

Wireless MAC Filter

The MAC filter screen allows you to configure the router to give exclusive access to up to 8 devices (Allow Association) or exclude up to 8 devices from accessing the router (Deny Association). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:AA:BB:00:00:02.

You need to know the MAC address of the devices you wish to filter.

Configuration

Wireless MAC Address Filter

SSID Index: SSID1

Active: Activated Deactivated

Action: Allow the follow Wireless LAN station(s) association.

MAC Address:

Wireless MAC Address Filter Listing

Index	MAC Address	Edit	Delete
-------	-------------	------	--------

SSID Index: Select the targeted SSID you want the MAC filter rules to apply to.

Active: Select **Activated** to enable MAC address filtering.

Action: Define the filter action for the list of MAC addresses in the MAC address filter table.

Select **Deny** to block access to the AP, MAC addresses not listed will be allowed to access the router. Select **Allow** to permit access to the router, MAC addresses not listed will be denied access to the router.

MAC Address: Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless station that are allowed or denied access to the specified in these address fields.

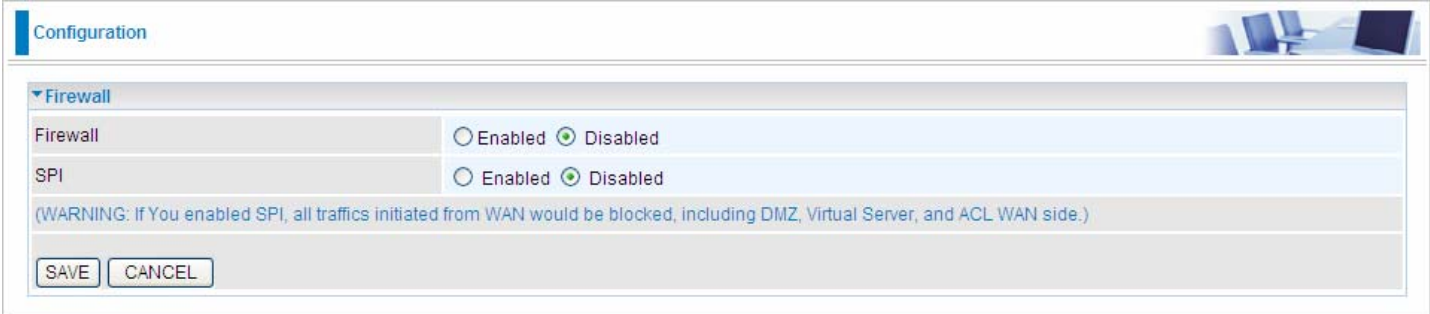
Advanced Setup

Advanced Step provides advanced features including **Firewall, Routing, NAT, Static DNS, QoS, IPSEC Setting, PPTP Server, PPTP Client, L2TP, Internet Grouping, and Time Schedule** for advanced users.

The screenshot displays the configuration page for a BILLION 4G/LTE Wireless-N BB Gateway. The interface includes a navigation menu on the left with options like Status, Quick Start, Configuration, Interface Setup, Advanced Setup (with sub-items: Firewall, Routing, NAT, Static DNS, QoS, IPSEC Setting, PPTP Server, PPTP Client, L2TP, Port Isolation), VOIP, Access Management, Maintenance, and Language. The main content area is titled 'Configuration' and shows the 'Firewall' settings. Both 'Firewall' and 'SPI' are currently set to 'Disabled' (indicated by a selected radio button). A warning message states: '(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)'. Below the settings are 'SAVE' and 'CANCEL' buttons. At the bottom right, there are 'Restart' and 'Logout' buttons. The footer contains the copyright notice: 'Copyright © Billion Electric Co., Ltd. All rights reserved.'

Firewall

Your router includes a firewall for helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a “natural” Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet.



Configuration

Firewall

Firewall Enabled Disabled

SPI Enabled Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

SAVE CANCEL

Firewall: To automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

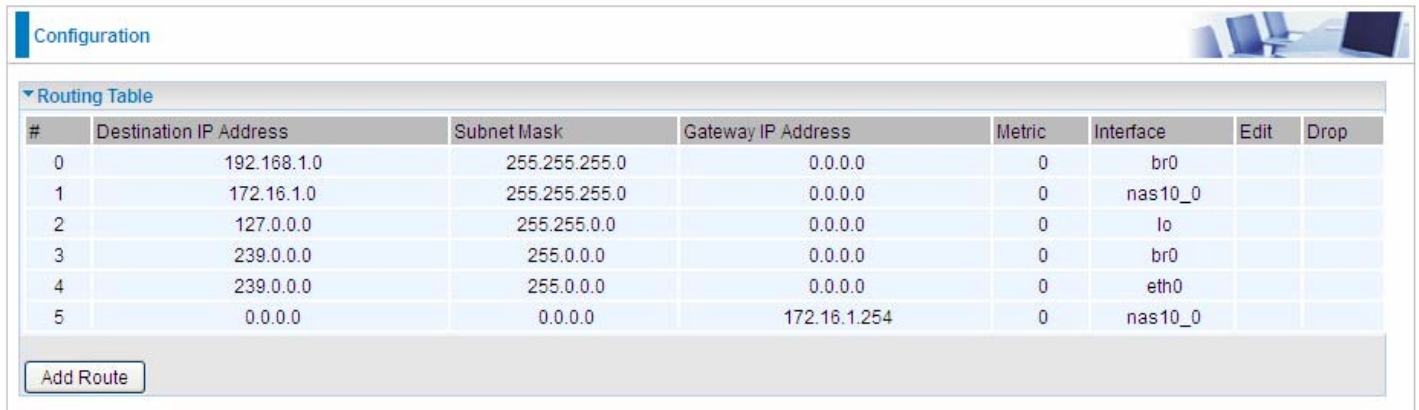
- ▶ **Enabled:** It activates your firewall function.
- ▶ **Disabled:** It disables the firewall function.

SPI: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

- ▶ **Enabled:** It activates your SPI function.
- ▶ **Disabled:** It disables the SPI function.

Routing

This is static route feature. You are equipped with the capability to control the routing of all the traffic across your network. With each routing rule created, user can specifically assign the destination where the traffic will be routed to.



#	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
0	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
1	172.16.1.0	255.255.255.0	0.0.0.0	0	nas10_0		
2	127.0.0.0	255.255.0.0	0.0.0.0	0	lo		
3	239.0.0.0	255.0.0.0	0.0.0.0	0	br0		
4	239.0.0.0	255.0.0.0	0.0.0.0	0	eth0		
5	0.0.0.0	0.0.0.0	172.16.1.254	0	nas10_0		

Add Route

#: Item number

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

Gateway IP Address: IP address of the gateway or existing interface that this route uses.

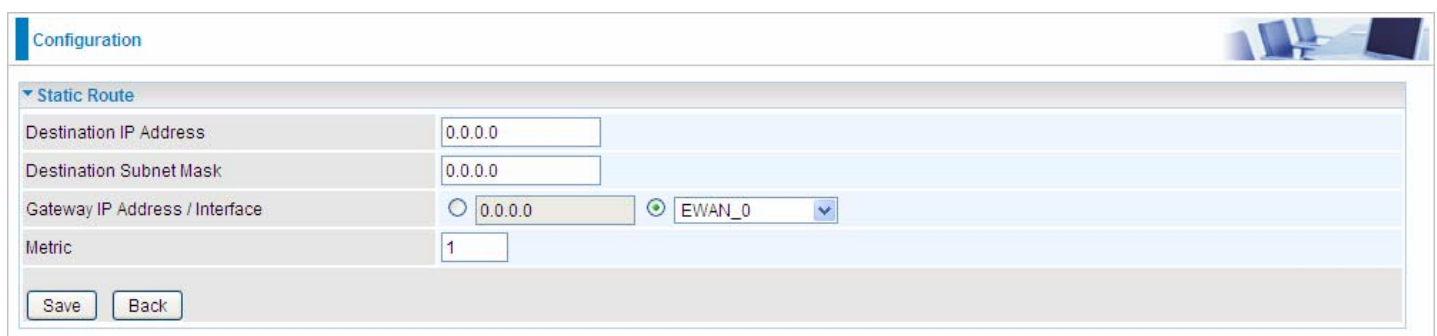
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Interface: Media/channel selected to append the route.

Edit: Edit the route; this icon is not shown for system default route.

Drop: Drop the route; this icon is not shown for system default route.

Add Route



Configuration

Static Route

Destination IP Address: 0.0.0.0

Destination Subnet Mask: 0.0.0.0

Gateway IP Address / Interface: 0.0.0.0 EWAN_0

Metric: 1

Save Back

Destination IP Address: This is the destination subnet IP address.

Destination Subnet Mask: The subnet mask of destination network.

Gateway IP Address/Interface: This is the gateway IP address or existing interface to which packets are to be forwarded.

Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

NAT

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/ PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.

In this session, there are “VPN Passthrough”, “SIP ALG”, “DMZ” and “Virtual Server” provided to solve these nasty problems.



Configuration	
NAT	
NAT Status	Enable
ALG	
VPN Passthrough	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
SIP ALG	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
DMZ / Virtual Server	
Interface	EWAN
Service Index	0
DMZ	Edit
Virtual Server	Edit

NAT Status: Enabled. It depends on ISP Connection Type in Internet settings.

VPN Passthrough: VPN pass-through is a feature of routers which allows VPN client on a private network to establish outbound VPNs unhindered.

SIP ALG: Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP ALG when SIP phone includes NAT-Traversal algorithm.

Interface: Select to set DMZ/Virtual Server for “EWAN”, “3G/4G-LTE” or “3G/4G-LTE USB”.

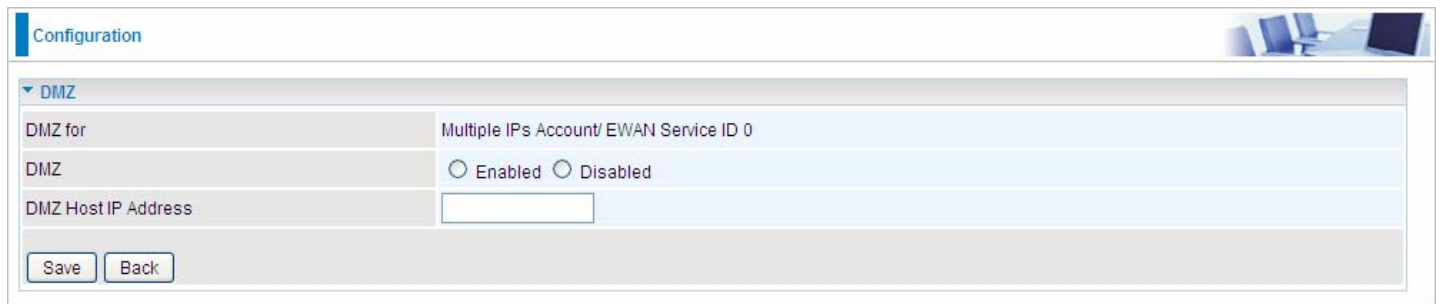
Service Index: Associated to EWAN interface marking each EWAN service (0-7), to select which EWAN service the DMZ and Virtual server are applied to.

Click **DMZ** [Edit](#) or **Virtual Server** [Edit](#) to move on to set the DMZ or Virtual Server parameters, which are represented in the following scenario.

DMZ

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode.

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by the Firewall and NAT algorithms then passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.



The screenshot shows a web configuration page titled "Configuration". Under the "DMZ" section, there are three fields: "DMZ for" set to "Multiple IPs Account/ EWAN Service ID 0", "DMZ" with radio buttons for "Enabled" (selected) and "Disabled", and "DMZ Host IP Address" with an empty text input field. At the bottom of the form are "Save" and "Back" buttons.

DMZ for: Indicate the related WAN interface which allows outside network to connect in and communicate. **Note:** Here you can see the Multiple IPs Account/EWAN Service ID 0. It is the interface set in the previous NAT page.

DMZ:

- ▶ **Enabled:** It activates your DMZ function.
- ▶ **Disabled:** It disables the DMZ function.

DMZ Host IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

Select the **Save** button to apply your changes.

Virtual Server

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode.

In TCP/IP networks, a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server.

The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your PCs. Please see the **WAN** configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

The screenshot shows a web interface for configuring Virtual Servers. The 'Virtual Server' section is expanded, showing the following fields:

- Virtual Server for: Multiple IPs Account/ EWAN
- Protocol: TCP
- Start Port Number: [input field]
- End Port Number: [input field]
- Local IP Address: [input field]
- Start Port Number (Local): [input field]
- End Port Number(Local): [input field]

Below the form are 'Save' and 'Back' buttons. Underneath is a 'Virtual Server Listing' table:

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	N/A	N/A	N/A	N/A	N/A	N/A		
1	N/A	N/A	N/A	N/A	N/A	N/A		
2	N/A	N/A	N/A	N/A	N/A	N/A		
3	N/A	N/A	N/A	N/A	N/A	N/A		
4	N/A	N/A	N/A	N/A	N/A	N/A		
5	N/A	N/A	N/A	N/A	N/A	N/A		
6	N/A	N/A	N/A	N/A	N/A	N/A		
7	N/A	N/A	N/A	N/A	N/A	N/A		
8	N/A	N/A	N/A	N/A	N/A	N/A		
9	N/A	N/A	N/A	N/A	N/A	N/A		

Virtual Server for: Indicate the related WAN interface which allows outside network to connect in and communicate.

Protocol: Choose the application protocol.

Start / End Port Number: Enter a port or port range you want to forward.

(Example: Start / End: 1000 or Start: 1000, End: 2000).

The starting greater than zero (0) and the ending port must be the same or larger than the starting port.

Local IP Address: Enter your server IP address in this field.

Start / End Port Number (Local): Enter the start / end port number of the local application (service).

Examples of well-known and registered port numbers are shown below. For further information, please see IANA's website at <http://www.iana.org/assignments/port-numbers>

Well-known and Registered Ports

Port Number	Protocol	Description
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
7070	UDP	RealAudio



Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.



Attention

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Example : How to setup Port Forwarding for port 21 (FTP server)

If you have a FTP server in your LAN network and want others to access it through WAN.

Step 1: Assign a static IP to your local computer that is hosting the FTP server.

Step 2: Login to the Gateway and go to **Configuration / Advanced Setup / NAT / Virtual Server**.

FTP server uses TCP protocol with port 21.

Enter "21" to Start and End Port Number. BiPAC 6300VNP(O)Z will accept port 21 requests from WAN side.

Enter the static IP assigned to the local PC that is hosting the FTP server. Ex: 192.168.1.102

Enter "21" to Local Start and End Port number. BiPAC 6300VNP(O)Z will forward port 21 request from WAN to the specific LAN PC (ex:192.168.1.102) in the network.

Step 3: Click **Save** to save settings.

The screenshot shows the 'Configuration' page with the 'Virtual Server' section expanded. The settings are as follows:

- Virtual Server for: Multiple IPs Account/ EWAN
- Protocol: TCP
- Start Port Number: 21
- End Port Number: 21
- Local IP Address: 192.168.1.102
- Start Port Number (Local): 21
- End Port Number(Local): 21

Below the settings are 'Save' and 'Back' buttons. Underneath is a 'Virtual Server Listing' table:

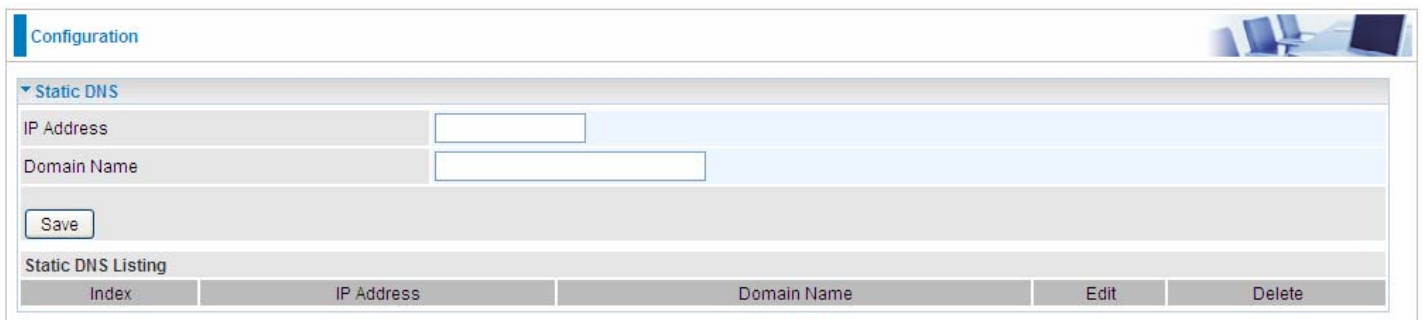
Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.102	21	21		
1	N/A	N/A	N/A	N/A	N/A	N/A		
2	N/A	N/A	N/A	N/A	N/A	N/A		
3	N/A	N/A	N/A	N/A	N/A	N/A		
4	N/A	N/A	N/A	N/A	N/A	N/A		
5	N/A	N/A	N/A	N/A	N/A	N/A		
6	N/A	N/A	N/A	N/A	N/A	N/A		
7	N/A	N/A	N/A	N/A	N/A	N/A		
8	N/A	N/A	N/A	N/A	N/A	N/A		
9	N/A	N/A	N/A	N/A	N/A	N/A		

Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network associates various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name `www.example.com` can be translated into the addresses `192.0.32.10` (IPv4).

Static DNS is a concept relative to Dynamic DNS, in static DNS system, the IP mapped is static without change.



The screenshot displays a web-based configuration interface. At the top left, there is a 'Configuration' tab. Below it, a section titled 'Static DNS' is expanded, showing two input fields: 'IP Address' and 'Domain Name'. A 'Save' button is located below these fields. Underneath, there is a table titled 'Static DNS Listing' with the following columns: Index, IP Address, Domain Name, Edit, and Delete.

IP Address: The IP address you are going to give a specific domain name.

Domain Name: The friendly domain name for the IP address.

Press **Save** button to apply your settings.

QoS

QoS helps you control the upload traffic of each application from LAN (Ethernet and/or Wireless) to WAN (Internet).

It facilitates you the features to control the quality of throughput for each application. This is useful when there on certain types of data you want give higher priority to, such as voice data packets given higher priority than web data packets.

The screenshot shows a web-based configuration interface for Quality of Service (QoS). At the top, there is a 'Configuration' tab and a 'Quality of Service' section. The 'QoS' section has two radio buttons: 'Activated' (selected) and 'Deactivated'. Below this are 'Save' and 'Rules Summary' buttons. The 'Rule' section contains several fields: 'Rule Index' (a dropdown menu set to '0'), 'Active' (radio buttons for 'Yes' and 'No', with 'No' selected), 'Destination IPv4/IPv6 Address', 'Destination Subnet Mask / IPv6 Prefix', 'Destination Port Range' (two input boxes with a tilde separator), 'Source IPv4/IPv6 Address', 'Source Subnet Mask / IPv6 Prefix', 'Source Port Range' (two input boxes with a tilde separator), 'Protocol ID' (a dropdown menu), and 'Priority' (a dropdown menu). At the bottom of the rule configuration area are 'Save' and 'Delete' buttons.

Click **SETTING** to add QoS rules (up to **16** QoS rules).

Rule Index: Index marking for each rule up to maximum of 16.

Active: Select whether to activate the rule.

Destination IPv4/IPv6: Set the IPv4/IPv6 address that you want to filter on destination side.

Destination Subnet Mask / IPv6 Prefix: Specify the Destination Subnet Mask for IPv4 or prefix for IPv6.

Destination Port Range: Set the port range value that you want to filter on destination side.

Source IPv4/IPv6 Address: Set the IP address value that you want to filter on source side in IPv4 or IPv6.

Source Subnet Mask / IPv6 Prefix: Specify the Source Subnet Mask for IPv4 or prefix for IPv6.

Source Port Range: Set the port range value that you want to filter on source side.

Protocol ID: Set the protocol ID type of packets that you want to filter (TCP, UDP, ICMP, and IGMP).

Priority: Select to prioritize the traffic which the rule categorizes, High or Low.

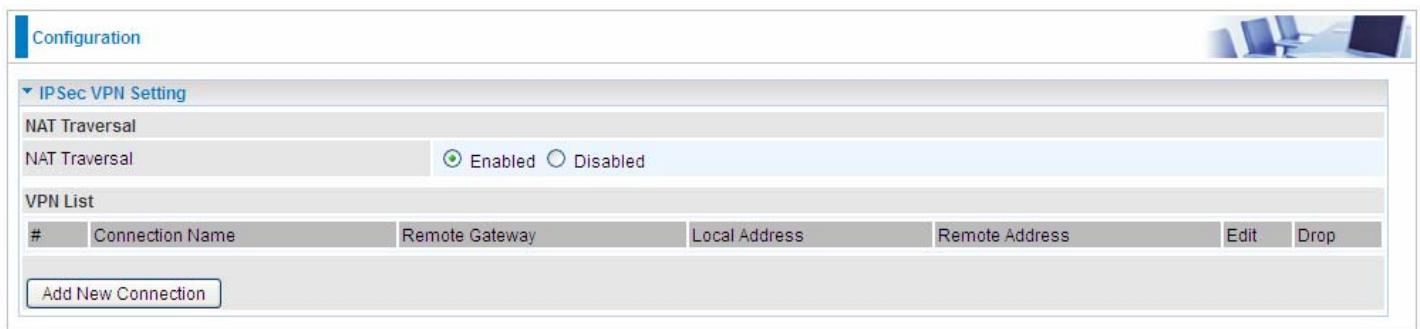
IPSEC Setting (6300VNOZ only)

A **Virtual Private Network (VPN)** is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

A total of 8 IPSec tunnels can be added.



Configuration

IPSec VPN Setting

NAT Traversal

NAT Traversal Enabled Disabled

VPN List

#	Connection Name	Remote Gateway	Local Address	Remote Address	Edit	Drop
---	-----------------	----------------	---------------	----------------	------	------

Add New Connection

NAT Traversal: This directly enables use of the NAT-Traversal IPsec extension (NAT-T). NAT-T allows one or both peers to reside behind a NAT gateway (i.e., doing address- or port-translation).

Click **Add New Connection** to create IPSec connections.

VPN Connection Setting

Active: Select **Yes** to activate the tunnel.

Connection Name: A given name for the connection (e.g. “connection to office”).

Interface: Select the set used interface for the IPSec connection, when you select EWAN interface, the IPSec tunnel would transmit data via this interface to connect to the remote peer.

Remote Gateway IP: The WAN IP address of the remote VPN gateway that is to be connected, establishing a VPN tunnel.

Local Access Range: Set the IP address or subnet of the local network.

- ▶ **Single IP:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).
- ▶ **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

Remote Access Range: Set the IP address or subnet of the remote network.

- ▶ **Single IP:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*). If the remote peer is a host, select Single Address.
- ▶ **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*), If the remote peer is a network, select Subnet.

IKE Mode: IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations(SA). Select Main or Aggressive

mode.

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Local ID Type and Remote ID Type: When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

IDContent: Enter IDContent the name you want to identify when the Local and Remote Type are Domain Name; Enter IDContent IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ▶ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- ▶ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- ▶ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ▶ **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ▶ **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

IPSec Proposal: Select the IPSec security method. There are two methods of verifying the authentication information, AH(Authentication Header) and ESP(Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted and the data origin be authenticated but using AH data origin will only be authenticated but not encrypted.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- ▶ **MD5:** A one-way hashing algorithm that produces a 128-bit hash.
- ▶ **SHA1:** A one-way hashing algorithm that produces a 160-bit hash.

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

- ▶ **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- ▶ **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.

- ▶ **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, an IKE SA is used by IKE.

- ▶ **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.
- ▶ **Phase 2 (IPSec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes. A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

PING for Keep Alive:

- ▶ **None:** The default setting is None. To this mode, it will not detect the remote IPSec peer has been lost or not. It only follows the policy of Disconnection time after no traffic, which the remote IPSec will be disconnected after the time you set in this function.
- ▶ **PING:** This mode will detect the remote IPSec peer has lost or not by pinging specify IP address.
- ▶ **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost. Please be noted, it must be enabled on the both sites.

PING to the IP: It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is required. Default setting is 0.0.0.0 which disables the function

Interval: This sets the time interval between Pings to the IP function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

Ping to the IP	Interval (sec)	Ping to the IP Action
0.0.0.0	0	No
0.0.0.0	2000	No
xxx.xxx.xxx.xxx (A valid IP Address)	0	No
xxx.xxx.xxx.xxx(A valid IP Address)	2000	Yes, activate it in every 2000 second.

Disconnection Time after no traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the Reconnection Time set. 180 seconds is minimum time interval for this function.

Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. 3 minutes is minimum time interval for this function.

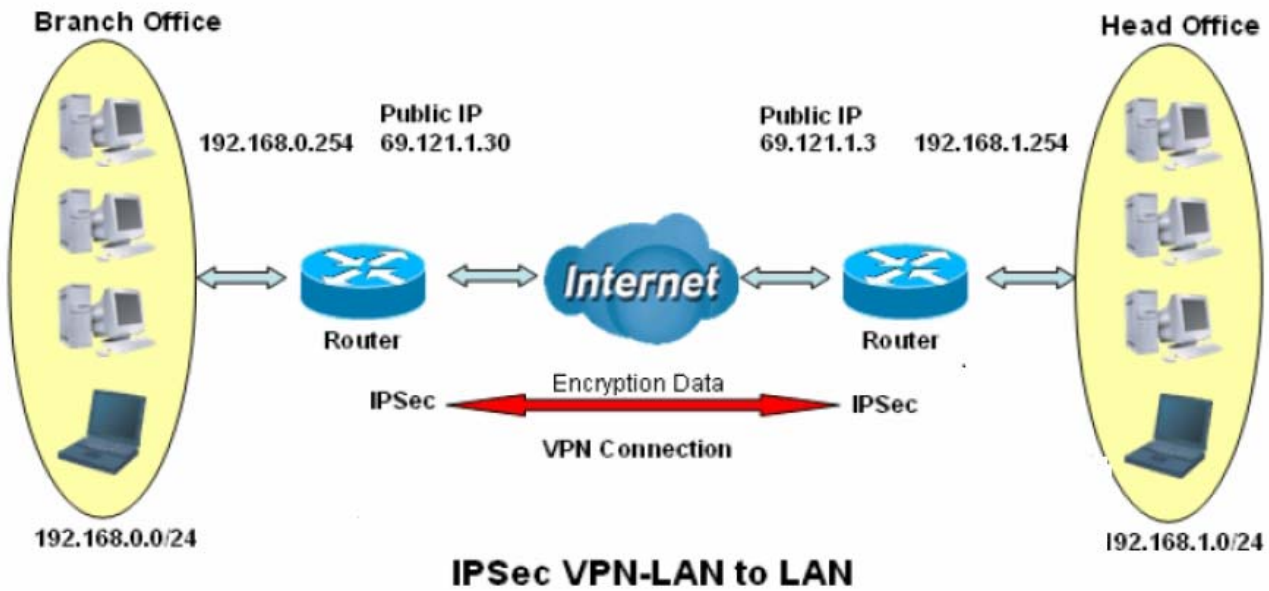
Click **SAVE** to submit the settings.

Examples: How to establish an IPsec Tunnel

1. LAN-to-LAN connection

Two BiPAC 6300VNOZs want to setup a secure IPsec VPN tunnel


Note: The IPsec Settings shall be consistent between the two routers.



Head Office Side:

Setup details:

Item	Function	Description
1	Connection Name	H-to-B Give a name for IPSec connection
2	Local Network	
	Subnet	Select Subnet
	IP Address	192.168.1.0
	Netmask	255.255.255.0
3	Secure Gateway Address(Hostanme)	69.121.1.30 IP address of the Branch office router (on WAN side)
4	Remote Network	
	Subnet	Select Subnet
	IP Address	192.168.0.0
	Netmask	255.255.255.0
5	Proposal	
	Method	ESP
	Authentication	MD5
	Encryption	3DES
	Prefer Forward Security	MODP 1024(group2)
	Pre-shared Key	123456

Configuration 

VPN Connection Setting

Active	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Connection Name	H-to-B	Interface	EWAN
Remote Gateway IP	69.121.1.30 (0.0.0.0 means any)		
Local Access Range	Subnet	Local IP Address	192.168.1.0
		IP Subnetmask	255.255.255.0
Remote Access Range	Subnet	Remote IP Address	192.168.0.0
		IP Subnetmask	255.255.255.0
IKE Mode	Main	Pre-Shared Key	123456
Local ID Type	Default Wan IP	IDContent	*
Remote ID Type	Default Wan IP	IDContent	*
Encryption Algorithm	3DES	Authentication Algorithm	MD5
		Diffie-Hellman Group	MODP1024(DH2)
IPSec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH		
	Authentication Algorithm	MD5	Encryption Algorithm
		3DES	
Perfect Forward Secrecy	MODP1024(DH2)		
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)
PING for keepalive	None	PING to the IP(0.0.0.0:NEVER)	0.0.0.0
		Interval	10 seconds **
Disconnection Time after no traffic	180 seconds (180 at least)		
Reconnection Time	3 min(s) (3 at least)		


Note * : FQDN with @ as first character means don't resolve domain name.

Note ** : (0-3600, 0 means NEVER)

Branch Office Side:

Setup details: the same operation as done in Head Office side

Item	Function		Description	
1	Connection Name	B-to-H	Give a name for IPSec connection	
2	Local Network		Branch Office network	
	Subnet			Select Subnet
	IP Address	192.168.0.0		
	Netmask	255.255.255.0		
3	Remote Secure Gateway Address(Hostanme)	69.121.1.3	IP address of the Head office router (on WAN side)	
4	Remote Network		Head office network	
	Subnet			Select Subnet
	IP Address	192.168.1.0		
	Netmask	255.255.255.0		
5	Proposal		Security Plan	
	Method	ESP		
	Authentication	MD5		
	Encryption	3DES		
	Prefer Forward Security	MODP 1024(group2)		
	Pre-shared Key	123456		

Configuration 

VPN Connection Setting

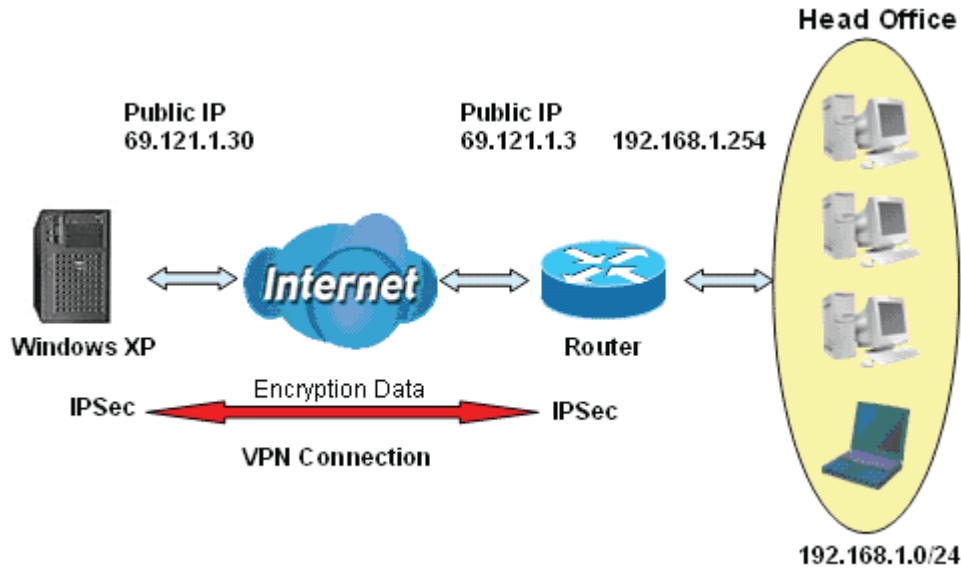
Active	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Connection Name	<input type="text" value="B-to-H"/>	Interface	<input type="text" value="EWAN"/>
Remote Gateway IP	<input type="text" value="69.121.1.3"/> (0.0.0.0 means any)		
Local Access Range	<input type="text" value="Subnet"/>	Local IP Address	<input type="text" value="192.168.0.0"/> IP Subnetmask <input type="text" value="255.255.255.0"/>
Remote Access Range	<input type="text" value="Subnet"/>	Remote IP Address	<input type="text" value="192.168.1.0"/> IP Subnetmask <input type="text" value="255.255.255.0"/>
IKE Mode	<input type="text" value="Main"/>	Pre-Shared Key	<input type="text" value="123456"/>
Local ID Type	<input type="text" value="Default Wan IP"/>	IDContent	<input type="text"/> *
Remote ID Type	<input type="text" value="Default Wan IP"/>	IDContent	<input type="text"/> *
Encryption Algorithm	<input type="text" value="3DES"/>	Authentication Algorithm	<input type="text" value="MD5"/> Diffie-Hellman Group <input type="text" value="MODP1024(DH2)"/>
IPSec Proposal	<input checked="" type="radio"/> ESP <input type="radio"/> AH Authentication Algorithm <input type="text" value="MD5"/> Encryption Algorithm <input type="text" value="3DES"/>		
Perfect Forward Secrecy	<input type="text" value="MODP1024(DH2)"/>		
Phase 1 (IKE)SA Lifetime	<input type="text" value="480"/> min(s)	Phase 2 (IPSec)	<input type="text" value="60"/> min(s)
PING for keepalive	<input type="text" value="None"/>	PING to the IP(0.0.0.0:NEVER)	<input type="text" value="0.0.0.0"/> Interval <input type="text" value="10"/> seconds **
Disconnection Time after no traffic	<input type="text" value="180"/> seconds (180 at least)		
Reconnection Time	<input type="text" value="3"/> min(s) (3 at least)		

Note * : FQDN with @ as first character means don't resolve domain name.

Note ** : (0-3600, 0 means NEVER)

2. Host to LAN

Router servers as VPN server, and host should install the IPSec client to connect to head office through IPSec VPN.



IPSec VPN-Host to LAN

Item	Function		Description
1	Connection Name	Host-to-Headoff	Give a name for IPSec connection
2	Local Network		
	Subnet		Select Subnet
	IP Address	192.168.1.0	Head Office network
	Netmask	255.255.255.0	
3	Remote Secure Gateway (Hostanme)	69.121.1.30	IP address of the Branch office router (on WAN side)
4	Remote Network		
	Single Address	69.121.1.30	Host
5	Proposal		
	Method	ESP	Security Plan
	Authentication	MD5	
	Encryption	3DES	
	Prefer Forward Security	MODP 1024(group2)	
	Pre-shared Key	123456	

Configuration

VPN Connection Setting

Active Yes No

Connection Name: Host-to-Headoff Interface: EWAN

Remote Gateway IP: 69.121.1.30 (0.0.0.0 means any)

Local Access Range: Subnet Local IP Address: 192.168.0.0 IP Subnetmask: 255.255.255.0

Remote Access Range: Single IP Remote IP Address: 69.121.1.30 IP Subnetmask:

IKE Mode: Main Pre-Shared Key: 123456

Local ID Type: Default Wan IP IDContent: *

Remote ID Type: Default Wan IP IDContent: *

Encryption Algorithm: 3DES Authentication Algorithm: MD5 Diffie-Hellman Group: MODP1024(DH2)

IPSec Proposal: ESP AH
 Authentication Algorithm: MD5 Encryption Algorithm: 3DES

Perfect Forward Secrecy: MODP1024(DH2)

Phase 1 (IKE)SA Lifetime: 480 min(s) Phase 2 (IPSec): 60 min(s)

PING for keepalive: None PING to the IP(0.0.0.0:NEVER): 0.0.0.0 Interval: 10 seconds **

Disconnection Time after no traffic: 180 seconds (180 at least)

Reconnection Time: 3 min(s) (3 at least)

Note *: FQDN with @ as first character means don't resolve domain name.
 Note **: (0-3600, 0 means NEVER)

SAVE BACK

PPTP Server (6300VNOZ only)

The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network. PPTP uses an enhanced GRE (Generic Routing Encapsulation) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, and Microsoft CHAP V1/V2 . The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2.

Note: 4 sessions for Client and 4 sessions for Server respectively.

In PPTP session, users can set the basic parameters(authentication, encryption, peer address, etc) for PPTP Server and then set the accounts, and 4 accounts or connections are to be set for PPTP Server.

User	Connection Name	Active	Username	Connection Type	AssignIP

Enable: Select **Yes** to activate PPTP Server. **No** to deactivate PPTP Server.

WAN Interface: Select the exact WAN interface configured for the tunnel. Select Default to use the now-working WAN interface for the tunnel.

Auth. Type: The authentication type, Pap or Chap, and MPPE 128bit Encryption. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

MS-DNS: Directly set the IP of DNS server or let the 192.168.1.254(the router by default) be the MS-DNS server.

User select: 4 sessions for server by default, user1 stands for the first session, and so does user2, etc.

Connection Name: User-defined name for the PPTP connection.

Active: Select **Enable** to activate the account. PPTP server is waiting for the client to connect to this account.

Username: Please input the username for this account.

Password: Please input the password for this account.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Private IP Address Assigned to Dialin user: Specify the private IP address to be assigned to dialin clients, and the IP should be in the same subnet as local LAN, but not occupied.

Peer Network IP: Please input the subnet IP for remote network.

Peer Netmask: Please input the Netmask for remote network.

PPTP Client (6300VNOZ only)

PPTP client can help you dial-in the PPTP server to establish PPTP tunnel over Internet. A total of 4 sessions can be created for PPTP client.

User	Connection Name	Active	Username	Connection Type	ServerIP
User1		<input type="radio"/> Yes <input checked="" type="radio"/> No		Remote Access	

User select: 4 sessions for client connection by default, user1 stands for the first session, and so does user2, etc.

Connection Name: user-defined name for identification.

Auth. Type: The authentication type, Pap or Chap, and MPPE 128bit Encryption. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported. Set the same authentication type as set in the server side.

Active: Select **Yes** to enable the connection to the VPN server.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

PPTP Server Address: Enter the WAN IP address of the PPTP server.

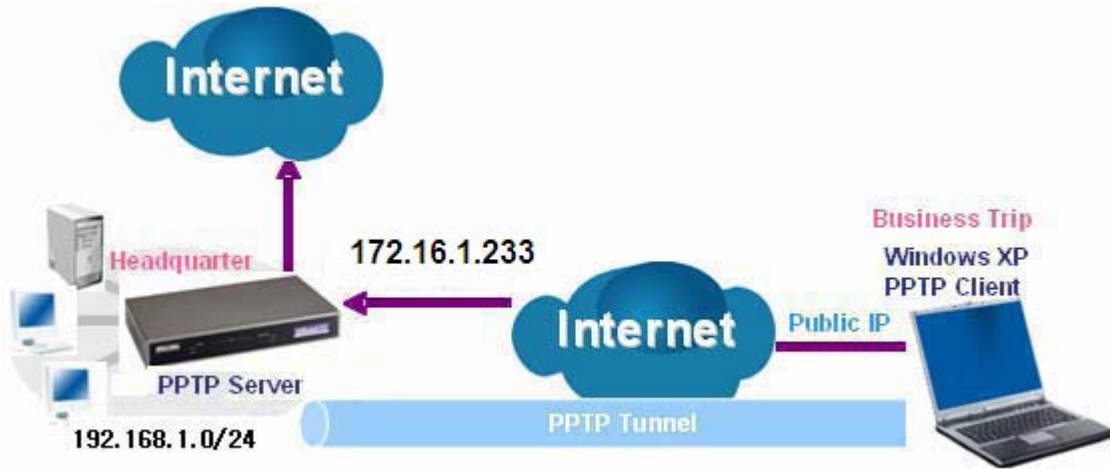
Peer Network IP: Please input the subnet IP for Server peer.

Peer Netmask: Please input the Netmask for server peer.

Click **SET** button to save your changes.

Example: PPTP Remote Access with Windows7

(Note: inside test with 172.16.1.233, just an example for illustration)



Server Side:

1. Please move to **Configuration > PPTP Server**, Enable the PPTP Server and add an account as "test". The exact setting can be found in the screenshot shown below.

Configuration

▼ PPTP Server

Parameters

Enable Yes No

Auth.Type MPPE 128bit Encryption

MS-DNS 192.168.1.254

User select User1

Connection Name test Active Yes No

Username test Password

Connection Type Remote Access Private IP Address Assigned to Dialin user 192.168.1.2

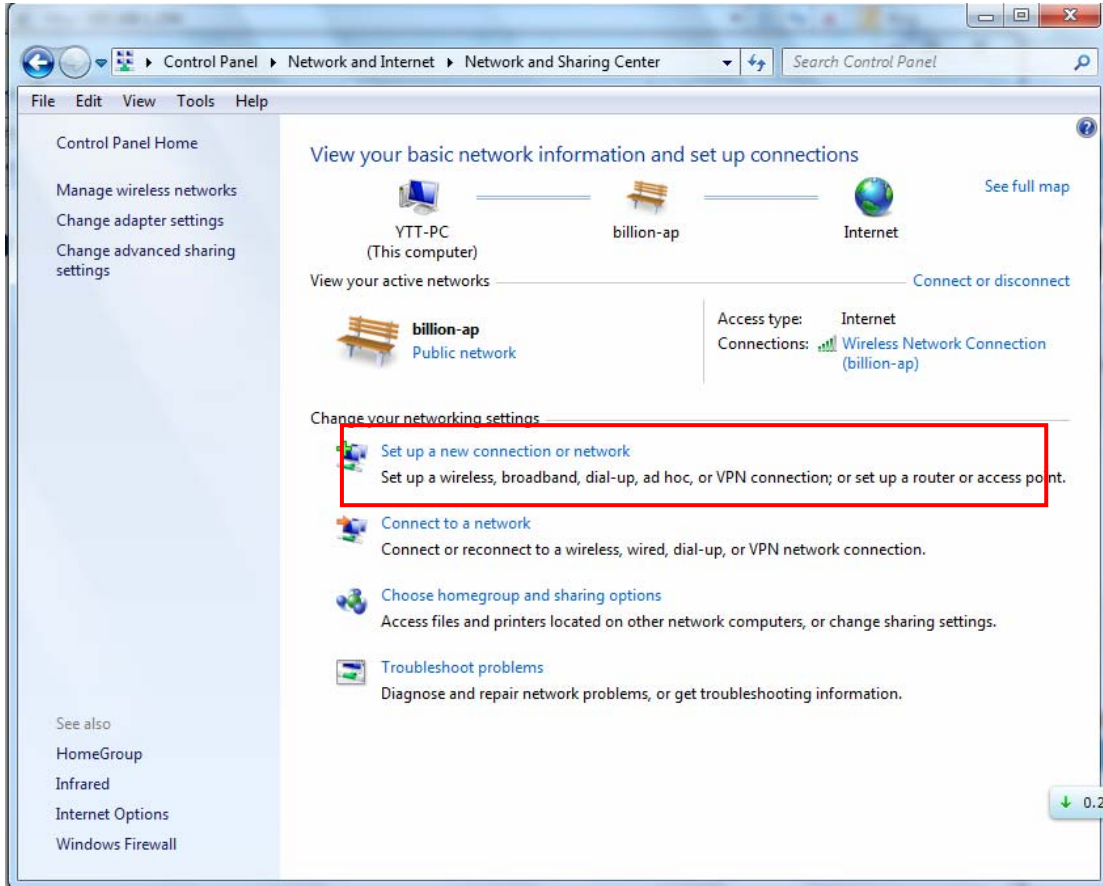
Peer Network IP Netmask

SET DELETE

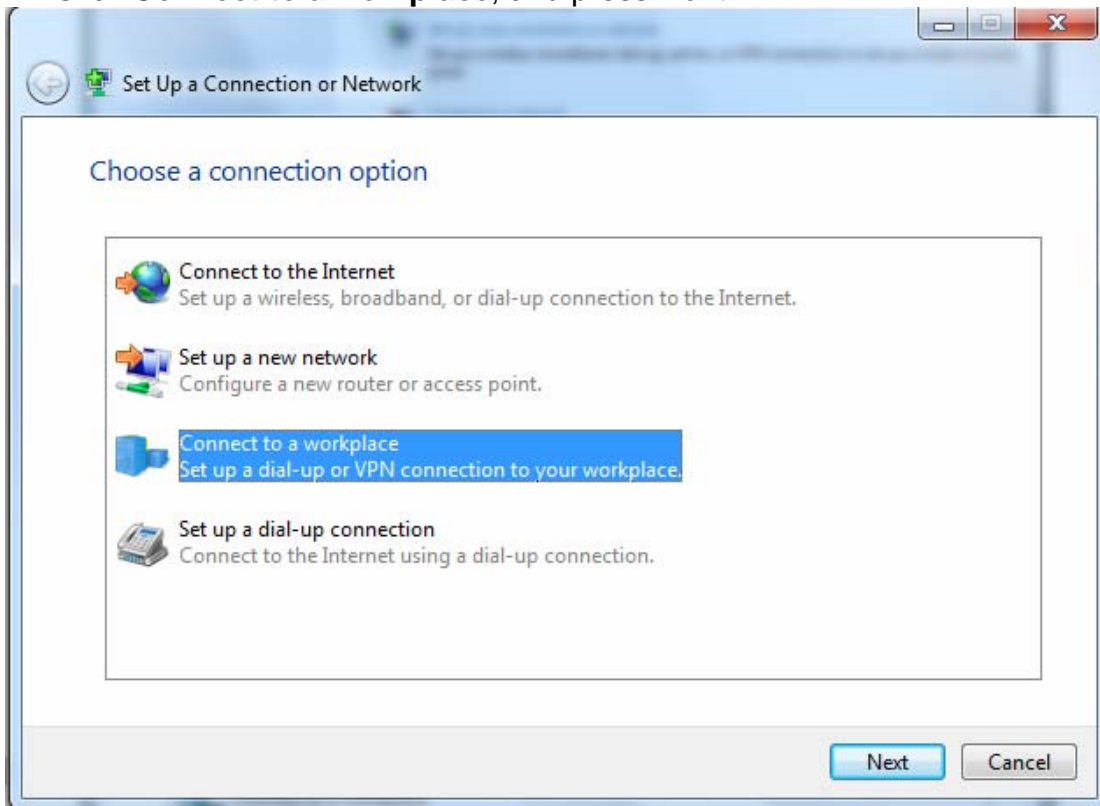
User	Connection Name	Active	Username	Connection Type	AssignIP
User1	test	Yes	test	Remote Access	192.168.1.2

Client Side:

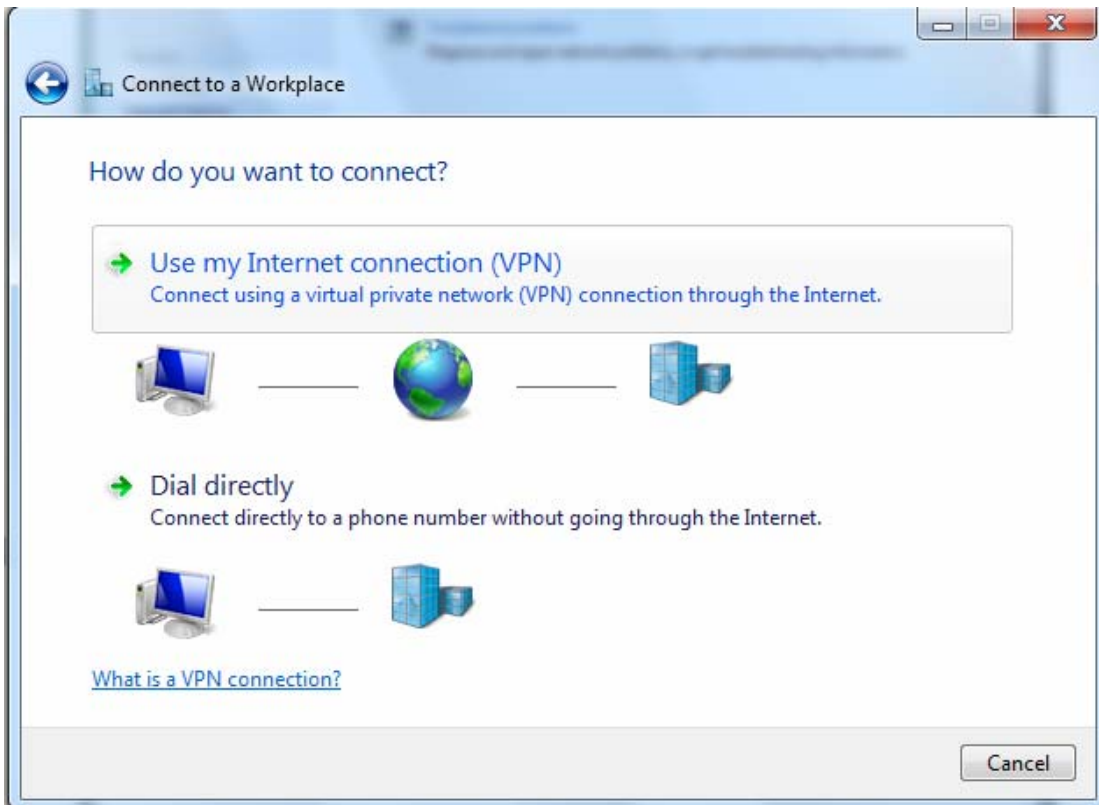
1. In Windows7 click **Start > Control Panel> Network and Sharing Center**, Click **Set up a new connection or network**.



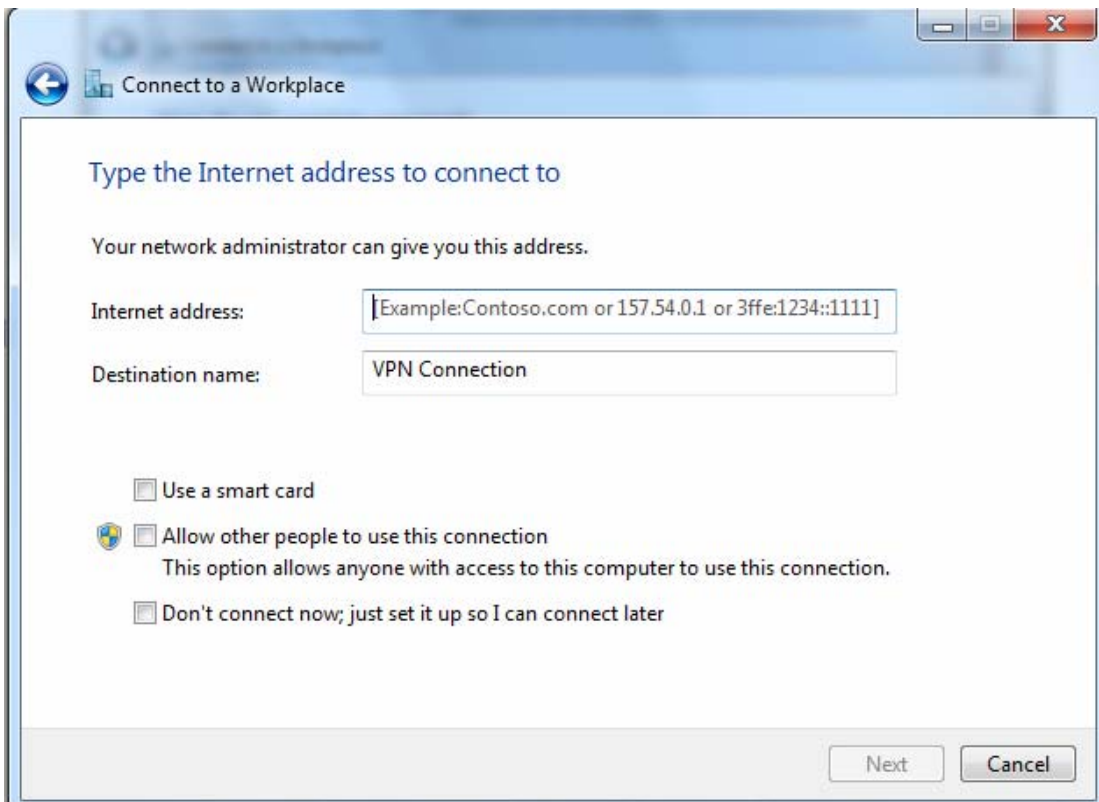
2. Click **Connect to a workplace**, and press **Next**.

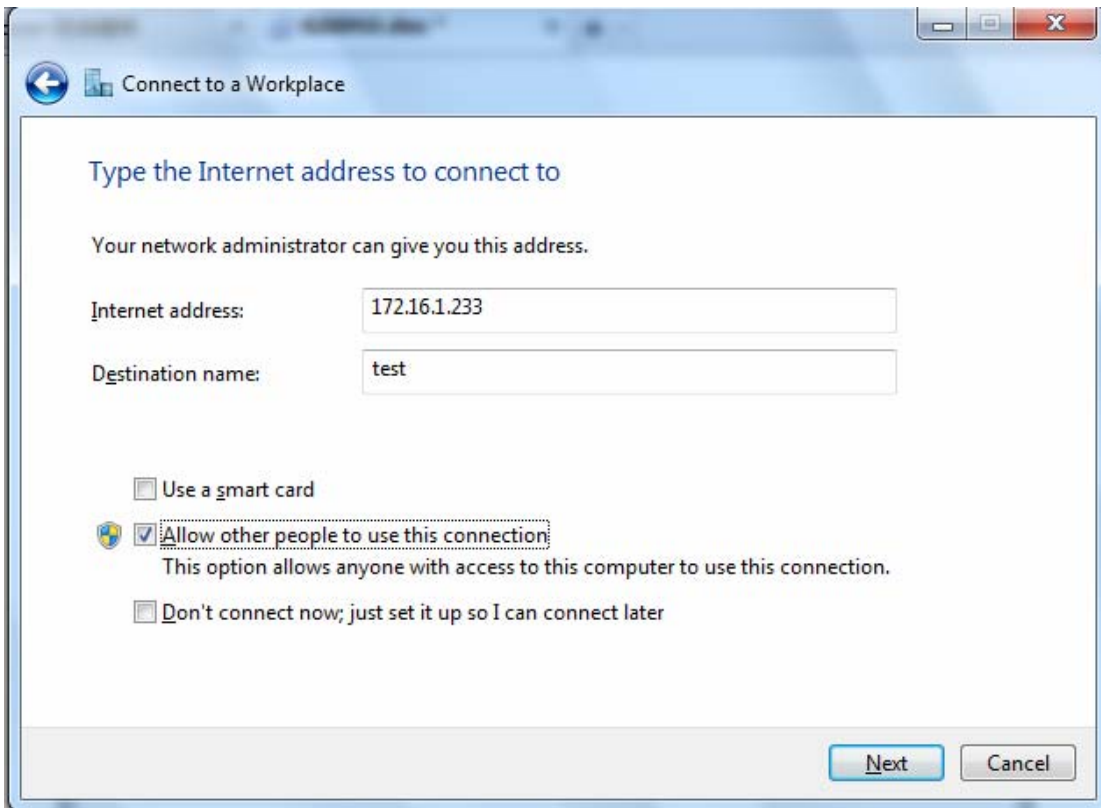


3. Select **Use my Internet connection (VPN)** and press **Next**.

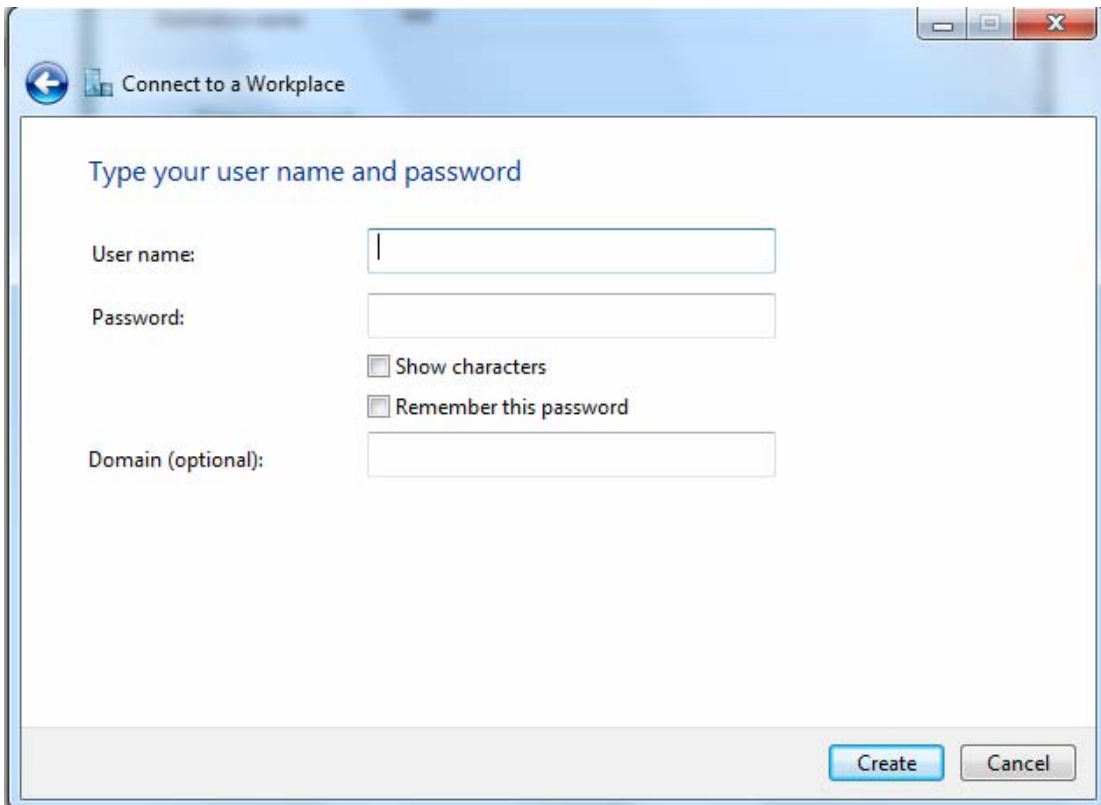


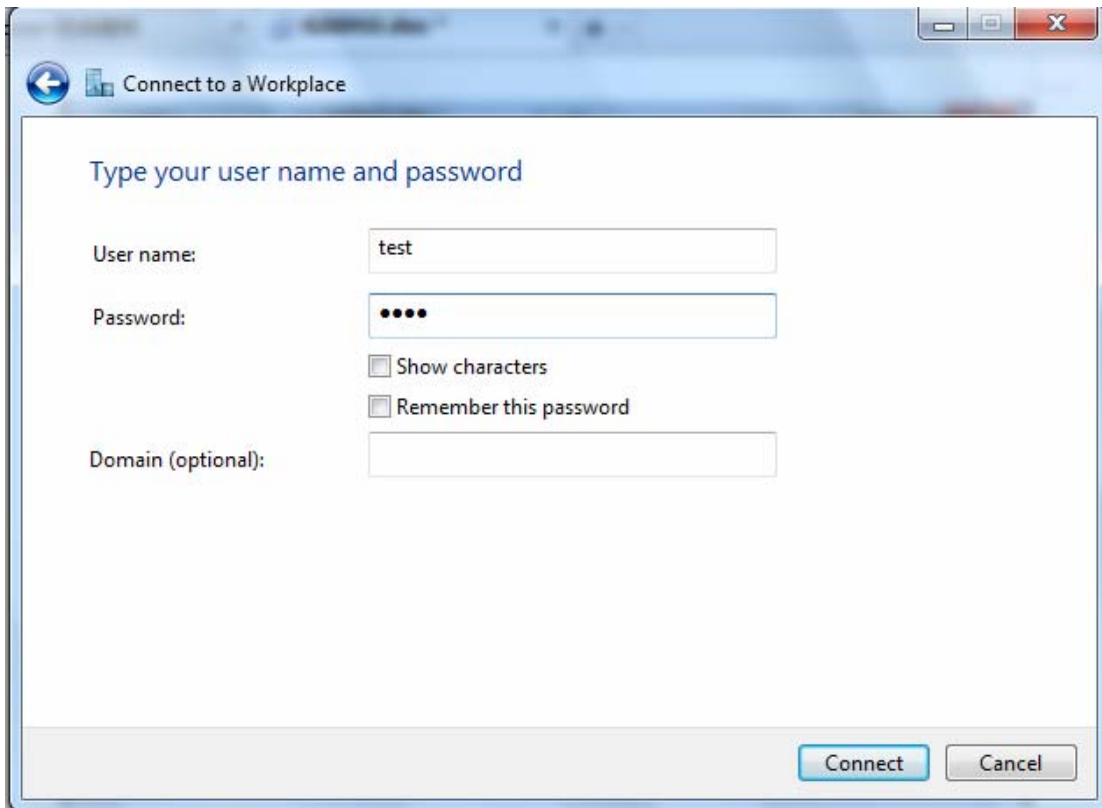
4. Input **Internet address** and **Destination name** for this connection and press **Next**.



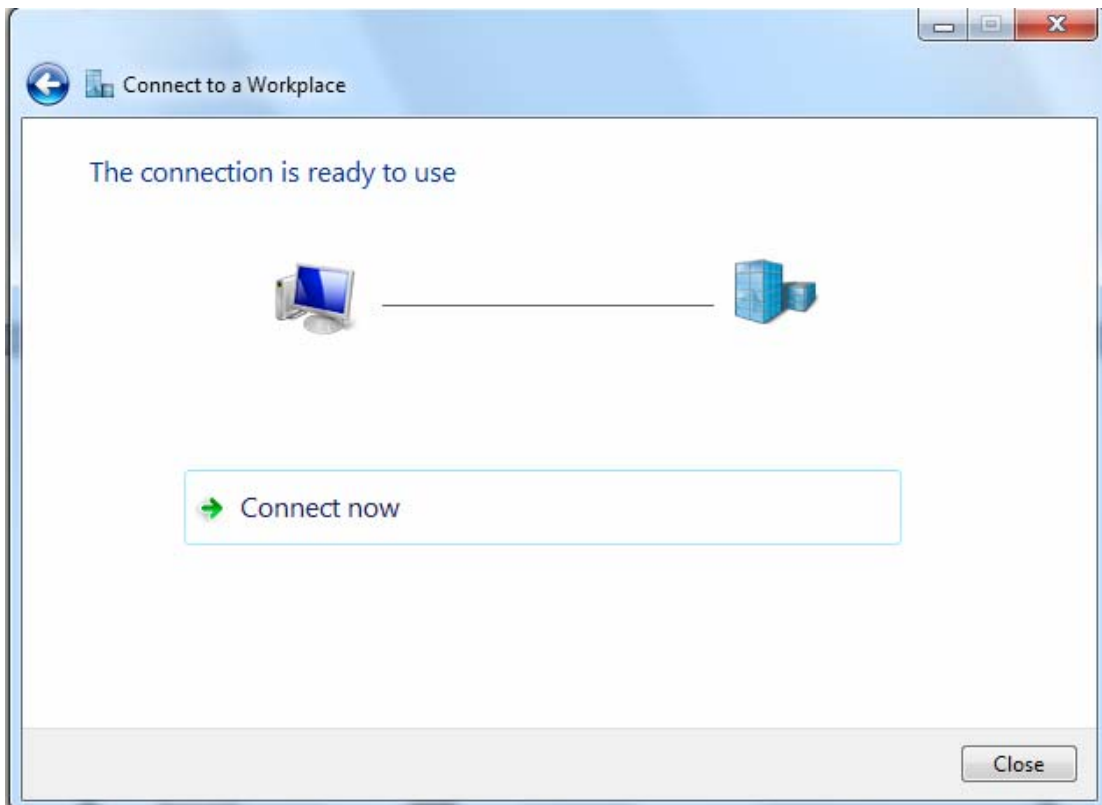


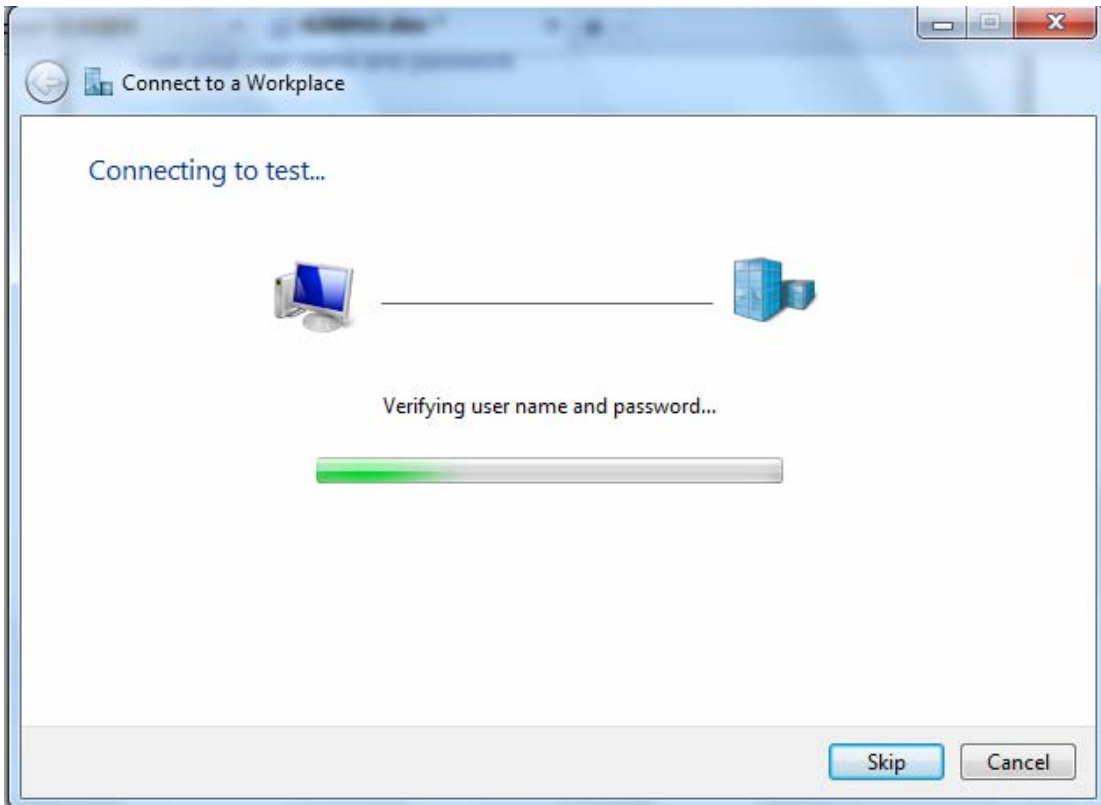
5. Input the account (**user name** and **password**) and press **Create**.



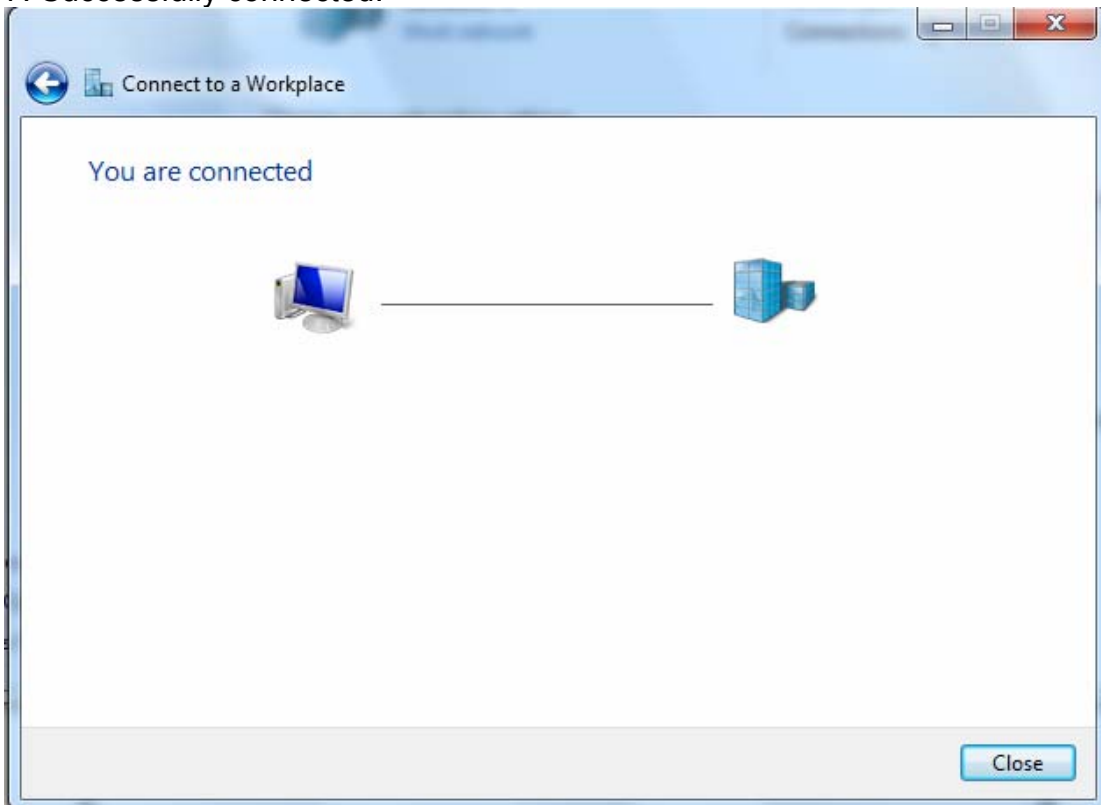


6. Connect to the server.

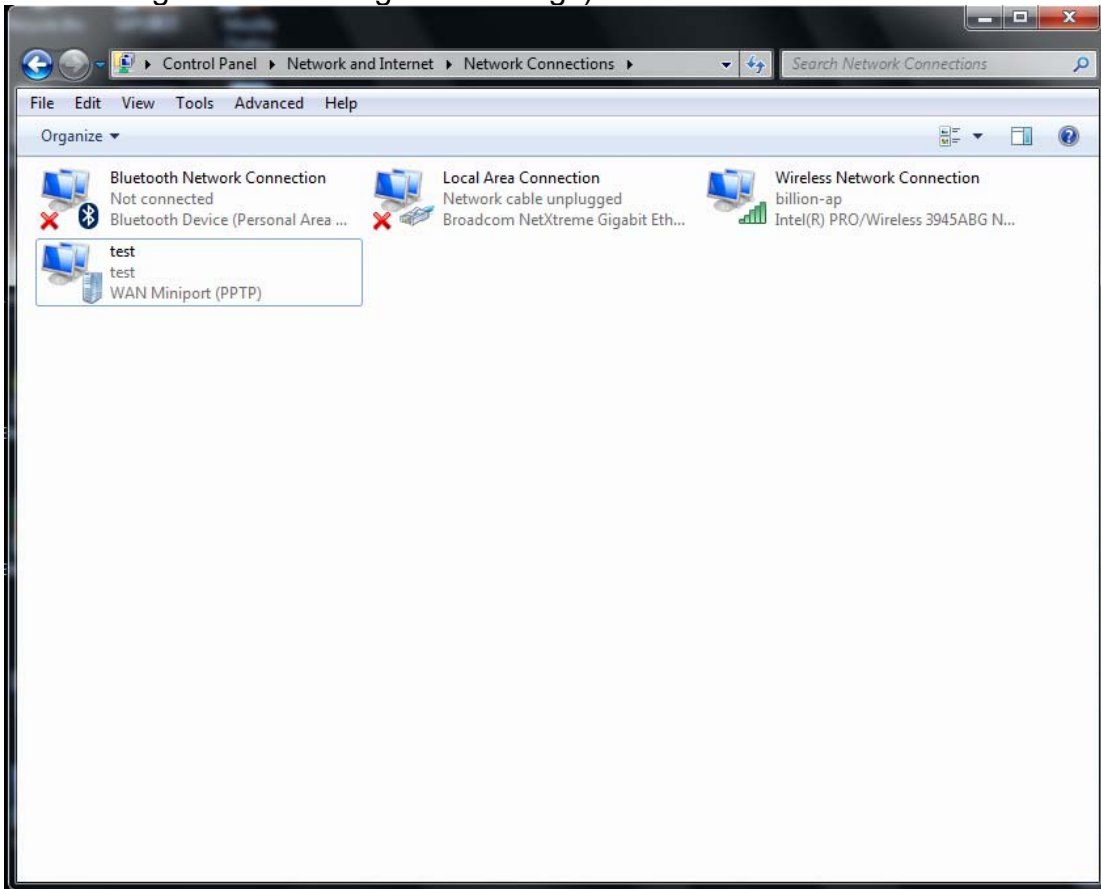


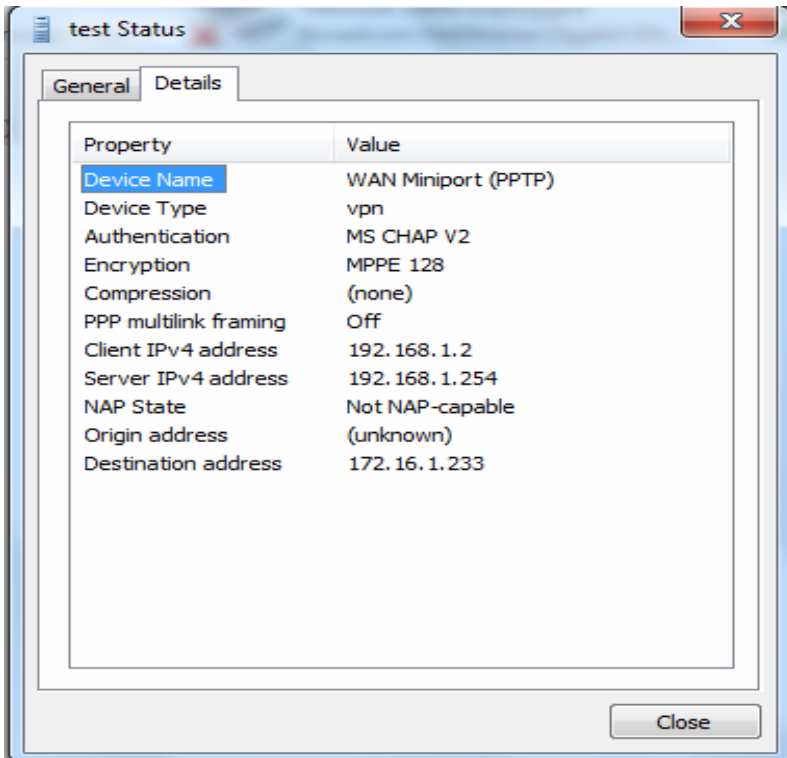
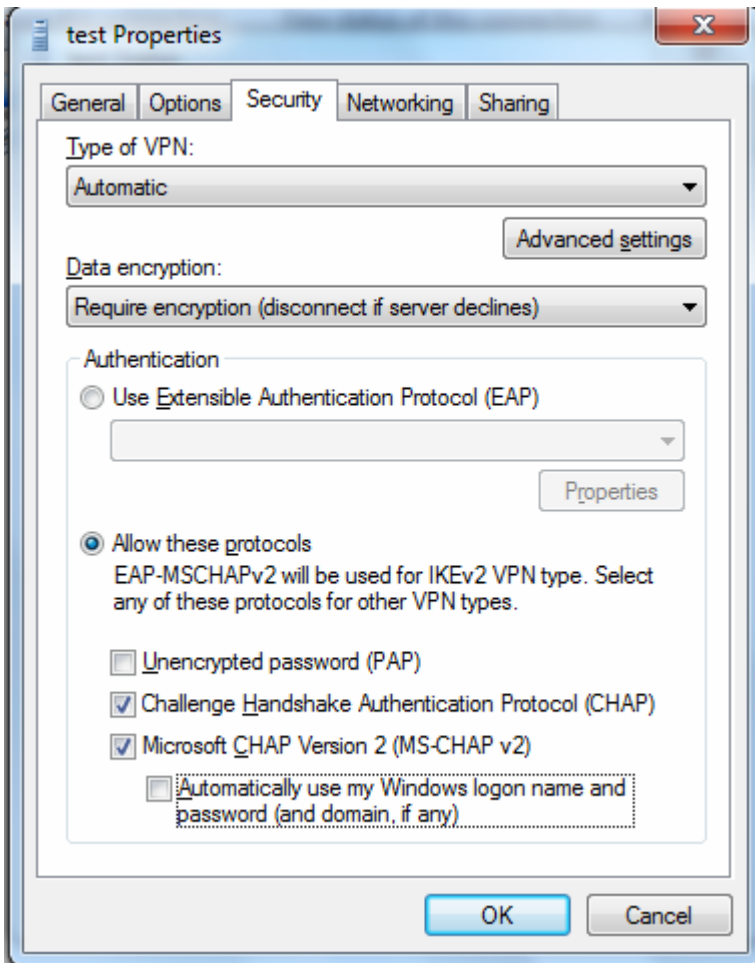


7. Successfully connected.



PS: You can also go to **Network Connections** shown below to check the detail of the connection. Right click “test” icon, and select “Properties” to change the security parameters (if the connection fails, users can go here to change the settings)

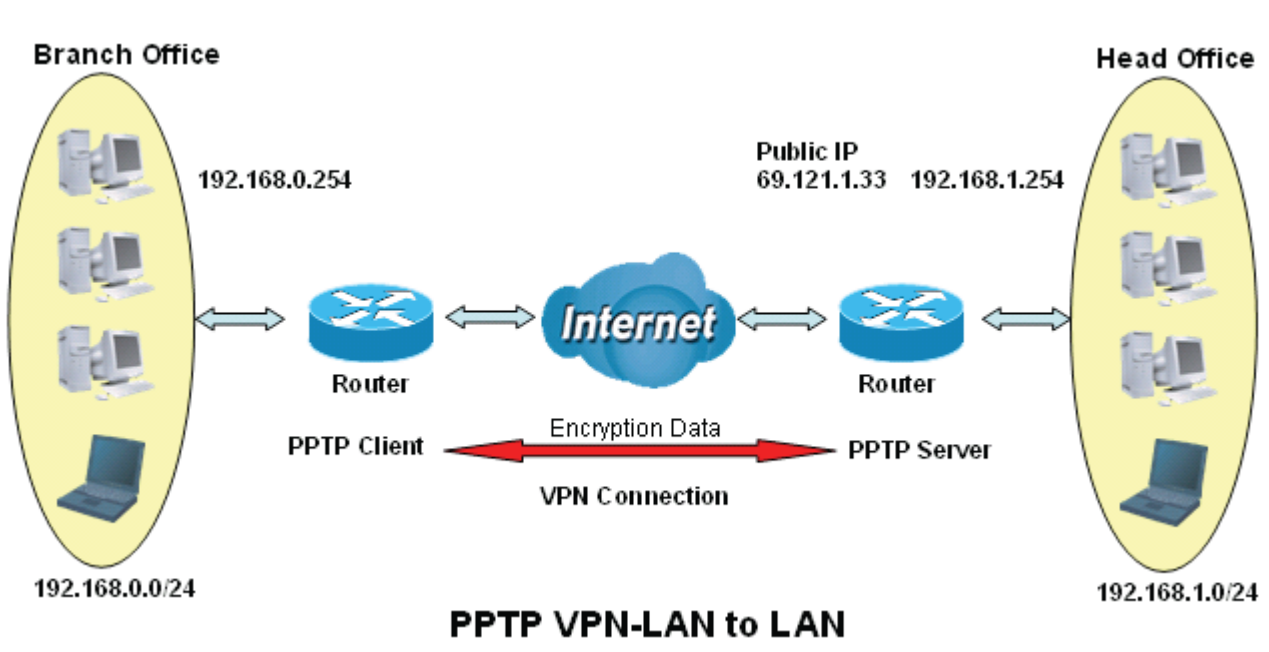




Example: Configuring a LAN-to-LAN PPTP VPN Connection

The branch office establishes a PPTP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch offices accordingly.

Note: Both office LAN networks must be in different subnets with the LAN-LAN application.



Server side: Head Office

Set an account of “test” in PPTP server waiting to connect in from PPTP client (192.168.0.0/24). The exact authentication type and other parameters are shown below.

Configuration

PPTP Server

Parameters

Enable Yes No

Auth.Type MPPE 128bit Encryption

MS-DNS 192.168.1.254

User select User1

Connection Name HO Active Yes No

Username test Password

Connection Type LAN to LAN Private IP Address Assigned to Dialin user 192.168.1.2

Peer Network IP 192.168.0.0 Netmask 255.255.255.0

SET DELETE

User	Connection Name	Active	Username	Connection Type	AssignIP
User1	HO	Yes	test	Lan to Lan	192.168.1.2

Edit	Name	Tunnel	Connection Type	Peer Network IP	Peer Netmask	Delete
<input type="radio"/>	HO	Enable	LAN to LAN	192.168.0.0	255.255.255.0	<input type="checkbox"/>

Client Side: Branch Office

The client user can set up a session connecting to the PPTP server.

Configuration

PPTP Client

Parameters

User select	<input type="text" value="User1"/>	Connection Name	<input type="text" value="BO"/>
Auth.Type	<input type="text" value="MPPE 128bit Encryption"/>	Active	<input checked="" type="radio"/> Yes <input type="radio"/> No
Username	<input type="text" value="test"/>	Password	<input type="text" value="••••"/>
Connection Type	<input type="text" value="LAN to LAN"/>	Server IP	<input type="text" value="69.121.1.33"/>
Peer Network IP	<input type="text" value="192.168.1.0"/>	Netmask	<input type="text" value="255.255.255.0"/>

User	Connection Name	Active	Username	Connection Type	ServerIP
User1	BO	Yes	test	Lan to Lan	69.121.1.33

L2TP (6300VNOZ only)

L2TP, Layer 2 Tunneling Protocol is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself; it relies on an encryption protocol that it passes within the tunnel to provide.

Note: 4 sessions for dial-in connections and 4 sessions for dial-out connections

Configuration

▼ L2TP

Name	<input type="text"/>
Rule Index	1 ▼
Type	Dial in ▼
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Private IP Address Assigned to Dialin user	<input type="text"/>
Auth. Type(Chap means auto)	Chap(Auto) ▼
Tunnelauth	<input type="checkbox"/> Enable
Secret	<input type="text"/>
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	<input type="text"/>
Local Host Name	<input type="text"/>
Connection Type	Remote Access ▼

SET
DELETE
CANCEL

L2TP Listing						
#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork

Name: User-defined name for the connection.

Rule Index: The Index to mark the session.

Type: Select Dial Out if you want your router to operate as a client (connecting to a remote VPN Server, e.g, your office server), while choose Dial In to operate as a VPN server.

❖ Dial in

Type	Dial in ▾
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Private IP Address Assigned to Dialin user	<input type="text"/>
Auth. Type(Chap means auto)	Chap(Auto) ▾
Tunnelauth	<input type="checkbox"/> Enable
Secret	<input type="text"/>
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	<input type="text"/>
Local Host Name	<input type="text"/>
Connection Type	Remote Access ▾

Active: To enable or disable the tunnel.

Username: Please input the username for this account.

Password: Please input the password for this account.

Private IP Address Assigned to Dialin user: The private IP to be assigned to dialin user by L2TP server. The IP should be in the same subnet as local LAN, and should not be occupied.

Auth. Type: Default is Auto(CHAP, Challenge Handshake Authentication Protocol) if you want the router to determine the authentication type to use, or else manually specify PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

Tunnelauth: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret: The secure password length should be 16 characters which may include numbers and characters.

Remote Host Name: Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

Local Host Name: Enter hostname of Local VPN device that is connected / establishes a VPN tunnel.

Connection Type: Remote Access or LAN to LAN. If “LAN to LAN” is selected, enter the peer network information, such as network address and netmask.

❖ Dial out

Type	Dial out ▼
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text"/>
Password	<input type="text"/>
Server IP Address	<input type="text"/>
Auth. Type(Chap means auto)	Chap(Auto) ▼
Tunnelauth	<input type="checkbox"/> Enable
Secret	<input type="text"/>
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	<input type="text"/>
Local Host Name	<input type="text"/>
Connection Type	Remote Access ▼

Active: To enable or disable the tunnel.

Username: Enter the username provided by your VPN Server.

Password: Enter the password provided by your VPN Server.

Server IP Address: Enter the IP address of your VPN Server.

Auth. Type: Default is Auto(CHAP, Challenge Handshake Authentication Protocol) if you want the router to determine the authentication type to use, or else manually specify PAP (Password Authentication Protocol) if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server). When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client.

Tunnelauth: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret: The secure password length should be 16 characters which may include numbers and characters.

Active as default route: Enabled to let the tunnel to be the default route for traffic, under this circumstance, all packets will be forwarded to this tunnel and routed to the next hop.

Remote Host Name: Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

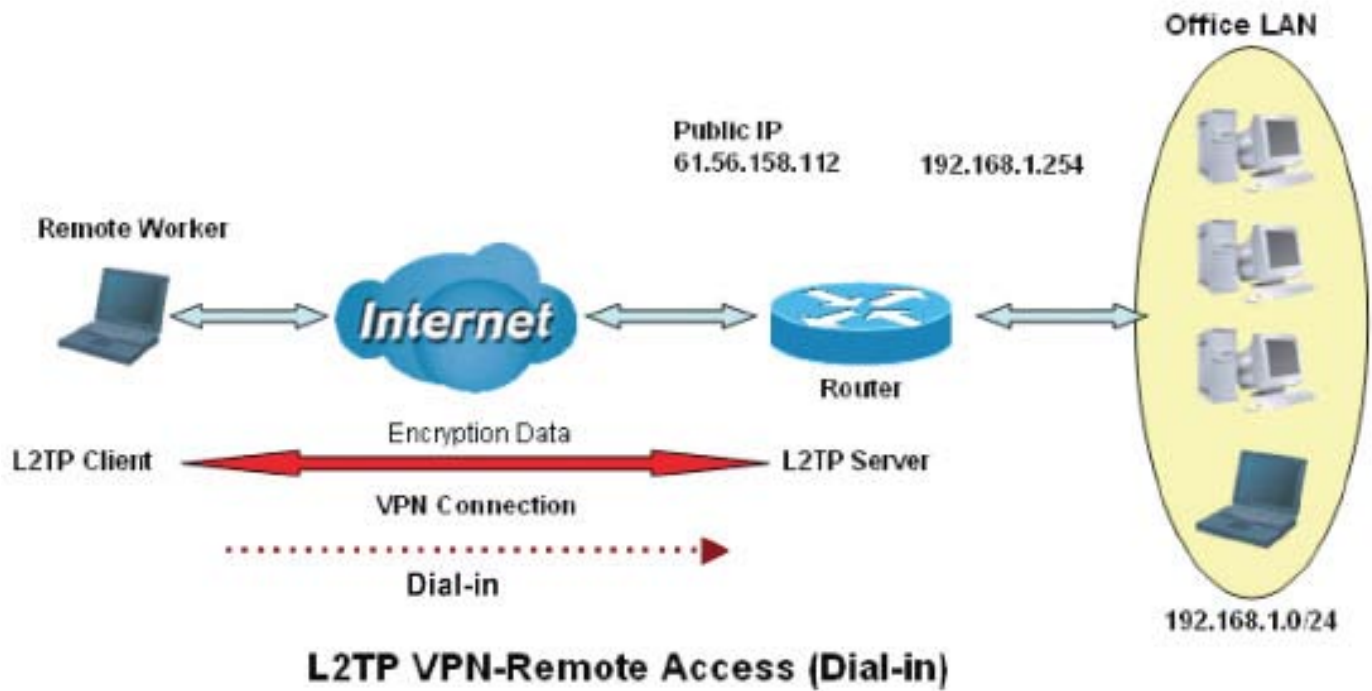
Local Host Name: Enter hostname of Local VPN device that is connected / establishes a VPN tunnel.

Connection Type: Remote Access or LAN to LAN. If “LAN to LAN” is selected, enter the peer network information, such as network address and netmask

Examples:

1. Configuring a L2TP VPN - Remote Access Dial-in Connection

A remote worker establishes a L2TP VPN connection with the head office using Microsoft's VPN Adapter (included with Windows XP/2000/ME, etc.). The router is installed in the head office, connected to a couple of PCs and Servers.



Configuring L2TP VPN in the Office

The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

The screenshot shows the L2TP configuration page. The form fields are as follows:

- Name: VPN_Server
- Rule Index: 1
- Type: Dial in
- Active: Enable Disable
- Username: test
- Password: [masked]
- Private IP Address Assigned to Dialin user: 192.168.1.200
- Auth. Type(Chap means auto): Chap(Auto)
- Tunnelauth: Enable
- Secret: [empty]
- Active as default route: Enable
- Remote Host Name: [empty]
- Local Host Name: [empty]
- Connection Type: Remote Access

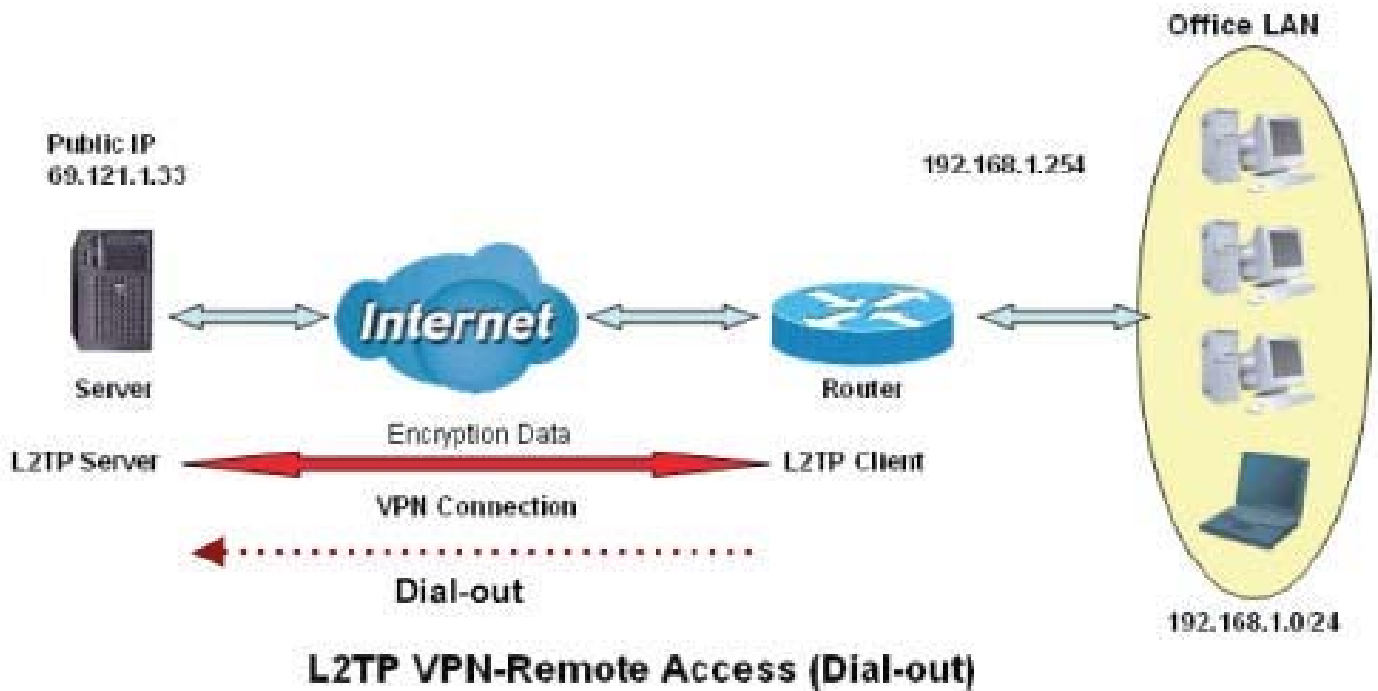
Buttons: SET, DELETE, CANCEL

#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
1	Yes	VPN_Server	remote access	dialin	chap	

Function		Description
Name	VPN_Server	Give a name of L2TP Connection
Connection Type	Remote Access	Select Remote Access from the Connection Type drop-down menu
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	192.168.1.200	An IP assigned to the remote client
Username	test	Enter the username and password to authenticate a remote client
Password	test	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases

2. Configuring a Remote Access L2TP VPN Dial-out Connection

A company's office establishes a L2TP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



Configuring L2TP VPN in the Office

Configuration

▼ L2TP

Name	VPN_Client
Rule Index	1
Type	Dial out
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test
Password	••••
Server IP Address	69.121.1.33
Auth. Type(Chap means auto)	Chap(Auto)
Tunnelauth	<input type="checkbox"/> Enable
Secret	
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	
Local Host Name	
Connection Type	Remote Access

SET DELETE CANCEL

L2TP Listing

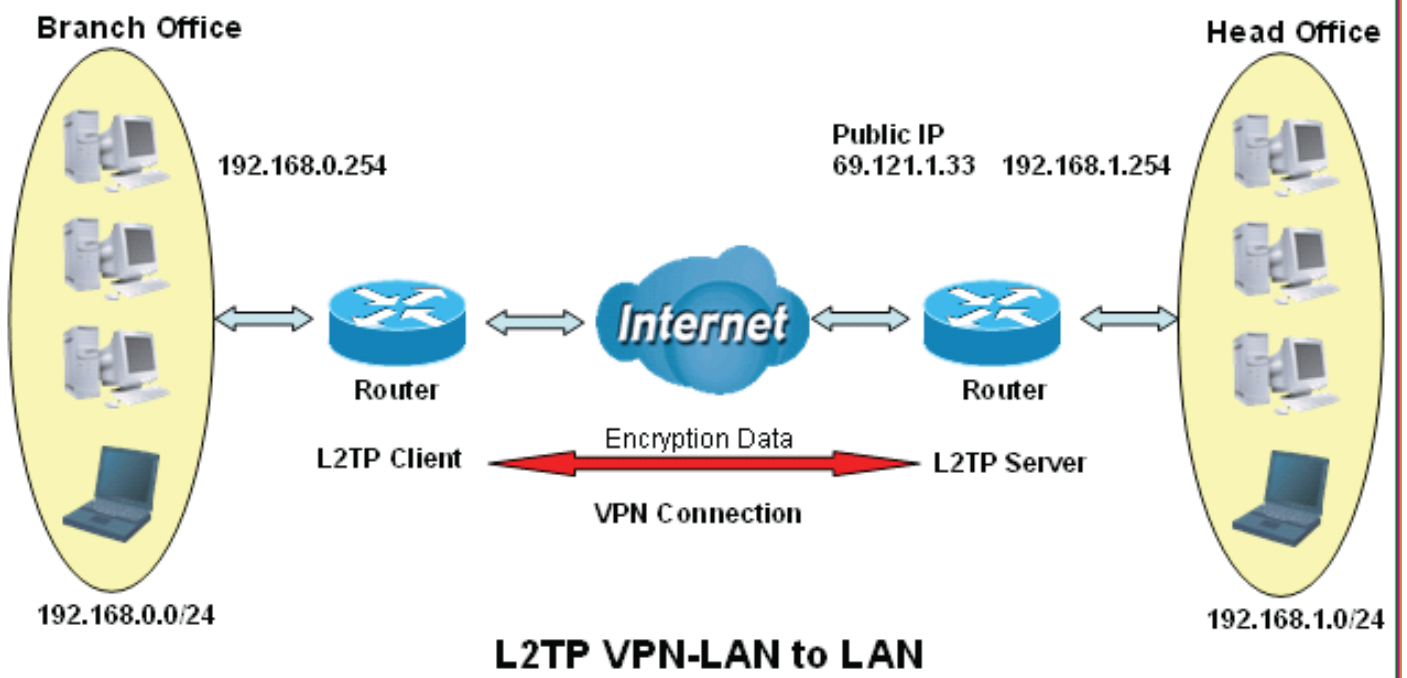
#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
1	Yes	VPN_Client	remote access	dialout	chap	

Function		Description
Name	VPN_Client	Give a name of L2TP Connection
Connection Type	Remote Access	Select Remote Access from the Connection Type drop-down menu
Type	Dial out	Select Dial out from the Type drop down menu
IP Address (or Domain Name)	69.121.1.33	A Dialed Server IP
Username	test	An assigned username and password
Password	test	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases

Example: Configuring L2TP LAN-to-LAN VPN Connection

The branch office establishes a L2TP VPN tunnel with head office to connect two private networks over the Internet. The routers are installed in the head office and branch office accordingly.

Note: Both office LAN networks must be in different subnets with the LAN-LAN application.



Configuring L2TP VPN in the Head Office

The IP address 192.168.1.200 will be assigned to the router located in the branch office. Please make sure this IP is not used in the head office LAN.

L2TP

Name	VPN_Server
Rule Index	1
Type	Dial in
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	test
Password	••••
Private IP Address Assigned to Dialin user	192.168.1.200
Auth. Type(Chap means auto)	Chap(Auto)
Tunnelauth	<input type="checkbox"/> Enable
Secret	
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	
Local Host Name	
Connection Type	Lan to Lan
PeerNetwork	192.168.0.0
Netmask	255.255.255.0

L2TP Listing						
#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
1	Yes	VPN_Server	lan to lan	dialin	chap	192.168.0.0

Function		Description
Name	HeadOffice	Give a name of L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type
Type	Dial in	Select Dial in from the Type drop down menu
IP Address	192.168.1.200	IP address assigned to branch office network
Peer Network IP	192.168.0.0	Branch office network
Username	test	An assigned username and password to authenticate branch office network
Password	test	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases

Configuring L2TP VPN in the Branch Office

The IP address 69.1.121.33 is the Public IP address of the router located in head office. If you registered the DDNS (please refer to the DDNS section of this manual), you can also use the domain name instead of the IP address to reach the router.

▼ L2TP

Name	<input type="text" value="VPN_Client"/>
Rule Index	<input type="text" value="1"/>
Type	<input type="text" value="Dial out"/>
Active	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="test"/>
Password	<input type="password" value="••••"/>
Server IP Address	<input type="text" value="69.121.1.33"/>
Auth. Type(Chap means auto)	<input type="text" value="Chap(Auto)"/>
Tunnelauth	<input type="checkbox"/> Enable
Secret	<input type="text"/>
Active as default route	<input type="checkbox"/> Enable
Remote Host Name	<input type="text"/>
Local Host Name	<input type="text"/>
Connection Type	<input type="text" value="Lan to Lan"/>
PeerNetwork	<input type="text" value="192.168.1.0"/>
Netmask	<input type="text" value="255.255.255.0"/>

L2TP Listing						
#	Active	Name	Connection Type	Type	Auth. Type	PeerNetwork
1	Yes	VPN_Client	lan to lan	dialout	chap	192.168.1.0

Function	Description	
Name	VPN_Client	Give a name of L2TP Connection
Connection Type	LAN to LAN	Select LAN to LAN from the Connection Type
Type	Dial out	Select Dial out from the Type drop down menu
IP Address	69.121.1.33	IP address of the server
Peer Network IP	192.168.1.0	Head office network
Netmask	255.255.255.0	
Username	test	An assigned username and password to authenticate branch office network
Password	test	
Auth. Type	Chap (Auto)	Keep this as the default value for most cases

Interface Grouping (6300VNPZ only)

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Similarly, they may also have been split into two different groups, even if they are on the same switch.

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 **Save** button.

The screenshot shows the 'Configuration' page for 'Interface Grouping'. The 'Interface Grouping' section is currently set to 'Deactivated'. The 'Group Index' is set to 0. The 'EWAN Service' is set to EWAN0. The 'Ethernet LAN' section shows three checkboxes for LAN1, LAN2, and LAN3. The 'Wireless LAN' section shows one checkbox for WLAN1. The 'Group Summary' section has a 'Group Summary' button. At the bottom of the configuration area are 'Save' and 'Delete' buttons.

Interface Grouping: Select **Yes** to enable Interface Grouping feature.

Group Index: The index number indicating the current group ranging from 0 to 15.

EWAN Service: The available EWAN interface. Move to [Interface Setup](#) to add other EWAN interface.

Ethernet LAN: The available Ethernet ports.

Wireless LAN: The available wireless port(s).

Group Summary: Press **PortBinding Summary** to check the current group information.

Example: Create two EWAN services, Service0 (PPPoE) and Service1 (Bridge).

Status			
Service Information Summary			
WAN 0	Active	ISP	IP Address
0	Yes	Dynamic	Dynamic
1	Yes	Bridge	N/A
2	No	Bridge	N/A
3	No	Bridge	N/A
4	No	Bridge	N/A
5	No	Bridge	N/A
6	No	Bridge	N/A
7	No	Bridge	N/A

You are going to group the ports and services into two working group, as shown below.

Group Index	Group Port
0	EWAN0, LAN1, LAN2, WLAN1
1	EWAN1, LAN3

Configuration

▼ Interface Grouping

Interface Grouping Activated Deactivated

Group Index: 0

EWAN Service: EWAN0 EWAN1

Ethernet LAN: LAN1 LAN2 LAN3

Wireless LAN: WLAN1

Group Summary: [Group Summary](#)

[Save](#) [Delete](#)

Configuration

▼ Interface Grouping

Interface Grouping Activated Deactivated

Group Index: 1

EWAN Service: EWAN0 EWAN1

Ethernet LAN: LAN1 LAN2 LAN3

Wireless LAN: WLAN1

Group Summary: [Group Summary](#)


[Save](#) [Delete](#)

Click **Group Summary** to show the configuration results.

Group ID	Group port
0	wan0_0,e1,e2,w1
1	wan0_1,e3

Port Isolation


Port isolation is a mechanism to allow or block devices in one port (indicates the LAN1 - LAN3 and WLAN1 - WLAN4, need to enable multiple SSID in wireless section) to access other devices in other ports. By default, all ports (LAN port and WLAN port) are sharing one group, and devices in all these ports can have access to each other.

Configuration 

▼ Port Isolation

Port Group	Ethernet LAN			Wireless LAN
	LAN1	LAN2	LAN3	WLAN1
Group 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The most typical one example is to isolate all port from each other shown below. Each port has its own group, under this circumstance, devices connected to each port have no access to other devices connected to other ports. This is a special example, and users can change the settings to determine how the ports are belonged to the group.

Configuration 

▼ Port Isolation

Port Group	Ethernet LAN			Wireless LAN			
	LAN1	LAN2	LAN3	WLAN1	WLAN2	WLAN3	WLAN4
Group 1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Time Schedule

The Time Schedule supports up to **16** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet.

Configuration

Time Schedule

Rule Index: 0

Rule Name: TimeSlot1

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00

Save

Time Index: The rule index (0-15) for identifying each timeslot.

Name: User-defined identification for each time period.

Day of Week: Mon. to Sun. Specify the time interval for each timeslot from “Day of Week”. For example, user can add a timeslot named “TimeSlot1” which features a period from 9:00 of Monday to 18:00 of Tuesday.

Configuration

Time Schedule

Rule Index: 0

Rule Name: TimeSlot1

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	09:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	24:00	18:00	00:00	00:00	00:00	00:00	00:00

Save

Another TimeSlot2 spanning from 09:00 to 18:00 of Friday

Configuration

Time Schedule

Rule Index: 1

Rule Name: TimeSlot2

	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Start Time	00:00	00:00	00:00	00:00	09:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	18:00	00:00	00:00

Save

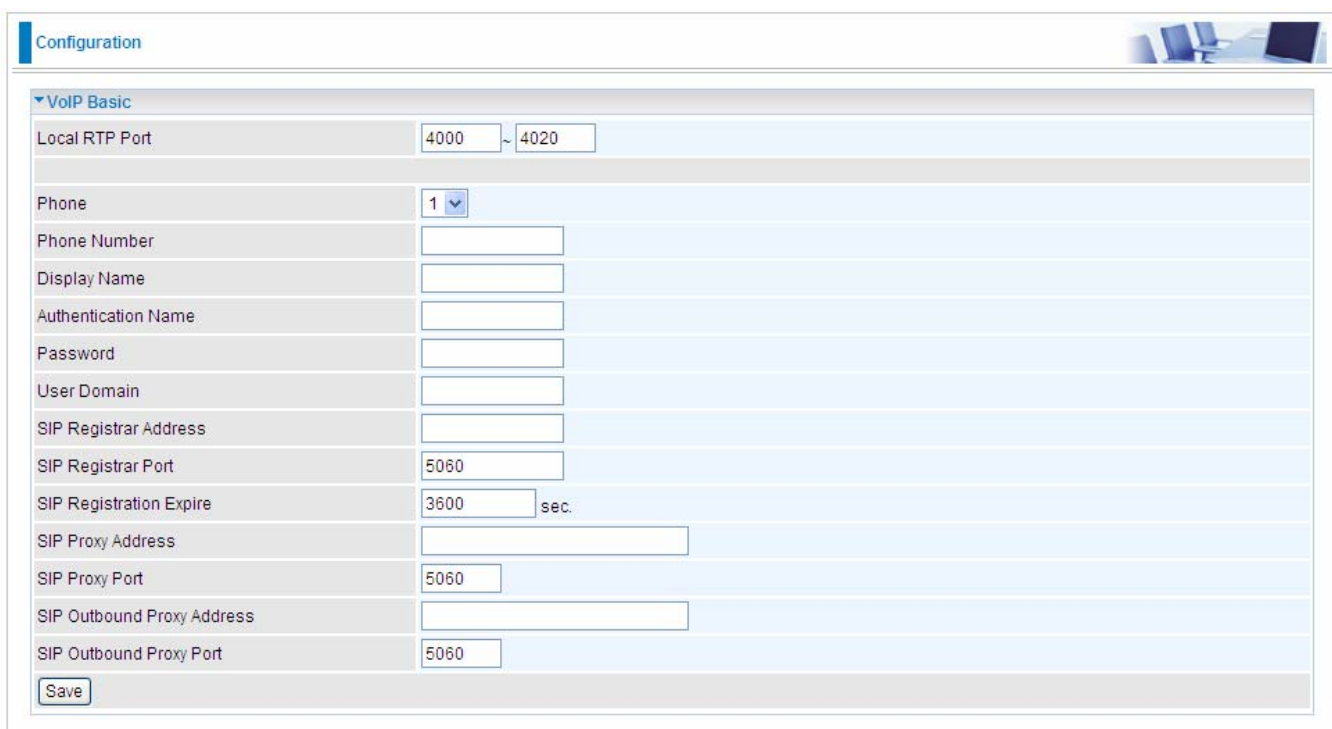
VoIP

VoIP, or Voice over Internet Protocol, enables telephone calls through existing internet connections instead of going through the traditional PSTN (Public Switched Telephone Network). It is not only cost-effective, especially for a long-distance call, but also top quality voice calls over the internet.

This section covers **Basic**, **Media**, **Advanced**, **Speed Dial**, and **Call Features** of VoIP.

Basic

Register to a SIP service provider is an essential step before making the VoIP call. You can find out this information from your SIP service provider.



Local RTP Port	4000 ~ 4020
Phone	1
Phone Number	
Display Name	
Authentication Name	
Password	
User Domain	
SIP Registrar Address	
SIP Registrar Port	5060
SIP Registration Expire	3600 sec.
SIP Proxy Address	
SIP Proxy Port	5060
SIP Outbound Proxy Address	
SIP Outbound Proxy Port	5060

Save

Local RTP Port: Set the local RTP port range used to receive voice packet. This setting applies to both the phone ports, Phone_1 and Phone_2, and these phone ports share the same local RTP port.

Phone: Select “1”, the following parameters will be applicable to Phone1. In BiPAC 6300VNP(O)Z, Phone_1 and Phone_2 are allowed to be of different characteristics, including different SIP registrar. You need to configure individually for phone1 and phone 2 and can have up to 2 different VoIP accounts.

Phone Number: Set your phone number or outgoing call number, which is usually obtained when registering in your ITSP. It is used for destination to identify which this call is made from.

Display Name: A user-friendly display name for the phone number to be easily identified.

Authentication Name: Set the account used to register, usually the Phone Number.

Password: Set the registering account password.

User Domain: Set the SIP Registrar Domain name you are going to register to, usually just the SIP registrar address.

SIP Registrar Address: Enter the SIP registrar address where offers the service of registering the

VoIP account. It is definitely a VoIP server.

SIP Registrar Port: Type the port; it will listen to register requests from VoIP devices.

SIP Registration Expire: Set the time interval. The device can update (usually re-login the account) the VoIP account information with the SIP server very the time interval.

SIP Proxy Address: Enter the SIP proxy address provided by your ITSP. When destination and source phones are not sharing the same SIP registrar domain, the SIP proxy is needed to deliver call information and make the communication through.

SIP Proxy Port: Set the SIP proxy port.

SIP Outbound Proxy Address: Set the SIP outbound proxy address. It is usually used to realize the communication between two phones when at least one of them is located behind a NAT router.

SIP Outbound Proxy Port: Set the SIP Outbound proxy port.

Media

Media offers for kinds of codec, G.711 u-law, G.711 A-law, G.729, G.726, from greatest to lowest in priority.

Priority	Codec	Packetization Time
Priority 1	G.711 u-law	20
Priority 2	G.711 A-law	20
Priority 3	G.729	20
Priority 4	G.726	20

Phone: Select to set the following configurations for Phone_1 or Phone_2. When phone1 is selected, the following set media codec will be applied to phone_1.

T.38: T.38 relay is a way to permit faxes to be transported across IP networks between existing fax terminals. Click Enable to allow transmission of fax over IP network between two fax machines. If T.38 is disabled, the analog fax signal is transmitted as the normal audio data. If T.38 relay is enabled, the fax signal is converted to T.38 signal.

- ▶ **G.711u-Law:** It is a basic non-compressed encoder and decoder technique. μ -LAW uses pulse code modulation (PCM) encoder and decoder to convert 14-bit linear sample.
- ▶ **G.711A-LAW:** It is a basic non-compressed encoder and decoder technique. A-LAW uses pulse code modulation (PCM) encoder and decoder to convert 13-bit linear sample into 8-bit value.
- ▶ **G.729:** It is used to encoder and decoder voice information into a single packet which reduces the bandwidth consumption.
- ▶ **G.726:** It is an [ITU-T ADPCM speech codec](#) standard covering the transmission of voice at rates of 32kbit/s.

Advanced

Advance section equipment the users with the ability to do some advanced settings to each phone port. Go on to see.

VoIP Advanced	
Region	CHN-China
Phone	1
Silence Suppression(VAD)	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Echo Cancellation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DTMF Transport Mode	Inband
Listening Volume	0 db (-6~6)
Speaking Volume	0 db (-6~6)

Save

Region: Select the exact region from the drop-down menu to adjust the phone custom in the exact region, like ring tone, busy tone, dial tone, etc, as different regions may have different phone using traditions. The setting is to be applied to both phone 1 and phone 2.

Phone: Select the phone 1 or Phone 2 to have the following configurations applied to the phone.

Silence Suppression (VAD): Enable to minimize the use of bandwidth by automatically decreasing transmission of background noise when the device detects on voice input by the user on the phone.

Echo Cancellation: Enable to cancel echo for the other side in communication so as to make a clear listening environment. In order to avoid the other side in communication hearing the echo, please enable echo cancellation.

DTMF Transport Mode: Select the DTMF mode.

Listening Volume: Adjust the volume of listener, -6 to 6, from lowest to highest.

Speaking Volume: Adjust the volume of microphone; -6 to 6, from lowest to highest.

Speed Dial

Speed Dial comes at hand to store frequently used telephone number(s) that you can press set ‘speed dial number’ instead of the exact dialing-out number on the phone keyboard to make a quick dialing.

The screenshot shows the 'Speed Dial' configuration page. At the top, there is a 'Configuration' header. Below it, the 'Speed Dial' section contains a form with the following fields:

- Index:** 0
- Phone:** 1 (selected from a dropdown)
- Speed Dial Number:** (empty text box)
- Phone Number:** (empty text box)
- Save:** (button)

Below the form is the 'Speed Dial List' table:

Index	Phone	Speed Dial Number	Phone Number	Edit	Drop
0		N/A			
1		N/A			
2		N/A			
3		N/A			
4		N/A			
5		N/A			
6		N/A			
7		N/A			
8		N/A			
9		N/A			

Index: The index to mark the speed dial number mapping, 0-9.

Phone: Select Phone 1 or Phone 2 to have your set speed dial number applied to the phone. If Phone_1 is selected, your set speed dial number is about to be applied to Phone_1.

Speed Dial Number: Set an easily remembered and simple number to replace the Phone number, it can be a sequence in varying length from 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9 *. #, but note * or # must be included in the sequence.

Phone Number: The complete destination number

Example: Save phone number 83455301 to the speed dial list.

The screenshot shows the 'Speed Dial' configuration page with the following values entered:

- Index:** 0
- Phone:** 1 (selected from a dropdown)
- Speed Dial Number:** 301#
- Phone Number:** 83455301
- Save:** (button)

Below the form is the updated 'Speed Dial List' table:

Index	Phone	Speed Dial Number	Phone Number	Edit	Drop
0	1	301#	83455301		
1		N/A			
2		N/A			
3		N/A			
4		N/A			
5		N/A			
6		N/A			
7		N/A			
8		N/A			
9		N/A			

When you want call 83455301 through phone 1, you can simply dial 301# to make your desired call.

Call Features

Call Features provides users with some advanced phone characteristics, including Call waiting, Conference Call, etc.

Call Features	
Phone	1 ▼
Call Waiting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Conference Call	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Anonymous Call	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Distinctive Ring	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Vertical Service Code (VSC)	
Pass VSC to Softswitch	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Return Call(Dial number: *69)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Redial(Dial number: *68)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Don't Disturb(Enable: *78, Disable: *79)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="Save"/>	

Phone: Select the phone 1 or Phone 2 to have the following characteristics applied to the phone.

Call Waiting: Enable to activate Call Waiting feature. When you are busy on a call with, for example, A, and another call comes in, B, while the Call Waiting feature is enabled, you can hear a hint sound indicating there is another call in for you to decide to answer B by pressing the “flash” button on the phone to keep the original call with A.

Conference Call: Enable to allow 3-way conference call. Please note, only 3 parties are allowed (device, A, and B).

Anonymous Call: This feature enables you to restrict your phone number from displaying to the called party. When enabled, your phone number will be withheld and not be revealing to the called party.

Distinctive Ring: This call feature is only available from a VoIP Service Provider which enables each telephone number to have a distinctive ring sound.

Note: Before enabling this feature, please consult with your VoIP Service Provider to be sure it can be supported.

There is a ringtone list available in the BiPAC 6300VNP(O)Z, after enabling this feature, your BiPAC 6300VNP(O)Z will adapt a specific ring pattern on the list requested by your VoIP Service Provider for a specific telephone number.

When it is being disabled, all income calls will adapt the default ringtone for all telephone lines.

Pass VSC to Softswitch:

- ▶ **Enable** to pass VSC(Vertical Service Code) to the SIP server of ITSP which allows the SIP server to handle all its unique calling features such as Return Call, Call Redial, Don't Disturb, etc. Under this circumstance, users need to pay for such service, please ensure you check with your SIP provider for more information.
- ▶ **Disable** to let the the gateway to handle all available call features.

Return Call (Dial number: *69): Dial *69 to redial the latest incoming call number.

Redial (Dial number: *68): Dial *68 to redial the latest outgoing call number.

Don't Disturb (Enable: *78, Disable: *79): Press *78 to enable Don't Disturb feature so as to make it not ring when a call comes in; while press *79 to disable Don't Disturb feature, if a call comes with a ringing indication.

Example: How to establish 3-way conference call



Case 1: Bill and Larry are talking. Bill wants to invite Mark to join a conference call.

Step – 1: Billy and Larry are discussing on the phone. Bill tells Larry that he wants to set up a conference call with Mark.

Step – 2: Bill **presses flash** (hold original call), and Bill hears the dial tone.

Step – 3: Bill calls Mark. Bill and Mark are on a new call.

Step – 4: Bill tells Mark that Mark is invited to join a conference call.

Step – 5: Bill **presses flash** (hold new call) and return to original call.

Step – 4: Bill tells Larry that Mark is on the phone.

Step – 6: Bill **presses flash again** to merge all 3 calls.

Step – 7: Bill, Larry and Mark hold a 3-way conference call from now on.

Case 2: When Bill and Larry are talking on the phone, Bill received a phone call from Mark. Bill decided to ask Mark to join the conference call.

Step – 1: Bill and Larry on a call, then Mark dials Bill and Bill hears a waiting tone.

Step – 2: Bill **presses flash** and picks up the call waiting call.

Step – 3: Bill tells Mark that he and Larry are talking on the phone; they can have a conference call.

Step – 4: Bill **presses flash** to hold the call with Mark and return to original call with Larry.

Step – 5: Bill tells Larry that it is Mark and he wants to set up a conference with Mark.


Step – 6: Bill **presses flash again** to merge all 3 calls.

Step – 7: Bill, Larry and Mark hold a 3-way conference call from now on.

Access Management

Device Management

Device management offers users a way to change the embedded web server accessing port, default 80. User can change the http port to 8080 or something else here.



The screenshot shows a web interface for configuration. At the top, there is a 'Configuration' tab. Below it, a 'Device Management' section is expanded. Under 'Device Management', there is a sub-section for 'Embedded Web Server'. Within this sub-section, there is a label 'HTTP Port' followed by a text input field containing the number '80'. To the right of the input field, there is a note: '(The HTTP portnumber is 80.)'. At the bottom left of this section, there is a 'Save' button.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. BiPAC 6300VNP(O)Z serves as a SNMP agent which allows a manager station to manage and monitor the router through the network.

Configuration

SNMP

SNMP Activated Deactivated

Get Community

Set Community

Trap Manager IP

SNMPv3

SNMPv3 Enable Disable

Username

Access Permissions

Authentication Protocol

Authentication Key (8~31 characters)

Privacy Protocol

Privacy Key (8~31 characters)

Save

SNMP: Select to enable SNMP feature.

Get Community: Type the Get Community, which is the password for the incoming Get-and-GetNext requests from the management station.

Set Community: Type the Set Community, which is the password for incoming Set requests from the management station.

Trap Manager IP: Enter the IP of the server receiving the trap message (when some exception occurs) sent by this SNMP agent.

SNMPv3: Enable to activate the SNMPv3.

User Name: Enter the name allowed to access the SNMP agent.

Access Permissions: Set the access permissions for the user; RO--read only and RW--read and writer.

Authentication Protocol: Select the authentication protocol, MD5 and SHA. SNMP agent can communicate with the manager station through authentication and encryption to secure the message exchange. Set the authentication and encryption information here and below.

Authentication Key: Set the authentication key, 8-31 characters.

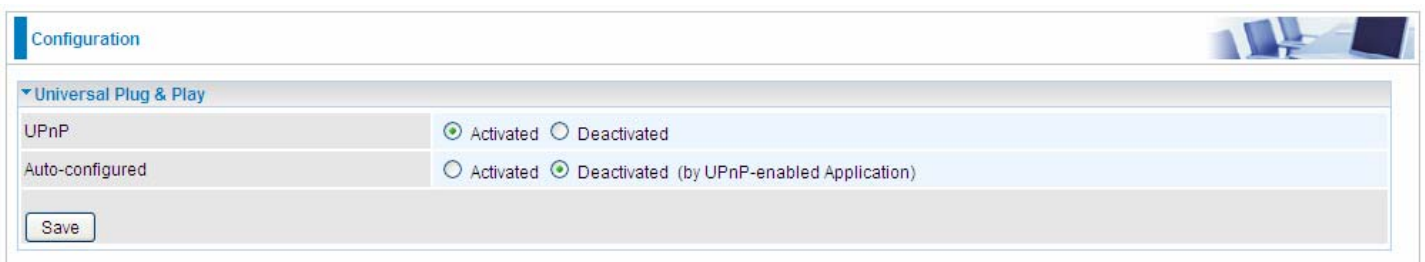
Privacy Protocol: Select the privacy mode, DES and AES.

Privacy Key: Set the privacy key, 8-31 characters.

Universal Plug & Play

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user's Operating System and the relevant application must support UPnP in addition to the router. Windows XP and Windows ME natively support UPnP (when the component is installed), and Windows 98 users may install the Internet Connection Sharing client from Windows XP in order to support UPnP. Windows 2000 does not support UPnP.



The screenshot shows a configuration window titled "Configuration" with a sub-section for "Universal Plug & Play". It contains two rows of settings:

Setting	Value
UPnP	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Auto-configured	<input type="radio"/> Activated <input checked="" type="radio"/> Deactivated (by UPnP-enabled Application)

A "Save" button is located at the bottom left of the configuration area.

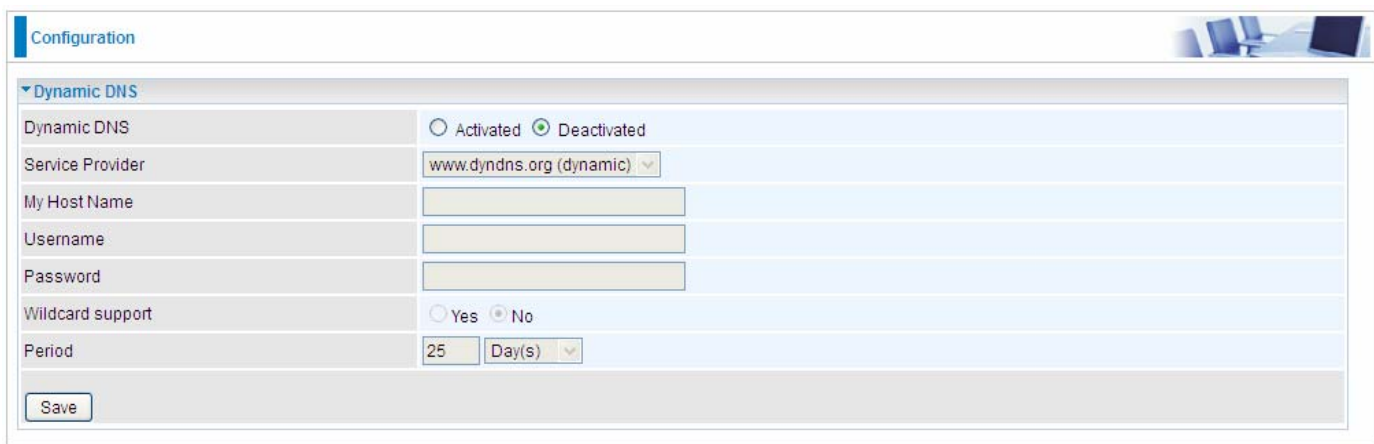
UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use a UPnP application to open the web configuration's login screen without entering the BiPAC 6300VNP(O)Z ' IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BiPAC 6300VNP(O)Z so that they can communicate through the gateway, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your internet connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS(es). But note that first users have to go to the Dynamic DNS registration service provider to register an account.



The screenshot shows a web configuration page titled "Configuration" with a sub-section for "Dynamic DNS". The form includes the following fields and options:

- Dynamic DNS:** Radio buttons for "Activated" (unselected) and "Deactivated" (selected).
- Service Provider:** A drop-down menu showing "www.dyndns.org (dynamic)".
- My Host Name:** An empty text input field.
- Username:** An empty text input field.
- Password:** An empty text input field.
- Wildcard support:** Radio buttons for "Yes" (unselected) and "No" (selected).
- Period:** A text input field containing "25" and a drop-down menu for "Day(s)".

A "Save" button is located at the bottom left of the form.

Dynamic DNS: Select this check box to activate Dynamic DNS.

Service Provider: Select from drop-down menu for the appropriate service provider, for example: www.dyndns.org.

My Host Name: Type the domain name assigned to your router by your Dynamic DNS provider.

Username: Type your user name.

Password: Type the password.

Wildcard support: Select this check box to enable DYNDNS Wildcard.

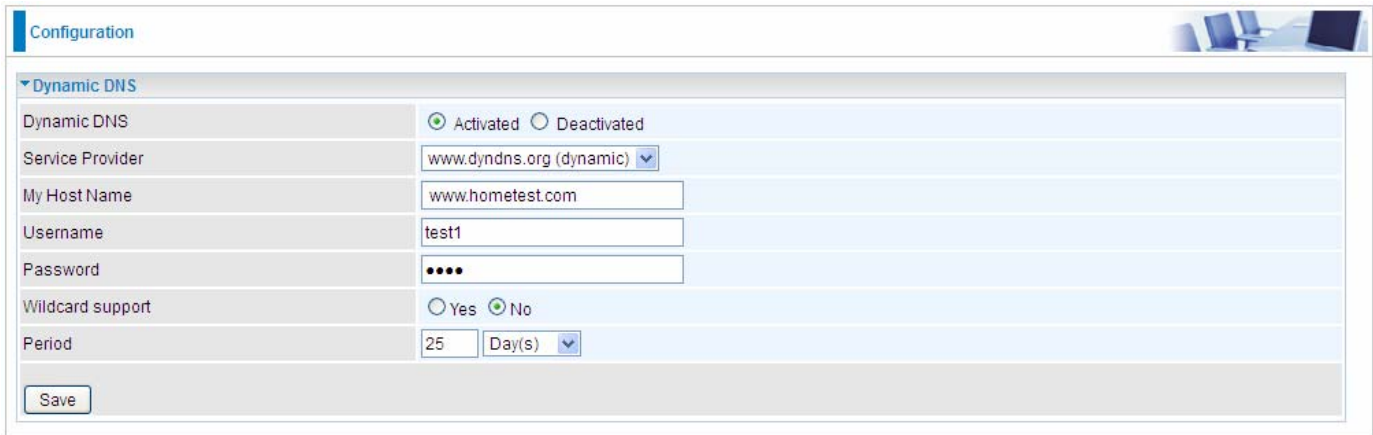
Period: Set the time period between updates, for the Router to exchange information with the DDNS server. In addition to updating periodically as per your settings, the router will perform an update when your dynamic IP address changes.

Example: How to register a DDNS account

Note first users have to go to the Dynamic DNS registration service provider to register an account.

User **test1** register a Dynamic Domain Names in DDNS provider <http://www.dyndns.org/> .

DDNS: www.hometest.com using username/password test/test



The screenshot shows a web-based configuration page for Dynamic DNS. The page has a 'Configuration' header and a 'Dynamic DNS' section. The 'Dynamic DNS' section is expanded, showing several fields: 'Dynamic DNS' (Activated), 'Service Provider' (www.dyndns.org (dynamic)), 'My Host Name' (www.hometest.com), 'Username' (test1), 'Password' (masked with dots), 'Wildcard support' (No), and 'Period' (25 Day(s)). A 'Save' button is located at the bottom left of the configuration area.

Dynamic DNS	
Dynamic DNS	<input checked="" type="radio"/> Activated <input type="radio"/> Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	www.hometest.com
Username	test1
Password	••••
Wildcard support	<input type="radio"/> Yes <input checked="" type="radio"/> No
Period	25 Day(s) ▼

Save

Access Control

Access Control Listing allows you to determine which services/protocols can access BiPAC 6300VNP(O)Z interface from which computers. It is a management tool aimed to allow IPs (set in secure IP address) to access specified embedded applications (Web, etc, user can set) through some specified interface (LAN, WAN or both). User can have an elaborate understanding in the examples below.

The maximum number of entries is **16**.

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Access Control: Select whether to make Access Control function available.

Rule Index: This is item number

Active: Select to activate the rule.

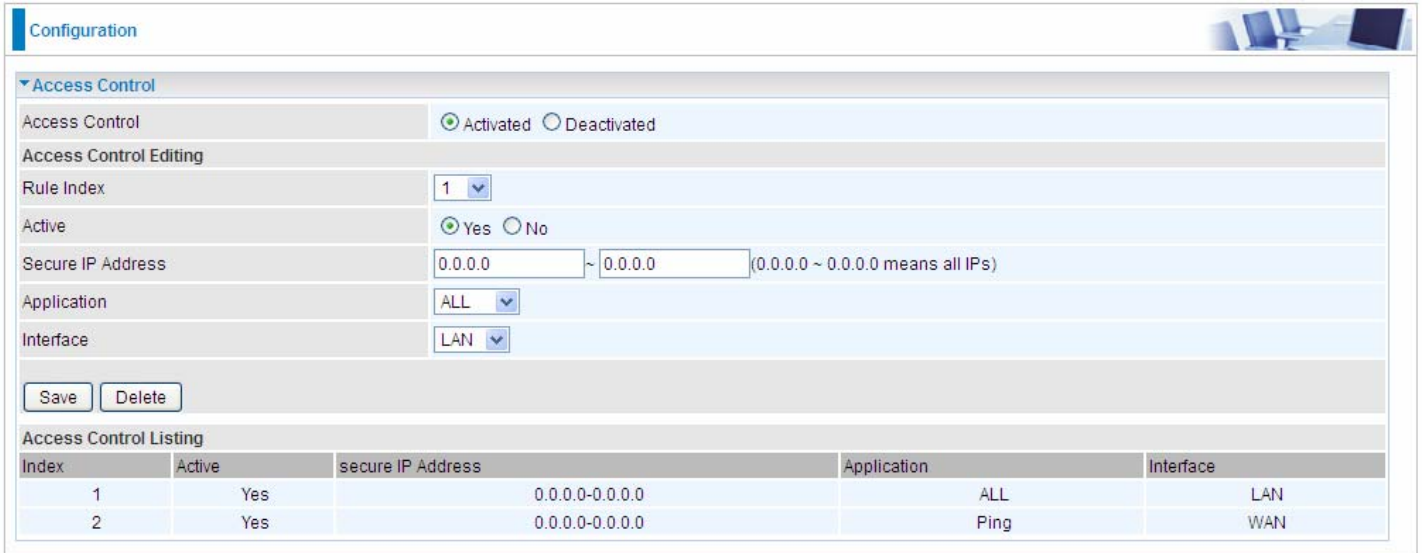
Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the gateway. Type an IP address range to restrict access to the client(s) without a matching IP address.

Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the common used applications.

Interface: Select the access interface. Choices are **LAN**, **WAN** and **Both**.

By default, the “Access Control” has **two default rules**.

Default Rule 1: (Index 1), a rule to allow only clients from LAN to have access to all embedded applications (Web, FTP, etc). Under this situation, clients from WAN cannot access the router even from Ping.



Configuration

Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index: 1

Active: Yes No

Secure IP Address: 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application: ALL

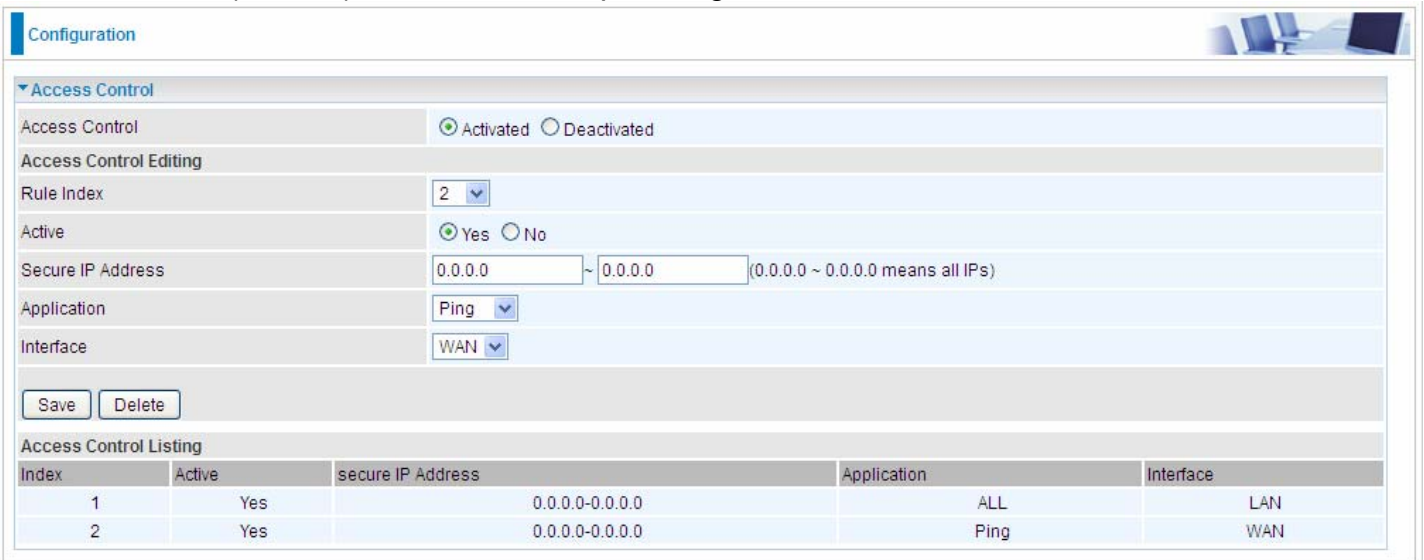
Interface: LAN

Save Delete

Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Default Rule 2: (Index 2), an ACL rule to open Ping to WAN side.



Configuration

Access Control

Access Control Activated Deactivated

Access Control Editing

Rule Index: 2

Active: Yes No

Secure IP Address: 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)

Application: Ping

Interface: WAN

Save Delete

Access Control Listing

Index	Active	secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Packet Filter

You can filter the packages by MAC address, IP address, Protocol, Port number and Application or URL.

❖ Packet Filter - IP & MAC Filter

The screenshot shows a web-based configuration interface for a Packet Filter. The 'Filter Type' is set to 'IP & MAC Filter'. Under 'IP & MAC Filter Editing', the 'Rule Index' is 1, 'Individual Active' is 'No', 'Action' is 'Black List', 'Interface' is 'LAN', 'Direction' is 'Both', and 'Type' is 'IPv4'. The 'Source' and 'Destination' fields for IP Address, Subnet Mask, and Port Number are all set to 0, with a note that 0 means 'Don't care'. The 'DSCP' is set to 0 (Value Range: 0~64, 64 means Don't care) and the 'Protocol' is 'TCP'. There are 'Save' and 'Delete' buttons at the bottom of the configuration area. Below the configuration is a table titled 'IP & MAC Filter List' with columns for #, Active, Interface, Direction, Source IP(IPv6) Address/Mask(Prefix), Destination IP(IPv6) Address/Mask(Prefix), Source MAC Address, Source Port, Destination Port, DSCP, and Protocol.

Packet Filter

Filter Type: There are three types “IP & MAC Filter”, “Application Filter”, and “URL Filter” that user can select for this filter rule. Here we set **IP & MAC Filter**.

IP & MAC Filter Editing

Rule Index: This is item number

Individual Active: Select **Yes** to activate the rule.

Action: This is how to deal with the packets matching the rule. Allow please select White List or block selecting Black List.

Interface: Select to determine which interface the rule will be applied to.

Direction: Select to determine whether the rule applies to outgoing packets, incoming packets or packets of both directions.

Type: Choose type of field you want to specify to monitor. Select “IPv4” for IPv4 address, port number and protocol. Select “IPv6” for IPv6 address, port number and protocol. Select “MAC” for MAC address.

Source IP Address: The source IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Source Subnet Mask: Enter the subnet mask of the source network.

Source Port Number: The source port number of packets to be monitored. 0 means “Don’t care”.

Destination IP Address: The destination IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Destination Subnet Mask: Enter the subnet mask of the destination network.

Destination Port Number: This is the Port that defines the application. (e.g. HTTP is port 80.)

DSCP: DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don’t care.)

Protocol: Specify the packet type (TCP, UDP, ICMP, and ICMPv6) that the rule applies to.

IP/MAC Filter Listing

#: Item number.

Active: Whether the connection is currently active.

Interface: show the interface the rule applied to.

Direction: show the direction the rule applied to.

Source IP (IPv6) Address/Mask (Prefix): The source IP address or range of packets to be monitored.

Destination IP (IPv6) Address/Mask (Prefix): This is the destination subnet IP address.

Source MAC Address: show the MAC address of the rule applied.

Source Port: The source port number of packets to be monitored.

Destination Port: This is the Port or Port Ranges that defines the application.

DSCP: show the set DSCP.

Protocol: It is the packet protocol type used by the application. Select either **TCP** or **UDP** or **ICMP** or **ICMPv6**

❖ Packet Filter - Application Filter

Application Filter: Select this option to Activated/Deactivated the Application filter.

ICQ: Select this option to Allow/Deny ICQ.

MSN: Select this option to Allow/Deny MSN.

YMSG: Select this option to Allow/Deny Yahoo messenger.

Real Audio/Video (RTSP): Select this option to Allow/Deny Real Audio/Video (RTSP).

❖ Packet Filter - URL Filter

Index	Active	URL
1	Yes	www.yahoo.com

URL Filter: Select **Activated** to enable URL Filter.

URL Filter Rule Index: This is item number.

Individual Active: To give control to the specific URL access individually, for example, you want to prohibit access to www.yahoo.com, please first press Activated in “URL Filter” field, and also Yes in “Individual Active” field; if some time you want to allow access to this URL, you simply select No in individual active field. In a word, the command serves as a switch to the access of some specific URL with the filter on.

URL (Host): Specified URL which is prohibited from accessing.

CWMP (TR-069)

CWMP, short for CPE WAN Management Protocol, also called TR069 is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provide the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones). At the same time the configuration of this equipment became more complicated – too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.

Configuration

▼ CWMP (TR-069)

CWMP Activated Deactivated

ACS Login Information

URL

Username

Password

Connection Request Information

Path

Username

Password

Periodic Inform Config

Periodic Inform Activated Deactivated

Interval

Save

CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

User Name: Specify the ACS User Name for ACS authentication to the connection from CPE.

Password: Enter the ACS server login password.

Connection Request Information

Path: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

Username: Username used to authenticate an ACS making a Connection Request to the CPE.

Password: Password used to authenticate an ACS making a Connection Request to the CPE.

Periodic Inform Config

Periodic Inform: Select Activated to authorize the router to send an Inform message to the ACS automatically.

Interval(s): Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

Parental Control

With this feature, router can reject to provide **Internet** services to the specified computer during some specified time interval. This can be very useful for parents to give control to children using computer without restraint.

Configuration

Parental Control

Parental Control Activated Deactivated

MAC Address Browser's MAC Address

Block Schedule

Save

Parent Control: Select Activated to enable this feature.

MAC Address: Type the MAC address(es) you want to block to access the internet (access to the router is sustained). The format of MAC address could be: xx:xx:xx:xx:xx:xx . If you want to set restriction to the Browser PC, you can directly check the checkbox of Browser's MAC Address.

Block Schedule: Select a timeslot throughout which the above set MAC is restricted to access internet. See [Time Schedule](#) to set the exact timeslot.

Configuration

Parental Control

Parental Control Activated Deactivated

MAC Address Browser's MAC Address

Block Schedule

SAVE

Timeslot1 at Time Schedule:

Configuration

Time Schedule

Time Index

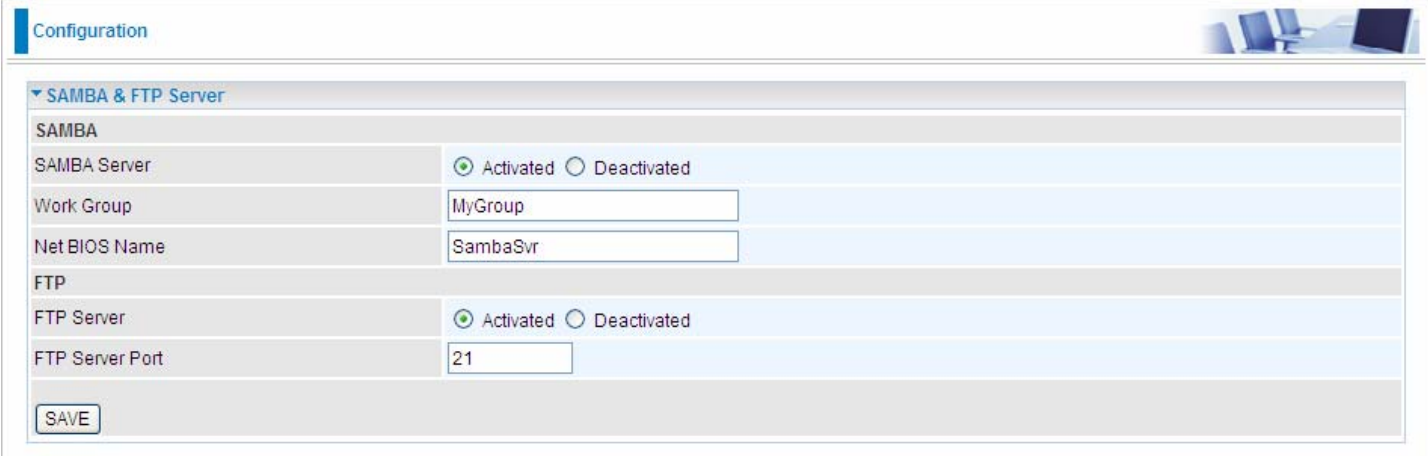
Name

Day of Week	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="text" value="09:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>
	<input type="text" value="24:00"/>	<input type="text" value="18:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>	<input type="text" value="00:00"/>

Save

SAMBA & FTP Server

Samba and FTP are served as network sharing.



Configuration

▼ SAMBA & FTP Server

SAMBA

SAMBA Server Activated Deactivated

Work Group

Net BIOS Name

FTP

FTP Server Activated Deactivated

FTP Server Port

SAVE

SAMBA Server: Activated to enable SAMBA sharing.

Work Group: The same mechanism like in Microsoft work group, please set the Work Group name.

NetBIOS Name: The sharing NetBIOS name.

FTP Server: Activated to enable FTP sharing.

FTP Server Port: Set the working port. Well-known one is 21. User can change it.

SAMBA/FTP login account:

- ▶ **Default user:** admin/admin, it is the administrative user and a super user, it has the full authority of SAMBA /FTP access and operation permission of objects in SAMBA and FTP server.
- ▶ **New user:** users can create new user(s) to grant it (them) access and permission to the SAMBA & FTP server.

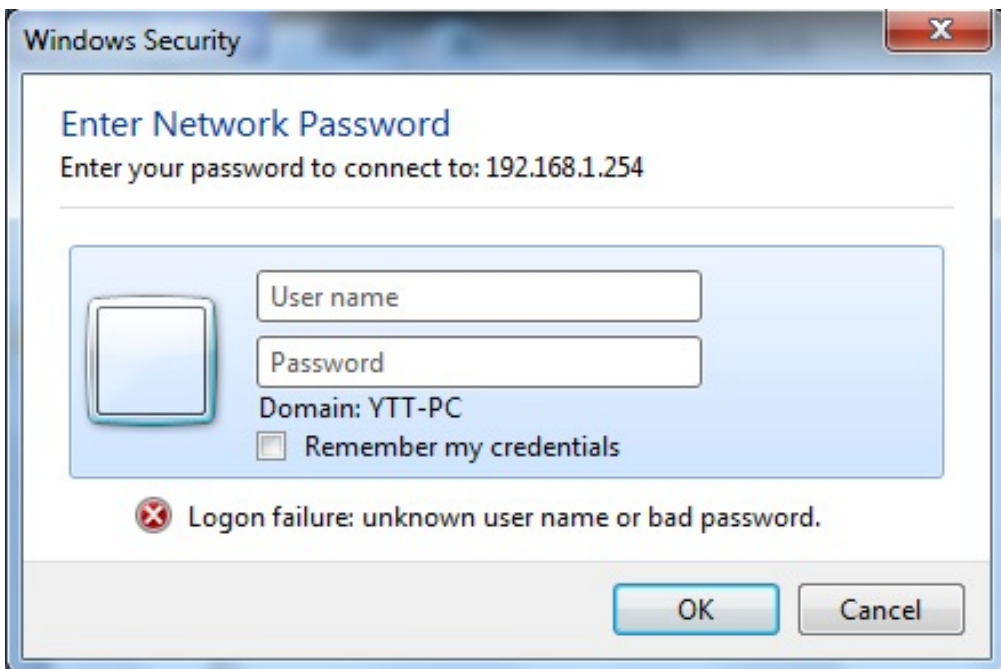
Please see [User Management](#).

Example: How to setup Samb

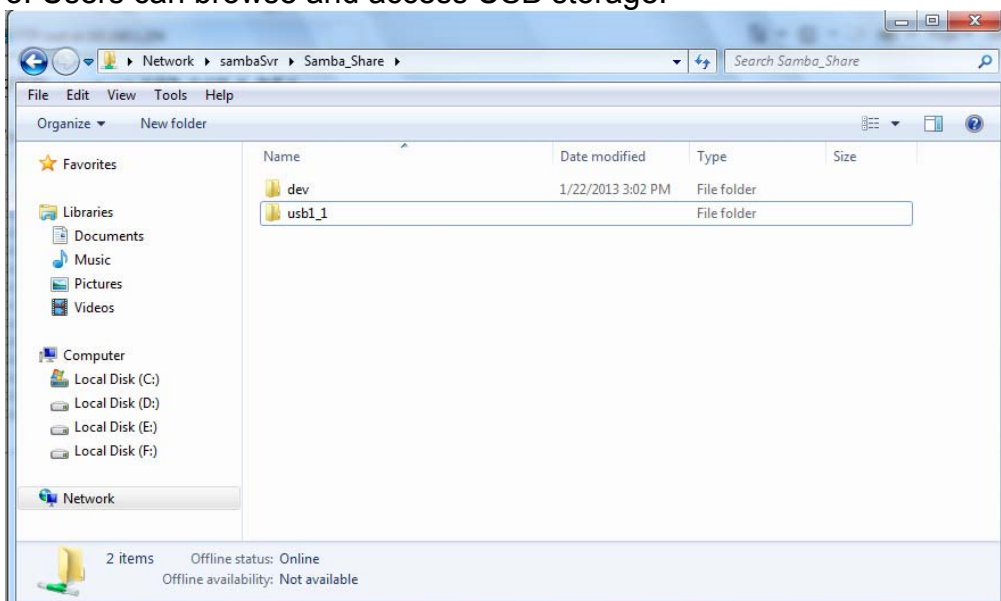
1. Go directly to Start > Run (enter [\\192.168.1.254](#) (from LAN side), [\\SambaSvr](#) , but if you enter [\\SambaSvr](#), please be sure your working PC is in the same workgroup as set in the samba server set above.)



2. Enter the Username and password.



3. Users can browse and access USB storage.

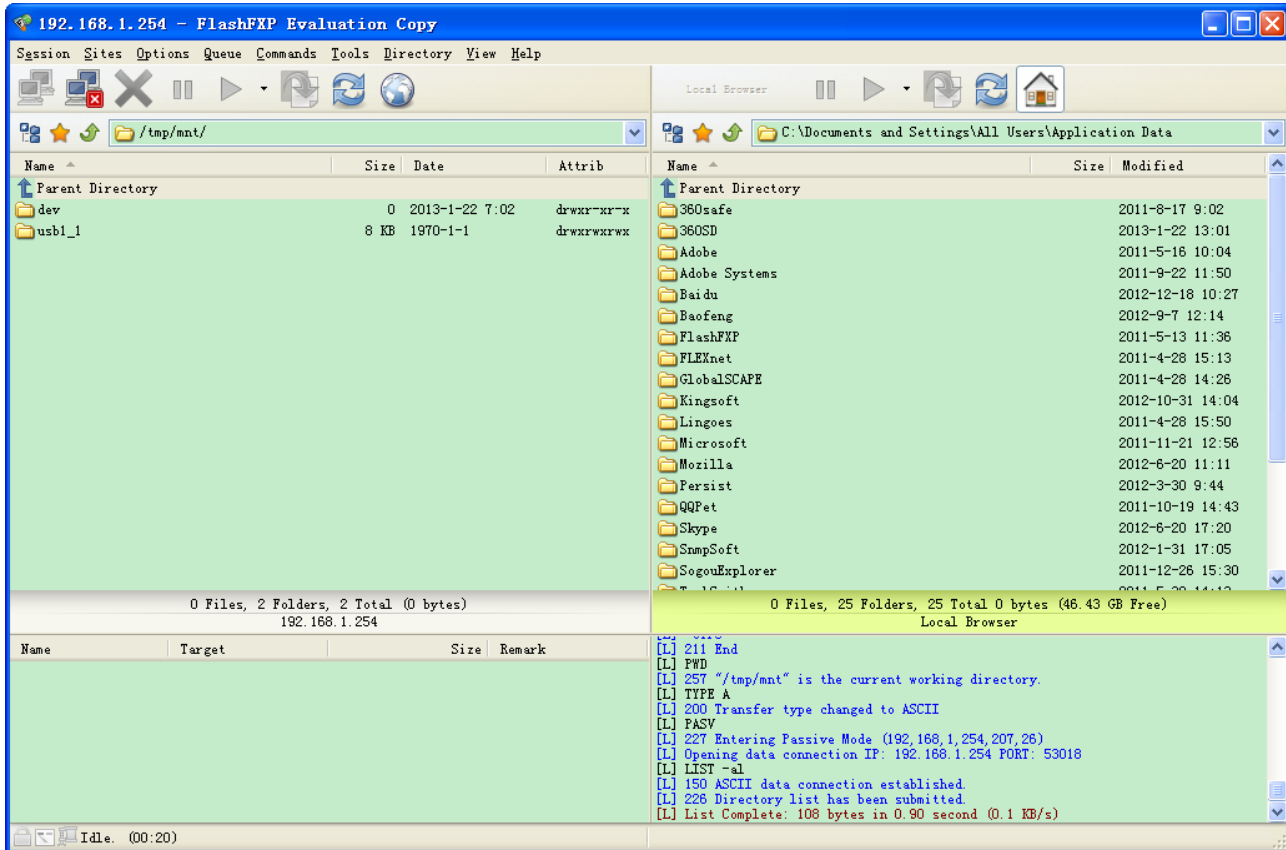


Example: How to setup FTP :

1. Access via FTP tools

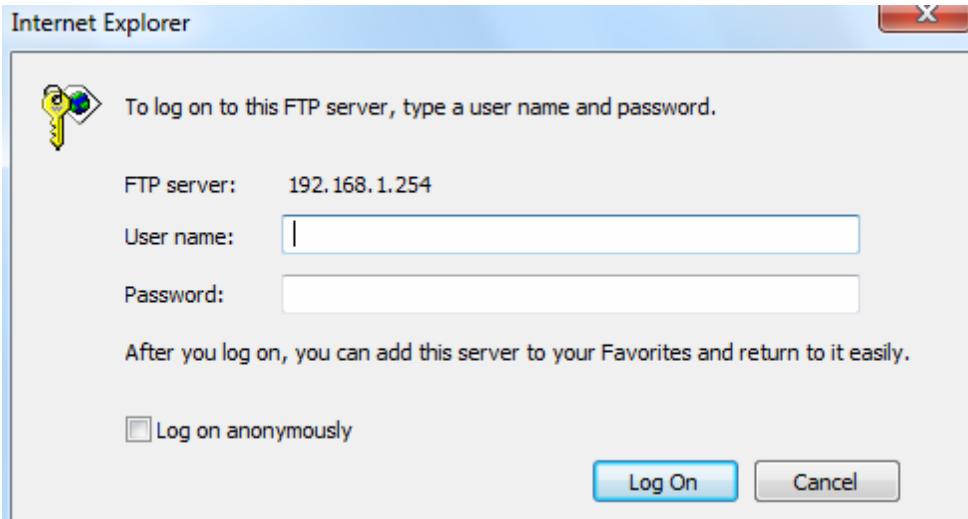
Take popular FTP tool of FlashFXP for example:

- 1) Open FlashFXP
- 2) Create ftp sites (LAN IP / WAN IP, 192.168.1.254, and set the account, port).
- 3) Connect to the ftp site.



2. Web FTP access

- 1) Enter <ftp://192.168.1.254> at the address bar of the web page.
- 2) Enter the account's username and password.



Maintenance

Maintenance equipments the users with the ability of maintaining the device as well as examining the connectivity of the WAN connections, including **User Management, Time Zone, Firmware & Configuration, System Restart, and Diagnostic Tool.**

User Management

User Management controls the Router Web GUI permission, FTP/SAMBA access to the specific account.

In factory setting, the default accounts are **admin/admin** and **user/user**. The default root account admin has been authorized to web access of router, Samba access, and FTP access. **user/user** is equipment with limited access (specified by advanced users with admin account) to router web, and FTP/SAMBA . A total of **6** other accounts can be created to grant access to the access of Samba and FTP and web page (need to be specified).

Note: Please go to [SAMBA & FTP Server](#) to re-activate FTP and SAMBA server to enable the changes to the FTP and SAMBA account set here.

❖ Admin / Admin

admin/admin is the root account provided by our router.

User Management

User Account

Index: 1

Username: admin

New Password:

Confirm Password:

FTP Authority Setup

FTP Access: Enable Disable

Permission: Read/Write Read

SAMBA Authority Setup

SAMBA Access: Enable Disable

Permission: Read/Write Read

Please restart the Storage server after config changed

Save Delete

User Account List

#	User Name	FTP Access	FTP Permission	SAMBA Access	SAMBA Permission
1	admin	Enable	Read/Write	Enable	Read/Write
2	user	Disable	Read	Disable	Read

User Setup

Index: User account index, total is 8.

User Name: Users can create account(s) to give it (them) access to SAMBA and FTP.

New Password: Enter a new password for this user account.

Confirmed Password: Re-enter the new password again; you must enter the password exactly the same as in the previous field

FTP Authority Setup

FTP Access: Enable to grant the user access to the FTP server.

Permission: Set the operation permission for the user, Read/Write or Read.

SAMBA Authority

SAMBA Access: Enable to grant the user access to the SAMBA server.

Permission: Set the operation permission for the user, Read/Write or Read.

Web GUI Permission

Login using the Administrator account, you will have the full accessibility to manage & control your gateway device and can also create user accounts for others to control some of the open configuration settings.

▶ Status
• Quick Start
▼ Configuration
▶ Interface Setup
▶ Advanced Setup
▶ VoIP
▶ Access Management
▶ Maintenance
▶ Language

❖ User / User and/or Adding additional user accounts

Configuration

User Management

User Account

Index:

Username:

New Password:

Confirm Password:

FTP Authority Setup

FTP Access: Enable Disable

Permission: Read/Write Read

SAMBA Authority Setup

SAMBA Access: Enable Disable

Permission: Read/Write Read

Web GUI Permission

Guest Account: Enable Disable

Interface Setup: Enable Disable

Advanced Setup: Enable Disable

VOIP Setup: Enable Disable

Access Management: Enable Disable

Maintenance: Enable Disable

Please restart the Storage server after config changed

User Account List

#	User Name	FTP Access	FTP Permission	SAMBA Access	SAMBA Permission
1	admin	Enable	Read/Write	Enable	Read/Write
2	user	Disable	Read	Disable	Read

User Setup

Index: User account index, total is 8.

User Name: Users can create account(s) to give it (them) access to SAMBA and FTP.

New Password: Type the password for the user account.

Confirmed Password: Type password again for confirmation.

FTP Authority Setup

FTP Access: Enable to grant the user access to the FTP server.

Permission: Set the operation permission for the user, Read/Write or Read.

SAMBA Authority

SAMBA Access: Enable to grant the user access to the SAMBA server.

Permission: Set the operation permission for the user, Read/Write or Read.

Web GUI Permission

Guest Account: A pre-set guest account setting granted with **Interface Setup**, **Advanced Setup**, **Access Management** access. Enable to have access to Interface Setup, Advanced Setup and Access Management or disable to set the specifics yourself.

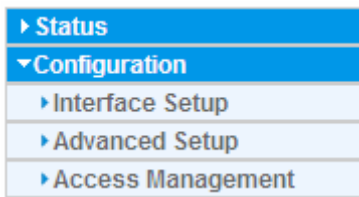
Interface Setup: Enable to allowing access to Interface Setup with this account.

Advanced Setup: Enable to allowing access to Advanced Setup with this account.

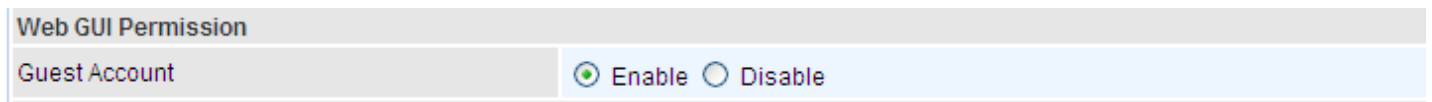
VOIP Setup: Enable to allowing access to VoIP Setup with this account.

Access Management: Enable to allowing access to Access Management with this account.

Maintenance: Enable to allowing access to Maintenance with this account.



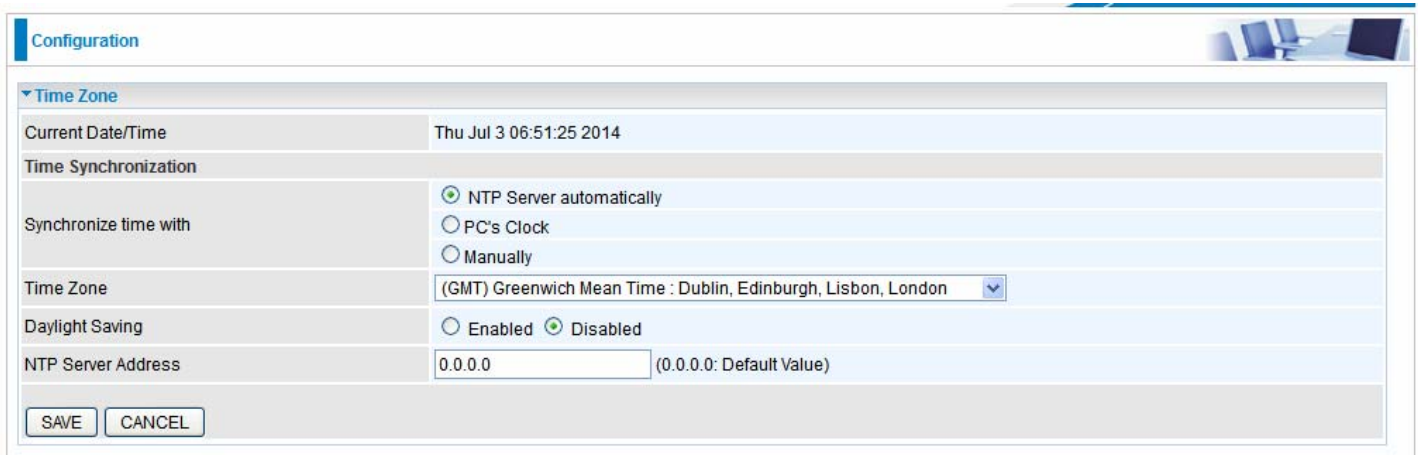
When customers use the “user” account to login to the router, they are offered with only configuration items set in **Web GUI Permission**.



(Configuration items shown when “user” account uses Guest account on Web GUI Permission)

Time Zone

The router does not have a real time clock on board; instead, it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server outside your network. Choose your local time zone. After a successful connection to the Internet, the router will retrieve the correct local time from the SNTP server you have specified. If you prefer to specify an SNTP server other than the default, simply enter its IP address as shown above. Your ISP may provide an SNTP server for you to use.



The screenshot shows a web-based configuration interface for a router. The main heading is "Configuration". Underneath, there is a section titled "Time Zone". The "Current Date/Time" is displayed as "Thu Jul 3 06:51:25 2014". The "Time Synchronization" section has three radio button options: "NTP Server automatically" (which is selected), "PC's Clock", and "Manually". The "Time Zone" is set to "(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London" via a dropdown menu. The "Daylight Saving" section has two radio button options: "Enabled" and "Disabled" (which is selected). The "NTP Server Address" is set to "0.0.0.0" with a note "(0.0.0.0: Default Value)". At the bottom of the configuration area, there are "SAVE" and "CANCEL" buttons.

Synchronize time with: Select the methods to synchronize the time.

- ▶ **NTP Server automatically:** To synchronize time with the NTP server.
- ▶ **PC's Clock:** To synchronize time with the PC's clock.
- ▶ **Manually:** Select this, user need to set the time yourself manually.

Time Zone: Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Daylight Saving: Select this option if you use daylight savings time.

NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your BiPAC 6300VNP(O)Z provides an easy way to update the code to take advantage of the changes. .

To upgrade the firmware of BiPAC 6300VNP(O)Z, you should download or copy the firmware to your local environment first. Press the “**Browse...**” button to specify the path of the firmware file. Then, click “**Upgrade**” to start upgrading. When the procedure is completed, BiPAC 6300VNP(O)Z will reset automatically to make the new firmware work.

The screenshot shows a web interface for configuration. The main heading is 'Configuration'. Below it is a section titled 'Firmware & Configuration'. This section contains several rows of controls:

- Upgrade:** Two radio buttons, 'Firmware' (selected) and 'Configuration'.
- System Restart with:** Two radio buttons, 'Current Settings' (selected) and 'Factory Default Settings'.
- File:** A text input field followed by a 'Browse...' button.
- Backup Configuration:** A 'Backup' button.
- Status:** A text area.

Below these controls is a warning message: 'It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.' At the bottom of the section is an 'Upgrade' button.

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

- ▶ **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.
- ▶ **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.

File: Type in the location of the file you want to upload in this field or click **Browse** to find it.

Browse: Click **Browse...** to find the configuration file or firmware file you want to upload. Remember that you must extract / decompress / unzip the .zip files before you can upload them.

Backup Configuration: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your device when making false configurations and want to restore to the original settings.

The screenshot shows a standard file dialog box. The text inside reads: 'Do you want to open or save romfile.cfg (35.8 KB) from 192.168.1.254?'. On the right side, there are three buttons: 'Open', 'Save', and 'Cancel'. There is also a small 'x' icon in the top right corner of the dialog box.

UPGRADE: Click **UPGRADE** to begin the upload process. This process may take up to two minutes.

Configuration 

▼ Firmware Upgrade

File upload succeeded, starting flash erasing and programming!!

Progress 

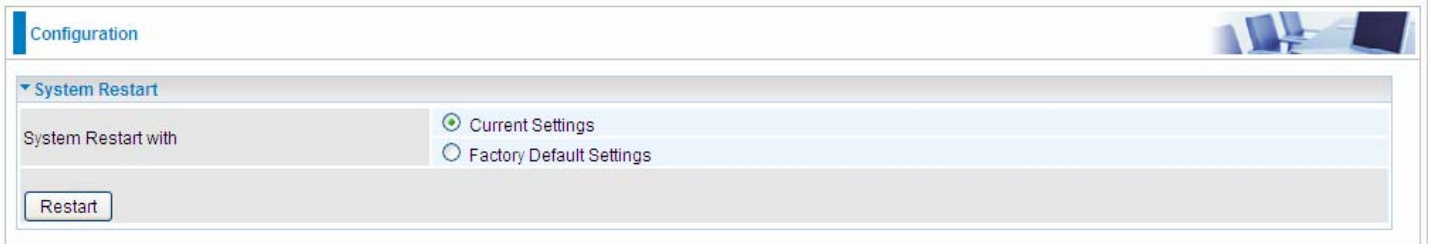
Percent 16 %



DO NOT turn off / power off the device or interrupt the firmware upgrading while it is still in process. Improper operation could damage your BiPAC 6300VNP(O)Z.

System Restart

Click **System Restart** with option **Current Settings** to reboot your router.



The screenshot shows a web interface for system configuration. At the top, there is a 'Configuration' tab. Below it, a 'System Restart' section is expanded. Under 'System Restart with', there are two radio button options: 'Current Settings' (which is selected) and 'Factory Default Settings'. A 'Restart' button is located at the bottom left of the section.

If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to restore to factory default settings.

You may also restore your router to factory settings by holding the small Reset pinhole button on the back of your router in about more than 6s seconds whilst the router is turned on.

Diagnostics Tool

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

3G/4G-LTE or 3G/4G-LTE USB:

The screenshot shows the 'Diagnostic Tool' configuration page. The 'WAN Interface' is set to '3G/4G-LTE'. The test results are as follows:

WAN Interface	3G/4G-LTE
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (221.6.4.66)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A

A 'Start' button is located at the bottom left of the configuration area.

Click START to begin to diagnose the connection.

The screenshot shows the 'Diagnostic Tool' configuration page after the tests have been executed. The 'WAN Interface' remains '3G/4G-LTE'. The test results are now:

WAN Interface	3G/4G-LTE
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (221.6.4.66)	PASS
Ping www.google.com	PASS
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	Skipped

The 'Start' button is still present at the bottom left.

EWAN:



The screenshot shows the 'Configuration' page with a 'Diagnostic Tool' section. The 'WAN Interface' is set to 'EWAN'. The test results are as follows:

Test	Result
WAN Interface	EWAN
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (218.2.135.1)	N/A
Ping www.google.com	N/A
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	N/A

A 'Start' button is located at the bottom left of the diagnostic tool area.

Click START to begin to diagnose the connection.



The screenshot shows the 'Configuration' page with the 'Diagnostic Tool' section. The 'WAN Interface' is set to 'EWAN'. The test results are as follows:

Test	Result
WAN Interface	EWAN
Testing Ethernet LAN Connection	PASS
Ping Primary DNS (218.2.135.1)	PASS
Ping www.google.com	PASS
Ping other IP Address <input type="radio"/> Yes <input checked="" type="radio"/> No	Skipped

A 'Start' button is located at the bottom left of the diagnostic tool area.

Chapter 5: Troubleshooting

If your BiPAC 6300VNP(O)Z is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problem with LAN Interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not lit, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Recovery Procedures

Problem	Suggested Action
<ul style="list-style-type: none">- The front LEDs display incorrectly- Still cannot access to the router management interface after pressing the RESET button.- Software / Firmware upgrade failure	<ol style="list-style-type: none">1. Power on the router, once the Power LED lit red, please press this reset button using the end of paper clip or other small pointed object immediately.2. The router's emergency-reflash web interface will then be accessible via http://192.168.1.1 where you can upload a firmware image to restore the router to a functional state, Please note that the router will only respond with its web interface at this address (192.168.1.1), and will not respond to ping request from your PC or other telnet operations.

Appendix: Product Support & Contact

If you come across any problems please contact the dealer from where you have purchased the product.

Contact Billion

WORLDWIDE

<http://www.billion.com>

MAC OS is a registered Trademark of Apple Computer, Inc.

Windows 7/98, Windows NT, Windows 2000, Windows ME, Windows XP, and Windows Vista are registered Trademarks of Microsoft Corporation.

Federal Communication Commission Interference Statement

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

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
- (2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC 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.