

ZMD-DD-SBN4

Remote Network Setup

Once you have completed the [Local Network Setup](#), you should have an internal IP address for your DVR.

The next step in the process is to forward ports pertaining to the DVR, so that you can see your cameras remotely.

We recommend that you follow the steps in our network tutorial located at [www.zmodo.com/network](#). This video walks through using our network tutorial:

Forward DVR's Ports

- 1) Log in to your router by entering the gateway IP, such as 192.168.1.1, in to your browser window. Enter the login information for your router. If you cannot remember this, you can check the default username/password combinations for most routers at <http://www.pcwintech.com/default-router-modem-passwords>. If you are unable to locate this information, please contact your router manufacturer or Internet Service Provider.
- 2) Once you've logged in to your router, you will need to enter the Port Forwarding section of your router. There, you'll enter the IP address, protocols, and port numbers for your DVR.

IP Address = IP address in your DVR's Network Settings

Protocol = BOTH (TCP/UDP) OR TCP

Service or Application Name can be anything you wish, like DVR1 or DVR2

ZMD-DD-SBN4

Create 1 rule per port number; Start and End Ports will be the same number

Here are the default ports for Zmodo units (last port # is the mobile port):

H9104, H9108, H9106, H9116: 80, 9000, 18004

H9114, H9118: 80, 5050, 6050, 7050

H9124, H9128, DR-SFN6: 80, 9000, 15961

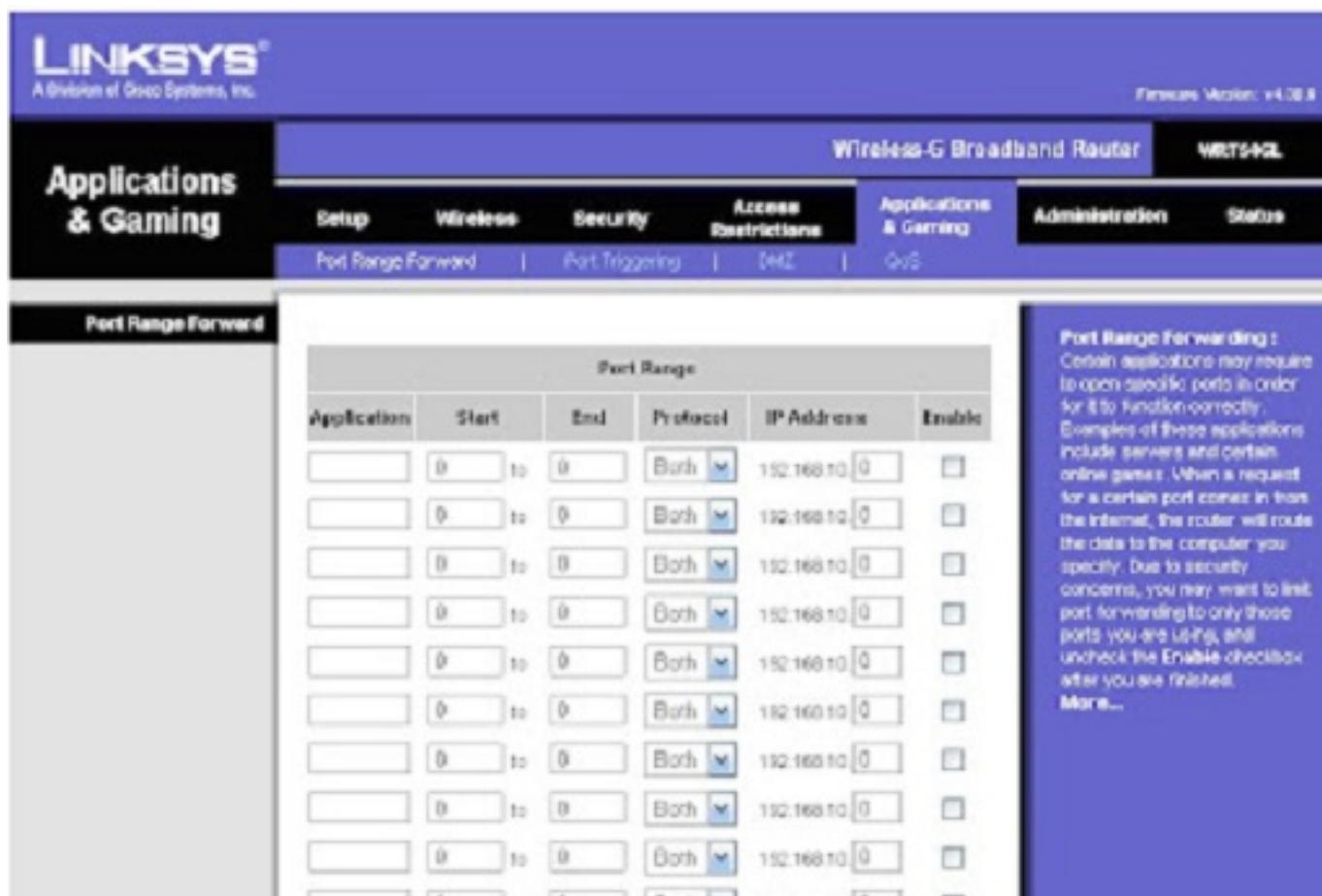
H8000/H8100 series: 80, 7777, 8888

Note: If you are using a DSL internet service, you may need to use port 81 (instead of 80) as your web port. If so, be sure to change this in your DVR's network settings, and restart the unit. Once the port number is changed, you will need to use it when connecting to the unit (ie. <http://192.168.1.1> becomes <http://192.168.1.140:81>)

3) Below are screenshot samples of common router's Port Forwarding sections. Please note that exact locations may differ depending on your router's model. If your model is not listed, try looking through Advanced, Firewall, or Forwarding sections in your router to find the exact location.

ZMD-DD-SBN4

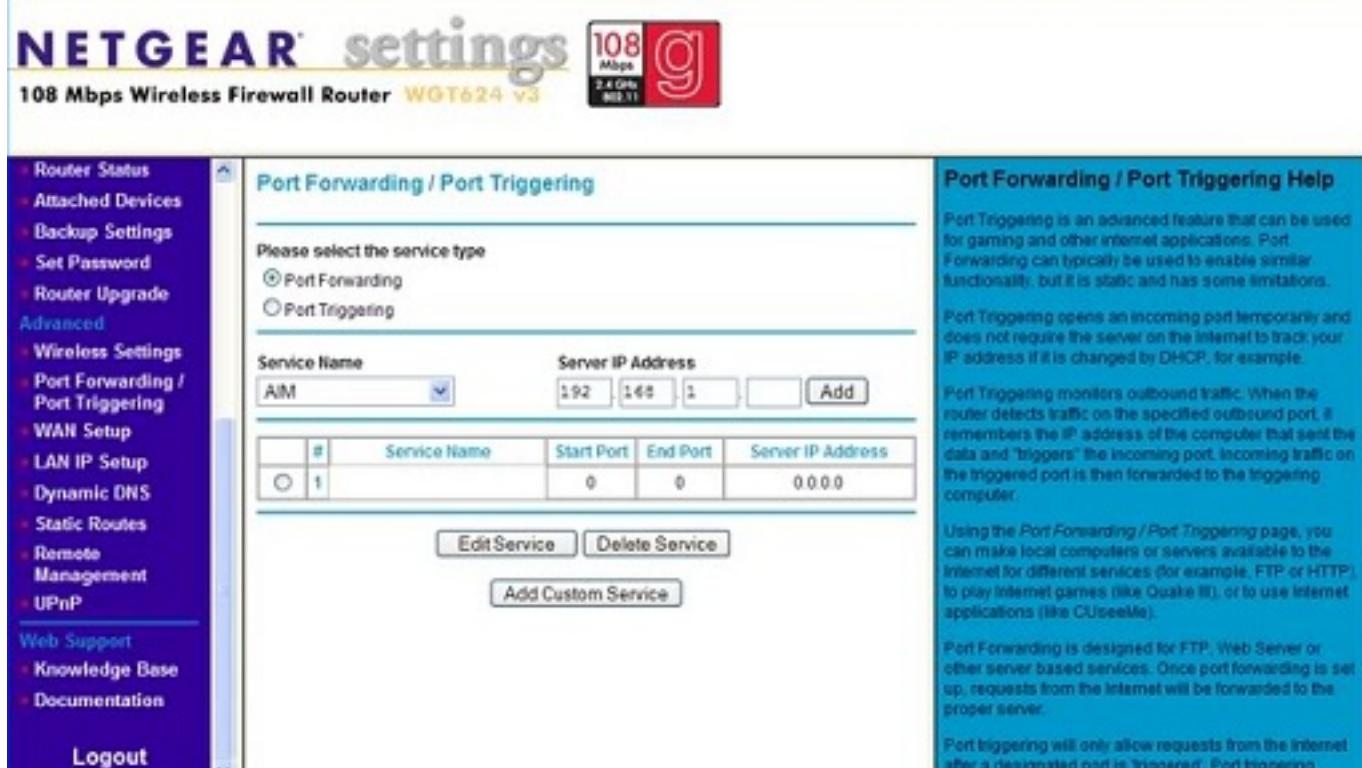
Linksys



The screenshot shows the Linksys Applications & Gaming interface. The top navigation bar includes tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming (which is selected), Administration, and Status. Below the navigation bar, there are sub-tabs: Port Range Forward, Port Triggering, DMZ, and QoS. The main content area is titled "Port Range Forward" and contains a table titled "Port Range". The table has columns for Application, Start, End, Protocol, IP Address, and Enable. There are 10 rows in the table, each with a checkbox in the "Enable" column. The IP address for all rows is 192.168.10.0. The "Protocol" dropdown is set to "Both" for all rows. The "Enable" checkboxes are all unchecked. A sidebar on the right provides a detailed explanation of Port Range Forwarding, stating that certain applications may require specific ports to function correctly, and that users can limit port forwarding to specific ports. It also mentions security concerns and the "Enable" checkbox.

In Linksys routers, you will typically enter Applications & Gaming, then Port Range Forward. Exact names/places will differ depending on model. Be sure to create forward 1 port range per line, and check the 'Enable' box at the end of the line, then save changes.

Netgear



The screenshot shows the Netgear WGT624 v3 settings interface. The left sidebar contains a navigation menu with the following items:

- Router Status
- Attached Devices
- Backup Settings
- Set Password
- Router Upgrade
- Advanced** (selected)
- Wireless Settings
- Port Forwarding / Port Triggering
- WAN Setup
- LAN IP Setup
- Dynamic DNS
- Static Routes
- Remote Management
- UPnP
- Web Support
- Knowledge Base
- Documentation
- Logout

The main content area is titled "Port Forwarding / Port Triggering". It includes a section for selecting the service type, with "Port Forwarding" selected. Below this is a table for defining services, with one entry for "AIM" (Service Name) and "0.0.0.0" (Server IP Address). The table has columns for #, Service Name, Start Port, End Port, and Server IP Address. Buttons for "Edit Service", "Delete Service", and "Add Custom Service" are also present.

The right sidebar contains a "Port Forwarding / Port Triggering Help" section with the following text:

Port Triggering is an advanced feature that can be used for gaming and other internet applications. Port Forwarding can typically be used to enable similar functionality, but it is static and has some limitations. Port Triggering opens an incoming port temporarily and does not require the server on the internet to track your IP address if it is changed by DHCP, for example. Port Triggering monitors outbound traffic. When the router detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data and "triggers" the incoming port. Incoming traffic on the triggered port is then forwarded to the triggering computer.

Using the Port Forwarding / Port Triggering page, you can make local computers or servers available to the internet for different services (for example, FTP or HTTP) to play internet games (like Quake III), or to use internet applications (like CUseeMe).

Port Forwarding is designed for FTP, Web Server or other server based services. Once port forwarding is set up, requests from the internet will be forwarded to the proper server.

Port Triggering will only allow requests from the internet after a designated port is "triggered". Port Triggering

In Netgear routers, you will typically look under Advanced for Port Forwarding/Triggering. Select Port Forwarding as your service type. Then, select 'Add Custom Service' for each port you forward.

D-Link



DSL-2740B //	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP																						
Port Forwarding	PORT FORWARDING This is the ability to open ports in your router and re-direct data through those ports to a single PC on your network.																										
Application Rules	PORT FORWARDING RULES CONFIGURATION Remaining number of rules that can be created: 48																										
QoS Setup	<table border="1"><tr><td>Name</td><td><input type="text"/> Application Name</td><td>External Port</td><td>Internal Port</td></tr><tr><td>IP Address</td><td><input type="text"/> Computer Name</td><td>TCP</td><td>TCP</td></tr><tr><td>Use Interface:</td><td><input type="text"/> pppoa_0/pppoa0</td><td>UDP</td><td>UDP</td></tr><tr><td colspan="4"><input type="button" value="Add/Apply"/></td></tr></table>	Name	<input type="text"/> Application Name	External Port	Internal Port	IP Address	<input type="text"/> Computer Name	TCP	TCP	Use Interface:	<input type="text"/> pppoa_0/pppoa0	UDP	UDP	<input type="button" value="Add/Apply"/>				ACTIVE PORT FORWARDING RULES <table border="1"><thead><tr><th>Name</th><th>Address</th><th>External Port</th><th>Internal Port</th><th>Protocol</th><th>WAN Interface</th><th>Edit</th><th>Remove</th></tr></thead></table>	Name	Address	External Port	Internal Port	Protocol	WAN Interface	Edit	Remove	Helpful Hints... Check the Application Name drop down menu for a list of predefined applications. If not you can still easily define a new rule. More...
Name	<input type="text"/> Application Name	External Port	Internal Port																								
IP Address	<input type="text"/> Computer Name	TCP	TCP																								
Use Interface:	<input type="text"/> pppoa_0/pppoa0	UDP	UDP																								
<input type="button" value="Add/Apply"/>																											
Name	Address	External Port	Internal Port	Protocol	WAN Interface	Edit	Remove																				
Outbound Filter																											
Inbound Filter																											
Wireless Filter																											
DNS Setup																											
Firewall & DMZ																											
Advanced Internet																											
Advanced Wireless																											
Advanced LAN																											
SNMP Setup																											
Remote Management																											
Routing Setup																											
Wi-Fi Protected Setup																											
Logout																											

For D-Link Routers, you will enter Advanced, then Port Forwarding. Click 'Add/Apply' when you have finished each rule.

Belkin

ZMD-DD-SBN4

BELKIN. Router Setup Utility Home | Help | Logout Internet Status: Connected

LAN Setup
LAN Settings
DHCP Client List
Internet WAN
Connection Type
DNS
MAC Address
Wireless
Channel and SSID
Security
Wi-Fi Protected Setup
Use as Access Point
MAC Address Control
Firewall
Virtual Servers
Client IP Filters
MAC Address Filtering
DMZ
DDNS
WAN Ping Blocking
Security Log
Utilities

Firewall > Virtual servers

This function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. [More Info](#)

Add

Clear entry

	Enable	Description	Inbound port	Type	Private IP address	Private port
1.	<input type="checkbox"/>		-	BOTH	192.168.2.	-
2.	<input type="checkbox"/>		-	BOTH	192.168.2.	-
3.	<input type="checkbox"/>		-	BOTH	192.168.2.	-
4.	<input type="checkbox"/>		-	BOTH	192.168.2.	-
5.	<input type="checkbox"/>		-	BOTH	192.168.2.	-
6.	<input type="checkbox"/>		-	BOTH	192.168.2.	-
7.	<input type="checkbox"/>		-	BOTH	192.168.2.	-
8.	<input type="checkbox"/>		-	BOTH	192.168.2.	-
9.	<input type="checkbox"/>		-	BOTH	192.168.2.	-

For Belkin routers, access port fowarding under Firewall, Virtual Servers. Be sure to check the 'Enable' box, then hit the 'Set' button, and save your changes.

2-Wire

For 2-Wire modems, enter Firewall, then Advanced Settings.

ZMD-DD-SBN4

To Allow Users Through the Firewall to Hosted Applications...

1 Select a computer

Choose the computer that will host applications through the firewall:

2 Edit firewall settings for this computer:

Maximum protection – Disallow unsolicited inbound traffic.

Allow individual application(s) – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.



Allow all applications (DMZplus mode) – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

First, look for the DVR's IP address under (1) Select a computer. If you do not see the DVR's IP address here, you may need to go in to the DVR's Network Settings, and set the DVR to DHCP (instead of Static), then reboot the DVR. Once the unit reboots, check it's IP address in the Network Settings, then go back to your router to select the DVR from the list.

Next, you will need to click on "Add a new user-defined application", to come to the this new screen:

ZMD-DD-SBN4

Settings

Profile Name:
Enter a name for the application profile that you are creating.

Application Name:

Definition

Choose a protocol and enter the port(s) for this application, then click ADD DEFINITION to add the definition to the Definition List. If the application requires multiple ports or both TCP and UDP ports, you will need to add multiple definitions.

Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu below, it is recommended that you select it.

Protocol: TCP UDP

Port (or Range): From: To:

Protocol Timeout (seconds): TCP default 86400
UDP default 600

Map to Host Port: Default = the same port as defined above.

Application Type:

ADD DEFINITION

BACK

Create your rule, and click 'Add Definition'. Create a rule for each port. Then, click Back.

ZMD-DD-SBN4

To Allow Users Through the Firewall to Hosted Applications...

1 Select a computer

Choose the computer that will host applications through the firewall:

2 Edit firewall settings for this computer:

Maximum protection – Disallow unsolicited inbound traffic.

Allow individual application(s) – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.



Allow all applications (DMZplus mode) – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.

When done, select each application you have created, and click 'Add', so that you see the desired applications in the Hosted Applications table. When finished, click 'Done' at the bottom of the screen.

Netopia

For Netopia routers, click on the Configure tab at the top of the page.

ZMD-DD-SBN4

To make configuration changes, follow these steps:

1. Make a change to a field or parameter.
2. Click Submit. This change isn't permanent; you'll save it later. The Alert button (top right corner) appears.
3. Make more changes, if desired.
4. Click the Alert button. The Save Changes page appears.
5. If your changes are validated, you can save them. If not, a descriptive message appears.
6. Choose Save and Restart. The Gateway restarts with your changes.

Quickstart For most users, Quickstart includes everything needed to configure a connection to your Service Provider.

LAN Configuration options for the Local Area Network side of the Gateway.

WAN Configuration options for the Wide Area Network connection on the Gateway.

Advanced Advanced configuration options for the Gateway. Consult the user documentation or help text before changing any of these configuration options.

Next, click on Advanced.

Network Configuration

- [IP Static Routes](#) Build IP static route table
- [IP Static ARP](#) Build IP static ARP table

NAT

- [Pinholes](#) Set up pinholes through NAT
- [IPMaps](#) Set up NAT one-to-one IP address mappings
- [Default Server](#) Set up NAT default server options
- [NAT Table Monitoring](#) Set up NAT Table Monitoring options

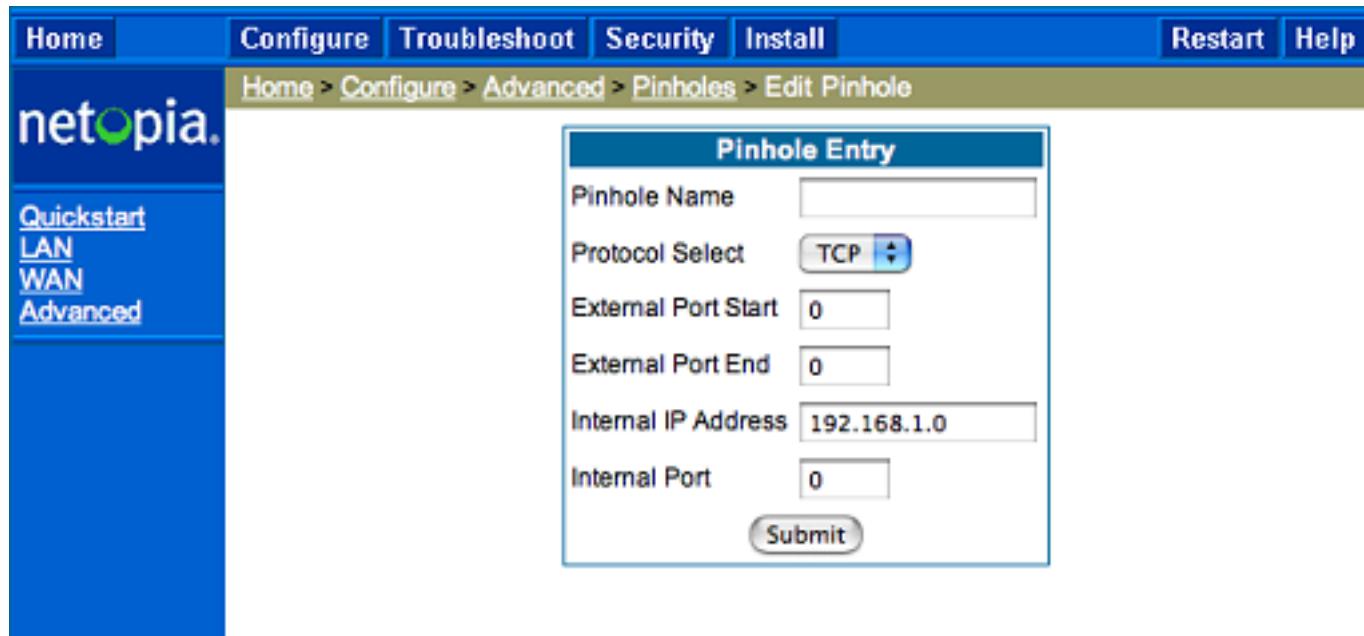
Services

- [Differentiated Services](#) Set up Differentiated Service options
- [DNS](#) Set up DNS options
- [DHCP Server](#) Set up DHCP server and relay-agent options
- [RADIUS Server](#) Set up RADIUS server options
- [SNMP](#) Set up SNMP community, trap and system group options
- [IGMP](#) Set up IGMP options
- [Access Control](#) Set up Access Control
- [UPnP](#) Enable or disable Universal Plug'n'Play
- [LAN Management \(TR-064\)](#) Enable or disable DSL Forum LAN-Side DSL CPE Configuration services
- [Ethernet Bridge](#) Set up ethernet MAC bridge

Miscellaneous

ZMD-DD-SBN4

From the Advanced menu, click on Pinholes.



Create your rule, then hit 'Submit', and repeat for each port. When you have completed, click on the yellow triangle with an '!' inside (located at the top righthand corner) to save your changes.

Checking Your Connection

4) Once you have forwarded all ports necessary for your DVR, you'll want to check and make sure each of these ports was successfully opened. To check this, go to <http://www.yougetsignal.com/tools/open-ports/>

Here, you will see fields for **Remote Address** and **Port Number**.

ZMD-DD-SBN4

To check that your ports are open, enter each port you've forwarded (one at a time) in to the Port Number field, and click 'Check'.

If you see a green flag, and a statement "Port X is open on XXX.XXX.XXX.XXX", you have forwarded your ports correctly. You are now able to view your DVR remotely.

If you see a red flag, the port is not open. Go back in to your router, and double check that all information is correct. In some cases, a port may be blocked by your ISP. To find out why, or to request it opened, please contact your ISP.

Important: The Remote Address that you see is **your DVR's external IP address**. This is the address that you will use to access your DVR from a different computer. Write this down!! And remember, ActiveX settings must be changed on each new computer that you are viewing from before you'll be able to bring your DVR up.

Unique solution ID: #1003

Author: Jamie Alksnis

Last update: 2014-10-01 15:41