

# Table of contents

<b>1</b>	<b>LED BEHAVIOUR.....</b>	<b>4</b>
1.1	POWER .....	4
1.2	STATUS.....	4
1.3	WAN .....	4
1.4	LAN.....	4
1.5	PHONE 1 VOIP .....	4
1.6	PHONE 1 “HOOK” .....	4
<b>2</b>	<b>RESETTING THE VOOD TO FACTORY DEFAULTS.....</b>	<b>4</b>
<b>3</b>	<b>LOG IN TO MANUAL VOOD CONFIGURATION .....</b>	<b>5</b>
<b>4</b>	<b>SETUP.....</b>	<b>6</b>
4.1	LAN SETUP.....	6
4.1.1	LAN clients.....	6
4.1.2	LAN configuration .....	7
4.1.3	LAN group configuration.....	7
4.1.4	Firewall/NAT services .....	7
4.2	WAN SETUP.....	7
4.2.1	WAN overview.....	7
4.2.2	Uplink Bandwidth .....	8
4.2.3	Vood router WAN-side IP address allocation over virtual connection.....	8
4.2.4	Subscriber authentication .....	8
4.2.5	New connection.....	8
4.2.6	PPP connections .....	9
4.2.7	Bridged connections .....	9
4.2.8	DHCP connections .....	10
4.2.9	Static connections .....	10
<b>5</b>	<b>ADVANCED.....</b>	<b>11</b>
5.1	UPnP .....	11
5.2	SNMP .....	12
5.3	IP QoS (QUALITY OF SERVICE) .....	12
5.4	PORT FORWARDING.....	13
5.5	IP FILTERS.....	14
5.6	LAN CLIENTS .....	15
5.7	BRIDGE FILTERS .....	15
5.8	WEB FILTERS .....	16
5.9	MULTICAST .....	16
5.10	STATIC ROUTING.....	17
5.11	DYNAMIC ROUTING.....	17
5.12	ACCESS CONTROL .....	18
<b>6</b>	<b>TOOLS.....</b>	<b>18</b>
6.1	SYSTEM COMMANDS .....	19
6.2	REMOTE LOG.....	19
6.3	USER MANAGEMENT .....	19
6.4	PING TEST .....	20
<b>7</b>	<b>STATUS.....</b>	<b>20</b>
<b>8</b>	<b>HELP.....</b>	<b>21</b>
<b>9</b>	<b>LOGIN TO VOOD USER PAGES CONFIGURATION .....</b>	<b>1</b>
<b>10</b>	<b>SERVICES.....</b>	<b>22</b>
10.1	CALL WAITING WITH CALL HOLD.....	22
10.2	CALL WAITING DEFAULT: ON.....	22

10.3	INQUIRY CALL WITH CALL HOLD .....	22
10.4	MESSAGE WAITING .....	22
10.5	THREE-WAY CONFERENCING .....	22
10.6	CLICK TO DIAL SERVICE .....	22
10.7	FAST RE-DIAL SERVICE .....	23
10.8	ANSWERING MACHINE SERVICE.....	23
10.8.1	Mail configuration .....	23
10.8.2	Administration of locally stored messages.....	24
10.8.3	Recording a greeting message .....	24
10.8.4	Redirect to the answering machine .....	24
10.9	SERVICE CALLING LINE ID RESTRICTION FOR ANONYMOUS CALLING .....	24
<b>11</b>	<b>NAT AND FIREWALL OVERVIEW .....</b>	<b>24</b>
<b>12</b>	<b>SERVICES.....</b>	<b>25</b>
12.1	PORT FORWARDING .....	25
12.2	IP FILTERS.....	25
12.3	ACCESS CONTROL .....	25
12.4	DMZ .....	25
12.5	PING.....	25

# 1 LED Behaviour

The LED lights on the front of the Vood 322 shows the status of the service, here listed from left to right:

## 1.1 Power

- |       |  |
|-------|--|
| ☀ On  | - The Vood unit is connected to a power supply             |
| ☀ Off | - No power supply is connected or the connection is broken |

## 1.2 Status

- |               |  |
|---------------|--|
| ☀ On          | - Vood 300 unit got a WAN address and successfully contacted VCM |
| ☀ Off         | - No WAN address obtained  |
| ☀ Quick Flash | - Vood 300 unit interacts with VCM i.e. loading software, etc.   |
| ☀ Slow Flash  | - Vood 300 unit tries to contact VCM                             |

## 1.3 WAN

- |       |           |
|-------|-----------|
| ☀ On  | - Link    |
| ☀ Off | - No link |

## 1.4 LAN

- |       |           |
|-------|-----------|
| ☀ On  | - Link    |
| ☀ Off | - No link |

## 1.5 Phone 1 Voip

- |               |  |
|---------------|--|
| ☀ On          | - Channel is registered, or configured not to register |
| ☀ Off         | - Channel failed to register                           |
| ☀ Quick Flash | - Message Waiting                                      |

## 1.6 Phone 1 "Hook"

- |               |                 |
|---------------|-----------------|
| ☀ On          | - Hook off      |
| ☀ Off         | - Hook on       |
| ☀ Quick Flash | - Incoming call |

# 2 Resetting the Vood to Factory Defaults

In order to reset the Vood unit to the original factory settings, use the reset button found on the back of the box inside a small opening next to the power cable. Push the reset button by using a thin pen, needle or similar object, until all LEDs are lit (approximately 15 seconds).

Before resetting the Vood, make sure it has power and that it has booted up properly. Do so by waiting at least 30 seconds after the power cable has been connected before the reset button is pushed.

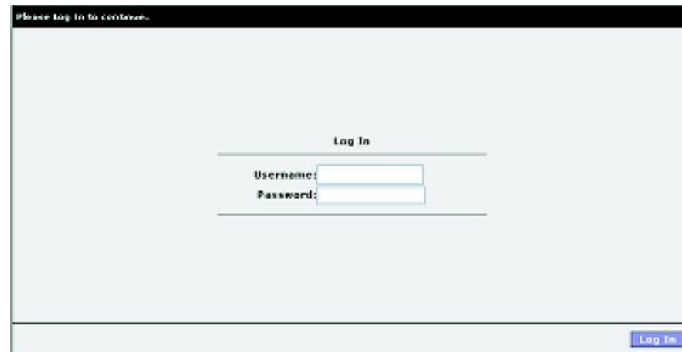
Note: Only the configuration parameters are affected by this reset. The software itself is not reset. (The Vood unit will NOT be restored to the production software.)

Warning: All previously entered configuration data will be lost. This means the Vood unit will have to be configured again.

### 3 Log In to Manual Vood Configuration

To use the web-based management software, connect your computer to the LAN port, launch a suitable web browser and direct it to the IP address of the Vood 300 series unit. Type in the default IP address — <http://192.168.1.1> — in the address bar of the browser. The URL in the address bar should read: <http://192.168.1.1>

A new window will appear and you will be prompted for a user name and password to access the web-based manager.



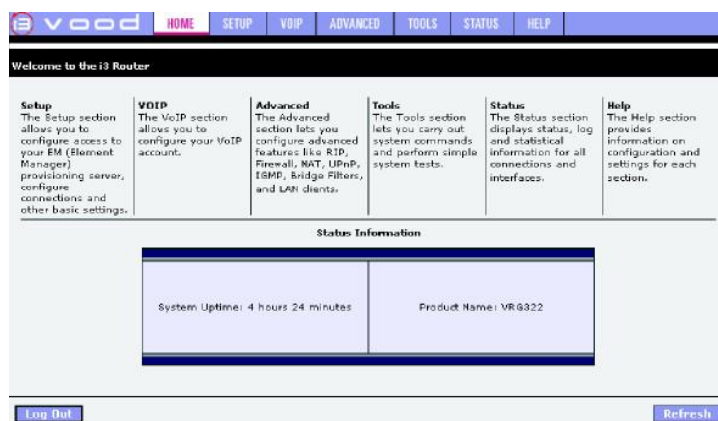
Use the default user name **Conf** and password **admin** for first time setup. You should change the web-based manager access user name and password after you have verified that a connection can be established. The user name and password allows any PC within the same subnet as the Vood unit to access the web-based manager.

Default settings for web-based manager:

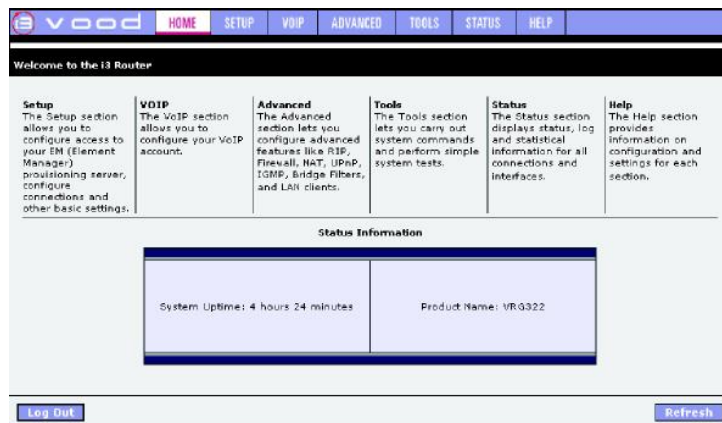
Default IP address: <http://192.168.1.1>

Default User name: **Conf**

Default password: **admin**



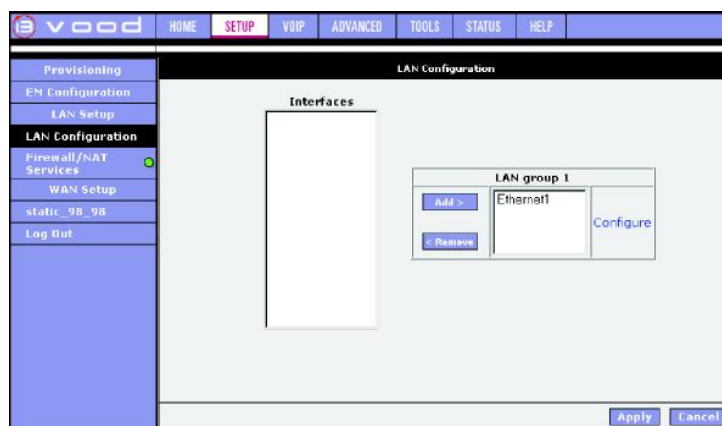
## 4 Setup



Note: To save all changed parameters permanently, you must go to **Tools- >System Commands ->Save All**.

The Setup window offers links to menus that configure settings for the LAN (Local Area Network), FW/NAT Services and for the WAN (Wide Area Network) setup.

### 4.1 LAN Setup



#### 4.1.1 LAN clients

With this feature the end-user can see all the PCs on the LAN segment. Each PC is qualified to be either "**dynamic**" (each PC has obtained a lease from this router) or "**static**" (each PC has a manually configured IP address).

The user can add a "**static**" IP address (belonging to the network segment of the router LAN IP address). Any existing static entry falling within the DHCP server's range can be deleted and the IP address would then be available for future allocation.

Once an IP address is allocated it shows up in the list of LAN clients as a "**dynamic**" entry. Any dynamic entry can be converted into a static entry by using the "**reserve**" checkbox.

Note: Dynamic clients show up in the list only when the DHCP server is running.

### 4.1.2 LAN configuration

The router can be configured to handle up to three LAN groups in which the IP address scheme can be configured as needed. Add interfaces to the chosen LAN group and click on **Configure**.

### 4.1.3 LAN group configuration

The LAN group can use any IP address scheme. You can also use the embedded DHCP server to provide IP settings for DHCP client stations on the LAN Group.

The Ethernet IP address is listed in the top row of the menu. You can type in an IP address that fits within the existing IP scheme or use the default IP address 192.168.1.1 and subnet mask 255.255.255.0. To change the subnet mask, choose a mask that is appropriate for your network from the pull-down menu.

The secondary IP address and secondary subnet mask are used to set up a second subnet on the LAN that uses the router as a default gateway.

The local domain name parameter may be used if the local network uses a domain name system. When you have configured the LAN settings as you want them, click the **Apply** button to commit the new settings and restart the router.

Note: To save all changed parameters permanently, you must Go *Tools- >System Commands ->Save All*.

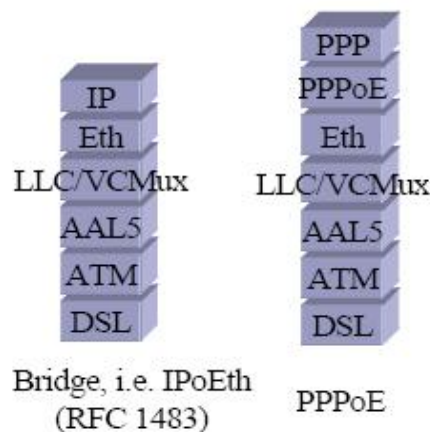
### 4.1.4 Firewall/NAT services

Enable Firewall and NAT service

## 4.2 WAN Setup

### 4.2.1 WAN overview

The Vood unit supports up to 8 virtual connections over the WAN interface. These connections can be of various types depending on what protocols being used.



- PPPoE: Point to Point Protocol over Ethernet
- Bridge: IP over Ethernet

## 4.2.2 Uplink Bandwidth

If a terminal sits behind any sort of modem (ADSL, cable), it is important to configure the bandwidth for the uplink internet connection. This is particularly critical if it's a slow connection (less than 1Mbps) in order to reserve bandwidth for voice traffic so that QoS (Quality of Service) can be achieved even when internet traffic is heavy.

Reserved bandwidth is only allocated during actual voice calls so that performance is still optimized for other functions when there are no ongoing conversations. Units are in Kbps.

## 4.2.3 Vood router WAN-side IP address allocation over virtual connection

For each virtual connection type a different IP allocation method is used:

- **PPPoE:** Dynamic IP address allocation through PPP
- **Bridge:** The virtual connection is bridged to one or more LAN port(s) via the Vood router.
- **Static:** The WAN side of the Vood router is configured with a static IP address
- **DHCP:** The WAN side of the Vood router is configured with a dynamic IP address
- 

## 4.2.4 Subscriber authentication

For PPP connections subscriber authentication is provided by means of PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). Which protocol to use is manually configurable, but the default setting is that protocol selection is made automatically.

## 4.2.5 New connection

The New Connection page allows the creation and definition of up to 8 connections of various types. For each of the connections individual parameter settings can be made.

Each configured "connection name" will appear in the menu to the right, for example VLAN\_5\_DATA in the figure above. In this way created connections can be edited by clicking on the "connection name" to the right.

Note: To save all changed parameters permanently, you must go to **Tools- >System Commands ->Save All**.

#### 4.2.6 PPP connections

**PPP** ("Point-to-Point protocol") is a standard method of establishing a network connection/session between networked devices. Different forms of PPP, including **PPPoE** (PPP over Ethernet"), involve an authentication process that requires a username and password to gain access to the network.

In the New Connection page you can define a name for this virtual connection that you write in the Name field. Then choose connection type from the scroll bar under Type:

- PPPoE as described in RFC 2516, is a method of using PPP over Ethernet networks.

##### **PPP configuration:**

<i>Username:</i>	The username for the DSL access
<i>Password:</i>	The password for the DSL access.
<i>Authentication:</i>	Specifies the authentication protocol required to establish a connection.
<i>On-Demand:</i>	Enable on-demand mode. The connection will disconnect if no activity is detected after the specified idle time-out value.
<i>Idle Timeout:</i>	Specifies that the DSL should be disconnected if the link has no activity detected for n seconds. A non-zero value.
<i>Keep Alive:</i>	When the on-demand option is not enabled, this value specifies the time to wait without being connected to the provider before terminating the connection. A non-zero value.
<i>Set Default route:</i>	Specify connection as the default-route.
<i>MRU:</i>	Maximum Receive Unit sets an upper limit to the packet size the connection can receive. This is a negotiated value that asks the provider to send packets of no more than n bytes. The minimum MRU value is 128.
<i>Enforce: MRU:</i>	Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MRU by changing TCP Maximum Segment Size to PPP MRU.
<i>Debug:</i>	Enables PPP connection debugging facilities.
<i>Connect:</i>	Use the current settings to establish a PPP connection. In "On Demand" mode "Connect" takes no action in establishing connection.
<i>Disconnect:</i>	Disconnects the PPP connection.

##### **Voodoo side of the bridge:**

<i>Sharing of WAN connection:</i>	[Enable, Disable, VLAN]
<i>VLAN ID:</i>	Define IEEE 802.1Q VLAN
<i>Priority bits:</i>	Define IEEE 802.p Class of Service

#### 4.2.7 Bridged connections

"**Bridge**" means a pure bridged connection with no IP address assigned to the router. This connection method makes the router act as a bridge, and just passes packets across the WAN Ethernet port. When the device is used in this manner, it is necessary to install additional connection software on any computer, server or other IP hosts.

In the New Connection page you define a name for this virtual connection. Enter the assigned name in the Name field. Then choose a connection type from the scroll bar under **Type**: Bridge.



### Vood router WAN side

Sharing of WAN connection: [Enable, Disable, VLAN]

VLAN ID: Define IEEE 802.1Q VLAN

Priority bits: Define IEEE 802.p Class of Service

### 4.2.8 DHCP connections

DHCP is used whenever an IP address is to be obtained dynamically

The screenshot shows the Vood router's web interface. The top navigation bar includes links for HOME, SETUP (highlighted), VOIP, ADVANCED, TOOLS, STATUS, and HELP. A left sidebar contains a menu with options: Provisioning, EN Configuration, LAN Setup, LAN Configuration, Firewall/NAT Services, WAN Setup, New Connection, Modem, VLAN\_5\_DATA, VLAN\_4\_IPTV (highlighted), and Log Out. The main content area is titled 'DHCP Connection Setup'. It features a 'Name' field with 'VLAN\_4\_IPTV', a 'Type' dropdown set to 'DHCP', and a 'Sharing' dropdown set to 'VLAN'. Below these are checkboxes for 'Options' (NAT and Firewall) and fields for 'VLAN ID' (set to 4) and 'Priority Bits' (set to 7). The 'DHCP Settings' section includes 'Encapsulation' (radio buttons for LLC and VC, with VC selected), 'IP Address' (NA), 'Mask' (NA), 'Gateway' (NA), and a 'Default Gateway' checkbox. There are 'Renew' and 'Release' buttons. The 'PVC Settings' section includes a 'PVC' dropdown (set to 0/35), 'VPI' (8), 'VCI' (35), 'QoS' (UBR), and fields for 'PCR' (0 kps), 'SCR' (0 kps), 'MBS' (0 cells), and 'CDVT' (0 usecs). At the bottom right are 'Apply', 'Delete', and 'Cancel' buttons.

#### IP stack:

Default Gateway

Choose whether or not the IP default gateway should be configured

Renew button

Renew the IP configuration.

Release button

Release the IP configuration

#### Vood router WAN configuration:

Sharing of WAN connection: [Enable, Disable, VLAN]

VLAN ID: Define IEEE 802.1Q VLAN

Priority bits: Define IEEE 802.p Class of Service

Bridged or Router mode

NAT

Firewall

### 4.2.9 Static connections

Static is used whenever a known static IP is assigned. The accompanying information such as the subnet mask and the gateway should also be specified in order to be able to connect. Up to three Domain Name Server (DNS) addresses can also be specified. These are the servers that enable you to have access to other web servers. Valid IP addresses range from 0.0.0.0 to 255.255.255.255.

#### IP stack

IP Address:

Mask:

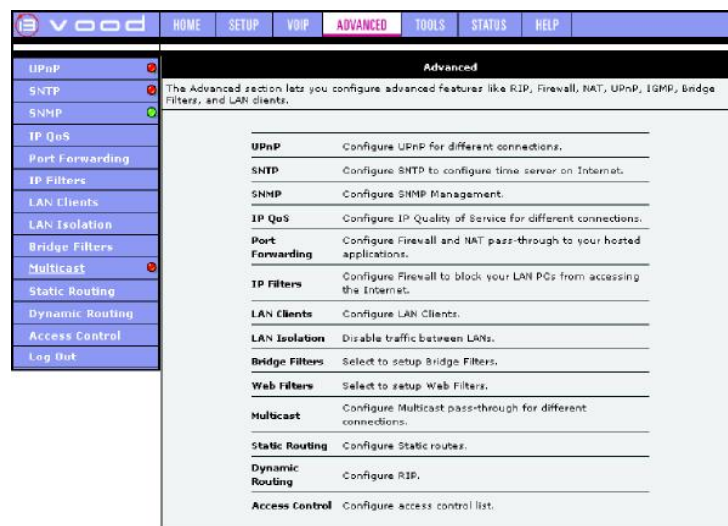
Default Gateway:

DNS 1 to 3:

## Vood router WAN configuration:

Sharing of WAN connection: [Enable, Disable, VLAN]  
VLAN ID: Define IEEE 802.1Q VLAN  
Priority bits: Define IEEE 802.p Class of Service  
Bridged or Router mode  
NAT  
Firewall

## 5 Advanced



Note: To save all changed parameters permanently, you must go to **Tools- >System Commands** ->**Save All**.

### 5.1 UPnP



UPnP NAT and Firewall Traversal allow traffic to pass-through the router for applications using the UPnP protocol. This feature requires one active connection. In presence of multiple connections, select the one over which the incoming traffic will be present, for example the default Internet connection.

## 5.2 SNMP

The screenshot shows the Vood web interface with the 'ADVANCED' tab selected. The left sidebar lists various configuration options, with 'SNMP' highlighted. The main content area is titled 'SNMP Management' and contains the following fields:

- ☒ Enable SNMP Agent
- ☒ Enable SNMP Traps
- Name:
- Location:
- Contact:
- Vendor OID:

Below these fields is a 'Community' section with a table:

Name	Access Right
public	Read Only
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

At the bottom is a 'Traps' section with a table:

Destination IP	Trap Community	Trap Version
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

'Apply' and 'Cancel' buttons are at the bottom right.

Configure SNMP Management

## 5.3 IP QoS (Quality of Service)

IP QoS Engine in the Vood unit is applicable to the output device (egress side), meaning that IP QoS traffic shaping is associated with any transmitted traffic from the perspective of the Vood unit. Each output device has 4 priority queues associated with transmit data. There are 2 high priority queues that have strict priority over medium and low priority queues. The first high priority queue is dedicated to the VoIP traffic generated by the Vood unit and this cannot be configured manually. The medium and low priority queues are serviced on a round robin priority basis according to the con-figured weights (WRR), after the high priority queue has been completely serviced.

The "IP QoS" section under "Advanced section" allows you to set up IP QoS for a connection. The "IP QoS" section has two sub-sections — QoS Setup Page and Rule Setup Page.

### QoS setup page

The QoS setup page allows you to configure IP QoS for a connection, to view the con-figured QoS rules and to add/delete a QoS rule.

The screenshot shows the Vood web interface with the 'ADVANCED' tab selected. The left sidebar lists various configuration options, with 'IP QoS' highlighted. The main content area is titled 'IP QoS' and contains the following fields:

- Choose a connection:
- Low priority weight:
- Medium priority weight:
- Enable IPQoS: ☐
- Trusted Mode: ☐

Below these fields is a table for QoS rules:

Name	Source IP Mask	Source Port Start	Source Port End	Destination IP Mask	Destination Port Start	Destination Port End	Protocol	Priority	Phy Port	TOS	Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

'Add', 'Apply', and 'Cancel' buttons are at the bottom.

**Choose a connection:** This field allows you choose a connection from the list of available connections. For example, choose a WAN connection to enable IP QoS for the upstream traffic of the modem. On the other hand, choose the LAN connection (Ethernet) for the downstream traffic.

**Low/Medium priority weights:** These 2 fields will allow you to select the weights of the medium and low priority queues in increments of 10 percent, so that the sum of the weights of these 2 queues is equal to 100 percent.

**Enable IP QoS:** This field allows you to enable/disable IP QoS for the chosen connection.

**Trusted Mode:** The QoS Engine has two primary modes of operation with regard to queue traffic prioritization — Trusted and Un-Trusted. This field allows you to choose the mode — Trusted (checked) and Un-trusted (Unchecked). In "Trusted mode" all the rules will be applied first, regardless of the setting of the TOS bits. After the rules have been exhausted the existing TOS bit settings will be honored. The "Un-Trusted" mode will match first against all rules as in "Trusted" mode. The difference is that if there is no match then a default rule will be used. The default rule will have an associated queuing priority — low.

**Rules section:** This section displays a list of configured rules, allows you to add a new rule and allows you to delete an existing rule. Each rule has a matching criteria that identifies an application traffic to be transmitted by the QoS engine using one of the 3 configurable priority queues — high, medium and low.

Note: If IP QoS is enabled and no rules are defined, a default rule is added that is hidden. The default rule puts all the traffic to be transmitted in the low priority queue.

The screenshot shows the VooD configuration interface. On the left is a sidebar menu with options: VooD, DHCP, SNTP, SNMP, IP QoS (selected), Port Forwarding, IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Web Filters, Multicast, Static Routing, Dynamic Routing, Access Control, and Log Out. The main area is titled "IP QoS Traffic Rule". It contains several input fields: Rule Name, Source IP, Source Start Port, Destination IP, Destination Start Port, Source Netmask, Source End Port, Destination Netmask, and Destination End Port. There are also dropdown menus for Protocol (set to TCP) and Traffic Priority (set to Low). A Physical Port dropdown is set to None. At the bottom, there is a TOS Marking section with a checkbox for "Normal Service" and a list of options: Minimize monetary cost, Maximize reliability, and Maximize throughput. At the very bottom right are "Apply" and "Cancel" buttons.

This page is invoked when you click on the **Add** button of "**QoS Setup Page**". This page allows you add a rule or matching criteria that identifies an application traffic. The application traffic can be identified by rule name, source/destination IP address and netmask, source/destination port range, protocol and traffic priority.

The traffic priority field corresponds to the priority queue (high/medium/low) for this traffic. The possible options for protocol are — ANY, ICMP, TCP and UDP. Wildcard (\*) entries are allowed for IP address/netmask and port range fields.

The additional TOS marking field allows you to assign a TOS value to this traffic. The values for the TOS marking can be — No Change, Normal Service, Minimize monetary cost, Maximize reliability, Maximize throughput and Minimize delay.

## 5.4 Port Forwarding

Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or to play Internet games.



To configure a service, game or other application, select the external connection (for example the Internet connection), select the computer hosting the service and add the corresponding firewall rule. If you want to add a custom application, select the User category, click **New** and fill in the port, protocols and description for the application. You can also add/edit/delete rules without using the pre-defined firewall policy database (games, services, etc.). Click on "Custom Rules" to access this type of interface. In the presence of the firewall, anonymous Internet traffic is blocked.

## DMZ

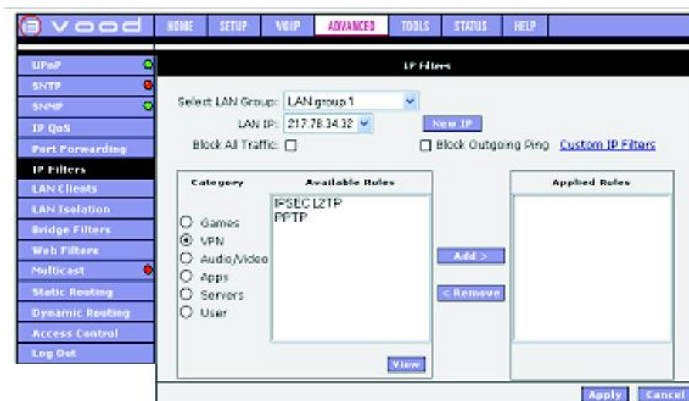
Setting a computer on the local network as a DMZ will forward any network traffic that is not redirected to another computer via the port forwarding feature to the specified computer's IP address. This opens the access to the DMZ computer from the Internet.

## PING

Enabling incoming ping (ICMP) requests on the Port Forwarding page allows the router to respond to a ping from the Internet. Blocking outgoing pings (ICMP) (IP Filters page) generated from a particular LAN IP can be used if the PC has a virus that attempts a Ping-of-Death Denial of Service attack.

## 5.5 IP Filters

This firewall feature allows you to block network access based on a user's computer IP address.



You can use this page to block specific traffic (for example block web access) or any traffic from a computer on the local network. To configure an IP Filter rule select the computers' IP address and add the corresponding firewall traffic definition from the firewall policy database. If the traffic type is set to **"Any"** all network traffic from that computer will be blocked. You can also add/edit/delete IP filter rules without using the pre-defined firewall policy database (games, services, etc.). Click

on "Custom Rules" to access this type of interface.

## 5.6 LAN Clients

Configure LAN Clients.

Delete	IP Address	Hostname	MAC	Type
<input type="checkbox"/>	217.78.34.32			Static

## 5.7 Bridge Filters

The bridge filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type.

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

When bridge filtering is enabled, each frame is examined against each defined filter rule sequentially, and when a match is found, the appropriate filtering action (determined by the access type selected ... i.e. allow or deny) is performed. The user should note that the bridge filter will only examine frames from interfaces that are part of the bridge itself. Up to twenty filter rules are supported with bridge filtering.

The User Interface for Bridge Filter allows the user to add/edit/delete and enable/disable the filter rules. To add a rule, simply define the source MAC address, destination MAC address and frame type with the desired filtering type (i.e. allow/deny), and press the **Add** button. The MAC address must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 as "don't care". Blanks can also be used in the MAC address space and these would be considered as "don't care".

To edit/modify an exist filter rule, select the desired rule created previously from **Add** in the **Edit** select box. The selected filter rule will appear in the top section, as with the "Add" filter rule. Make the desired change to the MAC address, frame type and/or access type, and press **Apply**.



To delete filter rule(s), select the filter rule entry to delete in the **Delete** selection box. Note that multiple deletion is possible. Once all the desired filter rule(s) is/are selected for deletion, press the **Apply** button. The **Select All** select box can also be used to delete all the filter rule. It provides a quick method of selecting all filter rules for deletion.

The **Enable Bridge Filters** button allows the user to enable or disable bridge filtering. It can be set/unset during any add/edit/delete operation. It can also be set/unset independently by just pressing the **Apply** button.

Note: There are three hidden filter rules within the bridge filter table. These rules are entered automatically by the system to ensure that users do not "lock" themselves out of the system. The first rule allows any and all ARP frames through the system. The second rule allows all IPv4 frames with the destination MAC address of the bridge to go through. The third rule allows all IPv4 frames with the source MAC address of the bridge to go through.

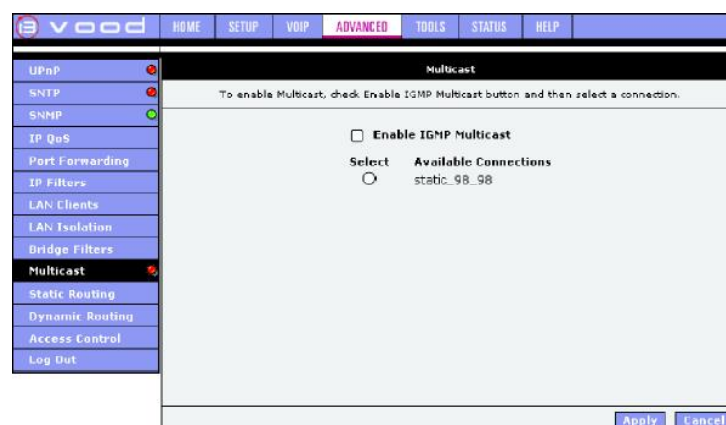
## 5.8 Web Filters

Select to set up Web Filters:

- Proxy
- Cookies
- Java Applets
- ActiveX
- Pop-Ups

## 5.9 Multicast

Configure IGMP multicast for different connections. The Vood unit is capable of proxying for applications that are using multicast IP for accessing video content. This application must be run when NAT is enabled. The IGMP proxy intercepts the join and leave commands for version 1 and 2 IGMP messages. On a join the proxy sets up a multicast route for the interface and PC requesting the video content. It then forwards the join to the upstream multicast router. The multicast IP traffic will then be forwarded to the requesting device. Multicast traffic does not pass through the firewall or through NAT. On a leave the proxy removes the route and then forwards the leave to the upstream multicast router.



However, multicast traffic in a triple play deployment will in most cases not go through routed connections. Instead, the network is structured in separate VLANs where the multicast traffic will

be assigned a separate VLAN that will be mapped onto specific Ethernet port(s).

## 5.10 Static Routing

This page is for configuring static routes over WAN connections

The screenshot shows the Vood web interface with the 'ADVANCED' tab selected. The left sidebar contains a menu with options: UPnP, SNTP, SNMP, IP QoS, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Multicast, Static Routing (highlighted), Dynamic Routing, Access Control, and Log Out. The main content area is titled 'Static Routing'. It features a dropdown menu 'Choose a connection:' with 'static\_98\_98' selected. Below this are input fields for 'New Destination IP:', 'Mask:' (pre-filled with '255.255.255.0'), 'Gateway:', and 'Metric:' (pre-filled with '0'). A message states 'The Routing Table is empty.' At the bottom right are 'Apply' and 'Cancel' buttons.

## 5.11 Dynamic Routing

This page is for configuring RIP

The screenshot shows the Vood web interface with the 'ADVANCED' tab selected. The left sidebar is the same as in the previous screenshot, with 'Dynamic Routing' highlighted. The main content area is titled 'Dynamic Routing'. It contains a checkbox 'Enable RIP' which is unchecked, with a 'Protocol:' dropdown set to 'RIPv2'. Below this is a checked checkbox 'Enable Password' with a 'Password:' input field. At the bottom, there is a table with two columns: 'Interface' and 'Direction'. The table has two rows: 'LAN group 1' and 'static\_98\_98', both with 'Both' in the 'Direction' column. At the bottom right are 'Apply' and 'Cancel' buttons.



## 5.12 Access Control

Open the access from the Internet (WAN) or LAN to the router's management ports (web, SSH, FTP, TFTP, SNMP).

The screenshot shows the Vood router's web interface. The left sidebar contains a menu with items: UPnP, SNTP, SNMP, IP QoS, Port Forwarding, IP Filters, LAN Clients, LAN Isolation, Bridge Filters, Multicast, Static Routing, Dynamic Routing, Access Control (highlighted), and Log Out. The main content area is titled 'Access Control'. It features a checkbox 'Enable Access Control' which is currently unchecked. Below this, a status message reads 'All LAN access allowed, all WAN access denied.' There is a table with three columns: 'Service Name', 'WAN', and 'LAN group 1'. The rows are 'Web', 'TFTP', and 'SNMP'. The 'Web' row has an unchecked checkbox under 'WAN' and a checked checkbox under 'LAN group 1'. The 'TFTP' and 'SNMP' rows have unchecked checkboxes in both columns. Below the table, there is a section for 'IP Access List' with a 'Selected IP' dropdown menu, a 'New IP:' text input field, and 'Delete' and 'Add' buttons. At the bottom right of the main area are 'Apply' and 'Cancel' buttons.

Service Name	WAN	LAN group 1
Web	<input type="checkbox"/>	<input checked="" type="checkbox"/>
TFTP	<input type="checkbox"/>	<input type="checkbox"/>
SNMP	<input type="checkbox"/>	<input type="checkbox"/>

There are security risks associated with this action. For this reason remote management is restricted to computers on the network specified in the IP Access Control List (ACL), a list that can hold up to 16 IP addresses. The ACL provides a global enable/disable that will enable or disable the ACL. If the ACL is disabled, the default behaviour (i.e. DENY on the WAN, Accept on the LAN) is enforced for all IP addresses. If no IP addresses are specified within the ACL, the ACL will be will act as if it is disabled until the first IP address is added.

## 6 Tools

The screenshot shows the Vood router's web interface with the 'TOOLS' tab selected in the top navigation bar. The left sidebar menu is the same as in the previous screenshot. The main content area is titled 'Tools'. It contains a descriptive paragraph: 'The Tools section allows you to save the configuration, restart the gateway, update the gateway firmware, setup user and remote log information and run Ping and Modem tests.' Below this, there are four sections, each with a title and a description: 'System Commands' (Save the current configuration, Restart the gateway, and Restore to factory defaults.), 'Remote Log' (Setup Remote Log Information.), 'User Management' (Configure User Name and password.), and 'Ping Test' (Run a Ping Test.).

The Tools section allows you to save the configuration, restart the gateway, update the gateway firmware, set up user and remote log information and run ping and modem tests.

## 6.1 System Commands

The screenshot shows the vood web interface with the 'TOOLS' tab selected. The left sidebar contains links for System Commands, Remote Log, User Management, Ping Test, and Log Out. The main content area is titled 'System Commands' and contains a description: 'System Commands allow you to carry out basic system actions. Press the button to execute a command.' Below this are three buttons: 'Save All', 'Restart', and 'Restore Defaults'. Each button has a corresponding instruction: 'Save All' is for saving the current configuration; 'Restart' is for restarting the system, with a note that connectivity will be lost; 'Restore Defaults' is for restoring factory default configuration, also with a note about lost connectivity.

Save the current configuration, restart the gateway and restore to factory defaults.

## 6.2 Remote Log

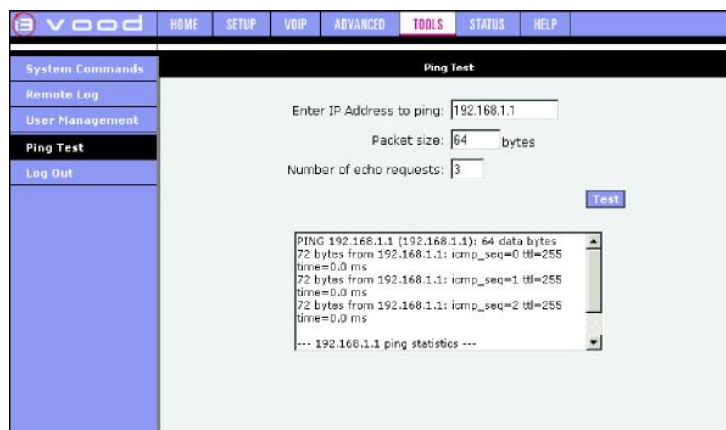
Set up Remote Log Information.

## 6.3 User Management

The screenshot shows the vood web interface with the 'TOOLS' tab selected. The left sidebar contains links for System Commands, Remote Log, User Management, Ping Test, and Log Out. The main content area is titled 'User Management' and contains a form with four input fields: 'User Name' (containing 'Conf'), 'Old Password', 'Password', and 'Confirmed Password'. Below the fields is a 'Save Changes' button.

Configure User Name and password.

## 6.4 Ping Test



**vood** HOME SETUP VOIP ADVANCED **TOOLS** STATUS HELP

System Commands  
Remote Log  
User Management  
**Ping Test**  
Log Out

**Ping Test**

Enter IP Address to ping:

Packet size:  bytes

Number of echo requests:

```
PING 192.168.1.1 (192.168.1.1): 64 data bytes
72 bytes from 192.168.1.1: icmp_seq=0 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=1 ttl=255
time=0.0 ms
72 bytes from 192.168.1.1: icmp_seq=2 ttl=255
time=0.0 ms
--- 192.168.1.1 ping statistics ---
```

Run a ping test.

## 7 Status



**vood** HOME SETUP VOIP ADVANCED **TOOLS** **STATUS** HELP

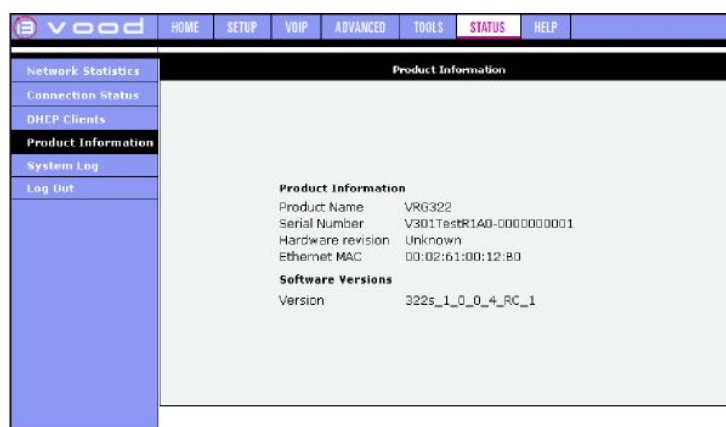
Network Statistics  
Connection Status  
DHCP Clients  
Product Information  
System Log  
Log Out

**Status**

The Status section allows you to view the Status/Statistics of different connections and interfaces.

- Network Statistics** View the Statistics of different interfaces - Ethernet.
- Connection Status** View the Status of different connections.
- DHCP Clients** View the list of DHCP clients.
- Product Information** View the Product Information and Software Versions.
- System Log** View the Log messages.

Information about the current status of the Vood unit can be accessed on the Product Information page of the Vood web interface (an option under the Status tab). See section 9 “**Log In to Manual Vood Configuration**” for information on how to access this web interface.



**vood** HOME SETUP VOIP ADVANCED **TOOLS** **STATUS** HELP

Network Statistics  
Connection Status  
DHCP Clients  
**Product Information**  
System Log  
Log Out

**Product Information**

Product Name: VRG322  
Serial Number: V301TestR140-000000001  
Hardware revision: Unknown  
Ethernet MAC: 00:02:61:00:12:B0

**Software Versions**

Version: 322s\_1\_0\_0\_4\_RC\_1

## 8 Help

Help for the following topics are available on the Help page:

- Firewall
- Bridge Filters
- LAN Clients
- PPP Connections
- UPnP
- IP QoS



## 9 Login to Vood User Pages Configuration

To enter the user pages configuration interface:

1. Connect your computer to the LAN port
2. Open a suitable web browser
3. Enter “<http://192.168.1.1:8080/user>” in the web address field
4. Enter a username and password when the login page appears

The user pages are locked by default for security reasons and you need to contact the Customer Service to unlock these pages and also to supply you with your unique username and password. Once you are logged in, you should change your password to something only you know.

## 10 Services

This chapter contains the services supported by the Vood 322.

### 10.1 Call Waiting with Call Hold

#### 10.2 Call waiting Default: On

During an established call:

- If you do not want to answer the waiting call, press **R 0**. If call forwarding on busy or answering machine on busy is configured, the appropriate service will then be activated. Otherwise, the waiting call will get a busy signal. If you do not answer the waiting call within a specified time, action will be taken as if **R 0** had been pressed.
- If you do want to answer the waiting call, press **R 2**.
- To switch back to the original call, press **R 2** again.
- Pressing **R 2** a number of times will switch back and forth between the two calls.
- Pressing **R 1** will finish the current call. When you press **R 1** you will also automatically switch to the other call.

### 10.3 Inquiry Call with Call Hold

When you have established a call with person 1, press **R** to start a new call. Dial the number to person 2 and wait for an answer. When both calls have been established, you can press **R 2** to switch back and forth between the two calls. Press **R 1** to terminate one of the calls and switch to the other.

### 10.4 Message Waiting

If an incoming call is diverted to the answering machine, the LEDs will flash: they will alternate between on for 100 ms, and off for 100 ms. The message waiting indication can be cancelled by lifting the receiver.

### 10.5 Three-Way Conferencing

To start three-way conferencing, perform the *inquiry call* service, then press **R 3**.

If a call is waiting, answer the waiting call with **R 2** and then press **R 3** to establish three-way conferencing.

### 10.6 Click to Dial Service

It is possible to use *click to dial* from the web server's phone lists. If a stored number is clicked and the receiver is lifted within 15 seconds, that number is dialed automatically. It is also possible to first lift the receiver and then click the number. In this case the number will be dialed directly.

## 10.7 Fast Re-Dial Service

To repeat the last dialed number, press the asterisk key three times **\*\*\*** on your phone keypad.

## 10.8 Answering Machine Service

The Vood unit's built-in answering machine works in conjunction with a possible email server. The answering machine records messages to sound files that are stored locally and can append them to emails sent to a specified email address. The local sound files can be administrated using the telephone. The email sound files can be listened to by opening the email in an e-mail client.

Note: Please note regarding the answering machine service:

- The locally stored sound files are NOT stored permanently. This means that if the Vood unit loses power or reboots due to manually entered configuration changes, etc., the locally stored messages will be lost. So usage of the email function is recommended.
- The amount of storage is limited on the Vood unit so when the storage area is full the oldest message will automatically be removed. The number of messages that can be stored locally is currently 10 for each telephone port on the Vood unit. Each message has a maximum length of about 40 seconds.

The answering machine may be managed either from an analog phone or a web page.

### 10.8.1 Mail configuration

#### Mail address 1 (user parameter)

The user must define a mail address in the Vood unit, to indicate where recorded messages should be sent. This parameter can be found in the user-specific web page <answering machine>.

The parameter is: mail address 1.

Default: -

Example:

john.smith@home.se

#### Mail address 2 (user parameter)

Mail address 2 is optional. It can be used if the recorded message should also be sent to a second email address.

Default: —

#### SMTP address (user parameter)

The email server to contact has to be configured in the parameter SMTP address.

Default: —

Example:

mailserver.company.se

When the mail address and SMTP address have been defined, a test mail can be sent with the current settings. To do this, click the Test Mail button in the user-specific <answering machine> web page.

### 10.8.2 Administration of locally stored messages

By using the telephone and dialling the code \*51# you can administer your recorded messages. After dialling the code the Vood unit will automatically play every recorded message in the order they were recorded. When no more messages are available a continuous beeping is played.

### 10.8.3 Recording a greeting message

You also need to record a greeting message. This can be done either from the web interface or from the telephone. The greeting message has a maximum length of about 20 seconds.

### 10.8.4 Redirect to the answering machine

It is possible to redirect calls to the answer machine in three different ways.

- Immediately directed to the answering machine.
- Directed to the answering machine on busy.
- Directed to the answering machine if there is no answer within a specified time.

## 10.9 Service Calling Line ID Restriction for Anonymous Calling

For outgoing calls from the terminal, the following procedure can be applied to suppress calling line ID presentation at the called party end. This restriction will be valid for one call:

Press \*31# to activate calling line ID restriction for the next outgoing call. A dial tone will indicate that the service has been activated.

The service will be disabled automatically when the call is terminated.

## 11 NAT and Firewall Overview

The Vood router uses Network Address Translation (NAT) and a Stateful Packet Inspection (SPI) firewall to protect the home network. The NAT and firewall service can be globally (for LAN and all WAN connections) disabled/enabled from the Setup Firewall/NAT Service page. If disabled, no NAT functionality or firewall protection can be provided. For each WAN connection (e.g., Internet connection) the NAT and fire-wall can be enabled/disabled. With the firewall enabled on a WAN connection all incoming packets are examined by the SPI engine and traffic is dropped if it does not match an existing connection opened from LAN side or a port forwarding rule. Connections from the LAN side to the Internet are trusted and allowed to pass through the router unless explicit IP filter rules are used to block such LAN traffic. This asymmetric permissive firewall setup (drop from WAN, allow from LAN) provides easy to use Internet access while protecting the home network.

## **12 Services**

### **12.1 Port Forwarding**

With the Port Forwarding page you can provide local services (for example, web hosting) for people on the Internet or allow Internet games. To configure a service, game or other application, select the external connection (for example the Internet connection), select the computer hosting the service and create an appropriate firewall rule. If you want to add a custom application, select the User category, click New and fill in the port, protocols and description for the application. You can also add/edit/delete rules without using the pre-defined firewall policy database (games, services, etc.). Click on "Custom Rules" to access this type of interface. In the presence of the fire-wall, anonymous Internet traffic is blocked.

### **12.2 IP Filters**

This firewall feature allows you to block network access based on a user's computer IP address. You can use this page to block specific traffic (for example, block web access) or any traffic from a computer on the local network. To configure an IP filter rule, select the computer's IP address and add the corresponding firewall traffic definition from the firewall policy database. If the traffic type is set to "Any", all network traffic from that computer will be blocked. You can also add/edit/delete IP filter rules without using the pre-defined firewall policy database (games, services, etc.). Click on "Custom Rules" to access this type of interface.

### **12.3 Access Control**

Open the access from the Internet (WAN) or LAN to the router's management ports (web, SSH, FTP, TFTP, SNMP). There are security risks associated with this action. For this reason remote management is restricted to computers on the network specified in the IP access control list, a list that can hold up to 16 IP addresses. The access control list provides a global enable/disable that will enable or disable the Access Control List (ACL). If the ACL is disabled, the default behaviour (i.e. DENY on the WAN, Accept on the LAN is enabled for all IP addresses) is enforced. If no IP addresses are specified within the ACL, the ACL will act as if it is disabled until the first IP address is added.

### **12.4 DMZ**

Setting a computer on the local network as DMZ forwards any network traffic that is not redirected to another computer via the port forwarding feature to the computer's IP address. This opens access to the DMZ computer from the Internet.

### **12.5 PING**

Enabling incoming ping (ICMP) requests on the Port Forwarding page allows the router to respond to a ping from the Internet. Blocking outgoing pings (ICMP) (IP Filters page) generated from a particular LAN IP can be used if the PC has a virus that attempts a Ping-of-Death Denial of Service attack.