| Parameter | Description |
|------------------|--|
| Confirm Password | Confirm password |
| MTU | Leave the Maximum Transmission Unit (MTU) at the default value unless instructed by your ISP |

1483 Routing

| | ATM1 |
|-----------------|----------------|
| Protocol | 1483 Routing |
| IP Address | 0.0.0.0 |
| Subnet Mask | 0.0.0.0 |
| Default Gateway | 0.0.0.0 |
| VPI/VCI | 1 /32 |
| Encapsulation | |
| QoS Class | UBR - |
| PCR/SCR/MBS | 4000 /4000 /10 |
| DHCP Client | |

| Parameter | Description |
|-----------------|--|
| IP Address | Enter the IP address provided by your ISP. |
| Subnet Mask | Enter the subnet mask address provided by your ISP. |
| Default Gateway | Enter the gateway address provided by your ISP. |
| VPI/VCI | Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP. |
| Encapsulation | Select the encapsulation used by ISP from the drop down list. |
| QoS Class | ATM QoS classes including CBR, UBR and VBR |
| PCR/SCR/MBS | QoS Parameters - PCR, SCR and MBS are configurable. |
| DHCP Client | Check the box if your ISP assigns an IP address dynamically. |

CONFIGURATION PARAMETERS

PPP₀E

| | ATM1 |
|--------------------|---------------------------------|
| Protocol | PPPoE 🔽 |
| VPI/VCI | 1 /32 |
| Encapsulation | LLC 🔽 |
| QoS Class | UBR - |
| PCR/SCR/MBS | 4000 /4000 /10 |
| IP assigned by ISP | Yes 🗸 |
| IP Address | 0.0.0.0 |
| Subnet Mask | 0.0.0.0 |
| Connect Type | Auto - Triggered by traffic 🛛 💌 |
| Idle Time (Minute) | 20 |
| Username | t0338890 |
| Password | **** |
| Confirm Password | **** |
| MTU | 1492 |

| Parameter | Description |
|-----------------------|--|
| VPI/VCI | Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP. |
| Encapsulation | Select the encapsulation used by ISP from the drop-down menu. |
| QoS Class | ATM QoS classes including CBR, UBR and VBR |
| PCR/SCR/MBS | QoS Parameters - PCR, SCR and MBS are configurable. |
| IP assigned by ISP | Select yes, if your ISP assigns IP address dynamically. |
| IP Address | If you have selected "No" in the previous field, type in the IP address provided by your ISP. |
| Subnet Mask | Enter the subnet mask address provided by your ISP. |
| Connect Type | Sets connection mode to Always connected, Auto-Triggered by traffic or Manual connection. For flat rate services use Always connected. |
| Idle Time (Minute) | Enter the maximum idle time for the Internet connection. After this time has been exceeded the connection will be terminated. This setting only applies when the Connect Type is set to Auto-Triggered by traffic. |
| Username | Enter user name. |
| Password | Enter password. |

| Parameter | Description |
|------------------|---|
| Confirm Password | Confirm password |
| MTU | Leave the Maximum Transmission Unit (MTU) at the default value unless instructed by your ISP. |

IP Over RFC1483 bridged

| | ATM1 |
|-----------------|---------------------------|
| Protocol | IP over RFC1483 bridged 💌 |
| IP Address | 0.0.0.0 |
| Subnet Mask | 0.0.0.0 |
| Default Gateway | 0.0.0.0 |
| VPI/VCI | 1 /32 |
| Encapsulation | LLC 💽 |
| QoS Class | UBR 🔽 |
| PCR/SCR/MBS | 4000 / 4000 / 10 |
| DHCP Client | |

| Parameter | Description |
|-----------------|--|
| IP Address | Enter the IP address provided by your ISP. |
| Subnet Mask | Enter the subnet mask address provided by your ISP. |
| Default Gateway | Enter the gateway address provided by your ISP. |
| VPI/VCI | Enter the Virtual Path Identifier (VPI) and Virtual Circuit Identifier (VCI) supplied by your ISP. |
| Encapsulation | Select the encapsulation used by ISP from the drop-down menu. |
| QoS Class | ATM QoS classes including CBR, UBR and VBR |
| PCR/SCR/MBS | QoS Parameters - PCR, SCR and MBS are configurable. |
| DHCP Client | Check the box if your ISP assigns an IP address dynamically. |

Clone MAC Address

Some ISPs require you to register your MAC address with them. If this is the case, and you have previously registered the MAC address of another device, the MAC address of the Barricade must be changed to the MAC address that you have registered with your ISP.



DNS

A Domain Name Server (DNS) is an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.smc.com, a DNS server will find that name in its index and find the matching IP address: xxx.xxx.xxx. Most ISPs provide a DNS server for speed and convenience. Since your Service Provider may connect to the Internet with dynamic IP settings, it is likely that the DNS server IP's are also provided dynamically. However, if there is a DNS server that you would rather use, you need to specify the IP address here.



LAN

The LAN settings menu allows you to change the default IP address of the Barricade, modify the DHCP server settings.

| http://192.168.2.1 | 1/Index.stm - Microsoft Internet Explorer | _ (7) × |
|--|--|-----------------|
| Address () http://192.16 | 8.2.1/index.stm | . 🗭 |
| SMC® | Advanced | |
| " SETUP WIZARD SYSTEM WAN LAN NITELESS NAT ROUTING FIREWALL SYNTH UPAP AOSL DONS TOOLS STATUS | LAN Settings The care make DHC of dynamically allocate IP address are your cleant PCs, or configure Ritering on specific blead or protects: The router mutation and the scale network. LAN IP IP Address Pool IP Address Pool | Arrotions based |
| | Start 1P 192 168 2 100 | |
| | End 1P 192 | |
| | Demain Name | |
| | HELP SAVE SET | TTINGS Cancel |

| Parameter | Description |
|-------------------------------------|--|
| LAN IP | |
| IP Address | The IP address of the Barricade. |
| IP Subnet Mask | The subnet mask of the Barricade. |
| DHCP Server | This option allows you to enable or disable the DHCP server function. By default DHCP is enabled. |
| Lease Time | Allows you to select a pre-defined lease time for IP addresses assigned using DHCP. For home networks this may be set to Forever, which means there is no time limit on the IP address lease. |
| IP Address Pool | |
| Start IP Address/ End IP address | Specify the start/end IP address of the DHCP pool. Do not include the gateway address of the Barricade in the client address pool. If you change the pool range, make sure the first three octets match the gateway's IP address, i.e., 192.168.2.xxx. |
| Domain Name | If your network uses a domain name, enter it here. Otherwise, leave this field blank. |

Wireless

The router also operates as a wireless access point, allowing wireless computers to communicate with each other. To configure this function, all you need to do is enable the wireless function, define the radio channel, the domain identifier, and the security options.

| http://192.168.2.3 | 1/index.stm - Microsoft Internet Explorer |
|--|--|
| Address http://192.16 | 58.2.1/index.stm |
| SMC® | |
| SETUP WIZARD SYSTEM WAN LAN LAN WIRELESS Common and parts Arcrang Lowers WIRE WIRE | Wireless Settings The router can be quickly configured as an wireless access point for roaming clients by setting the service set identified (SSID) and channel number. It also supports data encryption and client filtering. Enable or disable Wireless module function : * Enable * Clicable |
| NAT | |
| ROUTING FIREWALL SNMP UPNP ADSL DDNS TOOLS STATUS | |

• Enable or disable Wireless module function: select to enable or disable the wireless function.

Channel and SSID

You must specify a common radio channel and SSID (Service Set ID) to be used by the router and all of its wireless clients. Be sure you configure all of its clients to the same values.



| Parameter | Description |
|----------------|--|
| SSID | This is the Service Set ID. The SSID must be the same on the router and all of its wireless clients. |
| SSID Broadcast | Select to enable/disable the brocasting of SSID. Enable this function for easy connection for the clients. Disable this function for increased security. |
| Wireless Mode | The Router supports 11n, 11g, and 11b wireless networks. |
| | SMC recommend using "Mixed 802.11n, 802.11g and 802.11b" to provide compatibility with 11n, 11g and 11b wireless clients. |
| Channel | This is the radio channel used for wireless communication. |

| Parameter | Description |
|-------------------|---|
| Bandwidth | Select the bandwidth: |
| | •20 MHz: Sets the operation bandwidth as 20 MHz. when 20 MHz is selected, there would be no extension channel available. |
| | •20/40 MHz: Allows automatic detection of the operation bandwidth between 20 and 40 MHz. Choosing this mode allows you to use the extension channel. |
| Extension Channel | This is the optional channel for use. Setting the Bandwith to 20/40 MHz allows you to use this extension channel as the secondary channel for doubling the bandwith of your wireless network. |
| Protected Mode | In most situations, best performance is achieved with Protected Mode turning Off. If you are operating in an environment with heavy 802.11b traffic or interference, best performance may be achieved with Protected Mode turning On. |
| 802.11e/WMM QoS | Select to turn on/turn off the QoS function. |

- **Notes: 1.** When bandwidth is set to 20 MHz, there would be no extension channel that can be selected. The extension channel is based on the main or primary channel. When the main channel is set to channel 1, channel 5 will be used as the extension channel. When the main channel is set to 9, the extension channel can be channel 5 or 13.
 - **2.** The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Access Control

Using the Access Control functionality, you can restrict access based on MAC address. Each PC has a unique identifier known as a Medium Access Control (MAC) address. With MAC filtering enabled, the computers whose MAC address you have listed in the filtering table will be able to connect (or will be denied access) to the router.

| http://192.168.2. | 1/index.stm - Micros | oft Internet Explo | orer | | _ | - | | | _ 8 × |
|--|--------------------------------|--|--------------------------|-------------|------------|------------|--------------|------------------|-----------------|
| Address Address Address | 58.2.1/index.stm | | | - 1 F | le Edit | View Far | vorites Too | ks Help | |
| SMC® | | | | | 1 | | | et llome. | Rief) Okoșed |
| » SETUP WIZARD | Access Conto | 1 | | | 3 | | | | - |
| SYSTEM | Access Contr | 01 | | | | | | | |
| WAN | For a more secure | wireless network yo | ou can spe | cify that o | nly certai | n Wireless | PCs can co | nnect to the Aci | cess Peint. Up |
| LAN | to 32 MAC address | ies can be added to knows Dule | the MAC F | iltering Ta | ible, Whet | r enabled, | al registers | d MAC addresse | s are |
| WIRELESS | Contrained by the s | SECTOR PLANE. | | | | | | | |
| Change deal | Enable MAG | Filtering : Cite | s @No | | | | | | |
| Access Longer | | | | | | | | | |
| VEP VITA 802.1% | MAC Addres | ss Filtering List | ic address | 1 1 205 | ow is De | ny. | | | |
| PW-T) Protected Bellin PIN PBC Manufi | Wreless DHC MAC Filterin | P Client List: 19=19 ng Table (up to 32 | 2.168.2.101 stations) | name=test- | pc | • • | OPY TO 1 | 3 | - |
| NAT | 10 | | | Ma | C Address | | | | |
| ROUTING | 4 | 00 | : 00 | : 00 | : 00 | : 00 | : 00 | | |
| FIREWALL | 2 | 00 | ; 00 | ; 00 | ; 00 | ; 00 | ; 00 | | |
| SNMP | | m | . 00 | . 100 | . 00 | . 00 | . 00 | | |
| UPnP | | 50 | - 100 | - 100 | - 100 | 1 100 | | | |
| ADSL | _ | 10 | : 00 | : 100 | : [00 | : 100 | : 100 | | |
| DDNS | 5 | 00 | : 00 | : 00 | : 00 | : 00 | :]00 | | |
| TOOLS | 6 | 00 | : 00 | : 00 | : 00 | ; 00 | : 00 | | |
| STATUS | 7 | 00 | : 00 | : 00 | : 00 | : 00 | : 00 | | |
| | p | 00 | ; 00 | : 00 | : 00 | ; 00 | : 00 | | |
| | | 100 | - 60 | 600 | 60 | 600 | 00 | | |

- Enable MAC Filtering: select to enable or disable this function.
- Access Rule for registered MAC address: select to allow/deny access for the registered MAC addresses. Selecting Allow means only MAC addresses registered here will be able to connect to the router. Selecting Deny means only the MAC addresses registered here will be denied access to the router.
- Wireless DHCP Client List: use the drop down list to quickly copy the current entry to the table.
- MAC Filtering Table: you can enter up to 32 stations to the table.

Security

To make your wireless network safe, you should turn on the security function.



Allowed Client Type:

- No WEP, No WPA this means no security mechanism will be used on your wireless network.
- WEP only this menas only WEP will be used for your wireless communication.
- WPA only this means only WPA will be used for the wireless network.

$W\!EP$

| http://192.168.2.1/6 | ndex.stm - Microsoft Internet Explorer |
|------------------------------|---|
| Address () http://192.168.2. | 1/index.stm |
| SMC® | |
| . SETUP WIZARD | 4 |
| SYSTEM | WEP |
| WAN LAN | WEP is the basic mechanism to transmit your data securely over the wireless network. Matching encryption keys must be setup on your router and wireless client devices to use WEP. |
| WIRELESS | The second s |
| - Change and Saru | WEP Mode @ 64-bit C 128-bit |
| . Leturh | Key Entry Method Rev CASCII |
| WEP WITA 802.1% | Key Provisioning 🖉 Static C Dynamic |
| - Wi-Ti Troucted Eek- | Static WEP Key Setting |
| PIN PBC Manual | 10/26 hex digits for 64-WEP/128-WEP |
| NAT | Defailt Key (D) |
| ROUTING | |
| FIREWALL | Passphrase (1~32 characters) |
| UPnP | Novi 1 |
| ADSL | |
| DDNS | Kay 2 |
| TOOLS | Koy 3 |
| STATUS | Key 4 |
| | Clear |
| Parameter | Description |
| WEP Mode | Select 64 bit, or 128 bit. |
| Key Entry M | fethod Select Hex, or ASCII. |
| | |

Key ProvisioningSelect Static, or Dynamic. If you select Static, you
will need to configure the Static WEP Key Setting
section. If you choose Dynamic, then 802.1X
authentication should be enabled.

To automatically generate encryption keys using the passphrase function, when Key Entry Method is set to **Hex**, enter a string into the passphrase field, then click **Generate**. Select the **Default Key ID** from the drop-down menu and click **SAVE SETTINGS**.

To manually configure the encryption key, enter five hexadecimal pairs of digits for each 64-bit key, or enter 13 pairs for the single 128-bit key.

Note: A hexadecimal digit is a number or letter in the range 0-9 or A-F. The passphrase can consist of up to 32 alphanumeric characters.

WPA

Wi-Fi Protected Access (WPA) combines temporal key integrity protocol (TKIP) and 802.1X mechanisms. It provides dynamic key encryption and 802.1X authentication service. The router supports both WPA and WPA2.



| Parameter | Description |
|---------------------|---|
| WPA mode | Select WPA, WPA2 or mixed mode. |
| Cypher suite | Select the encryption cypher for use. |
| Authentication | Choose 802.1X or Pre-shared Key to use as the authentication method. |
| | •802.1X: for the enterprise network with a RADIUS server. |
| | •Pre-shared key: for the SOHO network environment without an authentication server. |
| Pre-shared key type | Select the key type to be used in the Pre-shared Key. |
| Pre-shared Key | Enter the key string here. |
| Group Key Re_Keying | Define the time period for re-obtain the key. |

802.1X

Server Port

If 802.1X is used in your network, then you should enable this function for the router.

| http://192.168.2.1 | /index.stm - Microsoft Internet Explorer |
|---|--|
| Address 1 http://192.168 | 2.1/index.stm |
| SMC° | Advanced State |
| » SETUP WIZARD System Wan Lan Widel csc | 802.1X This page allows you to set the 802.1%, a method for performing authentication to wireless connection. These parameters are used for this access point to connect to the Authentication Server. |
| Chuncel and S210 | BI2.3X Authentication C Enable C Disable |
| Attess Dontrol | Section Mar Tenuent BTD - Records (0 for on timeral absolute) |
| WPA | Re-Authentication Percei 3500 Seconds (0 for no re-euthentication) |
| Wh FJ Protected Setup | Quist Period 60 Seconds after authentication failed |
| PIN PBC | Server Type RADUS |
| NAT | RADIUS Server Parameters |
| ROUTING | |
| FIREWALL | Server 12 [192 . [160 . [2 .]] |
| SNMP | Server Port 1812 |
| IDSL | Sarrat Kay |
| DDNS | |
| TOOLS | NAS-ID |
| | |

| Parameter | Description | | |
|-----------------------------|--|--|--|
| 802.1X authentication | Choose to enable or disable this function. | | |
| Session Idle Timeout | Defines a maximum period of time for which the connection is maintained during inactivity. | | |
| Re-Authentication Period | Defines a maximum period of time for which the authentication server will dynamically re-assign a session key to a connected client. | | |
| Quiet Period | Defines a maximum period of time for which the router will wait between failed authentications. | | |
| Server Type | Select RADIUS. | | |
| RADIUS Server Parameters | | | |
| Server IP | Enter the authentication server IP address. | | |

Enter the port number.

| Parameter | Description |
|------------|--|
| Secret Key | The secret key shared between the authentication server and its clients. |
| NAS-ID | Defines the request identifier of the Network Access Server. |

WPS (Wi-Fi Protected Setup)

The Barricade was implemented with the ease-of-use Wi-Fi Protected Setup (WPS). WPS makes a secure wireless network much easier to achieve by using a PIN number and the Push Button Control (PBC).



- Enable or disable WPS features: select to enable or disable.
- Generate New PIN: click this button to create a new PIN.
- Restore Default PIN: click this button to restore the PIN.

PIN

Enter the PIN of the client device and click **Start PIN**. Then start WPS on the client device from it's wireless utility or WPS application within 2 minutes.



Take the following steps for easy network security settings.

- 1. Power on your client device supporting WPS PIN code method.
- 2. Start WPS PIN process on client device. For instructions on how to do this refer to the client devices user manual.
- 3. Enter the PIN code of client device. Note: The PIN code is generally printed on the bottom of the unit or displayed in the utility.
- 4. Click the **Start PIN** button on the screen.

PBC (Push Button Configuration)

To achieve successful WPS connection, you can use one of the following ways:



(1) push and hold the WPS button on this router for 4 seconds

or

(2) click the Start PBC button on this screen.

Now click the WPS button on the client device which you are connecting. Make sure the client device is powered on.

Note: This connection procedure must be done within 2 minutes after pressing the WPS button on the router.

Manual

For client devices without the WPS function, you should manually configure the client device with the settings on this screen.



NAT

Network Address Translation (NAT) allows multiple users to access the Internet sharing one public IP.



• Enable or disable NAT module function: select to enable or disable this function.

Address Mapping

Allows one or more public IP addresses to be shared by multiple internal users. This also hides the internal network for increased privacy and security.



- Enter the Public IP address you wish to share into the Global IP field.
- Enter a range of internal IPs that will share the global IP into the "from" field.

Virtual Server

If you configure the Barricade as a virtual server, remote users accessing services such as web or FTP at your local site via public IP addresses can be automatically redirected to local servers configured with private IP addresses. In other words, depending on the requested service (TCP/UDP port number), the Barricade redirects the external service request to the appropriate server (located at another internal IP address).



For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.2.2/80, then all HTTP requests from outside users will be transferred to 192.168.2.2 on port 80. Therefore, by just entering the IP address provided by the ISP, Internet users can access the service they need at the local address to which you redirect them.

The more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.

A list of ports is maintained at the following link: http://www.iana.org/assignments/port-numbers.

Special Application

Some applications require multiple connections, such as Internet gaming, video-conferencing, and Internet telephony. These applications may not work when Network Address Translation (NAT) is enabled. If you need to run applications that require multiple connections, use these screens to specify the additional public ports to be opened for each application.

| File Edit View Favor | ites Tools Help | Address http://192 | 168.2.1/index.stm | | - |
|---|--|--|--|---|---|
| SMC [®] | | | Adv | anoed | a B Lopeut |
| SETUP WIZARD YSTEM AN AN IRELESS | Special App Some application others. These ap applications that Port' field, selec open them for in | lication is require multiple connect program withple connect to the protocol type as TC bound traffic. | tions, such as Internet gaming, vider hen Network Address Translation (NA- ons, specify the port normality associ P or UDP, then enter the public ports | a conferencing, internet / art) is enabled. If you nee ated with an application r associated with the trig | telephony and of to run in the "Trigge ger port to |
| AT Addisus Macping Villuar Server | Note: The range | of the Trigger Ports is fr Trigger Type | om 1 to 65535. Public Port | Public Type | Enabled |
| Special Application NAT Mapping Table | 1. | | | C TCP | E |
| OUTING REWALL | 2. | G TCP | | F TCP C UDP | F |
| IMP PnP | 3. | F TCP | | F TCP C UDP | E |
| DSL DNS | 4. | C UDP | | IF TOP | E |
| DOLS | 5. | C UDP | | A TCP | P |
| Constant of the local division of the local | 6. | C UDP | | C LOP | F |
| | | # TCP | | @ TCP | - |

• Use the Popular applications drop down menu to quickly copy the entry to the table.

NAT Mapping Table

This screen displays the current NAPT (Network Address Port Translation) address mappings. Click **Refresh** to update the table.



Routing

These screens define routing related parameters, including static routes and RIP (Routing Information Protocol) parameters.

Static Route

Subnet Mask

Gateway

| 2 http://192.168.2. | 1/index.stm - Mic | rosoft Internet Explorer | _ (7) × |
|--|--|---|-------------------------|
| File Edit View Faw SINCE SYSTEM VAN LAN WIRELESS NAT ROUTING = State Fount = State Foun | Static Roul Please Enter th Tedas 2011 | Address (E) http://02.166.2.j/ndoc.dm Address (E) http://02.166.2.j/ndoc.dm PERENT PERENT PERENT PERENT No Valid Static Route Entry III HERP | SAVE SETTINOS Cancel |
| Parameter | | Description | |
| Index | | Check the box of the route you w | vish to delete or modif |
| Network Ad | dress | Enter the IP address of the remo to set a static route. | te computer for which |

Click **Add** to add a new static route to the list, or check the box of an already entered route and click **Modify**. Clicking **Delete** will remove an entry from the list.

to set a static route.

network.

Enter the subnet mask of the remote network for which

Enter the WAN IP address of the gateway to the remote

Configuring the Barricade

RIP

| File Edit View Fav | I / Index.stm • Microsoft Internet Explorer | 8 |
|--------------------|--|---|
| SMC® | Advanced State | 1 |
| SETUP WIZARD | DID Deservation | |
| YSTEM | KIP Parallicter | |
| VAN | Please Enter the following Configuration Parameters: | |
| AN | General RIP parameter: | |
| VIRELESS | RIP mode: IP Disable IP Enable | |
| IAT | Auto summary IP Disable C Enable | |
| OUTING | Table of current interface RIP parameter: | |
| Static Rosse | Poison Authentication | |
| FIF | unternace Mode Version Reverse Required Code | |
| Environ Tabin | LAN Disable 1 Disable None | |
| IREWALL | WILAN Disable 1 Disable None | |
| NMP | ATM1 Disable 1 M Disable A Mone | |
| PnP | ATM2 Disable 1 Disable None | |
| OSL | ATM3 Disable 1 Disable None | |
| DNS | ATM4 Disable 1 Disable None | |
| OOLS | ATMS Disable 1 Disable None | |
| TATUS | ATMD Disable 1 + Disable + None + | |
| | ATM7 Disable 1 T Disable None | |
| | ATME Disable 1 Disable None | |
| | PPPuEl Disable 1 Disable None | |
| | PPDoE2 Disable 1 Disable None | |
| | And a second sec | |

| Parameter | Description |
|--------------------------------|---|
| General RIP Parameters | |
| RIP mode | Globally enables or disables RIP. |
| Auto summary | If Auto summary is disabled, then RIP packets will include sub-network information from all sub-networks connected to the router. If enabled, this sub-network information will be summarized to one piece of information covering all sub-networks. |
| Table of current Interface RIP | parameter |
| Interface | The WAN interface to be configured. |
| Operation Mode | Disable: RIP disabled on this interface. |
| | Enable: RIP enabled on this interface. |
| | Silent: Listens for route broadcasts and updates its route table. It does not participate in sending route broadcasts. |

Version Sets the RIP (Routing Information Protocol) version to use on this interface.

| Parameter | Description |
|-------------------------|---|
| Poison Reverse | A method for preventing loops that would cause endless retransmission of data traffic. |
| Authentication Required | • None: No authentication. |
| | • Password: A password authentication key is included in the packet. If this does not match what is expected, the packet will be discarded. This method provides very little security as it is possible to learn the authentication key by watching RIP packets. |
| | • MD5: An algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to a specific individual. |
| Authentication Code | Password or MD5 Authentication key. |

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. RIP routers maintain only the best route to a destination. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change.

Configuring the Barricade

Routing Table

| File Edit View Favor | Indexustm - Microsoft Internet Explorer es Tools Heb Address http://192.168.2.1/mdexustm |
|---|---|
| SMC | Advanceds about |
| N SETUP WIZARD SYSTEM WAN LAN MOUTING ROUTING NAT FORMER FIREWALL STAMP UPAP ADEL DDNS TOOLS STATUS | Routing Table List Routing Table Papel Freework Address National Sateway Interface (Matrix C 197:00.1 255:255:85:0 denotity LAN **** C 197:00.1 255:255:55:00 forectly upphate **** Flags : C - desctly connected, S - static, R = RIP, 1 - ICMP Radrect |
| Parameter | Description |
| Flags | Indicates the route status: |
| | C = Direct connection on the same subnet. |
| | S = Static route. |
| | R = RIP (Routing Information Protocol) assigned route. |
| | I = ICMP (Internet Control Message Protocol) Redirect route. |
| Network Address | Destination IP address. |
| Netmask | The subnetwork associated with the destination. |
| | This is a template that identifies the address bits in the destination address used for routing to specific subnets. Each bit that corresponds to a "1" is part of the subnet mask number; each bit that corresponds to "0" is part of the host number. |
| Gateway | The IP address of the router at the next hop to which frames are forwarded. |
| Interface | The local interface through which the next hop of this route is reached. |
| Metric | When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metri value indicated in the update and enters the network in the routin table. |

Firewall

The Barricade Router's firewall inspects packets at the application layer, maintains TCP and UDP session information including time-outs and the number of active sessions, and provides the ability to detect and prevent certain types of network attacks.

Network attacks that deny access to a network device are called Denial-of-Service (DoS) attacks. DoS attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources.

The Barricade protects against the following DoS attacks: IP Spoofing, Land Attack, Ping of Death, IP with zero length, Smurf Attack, UDP port loopback, Snork Attack, TCP null scan, and TCP SYN flooding. (For details see page 4-60.)



The firewall does not significantly affect system performance, so we advise enabling the function to protect your network.

Select **Enable** and click the **SAVE SETTINGS** button.

Access Control

Access Control allows users to define the outgoing traffic permitted or not-permitted through the WAN interface. The default is to permit all outgoing traffic.



| Parameter | Description |
|------------------------------|---|
| Enable Filtering Function | Enable or Disable Access control function. |
| Normal Filtering Table | Displays descriptive list of filtering rules defined. |

To create a new access control rule:

- 1. Click **Add PC** on the Access Control screen. The Access Control Add PC screen will appear.
- 2. Define the appropriate rule settings for client PC services.
- 3. Click **OK** and then click **SAVE SETTINGS** to save your settings.

| http://192.168.2. File Edit View Fav | 1/index.stm - Microsoft Internet Ex ontes Tools Help Address Ch | plorer ttp://192.168.2.1/index.stm | |
|---|--|--|-------------------------|
| SMC [®] | | Advance | THoma IB Logout |
| SETUP WIZARD | Access Control Add PC | | |
| YSTEM | | | |
| VAN | criteria. For the URL blocking functi | rvice imitations of client PCs, including IP address, service typ on, you need to configure the URL address first on the "URL 8 | locking Site* page. For |
| AN | the scheduling function, you also n | eed to configure the schedule rule first on the "Schedule Rule" | , bode- |
| VIRELESS | Pule Description: | | |
| IAT | - mile besteription. (| | |
| ROUTING | Client PC IP Address: 192.1 | 68.2. | |
| IREWALL | | | |
| Accuse Control | Client PC Service: Secure Name | Detail Description | Blockupd |
| MACTINE | CONTRACT CONTRACT | HTTP TCP Port 80 3128 8000 8001 8080 | E . |
| UNL Mocking | WWW with UPI Blacking | HTTP (Per UP) Biorking Site Page) | E |
| Ellindors Rols | Funail Section | CMTD T/D Bowt 2E | - |
| Influence Detailing | Alows Conims | NNTR TCP Port 110 | - |
| DMAZ | Femal Paraisian | 0003 TC0 Port 119 | - |
| NMP | Converting | UTTOR TOP Best 442 | |
| PnP | Section Hill | 575 705 Bed 51 | - |
| DSL | Talaat Camina | TCD Devit 02 | F |
| DNS | Tenlec Service | 100 Port 25 | - |
| 00L5 | AIM | AOL Instant Messenger, TCP Port 5190 | |
| TATUS | Netweeting | H.323, TCP Port 1/20, 1503 | |
| | UNS | OUP PORT 53 | |
| | SNMP | UDP Port 161, 162 | - |
| | VPN-PP1P | 1CP P0rt 1723 | |

MAC Filter

The MAC Filter allows you to define what client PC's can access the Internet. When filtering function is enabled only the MAC addresses defined in the MAC Filtering table will have access to the Internet. All other client devices will be denied access.

You can enter up to 32 MAC addresses in this table.

| http://192.168.2. | 1/index.stm - Mi | crosoft Inter | et Explo | /192 168 2 | Lönder stm | | _ | | X |
|-------------------------|------------------|------------------|-------------|-------------|-------------|--------------|-----------------------------|-----------------------------------|---|
| SMC° | | p provide | a let under | ATTE MAR | A PRESIDENT | A | dva | nced | |
| » SETUP WIZARD | MAC Filter | ring Table | | | | ~ | | | 4 |
| SYSTEM | - | | | | | | | | and the second se |
| WAN | network. All of | ther client devi | cer contig | et denied a | coess. This | security fea | addresses c iture can su | ipport up to 32 c | levices and applies |
| LAN | to clients. | | | | | | | | |
| WIRELESS | • MAG Ad | Idress Control | i cu | ns e No | | | | | |
| NAT | | | | | | | | | |
| ROUTING | MAGEN | taslas Table f | | | | | | | |
| FIREWALL | · MAC PA | tering rabie (i | in to az | computers | 0 | | | | |
| o Aprilia Control | | 1D- | 1000 | - | - | MAC Addres | \$ | | |
| o MACINIER | | 1 | | : | + | | : | | |
| w UHL Macking | | 2 | | : [| : [| | ; [| | - |
| a Sthedaw Role | | -3 | | | . [| | . [| 1 | |
| a Internation Detection | | 4 | 1 | | | | | | |
| o DMZ | | 6 | | | | | | | |
| SNMP | | | 1 | _ | | | | | |
| UPnP | | 8 | - | | | | _ :_ | | |
| ADSL | | 1 | | | - | : | | | |
| DDNS | | 0 | | : 1 | | + | + 1 | | |
| TOOLS | | 9 | | 1: | 4 | : | + | + | |
| STATUS | | 10 | | : [| : [| : | : | : | |
| | | 11 | | : [| | 1: | : [| 1 | |
| | | 12 | | | : [| - : E | | : | |
| | | | _ | | | _ | _ | and the owner of the owner, where | |

- MAC Address Control: select enable or disable.
- MAC Filtering Table: enter the MAC address in the space provided.

URL Blocking

The Barricade allows the user to block access to web sites by entering either a full URL address or just a keyword. This feature can be used to protect children from accessing violent or pornographic web sites. You can define up to 30 sites here.

| http://192.168.2. | 1/index.stm - Microsoft Internet | Explorer | | | _ (7) X |
|----------------------------|----------------------------------|-----------------------------|--------------------------------|-----------------------------------|----------------|
| File Edit View Fav | vontes Tools Help Address | http://192.168.2.1/index.st | m | | |
| SMC° | | | Ad | Vanceds | B Logout |
| » SETUP WIZARD | UDI Plesking | | - | | <u>*</u> |
| SYSTEM | ORE BIOCKING | | | | |
| WAN | Disallowed Web Sites and Keywo | ords. | | | |
| LAN | You can block access to certain | Web sites from a particu | lar PC by entering | either a full URL address or just | t a keyword of |
| WIRELESS | the Web site. | | | | |
| NAT | To specify the particular PC, go | back to the "Access Con | trol ^e page and che | ck the box for "Http with URL B | locking*in the |
| ROUTING | "Normal Filtering Table", | | | | |
| FIREWALL | Rule Number | URL / Keyword | Rule Number | URL / Keyword | |
| a Aprese Control | Site 1 | | Site 16 | | |
| O MACTERIE | Site 2 | | Site 17 | | |
| w UML Macking | Site 3 | | Site 18 | | |
| a Silvedane Rate | Site 4 | | Site 19 | | |
| in Information Detailthing | Site 5 | | Site 20 | | |
| o DMZ | site 6 | | Site 21 | | |
| SNMP | Site 7 | | Site 22 | | |
| UPnP | Site 8 | | Site 23 | | |
| ADSL | Site 9 | | Site 24 | | _ |
| DDNS | Site 10 | | Site 25 | | |
| TOOLS | 514 11 | | Site 26 | | |
| STATUS | Site 11 | | Eite 27 | | |
| | Site 12 | | | | |
| | Site 13 | | 5/10/28 | | - |
| 13 | Site 14 | | and the | | |

Schedule Rule

You may filter Internet access for local clients based on rules. Each access control rule may be activated at a scheduled time. Define the schedule on the Schedule Rule screen, and apply the rule on the Access Control screen.



Follow these steps to add a schedule rule:

- 1. Click **Add Schedule Rule** on the Schedule Rule screen. The Edit Schedule Rule screen will appear.
- 2. Define the appropriate settings for a schedule rule.
- 3. Click **OK** and then click **SAVE SETTINGS** to save your settings.

| http://192.168.2. File Edit View Faw | 1/index.stm - Microsoft In ontes Tools Help Ad | ternet Explorer dress (2) http://192.166 | 8.2.1/index.str | | | | | - 8 |
|---|---|---|-----------------|-------------|------------|--------------|------------|-----|
| SMC® | | | | A | lVé | ance | Home Blogo | en) |
| » SETUP WIZARD | Edit Schedule Rul | e | - | | | | | |
| WAN | Name: | _ | | | | | | |
| LAN WIRELESS | Comment : | - | | | | | | |
| NAT | Activate Time Penod: | | | | | | | |
| ROUTING | | | | | | _ | | |
| FIREWALL | | Week Day | Start T | ime (nh:mm) | Eng | Time (nh:mm) | | |
| Accuse Control | | Every Day | | | | | | |
| MACTINE. | | Sunday | | | | | | |
| w Unit, Muching | | Monday | | : | | | | |
| a Sthedaw Rate | | Tuesday | | | T | | | |
| Information Detailth in a | | Wednesday | | | F | -1- | | |
| o DMZ | | Thursday | | | The second | | | |
| SNMP | | Friday | | | | | | |
| UPnP | | Filoay | | - | | | | |
| ADSL | | Saturday | | 3 | 14 | | | |
| DONS | | | OK | Cancel | | | | |
| TOOLS | | | | | | | | |
| STATUS | | | | | | | | |
| | | | | | | | | |

Intrusion Detection

• Intrusion Detection Feature

Stateful Packet Inspection (SPI) and Anti-DoS firewall protection (Default: Enabled) — The Intrusion Detection Feature of the Barricade Router limits access for incoming traffic at the WAN port. When the SPI feature is turned on, all incoming packets will be blocked except for those types marked in the Stateful Packet Inspection section.

RIP Defect (Default: Enabled) — If an RIP request packet is not acknowledged to by the router, it will stay in the input queue and not be released. Accumulated packets could cause the input queue to fill, causing severe problems for all protocols. Enabling this feature prevents the packets from accumulating.

Discard Ping to WAN (Default: Disabled) — Prevent a ping on the Barricade's WAN port from being routed to the network.



Scroll down to view more information.

| http://192.168.2.1/index.stm - Microsoft Internet Explorer | _ 8 × |
|--|-------|
| File Edit View Favorites Tools Help Address Thttp://192.168.2.1/index.stm | - eff |
| SMC° Adva | |
| • SETUP WIZARD • When hackers attempt to enter your network, we can alert you by e | -mail |
| SYSTEM | |
| WAN Your E-mail Address :) | |
| LAN SMTP Server Address : | |
| NAT POP3 Server Address : | |
| ROUTING | |
| FIREWALL User name : | |
| n Access Control Password : | |
| • UNL Macking • Connection Policy | |
| * 2014-dow Rote Unturnen Deutzhav Fragmentation half-open wait: 10 secs | |
| TCP SYN wat: 30 sec. | |
| SNMP | |
| ADDEL | |
| DDNS TCP connection idle timeout: 3600 sec. | |
| TOOLS IDD session intermenut: 30 sec. | |
| STATUS | |
| H.323 data channel idle timeout: 180 sec. | |
| + DoS Detect Criteria: | |

| File Edit View Favor | Index.stm - Microsoft Internet Explorer |
|------------------------|--|
| SMC® | Advanced Store |
| » SETUP WIZARD | |
| SYSTEM | UDP session idle timeout: PU sec. |
| WAN | H.322 data channel idle timeput: 100 sec. |
| LAN | |
| WIRELESS | DoS Detect Criteria: |
| NAT | Total incomplete TCBAIDD sessions HIGH- 300 session |
| ROUTING | Communities and an analysis and a second |
| FIREWALL | Total incomplete TCP/UDP sessions LOW: 250 session |
| n Accuse Control | and the second |
| o MACTHER | Incomplete TCP/UDP sessions (per min) HIGH: (20 session |
| e URL Macking | Incomplete TCP/UDP sessions (per min) LOW: 200 session |
| a Sthedaw Rate | |
| in Inthinian Delithian | Maximum incomplete TCP/UDP sessions number from same host: 10 |
| o DMZ | |
| SNMP | Incomplete TCP/UCP sessions detect sensitive time period: 1900 msec. |
| UPnP | Maximum half-open fragmentation packet number from same host: 30 |
| ADSL | |
| DDNS | Half-open fragmentation detect sensitive time period: 10000 msec. |
| TOOLS | 204 (204 (204 (204 (204 (204 (204 (204 (|
| STATUS | Flooding cracker block time: Isw sec. |
| | HELP SAVE SETTINGS CANCEL |
| Done | 📩 Internet |

• Stateful Packet Inspection

This is called a "stateful" packet inspection because it examines the contents of the packet to determine the state of the communications; i.e., it ensures that the stated destination computer has previously requested the current communication. This is a way of ensuring that all communications are initiated by the recipient computer and are taking place only with sources that are known and trusted from previous interactions. In addition to being more rigorous in their inspection of packets, stateful inspection firewalls also close off ports until connection to the specific port is requested.

When particular types of traffic are checked, only the particular type of traffic initiated from the internal LAN will be allowed. For example, if the user only checks "FTP Service" in the Stateful Packet Inspection section, all incoming traffic will be blocked except for FTP connections initiated from the local LAN.

Stateful Packet Inspection allows you to select different application types that are using dynamic port numbers. If you wish to use the Stateful Packet Inspection (SPI) to block packets, click on the Yes radio button in the "Enable SPI and Anti-DoS firewall protection" field and then check the inspection type that you need, such as Packet Fragmentation, TCP Connection, UDP Session, FTP Service, H.323 Service, or TFTP Service.

• When hackers attempt to enter your network, we can alert you by e-mail

Enter your email address. Specify your SMTP and POP3 servers, user name, and password.

Connection Policy

Enter the appropriate values for TCP/UDP sessions as described in the following table.

| Parameter | Defaults | Description |
|---------------------------------------|-----------------------------|---|
| Fragmentation half-open wait | 10 sec | Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. |
| TCP SYN wait | 30 sec | Defines how long the software will wait for a TCP session to synchronize before dropping the session. |
| TCP FIN wait | 5 sec | Specifies how long a TCP session will be maintained after the firewall detects a FIN packet. |
| TCP connection idle timeout | 3600 seconds (1 hour) | The length of time for which a TCP session will be managed if there is no activity. |
| UDP session idle timeout | 30 sec | The length of time for which a UDP session will be managed if there is no activity. |
| H.323 data channel idle timeout | 180 sec | The length of time for which an H.323 session will be managed if there is no activity. |

• DoS Criteria and Port Scan Criteria

Set up DoS and port scan criteria in the spaces provided (as shown below).

| Parameter | Defaults | Description |
|---|-----------------|--|
| Total incomplete TCP/UDP sessions HIGH | 300 sessions | Defines the rate of new unestablished sessions that will cause the software to <i>start</i> deleting half-open sessions. |
| Total incomplete TCP/UDP sessions LOW | 250 sessions | Defines the rate of new unestablished sessions that will cause the software to <i>stop</i> deleting half-open sessions. |
| Incomplete TCP/UDP sessions (per min) HIGH | 250 sessions | Maximum number of allowed incomplete TCP/UDP sessions per minute. |
| Incomplete TCP/UDP sessions (per min) LOW | 200 sessions | Minimum number of allowed incomplete TCP/UDP sessions per minute. |
| Maximum incomplete TCP/UDP sessions number from same host | 10 | Maximum number of incomplete TCP/UDP sessions from the same host. |
| Incomplete TCP/UDP sessions detect sensitive time period | 300 msec | Length of time before an incomplete TCP/UDP session is detected as incomplete. |
| Maximum half-open fragmentation packet number from same host | 30 | Maximum number of half-open fragmentation packets from the same host. |
| Half-open fragmentation detect sensitive time period | 10000 msec | Length of time before a half-open fragmentation session is detected as half-open. |
| Flooding cracker block time | 300 second | Length of time from detecting a flood attack to blocking the attack. |

Note: The firewall does not significantly affect system performance, so we advise enabling the prevention features to protect your network.

DMZ

If you have a client PC that cannot run an Internet application properly from behind the firewall, you can open the client up to unrestricted two-way Internet access. Enter the IP address of a DMZ (Demilitarized Zone) host on this screen. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

| http://192.168.2.1 | /index | .stm - | Microsof | it Interne | et Explorer | | R × |
|--|--|----------|--|--|--|--|--|
| File Edit View Favo | intes T | Tools I | telp | Address | http://192.168.2.; | 1/index.stm | |
| SMC° | | | | | | Advanc | |
| » SETUP WIZARD SYSTEM WAN LAN WIRELESS NAT ROUTING | DM If y can Ena Mul VPN | tiple PC | e a local o he client Z: C V Is can be otions. T | rized Z client PC t up to unn (es ©) exposed t o use the | one) that cannot run an estincted two-way Vo to the Internet for DM2, you must se | Internet application properly from behind Internet access by defining a Virtual DM2 two-way communications e.g. Internet g t a static IP address for that PC. | the NAT firewall, then you Host. aming, wideo conferencing, pr |
| FIREWALL | | | | | | | - |
| n Accuse Control n MAC Litter | 1. | 0.0.0 | .0 | PUBI | C IP Address | 192.168.2.0 | |
| w UML Mocking | 2. | þ | . 0 | , D | , o | 192.168.2.0 | |
| a Sthedaw Role | 2. | 0 | 0 | . 10 | , lo | 192.168.2.0 | |
| in Intrumin Delution | -4, | p | 0 | . p | , p | 192.168.2.0 | |
| 01000 | 5. | p | Ø | . 0 | . 0 | 192.168.2.0 | |
| UPnP | 6. | p | . 0 | . 0 | , 0 | 192.168.2.0 | |
| ADSL | 7. | p | . 0 | . 0 | . 0 | 192.168.2.0 | |
| DDNS | 8. | þ | . 0 | . 0 | . 0 | 192.168.2.0 | |
| TOOLS | | | | | | | |
| STATUS | | | | | | HEID G | |
| | | | | | | neur ja | WE SETTINGS CHILLE |
| | | | | | | | |
| Done | | | | | | | internet |

Configuring the Barricade

SNMP

Use the SNMP configuration screen to display and modify parameters for the Simple Network Management Protocol (SNMP).



• Select the SNMP Operation mode from the drop down menu.

Community

A computer attached to the network, called a Network Management Station (NMS), can be used to access this information. Access rights to the agent are controlled by community strings. To communicate with the Barricade, the NMS must first submit a valid community string for authentication.

| 2 http://192.168.2.1/ | ndex.stm - Microsoft Internet Explorer | _[7] x | | | |
|---|---|---|--|--|--|
| File Edit View Favorit | es Tools Help Address [4] http://192168.2.1/index.str | Advanced | | | |
| SETUP WIZARD VYSTEM VAN AN KAN KOUTING SIREWALL | SHEP Community Image: State Community | t and a set of State munager defined security blow at the agent, the agent establishes one comunity organized status within that community are provided within rise. The agent muy establish a number of communities, with Access Vale Read P Read P | | | |
| Parameter | Description | A hereite | | | |
| Community | A community name authorized for management access. | | | | |
| Access | Management access is | s restricted to Read Only (Read) or | | | |

| Valid | Enables/disables the entry. | | | |
|-------|-----------------------------|--|--|--|
| | | | | |

Read/Write (Write).

Note: Up to five community names may be entered.

Trap

Specify the IP address of the NMS to notify when a significant event is detected by the agent. When a trap condition occurs, the SNMP agent sends an SNMP trap message to any NMS specified as a trap receiver.



| Parameter | Description | |
|------------|---|--|
| IP Address | Traps are sent to this address when errors or specific events occur on the network. | |
| Community | A community string (password) specified for trap management. Enter a word, something other than public or private, to prevent unauthorized individuals from accessing information on your system. | |
| Version | Sets the trap status to disabled, or enabled with V1 or V2c. | |
| | The v2c protocol was proposed in late 1995 and includes enhancements to v1 that are universally accepted. These include a get-bulk command to reduce network management traffic when retrieving a sequence of MIB variables, and a more elaborate set of error codes for improved reporting to a Network Management Station. | |

UPnP

The Universal Plug and Play architecture offers pervasive peer-to-peer network connectivity of PCs of all form factors, intelligent appliances, and wireless devices.

UPnP enables seamless proximity network in addition to control and data transfer among networked devices in the office, home and everywhere within your network.



UPnP allows the device to automatically:

- join a network
- obtain an IP address
- convey its capabilities and learn about the presence and capabilities of other devices.

Check **Enable** to activate this function.

ADSL

ADSL (Asymmetric Digital Subscriber Line) is designed to deliver more bandwidth downstream (from the central office to the customer site) than upstream. This section is used to configure the ADSL operation type and shows the ADSL status.

ADSL Parameters

This screen is designed for the engineer to test the ADSL loop condition. Therefore, it is advised that users should not change the settings here at all.



G.992.5 ADSL2+

ADSL Status

The Status screen displays information on connection line status, data rate, operation data and defect indication, and statistics.

| File Edit View Faw | ontes Tools Help Address Chittp: | orer ://192.168.2.1/index. | stm | 1012 |
|--------------------|--|-------------------------------|-------------------|----------------|
| SMC® | | | Advan | THome B Logout |
| SETUP WIZARD | Monitoring Index: | | | |
| AN | ADSL Status Information: | | | |
| AN | <u>Status</u> | | | |
| IRELESS | Data Rate Information | | | |
| AT. | Defect/Failure Indication Statistics | | | |
| | - soundlike | | | |
| OUTING | Status: | | | |
| REWALL | | Configured | Current | |
| IMP | Line Status | | READY | |
| PnP | Link Type | | 111 | |
| DSL | - [GO TOD] | | | |
| Samelers | Data Rate: | | | |
| table | Stream Type | Actua | Data Rate | |
| a second a | Up Stream | 0. | (Kbps.) | |
| INS | Down Stream | D | (Kbps.) | |
| OLS | [Go Top] | | | |
| ATUS | Operation Data / Defect Indicat | ion: | | |
| | operation Data | Upstream | Downstream | |
| | Noise Margin | 0 dB | D dis | |
| | Attenuation | 0 dB | 0 de | |
| | Indicator Name Near E | ind Indicator | Far End Indicator | |
| | HEC Error | 0 | 0 | |
| | CRC Error | a | 0 | |
| | IGn Trip1 | | 1 | |

Parameter

Description

| Status | |
|-----------------------|--|
| Line Status | Shows the current status of the ADSL line connection. |
| Data Rate | |
| Upstream | Maximum upstream data rate. |
| Downstream | Maximum downstream data rate. |
| Operation Data/Defect | Indication |
| Noise Margin | Maximum upstream and downstream noise margin. |
| Output Power | Maximum fluctuation in the output power. |
| Attenuation | Maximum reduction in the strength of the upstream and downstream signal. |

| Parameter | Description |
|------------------------------------|--|
| Fast Path FEC Correction | There are two latency paths that may be used: fast and interleaved. For either path, a forward error correction (FEC) scheme is employed to ensure higher data integrity. For maximum noise immunity, an interleaver may be used to supplement FEC. |
| Interleaved Path FEC Correction | An interleaver is basically a buffer used to introduce a delay, allowing for additional error correction techniques to handle noise. Interleaving slows the data flow and may not be optimal for real-time signals such as video transmission. |
| Fast Path CRC Error | The number of Fast Path Cyclic Redundancy Check errors. |
| Interleaved Path CRC Error | The number of Interleaved Path Cyclic Redundancy Check errors. |
| Loss of Signal Defect | Momentary signal discontinuities. |
| Loss of Frame Defect | Failures due to loss of frames. |
| Loss of Power Defect | Failures due to loss of power. |
| Fast Path HEC Error | Fast Path Header Error Concealment errors. |
| Interleaved Path HEC Error | Interleaved Path Header Error Concealment errors. |
| Statistics | |
| Received Cells | Number of cells received. |
| Transmitted Cells | Number of cells transmitted. |

DDNS

Dynamic Domain Name Service (DDNS) provides users on the Internet with a method to tie their domain name to a computer or server. DDNS allows your domain name to follow your IP address automatically by having your DNS records changed when your IP address changes. This DNS feature is powered by DynDNS.org or NO-IP.com or TZO.com. With a DDNS connection you can host your own web site, email server, FTP site, and more at your own location even if you have a dynamic IP address.

| http://192.168.2. File Edit View Faw | 1/Index.stm - Microsoft Internet Explo ontes Tools Help Address (2) http: | //192.168.2.1/index.stm | X |
|---|--|---|-------------------------|
| SMC® | | Advanc | THOME B Logout |
| » SETUP WIZARD | DDNS (Dynamic DNS) Set | tions | |
| SYSTEM | bond (bynamic bird) see | unga | |
| WAN | Dynamic DNS provides users on the I | internet a method to tie their domain name(s) to comp | uters or servers. DONS |
| LAN | address changes. | on the address adroniatically by naving your onits record | to changes when your in |
| WIRELESS | | | |
| NAT | Dynamic DNS | C Enable @ Disable | |
| ROUTING | Provider | DynDNS era * | |
| FIREWALL | - | | |
| SNMP | Domain Name | | |
| OPHP | Account / E-mail | [| |
| AUSL | Pussword / Key | - | |
| 70018 | | | |
| | | | |
| STATUS | | | |
| | | HEID COM | CETTINGS CANCEL |
| | | HELP SAVE | SETTINOS CANCEL |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Tools

Use the Tools menu to ping, trace route, backup the current configuration, restore a previously saved configuration, update firmware, and reset the Barricade.

Ping Utility

This tool allows you to test your network connection. You can specify a domain name or a valid IP address of the remote host for ping test.



• Enter the address in the Destination address field, then click **Execute**. The result will show in the Test Result area.

Trace Route Utility

Traceroute is a TCP/IP utility which allows the user to determine the route packets take to reach a particular host.

| http://192.168.2.1 | /index.stm - Microsoft Internet Explorer | _l∂l x |
|-----------------------|---|-----------------|
| File Edit View Favor | ites Tools Help Address (2) http://192.168.2.1/index.stm | 1 E |
| SMC° | | Advanced Salet |
| . SETUP WIZARD | and the second se | |
| SYSTEM | TraceRoute Utility | |
| WAN | IP Address or Domain Name: | Traceroute |
| LAN | | |
| WIRELESS | | |
| NAT | | |
| ROUTING | | |
| FIREWALL | | |
| SNMP | | |
| UPnP | | |
| ADSL | | |
| DDNS | | |
| TOOLS | | |
| n Ping Otim | | |
| w TraceRoute Uskry | | |
| w Configuration Tools | | CIEADIOG HEID |
| e Eliminare Upgrade | | |
| « Resel | | |
| STATUS | | |
| | | |
| | | |
| - | | |
| (e) | | 📦 Internet |

• Enter the information in the IP Address or Domain Name field, and click the **Traceroute** button.

Configuration Tools

Choose a function and click Next.

| http://192.168.2.3 | /index.stm - Microsoft Internet Explorer | _ (7) X |
|---|--|--|
| File Edit View Favo | ntes Tools Heb Address Anttp://192.168.2.1/index.stm | · · |
| SMC® | Advanced. | |
| IN SETUP WIZARD SYSTEM WAN LAN WIRELESS NAT ROUTING FIREWALL SNMP UPAP ADSL DDNS TOOLS I TOOLS I TOOLS | Configuration Tools The the Stackup to lot save the router's current configuration to a fiel named backup bin' on your for the stackup tool to force the router to perform a power riset and restore the original factors. A charge Bouter Configuration Castore router to Factory Defaults Text >> | C. You can use the Restore settings. |
| 1910me | | Internet |

- Backup Router Configuration: this allows you to save the Barricade's configuration to a file.
- Restore from saved Configuration file: this function is used to restore the previously saved backup configuration file.
- Restore router to Factory Defaults: this resets the Barricade back to the original default settings.

Firmware Upgrade

Use this screen to update the firmware or user interface to the latest versions.

- 1. Download the upgrade file from the SMC web site first, and save it to your hard drive.
- 2. Then click **Browse...** to look for the downloaded file. Click **BEGIN UPGRADE**.



Check the Status screen Information section to confirm that the upgrade process was successful.

Configuring the Barricade

Reset

Click **REBOOT ROUTER** to reset the Barricade. The reset will be complete when the power LED stops blinking.



If you perform a reset from this screen, the configurations will not be changed back to the factory default settings.

Note: If you use the Reset button on the back panel, the Barricade performs a power reset. If the button is pressed for over 10 seconds, all the LEDs will illuminate and the factory default settings will be restored.

Status

The Status screen displays WAN/LAN connection status, firmware, and hardware version numbers, illegal attempts to access your network, as well as information on DHCP clients connected to your network. The security log may be saved to a file by clicking **Save** and choosing a location.



Scroll down to view more information on the Status screen.

| SMC [®] | ontes toois hep jao | cress (@_http://192_168.2_1/index.st | Advanced | |
|--------------------------|---------------------|--------------------------------------|-----------|--|
| » SETUP WIZARD SYSTEM | ATM PVC | | | |
| WAN | | | 1 | |
| LAN | VC. | | VG2 | |
| WIRELESS | VPL/VCI | 1/32 | | |
| NAT | Encapsulation | LLC | | |
| ROUTING | ID Address | Down | | |
| FIREWALL | Subnet Mask | and and a | Piculated | |
| SNMP | Gateway | at all as | Disabled | |
| LIPOP | Primary DNS | | | |
| ADRI | Secondary DNS | | | |
| DONE | Disconnect Conne | ict | | |
| 70010 | | | 1 | |
| 10060 | NO: | 1 | Ver | |
| STATUS | | | | |
| | Disab | led I | Disabled | |
| | | | | |



| Parameter | Description |
|-----------------|---|
| INTERNET | Displays WAN connection type and status. |
| Release | Click on this button to disconnect from the WAN. |
| Renew | Click on this button to establish a connection to the WAN. |
| GATEWAY | Displays system IP settings, as well as DHCP Server and Firewall status. |
| INFORMATION | Displays the number of attached clients, the firmware versions, the physical MAC address for each media interface and for the Barricade, as well as the hardware version and serial number. |
| ATM PVC | Displays ATM connection type and status. |
| Disabled | The ATM connection is disabled. |
| Connect | Click on this button to establish a connection to the ATM connection. |
| Security Log | Displays attempts to access your network. |
| Save | Click on this button to save the security log file. |
| Clear | Click on this button to delete the access log. |
| Refresh | Click on this button to refresh the screen. |
| DHCP Client Log | Displays information on DHCP clients on your network. |

The following items are included on the Status screen:

Finding the MAC address of a Network Card

Windows 2000/XP

Click Start/Programs/Command Prompt. Type "ipconfig /all" and press "ENTER".

The MAC address is listed as the "Physical Address."

Macintosh

Click System Preferences/Network.

The MAC address is listed as the "Ethernet Address" on the TCP/IP tab.

Linux

Run the command "/sbin/ifconfig."

The MAC address is the value after the word "HWaddr."

Appendix A Troubleshooting

This section describes common problems you may encounter and possible solutions to them. The Barricade can be easily monitored through panel indicators to identify problems.

| Troubleshooting Chart | | |
|-----------------------|---|--|
| Symptom | Action | |
| LED Indicators | | |
| Power LED is Off | Check connections between the Barricade, the external power supply, and the wall outlet. | |
| | • If the power indicator does not turn on when the power cord is plugged in, you may have a problem with the power outlet, power cord, or external power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses, or surges at the power outlet. If you still cannot isolate the problem, then the external power supply may be defective. In this case, contact Technical Support for assistance. | |

TROUBLESHOOTING

| Troubleshooting Chart | | | |
|--|--|--|--|
| Symptom | Action | | |
| LED Indicators | | | |
| Link LED is Off | Verify that the Barricade and attached device are powered on. | | |
| | • Be sure the cable is plugged into both the Barricade and the corresponding device. | | |
| | • Verify that the proper cable type is used and that its length does not exceed the specified limits. | | |
| | • Be sure that the network interface on the attached device is configured for the proper communication speed and duplex mode. | | |
| | • Check the adapter on the attached device and cable connections for possible defects. Replace any defective adapter or cable if necessary. | | |
| Network Connecti | ion Problems | | |
| Cannot ping the Barricade from the attached LAN | • Verify that the IP addresses are properly configured. For most applications, you should use the Barricade's DHCP function to dynamically assign IP addresses to hosts on the attached LAN. However, if you manually configure IP addresses on the LAN, verify that the same network address (network component of the IP address) and subnet mask are used for both the Barricade and any attached LAN devices. | | |
| | • Be sure the device you want to ping (or from which you are pinging) has been configured for TCP/IP. | | |

| Troubleshooting Chart | | |
|--|--|--|
| Symptom | Action | |
| Management Problems | | |
| Cannot connect using the web browser | • Be sure to have configured the Barricade with a valid IP address, subnet mask, and default gateway. | |
| | Check that you have a valid network connection to the Barricade and that the port you are using has not been disabled. | |
| | • Check the network cabling between the management station and the Barricade. | |
| Forgot or lost the password | • Press the Reset button on the rear panel (holding it down for at least 10 seconds) to restore the factory defaults. | |

Appendix B Cables

Ethernet Cable

Caution: DO NOT plug a phone jack connector into any RJ-45 port. Use only twisted-pair cables with RJ-45 connectors that conform with FCC standards.

Specifications

| Cable Types and Specifications | | | |
|--------------------------------|--------------------------|----------------|-----------|
| Cable | Туре | Max. Length | Connector |
| 10BASE-T | Cat. 3, 4, 5 100-ohm UTP | 100 m (328 ft) | RJ-45 |
| 100BASE-TX | Cat. 5 100-ohm UTP | 100 m (328 ft) | RJ-45 |

Wiring Conventions

For Ethernet connections, a twisted-pair cable must have two pairs of wires. Each wire pair is identified by two different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-45 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-45 connectors in a specific orientation. The following figure illustrates how the pins on an Ethernet RJ-45 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



Figure B-1. RJ-45 Ethernet Connector Pin Numbers

RJ-45 Port Connection

Use the straight-through CAT-5 Ethernet cable provided in the package to connect the Barricade to your PC. When connecting to other network devices such as an Ethernet switch, use the cable type shown in the following table.

| AttachedDevicePortType | Connecting Cable Type |
|------------------------|-----------------------|
| MDI-X | Straight-through |
| MDI | Crossover |

Pin Assignments

With 100BASE-TX/10BASE-T cable, pins 1 and 2 are used for transmitting data, and pins 3 and 6 for receiving data.

| RJ-45 Pin Assignments | | |
|-----------------------|-------------------------|--|
| Pin Number | Assignment ¹ | |
| 1 | Tx+ | |
| 2 | Tx- | |
| 3 | Rx+ | |
| 6 | Rx- | |

1: The "+" and "-" signs represent the polarity of the wires that make up each wire pair.

Straight-Through Wiring

If the port on the attached device has internal crossover wiring (MDI-X), then use straight-through cable.

| Straight-Through Cable Pin Assignments | | |
|--|---------|--|
| End 1 | End 2 | |
| 1 (Tx+) | 1 (Tx+) | |
| 2 (Tx-) | 2 (Tx-) | |
| 3 (Rx+) | 3 (Rx+) | |
| 6 (Rx-) | 6 (Rx-) | |

CABLES

Crossover Wiring

If the port on the attached device has straight-through wiring (MDI), use crossover cable.

| Crossover Cable Pin Assignments | |
|---------------------------------|---------|
| End 1 | End 2 |
| 1 (Tx+) | 3 (Rx+) |
| 2 (Tx-) | 6 (Rx-) |
| 3 (Rx+) | 1 (Tx+) |
| 6 (Rx-) | 2 (Tx-) |

ADSL Cable

Use standard telephone cable to connect the RJ-11 telephone wall outlet to the RJ-11 ADSL port on the ADSL Router.

Caution: Do not plug a phone jack connector into an RJ-45 port.

Specifications

| Cable Types and Specifications | | |
|--------------------------------|--------------------------|-----------|
| Cable Type Connected | | Connector |
| ADSL Line | Standard Telephone Cable | RJ-11 |

Wiring Conventions

For ADSL connections, a cable requires one pair of wires. Each wire is identified by different colors. For example, one wire might be red and the other, red with white stripes. Also, an RJ-11 connector must be attached to both ends of the cable.

Each wire pair must be attached to the RJ-11 connectors in a specific orientation. The following figure illustrates how the pins on the RJ-11 connector are numbered. Be sure to hold the connectors in the same orientation when attaching the wires to the pins.



Figure B-2. RJ-11 Connector Pin Numbers



| Pin | Signal Name | Wire Color |
|-----|-------------|------------------------|
| 1 | Not used | |
| 2 | Line 2 Tip | Black or White/Orange |
| 3 | Line 1 Ring | Red or Blue/White |
| 4 | Line 1 Tip | Green or White/Blue |
| 5 | Line 2 Ring | Yellow or Orange/White |
| 6 | Not used | |

Figure B-3. RJ-11 Pinouts

Appendix C Specifications

Physical Characteristics

Ports

Four 10/100Mbps RJ-45 ports One ADSL port (RJ-11)

ADSL Features

Supports DMT line modulation

Supports Annex A Full-Rate ADSL: up to 8 Mbps downstream, up to 1 Mbps upstream (G.992.1 &T1.413, Issue 2) and ADSL2 (G.992.3) and ADSl2+ (G.992.5) Supports G.Lite ADSL: up to 1.5 Mbps downstream, up to 512 Kbps

upstream Dying GASP support

ATM Features

RFC1483 Encapsulation (IP, Bridging and encapsulated routing) PPP over ATM (LLC &VC multiplexing) (RFC2364) Classical IP (RFC1577) Traffic shaping (UBR, CBR) OAM F4/F5 support PPP over Ethernet Client

Management Features

Firmware upgrade via web based management web based management (configuration) Power Indicators Event and History logging Network Ping Traceroute

SPECIFICATIONS

Security Features

Password protected configuration access User authentication (PAP/CHAP) with PPP Firewall NAT NAPT VPN pass through (IPSec-ESP Tunnel mode,L2TP, PPTP)

LAN Features

IEEE 802.1D (self-learning transparent Bridging) DHCP Server DNS Proxy Static Routing, RIPv1 and RIP

Temperature: IEC 68-2-14

0 to 40 degrees C (Standard Operating) -40 to 70 degree C (Non-operation)

Humidity

10% to 90% (Non-condensing)

Vibration: IEC 68-2-36, IEC 68-2-6

Shock: IEC 68-2-29

Drop: IEC 68-2-32

Dimensions: 143mm(L) x 94mm(D) x 32mm(H)

Weight: 500 g

Input Power: 15 V 0.8A

IEEE Standards

IEEE 802.3, 802.3u, 802.11g, 802.1D , 802.11 n draft ITU G.dmt, ITU G.Handshake, ITU T.413 issue 2 - ADSL full rate

Standards Conformance Electromagnetic Compatibility CE, ETSI, R&TTE, FCC part 15 class B & FCC part 68

Safety EN 60950-1

Wireless Frequency Band

802.11b/g/n Radio: 2.4 GHz USA - FCC 2412~2462 MHz (Ch1~Ch11) Europe - ETSI 2412~2472 MHz (Ch1~Ch13) France 2457~2472 MHz (Ch10~Ch13)

Modulation Technology: DSSS, OFDM

Operating Channels:

IEEE 802.11b compliant: 11 channels (US, Canada) 13 channels (ETSI) 4 channels (France)

IEEE 802.11g compliant: 11 channels (US, Canada) 13 channels (Europe)

IEEE draft 802.11n 20MHz compliant: 11 channels (US, Canada) 13 channels (Europe)

IEEE draft 802.11n 40MHz compliant: 7 channels (US, Canada) 9 channels (Europe)

Signal Type: DSSS/OFDM Operating Frequency: 2.412 - 2.462GHz



TECHNICAL SUPPORT From U.S.A. and Canada (24 hours a day, 7 days a week) Phn: (800) SMC-4-YOU / (949) 679-8000 Fax: (949) 679-1481

ENGLISH Technical Support information available at www.smc.com

FRENCH Informations Support Technique sur www.smc.com

DEUTSCH Technischer Support und weitere Information unter www.smc.com

SPANISH En www.smc.com Ud. podrá encontrar la información relativa a servicios de soporte técnico

DUTCH Technische ondersteuningsinformatie beschikbaar op www.smc.com

PORTUGUES Informações sobre Suporte Técnico em www.smc.com

SWEDISH Information om Teknisk Support finns tillgängligt på www.smc.com

INTERNET E-mail address: techsupport@smc.com

Driver updates http://www.smc.com/index.cfm?action=tech_support_drivers_downloads

World Wide Web http://www.smc.com/

SMC7904WBRA-N