



## **Network Configuration Guide (Generic)**

# Table of Contents

<b><u>TABLE OF CONTENTS</u></b> .....	<b>2</b>
<b><u>GETTING STARTED</u></b> .....	<b>4</b>
INTRODUCTION.....	4
DISCLAIMER .....	4
<b><u>QUICK SETUP GUIDE (POWER USERS ONLY)</u></b> .....	<b>4</b>
<b><u>PLANNING</u></b> .....	<b>4</b>
<b>EQUIPMENT NEEDED</b> .....	<b>4</b>
<b>GATHERING INFORMATION</b> .....	<b>5</b>
INFORMATION GATHERING CHECKLIST .....	7
YOUR ROUTER’S INTERNAL IP ADDRESS .....	8
YOUR ROUTER’S PUBLIC IP ADDRESS.....	8
YOUR ROUTER’S USERNAME AND PASSWORD.....	8
YOUR NETWORK’S DHCP RANGE .....	8
YOUR NETWORK’S SUBNET MASK.....	8
THE IP ADDRESS YOU WILL GIVE YOUR PRODUCT .....	8
YOUR PRODUCT’S USERNAME AND PASSWORD.....	9
EXISTING PORT FORWARD / NAT INFORMATION.....	9
THE DEFAULT PORTS AND PROTOCOLS FOR YOUR PRODUCT.....	9
<b>PITFALLS TO AVOID</b> .....	<b>9</b>
IP ADDRESSES IN YOUR DHCP RANGE.....	9
DYNAMIC IP ADDRESSES .....	9
USING PUBLIC DNS SERVERS .....	10
USING DYNAMIC PUBLIC IP ADDRESSES WITHOUT DYNAMIC DNS.....	12
<b><u>CONFIGURATION</u></b> .....	<b>12</b>
<b>CONFIGURING YOUR PRODUCT</b> .....	<b>12</b>
USER ACCOUNTS .....	12
NETWORK SETTINGS .....	13
<b>CONFIGURING YOUR ROUTER</b> .....	<b>13</b>
CHECKING FOR CONFLICTS .....	13
FINALIZING YOUR SETUP .....	13
<b>TESTING</b> .....	<b>14</b>
TESTING FROM YOUR LAN (INTERNAL).....	14
TESTING FROM THE WAN (INTERNET).....	14
<b><u>ADDITIONAL RESOURCES</u></b> .....	<b>14</b>

<b>NETWORKING</b> .....	<b>14</b>
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) .....	14
IP ADDRESSING .....	14
LOCAL AREA NETWORKS (LAN) .....	14
NETWORK ADDRESS TRANSLATION (NAT) .....	14
PORT FORWARDING .....	14
PORTS .....	15
ROUTING / ROUTER CONFIGURATION .....	15
SUBNET / SUBNET MASKING .....	15
TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL (TCP/IP) .....	15
USER DATAGRAM PROTOCOL .....	15
WIDE AREA NETWORKS (WAN) .....	15
<b>FIREWALLS</b> .....	<b>15</b>
GENERAL INFORMATION .....	15
COMMON PORT NUMBERS.....	15
SOFTWARE FIREWALLS .....	16

Apex CCTV

# Getting Started

## ***Introduction***

Thank you for choosing ApexCCTV. We hope that this document will assist you in configuring your new product for use on your network and via the internet. This document follows industry standard best practices, and while you do not need to follow every single step on this list, doing so will provide you with a reliable and secure connection to your product.

## ***Disclaimer***

This document requires a basic understanding of networking principles including, but not limited to, network address translation (NAT), transmission control protocol/internet protocol (TCP/IP), user datagram protocol (UDP), subnet and subnet mask configuration, dynamic host configuration protocol (DHCP), IP addresses, routing and router configuration, public vs. private networks, etc...

The basic knowledge described above is outside the scope of this document, and will be covered briefly or not at all, and only as it applies to an individual step you need to take in configuring your product. Please find other resources in the “Additional Resources” section at the end of this document.

## **Quick Setup Guide (Power Users Only)**

The gist of setting up surveillance products for network use is very straightforward.

- 1) Configure your product with an appropriate network address (use best practices).
- 2) Determine the ports that it needs access on.
- 3) Forward those ports appropriately through one or more routers, starting with your internet gateway.

## **Planning**

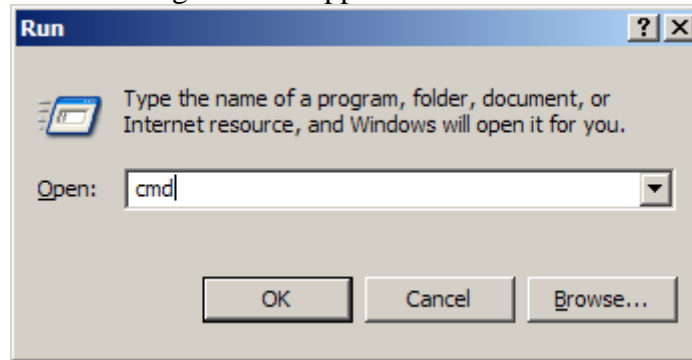
### ***Equipment Needed***

- 1) Your network enabled product from ApexCCTV, with working cameras connected.
- 2) Any software CDs that came with your product.
- 3) Your product manual (may be on your CD)
- 4) A Television monitor, hooked up to the DVR.
- 5) A Network cable connecting your DVR to your network.
- 6) A router.
- 7) An additional PC on your network with Windows (Preferably XP) installed.

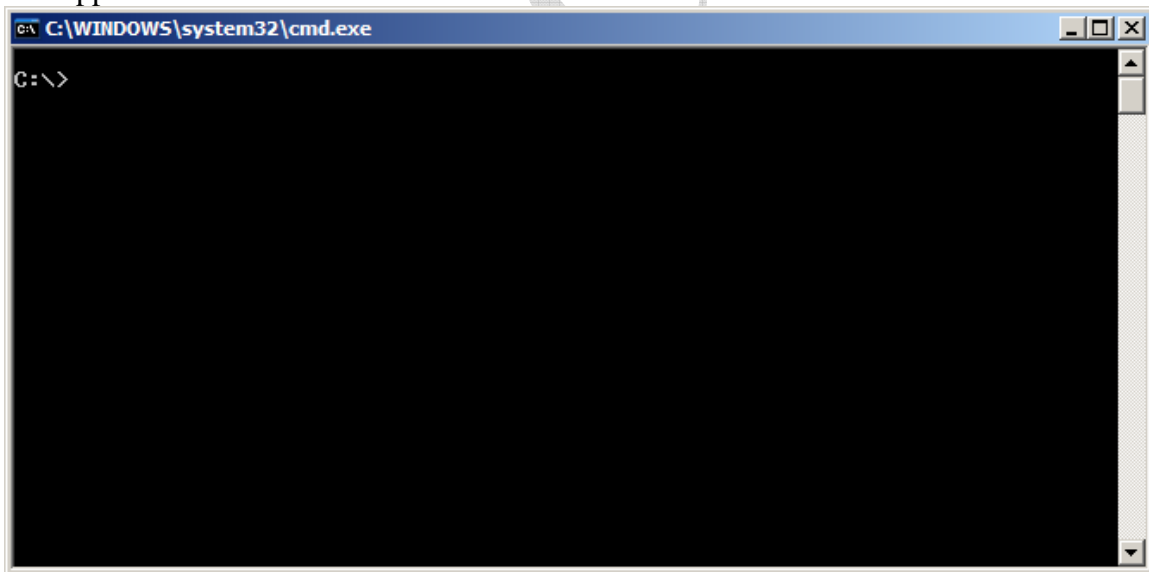
## ***Gathering Information***

Before continuing, you will need to gather the following information. If you do not know or cannot find some of this information, please contact your network administrator or your internet service provider (ISP).

There is some specific network information you will need to have readily available before you start configuring your network and surveillance product. You can find much of this information (in Windows XP) by clicking Start → Accessories → Command Prompt. If there is no option under accessories for “Command Prompt,” you can also click on Start → Run. A dialog box will appear:



Type “cmd” in the dialog box and click the OK button to continue. A command prompt will appear that looks similar to this:



Once you have a command prompt up, type the following line and press the Enter key:

```
ipconfig /all
```

You should have some information similar to what is below on your screen:

```
C:\WINDOWS\system32\cmd.exe
C:\>ipconfig /all

Windows IP Configuration

    Host Name . . . . . : eric
    Primary Dns Suffix . . . . . : vs-us.local
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : vs-us.local

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    Description . . . . . : Attansic L1 Gigabit Ethernet 10/100/
1000Base-T Controller
    Physical Address. . . . . : 00-1B-FC-C9-FD-B7
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 192.168.1.33
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DNS Servers . . . . . : 192.168.1.6
                          192.168.1.10
                          66.180.96.12
                          64.238.96.12
    Primary WINS Server . . . . . : 192.168.1.6
    Secondary WINS Server . . . . . : 192.168.1.10

C:\>
```

Please take special note of the Subnet mask, Default Gateway, and DNS Servers.

The complete list of information you will need is listed below. We recommend using the checklist on the following page as you gather information to be sure you will have everything you need before you begin. If you are unsure of how to find some of this information, there are tips for each item following the Information Gathering Checklist.

## Information Gathering Checklist

Your router's internal IP address

Your router's public IP address

Your router's username and password

Your network's DHCP range

Your network's DNS server addresses

Your network's subnet mask

The IP Address you will give your product

Your product's username and password

Existing forwarded ports or NAT entries from your router

The default ports that your product uses.

## **Your router's internal IP address**

This is typically the same as the “default gateway” from the above information.

## **Your router's public IP address**

You can find this by visiting [www.whatismyip.com](http://www.whatismyip.com).

## **Your router's username and password**

If you do not know this information, you will need to look in your product manual or contact your network administrator or internet service provider. If you have not changed your router's default username and password, you can probably find it on the internet. Try looking at your router, jotting down its manufacturer and model number, and then doing a search on Google for the model number, plus “default username.” For instance, if my router is a D-Link DFL-200, I would search for:

DFL-200 default username

You can also use find your Router's default guide on [www.portforward.com](http://www.portforward.com).

Either of these will more likely than not help you find the login information you need.

## **Your network's DHCP range**

Most networks employ DHCP. Typically, your router doubles as your DHCP server. To find your network's DHCP range, you will need to log into your router (or other DHCP server) and find the page containing those settings. If you cannot find these settings, contact your network administrator or internet service provider.

## **Your network's subnet Mask**

A subnet mask (this is a VERY short simplification) is used to “subdivide” your network into segments. You should be able to find your network's subnet mask in the settings you saw earlier when you ran “ipconfig /all” from a command prompt. You can also find these under Control Panel → Network Connections → Local Area Connection (or your network adapter's name) → Properties → Internet Protocol (TCP/IP) Properties.

## **The IP Address you will give your product**

You should first log into your router (or other DHCP server) and determine your DHCP range. You need to pick a valid static IP address that is outside your DHCP range. You should also (as a minimum) ping the IP address you have selected to make sure another network device is not occupying it. On windows XP:

Start → Accessories → Command Prompt → Type:

```
ping [IP Address]
```

If you get a valid response, you should choose another address.

## **Your product's username and password**

You will need the administrative username and password for your product so that you can log into it and make changes. Your default user name and password are in your product manual. If your defaults have been changed, you will need to get this information from within your organization.

## **Existing port forward / NAT information**

You need know your existing port forward and/or NAT settings before adding new ones in order to avoid conflicts. **If you use point of sales software on your network you should call your vendor and make CERTAIN you have the settings and know how to avoid creating conflicts with them.** Failing to do so could threaten your ability to create new transactions for a significant period of time.

## **The default ports and protocols for your product**

You can find the default ports that you product uses in your usual manual. Many networkable surveillance products show these port numbers on one or more settings screens as well.

## ***Pitfalls to Avoid***

### **IP Addresses in Your DHCP Range**

DHCP servers are used for giving out temporary IP addresses to products on your network that need them. This means that the IP address of any DHCP on your network can and will change as these IP address leases expire.

Your DHCP server will have a range of IP addresses that it can use for this purpose. If you set your product's static IP address to be within this range, you are creating the possibility that another product will be given the same IP address by your DHCP server. Should this occur, both of your products will cease to function on your network until the problem is resolved.

A best practice is to set the static IP address of your product to be outside of your DHCP server range, avoiding the possibility of this type of conflict. For example, if your DHCP server's IP address range was 192.168.1.100 – 192.168.1.200, good IP addresses for your product would be 192.168.1.50 or 192.168.1.250, but not 192.168.1.105.

### **Dynamic IP Addresses**

If you leave your product set to acquire a dynamic IP address, its IP address is likely to change over time, nullifying the effects of any forwarded ports or NAT routes to your product and breaking access to it from the internet. If this occurs, you will have to re-configure your router to pass the correct ports to it again.

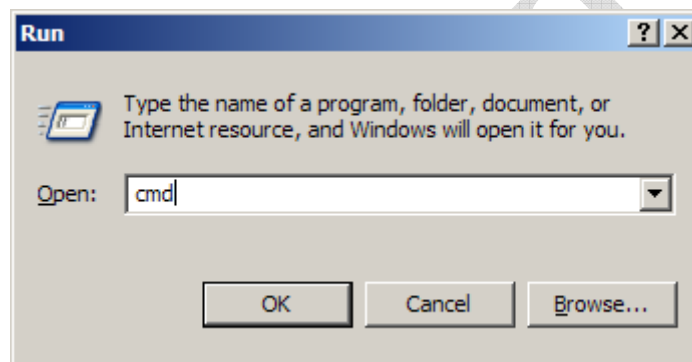
A best practice is to use static IP addresses that are outside your DHCP range for all products that will have ports forwarded to them.

## Using Public DNS Servers

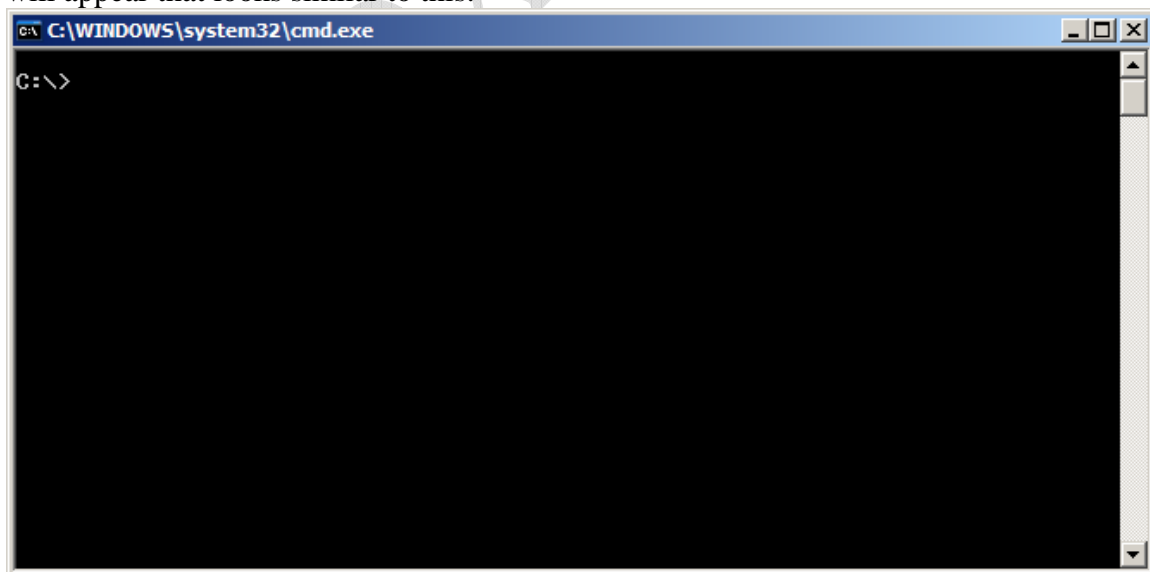
Very often a DHCP server will configure products not to use an internal DNS server, as they should, but rather the public DNS servers provided by your internet service provider. This is fine if your public IP address is static, but if it is dynamic your DNS server addresses may possibly change from time to time.

As a best practice use your router's IP address or another internal DNS server that can forward DNS requests to external servers if at all possible. This way, if your router is assigned a new IP address and DNS server settings from your ISP, DNS will still function on your product.

You can determine if you can use your router as a DNS server (in Windows XP) by clicking Start → Accessories → Command Prompt. If there is no option under accessories for "Command Prompt," you can also click on Start → Run. A dialog box will appear:



Type "cmd" in the dialog box and click the OK button to continue. A command prompt will appear that looks similar to this:



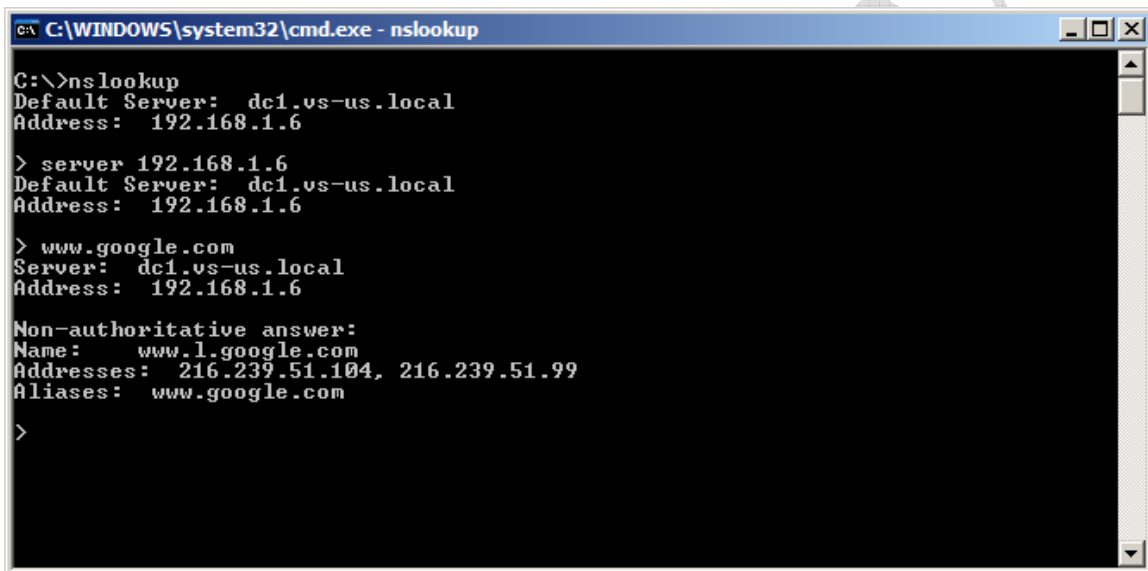
Once you have a command prompt up, type the following commands and press the Enter key after each one:

```
nslookup
```

```
server [router's IP address here] – example "server 192.168.1.1"
```

```
www.google.com
```

If the response looks something like the following, you should use your router's IP address when configuring your product's primary DNS server setting.

A screenshot of a Windows command prompt window titled "C:\WINDOWS\system32\cmd.exe - nslookup". The window shows the following text:

```
C:\>nslookup
Default Server:  dc1.us-us.local
Address:  192.168.1.6

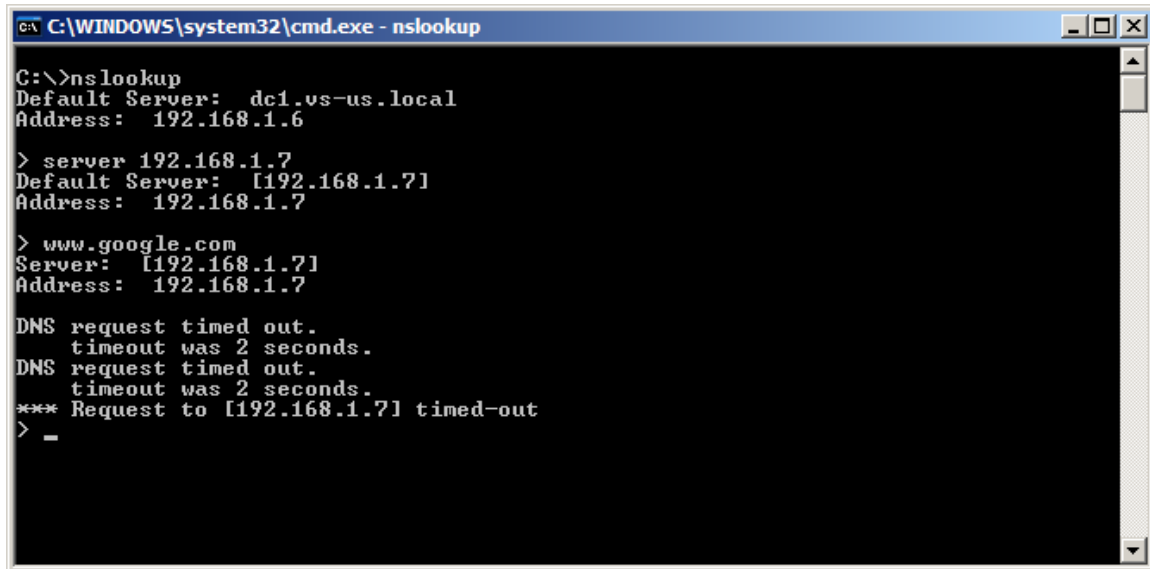
> server 192.168.1.6
Default Server:  dc1.us-us.local
Address:  192.168.1.6

> www.google.com
Server:  dc1.us-us.local
Address:  192.168.1.6

Non-authoritative answer:
Name:    www.l.google.com
Addresses:  216.239.51.104, 216.239.51.99
Aliases:  www.google.com

>
```

However, if the response looks more like the following, you should use whatever value was under the "DNS Servers" section when you ran Windows IP Configuration.



```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\>nslookup
Default Server:  dc1.us-us.local
Address:  192.168.1.6

> server 192.168.1.7
Default Server:  [192.168.1.7]
Address:  192.168.1.7

> www.google.com
Server:  [192.168.1.7]
Address:  192.168.1.7

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
*** Request to [192.168.1.7] timed-out
> _
```

## Using Dynamic Public IP Addresses without Dynamic DNS

If your Internet Service Provider has given you a dynamic IP address with your internet connection, it is best, if possible, to acquire a static IP address from them. This way, you can browse to your product on the internet by simply using your public IP address. For example, if your public IP address (from your information gathering checklist) is 96.226.2.104, you would simply open Internet Explorer and enter [http:// 96.226.2.104/](http://96.226.2.104/) in your address bar to view your product.

If you cannot acquire a static IP address, there are two possibilities. First, if your public IP address changes and you can no longer view your product, simply browse to [www.whatismyip.com](http://www.whatismyip.com) from within your network to see your new public IP address, and use that one until it changes again (usually several months).

If you do not like this option, you can use a dynamic DNS service. This way, you can browse to a name, rather than address, such as <http://mydvr.mydomain.com>. There are several of these services that offer free accounts. We prefer [www.dyndns.org](http://www.dyndns.org), and wholeheartedly recommend them. Their setup is easy and free, and they offer software that prevents your free account from expiring if your public IP address does not change often enough. Please visit their site for more information.

## Configuration

### *Configuring your Product*

#### User Accounts

**First and foremost, if you are exposing your DVR to the internet, as a best practice you should change your default password to protect yourself from malicious individuals.** Many products allow remote administration, including changing their

settings and deleting data from their hard drives. Changing your password is your best defense against attack.

You should change your password every 90 days.

Some products do not allow multiple accounts, but wherever possible, use a separate account for remote viewing or giving your employees that does NOT have administrative privileges. Only use your administrative account for reviewing events or changing your settings.

## **Network Settings**

Before beginning this section, please make sure your product is connected to your network.

By now you should have determined the following settings to your product. Please log into it, open your networks settings page/screen, and update the following information.

IP Address should be **static**, not **DHCP**.

IP Address

Subnet Mask

Default Gateway (or just Gateway)

DNS Servers

## ***Configuring Your Router***

### **Checking For Conflicts**

Be sure to look at any forwarded ports or NAT routes you already have configured. Make sure they do not conflict (use any of the same ports) as your product. If they do, for any reason, you should change the conflicting default ports on your product to something else, so that you will not be causing problems for both applications.

### **Finalizing Your Setup**

First, log into your Router with administrative privileges. Once you are logged in, locate the settings page/screen containing port forwarding (sometimes called application settings or triggers) or NAT configuration page. These settings are usually under the “Firewall” or “Advanced” section of your router configuration.

Using the appropriate page/screen in your router, make entries for each of the ports (be sure to use the correct protocol as well) required by your product. Be sure your mappings point to the internal IP address you selected for your product, and that you click any “activate” or “enable” check boxes for each entry.

## ***Testing***

### **Testing from your LAN (Internal)**

Open internet explorer and browse to the IP address that you assigned to your product. You should be looking at the login or default screen for your product. Make sure to include the web server port (If something other than port 80) you have assigned to you have your product. For example, if you product uses port 81 for its web server and has an IP address of 192.168.1.50, you would browse to <http://192.168.1.50:81>.

### **Testing from the WAN (Internet)**

You should be able to substitute your public IP address for your internal one (see your information gathering checklist) from a PC outside your network (Viewing a product at your office from home or vice-versa) and achieve the same result. For example, if your public IP address is 96.226.2.104 and your product uses port 81 for its web server, you would browse to <http://96.226.2.104:81>.

## **Additional Resources**

### ***Networking***

#### **Dynamic Host Configuration Protocol (DHCP)**

[http://en.wikipedia.org/wiki/Dynamic\\_Host\\_Configuration\\_Protocol](http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)

<http://www.dhcp.org/>

[http://www.dhcp-handbook.com/dhcp\\_faq.html](http://www.dhcp-handbook.com/dhcp_faq.html)

<http://www.webopedia.com/TERM/D/DHCP.html>

#### **IP Addressing**

[http://en.wikipedia.org/wiki/IP\\_address](http://en.wikipedia.org/wiki/IP_address)

[http://www.3com.com/other/pdfs/infra/corpinfo/en\\_US/501302.pdf](http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf)

<http://computer.howstuffworks.com/question549.htm>

[http://www.webopedia.com/TERM/I/IP\\_address.html](http://www.webopedia.com/TERM/I/IP_address.html)

#### **Local Area Networks (LAN)**

[http://en.wikipedia.org/wiki/Local\\_area\\_network](http://en.wikipedia.org/wiki/Local_area_network)

[http://compnetworking.about.com/cs/lanvlanwan/g/bldef\\_lan.htm](http://compnetworking.about.com/cs/lanvlanwan/g/bldef_lan.htm)

[http://www.webopedia.com/TERM/L/local\\_area\\_network\\_LAN.html](http://www.webopedia.com/TERM/L/local_area_network_LAN.html)

#### **Network Address Translation (NAT)**

[http://en.wikipedia.org/wiki/Network\\_address\\_translation](http://en.wikipedia.org/wiki/Network_address_translation)

<http://computer.howstuffworks.com/nat.htm>

<http://www.webopedia.com/TERM/N/NAT.html>

#### **Port Forwarding**

<http://www.portforward.com/>

[http://en.wikipedia.org/wiki/Port\\_forwarding](http://en.wikipedia.org/wiki/Port_forwarding)  
<http://www.zeropaid.com/news/6160/Introduction+to+Port+Forwarding>

## **Ports**

[http://en.wikipedia.org/wiki/Computer\\_port\\_%28software%29](http://en.wikipedia.org/wiki/Computer_port_%28software%29)  
<http://itmanagement.webopedia.com/TERM/P/port.html>

## **Routing / Router Configuration**

<http://en.wikipedia.org/wiki/Routing>  
[http://cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/routing.htm](http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm)  
<http://www.webopedia.com/TERM/R/routing.html>

## **Subnet / Subnet Masking**

<http://en.wikipedia.org/wiki/Subnetwork>  
<http://www.networkcomputing.com/unixworld/tutorial/001.html>  
<http://www.webopedia.com/TERM/S/subnet.html>

## **Transmission Control Protocol / Internet Protocol (TCP/IP)**

[http://en.wikipedia.org/wiki/Internet\\_protocol\\_suite](http://en.wikipedia.org/wiki/Internet_protocol_suite)  
[http://www.webopedia.com/TERM/T/TCP\\_IP.html](http://www.webopedia.com/TERM/T/TCP_IP.html)

## **User Datagram Protocol**

[http://en.wikipedia.org/wiki/User\\_Datagram\\_Protocol](http://en.wikipedia.org/wiki/User_Datagram_Protocol)  
<http://www.webopedia.com/TERM/U/UDP.html>

## **Wide Area Networks (WAN)**

[http://en.wikipedia.org/wiki/Wide\\_area\\_network](http://en.wikipedia.org/wiki/Wide_area_network)  
[http://www.webopedia.com/TERM/W/wide\\_area\\_network\\_WAN.html](http://www.webopedia.com/TERM/W/wide_area_network_WAN.html)

## **Firewalls**

While firewall configuration is outside the scope of this document, various hardware and software firewalls can create configuration and remote access problems for various security products. The following information is provided in helps of providing starting points for troubleshooting firewall issues. Links to many common software firewall products and vendors are provided.

## **General Information**

[http://en.wikipedia.org/wiki/Firewall\\_\(networking\)](http://en.wikipedia.org/wiki/Firewall_(networking))  
<http://www.howstuffworks.com/firewall.htm>  
<http://www.webopedia.com/TERM/f/firewall.html>

## **Common Port Numbers**

<http://www.iana.org/assignments/port-numbers>  
[http://en.wikipedia.org/wiki/List\\_of\\_TCP\\_and\\_UDP\\_port\\_numbers](http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers)

[http://www.webopedia.com/quick\\_ref/portnumbers.asp](http://www.webopedia.com/quick_ref/portnumbers.asp)

## **Software Firewalls**

BlackICE PC Protection

<http://www.iss.net/>

BullGuard Suite

<http://www.bullguard.com/default.aspx>

Comodo Personal Firewall

<http://www.personalfirewall.comodo.com/>

F-Secure Internet Security

[http://www.f-secure.com/home\\_user/products\\_a-z/fsis2007.html](http://www.f-secure.com/home_user/products_a-z/fsis2007.html)

Jetico Personal Firewall

<http://www.jetico.com/>

Kaspersky Internet Security

<http://www.kaspersky.com/>

LavaSoft Personal Firewall

[http://www.lavasoftusa.com/products/lavasoft\\_personal\\_firewall.php](http://www.lavasoftusa.com/products/lavasoft_personal_firewall.php)

McAfee Personal Firewall

<http://us.mcafee.com/default.asp>

Microsoft Windows Firewall

[http://www.microsoft.com/windowsxp/using/security/internet/sp2\\_wfintro.mspx](http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx)

NeT Firewall

<http://www.ntkernel.com/w&p.php?id=18>

Norman Personal Firewall

[http://www.norman.com/products\\_npf.shtml](http://www.norman.com/products_npf.shtml)

OutpostPro Firewall

<http://www.agnitum.com/>

Panda Platinum Internet Security

[http://us.pandasoftware.com/products/platinum\\_is/](http://us.pandasoftware.com/products/platinum_is/)

pcInternet Patrol

<http://www.pcinternetpatrol.com/>

Preventon

<http://www.preventon.com/>

PrivateFirewall

<http://www.privacyware.com/features.html>

Terminet

<http://www.infotecs.biz/Soft/terminet.htm>

Trend Micro PC-cillin Internet Security

<http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm>

VisNetic Firewall

<http://www.deerfield.com/products/visnetic-firewall/>

Webroot Personal Firewall

<http://send.onenetworkdirect.net/z/11246/CD45178/>

Apex CCTV