

MyOwn Telco: D-Link DIR-655 Router Configuration Guide

Here follows the configuration steps for the D-Link DIR-655 router for VoIP usage.

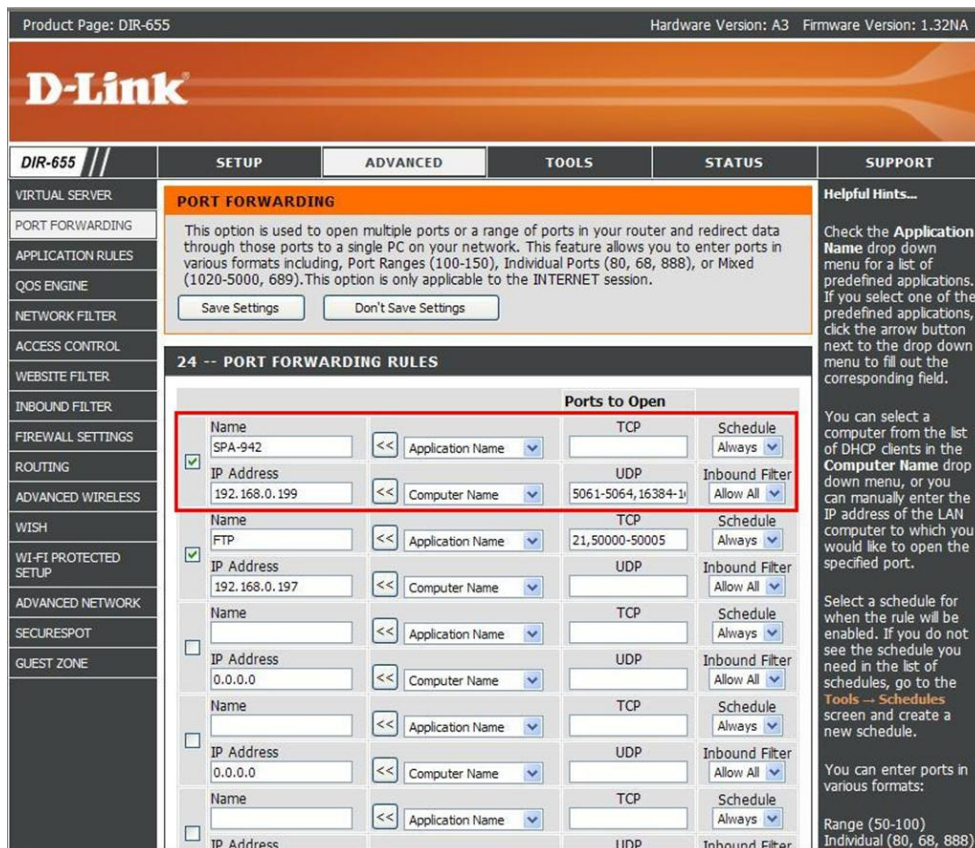
1) Open a web browser and navigate to you router IP address, which is usually something like <http://192.168.0.1>, and log in using the **Admin** username. If you don't know the IP address of your router, you may want to open a Windows DOS session using "**cmd**" and execute the "**ipconfig**" command; the IP address will then normally be identified with the **Default Gateway** field.

2) Once you are logged in, navigate to the **Advanced** tab and select the **Port Forwarding** menu item. Afterward, click on the check box of an empty section and secondly, fill in the following fields and when done, click on the **Save Settings** button.

Name: Put your VoIP device name (e.g. "IP Phone")

IP Address: Gather your device name's IP address and specify it here (e.g. "192.168.0.199")

UDP: Specify the SIP range of ports that will be used for communications. If you don't know which ports are being used, verify your VoIP device's configuration. Usually 5060 is used but you could also use a range of ports if you have several lines on your device. The same applies for the RTP ports. In this example, a Linksys SPA-942 that has 4 lines uses ports 5061 to 5064 for signalling and ports 16384 to 16482 for RTP. (e.g. "5061-5064,16384-16482"). For a single port IP phone, it could also be "5060,16384-16482", just make sure it reflects your phone configuration. If you are still unsure, use "5060,10000-20000".



Product Page: DIR-655 Hardware Version: A3 Firmware Version: 1.32NA

D-Link

DIR-655 // 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). This option is only applicable to the INTERNET session.

Save Settings Don't Save Settings

24 -- PORT FORWARDING RULES

	Name	IP Address	Application Name	Computer Name	Ports to Open	Schedule	Inbound Filter
<input checked="" type="checkbox"/>	SPA-942	192.168.0.199	Application Name	Computer Name	TCP 5061-5064, 16384-16482	TCP Always	Allow All
<input checked="" type="checkbox"/>	FTP	192.168.0.197	Application Name	Computer Name	TCP 21,50000-50005	TCP Always	Allow All
<input type="checkbox"/>		0.0.0.0	Application Name	Computer Name	TCP	Schedule Always	Allow All
<input type="checkbox"/>		0.0.0.0	Application Name	Computer Name	UDP	Schedule Always	Allow All
<input type="checkbox"/>		0.0.0.0	Application Name	Computer Name	TCP	Schedule Always	Allow All
<input type="checkbox"/>		0.0.0.0	Application Name	Computer Name	UDP	Schedule Always	Allow All

Helpful Hints...

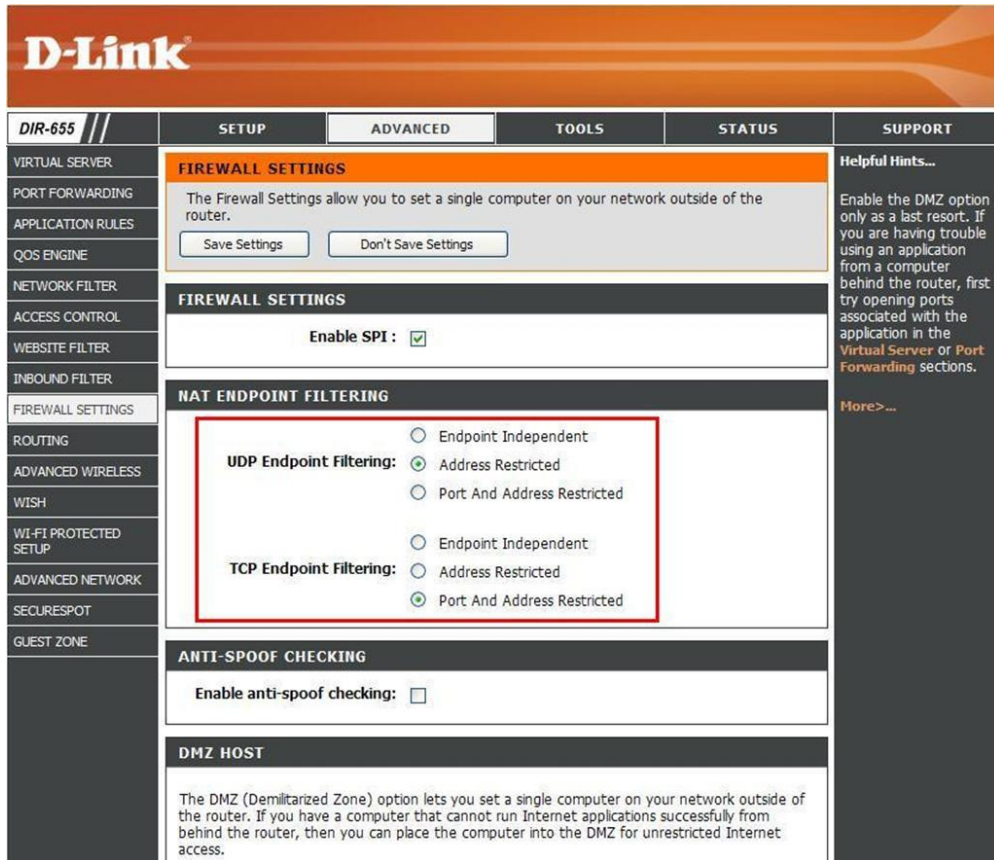
Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

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 **Tools -- Schedules** screen and create a new schedule.

You can enter ports in various formats:
Range (50-100)
Individual (80, 68, 888)

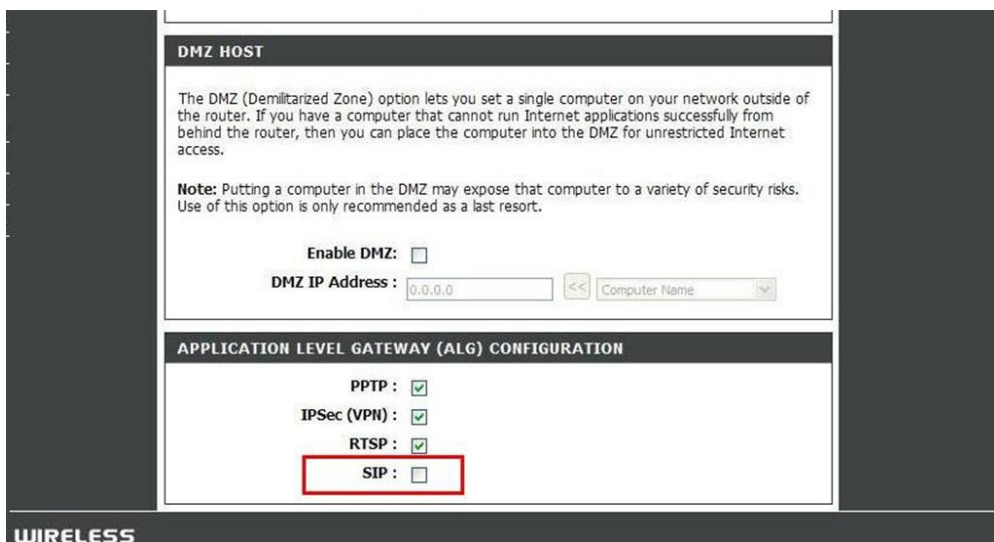
3) Using the same **Advanced** tab, select the **Firewall Settings** menu item. In the **NAT Endpoint Filtering** section, select **Address Restricted** for the **UDP Endpoint Filtering** setting and **Port And Address Restricted** for the **TCP End Point Filtering** settings.



The screenshot shows the D-Link DIR-655 Advanced Firewall Settings page. The 'NAT ENDPOINT FILTERING' section is highlighted with a red box. It contains the following settings:

- UDP Endpoint Filtering:**
 - Endpoint Independent
 - Address Restricted
 - Port And Address Restricted
- TCP Endpoint Filtering:**
 - Endpoint Independent
 - Address Restricted
 - Port And Address Restricted

Then scroll down the page and unselect the **SIP** check box within the **ALG Configuration** section and then click the **Save Settings** button at the top of the page.



The screenshot shows the DMZ Host and ALG Configuration sections. The 'SIP' checkbox in the 'APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION' section is highlighted with a red box.

DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Enable DMZ:

DMZ IP Address: << Computer Name:

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

- PPTP:
- IPSec (VPN):
- RTSP:
- SIP:**

4) Again, stay on the **Advanced** tab, and click on the **QoS Engine** menu item; in the **WAN Traffic Shaping** section, make sure that **Enable Traffic Shaping** is selected. Also make sure that both the **Enable QoS Engine** and the **Automatic Classification** check boxes are selected within the **QoS Engine Setup** section. Finally, select an empty item in the **QoS Engine Rules** section and configure the fields using this information:

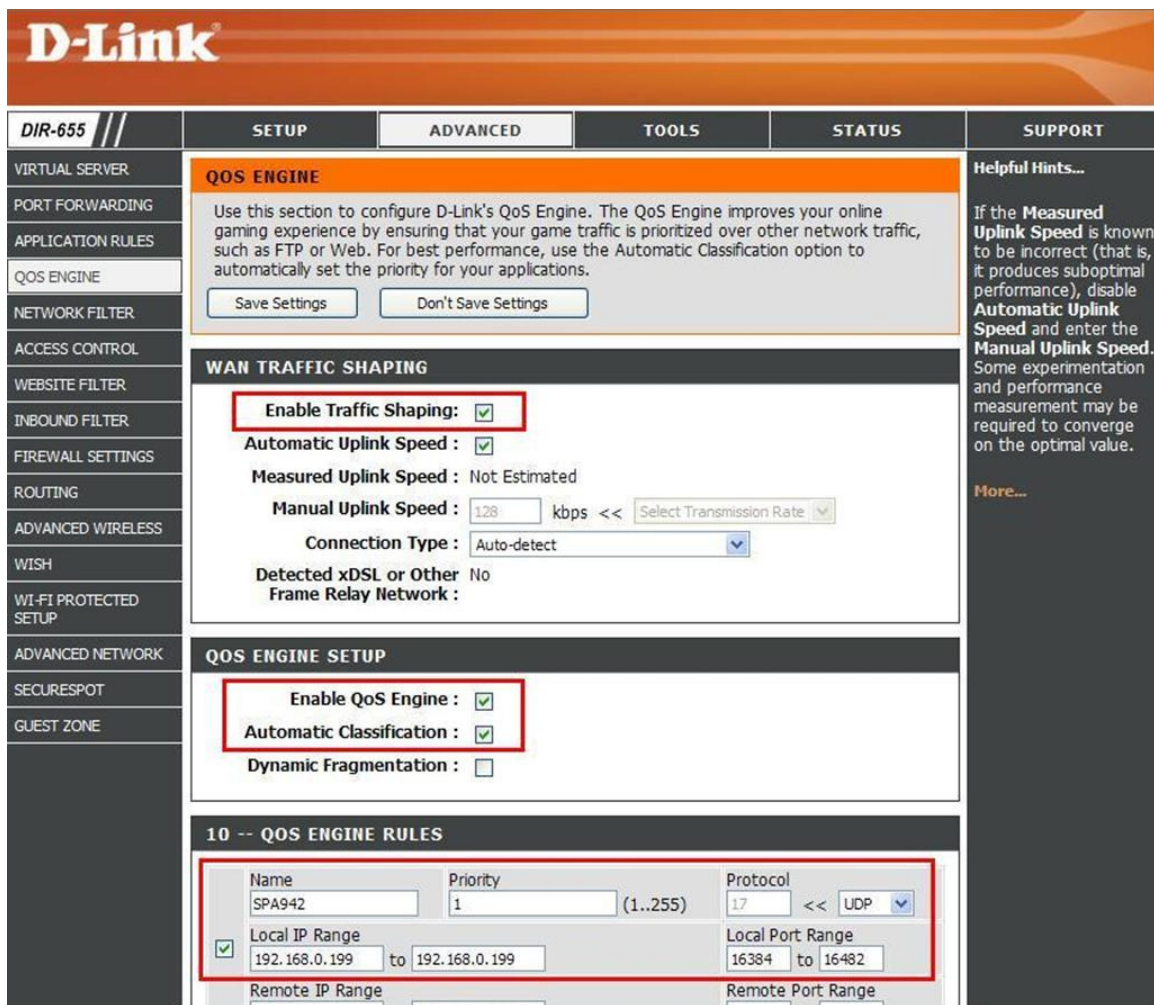
Name: Put your VoIP device name (e.g. "IP Phone")

Priority: "1" (Voice will have highest priority)

Local IP Range: This is the IP address for your VoIP device, which should be the same as the one you typed in at step 2)

Protocol: UDP ("17")

Local Port Range: These are also the same UDP RTP port that you typed in at step 2) (e.g. "16384-16482")



D-Link

DIR-655 // SETUP **ADVANCED** TOOLS STATUS SUPPORT

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: Not Estimated

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
SPA942	1 (1..255)	17 << UDP
Local IP Range	Local Port Range	
192.168.0.199 to 192.168.0.199	16384 to 16482	
Remote IP Range	Remote Port Range	

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...

When you are done, click on the **Save Settings** button and reboot your router.