications, like instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.





Enable UPnP: Check/uncheck to enable/disable the UPnP feature.

# ANOTE

UPnP is activated only when there is a live WAN service with NAT enabled.

# 4.2.5 Security

This section explains the following information:

- IP Filtering
- MAC Filtering

# **IP Filtering**

#### **Outgoing IP Filtering Setup**

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be **BLOCKED** by setting up filters. Choose **Add** or **Remove** to configure outgoing IP filters.

Device Info	Outgoing IP Filtering Setup
Advanced Setup	
Layer2 Interface	by default, all outgoing it' traffic from LAW is allowed, but some it' traffic can be <b>BLOCKED</b> by setting up inters,
WAN Service	Choose Add or Remove to configure outgoing 10 filters
LAN	choose Add by Remove to configure bacgoing as inters.
LAIN	
NAT	Eiter Name ID Version Brotocol CrrID/ Brofivi eanth CrrDart DetB/ Brofivi eanth DrtBart Demovo

Choose Add to enter the following screen:



Tend		lome Pag
Device Info Advanced Setup	Add IP Filter Outgoing	
Layer2 Interface	The screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule	must
WAN Service	be satisfied for the rule to take effect. Click 'Apply/Save' to save and activate the filter.	
LAN		
NAT	Filter Name:	
Security	IP Version: IPv4 •	
IP Filtering	Protocol:	
Outgoing	Source IP address/prefix length]:	
Incoming	Source Port (port or portsport):	
MAC Filtering	Destination IP address(/orefix length)	
Parental Control		
Bandwidth Control	Destination Port (port or portport):	
Routing		
DNS	(Learning)	
DSL	Apply/Save	

This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click

Apply/Save to save and activate the filter.

- **Filter Name:** Enter a descriptive filtering name.
- **IP Version:** Support IPv4.
- **Protocol:** TCP/UDP, TCP, UDP and ICMP are available for your option.
- Source IP address [/prefix length]: Enter the LAN IP address to be filtered.
- Source Port (port or port: port): Specify a port number or a range of ports used by LAN PCs to access the Internet. If you are unsure, leave it blank.
- Destination IP address [/prefix length]: Specify the external network IP address to be accessed by specified LAN PCs.
- **Destination Port** (port or port:port): Specify a port number or a range of ports used by LAN PCs to access external network.

#### **Incoming IP Filtering Setup**

When the firewall is enabled on a WAN or LAN interface, all incoming IP traffic is BLOCKED. However, some IP

traffic can be **ACCEPTED** by setting up filters.

Choose Add or Remove to configure incoming IP filters.

Tend	a
Device Info	Incoming IP Filtering Setup
Advanced Setup	
Layer2 Interface	When the firewail is enabled on a WAN or LAW interface, all incoming IP traffic is BLUCKED. However, some IP traffic can be ACCEPTED by setting up filters.
WAN Service	Choose Add or Remove to configure incoming IP filters
LAN	choose had on nemore to company mooning a mean
NAT	Filter Name Interfaces IP Version Protocol SrcIP/ PrefixLength SrcPort DttlP/ PrefixLength DstPort Remove
Security	turci dente internece in activen interese inter a concernant internet and internet.
IP Filtering	Add Domain
Outgoing	And Kennos
Incoming	



#### Click **Add** to enter the following screen:

evice Info	Add IP Filter Incoming		
dvanced Setup			
Layer2 Interface	The screen allows you to create a filter	rule to identify incoming IP	<sup>1</sup> traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must
WAN Service	be satisfied for the rule to take effect.	Click 'Apply/Save' to save an	nd activate the filter.
LAN			
NAT	Filter Name:		
Security	IP Version:	IPv4 v	
IP Filtering	Protocol:		
Outgoing	Source IP address[/prefix length]:		
Incoming	Source Port (port or port:port):		
MAC Filtering	Destination IP address[/prefix length]:		
arental Control	Destination Red (part or partment)		
andwidth Control	Destination Port (port of portport).		
Routing	MAN Interform (Configured in David	in a neadle and midde financel	I surplied and LAN tokenings
NS	Colort and a second way a second	ng mode and with firewal	Tenabled) and LAN Interfaces
DSL	select one of more wanycan interiac	es displayed below to apply	uns juie.
torage Service			
nterface Grouping	Select All S ipoe_eth0/eth0.2	br0/br0	
P Tunnel			
Certificate			
			Apply/Save

This screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click

Apply/Save to save and activate the filter.

- **IP Version:** Select IP version.
- **Protocol:** TCP/UDP, TCP, UDP and ICMP are available for your option.
- Source IP address [/prefix length]: Enter the Internal IP address [/prefix length] to be filtered.
- Source Port (port or port: port): Specify a port number or a range of ports used by PCs from external network to access your internal network.
- **Destination IP address [/prefix length]:** Specify the internal network IP address [/prefix length] to be accessed by the specified PCs from external network.
- **Destination Port** (port or port:port): Specify a port number or a range of ports used by PCs from external network to access your internal network.

## **MAC Filtering**

A bridge WAN service is needed to configure this service.

MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be forwarded except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be blocked except those matching with any of the specified rules in the following table. Choose **Add** or **Remove** to configure MAC filtering rules.



Device Info	MAC Filtering Setup
Advanced Setup Layer2 Interface WAN Service	MAC Filtering is only effective on ATM PVCs configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table.
LAN NAT Security IP Filtering	MAC Filtering Policy For Each Interface: WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.
MAC Filtering Parental Control Bandwidth Control Routing DNS DSL	Interface     Policy     Change       eth0.1     FORWARD     Image       Change Policy     Change Policy
Storage Service Interface Grouping IP Tunnel Certificate Multicast	Choose Add or Remove to configure MAC filtering rules. Interface Protocol Destination MAC Source MAC Frame Direction Remove Add Remove



Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED

AUTOMATICALLY! You will need to create new rules for the new policy.

Click Add to enter the following screen:

Tend	a
Device Info Advanced Setup Layer2 Interface WAN Service LAN NAT Security IP Filtering	Add MAC Filter Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.A maximum 32 entries can be configured. Protocol Type: Destination MAC Address: Source MAC Address: Frame Direction: LAN<=>WAN
Mac Filtering Parental Control Bandwidth Control Routing DNS DSL	WAN Interfaces (Configured in Bridge mode only)           br_eth0leth0.1 •           Save/Apply

Here you can create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple

conditions are specified, all of them take effect. Click Save/Apply to save and activate the filter.

Protocol Type: Select a protocol type from the drop-down list.

Destination MAC Address: Enter the MAC address of data frame being restricted to arrive.

Source MAC Address: Enter the MAC address of data frame being restricted to come.

Frame Direction: Select a frame direction from the drop-down list.

WAN Interfaces: Select a WAN interface from the drop-down list.

# **4.2.6 Parental Control**

This section explains the following information:



- Time Restriction
- URL Filter

# **Time Restriction**

Click **Parental Control > Time Restriction > Add** to enter the following screen.

Tend	a	Home Pag
Device Info	Access Time Restriction	
Advanced Setup		
Layer2 Interface	This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device	ce where the
WAN Service	browser is running. To restrict other LAN device, click the *Other MAC Address* button and enter the MAC address of the other LAN device. To find out the MAC address of a	Windows based
LAN	PC, go to command window and type *ipconfig /all*,	
NAT		
Security	User Name	
Parental Control		
Time Restriction	Browser's MAC Address 44:37:e6:36:tb:25	
Url Filter	Other MAC Address	
Bandwidth Control	(proprior province (province)	
Routing		
DNS	Description of the second star and star and star	
DSL		
Storage Service	Click to select	
Interface Grouping		
IP Tunnel	Start Blocking Time (hhmm)	
Certificate	End Blocking Time (hh:mm)	
	Apply/Save	

Here you can add time of day restriction that an attached LAN device can access the Internet.

The Browser's MAC Address automatically displays the MAC address of the LAN device where the browser is running.

To restrict other LAN device, check the "Other MAC Address" option and enter its MAC address.

- User Name: Enter a user name.
- **Browser's MAC Address:** Automatically adds the MAC address of the attached LAN device where the browser is running.
- Other MAC Address: Specify the MAC address of the computer that you want to apply Internet access restriction.
- Days of the week: Click to select the days of the week during which you wish to restrict Internet access.
- Start Blocking Time/ End Blocking Time: Specify time of day restriction to an attached LAN device. Within this specified time length of the day, this LAN device will be blocked from the Internet.
- Apply/Save: Click Apply/Save to save and apply your settings.

## **URL Filter**

Here you can add URL access restriction to specific LAN PCs.



Select the URL List Type (Exclude or Include) first and then click Add to enter the screen below for configuring the list

entries.

Device Info	Parental Control URL Filter	Add		
Advanced Setup				
Layer2 Interface	Enter the URL address then cli	ck "Apply/Save" to a	add the entry to the URL filter	9-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1-1
WAN Service				
LAN				
NAT	URL Address:			
Security				
Parental Control				
Time Restriction				Apply/Save

URL Address: Enter a specific URL or a key word of domain name in this field.

Click Apply/Save to apply and save the settings.

# ANOTE

If you have accessed the URL before you include it in a URL filter rule, you must reboot the router and erase it from

your PC to activate this URL filter rule. To erase the domain name from your PC:

**1.** Click the keys  $\mathbf{H} + \mathbf{R}$  on the keyboard to enable "Run" dialog, and type **cmd** > click **OK**.

(Note that different operation systems may have different ways to enable "Run"; Windows is taken a guide here.)



📼 Run	×
	Type the name of a program, folder, document or Internet resource, and Windows will open it for you.
Open:	cmd 🗸
	OK Cancel <u>B</u> rowse

2. Then type **ipconfig** /flushdns and hit Enter on the keyboard.

C:\WINDOWS\system32\cmd.exe	-	×
Microsoft Windows [Version 10.0.10130] (c) 2015 Microsoft Corporation. All rights reserved.		^
C:\Users\Vita Wu>ipconfig /flushdns		
Windows IP Configuration		
Successfully flushed the DNS Resolver Cache.		
C:\Users\Vita Wu>		

# 4.2.7 Bandwidth Control

When multiple devices each of which requests a different bandwidth attach to the modem router, to ensure the attached devices obtaining a fair bandwidth and getting a fluent Internet experience, set a bandwidth control rule.

Check Enable Bandwidth Control to enable this feature.

evice Info	QoS Bandwidth Control								
dvanced Setup	This page allows you to control bandwidth of the specified IP segment. ID *0* is an example as a reference. You can add details in blanks below the list. If you want to limit a sing								
Layer2 Interface	address'bandwidth,say,192.168.1.2, keep its start IP Address the same as its end IP ,namely,enter 192.168.1.2-2 in the IP Address Range field.								
WAN Service	How	v to add a new entr	y? 1.Edit the r	ules	in banks; 2,Click C	ommit; 3, Click A	pply/Save to acti	ate your configurations.	
LAN	Not	e:Up to 16 entries	can be allowed	l,Th	e End IP Address ju	ust could edit the h	ost number.To a	tivate your configurations	s,click Apply/Save.
NAT									
Security									
Parental Control	🕑 E	Enable Bandwidth (	Control						
Bandwidth Control		5	al.m.			Max Uplink	Max		
Routing	ID	Description	Status		IP Address	Speed (Kbps)	Downlink	Action	
DNS		A STREET OF	-	-	States and states	1.000	sheed (kobs)	(	
SL.	0	Example	Enable		192,168,1.2-2	200	400	Edit Delete	
torage Service									
Tunnel	Des	cription							
ertificate	IP A	ddress Range	1			-			
Iulticast				_					
TV	Max	(Upstream Speed)	Kbps)						
	Max	Downstream Spe	ed(Kbps)						
reless									
reless anostics	C		10	Inal					



Description: Name the bandwidth control rule as you like.

IP Address Range: Type the IP address range of	of target hosts. Follow t	he example	192.168.1.2	-	254	•
If you want to set one host, follow the example	192.168.1.2	- 2				

Max Upstream Speed (Kbps): Set the upstream speed as your actual bandwidth need.

Max Downstream Speed (Kbps): Set the downstream speed as your actual bandwidth need.

Status: Enable or Disable.

After you have edited the details of the bandwidth control rule, click Commit first to save and then click Apply/Save to activate the settings.

# 4.2.8 Routing

This section explains the following:

- Default Gateway
- Static Route

## **Default Gateway**

Default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.

Device Info	Routing Default Gateway	
Advanced Setup		
Layer2 Interface		
WAN Service	Default gateway interface list c	an have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the
LAN	last one the lowest priority if th	e WAN interface is connected. Priority order can be changed by removing all and adding them back in again.
NAT		
Security	Selected Default	Available Routed WAN
Parental Control	Gateway Interfaces	Interfaces
Bandwidth Control		
Routing	eth0.1 🔟	4
Default Gateway		
Static Route	.>	
DNS	<-	
DSL		
Storage Service		
Interface Grouping		
IP Tunnel		
Certificate	TRUG - Calanta and found and the	
Multicast	19V0 : select a preferred wan in	terrace as the system default invo gateway.
IPTV	Selected WAN Interface NO CO	INFIGURED INTERFACE V
Nireless		

Selected Default Gateway Interfaces: Displays the selected default gateway interfaces. Select a WAN interface .

and click the *interfaces* box.



• Available Routed WAN Interfaces: Displays the available routed WAN interfaces. Select a WAN interface and

click the 🔛 button to add it to the **Selected Default Gateway Interfaces** box.

Apply/Save: Click to save and activate your settings.

## **Static Route**

Static routes provide additional routing information to your router. Typically, you do not need to add static routes. However, when there are several routers in the network, you may want to set up static routing. Static routing determines the path of the data in your network. You can use this feature to allow users on different IP domains to access the Internet via this device. It is not recommended to use this setting unless you are familiar with static routing. In most cases, dynamic routing is recommended, because this feature allows the router to detect the physical changes of the network layout automatically.



#### Click Add to enter the following screen:

Tend	а		
Device Info	Routing Static Route Add		
Advanced Setup			
Layer2 Interface	Enter the destination network address, subr	et mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to	the routing table.
WAN Service			
LAN			
NAT	IP Version:	IPv4 T	
Security	Destination IP address/prefix length:		
Parental Control	Interface:	<b>T</b>	
Bandwidth Control	Gateway IP Address:		
Routing	(optional: metric number should be greater	than or equal to zero)	
Default Gateway	Metric:	(Ranger1-9990)	
Static Route	We the	(Kanger 5555)	
DNS		Apple/Sour	
DSL		Abbiligade	

- **IP Version:** Select IP version.
- Destination IP address/prefix length: Enter the destination IP address and prefix length of the final destination.
- Interface: Select an interface from the drop-down list.
- Gateway IP address: Enter the gateway IP address, which must be a router on the same LAN segment as the



router.

- **Metric:** Enter a number in the Metric field. This stands for the number of routers between your network and the destination.
- Apply /Save: Click to apply and save your settings.

## ANOTE

- 1. Destination IP address cannot be on the same IP segment as WAN or LAN segment as the router.
- 2. Only configure additional static routes for unusual cases such as multiple routers or multiple IP subnets located on

your network. Wrong static routes may lead to network failure.

3. For system created route, the "Remove" checkbox is disabled.

# 4.2.9 DNS

## **DNS Server (Static DNS)**

The DNS server translates domain names to numeric IP addresses. It is used to look up site addresses based on their

names. If the DNS server works incorrectly, Internet access will be blocked.

DNS server is configured when you are setting up your Internet connectivity. So, you do not have to finish DNS server setup here unless your network works false.

### For IPv4

1 Click Advanced Setup > DNS > DNS Server, and enter the screen below.

Tend	a Home Fag
Device Info Advanced Setup Layer2 Interface WAN Service LAN NAT Security Parental Control Bandwidth Control	DNS Server Configuration Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. DNS Server Interfaces can have multiple WAN interfaces served as system dns servers but only one will be used according to the priority with the first being the higest and the fast one the lowest priority if the WAN interfaces: Select DNS Server Interface from available WAN interfaces: Select DNS Server Interface from available WAN interfaces:
Routing DNS DNS Server Dynamic DNS	Interfaces eth0.1 End IPV4 settings
DSL Storage Service Interface Grouping IP Tunnel Certificate Multicast JPTV Wireless	Use the following Static DNS IP address:       Primary DNS server:       Secondary DNS server:



2 Check the Select DNS Server Interface from available WAN interfaces option if the device gets a DNS

address automatically from an upstream device. Or select the **Use the following Static DNS IP address** option and enter static DNS server address provided by your ISP.

3 Click **Apply/Save** at the bottom of the page.

#### For IPv6

Storage Service Interface Grouping	<b>IPV6 :</b> Select the configured WAN interface for IPv6 DNS server information OR e Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Clie	enter the static IPv6 DNS server Addresses. nt on that interface.
IP Tunnel Certificate Multicast IPTV Wireless Diagnostics Management	<ul> <li>Obtain IPv6 DNS info from a WAN interface:</li> <li>WAN Interface selected: NO CONFIGURED INTERFACE </li> <li>Use the following Static IPv6 DNS address:</li> <li>Primary IPv6 DNS server:</li></ul>	For IPv6 settings
	Аррі	ly/Save

2 Select the Obtain IPv6 DNS info from a WAN interface option if the device gets a DNS server address from the upstream device automatically. And select a configured WAN interface for the IPv6 DNS server information. Or select the Use the following Static IPv6 DNS address option and enter the static IPv6 DNS server address provided by your ISP.

#### 3 Click **Apply/Save**.

## ANOTE

- 1. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.
- 2. If you are not clear about the static DNS server IP information, ask your ISP to provide it.
- **3.** The default settings are recommended if you are unsure about the DNS server addresses. If a wrong DNS server address is configured, webpages may not be open.

## **Dynamic DNS (DDNS)**

If your Internet service provider (ISP) gave you a static (fixed) public IP address, you can register a domain name and have that name associated with your IP address by public Domain Name Servers (DNS). However, if your ISP gave you a dynamic (changing) public IP address, you cannot predict what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. It allows you to register your domain to their IP address and forward traffic directed at your domain to your frequently changing IP address. If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private



addresses are not routed on the Internet.

Click Advanced Setup > DNS > Dynamic DNS to enter the Dynamic DNS screen.



Click Add to configure the DDNS settings.

Device Info	Add Dynamic DNS	
Advanced Setup		
Layer2 Interface	This name allows you to	add a Dunamic DNS address from dun com or TZO, or NO-IP
WAN Service	D-DNS provider	dvn.com V
LAN	e ette planati	
NAT	Hostname	
Security	Interface	ipoe_eth0/eth0.1 🔻
Parental Control		
Bandwidth Control	DynDNS Settings	
Routing	Username	
DNS	Password	
DNS Server		ánniv/Sa

D-DNS Provider: Select your DDNS service provider from the drop-down menu.

Hostname: Enter the DDNS domain name registered with your DDNS service provider.

Interface: Specify a WAN connection interface.

Username: Enter the DDNS user name registered with your DDNS service provider.

Password: Enter the DDNS Password registered with your DDNS service provider.

Click Apply/Save to save your settings.

#### Example: dyn.com

Hostname: tenda.dyndns.org

Username: tenda

Password: 123456789

#### **Add Dynamic DNS**



Select **dyn.com** from the **D-DNS provider** drop-down menu.



- 2 Enter the hostname. Here is "tenda.dyndns.org" for example.
- 3 Specify a WAN connection interface.

#### **DynDNS Settings**

4 Enter your DynDNS username. Here is "tenda"

for example.

- 5 Enter the password of DynDNS account.
- Here is "123456789" for example.
- 6 Click Apply/Save to save your configuration.

Example	
Add Dynamic DNS	
This page allows you to	add a Dynamic DNS address from dyn.com or TZO, or NO-IF
D-DNS provider	dyn.com 🗸
Hostname	tenda dyndns org
Interface	ipoe_eth0/eth0.1 V
DvnDNS Settings	
Username	tenda
Password	•••••

# 4.2.10 DSL

This screen provides multiple ASDL modulation modes to meet diversified environments. You can also select phone line pair and Capability.

DSL parameter configurations must be supported by ISP to take effect. Actual parameters (see Statistics-DSL) resulted

from the negotiation between your router and ISP. Wrong configurations may fail your Internet access.

The best DSL configurations are the factory defaults. Only change them with the support of your ISP or our technical

staff when your router fails to negotiate with ISP in DSL (ATM) mode.

Device Info	DSL Settings	
Advanced Setup		
Layer2 Interface	Select the modulation below.	
WAN Service	G.Dmt Enabled	
LAN	Glite Enabled	
NAT	es Ginte Enabled	
Security	T1.413 Enabled	
Parental Control	ADSL2 Enabled	
Bandwidth Control	Anneyl Enabled	
Routing		
DNS	ADSL2+ Enabled	
DSL	AnnexM Enabled	
Storage Service		
Interface Grouping	Select the phone line pair below.	
IP Tunnel	Inner pair	
Certificate		
Multicast	Outer pair	
IPTV		
Vireless	Capability	
Diagnostics	🗷 Bitswap Enable	
Management	SRA Enable	



Check the checkbox next to a modulation to enable it and then click

Apply/Save

Advanced Settings: Click it to enter the Advanced Settings screen as below.

Device Info	DSL Advanced Settings	
Advanced Setup		
Layer2 Interface	Select the test mode below.	
WAN Service		
LAN	Normal	
NAT	Reverb	
Security	(DAL) (CAL)	
Parental Control	Medley	
Bandwidth Control	No retrain	
Routing	() L3	
DNS		
DSL		
Storage Service		Apply Tone Selection

Here you can select the test mode and tone.

# TIP

If you are unsure about the DSL parameters, please apply the factory default settings. Wrong configurations may fail

your Internet access.

# 4.2.11 Storage Service

This section explains the following:

- Storage Device Info
- User Account

The modem router provides a USB port. You can attach a USB storage device to it and share your USB device with a user in the LAN.

# **Storage Device Info**

Once you plug your USB storage device into the USB port, the details about the USB storage will be recorded shown as below table.



Image: Enable Samba The Storage service allows you to use Storage devices with modern Connect your USB device, you can share your device with other Lan Umount button is mainly used to disconnect your USB device, you may lose data if remove USB device directly.           Volumename         FileSystem         Total Space(MB)         Used Space(MB)           usb1_1         fat         14278         5		your device with other Lan H
The Storage service allows you to use Storage devices with modem Connect your USB device, you can share your device with other Lan Umount button is mainly used to disconnect your USB device, you may lose data if remove USB device directly.           Volumename         FileSystem         Total Space(MB)         Used Space(MB)           usb1_1         fat         14278         5	The Storage service allows you to use Storage devices with modem Connect your USB device, you can shar Umount button is mainly used to disconnect your USB device, you may lose data if remove USB device dire	your device with other Lan H
Volumename       FileSystem       Total Space(MB)       Used Space(MB)         usb1_1       fat       14278       5	Umount button is mainly used to disconnect your USB device, you may lose data if remove USB device dire	
VolumenameFileSystemTotal Space(MB)Used Space(MB)usb1_1fat142785Umount		ctly.
VolumenameFileSystemTotal Space(MB)Used Space(MB)usb1_1fat142785Umount		
usb1_1 fat 14278 5	Volumename FileSystem Total Space(N	B) Used Space(MB)
Umount	usb1_1 fat 14278	5
Umount		5
	Umount	

Umount and then uplug your USB device. Removing directly may damage your USB storage device.

# **User Account**

Click

Accessing the USB storage device requires an account. You can click Apply/Save to use the default account or you can customize a new one. Pay attention to that your computer system will record the account you used at the first time.

Storage Use	er Account Setup	
In the boxes Note that us (you can use	below, enter the us er name should not only simple letters,	er name/password you like to access the Storage Service. be any of 'admin', 'support', 'nobody' or 'user'. numbers and underscores.)
Username:	samba	[3-64]
Password:	samba	[3-64]
		Apply/Save

## Application: How to access the USB storage device attached to the

## modem router?

Step 1: Plug USB storage device.

Plug your USB storage device into the USB port, and make sure the USB LED indicator is on.

Step 2: Create an account.

Go to User Account interface, and set up your account. Here the default account "samba" is kept. And click Apply/Save



to save and apply.

In the boxes	below, enter the u	user name/password you like to access the Storage Sen
Note that us	er name should no	ot be any of 'admin', 'support', 'nobody' or 'user'.
(you can use	only simple letter	s, numbers and underscores.)
Username:	samba	[3-64]
Password:	samba	[3-64]

Step 3: Access the USB storage device from a computer.

Click  $\mathbf{R}$  on the keyboard to pop up the **Run** dialog, and type  $\underline{192.168.1.1}$  in the blank field.

Click OK.

🖅 Run		Х
	Type the name of a program, folder, document or Interne resource, and Windows will open it for you.	ŧt
<u>O</u> pen:	\\192.168.1.1	*
	OK Cancel <u>B</u> rowse	

Step 4: Access the USB storage device with the account "samba".

Double click \_\_\_\_\_\_, and enter your account "samba" and password to finish the credentials. Then, click **OK**.



INCLUM	ork = 192.168.1.1	~ X	Search 192.168.1.1	۶
Downloads Music	usb1_1			
Videos	Windows Security	×	1	
Local Disk (C:) SWindows.~BT	Enter network credentials Enter your credentials to connect to: 192.168.1.1			
CommonFram	samba			
Intel				
MSOCache				
PerfLogs	Domain: WIN-4CQNT5DOL2J			
Program Files	Remember my credentials			
Program Files (	🚫 Access is denied.			
ProgramData				

#### Access successfully!

🖳   🛃	usb1_1 Home Shar	e View				-	- ×
÷	~ ↑ 🖵 > 1	Network > 192.168.1	.1 ⇒ usb1_1		~ C	Search usb1_1	p
	EFI ^	Name	et	Date modified 03/07/2015 17:14	Type File folder	Size	
	MSOCache PerfLogs Program Files	icon.ico	This is n	12/02/2014 02:02	lcon	287 KB	

# 4.2.12 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button. The **Remove** button will remove the grouping and add the ungrouped interfaces to the Default group.

levice Info	Interface Grou	iping A i	maximum 16 en	tries can be confi	igured					
dvanced Setup Layer2 Interface ATM Interface ETH Interface	Interface Group interfaces using	ping suppo g the Add l:	irts multiple ports outton. The Remo	to PVC and brid ove button will re	ging groups. Each gr move the grouping a	roup will perform as an indep and add the ungrouped inter	pendent network. To su faces to the Default gr	opport this feature, you mus oup. Only the default group	st create mapping groups with appropriat a has IP interface.	te LAN and W
WAN Service										
WAN Service LAN	Group Name	Remove	WAN Interface	LAN Interfaces	DHCP Vendor IDs	1				
VAN Service AN IAT	Group Name	Remove	WAN Interface	LAN Interfaces eth1	DHCP Vendor IDs					
VAN Service AN IAT ecurity	Group Name	Remove	WAN Interface ppp0.1 atm0.2	LAN Interfaces eth1 eth2	DHCP Vendor IDs	-				
VAN Service AN IAT ecurity arental Control	Group Name Default	Remove	WAN Interface ppp0.1 atm0.2	LAN Interfaces eth1 eth2 eth3	DHCP Vendor IDs	-				
VAN Service AN IAT ecurity arental Control andwidth Control	Group Name Default	Remove	WAN Interface ppp0.1 atm0.2	LAN Interfaces eth1 eth2 eth3 eth0	DHCP Vendor IDs	-				
AN Service N AT curity rental Control ndwidth Control uting	Group Name Default	Remove	WAN Interface ppp0.1 atm0.2	LAN Interfaces eth1 eth2 eth3 eth0	DHCP Vendor IDs					
AN Service IN AT scurity arental Control andwidth Control suting VS	Group Name Default	Remove	WAN Interface ppp0.1 atm0.2	LAN Interfaces eth1 eth2 eth3 eth0	DHCP Vendor IDs	-				



#### Click **Add** to enter the screen below:

Tenda		н
Device Info	Interface grouping Configuration	
Advanced Setup		
Layer2 Interface	To create a new interface group:	
ATM Interface	1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:	
ETH Interface		
WAN Service	2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified ven	dor ID
LAN	(DHCP option 60) will be denied an IP address from the local DHCP server.	
NAT		
Security	3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. Note that these clients may obtain public	IP
Parental Control	addresses	
Bandwidth Control		
Routing	4. Click Apply/Save button to make the changes effective immediately	
DNS		
DSL		
Storage Service		
Interface Grouping	IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modern to allow it to obtain an appropriate IP address.	
IP Tunnel		
Certificate	Group Name:	
Multicast		
IPTV	WAN Interface used in the grouping br.0.0_35/atm0.2 🔻	
Vireless		
Diagnostics		
Management		
2	Grouped LAN Interfaces Available LAN Interfaces	
	etto .	

- **Group Name:** Define a name for group.
- WAN Interface used in the grouping: WAN connection to which the interface grouping rules apply.
- Available LAN Interfaces: LAN interfaces which are available for interface grouping.
- Grouped LAN Interfaces: LAN interfaces which are classed into the specified WAN connection.

#### To create a new interface group:

- 1 Enter the Group name and the group name must be unique.
- 2 Select an available WAN interface for the LAN network proxy.
- 3 Define the available LAN interface to connect to the specified WAN interface. Select interfaces from the

Available LAN Interfaces list and add it to the Grouped LAN Interfaces list using the arrow buttons to create the required mapping of the ports.

(4) Click **Apply/Save** button to make the changes effective immediately.

If you want to bypass NAT via the router's interface and obtain the public IP address automatically, you need to add the DHCP vendor ID in the **Automatically Add Clients with the following DHCP Vendor IDs** section. After the ID takes effect, your router will automatically detect the DHCP request from computers on the LAN, and it will forward the DHCP vendor ID and the corresponding DHCP request to the WAN interface used in the interface rules.

# ANOTE

- 1. Eth0, eth1, eth2 and eth3 respectively represent 1/WAN, 2, 3 and 4/iTV port of the device. And wlan0 is the port for all wireless devices connecting to the modem router.
- **2.** If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.
- 3. No Interface/None indicates that there is no WAN port.



# 4.2.13 IP Tunnel

This section explains the following information:

- IPv6inIPv4
- IPv4inIPv6

## IPv6inIPv4

Click IPv6inIPv4 and Add to enter the following screen:

evice Info	IP Tunneling 6in4 Tunnel Configurat	tion
dvanced Setup		
Layer2 Interface	Currently, only 6rd configuration is supp	orted.
WAN Service		
LAN	Tunnel Name	
NAT	Mechanism:	6RD 🔻
Security	Associated WAN Interface:	· · · · · · · · · · · · · · · · · · ·
Parental Control	Associated LAN Interface:	LAN/br0 🔻
Bandwidth Control	Manual Automatic	
Routing		
DNS		
DSL Storage Service	IPv4 Mask Length:	
Interface Grouping	6rd Prefix with Prefix Length:	
IP Tunnel	Border Relay IPv4 Address:	

- **Tunnel Name:** Specify the name of the tunnel.
- Mechanism: Currently, only 6RD configuration is supported.
- Associated WAN Interface: Specify the WAN interface of the tunnel.
- Associated LAN Interface: Specify the LAN interface of the tunnel.
- Manual: If you select Manual, configure the following settings also:
  - **IPv4 Mask Length:** Specify the IPv4 Mask Length.
  - **6rd Prefix with Prefix Length:** Specify the 6rd Prefix with Prefix Length.
  - Sorder Relay IPv4 Address: Specify the Border Relay IPv4 Address.
- Automatic: If Automatic is selected, no configurations are required.
- Apply/Save: Click to apply and save your settings.



# IPv4inIPv6

Click **IPv4inIPv6** and **Add** to enter the following screen:

Device Info	IP Tunneling 4in6 Tunnel Configuration		
Advanced Setup			
Layer2 Interface	Currently, only DS-Lite configuration is supp	oorted.	
WAN Service			
LAN	Tunnel Name		
NAT	Mechanism:	DS-Lite •	
Security	Associated WAN Interface:	•	
Parental Control	Associated LAN Interface:	LAN/br0 •	
Bandwidth Control	Manual Automatic		
Routing			
DNS	AFTR:		
DSL			
Storage Service			
Interface Grouping			
IP Tunnel			
IPv6inIPv4			Anathiltian

- **Tunnel Name:** Specify the name of the tunnel.
- Mechanism: Currently, only DS-Lite configuration is supported.
- Associated WAN Interface: Specify the WAN interface of the tunnel.
- Associated LAN Interface: Specify the LAN interface of the tunnel.
- Manual: If you select Manual, enter the AFTR information also:
- Automatic: If Automatic is selected, no configurations are required.
- Apply/Save: Click to apply and save your settings.

# 4.2.14 Certificate

This section explains the following information:

- Local Certificates
- Trusted CA (Certificate Authority) Certificates

## **Local Certificates**

Here you can add, view or remove certificates. Local certificates are used by peers to verify your identity. Maximum 4



	Local Certificates
Device Info	
dvanced Setup	Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Layer2 Interface	Maximum 4 certificates can be stored,
WAN Service	
LAN	
NAT	
Security	
Parental Control	Name In Use Subject Type Action
Bandwidth Control	
Routing	Create Certificate Request Import Certificate
DNS	
DSL	
Storage Service	
Interface Grouping	
IP Tunnel	
Certificate	
Local	
Trusted CA	

#### To generate a certificate signing request:

1 Click the **Create Certificate Request** button to enter the page below.

Davias Info	Create new certificate requ	nect
Advanced Cotur	erente neur certificate req.	
Lover2 Interface	To generate a certificate sig	ming request you need to include Common Name. Organization Name. State/Province Name, and the 2-letter Country Code for the certificate
MAN Somico	te generate a certanaate sig	
IAN	Certificate Name:	
NAT	Common Name:	
Security	Operation Name	
Parental Control	Organization Marne:	
Bandwidth Control	State/Province Name:	
Routing	Country/Region Name:	US (United States)
DNS		
DSL		
Storage Service		
Interface Grouping		Anniv
IP Tunnel		1.45.47
Certificate		
Local		
Trusted CA		

- 2 Specify the Common Name, Organization Name and State/Province Name
- 3 Enter the 2-letter Country Code for the certificate.
- 4 Click **Apply** to apply your settings.

#### To Import certificate:

1 Click the **Import Certificate** button on the local certificates page to enter the page below.



Device Info	Import certificate		
Advanced Setup			
Layer2 Interface	Enter certificate name, p	aste certificate content and private key,	
WAN Service			
LAN	Certificate Name:		
NAT		BEGIN CERTIFICATE	
Security		<insert certificate="" nere=""></insert>	
Parental Control			
Bandwidth Control			
Routing			
DNS			
DSL	Certificate:		
Storage Service			
Interface Grouping			
IP Tunnel			
Certificate			
Local			
Trusted CA		BEGIN RSA PRIVATE KEY	
		<insert here="" key="" private=""></insert>	

- 3 Paste the certificate content and private key.
- (4) Click **Apply** to apply your settings.

# **Trusted CA (Certificate Authority) Certificates**

Here you can add, view or remove CA certificates. CA certificates are used by you to verify peers' certificates. Maximum

4 certificates can be stored.

Device Info	Trusted CA (Certificate Authority) Certificates
Sevice Info Idvanced Setup Layer2 Interface WAN Service LAN NAT Security Parental Control Bandwidth Control Routing DNS DSL Storage Service Interface Grouping IP Tunnel Certificate Local	Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates Maximum 4 certificates can be stored. Name Subject Type Action Import Certificate



#### To Import certificate:

1 Click the **Import Certificate** button to enter the page below.

Device Info	Import CA certificate		
Advanced Setup			
Layer2 Interface	Enter certificate name an	d paste certificate content.	
WAN Service			
LAN	Certificate Name:		
NAT		BEGIN CERTIFICATE	
Security		END CERTIFICATE	
Parental Control			
Bandwidth Control			
Routing			
DNS			
DSL	Certificate:		
Storage Service			
Interface Grouping			
IP Tunnel			
Certificate			
Local			11
Trusted CA			
Multicast			Apply
IPTV			1.11.1
_			

4 Click **Apply** to apply your settings.

# 4.2.15 Multicast

Here you can configure the multicast feature.

## To configure IGMP for IPv4

- 1 Check the LAN to LAN (Intra LAN) Multicast Enable box.
- 2 Check the **Membership Join Immediate** (**IPTV**) box. This is only required for IPTV.
- 3 Keep other options unchanged from factory defaults if you are not an advanced user. This is strongly

recommended.





Device Info		
Advanced Setup	Multicast Precedence:	Disable V lower value, higher priority
Layer2 Interface		
WAN Service		
LAN	IGMP Configuration	
NAT		
Security	Enter IGMP protocol configuration fields if you want mo	dify default values shown below.
Parental Control		
Bandwidth Control	Default Version:	3
Routing	Query Interval:	125
DNS	Query Response Interval:	10
DSL Storage Service	Last Member Query Interval:	10
Interface Grouping	Robustness Value:	2
IP Tunnel	Maximum Multicast Groups:	25
Certificate	Maximum Multicast Data Sources (for IGMPv3 : [1-24]):	10
Multicast	Maximum Multicast Group Members:	25
IPTV	Fast Leave Enable:	
Wireless	LAN to LAN (Intra LAN) Multicast Enable:	
Diagnostics	Mebership Join Immediate (IPTV):	
Management		

## To configure IGMP for IPv6

- 1 Check the LAN to LAN (Intra LAN) Multicast Enable box.
- 2 Keep other options unchanged from factory defaults if you are not an advanced user. This is strongly

#### recommended.

Device Info	Maximum Multicast Group Members:	25	
Advanced Setup	Fast Leave Enable:		
Layer2 Interface	LAN to LAN (Intra LAN) Multicast Enable:		
WAN Service	Mebership Join Immediate (IPTV):		
LAN			
NAT			
Security			
Parental Control	MLD Configuration		
Bandwidth Control			
Routing	Enter MLD protocol (IPv6 Multicast) configuration fields if you want modify default value		
DNS			
DSL	Default Version:	2	
DSL Storage Service	Default Version: Query Interval:	2	
DSL Storage Service Interface Grouping	Default Version: Query Interval: Query Response Interval:	2 125 10	
DSL Storage Service Interface Grouping IP Tunnel	Default Version: Query Interval: Query Response Interval: Last Member Query Interval:	2 125 10 10	
DSL Storage Service Interface Grouping IP Tunnel Certificate	Default Version: Query Interval: Query Response Interval: Last Member Query Interval: Robustness Value:	2 125 10 10	
DSL Storage Service Interface Grouping IP Tunnel Certificate Multicast	Default Version: Query Interval: Query Response Interval: Last Member Query Interval: Robustness Value:	2 125 10 10 2 2	
DSL Storage Service Interface Grouping IP Tunnel Certificate Multicast IPTV	Default Version: Query Interval: Query Response Interval: Last Member Query Interval: Robustness Value: Maximum Multicast Groups:	2 125 10 10 2 10	
DSL Storage Service Interface Grouping IP Tunnel Certificate Multicast IPTV Vireless	Default Version: Query Interval: Query Response Interval: Last Member Query Interval: Robustness Value: Maximum Multicast Groups: Maximum Multicast Data Sources:	2 125 10 10 2 10 10	
DSL Storage Service Interface Grouping IP Tunnel Certificate Multicast IPTV Wireless Diagnostics	Default Version: Query Interval: Query Response Interval: Last Member Query Interval: Robustness Value: Maximum Multicast Groups: Maximum Multicast Data Sources: Maximum Multicast Group Members:	2 125 10 10 2 10 10 10 10	
DSL Storage Service Interface Grouping IP Tunnel Certificate Multicast IPTV Vireless Diagnostics Management	Default Version: Query Interval: Query Response Interval: Last Member Query Interval: Robustness Value: Maximum Multicast Groups: Maximum Multicast Data Sources: Maximum Multicast Group Members: Fast Leave Enable:	2 125 10 10 2 10 10 10 10 2	

Apply/Save



# 4.2.16 IPTV

If you check the Enable IPTV checkbox, you must choose a layer2 interface, and then configure the PVC info (ATM),

or VLAN info (ETH). Click

Apply/Save to save it.

Enable IPTV: Check to enable the IPTV service, or disable it.

Tenda			
Device Info	IPTV IPTV Management Configuration		
Advanced Setup			
Layer2 Interface	If IPTV checkbox is selected, choose layer2 interface, then configure the PVC info(ATM), or ETH VLAN info(ETH). Click 'Apply/Save' button to save it.		
WAN Service	☑ Enable IPTV		
LAN			
NAT	Select Laver2 Interface		
Security	• ATM Interface		
Parental Control	© FTH Interface		
Bandwidth Control			
Routing	This screen allows you to configure an ATM PVC.		
DNS	VPI- 0 [0-255]		
DSL Storage Service	VCI: 35 [0-65535]		
Interface Grouping			
IP Tunnel			
Certificate			
Multicast	Apply/Save		
IPTV			

**IPTV configuration for DSL Internet Access user:** 

- (1)Enable **IPTV**.
- 2 Select Layer2 interface: ATM Interface.
- 3 Configure an available VPI/VCI value which should be provided by your ISP.
- Click Apply/Save (4)

#### **IPTV** configuration for Ethernet Internet Access user:

- 1 Enable **IPTV**.
- (2) Select Layer2 Interface: ETH Interface.
- Click Apply/Save 3

Device Info	IPTV IPTV Management Configuration	n	
Advanced Setup			
Layer2 Interface	If IPTV checkbox is selected, choose layer2	interface, then configure the PVC info(ATM), or ETH VLAN info(ETH). Click 'Apply/Save' button to save	
WAN Service	Enable IPTV		
LAN			
NAT	Select Layer2 Interface		
Security	C ATM Interface		
Parental Control	ETH Interface		
Bandwidth Control			
Routing			
DNS	For tagged service, enter valid 802.1P Priority and 802.1O VLAN ID.		
DSL	For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.		
Storage Service	Enter 802.1P Priority [0-7]:	-1	
Interface Grouping	Enter 202 10 VI AN ID 11 40041		
IP Tunnel	Enter BOZ.1Q VEAN ID [1-4034].	-1	
Certificate			
Multicast		Apply/Save	
IPTV			


After successful IPTV configurations, Port 4/iTV on the back panel of the device can only be an IPTV port.

# TIP

For tagged service, enter valid 802.1P Priority and 802.1Q VLAN ID.

For untagged service, set -1 to both 802.1P Priority and 802.1Q VLAN ID.

# 4.3 Wireless

This section explains the following information:

- Basic
- Security
- MAC Filter
- Wireless Bridge
- Station Info

## 4.3.1 Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

iend	<b>a</b>	Hor
Device Info	Wireless Basic	
Advanced Setup		
Wireless	This page allows you to a	configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the netwo
Basic	from active scans, set the	e wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Security	Click "Apply/Save" to cor	nfigure the basic wireless options.
MAC Filter		
Wireless Bridge	Enable Wireless	
Station Info		
Diagnostics	Hide Access Point	t
Management	Enable Wireless N	Multicast Forwarding (WMF)
	SSID:	Tenda_SC0650
	BSSID:	C8:3A:35:5C:06:51
	Wireless Mode:	802.11b/g/n Mixed 🔻
	Country:	ALL
	Channel:	Auto
	Bandwidth:	40MHz V
	Control Sideband:	Lower •
	RF Power:	Normal      Enhance
	he come and	



- Enable Wireless: check/uncheck to enable/disable the wireless feature.
- Hide Access Point (Hide SSID): This option allows you to have your network names (SSID) publicly broadcast. If you choose to enable it, the SSID will be hidden.
- **SSID:** This is the public name of your WiFi.
- **BSSID:** Display the MAC address of the wireless network.
- Country: Select your country.
- **Channel:** Select a channel, or select **Auto** to let system automatically select one for your wireless network to operate on if you are unsure. The best selection is a channel that is the least used by adjacent networks.
- Bandwidth: Configure the wireless bandwidth. The default is 40MHz.
- **RF Power:** Normal or Enhance. This option may adjust the wireless signal strength.

## 4.3.2 Security

This page allows you to configure security features of the wireless LAN interface. You may set up configuration

manually or through WiFi Protected Setup (WPS).

Tend	a
	Wireless Security
Device Info	
Advanced Setup	This page allows you to configure security features of the wireless LAN interface.
Wireless	You may setup configuration manually
Basic	OR
Security	through WiFi Prototed Setup(WPS)
MAC Filter	Note: When the STA PIN is empty, PBC is used. If Hide Access Point enabled or Mac filter list is empty with "allow" chosen, WPS2 will be disabled
Wireless Bridge	
Station Info	
Diagnostics	WPS Setup
Management	
	Enable WPS Disabled •
	Manual Setup AP
	You can set the network authentication method, selecting data encryption,
	specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
	Click "Apply/Save" when done.
	Network Authentication: Open 🔻
	WEP Encryption: Disabled V



#### WPS Setup

Wi-Fi Protected Setup makes it easy for home users who know little of wireless security to establish a home network, as

well as to add new devices to an existing network without entering long passphrases or configuring complicated settings.

Enable WPS	Enabled <b>v</b>			
Add <b>Client</b> (This fea	ture is available only when WPA2 PSK, Mix	ed WPA/WPA2 P	PSK or OPEN mode is co	onfigu
Add <b>Client</b> (This fea	ture is available only when WPA2 PSK, Mix	ed WPA/WPA2 F Add Enrollee	PSK or OPEN mode is co	onfigu
Add <b>Client</b> (This fea	ture is available only when WPA2 PSK, Mix Enter STA PIN  Use AP PIN Help	ed WPA/WPA2 F Add Enrollee	PSK or OPEN mode is co	onfigu

Enable WPS: This is WPS ON/OFF turn. Click it to enable or disable WPS. WPS is disabled by default.

Device PIN: This is PIN code of the modem router for WPS PIN mode.

Enter SAT PIN: "SAT" means the remote wireless client requiring a connection. Enter its PIN code in the blank if you

select this option, and then click Add Enrollee

Use AP PIN: "AP" means the modem router. Select this option if you copy the PIN code of the modem router to the remote wireless client.

## **A**NOTE

- WPS/RST button in the device back panel: When WPS feature is enabled, press this button on the device for 1~3 seconds and the WPS LED will keep blinking for about 2 minutes. Within the 2 minutes, press the WPS button on your wireless clients. When the WPS displays a solid light, the wireless client has joined in your wireless network.
- 2. To use the WPS security, the wireless client must be also WPS-capable.
- WPS only supports WPA2, which means only when you select "WPA2" encryption or "Open" you can change WPS status.



#### Manual Setup AP

You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Click Apply/Save when done.

Manual Setup AP	
You can set the network aut	hentication method, selecting data encryption, ev is required to authenticate to this wireless network and specify the encryption strength
Click "Apply/Save" when do	те,
Network Authentication:	Open 🔻
WEP Encryption:	Disabled <b>v</b>
	Apply/Save

• Network Authentication: Select Open, Shared, WPA-PSK, WPA2-PSK or Mixed WPA/ WPA2-PSK from the drop-down list to encrypt your wireless network.

Depending on the type of network authentication you select, you will be prompted to enter corresponding settings.

- WEP Encryption: Select Enabled or Disabled.
- Encryption Strength: Select 128-bit or 64-bit.
- **Current Network Key:** Select a network key to be active.
- Network Key 1/2/3/4: Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys; enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.
- WPA/WAPI passphrase: Enter a WPA/WAPI network key.
- WPA Group Rekey Interval: Specify a key update interval.
- WPA/WAPI Encryption: Select AES or TKIP+AES.



## 4.3.3 MAC Filter

The MAC-based Wireless Access Control feature can be used to allow or disallow clients to connect to your wireless

network.

Device Info	Wireless MAC Filter
Advanced Setup	
Wireless	Note: If 'Allow' is choosed and mac filter is empty, WPS will be disabled, and you will not be able to access the router wirelessly. Up to 32 MAC address entries
Basic	
Security	
MAC Filter	
Wireless Bridge	MAC Restrict Mode: 🖲 Disabled 🔍 Allow 🔍 Deny
Station Info	
Diagnostics	Apply/Save
Management	
	ASS Address Remove
	mac Address Remove

#### MAC Restrict Mode: Disabled, Allow and Deny

- Allow: Only allow PCs at specified MAC addresses (in the list) to connect to your wireless network.
- **Deny:** Block only PCs at specified MAC addresses from connecting to your wireless network.
- **Disable:** Disable this feature.

Add: Click it to add a MAC address.

**Remove:** To delete an existing MAC address, first check the **Remove** box next to the MAC address in list and then click this button.

**Example 1:** To allow only the PC at the MAC address of 00:1A:3D:9C:BB:23 to connect to your wireless network, do as follows:

1 Select Allow, and click Apply/Sa	ve		
MAC Restrict Mode: 💮 Disabled	Allow	Dény Dény	
			Apply/Save







3 Enter **00:1A:3D:9C:BB:23** in the MAC address box as shown in the figure below, and click Apply/Save

Device Info	Wireless MAG	C Filter	
Advanced Setup			
Wireless	Enter the MAC a	ddress and click "Apply/	Save" to add the MAC address to the wireless MAC address filters. Up to 32 MAC address entries
Basic			
Security	MAC Address:	00:1A:3D:9C:BB:23	(жажажажажа)
MAC Filter			
Wireless Bridge			Apply/Save
Station Info			

Device Info	Wireless MAC Filter
Advanced Setup	
Wireless	Note: If 'Allow' is choosed and mac filter is empty, WPS will be disabled, and you will not be able to access the router wirelessly. Up to 32 MAC address entrie
Basic	
Security	
MAC Filter	
Wireless Bridge	MAC Restrict Mode: 🔍 Disabled 🛛 🖲 Allow 🔍 Deny
Station Info	
Diagnostics	Apply/Save
Management	
	MAC Address Remove
	00:1A;3D:9C:BB:23
	MAC Address Remove 00:1A:3D:9C:BB:23

## ANOTE

If "Allow" mode is activated with no MAC address being limited, WPS feature will be disabled. Go to Wireless >

Security to check WPS status).

## 4.3.4 Wireless Bridge

This page allows you to configure wireless bridge (also known as Wireless Distribution System) features of the wireless interface.

Wireless distribution system (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them.



Device Info	Wireless Bridge	
dvanced Setup		
lireless	This page allows you to configure	wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution
Basic	System) to disable access point fu	nctionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available
Security	and wireless stations will be able t	o associate to the AP. Select Disabled in Bridge Action which disables wireless bridge. Selecting Enabled or Enabled(Scan)
MAC Filter	enables wireless bridge restriction	Only those bridges selected in Remote Bridges will be granted access.
Wireless Bridge	Click "Refresh" to update the rem	ote bridges. Wait for few seconds to update.
Station Info	Click "Apply/Save" to configure th	e wireless bridge options.
iagnostics		
lanagement	AP Mode:	Access Point
	Bridge Action:	Enabled V
	Remote Bridges MAC Address	

**AP Mode:** You can select **Wireless Bridge** (also known as Wireless Distribution System) to disable access point functionality. Selecting **Access Point** enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP.

Bridge Action: There are three options available: Enabled, Enabled (Scan) and Disabled. Disabled mode means disabling the wireless bridge function. If Enabled mode is selected, you need to enter the remote device MAC address manually. If Enabled (Scan) is selected, the system automatically scans the remote device MAC address and SSID.
Remote Bridges MAC Address: Here displays the remote device info, MAC address and SSID (if Bridge Action is Enabled Scan), or offers you field to enter the remote info, MAC address (if Bridge Action is Enabled).
Refresh: Click to refresh the Wireless Name (SSID). Wait for few seconds to refresh.

Apply/Save: Click to apply and save the settings.

#### Instance

Assume that there is a wireless router in your living room, far away from your study room. Every time you join the WiFi in the study room, it seems hard for you to watch a high-quality live streaming video. To add another wireless router in the study room is an ideal choice to solve your problem. **Wireless Bridge** function of the modem router helps you to extend your wireless coverage, speed up downloading. Then your video will run smoother and faster. Assume that the router in your living room is **Router 1**, and the other one in study room is **Router 2**.





#### Before you get started:

- (1) View and note down the security settings of Router 1: wireless name (SSID), channel, security mode, MAC address and wireless key.
- a) Click Advanced > Wireless > Basic to check the SSID, MAC address (BSSID) and Channel.

Tend	a	Home Pag
Device Info Advanced Setup	Wireless Basic	
Wireless	This page allows you to cor	nfigure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the
Basic	network from active scans,	set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.
Security	Click "Apply/Save" to config	gure the basic wireless options.
MAC Filter		
Wireless Bridge	Enable Wireless	
Station Info		
Diagnostics	Hide Access Point	
Management	Enable Wireless Mu	lticast Forwarding (WMF)
	SSID:	Tenda_112252
	BSSID:	00.90:4C:11:22:53
	Wireless Mode:	802.11b/g/n Mixed 🗸
	Country:	ALL
	Channel:	6 🗸
	Bandwidth:	40MHz ∨
	Control Sideband:	Upper 🗸
	RF Power:	
	Apply/Save	

**SSID:** Tenda\_112252

BSSID: 00:90:4C:11:22:53

#### Channel: 6

b) Click Advanced > Wireless > Security to check security mode and wireless key.





Security Mode: WPA2-PSK / AES

Wireless Key: 12345678

**2** View the LAN settings of Router 1.

Click **Advanced** > **Advanced Setup** > **LAN** to check LAN IP address and Subnet Mask, and verify that the DHCP Server is enabled.

LAN IP Address: 192.168.1.1;

Subnet Mask: 255.255.255.0



# <u>tenda</u>

Device Info	Local Area Network (LAN) Setup				
Advanced Setup	Configure the Broadband Router IP Address and Subnet Mask for LAN interf				
Layer2 Interface	GroupName Default	ne Default 🗸			
WAN Service	IP Address:	192.168.1.1			
LAN	Subnet Mask	255.255.255.0			
IPv6 Autoconfig	☑ Enable IGMP Snooping				
NAT	C Disable DHCP Se	rver			
Security	Enable DHCP Server				
Parental Control	Start IP Address:	192.168.1.2			
Bandwidth Control	End IP Address:	192 168 1 254			
Routing	Lessed Time tho	24			
DNS	DNC Contrary Action				
DSI	Divis Servers Assign	ed by DHCP server.			

#### After you prepare two steps above, do as follows:

#### **Configure Router 2:**

- 1 Set the LAN IP address of Router 2 to a different IP address yet on the same segment as Router 1.
  - Click Advanced > Advanced Setup > LAN to change the LAN IP address into 192.168.1.10.
  - Disable your DHCP server.

Device Info	Local Area Network (LAN) Setup Configure the Broadband Router IP Address and Subnet Mask for LAN interface. GroupName Default V		
Layer2 Interface			
WAN Service	1P Address: 192.168.1.10		
LAN	Subnet Mask:	255.255.255.0	
IPv6 Autoconfig	Enable IGMP Snooping		
NAT	Disable DHCP Server		
Security	O Enable DHCP Se	rver	
Parental Control	Start IP Address	: 192.168.1.11	

- Click Advanced > Wireless > Basic to check the SSID and Channel. They should be the same as Router 1's. If not, correct them manually. Click Apply/Save to save your settings.
- Click Advanced > Wireless > Security to check the security mode and wireless key. Verify that they are the same as Router 1's. If not, correct them manually. Click Apply/Save to save your settings.
- (4) Click **Advanced > Wireless > Wireless Bridge** to configure wireless bridge.
  - Access Point (Recommended):

Two ways to bridge Router 1 by using Access Point:

a. If you select Enable in Bridge Action field.



- Enter the MAC address of Router 1 which you have noted down (00:90:4C:11:22:53).
- Then click **Apply/Save** to save the settings.

evice Info	Wireless Bridge		
dvanced Setup			
/ireless	This page allows you to configure	wireless bridge features of the wireless LAN interface. You can select Wireless Bridge	also known as Wireless :
Basic	Distribution System) to disable ac	cess point functionality. Selecting Access Point enables access point functionality. Wi	reless bridge functionality
Security	will still be available and wireless a	tations will be able to associate to the AP. Select Disabled in Bridge Action which dis	ables wireless bridge.
MAC Filter	Selecting Enabled or Enabled(Scar	n) enables wireless bridge restriction. Only those bridges selected in Remote Bridges	will be granted access.
Wireless Bridge	Click "Refresh" to update the rem	ote bridges. Wait for few seconds to update.	
Station Info	Click "Apply/Save" to configure th	e wireless bridge options.	
lagnostics.			
anagement	AP Mode:	Access Point	
	Bridge Action:	Enabled V	
	Remote Bridges MAC Address:	00:90:4C:11:22:53	

b. If you select Enable(Scan) in Bridge Action field.

- Select the SSID of Router 1 (Tenda\_112252) in Remote Bridges MAC Address field.
- If you cannot find the SSID on the list, click **Refresh** to refresh the list.
- Then click **Apply/Save** to save your settings.

10 IU	G							iume.	- 49
Device Info	Wireless Bridge								
Advanced Setup									
Wireless	This page allows you to configure	wirele	ss bridge features of the wireles	s LAN interface. You can select W	ireless Brid	dge (also known a	s Wireless Distributi	ion System) to disable access point	
Basic	functionality. Selecting Access Point	nt enal	bles access point functionality. V	Wireless bridge functionality will s	till be avai	lable and wireless	stations will be able	e to associate to the AP. Select	
Security	Disabled in Bridge Action which di	sables	wireless bridge. Selecting Enab	led or Enabled(Scan) enables wire	less bridg	e restriction. Only	those bridges select	ted in Remote Bridges will be	
MAC Filter	granted access.								
Wireless Bridge	Click "Refresh" to update the remo	te bri	dges. Wait for few seconds to up	pdate.					
Station Info	Click "Apply/Save" to configure the	wirel	ess bridge options.						
Diagnostics		_							
Management	AP Mode:	Act	cess Point 🗸						
	Bridge Action:	Eni	abled(Scan) 🗸						
	Remote Bridges MAC Address:		SSID	BSSID	channel	security	RSSI(dBm)		
			bx_zhouweixin	C8:3A:35:03:2E:F0	13	WPA/AES	-50		
			GT_office	C8:3A:35:49:C7:31	13	wep	-58		
			Tenda_C8DABB	C8:3A:35:C8:DA:BB	13	wep	-46		
			Tenda_112252	00:90:4C:11:22:53	6	WPA2/AES	-28		
			<>,./?\\\[[{]~~`;;*	C8:3A:35:03:2E:F1	13	wep	-41		
			SY-CW1000-test	00:B0:C6:4E:9C:B0	13	wep	-45	-	
			BX_LZM_Visitor	C8:3A:35:52:85:1B	13	wep	-39		
			BX_LZM_TEST	C8:3A:35:52:85:19	13	WPA/AES	-39		

#### > Wireless Bridge

Two ways to bridge Router 1 by using Wireless Bridge:

a. If you select Enable in Bridge Action field.

- Enter the MAC address of Router 1 which you have noted down (00:90:4C:11:22:53).
- Then click **Apply/Save** to save the settings.



ine	wireless Bridge	
ed Setup		
s	This page allows you to configure	wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless
	Distribution System) to disable acc	ess point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality
ity	will still be available and wireless s	tations will be able to associate to the AP. Select Disabled in Bridge Action which disables wireless bridge.
Filter	Selecting Enabled or Enabled(Scan	) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
ess Bridge	Click "Refresh" to update the remo	ite bridges. Wait for few seconds to update.
on Info	Click "Apply/Save" to configure the	e wireless bridge options.
stics		
ement	AP Mode:	Wireless Bridge 🗸
	Bridge Action:	Enabled
	Remote Bridges MAC Address:	00:90:4C:11:22:53
ement	AP Mode: Bridge Action: Remote Bridges MAC Address:	Wireless Bridge  Enabled U0:90:4C:11:22:53

b. If you select Enable(Scan) in Bridge Action field:

- Select the SSID of Router 1 (Tenda\_112252) in Remote Bridges MAC Address field. If you cannot find the SSID on the list, click Refresh to refresh the list.
- Then click **Apply/Save** to save your settings.

Tenda	a –						
Device Info	Wireless Bridge						
Advanced Setup							
Wireless	This page allows you to configure	wireless bridge features of the w	ireless LAN interface. You can select Wi	ireless Bri	dge (also known a	Wireless Distribution System) to disab	le access point
Basic	functionality. Selecting Access Point	nt enables access point functiona	ality. Wireless bridge functionality will st	till be avai	lable and wireless	stations will be able to associate to the	AP, Select
Security	Disabled in Bridge Action which di	sables wireless bridge. Selecting	Enabled or Enabled(Scan) enables wire	less bridg	e restriction. Only	those bridges selected in Remote Bridg	jes will be
MAC Filter	granted access.						
Wireless Bridge	Click "Refresh" to update the remo	ote bridges. Wait for few seconds	to update.				
Station Info	Click "Apply/Save" to configure th	e wireless bridge options.					
Diagnostics		-					
Management	AP Mode:	Wireless Bridge 🛩					
	Bridge Action:	Enabled(Scan) 🗸					
	Remote Bridges MAC Address:	SSID	BSSID	channel	security	RSSI(dBm)	
		bx_zhouweixin	C8:3A:35:03:2E:F0	13	WPA/AES	-50	
		GT_office	C8:3A:35:49:C7:31	13	wep	-58	
		Tenda_C8DABB	C8:3A:35:C8:DA:BB	13	wep	-46	
		Tenda_112252	00:90:4C:11:22:53	6	WPA2/AES	-28	
		<>,./?\\\[[{]~`;;'	C8:3A:35:03:2E:F1	13	wep	-41	
		SY-CW1000-test	00:B0:C6:4E:9C:B0	13	wep	-45	
		BX_LZM_Visitor	C8:3A:35:52:85:1B	13	wep	-39	
		BX_LZM_TEST	C8:3A:35:52:85:19	13	WPA/AES	-39	

After you fininsh the settings on Router 2 above, do as follows:

#### **Configure Router 1:**

- 1 Click Advanced > Wireless > Wireless Bridge.
- 2 Select Access Point in AP Mode field. (If you select Wireless Bridge here, the wireless devices will not be

able to connect Router 1 wirelessly.)

- If **AP Mode** of Router 2 is **Access Point**, there are two ways to bridge Router 2.
- a. If you select Enable in Bridge Action field:
  - Enter the MAC address of Router 2 which you can check on **Wireless** > **Basic** interface, say **BSSID** (02:10:18:01:00:02).



• Then click **Apply/Save** to save the settings.

Tena	а	Home Pag
Device Info	Wireless Bridge	
Advanced Setup		
Wireless	This page allows you to configure	wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless
Basic	Distribution System) to disable ac	cess point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality
Security	will still be available and wireless	stations will be able to associate to the AP. Select Disabled in Bridge Action which disables wireless bridge,
MAC Filter	Selecting Enabled or Enabled(Scar	1) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access.
Wireless Bridge	Click "Refresh" to update the rem	ote bridges. Wait for few seconds to update.
Station Info	Click "Apply/Save" to configure th	e wireless bridge options.
Diagnostics		
Management	AP Mode:	Access Point
	Bridge Action:	Enabled V
	Remote Bridges MAC Address:	02:10:18:01:00:02
		Refrech Anniv/Save
		Transaction ( ) Mile Annual

b. If you select Enable(Scan) in Bridge Action field:

- Select the SSID of Router 2 (Tenda\_112252) in Remote Bridges MAC Address field.
- If you cannot find the SSID on the list, click **Refresh** to refresh the list.
- Then click **Apply/Save** to save your settings.

Tend	<b>a</b>								Home Ragi
Device Info	Wireless Bridge								
Advanced Setup									
Wireless	This page allows you to configure	wirele	ss bridge features of the wireless l	AN interface. You can select W	ireless Brid	ige (also known a	s Wireless Distributio	ion System) to disable access p	oint
Basic	functionality. Selecting Access Point	nt enal	bles access point functionality. Wi	reless bridge functionality will st	till be avai	lable and wireless	stations will be able	e to associate to the AP. Select	
Security	Disabled in Bridge Action which di	sables	wireless bridge. Selecting Enabled	d or Enabled(Scan) enables wire	less bridg	e restriction. Only	those bridges select	ted in Remote Bridges will be	
MAC Filter	granted access.								
Wireless Bridge	Click "Refresh" to update the remo	ote bri	dges. Wait for few seconds to upd	ate.					
Station Info	Click "Apply/Save" to configure th	e wirel	ess bridge options.						
Diagnostics		-							
Management	AP Mode:	Ac	cess Point						
	Bridge Action:	En	abled(Scan) 🗸						
	Remote Bridges MAC Address:		SSID	BSSID	channel	security	RSSI(dBm)		
			bx_zhouweixin	C8:3A:35:03:2E:F0	13	WPA/AES	-50		
			GT_office	C8:3A:35:49:C7:31	13	wep	-58		
			Tenda_C8DABB	C8:3A:35:C8:DA:BB	13	wep	-46		
			Tenda_112252	02:10:18:01:00:02	6	WPA2/AES	-28		
			<>,/?\\\[]{}~~;;*	C8:3A:35:03:2E:F1	13	wep	-41		
			SY-CW1000-test	00:80:C6:4E:9C:80	13	wep	-45		
			BX_LZM_Visitor	C8:3A:35:52:85:1B	13	wep	-39		
			BX_LZM_TEST	C8:3A:35:52:85:19	13	WPA/AES	-39		

The configuration is finished. Then the devices can connect Router 2 wirelessly or via Ethernet cables.

If AP Mode of Router 2 is Wireless Bridge, you can only select Enable and enter the MAC address (02:10:18:01:00:02)

to bridge Router 2.



Device Info	Wireless Bridge		
Advanced Setup			
Wireless	This page allows you to configure	wireless bridge features of the wireless LAN interface. You can	select Wireless Bridge (also known as Wireless
Basic	Distribution System) to disable acc	ess point functionality. Selecting Access Point enables access p	oint functionality. Wireless bridge functionality
Security	will still be available and wireless s	ations will be able to associate to the AP. Select Disabled in Br	idge Action which disables wireless bridge.
MAC Filter	Selecting Enabled or Enabled(Scan	enables wireless bridge restriction. Only those bridges selecte	d in Remote Bridges will be granted access.
Wireless Bridge	Click "Refresh" to update the remo	te bridges. Wait for few seconds to update.	
Station Info	Click "Apply/Save" to configure th	wireless bridge options.	
Diagnostics			
Aanagement	AP Mode:	Wireless Bridge 🗸	
	Bridge Action:	Enabled V	
	Remote Bridges MAC Address:	02:10:18:01:00:02	

The configuration is finished. Then the devices can only connect Router 2 via Ethernet cables.

## ANOTE

The WDS feature (also known as Wireless Bridge) can only be implemented between 2 WDS-capable wireless devices.

Plus, SSID, channel, security settings and security key must be exactly the same on both such devices.

## 4.3.5 Station Info

This page shows authenticated wireless stations and their status.

Device Info	Wireless Authenticated Stations	
Advanced Setup Nireless	This page shows authenticated wireless stations and their status.	
Basic Security	MAC Associated Authorized SSID Interface	
MAC Filter Wireless Bridge		Refresh
Station Info		

## **4.4 Diagnostics**

this part includes the following information:

- Diagnostics
- Ping test



#### **4.4.1 Diagnostics**

The device is capable of testing the connection to your DSL service provider, the connection to your Internet service provider and the connection to your local network. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

evice Info dvanced Setup /ireless	ipoe_eth0 Diagnostics The individual tests are listed bel Test the connection to your loc	ow. If a s	test displa ork	ys a fail s	atus, click "H	Ielp" and fo	llow the trou	ubleshooting proce	
lagnostics	Test your eth2 Connection:	FAIL	Help						
Diagnostics	Test your eth3 Connection:	FAIL	Help						
Ping test anagement	Test your eth1 Connection:	PASS	Help						
	Test your Wireless Connection:	PASS	Help						
	Test the connection to your Internet service provider								
	Ping default gateway:		PASS	Help					
	Ping primary Domain Name Se	erver:	PASS	Help					
	Ping default gateway: Ping primary Domain Name Se	erver:	PASS PASS	Help Help					

Pass: Indicates that the Ethernet interface from your computer is connected to the LAN port of the device.

Fail: Indicates that the device does not detect the Ethernet interface on your computer.

#### 4.4.2 Ping test

Ping utility can help test whether the device has built a proper connection with your host.

Type in the IP address of your host in the Ping IP Address field, and click **Ping**. If you get a similar screen shown as

below, it indicates the connection between the Ping object (Here is 192.168.1.2) and the device has been established.

Device Info	System Tools Ping tool	
Advanced Setup	Ping IP Address:	Ping
Wireless	PING 192,168,1,2 (192,168,1,2	): 56 data bytes
Diagnostics	64 bytes from 192,168,1.2; sec	=0 ttl=64 time=1.992 ms
Diagnostics	64 bytes from 192,168,1.2; sec	q=1 ttl=64 time=1.870 ms
Ping test	64 bytes from 192,168,1,2; sec	q=2 ttl=64 time=0.885 ms
Management	64 bytes from 192.168.1.2: sec	q=3 ttl=64 time=1,092 ms
	192.168.1.2 ping statistics	
	4 packets transmitted, 4 packet	ets received, 0% packet loss
	round-trip min/avg/max = 0.8	85/1.459/1.992 ms



## 4.5 Management

This section explains the following information:

- Settings
- System Logs
- SNMP Agent
- TR-069 Client
- Internet Time
- Access Control
- Update Software
- Reboot

## 4.5.1 Settings

This section explains the following information:

- Backup
- Restore Backup
- Restore Default

### Backup

Here you can save a copy of your device's configurations to your computer. Once you have configured the device, you can save these settings to a configuration file on your local hard drive. The configuration file can later be imported to





### **Restore Backup**

Here you can restore the configurations of the modem router from a file saved on your PC.

Device Info	Tools Update Settings	
Advanced Setup		
Wireless	Update Broadband Router settings. You may update your router settings	using your saved files.
Diagnostics		
	the second se	
Management	Settings File Name: Choose file No file chosen	
Management Settings	Settings File Name: Choose file No file chosen	Update Settings
Management Settings Backup	Settings File Name: Choose file No file chosen	Update Settings
Management Settings Backup Restore Backup	Settings File Name: Choose file No file chosen	Update Settings

### **Restore Default**

Under some circumstances (for example, join a different network or unfortunately forgetting the login password), you

may need to remove the existing configuration and restore the factory default settings.



## 4.5.2 System Logs

The System Log dialog allows you to view the system log and configure the system log options.

lend	
Device Info	System Log
Advanced Setup	
Wireless	The System Log dialog allows you to view the System Log and configure the System Log options.
Diagnostics	
Management	Click "View System Log" to view the System Log.
Settings	
System Log	Click "Configure System Log" to configure the System Log options.
SNMP Agent	
TR-069 Client	
Internet Time	View System Log Configure System Log



To configure the system log, click Configure System Log.



- Log: If Enable is selected, the system will begin to log all the selected events.
- Log Level: Set the log level. All events above or equal to the selected level will be logged.
- **Display Level:** Set the log display level. All logged events above or equal to the selected level will be displayed.
- **Apply/Save:** click to apply and save the system log settings.

To view the system log, firstly ensure log is enabled, otherwise you cannot read any log.

System Log				
Date/Time	Facility	Severity	Message	
Jan 1 01:41:27		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:42:06		crit	kernel: eth1 Link DOWN.	
Jan 1 01:42:10		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:42:34		crit	kernel: eth1 Link DOWN.	
Jan 1 01:42:36		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:44:10		crit	kernel: eth1 Link DOWN.	
Jan 1 01:44:12		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:44:13		crit	kernel: eth1 Link DOWN.	
Jan 1 01:44:16		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:44:58		crit	kernel: eth1 Link DOWN.	
Jan 1 01:45:00		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:46:19		crit	kernel: eth1 Link DOWN.	
Jan 1 01:46:21		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:48:10		crit	kernel: eth1 Link DOWN.	
Jan 1 01:48:12		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:48:15		crit	kernel: eth1 Link DOWN.	
Jan 1 01:48:17		crit	kernel: eth1 Link UP 100 mbps full duple	
Jan 1 01:48:48		crit	kernel: eth1 Link DOWN.	
Jan 1 01:48:50		crit	kernel: eth1 Link UP 100 mbps full duple	

## 4.5.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from

the SNMP agent in this device.



Tend	a		
Device Info	SNMP - Configurati	on	
Advanced Setup			
Wireless	Simple Network Man	agement Protocol (SN	MP) allows a management application to retrieve statistics and status from the SNMP agent in this device
Diagnostics			
Management	Select the desired va	lues and click "Apply/S	ave" to configure the SNMP options.
Settings			
System Log	SNMP Agent 🖲 Dis	able 🄍 Enable	
SNMP Agent			
TR-069 Client	Read Community:	public	
Internet Time	Set Community:	private	
Access Control	System Name:	Tenda	
Update Firmware	System Location:	unknown	
Reboot	System Edition.	unknown	
	System Contact:	unknown	
	Trap Manager IP:	0.0.0.0	
			Apply/Save

- SNMP Agent: Select "Enable" to activate the SNMP Agent feature or "Disable" to deactivate it.
- **Read Community:** Specify a Read Community string. The default is public.
- Set Community: Specify a Set Community string. The default is private.
- System Name: Specify a descriptive system name.
- System Location: Specify a system location.
- System Contact: Specify a system contact.
- Trap Manager IP: Specify the IP address of the Trap Manager.

## 4.5.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration,

provision, collection, and diagnostics to this device.

Click the <b>TR-069 Client</b> tab to enter the TR-06	9 Client configuration screen as seen b	elow:
---	---	-------

Tend	а	
Device Info	TR-069 client - Configuration	
Advanced Setup		
Wireless	WAN Management Protocol (TR-069) all	lows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device
Diagnostics		
Management	Select the desired values and click "Appl	ly/Save" to configure the TR-069 client options.
Settings		
System Log	Inform	● Disable ○ Enable
SNMP Agent		
TR-069 Client	Inform Interval:	300
Internet Time	ACS URL:	
Access Control	ACS User Name:	admin
Update Firmware	ACS Password:	*****
Reboot	WAN Interface used by TR-069 client:	Any_WAN V
	Display SOAP messages on serial consol	le 🖲 Disable 🔾 Enable
	Connection Request Authentication	
	Connection Request User Name:	admin
	Connection Request Password:	
	Connection Request URL:	http://192.168.20.101.30005/



- Inform: Select Enable/Disable to enable/disable the TR-069 Client function. By default, it is disabled.
- **Inform Interval:** Specify the inform interval.
- ACS URL: Enter the ACS (Auto-Configuration Server) URL address.
- ACS User Name: Enter the ACS (Auto-Configuration Server) user name.
- ACS Password: Enter the ACS (Auto-Configuration Server) password.
- WAN Interface used by TR-069 client: Select the WAN interface used by the TR-069 client from the drop-down list.
- **Display SOAP messages on serial console:** If Enable is selected, SOAP messages will be displayed on serial console; if Disable is selected, SOAP messages will not be displayed on serial console.
- Connection Request Authentication: Check/uncheck to enable/disable the connection request authentication.
- Connection Request User Name: Enter the connection request user name.
- Connection Request Password: Enter the connection request password.
- Connection Request URL: Specify the connection request URL.

## 4.5.5 Internet Time

This page is used to set the router's system time. If **Automatically synchronize with Internet time servers** is checked, the system will automatically connect to NTP server to synchronize the time.

Device Info	Time settings			
Advanced Setup				
Wireless	This page allows you to th	re modem's time confi	guration.	
Diagnostics				
Management	Automatically synchron	nize with Internet time	servers	
Settings				
System Log	First NTP time server:	time.nist.gov	~	
SNMP Agent	Second NTP time server:	ntp1.tummy.com	Y	
TR-069 Client	Third NTP time server:	None	~	
Internet Time	Fourth NTP time server:	None	~	
Access Control	Fifth NTP time server.	None	V	
Update Firmware				
Reboot	Time zone offset:	(GMT+08:00) Beijing, (	Chonaging, Hong Kong, Urumai	

**First/Second/Third/Fourth/Fifth NTP time server:** Select a NTP time server from the drop-down list. If the NTP time server you are looking for is not included in the list, select "Other" and then enter it manually in the box.

Time zone offset: Select your time zone from the drop-down list.



## 4.5.6 Access Control

This section explains the following information:

- Password
- AccessControl Service

#### Password

Access to your broadband router is controlled through two user accounts: admin and support.

Admin has unrestricted access to change and view configuration of your Broadband Router.

Support is used to allow a professional technician to access your Broadband Router for maintenance and to run

diagnostics.

Device Info	Access Control Passwords
Advanced Setup	
Wireless	Access to your broadband router is controlled through two user accounts; admin and support.
Diagnostics	
Management	The user name "admin" has unrestricted access to change and view configuration of your Broadband Router.
Settings	
System Log	The user name "support" is used to allow an ISP technician to access your Broadband Router for maintenance and to run diagno
SNMP Agent	
TR-069 Client	Use the fields below to enter up to 16 characters and click "Apply/Save" to change or create passwords.
Internet Time	Note: User Name and Password can only include letters, numbers or underscore.
Access Control	User Name:
Passwords	Old Password:
AccessCtrl	New Password:
Update Firmware	Confirm Password:
Dehast	

User Name: Enter the user name of up to 16 characters. The default is "admin".

Old Password: Enter the old password of up to 16 characters. The default is "admin".

New Password: Enter a new password of up to 16 characters.

Confirm Password: Re-enter to confirm the new password.

Apply/Save: Click to change or create passwords.

## **A**NOTE

Password cannot contain a space.

# Tenda

### **Access Control - Service**

Here you can manage the device either from LAN or WAN side using HTTP, ICMP, TELNET, SNMP, FTP, TFTP and

HTTPS.

Device Info	Access Control	Services			
Advanced Setup	A Sarvice Contro	l List ("SCL") enabl	es or disables servic	es from being	; used.
Wireless	Note: When ena	bling WAN Access	Control with HTTP,	HTTPS, TETP, 1	TELNET or SNMP service, you can use the default port numb
Diagnostics	when the defaul	t one can't work(ft	p is used by 'Update	e Firmware' pa	age for upgrading, so it does not need port change).
Management	Services	LAN	WAN	PORT	and the second second second second
Settings	HTTP	🕑 Enable	Enable	80	
System Log	101.05		E		-
SNMP Agent	ICMP	M Enable	E Enable		-
TR-069 Client	TELNET	🗹 Enable	🗌 Enable	23	
Internet Time	SNMP	🗹 Enable	Enable	161	-
Passwords	FTP	🗹 Enable	🗌 Enable		-
AccessCtrl	TETP	🗹 Enable	🗆 Enable	69	-
Update Firmware Reboot	HTTPS	🗹 Enable	🗌 Enable	443	-

## ANOTE

If you are not an advanced user, it is recommended to keep the default settings.

# 4.5.7 Update Software

Firmware upgrade is released periodically to improve the functionality of your device and add any new features. If you

run into a problem with a specific feature of the device you could log in to our website (<u>www.tendacn.com</u>) to download

the latest firmware to update your device.



Device Info	Step 1: Obtain an updated software image file from your ISP.					
Advanced Setup						
Wireless	Step 2: Click the "Browse" button	Step 2: Click the "Browse" button to locate the image file.				
Diagnostics						
Management	Step 3: Click the "Update Softwar	e" button once to uploa	d the new image file.			
Settings						
System Log	NOTE: The update process takes a	bout 2 minutes to com	plete, and your Broadband Router will reboot.			
SNMP Agent						
TR-069 Client	Software File Name:	Browse	Current Version: V50.1.3051.3_en_td			
Internet Time			Update Software			
Access Control	FTP Firmware Update					
Update Firmware						
Reboot	FTP Server IP:	[eg:192.16	8.1.1)			
	Port:	[1-65535]				
	User Name:	[1-32]				
	Password:	(1-32)				
	Software File Name:	[1-127]				
			FTP Update Software			
	TFTP Firmware Update					
	TFTP Server IP;	[eg:192.16	8.1.1]			
	Software File Name:	[1-127]				

This modem router supports three types to update firmware.

## **Type 1: General Update**

#### To update software, do as follows:

1 Obtain an updated software image file from our website: <u>www.tendacn.com</u>.





2 Click the "Browse" button to locate the firmware file.

Software F	ile Name:		Browse	Current Version: V50.1	.3051.3_en_td
					Update Software
3 C	lick	late Software to start	updating.		

## **Type 2: Updating Via FTP Server**

Updating via FTP server is supported. Make sure there is an available FTP server.

	FTP Firmware Update				
	FTP Server IP:	[eg:192.168	1.1]		
	Port:	[1-65535]			
	User Name:	[1-32]			
	Password:	[1-32]			
	Software File Name:	[1-127]			
				FTP Update Softwa	are
1	Type the FTP Server IP address, like the right	nt figure	Example		
2	Type the port the FTP server used.		FTP Server IP:	192.168.1.2	[eg:192.168.1.1]
	Type the user name and password to access t	he FTD	Port:	21	[1-65535]
0	Type the user name and password to access t		User Name:	XXX	[1-32]
server.			Password:	XXX	[1-32]
4	Copy the name of the firmware.		Software File Name:	US_D305V1br_V50.1.30	[1-127]
5	Click FTP Update Software to start updatin	ıg.	I		FTP Update Software

## **Type 3: Updating Via TFTP Server**

Updating via TFTP server is supported. Make sure there is an available TFTP server.

TFTP	Firmware	Update
------	----------	--------

TFTP Server IP:	[eg:192.168.1.1]
Software File Name:	[1-127]

TFTP Update Software

1	Type the TFTP Server IP address in the field.	Example		
2	Copy the name of the firmware.	TFTP Server IP: Software File Name:	192.168.1.2 US_D305V1br_V50.1.3	[eg:192.168.1.1] 0 [1-127]
3	Click TFTP Update Software to start updating.			
			T	TP Update Software



## ANOTE

The update process will cost 2 minutes, and the device will reboot.

## 4.5.8 Reboot

Click the **Reboot** button to reboot the router.





# **Appendix 1 Applications**

## **Application 1: How to change SSID and wireless password?**

- (1) Go to **Wireless** > **Basic** interface.
- 2 Specify a SSID as you like, like **Tenda\_myhome**.
- 3 Click **Apply/Save** to save the settings.

Device Info Advanced Setup	Wireless Basic					
Wireless	This page allows you to c	This page allows you to configure basic features of the wireless LAN interface. You can enable o				
Basic	name (also known as SSIE	name (also known as SSID) and restrict the channel set based on country requirements.				
Security	Click "Apply/Save" to con	figure the basic wireless options.				
MAC Filter						
Wireless Bridge	Enable Wireless					
Station Info	Dutter					
Diagnostics	Hide Access Point					
Management	Enable Wireless M	ulticast Forwarding (WMF)				
	2 SSID:	Tenda_myhome				
	BSSID:	C8:3A:35:5C:06:51				
	Wireless Mode:	802.11b/g/n Mixed 🔻				
	Country:	ALL				
	Channel:	Auto				
	Bandwidth:	40MHz <b>v</b>				
	Control Sideband:	Lower •				
	DE Devices	(i) Manual (ii) Falsana				

- 4 Go to **Wireless** > **Security** interface.
- 5 Choose a network authentication (WPA2-PSK is recommended) and set a passphrase.
- 6 Click **Apply/Save** to save the settings.

Wireless	WPS Setup		
MAC Filter	Enable WPS	Disabled V	
Wireless Bridge			
Station Info			
Diagnostics			
Management	Manual Setup AP		
	War and a start a second start	conficialization and a structure of	las anna das
	You can set the network auth	entication method, selecting o	ata encryption,
	specify whether a network ke	y is required to authenticate to	o this wireless network and specify the encryption strength
	Click "Apply/Save" when done	ð,	
6	Network Authentication:	WPA2 -PSK	
	WPA/WAPI passphrase:		<u>Click here to display</u>
	WPA Group Rekey Interval:	0	
	WPA/WAPI Encryption:	AES V	
	WEP Encryption:	Disabled V	
	6	Apply/Save	



# **Application 2: How to reset the modem router?**

The device supports two methods to reset to factory defaults. Note that after you reset the device, you should reconfigure

it for Internet service.

### Method 1: WPS/RST button

Press the WPS/RST button on the back of the modem router for about 8 seconds to reset it to factory defaults.



### Method 2: Restore Default Settings from User Interface

(1) Go to **Management > Settings > Restore Default** to enter the interface below.





# **Appendix 2 Configure Your PC**

This part is just for your references when your computer connecting to the modem router cannot get an IP address.

Screens to configure TCP/IP properties in other Operating Systems are similar to those below.

## Windows 8

**1.** Right click the icon is or is on the bottom right corner of your desktop.



2. Click Open Network and Sharing Center.

Trouble	esho	ot pr	obler	ns	
Open N	letwo	ork a	nd Sł	naring C	enter
		97	$\langle \rangle$	ENV	7/20/2015

**3.** Click **Ethernet > Properties**.





4. Find and double click Internet Protocol Version

#### 4(TCP/IPv4).

ļ	Ethernet Properties	×							
N	Networking								
	Connect using:								
	Intel(R) 82574L Gigabit Network Connection								
	Configure								
	This connection uses the following items:								
	<ul> <li>✓ ■ File and Printer Sharing for Microsoft Networks</li> <li>▲ Microsoft Network Adapter Multiplexor Protocol</li> <li>✓ Microsoft LLDP Protocol Driver</li> <li>✓ ▲ Link-Layer Topology Discovery Mapper I/O Driver</li> <li>✓ ▲ Link-Layer Topology Discovery Responder</li> <li>✓ ▲ Intermet Protocol Version 6 (TCP/IPv6)</li> </ul>								
	< >>								
	Install Uninstall Properties								
	Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.								
	OK Cancel								

 Select Obtain an IP address automatically and Obtain DNS server address automatically and click OK.

Internet Protocol Version	4 (TCP/IPv4) Properties					
General Alternate Configuration						
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.						
Obtain an IP address automatica	lly					
Use the following IP address:						
IP address:						
Subnet mask:	· · · · · · ·					
Default gateway:						
Obtain DNS server address autor	matically					
O Use the following DNS server add	dresses:					
Preferred DNS server:						
Alternate DNS server:						
Validate settings upon exit	Advanced					
	OK Cancel					

6. Click OK on the Ethernet Properties window (see Step 4 for the screenshot).



# Windows 7

- 1. Click the icon 🔯 on the bottom right corner of your desktop.
- 2. Click Open Network and Sharing Center.



3. Click Local Area Connection > Properties.

ontrol Panel Home	Local Area Connection Status	_	set up connections
nange adapter setti	General		See full ma
hange advanced sh ttings	Connection IPv4 Connectivity:	No Internet access	Internet
	IPv6 Connectivity: Media State:	No Internet access Enabled	Connect or disconne
	Duration:	03:40:31	No Internet accord
	Speed:	1.0 Gbps	ections:
	Activity	-	
	Sent —	Received	or very connection; or set up a
	Bytes: 758,61	8 8,236,680	-up, or VPN network connection.
	Properties Disable	Diagnose	

Find and double click Internet Protocol Version 4(TCP/IPv4).

	1000 MT Network Conn	ection
<b>T</b>	the full stars in the second	Configure
Inis connection use	s the following items:	
Ulient for M	Icrosoft Networks	
File and Pri	nter Sharing for Microsof	t Networks
Internet Pro	tocol Version 6 (TCP/IP	v6)
🗹 🗻 Internet Pro	otocol Version 4 (TCP/IP	v4)
🗹 🔺 Link-Layer	Topology Discovery Mar	oper I/O Driver
Link-Layer	Topology Discovery Res	ponder
Install	Uninstall	Properties
Description		
-	tral Protocol /Internet Pro	ntocol. The default
Transmission Con	and internet inc	report. The deridat



 Select Obtain an IP address automatically and Obtain DNS server address automatically and click OK.

eneral	Alternate Configuration				
You car this cap for the	n get IP settings assigned aut bability. Otherwise, you need appropriate IP settings.	comatically if to ask your r	your n netwoi	etwork su rk adminis	pports trator
0	btain an IP address automatic	ally			
) U:	se the following IP address:				
IP a	dress:	4.0	÷.		
Subr	net mask:	-			
Defa	ult gateway:	10	-1		
0	btain DNS server address aut	omatically			
O Us	se the following DNS server a	ddresses:			
Pref	erred DNS server:	÷	i.		
Alter	nate DNS server:		4	<i>1</i>	
	alidate settings upon exit			Advan	iced

6. Click OK on the Local Area Connection Properties window (see Step 4 for the screenshot).



# MAC

1. Click on the Apple icon from the top-left corner and select System

Preferences.

2. Click Network.

	<b>Finder</b>	File	Edit	View
	About This M	Лас		
	Software Up	date.		
	Mac OS X So	ftwar	e	
Ì	System Pre	feren	ces	
1	Dock			•
	Location			•
	Recent Item	s		•
	Force Quit F	inder	27	CH



- 3. Click on Ethernet.
- 4. Select Using DHCP.
- 5. Click Apply.





# **Appendix 3 Join Your Wireless Network**

# Windows 8

1. Click the icon in on the bottom right corner of your desktop.

# P• ∰ ♠ ⊗ M 16:59 2015/7/7

#### TIP:

on your PC.

If you cannot find the icon in please move your mouse to the top right corner of your desktop, select Settings > Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings, right click Wi-Fi and select Connect/Disconnect.
 If you cannot find your wireless network from the list, ensure the Airplane Mode is not enabled

**2.** Select your wireless network from the list, click **Connect** and then follow onscreen instructions.



**3.** When your wireless network is connected successfully, the following screen will appear.

Networks		
Wi-Fi 2		
Tenda_home	Connected	.atl



# Windows 7

- 1. Click the icon **on** the bottom right corner of your desktop.
- **2.** Double click your SSID (wireless network name) and then follow onscreen instructions.



**3.** When your SSID (wireless network name) displays **Connected** as shown below, you've connected to it for Internet access successfully.





# MAC

1. Click > System Preferences.

Finder File Edit View
 About This Mac
 Software Update...
 Mac OS X Software...
 System Preferences...
 Dock
 Location

2. Select Network from Internet & Network.



- 3. Click WiFi.
- 4. Turn WiFi on.
- 5. Click No network selected.
- **6.** Select the wireless network name of your router.



7. Enter the wireless password and click Join.





@ 46%.##

# iPhone/iPad

1. Scroll screen to find the **Settings** icon and click it.



- 2. Click WiFi, and turn on WiFi.
- **3.** Find the name of the wireless network you wish to connect, and click it.

Settings	Wi-Fi	
Airplane Mode OFF  Wir FP Discurrence Left Bluetooth Off C Do Not Disturb OFF  Notifications	Wi-Fi Choose a Network Tenda_home Tenda_XXXXXX	47 0 47 0
General Sounds Brightness & Wallpaper Picture Frame		
Privacy Coud Mail, Contacts, Calendars Notes Reminders	Other Ask to Join Networks Known networks will be joined au known networks are available, y	Somatically, if na

4. Enter the wireless password and click Join.



#### Connected successfully!




## **Appendix 4 FAQs**

#### 1. What information should I have to access the Internet via the DSL uplink?

If you have DSL broadband service, you might need the following information to set up your modem router.

- Active Internet service provided by a DSL account
- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address

Depending on how your ISP set up your Internet account, you could need to know the Virtual path identifier (VPI) and virtual channel identifier (VCI) parameters for a manual setup.

#### 2. I cannot access the device's User Interface (UI). What should I do?

1) Verify the physical connection (namely, the Ethernet cable) between your PC and the modem router. For details, see

## Chapter 2 Hardware Installation hereof.

2) Double check the TCP/IP settings on your PC. For details, see <u>Appendix 2 Configure Your PC</u> hereof.

3) Press the **WPS/RST** button on the device for about 8 seconds and then re-access the UI with the default login info "admin".

- 4) Change the Ethernet cable that connects your PC and the device.
- 5) Try accessing device management interface from other PCs, smart phones or iPads.
- 6) Connect your PC alone to one of the LAN ports on the device.

## 3. What can I do if I forget my password?

- If you forgot your login password, restore the device to its factory default settings and then use the default User Name "admin" and Password "admin" to log in.
- If you forgot your wireless network password, log in to the device User Interface, and go to Wireless > Security to check or change your password.

#### 4. Why cannot I connect to the searched wireless network?

1) Verify that you entered a correct security key.

2) Log in to the device, select **Advanced** > **Wireless** and change the wireless network name (SSID). Then connect again.

3) Log in to the device, select Advanced > Wireless > Security and change the security settings. Then connect again.



# **Appendix 5 VPI/VCI List**

The following table lists common ISPs and their VPI and VCI numbers. If you cannot locate your ISP and their VPI and

VCI information here, ask your ISP to provide it.

Country	ISP	VPI	VCI	Encapsulation
Australia	Telstra	8	35	PPPoA LLC
Australia	GoldenIT	8	35	PPPOA_VCMUX
Australia	Telstra Bigpond	8	35	PPPOE_LLC
Australia	OptusNET	8	35	PPPOE_VCMUX
Australia	ААРТ	8	35	PPPOE_VCMUX
Australia	ADSL Direct	8	35	PPPOE_LLC
Australia	Ausie Broadband	8	35	PPPOE_LLC
Australia	Australia On Line	8	35	PPPOA_VCMUX
Australia	Connexus	8	35	PPPOE_LLC
Australia	Dodo	8	35	PPPOE_LLC
Australia	Gotalk	8	35	PPPOE_VCMUX
Australia	Internode	8	35	PPPOE_VCMUX
Australia	iPrimus	8	35	PPPOA_VCMUX
Australia	Netspace	8	35	PPPOE_VCMUX
Australia	Southern Cross Telco	8	35	PPPOE_LLC
Australia	TPG Internet	8	35	PPPOE_LLC
Argentina	Telecom	0	33	PPPoE LLC
Argentina	Telefonica	8	35	PPPoE LLC
Argentina		1	33	PPPoA VC-MUX
Belgium	ADSL Office	8	35	1483 Routed IP LLC
Belgium	Turboline	8	35	PPPoA LLC
Belgium	Turboline	8	35	1483 Bridged IP LLC
Belgium	ADSL Office	8	35	1483 Bridged IP LLC
Bolivia		0	34	1483 Routed IP LLC
Brazil	Brasil Telcom	0	35	PPPoE LLC
Brazil	Telefonica	8	35	PPPoE LLC



Country	ISP	VPI	VCI	Encapsulation
Brazil	Telmar	0	33	PPPoE LLC
Brazil	South Region	1	32	PPPoE LLC
Canada	Primus Canada	0	35	PPPoE LLC
Canada	Rogers Canada (1)	0	35	PPPoE LLC
Canada	Rogers Canada (2)	8	35	1483 Bridged IP LLC
Canada	Rogers Canada (3)	0	35	1484 Bridged IP LLC
Canada	BellSouth(1) Canada	8	35	PPPoE LLC
Canada	BellSouth(2) Canada	0	35	PPPoE LLC
Canada	Sprint (1) Canada	0	35	PPPoA LLC
Canada	Sprint (2) Canada	8	35	PPPoE LLC
Canada	Verizon (1) Canada	0	35	PPPoE LLC
Canada	Verizon (2) Canada	0	35	1483 Bridged IP LLC
Colombia	EMCALI	0	33	PPPoA VC-MUX
Columbia	ETB	0	33	PPPoE LLC
Costa Rica	ICE	1	50	1483 Routed IP LLC
Czech Republic		8	48	1483 Bridged IP LLC
Denmark	Cybercity, Tiscali	0	35	PPPoA VC-MUX
Dominican Republic		0	33	1483 Bridged IP LLC
Dubai		0	50	1483 Bridged IP LLC
Egypt:	TE-data	0	35	1483 Bridged IP LLC
Egypt:	Linkdsl	0	35	1483 Bridged IP LLC
Egypt:	Vodafone	8	35	1483 Bridged IP LLC
Finland	Saunalahti	0	100	1483 Bridged IP LLC
Finland	Elisa	0	100	1483 Bridged IP LLC
Finland	DNA	0	100	1483 Bridged IP LLC
Finland	Sonera	0	35	1483 Bridged IP LLC
France	Free	8	36	LLC
France (1)	Orange	8	35	PPPoE LLC
France (2)		8	67	PPPoE LLC
France (3)	SFR	8	35	PPPoA VC-MUX
Germany		1	32	PPPoE LLC



Country	ISP	VPI	VCI	Encapsulation
Hungary	Sci-Network	0	35	PPPoE LLC
Iceland	Islandssimi	0	35	PPPoA VC-MUX
Iceland	Siminn	8	48	PPPoA VC-MUX
India	Airtel	1	32	1483 Bridged IP LLC
India	BSNL	0	35	1483 Bridged IP LLC
India	MTNL	0	35	1483 Bridged IP LLC
India	RELIANCE	0	35	PPPOE LLC
India	TATA INDICOM	0	32	PPPOE LLC
India	CONNECT	1	32	PPPOE LLC
Indonesia Speedy Telkomnet		8	81	PPPoE LLC
Iran	[Shatel] Aria-Rasaneh-Tadbir	0	35	PPPOE LLC
Iran	Asia-Tech	0	35	PPPOE LLC
Iran	Pars-Online (Tehran)	0	35	PPPOE LLC
Iran	Pars-Online (Provinces)	0	59	PPPOE LLC
Iran	[Saba-Net] Neda-Gostar-Saba	0	35	PPPOE LLC
Iran	Pishgaman-Tose	0	35	PPPOE LLC
Iran	Fan-Ava	8	35	PPPOE LLC
Iran	Datak	0	35	PPPOE LLC
Iran	Laser (General)	0	35	PPPOE LLC
Iran	Laser (Privates)	0	32	PPPOE LLC
Iran	Asr-Enteghal-Dadeha	8	35	PPPOE LLC
Iran	Kara-Amin-Ertebat	0	33	PPPOE LLC
Iran	ITC	0	35	PPPOE LLC
Iran (1)		0	35	PPPoE LLC
Iran (2)		8	81	PPPoE LLC
Iran	Dadegostar Asre Novin	0	33	PPPOE LLC
Israel		8	35	PPPoA VC-MUX



Country	ISP	VPI	VCI	Encapsulation
Israel(1)		8	48	PPPoA VC-MUX
Italy		8	35	1483 Bridged IP LLC
Italy		8	35	PPPoA VC-MUX
Jamaica (1)		8	35	PPPoA VC-MUX
Jamaica (2)		0	35	PPPoA VC-MUX
Jamaica (3)		8	35	1483 Bridged IP LLC SNAP
Jamaica (4)		0	35	1483 Bridged IP LLC SNAP
Kazakhstan	Kazakhtelecom «Megaline»	0	40	LLC/SNAP Bridging
Kazakhstan		0	33	PPPoA VC-MUX
kuwait unitednetwork		0	33	1483 Bridged IP LLC
Malaysia	Streamyx	0	35	PPPOE LLC
Malaysia		0	35	PPPoE LLC
Mexico	Telmex (1)	8	81	PPPoE LLC
Mexico	Telmex (2)	8	35	PPPoE LLC
Mexico	Telmex (3)	0	81	PPPoE LLC
Mexico	Telmex (4)	0	35	PPPoE LLC
morocco	IAM	8	35	PPPOE
Netherlands	BBNED	0	35	PPPoA VC-MUX
Netherlands	MXSTREAM	8	48	1483 Bridged IP LLC
Netherlands	BBNED	0	35	1483 Bridged IP LLC
Netherlands	MX Stream	8	48	PPPoA VC-MUX
New Zealand	Xtra	0	35	PPPoA VC-MUX
New Zealand	Slingshot	0	100	PPPoA VC-MUX
Orange Nyumbani		0	25	
(Kenya)		0	55	
Pakistan (PALESTINE)		8	35	1483 Bridged IP LLC
Pakistan for PTCL		0	103	1483 Bridged IP LLC
Pakistan (cyber net)		8	35	PPPoE LLC
Pakistan (linkDotnet)		0	35	PPPoA LLC
Pakistan(PTCL)		8	81	PPPoE LLc

Country	ISP	VPI	VCI	Encapsulation
Philippines(1)		0	35	1483 Bridged IP LLC
Philippines(2)		0	100	1483 Bridged IP LLC
Portugal		0	35	PPPoE LLC
Puerto Rico	Coqui.net	0	35	PPPoA LLC
RomTelecom Romania:		0	35	1483 Bridged IP LLC
Russia	Rostel	0	35	PPPoE LLC
Russia	Port telecom	0	35	PPPoE LLC
Russia	VNTC	8	35	PPPoE LLC
Saudi Arabia (1)		0	33	PPPoE LLC
Saudi Arabia (2)		0	35	PPPoE LLC
Saudi Arabia (3)		0	33	1483 Bridged IP LLC
Saudi Arabia (4)		0	33	1483 Routed IP LLC
Saudi Arabia (5)		0	35	1483 Bridged IP LLC
Saudi Arabia (6)		0	35	1483 Routed IP LLC
Spain	Arrakis	0	35	1483 Bridged IP VC-MUX
Spain	Auna	8	35	1483 Bridged IP VC-MUX
Spain	Comunitel	0	33	1483 Bridged IP VC-MUX
Spain	Eresmas	8	35	1483 Bridged IP VC-MUX
Spain	Jazztel	8	35	IPOE VC-MUX
Spain	Jazztel ADSL2+/ Desagregado	8	35	1483 Bridged IP LLC-BRIDGING
Spain	OpenforYou	8	32	1483 Bridged IP VC-MUX
Spain	Tele2	8	35	1483 Bridged IP VC-MUX
Spain	Telefónica (España)	8	32	1483 Bridged IP LLC/SNAP
Spain	Albura, Tiscali	1	32	PPPoA VC-MUX
Spain	Colt Telecom, Ola Internet	0	35	PPPoA VC-MUX
Spain	EresMas, Retevision	8	35	PPPoA VC-MUX
Spain	Telefonica (1)	8	32	PPPoE LLC
Spain	Telefonica (2), Terra	8	32	1483 Routed IP LLC
Spain	Wanadoo (1)	8	35	PPPoA VC-MUX

Country	ISP	VPI	VCI	Encapsulation
Spain	Wanadoo (2)	8	32	PPPoE LLC
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Uni2	1	33	1483 Bridged IP VC-MUX
Spain	Orange	8	35	1483 Bridged IP VC-MUX
Spain	Orange 20 Megas	8	35	LLC-BRIDGING
Spain	Orange	8	32	1483 Bridged IP LLC/SNAP
Spain	Ya.com	8	32	1483 Bridged IP VC - MUX
Spain	Ya.com	8	32	1483 Bridged IP LLC/SNAP
Spain	Wanadoo (3)	8	32	1483 Routed IP LLC
SpainWanadoo		8	32	1483 Bridged IP LLC
Sri Lanka		Q	25	
Telecom-(SLT)		0	- 55	FFFOE LLC
Sweden	Telenordia	8	35	PPPoE
Sweden	Telia	8	35	1483 Routed IP LLC
Switzerland		8	35	1483 Bridged IP LLC
Switzerland		8	35	PPPoE LLC
Telefónica (Argentina)		8	35	1483 Bridged IP LLC-based
Telefónica (Perú)		8	48	1483 Bridged IP VC-MUX
Thailand	TRUE	0	100	PPPoE LLC
Thailand	ТОТ	1	32	PPPoE LLC
Thailand	3BB	0	33	PPPoE LLC
Thailand	Cat Telecom	0	35	PPPoE LLC
Thailand	BuddyBB	0	35	PPPoE LLC
Trinidad & Tobago	TSTT	0	35	PPPoA VC-MUX
Turkey (1)		8	35	PPPoE LLC
Turkey (2)		8	35	PPPoA VC-MUX
UAE (Al sahmil)		0	50	1483 Bridged IP LLC
United States	4DV.Net	0	32	PPPoA VC-MUX
United States	All Tel (1)	0	35	PPPoE LLC
United States	All Tel (2)	0	35	1483 Bridged IP LLC



Country	ISP	VPI	VCI	Encapsulation
United States	Ameritech	8	35	PPPoA LLC
United States	AT&T (1)	0	35	PPPoE LLC
United States	AT&T (2)	8	35	1483 Bridged IP LLC
United States	AT&T (3)	0	35	1483 Bridged IP LLC
United States	August.net (1)	0	35	1483 Bridged IP LLC
United States	August.net (2)	8	35	1483 Bridged IP LLC
United States	BellSouth	8	35	PPPoE LLC
United States	Casstle.Net	0	96	1483 Bridged IP LLC
United States	CenturyTel (1)	8	35	PPPoE LLC
United States	CenturyTel (2)	8	35	1483 Bridged IP LLC
United States	Coqui.net	0	35	PPPoA LLC
United States	Covad	0	35	PPPoE LLC
United States	Earthlink (1)	0	35	PPPoE LLC
United States	Earthlink (2)	8	35	PPPoE LLC
United States	Earthlink (3)	8	35	PPPoE VC-MUX
United States	Earthlink (4)	0	32	PPPoA LLC
United States	Eastex	0	100	PPPoA LLC
United States	Embarq	8	35	1483 Bridged IP LLC
United States	Frontier	0	35	PPPoE LLC
United States	Grande ommunications	1	34	PPPoE LLC
United States	GWI	0	35	1483 Bridged IP LLC
United States	Hotwire	0	35	1483 Bridged IP LLC
United States	Internet Junction	0	35	1484 Bridged IP LLC
United States	PVT	0	35	1485 Bridged IP LLC
United States	QWest (1)	0	32	PPPoALLC
United States	QWest (2)	0	32	PPPoA VC-MUX
United States	QWest (3)	0	32	1483 Bridged IP LLC
United States	QWest (4)	0	32	PPPoE LLC
United States	SBC (1)	0	35	PPPoE LLC
United States	SBC (2)	0	35	1483 Bridged IP LLC
United States	SBC (3)	8	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
United States	Sonic	0	35	1484 Bridged IP LLC
United States	SouthWestern Bell	0	35	1483 Bridged IP LLC
United States	Sprint (1)	0	35	PPPoALLC
United States	Sprint (2)	8	35	PPPoE LLC
United States	Sprint Territory	0	35	PPPoE LLC
Linited States	SureWest	0	24	1492 Dridged LLC Snor
United States	Communications(1)	0	54	1485 Bridged LLC Shap
United States	SureWest	0	20	
United States	Communications(2)	0	52	FFFOE LLC
United States	SureWest	0	32	DDDo A I I C
United States	Communications(3)	0	52	FFF0ALLC
United States	Toast.Net	0	35	PPPoE LLC
United States	Uniserv	0	33	1483 Bridged IP LLC
United States	US West	0	32	PPPoA VC-MUX
United States	Verizon (1)	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United States	Windstream	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United Kingdom (1)		0	38	PPPoA VC-MUX
United Kingdom (2)		0	38	PPPoE LLC
United Kingdom	AOL	0	38	PPPoE VC-MUX
United Kingdom	Karoo	1	50	PPPoA LLC
UK		0	38	1483 Bridged IP LLC
Uzbekistan	Sharq Stream	8	35	PPPoE LLC
Uzbekistan	Sarkor	0	33	PPPoE LLC
Uzbekistan	TShTT	0	35	PPPoE LLC
Venezuela	CANTV	0	33	1483 Routed IP LLC
Vietnam		0	35	PPPoE LLC
Vietnam	VDC	8	35	PPPoE LLC
Vietnam	Viettel	8	35	PPPoE LLC
Vietnam	FPT	0	33	PPPoE LLC



Country	ISP	VPI	VCI	Encapsulation
Australia	Telstra	8	35	PPPoA LLC
Australia	GoldenIT	8	35	_PPPOA_VCMUX
Australia	Telstra Bigpond	8	35	PPPOE_LLC
Australia	OptusNET	8	35	PPPOE_VCMUX
Australia	AAPT	8	35	PPPOE_VCMUX
Australia	ADSL Direct	8	35	PPPOE_LLC
Australia	Ausie Broadband	8	35	PPPOE_LLC
Australia	Australia On Line	8	35	PPPOA_VCMUX
Australia	Connexus	8	35	PPPOE_LLC
Australia	Dodo	8	35	PPPOE_LLC
Australia	Gotalk	8	35	PPPOE_VCMUX
Australia	Internode	8	35	PPPOE_VCMUX
Australia	iPrimus	8	35	PPPOA_VCMUX
Australia	Netspace	8	35	PPPOE_VCMUX
Australia	Southern Cross Telco	8	35	PPPOE_LLC
Australia	TPG Internet	8	35	PPPOE_LLC
Argentina	Telecom	0	33	PPPoE LLC
Argentina	Telefonica	8	35	PPPoE LLC
Argentina		1	33	PPPoA VC-MUX
Belgium	ADSL Office	8	35	1483 Routed IP LLC
Belgium	Turboline	8	35	PPPoA LLC
Belgium	Turboline	8	35	1483 Bridged IP LLC
Belgium	ADSL Office	8	35	1483 Bridged IP LLC
Bolivia		0	34	1483 Routed IP LLC
Brazil	Brasil Telcom	0	35	PPPoE LLC
Brazil	Telefonica	8	35	PPPoE LLC
Brazil	Telmar	0	33	PPPoE LLC
Brazil	South Region	1	32	PPPoE LLC
Canada	Primus Canada	0	35	PPPoE LLC
Canada	Rogers Canada (1)	0	35	PPPoE LLC
Canada	Rogers Canada (2)	8	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
Canada	Rogers Canada (3)	0	35	1484 Bridged IP LLC
Canada	BellSouth(1) Canada	8	35	PPPoE LLC
Canada	BellSouth(2) Canada	0	35	PPPoE LLC
Canada	Sprint (1) Canada	0	35	PPPoA LLC
Canada	Sprint (2) Canada	8	35	PPPoE LLC
Canada	Verizon (1) Canada	0	35	PPPoE LLC
Canada	Verizon (2) Canada	0	35	1483 Bridged IP LLC
Colombia	EMCALI	0	33	PPPoA VC-MUX
Columbia	ЕТВ	0	33	PPPoE LLC
Costa Rica	ICE	1	50	1483 Routed IP LLC
Czech Republic		8	48	1483 Bridged IP LLC
Denmark	Cybercity, Tiscali	0	35	PPPoA VC-MUX
Dominican Republic		0	33	1483 Bridged IP LLC
Dubai		0	50	1483 Bridged IP LLC
Egypt:	TE-data	0	35	1483 Bridged IP LLC
Egypt:	Linkdsl	0	35	1483 Bridged IP LLC
Egypt:	Vodafone	8	35	1483 Bridged IP LLC
Finland	Saunalahti	0	100	1483 Bridged IP LLC
Finland	Elisa	0	100	1483 Bridged IP LLC
Finland	DNA	0	100	1483 Bridged IP LLC
Finland	Sonera	0	35	1483 Bridged IP LLC
France	Free	8	36	LLC
France (1)	Orange	8	35	PPPoE LLC
France (2)		8	67	PPPoE LLC
France (3)	SFR	8	35	PPPoA VC-MUX
Germany		1	32	PPPoE LLC
Hungary	Sci-Network	0	35	PPPoE LLC
Iceland	Islandssimi	0	35	PPPoA VC-MUX
Iceland	Siminn	8	48	PPPoA VC-MUX
India	Airtel	1	32	1483 Bridged IP LLC
India	BSNL	0	35	1483 Bridged IP LLC



Country	ISP	VPI	VCI	Encapsulation
India	MTNL	0	35	1483 Bridged IP LLC
India	RELIANCE	0	35	
India	COMMUNICATION	0	55	
India	TATA INDICOM	0	32	PPPOE LLC
India	CONNECT	1	32	PPPOE LLC
Indonesia Speedy		8	81	PPPoF LLC
Telkomnet		0	01	
Iran	[Shatel]	0	35	PPPOF LLC
	Aria-Rasaneh-Tadbir	0	55	
Iran	Asia-Tech	0	35	PPPOE LLC
Iran	Pars-Online (Tehran)	0	35	PPPOE LLC
Iran	Pars-Online (Provinces)	0	59	PPPOE LLC
Iran	[Saba-Net]	0	35	PPPOE LLC
	Neda-Gostar-Saba		55	
Iran	Pishgaman-Tose	0	35	PPPOE LLC
Iran	Fan-Ava	8	35	PPPOE LLC
Iran	Datak	0	35	PPPOE LLC
Iran	Laser (General)	0	35	PPPOE LLC
Iran	Laser (Privates)	0	32	PPPOE LLC
Iran	Asr-Enteghal-Dadeha	8	35	PPPOE LLC
Iran	Kara-Amin-Ertebat	0	33	PPPOE LLC
Iran	ITC	0	35	PPPOE LLC
Iran (1)		0	35	PPPoE LLC
Iran (2)		8	81	PPPoE LLC
Iran	Dadegostar Asre Novin	0	33	PPPOE LLC
Israel		8	35	PPPoA VC-MUX
Israel(1)		8	48	PPPoA VC-MUX
Italy		8	35	1483 Bridged IP LLC
Italy		8	35	PPPoA VC-MUX
Jamaica (1)		8	35	PPPoA VC-MUX
Jamaica (2)		0	35	PPPoA VC-MUX

Country	ISP	VPI	VCI	Encapsulation
Jamaica (3)		8	35	1483 Bridged IP LLC SNAP
Jamaica (4)		0	35	1483 Bridged IP LLC SNAP
Kazakhstan	Kazakhtelecom «Megaline»	0	40	LLC/SNAP Bridging
Kazakhstan		0	33	PPPoA VC-MUX
kuwait unitednetwork		0	33	1483 Bridged IP LLC
Malaysia	Streamyx	0	35	PPPOE LLC
Malaysia		0	35	PPPoE LLC
Mexico	Telmex (1)	8	81	PPPoE LLC
Mexico	Telmex (2)	8	35	PPPoE LLC
Mexico	Telmex (3)	0	81	PPPoE LLC
Mexico	Telmex (4)	0	35	PPPoE LLC
morocco	IAM	8	35	PPPOE
Netherlands	BBNED	0	35	PPPoA VC-MUX
Netherlands	MXSTREAM	8	48	1483 Bridged IP LLC
Netherlands	BBNED	0	35	1483 Bridged IP LLC
Netherlands	MX Stream	8	48	PPPoA VC-MUX
New Zealand	Xtra	0	35	PPPoA VC-MUX
New Zealand	Slingshot	0	100	PPPoA VC-MUX
Orange Nyumbani (Kenya)		0	35	PPPoE LLC
Pakistan (PALESTINE)		8	35	1483 Bridged IP LLC
Pakistan for PTCL		0	103	1483 Bridged IP LLC
Pakistan (cyber net)		8	35	PPPoE LLC
Pakistan (linkDotnet)		0	35	PPPoA LLC
Pakistan(PTCL)		8	81	PPPoE LLc
Philippines(1)		0	35	1483 Bridged IP LLC
Philippines(2)		0	100	1483 Bridged IP LLC
Portugal		0	35	PPPoE LLC
Puerto Rico	Coqui.net	0	35	PPPoA LLC
RomTelecom Romania:		0	35	1483 Bridged IP LLC



Country	ISP	VPI	VCI	Encapsulation
Russia	Rostel	0	35	PPPoE LLC
Russia	Port telecom	0	35	PPPoE LLC
Russia	VNTC	8	35	PPPoE LLC
Saudi Arabia (1)		0	33	PPPoE LLC
Saudi Arabia (2)		0	35	PPPoE LLC
Saudi Arabia (3)		0	33	1483 Bridged IP LLC
Saudi Arabia (4)		0	33	1483 Routed IP LLC
Saudi Arabia (5)		0	35	1483 Bridged IP LLC
Saudi Arabia (6)		0	35	1483 Routed IP LLC
Spain	Arrakis	0	35	1483 Bridged IP VC-MUX
Spain	Auna	8	35	1483 Bridged IP VC-MUX
Spain	Comunitel	0	33	1483 Bridged IP VC-MUX
Spain	Eresmas	8	35	1483 Bridged IP VC-MUX
Spain	Jazztel	8	35	IPOE VC-MUX
Spain	Jazztel ADSL2+ / Desagregado	8	35	1483 Bridged IP LLC-BRIDGING
Spain	OpenforYou	8	32	1483 Bridged IP VC-MUX
Spain	Tele2	8	35	1483 Bridged IP VC-MUX
Spain	Telefónica (España)	8	32	1483 Bridged IP LLC/SNAP
Spain	Albura, Tiscali	1	32	PPPoA VC-MUX
Spain	Colt Telecom, Ola Internet	0	35	PPPoA VC-MUX
Spain	EresMas, Retevision	8	35	PPPoA VC-MUX
Spain	Telefonica (1)	8	32	PPPoE LLC
Spain	Telefonica (2), Terra	8	32	1483 Routed IP LLC
Spain	Wanadoo (1)	8	35	PPPoA VC-MUX
Spain	Wanadoo (2)	8	32	PPPoE LLC
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Terra	8	32	1483 Bridged IP LLC/SNAP
Spain	Uni2	1	33	1483 Bridged IP VC-MUX
Spain	Orange	8	35	1483 Bridged IP VC-MUX



Country	ISP	VPI	VCI	Encapsulation
Spain	Orange 20 Megas	8	35	LLC-BRIDGING
Spain	Orange	8	32	1483 Bridged IP LLC/SNAP
Spain	Ya.com	8	32	1483 Bridged IP VC - MUX
Spain	Ya.com	8	32	1483 Bridged IP LLC/SNAP
Spain	Wanadoo (3)	8	32	1483 Routed IP LLC
SpainWanadoo		8	32	1483 Bridged IP LLC
Sri Lanka		0	25	
Telecom-(SLT)		8	35	PPPOE LLC
Sweden	Telenordia	8	35	PPPoE
Sweden	Telia	8	35	1483 Routed IP LLC
Switzerland		8	35	1483 Bridged IP LLC
Switzerland		8	35	PPPoE LLC
Telefónica (Argentina)		8	35	1483 Bridged IP LLC-based
Telefónica (Perú)		8	48	1483 Bridged IP VC-MUX
Thailand	TRUE	0	100	PPPoE LLC
Thailand	ТОТ	1	32	PPPoE LLC
Thailand	3BB	0	33	PPPoE LLC
Thailand	Cat Telecom	0	35	PPPoE LLC
Thailand	BuddyBB	0	35	PPPoE LLC
Trinidad & Tobago	TSTT	0	35	PPPoA VC-MUX
Turkey (1)		8	35	PPPoE LLC
Turkey (2)		8	35	PPPoA VC-MUX
UAE (Al sahmil)		0	50	1483 Bridged IP LLC
United States	4DV.Net	0	32	PPPoA VC-MUX
United States	All Tel (1)	0	35	PPPoE LLC
United States	All Tel (2)	0	35	1483 Bridged IP LLC
United States	Ameritech	8	35	PPPoA LLC
United States	AT&T (1)	0	35	PPPoE LLC
United States	AT&T (2)	8	35	1483 Bridged IP LLC
United States	AT&T (3)	0	35	1483 Bridged IP LLC
United States	August.net (1)	0	35	1483 Bridged IP LLC

Country	ISP	VPI	VCI	Encapsulation
United States	August.net (2)	8	35	1483 Bridged IP LLC
United States	BellSouth	8	35	PPPoE LLC
United States	Casstle.Net	0	96	1483 Bridged IP LLC
United States	CenturyTel (1)	8	35	PPPoE LLC
United States	CenturyTel (2)	8	35	1483 Bridged IP LLC
United States	Coqui.net	0	35	PPPoA LLC
United States	Covad	0	35	PPPoE LLC
United States	Earthlink (1)	0	35	PPPoE LLC
United States	Earthlink (2)	8	35	PPPoE LLC
United States	Earthlink (3)	8	35	PPPoE VC-MUX
United States	Earthlink (4)	0	32	PPPoA LLC
United States	Eastex	0	100	PPPoA LLC
United States	Embarq	8	35	1483 Bridged IP LLC
United States	Frontier	0	35	PPPoE LLC
United States	Grande ommunications	1	34	PPPoE LLC
United States	GWI	0	35	1483 Bridged IP LLC
United States	Hotwire	0	35	1483 Bridged IP LLC
United States	Internet Junction	0	35	1484 Bridged IP LLC
United States	PVT	0	35	1485 Bridged IP LLC
United States	QWest (1)	0	32	PPPoALLC
United States	QWest (2)	0	32	PPPoA VC-MUX
United States	QWest (3)	0	32	1483 Bridged IP LLC
United States	QWest (4)	0	32	PPPoE LLC
United States	SBC (1)	0	35	PPPoE LLC
United States	SBC (2)	0	35	1483 Bridged IP LLC
United States	SBC (3)	8	35	1483 Bridged IP LLC
United States	Sonic	0	35	1484 Bridged IP LLC
United States	SouthWestern Bell	0	35	1483 Bridged IP LLC
United States	Sprint (1)	0	35	PPPoALLC
United States	Sprint (2)	8	35	PPPoE LLC
United States	Sprint Territory	0	35	PPPoE LLC



Country	ISP	VPI	VCI	Encapsulation
United States	SureWest Communications(1)	0	34	1483 Bridged LLC Snap
United States	SureWest Communications(2)	0	32	PPPoE LLC
United States	SureWest Communications(3)	0	32	PPPoA LLC
United States	Toast.Net	0	35	PPPoE LLC
United States	Uniserv	0	33	1483 Bridged IP LLC
United States	US West	0	32	PPPoA VC-MUX
United States	Verizon (1)	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United States	Windstream	0	35	PPPoE LLC
United States	Verizon (2)	0	35	1483 Bridged IP LLC
United Kingdom (1)		0	38	PPPoA VC-MUX
United Kingdom (2)		0	38	PPPoE LLC
United Kingdom	AOL	0	38	PPPoE VC-MUX
United Kingdom	Karoo	1	50	PPPoA LLC
UK		0	38	1483 Bridged IP LLC
Uzbekistan	Sharq Stream	8	35	PPPoE LLC
Uzbekistan	Sarkor	0	33	PPPoE LLC
Uzbekistan	TShTT	0	35	PPPoE LLC
Venezuela	CANTV	0	33	1483 Routed IP LLC
Vietnam		0	35	PPPoE LLC
Vietnam	VDC	8	35	PPPoE LLC
Vietnam	Viettel	8	35	PPPoE LLC
Vietnam	FPT	0	33	PPPoE LLC



# Appendix 6 Regulatory Compliance Information

# CE

#### **CE Mark Warning**

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

**NOTE:** (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.



#### FCC Statement

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

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

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

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

## **Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.