

Xrio UBM Manual May 2008

Configuring The UBM

Your UBM appliance was shipped with the following items in the box.

- The UBM unit
- AC Power Cable
- CAT 5 Network Cable
- Rack-mount kit (UBM models 1000, 1500, 2000, and 3000 only)

Verify that all items are present before installing and configuring the UBM.

Important Considerations

Prior to configuring the UBM appliance, verify that you have access to all of the following.

- A minimum of eight contiguous public IP addresses. This is a /29 address block which uses a subnet mask of 255.255.255.248.
- A firewall that is configured with an IP address that operates within the range assigned to the ISP link(s) you intend to connect to the UBM appliance.
- The firewall's default gateway points to the router.

NOTE: Clearing The ARP Cache

The UBM appliance will not route traffic until the ARP caches on both the firewall and the router have been cleared. The simplest way to reset the ARP caches is to reboot each of these devices.

Installation and setup

To begin the physical installation process for the UBM appliance, connect the AC power cable to the device and plug it into a functional wall outlet. Turn on the UBM appliance, using the power switch, located on the rear panel of the UBM (excludes UBM 200 and UBM 400).

If you have purchased a 1U UBM, follow the mounting instructions included with the Rack Mount Kit.

Connect the CAT network cable supplied with the UBM appliance to the last numerical port (i.e., the highest-numbered port) on the front panel of the appliance. This port has a special permanent configuration and is the only port from which the UBM appliance will accept management

information. Connect the remaining cable end to your Network Management Workstation.

The UBM offers a platform-independent Web-based management interface. Your Network Management Workstation should be loaded with the current version of a common Web browser. Internet Explorer, Firefox and Opera are all known to work correctly with the UBM management interface. Other browsers may or may not function properly and have not been tested with the UBM management interface by Xrio. The screen resolution of your network management workstation should be set to no less than 1024 x 768.

Initial Configuration

On the network management workstation, select Control Panel > Network Connections. Right-click on the LAN icon and select Properties. Select TCP/IP from the list and select Properties. Use the following IP address. Enter 172.31.3.2. Do not use any other IP address for this configuration. Use 255.255.255.0 as the Subnet Mask. Apply the changes and close the Network Connections window.

NOTE: Private IP Address

The private IP address you've assigned will disable normal Internet connectivity for the Network Management Workstation. Once the UBM configuration process is complete, you may re-assign the workstation's normal operating IP address. You will need to modify the Network Management Workstation's IP address if you need to repeat the initial configuration steps.

Open your web browser. To access the UBM's management interface, type <https://172.31.3.1> in the browser's location bar. Note that you must use the secure HTTP protocol to access the unit.

Enter the default login and password in the login window. The default login and password are:

Username: admin

Password: password

The UBM's configuration will be initialised and will display the UBM management interface on the Network Management Workstation.

NOTE: Connection Difficulties

If the UBM does not respond, verify that the management workstation can communicate with the device by performing a ping test on the device IP address. Verify that the cables are connected properly at each end and that the initial configuration information has been entered properly.

Dashboard

The UBM management interface displays information about itself and is presented on the management interface dashboard. The dashboard will always display the UBM's version information, IP addresses, serial number and historical link usage information.

Tour

This section will review the basic appearance of the UBM management interface and introduce descriptive terminology that will be used throughout this manual.

Tab Bar:

The **Tab bar** is located immediately adjacent to the Xrio logo at the top of the UBM management interface. The Tab bar contains the following tabbed major menu options:

- **Configure:** This tab enables the administrator to access all configuration functions. These settings control the UBM's performance.
- **Monitor:** This tab enables the administrator to monitor activity on all configured links.
- **Settings:** The Settings tab contains customisable account information settings, and provides access to device maintenance and upgrade functions.

Groups

Each tab also contains related actions in the **Groups** panel, on the left side of the management interface. Each group may contain several related configuration tools. Selecting a group by clicking it with the mouse will reveal all related tools in the group. To activate a particular tool or function, select it with the mouse.

Action Menu

Each group within a tab also contains a set of actions that can be performed when a particular configuration tool is active. The **Action Menu**, located directly underneath the Tab bar, indicates the range of actions that can be performed within the selected configuration tool.

Data View

The **Data View** appears beneath the **Action Menu** and shows all information that is related to the selected **Group** tools. For example, if the Interfaces tool is selected, the Data View will show all available interfaces. Access an individual item in the Data View by selecting it with the mouse. The properties of the selected item will be displayed in the

Properties Panel below the Data View. Hovering the mouse over an item will also enable the **Edit** function for the item being reviewed.

Properties Panel

The **Properties Panel** shows the properties of an item selected in the Data View. Configuration information is entered and edited in the Properties Panel. When a new configuration is complete, or an existing configuration has been changed, the changes must be applied. The **Apply Button** is located at the base of the Properties Panel.

NOTE: Applying Changes

Applied changes are temporary; a change to a configuration does not permanently save the new configuration information. Temporary configurations will be lost if power is interrupted to the UBM appliance. To save a configuration change permanently, select Commit changes in the upper right corner of the interface, on the **Action Menu**.

Configure

This section introduces the **Groups** that reside in the **Configure** tab. These functions determine how the UBM will operate, identify connections to and from itself, and manage traffic.

Interfaces

The **Interfaces Group** enables the administrator to add and configure links to the UBM appliance. A link is a physical connection through which packets are exchanged with an ISP. Depending upon the model you have purchased, the UBM appliance will accept between 2 and 32 links.

Link

Links are the ISP connections that connect directly to the UBM appliance. To route data over these links you must give the UBM appliance some information about the link type and the IP addresses that your ISP has provided.

To create a new link, activate the **Configure** tab and select **Interfaces** from the **Groups** panel on the left side of the management interface. Select **Link** from Interfaces Group and then from the **Action Menu**, choose **Add A Link**.

The **Properties Panel** will activate and enable you to provide information about the link. To configure a link, supply the following information:

Port: Identify the port on the front panel of the UBM appliance that your new link is attached to.

Bandwidth: Identify the upload and download speeds of the new link.

Interface type: Identify the link's interface type. The UBM appliance supports Static, PPPoE and Dynamic (DHCP) links. If a link is defined as "static" or "PPPoE" additional configuration information is required. See below.

Health Check Address: Enter the address of a reliable Internet host or a host on your network. Normally, a DNS server or other highly available host is used. The UBM appliance will use this address to verify its ability to communicate.

Additional Configuration For Static Links

If you have identified a link as "static" you must supply additional configuration information. Select the **IP Addressing** tab, found on the **Properties Panel**, and enter the following:

Endpoint IP: This IP address will be applied to the UBM appliance. It should be a publicly routable address and will be used for remote management and Network Address Translation (NAT).

Gateway IP: Enter the router's address.

Subnet: Enter the correct subnet mask. The UBM appliance will use this information to identify available IP addresses.

Additional Configuration For PPPoE Links

A PPPoE link enables the UBM appliance to connect and authenticate to the ISP directly. A PPPoE link is useful if your ISP did not allocate multiple public IP addresses to your network.

If you have identified your link as "PPPoE", select the PPPoE Properties tab from the Properties Panel and enter the following additional information:

User Name: Enter your user name

Password: Enter your password

Auth Type: Enter the authorisation type you'll be using.

When you are satisfied with the configuration information you've entered, select Apply this Link. Once applied, the link will appear in the Data View. You may edit the link configuration by selecting the floating Edit command that appears when the link is highlighted in the Data View.

Remember: Your link configuration is temporary until you save it to the UBM's permanent configuration file. The Commit Changes option is located in the top right corner of the UBM management interface on the Action Bar.

Virtual Tunnels

Many organizations use Virtual Private Networks (VPN) to carry sensitive data between sites, to transfer data between external and internal networks, or to transmit packets that are otherwise unroutable. A virtual tunnel is a dedicated pathway between two end points. Network devices at each end of the tunnel establish a connection between themselves. No other device shares this connection while it is active.

Usually, a virtual tunnel depends upon a single physical path. For an organization that uses multiple data lines, a virtual tunnel could not exceed the size of the physical link. If that link went down, the virtual tunnel would also go down.

The UBM appliance allows virtual tunnels to span more than one physical link without expensive upgrades to infrastructure at either location. In this

setup, a UBM appliance sits outside the firewall at each site to manage load balancing for the virtual tunnel.

As applications or data volumes grow in size, additional bandwidth can be added easily, eliminating bottlenecks and congestion between tunnel sites. Time-sensitive traffic, like Voice over IP and video conferencing benefit because a load-balanced tunnel setup allows bandwidth to be allocated to these services when and where they're used.

To add a virtual tunnel, from the **Configure tab**, select **Interfaces | Virtual Tunnel** from the **Groups** panel on the left side of the management interface. Select **Add a Tunnel** from the **Action Menu**. This will activate the **Properties Panel** in the lower portion of the management interface.

Provide the following information to establish the virtual tunnel:

Local Endpoint: Identify the link to which the tunnel will apply. If you wish to edit the name of the tunnel, select the **Edit** link from the gray bar above the **Properties Panel** and assign a name to the tunnel. If you do not assign a name, the UBM appliance will provide a default numerical name. If you intend to create several tunnels, or more than one person administers your network, you may wish to provide meaningful names for each virtual tunnel, such as one that identifies the tunnel's other end point.

Remote Endpoint: This is the routable IP address of the remote device with which the UBM appliance will communicate.

Bandwidth: Assign download and upload limits to the tunnel. This bandwidth will be designated for use by this tunnel only and will not be available to other devices that share the link, even when this tunnel is not transporting data.

Local Virtual IP: Identify the local virtual IP address of the device that will send or receive data through this tunnel.

Remote Virtual IP: Identify the virtual IP address of the remote device that will send or receive data through this tunnel.

Transparent

The UBM appliance can be installed transparently into the network. In this configuration, the UBM appliance does nothing with incoming and outgoing packets, except to route them to their intended destination. Transparent mode requires no configuration changes to the network. Traffic from the network – usually from the firewall – passes through the UBM appliance. In this configuration, the UBM appliance can be removed entirely while the administrator resolves topology or planning issues without disrupting network activity.

To create a transparent link, activate the **Configure** tab and select Interfaces>Transparent from the Groups panel on the left side of the management interface. From the **Action Menu**, choose Add A Link. Any existing transparent links will be shown in the Data View.

The **Properties Panel** will activate and enable you to provide information about the link. To configure a link, supply the following information:

Link Name: Select the link's name from the pull-down menu. If you wish to assign a name to the link select edit from the gray bar above the **Properties Panel** and enter a name. If you do not enter a name, the UBM appliance will use the numerical default name it assigned when it created the link.

Port: Indicate the physical port on the front of the UBM appliance to which the transparent link is connected.

IP Addresses: Select the IP address associated with this link. To select multiple IP addresses, press the CTRL key while you select multiple links.

When you are satisfied with the configuration of the transparent link, click Apply this Interface in the lower right corner of the **Properties Panel**. As with other configuration changes, the new transparent link will be temporary, unless it is saved into the permanent configuration file. To save a configuration, select Commit Changes in the upper right corner of the **Action Menu**, once the change has been applied.

LAN

The UBM appliance can act as the default gateway on one or more local area networks. To use the UBM appliance as a default gateway, a LAN interface must be added to the UBM's configuration.

In this configuration, the specified port on the UBM appliance is connected directly to the network switch, which in turn, is connected to the Local Area Network devices.

To create a LAN Interface, from the **Configure tab**, select **Interfaces | LAN** from the Groups panel on the left side of the management interface. From the **Action Menu**, select Add an Interface. The **Properties Panel** will activate. Provide the following information about the new interface:

LAN Interface: Identify the physical port on the UBM to which the network switch or router is connected. The interface will provide a pull-down menu that shows all ports.

Destination Subnet: Enter the network address of the LAN and include its CIDR designation.

Endpoint IP: Assign an address to the UBM appliance. The devices on the LAN will use this address as their default gateway.

When you are satisfied with the configuration, select Apply this Interface at the bottom right corner of the **Properties Panel**. The configuration will be temporary until it is saved into the appliance's permanent configuration file.

Entities

Interface Teams

An **Interface Team** is a logical group of interfaces. There are no limits to the number of Interface Teams that can be created. A routing policy, known as an algorithm, must be assigned to each Interface Team. The algorithm determines how the interfaces within the logical group will handle the traffic.

The UBM appliance supports four different routing algorithms:

Distribute Connections: Data sessions will be assigned to a specific link by the UBM appliance at the time they are initiated. The link assignments are made using a weighted Round Robin system.

Sticky Connections: Similar to Distribute Connections. With a "sticky connection" the UBM appliance will remember the destination and the selected link. Future sessions will connect to the destination using the original link.

Simple Bonding: Simple Bonding usually requires two UBM appliances. Packets are distributed over multiple links simultaneously and provides access to the links' aggregated bandwidth.

Advanced Bonding: Similar to Simple Bonding. Advanced Bonding is used in circumstances where the quality or reliability of a link fluctuates.

A common configuration might have four links, two of which will be used to route regular Internet traffic and the remaining two will be aggregated to support a VPN connection. To create this setup, define two **Interface Teams** and specify the required routing algorithm. These teams can also be used to specify traffic flow.

To create an **Interface Team**, select the **Configure tab**. From the **Groups** menu on the left side of the management console, choose **Entities**, then **Interface Teams**. From the **Action Menu** choose **Add a Team**. This will display the **Properties Panel** at the bottom of the management console, to which the following information should be entered:

Algorithm: Choose the routing algorithm the Interface Team will use.

Backup Team: A Backup Team is a second logical group of links that should route traffic if the primary Interface Team fails. All links on the primary Interface Team must fail for the Backup Team to take over.

Team Type: In most cases, the default "Link" value will be selected. **Virtual Tunnel Teams** are used only with bonded links.

Included Links: A list of available links will be shown in the **Properties Panel**.

To include a link in an Interface Team, toggle the check box next in the **Include** column at the left of the interface list. If not all links show within the **Properties Panel**, use the **Expand List** option to show the full list of available links.

When you have identified all links, use the **Collapse List** option to return the display to its normal appearance. Choose **Apply this Team** to activate the Interface Team.

Address Aliases

Dealing with a number of IP addresses can be confusing; it can also lead to configuration errors that negatively affect the performance of a link. An Address Alias avoids this confusion by represents an IP address by name. Using an Address Alias is analogous to using a host name to identify a device instead of an IP address. Address Aliases are often used for advanced configurations.

To create an Address Alias, select the **Configure tab**. From the **Groups** menu on the left side of the management interface, choose **Entities**, then **Address Alias**. From the **Action Menu**, select **Add an Entity**, and supply the following information in the **Properties Panel**:

Alias Type: The **Alias Type** can be a Source Subnet, Interface Endpoint, Internal Server, Remote IP Address, or a Remote Subnet.

After identifying the Alias Type, supply the address of the interface. In the case of an **Interface Endpoint**, you will also need to identify the link and the associated IP address. To given the **Address Alias** a name, choose the **Edit** link in the gray bar above the **Properties Panel**. If you do not supply a name, the UBM management interface will assign a numerical name to the **Address Alias**.

Service Definitions

The UBM appliance maintains a list of common IP services for use with Address Aliases. Most common services and protocols have been predefined for you, however you may need to create your own **Service Definitions** for custom services you might use.

Typical examples of these would be Voice over IP or Video Conferencing systems, please refer to the application vendor for the correct protocol definitions. The default set of system services cannot be edited, but new services can be added.

To add a new service definition, select the **Configure tab**. From the **Groups** menu on the left side of the management interface, select **Entities**, then **Service Definitions**. Select **Add a Service** from the **Action Menu**. This will activate the **Properties Panel**. Supply the following information for a new service:

To edit the name of the new service, choose the **Edit** link in the gray bar above the **Properties Panel**. If no name is supplied, the UBM management interface will assign the default name **New Service**.

Description: Enter a brief text description of the new service.

Protocol: Identify the protocol number(s) associated with this service. Use the [+] and [-] links to add or subtract data. Enter data in the text box provided. Identify the protocol as TCP or UDP and provide the port number on which the service operates. If a service operates on both TCP and UDP, make separate entries for each service and port.

Routing Policy

Once the proper entities have been created, routing policies can be applied to traffic managed by the UBM appliance. The UBM appliance accepts four types of routing policies. They are:

Outbound Policies: Outbound policies apply to traffic that is leaving the network via the UBM appliance. As traffic passes through the UBM device, the most specific policy will be applied and then routed to the external network. Policies can be created from any combination of Source IP, Destination IP and Service and then finally assigned to a previously defined Interface Team. This granular approach can allow you to build highly flexible routing policies.

Inbound Policies: Inbound policies are required for traffic that is destined in to your network. Inbound policies are applied based upon the link that carries the traffic, its network destination and the protocol contained in the packet. For example, the UBM appliance can redirect all inbound HTTP traffic to a private address inside the network.

An Inbound Policy is required when:

- Transparent Mode is not set on a link

- Transparent Mode is set but you want to route inbound traffic that is destined to a secondary link
- It is desirable to route traffic to a server that is related to a defined LAN Interface

Intelligent DNS: The UBM appliance can perform DNS functions for multiple domains and can use multiple links to route traffic in the most efficient way without disrupting established sessions.

Static Routes: A static route forwards traffic to a pre-determined destination. Typically, a static route is used when a defined LAN Interface requires traffic to be routed to another upstream router that may have intelligence about other network topologies.

When a static route policy has been assigned on the UBM appliance, packets received on the specified ports will always be sent to the device identified in the policy. If the device becomes non-responsive, the packets directed to it will be lost.

Outbound Policies

To add an Outbound Policy, select the **Configure tab**. From the **Groups** menu on the left side of the management interface, select **Routing Policy**, then **Outbound Policies**. The management interface will provide a list of all existing outbound policies.

From the **Action Menu** select Add a Policy. In the **Properties Panel** at the bottom of the management interface, supply a name for the policy by selecting the Edit link in the gray bar above the **Properties Panel**. Once you have assigned a name, choose **Save**.

Choose the **Source address** to which the policy will be applied. Alternately, if the policy is global, choose **Any**.

Provide the **Destination address** to which the policy should apply. If the policy applies to destinations universally, choose **Any**.

Identify the **service** to which the policy should apply by selecting it from the pull-down menu, which shows all known services.

Choose the **Interface Team** to which the policy should apply, using the pull-down menu that shows all known Interface Teams.

Choose the **Translate** method for the policy by selecting the **Auto** (default), **Manual**, or **Disable** button.

When you are satisfied with the policy configuration, select **Apply this Policy**. Remember, this application is temporary until it is saved in the UBM configuration file. If the policy is not saved, it will be lost if the UBM appliance loses power for any reason.

Inbound Policies

To create an **Inbound Policy**, select the **Configure** tab. From the **Groups** menu on the left side of the management interface, select **Routing Policy**, then **Inbound Policies**. The management interface will provide a list of all existing inbound policies.

From the **Action Menu** select **Add a Policy**. In the **Properties Panel** at the bottom of the management interface, supply a name for the policy by selecting the **Edit** link in the gray bar above the **Properties Panel**. If you do not assign a name, the UBM appliance will assign a default name to the policy. Once you have assigned a descriptive name, choose **Save**.

Choose the **Link Name** to which the Inbound Policy will apply. Choose the **Destination Endpoint** to which the policy will apply. This is an IP address that belongs to a device in your network.

Choose a **Redirected Endpoint**. The UBM appliance will provide a list of known IP address aliases.

Choose the **Destination Service** to which the inbound policy will apply. The UBM appliance will provide a pull-down menu containing a list of all known services. If the policy applies to all services, choose **Any**.

Choose a **Redirected Service**, which will be provided by the redirected endpoint. If the inbound policy applies to all services, choose **Any**.

Intelligent DNS

When managing multiple links from different ISPs, the UBM appliance must correctly navigate DNS and other service requests according to the specified load balancing parameters. To ascertain that service requests are received, acknowledged and responded to properly, the UBM appliance must be configured with DNS information for all ISP links it manages.

At times, the UBM appliance may receive a DNS request over one of the WAN links it manages, but load conditions dictate that the subsequent information response traverse a different link. If server mappings on the UBM appliance are set up properly, the UBM appliance can manage this data exchange with no problems.

To illustrate:

The UBM appliance receives a DNS request from the WAN1 link, which it forwards to the DNS server. The DNS server formulates a response and

sends it back to the UBM appliance. The UBM appliance checks the load on all of the links it manages and notes that WAN2 link has less traffic and would provide a faster response.

The UBM appliance forwards the DNS response back to the requester via the WAN1 link, (the same link that delivered the request) so as not to confuse the requester, which is expecting a response from the WAN1 link. The UBM appliance's response indicates that the correct host can be found using the less congested WAN2 link.

The requester then uses the DNS information to request a service from a host on the internal network, via the WAN2 link. The UBM appliance responds to the request on the WAN2 link.

To configure the UBM appliance to operate like this, it needs to have DNS information about all of the WAN links it manages. First, DNS requests for the domain must be directed to the UBM appliance.

Static Routes

To create a static route, select the **Configure** tab. From the **Groups** menu on the left side of the management interface, select **Routing Policy**, then **Static Routes**.

To add a static route, select **Add a Route** from the **Action Menu** at the top of the management interface.

Use the **Edit** link in the gray bar above the **Properties Panel** to assign a name to the static route. If you do not assign a name, the UBM management interface will assign a default unique name to the new static route. Click Save to save the new policy.

Using the drop-down menu in the Interface field, select the physical **Port** on the UBM to which the static route will apply.

Enter the **Destination subnet**, including its CIDR designation. (e.g., 198.168.1.0/24).

Enter the **Next Hop** (gateway) address that traffic should be routed to.

Management

The UBM appliance offers several management options that will grant or restrict access to the appliance from a remote host. The management interface enables you to restrict or allow HTTPS and SSH access, and Ping responses from the Internet.

Remote Access

The remote access permissions are granted or denied using the Management group on the left side of the management interface. To

configure remote access, select Remote Access. The management interface will show three check boxes:

Allow HTTPS Management from the Internet

Allow SSH Management from the Internet

Allow PING Response from the Internet

Check any or all of the boxes to permit the specified remote access protocol. Uncheck any or all of the boxes to disallow the specified remote access protocol.

To permanently save these changes, select **Commit Changes** from the **Action Menu**.

Monitor

The Monitor tab allows you to receive activity reports on all configured links. The UBM appliance creates a visual representation of each link. The graphs indicate each link's operational status and the amount of traffic in kb/sec each link is carrying at a given instant.

Reporting Analysis

The Reporting Analysis group contains two items: Live Link Monitor and PPPoE Link Status.

Live Link Monitor

To monitor the activity on all configured links, select the **Monitor tab**. From the **Groups** menu on the left side of the management interface, you may select either the **Live Link Monitor** or the **PPPoE Link Status**. The UBM appliance will create a status graph for each active link. The X-axis will update dynamically each second. You may mouse over the X-axis at any point and see a pop-up display of the upload and download speed, as well as the number of packets passed at any given instant on the graph. You may stop instantaneous monitoring by selecting **Stop Monitoring**, above the graphical display.

PPPoE Link Status

Settings

The **Settings tab** allows you to create users, accept firmware upgrades, and upload or download configuration files.

User Accounts

To create a new user account, select the **Settings tab**. From the **Groups** panel, select **Settings**, then **User Accounts**. From the **Action Menu**, select **Add a User**. This will enable the **Properties Panel** at the bottom of the UBM management interface.

Enter a username for the new account. Enter a valid email address for the new user account. Provide a secure Password for the new user account and select the access level granted to the user. Only those users with Administrator rights can make configuration changes to the UBM appliance.

Firmware Upgrades

To add a firmware upgrade to the UBM appliance, select the **Settings tab**. From the **Groups** panel, select **Settings**, then **Firmware Upgrade**. Using the **Browse button**, select the appropriate file and **Send** it to the UBM appliance.

Configurations

You may upload or download configuration files to the UBM appliance. To access the **Configuration** function, select the **Settings tab**. From the **Groups** panel, select **Settings**, then **Configurations**.

To download the UBM appliance's current configuration file, press the **Download Configuration** button on the UBM management interface. To upload a new configuration file, use the **Browse** button to select the new configuration file from the local host and press **Send**.

Select **Commit Changes** to write any changes into the UBM appliance's permanent configuration file.