

Remote Access 101: Set up with Multiple Routers

If you have properly port forwarded your router and remote access still does NOT work, you may have multiple routers on your network. This white paper describes the steps you can take to properly configure your network for remote access.

| | |
|----------------------------------------------------|---|
| Introduction | 2 |
| Enabling the DMZ | 2 |
| Configuring Port Forwarding on Double NAT Networks | 3 |
| Actiontec Routers | 3 |
| Buffalo Routers | 3 |
| D-Link Routers | 4 |
| Routers with DD-WRT Firmware | 4 |
| Linksys Routers (Original Firmware) | 5 |
| Netgear Routers | 6 |
| Routers with Tomato Firmware | 6 |
| Bridging the Secondary Router | 7 |
| Bridging the Primary Router | 7 |



an EMC company

Introduction

If you have properly port forwarded your router and remote access still does NOT work, you may have multiple routers on your network. In this situation you will most likely have two NAT (Network Address Translation) firewalls.

1. One of the easiest ways to identify this issue is to login to the router to which the Iomega Device is connected.
2. Once you have logged in, go to the page that shows the router's WAN IP address—usually Status or Network Info.
3. If the WAN IP address begins with 192.168, 10, or 172, you may have a NAT Firewall between the router and Internet connection.

There are several options for resolving double NAT situations. The sections below will explore the pros and cons of each resolution:

NOTE: These instructions will refer to the router that is connected directly to the internet as the "Primary Router." The cascaded router or router to which your StorCenter is connected will be referred to as the "Secondary Router."

- Use the primary router's DMZ
- Port forward the primary router to the secondary router
- Put the secondary router in bridging mode
- Put the primary router in bridging mode

Enabling the DMZ

Most routers have a feature called DMZ or Default Server. DMZ stands for "Demilitarized Zone," "Data Management Zone," "Demarcation Done" or perimeter network. The DMZ allows you to enter an IP address that will exist outside the router's NAT Firewall.

This is the easiest way to configure your network to handle double NAT situations, however, it is dependent on your primary router having DMZ functionality.

To enable the DMZ:

1. Log into the primary router.
2. Navigate to the settings page for DMZ or Default Server. You will need to consult the documentation that came with your router for information on where this feature is found.
3. Enter the secondary router's IP address.
4. Save your settings.

Your secondary router is no longer behind your primary router's firewall. If port forwarding is correctly configured, remote access should now be working properly. Moving your secondary router into the DMZ should not have any effect on the security of the network since it is still protected by the secondary router's firewall.



Configuring Port Forwarding on Double NAT Networks

If for some reason the network configuration cannot be changed and your setup requires the double NAT, you must perform the port forwarding steps twice. On the primary router, port forward to the cascaded router's external IP address. On the Cascaded router, port forward to the StorCenter's IP address.

NOTE: These instructions assume that you have already port forwarded your secondary router. Iomega is **NOT** responsible for network intrusions caused by opening ports in your internet gateway's firewall (port forwarding).

Actiontec Routers

1. Log into your primary router by entering its IP address in the browser's URL field. The default IP address for this router is **192.168.0.1**.
2. If necessary, enter your router's username and password, then click **OK**.
3. Click **Setup/Configuration** in the Main Menu.
4. Click **Advanced Setup** in the left-hand navigation pane.
5. Click **Begin Advanced Setup**.
6. Click **Port Forwarding** in the left-hand navigation pane.
7. Enter **443** in both field under **IP Port Range**.
8. Select **TCP** from the **Protocol** drop-down menu.
9. Enter the IP Address of your secondary router in the **IP Address field**.
10. Click **Add**.
11. If you are only forwarding the ports for Remote Access, skip to step 16. For information of port forwarding FTP, proceed to the next step.
12. Enter **21** in both fields under **IP Port Range**.
13. Select **TCP** from the **Protocol** drop-down menu.
14. Enter the IP Address of your secondary router in the **IP Address field**.
15. Click **Add**.
16. Click **Save and Restart**.

These instructions are based on an Actiontec GT701-WG with QW04-3.60.2.0.6.3-GT701-WG firmware.

Buffalo Routers

1. Log into your primary router by entering its IP address in the browser's URL field. The default IP address for this router is **192.168.0.10**.
2. If necessary, enter your router's username and password, then click **OK**. The Default username is **root**. The default password is blank.
3. Click **Internet Games (Port Mapping)** in the left-hand navigation pane.
4. Enter **443** in the **TCP** field.



5. Click the **Manual Configuration** radio button.
6. Enter your secondary router's IP address.
7. Click **Apply**.
8. If you are only forwarding the ports for Remote Access, you have completed the configuration. For information of port forwarding FTP, proceed to the next step.
9. Enter **21** in the **TCP** field.
10. Click the **Manual Configuration** radio button.
11. Enter your secondary router's IP address.
12. Click **Apply**.

These instructions are based on a Buffalo WHR-HP-G54.

D-Link Routers

1. Log into your primary router by entering its IP address in the browser's URL field. The default IP address for this router is **192.168.0.1**.
2. If necessary, enter your router's username and password, then click **OK**. The Default username is **admin**. The default password is blank.
3. Click the **Advanced** tab.
4. Click **Port Forwarding** in the left-hand navigation pane.
5. Enter **StorCenter Remote Access** in the **Name** field.
6. Enter your secondary router's IP address in the **IP Address** field.
7. Enter **443** in both the **Start** and **End** fields
8. Select **TCP** from the **Traffic Type** drop-down menu.
9. Check the untitled box on the left-side of the line to enable the forwarding rule.
10. If you are only forwarding the ports for Remote Access, skip to step 15. For information of port forwarding FTP, proceed to the next step.
11. Enter your secondary router's IP address in the **IP Address** field.
12. Enter **21** in both the **Start** and **End** fields
13. Select **TCP** from the **Traffic Type** drop-down menu.
14. Check the untitled box on the left-side of the line to enable the forwarding rule.
15. Click **Save Settings**.

These instructions are based on a D-Link EBR-2310.

Routers with DD-WRT Firmware

1. Log into your primary router by entering its IP address in the browser's URL field. The default IP address for this router is **192.168.2.1**.
2. If necessary, enter your router's username and password, then click **OK**. The Default username is **root**. The default password is **admin**.



3. Click the **Applications & Gaming** tab.
4. Click the **Port Range Forwarding** sub-tab.
5. Enter **StorCenter Remote Access** in the **Application** field.
6. Enter **443** in the **Start** and **End** fields.
7. Select **TCP** from the **Protocol** drop-down menu.
8. Enter your secondary router's IP address in the **IP Address** field.
9. Check the **Enable** box to enable the forwarding rule.
10. Click **Add**.
11. If you are only forwarding the ports for Remote Access, skip to step 18. For information of port forwarding FTP, proceed to the next step.
12. Enter **StorCenter FTP** in the **Application** field.
13. Enter **21** in the **Start** and **End** fields.
14. Select **TCP** from the **Protocol** drop-down menu.
15. Enter your secondary router's IP address in the **IP Address** field.
16. Check the **Enable** box to enable the forwarding rule.
17. Click **Add**.
18. Click **Save Settings**.

These instructions are based on DD-WRT firmware v23 SP2 on a Linksys WRT-54G.

Linksys Routers (Original Firmware)

1. Log into your primary router by entering its IP address in the browser's URL field. The default IP address for this router is **192.168.1.1**.
2. If necessary, enter your router's username and password, then click OK. The Default username is blank. The default password is **admin**.
3. Click the **Security** tab.
4. Deselect **Block Anonymous Internet Requests**.
5. Click the **Save Settings** button.
6. Click the **Applications & Gaming** tab.
7. Click the **Port Range Forwarding** sub-tab.
8. Enter **StorCenter Remote Access** in the **Application** field.
9. Enter **443** in the **Start** and **End** fields.
10. Select **TCP** from the **Protocol** drop-down menu.
11. Enter your secondary router's IP address in the **IP Address** field.
12. Check the **Enable** box to enable the forwarding rule.
13. If you are only forwarding the ports for Remote Access, skip to step 19. For information of port forwarding FTP, proceed to the next step.



14. Enter **StorCenter FTP** in the **Application** field.
15. Enter **21** in the **Start** and **End** fields.
16. Select **TCP** from the **Protocol** drop-down menu.
17. Enter your secondary router's IP address in the **IP Address** field.
18. Check the **Enable** box to enable the forwarding rule.
19. Click **Save Settings**.

These instructions are based on DD-WRT firmware v23 SP2 on a Linksys WRT-54G.

Netgear Routers

1. Log into your primary router by entering its IP address in the browser's URL field. The default IP address for this router is **192.168.0.1**.
2. If necessary, enter your router's username and password, then click OK. The Default username is **admin**. The default password is **password**.
3. Click **Port Forwarding** in the left-hand navigation pane.
4. Click the **Add Custom Service** button.
5. Enter **StorCenter Remote Access** in the **Service Name** field.
6. Enter **443** in the **Starting Port** and **Ending Port** fields.
7. Enter your secondary router's IP address in the **Server IP Address** field.
8. Check the **Enable** box to enable the forwarding rule.
9. Click **Add**.
10. If you are only forwarding the ports for Remote Access, you have completed the configuration. For information of port forwarding FTP, proceed to the next step.
11. Click the **Add Custom Service** button.
12. Enter **StorCenter FTP** in the **Service Name** field.
13. Enter **21** in the **Starting Port** and **Ending Port** fields.
14. Enter your secondary router's IP address in the **Server IP Address** field.
15. Check the **Enable** box to enable the forwarding rule.
16. Click **Add**.

These instructions are based on a Netgear RP614.

Routers with Tomato Firmware

1. Log into your primary router by entering its IP address in the browser's URL field.
2. If necessary, enter your router's username and password, then click **OK**.
3. Click the **Port Forwarding** in the left-hand navigation pane.
4. Select **TCP** from the **Proto** drop-down menu.
5. Enter **443** in the **Ext Ports** and **Int Ports** fields.



6. Enter your secondary router's IP address in the **Int Address** field.
7. Enter **StorCenter Remote Access** in the **Description** field.
8. Check the **Enable** box to enable the forwarding rule.
9. Click **Add**.
10. If you are only forwarding the ports for Remote Access, skip to step 17. For information of port forwarding FTP, proceed to the next step.
11. Select **TCP** from the **Proto** drop-down menu.
12. Enter **21** in the **Ext Ports** and **Int Ports** fields.
13. Enter your secondary router's IP address in the **Int Address** field.
14. Enter **StorCenter FTP** in the **Description** field.
15. Check the **Enable** box to enable the forwarding rule.
16. Click **Add**.
17. Click **Save**.

These instructions are based on a Tomato v1.23 on a Linksys WRT-54G.

Bridging the Secondary Router

Make sure that the primary router (usually the one connected to or acting as the DSL/Cable modem) is the only one with DHCP (Dynamic Host Configuration Protocol) and NAT (Network Address Translation) enabled. The secondary should be changed to bridging mode. Make sure the second router connects to the primary router using a standard port rather than the port labeled uplink or Internet. This will basically turn your secondary router into a switch; however, you can still enable its Wireless Access Point (if equipped).

See the documentation that came with your router for configuration information and settings.

Linksys Users: To properly bridge your router, navigate to the **Setup** → **Advanced Routing** and make sure that **NAT** is **Disabled** and/or the **Operation Mode** is set to **Intranet Router**. Your router will most likely NOT have both features.

Bridging the Primary Router

If none of the above options are available, you will need to enable transparent bridging on your primary router. You will probably need to call your ISP (Internet Service Provider) to have the DSL or Cable Modem/NAT put into Bridge mode which will disable the first NAT/Firewall. Once this first firewall in the modem is disabled, the secondary router will handle all the network traffic, Port Forwarding, and allow Remote Access to work.

CAUTION! This is not something you should attempt without help from the ISP. If bridge mode is attempted by the Customer and not configured properly it can render the Customers Internet connection inoperable. Primary router bridging may also require special configuration information and settings on the secondary router.



Copyright © 2009 Iomega Corporation. All rights reserved. Iomega, StorCenter, and the stylized "i" logo are registered trademarks of Iomega Corporation in the United States and/or other countries. EMC and Retrospect are registered trademarks of EMC Corporation in the United States and/or other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Apple, Macintosh, and Mac are either registered trademarks or trademarks of Apple Inc. in the United States and/or other countries. Certain other product names, brand names, and company names may be trademarks or designations of their respective owners. 041309d