

# Network Settings

This section will allow you to change the local network settings of the router and to configure the DHCP settings.

**IP Address:** Enter the IP address of the router. The default IP address is 192.168.0.1.

If you change the IP address, once you click **Apply**, you will need to enter the new IP address in your browser to get back into the configuration utility.

**Subnet Mask:** Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

**Device Name:** Enter a name for the router.

**Local Domain:** Enter the Domain name (Optional).

**Enable DNS Relay:** Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.

**D-Link**

DIR-628 // SETUP ADVANCED TOOLS STATUS SUPPORT

**NETWORK SETTINGS**

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP Server to assign IP addresses to the computers on your network. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Save Settings Don't Save Settings

**ROUTER SETTINGS**

Use this section to configure the internal network settings of your router. The IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Device Name: dlinkrouter

Local Domain Name: (optional)

Enable DNS Relay:

**Helpful Hints...**

If you already have a DHCP server on your network or are using static IP addresses on all the devices on your network, uncheck **Enable DHCP Server** to disable this feature.

If you have devices on your network that should always have fixed IP addresses, add a **DHCP Reservation** for each such device.

[More...](#)

## DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-628 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to “Obtain an IP Address Automatically.” When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-628. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

**Enable DHCP Server:** Check this box to enable the DHCP server on your router. Uncheck to disable this function.

**DHCP IP Address Range:** Enter the starting and ending IP addresses for the DHCP server’s IP assignment.

**Note:** If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.

**DHCP Lease Time:** The length of time for the IP address lease. Enter the Lease time in minutes.

**Always Broadcast:** Enable this feature to broadcast your networks DHCP server to LAN/WLAN clients.

**NetBIOS Announcement:** NetBIOS allows LAN hosts to discover all other computers within the network, enable this feature to allow the DHCP Server to offer NetBIOS configuration settings.

**Learn NetBIOS from WAN:** Enable this feature to allow WINS information to be learned from the WAN side, disable to allow manual configuration.

### DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

**Enable DHCP Server:**

**DHCP IP Address Range:**  to

**DHCP Lease Time:**  (minutes)

**Always broadcast:**  (compatibility for some DHCP Clients)

**NetBIOS announcement:**

**Learn NetBIOS from WAN:**

**NetBIOS Scope:**  (optional)

**NetBIOS node type :**

- Broadcast only (use when no WINS servers configured)
- Point-to-Point (no broadcast)
- Mixed-mode (Broadcast then Point-to-Point)
- Hybrid (Point-to-Point then Broadcast)

**Primary WINS IP Address:**

**Secondary WINS IP Address:**

**NetBIOS Scope:** This feature allows the configuration of a NetBIOS 'domain' name under which network hosts operates. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated."

**NetBIOS Mode Type:** Select the different type of NetBIOS node: **Broadcast only**, **Point-to-Point**, **Mixed-mode**, and **Hybrid**.

**Primary/Secondary WINS IP Address:** Enter your Primary (and Secondary) WINS IP address(es).

## DHCP Reservation

If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

**Note:** This IP address must be within the DHCP IP Address Range.

**Enable:** Check this box to enable the reservation.

**Computer Name:** Enter the computer name or select from the drop-down menu and click <<.

**IP Address:** Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.

**MAC Address:** Enter the MAC address of the computer or device.

**Copy Your PC's MAC Address:** If you want to assign an IP address to the computer you are currently on, click this button to populate the fields.

**Save:** Click **Save** to save your entry. You must click **Save Settings** at the top to activate your reservations.

**Number of Dynamic DHCP Clients:** In this section you can see what LAN devices are currently leasing IP addresses.

**Revoke:** Click **Revoke** to cancel the lease for a specific LAN device and free an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

**ADD DHCP RESERVATION**

**Enable:**

**Computer Name:**  << Computer Name ▼

**IP Address:**

**MAC Address:**

**DHCP RESERVATIONS LIST**

Enable	Computer Name	MAC Address	IP Address
<input type="checkbox"/>			

**NUMBER OF DYNAMIC DHCP CLIENTS: 2**

Hardware Address	Assigned IP	Hostname	Expires	
00:0c:f1:fe:ee:cd	192.168.0.197	PMLab16	22 Hours 48 Minutes	<a href="#">Revoke</a> <a href="#">Reserve</a>
00:16:17:44:4a:d9	192.168.0.199	PMLab15	14 Hours 54 Minutes	<a href="#">Revoke</a> <a href="#">Reserve</a>

**Note:** The Revoke option will not disconnect a PC with a current network session from the network; you would need to use MAC Address Filter to do that. Revoke will only free up a DHCP Address for the very next requester. If the previous owner is still available, those two devices may both receive an IP Address Conflict error, or the second device may still not receive an IP Address; in that case, you may still need to extend the “DHCP IP Address Range” to address the issue, it is located in the DHCP Server section.

**Reserve:** The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.

## Virtual Server

The DIR-628 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DIR-628 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-628 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DIR-628 redirects the external service request to the appropriate server within the LAN network.

The DIR-628 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. There are pre-defined virtual services already in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

For a list of ports for common applications, please visit [http://support.dlink.com/faq/view.asp?prod\\_id=1191](http://support.dlink.com/faq/view.asp?prod_id=1191).

This will allow you to open a single port. If you would like to open a range of ports, refer to page 35.

**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the “Computer Name” drop-down menu. Select your computer and click <<.

**Private Port/ Public Port:** Enter the port that you want to open next to Private Port and Public Port. The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.

**Protocol Type:** Select **TCP**, **UDP**, or **Both** from the drop-down menu.

**Inbound Filter:** Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

**Schedule:** The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**D-Link**

DIR-628

SETUP ADVANCED TOOLS STATUS SUPPORT

**VIRTUAL SERVER**

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

**24--VIRTUAL SERVERS LIST**

	Name	IP Address	Port	Traffic Type	Schedule
<input type="checkbox"/>	<< Application Name	<< Computer Name	Public 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0		Private 0	6	Inbound Filter Allow All
<input type="checkbox"/>	<< Application Name	<< Computer Name	Public 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0		Private 0	6	Inbound Filter Allow All
<input type="checkbox"/>	<< Application Name	<< Computer Name	Public 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0		Private 0	6	Inbound Filter Allow All
<input type="checkbox"/>	<< Application Name	<< Computer Name	Public 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0		Private 0	6	Inbound Filter Allow All

**Helpful Hints...**

Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.

Select a schedule for when the virtual server will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** screen and create a new schedule.

# Port Forwarding

This will allow you to open a single port or a range of ports.

**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the “Computer Name” drop-down menu. Select your computer and click <<.

**TCP/UDP:** Enter the TCP and/or UDP port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common.

Example: 24,1009,3000-4000

**Inbound Filter:** Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

**Schedule:** The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**D-Link**

DIR-628 // SETUP ADVANCED TOOLS STATUS SUPPORT

**PORT FORWARDING**

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

Save Settings Don't Save Settings

**24 -- PORT FORWARDING RULES**

		Ports to Open		
<input type="checkbox"/>	Name	<< Application Name	TCP	Schedule Always
	IP Address	<< Computer Name	UDP	Inbound Filter Allow All
	0.0.0.0			
<input type="checkbox"/>	Name	<< Application Name	TCP	Schedule Always
	IP Address	<< Computer Name	UDP	Inbound Filter Allow All
	0.0.0.0			
<input type="checkbox"/>	Name	<< Application Name	TCP	Schedule Always
	IP Address	<< Computer Name	UDP	Inbound Filter Allow All
	0.0.0.0			

**Helpful Hints...**

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the LAN computer to which you would like to open the specified port.

Select a schedule for when the rule will be enabled. If you do not see the schedule you need in the list of schedules, go to the



# Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DIR-628. If you need to run applications that require multiple connections, specify the port normally associated with an application in the “Trigger Port” field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DIR-628 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

**Name:** Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click <<.

**Trigger:** This is the port used to trigger the application. It can be either a single port or a range of ports.

**Traffic Type:** Select the protocol of the trigger port (TCP, UDP, or Both).

**Firewall:** This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

**Traffic Type:** Select the protocol of the firewall port (TCP, UDP, or Both).

**Schedule:** The schedule of time when the Application Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

The screenshot shows the D-Link DIR-628 web interface. The top navigation bar includes 'DIR-628', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'ADVANCED' tab is selected, and the 'APPLICATION RULES' sub-tab is active. The main content area displays a table of predefined application rules. The table has columns for 'Name', 'Application', 'Port', 'Traffic Type', and 'Schedule'. The 'Application' column contains a dropdown menu with '<<' and 'Application Name' options. The 'Port' column has a 'Trigger' field and a 'Firewall' field. The 'Traffic Type' column has a dropdown menu with 'TCP' selected. The 'Schedule' column has a dropdown menu with 'Always' selected. The table contains three rows of predefined rules. To the right of the table is a 'Helpful Hints...' sidebar with text explaining the feature and providing instructions on how to use the predefined applications.

Name	Application	Port	Traffic Type	Schedule
<input type="checkbox"/>	<< Application Name	Trigger Firewall	TCP TCP	Always
<input type="checkbox"/>	<< Application Name	Trigger Firewall	TCP TCP	Always
<input type="checkbox"/>	<< Application Name	Trigger Firewall	TCP TCP	Always

**Helpful Hints...**  
Use this feature if you are trying to execute one of the listed network applications and it is not communicating as expected.  
Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.  
Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools -> Schedules** screen and create a

# QoS Engine

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.

**Enable Traffic Shaping:** Traffic Shaping

**Automatic Uplink Speed:** This option is enabled by default when the Traffic Shaping option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

**Measured Uplink:** This displays the detected uplink speed.

**Manual Uplink Speed:** The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as [www.dslreports.com](http://www.dslreports.com).

**Connection Type:** By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either "Static" or "DHCP" in the Internet settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

**QoS Engine**

Use this section to configure D-Link's QoS Engine. The QoS Engine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web. For best performance, use the Automatic Classification option to automatically set the priority for your applications.

Save Settings Don't Save Settings

**WAN TRAFFIC SHAPING**

Enable Traffic Shaping:

Automatic Uplink Speed:

Measured Uplink Speed: 1682 kbps

Manual Uplink Speed: 128 kbps << Select Transmission Rate

Connection Type: Auto-detect

Detected xDSL or Other Frame Relay Network: No

**QoS ENGINE SETUP**

Enable QoS Engine:

Automatic Classification:

Dynamic Fragmentation:

**10 -- QoS ENGINE RULES**

Name	Priority	Protocol	Local IP Range	Local Port Range	Remote IP Range	Remote Port Range
	1 (1..255)	TCP	0.0.0.0 to 255.255.255.255	0 to 65535	0.0.0.0 to 255.255.255.255	0 to 65535

**Helpful Hints...**

If the **Measured Uplink Speed** is known to be incorrect (that is, it produces suboptimal performance), disable **Automatic Uplink Speed** and enter the **Manual Uplink Speed**. Some experimentation and performance measurement may be required to converge on the optimal value.

[More...](#)

**Detected xDSL:** When Connection Type is set to automatic, the automatically detected connection type is displayed here.

**Enable QoS Engine:** This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

**Automatic Classification:** This option is enabled by default. This will allow your router to automatically determine the network priority of running programs.

**Dynamic Fragmentation:** This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones.

## Network Filters

Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

**Configure MAC Filtering:** Select **Turn MAC Filtering Off, allow MAC addresses listed below**, or **deny MAC addresses listed below** from the drop-down menu.

**MAC Address:** Enter the MAC address you would like to filter.

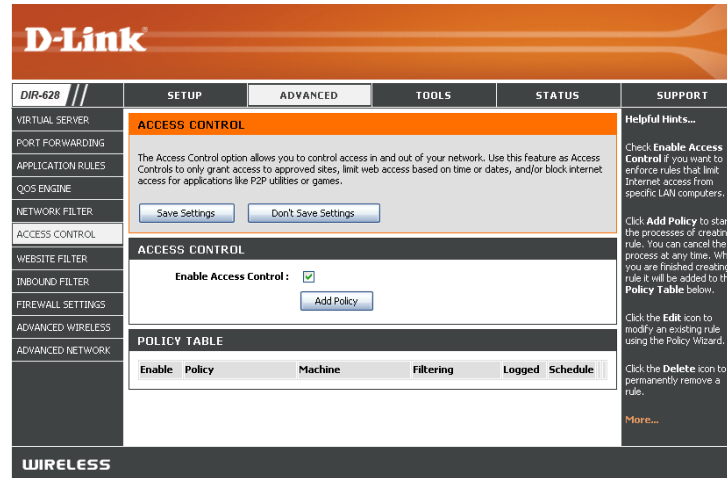
To find the MAC address on a computer, please refer to the **Networking Basics** section in this manual.

**DHCP Client:** Select a DHCP client from the drop-down menu and click << to copy that MAC Address.

# Access Control

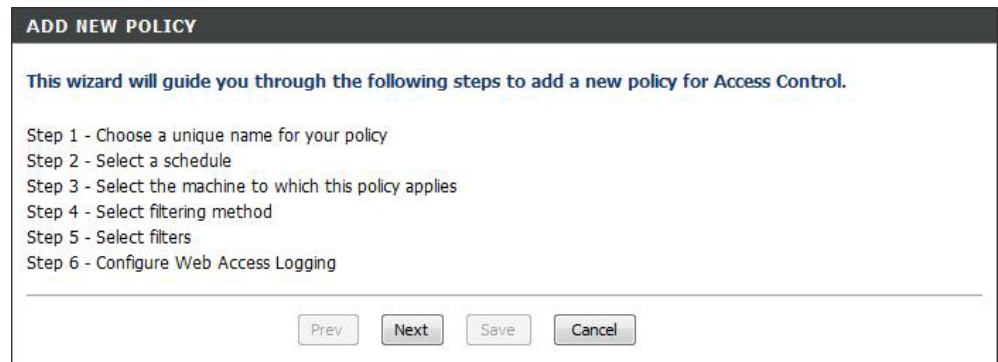
The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

**Add Policy:** Click the **Add Policy** button to start the Access Control Wizard.



## Access Control Wizard

Click **Next** to continue with the wizard.



## Access Control Wizard (continued)

Enter a name for the policy and then click **Next** to continue.

**STEP 1: CHOOSE POLICY NAME**

Choose a unique name for your policy.

Policy Name :

Select a schedule (I.E. Always) from the drop-down menu and then click **Next** to continue.

**STEP 2: SELECT SCHEDULE**

Choose a schedule to apply to this policy.

Always

Details : Always

Enter the following information and then click **Next** to continue.

- **Address Type** - Select IP address, MAC address, or Other Machines.
- **IP Address** - Enter the IP address of the computer you want to apply the rule to.

**STEP 3: SELECT MACHINE**

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

Address Type :  IP  MAC  Other Machines

IP Address :  <<  Computer Name

Machine Address :  <<  Computer Name

Machine

## Access Control Wizard (continued)

Select the filtering method and then click **Next** to continue.

**STEP 4: SELECT FILTERING METHOD**

Select the method for filtering.

**Method :**  Log Web Access Only  Block All Access  Block Some Access

**Apply Web Filter :**

**Apply Advanced Port Filters :**

Enter the rule:

**Enable** - Check to enable the rule.

**Name** - Enter a name for your rule.

**Dest IP Start** - Enter the starting IP address.

**Dest IP End** - Enter the ending IP address.

**Protocol** - Select the protocol.

**Dest Port Start** - Enter the starting port number.

**Dest Port End** - Enter the ending port number.

**STEP 5: PORT FILTER**

**Add Port Filters Rules.**

Specify rules to prohibit access to specific IP addresses and ports.

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535
<input type="checkbox"/>		0.0.0.0	255.255.255.255	Any	1	65535

To enable web logging, click **Enable**.

Click **Save** to save the access control rule.

**STEP 6: CONFIGURE WEB ACCESS LOGGING**

**Web Access Logging :**  Disabled  Enabled

## Website Filters

Website Filters are used to allow you to set up a list of allowed Web sites that can be used by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section (page 43).

**Add Website Filtering Rule:** Select **Allow** or **Deny**.

**Website URL/ Domain:** Enter the keywords or URLs that you want to allow or block. Click **Save Settings**.

The screenshot shows the D-Link DIR-628 web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options, with 'WEBSITE FILTER' selected. The main content area is titled 'WEBSITE FILTER' and contains the following text: 'The Website Filter option allows you to set up a list of Web sites you would like to allow or deny through your network. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. A section titled '40 -- WEBSITE FILTERING RULES' contains the text 'Configure Website Filter below:' followed by a dropdown menu set to 'DENY computers access to ONLY these sites'. Below the dropdown is a 'Clear the list below...' button. At the bottom, there is a table with the header 'Website URL/Domain' and three rows of input fields for entering website URLs or domains.