

# Networking

## 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](http://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

# Networking

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.

# Networking

## Linksys

The screenshot shows the Linksys router web interface. At the top, the Linksys logo is on the left, and 'Firewall Version: v4.0B.8' is on the right. Below the logo, it says 'A Division of Cisco Systems, Inc.'. The main navigation bar includes 'Applications & Gaming' (selected), 'Setup', 'Wireless', 'Security', 'Access Restrictions', 'Applications & Gaming', 'Administration', and 'Status'. Under 'Applications & Gaming', there are sub-links: 'Port Range Forward' (selected), 'Port Triggering', 'DMZ', and 'QoS'. The 'Port Range Forward' page has a table with the following columns: 'Application', 'Start', 'End', 'Protocol', 'IP Address', and 'Enable'. The table contains 10 rows, each with input fields for 'Start' and 'End' (both set to 0), a 'Both' protocol dropdown, an 'IP Address' field (set to 192.168.10.0), and an 'Enable' checkbox. To the right of the table is a blue sidebar with the text: 'Port Range Forwarding: Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request for a certain port comes in from the Internet, the router will route the data to the computer you specify. Due to security concerns, you may want to limit port forwarding to only those ports you are using, and uncheck the Enable checkbox after you are finished. More...'

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

# Networking

The screenshot shows the Netgear settings interface for a 108 Mbps Wireless Firewall Router (WGT624 v3). The main heading is "Port Forwarding / Port Triggering". On the left is a navigation menu with options like Router Status, Attached Devices, Backup Settings, Set Password, Router Upgrade, and Advanced settings including Wireless Settings, Port Forwarding / Port Triggering, WAN Setup, LAN IP Setup, Dynamic DNS, Static Routes, Remote Management, and UPnP. The main content area has a sub-heading "Port Forwarding / Port Triggering" and a section "Please select the service type" with radio buttons for "Port Forwarding" (selected) and "Port Triggering". Below this is a form for adding a service with a "Service Name" dropdown (set to "AIM"), a "Server IP Address" field (192.168.1.1), and an "Add" button. A table below shows a single service entry with columns for #, Service Name, Start Port, End Port, and Server IP Address. The table contains one row with #1, Service Name AIM, Start Port 0, End Port 0, and Server IP Address 0.0.0. Below the table are buttons for "Edit Service", "Delete Service", and "Add Custom Service". On the right is a "Port Forwarding / Port Triggering Help" section with explanatory text.

**NETGEAR settings**  
108 Mbps Wireless Firewall Router WGT624 v3

**Port Forwarding / Port Triggering**

Please select the service type

Port Forwarding  
 Port Triggering

Service Name: AIM Server IP Address: 192.168.1.1 Add

#	Service Name	Start Port	End Port	Server IP Address
1	AIM	0	0	0.0.0.0

Edit Service Delete Service Add Custom Service

**Port Forwarding / Port Triggering Help**

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

# Networking

Product: DSL-2740B Firmware Version: EU\_5.17

**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.

**PORT FORWARDING RULES CONFIGURATION**

Remaining number of rules that can be created: 48

Name	Application Name	External Port	Internal Port
<input type="text"/>	<< Application Name ▾	TCP	TCP
IP Address	<< Computer Name ▾	UDP	UDP

Use Interface: pppoa\_0/pppob0 ▾

Add/Apply

**ACTIVE PORT FORWARDING RULES**

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...](#)

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

## Belkin

# Networking

**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  
WiFi 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

**STATES**

### 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](#)

Clear Changes Apply Changes

Add Active Worlds Add

Clear entry 1 Clear

	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 forwarding 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.

# Networking

## 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.

All applications

Age of Empires Age of Kings Age of Wonders Aliens vs Predator Anarchy Online Asheron's Call Baldur's Gate BattleCom Battlefield Communicator Black and White	<input type="button" value="Add"/> <input type="button" value="Remove"/>	Hosted Applications: <div style="border: 1px solid gray; height: 100px;"></div>
---	---	--

[Add a new user-defined application](#)

- 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:

# Networking

**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.



# Networking

## 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.

All applications

Age of Empires Age of Kings Age of Wonders Aliens vs Predator Anarchy Online Asheron's Call Baldur's Gate BattleCom Battlefield Communicator Black and White	<input type="button" value="Add"/> <input type="button" value="Remove"/>	<b>Hosted Applications:</b> <div style="border: 1px solid gray; height: 100px;"></div>
---	---	---

[Add a new user-defined application](#)

- 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.

# Networking

Home - Configure

**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.

<a href="#">Quickstart</a>	For most users, Quickstart includes everything needed to configure a connection to your Service Provider.
<a href="#">LAN</a>	Configuration options for the Local Area Network side of the Gateway.
<a href="#">WAN</a>	Configuration options for the Wide Area Network connection on the Gateway.
<a href="#">Advanced</a>	Advanced configuration options for the Gateway. Consult the user documentation or help text before changing any of these configuration options.

© 2005 Netopia, Inc.

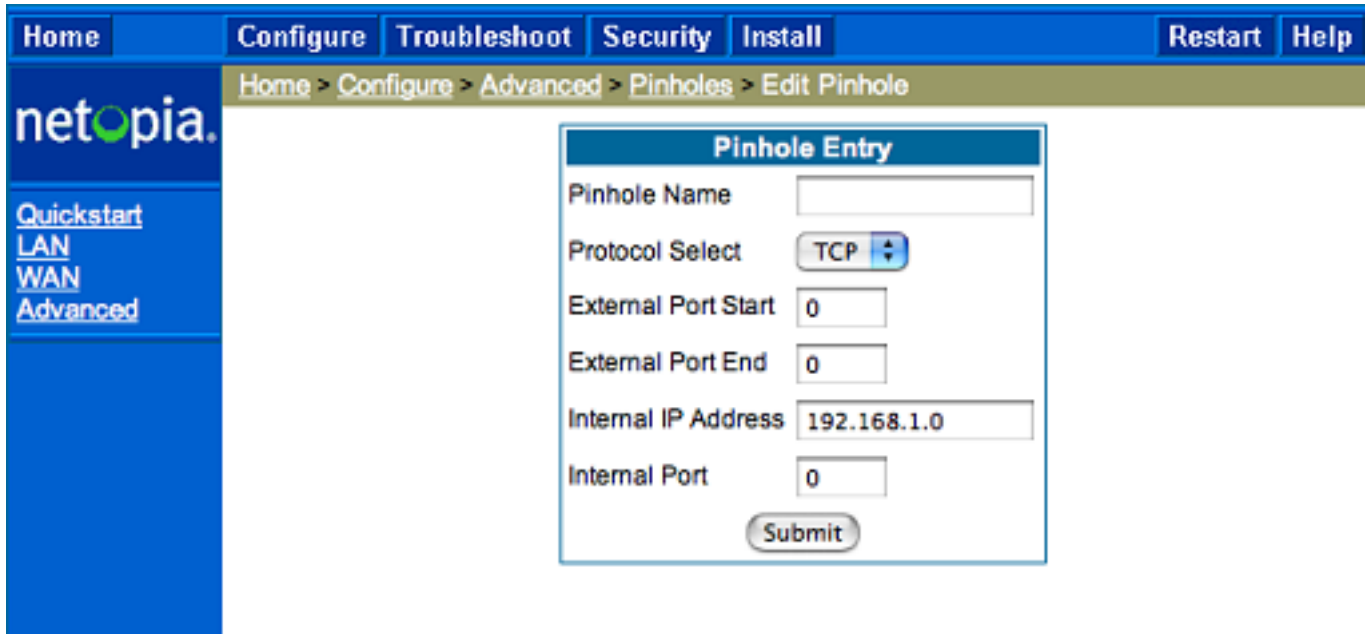
Next, click on Advanced.

Home - Configure - Advanced

Network Configuration	
<a href="#">IP Static Routes</a>	Build IP static route table
<a href="#">IP Static ARP</a>	Build IP static ARP table
NAT	
<a href="#">Pinholes</a>	Set up pinholes through NAT
<a href="#">IPMaps</a>	Set up NAT one-to-one IP address mappings
<a href="#">Default Server</a>	Set up NAT default server options
<a href="#">NAT Table Monitoring</a>	Set up NAT Table Monitoring options
Services	
<a href="#">Differentiated Services</a>	Set up Differentiated Service options
<a href="#">DNS</a>	Set up DNS options
<a href="#">DHCP Server</a>	Set up DHCP server and relay-agent options
<a href="#">RADIUS Server</a>	Set up RADIUS server options
<a href="#">SNMP</a>	Set up SNMP community, trap and system group options
<a href="#">IGMP</a>	Set up IGMP options
<a href="#">Access Control</a>	Set up Access Control
<a href="#">UPnP</a>	Enable or disable Universal Plug'n'Play
<a href="#">LAN Management (TR-064)</a>	Enable or disable DSL Forum LAN-Side DSL CPE Configuration services
<a href="#">Ethernet Bridge</a>	Set up ethernet MAC bridge
Miscellaneous	

# Networking

From the Advanced menu, click on Pinholes.



The screenshot shows the Netopia web interface. At the top, there is a navigation bar with buttons for Home, Configure, Troubleshoot, Security, Install, Restart, and Help. Below this is a breadcrumb trail: Home > Configure > Advanced > Pinholes > Edit Pinhole. On the left side, there is a sidebar with the Netopia logo and links for Quickstart, LAN, WAN, and Advanced. The main content area displays a 'Pinhole Entry' form with the following fields: Pinhole Name (text input), Protocol Select (dropdown menu set to TCP), External Port Start (text input set to 0), External Port End (text input set to 0), Internal IP Address (text input set to 192.168.1.0), and Internal Port (text input set to 0). A Submit button is located at the bottom of the form.

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**.

# Networking

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 be 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